ДОГОВІР
про банківське обслуговування з використанням програмно-технічного комплексу"Клієнт-Банк"

м. _____ №_____ "__"_____201_р.

СТОРОНА 1: Юридична особа за законодавством України – АКЦІОНЕРНЕ ТОВАРИСТВО „КОМЕРЦІЙНИЙ БАНК «ГЛОБУС», надалі за текстом – «**Банк»,** від імені якого на підставі Довіреності від __.__.201_р. діє _____ _____, з однієї сторони, та
СТОРОНА 2: _____, надалі за текстом - "Клієнт", в особі _____, що діє на підставі _____, з другої сторони,

які в подальшому разом іменуються «Сторони», а окремо – «Сторона», уклали цей договір (надалі – «Договір») про наступне:

1. ПРЕДМЕТ ДОГОВОРУ

З метою оперативного ведення Клієнтом своїх рахунків у Банку та обміном технологічною та іншою інформацією Сторони дійшли згоди, що Клієнт доручає, а Банк бере на себе зобов'язання здійснювати дистанційне обслуговування поточних рахунків Клієнта з використанням програмно – технічного комплексу «Клієнт – Банк» (надалі – «ПТК КБ»). Договір укладено Сторонами в доповнення до договору банківського рахунку №_____ про відкриття та обслуговування банківського рахунку від __.__._____р.

2. ЗОБОВ`ЯЗАННЯ СТОРІН

2.1. Банк бере на себе зобов`язання:
2.1.1. Передати Клієнту програмне забезпечення, технічні засоби захисту інформації та документацію, яка регламентує правила та регламент використання ПТК КБ. Надавати Клієнту необхідні консультаційні послуги щодо роботи з ПТК КБ.
2.1.2. Проводити списання коштів з рахунку Клієнта в строк передбачений чинним законодавством України**.**
2.1.3. Формувати для Клієнта необхідну технологічну інформацію, що містить результат обробки кожного розрахункового документа.
2.1.4. Не проводити списання коштів з рахунку Клієнта, якщо електронний розрахунковий документ, переданий Клієнтом телекомунікаційними лініями зв'язку, не відповідає встановленому порядку оформлення таких розрахункових документів, зокрема не підписаний електронними цифровими підписами (надалі – «ЕЦП») Клієнта або у разі руйнування електронного підпису**.**
2.1.5. Приймати до виконання документи Клієнта на паперових носіях.
2.1.6. Забезпечити конфіденційність системи генерації ключів та збереження інформації щодо реалізації Договору на весь термін його дії.
2.1.7. Розглядати документи, виготовлені з використанням ЕЦП, як такі, що мають рівну юридичну силу з документами, які підписані службовими особами та завірені печаткою Клієнта традиційним способом (на паперових носіях).
2.1.8. Виконувати планову заміну ключів ЕЦП в терміни, що узгоджені Сторонами**.**
2.1.9. Надавати інформацію Клієнту про рух коштів (надходження та списання) по рахунку за допомогою послуги «SMS-Банкінг» після підключення до обслуговування в системі «SMS-Банкінг» та активування її функцій на підставі заяви Клієнта.
2.1.10. З моменту надходження повідомлення Клієнта про доступ сторонніх осіб до секретних ключів ЕЦП або підозри, що такий доступ мав місце, зупиняти прийняття платіжних доручень Клієнта в ПТК КБ.

2.2. Клієнт бере на себе зобов`язання:
2.2.1. Забезпечити робоче місце для роботи ПТК КБ згідно мінімальних вимог (п.2 Додатку №2 Договору).
2.2.2. Під час створення електронного розрахункового документу накладати підписи відповідальними особами, які уповноважені розпоряджатися рахунком і на законних підставах володіють особистим ключем ЕЦП**.**
2.2.3. Виконувати усі вимоги щодо захисту інформації в ПТК КБ, які встановлені Банком**.**
2.2.4. Регулярно протягом дня перевіряти стан рахунку з урахуванням відправлених платежів. У разі невідповідності відправлених і проведених платежів негайно припинити роботу в системі до з'ясування обставин та повідомити Банк про виявлені розбіжності.
2.2.5. Забезпечити надійне зберігання засобів захисту інформації, а також відповідної документації.
2.2.6. Дотримуватися технології роботи в системі електронних розрахунків ПТК КБ, які викладені в керівництві користувача системи.
2.2.7. Дотримуватися встановленого порядку звірки надісланих електронних розрахункових документів та документів, прийнятих Банком до оплати.
2.2.8. Зберігати архіви ПТК КБ протягом трьох років.
2.2.9. При отриманні ПТК КБ підписати Акт передачі прав на використання ПТК КБ. У разі обрання обслуговування з використання носія ЕЦП USB-токен підписати Акт приймання - передачі носіїв ЕЦП USB-токен ПТК КБ у тимчасове користування.
2.2.10. Уникати дій, які можуть привести до псування зовнішнього носія інформації (фізичні та температурні впливи).
2.2.11. Встановити на робочу станцію, на якій працює ПТК КБ, антивірусне програмне забезпечення, для уникнення дій вірусів на засоби захисту та програмне забезпечення. Забезпечити регулярне оновлення антивірусних баз.
2.2.12. У випадку доступу сторонніх осіб до секретних ключів ЕЦП або підозри, що такий доступ мав місце, Клієнт зобов'язаний повідомити про це Банк будь-якими доступними засобами зв`язку і в подальшому надати в Банк оригінал такого повідомлення з роз`ясненнями, за підписом уповноваженої особи Клієнта і відбитком печатки (у разі її наявності). З моменту надходження повідомлення Банк зупиняє прийняття платіжних доручень Клієнта по ПТК КБ. Для відновлення роботи з ПТК КБ Клієнт повинен виконати перегенерацію всіх ключів ЕЦП.
2.2.13. Виконувати планову заміну ключів в терміни, узгоджені Сторонами, після чого знищити старі ключі шляхом

переформатування зовнішнього носія інформації.
2.2.14. Зберігати носії електронного цифрового підпису в добре захищеному місці (наприклад, в сейфі), що виключає можливість несанкціонованого використання пристроїв третіми особами.
2.2.15. Забезпечити обмеження доступу та конфіденційність системи генерації ключів та самих ключів ЕЦП документів, що передаються, а також паролів, які використовуються.
2.2.16. Розглядати документи, виготовлені з використанням ЕЦП, як такі, що мають рівну юридичну силу з документами, які підписані службовими особами та завірені печаткою Клієнта традиційним способом (на паперових носіях).
2.2.17. Про кожну виявлену спробу несанкціонованого втручання у систему або пошкодження засобів ЕЦП негайно інформувати Банк.
2.2.18. Здійснювати оплату за виконані Банком операції і надані послуги згідно з тарифами Банку не пізніше 5-го числа наступного місяця. У разі відсутності коштів на рахунку своєчасно поповнювати рахунок грошовими коштами.

3. ПРАВА СТОРІН

3.1. Банк має право:
3.1.1. Виконувати періодичні перевірки виконання Клієнтом вимог щодо захисту інформації та зберігання засобів захисту і припиняти обслуговування Клієнта за допомогою ПТК КБ в разі невиконання ним вимог безпеки.
3.1.2. Вимагати в окремих випадках від Клієнта підтвердження розрахункового документа на паперовому носії, завіреному підписами та печаткою Клієнта, у відповідності з наданими картками зразків підписів і відбитка печатки.
3.1.3. Здійснювати договірне списання з рахунку Клієнта, який відкрито у Банку, вартості послуг за Договором в межах сум, які належать до сплати Банку, згідно з тарифами, строками та порядком оплати, передбаченими Банком.
3.1.4. Припинити обслуговування Клієнта через ПТК КБ у разі:
- порушення Клієнтом фінансових угод, передбачених Договором;
- неодноразового порушення графіку приймання-передавання електронних документів;
- несвоєчасної звірки з Банком оплачених документів;
- порушення правил зберігання та використання засобів захисту інформації.

3.1.5. На виконання вимог Положення про здійснення банками фінансового моніторингу, затвердженого постановою Правління НБУ від 14.05.03 № 189, у разі необхідності, Банк має право витребувати, а Клієнт зобов'язаний надати, протягом трьох днів з моменту звернення Банку, додаткові відомості щодо його ідентифікації або проведення ним фінансової операції.
3.1.6. У разі відмови Клієнта щодо надання зазначеної інформації, Банк має право відмовити Клієнту у обслуговуванні рахунку або проведенні фінансової операції.
3.1.7. Запроваджувати нові програмно-технічні та технологічні засоби з метою поліпшення функціонування ПТК КБ.
3.2. Клієнт має право:
3.2.1. У разі неможливості передавання з технічних причин електронних розрахункових документів, подавати в Банк розрахункові документи на паперових носіях, оформлені належним чином.
3.2.2. Отримувати, у разі необхідності, в день проходження (або наступного дня) електронного платежу підтвердження на паперових носіях.
3.2.3. Вимагати від Банку своєчасного проведення електронних розрахункових документів, переданих до Банку телекомунікаційними лініями зв'язку, якщо ці документи оформлені належним чином та передані у строки, передбачені договором банківського рахунку, у відповідності з діючим регламентом проходження платежів за допомогою ПТК КБ.
3.2.4. Отримувати від Банку інформацію про рух коштів (надходження та списання) по рахунку за допомогою послуги «SMS-Банкінг» після підключення до обслуговування в системі «SMS-Банкінг» та активування її функцій на підставі заяви Клієнта, при цьому Клієнт має пересвідчитись у можливості отримання даної послуги у свого мобільного оператора .

4. ПОРЯДОК ЗДІЙСНЕННЯ ОБСЛУГОВУВАННЯ

4.1. Банк протягом п'яти робочих днів після отримання Заяви на підключення до обслуговування в ПТК КБ та SMS-Банкінг передає програмне забезпечення та засоби захисту інформації для встановлення на ПК Клієнта.
4.2. Клієнт не має права вносити будь-які зміни у надане йому програмне забезпечення. Порушення цілісності програмного забезпечення (включаючи зараження програмними "вірусами") внаслідок недбальства або некомпетентності службових осіб Клієнта вважається порушенням цього пункту Договору.
4.3. Банк приймає розрахункові документи за рахунками Клієнта за допомогою телекомунікаційного зв'язку, перевіряє електронні підписи, контролює реквізити, інформує Клієнта засобами ПТК КБ про результати оброблення документів. Протягом дня Клієнт формує поточні виписки стану рахунку. Після закриття операційного дня банку Клієнт формує остаточну виписку стану рахунку.
4.4. Щоденно після підведення заключного балансу Банк друкує реєстри електронних розрахункових документів, отриманих в ПТК КБ.
4.5. Клієнт виконує кінцеву звірку надісланих електронних розрахункових документів та документів, прийнятих Банком до оплати, після отримання остаточної виписки стану рахунку.
4.6. Банк списує кошти з рахунку Клієнта згідно електронних розрахункових платежів в межах залишку на його рахунку.

5. ВІДПОВІДАЛЬНІСТЬ СТОРІН

5.1. Кожна із Сторін несе відповідальність за збої в обміні інформацією, викликані необережними, некомпетентними та зловмисними діями її персоналу. До зловмисних, зокрема**,** відносяться дії персоналу, пов'язані із порушенням або із спробою порушення заходів щодо захисту інформації у ПТК КБ.
5.2. Винна Сторона відшкодовує іншій Стороні у повному обсязі збитки, які виникли через невиконання або неналежне виконання своїх зобов'язань, передбачених Договором.
5.3. Відповідальність за збереження та використання засобів захисту інформації та клієнтської програмної частини ПТК КБ повністю покладається на осіб, які вповноважені розпоряджатися рахунком і на законних підставах володіють особистим ключем.
5.4. Клієнт несе відповідальність перед Банком у разі незбереження (викрадення, втрати, компрометації тощо) засобів захисту

інформації та програмної частини ПТК КБ.
5.5. Банк не несе відповідальність:
5.5.1 за збої в обміні інформацією, які виникли через несправність ліній зв'язку, відключення або перебої електропостачання, несправність апаратних засобів Клієнта;
5.5.2. за несанкціоноване списання коштів з рахунку Клієнта у випадку, якщо передані телекомунікаційними лініями зв'язку електронні розрахункові документи були складені правильно та завірені ЕЦП Клієнта;
5.5.3. за навмисну або необережну передачу Клієнтом паролів, ключів та системи захисту третій стороні.
5.6. Сторони звільняються від відповідальності за часткове або повне невиконання будь-якого з положень Договору, якщо це невиконання стало наслідком причин, що знаходяться поза сферою контролю невиконуючої Сторони. Такі причини включають стихійне лихо, екстремальні погодні умови, пожежі, війни, страйки, військові дії, громадське безладдя і таке інше, а також дії Уряду або Національного банку України, які заборонять, обмежать чи будь-яким іншим чином унеможливлять повернення коштів згідно з умовами Договору (далі -"форс-мажор"), але не обмежуються ними. Період звільнення від відповідальності починається з моменту оголошення невиконуючою Стороною "форс-мажору" і закінчується чи закінчився б, якщо невиконуюча Сторона вжила б заходів, які вона і справді могла вжити для виходу з "форс-мажору". "Форс-мажор" автоматично продовжує термін виконання зобов’язань на весь період його дії та ліквідації наслідків. Про настання "форс мажорних" обставин Сторони мають інформувати одна одну невідкладно. Якщо ці обставини триватимуть більше ніж 6 місяців, то кожна із Сторін матиме право відмовитись від подальшого виконання зобов’язань за Договором, і в такому разі жодна із Сторін не матиме права на відшкодування другою Стороною можливих збитків.

6. БАНКІВСЬКА ТАЄМНИЦЯ

6.1. Банк зобов’язується не розголошувати інформацію щодо діяльності та фінансового стану Клієнта, яка складає банківську таємницю, за виключенням випадків, коли розкриття банківської таємниці без погодження з Клієнтом є обов’язковим для Банку у відповідності з чинним законодавством України та у випадках, передбачених цим Договором.
6.2. Клієнт погоджується, що умови, передбачені п. 6.1. цього Договору щодо збереження банківської таємниці, не поширюються на випадки розкриття Банком третім особам інформації щодо Клієнта, що складає банківську таємницю (в т.ч. інформації про причини невиконання зобов’язань перед Банком, характеристики виконання зобов’язань Клієнта перед Банком, про майно, що виступає у якості забезпечення за цим Договором тощо) у випадках порушення Клієнтом умов цього Договору. Клієнт, підписанням цього Договору, надає згоду Банку розкривати інформацію, що складає банківську таємницю, у випадках порушення Клієнтом умов цього Договору, шляхом надання її у спосіб та в обсягах, визначених Банком, необмеженому колу третіх осіб, у т.ч. правоохоронним органам, судам, фінансовим установам, іншим установам, підприємствам, організаціям тощо.
6.3. Клієнт також надає згоду Банку на розкриття останнім банківської таємниці у випадках та обсягах, необхідних для проведення перевірок діяльності Банку з боку аудиторських організацій або уповноважених державних органів.
6.4. Клієнт також згоден, що Банк на власний розсуд будь-яку кількість разів буде телефонувати йому, направляти відомості про строк та розміри його зобов’язань перед Банком, нарахування, виконання/неналежне виконання Клієнтом своїх зобов’язань за цим Договором, іншу інформацію та повідомлення, пов’язані/передбачені Договором, також комерційні пропозиції Банку та рекламні матеріали за допомогою поштових відправлень та листів-звернень, електронних засобів зв’язку, SMS - повідомлень, тощо на адреси/номери телефонів, адреси електронної пошти (e-mail), вказані Клієнтом в анкеті, заяві тощо. При цьому Клієнт несе всі ризики, пов’язані з тим, що направлена Банком інформація стане доступною третім особам та, відповідно, надає згоду на її розголошення.
6.5. Підписанням цього Договору, Клієнт свідчить, що він згоден з умовами та порядком розкриття банківської таємниці, викладеними у ньому. Умови цього розділу застосовуються також до договорів, що укладені між Банком та Клієнтом для забезпечення зобов’язань Клієнта за цим Договором.
6.6. За незаконне розголошення інформації, що містить банківську таємницю Банк несе відповідальність, передбачену чинним законодавством України.

7. СТРОК ДІЇ ДОГОВОРУ. ВНЕСЕННЯ ЗМІН І РОЗІРВАННЯ

7.1. Договір вважається укладеним на невизначений термін і набуває чинності з дня його підписання обома Сторонами.
7.2. Договір може бути змінений або доповнений за згодою Сторін. Сторона, яка вважає за необхідне змінити або доповнити Договір, надсилає пропозиції про це другій Стороні за Договором.
7.3. Всі додатки, зміни та доповнення до цього Договору мають бути викладені в письмовій формі та підписані уповноваженими на те представниками Сторін.
7.4. Договір може бути розірвано достроково за взаємною письмовою згодою двох Сторін з попередженням іншої Сторони за десять днів до розірвання.
7.5. В разі невиконання Клієнтом своїх зобов’язань за Договором, Банк має право достроково розірвати Договір в односторонньому порядку, з обов’язковим попередженням Клієнта за десять календарних днів до передбачуваної дати розірвання.
7.6. Клієнт має право розірвати Договір у разі незгоди із запропонованими Банком змінами до тарифів.

8. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

8.1. Всі спори та розбіжності, які можуть виникнути між Сторонами щодо тлумачення та/або застосування положень цього Договору, підлягають врегулюванню шляхом взаємних консультацій та переговорів. Підписанням цього Договору Сторони засвідчують, що його укладання відповідає вільному волевиявленню Сторін, жодна із Сторін не знаходиться під впливом тяжких обставин та умови цього Договору є взаємовигідними і цілком зрозумілими для обох Сторін.
8.2. У випадку, якщо Сторони протягом одного місяця не зможуть дійти згоди зі спірних питань шляхом переговорів, такий спір підлягає передачі на розгляд суду, згідно з чинним законодавством України.
8.3. Цей Договір укладено в двох оригінальних примірниках українською мовою, по одному для кожної Сторони. Всі примірники мають однакову юридичну силу.
8.4. З укладанням цього Договору Клієнт свідчить про ознайомлення та згоду з тарифами Банку, що є чинними на дату

укладання цього Договору.
8.5. Банк є платником податку на прибуток на загальних умовах, Клієнт є платником податку на прибуток на _____, відповідно до вимог чинного законодавства.

9. РЕКВІЗИТИ І ПІДПИСИ СТОРІН

БАНК	КЛІЄНТ
АТ "КБ "ГЛОБУС" Адреса: Україна, _____ Код: 380526, код за ЄДРПОУ 35591059 Тел.: _____	_____ **Адреса:** _____ **Код ЄДРПОУ**_____ **Тел.** **Тел./факс.**_____
ПІДПИСИ СТОРІН:	
від Банку **М.П.** _____ _____ П.І.Б.	**від Клієнта** **М.П.** _____ _____ П.І.Б.

Один примірник Договору отримав _____ _____
(підпис)

Додаток 1
до Договору про банківське обслуговування
з використанням програмно-технічного комплексу
"Клієнт-Банк" № _____
від __ _____ 201_ р.

ПРАВИЛА ЗБЕРІГАННЯ ТА ВИКОРИСТАННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ПТК КБ

Засоби захисту інформації являють собою зовнішні носії інформації, на яких записані ключі електронного цифрового підпису (ЕЦП) керівників Клієнта.

При отриманні ключів підписати Акт про отримання ключів від уповноваженої особи Банку.

Для виключення псування та компрометації ключів необхідно виконувати наступні заходи:

1. Уникати дій, які можуть привести до псування зовнішнього носія інформації (фізичні та температурні впливи).

2. Встановити на робочу станцію, на якій працює ПТК КБ, антивірусне програмне забезпечення для запобігання дії вірусів на засоби захисту та програмне забезпечення.

3. Забезпечити регулярне оновлення антивірусних баз.

4. У випадку доступу сторонніх осіб до секретних ключів ЕЦП або підозри, що такий доступ мав місце, Клієнт зобов'язаний без зволікання повідомити про це Банк в усній та письмовій формі. З моменту надходження повідомлення Банк зобов'язаний зупинити прийняття платіжних доручень Клієнта по ПТК КБ. Для відновлення роботи в ПТК КБ Клієнт виконує перегенерацію усіх ключів ЕЦП.

5. Після планової заміни ключів ЕЦП знищити старі шляхом переформатування зовнішнього носія інформації.

6. Не залишати у місті з необмеженим доступом зовнішні носії інформації з ЕЦП на період відсутності особи відповідальної за їх збереження.

Додаток 2
до Договору про банківське обслуговування
з використанням програмно-технічного комплексу
"Клієнт-Банк" № _____
від __ _____ 201_ р.

РЕГЛАМЕНТ РОБОТИ ПТК КБ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ.

1.1. Цей додаток визначає порядок і характер робіт, необхідних для здійснення електронних платежів за допомогою ПТК КБ. Умови, не зазначені у цьому додатку, визначаються поточною документацією з експлуатації ПТК КБ.

1.2. Використання Клієнтом ПТК КБ не виключає можливість здійснення платежів з використанням паперових носіїв.

1.3. Банк приймає до виконання електронні платежі, підписані секретними ключами ЕЦП Клієнта, які пройшли без зауважень всі технологічні стадії обробки і розшифровки з використанням відкритих ключів ЕЦП Клієнта.

1.4. При обробці електронних документів Банк здійснює перевірку електронного підпису кожного електронного розрахункового документа, та пакета в цілому.

1.5. Клієнт є ініціативною стороною при проведенні електронних платежів, отриманні інформації про статус електронних платіжних документів, в т.ч. з архіву платіжних документів Клієнта за певний період часу, отриманні виписок про стан поточних рахунків та додаткової інформації.

1.6. Клієнт самостійно здійснює перегенерацію ключів і зміну паролів, що використовується ПТК КБ, у наступних випадках:

- відразу після інсталяції ПТК КБ;
- пошкодження ключового зовнішнього носія інформації;
- втрати паролів;
- звільнення осіб, що мали доступ до ключів ЕЦП та (або) паролів;
- в інших випадках, коли виникає необхідність здійснення зазначених дій.

1.7. Зупинка або відновлення проведення електронних платежів здійснюється Банком на підставі письмової заяви Клієнта у випадку, якщо немає обставин, що перешкоджають цьому (порушення Клієнтом умов цього Договору, тимчасова технічна неможливість і т.п.).

1.8. У випадку необхідності, зміни в Регламент роботи вносяться за ініціативою Банку, з письмовим повідомленням про це Клієнта за 7 робочих днів до зміни із зазначенням дати зміни, що планується.

Банк не несе відповідальності за збої в роботі ПТК КБ, викликані несправністю ліній зв'язку, відключенням або перебоями в лініях електропередач, несправностями апаратних засобів Клієнта та іншими незалежними від Банку причинами.

2. МІНІМАЛЬНІ ВИМОГИ ДО ЗАБЕЗПЕЧЕННЯ РОБОЧОГО МІСЦЯ КЛІЄНТА.

2.1. Канал зв’язку для підключення до мережі “Інтернет”.

2.2. ПК з операційною системою Windows XP і вище та MS Internet Explorer версії 6.0 і вище. Вільного місця на початок роботи на жорсткому диску повинно бути не менше 5 МгБ.

2.3. Лазерний або матричний принтер.

3. ОРГАНІЗАЦІЯ ОБМІНУ ІНФОРМАЦІЄЮ.

3.1. Інсталяція клієнтської частини ПТК КБ може бути проведена на ПЕОМ Клієнтом в Банку, або Банк створює інсталяційний пакет для Клієнта на зовнішньому носію інформації.

3.2. Встановлення програмно - технічного комплексу на робочому місці, налагодження робочого середовища, введення паролів і генерацію ключів ЕЦП в процесі роботи Клієнт виконує самостійно. На прохання Клієнта на етапі встановлення Банк надає консультативну допомогу.

3.3. Обмін інформацією в ПТК КБ між Банком і Клієнтом можливий тільки після здійснення в Банку процедури сертифікації ключів ЕЦП, згенерованих Клієнтом. Під час сертифікації відкриті ключі ЕЦП Клієнта заносяться в базу ключів Банку.

3.4. Банк має право ініціювати перегенерацію ключів ЕЦП Клієнта, повідомивши про це Клієнта не пізніше, ніж за три банківських дні.

3.5. Після отримання інформації про прийом Банком документів переговори про проходження платежу ведуться з операціоністом, що веде рахунок Клієнта.

3.6. Контроль проходження платежів за допомогою ПТК КБ Клієнт здійснює шляхом отримання стану документів, переданих в Банк, та отримання поточного стану рахунків Клієнту. Клієнт формує запити про поточні або підсумкові виписки за своїми рахунками.

3.7. Клієнт може надавати Банку заяви про купівлю, продаж та конвертацію іноземної валюти (за умови своєчасного надання Банку необхідних документів, які є підставою для здійснення цих операцій згідно з діючими Правилами здійснення операцій на МВРУ) за допомогою ПТК КБ.

3.8. Платіжні доручення в іноземній валюті на переказ коштів за межі та в межах України приймаються Банком в операційний час.

Банк залишає за собою право анулювати заяви, що надані пізніше зазначених у цьому додатку строків або заповнені з порушеннями, про що повідомляє Клієнта протягом 1 години з часу її отримання за телефоном, зазначеним у заяві.

Додаток 3
до Договору про банківське обслуговування
з використанням програмно-технічного комплексу
"Клієнт-Банк" № _____
від __ _____ 201_ р.

Правила безпеки при роботі в системі iFOBS

Кожен користувач системи iFOBS - є гарантом і складовою частиною системи безпеки і повинен дотримувати наступних правил:
• Не розголошуйте свій логін і паролі третім особам;
• Зберігайте Ваш особистий сертифікат і секретний ключ на зовнішньому носії інформації (USB-токен, накопичувачі на флеш-памяті та ін) в недоступному для сторонніх осіб місці;
• Не зберігайте зовнішній носій інформації з Вашим особистим сертифікатом і ключем разом з логіном і паролями;
• Не довіряйте стороннім користуватися Вашим особистим сертифікатом і секретним ключем для підписання документів «від імені»;
• Користуйтеся кнопкою «Вихід» для завершення сеансу роботи із системою;
• Не забувайте дістати зовнішній носій інформації, як тільки завершите роботу з системою iFOBS;
• Застосовуйте інші рекомендації банку щодо забезпечення безпеки і цілісності інформації при роботі з системою iFOBS.
.

Не розголошуйте свій логін і паролі третім особам!

Система iFOBS ідентифікує користувача по логіну, паролю на вхід у систему, секретному ключу й паролю на нього. Щоб уникнути несанкціонованого доступу до Вашої конфіденційної інформації не розголошуйте свої реквізити на вхід в систему третім особам.
Кожному користувачеві Банк видає:
• логін - ім'я користувача,
• пароль - пароль на вхід в систему,
• пароль на секретний ключ,
• зовнішній носій інформації, що містить первинний сертифікат і секретний ключ.
При першому вході з цими реквізитами система iFOBS автоматично ініціює процес створення нового сертифіката й секретного ключа. Так само, в цілях безпеки, необхідно змінити пароль на вхід в систему.
Надалі система iFOBS періодично наполегливо рекомендує користувачеві запустити процес створення нового сертифіката й секретного ключа по закінченню терміну дії попередніх.
Система iFOBS фіксує всі спроби зміни й підбору пароля на вхід в систему.

Зберігайте Ваш особистий сертифікат і секретний ключ на зовнішньому носії інформації (USB-токен, накопичувач на флеш-пам'яті тощо)

Банк видає первинні сертифікати й ключі на зовнішньому носії інформації (USB-токен, накопичувач на флеш-пам'яті тощо)
Зберігання цієї інформації на зовнішніх носіях забезпечує не тільки захист Вашої конфіденційної інформації в системі iFOBS, але і забезпечує збереження сертифікатів і секретних ключів при раптових проблемах у роботі Вашого комп'ютера. При генерації / перегенерації робочого сертифіката та секретного ключа, необхідно вказувати шлях на той носій інформації де вони будуть зберігатись.

Не зберігайте зовнішній носій інформації з Вашим особистим сертифікатом і секретним ключем разом з логіном і паролями

Не зберігайте зовнішній носій інформації з Вашими особистим сертифікатом і ключем разом з логіном і паролями. У разі втрати - цією інформацією можуть скористатися сторонні особи в своїх цілях.

Не довіряйте стороннім користуватися Вашим особистим сертифікатом і секретним ключем для підписання документів «від імені»

Однією з функцій системи iFOBS під час підписання документів є «Підписати від імені ...». Дана функція системи дозволяє скоротити час на підготовку документів для відправлення в банк. Не довіряйте виконувати цю операцію від Вашого імені іншим користувачам системи - завжди самостійно вводьте логін і пароль, а також самостійно підключайте зовнішній носій з Вашим особистим сертифікатом і секретним ключем. По закінченню виконання операції не забувайте Ваш зовнішній носій на комп'ютері іншого користувача.

Використовуйте кнопку «Вихід» по завершенню сеансу роботи із системою

Відволікання Вас від комп'ютера при вході в систему, без завершення сеансу роботи з програмою, може спровокувати третю особу скористатися ситуацією.

Не забувайте видалити зовнішній носій інформації, як тільки завершите роботу з системою iFOBS

Не забувайте видалити зовнішній носій інформації, як тільки завершите роботу з системою iFOBS - цією інформацією можуть скористатися сторонні особи, вона може бути безповоротно втрачена або пошкоджена в процесі роботи інших програм.

Застосовуйте інші рекомендації щодо забезпечення безпеки Вашої інформації при роботі з системою iFOBS

Не рекомендується користувачеві працювати із системою iFOBS:

• в інтернет-кафе та інших подібних місцях, де немає гарантії того, що за діями користувача не стежить стороння людина;

• в місцях, де встановлені пристрої відеоспостереження, за допомогою яких можна одержати інформацію про паролі користувача;

• якщо немає впевненості в безпеці використання програмного забезпечення (наявність вірусів, спеціальних програм, що надсилають паролі користувача третім особам і т.п.).

Правила безпеки при роботі через Інтернет

Безпека обміну даними при роботі в мережі Інтернет забезпечується на рівні чіткої взаємної аутентифікації учасників обміну даними.

Клієнтська частина передає на сервер запит на встановлення з'єднання, підписаний цифровим підписом користувача, після чого бібліотеки криптографічного захисту формують необхідні секретні параметри та ключі й підтверджують установку з'єднання. Таким чином, кожне з'єднання має унікальні параметри і дозволяє однозначно ідентифікувати учасників обміну даними.

Обмін даними може бути розпочатий тільки після встановлення криптографічного зв'язку між вузлами «Клієнт» і «Сервер». Весь обмін даними між клієнтом і сервером системи, включаючи передачу на сервер аутентичних повноважень клієнта (паролі) для реєстрації та допуску до даних і операцій, виконується в зашифрованому вигляді. Операції шифрування / розшифрування даних забезпечуються бібліотеками криптографічного та виконуються на прикладному рівні, в процесі підготовки даних для передачі в банк.

Права користувача

В залежності від того, який режим роботи указаний у договорі на підключення й обслуговування клієнта системи iFOBS, користувачеві може бути наданий повний або обмежений доступ до меню системи iFOBS, рахунків, права виконувати операції або ж тільки переглядати інформацію.

Так само можуть бути застосовані обмеження прав користувача, наприклад, користувач має право готувати документи, але не має право їх підписувати.

Для внесень змін у права користувача необхідно звернутися в Банк до адміністратора системи iFOBS.

ЗАЯВА

на підключення до обслуговування в ПТК КБ та SMS-Банкінг

__ _____ 201_ р.

_____ в особі _____ згідно Договору № _____ від __ _____ **201_ р.** заявляє бажання підключитись до обслуговування в ПТК КБ та SMS-Банкінг

Номери поточних рахунків для обслуговування в системі:	_____

Для підключення до ПТК КБ необхідно вказати:

1. Дані користувача для підключення:

ПІБ користувача системи	Право І-го підпису документа	Право ІІ-го підпису документа
	☐	☐

2. Адресу розташування робочого місця, де встановлюватиметься ПТК КБ:

_____

(адреса розташування робочого місця)

Для підключення до системи SMS-Банкінг необхідно вказати:

1. Оператор мобільного зв`язку та номер мобільного телефону

Оператор											
3	8	0									

2. Електронну адресу для отримання E-mail повідомлень про стан Вашого рахунку:

3. Надання інформації про стан рахунку в системі SMS-банкінг:

☐ **на початок операційного дня**	☐ **- на кінець операційного дня**	☐ **- у випадку руху коштів**

_____

З питань організації підключення до ПТК КБ і системи SMS-Банкінг зі сторони підприємства, просимо звертатись до:

_____

(повне ім`я контактної особи)

за телефонами: (_____)_____

(контактні номери телефонів)

Користувач погоджується з тим, що абонентська плата за обслуговування в ПТК КБ починає нараховуватись з дати підготовки Банком програмного забезпечення згідно даної Заяви.

Керівник

(підприємства, організації)_____(_____)

М.П.

Відповідальна особа Банку _____ (_____)

Акт

передачі прав на використання ПТК КБ

__ _____ 201_ р.

Представник ПАТ КБ «ГЛОБУС» в особі _____
ПІБ

і представник _____ в особі

_____
ПІБ

підписали цей Акт до договору про нижченаведене:

1. Банк передав Клієнту ПТК КБ.
2. Банк навчив представника Клієнта роботі в ПТК КБ.
3. Банк передав Клієнту документацію по роботі в ПТК КБ в електронному вигляді.
4. Банк передав Клієнту зовнішній носій інформації з інсталяційним пакетом для встановлення ПТК КБ на комп'ютері Клієнта та генерації ЕЦП.
5. З моменту підписання цього Акту ПТК КБ вважається введеною в експлуатацію.
6. Клієнт не має претензій по виконанню вказаного в даному Акті.

Клієнт ознайомлений з правилами безпеки та регламентом роботи в ПТК КБ (Додатки№1-№3 до цього Договору) та зобов'язується їх неухильно виконувати

_____ (_____).

(підпис) (ПІБ)

Представник **АТ КБ «ГЛОБУС»**

_____
(підпис)
М.П.

Представник _____

_____
(підпис)
М.П.

Додаток 6
до Договору про банківське обслуговування
з використанням програмно-технічного комплексу
"Клієнт-Банк" № _____
від __ _____ 201_ р.

ПРАВИЛА ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КЛЮЧІВ ЕЛЕКТРОННО-ЦИФРОВОГО ПІДПИСУ (ЕЦП) НА КЛІЄНТСЬКОМУ МІСЦІ З ВИКОРИСТАННЯМ USB-ТОКЕН

В якості додаткових засобів для підвищення рівня інформаційної безпеки при роботі в ПТК КБ використовуються носії електронного цифрового підпису "Securetoken 337" (далі – «USB-токен»).

Даний апаратно-програмний засіб призначений для організації захищеного зберігання і використання ключів електронного цифрового підпису.

Для забезпечення неможливості несанкціонованого доступу до рахунків та розкрадання коштів кібер-злочинцями, Клієнт повинен належно використовувати USB-токен з дотриманням наступних правил:

1. Генерація та зберігання ключів ЕЦП повинно відбуватись виключно на USB-токен;
2. Забороняється надавати USB-токен у користування третім особам та повідомляти їм пароль;
3. USB-токен необхідно зберігати в добре захищеному місці (наприклад, в сейфі), що виключає можливість несанкціонованого використання пристрою третіми особами, а також убезпечує USB–токен від впливу електромагнітних полів та потрапляння на нього вологи і пилу.

   Відповідальність за схоронність USB-токена та забезпечення його захисту від будь-яких пошкоджень покладається на Клієнта.
4. Клієнт не повинен залишати USB-токен безконтрольно постійно підключеним до комп’ютера. По закінченню роботи в ПТК КБ USB-токен повинен бути відключений від комп’ютера.

В разі втрати або викрадення USB–точена, Клієнту необхідно негайно повідомити про це Банк будь-якими доступними засобами зв`язку і в подальшому надати в Банк оригінал такого повідомлення з роз`ясненнями, за підписом уповноваженої особи Клієнта і відбитком печатки (у разі її наявності).

ЗАЯВА
на використання носія електронно-цифрового підпису
USB-токен в ПТК КБ

м. **_____** **__ _____ 201_ р.**

_____ в особі **_____** згідно Договору № **_____** від **__ _____ 201_ р.** заявляє бажання обслуговуватись в ПТК КБ з використанням носія ЕЦП USB-токен

Для використання USB-токену в ПТК КБ необхідно вказати дані користувача (ПІБ – обов'язково, ЛОГІН – за наявності):

Ідентифікатор користувача системи	
ПІБ	
ЛОГІН	

З питань генерації та зберігання ключа електронного цифрового підпису з використанням USB-токену зі сторони підприємства просимо звертатись до:

_____
(повне ім`я контактної особи)

за телефонами: (_____)_____
(контактні номери телефонів)

Керівник
(підприємства, організації)_____(_____)

М.П.

Відповідальна особа Банку _____ (_____)

Акт
приймання - передачі носіїв ЕЦП USB-токен ПТК КБ
у тимчасове користування

__ _____ 201_ р.

Представник ПАТ КБ «ГЛОБУС» в особі _____
ПІБ

і представник _____ в особі

_____
ПІБ

склали дійсний Акт до Договору про нижченаведене:

Банк передав, а Клієнт прийняв у тимчасове користування на період дії Договору USB-токен для генерації та зберігання ключів електронного цифрового підпису в кількості __ (_____) шт.

Клієнт ознайомлений з Правилами забезпечення захисту ключів електронного цифрового підпису (ЕЦП) на клієнтському місці з використанням USB-токен (Додаток №6 до Договору) та зобов'язується їх неухильно виконувати.

_____ (_____).

(підпис) (ПІБ)

Представник **АТ КБ «ГЛОБУС»**

_____
(підпис)
М.П.

Представник _____

_____
(підпис)
М.П.