КОРИСНА ІНФОРМАЦІЯ

Інформація щодо безпеки системи «PINbank Online»

Для запобігання доступу сторонніх осіб до конфіденційної інформації клієнта через систему «PINbank Online» , а також перегляду, передачі або модифікації даних використовується багаторівнева архітектура системи безпеки, що включає у себе:

- використання ssl-протоколу задля безпеки передавання даних із шифруванням каналів зв'язку;
- обов'язкову авторизацію та автентифікацію користувачів;
- протоколювання усіх дій користувачів в системі;
- обмін даними лише за стандартизованими інтерфейсами;
- електронний підпис документів з прив'язкою до параметрів документа;
- електронно-цифровий підпис документів з використанням асиметричних алгоритмів;
- електронно-цифровий підпис інформаційних запитів від клієнта з використанням асиметричних алгоритмів;
- контроль прав доступу користувача до об'єктів системи.

Під час доступу до системи «PINbank Online»:

Обов'язково впевніться, що в адресному рядку браузера наявна адреса саме системи «PINbank Online»: https://online.pinbank.ua;

Зауважте: зазвичай створені шахраями фішингові сайти мають адресу та зовнішній вигляд, як у оригінальної сторінки!

Завжди звертайте увагу на наявність у вікні браузера ознак захищеного з'єднання: піктограми у вигляді зачиненого замну (вид цієї піктограми та місце її відображення можуть відрізнятися в залежності від браузера та його версії), а також достовірний цифровий сертифікат банку;

Відмовтеся від використання функції збереження паролів, яку пропонує браузер.

Кожний користувач системи «PINbank Online» є гарантом і складовою частиною системи безпеки та повинен дотримуватись наступних правил:

- Не розголошуйте свій логін і паролі третім особам;
- Не передавайте свій мобільний пристрій, на який банк відправляє OTP-коди для підтвердження операцій в системі, у користування третім особам;
- Зберігайте ваш секретний ключ на зовнішньому носії інформації (флеш-карта);
- Не зберігайте зовнішній носій інформації з вашим секретним ключем разом з логіном і паролями;
- Користуйтеся кнопкою «Вихід» для завершення сеансу роботи з системою;
- Не забувайте виймати зовнішній носій інформації після завершення роботи з системою «PINbank Online» ;

- Застосовуйте інші рекомендації банку по забезпеченню захисту та цілісності інформації під час роботи з системою «PINbank Online» .

Не розголошуйте свій логін і паролі третім особам

Система «PINbank Online» ідентифікує користувача за логіном, паролем на вхід у систему, секретним ключем і паролем на нього або OTP-кодом. Щоб уникнути несанкціонованого доступу до вашої конфіденційної інформації, не розголошуйте свої реквізити на вхід у систему третім особам.

Кожному користувачеві (залежно від обраного способу підтвердження дій у системі) банк видає:

- логін – ім'я користувача;
- пароль – пароль на вхід до системи;
- секретний ключ та пароль до нього.

При першому вході з цими реквізитами система «PINbank Online» автоматично ініціює процес створення нового секретного ключа. Також з метою дотримання безпеки необхідно змінити пароль на вхід до системи. Надалі система «PINbank Online» періодично наполегливо рекомендує користувачеві запустити процес створення нового секретного ключа після закінчення терміну дії попереднього.

Система «PINbank Online» фіксує всі спроби зміни і підбору пароля на вхід до системи.

Приділяйте пильну увагу зберіганню та використанню секретних ключів у системі «PINbank Online»:

- Зберігайте секретний ключ на зовнішньому носії інформації (флеш-картці, токені тощо). Зберігання цієї інформації на зовнішніх носіях забезпечує не лише захист вашої конфіденційної інформації в системі «PINbank Online», але й цілісність секретних ключів при виникненні раптових проблем у роботі комп’ютера;
- Не тримайте носій з ключем постійно приєднаним до комп’ютера, а вмикайте його лише тоді, коли необхідно увійти до системи або підписати документи;
- Застосовуйте декілька підписів (2 ключі) для підтвердження та надсилання фінансового документу до банку на виконання;
- Під час генерації/перегенерації секретного ключа необхідно зазначати шлях до носія інформації, з якого були прочитані первинні дані;
- Не зберігайте зовнішній носій інформації з вашим секретним ключем разом з логіном та паролями. В разі втрати цією інформацією можуть скористатися треті особи у власних цілях.

Використовуйте кнопку «Вихід» після закінчення сеансу роботи з системою

Відволікання від комп'ютера при виконаному вході до системи без завершення сеансу роботи з програмою може спровокувати третю особу скористатися ситуацією.

Не забувайте виймати зовнішній носій інформації одразу після завершення роботи з системою «PINbank Online»

Не забувайте виймати зовнішній носій інформації одразу після завершення роботи з системою «PINbank Online» – цією інформацією можуть скористатися треті особи, вона може бути невідворотно втрачена або пошкоджена в процесі роботи інших програм.

Застосовуйте інші рекомендації по забезпеченню захисту вашої інформації під час роботи з системою «PINbank Online»

Додатково перевірити інформацію про банк та його окремі підрозділи ви можете у довіднику банків, що розміщений на офіційній сторінці НБУ за посиланням https://bank.gov.ua/ua/supervision/institutions/

Додатково перевірити, чи не внесений інтернет-сайт до бази шахрайських сайтів Української міжбанківської асоціації платіжних систем ЕМА можна за посиланням https://ema.com.ua/report-an-incident/black-list/

Встановлюйте складні паролі та періодично їх змінюйте

Встановлюйте паролі довжиною не менше 8 символів із використанням літер нижнього та верхнього регістрів, цифр та спеціальних символів. Щоб досягти більшої надійності та стійкості, використовуйте в якості пароля словосполучення або фразу. Періодично змінюйте паролі.

Не рекомендовано працювати з системою «PINbank Online»:

- в інтернет-кафе та інших подібних місцях, де немає гарантії того, що за діями користувача не стежить стороння людина;
- у місцях, де встановлені пристрої відеоспостереження, за допомогою яких можна отримати інформацію про паролі користувача;
- якщо немає упевненості в безпеці встановленого програмного забезпечення (наявність вірусів, спеціальних програм, що пересилають паролі користувача третім особам тощо).

Безпека роботи на комп'ютері або іншому пристрої, з якого ви здійснюєте доступ до «PINbank Online»

- Для постійної роботи на комп'ютері використовуйте обліковий запис звичайного користувача, а привілейовані облікові записи з правами адміністратора застосовуйте лише в разі необхідності, завжди звертайте увагу на запити операційної системи щодо підвищення привілеїв для встановлення програмного забезпечення або виконання операцій;
- Використовуйте актуальні версії операційних систем, браузерів, іншого програмного забезпечення та регулярно їх оновлюйте. Там, де це можливо, налаштуйте оновлення у автоматичному режимі;

- Використовуйте ліцензійні засоби антивірусного захисту та захисту від шкідливих програм, стежте за регулярним оновленням сигнатур, періодично здійснюйте повне сканування локальних дисків;
- Під час роботи з електронною поштою відкривайте вкладення та посилання лише від довірених відправників. Видаляйте без відкривання підозрілі електронні листи, файли із розширеннями * .exe, * .pif, * .vbs тощо.

Зауважте: Банк ніколи не розсилає електронною поштою програми для встановлення на комп'ютері або іншому пристрої, з якого здійснюється доступ до системи «PINbank Online».

Зауважте: Банк ніколи не вимагає у клієнтів повідомити паролі, одноразові коди, копії криптографічних ключів, ПИН-коди та інформацію щодо термінів дії платіжних карток, коди CVV – ані телефоном, ані sms-повідомленнями, ані електронною поштою.

Дотримання безпеки під час роботи через інтернет

Безпека обміну даними під час роботи в мережі інтернет забезпечується на рівні чіткої взаємної автентифікації учасників обміну даними.

Клієнтська частина передає на сервер запит на встановлення з'єднання, підписаний електронно-цифровим підписом (або електронним підписом) користувача, після чого бібліотеки криптозахисту формують необхідні секретні параметри і ключі та підтверджують встановлення з'єднання. Таким чином, кожне з'єднання має унікальні параметри і дозволяє однозначно ідентифікувати учасників обміну даними.

Обмін даними може бути розпочатий тільки після встановлення криптографічної зв'язаності між вузлами «Клієнт» і «Сервер». Увесь обмін даними між клієнтом і сервером системи, включаючи передачу на сервер автентичних повноважень клієнта (паролі) для реєстрації і допуску до даних і завдань, виконується в зашифрованому вигляді. Операції шифрування/розшифровки даних забезпечуються бібліотеками криптозахисту і виконуються на прикладному рівні, в процесі підготовки даних для передачі у банк.

Негайно зверніться до контакт-центру банку за телефонами 0-800-50-70-80 або (044) 428-61-28 в таких випадках:

- Ви загубили пароль;
- Ви загубили ключ;
- Неможливо увійти до системи через невідповідність пароля;
- Якщо виникла підозра, що паролі/ключі стали відомі третім особам;
- Виявлена спроба несанкціонованого доступу до системи;
- Виявлена сфальшована сторінка банку (фішинговий сайт);
- Для блокування доступу до системи та/або отримання рекомендацій щодо подальших дій.

Права користувача

Залежно від того, який режим роботи вказаний в договорі на підключення і обслуговування клієнта системи «PINbank Online» , користувачеві може бути дозволений повний або

обмежений доступ до меню системи і рахунків, право виконувати операції або ж тільки переглядати інформацію.

Також можуть бути обумовлені обмеження прав користувача, наприклад, користувач має право готувати документи, але не має права їх підписувати.

Для внесення змін до прав користувача необхідно звернутися в банк до адміністратора системи.

ЗАБУЛИ ПАРОЛЬ?

Я не маю облікових даних для першого входу до системи

Перед початком роботи з системою «PINbank Online» користувачеві для першого входу надаються:

- Логін – ім'я користувача;
- Пароль – пароль на вхід до системи;
- Секретний ключ та пароль до нього.

Якщо ви оформили доступ до «PINbank Online», але у вас відсутні будь-які із зазначених вище облікових даних, зверніться до адміністратора системи «PINbank Online» за номером телефону, що вказаний у лівому нижньому кутку сторінки входу до системи, або до контакт-центру банку для з`ясування параметрів вашого облікового запису.

Я забув пароль на вхід до системи

Увага! Якщо зазначений пароль виявився некоректним, не намагайтеся підібрати його - це призведе до того, що ваш обліковий запис буде заблоковано.

Якщо введений пароль виявився помилковим, зверніться до адміністратора системи «PINbank Online» за номером телефону, що вказаний у лівому нижньому кутку сторінки входу до системи, або до контакт-центру банку з проханням надати вам тимчасовий пароль. Після входу до системи під призначеним адміністратором тимчасовим паролем вас буде спрямовано на сторінку зміни пароля, де ви зможете замінити тимчасовий пароль на постійний.

Я забув пароль до секретного ключа

Увага! Не намагайтеся підібрати пароль - це призведе до того, що ваш обліковий запис буде заблоковано!

Якщо введений пароль до секретного ключа виявився помилковим, система повідомить про помилку й запропонує провести процедуру відновлення сертифікатів (при цьому ви зможете вказати новий пароль до секретного ключа). Якщо виникла така ситуація, зверніться до адміністратора системи «PINbank Online» за номером телефону, що вказаний у лівому нижньому кутку сторінки входу до системи, або до контакт-центру банку, для того щоб він призначив вам аварійний пароль. Після цього слід приступити до процедури відновлення сертифікату:

- Введіть ваш логін та пароль на вхід до системи;
- Введіть аварійний пароль, призначений адміністратором;

- Вигадайте новий пароль до секретного ключа, введіть його до відповідного поля на формі,
- продублюйте в полі Повторіть введення пароля, натисніть кнопку 'Відправити';
- На наступному кроці вам необхідно зберегти новий секретний ключ (за замовчанням його буде збережено до папки завантажень вашого браузера). Наполегливо рекомендуємо одразу після збереження нових ключів/сертифікатів перенести їх до окремої папки, де зберігаються ваші ключі та сертифікати;
- Далі необхідно переглянути і роздрукувати сформований сертифікат, після чого запит на авторизацію нового сертифіката буде відправлений до банку;
- Роздрукований та підписаний сертифікат необхідно обов’язково передати до банку для авторизації доступу;
- Для перевірки наявності нових сертифікатів через деякий час знову спробуйте увійти до системи (введіть логін і пароль на вхід до системи):
    - Якщо сертифікати авторизовані, система відобразить повідомлення про успішне завершення процедури відновлення сертифікатів, а також запропонує зберегти новий сертифікат - для цього буде потрібно ввести аварійний пароль, зазначити шлях та пароль до секретного ключа, а потім зберегти сертифікат (за замовчанням його буде збережено до папки завантажень вашого браузера). Наполегливо рекомендуємо одразу після збереження нових ключів/сертифікатів перенести їх до окремої папки, де зберігаються ваші ключі та сертифікати;
    - Якщо сертифікати ще не авторизовані, система відобразить повідомлення про те, що ваша заявка перебуває в черзі на розгляд. У цьому випадку спробу слід повторити пізніше.
- Після успішної авторизації й установки нових сертифікатів, використовуйте їх для підключення і роботи з системою.

Я втратив файли секретних ключів

У випадку втрати файлів секретних ключів або сертифікатів слід звернутися до адміністратора системи «PINbank Online» за номером телефону, що вказаний у лівому нижньому кутку сторінки входу до системи, або до контакт-центру банку, для того щоб він призначив вам аварійний пароль, який знадобиться для процедури відновлення. Подальші дії є аналогічними до тих, що описані в розділі Я забув пароль до секретного ключа