ПРАВИЛА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ КЛІЄНТОМ СИСТЕМИ ІНТЕРНЕТ-БАНКІНГА (сторінка 1)

З метою недопущення шахрайства відносно Клієнтів при використанні Системи дистанційного банківського обслуговування (далі - Система), Клієнт повинен з відповідальністю ставитися до вимог інформаційної безпеки, які націлені на недопущення заволодіння конфіденційною інформацією Клієнта (логін, паролями, ключами ЕЦП і т.д.).

При використанні Системи, Клієнт повинен дотримуватися таких організаційних заходів і правил:

1. Ніколи і ні за яких обставин не розголошуйте персональні дані, які використовуються Вами для роботи в Системі (логін і пароль для входу в Систему, пароль на електронно-цифровий підпис, разовий пароль, який направляється в SMS - повідомленні і т.д.) стороннім особам, навіть отримавши лист або дзвінок від осіб, що представляються співробітниками Банку. Не використовуйте їх на будь-яких інших сайтах, окрім безпосередньо робочої сторінки Системи.

2. Не зберігайте ці дані на ПК, а також в будь-якому іншому місці, яке може бути доступним стороннім особам. Тримайте ключі ЕЦП тільки на носіях інформації (дискета, USB Flash Drive, CD тощо), забезпечуйте їх збереження і не записуйте на ці змінні носії з ключем ЕЦП іншу інформацію.

3. Змінні носії з ключами ЕЦП використовуйте тільки при здійсненні переказу коштів. Відразу після проведення операцій з використанням ЕЦП відключайте носій ЕЦП від ПК.

4. Про підозру або факти компрометації ЕЦП терміново повідомити Банк для блокування ключів ЕЦП, провести процедуру генерування та реєстрації нових ключів ЕЦП в Системі з наданням в Банк оригіналів сертифікатів ЕЦП, завірених підписом Клієнта.

5. При втраті або викрадені носія з ЕЦП терміново повідомити Банк для блокування ключів ЕЦП та звернутися до Банку з відповідною заявою.

6. Утримуйтеся від використання комп'ютера, на якому виконується робота в Системі для розваг і інших неконтрольованих дій в мережі Інтернет, а також обмежте до нього фізичний і мережевий доступ сторонніх осіб. Для запобігання зовнішніх вторгнень і виключення можливості зовнішнього підключення зловмисників до комп'ютера Клієнта, який використовується для роботи з Системою, бажаним є застосування на ньому брандмауера.

7. Обов'язковими умовами є використання на клієнтських ПК, з яких здійснюється робота в Системі, ліцензійного антивірусного програмного забезпечення, регулярного оновлення вірусних баз на ньому, не рідше ніж 1 раз на день і періодичного проведення перевірок ПК на наявність вірусів і шпигунських програм. Також обов'язковим є регулярне оновлення операційної системи (в першу чергу це стосується поновлення безпеки).

8. У разі виявлення будь-якого шкідливого програмного забезпечення (віруси, троянські програми і т.д.) на обладнанні, з якого здійснювався вхід в Систему, необхідно обов'язково здійснити вхід в Систему з гарантовано не зараженого ПК і замінити пароль доступу до Системи.

9. При створенні пароля рекомендується використовувати комбінації з букв, цифр і спеціальних символів довжиною не менше 7 знаків і міняти пароль доступу в Систему не рідше 1 разу на три місяці.

10. Перед початком роботи з Системою і введенням персональних даних на сторінці авторизації, переконайтеся, що Ви саме на сторінці банку: http://agrocombank.com.ua/.

11. Переконатися, що Ви на правильній сторінці, можна перевіривши також сертифікат, за допомогою якого здійснюється захищене з'єднання. Відмітка, визначальна захищене з'єднання, найчастіше виглядає як «замок». У вікні властивостей сертифіката, який відкриється, ви зможете переконатися, кому він був виданий. При використанні веб - браузерів, починаючи з версії Internet Explorer 7, Firefox 3, Opera 9.5 фон адресного рядка повинен відображатися зеленим і містити назву організації.