Регламент використання електронних каналів для підприємців та інших суб'єктів

Регламент застосовується:

- з 15 грудня 2020 року – у разі договорів, укладених до 30 листопада 2020 року.

- з дня укладення договору – у разі договорів, укладених з 1 грудня 2020 року.

Використані в Регламенті поняття означають:

ВИЗНАЧЕННЯ

§1

Банк – Alior Bank S.A. з місцезнаходженням у Варшаві;

Інтернет-банкінг – послуга, що забезпечує доступ до інформації про Продукти та можливість подання розпоряджень за допомогою Інтернету та комп'ютера зі встановленим веб-браузером;

Маклерське бюро – відокремлений організаційний підрозділ Банку, відповідальний за надання Банком маклерських послуг;

Мобільний банкінг – послуга, що надає доступ до інформації про Продукти Клієнта та можливість подання розпоряджень за допомогою мобільних пристроїв з доступом до Інтернету, таких як стільникові телефони та планшети зі встановленим веб-браузером;

Центр продуктів – платформа електронного банкінгу, що надається Банком разом із Системою BusinessPro, яка забезпечує надання послуг та інформації на довговічному носії інформації, що використовується для:

1. подачі заявок на нові послуги та продукти з банківської пропозиції;
2. подання Розпоряджень щодо Продуктів, що належать Клієнту
3. обміну електронними документами та зв'язку між клієнтом і Банком.

Кваліфікований сертифікат – кваліфікований сертифікат у розумінні Закону від 5 вересня 2016 року про довірчі послуги та електронну ідентифікацію;

Contact Center – підрозділ Банку або Маклерського бюро, що надає телефонне обслуговування поточних та потенційних Користувачів у сфері інформації та збуту;

Зчитувач карт процесора – пристрій, що використовується для обробки та зчитування інформації, що міститься на карті процесора;

Ідентифікаційні дані – набір даних, що дають змогу ідентифікувати фізичну чи юридичну особу, або фізичну особу, яка представляє юридичну особу;

Розпорядження – волевиявлення, подане через Електронні канали уповноваженими Користувачами та авторизоване у спосіб, що відповідає даному каналу;

Група прийняття – набір Користувачів, позначених буквою, які мають однакові повноваження підписувати Розпорядження в системі;

Стартовий пароль – рядок символів, що надсилаються Користувачеві по Телефону на коди авторизації (довірений телефон) у вигляді SMS або надаються на папері у вигляді захищеного конверта, який використовується для активації Інтернет-банкінгу;

Пароль – рядок символів, самостійно визначених Користувачем в Інтернет-банкінгу, що при використанні разом з Ідентифікатором забезпечує доступ до Інтернет-банкінгу та Мобільного банкінгу;

Ідентифікатор (CIF) – унікальний номер, присвоєний Користувачеві Банком, з яким чітко пов'язані персональні та адресні дані, які використовуються, зокрема, для ідентифікації при використанні Електронних каналів;

Електронні канали – Інтернет-банкінг (включаючи окрему функціональність, призначену для ініціювання платежів третіми суб'єктами та функціональність, призначену для доступу третіх суб'єктів до інформації про платіжні рахунки, а також для послуг провайдерів, що випускають карткові інструменти), Мобільний банкінг;

Карта процесора – карта пам'яті процесора або апаратний токен, що становить фізичний носій Електронного ключа Системи BusinessPro;

Клієнт – підприємець, тобто фізична особа, юридична особа та організаційна одиниця, яка не є юридичною особою, якій окремим законом надається дієздатність, – що провадить підприємницьку діяльність від свого імені, у тому числі

партнери спільної господарської діяльності в обсязі їхньої підприємницької діяльності, та суб'єкти, які не здійснюють підприємницьку діяльність, наприклад, фонди, асоціації;

Електронний ключ – відкритий та закритий ключ, згенерований Користувачем в системі онлайн-банкінгу. Збережений на USB-пристрої чи Карті процесора, він використовується для авторизації розпоряджень та для входу в Інтернет-банкінг, якщо Клієнт вибрав цей спосіб автентифікації;

Електронний ключ Системи BusinessPro – конфіденційні, унікальні та присвоєні Користувачеві електронні дані, які є закритим ключем у технології RSA, із захищеним паролем доступом, які використовуються Користувачем для авторизації розпоряджень, згенеровані Компонентом електронного підпису Системи BusinessPro, що зберігаються на Карті процесора, на локальному носії (наприклад, USB-накопичувач) або на електронних носіях інформації, підконтрольних Банку (у сховищі Банку);

Компонент електронного ключа Системи BusinessPro – незалежний програмний модуль Системи BusinessPro, встановлений на робочому місці Користувача, що перебуває виключно під його контролем. Компонент забезпечує функціонал генерації пари ключів: приватного та публічного, використання Електронного ключа Системи BusinessPro;

Код авторизації – код у вигляді текстового повідомлення, надісланого на визначений Клієнтом Телефон для авторизації доручень, який використовується для авторизації Розпоряджень, поданих Клієнтом в рамках Інтернет-банкінгу або Мобільного банкінгу за допомогою веб-браузерів, надсилається Користувачеві, якщо він вибрав такий метод авторизації;

Добовий ліміт для Користувача Мобільного банкінгу Системи BusinessPro – ліміт, встановлений у Правовому модулі на загальну добову суму авторизованих операцій з використанням мобільних пристроїв. Значення Ліміту за замовчуванням для кожного Користувача становить 200000 злотих;

Ліміти суми – це параметри, що визначають вартість одноразової/добової/місячної суми операції, присвоєні відповідно до поділу для інтернет-банкінгу (включаючи постачальників послуг ініціювання платежу), для мобільного банкінгу;

Добовий ліміт авторизації Системи BusinessPro – ліміт, встановлений у Правовому модулі, на загальну добову суму авторизованих операцій з використанням коду авторизації на робочій станції Користувача, на якій не встановлено Компонент Електронного ключа;

Локація – місце розташування організаційного підрозділу Клієнта та користувачів, що стандартно використовують Систему BusinessPro;

Метод DFP – механізм, що дозволяє верифікувати та ідентифікувати пристрій Клієнта, який використовується для входу та доручення платіжних операцій в електронному та мобільному банкінгу. Він полягає в дослідженні певного набору функцій пристрою (ПК, ноутбук, смартфон, планшет тощо), які підтверджують, що це пристрій, яким користується Клієнт. Параметри, подані для аналізу, можуть включати, серед іншого: а) версію операційної системи пристрою, б) значення в реєстрі, пов’язані з середовищем запуску (профіль Windows, мовна версія), в) дані браузера (наприклад, версія браузера, встановлена мова) , г) зашифровані файли cookie з конкретними значеннями, що зберігаються для даного Клієнта, д) параметри відеокарти та звукової карти, е) параметри процесора та оперативної пам’яті, є) налаштування та роздільна здатність екрана, ж) дані про середовище запуску браузера, з) додатково є можливість зберегти конкретне значення (деякі браузери дозволяють зберігати дані, які надходять під час веб-сеансу в WebStorage), унікальне для клієнта та пов’язане з ним. Пристрій, ідентифікований методом DFP, є елементом Сильної автентифікації;

Правовий модуль – канал електронного зв’язку, наданий Банком разом із Системою BusinessPro, що використовується для підготовки, відтворення та обміну електронними документами між Клієнтом та Банком у незмінному вигляді, забезпечення обміну інформацією на довговічному носії інформації;

USB-накопичувач – пристрій для зберігання Електронного ключа;

Пакет підписки – певний набір функціональних можливостей у Системі BusinessPro, який надається Клієнту за щомісячну плату;

PIN-код для USB-накопичувача – послідовність цифр, встановлених Користувачем під час ініціалізації USB-накопичувача, що захищає Електронний ключ, який зберігається на USB-накопичувачі;

Комунікаційна платформа – (Комунікаційний модуль) Комунікаційна платформа для двостороннього обміну листуванням та документами між Банком і Клієнтом;

Продукт – банківський рахунок, кредитний продукт (зокрема: овердрафт, невідновлюваний кредит, відновлюваний кредит, інвестиційний кредит, кредитна картка та інші, що пропонуються Банком) або послуга, що пропонується Банком чи Маклерським бюро на підставі відповідного договору і регламенту;

Підприємець IDG – Клієнт, який є фізичною особою, який веде підприємницьку діяльність, у тому числі в рамках спільної господарської діяльності.

Точка продажу – організаційна одиниця Банку, яка здійснює продаж банківських та інвестиційних продуктів, що розповсюджуються Банком, або відділення, в якому здійснюється діяльність з продажу банківських та інвестиційних продуктів, що розповсюджуються Банком. Положення цього Регламенту щодо обслуговування Електронних каналів КВ поширюються на власні Філії та установи-партнери.

Схема приймання – правило, визначене Клієнтом, яке вказує, скільки користувачів і з яких Груп приймання має підписати Розпорядження, щоб воно було прийняте до виконання Банком

Схема приймання для Центру продуктів – правило, визначене Клієнтом, що вказує, скільки Користувачів і з яких Груп приймання повинні підписати заяву або розпорядження в Центрі продуктів, щоб заява була надіслана до Банку.

Схема довіреностей на Центр продуктів – правило, визначене Клієнтом, що визначає, скільки кількість Користувачів і з яких Груп приймання повинні підписати електронний документ у Центрі продуктів, щоб він був прийнятим.

Схема довіреностей на Правовий модуль – правило, визначене Клієнтом, що визначає, скільки Користувачів і з яких Груп приймання повинні підписати електронний документ у Правовому модулі, щоб його було прийнято.

Схема для комунікаційної платформи – правило, визначене Клієнтом, яке вказує, скільки Користувачів і з яких Груп приймання можуть подавати розпорядження та/або повинні підписати електронний документ на Платформі, щоб він був прийнятий.

Схема представництва – сукупність осіб, уповноважених робити декларації щодо майнових прав та обов'язків від імені та на користь Клієнта у зв'язку зі своїми функціями або на підставі виданих довіреностей.
Схема представництва встановлюється Банком на підставі поточних даних, наявних у публічних реєстрах, або на підставі документів, що мають обов'язкову силу, наданих Банку Клієнтом, і не потребує авторизації Клієнта.
Схема представництва не втрачає чинності, не змінюється, без обов’язкових документів, поданих до Банку Клієнтом, і не скасовується, доки не буде розірвано Рамковий договір між сторонами.

Сильна автентифікація – автентифікація користувача, що забезпечує захист конфіденційності даних на основі використання принаймні двох елементів, що належать до категорії:

1) знання про те, що знає лише Користувач,
2) володіння тим, чим володіє лише Користувач,
3) характерні риси Користувача,
   які є невід'ємною частиною цієї автентифікації та незалежні таким чином, що порушення одного з цих елементів не послаблює надійності інших,

В Банку в рамках методів сильної аутентифікації використовується метод DFP.

Система BankConnect – набір функцій на стороні банку, що забезпечує автоматичний обмін даними між IT-системою Клієнта та IT-системою Банку з мінімальним залученням операторів цих систем. Детальні правила функціонування цієї Системи розглядаються у Додатку № 1 до цього Регламенту

Система BusinessPro – команда взаємодіючих IT-пристроїв та програмного забезпечення, що забезпечує обробку та зберігання, а також надсилання та отримання даних через ІКТ-мережі за допомогою термінального пристрою, відповідного для даного виду мережі, у розумінні Закону про телекомунікації, що дає можливість Банку надавати послуги , яка є частиною Інтернет-банкінгу

Засіб електронної ідентифікації – нематеріальна сутність, що містить ідентифікаційні дані особи та використовується для автентифікації для онлайн-послуг.

Телефон для кодів авторизації (довірений телефон) – номер мобільного телефону, наданий Користувачем, на який надсилаються Стартовий пароль та коди авторизації;

Апаратний токен – зовнішній пристрій, що є фізичним носієм Електронного ключа Системи BusinessPro.

Довговічний носій інформації – Довговічний носій – це матеріал або інструмент, який сукупно відповідає наступним критеріям:

1. дає можливість адресату зберігати інформацію, адресовану особисто йому,
2. дозволяє доступ до інформації в майбутньому протягом періоду, відповідного цілям, для яких ця інформація використовується,
3. дозволяє відновити збережену інформацію без змін.

Договір – Рамковий договір про надання банківських послуг та про ведення рахунків і вкладів для підприємців та інших суб'єктів, укладений між Банком та Клієнтом, у частині, що стосується використання Електронних каналів, цей регламент та положення інших регламентів та договорів, укладених з Банком в частині, в якій вони стосуються використання Електронних каналів.

Рамковий договір – Рамковий договір про надання банківських послуг та ведення рахунків і вкладів для підприємців та інших суб'єктів, укладений між Банком і Клієнтом.

Спеціальний пристрій – пристрій, який Користувач використовує для автентифікації Користувача і який для цієї мети узгоджено між Банком і Користувачем (пов'язаний з Користувачем).

Користувач – Фізична особа з ідентифікатором CIF, уповноважена використовувати Електронні канали від імені Клієнта.

ЗАГАЛЬНІ ПОЛОЖЕННЯ

§2

Цей Регламент є невід'ємною частиною Рамкового договору та визначає правила та умови надання інформації про продукти Клієнта та подання розпоряджень через Електронні канали.

УМОВИ НАДАННЯ ДОСТУПУ ДО ЕЛЕКТРОННИХ КАНАЛІВ

§3

1. Умовою для надання Електронних каналів є:
   1) укладення Клієнтом Рамкового договору,
   2) вказівка Клієнтом хоча б одного Користувача, а також якщо він буде використовувати Інтернет-банкінг – доручення налаштувати для нього права на Продукти.

      В рамках Системи Інтернет-банкінгу для приватних підприємців Банк надає повноваження у повному обсязі без необхідності підписання документів з Клієнтом.
   3) активація Інтернет-банкінгу Користувачем шляхом введення ідентифікатора та стартового пароля,
2. Укладення Рамкового договору та вказівка Користувача може відбуватися особисто в Точці продажу, шляхом листування або іншим способом, запропонованим Банком.

МОБІЛЬНИЙ БАНКІНГ

§4

Умовою для надання Мобільного банкінгу є попередня активація Інтернет-банкінгу та встановлення пароля доступу.

§5

Після активації Інтернет-банкінгу Користувач отримує доступ до Продуктів у обсязі, якого запитує Клієнт.

§6

1. Клієнт може створити разом з іншим Клієнтом або Клієнтами Банку, які мають Систему BusinessPro, пов'язану групу, що полегшує роботу Користувачів шляхом зведеного доступу в Системі BusinessPro до інформації та даних щодо Клієнтів, включених до групи, на одному екрані.
2. Згода Клієнта на приєднання до пов'язаної групи має бути висловлена одноголосно всіма існуючими членами пов'язаної групи.

ОБСЯГ ПОСЛУГ ЕЛЕКТРОННИХ КАНАЛІВ

§7

Через електронні канали ви можете:

1. Керувати своїми коштами
2. Отримувати інформацію про продукти, якими ви володієте,
3. Подавати заявки та укладати договори на вибрані Продукти

Детальний обсяг доступної інформації та перелік Розпоряджень, які можна виконати в окремих Електронних каналах, опубліковані на сайтах Банку, Маклерського бюро та доступні в Точках продажу та у консультантів Contact Center.

РЕАЛІЗАЦІЯ РОЗПОРЯДЖЕНЬ ТА ПРАВИЛА КОРИСТУВАННЯ ЕЛЕКТРОННИМИ КАНАЛАМИ

§8

Розпорядження, розміщені через електронні канали, можна подавати щодня, цілодобово, за умови, що не кожен вид розпорядження може бути виконаний в негайному режимі. Актуальна інформація про порядок та умови виконання Розпорядження розміщена на веб-сайті Банку та Маклерського бюро.

§9

1. Розпорядження, подані через Інтернет-банкінг, потребують авторизації одного або кількох Користувачів відповідно до встановленого Клієнтом способу авторизації та Схеми приймання.
2. Авторизацію можна здійснити за допомогою коду авторизації, Електронного ключа для Системи BusinessPro або за допомогою Кваліфікованого сертифіката.
3. Під час перевірки правильності використаного Кваліфікованого сертифіката Банк спирається на списки CRL (списки відкликаних сертифікатів), які щогодини публікуються емітентами Кваліфікованих сертифікатів. Банк не несе відповідальності за правильність, повноту, актуальність і відповідність фактичному стану списків CRL.

§10

1. Належним чином авторизоване розпорядження з поточною датою виконання не може бути скасована.
2. Положення п. 1 не виключають можливості подання Розпорядження про скасування доручення в рамках надання маклерських послуг на умовах, визначених регламентом надання даної маклерської послуги.

§11

1. Дані, необхідні для правильного виконання Розпорядження, повинні бути надані відповідно до опису полів, наявних у формі розпорядження.
2. Перед авторизацією Користувач повинен переконатися, що Розпорядження є однозначним та відповідає його наміру.

§12

1. Користувач зобов'язаний на постійній основі перевіряти правильність виконання Розпорядження. Про будь-які виявлені порушення слід повідомити шляхом подання рекламації протягом 30 днів після закінчення місяця, якого вони стосуються.
2. Рекламації можуть бути подані:
   1) усно або письмово у відділенні банку,
   2) по телефону,
   3) через систему Інтернет-банкінгу (для зареєстрованого Клієнта),
   4) листом – на адресу для кореспонденції Банку.
3. Банк розглядає рекламації негайно, не пізніше 15 робочих днів (стосується надання платіжних послуг) або 30 календарних днів (в інших випадках) з дня отримання рекламації. У разі платіжних послуг – в особливо складних випадках, що унеможливлюють розгляд рекламації та надання відповіді у вищезазначений термін, Банк: 1) пояснює причину затримки; 2) зазначає обставини, які необхідно встановити для розгляду справи; 3) вказує очікуваний строк розгляду рекламації та відповіді на неї, який не може перевищувати 35 робочих днів з дня надходження рекламації. В інших особливо складних випадках (не пов'язаних з платіжними послугами) цей строк може бути продовжений, але не більше ніж на 60 календарних днів з дня надходження рекламації. Клієнт буде повідомлений про причини затримки, обставини, які потребують з'ясування, та очікуваний строк розгляду рекламації і надання відповіді на неї.
4. Рекламації щодо операцій, що здійснюються за допомогою Карток, розглядаються відповідно до правил та термінів, визначених у Регламенті дебетових карток для корпоративних клієнтів Alior Bank S.A. та в Регламенті кредитних карток для корпоративних клієнтів Alior Bank S.A.
5. Користувач електронних каналів зобов'язаний надати Банку всю інформацію щодо рекламованої операції та надати Банку на його вимогу документи, що стосуються рекламації (рахунки, рахунки-фактури, письмові виписки), а у разі рекламацій щодо несанкціонованих транзакцій чи операцій, Клієнт зобов'язаний передати до Банку:
   1) довідки з поліції або прокуратури про повідомлення про злочин,
   2) детальний опис обставин, за яких дані для входу були втрачені/викрадені (дата, місце, опис події),
   3) детальну заяву про місце і спосіб захисту даних для входу та інструментів для авторизації транзакцій та операцій,

4 іншу інформацію, необхідну для визначення обсягу відповідальності Банку та Користувача Електронних каналів.

6. Банк може попросити Клієнта надати документи щодо рекламованої справи. Якщо через ненадання Клієнтом вищевказаних документів та документів, зазначених у п. 5, буде неможливо провести процедуру рекламації, то відмова у надсиланні або відсутність надсилання цих документів у встановлений Банком строк призведе до розгляду Банком рекламації на підставі документів та інформації. наявних у Банку.
7. Якщо на Рахунок Клієнта була умовно зарахована сума, що є предметом рекламації, то у разі негативного розгляду рекламації Банк відкликає умовне зарахування (списує з Рахунка Клієнта суму рекламації), незалежно від суми балансу на рахунку. Поки рекламація не буде розглянута або умовне повернення не буде відкликано, тобто з Клієнта не буде повторно списана сума рекламації, рахунок не може бути закритий.
8. Відповідь на рекламацію може бути надана в узгодженій із Клієнтом формі:
   1) листом,
   2) через Інтернет-банкінг (для зареєстрованого Клієнта),
   3) через SMS,

   а в обґрунтованих випадках додатково:

   4) по телефону,
   5) у Відділенні Банку.
9. Рекламації на надані маклерські послуги необхідно подавати безпосередньо до Маклерського бюро на умовах, визначених договором або регламентом про надання даної маклерської послуги.

§13

1. Банк фіксує та зберігає на електронних носіях усі телефонні дзвінки, здійснені в рамках Contact Center.
   1) Клієнт і Користувач дають згоду на запис цих розмов;

2) у разі відсутності такої згоди або несправності записуючого пристрою Банк має право відмовити в прийнятті Розпорядження по телефону;
3) у разі сумнівів щодо змісту внесеного Розпорядження, записи розмов є вирішальними і можуть бути використані Банком у рекламаційній процедурі, а також для наведення доказів.

§14

Розпорядження щодо обробки постійних доручень, що виконуються з банківських рахунків, та скасування переказів з відстрочкою виконання приймаються не пізніше ніж за один робочий день до дати виконання Розпорядження.

§15

При виникненні обґрунтованої підозри щодо достовірності поданого Розпорядження Банк може призупинити його виконання до з'ясування сумнівів або відмовити у його виконанні.

§16

1. Через BusinessPro Клієнт і Користувачі можуть виконувати операції залежно від Пакету підписки, який має Клієнт, і додаткових функцій, придбаних для Пакету підписки (Додаткових модулів), відповідно до п. 3 і 4. Види пакетів та Ліміти на кількість Користувачів визначені в § 39 Регламенту.
2. Абонентська плата для кожного Користувача вище ліміту в Пакеті підписки вказана в Таблиці зборів і комісій і стягується наперед з рахунку Клієнта.
3. Функціональні можливості даного Пакету підписки стають доступними після укладання відповідного договору про продукт та його активації,
4. Банк має право змінювати Пакет підписки без зміни документації щодо Інтернет-банкінгу з Клієнтом у разі, якщо на даний момент у Клієнта є Пакет підписки, який був знятий з продажу та технічно вилучений з банківських систем.

ПРАВОВИЙ МОДУЛЬ В СИСТЕМІ BUSINESSPRO

§17

1. Заяви як Клієнта, так і Банку, пов'язані з здійсненням банківської діяльності, можуть бути подані та отримані в електронній формі через призначений для цього Правовий модуль.
2. Правовий модуль є невід'ємною частиною Системи BusinessPro.
3. Зробити доступною систему BusinessPro означає зробити доступним Правовий модуль. Правовий модуль доступний лише для користувачів Системи BusinessPro.
4. Клієнт вказує, скільки Користувачів і з яких Груп приймання має право підписувати електронні документи, подавати та отримувати заяви щодо його майнових прав та обов'язків.
5. Заяви осіб, зазначених у п. 4, вимагають авторизації за допомогою Електронного ключа Системи BusinessPro згідно зі Схемою представництва або Схемою довіреностей для Правового модуля.
6. Будь-які Розпорядження та заяви, подані та отримані через Правовий модуль, якщо вони подані відповідно до Схеми представництва або Схеми довіреностей для Правового модуля, мають юридичні наслідки для Клієнта. Розпорядження та декларації, надані через Правовий модуль, еквівалентні Розпорядженням та деклараціям у письмовій формі.
7. На вимогу Банку Клієнт надає документи, що підтверджують подання та отримання декларацій щодо його майнових прав та обов'язків особами, зазначеними в п. 4.

ЦЕНТР ПРОДУКТІВ

§18

Центр продуктів — це платформа електронного банкінгу, за допомогою якої Клієнт може подати Розпорядження на отримання нових функцій і продуктів, відповідно до пропозицій банківських послуг, доступній в Електронному банкінгу, та поточної Таблиці зборів і комісій.

1. Кожному Розпорядженню, надісланому до Центру продуктів, передуватиме перевірка Схеми приймання до Центру продуктів, зазначеному в § 1 цього Регламенту.
2. Використання Центру продуктів можливе на підставі відповідних дозволів, наданих Банком на підставі заяви Клієнта. Будь-які Розпорядження та заяви, зроблені та отримані через Центр продуктів, якщо вони авторизовані відповідно до Схеми представництва або Схеми довіреностей для Центру продуктів, мають юридичні наслідки незалежно від осіб, які подали Розпорядження чи заяву.
3. Розпорядження та заяви, зроблені через Центр продуктів, еквівалентні Розпорядженням та заявам, зробленим у письмовій формі.

ПРАВИЛА БЕЗПЕКИ

§19

Надаючи послуги на підставі цього Регламенту, Банк зобов'язується забезпечити Користувачеві безпеку виконання Розпоряджень, з належною ретельністю та з використанням відповідних технічних рішень.

§20

Користувач не може надавати неправомірні дані та зобов'язаний дотримуватися рекомендацій Банку щодо правил безпеки при використанні Електронних каналів; зокрема, Користувач зобов'язаний захищати:

- дані, які використовуються для входу в Електронні канали, зокрема: ідентифікатор, паролі, PIN-коди,
- USB-накопичувач із збереженим електронним ключем,
- Карту процесора
- мобільний телефон, номер якого надано в Банку як Телефон для Кодів авторизації (довірений телефон). Користувач зобов'язаний уважно ознайомитися зі змістом Коду авторизації, щоб перевірити його відповідність поданому Користувачем Розпорядженню. Користувач несе повну відповідальність за надання коду авторизації третім особам.

§21

1. У разі підозри, що треті особи володіють будь-яким із паролів, що використовуються в Електронних каналах, Користувач зобов'язаний негайно змінити його або заблокувати Електронні канали.
2. У разі втрати Користувачем USB-накопичувача або Карти процесора із збереженим на ній активним електронним ключем, Користувач зобов'язаний негайно заблокувати ключ.
3. У разі втрати прав особами, зазначеними у Схемі представництва, Клієнт зобов'язаний негайно повідомити Банк про цей факт, тобто про втрату особами, які входять до Схеми представництва, повноважень на подання декларацій щодо майнових прав та зобов'язань від імені та на користь Клієнта за виконуваними функціями або на підставі наданих довіреностей, зокрема, це управління, оприлюднене в Національному судовому реєстрі.

§22

Банк може негайно ввести обмеження та запобіжні заходи щодо Розпоряджень, розміщених Електронними каналами, у разі важливих обставин, що виправдовують введення таких заходів.

§23

Правила безпеки використання Електронних каналів та пов'язані з ними ризики розміщені на веб-сайтах Банку. Інформацію з цього приводу також надає Contact Center. Користувач зобов'язаний їх дотримуватися.

§24

Клієнт може визначити діапазон IP-адрес і часовий діапазон, у який допускається вхід в Систему BusinessPro.

§25

Слід пам'ятати, що електронний доступ до систем банкінгу пов'язаний із ризиками – зокрема, у разі недотримання встановлених Банком правил безпеки. Ці ризики в основному включають:

1. Ризик втрати або викрадення неуповноваженими особами даних або пристроїв:
   1) що використовуються для входу в систему (наприклад, ідентифікатор/пароль або PIN-код для мобільного застосунку),
   2) що використовуються для затвердження операції (наприклад, мобільний пристрій із встановленим застосунком).
2. Ризик атак соціальної інженерії, під час яких треті сторони, видаючи себе за Банк, будуть переконувати Клієнта затвердити операцію (наприклад, неправдива інформація про необхідність придбання транзакції).
3. Ризик несвідомого затвердження ненавмисних доручень Клієнтом (наприклад, без прочитання операції, описаної в SMS-повідомленні з кодом авторизації).
4. Ризик використання, під час використання Електронних каналів, пристроїв, над якими треті сторони взяли контроль віддаленим або фізичним способом (наприклад, за допомогою шкідливого програмного забезпечення, такого як віруси).
5. Наслідками виникнення вищезазначених ризиків можуть бути:
   a. доступ третіх осіб до даних Клієнта, доступних в системах електронного банкінгу,
   b. можливість здійснювати операції третіми особами від імені Клієнта, включаючи фінансові (наприклад, виконання переказів),
   c. можливість затвердження небажаної транзакції Клієнтом.

§26

Основні правила безпеки при використанні Електронних каналів:

1. Ви завжди повинні перевіряти правильність адреси входу в Систему Інтернет-банкінгу https://login.aliorbank.pl/

   При вході зверніть увагу на те, чи не відображає браузер попередження, пов'язані з сертифікатом безпеки (увійдіть у деталі та перевірте дійсність сертифіката) та на префіксом HTTPS в адресі сторінки входу, який доводить, що підключення до сайту Інтернет-банкінгу зашифроване.
2. Перед підтвердженням операції уважно прочитайте все повідомлення одноразового SMS-коду. Банк ніколи не запитуватиме підтвердження операції, яка не була доручена Користувачем.
3. Банк рекомендує регулярно оновлювати операційну систему та встановлене на ній програмне забезпечення, зокрема антивірусне програмне забезпечення (включаючи базу сигнатур вірусів) та використовуваний веб-браузер.
4. Не використовуйте не довірені пристрої для входу в систему Інтернет-банкінгу (наприклад, в інтернет-кафе) або на комп'ютері, на якому зареєстрований інший користувач – також не варто використовувати для цього загальнодоступні мережі Wi-Fi.
5. Слід звернути особливу увагу на атаки, спрямовані на те, щоб переконати вас виконати певну дію (наприклад, натиснути на посилання, завантажити програмне забезпечення, надати свої дані), які надсилаються електронною

поштою, SMS/MMS повідомленнями, соціальними мережами, месенджерами або передаються по телефону.

6. Банк рекомендує не відкривати вкладення та не використовувати посилання з підозрілих електронних листів (наприклад, з помилками, друкарськими помилками, неточною граматикою; з адреси, відмінної від офіційної, неочікувані, тощо), а також не відповідати на ці електронні листи. Підроблені електронні листи є найпоширенішою причиною зараження комп'ютера небезпечними шкідливими програмами.
7. Банк ніколи не вимагатиме від клієнта ввести пароль облікового запису або інші конфіденційні дані через електронну пошту. Будь-який електронний лист із невідомого джерела з посиланням на онлайн-банкінг слід розглядати як спробу фішингу чи інших методів соціальної інженерії. Якщо ви отримали таке повідомлення, ви повинні негайно видалити його. Крім того, доцільно також повідомити Банк про те, що така ситуація сталася.
8. Важливі дані (адреса, номери PESEL, паролі, логіни та інші конфіденційні дані) повинні бути належним чином захищені. Для Користувача неприпустимо передавати свої дані не довіреним суб'єктам або особам. Ви повинні захищати свої документи, а в разі їх втрати чи крадіжки негайно заблокувати їх. Зверніть увагу, що злочинці можуть використати перехоплення ваших даних для крадіжки вашої особи, даних або коштів.
9. Зокрема, варто звернути увагу на інформацію про нові загрози – на сайтах Банку регулярно з'являється інформація про те, як їх розпізнати та уникнути (у розділі Нові загрози та через інформаційні банери на сторінці входу).
10. Звертайте увагу на вміст сторінки входу в систему Інтернет-банкінгу. Якщо процес входу виглядає інакше, ніж зазвичай (наприклад, займає набагато більше часу, з'являються нові вікна, користувача просять підтвердити операцію за допомогою SMS-коду під час входу), негайно зверніться на гарячу лінію (за номером 19 502) – це може свідчити про те, що ваш комп'ютер заражений шкідливим програмним забезпеченням.
11. Якщо у вас виникли запитання/занепокоєння щодо безпеки послуг Банку або ви бажаєте повідомити про інцидент з безпекою, будь ласка, зверніться на гарячу лінію (19 502) або будь-яке відділення Alior Bank.
12. У разі виникнення сумнівів щодо достовірності повідомлень безпеки, отриманих електронною поштою чи іншим каналом, їх необхідно порівняти з інформацією на сайтах Банку в розділі Безпека.

БЛОКУВАННЯ ТА ВІДМОВА ВІД ЕЛЕКТРОННИХ КАНАЛОВ

§27

Блокування означає, що Користувач не може використовувати даний Електронний канал. Блокування Інтернет-банкінгу рівносильно блокуванню Мобільного банкінгу; блокування Мобільного банкінгу рівносильно блокуванню Інтернет-банкінгу.

§28

Кожен з Електронних каналів може бути заблокований Користувачем:

1. самостійно в Інтернет-банкінгу,
2. за телефонним розпорядженням, поданим консультанту Contact Center,
3. за усним розпорядженням, поданим в Точці продажу,
4. в результаті перевищення ліміту неправильних спроб входу, встановленого для даного Електронного каналу.

§29

Користувач може розблокувати Інтернет та Мобільний банкінг – за усним розпорядженням, поданим в Точці продажу, або за телефонним розпорядженням, поданим через Contact Center, за умови, що цей канал активний.

§30

У разі розірвання Договору Клієнтом, Банк блокує всі Електронні канали, які використовував Клієнт.

§31

Банк залишає за собою право постійно або тимчасово блокувати доступ Користувача до Електронних каналів:

1. якщо буде виявлено, що користувач істотно порушує положення:
   a. укладеного Договору,
   b. цього Регламенту
   c. положень чинного законодавства на території Республіки Польща;
2. у випадках, виправданих міркуваннями безпеки. Банк негайно повідомить Клієнта про таку подію.

ДОСТУП ДО ІНФОРМАЦІЇ ПРО РАХУНОК КЛІЄНТА

§32

1. Користувач Інтернет-банкінгу, який має доступ до рахунку бізнес-клієнта Alior Bank, може скористатися послугою доступу до інформації про рахунок у розумінні Закону про платіжні послуги від 19 серпня 2011 р.(зведений текст Законодавчий вісник, № 199, поз. 1175 із змінами);
2. Користувач не може, використовуючи послугу доступу до інформації, що надається третьою стороною, отримати більш широкий доступ до інформації про продукти, яку міг би отримати, увійшовши безпосередньо в Інтернет-банкінг.

СИЛЬНА АВТЕНТИКАЦІЯ КОРИСТУВАЧА

§33

1. Банк використовує сильну автентифікацію, коли Користувач отримує доступ до свого рахунку в режимі онлайн або

ініціює платіжну операцію через Інтернет-банк або Мобільний банкінг. Сильна автентифікація використовується з моменту її надання в IT-системах Банку протягом терміну, передбаченого законодавством.

2. Для входу в Інтернет-банкінг Банк використовує Сильну автентифікацію з використанням наступних методів:
   a. Користувач надає Ідентифікатор та Пароль доступу, а потім:
      i. у разі входу за допомогою Коду авторизації – вводить Код авторизації в Інтернет-банкінг;
   b. Користувач може визначити пристрій, з якого здійснюється вхід, як Виділений пристрій. У цьому випадку користувач вибирає даний пристрій в Інтернет-банкінгу як Виділений пристрій і зобов'язується гарантувати, що він буде єдиним користувачем цього Виділеного пристрою. Потім, щоразу, коли ви входите в систему, Банк перевіряє, чи входить користувач за допомогою Виділеного пристрою. Вхід в систему відбувається після введення Користувачем Ідентифікатора та Пароля, після чого банк перевіряє Виділений пристрій.
   c. Вхід за допомогою Виділеного пристрою може відбуватися протягом періоду, визначеного Банком, при цьому Банк може вимагати автентифікацію з використанням Коду авторизації також з міркувань безпеки.
3. Для входу в Мобільний банкінг за допомогою Мобільного додатка Банк використовує Сильну автентифікацію за допомогою методу верифікації Виділеного пристрою, а потім, у разі входу за допомогою PIN-коду авторизації, – Користувач вводить PIN-код авторизації в Мобільний застосунок.

§34

Користувач заявляє, що він є єдиним власником Виділеного пристрою, зазначеного в § 33, п. 2б, і зобов'язується не надавати цей пристрій третім особам.

ТЕХНІЧНА ПЕРЕРВА

§35

1. У разі планових перерв у доступі до Електронних каналів Банк завчасно повідомляє Клієнта про недоступність системи не менше ніж за 72 години. Банк звільняється від відповідальності за наслідки обмежень обслуговування.

ЗМІНА РЕГЛАМЕНТУ

§36

(Положення цього параграфа застосовуються лише до Клієнта, який не є Підприємцем IDG)

1. Банк залишає за собою право вносити зміни до цього Регламенту, зокрема з причин, зазначених у § 36a.

2. У разі внесення змін до положень Регламенту протягом терміну дії Рамкового договору, Банк зобов'язаний передати Власнику зміни до Регламенту або Регламент з урахуванням змін разом із визначенням терміну набрання чинності змінами, не менше 14 днів з дати вручення. Банк може повідомити про зміни:
   a. шляхом розміщення змін у банківській виписці з рахунка, наданого Власнику рахунку/пакету в порядку, визначеному в договорі рахунку/пакету або
   b. шляхом відправлення повідомлення в електронній формі на адресу електронної пошти – якщо послуга пропонується Банком та надання адреси електронної пошти для зв'язку з Банком Власником рахунку/пакету або
   c. шляхом доставки повідомлень Власнику в електронній формі через систему Інтернет-банкінгу – якщо Власник рахунку активував доступ до цієї системи або
   d. листом на вказану адресу для листування
3. Якщо Власник не розірве Договір протягом 14 днів з моменту отримання тексту внесених змін, вважається, що зміни прийняті і сторони є обов'язковими для виконання.

ЗМІНА РЕГЛАМЕНТУ

§36a

(Положення цього параграфа поширюються лише на Підприємця IDG)

1. Банк залишає за собою право вносити зміни до цього Регламенту лише за наявності хоча б однієї з наступних причин:
   a. зміна чинного законодавства, що регулюють виконання Банком Регламенту. Зміна буде відбуватися в тій мірі, в якій зміни мають прямий вплив на положення змінюваних положень Регламенту,
   b. видання рішення, вказівки, рекомендації чи тлумачення щодо виконання Договору органом державного управління чи іншим органом, який відповідно до чинного законодавства має або отримає в майбутньому повноваження щодо Банку, включаючи Національний банк Польщі, Комісію фінансового нагляду, Європейське управління фінансового нагляду (EBA), Європейський орган з цінних паперів і ринків (ESMA) – наскільки ці рішення, рекомендації, вказівки чи тлумачення мають прямий вплив на положення змінюваної частини Регламенту,
   c. надання нових функціональностей в Електронних каналах (далі: «функціональність»), з умовою, що зміни, внесені Банком, не можуть бути підставою для введення або підвищення зборів і комісій у сфері обслуговування функціональності (якщо зміни вносяться без згоди Клієнта),
   d. вилучення функціональності, якщо витрати, понесені Банком у результаті підтримки функціональності, є: 1) непропорційними кількості клієнтів, які використовують дану функціональність або 2) кількість клієнтів, які використовують дану функціональність, незначна по відношенню до всіх клієнтів, які використовують систему, яка пропонує дану функціональність, або 3) функціональність технологічно застаріла в порівнянні з рішеннями, пропонованими на банківському ринку. Банк сповіщає Клієнта про вилучення функціональності принаймні за три місяці.

e. зміна форми надання послуги шляхом її оцифровування (перенесення на Електронні канали), якщо зміна не суперечить чинному законодавству або прямому вибору Клієнта, висловленому при укладенні Договору,
f. відкликання окремих послуг, що надаються за Регламентом, якщо витрати, понесені Банком у зв'язку з наданням послуги, є: 1) непропорційними кількості клієнтів, які користуються послугою, або 2) кількість клієнтів, які користуються даною послугою, є незначною по відношенню до загальної кількості клієнтів, на яких поширюється дія Регламенту.

   Відкликані послуги не можуть бути істотними елементами змісту Регламенту. Банк повідомляє Клієнта про відкликання послуги щонайменше за три місяці,
g. зміна методів автентифікації, що використовуються на даний момент в Електронних каналах Банку, якщо на фінансовому ринку будуть доступні більш безпечні рішення, ніж ті, що використовуються на даний момент,
h. надання Клієнтам нових послуг або додаткових функціональностей опціонального характеру,
i. у разі зміни назв послуг або спрощення положень Регламенту, з умовою, що зміни будуть мати редакційний характер та не впливатимуть на взаємні права та обов'язки Банку та Клієнта,
j. внесення змін у порядок, що виникають внаслідок змін, внесених з причин, зазначених у пунктах a та вище.

2. У разі внесення змін до положень Регламенту протягом терміну дії Рамкового договору, Банк зобов'язаний передати Власнику зміни до Регламенту або Регламент з урахуванням змін разом із визначенням терміну набрання чинності змінами, не менше 14 днів з дати вручення. Банк може повідомити про зміни:
a. шляхом оприлюднення змін у виписці з банку з рахунку, доставленій Власнику рахунку/пакету способом, зазначеним у договорі рахунку/пакету або
b. шляхом відправлення повідомлення в електронній формі на адресу електронної пошти – якщо послуга пропонується Банком та надання адреси електронної пошти для зв'язку з Банком Власником рахунку/пакету або
c. шляхом доставки повідомлень Власнику в електронній формі через систему Інтернет-банкінгу – якщо Власник рахунку активував доступ до цієї системи або
d. листом на вказану адресу для листування

3. Якщо Власник не розірве Договір або Рамковий договір протягом 14 днів з моменту отримання тексту внесених змін, вважається, що зміни прийняті і сторони є обов'язковими.

§37

Банк залишає за собою право надавати певні послуги в рамках Електронних каналів через зовнішні організації, зокрема дочірні компанії. Дані, передані цим організаціям, є об'єктами банківської таємниці та положень Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також скасування Директиви 95/46/ЕС (загальний регламент про захист персональних даних) і підлягають захисту в такому ж обсязі, як і у випадку з Банком. Банк несе повну відповідальність за операції, що здійснюються через цих суб'єктів.

Заключні положення

§38

За діяльність, пов'язану з наданням та експлуатацією Електронних каналів, Банк стягує збори і комісію відповідно до чинного Тарифу зборів і комісій Банку або Маклерського бюро.

СПИСОК ФУНКЦІОНАЛЬНОСТЕЙ, ДОСТУПНИХ У ПАКЕТАХ ПІДПИСКИ СИСТЕМИ BusinessPro

§39

Список функціональностей, доступних у пакетах підписки системи BusinessPro

§1

Модуль або група функціональностей	**Функціональність або види операцій**	**Пакет Firma**	**Пакет Basic**	**Пакет Profes-sional**
Ліміт кількості Користувачів	Ліміт кількості Користувачів у рамках Пакету підписки	**3**	**6**	**9**
Персоналізація налаштувань	Персоналізація робочого столу, мовні версії (польська, англійська)	**Так**	**Так**	**Так**
Правовий модуль	Створення, надсилання, отримання та зберігання електронних документів, пов'язаних з банківською діяльністю, активацією та управлінням продуктом.	Ні	**Так**	**Так**
Комунікаційний модуль	Комунікаційна платформа для двостороннього обміну листуванням між Банком і Клієнтом	**Так**	**Так**	**Так**
Центр продуктів	Платформа для подачі заявок на нові функціональності та продукти з пропозиції послуг банку	**Так**	**Так**	**Так**
Обмеження в рамках безпеки	Вхід за допомогою електронного підпису, збереженого на мікропроцесорних картах, контроль доступу за часом (календар, дні тижня, години) та контроль IP-адрес	**Так**	**Так**	**Так**
Адміністрація	Попередній перегляд прав Користувачів і Схем приймання, керування Картками	**Так**	**Так**	**Так**
Фінансова інформація	Список банківських рахунків, поточний баланс, історичний баланс та обороти, історія операцій, виписки з Банківських рахунків (крім депозитів), платіжні картки	**Так**	**Так**	**Так**
Cash Management	Звіти Cash Management про транзакційні продукти – огляд та управління	Ні	**Так**	**Так**
Cash Management	Індивідуальні поточні та історичні курси валют	**Так**	**Так**	**Так**
Дані словника	Дані словника контрагентів, банків, номери рахунків податкових установ	**Так**	**Так**	**Так**
Платіжне доручення	Вихідний внутрішній переказ, внутрішній переказ (переказ між рахунками, що ведуться в Банку), переказ для податкових органів	**Так**	**Так**	**Так**
Платіжне доручення	Внутрішній переказ у валюті, іноземний переказ	**Так**	**Так**	**Так**
Платіжне доручення	Масові платежі (списання з рахунку однієї сукупної суми), Заробітна плата (зарплатний переказ)	Ні	**Так**	**Так**
Платіжне доручення	Регулярні доручення	Ні	**Так**	**Так**
Платіжне доручення	Повідомлення про зняття готівки	**Так**	**Так**	**Так**
Доручення	Управління дорученнями – перегляд доручень, підписання та відправлення доручень, історія доручень	**Так**	**Так**	**Так**
Експорт / Імпорт	Імпорт і експорт даних транзакцій і словника, звітів, завантаження файлів	Ні	**Так**	**Так**
Експорт / Імпорт	Попередньо визначені та індивідуально визначені формати імпорту та експорту, звітів	Ні	**Так**	**Так**
Депозити	Створення депозитів, перегляд депозитів	**Так**	**Так**	**Так**
AutoDealing	AutoDealing (підтримка податкових продуктів) AutoDealing Lite (підтримка податкових продуктів у мобільній версії), EfxTrader	**Так**	**Так**	**Так**
Модуль аналізу	Перегляд фінансів	Ні	**Так**	**Так**
Модуль аналізу	Моніторинг поточного балансу, аналіз ліквідності та історії операцій	Ні	**Так**	**Так**
Повідомлення	Електронна пошта та SMS-повідомлення, надіслані після події в Системі BusinessPro	Ні	**Так**	**Так**
Пов'язані групи	Створення Пов’язаної групи	Ні	Ні	**Так**
Додатковий модуль Cash Management	Прямий дебет, Обслуговування готівки у закритій формі, поповнення готівки та переказ готівки, автоматичне зняття готівки, факторинг	Ні	Ні*	**Так**
Додатковий модуль Модуль довіреності	Модуль довіреності – рахунки, портфелі, операції, корпоративні події	Ні	Ні*	**Так**
Мобільний банкінг	Використання Спрощеної версії Системи BusinessPro за допомогою мобільних пристроїв	**Так**	**Так**	**Так**

* **Так** у разі активації додаткового модуля, що розширює функціональність Пакету підписки Basic

§ 2

Модуль або група функціональностей	Функціональність або види операцій	Пакет CLASSIC
Ліміт кількості Користувачів	Ліміт кількості Користувачів у рамках Пакету підписки	**2**
Максимальна кількість користувачів	Максимальна кількість користувачів у Пакеті підписки	**Без обмежень**
Фінансова інформація	Список банківських рахунків, поточний баланс, історичний баланс та обороти, історія операцій, виписки з Банківських рахунків (крім депозитів)	**Так**
Фінансова інформація	Список кредитних рахунків, графік погашення, інформація про кредит	**Так**
Платіжні картки	Обслуговування платіжних карток, управління мультивалютною карткою	**Так**
Модуль аналізу	Моніторинг поточного балансу, аналіз ліквідності та історії операцій, Фінансовий огляд, Контроль поточного чистого балансу, Звіт про лінії заборгованості	**Так**
Платіжне доручення	Вихідний внутрішній переказ, внутрішній переказ (переказ між рахунками, що ведуться в Банку), переказ для податкових органів	**Так**
Платіжне доручення	Внутрішній переказ у валюті, іноземний переказ	**Так**
Платіжне доручення	Повідомлення про зняття готівки	**Так**
Платіжне доручення	Регулярні доручення	**Так**
Доручення	Управління дорученнями – перегляд доручень, підписання та відправлення доручень (кошик доручень), історія доручень	**Так**
Дані словника	Дані словника контрагентів, банків, номери рахунків податкових органів	**Так**
Депозити	Створення депозитів, перегляд депозитів	**Так**
Персоналізація налаштувань	Персоналізація робочого столу, мовні версії (польська, англійська)	**Так**
Правовий модуль	Створення, надсилання, отримання та зберігання електронних документів, пов'язаних з банківською діяльністю, активація та управління продуктами	**Так**
Комунікаційний модуль	Комунікаційна платформа для двостороннього обміну кореспонденцією між Банком та Клієнтом у сфері основних тематичних категорій	**Так**
Обмеження в рамках безпеки	Вхід з використанням електронного підпису, що зберігається на мікропроцесорних картах, контроль доступу за часом (календар, дні тижня, години) та контроль IP-адрес	**Так**
Адміністрація	Попередній перегляд прав користувачів і Схем приймання, можливість делегування прав	**Так**
Курси валют	Індивідуальні поточні та історичні курси валют	**Так**
Повідомлення	Електронна пошта та SMS-повідомлення, надіслані після події в Системі BusinessPro	**Так**
Мобільний банкінг	Використання Спрощеної версії Системи BusinessPro з використанням мобільних пристроїв	**Так**
AutoDealing	AutoDealing (підтримка податкових продуктів) AutoDealing Lite (підтримка податкових продуктів у мобільній версії), EfxTrader	**Так****
Факторинг	AliorFaktor (спеціальний застосунок для підтримки факторингу)	**Так****
Додатковий модуль Центру продуктів	Платформа для заявки на нові функціональні можливості та продукти з пропозиції банківських послуг	**Так**
Додатковий модуль Імпорт/Експорт	Імпорт та експорт даних операцій і словника, звітів, завантаження файлів; Попередньо визначені та індивідуально визначені формати для імпорту, експорту, звітів, масових платежів (списання з рахунку однієї сукупної суми), можливість експорту банківських виписок у форматах MT940 та JPK (стандартний контрольний файл).	Ні*
Додатковий модуль MRP – Рахунки житлового довірчого управління	Модуль призначений для обслуговування рахунків житлового довірчого управління	Ні*
Додатковий модуль Cash Management	Прямий дебет, Обслуговування готівки у закритій формі, поповнення та переказ готівки, автоматичне зняття готівки, масова обробка транзакцій, Звіти Cash Management про транзакційні продукти – огляд та управління; Заробітна плата (зарплатний переказ), масовий зарплатний переказ	Ні*
Додатковий модуль Пов'язані групи	Створення Пов'язаної групи (можливість об'єднання двох або більше компаній в одному робочому контексті)	Ні*
Додатковий модуль Довіреність	Модуль довіреності – рахунки, портфелі, операції, корпоративні події	Ні*

* **Так,** у разі активації додаткового модуля, що розширює функціональність Пакету
** Необхідно укласти спеціальний договір на продукт