Рекомендації клієнтам АТ «АБ «РАДАБАНК» щодо безпечного використання систем дистанційного обслуговування Банку

З метою забезпечення високого рівня безпеки інформації та унеможливлення доступу до конфіденційної інформації сторонніх осіб при роботі з системами дистанційного обслуговування рахунків (далі – СДОР), Банком для користувачів СДОР (клієнтів Банку) розроблено ряд рекомендацій наведених нижче. Перелік рекомендацій розділений на чотири категорії:

– загальні рекомендації, які стосуються всіх користувачів СДОР;
– рекомендації щодо безпечного використання СДОР «ВЕБ-банкінг для корпоративних клієнтів», які стосуються клієнтів Банку – юридичних осіб;
– рекомендації щодо безпечного використання СДОР «RB24» з використанням інтернет-браузерів, які стосуються клієнтів Банку – фізичних осіб;
– рекомендації щодо безпечного використання СДОР «RB24» з використанням мобільних пристроїв, які стосуються клієнтів Банку – фізичних осіб.

Дотримання даних рекомендацій є обов'язковою умовою використання СДОР для всіх користувачів.

1. Всім користувачам СДОР рекомендуємо дотримуватись наступних правил безпеки:

1.1. Необхідно обмежити доступ сторонніх осіб до пристрою на якому виконується робота зі СДОР (персонального комп'ютера, ноутбука, смартфона, планшета, тощо). У разі втрати пристрою необхідно негайно звернутися до контакт-центру Банку для блокування доступу. Реквізити контакт-центру Банку:

Тел. 0 800 500 999 – безкоштовно зі всіх телефонних номерів України
e-mail: ContactCenter@radabank.com.ua

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

1.3. 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.

1.4. Користувач має регулярно оновлювати програмне забезпечення, операційну систему, яка встановлена на його пристрої з офіційних джерел компаній-розробників.

1.5. 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.

1.6. У випадку виявлення несанкціонованого доступу до СДОР, користувач має негайно повідомити про це Банк зателефонувавши до контакт-центру Банку для блокування доступу до СДОР.

1.7. У разі будь-якої підозри на компрометацію особистих ключів для роботі зі СДОР необхідно негайно сповіщати про це Банк.

1.8. До уваги користувачів, Банк не здійснює дзвінки та розсилку електронних листів з проханням надати конфіденційну інформацію про логіни, паролі або інші конфіденційні дані.

1.9 Контролювати стан поточних рахунків.

1.10. Після закінчення роботи зі СДОР обов'язково здійснювати вихід із системи для недопущення використання системи сторонніми особами.

2. Рекомендації щодо безпечного використання СДОР «ВЕБ-банкінг для корпоративних клієнтів»:

2.1. При вході на офіційну сторінку Банку, користувач повинен уважно перевіряти доменне ім'я (Рис. 1) для впевненості, що це офіційна, а не фішингова сторінка зловмисників.

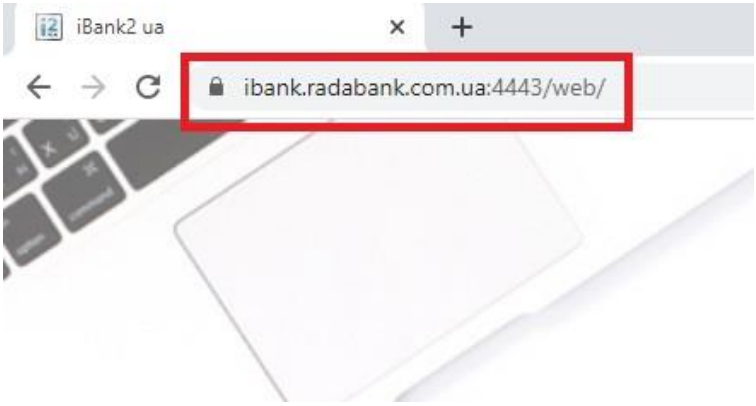

Рис. 1

2.2. Виконувати перевірку кому та ким виданий сертифікат і стежити за строком його дії. Натиснувши на значок замка можна переглянути властивості сертифікату (Рис.2).

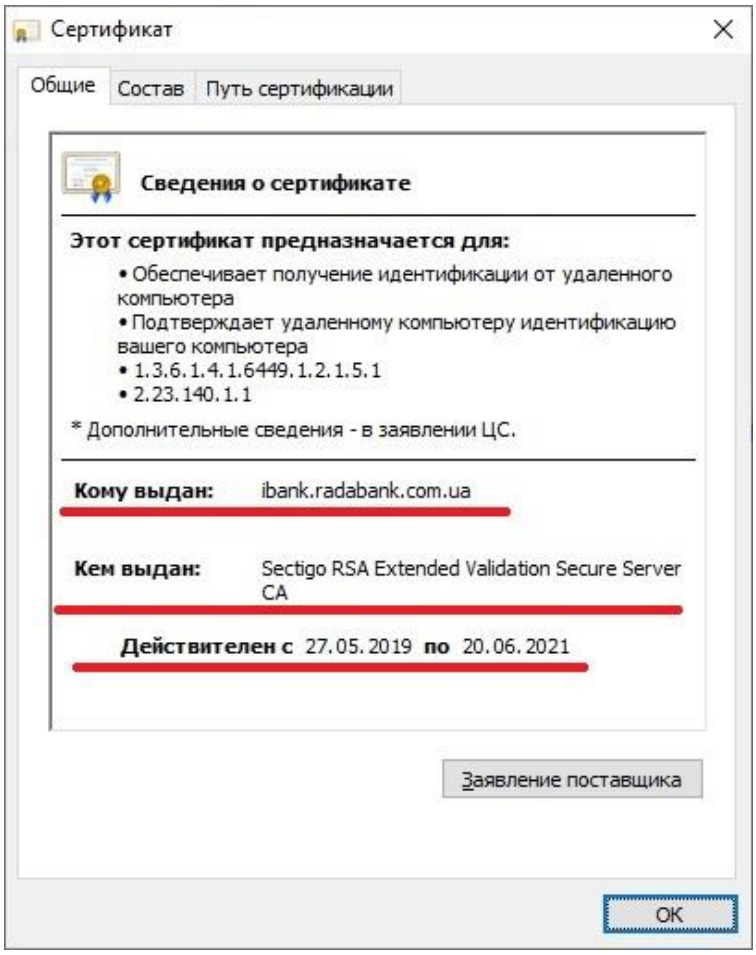

Рис.2

Зображення замкнутого замка (Рис.3) означає, що на сайті встановлений SSL-сертифікат і вся інформація передається по захищеному протоколу. SSL-сертифікат не дає шахраям перехопити або підмінити особисті дані користувачів.

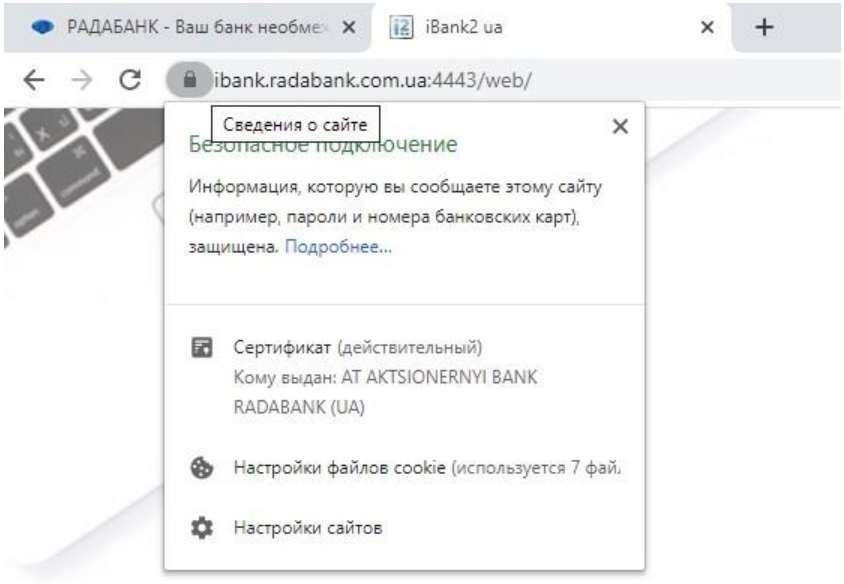

Рис.3

2.3. Використовувати програмний модуль та веб розширення «WebSigner», який завантажується з офіційного сайту Банку. Розширення "WebSigner" надає можливість накладення цифрового підпису з використанням файлових і апаратних носіїв ключової інформації.

Просимо також зауважити, що для забезпечення повноцінної роботи СДОР необхідно встановити дві версії модуля одночасно – для самого Інтернет-браузера (Рис.4) та для операційної системи (Рис.5).

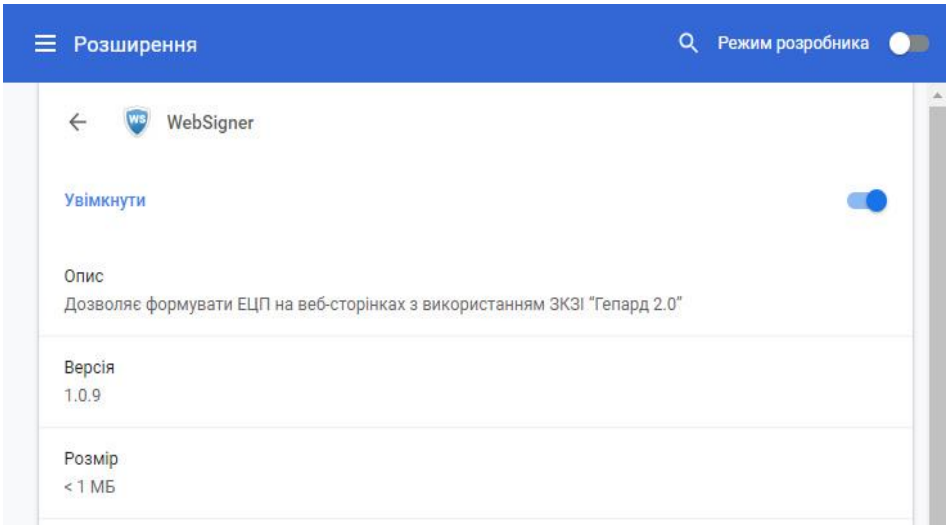

Рис.4

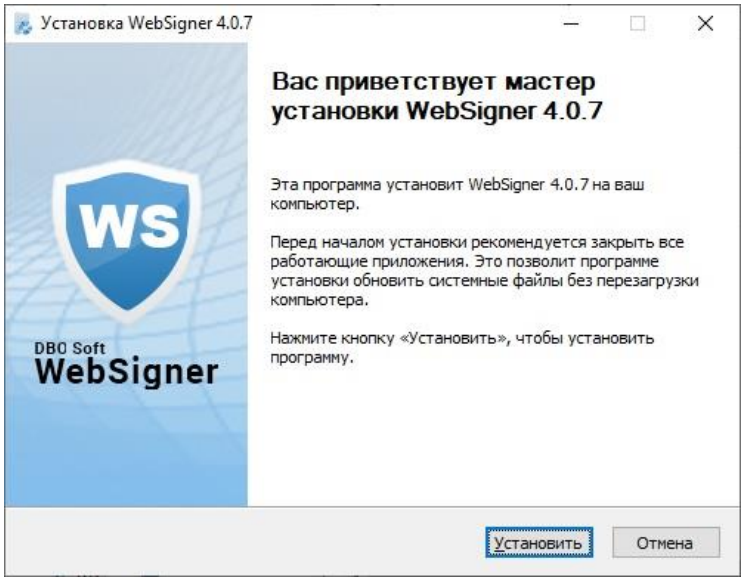

Рис.5

2.4. Вхід до особистого кабінету в СДОР «ВЕБ-банкінг для корпоративних клієнтів» (Рис.6) потрібно здійснювати з використанням згенерованого особистого ключа, який може знаходитися у вигляді файлу на жорсткому диску або на захищеному апаратному пристрої (USB-токену).

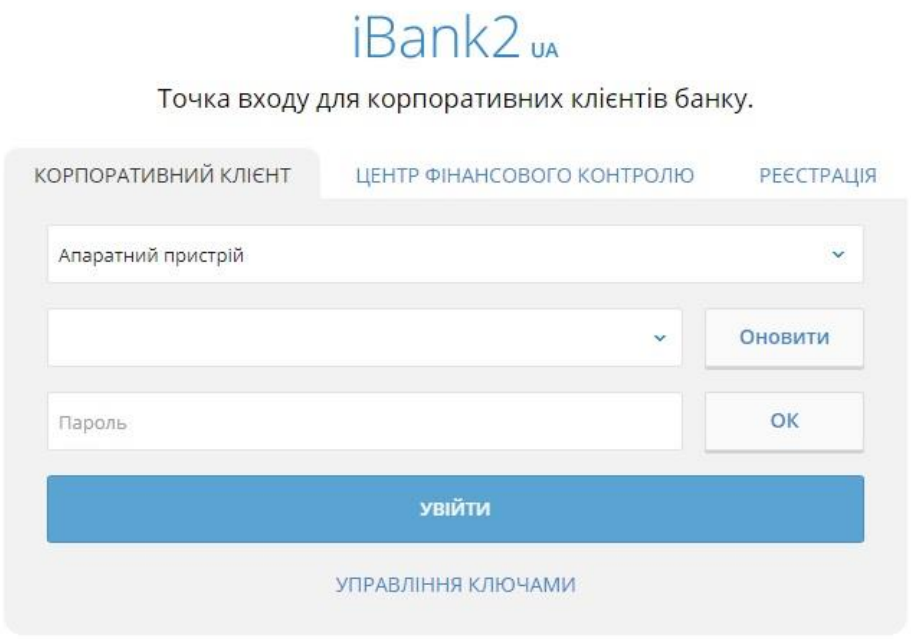

Рис.6

2.5. Використовувати багатофакторну автентифікацію за допомогою:

– одноразових паролів з СМС-повідомлень відправлених Банком;

– одноразових паролів (ОТР-кодів) згенерованих апаратними пристроями ОТР-токенами (Рис.7а);

– одноразових паролів (ОТР-кодів) згенерованих мобільним застосунком «Google Authenticator», який клієнт може встановити на своєму мобільному пристрої та виконати налаштування в особистому кабінеті СДОР (Рис.7б);

Рис.7а

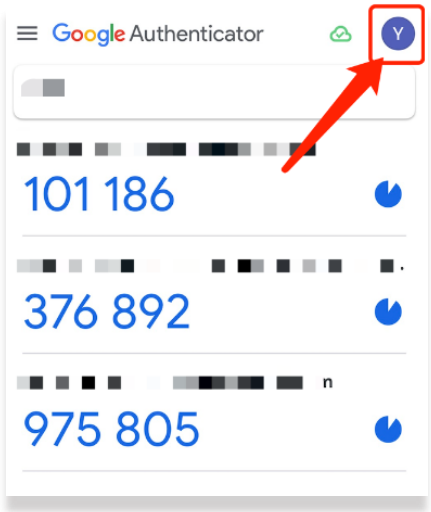

Рис.7б

3. Рекомендації щодо безпечного використання СДОР «RB24» з використанням інтернет-браузерів:

3.1. При вході на сайт, користувач повинен уважно перевіряти доменне ім’я (Рис.8).

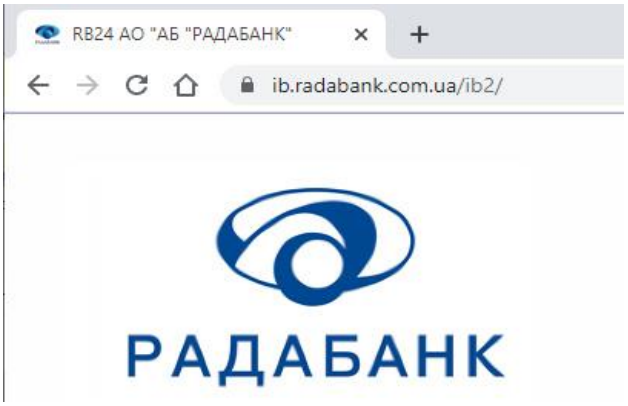

Рис.8

3.2. Виконувати перевірку кому та ким виданий сертифікат і стежити за строком його дії. Натиснувши на значок замка можна переглянути властивості сертифікату (Рис.9).

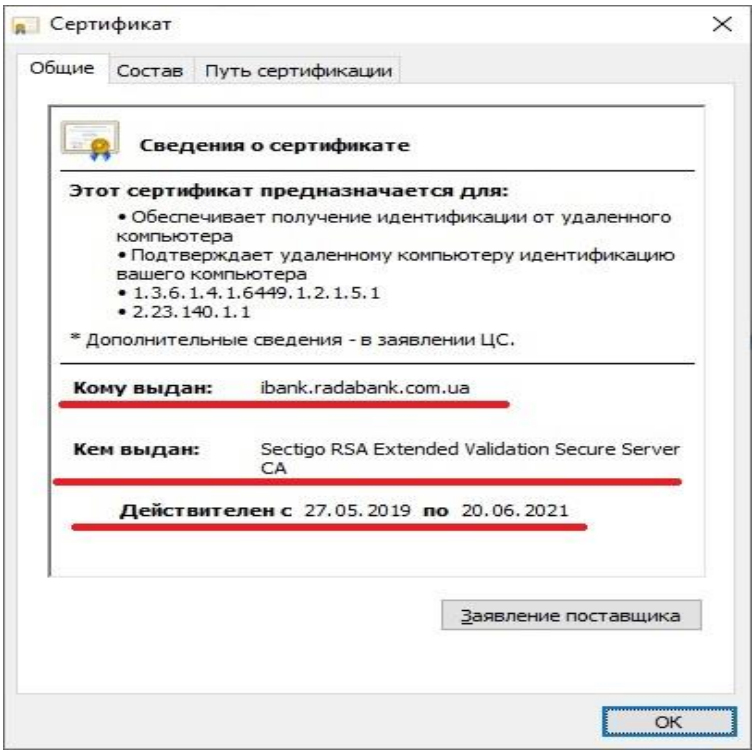

Рис.9

Зображення замкнутого замка (Рис.10) означає, що на сайті встановлений SSL-сертифікат і вся інформація передається по захищеному протоколу. SSL-сертифікат не дає шахраям перехопити або підмінити особисті дані користувачів.

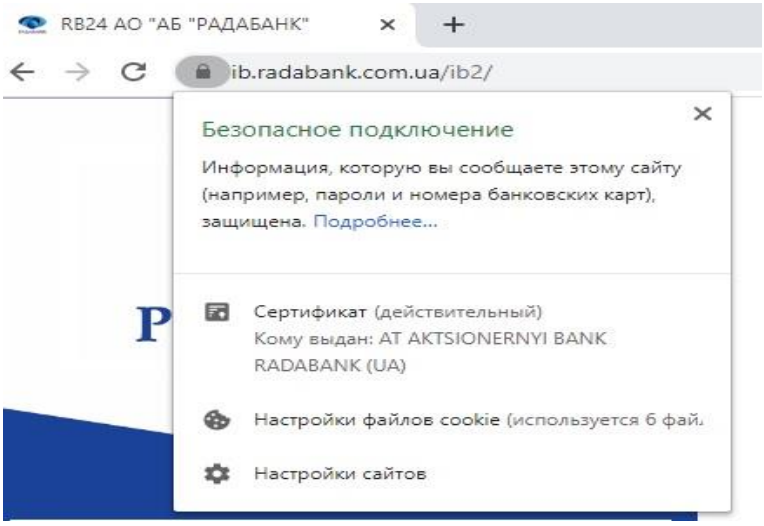

Рис.10

3.3. Використовувати багатофакторну автентифікацію за допомогою одноразових паролів з СМС-повідомлень. Користувач зобов'язаний тримати у таємниці та не повідомляти стороннім особам одноразовий код з СМС-повідомлення, який надається користувачу при вході до системи.

4. Рекомендації щодо безпечного використання СДОР «RB24» з використанням мобільних пристроїв:

4.1. Мобільний додаток «RB24» слід завантажувати з офіційного сайту Банку або офіційних магазинів додатків «App Store» для iOS пристроїв та «Google Play маркет» для Android пристроїв (Рис.11).

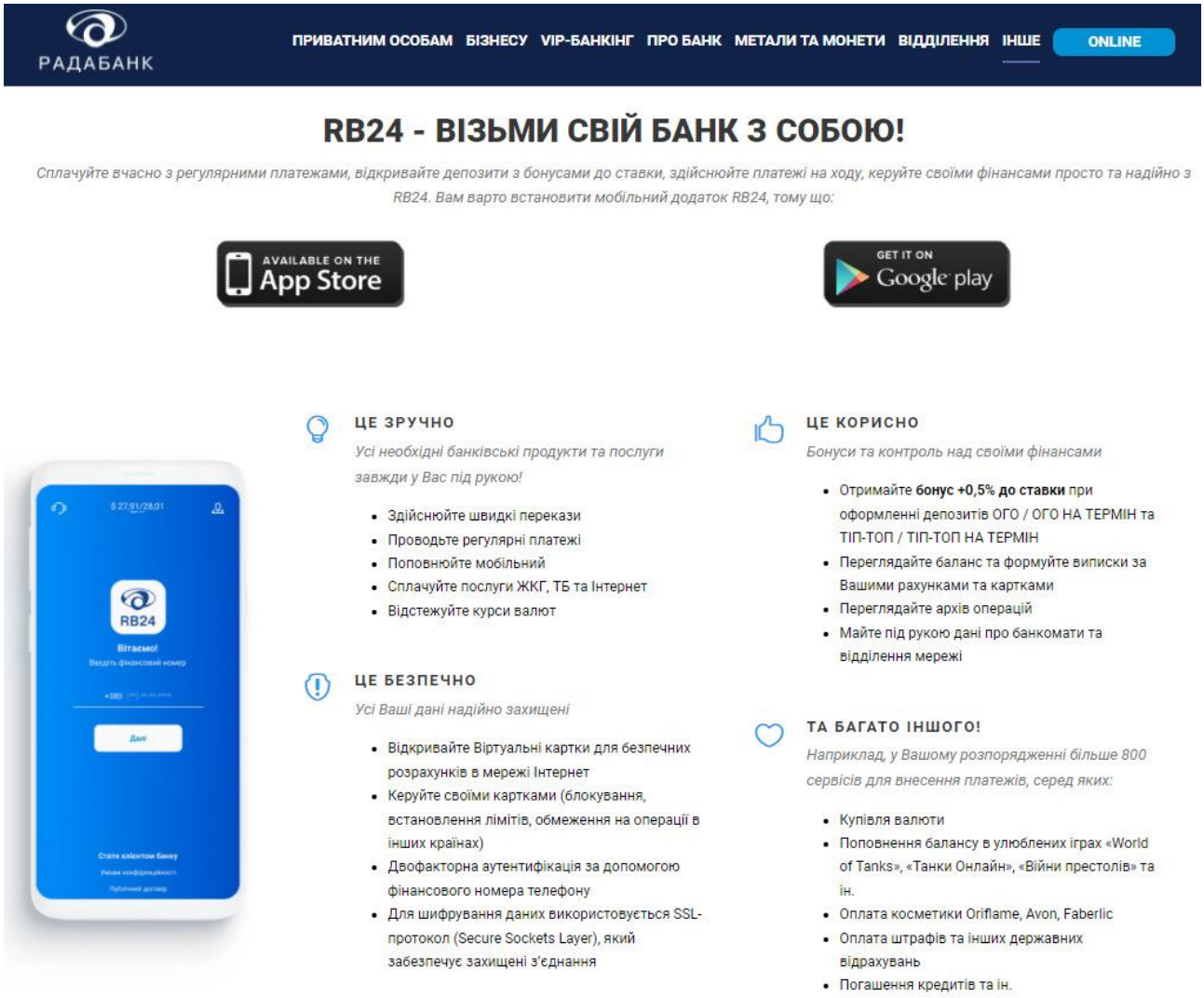

Рис.11

4.2. Завчасно виконувати оновлення мобільного додатку.

4.3. При здійсненні входу в мобільний додаток використовувати багатофакторну автентифікацію за допомогою одноразових паролів отриманих в СМС-повідомленнях.

4.4. У разі можливості використовувати блокування екрану мобільного пристрою із застосуванням графічного ключа, сканера відбитку пальця, використовуючи технологію розпізнавання по обличчю «Face ID».