Рекомендації клієнтам щодо забезпечення інформаційної безпеки при користуванні системою Клієнт-банк

1. Терміни та визначення

Система «Клієнт-Банк» – автоматизована інформаційна система дистанційного банківського обслуговування клієнтів «iFOBS», що реалізує послуги клієнт-банкінгу.

Клієнтська частина системи «Клієнт-Банк» – сукупність комп'ютерного обладнання клієнта (персональний комп'ютер, ноутбук, планшет тощо), а також спеціалізованого програмного забезпечення (далі – ПЗ), що надає можливість дистанційного обслуговування на стороні клієнта (ПЗ, надане Банком, а також стандартне ПЗ операційної системи комп'ютерного обладнання клієнта (наприклад, веб-браузер).

Веб-браузер – ПЗ, що надає можливість користувачу в мережі Інтернет переглядати текстову інформацію сторінок, малюнки, посилання на інші сайти тощо.

Електронно-цифровий підпис (ЕЦП) – вид електронного підпису, отриманого у результаті криптографічного перетворення електронного документу, який додається до цього документу або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати особу, яка підписала документ. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Відкритий ключ ЕЦП – це криптографічний ключ (дані, інформація), який отримано математичним обчисленням та який являється відкритою інформацією для перевірки ЕЦП користувача.

Секретний ключ ЕЦП – це криптографічний ключ, що зв'язаний із відкритим ключем спеціальним математичним співвідношенням, являється таємною інформацією, за допомого якої формується ЕЦП користувача.

Сертифікат (сертифікат ключа, сертифікат відкритого ключа) – документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа особі, яка володіє відповідним особистим ключем. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документів на папері та використовуватися для ідентифікації особи власника відповідного особистого ключа.

Персональний мережевий екран (фаєрвол, брандмауер) – ПЗ, встановлене на комп'ютері користувача і призначена для захисту від несанкціонованого доступу до цього комп'ютера.

Веб-сервер – сервер (спеціалізоване ПЗ), що приймає специфічні запити від веб-браузерів клієнтів, видає їм відповіді, зазвичай разом із інтернет-сторінкою, зображенням, файлом, медіа-потоком або іншими даними.

Антишпигунське ПЗ – програмне забезпечення, що виявляє та знешкоджує шкідливі програми, які збирають інформацію про дії користувача та передають її зловмиснику.

Сигнатури вірусу - характерні ознаки комп'ютерного вірусу, що використовуються для його виявлення.

Сигнатури шпигунського ПЗ - характерні ознаки шпигунського програмного забезпечення, що використовуються для його виявлення.

Антивірусні бази даних – бази даних, у яких зберігаються сигнатури вірусів.

Бази сигнатур антишпигунського ПЗ – бази даних, у яких зберігаються сигнатури шпигунського програмного забезпечення.

Обліковий запис – сукупність інформації про користувача, засобів та прав користувача відносно багатокористувацької системи (наприклад, administrator, user, ivanov тощо).

2. Базові рекомендації клієнтам щодо забезпечення захисту клієнтської частини системи «Клієнт-Банк»

- Під час роботи у системі «Клієнт-Банк» (далі Система) не залишайте комп'ютер без нагляду.
- Для запобігання несанкціонованого доступу до конфіденційної інформації не повідомляйте свої авторизаційні дані у Системі (логін, пароль, секретний ключ ЕЦП, пароль на секретний ключ ЕЦП третім особам (включаючи членів родини, друзів тощо).
- Рекомендується зберігати особистий сертифікат і секретний ключ на зовнішньому носії інформації (диск, накопичувачі із флеш-пам'яттю (USB-токени, флешки) та ін.), а не на комп'ютері. Зберігання даної інформації на зовнішніх носіях забезпечує додатковий захист конфіденційної інформації клієнта в Системі та забезпечує цілість сертифікатів і секретних ключів у разі виникнення раптових проблем, збоїв у роботі комп'ютера клієнта.
- Для максимального захисту конфіденційної інформації (особистий сертифікат, секретний ключ ЕЦП) рекомендується використовувати зовнішній носій інформації із захищеною пам'яттю (що унеможливлює несанкціоновану модифікацію даних, збережених на носії), наприклад, спеціалізований USB-токен.
- При використанні паролів не рекомендується зберігати їх на папері, на комп'ютері, на флеш-носіях, дискетах тощо. Пароль рекомендується запам'ятати!
- При використанні зовнішнього носія інформації з особистим сертифікатом та секретним ключем на ньому, не зберігайте даний носій інформації разом із логіном та паролями Системи (якщо клієнтом було прийнято рішення не запам'ятовувати, а зберігати паролі).
- Рекомендується завжди вилучати із комп'ютера зовнішній носій інформації по завершенню роботи в Системі.
- Підключення до Системи необхідно здійснювати тільки з надійних комп'ютерів, на яких встановлено антивірусне ПЗ та програмний персональний мережний екран.
- При вході до Системи необхідно впевнитись, що в адресному полі веб-браузера знаходиться адреса саме Системи Банку (наприклад, https://cb.ap-bank.com/ifobsClient/LoginShow.action).

- При підключенні до Системи необхідно перевірити чи ввімкнено шифрування між клієнтським комп'ютером та веб-сервером Банка. Про ввімкнене шифрування свідчить наявність піктограми  «Замок» у вікні браузера (справа від адресного поля браузера).
- Підтвердженням того, що між веб-браузером клієнта та веб-сервером Банку встановлено безпечне з'єднання, є наявність цифрового (електронного) сертифікату Банку. Рекомендується перевірити дійсність сертифікату та термін його дії.
- Після відкриття сесії роботи в Системі у веб-браузері перевіряйте дату останнього свого входу до системи та відстежуйте історію своїх операцій в Системі.
- Після завершення роботи у Системі необхідно закрити сесію, натиснувши піктограму «Вихід», та закрити вікно веб-браузера.
- Не рекомендується переглядати інші сайти в тому ж веб-браузері, в якому запущена Система.
- Рекомендується звертати увагу на можливі повідомлення веб-браузера про будь-яку небезпеку. У разі виникнення будь-якої підозри рекомендується завершити роботу із Системою та закрити сесію.
- Банк надсилає клієнту первинні секретні ключі та сертифікати тільки авторизованою електронною поштою cbsert@ap-bank.com. Не використовуйте будь-яку інформацію (ключі та сертифікати тощо) у Системі, вислану з інших електронних поштових адрес, навіть якщо вони схожі за назвою із авторизованою банківською електронною адресою (без попереднього офіційного повідомлення та погодження зі сторони Банку).
- Не відповідайте на запити (найчастіше запити розсилаються через SMS, електронною поштою тощо), які містять вимогу надати або перевірити логін, пароль, секретний ключ ЕЦП тощо.
- Банк, без попереднього офіційного повідомлення та погодження із клієнтом, за жодних обставин не здійснює розсилку із:
  - запитами на отримання персональних паролів клієнта;
  - додатковим ПЗ для Системи;
  - посиланнями на інші сайти із необхідністю завантажити додаткове ПЗ Системи тощо.
- Рекомендується видаляти підозрілі електронні листи без їх відкриття, особливо листи від невідомих адресатів із прикріпленими файлами, що мають розширення *.exe, *com, *zip, *rar, *bat, *jpeg, *.pif, *.vbs та інші файли, так як існує значна ймовірність зараження комп'ютера вірусами та іншим зловмисним ПЗ.

3. Рекомендації щодо забезпечення захисту комп'ютера клієнта

- Рекомендується, щоб комп'ютер (персональний комп'ютер, ноутбук, планшет тощо) клієнта, який використовується для роботи в Системі, мав:
  - ліцензійну операційну систему;
  - встановлену останню доступну версію веб-браузера;
  - програмне забезпечення захисту, що складається із ліцензійної антивірусної системи, антишпигунського ПЗ («antispyware») та програмного персонального мережного екрану.

- На комп'ютері із встановленою операційною системою Windows рекомендується активувати функцію автоматичного оновлення операційної системи.
- Рекомендується постійно оновлювати антивірусні бази даних та бази сигнатур антишпигунського ПЗ.
- Рекомендується регулярно (не рідше, ніж раз на тиждень) здійснювати повне сканування комп'ютера за допомогою антивірусного, антишпигунського ПЗ для виявлення вірусів та зловмисного ПЗ (вірусів, шпигунських програм тощо).
- У разі виявлення на комп'ютері будь-якого зловмисного ПЗ рекомендується не заходити з цього комп'ютера у Систему до повного видалення даного зловмисного ПЗ із комп'ютера. Наступний вхід до Системи обов'язково виконується із гарантовано незараженого комп'ютера, при цьому необхідно якнайшвидше змінити пароль доступу до Системи, а також пароль секретного ключа ЕЦП.
- Не рекомендується встановлювати на комп'ютер будь-яке неліцензійне ПЗ.
- Не рекомендується встановлювати на комп'ютер ПЗ із ненадійних джерел (наприклад, програмне забезпечення із невідомих повідомлень електронної пошти, файлових ресурсів (наприклад, EX.UA) із невідомих посилань на сайтах в Інтернет, що відвідуються клієнтом тощо).

4. Рекомендації щодо використання безпечних паролів

- При введенні паролю на доступ до Системи або паролю до секретного ключа ЕЦП переконайтесь, що за Вами ніхто не спостерігає.
- Рекомендується обмежити доступ сторонніх осіб до мобільного телефону клієнта, на який надходить SMS із первинним паролем доступу до Системи.
- Перед тим, як змінити пароль, перевірте сертифікат безпеки банківського веб- сервера.
- Не використовуйте функцію збереження паролів, яку може запропонувати веб- браузер.
- Для забезпечення найвищого рівня інформаційної безпеки при використанні паролів не рекомендується зберігати паролі, взагалі, в будь-якому місці (на папері, на комп'ютері, на флеш-носіях, дискетах тощо). Пароль рекомендується запам'ятати.
- За умови прийнятого рішення зі сторони клієнта щодо збереження паролів, рекомендується зберігати паролі у недоступному для інших місці.
- За умови прийнятого рішення зі сторони клієнта щодо збереження паролів, рекомендується зберігайте пароль на доступ до Системи та пароль до секретного ключа ЕЦП окремо.
- Паролі Системи не повинні містити словникові слова або ім'я, пов'язані з клієнтом (ім'я, прізвище, ім'я дружини, дітей, домашніх улюбленців тощо), не містити очевидних послідовностей символів (наприклад, abcdEF, Qwertyu тощо).
- Рекомендовані вимоги до створення та використання паролів:
  - мінімум 8 символів, мінімум 1 мала та 1 велика літери, мінімум 1 цифра та мінімум 1 спеціальний знак (наприклад, «*», «_» , «-», «!», «+» тощо);
  - 4-ри останні паролі не повинні співпадати;

- термін дії паролю – 90 днів.

5. Ризики і відповідальність

Клієнт, який використовує Систему, погоджується з тим, що розуміє всі ризики (звільняє Банк від відповідальності), пов'язані із розголошенням конфіденційної інформації (з провини клієнта) в рамках використання Системи (логін, пароль, секретний ключ ЕЦП, пароль на секретний ключ тощо), номеру його мобільного телефону (на який надсилається первинний пароль на вхід до Системи), будь-якої інформації, що є банківською таємницею (про свої рахунки тощо), ризики при здійсненні доступу до Системи не з власного комп'ютера та несе повну відповідальність за такі випадки.

Клієнт погоджується з тим, що розуміє всі ризики та несе повну відповідальність (звільняє Банк від відповідальності), пов'язану із здійсненням доступу до Системи через комп'ютер:

- на який не встановлено актуальне ПЗ антивірусного та мережного захисту (антивірусна система, антишпигунське програмне забезпечення та програмний персональний мережний екран);
- на якому встановлено ПЗ антивірусного та мережного захисту, що не оновлюється або оновлюється нерегулярно;
- на якому встановлено неліцензійне ПЗ (включаючи операційну систему);
- на якому відсутні оновлення безпеки операційної системи;
- на якому відсутнє розмежування доступу (доступ до операційної системи комп'ютера відбувається без паролю, використовується єдиний обліковий запис (наприклад, administrator, office, user, dom тощо) для будь-яких користувачів комп'ютера);
- із якого відбувається доступ в Інтернет до сайтів неналежного змісту (порнографічного характеру, ігрові та розважальні сайти, хакерські форуми тощо), на яких досить вірогідне зараження вірусним, шпигунським та іншим зловмисним ПЗ.

6. Порядок дій в екстремальних та непередбачених ситуаціях

Клієнт банку, який користується послугами системи «Клієнт-Банк» зобов'язаний припинити використання таємного ключа та негайно інформувати адміністратора системи захисту інформації СБК (працівник Управління безпеки і охорони, який супроводжує СБК) за допомогою телефона (044) 392-93-79 та електронної пошти cbsos@ap-bank.com в таких випадках:

- несанкціоноване зняття коштів з рахунків;
- виконання (спроби виконання) фіктивного платіжного документа;
- компрометація таємного ключа (ТК) системи «Клієнт-Банк».