БАНК КЛІРИНГОВИЙ ДІМ

Додаток 4а до Правил та загальних умов комплексного банківського обслуговування
(для малого та середнього бізнесу)

Правила роботи в системі "Інтернет-Клієнт–Банк"

1. ВИКОРИСТАННЯ СИСТЕМИ ЕЛЕКТРОННОГО ОБСЛУГОВУВАННЯ

1.1. Банк надає можливості здійснення операцій по рахунках Клієнта за допомогою системи електронного обслуговування «Інтернет-Клієнт-Банк» (далі – Система).

1.2. З моменту подання у письмовій формі Сертифікату відкритого ключа електронного цифрового підпису (далі – ЕЦП) у Системі , на підставі підписаного Договору Сторонами, операції по рахунках Клієнта будуть виконуватись на підставі електронного платіжного документу (далі - ЕПД), що готуються Клієнтом та передаються Системою у Банк.

1.3. При підключенні до Системи , Банк налаштовує послугу IP-фільтрація з наданням доступу тільки з IP-адрес провайдерів, що розміщені на території України. Для відключення IP-фільтрації, Клієнт повинен подати Заяву на відключення доступу до системи «Інтернет-Клієнт-Банк» з використанням IP-фільтрації, а для повторного підключення до послуги IP-фільтрація, Клієнт повинен подати Заяву на доступ до системи «Інтернет-Клієнт-Банк» з використанням IP-фільтрації.

1.4. Клієнт доручає Банку виконувати фінансові операції по його рахункам, відкритим в Банку, на підставі ЕПД, отриманих Банком по Системі та завірених зареєстрованими в Банку ЕЦП осіб, що мають право підпису розрахункових документів.

1.5. Банк приймає на себе обов'язки по поточному обслуговуванню Клієнта з використанням Системи, а саме: приймає та виконує доручення Клієнта, оформлені відповідно до вимог Договору, Правил роботи в Системі та нормативно – правових документів Національного банку України, у вигляді ЕПД, на здійснення операцій по рахункам Клієнта, передає Клієнту виписки по його рахункам у вигляді електронного документу (далі – ЕД), текстові ЕД, інформаційну та довідкову інформацію.

1.6. До послуг, які можуть надаватись Клієнту користувачу Системи, за його Заявою, належать послуги:

1.6.1. У випадку використання Системи - «IP-фільтрація», що дозволяє обмежити доступ Клієнтів тільки з визначених IP-адрес або чітко вказаної групи IP-адрес та/або дозволяє вхід лише з IP-адрес українських провайдерів;

1.6.2. Згідно з діючими тарифами Банку, Банк забезпечує Клієнта пристроєм для захисту носіїв ключової інформації - USB-токеном в Системі, який рекомендовано використовувати для генерації особистих секретних ключів ЕЦП;

1.6.3. сервіс «багатофакторна автентифікація» (процедура встановлення автентичності користувача при вході до Системи за допомогою введення одноразового шестизначного паролю до спеціального додаткового поля, який направляється у вигляді SMS-повідомлення на вказаний Клієнтом номер мобільного телефону і має обмежений термін дії -3 хв.);

1.6.4. сервіс «підтвердження платіжних документів одноразовим паролем» (процедура введення одноразового шестизначного паролю на певні платежі від зазначеної Клієнтом суми до спеціального додаткового поля, який направляється у вигляді SMS-повідомлення на вказаний Клієнтом номер мобільного телефону і має обмежений термін дії -3 хв.);

1.6.5. сервіс «підтвердження платіжних документів з урахуванням довідника довірених отримувачів» *(налаштування здійснюється Клієнтом самостійно, після надання доступу до сервісу);*

1.6.6. «отримання інформації про стан рахунку у вигляді SMS – повідомлення, за допомогою засобів мобільного зв'язку / поштового електронного повідомлення на *e-mail» (налаштування здійснюється Клієнтом самостійно, після надання доступу до сервісу).*

1.7. У разі здійснення операцій за допомогою Системи без використання пристрою для захисту носіїв ключової інформації, Клієнт обов'язково використовує послугу, визначену п.п. 1.6.1 п.1.6 цих Правил.

1.8. Клієнт несе відповідальність за належне оформлення, достовірність та відповідність вимогам чинного законодавства платіжних документів, надісланих Банку до виконання за допомогою Системи.

1.9. Банк приймає ЕПД в національній валюті та проводить їх протягом операційного часу згідно п.1.15.

1.10. На підставі виписок з рахунків, які надходять з Банку, Клієнт контролює вірність виконання Банком його доручень.

1.11. Усі операції за електронними платежами протоколюються відповідно регламенту, встановленому Банком. Протоколи операцій є документами, що підтверджують наявність та правомірність платежів.

1.12. Цей Договір не відміняє платіжних доручень, що обробляються в установленому порядку, у випадках:

- ✓ відмови засобів комунікації;
- ✓ відмови засобів обчислювальної техніки як Клієнта, так і Банка.

1.13. Проведення всіх поточних операцій та отримання всієї інформації по Системі здійснюється Клієнтом в режимі онлайн за допомогою мережі Інтернет під час сеансів зв'язку з Банком. При цьому протокол передачі інформації в Системі є https, що є міжнародним стандартом.

1.14. Всі довідники, шаблони ЕПД, ЕПД після їх збереження, а також виписки та будь-яка інша інформація в Системі знаходяться в Банку та доступні для роботи Клієнту тільки під час проведення авторизованих сеансів зв'язку з Банком через мережу Інтернет.

1.15. Прийом ЕПД від Клієнта здійснюється Банком постійно в автоматизованому режимі.

Банк здійснює списання грошових коштів з поточного рахунку Клієнта згідно документів, які надійшли до Банку по Системі до 16-00 в той же день, а ті, що надійшли після 16-00 – на наступний банківський день. Розрахунки за платіжними документами Клієнта, що надійшли по Системі в п'ятницю та передсвятковими днями здійснюються до 15-45, а ті що надійшли після 15-45 – на наступний банківський день. При зміні режиму обслуговування відповідно змінюється час прийому документів. Клієнт формує та передає в Банк ЕПД необхідного виду. Після отримання ЕПД Банк здійснює його перевірку та приймає ЕПД до виконання.

Причинами для відмови від виконання Банком ЕПД Клієнта є:

- ✓ відсутність в ЕПД зареєстрованого ЕЦП Клієнта;
- ✓ невірні або неповні реквізити ЕПД;
- ✓ недостача інформації та необхідних документів по операції, що здійснюється Клієнтом, у випадках, передбачених діючим законодавством;
- ✓ порушення діючого законодавства, нормативних документів НБУ або Банку, вимог Договору та Правил.

Для відкликання переданого в Банк ЕПД Клієнт формує клопотання на відкликання ЕПД, яке Банк приймає тільки в тому випадку, якщо ЕПД не виконаний до цього часу та Банк має технічну можливість відмінити його виконання.

1.16. Клієнт не має права вносити будь-які зміни у надане йому програмне забезпечення або до комплексу документації без письмового погодження Банку. Зараження програмними "вірусами" або порушення цілісності програмного забезпечення в наслідок недбальства або некомпетентності відповідальних співробітників Клієнта, вважається порушенням цієї умови.

1.17. Сторони встановлюють, що надані Клієнту згідно Договору програмно-технічні засоби та друковані матеріали розглядаються як секретні та їх суворе збереження повинно бути забезпечене в достатній мірі. В зв'язку з цим, всі посадові особи Клієнта, які мають до них доступ, повинні поводитись з ними належним чином та утримуватись від їх розголошення або копіювання у будь-якому вигляді.

1.18. Банк може проводити заміну програмного забезпечення та інструктивних матеріалів при збільшенні кількості інформації. Заміна проводиться планово, в погоджені з Клієнтом терміни.

1.19. Банк забезпечує оперативне роз'яснення та консультації з питань, пов'язаних з експлуатацією Системи.

1.20. На виконання п.1.5. Правил Клієнт доручає Банку самостійно здійснювати переказ (списання) коштів з рахунку (-ів) Клієнта на оплату відповідних додаткових послуг Банку, в розмірі та строки, визначені Тарифами Банку.

2. ТЕХНОЛОГІЯ ТА ПОРЯДОК ОФОРМЛЕННЯ ПЛАТІЖНИХ ДОКУМЕНТІВ

2.1. ЕПД, які надаються Клієнтом, повинні мати реквізити, вказані у Інструкції про безготівкові розрахунки в Україні в національній валюті, затвердженої Постановою Правління Національного банку України № 22 від 21.01.2004 р. (із змінами та доповненнями), далі за текстом - Інструкція.

2.2. Для забезпечення повноважності платежу та його конфіденційності використовуються апаратно - програмні засоби, які дозволяють виробляти авторизацію сформованих ЕПД за допомогою персональних ключових носіїв. Порядок використання секретних ключів описаний у Додатку №5 до Правил та загальних умов комплексного банківського обслуговування.

2.3. Зв'язок Клієнта з Банком здійснюється за допомогою мережі Інтернет при застосуванні Системи. Клієнт готує ЕПД, підписує його і надсилає у Банк. При надходженні від Клієнта підписаний ЕПД розпаковується, розшифровується та передається для обробки на автоматизоване робоче місце (далі – АРМ) операціоніста, який обслуговує рахунок клієнта.

При обробці на АРМ операціоніста у режимі "Електронні документи", платежі проходять попередній контроль за формальними ознаками згідно з Інструкцією.

2.4. Після попереднього контролю платежі стають доступними для обробки фахівцю Банка, що приймає рішення про їх акцепт. У випадку відмови від акцепту платежу, який не пройшов попереднього контролю або за рішенням фахівця, формується квитанція з відповідним кодом помилки, яка за допомогою Системи надсилається Клієнту для аналізу.

Виправлені ЕПД Клієнт може відправити у Банк для обробки.

2.5. На ЕПД, які пройшли попередній контроль та прийняті до оплати, формуються квитанції, які відсилаються Клієнту для звірки. На ці документи фахівець Банку з допомогою відповідних апаратно-програмних засобів формує електронні записи для програмного комплексу "Операційний день Банку".

У подальшому з ЕПД Клієнта здійснюються операції відповідно з встановленим порядком для

внутрішньобанківських та міжбанківських платежів.

3. ПРАВИЛА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Для забезпечення безпечної роботи в Системі рекомендовано дотримуватись наступних правил:

– утримуватись від використання комп'ютера, з якого виконується робота в Системі для розваг та серфінгу в мережі Інтернет;

– встановити антивірусне програмне забезпечення, регулярно поновлювати антивірусну базу та постійно проводити перевірку системи на наявність вірусів та шпигунських програм (троянів, кейлогерів та т.п.);

– обмежити доступ до комп'ютера сторонніх осіб, як фізичний, так і мережевий;

– не тримати особисті (секретні) ключі в директоріях жорсткого диску комп'ютера, а тільки на зовнішніх носіях (USB флеш накопичувачі, USB- токени, тощо) та забезпечити їх надійне зберігання;

– для унеможливлення викрадення (копіювання) таємного ключа рекомендуємо використовувати USB - токен;

– після закінчення роботи з Системою обов'язково виймати зовнішні носії (USB флеш накопичувачі, USB-токени, тощо) з секретними ключами с системного блоку комп'ютера;

– не розголошувати паролі доступу до таємних ключів, не записувати їх та не зберігати разом з носієм ключової інформації;

– встановлювати поновлення безпеки операційної системи (бажано в автоматичному режимі);

– налаштувати оглядач мережі Інтернет, а саме заборонити: автоматичне завантаження файлів з мережі Інтернет, автоматичний запуск файлів з мережі Інтернет, завантаження не підписаних елементів ActiveX;

– не працювати на комп'ютері з правами адміністратора;

– у випадку компрометації або спроби компрометації секретних ключів або комп'ютера, звільнення відповідального співробітника або IT спеціаліста Клієнта, який мав доступ до вказаного комп'ютера або секретних ключів необхідно терміново повідомити Банк для заблокування ключів ЕЦП, згенерувати та зареєструвати нові ключі ЕЦП;

– при будь-якій підозрі при роботі з Системою – необхідно терміново повідомити Банк для заблокування ключів ЕЦП та згенерувати та зареєструвати нові ключі ЕЦП;

– уважно слідкувати за повідомленнями, що виводяться на монітор комп'ютера при роботі в Системі. У випадку невідповідності їх тим, які виводяться зазвичай – повідомити Банк. Прикладом невідповідності може слугувати: нетипове вікно з іншим логотипом, при виборі ключа не відображається назва ключа, прохання встановити підозріле програмне забезпечення, тощо;

– при роботі через сайт Системи звертайте увагу на адресу сайту. Вона повинна починатись на https – що свідчить про захищене з'єднання;

Застереження: Банк ніколи не здійснює розсилку електронних листів з проханням надати конфіденційну інформацію (паролі, доступ до секретних (особистих) ключів, тощо) або таких, що містять комп'ютерні програми.

3.2. Рекомендації по створенню надійних (стійких) паролів.

При виборі пароля користувачеві необхідно керуватися запропонованими правилами:

– не використовувати атрибути користувача - імена і прізвища користувачів, пам'ятні дати і будь-яку іншу досяжну інформацію (наприклад, номери телефонів, адреси і тому подібне);

– заборонено використання комбінації символів / знаків з клавішею Ctrl;

– паролі повинні складатися шляхом комбінації двох або більше слів;

– довжина пароля повинна складати не менше 8 символів;

– пароль повинен містити не менш 3-х з 4-х наступних символів – великі , маленькі літери, цифри, спецсимволи;

– заборонено використовувати слова з реальних і вигаданих словників ; пароль необхідно змінювати не рідше ніж кожні 30 календарних днів.

Один з можливих варіантів (прикладів) вибору пароля: складіть список простих слів, наприклад, квітка, аркуш, ручка і так далі виберіть перші три букви і загальну кількість букв в словах; об'єднаєте отримані результати, додайте одну цифру і один із спеціальних символів ("&'{([-_@)]]}$*% !:/ ;., ?+-=) і зробіть одну з букв великою; при зміні пароля використовуйте приведені рекомендації з іншим набором слів. Приклад: яблуко, груша і наберіть їх в латинському регістрі.

Увага! Не використовуйте як пароль наведені приклади! Безумовно, для створення пароля можуть використовуватися інші методи створення надійного пароля, але вибраний пароль не має бути слабкіше запропонованої міри стійкості.

Увага! Пам'ятайте, що ні за яких обставин Ваш пароль не має бути відомий третім особам, ніхто не має права вимагати від Вас розкриття пароля, навіть співробітники Банку.

3.3. Використання пристрою захисту носіїв ключової інформації «USB-токен» в Системі.

Клієнту рекомендовано використовувати USB-токен для генерації особистих ключів ЕЦП.

USB-токен генерує особисті секретні ключі всередині себе, забезпечує їх захищене зберігання і формує

ЕЦП під електронними документами усередині пристрою згідно ДСТУ 4145.

Підтримка USB-токенів забезпечена для всього спектру настільних платформ – Windows, Linux і Mac OS X. Робота USB-токенів підтримується за основними каналами обслуговування корпоративних клієнтів системи «ibank 2 UA».

У одному USB-токені може зберігатися до 64-х особистих ключів. Можливе зберігання особистих ключів ЕЦП відповідальних співробітників корпоративних клієнтів.

Забезпечується одночасна робота відразу з декількома підключеними до комп'ютера USB-токенами.

3.4. Використання сервісу IP – фільтрація

3.4.1. Підключення, відключення сервісу IP – фільтрація.

У Систему вбудований механізм обмеження доступу клієнтів заданими IP-адресами. Для посилення заходів безпеки в разі постійної роботи з одних робочих місць рекомендується підключити сервіс IP-фільтрація в Системі. Даний механізм обмеження доступу по IP-адресах є індивідуальним для кожного Клієнта і налаштовується співробітником Банку за письмовою заявою клієнта з зазначенням переліку IP-адрес комп'ютерів Клієнта, з яких здійснюватиметься підключення до Системи . Якщо спроба входу в АРМ здійснюється із не заданої IP-адреси, видається повідомлення про помилку «Доступ заборонений», вхід в АРМ неможливий.

Існує можливість налаштування обмеження входу в Систему, використовуючи наступні IP-фільтри:

– вхід лише з IP-адрес українських провайдерів. Застосовується для обмеження доступу до Системи з IP-адрес зарубіжних провайдерів, оскільки досить часто з цих IP-адрес здійснюється несанкціонований вхід в Систему.

– вхід лише із заданих IP-адрес (індивідуальний список IP-адрес, з яких дозволено працювати вказаному Клієнтові). Перелік IP-адрес надає Клієнт.

– якщо Клієнт використовує для доступу до Системи IP-адреси іноземних провайдерів (буває за кордоном, де використовує для доступу до Системи місцеві інтернет - мережі), то необхідно надати в Банк заяву на відключення доступу до системи «Інтернет-Клієнт-Банк» з використанням IP-фільтрація, за встановленою типовою формою.

Увага! Рекомендується уточнювати і погоджувати перелік IP-адрес із службою технічної підтримки Банку. Якщо використовується великий перелік IP-адрес або IP-адреса постійно міняється в рамках діапазону, то рекомендуємо вказувати діапазон IP-адрес за допомогою маски мережі. Заява для активації сервісу підписується особами, уповноваженими на підписання договорів зі сторони Клієнта.

Увага! Клієнт зобов'язаний ознайомити всіх своїх співробітників, що мають право на роботу в Системі, з умовами обмеженого доступу з вказаних робочих станцій (комп'ютерів) і несе повну відповідальність за це.

4. НАДЗВИЧАЙНІ ОБСТАВИНИ

4.1. При виникненні надзвичайних, аварійних, інших нестандартних обставин, які заважають роботі по здійсненню електронних платежів, учасники платежів негайно повідомляють один одного про ці обставини та вживають заходів до їх ліквідації. Під час дії надзвичайних обставин Клієнт може здійснювати роботу з Банком за допомогою паперових платіжних документів.

КЛІЄНТ:

_____ _____ (_____)

Посада М.П. П.І.Б.