Затверджено
рішенням Правління ПАТ «АКБ «КОНКОРД»
Протокол №28 від 30.03.2016 р. ***з урахуванням змін затверджених рішенням Правління ПАТ «АКБ «КОНКОРД» Протоколом № 96 від 18.07.2018 р.***

ПРАВИЛА ВИКОРИСТАННЯ, ЗБЕРІГАННЯ НОСІЇВ КЛЮЧОВОЇ ІНФОРМАЦІЇ ПРИ КОРИСТУВАННІ СИСТЕМОЮ «ІНТЕРНЕТ-БАНК «icON business»

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Ці Правила визначають порядок використання, зберігання носіїв ключової інформації при користуванні Системою «ІНТЕРНЕТ-БАНК «icON business».

1.2. Ці правила є невід'ємною частиною Договору про дистанційне обслуговування за допомогою системи «ІНТЕРНЕТ-БАНК «icON business», який підписано між АКЦІОНЕРНИМ ТОВАРИСТВОМ «АКЦІОНЕРНИЙ КОМЕРЦІЙНИЙ БАНК «КОНКОРД» (надалі - «Банк») та відповідним Клієнтом (надалі – «Договір»).

У разі, якщо Положення цих Правил суперечать положенням Договору, застосовуються положення Договору.

1.3. Офіційним місцем оприлюднення цих правил є відповідна сторінка офіційного Інтернет-сайту АТ «АКБ «КОНКОРД» www.concord.com. У разі зміни Правил, Банк повідомляє про це Клієнтів шляхом розміщення на сайті нової версії Правил не пізніше ніж за 14 календарних днів до дня набрання чинності нової версії Правил.

2. ФУНКЦІОНУВАННЯ СИСТЕМИ «ІНТЕРНЕТ-БАНК «icON business»

Важливою властивістю Інтернет - банкінгу є забезпечення безпеки. У Системі «ІНТЕРНЕТ-БАНК «icON business» використовуються надійні механізми захисту, що повністю виключають можливість несанкціонованого доступу до рахунків і перехоплення інформації при передачі її через Інтернет.

Для забезпечення інформаційної безпеки Системи «ІНТЕРНЕТ-БАНК «icON business» служать наступні механізми:

• Електронний цифровий підпис (ЕЦП) служить для забезпечення цілісності та автентичності документів в Системі. Електронний документ з ЕЦП, надісланий Клієнтом і отриманий Банком, є підставою для проведення Банком фінансових операцій, і є аналогом особистого підпису. Для використання механізму ЕЦП клієнт генерує пару ключів (відкритий і секретний). Секретний ключ використовується для формування ЕЦП клієнта під фінансовим документом. Носієм секретного ключа може бути файл на жорсткому диску або на зовнішньому носії (USB-flash). Відкриті ключі ЕЦП зберігаються в БД «icON business» у вигляді Сертифікатів відкритих ключів. З їх допомогою перевіряється підпис клієнта під фінансовим документом.

• Передбачена можливість застосування одноразових паролів для аутентифікації клієнта. Як джерело одноразового пароля служить особистий мобільний телефон Клієнта, на який пароль доставляється в SMS-повідомленні.

• Доступ в Систему «ІНТЕРНЕТ-БАНК «icON business» здійснюється за допомогою введення логіна і пароля клієнтом Системи. Пароль є секретним набором символів, відомим тільки Клієнту.

• Всі комунікації між Банком і браузером клієнта здійснюються виключно за протоколом https (SSL), що забезпечує шифрування переданих даних, а отже,і їх захист від перегляду і модифікації третіми особами.

3. ЗАБЕЗПЕЧЕННЯ 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 установку з'єднання, підписаний цифровим підписом користувача, після чого бібліотеки криптографічного захисту формують необхідні секретні параметри й ключі й підтверджують установку з'єднання. Таким чином, кожне з'єднання має унікальні параметри й 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 криптографічними методами і виконуються на прикладному рівні, у процесі підготовки даних для передачі в Банк.

Система «ІНТЕРНЕТ-БАНК «icON business» ідентифікує користувача по логіну, паролю на вхід в Систему, секретному ключу й паролю до 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,

Клієнт зобов’язаний не рідше одного разу на 365 календарних днів для кожного окремого Користувача здійснювати перегенерацію електронного ключа (генерувати новий електронний ключ) та надавати до Банку Сертифікат відкритого ключа ЕЦП всіх Користувачів Системи (365 календарних днів обчислюється для кожного окремого Користувача в залежності від того коли останній раз Клієнт по даному Користувачу надавав до Банку Сертифікат відкритого ключа ЕЦП Клієнта та відбувалася авторизації цих ключів адміністратором Системи (Банком)). Робота з перегенерованими ключами користувачів можлива тільки після авторизації цих ключів Адміністратором Системи (Банком).

4. ПРАВИЛА БЕЗПЕКИ ПРИ КОРИСТУВАННІ СИСТЕМОЮ «ІНТЕРНЕТ-БАНК «icON business»

Кожен користувач Системи «ІНТЕРНЕТ-БАНК «icON business» - є гарантом і складовою частиною Системи безпеки і повинен дотримуватися таких правил:

- Не розголошуйте Ваш логін і паролі третім особам;
- Зберігайте Ваш особистий сертифікат і секретний ключ на зовнішньому носії інформації (дискета, накопичувачі на флеш-пам'яті та ін);
- Не зберігайте зовнішній носій інформації з Вашим особистим сертифікатом і секретним ключем разом з логіном і паролями. У разі втрати - цією інформацією можуть скористатися сторонні особи у своїх цілях.
- Не довіряйте стороннім користуватися Вашим особистим сертифікатом і секретним ключем для підписання документів.
- Не надавайте доступ стороннім до особистих мобільних телефонів, на які доставляється одноразовий пароль в SMS-повідомленні.
- Після закінчення виконання операції не забувайте Ваш зовнішній носій на комп'ютері іншого користувача.
- Використовуйте кнопку «Вихід» по завершенні сеансу роботи з Системою.
- Відволікання Вас від комп'ютера при роботі з Системою, без завершення сеансу роботи з програмою, може спровокувати третю особу скористатися ситуацією.
- Не забувайте дістати зовнішній носій інформації як тільки завершите роботу з Системою «ІНТЕРНЕТ-БАНК «icON business » - цією інформацією можуть скористатися

сторонні особи, вона може бути безповоротно втрачена або пошкоджена в процесі роботи інших програм.

Банк не рекомендує користувачеві працювати з Системою «ІНТЕРНЕТ-БАНК «icON business»:

- 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 використовуваного програмного забезпечення (наявність вірусів, спеціальних програм, що надсилають паролі користувача третім особам і т.п.).

Застосовуйте інші рекомендації Банку щодо забезпечення безпеки та цілісності інформації при роботі з Системою «ІНТЕРНЕТ-БАНК «icON business».

У разі виявлення факту та/або підозри про потрапляння секретної інформації, що стосується використання Системи «ІНТЕРНЕТ-БАНК «icON business», третім особам негайно здійснити такі заходи:

– самостійно заблокувати Систему «ІНТЕРНЕТ-БАНК «icON business» шляхом введення при вході до Системи завідомо неправильного пароля у такій кількості разів, після якого Система блокується;

– повідомити про це Банк (контактні дані Банку зазначені на офіційному сайті Банку - www.concord.ua у відповідному розділі).

5. ВІДПОВІДАЛЬНІСТЬ

Банк не несе відповідальності за наслідки, до яких може призвести порушення Клієнтом цих Правил та положень Договору.