Додаток 2 до Договору на приєднання до Публічної пропозиції за тарифним пакетом «____» №___ від __ _____ 20__ р.

.

ІНСТРУКЦІЯ ПРО ПОРЯДОК ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КЛЮЧОВОЇ ІНФОРМАЦІЇ

1. Персональний ключ ЕП та пароль доступу до нього є найбільш критичними даними з точки зору безпечної роботи користувача в Системі.

Персональні ключі ЕП можуть зберігатися на рухомому носії інформації (дискеті, DVD/CD-диску, USB-накопичувачу). Зберігання (у т.ч. тимчасове) персональних ключів ЕП на жорсткому диску комп'ютера не припустимо.

2. Носій ключової інформації (рухомий носій інформації, що містить ключ ЕП) повинен зберігатися під особистим контролем його власника – користувача Системи, який забезпечує унеможливлення доступу до нього інших осіб. Передавання носія ключової інформації та/або розголошення паролю доступу до персонального ключа ЕП іншим особам, у тому числі співробітникам Банку заборонено.

3. Носій ключової інформації повинен використовуватись тільки під час роботи в Системі. Не допустимо залишати носій ключової інформації приєднаним до персонального комп'ютера, коли робота в Системі призупинена або не проводиться.

Для персональних ключів ЕП, що зберігаються на рухомому носії, обов'язкове використання SMS-аутентифікації (додатковий пароль для входу в Систему, що надходить за допомогою SMS-повідомлення)..

4. Термін дії персонального ключа ЕП визначається Банком самостійно та зазначається в Додатку 2 до Договору. У разі нездійснення своєчасної зміни персонального ключа ЕП доступ користувача до Системи буде заблоковано. Користувач має право самостійно виконувати позапланову зміну персонального ключа ЕП. Після активації нового персонального ключа ЕП в Системі або у разі відключення від Системи користувач повинен знищити неактуальний ключ ЕП, що міститься на носії ключової інформації.

5. Пароль доступу до персонального ключа ЕП не повинен зберігатись у відкритому вигляді (наприклад, записаним на паперовому носії тощо) та використовуватись для доступу до інших систем та сервісів. Персональна відповідальність за збереження паролю доступу до персонального ключа ЕП та захист носія ключової інформації від використання іншою особою покладається на користувача.

6. Користувач зобов'язаний не рідше одного разу на місяць змінювати пароль доступу до персонального ключа ЕП, що повинен містити щонайменше 6 символів та складатися з цифр, літер верхнього та нижнього регістрів, спеціальних символів. При виборі паролю не допускається використання комбінацій, що легко вгадуються, наприклад, імен, дат народження, телефонних номерів тощо.

7. Необхідно забезпечити обов'язкову наявність на персональному комп'ютері, з якого здійснюється доступ до Системи, наступного програмного забезпечення:

7.1. ліцензійного антивірусного програмного забезпечення. База даних вірусних сигнатур повинна оновлятись щоденно;

7.2. ліцензійного антишпигунського програмного забезпечення (Antispyware);

7.3. мережевого екрану (Firewall, брандмаеру), який повинен бути налаштований таким чином, щоб максимально обмежити вихідний та вхідний мережевий трафік.

Антивірусне та антишпигунське програмне забезпечення повинне бути налаштоване для моніторингу всіх подій та періодичного сканування інформації, що зберігається на жорсткому диску персонального комп'ютера, з якого здійснюється доступ до Системи.

8. Забороняється встановлювати на персональний комп'ютер, з якого здійснюється доступ до Системи, програмне забезпечення з ненадійних джерел (публічні бібліотеки програмного забезпечення, програми в електронних повідомленнях тощо). Не рекомендується використовувати персональний комп'ютер, з якого здійснюється доступ до Системи, для доступу до ненадійних (незнайомих) інтернет-ресурсів.

9. Для поточної роботи в Системі забороняється використання облікового запису користувача з правами «Адміністратор».

10. Під час підключення до веб-сайту Банка (https://ibank.unexbank.ua) користувачу необхідно переконатися у коректній автентифікації веб-сайту Системи під час SSL-сесії.

Користувачу забороняється здійснювати доступ до Системи через посилання, отримані засобами електронної пошти, або з неконтрольованих та ненадійних робочих місць (інтернет-кафе, готелі, офіси інших організацій тощо).

11. З метою встановлення обмеження переліку IP-адресів та/або IP-підмереж, з яких можливе підключення до Системи, Клієнт може звернутися до Банку шляхом подання письмової заяви про встановлення зазначеного обмеження за підписом уповноважених осіб та відбитком печатки Клієнта (за наявності).

12. Якщо налаштування персонального комп'ютера, з якого здійснюється доступ до Системи, здійснює інша особа, необхідно забезпечити контроль за всіма діями такої особи на персональному комп'ютері.

13. З метою заволодіння приватними даними Клієнта (персональний ключ ЕЦП та пароль доступу до нього) для їх подальшого незаконного використання зловмисники здійснюють фішингові або хакерські атаки.

Основні методи заволодіння ключовою інформацією:

– розсилання Клієнту підроблених електронних листів та адрес інтернет-сайтів, що маскуються під банківські, з пропозицією надати інформацію щодо приватних даних Клієнта/ його уповноважених осіб начебто для звірки;
– розповсюдження через електронні листи або інтернет-сайти програмного забезпечення із зловмисним кодом (програмним вірусом) для заволодіння приватними даними Клієнта/ його уповноважених осіб;
– несанкціоноване дистанційне управління персональним комп'ютером Клієнта шляхом віддаленого доступу.

При виконанні Клієнтом запропонованих дій або при виконанні стандартних дій входу до Системи програмний вірус копіює персональний ключ ЕП та пароль доступу до нього, та передає цю інформацію зловмисникам.

Щоб запобігти несанкціонований доступ та заволодіння ключовою інформацією необхідно знати, що Банк не здійснює розсилку електронних листів з вимогою надіслати персональний ключ ЕП та/або пароль доступу до нього, не пропонує перейти за вказаною електронною адресою та не розповсюджує електронною поштою комп'ютерні програми.

Відповідальність за збереження конфіденційності персональних ключів ЕП покладається на Клієнта, як на єдиного власника таких ключів.

У разі отримання листів, програм чи будь-яких повідомлень засобами електронної пошти, що вимагають надіслання персональних ключів ЕП та/або введення паролю доступу до персонального ключа ЕП або інших дій, пов'язаних із несанкціонованим доступом до Системи, Клієнт зобов'язаний негайно повідомити Банк відповідно до умов Договору.

Рекомендується видаляти підозрілі повідомлення, що надійшли засобами електронної пошти, без їх відкриття. Користувач повинен запобігати відкриттю електронних листів від невідомих відправників з приєднаними файлами, що мають розширення *.exe, *.pif, *.vbs та інші файли, що можуть бути виконані.

З Інструкцією ознайомлений та згоден нести відповідальність за її неналежне виконання:

__ _____ 20__ р. _____ _____

підпис *П.І.Б.*

м. п. (за наявності)

Сторона 1. Банк		**Сторона 2. Клієнт**	
Найменування Банку:	**АТ «ЮНЕКС БАНК»**	**Найменування:**	
Адреса реєстрації:	03040, Україна, м. Київ, вул. Васильківська, 14	**Адреса реєстрації:**	
Тел./ факс:		**Тел./ факс:**	
Код банку:	322539	**Адреса для листування:**	
Код ЄДРПОУ:	20023569	**Код ЄДРПОУ / податковий номер:**	
Міжнародний номер банківського рахунку (IBAN):	UA503000010000032003119701026	**Міжнародний номер банківського рахунку (IBAN):**	
Відділення банку:			
Адреса відділення банку:			
Тел./факс відділення:			
Посада:	_____	**Посада:**	_____
_____	_____	_____	_____
(підпис) М.П.	(ПІБ)	(підпис)	(ПІБ)