# Вимоги до системи користувацьких інтерфейсів (B2B2C-платформи), в ПрАТ «УКРФІНЖИТЛО»

## ТЕРМІНИ, СКОРОЧЕННЯ ТА ЇХ ВИЗНАЧЕННЯ

| Термін/скорочення | Визначення |
|---|---|
| Система (B2B2C-платформа) | Єдиний інформаційно-програмний комплекс, що реалізує бізнес-модель взаємодії «Бізнес-для-Бізнесу-для-Споживача». Система об'єднує архітектуру бази даних, внутрішню логіку (Backend) та розрізнені користувацькі інтерфейси (Мобільний додаток та Веб-інтерфейс) для забезпечення наскрізного процесу взаємодії між Партнерами та Клієнтами. |
| Веб-кабінет | Система користувацького інтерфейсу для Партнерів (юридичні особи: банки, СОД, страхові компанії, ін.). *Окремий функціонал для Клієнтів (фізичних осіб) може бути реалізовано в веб-кабінеті.* |
| Мобільний додаток | Система користувацького інтерфейсу для Клієнтів (фізичних осіб). |
| BankID | Сервіс електронної ідентифікації та автентифікації користувачів, який дозволяє підтвердити особу онлайн через банк, у якому людина вже ідентифікована. |
| BPM | Система управління бізнес-процесами за стандартами BPM. |
| Deep link (deeplink) | Спеціальне посилання, яке веде не на головну сторінку, а безпосередньо на конкретний екран, розділ або дію всередині веб-сайту чи мобільного застосунку. |
| HRM | Програмне забезпечення для ведення кадрового обліку. |
| Inline-валідація | Перевірка введених користувачем даних, яка відбувається безпосередньо під час заповнення поля форми або одразу після виходу з нього, без перезавантаження сторінки і без відправки всієї форми (технологія, що одразу підказує, що дані введені некоректно. |
| 2FA | Двохфакторна авторизація. |
| БД | База(и) даних. |
| АБС Б2 | Автоматизована банківська система Б2 – основна система обліку операцій та формування звітності ПрАТ «УКРФІНЖИТЛО». |
| ДІЯ | Портал Дія з відповідними механізмами обміну. |
| ДСТУ | Державні стандарти України. |
| ЕЦП | Електронний цифровий підпис. |
| КЕП | Кваліфікований електронний цифровий підпис. |
| НБУ | Національний банк України. |
| ПЗ | Програмне забезпечення. |
| СЕД Clever Forms | Система електронного документообігу та зберігання кредитних справ. |
| СУБД | Система управління базами даних. |
| Технологія Liveness | Технологія перевірки, що підтверджує, що перед системою жива реальна людина, а не фото, відео, маска чи інша підробка. |
| Товариство, ПрАТ « УКРФІНЖИТЛО» | ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «УКРАЇНСЬКА ФІНАНСОВА ЖИТЛОВА КОМПАНІЯ». |
| ФОП | Фізична особа – підприємець. |
| Партнер (B2B-користувач) | Юридична особа, з якою укладений договір про отримання, обробку, обмін даними / документами. |
| Клієнт (B2C-користувач / Кінцевий споживач) | Фізична особа, яка зареєстрована в Системі (подала заявку на участь у програмі єОселя) та використовує її функціонал для оформлення та подальшого обслуговування за іпотечними (або іншими фінансовими продуктами) в рамках програми єОселя. |

## Мета та загальний опис концепції

Призначенням Системи є створення єдиного B2B2C-сервісу (платформи), що об'єднує функціонал для взаємодії між Партнерами (юридичними особами: банки, СОД, страхові компанії, ін.) та Клієнтами (фізичними особами), забезпечуючи наскрізні бізнес-процеси оформлення та супроводу іпотечних угод (або інших видів фінансових продуктів).

Головною метою Системи є цифровізація та комплексна автоматизація процесів супроводу/ формування кредитних угод, зокрема:

- виконання нефінансових зобов'язань (ковенант);
- створення, збору, підписання та опрацювання документів кредитної справи;
- забезпечення дистанційної взаємодії клієнтів з Товариством та банками-партнерами без необхідності фізичної присутності;
- здійснення ідентифікації та верифікації клієнтів Товариства без необхідності фізичної присутності.

Система має забезпечувати надійне та безпечне підключення користувачів із застосуванням двофакторної автентифікації (2FA), а також обов'язкове логування дій користувачів для цілей контролю та аудиту.

Система надає клієнтам можливість:

- дистанційно надавати документи за для виконання нефінансових зобов'язань за кредитними угодами;
- переглядати актуальну інформацію щодо стану та умов своєї кредитної угоди;
- отримувати push-повідомлення та нагадування про події, дії або зобов'язання, що мають бути виконані у визначені строки.

Система передбачає автоматизацію повного циклу процесів, пов'язаних із виконанням нефінансових зобов'язань та формуванням кредитної справи, документообігом, зокрема за такими сценаріями:

1. **Отримання та обробка даних**
   - автоматизоване отримання даних з державних та інших реєстрів (у тому числі через інтеграційні платформи та облікової системи Товариства);
   - ініціація отримання даних на підставі подій або встановлених бізнес-правил.
2. **Формування та підписання документів**
   - формування електронних документів на основі отриманих даних;
   - підписання сформованих документів клієнтом та або підписання обома сторонами із використанням КЕП.
   - зберігання та відображення сформованих / підписаних документів.
3. **Передача та опрацювання документів/отриманих даних**
   - автоматичне направлення підписаних документів до Товариства та/ або до іншого контрагента;
   - використання документів як підтвердження виконання відповідних зобов'язань;
   - подальша валідація, перевірка та опрацювання документів, збереження документів відповідно до внутрішніх процесів Товариства.

Для процесів, щодо яких автоматизоване отримання даних з реєстрів є неможливим, система передбачає:

- завантаження клієнтом електронних копій документів у форматі PDF;
- підписання завантажених документів КЕП;
- автоматичну передачу документів до систем Товариства для перевірки та подальшого опрацювання (можливість підтвердження документу/підписання зі сторони Товариства за потреби).

4. **Категорії користувачів та модель доступу**

4.1. Система має передбачати наявність користувацьких інтерфесів для трьох основних категорій користувачів:

- **Клієнти (фізичні особи**) — кінцеві споживачі послуг, які виконують нефінансові зобов'язання, формують / отримують / підписують документи та отримують повідомлення. Для цих користувачів передбачається наявність мобільного застосунку (Android, IOS), back-система, якого пов'язана з системою веб-кабінету. Певний функціонал додатково може бути реалізовано на веб-платформі.
- **Партнери** — юридичні особи, ФОП та державні органи, залучені до процесів формування, підтвердження або перевірки документів / отриманих даних.
- **Адміністратори** — співробітники ПрАТ «УКРФІНЖИТЛО», які здійснюють налаштування процесів, контроль виконання та опрацювання результатів.

4.2. Доступ до функціональних можливостей системи регулюється гнучкою рольовою моделлю. Функціонал для партнерів є динамічним та налаштовується відповідно до конкретного бізнес-процесу або сценарію взаємодії. Адміністратори та партнери працюють виключно в межах визначених ролей, що обмежують або розширюють доступ до інструментів обробки документів, електронних форм та workflow-етапів.

5. **Робота з партнерами та третіми сторонами**

5.1. Веб-кабінет повинен підтримувати можливість залучення до бізнес-процесів партнерів та третіх осіб, зокрема:

- страхових компаній;
- суб'єктів оціночної діяльності;
- ФОП та інших учасників процесу.

5.2. Партнери можуть бути інтегровані у відповідні **workflow-сценарії**, з визначенням їх ролей, прав доступу та відповідальності на окремих етапах процесу.

**6. BPM-модуль та управління процесами**

**6.1.** Система має включати **BPM-модуль**, який забезпечує:

- самостійну побудову та модифікацію бізнес-процесів;
- налаштування етапів та проходження оформлення угоди;
- налаштування маршрутів документів і сценаріїв виконання ковенант;
- управління подіями, строками та статусами процесів;
- моніторинг виконання та оперативне реагування на відхилення;
- можливість використання у процесах зовнішніх сервісів (як для отримання інформації, так і для відправки), та обробки отриманої інформації у власних процесах;
- можливість отримання інформації про результати роботи процесів, що налаштовані у BPM-модулі.

6.2. Процеси можуть виконуватися як за участю третіх сторін, так і повністю автоматизовано — з використанням алгоритмів, правил обробки подій та інтегрованих інформаційних систем. У межах реалізації Системи допускається можливість розгляду інтеграції з готовим BPM-продуктом

**7. Інтеграційна складова.** Веб-кабінет та мобільний застосунок повині мати можливість інтегруватися з багатьма зовнішніми сервісами, і мати власний інтеграційний рівень.

**8. Автентифікація:**

Передбачається комбінована модель автентифікації:

- Клієнти (фізичні особи): Дія / BankID / логін-пароль;
- Партнери: КЕП / логін-пароль;
- Адміністратори (співробітники): Active Directory (AD\Entra ID);

Додаткові вимоги:

Система має бути реалізована як конфігурована система, що дозволяє додавати нові процеси, форми, поля та правила без зміни (або з невеликими змінами) програмного коду. Основний функціонал повинен бути побудований на BPM-рушії з можливістю подальшого розширення процесів через адміністративний інтерфейс. Система має підтримувати розширювану модель даних, налаштовувані ролі та відкритий API для майбутніх інтеграцій. Усі можливі сценарії другого етапу повинні мати технічну можливість реалізації через механізми налаштувань та підтримки, без модифікації ядра платформи.

## Функціональні вимоги

| **Категорія користувача: Клієнт** | **Обов'язковість для мобільного додатку** | **Обов'язковість для веб версії** | **Етап впровадження** |
|---|---|---|---|
| **Автентифікація та авторизація** | | | |
| 1. Система повинна забезпечувати автентифікацію користувачів через Дія, НБУ, BankID, після проходження авторизації клієнту формується обліковий запис з логіном та паролем. Після автентифікації повинен застосовуватись стандартний логін-пароль. У випадку, якщо користувач не проходив авторизацію у системі більш ніж деякий період (окрема змінна), система має вимагати повторну автентифікацію клієнта. Якщо клієнт не заходив до додатку більш ніж n днів, система має заново пропонувати пройти ідентифікацію клієнта через ДІЯ/BankID, але авторизувати на поточному обліковому записі. У випадку постійної присутності клієнта у додатку, система завжди пропонує авторизуватися через логін та пароль. | так | так | Перший етап |

| | | | | |
|---|---|---|---|---|
| 2. | Можливість забезпечення багатофакторної автентифікації (MFA) для всіх користувачів. | так | так | Перший етап |
| 3. | Заповнення/оновлення даних в картці клієнта під час його автентифікації через Дія, НБУ, BankID. Оновлення даних з облікової системи Товариства. | так | так | Перший етап |
| 4. | Оновлення в картці клієнта даних з облікових систем по клієнтам позичальникам(з урахуванням інформації в специфікації OpenBank API). | так | так | Другий етап |
| 5. | При першому вході в систему пошук та відображення інформації по:<br>- Заявках клієнта<br>- Угодах клієнта, що на балансі компанії (включно з усіма його зобов'язаннями)<br>- | так | ні | Перший етап |
| 6. | При першому вході в систему<br>- інформація по угодах клієнтах, що на балансі банків-партнерів<br>- пошук та відображення інформації, що отримана через Openbank API. | так | ні | Другий етап |
| 7. | Відновлення доступу повинно відбуватись через нову автентифікацію через Дія, НБУ, BankID. | так | так | Перший етап |
| 8. | Система повинна визначати роль та доступний функціонал залежно від та наявних даних про клієнта.<br>Перший етап: клієнт Товариства, які мають кредит, громадянин України, який планує отримати кредит, або який вже подав заявку на отримання через додаток ДІЯ;<br>Другий етап: клієнт банку-партнера. | так | так | Перший, другий етап |
| 9. | Під час онбордінгу та автентифікації в системі, користувач повинен мати можливість заповнення та оновлення анкети-опитувальника фінансового моніторингу. | так | так | Перший етап |
| 10. | Підтримка технології Liveness. Використання планується тільки на етапі онбординга, або у випадку повторної ідентифікації клієнта. | ні | ні | Другий етап |
| 11. | Підтримка пристроїв біометричної авторизації користувача у системі (Face ID / Windows Hello, Fingerprint / Touch ID). | так | ні | Перший етап |
| **Основний функціонал** | | | | |
| 1. | Система повинна забезпечувати формування документів з заздалегідь доданих шаблонів, мати змогу виводити сформований документ на перегляд та забезпечувати підписання КЕП як сформованих документів що наповнюється даними з реєстрів/інтегрованих систем так і документів, які надаються користувачем через інтерфейс. | так | так | Перший етап |

| | | | |
|---|---|---|---|
| 2. Система повинна забезпечувати збір і обробку **структурованих даних** із різних державних реєстрів та джерел. На основі цих даних повинні формуватися документи у стандартних шаблонах (PDF, DOCX). | ні (обробка на BACK) | так | Перший етап |
| 3. Користувач повинен мати можливість завантажувати документи у форматах .jpg, .pdf, .png через інтерфейс (можливість конвертації через власні бібліотеки чи через сторонній сервіс у PDF) та можливість накладання власного КЕП на такі документи. | так | так | Перший етап |
| 4. Система забезпечує введення даних користувачем у форми та можливість налаштування валідації даних , та потреби у такій валідації (тип/формат на етапі введення). | так | так | Перший етап |
| 5. Забезпечується відображення статусу обробки сформованих , або завантажених документів/інформації /даних зазначених користувачем/партнером. | так | так | Перший етап |
| 6. Користувач повинен мати можливість надавати доступ до своїх документів іншим користувачам цього ж додатку, відправляти запити на приєднання та шерингові запити. Запити на приєднання або опрацювання документу мають пересилатися або через визначений месенджер, або через електронну пошту. У випадку, коли громадянин, якому надали посилання не є користувачем системи, обов'язкова автентифікація наявними механізмами. | так | так | Другий етап |
| 7. Система повинна надавати можливість перегляду інформації:<br>- по заявках;<br>- по рахунках (рух коштів, формування виписок);<br>- по доступних акредитованих будинках (квартирах);<br>- по угодах та усіх її складових (кредитній угоді, угоді забезпечення, угоді страхування та інш.);<br>- по ідентифікаційним даним користувача/опитувальнику (у тому числі для своєчасного оновлення).<br>Повинна забезпечувати відображення користувачу статусу угод, заявок, зобов'язань (ковенант) та кредитів, а також надавати перелік необхідних дій у правильній послідовності з відповідним функціоналом для їх виконання. | так | так | Перший етап |
| Можливість сплати по рахунку через deeplink у платіжний додаток банку, або за допомогою OpenBank API. | | так | |

| | | | |
|---|---|---|---|
| Система повинна забезпечувати можливість формування та ініціації платежів клієнта за кредитними зобов'язаннями, включаючи прострочену заборгованість.<br>Можливі сценарії:<br>**Deep Link:** система формує deep link для мобільного застосунку клієнта, передаючи суму та реквізити для оплати.<br>8. **OpenBank API:** система підтримує подальшу можливість ініціювання списання коштів безпосередньо з поточних рахунків клієнта для погашення фінансових зобов'язань за кредитом. | так | | Другий етап |
| 9. Система повинна мати модуль push-нотифікацій. Забезпечувати отримання push-повідомлень з посиланнями та можливістю переходу з цих посилань до відповідного функціоналу(після авторизації).<br>Система повинна підтримувати інтеграцію з **SMS-шлюзами** та популярними **месенджерами** (зокрема Viber та Telegram) для надсилання повідомлень клієнтам та учасникам процесів. | так | так | Перший етап |
| 10. Система повинна забезпечувати візуалізацію електронного документа у форматі друкованої форми. | так | так | Перший етап |
| 11. Користувач повинен мати можливість завантаження підписаних документів на свій пристрій. | так | так | Перший етап |
| 12. У системі повинна бути оболонка для онлайн-чату для комунікації користувача, зі збереженням усієї історії спілкування (глибина збереження по налаштуванням). Також можливість вивантаження історії спілкування до CRM системи.<br>Система повинна забезпечувати ефективну комунікацію між клієнтом та відповідними учасниками процесу, зокрема співробітниками Товариства або партнера, для обміну інформацією, узгодження документів та виконання операцій у межах бізнес-процесів. | так | так | Другий етап |
| 13. Перед накладанням другого, та інших підписів, система має контролювати валідність існуючого підпису на документі, тобто перевіряти чи не було цей документ змінено після накладання минулих підписів. | ні (перевірка на BACK) | так | Перший етап |
| **UI/UX** | | | |
| 1. Для користувачів «Клієнт» має бути доступний функціонал як у мобільному додатку (Android, IOS) та скорочений (цільовий функціонал) у web-інтерфейсі. | так | так | Перший етап |

| | | | | |
|---|---|---|---|---|
| | Опис / розподіл функціоналу у розділі «Базовий функціонал» | | | |
| 2. | Мобільний додаток повинен мати загальний стиль нативного банківського застосунку | так | - | Перший етап |
| 3. | Інтерфейс web-кабінету має бути адаптований під екрани планшетів та мобільних телефонів. | - | так | Перший етап |
| 4. | **iOS (Human Interface Guidelines):** Інтерфейс має відповідати стандартам Apple (навігація через Tab Bar, використання нативних шторкових меню, жестів змахтування назад тощо). **Android (Material Design):** Інтерфейс має відповідати стандартам Google (навігація через Navigation Rail або Bottom Navigation, плаваючі кнопки дій FAB, характерна типографіка та сітки). **Уніфікація бренду:** Попри архітектурні відмінності платформ, логіка користувацьких сценаріїв, колірна гама та тональність бренду мають залишатися єдиними. | так | - | Перший етап |
| 5. | **Правило 3-х кліків:** Доступ до будь-якої ключової функції або розділу додатку має займати не більше трьох кроків (тапів) від головного екрана. **Пріоритет великого пальця (Thumb Zone):** Усі інтерактивні елементи, що часто використовуються (кнопки «Далі», «Підтвердити»), мають розташовуватися в зоні комфортної досяжності великого пальця — у нижній третині екрана. **Зрозумілий статус системи:** Користувач завжди має розуміти, що відбувається. Будь-яка дія супроводжується фідбеком: скелетони (skeleton loaders) під час завантаження даних, лоадери на кнопках, мікровзаємодії (анімації). **Динамічний розмір шрифту:** Підтримка системних налаштувань користувача (якщо у системі виставлено великий шрифт через особливості зору, додаток має адаптувати текст без руйнування верстки). | так | - | Перший етап |
| 6. | Початкове завантаження веб-кабінету (Time to Interactive) має становити **не більше 2 секунд** за умови:<br>- швидкості інтернет-з'єднання користувача **не менше 10 Мбіт/с**;<br>- затримки мережі **не більше 100 мс**; | | так | Перший етап |

| | | | | |
|---|---|---|---|---|
| | - використання настільного браузера (Chrome, Edge, Firefox, Safari) останніх двох стабільних версій;<br>- клієнтського пристрою з обсягом оперативної пам'яті **не менше 8 ГБ**.<br>- Переходи між екранами веб-кабінету здійснюються **без повного перезавантаження сторінки** та мають виконуватися **не більше ніж за 500 мс**, **без урахування часу відповіді зовнішніх інтеграційних систем**. (Взаємодія з АБС Б2 та Clever Forms буде через сервер черг, для синхронних запитів буде обговорюватися швидкість обробки та надання відповідей.<br>Переходи між екранами без повного reload. | ні | | |
| 7. | **Обов'язкові preload / skeleton-екрани**; відсутність "білого екрану".<br>**Контекстні клавіатури:** При фокусі на полі введення має відкриватися відповідна клавіатура (цифрова — для номеру телефону чи картки, з символом @ — для email, звичайна текстова — для ПІБ).<br>**Валідація «на льоту»:** Помилки у формах (наприклад, неправильний формат пароля) мають підсвічуватися одразу під час введення, а не після натискання кнопки «Надіслати».<br>**Маски та автозаповнення:** Використання масок для введення дат, телефонів. Підтримка системного автозаповнення (SMS-коди, збережені адреси, паролі). | так | так | Перший етап |
| 8. | **Нативні жести:** Інтеграція стандартних жестів: *pull-to-refresh* (потягнути вниз для оновлення списку), *swipe-to-delete* (змахнути для видалення елемента), *pinch-to-zoom* (для перегляду фотографій).<br>**Біометрична автентифікація:** Нативна інтеграція Face ID / Touch ID (iOS) та BiometricPrompt (Android) для швидкого та безпечного входу без постійного введення пароля. | так | - | Перший етап |
| 9. | Введені користувачем дані не втрачаються у разі помилок або повторних запитів. | так | так | Перший етап |
| 10. | **Відсутність критичної інформації не лише в кольорі:** Якщо поле заповнене з помилкою, воно має виділятися не | так | так | Перший етап |

| | | | |
|---|---|---|---|
| лише червоним кольором, а й іконкою помилки або текстовим поясненням. | | | |
| 11. **Миттєвий старт (Splash Screen):** Нативна заставка (Splash/Launch screen) з'являється миттєво при тапі на іконку додатку і плавно переходить у головний екран, маскуючи час ініціалізації системи. | так | ні | Перший етап |
| 12. **Оптимізація під різні екрани:** Інтерфейс має однаково коректно відображатися на смартфонах із «чілками», вирізами під камеру (Punch-hole), закругленими кутами та на пристроях із різним співвідношенням сторін (від SE до Pro Max лінійок). | так | - | Перший етап |
| 13. **Мобільний додаток.** **Темна тема (Dark Mode):** Обов'язкова підтримка темної теми на системному рівні. Кольори не повинні бути просто інвертованими; для темної теми розробляється окрема палітра (базові темні відтінки замість чисто чорного для зменшення навантаження на очі). | так | - | Перший етап |
| 14. Мобільний додаток. Заборона принтскрину певних екранів. | так | ні | Перший етап |
| **Категорія користувача: Партнери** | | **Обов'язковість** | **Коментар** |
| **Автентифікація** | | | |
| 1. Система повинна забезпечувати реєстрацію юридичної особи (ФОП) виключно з використанням кваліфікованого електронного підпису (КЕП), який належить відповідній юридичній особі (Компанії). | - | так | Другий етап |
| 2. Під час реєстрації система повинна здійснювати перевірку чинності та коректності КЕП. | - | так | Другий етап |
| 3. Перший користувач, який успішно зареєстрував юридичну особу в системі, автоматично набуває статус адміністратора кабінету Компанії або іншої визначеної ролі з розширеними правами, з можливістю зміни адміністратора компанії або адміністратором системи, або співробітником компанії, з відповідними правами. (підтвердження авторизації з боку бізнес-адміністратора Товариства). Першого користувача має акцептувати адміністратор процесу. | - | так | Другий етап |
| 4. Система повинна забезпечувати можливість первинному користувачу Компанії запрошувати інших працівників до кабінету юридичної особи (заведення користувачів, надання їм ролі, та відправка посилань на електронну пошту). За посиланням користувачі заходять по тимчасовому доступу, з обов'язковим введенням паролів. Термін дії посилання з | - | так | Другий етап |

| | | | |
|---|---|---|---|
| тимчасовим паролем, повинен задаватися адміністратором системи.<br>Система повинна забезпечувати можливість локальної автентифікації партнера за логіном та паролем.<br>У разі втрати або забуття пароля користувачем, Система повинна передбачати механізм відновлення доступу шляхом:<br>- надсилання одноразового пароля (OTP);<br>- або надсилання одноразового захищеного посилання для встановлення нового пароля на раніше підтверджену електронну пошту або номер мобільного телефону користувача.<br>Одноразовий пароль або посилання повинні:<br>- мати обмежений строк дії;<br>- бути дійсними для одноразового використання;<br>- відповідати вимогам інформаційної безпеки. | | | |
| 5. Надсилання запрошень іншим користувачам здійснюється через електронне повідомлення на вказану адресу електронної пошти з заздалегідь визначеною адміністратором роллю. | - | так | Другий етап |
| 6. Доступ запрошених користувачів до системи надається після проходження ними процедури авторизації відповідно до встановлених правил системи. | - | так | Другий етап |
| 7. Система повинна забезпечувати можливість відновлення доступу користувача (через ті ж механізми, якими користувач автентифікувався у системі, *п 4.-автентифікація-партнери*). | - | так | Другий етап |
| **Основний функціонал** | | | |
| 1. Система повинна забезпечувати формування документів з заздалегідь доданих шаблонів, мати змогу виводити сформований документ на перегляд та забезпечувати підписання КЕП (одним підписом КЕП чи декількома, в залежності від типу документу) як сформованих документів що наповнюється даними з реєстрів /інтегрованих систем так і документів, які надаються користувачем через інтерфейс. | - | так | Другий етап |
| 2. Забезпечується наявність конструктора шаблонів форм електронних документів (Jasper, Fastreport). | - | так | Другий етап |
| 3. Система повинна підтримувати використання заздалегідь | - | ні | Другий етап |

| | | | |
|---|---|---|---|
| налаштованих та довільних маршрутів проходження документів для категорії Партнери. | | | |
| 4. Система повинна забезпечувати електронне узгодження документів з можливістю як послідовного, так і паралельного узгодження різними компаніями. | - | так | Другий етап |
| 5. Забезпечується моніторинг проходження та обробки документів з візуалізацією статусів та основних реквізитів документів. | - | так | Другий етап |
| 6. Користувач повинен мати можливість накладати електронний підпис на документи та файли, згенеровані системою або завантажені в систему. | - | так | Другий етап |
| 7. Система повинна забезпечувати перегляд статусу обробки документів та файлів, до яких користувач має доступ. Має бути механізм нагадувань щодо невиконаних подій, шляхом повідомлень на електронну пошту / месенджер. | - | так | Другий етап |
| 8. Користувач повинен мати можливість надавати доступ до своїх документів іншим користувачам, компаніям або клієнтам. | - | так | Другий етап |
| 9. Система повинна забезпечувати обмін повідомленнями між користувачами, зі зберіганням історії спілкування. | - | так | Другий етап |
| 10. Система повинна забезпечувати сервіс поштових повідомлень щодо зміни статусу документа на всіх етапах його життєвого циклу. | - | так | Другий етап |
| 11. Користувач повинен мати можливість вивантаження підписаних документів на диск ПК для подальшого використання у вигляді файлу та/або розміщення в окремому електронному архіві (за наявності). | - | так | Другий етап |
| 12. Система повинна забезпечувати розгалужений інструмент швидкого пошуку необхідних документів. | - | так | Другий етап |
| **UI/UX** | - | | |
| 1. Інтерфейс зрозумілий, послідовний, максимально наближений до нативного офісного софту. | - | так | Другий етап |
| 2. Чітка навігація: sidebar / панель меню, breadcrumbs, фільтри та сортування без перезавантаження. | - | так | Другий етап |
| 3. Списки документів із ключовими атрибутами (назва, дата, статус, відповідальний) та preview у модальному вікні. | - | так | Другий етап |
| 4. Inline-перевірка полів та підказки при додаванні документів або метаданих. | - | так | Другий етап |
| 5. UI-відповідь на всі дії: loader під час обробки, toast при успіху, confirmation для критичних дій. | - | так | Другий етап |

| | | | |
|---|---|---|---|
| 6. Пошук і фільтри з багатовибором, динамічне оновлення списку та збереження останніх параметрів. | - | так | Другий етап |
| 7. Швидке завантаження списків (lazy loading), preview документів без повного завантаження, підтримка слабкого інтернету. | - | так | Другий етап |
| 8. Єдина дизайн-система, кольори статусів документів, видимі та чіткі CTA-кнопки. | - | так | Другий етап |

| **Категорія користувача: Адміністратори** | **Обов'язковість** | **Коментар** |
|---|---|---|
| **Автентифікація** | | |
| 1. Система повинна забезпечувати автентифікацію адміністраторів виключно через внутрішню систему автентифікації Компанії. Пароль через AD застосовується для усіх співробітників Товариства. | так | Перший етап |
| 2. Система повинна підтримувати інтеграцію з внутрішнім сервісом автентифікації (Ldap) із використанням встановлених протоколів безпеки. | так | Перший етап |
| 3. Доступ до адміністративного функціоналу Системи надається лише користувачам з роллю «Адміністратор». | так | Перший етап |
| 4. Система повинна підтримувати рольову модель доступу з можливістю розмежування прав адміністраторів за функціональними модулями. | так | Перший етап |
| 5. Процедура відновлення доступу повинна здійснюватися через внутрішню систему автентифікації Компанії та відповідати вимогам інформаційної безпеки. | так | Перший етап |
| 6. Дії адміністраторів повинні логуватися та бути захищеними від змін. | так | Перший етап |
| **Основний функціонал** | | |
| 1. Система має вести та відображати список користувачів. Призначати, змінювати та керувати системою ролей і прав доступу в межах повноважень. Блокувати користувачів системи. | так | Перший етап |
| 2. Управління конфігураціями Системи без необхідності внесення змін у програмний код. | так | Перший етап |
| 3. Налаштування шаблонів документів у конструкторі форм, бізнес-процесів за допомогою BPM-модуля. | так | Перший етап |
| 4. Система повинна підтримувати запуск бізнес-процесів на основі ключових подій, зокрема виконання клієнтом фінансових та нефінансових зобов'язань (наприклад, надання довідок, оформлення страховок тощо). Подія може надходити з іншої системи та ініціювати стартову ноду BPM через зовнішній API-запит. | так | Перший етап |
| 5. Можливість примусово змінювати статуси документів, по заздалегідь прописаним правилам. | так | Перший етап |
| 6. Фіксація усіх дій користувачів Системи у розрізі дат, Компаній і т. п. | так | Перший, другий етапи |
| 7. Перегляд журналу виконання користувачами операцій. | так | Перший етап |
| 8. Блокування в Системі роботи Компаній, Користувачів. | так | Перший, другий етапи |
| 9. Моніторинг працездатності та рівня навантаження. | так | Перший етап |
| 10. Система повинна забезпечувати візуалізацію дашборду для моніторингу процесів, налаштованих у BPM, з метою контролю статусу заявок/документів та дотримання регламентних таймінгів їх проходження а саме:<br>- Відображення стану процесів: | так | Перший етап |

| | | |
|---|---|---|
| a. відображати перелік BPM-процесів із різними кроками (steps).<br>b. Для кожного процесу та кожного кроку повинна відображатися:<br>• кількість заявок/документів, що наразі знаходяться на відповідному кроці;<br>• (опційно) розподіл за статусами: в роботі / на паузі / очікує дій тощо.<br>- Контроль таймінгів (SLA / нормативи);<br>- Користувач повинен мати можливість перейти з дашборду:<br>• до списку заявок/документів на конкретному кроці;<br>• до картки конкретної заявки/документа. | | |
| 11. Система повинна підтримувати можливість визначення та моніторингу SLA для бізнес-процесів, зокрема: у разі співпраці з партнерами; для клієнтів, де виконання зобов'язань (ковенантів) розглядається як показник дотримання рівня сервісу по відношенню до кредитора. | так | Перший етап |
| 12. Адміністратор повинен мати доступ до журналів виконання користувачами операцій, з можливістю фільтрування за датою, Компанією або користувачем. Журнали повинні містити повну інформацію про дії користувачів (автентифікація, створення/зміну/видалення документів, підписання КЕП). Можливість перегляду історії подій та експорт відповідних записів для проведення аналізу чи аудиту. | так | Перший етап |
| 13. Адміністратор повинен мати можливість налаштовувати інтеграційні параметри із зовнішніми системами (наприклад, внутрішні документообіг, ERP чи CRM) через BP/API або шину інтеграцій ESB. | так | Перший, другий етапи |
| 14. Система повинна забезпечувати участь «Адміністраторів» (співробітників Товариства) у бізнес-процесах на основі **ролей**, а не індивідуальних користувачів.<br>Доступ до функцій та документів повинен надаватися відповідно до ролей і визначатися налаштуванням процесу. «Адміністратори» повинні мати можливість виконувати лише ті дії, які передбачені процесом, наприклад погодження або відхилення документів. | так | Перший, другий етапи |

| **Нефункціональні вимоги** | **Обов'язковість мобільний додаток** | **Обов'язковість web-кабінет** | **Коментар** |
|---|---|---|---|
| **WEB кабінет клієнта/партнера** | | | |
| **Загальна інформація** | | | |
| 1. Україномовний інтерфейс. | так | так | Перший етап |
| 2. Передбачати реєстрацію (фіксацію та протоколювання ) будь-яких подій, проведених у Системі, та часу їх проведення до мілісекунд (у тому числі налаштування прав доступу, авторизації процесів). | так | так | Перший етап |
| 3. Має використовувати типи підписів CAdES-LT / CAdES-LTA, та/або PAdES-LT / PAdES-LTA. Контейнер ASIC-E. Система повинна підтримувати механізми довготривалої валідації та | так | так | Перший етап |

| | | | |
|---|---|---|---|
| архівного зберігання електронних підписів відповідно до таких форматів:<br>• **CAdES-LT** — із додаванням мітки часу (Timestamp) та даних перевірки статусу сертифіката (OCSP/CRL) для забезпечення довгострокової валідації підпису.<br>• **CAdES-LTA** — розширений формат, що включає **CAdES-LT** та архівні мітки часу для забезпечення архівного зберігання та підтвердження юридичної значущості документів протягом 10–50 і більше років.<br>Система повинна забезпечувати можливість перевірки дійсності підпису протягом усього встановленого строку зберігання документів. | | | |
| 4. Інтеграція з хмарним Microsoft AD (Entra ID) та наземним Microsoft AD (для співробітників). | ні | так | Перший етап |
| **Вимоги до документації** | | | |
| 1. Документація для розробника ПЗ, в якій описані механізми налаштування, API інтерфейсів та доопрацювання системи, без залучення співробітників компанії виробника. | так | так | Перший етап |
| 2. Документація для адміністратора програмного забезпечення, в якій описані механізми адміністрування та розгортання поточної версії програмного забезпечення, в тому числі для відновлення програмного забезпечення з резервної копії. | так | так | Перший етап |
| 3. По всій документації має бути створений Єдиний словник термінів та визначень. | так | так | Перший етап |
| 4. Документація для кінцевого користувача системи (у розрізі ролей) – інструкції користувача, в якій повністю описані всі функції поточної версії ПЗ. | так | так | Перший етап |
| **Система розподілення прав доступу** | | | |
| 1. Розмежування та налаштування прав доступу (перегляд, редагування, підписання, адміністрування) без розробників ПЗ – застосування рольової моделі доступу з урахуванням структури організації, функцій та повноважень; Захищеність даних. | так | так | Перший етап |
| **Навантаження на систему** | | | |
| 1. Кількість активних клієнтів системи, які мають обліковий запис -<br>2. не менше 1 000 000 шт. | так | так | Перший етап |
| 3. Кількість користувачів, які одночасно знаходяться в системі не менше 10000 шт. Прогнозується як середнє навантаження. | так | так | Перший етап |
| **Використання КЕП** | | | |
| 1. Використання ДІЯ підпис для клієнтів фізичних осіб для накладання КЕП на документи | так | так | Перший етап |

| | | | |
|---|---|---|---|
| 2. Використання КЕП організації для накладання КЕП на документи зі сторони юридичної особи. | - | так | Перший, другий етапи |
| **Інтеграції** | | | Перший та другий етапи |
| 1. Вивантаження опрацьованих документів до сховища (реєстру) кредитних справ (інтеграція с СЕД Clever Forms у відповідності до існуючого API) | - (в рамках BACK) | так | |
| 2. Зі страховими компаніями (відповідно до переліку авторизованих страхових).Вибір продуктів страхування, передача запитів на оформлення, та фіксація результату обробки запитів на стороні Страхової | так | так | |
| 3. Державними реєстрами , такими як (але не виключно): ЄДР, ДРРПНМ, ДРОРМ, бази даних ПФУ/ДПІ, ЄДЕССБ, БКІ, портал ДІЯ. | - (в рамках BACK) | так | |
| 4. АБС Б2 (отримання / передача даних, подій) | - (в рамках BACK) | так | |
| 4.1. Отримання подій та їх обробка. | - (в рамках BACK) | так | |
| 4.2. Формування електронних документів у відповідності до шаблонів | - (в рамках BACK) | так | |
| 4.3. Запуск документів за маршрутами підписання | так | так | |
| 5. З системою HRM, для заведення користувачів Товариства | - (в рамках BACK) | так | |
| **Маршрути** | | | |
| 1. Розподіл та налаштування маршрутів проходження кожного типу документу | - (в рамках BACK) | так | Перший, другий етапи |
| **Заведення користувачів** | | | |
| 1. Фізичні особи позичальники | | так | |
| 1.1. За допомогою посилання з обов'язковою авторизацією. | так | так | Перший етап |
| 1.2. За допомогою встановлення мобільного додатку | так | ні | Перший етап |
| 2. Юридичні особи | | так | |
| 2.1. Заведення адміністраторами юридичних організацій. | - | так | Другий етап |
| 2.2. Адміністратори юридичних організацій заводяться/акцептуються бізнес-адміністраторами Товариства. | - | так | Другий етап |
| 2.3. Можливість реєстрації у Системі за допомогою КЕП відповідної Компанії. | - | так | Другий етап |
| 3. Співробітники Товариства | - (в рамках BACK) | так | |
| 3.1. Заведення адміністраторами Товариства. | | так | Перший етап |
| **Аналітика** | | | |

| | | | |
|---|---|---|---|
| 1. | Має бути реалізований централізований Data Layer (аналітична обгортка), який забезпечує збір, стандартизацію та передачу даних про дії користувачів, бізнес-процеси та системні події.<br>Всі аналітичні події повинні передаватися через єдиний механізм збору даних, незалежний від конкретних систем аналітики та звітності.<br>Рішення повинно забезпечувати:<br>- можливість додавання нових подій та параметрів без суттєвих змін архітектури рішення;<br>- використання єдиної структури подій та параметрів;<br>- передачу системних, користувацьких та бізнес-атрибутів подій;<br>- можливість інтеграції з зовнішніми аналітичними платформами та BI-системами;<br>- ведення каталогу подій із описом подій, параметрів та правил їх формування.<br>Архітектура збору даних повинна забезпечувати масштабованість та можливість подальшого розширення аналітичних сценаріїв без внесення змін до бізнес-логіки інтерфейсів. | так | так | Перший етап |
| 2. | Функціонал повинен забезпечувати збір, зберігання / передачі даних по подіям створених користувачами. | так | так | Перший етап |
| *3.* | Налаштування аналітики мають здійснюватися без значних внесень змін у програмний код. *Один з варіантів, за допомогою Remote Config.*<br>*Адмінка / Config Service*<br>*↓ (JSON)*<br>*Remote Config API*<br>*↓*<br>*Mobile App*<br>*↓*<br>*Event Processor (в коді)*<br>*↓*<br>*Analytics Collector API (ваш backend)*<br>*↓*<br>*DB / DWH / BI.* | так | так | Перший етап, другий етапи |
| 4. | Реалізація архітектури Analytics Wrapper (шар абстракції): реалізація аналітики через єдиний інтерфейс-обгортку в коді додатка. Прямий виклик сторонніх SDK (наприклад, Amplitude) у бізнес-логіці екранів заборонений. | так | - | Перший етап |
| 5. | Підтримка гібридного трекінгу (Client-to-Server + Server-to-Server): забезпечення передачі інтерфейсних подій з додатка, а транзакційних та реєстраційних статусів — з боку бекенду (серверної частини рішення). | так | - | Перший етап |

| | | | |
|---|---|---|---|
| 6. Гнучкість конфігурації без перерелізу додатка: можливість віддаленого ввімкнення/вимкнення окремих аналітичних SDK або зміни параметрів пакетної відправки (Batching) через конфігураційний файл на сервері або за допомогою систем типу Firebase Remote Config. | так | - | Перший етап |
| 6. Розробка та передача Аналітичної матриці (Event Dictionary): формування детального документу (таблицю), що містить:<br><br>Повний перелік усіх екранів (Screen Views) та інтерактивних елементів (кліків), що трекаються.<br><br>Суворі назви подій та їхніх параметрів (наприклад, тип даних: string, boolean, integer).<br><br>Тригери (точні умови в коді), за яких подія вважається активованою. | так | так | Перший етап |
| 7. Система повинна підтримувати визначення та управління переліком подій, що фіксуються. | так | так | Перший етап |
| 8. Для кожної події має бути можливість налаштування параметрів (атрибутів), типів даних та обов'язковості заповнення. | так | так | Перший етап |
| 9. Повинна бути можливість вмикати або вимикати збір окремих подій. | так | так | Перший етап |
| 10. Аналітичні дані, що формуються клієнтським застосунком, повинні передаватися разом із уніфікованим набором метаданих, які описують час формування даних, контекст їх виникнення, характеристики клієнтського середовища та параметри сесії користувача. | так | так | Перший, другий етапи |
| 11. Система повинна підтримувати передачу аналітичних даних до зовнішніх систем (BI / DWH) через API або інші інтеграційні механізми. | так | так | Перший етап |
| 12. Має бути передбачена можливість анонімізації або маскування даних. | так | так | Перший етап |
| 13. Система повинна надавати можливість проведення A/B тестування функціоналу. | так | так | Другий етап |
| **Інформаційна безпека та захист даних** | | | |
| В Системі має оброблятись інформація що містить — персональні дані, банківську таємницю, відомості з державних реєстрів та юридично значимі документи з накладеним КЕП, що передбачено процесами автентифікації, збору ідентифікаційних даних, доступу до кредитних матеріалів, фінансової інформації та інтеграцій з державними інформаційними реєстрами (системами). Сукупність таких даних відноситься до інформації з обмеженим доступом і підпадає під посилені вимоги захисту відповідно до законодавства України (банки, фінансові компанії), що зумовлює необхідність комплексного впровадження заходів інформаційної безпеки та контролю доступу в системі. | | | |
| **1. Вимоги до контролю доступу (управління ідентифікацією, автентифікацією та доступом):** | | | |
| 1.1. Система повинна підтримувати інтеграцію з Microsoft Active Directory / Entra ID або іншим | ні | так | Перший етап |

| | | | |
|---|---|---|---|
| корпоративним сервісом автентифікації Замовника для автентифікації працівників. | | | |
| 1.2. Для входу користувачів до Системи повинна застосовуватись автентифікація відповідно до типу користувача та сценарію використання. Для клієнтів допускається вхід за логіном/паролем, PIN або біометрією після первинної ідентифікації через Дія/BankID. Повторна посилена автентифікація через Дія/BankID повинна вимагатися у разі тривалої неактивності користувача. Для платіжних, фінансових та інших критичних операцій має застосовуватись додаткове підтвердження дії (SMS/OTP, Дія.Підпис, КЕП тощо). | так | так | Перший етап / Другий етап для платіжних сценаріїв |
| 1.3. При першому вході або створенні облікового запису користувача мають застосовуватись механізми підтвердження особи/доступу відповідно до типу користувача: Дія/BankID для фізичних осіб, КЕП або визначений механізм запрошення для юридичних осіб, корпоративна автентифікація для співробітників. | так | так | Перший етап |
| 1.4. У разі використання тимчасового пароля користувач повинен змінити його на власний пароль відповідно до політики паролів під час першого входу. | так | так | Перший етап |
| 1.5. Повинні бути визначені та налаштовувані правила блокування облікових записів: максимальна кількість невдалих спроб входу, тривалість тимчасового блокування, умови постійного блокування, процедура розблокування та події для журналювання. | так | так | Перший етап |
| 1.6. Доступ до Системи повинен бути можливий лише для автентифікованих користувачів. Усі спроби доступу без підтвердженої автентифікації повинні блокуватись та журналюватись. | так | так | Перший етап |
| 1.7. Система повинна завершувати сесію користувача при неактивності понад встановлений час. Значення тайм-ауту сесії має бути параметром, що передається з backend під час автентифікації та діє в межах відповідної сесії. Для фінансових та критичних операцій має бути передбачена можливість встановлення скороченого тайм-ауту. | так | так | Перший етап |
| 1.8. Система повинна підтримувати рольову модель доступу (RBAC) та налаштування доступу до документів, задач BPM і об’єктів процесу залежно від ролі користувача, організації користувача, типу документа та етапу бізнес-процесу. | так, у частині клієнтських сценаріїв | так | Перший етап / розширення на Другому етапі для партнерів |
| 1.9. Система повинна підтримувати механізм реєстрації довірених пристроїв користувача або формування технічного відбитка пристрою. При вході з нового або підозрілого пристрою повинна бути можливість вимагати додаткове підтвердження особи користувача та фіксувати подію в журналі аудиту. | так | так | Перший етап |
| **2. Аудит, контроль дій та незмінність журналів:** | | | |
| 2.1. Система повинна логувати дії користувачів, включаючи автентифікацію, невдалі входи, зміну ролей, зміну прав доступу, | так, у частині подій | так | Перший етап |

| | | | |
|---|---|---|---|
| створення/зміну/видалення документів, підписання документів, доступ до інтеграцій та доступ до критичних даних. | мобільного додатку | | |
| 2.2. Для важливих операцій, зокрема зміни критичних даних, підписання документів, видалення або відкликання документів, має бути реалізовано додаткове підтвердження дії або інший налаштовуваний контроль відповідно до сценарію. | так | так | Перший етап |
| 2.3. Система повинна зберігати історію змін і версійність документів із можливістю перегляду історії та, за наявності відповідних прав, відновлення попередньої версії. | так, у частині перегляду/дій клієнта | так | Перший етап |
| 2.4. Логи безпеки та аудиту повинні зберігатися не менше одного року або відповідно до внутрішніх політик Замовника. Система повинна підтримувати ротацію журналів та можливість передавання/вивантаження журналів у зовнішнє сховище або систему обробки журналів. | так, у частині подій мобільного додатку | так | Перший етап |
| 2.5. Система повинна формувати структуровані журнали подій у погодженому машинозчитуваному форматі, придатному для подальшої обробки зовнішніми системами збору логів, моніторингу або SIEM. Впровадження SIEM як окремої платформи не є предметом поставки розробника, якщо інше не визначено договором. | так | так | Перший етап |
| **3. Криптографічний захист (захист даних та управління інформацією):** | | | |
| 3.1. Система повинна підтримувати модель класифікації інформації та забезпечувати присвоєння документам, файлам, записам або типам даних відповідної категорії відповідно до довідника класифікації. Мінімально мають підтримуватись категорії: персональні дані, банківська таємниця, таємниця фінансової послуги, інформація з державних реєстрів, внутрішня інформація, юридично значимі документи з КЕП. | так, у частині даних мобільного додатку | так | Перший етап |
| 3.2. Для кожної категорії інформації повинна бути визначена централізована політика безпеки, яка автоматично застосовується до об’єктів відповідної категорії та визначає: правила доступу, правила маскування, вимоги до журналювання, правила експорту/завантаження/передачі даних, а також необхідність додаткового погодження критичних або масових операцій. | так, у частині відображення та операцій клієнта | так | Перший етап |
| 3.3. Маскування даних повинно застосовуватися в усіх нефункціональних контурах, де використовуються реальні або наближені до реальних дані: DEV, TEST/QA, STAGE/PRE-PROD. | так | так | Перший етап |
| 3.4. Система повинна підтримувати роботу з КЕП/ЕЦП згідно з чинними вимогами законодавства України та стандартами, включаючи можливість використання форматів довготривалого зберігання підпису, якщо це передбачено бізнес-процесом. | так | так | Перший етап |
| 3.5. Система повинна підтримувати інтеграцію з криптографічними бібліотеками та/або засобами захисту ключів, що використовуються | так | так | Перший етап / Другий етап |

| | | | |
|---|---|---|---|
| Замовником, включаючи можливість роботи з HSM або Cloud HSM для операцій, де ключі належать Замовнику або юридичній особі. Для фізичних осіб допускається використання Дія.Підпис або іншого зовнішнього сервісу КЕП. | | | для партнерів-юридичних осіб |
| 3.6. Система не повинна зберігати у відкритому вигляді паролі, токени, API-ключі, сертифікати, приватні ключі та інші секрети. Повинна бути забезпечена можливість використання зовнішнього або вбудованого захищеного сховища секретів із розмежуванням доступу, аудитом доступу та можливістю ротації секретів. | так | так | Перший етап |
| **4. Захист каналів передачі даних:** | | | |
| 4.1. Для критичних інтеграцій, включаючи АБС Б2, Open Banking, державні реєстри, СЕД Clever Forms, HRM та інші погоджені системи, повинна застосовуватись захищена взаємодія із використанням TLS 1.2+ або вище. Для критичних server-to-server інтеграцій повинна підтримуватись взаємна TLS-автентифікація (mTLS), якщо це підтримується інтегрованою стороною. | так, у частині взаємодії через backend | так | Перший етап / Другий етап для Open Banking |
| 4.2. Система не повинна використовувати незахищені протоколи для передавання чутливої інформації, зокрема HTTP, FTP, Telnet та інші протоколи без шифрування. | так | так | Перший етап |
| 4.3. Система повинна підтримувати контроль строків дії та заміни сертифікатів, що використовуються для інтеграційних каналів, а також журналювання помилок перевірки сертифікатів або неможливості встановлення захищеного з'єднання. | так, у частині backend/API | так | Перший етап |
| **5. Захист системи та API*:** | | | |
| 5.1. Система та її публічні API повинні бути сумісними з використанням WAF або іншого периметрового засобу захисту. Реалізація WAF як інфраструктурного компонента може бути зоною відповідальності Замовника, якщо інше не визначено договором. | так, у частині API | так | Перший етап |
| 5.2. API Системи повинні підтримувати захищену авторизацію доступу з використанням OAuth 2.0, OpenID Connect та/або JWT відповідно до погодженої архітектури. Backend-сервіси повинні перевіряти валідність токенів, права доступу та контекст виконання операцій. Захист від Brute Force має реалізовуватись на рівні Системи для сценаріїв автентифікації та може доповнюватися засобами WAF/API Gateway на інфраструктурному рівні. | так | так | Перший етап |
| 5.3. Система має бути піддана тестуванню на проникнення відповідно до методології OWASP перед введенням у продуктивну експлуатацію. Усі критичні та високі вразливості, що належать до зони відповідальності розробника, повинні бути усунені до запуску або в інший строк, погоджений із Замовником. | так | так | Перший етап |
| 5.4. Система повинна фіксувати технічні та бізнес-події, необхідні для подальшого виявлення підозрілої активності та шахрайських сценаріїв: підозрілі входи, нові пристрої, багаторазові | так | так | Перший етап / Другий етап для Open |

| | | | |
|---|---|---|---|
| невдалі спроби входу, масові операції, операції з фінансовими даними, створення або відкликання згод, ініціювання платіжних сценаріїв. | | | Banking та платежів |
| 5.5. Для Open Banking інтеграцій, якщо такі реалізуються в межах Системи, повинні бути передбачені: облік згод клієнта, фіксація строку дії згоди, можливість відкликання згоди, журналювання звернень до рахунків, захищене зберігання або незберігання токенів відповідно до погодженої архітектури, обмеження доступу до отриманих фінансових даних згідно з політиками класифікації. | так | так | Другий етап |
| **6. Вимоги до безпечної розробки** | | | |
| 6.1. Розробник повинен застосовувати практики безпечного життєвого циклу розробки (Secure SDLC) для компонентів, що розробляються або доопрацьовуються в межах проєкту. | так | так | Перший етап |
| 6.2. Для вихідного коду, що розробляється в межах проєкту, повинні виконуватись SAST-перевірки або еквівалентний статичний аналіз безпеки коду. | так | так | Перший етап |
| 6.3. Для вебкомпонентів та API повинні виконуватись DAST-перевірки або еквівалентний динамічний аналіз безпеки застосунку перед продуктивним запуском. | так, у частині API та mobile backend | так | Перший етап |
| 6.4. Розробник повинен забезпечити аналіз сторонніх бібліотек та open-source компонентів на наявність відомих критичних вразливостей. | так | так | Перший етап |
| 6.5. Розробник повинен забезпечити контроль відсутності паролів, токенів, ключів та інших секретів у вихідному коді, репозиторіях і артефактах збірки. | так | так | Перший етап |
| 6.6. Критичні та високі вразливості, підтверджені результатами перевірок безпеки та віднесені до зони відповідальності розробника, повинні бути усунені до введення рішення в продуктивну експлуатацію або в строк, погоджений із Замовником. | так | так | Перший етап |
| **7. Вимоги до безпеки Open Banking сценаріїв**<br>Цей розділ застосовується лише у випадку реалізації в Системі функціоналу Open Banking, доступу до рахунків банків-партнерів або ініціювання платіжних сценаріїв. | | | |
| 7.1. Система повинна забезпечити облік згод клієнта на доступ до рахунків, фінансових даних або ініціювання операцій, якщо така згода збирається або зберігається у Системі. | так | так | Другий етап |
| 7.2. Для кожної згоди повинні фіксуватись мінімально необхідні реквізити: користувач, дата та час надання, строк дії, обсяг дозволених даних або дій, джерело/банк, статус згоди, дата відкликання або завершення строку дії. | так | так | Другий етап |
| 7.3. Система повинна журналювати всі звернення до Open Banking API або API банків-партнерів, включаючи користувача, джерело запиту, тип операції, результат, час виконання та ідентифікатор зовнішнього запиту/відповіді, якщо він надається інтегрованою стороною. | так | так | Другий етап |
| 7.4. Токени доступу або інші технічні облікові дані Open Banking не повинні зберігатися у відкритому вигляді. Має бути забезпечено обмеження доступу | так | так | Другий етап |

| | | | |
|---|---|---|---|
| до таких токенів, журналювання доступу та можливість їх відкликання/ротації відповідно до погодженої архітектури. | | | |
| 7.5. Отримані через Open Banking фінансові дані повинні оброблятися відповідно до класифікації інформації, правил доступу, маскування, журналювання та строків зберігання, визначених у Системі та внутрішніх політиках Замовника. | так | так | Другий етап |
| **Технічна інфраструктура** | | | |
| 1. Наявність BPM модулю для самостійної побудови та управління процесами. | (В рамках BACK) | так | Перший етап |
| 2. Система у рамках функціонування має бути багатокомпонентною системою, тобто побудована за багаторівневою архітектурою (програмний додаток, що підключений до сервера(-ів) додатків, який у свою чергу підключений до сервера бази даних), з WEB інтерфейсом і підтримувати операційні системи Windows 11 та вище, MacOS, та браузери MS EDGE, Google Chrome, Safari. | так | так | |
| 3. Всі сторінки веб-додатків повинні бути відображені правильно (без перерв у макеті) в тій же зручній формі на настільному комп'ютері та на мобільному пристрої (планшет, ноутбук, смартфон), незалежно від типу пристрою (без використання окремої мобільної версії Системи), тобто Web – клієнт повинен перебувати в адаптивному «Google Material Design» інтерфейсі. | - | так | Перший етап |
| 4. Для певного типу користувачів (фізичні особи) має бути доступний функціонал у мобільному додатку | так | - | Перший етап |
| 5. Архітектура системи повинна підтримувати роботу в кластері, для забезпечення максимальної відмово стійкості компонент системи. | (В рамках BACK) | так | Перший етап |
| 6. База даних, яка використовується для зберігання даних, повинна мати можливість роботи в ACTIVE/PASIVE режимі з мінімальним терміном переключення, у разі виходу з ладу ACTIVE бази, та/або мати можливість роботи в кластері. | (В рамках BACK) | так | Перший етап |
| 7. Багатокористувацький режим роботи. | - | так | Перший етап |
| 8. Можливість централізованого автоматичного оновлення Системи, без зупинки процесів (не стосується БД). | так | так | Перший етап |
| 9. Система повинна мати підсистему адміністрування. | (В рамках BACK) | так | Перший етап |
| 10. Система повинна надавати можливість апаратного та програмного масштабування. | так | так | Перший етап |
| 11. Система має бути реалізовано з урахуванням вимоги безперервності ведення діяльності, у тому числі: резервне копіювання (гарячий та | (В рамках BACK) | так | Перший етап |

| | | | |
|---|---|---|---|
| холодний бекап) баз даних та інформації, встановлення оновлень. | | | |
| 12. Система має підтримувати роботу з промисловою СУБД (одна з: Microsoft SQL, Oracle, PostgreSQL) включаючи роботу з застосування вищевказаних СУБД в хмарному середовищі. | (В рамках BACK) | так | Перший етап |
| 13. Система має працювати по невиділеному каналу зв'язку між клієнтською робочою станцією і сервером додатків. Допускається мобільний доступ (LTE\5G), виділена лінія, локальна мережа. | так | так | Перший етап |
| 14. Система має підтримувати роботу клієнтських робочих місць у віддаленому доступі у будь-якій точці світу, у тому числі засобами VPN. | - | так | Перший етап |
| 15. Система повинна забезпечувати задовільну швидкість роботи за умови, що середні показники обладнання на робочих місцях:<br>✓ комп'ютер 8 ГБ ОЗУ, Частота процесору 2,5 Ghz, 150Gg HDD (мінімальна конфігурація ПК робочих місць користувачів - PC, CPU: 2 Core @ 2,5 Ghz, RAM: 8Gb, HDD: 150Gb);<br>✓ операційна система Windows 11 або вище;<br>✓ веб-браузер: відповідно до вимог, наведених вище;<br>✓ мережа: 2 Mbps і вище. | - | так | Перший етап |
| 16. Серверна частина Система повинна підтримувати роботу у хмарному віртуалізованому середовищі. | так | так | Перший етап |
| 17. Система має бути розгорнуто на промислових операційних системах (Windows, Linux). | (В рамках BACK) | так | Перший етап |
| 18. Система повинна мати механізми діагностики та моніторингу стану всіх компонентів та стану серверних додатків. | (В рамках BACK) | так | Перший етап |
| 19. Система повинна мати автоматичний збір даних про програмні помилки, збої в Системі, некоректне завершення сеансів користувачів Системи, та збереження у журналі подій. | (В рамках BACK) | так | Перший етап |
| 20. Можливість коригування та створення друкованих шаблонів. | (В рамках BACK) | так | Перший етап |
| 21. Розробник/Постачальник повинен надавати всі наявні оновлення версій згідно з договором підтримки, повідомляючи про їх наявність регулярно або за запитом. | так | так | Перший етап |
| 22. Система має підтримувати прозорий механізм оновлень з застосуванням 3-рівневої моделі середовищ (Розробки-Тестове-Продуктивне); | так | так | Перший етап |
| 23. Система має передбачати формування звіту про роботу користувачів. | так | так | Перший етап |

| | | | |
|---|---|---|---|
| 24. Система має передбачати можливість архівування інформації журналів роботи користувачів. | (В рамках BACK) | так | Перший етап |
| 25. Система не повинна використовувати системних файлових мережних дисків/ресурсів для обміну між серверами бази даних та серверами додатків/додатків або веб-серверами, взаємодія повинна відбуватися виключно по портах бази даних та портах, що використовують веб-додатки. Всі інші порти блокуються відповідно до політик безпеки Товариства. | (В рамках BACK) | так | Перший етап |
| 26. Глибина підтримки ОС<br>• Android:<br>○ Мінімальна версія: Android 11.0 (API 30).<br>○ Цільова версія (Target SDK): Android 15 (API 35) (вимога Google Play) і вище.<br>• iOS:<br>○ Мінімальна версія: iOS 16 і вище.<br><br>Підтримка мобільних браузерів та WebView: Повна сумісність із Blink (Chromium) та WebKit.<br><br>Браузери (Evergreen): Офіційна підтримка останніх 3 мажорних версій Google Chrome Mobile.<br><br>Safari (iOS): Підтримка версій Safari, що вбудовані в iOS 16 - iOS 18 і вище.<br><br>WebView: Використання стандартного Android WebView та iOS Safari View Controller для безпечного відображення веб-контенту всередині додатка. | так | так | Перший етап |
| | | | |
| **Інші вимоги** | | | |
| **Ліцензії на використання ПЗ** | | | |
| Якщо програмний продукт продається за умови строкової дії ліцензій, в розрахунок комерційної пропозиції має бути включена вартість сервісної підтримки протягом 3, 5 років. | так | | Перший етап |
| **Підтримка** | | | |
| В комерційну пропозицію мають бути включені витрати на сервісну підтримку ПЗ, при цьому: | | | Перший етап |
| - Строк гарантійного (безкоштовного) обслуговування не може бути меншим 12 місяців з моменту переходу до продуктивної експлуатації. | так | | Перший етап |

| | | |
|---|---|---|
| - Під сервісним та гарантійним обслуговуванням мається на увазі усунення виявлених помилок в роботі програмного забезпечення, моніторинг та проактивне налаштування ПЗ щодо змін в законодавстві, налаштування звітів та виконання необхідних доопрацювань. | так | Перший етап |

## Базовий функціонал для ролі «Клієнт» (процеси для впровадження)

Для ролі **Клієнт (B2C)** повноцінним каналом взаємодії із Системою є **Мобільний додаток**. У ньому зосереджено 100% клієнтського функціоналу.

**Веб-кабінет Клієнта НЕ є функціональним аналогом чи альтернативою Мобільного додатку.** Його розробка зумовлена виключно необхідністю забезпечення критично важливих для Компанії бізнес-процесів (наприклад: виконання певних ковенант (нефінансових зобов'язань), або сплата обов'язкового платежу (фінансових зобов'язань).

**Сценарій взаємодії за відсутності Мобільного додатку (Обмежений цільовий Fallback)**

Якщо Компанія ініціює критично важливий процес, а у Клієнта **не встановлено Мобільний додаток**, взаємодія через зовнішні канали (SMS, Email, месенджери) відбувається за логікою **ізольованого цільового коридору (Targeted Flow)**:

1. **Точкове посилання:** Клієнт отримує повідомлення з динамічним розумним посиланням, яке веде на конкретну бізнес-дію.
2. **Ізольована авторизація:** При переході через веб-браузер Клієнт проходить мінімально необхідну авторизацію (ДіяПідпис / BankID).
3. **Прямий редірект у бізнес-процес:** Одразу після авторизації Система скеровує Клієнта *виключно на екран виконання цієї критичної дії*.
4. **Обмеження навігації:** Клієнт не має доступу до загального функціоналу Системи у веб-версії. Інтерфейс Веб-кабінету в цьому сценарії є урізаним і фокусує користувача лише на виконані певної дії. (наприклад: екран завантаження документів, вікно підписання ЕЦП/КЕП або платіжний шлюз).
5. **Завершення процесу:** Після успішного виконання дії Система виводить екран успіху (Success Screen) із обов'язковим закликом до дії (CTA) — завантажити Мобільний додаток для подальшої роботи, після чого веб-сесія може бути завершена.

[ Клієнт без додатка клікає на посилання в SMS/e-mail ]

|

[ Авторизація у Веб ]

|

[ Ізольована цільова сторінка (JTBD) ]

|

[ Екран успіху + Заклик скачати додаток ]

Реалізація обмеженого функціоналу Веб-кабінету Клієнта має забезпечувати технічну можливість його подальшої модернізації та розширення до повнофункціональної веб-версії кабінету. Архітектурні рішення не мають блокувати або суттєво ускладнювати інтеграцію нових клієнтських сервісів у веб-інтерфейс у майбутньому.

| Функціонал | Обов'язковість для мобільного додатку | Обов'язковість для веб версії | Етап впровадження |
|---|---|---|---|
| 1. Авторизація та Онбординг, відновлення доступу (ДіяПідпис, BankID) | так | так | Перший етап |

| | | | |
|---|---|---|---|
| 2. Вхід з використанням паролю, біометричної авторизації | так | ні | Перший етап |
| 3. Відображення профілю користувача, Налаштування акаунта: зміна пароля. Видалення акаунта. | так | ні | Перший етап |
| 4. Сповіщення (Push Notifications), в т.ч. інтерактивні. | так | ні | Перший етап |
| 5. Зворотний зв'язок та підтримка: можливість написати в чат-бот компанії (модуль відображення чату, інтеграція з чат-ботом компанії) повідомити про баг або залишити відгук. | так | так | Перший етап |
| 6.Відображення інформації з заявки та статуси по заявці у розрізі банків (інтеграція з API мобільного додатку Дія). Порівняння умов банків, можливість обрати / скасувати пропозицію. | так | ні | Перший етап |
| 7. Інформація по умовам програми, що розраховується на основі даних з заявки. | так | ні | Перший етап |
| 8. Перевірка на критерії програми (чи проходить клієнт та на які умови проходить) | так | ні | Перший та другий етап |
| 9. Інформація по акредитованих будинках (або квартирах у будинках), посилання на контакти. Можливість сортування з урахуванням даних з заявки. | так | ні | Перший етап |
| 8. Можливість оцінити комунікацію з банком / послугу. | так | ні | Перший етап |
| 10. Відображення інформації по кредитах на балансі УФЖК (основний борг, відсотки, плановий платіж, виписка) | так | ні | Перший етап |
| 11. Відображення нефінансових зобов'язань (ковенант) та статусу їх виконання. | так | так | Перший етап |
| 12. Формування та підписання згоди для ПФУ | так | так | Перший етап |
| 13. Можливість оплати по кредиту на балансі УФЖК. | так | так | Другий етап |
| 14. Можливість надання / завантаження файлів (PDF, JPG) в рамках певних процесів (наприклад завантаження довідки про посаду або дохід) | так | так | Перший етап |

**ДОДАТКИ:**

1. Приклад схеми процесу Підтвердження оцінки об'єкту нерухомості.
2. Приклад схеми процесу Підтвердження фінансового стану позичальника.
3. Приклад схеми процесу Підтвердження страхування об'єкту нерухомості.
4. Приклад схеми процесу Підтвердження категорії позичальника.
5. Приклад схеми процесу Ідентифікації авторизації верифікація позичальника.


Додаток1.pdf


Додаток2.pdf


Додаток3.pdf


Додаток4.pdf


Додаток5.pdf