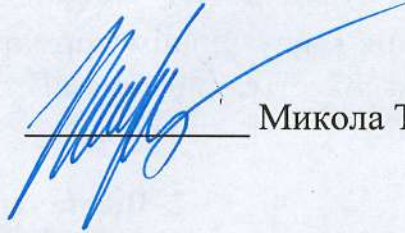


ЗАТВЕРДЖЕНО

Рішенням Правління Полікомбанку

(протокол від 23.07.2026 № 32)

Голова Правління



Микола ТАРАСОВЕЦЬ

ПОЛОЖЕННЯ

про відкритий банкінг в акціонерному товаристві "Полікомбанк"

1. Загальні положення

1.1. Положення визначає порядок взаємодії Банку при наданні доступу до фінансових даних клієнтів стороннім надавачам платіжних послуг під час надання нефінансових платіжних послуг через API.

1.2. Положення розроблено відповідно до таких нормативних документів:

- Закону України "Про платіжні послуги";
- Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку, затвердженого Постановою Правління НБУ від 03.05.2023 № 58, далі – Положення № 58;
- Положення про відкритий банкінг в Україні, затвердженого Постановою Правління НБУ від 25.07.2025 № 80, далі – Положення № 80;
- Положення про порядок здійснення авторизації діяльності надавачів нефінансових платіжних послуг, затвердженого Постановою Правління НБУ від 25.07.2025 № 81;
- Положення про використання електронних довірчих послуг під час отримання надавачами платіжних послуг доступу до рахунків користувачів платіжних послуг, затвердженого Постановою Правління НБУ від 25.07.2025 № 82.

1.3. Вимоги цього Положення поширюються на відносини, що виникають під час доступу до рахунків користувачів та надання користувачам нефінансових платіжних послуг сторонніми НПП між:

- 1) НПП з обслуговування рахунків;
- 2) сторонніми НПП;
- 3) технологічними операторами платіжних послуг, що отримали право на надання послуг у межах відкритого банкінгу (далі – технологічний оператор);
- 4) користувачами.

1.4. Положення визначає:

- 1) порядок та умови надання НПП з обслуговування рахунку доступу до рахунків користувачів сторонніми НПП у межах відкритого банкінгу;
- 2) порядок та умови отримання сторонніми НПП доступу до рахунків користувачів у межах відкритого банкінгу;
- 3) принципи взаємодії суб'єктів відкритого банкінгу;

- 4) умови надання сторонніми НПП нефінансових платіжних послуг користувачам;
- 5) порядок надання та відкликання згоди користувача;
- 6) принципи використання та класифікація спеціалізованих інтерфейсів, які використовуються у відкритому банкінгу.

1.5. Положення є внутрішнім нормативним документом, який затверджується, змінюється або скасовується рішенням Правління банку та підлягає виконанню всіма працівниками банку.

2. Визначення термінів

Відкритий банкінг – це безпечний обмін даними між Банком та стороннім НПП через спеціалізовані інтерфейси, який здійснюється за згодою користувача платіжних послуг (далі – користувач) під час доступу до рахунку користувача стороннього НПП, з метою надання таким стороннім НПП нефінансових платіжних послуг користувачу через стандартизовані API (інтерфейси програмування).

НПП з обслуговування рахунку – Акціонерне товариство «Полікомбанк»/Банк в якому відкритий рахунок користувача (платника) для виконання платіжних операцій;

Нефінансові платіжні послуги – це послуга з ініціювання платіжної операції та послуга з надання відомостей з рахунків, що надаються користувачу сторонніми НПП;

Сторонні НПП – це банки, що отримали право на надання нефінансових платіжних послуг, та надавачі нефінансових платіжних послуг;

Надавачі нефінансових платіжних послуг –

а) **НПП з ініціювання платіжної операції, далі – НПП з ініціювання**, – юридична особа, яка в установленому порядку, визначеному Законом та НБУ, отримала право на надання послуг з ініціювання платіжної операції;

б) **НПП з надання відомостей з рахунків, далі – НПП з надання відомостей**, – юридична особа, яка в установленому порядку, визначеному Законом та НБУ, отримала право на надання послуг з надання відомостей з рахунків;

Користувач – фізична або юридична особа, яка отримує чи має намір отримати платіжну послугу як платник або отримувач та/або є власником електронних грошей.

API – прикладні програмні інтерфейси, що ґрунтуються на загальних стандартах та забезпечують обмін даними між надавачами платіжних послуг, технологічними операторами платіжних послуг.

Базові спеціалізовані інтерфейси – загальнодоступні та безоплатні інтерфейси, що призначені для організації електронної взаємодії між НПП з обслуговування рахунку та стороннім НПП, реалізація яких є обов'язковою для всіх НПП з обслуговування рахунків, згідно з вимогами цього Положення, Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку, затвердженого постановою Правління НБУ від 03.05.2023 № 58 (далі – Положення НБУ № 58) та специфікації електронної взаємодії НПП з обслуговування рахунку та сторонніх НПП у відкритому банкінгу;

Спеціалізовані інтерфейси – це набір протоколів взаємодії, які забезпечують обмін даними між НПП з обслуговування рахунку та стороннім НПП шляхом взаємодії інформаційних систем під час доступу до рахунку користувача стороннього НПП з метою надання таким стороннім НПП нефінансових платіжних послуг користувачу;

Доступ до рахунку – можливість отримання стороннім НПП визначеного користувачем обсягу інформації щодо рахунку та користувача такого рахунку, якою на вимогу та за згодою такого користувача має забезпечити НПП з обслуговування рахунку з метою надання таким стороннім НПП такому користувачу послуг з ініціювання платіжної операції та/або з надання відомостей з рахунків;

Згода користувача – це згода користувача на надання відомостей з рахунків або згода на виконання платіжної операції, яка надається користувачем НПП з обслуговування рахунку через стороннього НПП, якому надається доступ до рахунку користувача через спеціалізовані інтерфейси з метою отримання таким користувачем нефінансових платіжних послуг, що надаються стороннім НПП;

Комерційні спеціалізовані інтерфейси – це інтерфейси, що призначені для організації електронної взаємодії між НПП з обслуговування рахунку та стороннім НПП, які не відносяться до базових спеціалізованих інтерфейсів і можуть включати плату за їх використання на умовах договірних відносин.

Посилена автентифікація – процедура автентифікації, яка передбачає використання двох чи більше сукупностей даних, що належать до таких категорій:

- 1) знань (володіння інформацією, що відома лише користувачу;
- 2) володінь (застосування матеріального предмету, яким володіє лише користувач);
- 3) притаманності (перевірка біометричних даних або інших властивостей, притаманних лише користувачу, що відрізняють його від інших користувачів)

Технологічний оператор платіжних послуг – юридична особа, що надає послуги процесингу, клірингу або виконує операційні, інформаційні та інші технологічні функції, пов'язані з наданням платіжних послуг, без залучення коштів за платіжними операціями на свій рахунок.

Реєстр платіжної інфраструктури – це офіційний перелік учасників платіжних систем, який веде Національний банк України. Він містить інформацію про банки та небанківських надавачів платіжних послуг, які отримали ліцензію на здійснення такої діяльності та є учасниками платіжних систем.

Відповідальний працівник – працівник Банку, на якого рішенням Голови Правління покладено функції щодо впровадження, супроводження, адміністрування, контролю та забезпечення діяльності Банку у сфері викритого банкінгу, а також взаємодії з іншими учасниками відкритого банкінгу в межах його повноважень.

Інші терміни в цьому Положенні вживаються в значеннях, наведених у Законі України “Про платіжні послуги” а також нормативно-правових актах НБУ з питань регулювання платіжного ринку.

3. Порядок роботи Банку в межах відкритого банкінгу

3.1. Банк надає сторонньому НПП доступ до рахунку користувача в режимі реального часу через спеціалізовані інтерфейси, що поділяються на базові спеціалізовані інтерфейси та комерційні спеціалізовані інтерфейси лише за згодою користувача.

3.2. Доступ до рахунку користувача через базові спеціалізовані інтерфейси надаються Банком на безоплатній основі для такого стороннього НПП та без укладання договору між такими НПП.

3.3. Банк під час надання сторонньому НПП доступу до рахунку користувача через базові спеціалізовані інтерфейси зобов'язаний забезпечити виконання:

1) платіжної інструкції щодо разової платіжної операції, наданої користувачем через НПП з ініціювання;

2) запитів щодо надання відомостей з рахунку, а саме щодо суми доступних коштів на рахунку користувача (баланс) та/або історії операцій (за період, що становить не більше, ніж 31 календарний день від поточної дати запиту) конкретного рахунку, наданих користувачем через НПП з надання відомостей з рахунків.

3.4. Банк надає сторонньому НПП доступ до рахунку користувача в режимі реального часу через спеціалізовані інтерфейси лише після:

1) здійснення успішної перевірки авторизації діяльності стороннього НПП щодо відповідної нефінансової платіжної послуги;

2) отримання згоди користувача;

3) отримання дозволу користувача на розкриття інформації, що містить банківську таємницю, комерційну таємницю, таємницю надавача платіжних послуг.

3.5. Банк при наданні послуг відкритого банкінгу зобов'язаний:

1) передбачити в договорі з користувачем на обслуговування рахунку умови надання доступу до рахунку користувача сторонньому НПП та відповідальність сторін під час надання Банком доступу до рахунку сторонньому НПП;

2) отримати дозвіл користувача на надання НПП з обслуговування рахунку стороннім НПП інформації, що містить банківську таємницю, комерційну таємницю, таємницю надавача платіжних послуг;

3) забезпечити можливість постійного доступу до поточних, вкладних рахунків своїх користувачів стороннім НПП у режимі реального часу через базові спеціалізовані інтерфейси;

4) отримавши платіжну інструкцію, забезпечити її наповнення обов'язковими реквізитами, передбаченими п. 4.2. цього Положення;

5) забезпечити безпечний обмін інформацією та захист інформації під час обміну такою інформацією зі стороннім НПП через спеціалізовані інтерфейси;

6) щоденно актуалізовувати відомості про сторонніх НПП, шляхом завантаження відомостей про них зі сторінки офіційного Інтернет-представництва НБУ.

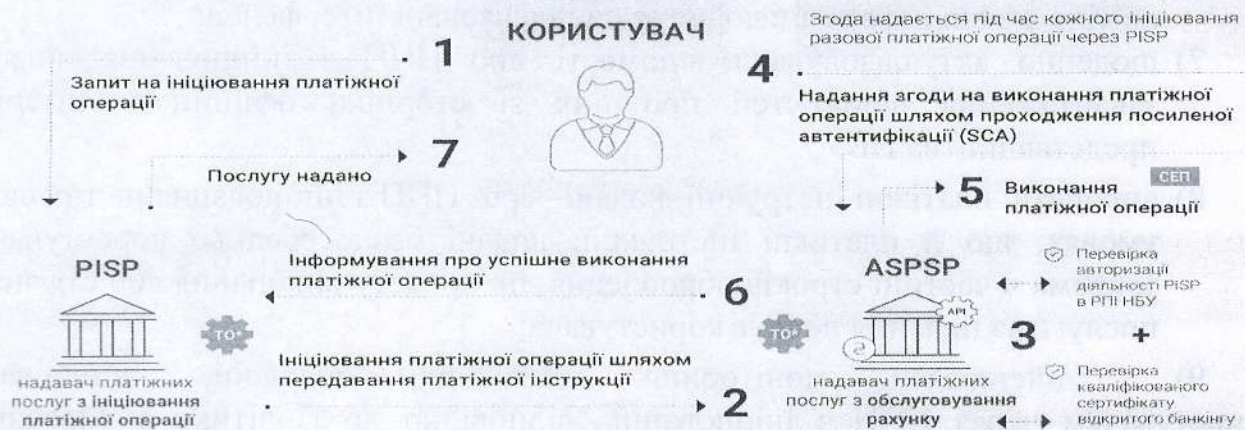
3.6. Перед наданням доступу до рахунку користувача, Банк щоразу здійснює автоматизовану перевірку авторизації діяльності стороннього НПП щодо відповідної нефінансової послуги шляхом:

- 1) перевірки чинності кваліфікованого сертифіката відкритого ключа стороннього НПП із урахуванням вимог Закону України “Про електронну ідентифікацію та електронні довірчі послуги”;
- 2) автентифікації стороннього НПП з використанням його кваліфікованого сертифіката відкритого банкінгу;
- 3) перевірки відомостей про стороннього НПП з Реєстру платіжної інфраструктури (далі – відомості про стороннього НПП);
- 4) порівняння відомостей про стороннього НПП з інформацією, що міститься у кваліфікованому сертифікаті відкритого ключа стороннього НПП.

3.7. Банк зобов’язаний надавати доступ до рахунку користувача лише за умови, що користувач надав активну згоду (тобто згода підтверджена посиленою автентифікацією та є дійсною). Згода користувача повинна бути конкретною: вона повинна визначати конкретного стороннього НПП, конкретний рахунок, нефінансову платіжну послугу, що надається, та точний обсяг інформації про рахунок та користувача, до якої буде надано доступ. Ця згода може бути отримана Банком через уповноваженого стороннього НПП, з яким користувач має договірні відносини.

4. Порядок взаємодії Банку з НПП з ініціювання

4.1. Схема надання послуги з ініціювання платіжної операції.



* Технологічні оператори можуть залучатися ASPSP PISP за потреби

4.2. Ініціювання платіжної операції через НПП з ініціювання здійснюється на підставі платіжної інструкції користувача (платника), яку НПП з ініціювання передає Банку за умови **надання користувачем згоди на ініціювання такої платіжної операції**.

Така платіжна інструкція користувача повинна містити реквізити, визначені чинним законодавством України.

4.3. Банку заборонено в платіжній інструкції користувача, отриманій від НПП з ініціювання, змінювати заповнені ним реквізити.

4.4. Банк виконує платіжну операцію, яка ініційована користувачем через НПП з ініціювання, з рахунку користувача – платника на рахунок отримувача з використанням інструменту кредитового трансферу. Рахунок платника та рахунок отримувача повинні бути відкритими в установах, що є резидентами України.

4.5. Банк зобов'язаний:

- 1) щоразу перед наданням НПП з ініціювання доступу до рахунку користувача, здійснювати перевірку авторизації діяльності НПП з ініціювання щодо відповідної платіжної операції;
- 2) під час отримання згоди на виконання платіжної операції відобразити користувачу (платнику) в засобах дистанційної комунікації деталізовану інформацію про НПП з ініціювання платіжної операції, через якого він ініціює платіжну операцію, дату та час отримання згоди; номер рахунку, з якого ініціюється платіжна операція;
- 3) надати підтвердження в простому форматі "так" або "ні" на запит стосовно наявності на рахунку платника потрібної суми коштів для здійснення платіжної операції;
- 4) забезпечити можливість постійного доступу до поточних, вкладних рахунків своїх користувачів НПП з ініціювання у режимі реального часу через базові спеціалізовані інтерфейси;
- 5) отримавши платіжну інструкцію, забезпечити її наповнення обов'язковими реквізитами, передбаченими п. 4.1. цього Положення;
- 6) забезпечити безпечний обмін інформацією та захист інформації під час обміну такою інформацією через спеціалізовані інтерфейси;
- 7) щоденно актуалізовувати відомості про НПП з ініціювання, шляхом завантаження відомостей про них зі сторінки офіційного Інтернет-представництва НБУ;
- 8) виконати платіжні інструкції, надані через НПП з ініціювання на тих самих умовах, що й платіжні інструкції, надані безпосередньо користувачем, зокрема в частині строків оброблення, пріоритету виконання або стягнення послуги за надання послуг користувача;
- 9) здійснювати моніторинг платіжних операцій, ініційованих користувачем через НПП з ініціювання, відповідно до Політики з управління операційним ризиком, затвердженим рішенням Наглядової ради від 15.09.2023 р., пр. № 15;
- 10) забезпечити зберігання документів та інформації щодо виконання платіжних операцій, ініційованих користувачем через НПП з ініціювання;
- 11) надати можливість користувачу заблокувати доступ до свого рахунку НПП з ініціювання у межах відкритого банкінгу.

4.6. Банк має право:

- 1) заблокувати доступ до рахунку користувача стороннім НПП у межах відкритого банкінгу без звернення користувача в разі виявлення ознак шахрайських чи інших неправомірних дій, пов'язаних з несанкціонованим доступом до рахунку або до вразливих платіжних даних користувача;

2) отримати кваліфікований сертифікат відкритого ключа;

3) передбачити в договорі з користувачем дозвіл користувача на надання НПП з обслуговування рахунку стороннім НПП інформації, що містить банківську таємницю, комерційну таємницю, таємницю надавача платіжних послуг;

4.6. Банку забороняється:

1) передавати інформацію про користувача, що не пов'язана з наданням послуги через спеціалізовані інтерфейси в межах відкритого банкінгу;

2) надавати доступ до рахунку НПП з ініціювання, який не пройшов перевірку авторизації діяльності;

3) надавати доступ до рахунку користувача через спеціалізований інтерфейс без отримання його згоди;

4.7. Банк несе відповідальність:

1) за шкоду, заподіяну користувачу в разі недотримання вимог Положення №80;

2) за невиконання або неналежне виконання платіжних операцій, ініційованих користувачем через НПП з ініціювання та умов укладеного договору, якщо не доведе, що платіжні операції виконані належним чином;

3) за виконання помилкової, неакцептованої платіжної операції.

4.8. Банк в разі здійснення неакцептованих, помилкових, неналежних платіжних операцій, ініційованих користувачем через НПП з ініціювання, на рахунок неналежного отримувача зобов'язаний:

1) на запит користувача щодо такої операції, невідкладно вжити заходів для отримання всієї наявної інформації про платіжну операцію та надати її користувачу без стягнення плати;

2) після виявлення помилкової операції, негайно переказати за рахунок власних коштів суму платіжної операції користувачу, а також сплатити йому пеню в розмірі 0,1% (нуль цілих одна десята відсотка) суми простроченого платежу за кожний день прострочення від дня завершення помилкової платіжної операції до дня переказу коштів на Рахунок користувача, але не більше 10% суми платіжної операції.

3) у разі виконання неакцептованої платіжної операції, негайно після виявлення факту виконання неакцептованої платіжної операції або після отримання повідомлення користувача (залежно від того, що відбулося раніше) повернути за рахунок власних коштів суму неакцептованої платіжної операції на рахунок користувача, а також сплатити йому пеню в розмірі подвійної облікової ставки НБУ за кожний день від дня списання з рахунку користувача коштів за неакцептованою платіжною операцією до дня повернення коштів на його рахунок. Банк зобов'язаний також відшкодувати користувачу суму утриманої/сплаченої ним комісійної винагороди за виконану неакцептовану платіжну операцію (за наявності такої комісійної винагороди).

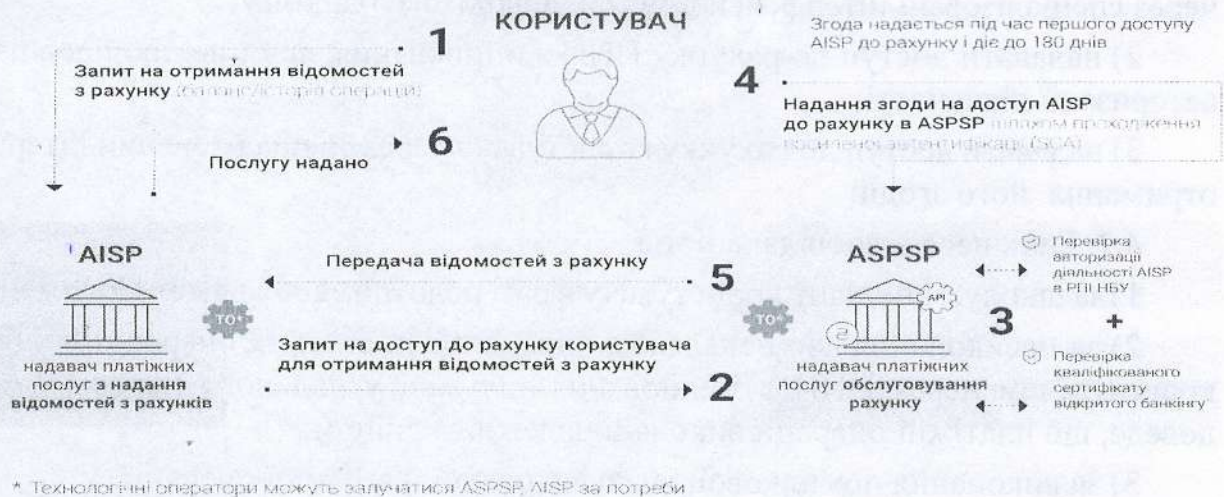
4.9. Банк у разі виникнення непередбачуваної події або помилки, яка сталася під час процесу ідентифікації, автентифікації та/або обміну даними, протягом одного дня надсилає НПП з ініціювання повідомлення/сповіщення з поясненнями стосовно причини непередбачуваної події або помилки.

4.10. Збитки, завдані Банку з вини користувача, або користувачу з вини Банку внаслідок неналежного виконання платіжних операцій, повинні бути відшкодовані

Сторонами в повному обсязі. При цьому Банк або користувач зобов'язані надати документи, що підтверджують факт завдання збитку та його розмір.

5. Порядок взаємодії Банку з НПП з надання відомостей

5.1. Схема надання послуги з надання відомостей з рахунків користувачів.



5.2. Перед наданням першої послуги з надання відомостей з рахунків користувача в договорі банківського рахунку, користувач **повинен надати згоду Банку** на надання НПП з надання відомостей інформації, що містить банківську таємницю, комерційну таємницю, таємницю надавача платіжних послуг, із здійсненням Банком посиленої автентифікації.

Така згода користувача надається Банку на строк, що не перевищує 180 календарних днів, та має відображати таку інформацію:

- 1) дату та час надання такої згоди;
- 2) дату та час відкликання користувачем такої згоди;
- 3) номер рахунку, до якого надано доступ;
- 4) дозволений обсяг отримання інформації щодо рахунку користувача.

5.3. Банк при отриманні згоди користувача на надання відомостей з його рахунків засобами дистанційної комунікації надає таку інформацію:

- 1) номер рахунку, до якого надається доступ;
- 2) обсяг інформації щодо рахунку користувача;
- 3) строк дії наданої дозволу користувачем;
- 4) умови відкликання дозволу користувача на надання відомостей та інформації або посилання на документ, в якому вони містяться.

5.4. Банк відмовляє користувачу у прийнятті його згоди про надання відомостей та інформації з закритих рахунків.

5.5. Послуга з надання відомостей з рахунків користувача в межах відкритого банкінгу має бути доступна НПП з надання відомостей до поточного, вкладного (депозитного) або платіжного рахунку користувача через базові спеціалізовані інтерфейси на безоплатній основі для такого НПП та без укладання з ним договору.

5.6. Банк щоразу, при взаємодії з НПП з надання відомостей:

- 1) перевіряє наявність згоди користувача на надання відомостей зі своїх рахунків;
- 2) перед наданням інформації по рахунку користувача, здійснює перевірку авторизації діяльності НПП з надання відомостей;
- 3) перевіряє чинність кваліфікованого сертифікату відкритого ключа стороннього НПП та порівняти наявні відомості про нього з інформацією, що міститься у кваліфікованому сертифікаті відкритого ключа;
- 4) перевіряє відомості про нього в Реєстрі платіжної інфраструктури;
- 5) виконує запити щодо надання відомостей з рахунку користувача у режимі реального часу через базові спеціалізовані інтерфейси, в тому числі щодо суми доступних коштів на рахунку користувача та/або історії операцій за період, що становить не більше ніж 31 календарний день від дати запиту;
- 6) забезпечує безпечний обмін інформацією та захист інформації під час обміну такою інформацією через спеціалізовані інтерфейси;
- 7) забезпечує фіксування у власній інформаційній системі дату та час отримання і відкликання згоди користувача на надання відомостей з рахунку;
- 8) здійснює моніторинг запитів щодо надання відомостей з рахунків, наданих через НПП з надання відомостей;
- 9) припиняє надання НПП з надання відомостей доступу до рахунку користувача, з моменту відкликання ним наданої згоди на надання відомостей з рахунків, відкритих в Банку;
- 10) забезпечує зберігання документів та інформації щодо надання відомостей з рахунків користувача не менше 5-и років після надання відомостей;
- 11) надає можливість користувачу заблокувати доступ до свого рахунку НПП з надання відомостей у межах відкритого банкінгу.

5.7. Банк при взаємодії з НПП з надання відомостей має право:

- 1) заблокувати доступ до рахунку користувача стороннім НПП у межах відкритого банкінгу без звернення користувача в разі виявлення ознак шахрайських чи інших неправомірних дій, пов'язаних з несанкціонованим доступом до рахунку або до вразливих платіжних даних користувача;
- 2) передбачити в договорі з користувачем на обслуговування поточного рахунку отримання дозволу користувача на надання НПП з надання відомостей інформації, що містить банківську таємницю, комерційну таємницю, таємницю надавача платіжних послуг.

5.8. Банк несе відповідальність за розкриття інформації, що містить банківську таємницю, комерційну таємницю, таємницю надавача платіжних послуг в обсязі, на який не отримано дозволу користувача.

5.9. Управління згодами користувачів на надання відомостей з рахунків у межах відкритого банкінгу.

5.9.1. Банк забезпечує користувачу можливість управління згодами на надання відомостей з рахунків у межах відкритого банкінгу через власні засоби дистанційної комунікації Банку, зокрема мобільний застосунок та/або систему дистанційного обслуговування клієнт-банк.

5.9.2. Процес управління дозволом включає наступне:

- 1) надання дозволу на отримання відомостей з рахунків у межах відкритого банкінгу;
- 2) перегляд активних згод;
- 3) деталізацію згоди;
- 4) відкликання згоди;
- 5) перегляд неактивних / відкликаних згод;
- 6) оновлення статусу згоди;
- 7) фіксацію подій щодо наданих або відкликаних згод в інформаційній системі Банку.

5.9.3. Надання згоди користувачем.

Надання згоди користувачем здійснюється до надання сторонньому НПП доступу до інформації за рахунком користувача.

Перед наданням згоди Банк надає користувачу інформацію про стороннього НПП, рахунок, обсяг інформації, до якої надається доступ, строк дії згоди та умови її відкликання. Факт надання згоди фіксується в інформаційній системі Банку із зазначенням дати та часу її надання.

5.9.4. Перегляд та деталізація згод.

Банк забезпечує користувачу можливість перегляду активних та неактивних згод у власних засобах дистанційної комунікації.

Щодо кожної згоди користувачу має бути доступна деталізована інформація, зокрема: найменування стороннього надавача платіжних послуг, номер рахунку, обсяг інформації, до якої надано доступ, дата та час надання згоди, строк дії, статус згоди, а в разі відкликання — дата та час відкликання.

5.9.5. Відкликання згоди.

5.9.5.1. Користувач має право відкликати згоду на надання відомостей з рахунків через засіб дистанційної комунікації Банку або через засіб дистанційної комунікації стороннього НПП.

Згода користувача на надання відомостей з рахунків може бути відкликана користувачем без необхідності застосування НПП з надання відомостей з рахунків або НПП з обслуговування рахунку посиленої автентифікації користувача під час відкликання ним такої згоди.

5.9.5.2. Банк забезпечує можливість відкликання згоди користувачем у власному засобі дистанційної комунікації. Після відкликання згоди Банк припиняє надання відповідному сторонньому НПП доступу до інформації за рахунком користувача. Факт відкликання згоди фіксується в інформаційній системі Банку із зазначенням дати та часу відкликання. В разі відкликання користувачем згоди на надання відомостей з рахунків через такого НПП, Банк зобов'язаний направити запит про відкликання такої згоди користувачем до НПП з обслуговування рахунку.

5.9.5.3. НПП з обслуговування рахунку після отримання запиту про відкликання згоди користувача на надання відомостей з рахунків, зобов'язаний припинити

надання такому НПП з надання відомостей з рахунків доступу до рахунку користувача, щодо якого була надана така згода.

5.9.6. Статуси згод.

Банк забезпечує оновлення та відображення актуального статусу згоди користувача. Згода може мати, зокрема, такі статуси:

- активна;
- відкликана користувачем;
- строк дії закінчився;
- припинена Банком у випадках, передбачених законодавством, договором або внутрішніми документами Банку;
- неактивна з інших підстав.

5.9.7. Зберігання та контроль інформації про згоди.

Інформація про надання, відкликання, зміну статусу та припинення дії згоди зберігається Банком в інформаційних системах протягом строків, визначених чинним законодавством України, нормативно-правовими актами НБУ та внутрішніми документами Банку.

Банк забезпечує належний захист такої інформації, її цілісність, доступність та можливість подальшого контролю / аудиту подій, пов'язаних із наданням та відкликанням згод.

5.9.8. Передбачений в цьому Положенні порядок надання згод користувачем стосується лише згод користувача на надання відомостей з рахунків у межах відкритого банкінгу та не підміняє порядок надання згоди на виконання окремої платіжної операції.

6. Вимоги та параметри доступу до інтерфейсів

6.1. Банк для забезпечення доступу до рахунків своїх користувачів у межах відкритого банкінгу розміщує на власному вебсайті <https://www.policombank.com> :

- 1) перелік спеціалізованих інтерфейсів через які Банк надає доступ до рахунку користувача стороннім НПП;
- 2) короткий опис функціоналу кожного інтерфейсу, через який надається доступ до рахунку користувача;
- 3) опис технічних характеристик усіх доступних інтерфейсів із зазначенням процедур, протоколів та інструментів для взаємодії з Банком через спеціалізовані інтерфейси;
- 4) опис програми тестування, що виконується стороннім НПП для перевірки результатів взаємодії стороннього НПП із НПП з обслуговування рахунку через спеціалізовані інтерфейси;
- 5) контакти підрозділу Банку, який відповідає за вирішення всіх питань по взаємодії із сторонніми НПП.
- 6) інформацію про проведення регламентних робіт, які призводять до неспроможності забезпечити доступ до рахунків користувачів, не пізніше ніж за один робочий день та зазначити тривалість таких робіт в годинах.

6.2. Банк для забезпечення доступу до рахунків у режимі реального часу використовує інтерфейси, що забезпечують виконання таких вимог:

1) Банк здійснює автентифікацію надавачів платіжних послуг з надання відомостей з рахунків, надавачів платіжних послуг з ініціювання платіжних операцій за допомогою їхніх кваліфікованих сертифікатів відкритих ключів;

2) НПП з надання відомостей з рахунків має можливість здійснювати безпечну електронну взаємодію щодо обміну інформацією про один або більшу кількість рахунків та пов'язаних із ними платіжних операцій;

3) НПП з ініціювання платіжної операції здійснює безпечну електронну взаємодію з метою ініціювання платіжної операції з рахунку, отримання інформації про ініціювання платіжної операції та стосовно виконання платіжної операції.

6.3. Інтерфейс Банку повинен відповідати таким вимогам:

1) НПП з ініціювання та/або НПП з надання відомостей повинні мати можливість надати доручення Банку розпочати та застосувати автентифікацію користувача;

2) між Банком та НПП з ініціювання, а також НПП з надання відомостей та будь-яким користувачем платіжних послуг протягом усієї процедури автентифікації встановлюється та підтримується безперервна електронна взаємодія;

3) під час електронної взаємодії забезпечується цілісність і конфіденційність вразливих платіжних даних та кодів автентифікації.

6.4. Банк забезпечує в режимі реального часу налаштування інтерфейсів доступу до рахунків, що надані користувачам.

6.5. Банк розробляє опис, у якому документує технічні характеристики будь-якого з інтерфейсів із зазначенням набору процедур, протоколів та інструментів, потрібних для НПП з ініціювання, НПП з надання відомостей.

7. Перевірка авторизації діяльності надавача платіжних послуг

7.1. Банк перед наданням Сторонньому надавачу платіжних послуг доступу до рахунку користувача зобов'язаний перевірити авторизацію діяльності такого стороннього НПП щодо відповідної платіжної послуги шляхом:

1) перевірки чинності кваліфікованого сертифіката відкритого ключа стороннього НПП;

2) автентифікації стороннього НПП з використанням його кваліфікованого сертифіката відкритого ключа;

3) перевірки наявності інформації про стороннього НПП у Реєстрі платіжної інфраструктури (далі – Реєстр); порівняння інформації про стороннього НПП, що міститься у Реєстрі, з інформацією, що міститься у кваліфікованому сертифікаті відкритого ключа стороннього НПП (порівнюються ідентифікаційні дані та відомості про вид (види) фінансової платіжної послуги).

Банк має право надавати доступ до рахунку користувача сторонньому НПП в разі, якщо результати всіх зазначених перевірок є успішними.

7.2. Кваліфіковані сертифікати ключів надавачів платіжних послуг повинні містити:

1) для банків: ідентифікаційний код/номер, що дає змогу ідентифікувати банк у Державному реєстрі банків;

2) для небанківських надавачів платіжних послуг: ідентифікаційний код/номер надавача платіжних послуг, що дає змогу ідентифікувати надавача платіжних послуг у Реєстрі;

- 3) інформацію про види нефінансових платіжних послуг, на які авторизовано небанківського надавача платіжних послуг.

8. Безпека сеансу зв'язку

8.1. Банк з метою надання фінансових та/або нефінансових платіжних послуг зобов'язаний забезпечити захист даних із використанням криптографічних алгоритмів шифрування, що є національними стандартами, або такими, на які за результатами державної експертизи Державної служби спеціального зв'язку та захисту інформації України надано позитивний експертний висновок під час обміну даними через мережі загального користування.

8.2. Банк зобов'язаний завершити будь-який сеанс зв'язку одразу після виконання запиту.

8.3. Сторонні НПП для підтримання паралельних сеансів зв'язку з Банком зобов'язані забезпечити умови, за яких ці сеанси безпечним чином пов'язані з відповідними сеансами, встановленими з користувачами платіжних послуг, з метою запобігання помилкової адресації будь-яких повідомлень або інформації.

8.4. Банк спільно зі сторонніми НПП для забезпечення безпеки сеансу зв'язку зобов'язані дотримуватись наступного:

- 1) сеанс зв'язку під час проведення платіжної операції повинен бути пов'язаний з відповідним користувачем або користувачами платіжної послуги з метою виділення кількох запитів від одного і того самого користувача або користувачів платіжної послуги;
- 2) для надання послуги з ініціювання платежів ініційована платіжна операція повинна бути ідентифікована;
- 3) для надання підтвердження наявності грошових коштів ідентифіковано запит, який пов'язано із сумою, потрібною для виконання платіжної операції.

8.5. Банк та сторонні НПП зобов'язані забезпечити, щоб під час передавання вразливих платіжних даних та кодів автентифікації ця інформація була захищена засобами криптографічного захисту інформації або представлена в такому вигляді, який унеможливило зчитування цієї інформації, прямо чи опосередковано, у будь-який час.

8.6. Банк у разі порушення конфіденційності та/або цілісності вразливих платіжних даних, зобов'язаний невідкладно повідомити про це пов'язаного з ним користувача щодо вразливих платіжних даних у разі настання цієї події.

9. Вимоги до спеціалізованих інтерфейсів

9.1. Банк для електронної взаємодії зі сторонніми НПП в межах відкритого банкінгу має окремо виділений інтерфейс для автентифікації та встановлення сеансу зв'язку з рахунком користувача (далі – спеціалізований інтерфейс/API), який забезпечує належний рівень доступності та продуктивності доступних користувачу платіжних послуг в режимі реального часу.

9.2. Встановлений Банком спеціалізований інтерфейс зобов'язаний мати основні показники ефективності та цілі з обслуговування щодо доступності та цілісності даних, а саме:

1) Доступність (Availability) - відсоток часу працездатності спеціалізованого інтерфейсу протягом доби/кварталу;

2) Швидкість та продуктивність (Average response time) - час відповіді API (середній час у мілісекундах, необхідний інтерфейсу для обробки запиту. Окремо вимірюються показники для інформаційних запитів (AIS) та ініціації платежів (PIS)).

3) Успішність обробки запитів API - відсотковий показник успішної обробки запитів TPR через API Open Banking, який розраховується як 100 відсотків мінус частка помилок, віднесених до відповідальності банку (ASPS), від загальної кількості отриманих запитів, включаючи запити сервісу Ping.

9.3. Щоквартально відповідальний працівник Банку на вебсайті розміщує статистику щодо порушень доступності та ефективності спеціалізованого інтерфейсу та інтерфейсу, що використовується користувачами платіжних послуг.

9.4. В описі використання спеціалізованого інтерфейсу Банк зазначає стратегію і плани заходів щодо дій у надзвичайних ситуаціях, якщо є запланована недоступність інтерфейсу та/або виявлення факту непрацездатності інтерфейсу. Виявлення непередбаченої недоступності або непрацездатності інтерфейсу відбувається, якщо п'ять послідовних запитів на доступ до послуги з ініціювання платежу або послуги з надання відомостей з рахунку не отримали відповіді протягом 30 секунд.

9.5. Сектор інформаційної безпеки розробляє План заходів щодо дій у надзвичайних ситуаціях, в якому повинно бути передбачено планування комунікацій з інформування надавачів платіжних послуг, які використовують спеціалізований інтерфейс, про заходи з відновлення такого інтерфейсу та інструкції щодо використання інших резервних спеціалізованих інтерфейсів.

10. Порядок проведення заходів, спрямованих на запобігання невиконанню або неналежному виконанню платіжних операцій та неналежному наданню відомостей з рахунків користувача стороннім НПП.

10.1. Під час обслуговування користувача у відкритому банкінгу Банк застосовує аналогічні механізми захисту даних користувачів, як і під час надання звичайних платіжних послуг, а саме:

дані користувача, платіжні операції, інформація щодо здійснених платіжних операцій користувача повинні бути захищені, відповідно до порядку, передбаченому Політикою управління інформаційною безпекою Полікомбанку, затвердженою рішенням Наглядової ради від 07.11.2024, протокол №17.

10.2. Отримавши платіжну інструкцію від НПП з ініціювання, Банк перевіряє її на відповідність вимогам щодо захисту інформації, установленим Банком з урахуванням вимог нормативно-правових актів Національного банку.

10.3. Платіжна інструкція, що використовується для здійснення платіжних та/або інших операцій у платіжній системі, має також відповідати вимогам відповідної платіжної системи щодо захисту інформації.

10.4. Банк несе відповідальність перед користувачем за невиконання або неналежне виконання платіжних операцій відповідно до умов укладених між ними договорів, якщо не доведе, що платіжні операції виконані цим надавачем платіжних

послуг належним чином відповідно до Закону України “Про платіжні послуги” та умов укладених між ними договорів.

10.5. Банк також несе передбачену Законом України “Про платіжні послуги” відповідальність перед користувачем за невиконання або неналежне виконання платіжних операцій, ініційованих через НПП з ініціювання платіжної операції.

10.6. Банк здійснює заходи, спрямовані на запобігання невиконанню або неналежному виконанню платіжних операцій та неналежному наданню відомостей з рахунків користувачів у межах відкритого банкінгу, а саме:

- 1) перевірку повноважень та статусу стороннього НПП шляхом використання інформації з Реєстру платіжної інфраструктури;
- 2) перевірку наявності та чинності згоди користувача на доступ до рахунку та/або ініціювання платіжної операції;
- 3) застосування посиленої автентифікації користувача у випадках, визначених законодавством України та нормативно-правовими актами Національного банку України;
- 4) контроль цілісності, достовірності та повноти інформації, що передається через спеціалізовані інтерфейси відкритого банкінгу;
- 5) автоматизований контроль параметрів платіжної операції, включаючи перевірку реквізитів, суми операції, статусу рахунку та наявності достатнього залишку коштів;
- 6) моніторинг доступів до рахунків користувачів та операцій, здійснених із використанням спеціалізованих інтерфейсів;
- 7) ведення журналів подій, реєстрацію запитів, відповідей та дій учасників взаємодії у межах відкритого банкінгу;
- 8) застосування засобів захисту інформації, криптографічного захисту даних та механізмів контролю несанкціонованого доступу;
- 9) виявлення та оброблення інцидентів інформаційної безпеки, кібербезпеки та операційних збоїв;
- 10) забезпечення безперервності функціонування спеціалізованих інтерфейсів та резервування критичних інформаційних систем.

10.7. У разі виявлення ознак несанкціонованого доступу, неналежного надання відомостей з рахунку, помилкового обміну даними або ризику неналежного виконання платіжної операції Банк має право обмежити або призупинити доступ стороннього НПП до спеціалізованого інтерфейсу в порядку, визначеному законодавством України та внутрішніми документами Банку.

10.8. Відповідальний працівник Банку здійснює постійний моніторинг функціонування спеціалізованих інтерфейсів, аналіз інцидентів, звернень користувачів та повідомлень сторонніх НПП з метою своєчасного виявлення причин можливого невиконання або неналежного виконання платіжних операцій та неналежного надання відомостей з рахунків.

10.9. За результатами виявлених інцидентів Банк забезпечує проведення розслідування причин їх виникнення, вживає заходів щодо усунення виявлених недоліків, мінімізації ризиків їх повторного виникнення та, у випадках, передбачених законодавством, інформує користувачів, сторонніх НПП та Національний банк України.

11. Порядок взаємодії Банку та НПП з ініціювання щодо здійснення неакцептованих, помилкових та неналежних платіжних операцій та порядок відшкодування збитків користувачу, завданих в результаті проведення таких платіжних операцій

11.1. Порядок взаємодії між Банком та НПП з ініціювання у випадку здійснення неакцептованих, помилкових, неналежних платіжних операцій (в тому числі з використанням платіжної інструкції) – відповідає загальній процедурі взаємодії з користувачем, з урахуванням наступного:

1) звернення НПП з ініціювання та/або користувача щодо випадку здійснення неакцептованих, помилкових, неналежних платіжних операцій розглядається відповідальним працівником Банку, який обслуговує цього користувача та начальником сектору інформаційної безпеки, або інший уповноважений працівник Банку, який має відповідний фах, компетенцію та досвід у сфері інформаційної безпеки;

2) звернення щодо випадку здійснення неакцептованих, помилкових, неналежних платіжних операцій розглядається Банком протягом 15 календарних днів, а про результати розгляду та прийняті рішення НПП з ініціювання повідомляється не пізніше 15 днів;

3) у разі необхідності повідомлення користувача або НПП з ініціювання про випадок здійснення з його рахунку неакцептованих, помилкових, неналежних платіжних операцій, він повідомляється невідкладно, а для передачі повідомлення використовується будь-який наявний спосіб зв'язку;

4) за результатами проведення відповідного розслідування щодо обставин здійснення неакцептованої, помилкової, неналежної платіжної операції, Банк не пізніше 15 днів надає користувачу інформацію у відповідному обсязі, включаючи відомості про факт отримання згоди користувача, застосовані процедури автентифікації та передані до Банку платіжні інструкції;

5) в разі незгоди з Банком, користувач подає письмову заяву щодо відшкодування збитків, складену у довільній формі та підписану у звичайний спосіб або за допомогою електронного підпису в разі подання заяви в електронному вигляді;

6) особливості порядку розгляду звернень користувача за неналежними та помилковими платіжними операціями, а також порядку повернення йому коштів за такими операціями – викладено у договорі на обслуговування його рахунку;

7) Банк приймає всіх можливих заходів у цілодобовому режимі без вихідних, для забезпечення взаємодії з НПП з ініціювання на випадок здійснення неакцептованих, помилкових, неналежних платіжних операцій.

11.2. Банк не несе відповідальності, якщо платіжна операція виконана Банком належним чином.

11.3. В разі встановлення Банком факту його вини, він відшкодовує нанесені користувачу збитки, завдані в результаті проведення неакцептованих, неналежних, помилкових платіжних операцій у строк не більше 3 банківських днів, з моменту встановлення факту вини.

Під збитками розуміються понесені користувачем збитки за встановленої вини Банку.

11.4. В разі невстановлення факту наявності вини Банку за результатами внутрішнього розслідування— Банк пропонує НПП з ініціювання інші способи врегулювання спорів.

11.5. Банк щоденно проводить моніторинг здійснених платіжних операцій через сторонніх НПП за параметрами, встановленими правилами платіжної системи, з метою ідентифікації помилкових та неналежних, суб'єктів цих платіжних операцій та вжиття заходів із запобігання або їх припинення.

12. Порядок розгляду звернень користувачів в межах відкритого банкінгу

12.1. Порядок розгляду звернень користувачів та/або НПП з ініціювання в межах відкритого банкінгу, Банк застосовує аналогічні механізми, які передбачені Порядком розгляду звернень та проведення особистого прийому клієнтів в Полікомбанку, затвердженого рішенням Правління від 07.03.2025, пр.№14.

12.2. У зверненні користувачем повинно зазначатись прізвище, ім'я, по батькові, місце проживання заявника та викладено суть порушеного питання.

В разі подачі електронного звернення користувач повинен зазначити електронну поштову адресу, на яку може бути надіслана відповідь або відомості про інші засоби зв'язку. Застосування кваліфікованого електронного підпису при надсиланні електронного звернення не вимагається (типова форма звернення розміщується на вебсайті Банку <https://www.policombank.com>).

12.3. За формою звернення може бути:

- усним, яке надійшло на телефон гарячої лінії Банку 0 800 210-115, або за телефонами контакт центрів: (0462) 77 48 95 та (0462) 678 000,

- викладеним користувачем у письмовому вигляді, яке надійшло до Банку поштою або надане Клієнтом до Банку особисто або через уповноважену ним особу, або законним представником в інтересах неповнолітніх і недієздатних осіб, якщо їх повноваження оформлені відповідно до чинного законодавства;

- електронним, яке надійшло на електронну адресу Банку info@policombank.com. При надходженні електронного звернення відповідь надається на електронну поштову адресу користувача або НПП з ініціювання, які зазначені у зверненні.

12.4. Всі отримані звернення реєструються секретарем Голови Правління. Під час реєстрації кожному зверненню присвоюється вхідний номер, який відповідає номеру в Журналі звернень. Повторні, неодноразові звернення реєструються як первинні.

12.5. На вимогу користувача або НПП з ініціювання, який особисто подав звернення до Банку, на другому екземплярі звернення або його копії Банком ставиться дата прийняття звернення та реєстраційний номер.

У разі отримання повторного звернення, секретар Голови Правління у правому верхньому куті першої сторінки звернення робить відмітку "повторно", зазначає дату, номер та виконавця попереднього звернення, а також прикріплює все попереднє листування.

12.6. Всі звернення Клієнтів розглядаються невідкладно, але не пізніше 15 календарних днів від дня їх надходження, а ті, які не потребують додаткового вивчення, – протягом 30 календарних днів. Якщо для вирішення порушених питань слід провести перевірку інформації, викладеної у зверненні, отримати додаткові матеріали, то строк розгляду звернення може бути продовжено ще на 15 календарних днів, про що повідомляється користувач або НПП, не пізніше ніж за день до закінчення раніше визначеного строку розгляду звернення, із зазначенням причини продовження. При цьому загальний термін вирішення питань, порушених у зверненні, не може перевищувати сорока п'яти днів.

12.7. Звернення вважається вирішеним, якщо розглянуто всі порушені в ньому питання, прийнято обґрунтоване рішення, ужито необхідних заходів для його виконання, а користувача або НПП з ініціювання повідомлено про результати розгляду звернення і прийняте рішення.

12.8. Рішення про відмову в задоволенні вимог, викладених у зверненні, доводиться до відома користувача або НПП з ініціювання, не пізніше, ніж через десять днів з дня його надходження.

12.9. В разі незгоди з отриманою відповіддю Банку, Клієнт має право звернутись із зверненням до Національного банку України, інформація щодо порядку розгляду звернень до якого розміщена у розділі "Звернення громадян" офіційного Інтернет-представництва НБУ або до суду відповідно до законодавства України.

13. Порядок дій Банку на випадок шахрайства (підозри шахрайства) або загрози безпеці виконання платіжної операції, ініційованої користувачем та/або надання відомостей з його рахунків

13.1. Банк забезпечує постійний моніторинг операцій, запитів на доступ до рахунків користувачів та функціонування спеціалізованих інтерфейсів відкритого банкінгу з метою своєчасного виявлення ознак шахрайства, підозрілої активності, несанкціонованого доступу або інших загроз безпеці виконання платіжних операцій та надання відомостей з рахунків користувачів.

13.2. Підставами для застосування заходів реагування можуть бути:

- 1) виявлення ознак несанкціонованого доступу до рахунку користувача;
- 2) виявлення ознак компрометації засобів автентифікації користувача;
- 3) надходження інформації про можливе шахрайство від користувача, стороннього НПП, інших надавачів платіжних послуг, правоохоронних органів або уповноважених державних органів;
- 4) виявлення аномальної або нетипової активності під час ініціювання платіжної операції чи доступу до відомостей з рахунку;
- 5) інші обставини, що можуть свідчити про загрозу безпеці користувача, Банку або учасників відкритого банкінгу.

13.3. У випадках шахрайства (підозри шахрайства), загрози безпеці виконання платіжної операції або неакцептованих, помилкових, неналежних платіжних операцій, ініційованої користувачем через НПП та/або надання відомостей з рахунків користувача через НПП, Банк під час розгляду звернення звертається до

стороннього НПП з вимогою отримання інформації щодо наданої таким стороннім НПП нефінансової платіжної послуги користувачу у такому порядку:

- 1) запитує у стороннього НПП усю необхідну інформацію щодо ініціювання платіжної операції та/або ініціювання згоди/ запитів на отримання відомостей з рахунків шляхом направлення запиту на публічну корпоративну електронну пошту такого НПП;
- 2) очікує відповідь від стороннього НПП у строк до 3х робочих днів. Якщо відповідь не отримано у зазначений строк Банк може звернутися до НБУ із скаргою щодо роботи такого НПП;
- 3) у разі звернення НПП до Банку – Банк опрацьовує таке звернення протягом 5-ти робочих днів з дати отримання такого звернення;
- 4) у випадку загрози безпеки, виконання платіжної операції регулюється внутрішньою інструкцією та планом реагування інформаційної безпеки. Взаємодія у випадках шахрайства (підозри шахрайства), неакцептованих, неналежних платіжних операцій регламентується внутрішнім нормативним документом Банку.

13.4. Порядок взаємодії між Банком та НПП з ініціювання та/або користувачем у випадку шахрайства (підозри шахрайства) або загрози безпеці виконання платіжної операції – відповідає загальній процедурі взаємодії з користувачем, з урахуванням наступного:

- 1) звернення НПП з ініціювання та/або користувачем щодо випадку шахрайства або загрози безпеці розглядається сектором інформаційної безпеки негайно після його отримання;
- 2) про результати розгляду та прийняті рішення користувач повідомляється невідкладно, а для передачі повідомлення використовується будь-який наявний спосіб зв'язку;

13.5. Взаємодія між Банком та користувачем на випадок шахрайства (підозри шахрайства) або загрози безпеці відкритого банкінгу передбачає обов'язок Банку брати участь у розслідуванні обставин несанкціонованого доступу до рахунку користувача, неакцептованих або неналежно виконаних платіжних операцій, неправомірного отримання відомостей з рахунків користувача, а також інших випадків, що можуть свідчити про шахрайство або порушення вимог безпеки. Банк надає користувачу інформацію, що може бути розкрита відповідно до законодавства України та необхідна для розслідування зазначених випадків.

13.6. Банк має право без попереднього погодження з користувачем:

- 1) повідомляти сторонніх НПП, інших надавачів платіжних послуг, платіжні системи, Національний банк України та інші уповноважені органи про виявлені ознаки шахрайства, несанкціонованого доступу або інші події, що можуть створювати загрозу безпеці відкритого банкінгу;
- 2) тимчасово обмежити або припинити доступ стороннього НПП до спеціалізованого інтерфейсу Банку, зупинити виконання платіжної операції або надання відомостей з рахунку користувача у разі наявності обґрунтованої підозри щодо шахрайства, несанкціонованого доступу, компрометації засобів автентифікації чи іншої загрози безпеці;

3) вимагати проведення додаткової автентифікації користувача або додаткового підтвердження правомірності запиту на доступ до рахунку чи ініціювання платіжної операції.

13.7. У договорі на обслуговування рахунку користувача повинно бути передбачено обов'язок користувача невідкладно повідомляти Банк про:

1) відомі йому факти або підозри щодо шахрайських дій, пов'язаних із використанням сервісів відкритого банкінгу;

2) виявлення несанкціонованих платіжних операцій або запитів щодо отримання інформації з його рахунків;

3) компрометацію засобів автентифікації, облікових даних або інших засобів доступу до сервісів відкритого банкінгу;

4) будь-які обставини, які можуть свідчити про загрозу безпеці його рахунків або персональних даних.

13.8. У разі виявлення шахрайської операції, підозри щодо її здійснення, несанкціонованого доступу до рахунку, неправомірного отримання відомостей з рахунку або іншої загрози безпеці відкритого банкінгу користувач зобов'язаний невідкладно повідомити про це Банк через визначені Банком канали зв'язку та надати всю наявну інформацію, необхідну для перевірки обставин інциденту, вжиття заходів реагування та проведення розслідування.

13.9. Банк з метою забезпечення безперервного функціонування інтерфейса, своєчасного оновлення програмного забезпечення, вживає заходи для протидії шахрайським схемам та їх впровадження в API відкритого банкінгу.

Під час здійснення операцій із сторонніми НППІ застосовує тимчасовий одноразовий пароль (шляхом надсилання SMS) для їх підтвердження та забезпечує захищене з'єднання на офіційному порталі Банку.

14. Порядок моніторингу та аналізу платіжних операцій та запитів щодо надання інформації

14.1. Банк щоденно здійснює моніторинг доступності інтерфейсів API. В разі відсутності доступу стороннім НППІ до API, відповідальний працівник Банку повідомляє Технологічного оператора в порядку, визначеному договором з Технологічним оператором.

14.2. Для проведення моніторингу доступності до API відповідальний працівник збирає дані за такими параметрами:

1) кількість отриманих запитів;

2) кількість запитів із технічною помилкою;

3) кількість запитів, у яких вичерпано термін очікування та не отримано відповідей;

4) середній час відповіді на запит.

14.3. Для проведення моніторингу ефективності, відповідальний працівник збирає дані за такими параметрами:

1) кількість користувачів;

2) кількість активних згод;

3) кількість відкликаних згод;

4) кількість запитів до API;

5) обсяг запитів на ініціювання платіжної операції.

14.4. За результатами проведеного моніторингу та аналізу, відповідальний працівник щоквартально розміщує на вебсайті Банку в розділі «відкритий банкінг» статистику щодо порушень доступності та ефективності API.

14.5. Банк за результатами проведеного моніторингу, у разі виявлення ознак шахрайства, несанкціонованого доступу, порушень вимог законодавства, загроз інформаційній безпеці або інших обставин, що можуть свідчити про ризик неналежного виконання платіжних операцій чи неналежного надання відомостей з рахунків користувачів, має право ухвалити одне з таких рішень:

- 1) тимчасове зупинення або припинення виконання платіжної операції, ініційованої через стороннього НПП;
- 2) тимчасове обмеження або припинення доступу стороннього НПП до спеціалізованого інтерфейсу відкритого банкінгу Банку;
- 3) проведення додаткової перевірки повноважень стороннього НПП, чинності наданої користувачем згоди та достовірності отриманих через спеціалізований інтерфейс даних;
- 4) проведення додаткової автентифікації користувача або перевірки правомірності ініціювання платіжної операції чи запиту на отримання відомостей з рахунку;
- 5) установлення тимчасових обмежень щодо обсягу, частоти або видів платіжних операцій та запитів на отримання відомостей з рахунків користувачів;

Начальник організаційно-правового
відділу



Тамара ФЕДОРОВА