Додаток1
до Наказу Голови Правління
№ 132 від 12.07.2019

ЗАТВЕРДЖЕНО
Наказом Голови Правління
АТ «УНІВЕРСАЛ БАНК»

Старомінська І.О.

Правила інформаційної безпеки АТ «УНІВЕРСАЛ БАНК»

Ці Правила інформаційної безпеки АТ «УНІВЕРСАЛ БАНК» (далі – **Правила**) обов'язкові до виконання всіма особами, які мають право використання електронного підпису (далі – **ЕП**) від імені Клієнта, а також особами, які відповідають за експлуатацію та адміністрування електронних пристроїв з встановленим програмним забезпеченням, що використовується для накладення електронного підпису від імені Клієнта при взаємодії з АТ «УНІВЕРСАЛ БАНК» (далі – **Банк**) .

Ефективність та безпека використання Клієнтами/представниками Клієнта (далі – **Клієнт**) при електронній взаємодії з Банком Системи «Інтернет-Банкінг» та/або Чат-бот та/або електронної взаємодії через інші електронно-інформаційні системи, обумовлені між Банком та Клієнтом (далі – **Система**) значною мірою залежить від неухильного дотримання Клієнтом вимог інформаційної безпеки в процесі її експлуатації.

Клієнт може використовувати Систему виключно за умови дотримання наступних Правил:

1. Щоденно аналізуйте всі повідомлення про прийняті та неприйняті Банком електронні документи та негайно повідомляйте Банк про випадки несанкціонованого зарахування (перерахування) коштів або виникнення інших підозрілих операцій в Системі.

2. Встановіть на робочу станцію, з якої здійснюється доступ до Системи, ліцензійне антивірусне програмне забезпечення. Підтримуйте оновлення версій, регулярно та своєчасно оновлюйте антивірусні бази даних.

3. Встановіть на робочу станцію, з якої здійснюється доступ до Системи:

- ліцензійне антишпигунське програмне забезпечення (antispyware);
- програмний персональний мережевий екран (файервол, брендмауер).

4. Регулярно та своєчасно оновлюйте системне програмне забезпечення робочої станції, за допомогою якого здійснюється доступ до Системи, особливо операційної системи, web-браузера, Java-машини.

5. Не встановлюйте на робочі станції, через які ведеться робота з Системи, програмне забезпечення з ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях тощо). Не рекомендується здійснювати з такої робочої станції доступ до ненадійних (незнайомих) Інтернет ресурсів.

6. Під час доступу до Системи суворо не рекомендується працювати в операційній системі з обліковим записом користувача, який має розширені права в операційній системі, наприклад, «Адміністратор».

8. Не рекомендується здійснювати доступ до Системи через посилання, отримані електронною поштою, а також із неконтрольованих та ненадійних робочих станцій, розташованих в Інтернет кафе, готелях, офісах, інших організаціях.

9. З метою заволодіння даними автентифікації користувачів Системи (особистий ключ ЕП та пароль доступу до нього) для їхнього подальшого незаконного використання, зловмисники інколи здійснюють атаки на робочі станції користувачів. Основні методи заволодіння ключовою інформацією:

- розсилання користувачам підроблених електронних листів із посиланням на адресу веб-сайту, що маскується під банківський;

- розповсюдження через електронні листи чи веб-сайти програмного забезпечення із зловмисним кодом (тобто програмного вірусу) для заволодіння даними автентифікації користувача;
- несанкціоноване дистанційне управління персональним комп'ютером користувача шляхом віддаленого доступу.

При виконанні Клієнтом запропонованих або стандартних дій, вірус копіює ключі та паролі та передає цю інформацію зловмисникам. Для запобігання виникненню подібних ситуацій необхідно знати, що Банк ніколи та за жодних обставин не здійснює розсилку електронних листів із вимогою надіслати ключ, пароль, перейти за вказаною електронною адресою, а також не розповсюджує електронною поштою комп'ютерні програми. Відповідальність за збереження ключів та паролів покладається на користувача. У разі отримання подібних листів, програм чи будь-яких повідомлень електронною поштою, просимо терміново проінформувати про це Банк листом або телефоном, які зазначено на сайті Банку. Рекомендується видаляти підозрілі електронні листи без їхнього відкриття, особливо листи від невідомих відправників із прикріпленими файлами, що мають розширення *.exe, *.pif, *.vbs, та інші файли.

10. Якщо налаштування робочої станції, з якої здійснюється доступ до Системи, здійснює сторонній спеціаліст, рекомендуємо забезпечити контроль за його діями.

11. Рекомендації щодо безпеки поводження з даними автентифікації (особистим ключем та паролем доступу до нього):

- Особистий ключ та пароль доступу до нього є найкритичнішими даними з точки зору безпечної роботи в Системі. Особистий ключ генерується за ініціативою користувача — його власника під особистим контролем. Банк за жодних обставин не має доступу до особистих ключів користувачів. Для забезпечення надійного зберігання та використання особистих ключів рекомендується використання апаратних пристроїв формування підпису (токенів), що постачаються Банком. У разі, якщо користувач обирає метод зберігання ключів в файловому контейнері, особисті ключі повинні зберігатися виключно на рухомому носії інформації (дискета, диск, USB-накопичувач). Не допускається навіть тимчасове зберігання ключів ЕП на робочих станціях.
- Носій ключової інформації, який містить чинний ключ (рухомий носій інформації, токен), повинен постійно бути під особистим контролем користувача, що забезпечує унеможливлення доступу до нього інших осіб. За жодних обставин не допускається передача носія ключової інформації (токену) та/або розголошення паролю до нього іншим особам, у тому числі співробітникам Банку.
- Носій ключової інформації, який містить чинний ключ (рухомий носій інформації, токен), повинен використовуватися тільки під час роботи у Системі. Не залишайте носій ключової інформації (токен) приєднаним до персонального комп'ютеру, якщо робота в системі призупинена чи не проводиться, персональний комп'ютер використовуються для виконання інших функцій, а також у неробочий час.
- Пароль доступу до особистих ключів не повинен зберігатися у відкритому вигляді (наприклад, бути записаним на папері) та використовуватися для інших систем та сервісів. Персональна відповідальність за збереження паролю доступу та унеможливлення використання носія ключової інформації іншою особою покладається виключно на користувача.
- Періодично змінюйте пароль доступу до ключа (не рідше одного разу на місяць). Пароль повинен складатися з цифр, літер верхнього та нижнього регістрів, а також спеціальних символів. При виборі паролю не використовуйте комбінації, що легко вгадуються, наприклад, імена, дати народження, телефонні номери тощо.
- У разі звільнення користувачів або переведення їх на посади, які не передбачають роботу у Системі, необхідно негайно звернутися до Банку з метою блокування їхніх ключів.