**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 систем дистанційного обслуговування клієнтів (Інтернет-банкінгу, чат-ботів, мобільних додатків та ін.), що використовується для накладення ЕП 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 систем дистанційного обслуговування клієнтів (далі – **СДО**) значною мірою залежить від неухильного дотримання Клієнтом вимог інформаційної безпеки в процесі її експлуатації.

**Клієнт може використовувати СДО виключно за умови дотримання наступних Правил:**

- Щоденно аналізувати 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 СДО.

- Встановити на персональний комп'ютер\ноутбук (далі – ПК), з якого здійснюється доступ до СДО, ліцензійне антивірусне програмне забезпечення. Підтримувати оновлення версій, регулярно та своєчасно оновлювати антивірусні бази даних.

- Встановити на ПК, з якого здійснюється доступ до СДО:
  - ліцензійне антишпигунське програмне забезпечення (antispyware);
  - програмний персональний мережевий екран (файервол, брандмауер).

- Регулярно та своєчасно оновлювати системне програмне забезпечення ПК, з якого здійснюється доступ до СДО, особливо операційної системи, web-браузера, Java-машини.

- Не встановлювати на ПК, з якого ведеться робота з СДО, програмне забезпечення з ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях тощо). Не рекомендується здійснювати з такого ПК доступ до ненадійних (незнайомих) Інтернет ресурсів.

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

- Не рекомендується здійснювати доступ до СДО через посилання, отримані електронною поштою, а також із неконтрольованих та ненадійних ПК, розташованих в публічних місцях, Інтернет-кафе, готелях, офісах, інших організаціях.

- Пам'ятати, що з метою заволодіння даними автентифікації користувачів СДО (особистий ключ ЕП та пароль доступу до нього) для їхнього подальшого незаконного використання, зловмисники інколи здійснюють атаки на ПК користувачів. При цьому основними методами заволодіння ключовою інформацією є:

  – 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 ПК 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 за 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.

- Якщо налаштування ПК, з якого здійснюється доступ до СДО, здійснює сторонній спеціаліст, рекомендуємо забезпечити контроль за його діями.

- 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 СДО. Особистий ключ генерується за ініціативою користувача — його власника, та під його 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 (USB-флешка та ін.). Не допускається навіть тимчасове зберігання ключів ЕП на ПК.

- Носій ключової інформації, який містить чинний ключ (рухомий носій інформації, токен), повинен постійно бути під особистим контролем користувача, що унеможливлює доступ до нього інших осіб. За жодних обставин не допускається передача носія ключової інформації та/або розголошення паролю до нього іншим особам, у тому числі співробітникам Банку.

- Носій ключової інформації, який містить чинний ключ, повинен використовуватися тільки під час роботи у СДО. Не залишайте носій ключової інформації приєднаним до ПК, якщо робота в СДО призупинена чи не проводиться, ПК 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 СДО, користувачу або керівнику користувача необхідно негайно звернутися до Банку з метою блокування ключів користувача.

**Правила використання та безпечної роботи з мобільних пристроїв (далі МП - телефони, смартфони, планшети та інші):**

- Використовувати тільки офіційні версії мобільних застосунків;

- Встановлювати застосунки на МП лише з офіційних та перевірених сервісів (Google Play Store для Android, App Store для iOS);

- Заборонити операційній системі МП автоматично встановлювати застосунки з невідомих джерел, шляхом здійснення відповідних налаштувань пристрою;

- Забезпечити фізичну безпеку МП;
- Максимально обмежити передавання МП іншим особам;
- Унеможливити залишання МП без нагляду, якщо не вжито заходів щодо забезпечення його фізичного збереження та обмеження доступу до них сторонніх осіб;
- Використовувати не тільки відбиток пальця/сканування обличчя для розблокування смартфону, але і пароль;
- Використовувати складні паролі;
- Ставити автоматичне блокування смартфону через 30 секунд або 1 хвилину;
- При використанні графічного ключа у ньому повинно бути не менше 5-6 рухів;
- Не використовувати root-доступ на МП.

**Правила про застосування електронних підписів:**

Правила про застосування ЕП окремо описані в документах щодо здійснення електронного документообігу в Банку, що розташовані на сайті Банку - https://www.universalbank.com.ua/

Дія цих правил поширюється на суб'єктів електронної взаємодії, які мають відповідним чином підписані договори з Банком, включаючи використання сервісу електронного документообігу «ВЧАСНО», Інтернет-Банкінг, чат-боти або мобільні застосунки Банку.