Затверджено
Протокол засідання Правління
публічного акціонерного товариства
"Розрахунковий центр з обслуговування
договорів на фінансових ринках"
04.02.2014 р. №08

Викладено у новій редакції
Протокол засідання Правління
публічного акціонерного товариства
"Розрахунковий центр з обслуговування
договорів на фінансових ринках"
05.12.2017 р. №58

Положення
про Систему дистанційного обслуговування "Інтернет-банкінг" публічного акціонерного товариства "Розрахунковий центр з обслуговування договорів на фінансових ринках"

1. Загальні положення

1.1. Терміни, які вживаються в Положенні про Систему дистанційного обслуговування "Інтернет-банкінг" публічного акціонерного товариства "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі – Положення):

- **Банк** – публічне акціонерне товариство "Розрахунковий центр з обслуговування договорів на фінансових ринках";
- **блокування доступу Користувача до Системи** – дії Банку внаслідок яких унеможливлюється доступ Користувача до Системи;
- **блокування сертифіката ключа** – тимчасове зупинення чинності сертифіката ключа;
- **відкритий ключ** – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;
- **електронний документ (ЕД)** – електронний розрахунковий документ, який сформований та відправлений Клієнтом до Банку за допомогою Системи, який містить розпорядження Клієнта Банку для здійснення операцій по Рахунку / Рахунках.
- **електронний цифровий підпис (далі – ЕЦП)** – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. ЕЦП накладається за допомогою особистого ключа і перевіряється за допомогою відкритого ключа;
- **компрометація особистого ключа** – будь-яка подія та / або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;
- **Клієнт** – фізична або юридична особа, яка уклала з Банком договір про обслуговування в системі інтернет-банкінгу;
- **Користувачі –** Клієнти-фізичні особи або фізичні особи, уповноважені Клієнтом розпоряджатися Рахунком / Рахунками Клієнта і підписувати електронні документи;
- **особистий ключ –** параметр криптографічного алгоритму формування ЕЦП, доступний тільки користувачу ЕЦП. Особистий ключ працює тільки в парі з відкритим ключем;
- **поновлення сертифіката ключа –** відновлення чинності попередньо заблокованого сертифіката ключа;

- **Рахунок / Рахунки** – поточний або кореспондентський рахунок Клієнта в Банку;
- **Система дистанційного обслуговування "Інтернет-банкінг" публічного акціонерного товариства "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі – Система)** – сукупність технічних засобів та програмного забезпечення, впровадженого в Банку, що дозволяють Клієнту дистанційно отримувати інформацію по Рахунках та здійснювати розрахункові операції по Рахунку / Рахунках на підставі електронних документів Клієнта, а також отримувати інші послуги в порядку та на умовах, передбачених договором про обслуговування в системі інтернет-банкінг, укладеним між Банком та Клієнтом;
- **скасування сертифіката ключа** – припинення чинності сертифіката ключа.

Інші терміни, що вживаються в цьому Положенні, використовуються відповідно до законодавства України.

1.2. Положення визначає загальний порядок обігу електронних документів між Банком та Клієнтом при роботі за допомогою Системи, умови допуску та порядок підключення Клієнта до Системи, порядок отримання від Банку засвідчених відкритих ключів, порядок дії при компрометації особистих ключів Клієнта.

2. Обіг електронних документів

2.1. Формування електронних документів Клієнтом здійснюється за допомогою програмних засобів, наданих Клієнту Банком.

2.2. Електронні документи, що надходять від Клієнта до Банку, повинні містити в собі реквізити, встановлені законодавством України, зокрема нормативно-правовими актами Національного банку України.

2.3. Юридична сила ЕД забезпечується накладенням ЕЦП Користувача відповідно до вимог цього Положення. Для накладення ЕЦП Користувача використовується особистий ключ.

2.4. У Банку перевіряється ЕЦП ЕД і правильність заповнення реквізитів ЕД. У разі позитивного результату контролю ЕД такий ЕД виконується. У разі негативного результату контролю ЕД такий ЕД не виконується Банком, Банк повертає Клієнту електронний документ засобами Системи із зазначенням причин відмови прийняти документ до виконання. Електронний документ набуває статус «Відхилений банком».

2.6. Банк протягом операційного дня обробляє ЕД, що надійшли від Клієнтів протягом операційного часу. ЕД, передані до Банку після операційного часу, виконуються протягом операційного часу не пізніше наступного операційного дня Банку. У разі відмови Банком від виконання ЕД Клієнта, надісланого засобами Системи, Банк повертає Клієнту електронний документ засобами Системи із зазначенням причин відмови прийняти документ до виконання. Електронний документ набуває статус «Відхилений банком».

2.7. Електронний документ Клієнта повинен містити наступну кількість ЕЦП:

2.7.1. для Клієнта-юридичної особи:

- один ЕЦП Користувача, який має право першого підпису відповідно до картки із зразками підписів Клієнта,
- один ЕЦП Користувача, який має право другого підпису відповідно до картки із зразками підписів Клієнта (крім випадків, коли відповідно до вимог законодавства України в картці із зразками підписів Клієнта не вказані особи, які мають право другого підпису),
- один ЕЦП печатки Клієнта (в разі використання Клієнтом печатки).

2.7.2. для Клієнта-фізичної особи – один ЕЦП Користувача.

3. Одержання додаткової інформації

3.1. Клієнт за допомогою Системи може отримати наступну додаткову інформацію:

- актуальний стан довідника банків України;
- актуальний стан залишків коштів на Рахунку / Рахунках Клієнта;
- актуальний список та стан розрахункових документів, проведених за Рахунком / Рахунками Клієнта;
- курси валют Національного банку України;
- виписка з Рахунку / Рахунків Клієнта;
- текстові повідомлення від Банку.

4. Підключення до Системи

4.1. Підключення до Системи можливе після виконання Клієнтом – фізичною особою таких умов:

4.1.1. Укладення з Банком договору банківського рахунку і договору про обслуговування в системі інтернет-банкінг;

4.1.2. У разі, якщо Клієнту необхідно отримати від Банку в користування носії ключової інформації "Secure Token 337" - оплата Клієнтом заставної вартості носіїв ключової інформації відповідно до умов договору про обслуговування в системі інтернет-банкінг і їх отримання від Банку. Підтвердженням надання Клієнту носія (носіїв) ключової інформації є Акт прийому-передачі носіїв ключової інформації (Додаток 9).

4.1.3. Отримання та інсталяція програмного забезпечення, що забезпечує підготовку даних для виконання алгоритмів ЕЦП та генерацію особистих ключів;

4.1.4. Генерація особистого ключа та відкритого ключа Користувача;

4.1.5. Відправка на електрону адресу cck@settlement.com.ua Банку відкритого ключа підпису Користувача на засвідчення та реєстрацію в системі.

4.1.6. Надання Банку заяви на підключення до Системи (Додаток 1);

4.1.7. Надання Банку заяви на засвідчення та реєстрацію відкритого ключа Користувача Клієнта в Системі (Додаток 2);

4.1.8. Налаштування робочого місця Клієнта відповідно вимог до програмно-технічного забезпечення Клієнтів (Додаток 7);

4.1.9. Підписання Акту про підключення до Системи між Банком та Клієнтом (Додаток 3).

4.2. Підключення до Системи можливе після виконання Клієнтом – юридичною особою таких умов:

4.2.1. Укладення з Банком договору банківського рахунку/ договору про відкриття та обслуговування кореспондентського рахунку та договору про обслуговування в системі інтернет-банкінг;

4.2.2. У разі, якщо Клієнту необхідно отримати від Банку в користування носії ключової інформації "Secure Token 337" - оплата Клієнтом заставної вартості носіїв ключової інформації відповідно до умов договору про обслуговування в системі інтернет-банкінг і їх отримання від Банку. Підтвердженням надання Клієнту носія (носіїв) ключової інформації є Акт прийому-передачі носіїв ключової інформації (Додаток 9).

4.2.3. Отримання та інсталяція програмного забезпечення, що забезпечує підготовку даних для виконання алгоритмів ЕЦП та генерацію особистих ключів;

4.2.4. Генерація особистих ключів та відкритих ключів Користувачам;

4.2.5. Відправка на електрону адресу cck@settlement.com.ua Банку відкритих ключів підпису Користувачів на засвідчення та реєстрацію в системі.

4.2.6. Надання Банку заяви на підключення до Системи (Додаток 4);

4.2.7. Надання Банку заяви на засвідчення та реєстрацію відкритого ключа Користувача Клієнта в Системі (Додаток 5);

4.2.8. Налаштування робочого місця Клієнта відповідно вимог до програмно-технічного забезпечення Клієнтів (Додаток 7);

4.2.9. Підписання Акту про підключення до Системи між Банком та Клієнтом (Додаток 6).

5. Вимоги до ЕЦП Клієнта

5.1. З метою захисту особистих ключів від несанкціонованого використання третіми особами в Системі для генерації та зберігання ключів ЕЦП застосовуються виключно спеціальні захищені носії ключової інформації виробництва ТОВ "Автор" (ЄДРПОУ 32248356), а саме - електронні носії "Secure Token 337".

5.2. Носії ключової інформації "Secure Token 337" придбаваються Клієнтом самостійно або надаються Клієнту в користування Банком відповідно до умов договору про обслуговування в системі інтернет-банкінг. В разі необхідності отримання в користування носіїв ключової інформації Клієнт зазначає про це в заявці на укладення договору про обслуговування в системі інтернет-банкінг, розміщеній на веб-сайті http://www.settlement.com.ua.

При поверненні Клієнтом Банку отриманих носіїв ключової інформації "Secure Token 337" без пошкоджень і в робочому стані складається Акт прийому-передачі носіїв ключової інформації (Додаток 10).

5.3. Клієнт для кожного свого Користувача генерує особистий ключ і відкритий ключ, які є унікальними.

5.4. Особистий ключ використовується в Системі для накладання ЕЦП, який в свою чергу використовується для ідентифікації особи, що накладає ЕЦП, і підтвердження цілісності електронного документа, що передається в Банк.

5.5. Відкритий ключ використовується Банком для перевірки ЕЦП Користувача на ЕД.

5.6. Користувачі, які здійснюють діяльність в Системі, зобов’язані володіти чинним особистим ключем. При зміні Користувачів генеруються нові особисті ключі

5.7. Клієнт повинен використовувати таку кількість особистих ключів, яка необхідна для накладення ЕЦП відповідно до вимог розділу 2 цього Положення.

5.8. Власник особистого ключа несе повну відповідальність за збереження особистого ключа і приймає всі заходи, що перешкоджають користуванню цим ключем сторонніми особами.

5.9. Термін дії кожного особистого ключа Клієнта становить **365** календарних днів з дня його генерації.

5.10. Для генерації особистих ключів Клієнт використовує необхідну кількість носіїв ключової інформації з дотриманням вимог, встановлених пунктом 5.7. цього Положення.

6. Порядок генерації ключів ЕЦП та засвідчення відкритих ключів Клієнта

6.1. Клієнт ознайомлюється з Інструкцією з генерації ключів ЕЦП та засвідчення відкритих ключів(далі - Інструкція) на веб-сайті Банку www.settlement.com.ua.

6.2. Відповідно до інструкції завантажує з ftp- серверу Банку ftp:\\settlement.com.ua утиліту для генерації ключів.

6.3. Далі Клієнт інсталює на робочому місці утиліту для генерації ключів.

6.4. Далі Клієнт відповідно до інструкції генерує для Користувача особистий та відкритий ключі.

6.5. Після цього Клієнт направляє в Банк заяву на засвідчення та реєстрацію відкритого ключа Користувача Клієнта в Системі в паперовій формі.

6.6. Далі відповідно до інструкції Клієнт направляє відкритий ключ на електронну адресу Банку.

6.7. Банк на підставі заяви на засвідчення та реєстрацію відкритого ключа Користувача Клієнта засвідчує та реєструє відкритий ключ в Системі.

6.8. Засвідчений відкритий ключ Банк направляє Клієнту засобами електронної пошти на адресу, з якої отримав відкритій ключ на засвідчення.

6.9. Клієнт відповідно до інструкції активує особистий ключ підпису занесенням засвідченого відкритого ключа на носій ключової інформації.

6.10. Для повторної генерації особистих та відкритих ключів Клієнт виконує дії відповідно п. 6.4.-6.6., 6.8.,6.9. цього Положення.

7. Забезпечення інформаційної безпеки в Системі

7.1. Засоби забезпечення інформаційної безпеки.

7.1.1. Інформаційна безпека в Системі реалізується за допомогою програмно-технічних та організаційних засобів.

7.1.2. До програмно-технічних засобів інформаційної безпеки відносяться:

7.1.2.1. Система паролів та ідентифікаторів для розмежування доступу Користувачів до технічних і програмних засобів Системи;

7.1.2.2. Використання програмного забезпечення для підготовки даних для виконання алгоритмів ЕЦП;

7.1.2.3. Програмно-апаратні засоби захисту від несанкціонованого доступу до ЕД та іншої інформації;

7.1.2.4. Криптографічне шифрування інформації в каналах зв’язку з використанням алгоритмів шифрування відповідно до ГОСТ 28147;

7.1.2.5. Засоби захисту від програмних вірусів.

7.1.3. До організаційних заходів відносяться:

7.1.3.1. Розміщення технічних засобів в приміщеннях з контрольованим доступом;

7.1.3.2. Адміністративні обмеження доступу до технічних засобів;

7.1.3.3. Допуск до Системи тільки спеціально підготовлених та уповноважених осіб;

7.1.3.4. Підтримка програмно-технічних засобів в справному стані.

7.2. Порядок дій при компрометації особистих ключів Клієнта.

7.2.1. До подій, на підставі яких Клієнт приймає рішення про компрометацію особистого ключа, відносяться наступні:

- втрата носія ключової інформації з особистим ключем;

- виникнення підозри на виток інформації або її спотворення за рахунок несанкціонованого використання.

7.2.2. В разі компрометації особистих ключів, Клієнт негайно повідомляє про це Банк шляхом надіслання засобами факсимільного зв'язку письмового повідомлення про компрометацію, підписаного Клієнтом-фізичною особою або керівником (особою, що виконує обов'язки керівника) Клієнта-юридичної особи, з подальшою відправкою оригіналу вказаного повідомлення поштою або кур'єрським зв'язком.

В разі ненадання Клієнтом такого повідомлення, особисті ключі якого скомпрометовані, для Банку відкриті ключі вважаються чинними і Банк не несе відповідальності за одержання, оброблення та здійснення інших дій щодо ЕД підписаних ЕЦП Клієнта.

7.2.3. В разі отримання Банком факсимільного письмового повідомлення від Клієнта про компрометацію особистого ключа, Банк здійснює блокування сертифіката ключа та блокування доступу Користувача до Системи.

Після отримання оригіналу письмового повідомлення Клієнта про компрометацію особистого ключа, Банк здійснює скасування сертифіката ключа Користувача та вносить відкритий ключ Клієнта в список відкликаних відкритих ключів (далі – СВВК).

7.2.4. Банк з моменту внесення відкритих ключів Клієнта в СВВК, припиняє обробку та виконання ЕД Клієнта, що підписані "скомпрометованими" особистими ключами Клієнта, які відповідають відкритим ключам включеним до СВВК.

8. Порядок блокування, поновлення та скасування сертифіката ключа Користувача, блокування доступу Користувача до Системи

8.1. Банк здійснює блокування сертифіката ключа Користувача та блокування доступу Користувача до Системи у таких випадках:

8.1.1. Закінчення строку повноважень Користувача розпоряджатися Рахунком / Рахунками Клієнта і підписувати електронні документи (в разі якщо Банку для відкриття чи обслуговування Рахунку / Рахунків Клієнта були надані документи, в яких вказані строки повноважень Користувача) – з дня наступного за днем закінчення строку повноважень Користувача;

8.1.2. Відсутності вклеєних в паспорт Користувача фотокарток при досягненні Користувачем 25 / 45-річного віку – з дня наступного за днем досягнення Користувачем 25 / 45-річного віку;

8.1.3. Призначення, зміни або припинення повноважень уповноваженої особи Фонду гарантування вкладів фізичних осіб на здійснення тимчасової адміністрації у Клієнті або на ліквідацію Клієнта – з дня розміщення відповідної інформації на сайті Фонду гарантування вкладів фізичних осіб;

8.1.4. Отримання Банком інформації з офіційних джерел (у тому числі веб-сайтів https://smida.gov.ua, https://stockmarket.gov.ua, https://usr.minjust.gov.ua, https://fg.gov.ua, https://lr.nssmc.gov.ua) щодо зміни інформації про Користувача – в день отримання Банком відповідної інформації;

8.1.5. Отримання факсимільного письмового повідомлення від Клієнта про компрометацію особистого ключа – в день отримання такого повідомлення від Клієнта.

8.2. Банк поновлює сертифікат ключа Користувача та розблоковує доступ Користувача до Системи у таких випадках:

8.2.1. Якщо блокування сертифіката ключа Користувача та блокування доступу Користувача до Системи було здійснено з підстави, вказаної в п.8.1.1. цього Положення – у день внесення Банком змін до документів справи з юридичного оформлення рахунку Клієнта,

які підтверджують продовження строку повноважень Користувача як особи, яка має право розпорядження Рахунком / Рахунками Клієнта та підписання розрахункових документів;

8.2.2. Якщо блокування сертифіката ключа Користувача та блокування доступу Користувача до Системи було здійснено з підстави, вказаної в п.8.1.2. цього Положення – у день внесення Банком змін до документів справи з юридичного оформлення рахунку Клієнта, які підтверджують наявність в паспорті Користувача фотокарток при досягнені Користувачем 25 / 45-річного віку;

8.2.3. Якщо блокування сертифіката ключа Користувача та блокування доступу Користувача до Системи було здійснено з підстави, вказаної в п.8.1.3. цього Положення – у день отримання Банком документів, що підтверджують повноваження Користувача як особи, яка має право розпорядження Рахунком / Рахунками Клієнта та підписання розрахункових документів;

8.2.4. Якщо блокування сертифіката ключа Користувача та блокування доступу Користувача до Системи було здійснено з підстави, вказаної в п.8.1.4. цього Положення – у день отримання Банком документів, що підтверджують повноваження Користувача як особи, яка має право розпорядження Рахунком / Рахунками Клієнта та підписання розрахункових документів, або документів, що підтверджують відсутність змін в інформації про Користувача, або у день внесення Банком змін до документів справи з юридичного оформлення Рахунку/Рахунків Клієнта, які підтверджують відповідні зміни щодо Користувача (якщо для поновлення сертифіката ключа Користувача та розблокування доступу Користувача до Системи необхідне внесення змін до документів справи з юридичного оформлення Рахунку/Рахунків Клієнта).

8.3. Банк здійснює скасування сертифіката ключа Користувача та блокування доступу Користувача до Системи у таких випадках:

8.3.1. Зміна Користувача або зміна прізвища, імені, по батькові Користувача – у день отримання Банком документів, що підтверджують ці зміни;

8.3.2. Зміна найменування Клієнта-юридичної особи – у день отримання Банком документів, що підтверджують ці зміни;

8.3.3. Закінчення строку чинності сертифіката – у день і час закінчення строку чинності сертифіката;

8.3.4. Закриття Рахунку Клієнта – у день закриття Рахунку;

8.3.5. Розірвання / припинення дії договору про обслуговування в системі інтернет-банкінгу, укладеного з Клієнтом – у день розірвання /припинення дії договору про обслуговування в системі інтернет-банкінгу;

8.3.6. Призначення, зміни або припинення повноважень уповноваженої особи Фонду гарантування вкладів фізичних осіб на здійснення тимчасової адміністрації у Клієнті або на ліквідацію Клієнта – у день отримання Банком документів щодо припинення повноважень Користувача як особи, яка має право розпорядження Рахунком / Рахунками Клієнта та підписання розрахункових документів, або у день внесення Банком змін до документів справи з юридичного оформлення Рахунку/Рахунків Клієнта, які підтверджують відповідні зміни щодо Користувача (якщо клієнтом були надані документи для внесення Банком змін до документів справи з юридичного оформлення Рахунку/Рахунків Клієнта);

8.3.7. Отримання оригіналу письмового повідомлення Клієнта про компрометацію особистого ключа – в день отримання такого повідомлення від Клієнта.

8.4. У разі скасування сертифіката ключа Користувача з підстав, вказаних в п.8.3.1., 8.3.2., 8.3.3., 8.3.7. цього Положення, для поновлення доступу Користувача до Системи Клієнту необхідно виконати повторну генерацію особистих та відкритих ключів відповідно до розділу 6 цього Положення.

9. Порядок вирішення конфліктних ситуацій та спорів у Системі

9.1. При роботі в Системі можливе виникнення конфліктних ситуацій, пов'язаних з формуванням, доставкою, отриманням, підтвердженням отримання ЕД, а також використанням в даних документах ЕЦП. Дані конфліктні ситуації можуть виникати в наступних випадках:

9.1.1. Заперечення факту формування, підписання ЕД особистими ключами Клієнта;

9.1.2. Заперечення факту відправлення ЕД в Системі;

9.1.3. Інші випадки виникнення конфліктних ситуацій, пов'язаних з функціонуванням Системи.

9.2. Конфліктна ситуація може виникнути у випадку, якщо Банк висловлює недовіру до складу і формату ЕД, що відправлено Клієнтом, а також якщо Банк висловлює недовіру до програмного забезпечення, що функціонує на робочому місці Клієнта.

9.3. Повідомлення про конфліктну ситуацію:

9.3.1. В разі виникнення конфліктної ситуації Клієнт, повинен негайно направити повідомлення про конфліктну ситуацію в Банк;

9.3.2. повідомлення про наявність конфліктної ситуації повинне містити інформацію про зміст конфліктної ситуації і обставини, які свідчать про наявність конфліктної ситуації. Незалежно від форми, в якій складено повідомлення (паперова форма або електронний документ), таке повідомлення повинне містити реквізити відповідного ЕД. Крім того, в ньому мають бути вказані прізвище, ім'я і по батькові, посада (за наявності), контактні телефони, факс (за наявності), адреса електронної пошти контактної особи або контактних осіб з питань врегулювання конфліктної ситуації.

9.4. Розгляд конфліктної ситуації

9.4.1. Конфліктна ситуація визнається вирішеною в робочому порядку у випадку, якщо Клієнт задоволений інформацією, отриманою від Банку.

9.4.2. У випадку, якщо Клієнт не задоволений отриманою від Банку інформацією, для розгляду конфліктної ситуації формується відповідна технічна комісія Банку.

9.4.3. Не пізніше ніж на наступний робочий день після того, як прийнято рішення про необхідність формування технічної комісії, або не пізніше, ніж на третій робочий день після отримання повідомлення про конфліктну ситуацію, у випадку, якщо конфліктна ситуація не була врегульована в робочому порядку, технічна комісія має бути сформована.

9.4.4. До складу технічної комісії можуть входити фахівці з числа працівників підрозділів інформаційної безпеки Клієнта. Особи, що входять до складу технічної комісії, повинні володіти необхідними знаннями в галузі побудови системи криптографічного захисту інформації, роботи комп'ютерних інформаційних систем та ЕЦП.

9.4.5. Загальна кількість членів технічної комісії – 5 осіб. До складу технічної комісії можуть входити Клієнти або представники Клієнтів. Повноваження представника Клієнта для участі в технічній комісії повинні бути підтвердженні згідно законодавства України.

9.4.6. Сформована технічна комісія при розгляді конфліктної ситуації встановлює на технологічному рівні наявність або відсутність фактичних обставин, що свідчать про факт і час складання та / або відправки ЕД, достовірність ЕД, а також факт підписання ЕД ЕЦП, автентичність відправленого документа отриманому та інші факти.

Технічна комісія має право розглядати будь-які інші технічні питання, необхідні для з'ясування причин і наслідків виникнення конфліктної ситуації.

9.4.7. Технічна комісія не дає правову або яку-небудь іншу оцінку професійній діяльності Клієнта або Банку, які були виконані або не виконані, або несвоєчасно виконані на підставі ЕД, у відношенні якого / яких розглядається конфліктна ситуація.

9.4.8. Всі дії, що здійснюються технічною комісією для з'ясування фактичних обставин, а також висновки, зроблені технічною комісією, заносяться в протокол засідання технічної комісії. Протокол засідання технічної комісії повинен містити наступні дані:

9.4.8.1. Склад технічної комісії з вказівкою відомостей про кваліфікацію кожного з членів технічної комісії;

9.4.8.2. Короткий виклад обставин конфліктної ситуації, що виникла;

9.4.8.3. Заходи, що проводяться технічною комісією для встановлення підстав виникнення і наслідків конфліктної ситуації, з вказівкою дати, часу і місця проведення заходів;

9.4.8.4. Висновки технічної комісії в результаті проведених досліджень конфліктної ситуації;

9.4.9. У випадку якщо думка члена технічної комісії щодо порядку, методики, мети заходів, що проводяться, не збігається з думкою більшості членів технічної комісії, про це в Протоколі засідання технічної комісії складається відповідний запис, який підписується членом (або членами технічної комісії), особливу думку якого / яких відображає відповідний запис.

9.4.10. Протокол засідання технічної комісії складається в двох примірниках на паперовому носії, який надається Клієнту.

9.5. Порядок врегулювання суперечок і розбіжностей

9.5.1. Всі спори і розбіжності, які можуть виникнути у зв'язку із застосуванням, порушенням, тлумаченням цього Положення, визнанням недійсними цього Положення, сторони прагнутимуть вирішити шляхом переговорів.

9.5.2. У випадку, якщо конфліктна ситуація не врегульована в процесі переговорів, може бути вирішена у судовому порядку.

10. Прикінцеві положення

10.1. Це Положення затверджується Правлінням та набуває чинності з моменту його затвердження.

10.2. Зміни та доповнення до цього Положення затверджуються Правлінням Банку. Внесення змін та доповнень здійснюється шляхом затвердження нової редакції цього Положення.

10.3. У випадку, якщо будь-яка частина цього Положення перестає відповідати законодавству України та / або Статуту, то відповідна частина цього Положення втрачає чинність і Положення застосовується лише в тій частині, що не суперечить законодавству України та Статуту.

Голова Правління **Ю.І. Шаповал**

РОЗРОБНИК:

Начальник відділу інформаційної безпеки _____ Ю.Ю. Желябовський

ПОГОДЖЕНО:

Начальник управління комплаєнс-контролю _____ І.В. Гнатюк

Начальник управління інформаційних технологій	_____	К.В. М’якушко
Начальник управління забезпечення розрахунків	_____	Б.Б. Жиров

Додатки

Додаток 1

Заява
на підключення до Системи дистанційного обслуговування "Інтернет-банкінг"

" ___" _____ 201_ р.

Я_____
(П.І.Б. Клієнта)

Прошу Вас підключити до Системи дистанційного обслуговування "Інтернет-банкінг" та надати доступ для дистанційного обслуговування Рахунку № ☐☐☐☐☐☐☐☐☐☐☐☐☐☐,
створити та налаштувати права доступу таким Користувачам:

1. Користувач (перша особа – власник Рахунку)*:

Прізвище	
Ім'я	
По батькові	
ІПН	
E-Mail	
Контактний тел.	

2. Користувач (друга особа - довірена особа (за наявності)*:

Прізвище	
Ім'я	
По батькові	
ІПН	
E-Mail	
Контактний тел.	

Клієнт _____ / _____ /
(підпис) (прізвище, ініціали)

* Особи зазначені в картці із зразками підписів Клієнта.

Продовження на звороті

Управління забезпечення розрахунків

_____

(вхідний номер, дата прийому, прізвище, ініціали та підпис)

Адміністратор системи "Інтернет-банкінг"

_____

(дата підключення, прізвище, ініціали та підпис)

Додаток 2

Заява
на засвідчення та реєстрацію
відкритого ключа Користувача Клієнта в Системі дистанційного обслуговування "Інтернет-банкінг"

" ___" _____ 201_ р.

Я_____
(П.І.Б. Клієнта)

Прошу Вас засвідчити та зареєструвати відкриті ключі в Системі дистанційного обслуговування "Інтернет-банкінг" таким Користувачам:

1. Користувач (перша особа – власник Рахунку)*:

Прізвище	
Ім'я	
По батькові	
E-Mail	
Контактний тел.	
Зразок підпису власника відкритого ключа	

Заповнюється працівником підрозділу інформаційної безпеки Банку:

Серійний номер сертифіката/дата засвідчення	
Прізвище, ініціали, підпис	

2. Користувач (друга особа - довірена особа (за наявності)*:

Прізвище	
Ім'я	
По батькові	
E-Mail	
Контактний тел.	
Зразок підпису власника відкритого ключа	

Заповнюється працівником підрозділу інформаційної безпеки Банку:

Серійний номер сертифіката/дата засвідчення	
Прізвище, ініціали, підпис	

Клієнт _____ / _____ /
(підпис) (прізвище, ініціали.)

* Особи зазначені в картці із зразками підписів Клієнта.

Продовження на звороті

Заповнюється працівниками Банку

Управління забезпечення розрахунків

_____

(вхідний номер, дата прийому, прізвище, ініціали та підпис)

Додаток 3

Акт про підключення
до Системи дистанційного обслуговування "Інтернет-банкінг"

м. Київ _____ 201__ року

Публічне акціонерне товариство "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі – Банк) в особі_____
_____,
який діє на підставі_____,
та_____(далі – Клієнт)
підписали цей акт про таке:

1. Банк підключив Клієнта до Системи дистанційного обслуговування "Інтернет-банкінг" та надав доступ для дистанційного обслуговування Рахунку

№ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐,

2. Банк створив та налаштував права доступу таким Користувачам:

- _____ створювати ЕД, підписувати ЕД, перегляд залишків коштів
  (П.І.Б. Користувача)
- _____ створювати ЕД, підписувати ЕД, перегляд залишків коштів
  (П.І.Б. Користувача)

3. Банк зареєстрував в Системі дистанційного обслуговування "Інтернет-банкінг" відкриті ключі таких Користувачів:

№	*Заповнюється клієнтом:*	*Заповнюється працівником підрозділу інформаційної безпеки Банку:*	
1.	Прізвище, ім'я, по батькові Користувача: _____	Серійний номер сертифіката _____	Прізвище, ініціали, підпис _____
2.	Прізвище, ім'я, по батькові Користувача: _____	Серійний номер сертифіката _____	Прізвище, ініціали, підпис _____

ПАТ "Розрахунковий центр" Клієнт

_____ _____ _____ _____
(підпис) (прізвище, ініціали) (підпис) (прізвище, ініціали)

Продовження на звороті

Управління забезпечення розрахунків

_____

(вхідний номер, дата прийому, прізвище, ініціали та підпис)

Додаток 4

Заява
на підключення до Системи дистанційного обслуговування "Інтернет-банкінг"

№_____ " ___" _____ 201_ р.

1. Просимо Вас підключити до Системи дистанційного обслуговування "Інтернет-банкінг"

_____
(повне найменування Клієнта)

та надати доступ для дистанційного обслуговування Рахунку №

☐☐☐☐☐☐☐☐☐☐☐☐☐☐

створити та налаштувати права доступу таким Користувачам.

1.1. Користувач (Особа, яка має право першого підпису)*:

Посада	
Прізвище	
Ім'я	
По батькові	
E-Mail	
Контактний тел.	

1.2. Користувач (Особа, яка має право другого підпису)*:

Посада	
Прізвище	
Ім'я	
По батькові	
E-Mail	
Контактний тел.	

1.3. Користувач (Особа, яка відповідальна за підпис печатки):**

Повне найменування Клієнта	
E-Mail	
ЄДРПОУ	
Прізвище, ім'я, по батькові відповідальної особи	
Контактний тел.	

Керівник Клієнта _____ / _____ /
(підпис) (прізвище, ініціали)

* Особи зазначені в картці із зразками підписів Клієнта. Вказується необхідна кількість осіб відповідно до картки із зразками підписів

** Заповнюється в разі використання Клієнтом печатки

Продовження на звороті

Управління забезпечення розрахунків

_____

(вхідний номер, дата прийому, прізвище, ініціали та підпис)

Адміністратор системи "Інтернет-банкінг"

_____

(дата підключення, прізвище, ініціали та підпис)

Додаток 5

Заява
на засвідчення та реєстрацію
відкритого ключа Користувача Клієнта в Системі дистанційного обслуговування "Інтернет-банкінг"
№_____ "___" _____ 201_ р.

1. Просимо Вас засвідчити та зареєструвати відкриті ключі в Системі дистанційного обслуговування "Інтернет-банкінг" таким Користувачам_____
(повне найменування Клієнта)

2. Користувач (Особа, яка має право першого підпису)*:

Посада	
Прізвище	
Ім'я	
По батькові	
E-Mail	
Контактний тел.	
Діє на підставі (статут, довіреність, інше)	
Зразок підпису власника відкритого ключа	

Заповнюється працівником підрозділу інформаційної безпеки Банку:

Серійний номер сертифіката/дата засвідчення	
Прізвище, ініціали, підпис	

3. Користувач (Особа, яка має право другого підпису)*:

Посада	
Прізвище	
Ім'я	
По батькові	
E-Mail	
Контактний тел.	
Діє на підставі (статут, довіреність, інше)	
Зразок підпису власника відкритого ключа	

Заповнюється працівником підрозділу інформаційної безпеки Банку:

Серійний номер сертифіката/дата засвідчення	
Прізвище, ініціали, підпис	

4. Користувач (Особа, яка відповідальна за підпис печатки) **:

Повне найменування Клієнта	
E-Mail	
ЄДРПОУ	
Прізвище, ім'я, по батькові відповідальної особи	
Контактний тел.	
Діє на підставі (статут, довіреність, інше)	

Заповнюється працівником підрозділу інформаційної безпеки Банку:

Серійний номер сертифіката/дата засвідчення	
Прізвище, ініціали, підпис	

Керівник Клієнта _____ / _____ /

(підпис) (прізвище, ініціали)

* Особи зазначені в картці із зразками підписів Клієнта. Вказується необхідна кількість осіб відповідно до картки із зразками підписів

** Заповнюється в разі використання Клієнтом печатки

Заповнюється працівниками Банку

Управління забезпечення розрахунків

_____

(вхідний номер, дата прийому, прізвище, ініціали та підпис)

Додаток 6

Акт про підключення
до Системи дистанційного обслуговування "Інтернет-банкінг"

м. Київ _____ 201__ року

Публічне акціонерне товариство "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі – Банк) в особі_____
_____,
який діє на підставі_____,
та_____(далі – Клієнт)
в особі _____.
який діє на підставі _____, підписали цей акт про таке:

1. Банк підключив Клієнта до Системи дистанційного обслуговування "Інтернет-банкінг" та надав доступ для дистанційного обслуговування Рахунку

№ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐,

2. Банк створив та налаштував права доступу таким Користувачам:

- _____ створювати ЕД, підписувати ЕД, перегляд залишків коштів,
(П.І.Б. Користувача)
- _____ створювати ЕД, підписувати ЕД, перегляд залишків коштів,
(П.І.Б. Користувача)
- _____ створювати ЕД, підписувати ЕД, перегляд залишків коштів
(П.І.Б. Користувача)

3. Банк зареєстрував в Системі дистанційного обслуговування "Інтернет-банкінг" відкриті ключі таких Користувачів:

№	*Заповнюється клієнтом:*	*Заповнюється працівником підрозділу інформаційної безпеки Банку:*	
1.	Прізвище, ім'я, по батькові Користувача: _____	Серійний номер сертифіката _____	Прізвище, ініціали, підпис _____
2.	Прізвище, ім'я, по батькові Користувача: _____	Серійний номер сертифіката _____	Прізвище, ініціали, підпис _____
3.	Прізвище, ім'я, по батькові Користувача: _____	Серійний номер сертифіката _____	Прізвище, ініціали, підпис _____

ПАТ "Розрахунковий центр" Клієнт

_____ _____ _____ _____
(підпис) (прізвище, ініціали) (підпис) (прізвище, ініціали)

Продовження на звороті

Заповнюється працівниками Банку

Управління забезпечення розрахунків

_____

(вхідний номер, дата прийому, прізвище, ініціали та підпис)

Додаток 7

Вимоги
до програмно-технічного забезпечення Клієнтів, що підключаються до Системи дистанційного обслуговування "Інтернет-банкінг" ПАТ "Розрахунковий Центр"

1. Вимоги до технічного забезпечення Клієнтів, що підключаються до Системи дистанційного обслуговування "Інтернет-банкінг" ПАТ "Розрахунковий центр"

Підключення до Системи дистанційного обслуговування "Інтернет-банкінг" ПАТ "Розрахунковий центр" (далі – Система "Інтернет-банкінг") передбачає наступні вимоги до технічного забезпечення Клієнтів:

- наявність персонального комп'ютера, що має порт USB 2.0;
- наявність швидкісного Internet-каналу(не менше ніж 256 кб/с). Безпосереднє (без використання проксі сервера) підключення до мережі Інтернет;
- забезпечити на стороні Користувача, проходження пакетів по ftp протоколу на адресу ibank.settlement.com.ua:10022, по http протоколу на адресу ibank.settlement.com.ua:10080 (при цьому – ftp протокол, порти 10022 та 10080 не повинні бути закриті).

2. Вимоги до системного програмного забезпечення Клієнтів, що підключаються до Системи "Інтернет-банкінг"

Підключення до Системи "Інтернет-банкінг"передбачає наступні вимоги до системного програмного забезпечення Клієнта:

- наявність ліцензійної версії однієї з операційних систем родини Windows, не нижче Windows XP SP3.
- наявність ліцензійної версії Internet Explorer не нижче 8, або наявність одного із наступних Інтернет браузерів: Chrome, Opera, *Mozilla Firefox* версії не нижче 3.

Рекомендації з інформаційної безпеки для клієнтів ПАТ "Розрахунковий центр", які мають доступ до системи "Інтернет-банкінг"

(розроблено за рекомендаціями Національного Банку України)

1. Для "входу" в систему "Інтернет-банкінг" ПАТ “Розрахунковий центр”, надалі Банку, використовуйте виключно програмне забезпечення **клієнтської частини системи "Інтернет-банкінг"** (Corp2) інсталяція якого знаходиться на сайті Банку (www.settlement.com.ua). Ніколи не інсталюйте програмне забезпечення з інших електронних ресурсів.

2. Уникайте використання системи "Інтернет-банкінг" з комп'ютерів в публічних місцях (Інтернет-кафе, бібліотеках, магазинах, торгівельних та розважальних центрах), а також з інших комп'ютерів, налаштування яких знаходиться поза Вашим контролем.

3. При користуванні бездротовою мережею інтернету Wi-Fi вдома, впевніться, що Ваша мережа захищена паролем. В публічних місцях вибирайте, по можливості, захищені паролем бездротові мережі.

4. Не користуйтеся функцією автоматичного запам'ятовування пароля в Вашому Інтернет-браузері.

5. Використовуйте як носії ключової інформації – електронні ключі "SecureToken-337" (далі – токен), які мають позитивний експертний висновок ДСТЗІ та призначені для надійного захисту та зберігання ключів електронного підпису.

6. Не використовуйте тривіальні й прості паролі. Використовуйте паролі, що складаються з літер, цифр і символів. Довжина пароля повинна бути 8 символів.

7. Клієнт несе персональну відповідальність за зберігання носія ключових даних. Рекомендовано зберігати токен у сейфі.

8. Клієнт повинен не допускати використання токену іншими особами, що не мають відповідних повноважень.

9. Клієнт повинен зберігати у таємниці значення ПІН-коду доступу до токену та значення коду розблокування токену.

10. Забороняється зберігати носії ключових даних та ПІН-коди до них в одному місці.

11. Клієнт повинен використовувати токен виключно за призначенням.

12. Не записуйте автентифікаційні дані: (пароль тощо) на папері, моніторі, у незашифрованому вигляді на комп’ютері, Нагадуємо, що КАТЕГОРИЧНО ЗАБОРОНЯЄТЬСЯ повідомляти пароль та будь-яку іншу ідентифікаційну інформацію повністю чи частково третім особам.

13. У випадку підозри, що пароль став відомий стороннім особам, негайно змініть його і зверніться до Банку для отримання додаткових консультацій.

14. Рекомендовано змінювати пароль не рідше одного разу в 3 місяці.

15. У разі, якщо Ви загубили токен з ключем (ключами) цифрового підпису, з якого відбувається підтвердження операцій в системі "Інтернет-банкінг", необхідно в терміновому порядку зв'язатися з Банком для блокування цього користувача та його сертифікату.

16. На комп'ютері, який використовується для роботи з системою "Інтернет-банкінг" рекомендується використовувати виключно ліцензійну операційну систему. Використання неліцензійних копій операційних систем (як і будь-яких неліцензійних копій інших програмних продуктів) вкрай небажано з наступних причин:

a) У випадку, якщо вони отримані не з довіреного джерела, наприклад, придбані на комп'ютерному ринку, отримані з файлообмінної мережі і т.д., вони можуть бути вже "заражені" вірусними програмами, або мати "несанкціоновані ходи", що використовуються зловмисниками; Програми-«активатори»[1], як правило, використовуються програми для обходу систем автентифікації, здебільшого використовують вірусні механізми і порушують механізми самозахисту систем, що може призвести до зараження операційної системи вірусними програмами або до установки в ній "троянської" компоненти[2].
b) Окремі категорії "троянських" вірусів здатні завдавати збитків віддаленим комп'ютерам та мережам, не порушуючи працездатності зараженого комп'ютера.
c) Замаскована програма може бути використана зловмисниками для отримання несанкціонованого доступу до комп'ютера.

17. На комп'ютері повинно бути встановлено і включено антивірусне програмне забезпечення, що постійно оновлюється в автоматичному режимі. Рекомендується використання наступних програмних продуктів: Kaspersky Internet Security 2012, BitDefender Internet Security 2011-2012, Panda Internet Security 2012, ESET NOD32, Symantec: Norton Internet Security 2012, AVG Anti-Virus тощо. Використання безкоштовних, умовно-платних програм або програм з обмеженою функціональністю категорично не допускається. По можливості, антивірусне програмне забезпечення повинно бути налагоджено способом, що забезпечує належний рівень реакції на виникаючі загрози без участі клієнта.

18. Захист від Фішінгу[3]. Фішинг-атака зловмисників досягається шляхом проведення масових розсилок електронних листів або повідомлень усередині соціальних мереж від імені популярних компаній в т.ч. і від імені банків. У листі часто міститься пряме посилання на сайт, який дуже схожий або навіть повністю співпадає з сайтом банку. Адреса відправника (наприклад, info@settlement.com.ua), від імені якого приходять такі фішінгові листи може повністю співпадати зі справжнім доменом, або бути дуже схожим на нього. Після того, як клієнт потрапляє на підроблену сторінку, шахраї намагаються різними психологічними прийомами спонукати клієнта ввести на підробленій сторінці свій пароль та будь-яку іншу ідентифікаційну інформацію, які він використовує для доступу до справжнього сайту, що дозволяє шахраям отримати доступ до облікових записів і банківських рахунків клієнта. Не відповідайте на листи з проханням вислати будь-які персональні данні пароль та будь-яку іншу ідентифікаційну інформацію. Подібні листи створюють зловмисники, **Банк НІКОЛИ не запитує у клієнтів конфіденційну інформацію по електронній пошті, не здійснює розсилку електронних листів з проханням прислати пароль, або будь-яку іншу конфіденційну інформацію, не розсилає програмне забезпечення для установки на Ваш комп'ютер.**

19. При роботі з електронною поштою та сервісами обміну миттєвими повідомленнями (Skype, ICQ та інші) звертайте особливу увагу на відправника повідомлення. Якщо відправник Вам невідомий та / або здається підозрілим, відкривати вкладені файли або переходити за посиланнями в мережі Інтернет є вкрай небезпечно.

20. Все інше програмне забезпечення, яке встановлене на комп'ютері, має бути ліцензійним або отримано з довіреного джерела. Якщо це передбачено виробником програмного продукту, то повинна бути включена можливість автоматичної установки оновлень для даного програмного забезпечення. Неприпустимо використання програм-генераторів інсталяційних ключів або програм зняття захисту від несанкціонованого доступу,

[1] **Програма-активатор** (від англ. executable file) змушує комп'ютер до виконання зазначеної задачі у відповідності з закодованою в програмі інструкцією.
[2] **Троянська компонента, Троянський вірус, Троянська програма** - комп'ютерна програма, яка добре вміє маскуватися під програмні продукти, а насправді виконує різні зловмисні дії: збирає та пересилає, змінює або псує інформацію, використовує ресурси комп'ютера на власний розсуд. Ці віруси самостійно не розмножуються. Вони видають себе за корисні програми, провокуючи користувача самостійно їх встановити.
[3] **Фішинг** (від англ. fishing-рибний лов, вивудження) - вид Інтернет-шахрайства, з метою отримання доступу до конфіденційної інформації користувачів (наприклад, логінів і паролів, номерів рахунків, карток міжнародних платіжних систем та інш.)

та інших сумнівних програм з ненадійних джерел на комп’ютері, що використовується для доступу до системи "Інтернет-банкінг".

21. Не рекомендується встановлення програм дистанційного керування Вашим комп’тером через мережу або будь-яких компонентів подібних програм.

Звертаємо увагу!

Наведені в даному документі рекомендації припускають, що їх реалізація буде доручена особам, які мають досвід роботи з комп’ютером. Кроки з забезпечення інформаційної безпеки здатні дати реальний ефект лише при дотриманні всіх рекомендацій та вимог. Більшість наведених в цьому додатку рекомендацій лежить в площині загальнопоширених знань. Тим не менш, якщо будь-яка з наведених рекомендацій Вам є незрозуміла з точки зору її технічного виконання, повідомляємо, що Банк не надає технічної підтримки для продуктів інших виробників та не консультує з основ користування комп’ютером, але й не обмежує клієнтів у звернені до інших осіб, що мають більш глибокі знання щодо впровадження вищенаведених рекомендацій. При цьому клієнт повинен оцінювати, усвідомлювати та приймати всі ризики, що мають місце при залученні до робіт з персональним комп’ютером третіх осіб та повинен самостійно переконатися в відсутності зловмисних намірів з боку третьої особи при роботі з комп’ютером та програмним забезпеченням.

Додаток 9

Акт
прийому-передачі носіїв ключової інформації
до Договору про обслуговування в системі інтернет-банкінгу
№ _____ від _____

м. Київ _____ 20__ р.

Публічне акціонерне товариство "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі - ПАТ "Розрахунковий центр") в особі _____ _____, який діє на підставі _____, з однієї сторони,

та _____ (далі - Клієнт) в особі _____, який діє на підставі _____, з другої сторони, підписали цей акт про наступне:

1. ПАТ "Розрахунковий центр" передав, а Клієнт прийняв:

1.1. носій ключової інформації "Secure Token 337" №_____

1.2. носій ключової інформації "Secure Token 337" №_____

2. Вказаний (вказані) в п.1 цього акту носій (носії) ключової інформації, переданий (передані) в робочому стані і без пошкоджень.

ПАТ "Розрахунковий центр"		Клієнт	
_____	_____	_____	_____
(підпис)	(прізвище, ініціали)	(підпис)	(прізвище, ініціали)

Додаток 10

Акт
прийому-передачі носіїв ключової інформації
до додаткового договору до договору про обслуговування в системі інтернет-банкінгу
№ _____ від _____
до Договору про обслуговування в системі інтернет-банкінгу
№ _____ від _____

м. Київ _____ 20__ р.

Публічне акціонерне товариство "Розрахунковий центр з обслуговування договорів на фінансових ринках" (далі - ПАТ "Розрахунковий центр") в особі _____
_____,
який діє на підставі _____,
з однієї сторони,
та _____ (далі - Клієнт) в особі _____,
який діє на підставі _____, з другої сторони, підписали цей акт про наступне:

1. Клієнт передав, а ПАТ "Розрахунковий центр" прийняв:

1.1. носій ключової інформації "Secure Token 337" №_____

1.2. носій ключової інформації "Secure Token 337" №_____

2. Вказаний (вказані) в п.1 цього акту носій (носії) ключової інформації переданий (передані) в робочому стані і без пошкоджень.

3. ПАТ "Розрахунковий центр" зобов'язується повернути Клієнту заставну вартість, вказаного (вказаних) в п.1 цього акту носія (носіїв) ключової інформації, протягом 5 робочих днів з дати підписання цього акту на поточний (кореспондентський) рахунок Клієнта:

рахунок № _____
в _____ (найменування банку)
код банку _____

ПАТ "Розрахунковий центр"		Клієнт	
_____	_____	_____	_____
(підпис)	(прізвище, ініціали)	(підпис)	(прізвище, ініціали)