ЗАТВЕРДЖЕНО
Рішенням Правління
Акціонерного товариства
«Комерційний Індустріальний Банк»
протокол №12/03-1 від «12» березня 2020 року

Набирають чинності 23.03.2020р.

ЗМІНИ №2 до Правил обслуговування фізичних осіб в Акціонерному товаристві «Комерційний Індустріальний Банк»

(Затверджених Правлінням Банку №18/07-2 від 18 липня 2018 року, протокол №18/07-02)

Київ – 2020

I. Підстава внесення змін:

Внесення змін у зв'язку із зміною процеса підключення клієнтів-фізичних осіб до системи дистанційного обслуговування «CIB-Online».

II. Текст змін:

2.1. До Правил обслуговування фізичних осіб в Акціонерному товаристві «Комерційний Індустріальний Банк» **(далі - Правила)** внести наступні зміни:

2.1.2. РОЗДІЛ 1. «ТЕРМІНИ» доповнити новими термінами:

«Технологія сканеру відбитків пальців - аутентифікація користувача за відбитком пальця (у разі, якщо на Мобільному пристрої ((смартфон, планшет тощо) активована така функція);

Технологія розпізнавання обличчя - аутентифікація користувача за об'ємно-просторовою формою обличчя людини (у разі, якщо на Мобільному пристрої ((смартфон, планшет тощо) активована така функція);

ПІН-код для входу в систему Інтернет-банкінгу «CIB-Online» – персональний ідентифікаційний номер, який складається з 4х цифр та є особистим ідентифікатором, який відомий лише Клієнту і може використовуватися для його ідентифікації під час здійснення входу в систему Інтернет-банкінгу «CIB-Online».»

2.1.3. Розділ 8 «ДИСТАНЦІЙНЕ ОБСЛУГОВУВАННЯ В СИСТЕМІ ІНТЕРНЕТ-БАНКІНГУ «CIB-Online»» викласти в редакції:

«РОЗДІЛ 8. ДИСТАНЦІЙНЕ ОБСЛУГОВУВАННЯ В СИСТЕМІ ІНТЕРНЕТ-БАНКІНГУ «CIB-Online»

8.1. Інтернет-банкінг «CIB-Online» – це система дистанційного обслуговування Клієнтів – фізичних осіб в середовищі Інтернет і мобільного зв'язку, який дає можливість віддаленого управління своїми рахунками для забезпечення контролю, здобуття інформації про Продукти Банку, переказу коштів між рахунками і конвертації коштів, а також здійснення оплати комунальних послуг і послуг мобільного зв'язку, інтернет і телебачення, здійснення оплати товарів в інтернет-магазинах і переказу коштів як фізичним, так і юридичним особам, дистанційного оформлення вкладу (депозиту), у т.ч. відкриття вкладного (депозитного) рахунку та надання Вкладнику доступу до цього рахунку.
8.2. Інтернет-банкінг «CIB-Online» може бути встановлений як Мобільний додаток («CIB-Online» можна завантажити на мобільний пристрій через «Google Play» або «App Store») та/або як Web-модуль (на сайті Банку).
8.3.Порядок реєстрації, Аутентифікації Клієнта як Користувача та здійснення операцій в системі Інтернет-банкінгу «CIB-Online» визначений в Інструкції користувача, що розміщена на сайті Банку.
8.4. За допомогою системи Інтернет-банкінг «CIB-Online» Банк надає Клієнту право дистанційного доступу до рахунків, що відкриті в Банку за видами Продуктів Банку (поточні, вкладні (депозитні), кредитні) та їх самостійного обслуговування.
8.5. Повний перелік послуг (операцій), що надається Клієнту з використанням системи дистанційного обслуговування Інтернет-банкінгу «CIB-Online» (що визначено у меню цієї системи), наступний:

8.5.1. зв'язок з Банком;
8.5.2. перегляд курсів валют, встановлених Банком;
8.5.3. розрахунок конвертації валют;
8.5.4. геолокація за відділеннями Банку, банкоматами, платіжними пристроями та іншими терміналами самообслуговування тощо;
8.5.5. перекази з платіжної картки Банку на картку іншого банку;

8.5.6. переказ грошових коштів між власними рахунками Клієнта в Банку (в т.ч. поточними, вкладними (депозитними), кредитними рахунками, якщо це передбачено умовами відповідних Продуктів Банку);
8.5.7. переказ з платіжної картки на іншу платіжну картку в межах Банку;
8.5.8. платежі постачальникам послуг;
8.5.9. переказ з платіжної картки за реквізитами за межі Банку;
8.5.10 перегляд стану та історії операцій за всіма рахунками/картками Клієнта в Банку;
8.5.11. поповнення поточних, вкладних (депозитних) рахунків;
8.5.12. управління платіжними картками (блокування/розблокування картки, замовлення, керування лімітами за картками);
8.5.13. направлення заявки на отримання кредиту, відповідно до вимог відповідного Продукту Банку ;
8.5.14. відкриття нових вкладних (депозитних) рахунків, відповідно до вимог відповідного Продукту Банку;
8.5.15. створення та редагування шаблонів в Особистому кабінеті;
8.5.16. погашення кредитів;
8.5.17. керування профілем Клієнта;
8.5.18. отримання повідомлень від Банку.

8.6. Персональний пароль та ОТР пароль, що заводяться Клієнтом в системі Інтернет-банкінгу «CIB-Online» під час здійснення операцій, є простим електронним підписом (ЕП) Клієнта, який відповідає аналогу його власноручного підпису. Вимоги та рекомендації щодо генерації Персонального пароля наведено в п. 8.24 цього розділу Правил. Застосування ОТР пароля для авторизації платіжної операції Клієнтом, який пройшов аутентифікацію у системі Інтернет-банкінгу «CIB-Online» за допомогою Персонального паролю, вважається накладанням Клієнтом простого електронного підпису (ЕП) на Електронний документ і прирівнюється до власноручного підпису Клієнта у паперовій копії цього Електронного документу.
8.7. Електронний документ створюється за ініціативою Клієнта. Під час створення Електронного документа засобами Інтернет-банкінгу «CIB-Online» Клієнт від свого імені накладає на цей Електронний документ свій ЕП у вигляді ОТР пароля у порядку, визначеному пунктом 8.8. цього розділу. Створенням Електронного документа Клієнт доручає Банку здійснювати договірне списання плати за здійснений платіж (переказ) в системі Інтернет-банкінгу «CIB-Online» згідно з Тарифами Банку.
8.8. Підтвердження Клієнтом запиту на проведення операції у системі Інтернет-банкінгу «CIB-Online» здійснюється в такому порядку:

1. На запит Клієнта на проведення операції, система Інтернет-банкінгу «CIB-Online» генерує ОТР пароль і разом з інформацією про операцію, яка має бути підтверджена Клієнтом, відправляє його на Фінансовий телефон Клієнта.
2. Після отримання СМС-повідомлення Клієнт здійснює перевірку інформації про операцію, і у разі згоди, передає отриманий ОТР пароль до Банку шляхом введення його у відповідному рядку платіжного сервісу системи Інтернет-банкінгу «CIB-Online».
3. Якщо було введено вірний ОТР пароль для підтвердження операціївважається, що Клієнт підтвердив інформацію про операцію і надав згоду на її виконання.
4. Здійснення платіжних операцій в системі Інтернет-банкінгу «CIB-Online» виконується лише після проведення Аутентифікації Клієнта та з обов'язковим підтвердженням інформації про операцію за допомогою ОТР паролю. Виключенням є операції між власними рахунками (окрім відкриття депозитної угоди).

8.9.Всі документи, операції, договори, підтвердження Клієнта про ознайомлення з інформацією тощо, що ініціюються/укладаються/підтверджуються в Інтернет-банкінгу «CIB-Online» в електронному вигляді і підписані/підтверджені за допомогою Електронного підпису, вважаються такими, що підписані власноручним підписом Клієнта. Електронний підпис не може бути визнано недійсним через те, що він не має статусу електронного цифрового підпису чи через його

електронну форму. Клієнт особисто та одноосібно несе відповідальність за зміст Електронного документа.

Зі сторони Банку укладання/підписання в Інтернет-банкінгу «CIB-Online» в електронному вигляді договорів, електронних документів за операціями здійснюється відповідно до п.8.26.

8.10. Всі банківські операції, договори, інші документи, що здійснені в Інтернет-банкінгу «CIB-Online» в електронному вигляді, є електронними документами і вважаються такими, що мають однакову юридичну силу з документами у паперовій формі, і не можуть бути оскаржені через їх електронну форму.

8.11. Електронний підпис може застосовуватись в системі Інтернет-банкінгу «CIB-Online» при укладанні Сторонами будь-яких договорів або при підтвердженні/ініціюванні Клієнтом будь-якої банківської операції за будь-яким рахунком Клієнта, відкритим у Банку, перелік яких визначений цими Правилами.

8.12. Будь-яка інформація, надана Клієнтом до Банку після проходження Клієнтом процедури Аутентифікації, вважається такою, що надана особисто Клієнтом та підлягає застосуванню Банком в порядку, визначеному цими Правилами.

8.13. Підписані Клієнтом та /або Банком документи, що пов'язані з укладеними правочинами, зберігаються Банком в електронному вигляді та можуть бути надані Клієнту як засобами Мобільного додатку або Web-модулю Клієнта, так і на паперовому носії на запит Клієнта у відділенні Банку.

8.14.У разі використання системи Інтернет-банкінгу «CIB-Online» Клієнт заздалегідь погоджується з усіма ризиками, які притаманні роботі в мережі Інтернет.

8.15. Клієнт самостійно і в повному обсязі несе відповідальність за всі наслідки, спричинені здійсненням доступу та/або ініціюванням банківських операцій третіми особами, у разі отримання ними інформації про Логін та/або Пароль першого входу, та/або Пароль для входу, та/або ОТП пароль в будь-який спосіб, зокрема, але не виключно, через безпосереднє з необережності чи умисне повідомлення Клієнтом зазначеної в цьому пункті конфіденційної інформації третім особам, підбору третіми особами Логіна, Пароля для входу та/або ОТП пароля тощо.

8.16. Клієнт несе усі ризики та негативні наслідки втрати, незаконного заволодіння, технічного перехоплення інформації тощо мобільного телефону Клієнта та/або відповідної SIM-карти.

8.17. **ПРАВА ТА ОБОВ'ЯЗКИ СТОРІН**

8.17.1. Банк зобов'язаний:

1) Забезпечувати доступність системи Інтернет-банкінгу «CIB-Online» в мережі Інтернет, а також функціонування системи з урахуванням цих Правил та умов Договору.

2) Ознайомити Клієнта з Інструкцією користувача системи Інтернет-банкінгу «CIB-Online» та Пам'яткою клієнта (Додаток 2 до цих Правил) в частини основних заходів безпеки при роботі з Інтернет-банкінгом (розташовано на Офіційному сайті Банку cib.com.ua), до підключення до Інтернет-банкінгу «CIB-Online».

3) Приймати до виконання та виконувати електронні розрахункові документи Клієнта, підтверджені ОТР паролем, та надавати інші послуги, у т.ч. інформаційні, згідно з переліком, що зазначений в п. 8.5. цих Правил.

4) Формувати на запит Клієнта електронні та/або паперові розрахункові документи, а також виконувати інші дії, необхідні для належного виконання умов цих Правил та договорів.

5) Не розголошувати третім особам інформацію щодо діяльності та фінансового стану Клієнта, яка складає банківську таємницю Клієнта, за винятком випадків, передбачених чинним законодавством та внутрішніми нормативними документами Банку.

8.17.2. Банк має право:

1) Розширювати перелік послуг, які надаються Банком за допомогою системи Інтернет-банкінгу «CIB-Online», заздалегідь повідомивши про це Клієнта, зокрема шляхом унесення змін до Правил, та розміщення їх на сайті Банку та інформаційних стендах.
2) З метою запобігання розголошення конфіденційної інформації про Клієнта системи Інтернет-банкінгу «CIB-Online» стороннім особам, Банк має право у телефонному режимі проводити перевірку даних Клієнта, що телефонує, а саме: перевіряти ПІБ, слово-пароль до платіжної картки, місце реєстрації, дату народження, паспортні дані (серія, номер) тощо. Якщо уповноважений працівник Банку (Контакт-центр) має сумніви щодо достовірності наданої Клієнтом інформації, він має право відмовити Клієнту в наданні послуг. При зверненні Клієнта до відділення Банку з метою тимчасового блокування доступу до системи Інтернет-банкінгу «CIB-Online» працівник Банку встановлює особу останнього за паспортом або іншим документом, що посвідчує особу.
3) Відмовити Клієнту у прийманні та/або виконанні Електронного розрахункового документу, наданого за допомогою системи Інтернет-банкінгу «CIB-Online», у наступних випадках:
- у разі недостатності на рахунку Клієнта, з якого здійснюється переказ коштів, суми коштів, необхідної для здійснення переказу та суми, необхідної для сплати комісійної винагороди за здійснення такої операції (якщо це передбачено Тарифами Банку, чинними на момент виконання електронного розрахункового документу);
- у разі неповного (неправильного) зазначення Клієнтом реквізитів електронного розрахункового документу;
- у разі, якщо електронний розрахунковий документ передбачає переказ коштів, здійснення якого заборонено законодавством України (зокрема на користь осіб, які не мають право бути отримувачами коштів від Клієнта тощо);
- в інших випадках, передбачених Договором.

4) Заблокувати доступ Клієнта до системи Інтернет-банкінгу «CIB-Online» у разі настання будь-якої з наступних умов:
- здійснення 3 (трьох) поспіль невдалих спроб введення Персонального пароля;
- здійснення 5 (п’яти) поспіль невдалих спроб введення OTP паролю;
- порушення або спроби порушення Клієнтів умов безпеки доступу до системи Інтернет-банкінгу «CIB-Online»;
- здійснення Клієнтом дій, що перешкоджають використанню системи Інтернет-банкінгу «CIB-Online» іншими Клієнтами
- несплати Клієнтом комісій чи інших платежів відповідно до Договору та/або Тарифів;
- на підставі заяви/телефонного звернення/повідомлення по додатку-месенджеру Viber (далі – Viber) Користувача тощо.

5) Здійснювати модернізацію системи Інтернет-банкінгу «CIB-Online» та/або впроваджувати її більш досконалі версії.
6) Здійснювати тимчасову зупинку системи Інтернет-банкінгу «CIB-Online» для проведення технічних робіт, при цьому зазначені дії не потребують попереднього погодження Клієнтів.
7) У будь-який час в односторонньому порядку за власною ініціативою припинити користування/надання доступу до системи Інтернет-банкінгу «CIB-Online» або припинити доступ Клієнта до цієї системи, про що Клієнт повідомляється за допомогою функціоналу системи «CIB-Online» за можливості за 10 (десять) календарних днів, але в будь-якому випадку не пізніше дня блокування системи Інтернет-банкінгу «CIB-Online» шляхом відправлення СМС-повідомлення на Фінансовий телефон, та/або розміщення відповідного повідомлення на сайті системи Інтернет-банкінгу «CIB-Online», та/або надсилання відповідного повідомлення на електронну адресу Клієнта.
8) Без попереднього повідомлення Клієнта припинити надання послуг, якщо є підозри вважати, що фінансова операція(ї), що ініціюється за допомогою системи Інтернет-банкінгу «CIB-Online», пов’язана(і) з легалізацією (відмиванням) доходів, одержаних злочинним шляхом, або фінансуванням тероризму та фінансування розповсюдження зброї масового знищення, та/або у випадку неможливості проведення ідентифікації Клієнта відповідно до чинного законодавства України, у тому числі в разі ненадання Клієнтом необхідних документів чи відомостей для з‘ясування суті (змісту) його діяльності, фінансового стану, а також в разі наявності при здійсненні

ідентифікації у Банку підозри щодо надання Клієнтом недостовірної інформації або навмисного подання інформації з метою введення Банк в оману.
9) Зупиняти видаткові операції за Рахунком Клієнта, щодо якого є публічне обтяження рухомого майна, у відповідності до розділу 3 та 4 цих Правил на підставі відповідних документів та в порядку, встановленому законодавством та внутрішніми процедурами Банку.
10) В односторонньому порядку та в будь-який строк дії договору блокувати сервіс щодо укладання Сторонами угод з використанням Електронного підпису та/чи підтвердження/ініціювання Клієнтом будь-яких банківських операцій з використанням Клієнтом Електронного підпису, про що Клієнт інформується за допомогою функціоналу системи Інтернет-банкінгу «CIB-Online».
11) Списувати з Рахунку Клієнта шляхом договірного списання вартості послуг, наданих Банком згідно з Тарифами Банку у строки, розмірах і порядку, визначених відповідно до Договору, Правил та Тарифів.

8.17.3. Клієнт зобов'язаний:
1) Самостійно ознайомитися з Інструкцією користувача системи Інтернет-банкінгу «CIB-Online» та Пам'яткою клієнта (Додаток 2 до цих Правил) в частини основних заходів безпеки при роботі з Інтернет-банкінгом (розташовано на сайті Банку cib.com.ua), до підключення до Інтернет-банкінгу «CIB-Online» та дотримуватися положень даних Правил при роботі в системі Інтернет-банкінгу «CIB-Online».
2) Для проведення Клієнтом в системі Інтернет-банкінгу «CIB-Online» операцій за своїм/їми Рахунком/ами, а також отримання від Банку інформаційних послуг, надати до Банку:
- визначену Банком інформацію з метою успішного проходження Клієнтом процедури Аутентифікації в системі;
- визначену системою Інтернет-банкінгу «CIB-Online» інформацію з метою створення Банком від імені та в інтересах Клієнта електронних розрахункових документів;
- надавати Банку іншу інформацію, яка необхідна Банку, з метою належного виконання своїх зобов'язань за цими Правилами та Договором;

3) В своїх правовідносинах з Банком використовувати Електронний підпис при підписанні/підтвердженні будь-яких документів, операцій, угод (правочинів) Клієнта, що ініціюються/укладаються в електронному вигляді.
4) Під час створення електронного документа з Електронним підписом ознайомитися з усім текстом електронно документа, повністю зрозуміти його зміст, не мати заперечень до тексту документа (або його заперечення внесені як окремий реквізит документа) та свідомо застосовував свій Електронний підпис у контексті, передбаченому документом (підписав, затвердив, погодив, завізував, засвідчив, ознайомився).
5) Здійснювати оплату послуг, наданих Банком, згідно з Тарифами Банку у строки, розмірах і порядку, визначених відповідно до Договору, Правил та Тарифів.
6) Не здійснювати в Інтернет-банкінгу «CIB-Online» дії, що можуть призвести до неможливості іншим Клієнтам постійно або тимчасово використовувати Інтернет-банкінг «CIB-Online».
7) Нести ризик і всю відповідальність за несанкціоноване використання Логіна, Персонального чи OTP-паролів, яке відбулося внаслідок невиконання Клієнтом зобов'язань за цими Правилами та рекомендацій Банку щодо безпеки використання системи «CIB-Online», визначених цими Правилами, в тому числі в Додатку 2 до цих Правил.
8) Виконувати інші, визначені Правилами чи Договорами до Продуктів обов'язки Клієнта, зокрема щодо операцій, що здійснюються Клієнтом в Інтернет-банкінгу «CIB-Online».
9) Використовувати систему Інтернет-банкінгу «CIB-Online» виключно для операцій, не пов'язаних зі здійсненням підприємницької діяльності.
10) Забезпечити недоступність даних Аутентифікації для третіх осіб, у т.ч. членів родини, зокрема не зберігати ці дані у вільному доступі на будь-якому носії (паперовому, електронному тощо).
11) У випадку підозри щодо несанкціонованого доступу до аутентифікаційних даних, а також у випадку втрати (крадіжки) аутентифікаційних даних та/або Мобільного апарату з Фінансовим телефоном, або при виявленні випадків здійснення за рахунком (-ами) Клієнта операцій, що не були ним санкціоновані, чи в будь-яких інших випадках компрометації аутентифікаційних даних негайно звернутися до Контакт-центру

за телефонами (044 290-79-00, 0 800 501 200) або надіславши повідомлення по Viber з вимогою блокування доступу до системи Інтернет-банкінгу «CIB-Online». При зверненні телефоном до Банку Клієнт зобов'язаний надати дані для встановлення його особи (процедура ідентифікації) та на вимогу працівника відділення Банку/Контакт-центру надати додаткові відомості про себе.

12) На першу вимогу Банку (у т.ч. виставлену за допомогою системи Інтернет-банкінгу «CIB-Online») змінити Персональний пароль авторизації до системи Інтернет-банкінгу «CIB-Online». Будь-який новий пароль Аутентифікації в системі Інтернет-банкінгу «CIB-Online» має відповідати вимогам Інструкції користувача (розміщено на сайті Банку).

13) Максимально зменшити випадки здійснення доступу до системи Мобільного додатку через Wi-Fi точки публічного доступу в громадських місцях (клуби, кафе, готелі тощо) тощо.

14) Не встановлювати на Мобільному пристрої (смартфон, планшет тощо, на якому встановлено Мобільний додаток «CIB-Online») програмне забезпечення/додатки з неофіційних джерел, на персональному комп'ютері (з якого здійснюється підключення до WEB-інтерфейсу «CIB-Online») неліцензійні операційні системи та програмне забезпечення.

15) Використовувати на Мобільному пристрої ((смартфон, планшет тощо), на якому встановлено Мобільний додаток), персональному комп'ютері (на якому встановлено Web-модуль) сучасне антивірусне програмне забезпечення і своєчасно встановлювати на нього оновлення антивірусних баз.

16) Клієнт погоджується з тим, що розуміє всі ризики, пов'язані з:

- розголошенням Логіна, Персонального паролю, OTP пароля, а також будь-якої інформації про свої рахунки, що є банківської таємницею та при здійсненні доступу до системи Інтернет-банкінгу «CIB-Online» не з власного комп'ютера або мобільного телефону, та несе всю відповідальність за такі випадки;
- несанкціонованим та неналежним використанням Логіна, Персонального пароля, OTP пароля та несе відповідальність за збитки, завдані цими діями;
- неповідомленням або несвоєчасним повідомленням ним Банку щодо зміни номера Фінансового телефону». При цьому Клієнт несе всю відповідальність та звільняє Банк від будь-якої відповідальності, що може виникнути у зв'язку з відправленням Банком OTP паролю на його попередній номер «фінансового телефону»;
- зі здійсненням доступу до системи Інтернет-банкінгу «CIB-Online» через робоче місце (комп'ютер, мобільний телефон тощо), що не обладнане засобами антивірусного захисту, та з тим, що несе всю відповідальність та звільняє Банк від будь-якої відповідальності, пов'язаної з відсутністю антивірусного захисту.

17) Перед підтвердженням Електронного розрахункового документа перевірити та переконатись, що СМС-повідомлення відправлено Банком (має бути зазначено ComInBank).

18) У випадку виникнення будь-яких підозр щодо недотримання (невиконання) умов, визначених Правилами, а також у разі надходження до Клієнта запиту від будь-якої особи (у т.ч. від Банку загалом або від окремого працівника Банку) щодо розкриття (повідомлення, передачі тощо) Клієнтом його Авторизаційних даних, чи в будь-яких інших випадках компрометації даних повідомити про це Банк, звернувшись до Контакт-центру за телефонами (044-290-79-00, 0-800-501-200) або надіславши повідомлення засобами Viber .

19) Здійснювати сплату комісій та інших платежів відповідно до Договору та Тарифів, а також здійснювати оплату банківських послуг, наданих за допомогою системи Інтернет-банкінгу «CIB-Online», відповідно до чинних на момент надання Банком відповідної банківської послуги Тарифів Банку на такі послуги.

20) Дотримуватися вимог Банку щодо забезпечення безпеки та належного обслуговування Клієнтів, в тому числі, при отриманні будь-якої банківської послуги з допомогою системи Інтернет-банкінгу «CIB-Online».

21) Своєчасно встановлювати доступні оновлення операційної системи і додатків на своєму «фінансовому телефоні» / пристрої, що використовується для підключення до Мобільного додатку, для належного отримання послуг через Мобільний додаток «CIB-Online».

22) Використовувати на Мобільному пристрої (смартфон, планшет, тощо) на якому встановлено Мобільний додаток «CIB-Online», персональному комп'ютері (з якого здійснюється підключення до WEB-інтерфейсу «CIB-Online»), сучасне антивірусне програмне забезпечення і своєчасно встановлювати на нього оновлення антивірусних баз.

8.17.4. Клієнт має право:

1) Особисто користуватися системою Інтернет-банкінгу «CIB-Online» (лише фізична особа, яка уклала з Банком договір).

2) Здійснювати доступ до системи Інтернет-банкінгу «CIB-Online» у будь-який час за власним бажанням 24 години 7 днів на тиждень.

3) У будь-який час за власним бажанням та на власний розсуд змінити Персональний пароль, Логін. При цьому логін може бути змінено Клієнтом шляхом подання до Банку заяви про зміну Логіну.

4) Формувати, підтверджувати та надавати Банку за допомогою системи Інтернет-банкінгу «CIB-Online» Електронні документи та вимагати від Банку їх виконання відповідно до Договору та Правил.

5) За власним бажанням змінити номер Фінансового телефону в порядку, передбаченому Інструкцією користувача та цими Правилами.

6) Самостійно здійснювати управління Індивідуальними лімітами Картки з урахуванням обмежень, встановлених Банком в Тарифах.

7) У будь-який час за власною ініціативою тимчасово заблокувати доступ до системи Інтернет-банкінгу «CIB-Online» повідомивши Банк. Для блокування доступу до системи Інтернет-банкінгу «CIB-Online» Клієнт повинен зателефонувати до Контакт-центру за телефонами (044 290-79-00, 0 800 501 200) або надіслати повідомлення по Viber, або звернутися до будь-якого відділення Банку.

8) У будь-який час за власною ініціативою відключитись від системи Інтернет-банкінгу «CIB-Online» шляхом надання до Банку заяви про відключення в електронному вигляді системою Інтернет-банкінгу «CIB-Online» або на паперових носіях до відділення Банку у порядку, визначеному внутрішніми нормативними документами Банку.

9) У разі відсутності у Клієнта електронної адреси, при бажанні оформити (відкрити) Вклад у системі «CIB-online», Клієнт може отримати на паперових носіях примірник Договору банківського вкладу у будь-якому відділенні Банку.

8.18. Платежі, що створені в системі Інтернет-банкінгу «CIB-Online», приймаються Банком цілодобово та обробляються за регламентом прийому платежів, визначеним цими Правилами, Інструкцією користувача та іншими внутрішніми нормативними документами Банк. При цьому, платежі, що надійшли в післяопераційний час, вихідні, неробочі та святкові дні, обробляються протягом першого робочого дня, наступного за ними згідно з регламентом роботи, визначеним наказом Банку.

Електронні документи, що підтверджені OTP паролем та надані через систему«CIB-Online», виконуються Банком в межах залишку грошових коштів на відповідному рахунку Клієнта та відповідно до вимог чинного законодавства України.

Електронні документи, підтверджені OTP паролем, Банк виконує відповідно до реквізитів цих документів та не несе відповідальності за невідповідність/неправильність таких реквізитів.

8.19. Клієнт заявляє та погоджується з тим, що несе повну відповідальність за збитки, завдані Банку, Клієнту або третій особі виконанням Банком Договору та/або Електронного документу, підтвердженого OTP паролем, якщо мало місце несанкціонованого використання Персонального пароля, чи номера Фінансового телефона, чи OTP пароля, яке відбулося внаслідок невиконання Клієнтом зобов'язань за цими Правилами та рекомендацій Банку щодо безпеки використання системи «CIB-Online», визначених цими Правилами, в тому числі в Додатку 2 до цих Правил.

8.20. З метою забезпечення відповідного рівня безпеки розрахунків за допомогою системи Інтернет-банкінгу «CIB-Online», Банк має право встановити спеціальні ліміти на здійснення операцій за допомогою системи Інтернет-банкінгу «CIB-Online», а саме регламентувати суму однієї операції, та в односторонньому порядку змінювати встановлені спеціальні ліміти на здійснення операцій за допомогою системи Інтернет-банкінгу «CIB-Online» в будь-який момент. Перелік та розмір

спеціальних лімітів на здійснення операцій за допомогою системи Інтернет-банкінгу «CIB-Online», встановлених Банком, оприлюднюється на Офіційному сайті Банку. Інформація щодо зміни спеціальних лімітів на здійснення операцій за допомогою системи Інтернет-банкінгу «CIB-Online» публікується на Офіційному сайті Банку.

8.21. Для зручності Клієнтів у системі Інтернет-банкінгу «CIB-Online» передбачено можливість збереження реквізитів отримувача, які вказуються в Електронних документах, у вигляді окремих шаблонів переказів.

8.22. Відповідно до вимог Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», Клієнт зобов'язаний на вимогу Банку відвідати відділення Банку, де він обслуговується, з метою уточнення своєї ідентифікаційної інформації. В разі настання терміну уточнення ідентифікаційних даних або в разі не явки Клієнта для уточнення даних по запиту Банку, Банк має право припинити обслуговування Клієнта в системі Інтернет-банкінгу.

8.23. Підключення Клієнта до системи Інтернет-банкінгу «CIB-Online»:

8.23.1. Основною умовою для підключення Клієнта до системи Інтернет-банкінгу «CIB-Online» є наявність в Банку поточного рахунку з використанням платіжної картки в національній валюті (основна картка).

8.23.2. Доступ до системи Інтернет-банкінгу «CIB-Online» надається Клієнту шляхом самостійної реєстрації.

8.23.3. Для проходження процедури самостійної реєстрації Клієнту у Web-модулі (на сайті Банку) або у Мобільному додатку «CIB-Online» необхідно ввести реквізити ПК (номер картки), номер Фінансового телефону, пароль та його підтвердження.

8.23.4. Здійснюючи підключення до системи Інтернет-банкінгу «CIB-Online» Клієнт підтверджує:

- згоду на обслуговування через систему Інтернет-банкінгу «CIB-Online» всіх своїх рахунків (поточних, карткових, депозитних, кредитних тощо), відкритих в АТ «КІБ»;
- що ознайомлений з тим, що забороняється використовувати особисті платіжні картки для проведення операцій, пов'язаних із здійсненням підприємницької діяльності;
- що під час створення електронного документу з Електронним підписом, цим самим засвідчує, що ознайомився з усім текстом документа, повністю зрозумів його зміст, не має заперечень до тексту документа (або його заперечення внесені як окремий реквізит документа) і свідомо застосовував свій ЕП у контексті, передбаченому документом (підписав, затвердив, погодив, завізував, засвідчив, ознайомився);
- що усвідомлює та готовий нести всі ризики, пов'язані з електронним виглядом документів, які формуються в Інтернет-банкінгу «CIB-Online», та використанням Персонального та OTP паролів, які є простим електронним підписом;
- ознайомлення і погодження з Пам'яткою клієнта з питань безпеки використання системи дистанційного банківського обслуговування (що є додатком до цих Правил), Тарифами на обслуговування в системі Інтернет-банкінгу «CIB-Online» та умовами ініціювання платежів за допомогою системи.

8.24. Вимоги та рекомендації щодо генерації (встановлення) Персонального пароля:

8.24.1. Значення Персонального паролю повинно складатись з не менш ніж восьми символів.

8.24.2. Персональний пароль повинен бути складний – одночасно містити букви латинського алфавіту в нижньому та верхньому регістри (тобто містити великі і маленькі літери) та спеціальні символи ("#","^","&" тощо).

8.24.3. Зміну та генерацію (встановлення) нового Персонального пароля бажано здійснювати 1 раз на рік.

8.24.4. За бажанням Клієнта він може встановити ПІН-код для входу в систему Інтернет-банкінгу «CIB-Online» та, у разі, якщо в його мобільному пристрої активована така функція, активувати використання Технології сканеру відбитків пальців або Технології розпізнавання обличчя для входу в систему Інтернет-банкінгу «CIB-Online».

8.25. Відключення Клієнта від системи Інтернет-банкінгу «CIB-Online»

8.25.1. Клієнт може за власним бажанням припинити користування системою Інтернет-банкінгу «CIB-Online». Для цього необхідно:

-або звернутися безпосередньо до відділення Банку і подати за встановленою Банком формою заяву на відключення від системи Інтернет-банкінгу «CIB-Online»

-або самостійно в системі CIB-Online подати заявку на відключення від системи Інтернет-банкінгу «CIB-Online».

8.25.2. Банк має право самостійно відключити Клієнта від системи Інтернет-банкінгу «CIB-Online» в разі, якщо Клієнт не користувався (не заходив) системою «CIB-Online» більше ніж 6 (шість) місяців поспіль або за інших умов, зокрема, але не виключно: наявність у Банку підозр про вчинення шахрайських операцій із рахунком (-ами) Клієнта, наявність у Банку підстав вважати, що фінансова операція/ї Клієнта може/уть бути пов'язана/і з легалізацією (відмиванням) кримінальних доходів або фінансуванням тероризму, чи в разі неможливості здійснення ідентифікації Клієнта відповідно до вимог чинного законодавства України та внутрішніх документів Банку, у т.ч. ненадання Клієнтом необхідних документів чи відомостей для з'ясування суті його діяльності, фінансового стану чи умисного надання Клієнтом неправдивих відомостей, визначених цими Правилами.

Про відключення Клієнта від системи Інтернет-банкінгу «CIB-Online» Банк негайно повідомляє Клієнта на номер Фінансового телефону усно або шляхом направлення СМС-повідомлення, чи на електронну адресу Клієнта, вказану в Договорі.

Відключення, що здійснюється Банком самостійно згідно цього пункту,. не є розірванням Договору з Банком.

8.26. Підписання договорів в системі Інтернет-банкінгу «CIB-Online»

8.26.1. При укладанні Договору та всіх його додатків і інших супутніх документів засобами системи «CIB-Online» Банком може бути застосовано факсимільне відтворення підпису уповноваженої особи та відбитку печатки Банку, що відтворені засобами механічного, електронного або іншого копіювання. Вищевказані відтворення відтиску печатки Банку та підпису уповноваженої особи Банку за своїми правовими наслідками прирівнюються до власноручного підпису документів уповноваженою особою Банку та скріплення документів печаткою Банку в оригіналі, і не можуть бути використані в майбутньому у якості підстав для визнання Договору/ документу недійсним, нікчемним або неукладеним.

8.26.2. Банк, керуючись нормами статті 207 Цивільного кодексу України пропонує Клієнту, а Клієнт погоджується з тим, що під час підписання з боку Банку документів, необхідних для укладання цього Договору та всіх його додатків і інших супутніх документів, використовуватиметься факсимільне відтворення підпису уповноваженої особи Банку та відбитку печатки Банку, які нанесені засобами електронного або іншого копіювання та зразки яких містяться в цьому пункті, а саме:

8.26.3 Зразок печатки Банку

8.26.4. Зразок підпису Голови Правління АТ «КІБ»

.»

2.1.4. Додаток 2 «ПАМ'ЯТКА КЛІЄНТА (з питань безпеки використання системи дистанційного банківського обслуговування)» викласти в редакції:

«Додаток 2
до Правил обслуговування фізичних осіб в
Акціонерному товаристві
«Комерційний Індустріальний Банк»

ПАМ'ЯТКА КЛІЄНТА

(з питань безпеки використання системи дистанційного банківського обслуговування)

Увага!!! Будь ласка, не ігноруйте текст нижче (для обов'язкового прочитання)

При здійсненні операцій засобами дистанційного банківського обслуговування:

1. Зберігайте у режимі суворої секретності Ваші аутентифікаційні дані: логіни, паролі, PIN-коди - які Ви використовуєте у роботі із сервісами системи дистанційного банківського обслуговування (далі - Система). Ніколи не зберігайте їх на SIM-картах, flash-накопичувачах і жорстких дисках Вашого мобільного телефону, планшету, ноутбуку або комп'ютера.
2. Нікому (у тому числі, і працівникам Банку) та ні за яких обставин не повідомляйте паролі та логіни по телефону або у поштовому повідомленні. Якщо Ви отримали електронний лист (у тому числі з будь-якої адреси Банку) з проханням повідомити або підтвердити Ваш логін або пароль – не відповідайте на запит. Зателефонуйте до служби підтримки клієнтів Банку та залиште повідомлення про спробу несанкціонованого отримання Ваших аутентифікаційних даних. Не надсилайте з власної ініціативи без прохання працівника служби підтримки отриманий лист на адреси Банку.
3. Пам'ятайте, що Банк ніколи не запитує та не повідомляє (!) конфіденційної інформації, логіни та паролі у телефонному режимі або електронною поштою, не розсилає засобами електронної пошти програмне забезпечення для встановлення на Ваші пристрої.
4. Відключіть функцію запам'ятовування паролів у браузерах (Internet Explorer, Google Ghrome, FireFox, Opera тощо) на мобільному телефоні, планшеті, ноутбуку і комп'ютері, з допомогою яких Ви працюєте з Системою.
5. Для входу у Систему завжди використовуйте власні логін і пароль.
6. Не залишайте без нагляду Ваш мобільний телефон, планшет, ноутбук або комп'ютер під час роботи з Системою.
7. У разі втрати мобільного телефону, на який Ви отримуєте SMS-повідомлення з одноразовими паролями, негайно заблокуйте SIM-карту (номер телефону).
8. На час довготривалого (декілька місяців і більше) перериву у роботі із Системою, зверніться до служби підтримки клієнтів Банку та заблокуйте свій логін.
9. Не здійснюйте роботу із Системою з комп'ютерів інтернет-кафе, бізнес-центрів, готелів, ігрових залів або інших осіб, оскільки Ви не можете бути впевненими, що вони відповідають вимогам безпеки та захисту Ваших даних. Такі комп'ютери можуть бути заражені програмами для пошуку і крадіжки паролів, номерів платіжних карт тощо.
10. Якщо це можливо, не працюйте на робочому місці з правами адміністратора операційної системи.
11. Під час роботи із сервісом Інтернет-банкінгу періодично перевіряйте чинність адреси сторінки Системи (https://cib-online.com.ua). У рядку адреси сторінки у Вашому браузері має бути присутнє зображення зачиненого замка. Рядок адреси сторінки в браузері Internet Explorer має бути підсвічено зеленим кольором. У разі виявлення підозрілих сайтів, імена яких та стиль оформлення схожі зі сторінкою Системи, негайно зателефонуйте до служби підтримки клієнтів Банку та залиште повідомлення про спробу фальсифікації сайту Системи.

12. Не відвідуйте сайтів сумнівного змісту та будь-яких інших Інтернет-ресурсів (соціальні мережі, конференції та чати, телефонні сервіси тощо) з персонального комп'ютера чи мобільного пристрою, на якому здійснюється підготовка та відправка документів до Банку. Не читайте пошту та не відкривайте поштових вкладень до електронних листів, які надійшли від невідомих або підозрілих адресатів. Не слід здійснювати установку та оновлення будь-якого програмного забезпечення не з офіційних сайтів виробників.

13. Не встановлюйте на мобільному пристрої (смартфоні, планшеті тощо, на якому встановлено Систему) програмне забезпечення/додатки з неофіційних джерел, на персональному комп'ютері (з якого здійснюється підключення до Web-інтерфейсу) неліцензійні операційні системи та програмне забезпечення.

14. Використовуйте сучасне антивірусне забезпечення, оновлюйте та проводьте антивірусну перевірку на персональних комп'ютерах та мобільних пристроях. Наголошуємо, що шкідливе програмне забезпечення здатне перехоплювати будь-які дані з персональних комп'ютерів і мобільних пристроїв, зберігати і поширювати таку інформацію для подальшого несанкціонованого використання сторонніми особами злочинним шляхом.

15. Забезпечуйте своєчасне встановлення оновлень безпеки операційної системи, браузерів та програмного забезпечення комп'ютерів/мобільних пристроїв. Необхідно встановити надійні паролі доступу на вхід до персонального комп'ютера/мобільного пристрою, забезпечити періодичну зміну цих паролів.

16. Пам'ятайте, що дотримання режиму захисту інформації та своєчасне виявлення факту компрометації Ваших аутентифікаційних даних дозволить мінімізувати ризики отримання збитків та усунути чинники загроз.

17. **Рекомендації щодо захисту від фішингу**

Фішинг (англ. phishing, від fishing – рибальство) — це вид інтернет-шахрайства, метою якого є отримання доступу до конфіденційної інформації користувачів - логінів та паролей. Це досягається шляхом проведення масових розсилок електронних листів або повідомлень в соціальних мережах від імені відомих організацій, наприклад, від імені банків. У листі, зазвичай, міститься пряме посилання на сайт, який ззовні не відрізняється від справжнього. Після того, як користувач потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами примусити його зазначити свій логін та пароль, який він використовує для отримання доступу до певного сайту. Отримання конфіденційної інформації користувача дає можливість шахраям використовувати облікові записи та банківські рахунки користувачів в своїх цілях.

17.1. Ознаки фішингових листів:

- Адреса відправника. Фішингові повідомлення, зазвичай, мають вигляд електронного листа, який ззовні не відрізняється від оригінального, відправленого з поштової системи АТ «КІБ». За допомогою шкідливого програмного забезпечення шахраї можуть підмінити електронну адресу, яка відображається в будь-якій поштовій скринці клієнта.
- Екстрений характер повідомлення. З метою збільшення кількості відгуків, зловмисники намагаються надати повідомленням екстрений характер, окреслюючи ліміт часу, і викликати необдумані дії користувача.
- Помилки в темі листа. Як правило, в фішингових листах, в полі «Тема» використовується різний регістр літер, набір літер та цифр, допускаються граматичні або друкарські помилки для уникнення фільтрів поштових програм.
- Гіперпосилання на підроблені сайти. Посилання, зазначені в фішингових листах, ззовні схожі на офіційну веб-адресу АТ «КІБ» і перенаправляють користувачів на веб-сайти, які імітують зовнішній вигляд легітимного сайту Банку.

17.2. Розпізнати підроблений сайт можливо за адресою веб-сайту та за спливаючими вікнами.

Більшість методів фішингу зводиться до маскування підроблених посилань на фішингові сайти під посилання реальних організацій. Шахраї часто використовують адресу з

друкарськими помилками або субдомени. В дійсності, адреса сайту (URL) складається з набору цифр та літер і вміст сайту є підробленим. Але частина інформації та некритичні посилання можуть бути оригінальними.

Користуючись різним шкідливим програмним забезпеченням, шахраї мають змогу створювати та розміщувати підроблені спливаючі вікна на основі легітимного сайту, котрі запитують конфіденційну інформацію. При цьому справжній сайт Банку буде відображатись в фоновому режимі. Таким чином, вся, зазначена Вами, інформація в підробленому спливаючому вікні буде доступна шахраям.

17.3. Виконання перерахованих нижче правил дозволить Вам успішно протистояти фішинговим атакам:

- Ніколи не надавайте логін, пароль та інші конфіденційні дані стороннім особам. Не відповідайте на листи з проханням вислати Вашу особисту або фінансову інформацію та не переходьте по вказаних посиланнях, оскільки всі листи, з запитом конфіденційної інформації є шахрайськими.
- Для входу на Web-сторінку Інтернет-банкінгу «CIB-Online» використовуйте лише адресу https://cib-online.com.ua, введену ВРУЧНУ в адресний рядок Вашого браузеру або користуйтесь власними закладками.
- Використовуйте останню версію браузера. Такі браузери як Internet Explorer, FireFox, Google Chrome, Opera систематично оновлюються і мають фільтр захисту від фішингу.
- Завжди перевіряйте, при передачі персональної інформації, та використовуйте шифроване з’єднання. При використанні безпечного з’єднання адреса сайту завжди розпочинається з "https://", а не з http://.

18. Якщо Ви отримали сумнівний електронний лист від імені АТ «КІБ», або виявили фішинговий вебсайт Банку, або виявили несанкціонований доступ та/або зміну ваших даних/інформації в Інтернет-банкінгу «CIB-Online» повідомте про це Контакт-Центр АТ «КІБ» за телефонами 0 800 501 200 (дзвінки безкоштовні у межах України), +38 (044) 290-79-00 (вартість дзвінків згідно з тарифами вашого оператора), або перешліть сумнівний лист/ відповідну інформацію про вебсайт/несанкціонований доступ/зміну вашої інформації з коментарями на електронну адресу: info@cib.com.ua.»