

Порядок взаємодії Банку зі стороннім надавачем платіжних послуг з ініціювання платіжної операції в межах відкритого банкінгу

(витяги з Положення про реалізацію відкритого банкінгу АТ «БАНК КРЕДИТ ДНІПРО» як надавачем платіжних послуг з обслуговування рахунку, затвердженого Комітетом з операційних, комплаєнс ризиків, ESG та інформаційної безпеки, протокол №48.1 від 30.07.2026 року)

1.1. Положення про реалізацію відкритого банкінгу АТ «БАНК КРЕДИТ ДНІПРО» як надавачем платіжних послуг з обслуговування рахунку (далі — Положення) регламентує умови здійснення відкритого банкінгу АТ «БАНК КРЕДИТ ДНІПРО» (далі — Банк) та порядок виконання дій структурними та відокремленими підрозділами Банку при реалізації відкритого банкінгу, яким є структурований і безпечний обмін даними між Банком як НПП з обслуговування рахунку та СНПП через спеціалізовані інтерфейси, який здійснюється за згодою користувача під час доступу СНПП до рахунку користувача з метою надання таким СНПП користувачу нефінансових платіжних послуг.

3.1. У цьому Положенні нижченаведені терміни вживаються у такому значенні:

- користувач – клієнт Банку – фізична особа, юридична особа, фізична особа – підприємець або фізична особа, яка провадить незалежну професійну діяльність, який має в Банку відкритий рахунок (крім кореспондентського рахунку банку та розрахункового рахунку надавача платіжних послуг);

3.2. У Положенні використані наступні скорочення:

- НПП – надавач платіжних послуг;

- СНПП – сторонній надавач платіжних послуг;

6.10. У разі виявлення неакцептованих, помилкових та неналежних платіжних операцій, ініційованих користувачем через НПП з ініціювання платіжної операції, здійснюється вжиття заходів для запобігання або припинення таких операцій, а саме:

6.10.1. У разі виявлення помилкової або неакцептованої операції по рахунку користувача, Банк зобов'язаний негайно після виявлення факту виконання такої операції або після отримання повідомлення користувача (залежно від того, що відбувалося раніше) повернути за рахунок власних коштів суму помилкової/ неакцептованої платіжної операції, а також суму утриманої / сплаченої користувачем комісійної винагороди за виконану помилкову/неакцептовану платіжну операцію (за наявності такої комісійної винагороди) на рахунок користувача.

6.10.2. Банк сприяє користувачу в поверненні коштів за неналежною, помилковою, неакцептованою платіжною операцією шляхом надання доступної йому інформації про таку операцію, у тому числі отриманої на його запит від надавача платіжних послуг, що обслуговує неналежного отримувача.

7.3. Взаємодія Банку з СНПП під час розгляду звернень:

7.3.1. У випадках отримання звернення користувача або самостійного виявлення Банком шахрайства (підозри шахрайства), загрози безпеці виконання платіжної операції, ініційованої користувачем через НПП з ініціювання платіжної операції, та/або надання відомостей з рахунків користувача через НПП з надання відомостей з рахунків, або здійснення неакцептованих, помилкових, неналежних платіжних операцій, ініційованої користувачем через СНПП та/або надання відомостей з рахунків користувача через СНПП Банк звертається до СНПП з вимогою надати інформацію та, за потреби, додаткові документи щодо наданої таким СНПП нефінансової платіжної послуги користувачу. Взаємодія з СНПП в такому випадку відбувається в наступному порядку:

1) Банк звертається до СНПП з письмовим запитом необхідної інформації/документів щодо ініціювання платіжної операції та/або ініціювання згоди/ запитів на отримання відомостей з рахунків шляхом направлення запиту на електронну пошту такого СНПП;

2) у разі надходження відповіді від СНПП протягом трьох робочих днів, Банк проводить розслідування, за наслідком якого, у разі відсутності вини користувача, Банк повертає грошові кошти за відповідними операціями користувачу, при цьому у випадку отримання доказів вини СНПП, через якого була

ініційована відповідна платіжна операція, Банк має право направити претензію до такого СНПП щодо відшкодування понесених збитків за відповідними платіжними операціями;

3) у разі ненадходження відповіді від СНПП протягом трьох робочих днів, Банк проводить додаткову комунікацію з відповідним СНПП засобами телефонного зв'язку, а у випадку неспішності такої комунікації Банк вирішує питання щодо доцільності звернення до НБУ із скаргою щодо роботи такого СНПП.

Дії Банку у випадку виявлення загрози безпеці виконання платіжної операції додатково регулюються внутрішніми документами з питань інформаційної безпеки.

У разі виявлення або отримання інформації про загрозу інформаційній безпеці при виконанні платіжних операцій, ініційованих користувачем у рамках відкритого банкінгу, Банк забезпечує взаємодію з СНПП та застосування заходів реагування, включаючи обмеження доступу. Джерелом інформації про такі загрози можуть бути повідомлення від користувачів (клієнтів Банку) або від СНПП. Порядок, канали та строки інформування, а також вимоги до обміну інформацією визначаються відповідними договорами (угодами) між Банком та СНПП з урахуванням вимог інформаційної безпеки Банку. Детальний порядок виявлення, реагування, розслідування та документування інцидентів інформаційної безпеки визначається Політикою інформаційної безпеки Банку, Політикою управління інцидентами інформаційної безпеки та Планом реагування на кіберзагрози, кібератаки та кіберінциденти в Банку.

7.3.2. У разі звернення СНПП до Банку з питань, пов'язаних з шахрайством (підозрою шахрайства), загрозою безпеці виконання платіжної операції або неакцептованими, помилковими, неналежними платіжними операціями, ініційованими користувачем через СНПП та/або наданням відомостей з рахунків користувача через СНПП, Банк опрацьовує такі звернення протягом 5 робочих днів з дати отримання такого звернення.