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

Терміни та визначення:

Система «Клієнт-Банк» –система дистанційного банківського «Клієнт-банк»».
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, що надано Банком, а також стандартне ПЗ Клієнта (наприклад, веб-браузер).
Веб-браузер – ПЗ, що надає можливість користувачу в мережі Інтернет переглядати текстову інформацію, малюнки, посилання на інші сайти, тощо на веб-сторінках.
Відкритий ключ ЕЦП – це криптографічний ключ (дані, інформація), який отримано математичним обчисленням та який являється відкритою інформацією для перевірки ЕЦП користувача.
ЕЦП - електронний цифровий підпис.
Закритий (секретний) ключ ЕЦП – це криптографічний ключ, що зв'язаний із відкритим ключем спеціальним математичним співвідношенням, та являється таємною інформацією, за допомого якої накладається 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.
Ключ ЕЦП - призначений для підписання (накладання ЕЦП) документів та повідомлень, які Клієнт надсилає засобами системи «Клієнт-банк» у Банк. Ключ складається з відкритої (публічної) та закритої частини. Відкрита частина відома Банку та зафіксована на паперовому носії (у вигляді геш-коду) в документі «Інформація про відкриті ключі користувача (запит)», закрита частина зберігається виключно на електронному носії у Клієнта. Під час накладання ЕЦП Клієнтом – використовується закрита частина Ключа ЕЦП. Відкрита частина використовується для перевірки достовірності підпису на документах та повідомленнях, під час приймання їх Банком. Даний механізм забезпечує ідентифікацію особи, що наклала особистий підпис та захист документів і повідомлень від підробки, під час передачі їх каналами зв'язку від Клієнта до Банку засобами системи «Клієнт – банк».
Токен - захищений носій ключової інформації, сертифікований відповідно до державних стандартів захисту інформації. Призначений для зберігання Ключів ЕЦП Користувачів.
OTP (one time password) токен – пристрій, призначений для генерації одноразових паролів з метою додаткової авторизації Користувача в системі «Клієнт-банк».
Персональний мережевий екран (файєрвол, брандмауер) – система, встановлена на комп'ютері користувача, та призначена для захисту від несанкціонованого доступу до його 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 – спеціальна одиниця інформації про Клієнта Банку у системі «Клієнт – банк».
.

Базові рекомендації Клієнту щодо забезпечення захисту клієнтської частини системи «Клієнт-Банк»

- Під час роботи у системі «Клієнт-Банк» (далі Система) не залишайте комп'ютер без нагляду.

1. 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 і т.д.).

- Рекомендується зберігати особистий сертифікат і секретний ключ ЕЦП 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 ЕЦП 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, тощо.
- 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!
- При використанні зовнішнього носія інформації з особистим сертифікатом та секретним ключем ЕЦП 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 сертифікати тільки авторизованою електронною поштою cb@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 з боку Банку).
- Не відповідайте на запити (найчастіше запити розсилаються через SMS-повідомлення засобами мобільного зв'язку, 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 даних (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/чи іншим зловмисним ПЗ.

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, яка отримує оновлення;
  - Встановлену останню доступну версію веб-браузера;
  - Програмне забезпечення захисту, що складається із ліцензійної антивірусної системи, антишпигунського ПЗ («antispyware») та програмного персонального мережевого 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, FEX.NET) із невідомих посилань на сайтах в Інтернет, що відвідуються Клієнтом тощо).

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 збоку Клієнта щодо збереження паролів, рекомендується зберігати паролі у недоступному для інших місці.
- За умови прийнятого рішення збоку 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.

Ризики і відповідальність

Клієнт, що 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 ЕЦП 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.

ПОРЯДОК ДІЙ В ЕКСТРЕМАЛЬНИХ ТА НЕПЕРЕДБАЧЕНИХ СИТУАЦІЯХ

Клієнт Банку, який користується послугами системи «Клієнт-Банк», зобов'язаний припинити використання секретного ключа (ТК) та негайно інформувати адміністратора системи захисту інформації СКБ за допомогою телефона (044) 392-93-79 та електронної пошти cb@ap-bank.com в таких випадках:

- несанкціоноване зняття коштів з рахунків;
- виконання (спроби виконання) фіктивного платіжного документа;
- компрометація таємного ключа (ТК) системи «Клієнт-Банк»;
- втрата контролю над OTP токеном (за наявності).