Рекомендації клієнтам щодо безпечного використання систем дистанційного обслуговування Банку (СДБО).

З метою забезпечення високого рівня безпеки інформації та унеможливлення доступу до конфіденційної інформації сторонніх осіб при роботі з системами дистанційного обслуговування рахунків (далі – СДБО), розроблено ряд рекомендацій наведених нижче:

- необхідно обмежити доступ сторонніх осіб до пристрою на якому виконується робота зі СДБО (персонального комп'ютера, ноутбука, смартфона, планшета, тощо). У разі втрати пристрою або у разі будь-якої підозри на компрометацію особистих ключів для роботі зі СДБО необхідно негайно сповіщати про це контакт-центр банку за номером телефону

0 800 300 392,(044) 392 00 00 24/7

- налаштовуйте окремо мережеве обладнання корпоративних і персональних комп'ютерів. Доступ до мережі Інтернет обмежуйте «білим списком» сайтів з усіх робочих місць, на яких здійснюється підготовка, підписання та відправлення платіжних документів. Радимо виконувати перевірку кому та ким виданий сертифікат надійності сайту на якому переглядаєте інформацію, а також стежити за строком його дії. Натиснувши на значок замка можна переглянути властивості сертифікату (Рис.1)

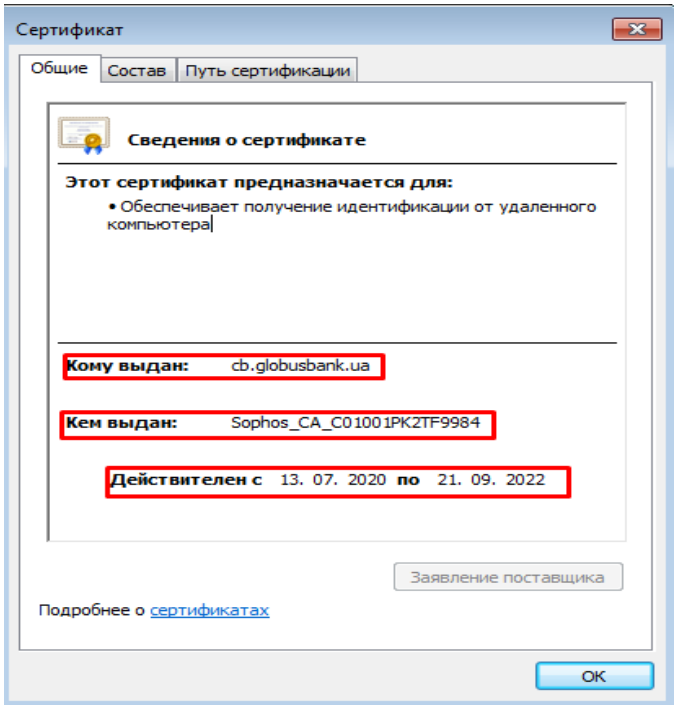

Рис.1

- користувачу не рекомендується встановлювати програмне забезпечення (додатки) завантажені з невідомих джерел/веб-сайтів і не відкривати файли, отримані з ненадійних джерел, надіслані електронною поштою від невідомих відправників. Використовувати ліцензійне програмне забезпечення для захисту від зловмисного коду, регулярно поновлювати антивірусні бази та регулярно здійснювати перевірку свого пристрою на наявність вірусів та шпигунських програм;

- Необхідно тримати у таємниці та не повідомляти стороннім особам свій логін, пароль, пароль з СМС-повідомлення, які використовуються для доступу до СДБО;

- завжди контролювати стан поточних рахунків;

- після закінчення роботи зі СДБО обов'язково здійснювати вихід із системи для недопущення використання системи сторонніми особами.

До уваги користувачів, АТ «КБ«ГЛОБУСБАНК» ніколи не здійснює дзвінки та розсилку електронних листів з проханням надати конфіденційну інформацію про логіни, паролі або інші конфіденційні дані.