Приватне акціонерне товариство
“Центр комп’ютерних технологій “ІнфоПлюс”

Україна, 02002, м. Київ, вул. Митрополита Андрея Шептицького, 4а, код ЄДРПОУ 16400836
+38 (044) 585 16 67 office@infoplus.com.ua

**ІНСТРУКЦІЯ**
**щодо реєстрації коду безпеки у застосунках**
**Google Authenticator, Microsoft Authenticator та DUO Mobile**

**Загальна інформація**

Якщо у системі електронного документообігу АСКОД (далі – СЕД АСКОД) ввімкнено двохфакторну авторизацію користувачу СЕД АСКОД у разі необхідності під час виконання входу у СЕД АСКОД виводиться інформаційне вікно “Отримання коду безпеки” (Рисунок 1).

Візуалізація інформаційного вікна “Отримання коду безпеки” користувачу необхідна у випадку, якщо після ввімкнення у СЕД АСКОД двохфакторної авторизації такий користувач виконує перший вхід у СЕД АСКОД.


**Рисунок 1 - Вікно інформування користувача щодо його індивідуального коду безпеки**

Користувач СЕД АСКОД під час візуалізації інформаційного вікна “Отримання коду безпеки”, не закриваючи такого вікна, повинен відкрити один із застосунків (Google Authenticator, Microsoft Authenticator, DUO Mobile), який буде ним використовуватись на мобільному пристрої для двохфакторної авторизації і зареєструвати отриманий через інформаційне вікно код безпеки у мобільному застосунку.

У випадку успішної реєстрації кода безпеки у мобільному застосунку, для облікового запису такого коду безпеки починає виконуватись кожні 30 секунд генерація тимчасового шестизначного коду. Користувачу потрібно ввести тимчасовий шестизначний код, який користувач бачить у мобільному застосунку (Google Authenticator, Microsoft Authenticator, DUO Mobile) к поле "Код". (Рисунок 1).

Користувач виконує введення тимчасового шестизначного коду і, якщо тимчасовий код є актуальним для коду безпеки користувача і поточного інтервалу часу, користувач успішно авторизується і виконується вхід такого користувача у СЕД АСКОД.

Якщо двохфакторну авторизацію (із використанням Google Authenticator або Microsoft Authenticator або DUO Mobile) ввімкнено у тестовому режимі, користувач може залишити поле для введення шестизначного коду порожнім і натиснути кнопку “Далі”.

Якщо двохфакторну авторизацію ввімкнено у робочому режимі введення шестизначного коду є обов`язковим, а невірний код викликає відповідне повідомлення, яке система надає користувачу, і вхід до СЕД АСКОД такому користувачу заборонений поки він не введе коректний шестизначний код.

Якщо користувач вводить підряд певну кількість разів невірний код СЕД АСКОД повертає користувача до вікна авторизації за першим фактором. Кількість дозволених введень невірного коду регулюється системними налаштуваннями СЕД АСКОД.

При повторній авторизації, користувачу не потрібно повторно реєструвати код безпеки у застосутку. Користувачу візуалізується поле введення коду (Рисунок 2).

Користувач виконує введення тимчасового шестизначного коду і, якщо тимчасовий код є актуальним для коду безпеки користувача і поточного інтервалу часу, користувач успішно авторизується і виконується вхід такого користувача у СЕД АСКОД.

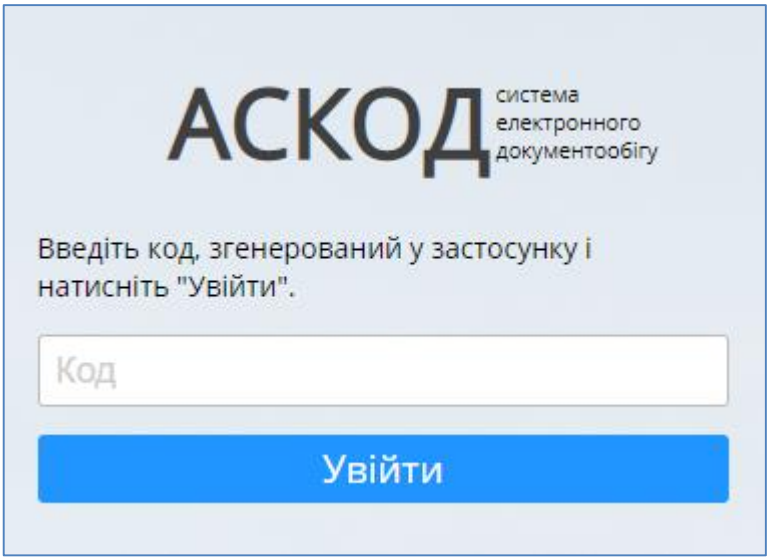


**Рисунок 2 - Вікно введення шестизначного тимчасового коду, отриманого у застосунку Google Authenticator або Microsoft Authenticator або DUO Mobile**

**Реєстрація коду безпеки у застосунку Google Authenticator**

Для реєстрації коду безпеки у застосунку Google Authenticator на мобільному пристрої слід відкрити застосунок і, якщо не було раніше зареєстровано жодного коду безпеки, натиснути кнопку “Почати” (Рисунок 3).


**Рисунок 3 - Початок роботи із застосунком Google Authenticator**

Після натискання кнопки “Почати” у новому вікні користувачу пропонується зареєструвати код безпеки одним з двох існуючих методів (Рисунок 4):

- Сканувати QR-код, який виведено у інформаційному вікні “Отримання коду безпеки” СЕД АСКОД (Рисунок 1);
- Або ввести ключ безпеки (ввести ключ налаштування), який отримано у інформаційному вікні “Отримання коду безпеки” СЕД АСКОД (Рисунок 1) через використання кнопки-ознаки візуалізації коду безпеки у явному вигляді.

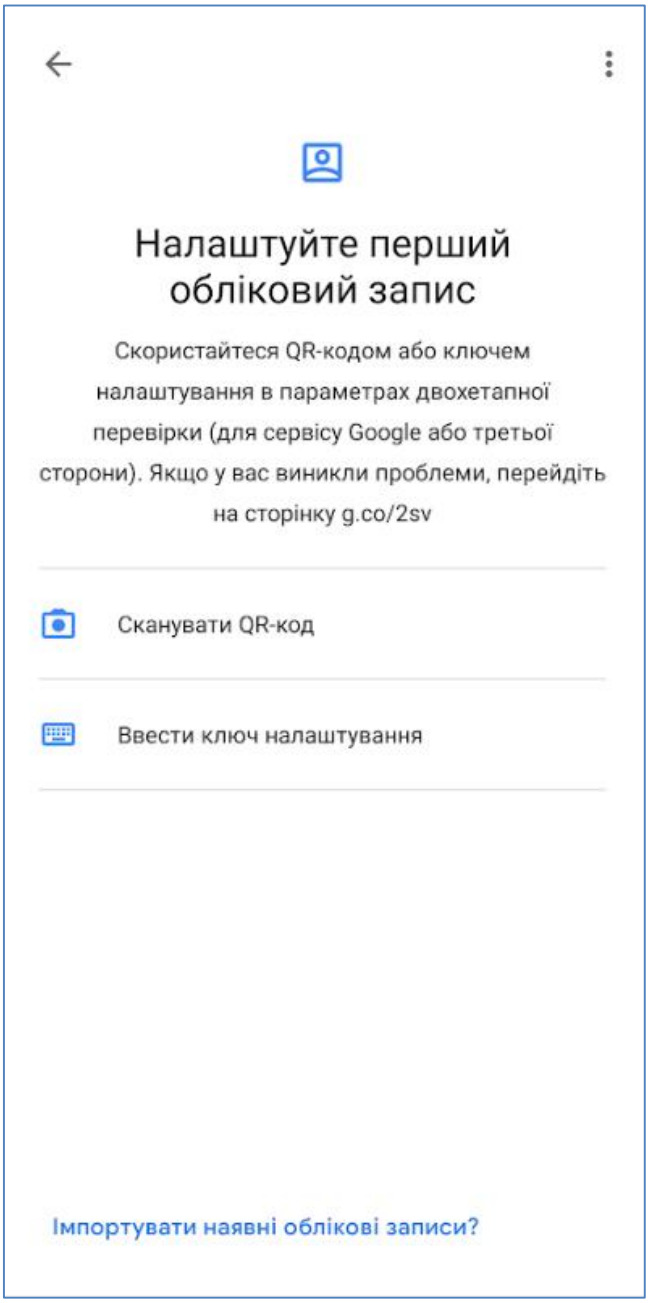


**Рисунок 4 - Вікно вибору методу реєстрації кода безпеки**

У випадку використання методу реєстрації коду безпеки через сканування QR-коду новий обліковий запис у застосунку Google Authenticator створюється автоматично, якщо таке сканування QR-коду успішно відбулось.

Якщо обрано другий метод реєстрації коду безпеки через пункт меню “Ввести ключ налаштування”, користувачу візуалізуються поля, до яких треба ввести необхідну для виконання реєстрації інформацію, а саме:

- Назва облікового запису (наприклад, АСКОД );
- Ваш ключ ( у це поле користувач повинен ввести вручну код безпеки, який він отримав у явному вигляді у інформаційному вікні);
- Тип ключа ( користувач повинен обрати значення “На основі часу”).

Після заповнення полів форми реєстрації облікового запису коду безпеки користувач для збереження таких даних і завершення процесу реєстрації повинен натиснути кнопку “Додати” (Рисунок 5).

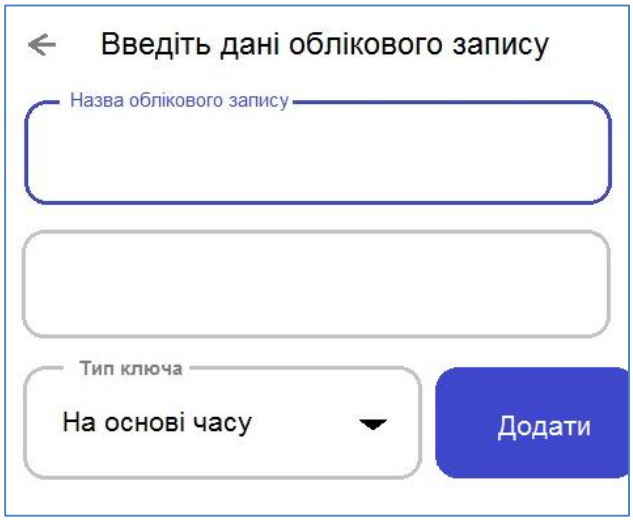


**Рисунок 5 - Вікно форми реєстрації облікового запису Google Authenticator**

Після реєстрації нового облікового запису коду безпеки у застосунку Google Authenticator для такого запису кожні 30 секунд генерується тимчасовий шестизначний код на базі коду безпеки користувача (Рисунок 6).

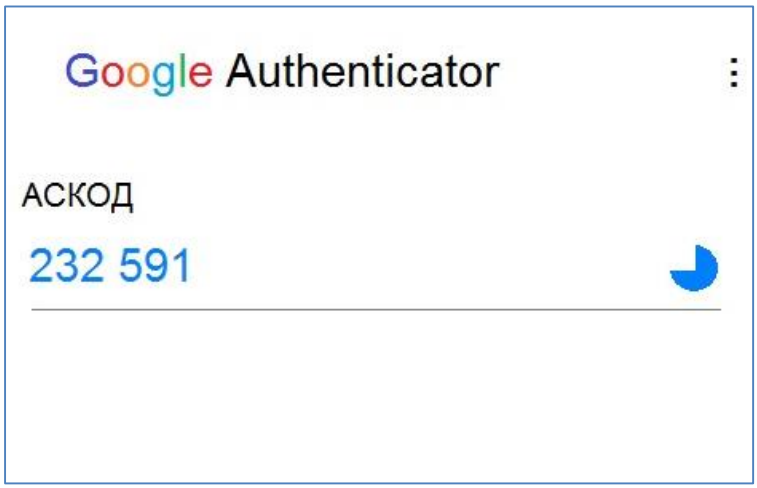


**Рисунок 6 - Тимчасовий шестизначний код візуалізується впродовж 30 секунд, за які колоподібний індикатор часу добігає до повного кола.**

Користувач виконує введення тимчасового шестизначного коду (Рисунок 1) і, якщо тимчасовий код є актуальним для коду безпеки користувача і поточного інтервалу часу, користувач успішно авторизується і виконується вхід такого користувача у СЕД АСКОД.

Якщо двохфакторну авторизацію із використанням Google Authenticator ввімкнено у тестовому режимі, користувач може залишити поле для введення шестизначного коду порожнім і натиснути кнопку “Далі”.

Якщо двохфакторну авторизацію ввімкнено у робочому режимі введення шестизначного коду є обов`язковим, а невірний код викликає відповідне повідомлення, яке система надає користувачу, і вхід до СЕД АСКОД такому користувачу заборонений поки він не введе коректний шестизначний код.

Якщо користувач вводить підряд певну кількість разів (наприклад, 5) невірний код СЕД АСКОД блокує обліковий запис такого користувача на певний період. Кількість дозволених введень невірного коду регулюється системними налаштуваннями СЕД АСКОД.

**Реєстрація коду безпеки у застосунку Microsoft Authenticator**

Для реєстрації коду безпеки у застосунку Microsoft Authenticator на мобільному пристрої слід відкрити застосунок і натиснути кнопку “Відсканувати QR-код” (Рисунок 7).

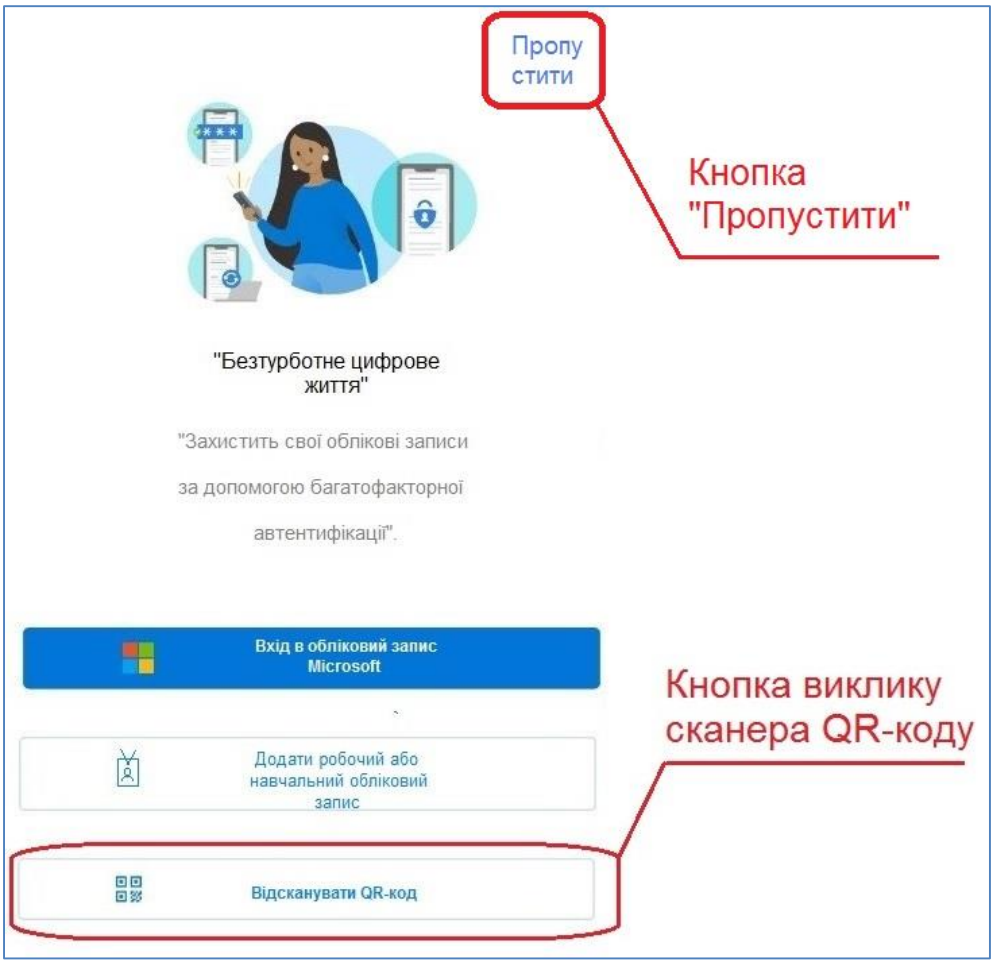


**Рисунок 7 - Кнопка “Відсканувати QR-код”**

Якщо користувач натиснув кнопку “Пропустити” (Рисунок 7), користувачу візуалізується вікно з кнопкою “Додати обліковий запис” (Рисунок 8).

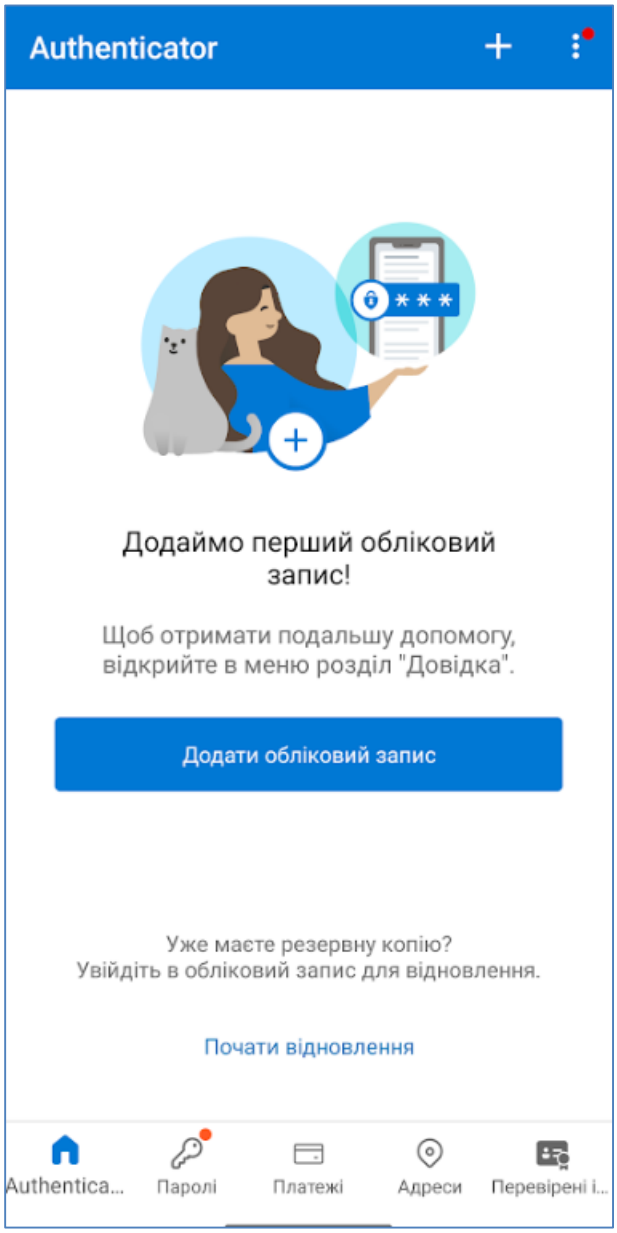


**Рисунок 8 - Кнопка “Додати обліковий запис”**

Якщо користувач натиснув кнопку “Відсканувати QR-код” (Рисунок 7), користувачу візуалізується вікно сканера QR-кодів (Рисунок 9).

За допомогою вікна сканера користувач має змогу зчитати QR-код з інформаційного вікна “Отримання коду безпеки” (Рисунок 1).

Якщо QR-код зчитано успішно, обліковий запис реєстрації коду безпеки у застосунку Microsoft Authenticator створюється автоматично.

Вікно сканування QR-кодів має пропозицію введення кода безпеки вручну (Рисунок 9). Такий варіант реєстрації коду безпеки користувач може задіяти у випадку, якщо, наприклад, QR-код з інформаційного вікна (Рисунок 1) не зчитується.

У випадку неможливості зчитати QR-код користувач може отримати код безпеки у явному вигляді у інформаційному вікні “Отримання коду безпеки” СЕД АСКОД через використання кнопки-ознаки візуалізації коду безпеки у явному вигляді і ввести отриманий код на формі реєстрації нового облікового запису (Рисунок 10).

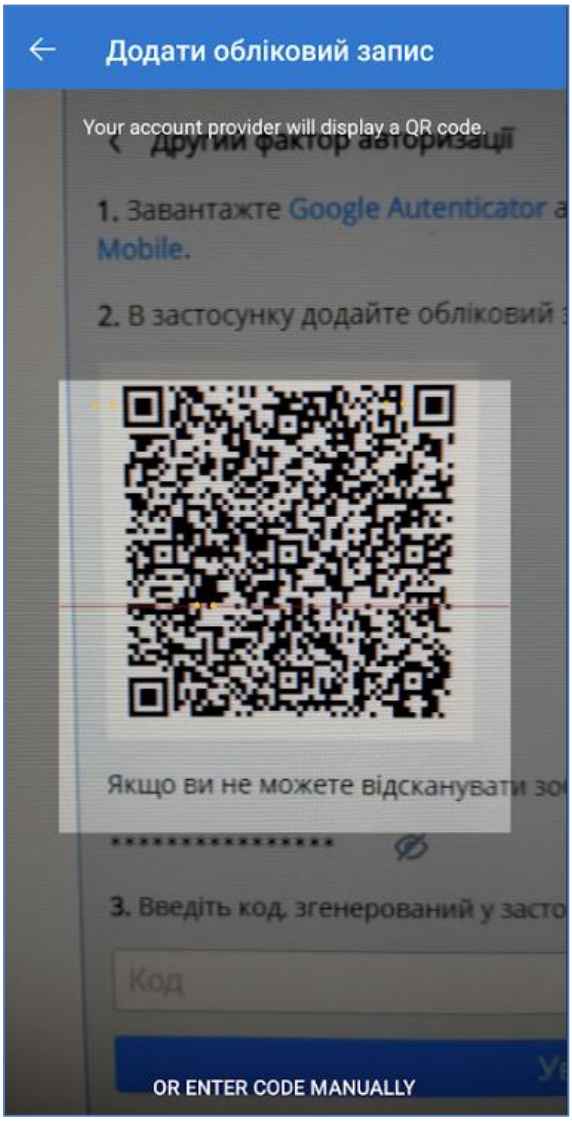


**Рисунок 9 - Вікно сканера QR-кодів**

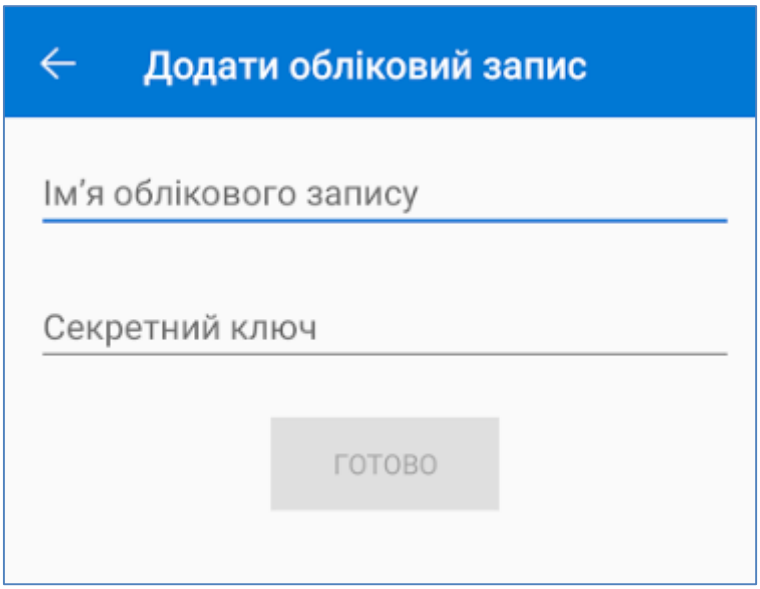


**Рисунок 10 - Вікно форми реєстрації коду безпеки у Microsoft Authenticator**

На формі (Рисунок 10) користувачу візуалізуються поля, до яких треба ввести необхідну для виконання реєстрації інформацію, а саме:

- Ім’я облікового запису (наприклад, АСКОД );
- Секретний ключ ( у це поле користувач  повинен ввести вручну код безпеки, який він отримав у явному вигляді у інформаційному вікні).

Після заповнення полів форми реєстрації облікового запису коду безпеки користувач для збереження таких даних і завершення процесу реєстрації повинен натиснути кнопку “ГОТОВО”.

Процес реєстрації коду безпеки завершено.

Якщо користувач розпочав процес реєстрації з вікна Microsoft Authenticator, яке наведено на Рисунок 8 і натиснув кнопку “Додати обліковий запис”, такому користувачу відкривається вікно для вибору типу облікового запису (Рисунок 11).

Для реєстрації  кода безпеки, який сгенеровано у СЕД АСКОД, користувач повинен обрати пункт “Інший обліковий запис (Google, Facebook тощо)”, після чого відкриється вікно сканера QR-коду (Рисунок 9).

Надалі користувач виконує реєстрацію шляхом сканування QR-коду або ручного введення коду безпеки.

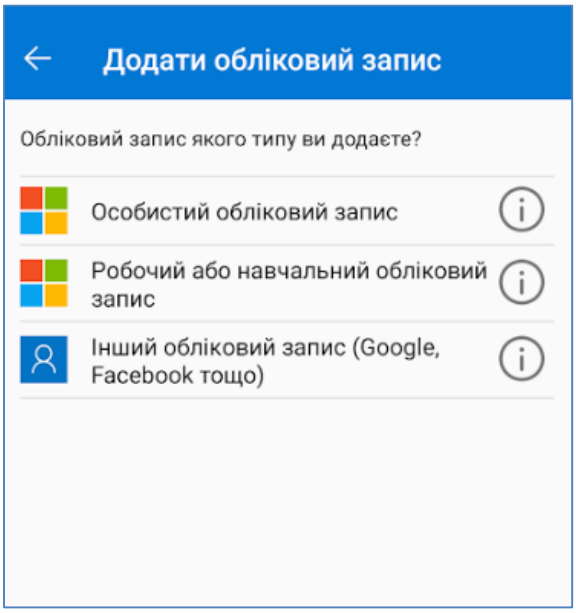


**Рисунок 11 - Вибір типу облікового запису.**

Після реєстрації коду безпеки коду безпеки у застосунку Microsoft Authenticator такий з`являється новий запис у переліку облікових записів (Рисунок 12).

Для такого запису кожні 30 секунд генерується тимчасовий шестизначний код на базі коду безпеки користувача (Рисунок 13).

Користувач виконує введення тимчасового шестизначного коду і, якщо тимчасовий код є актуальним для коду безпеки користувача і поточного інтервалу часу, користувач успішно авторизується і виконується вхід такого користувача у СЕД АСКОД.

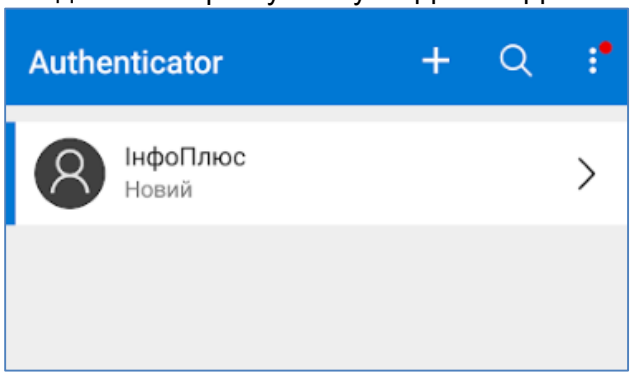


**Рисунок 12 - Перелік облікових записів Microsoft Authenticator**

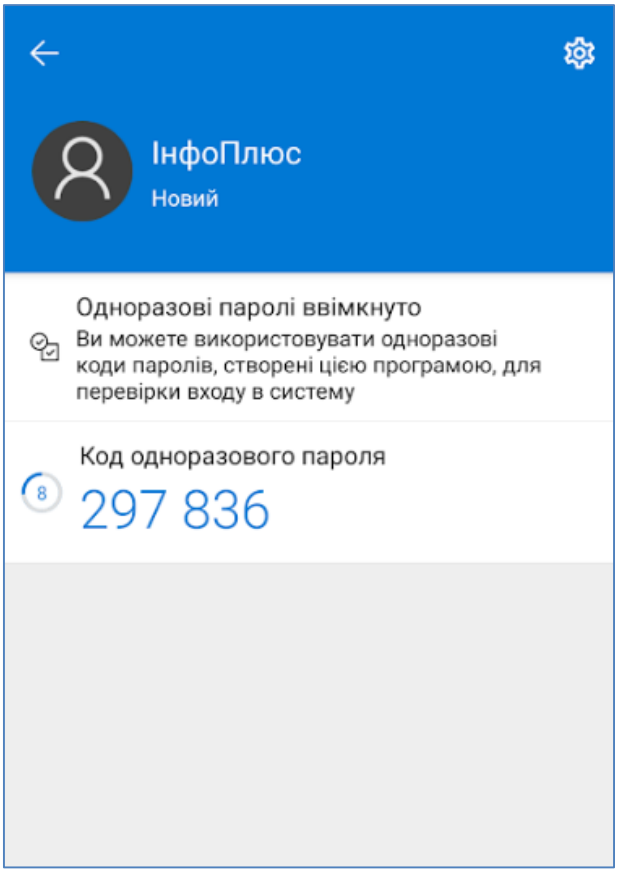


**Рисунок 13 - Кожні 30 секунд генерується тимчасовий шестизначний код**

Якщо двохфакторну авторизацію із використанням Microsoft Authenticator ввімкнено у тестовому режимі, користувач може залишити поле для введення шестизначного коду порожнім і натиснути кнопку “Далі”.

Якщо двохфакторну авторизацію ввімкнено у робочому режимі введення шестизначного коду є обов`язковим, а невірний код викликає відповідне повідомлення, яке система надає користувачу, і вхід до СЕД АСКОД такому користувачу заборонений поки він не введе коректний шестизначний код.

Якщо користувач вводить підряд певну кількість разів (наприклад, 5) невірний код СЕД АСКОД блокує обліковий запис такого користувача на певний період. Кількість дозволених введень невірного коду регулюється системними налаштуваннями СЕД АСКОД.

**Реєстрація коду безпеки у застосунку DUO Mobile**

Для реєстрації коду безпеки у застосунку DUO Mobile на мобільному пристрої слід відкрити застосунок і натиснути кнопку “+ Add” (Рисунок 14).

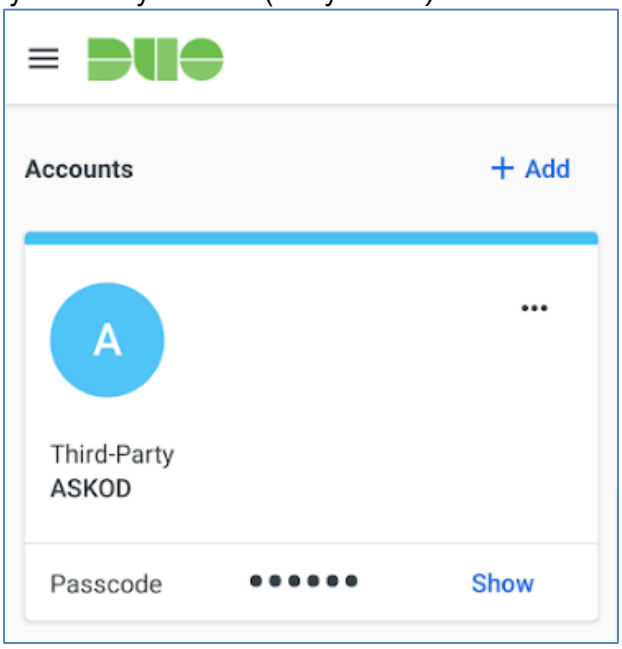


**Рисунок 14 - Кнопка “+ Add”, яка використовується для додавання нового коду безпеки АСКОД до переліку кодів безпеки застосунку DUO Mobile**

Після натискання кнопки “+ Add” відкривається вікно “Add account” (Рисунок 15), в якому є можливість виконати виклик зчитувача QR-коду (кнопка “Use QR code”) для автоматичного зчитування коду безпеки, згенерованого у системі АСКОД і який візуалізується під час авторизації до системи АСКОД (Рисунок 1) у тому випадку, якщо для користувача код безпеки ще не визначався раніше або такий код було очищено адміністратором системи.

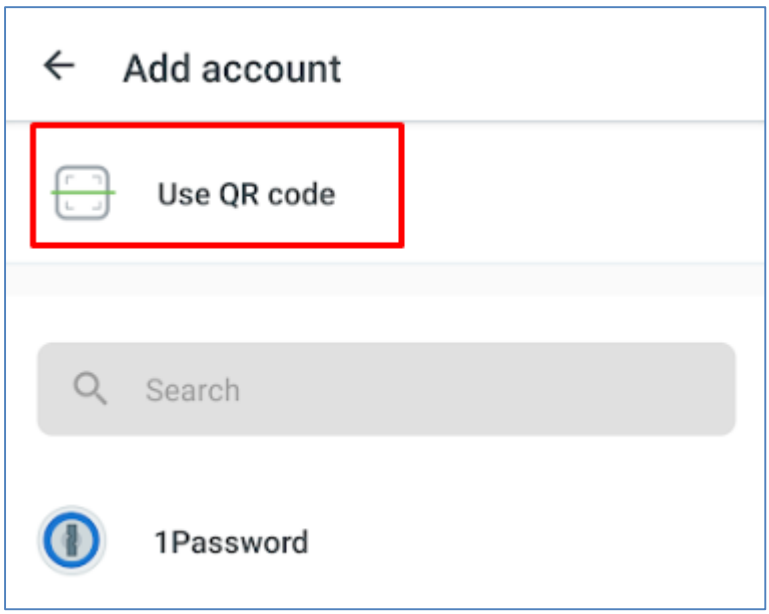


**Рисунок 15 - Кнопка “Use QR code”**

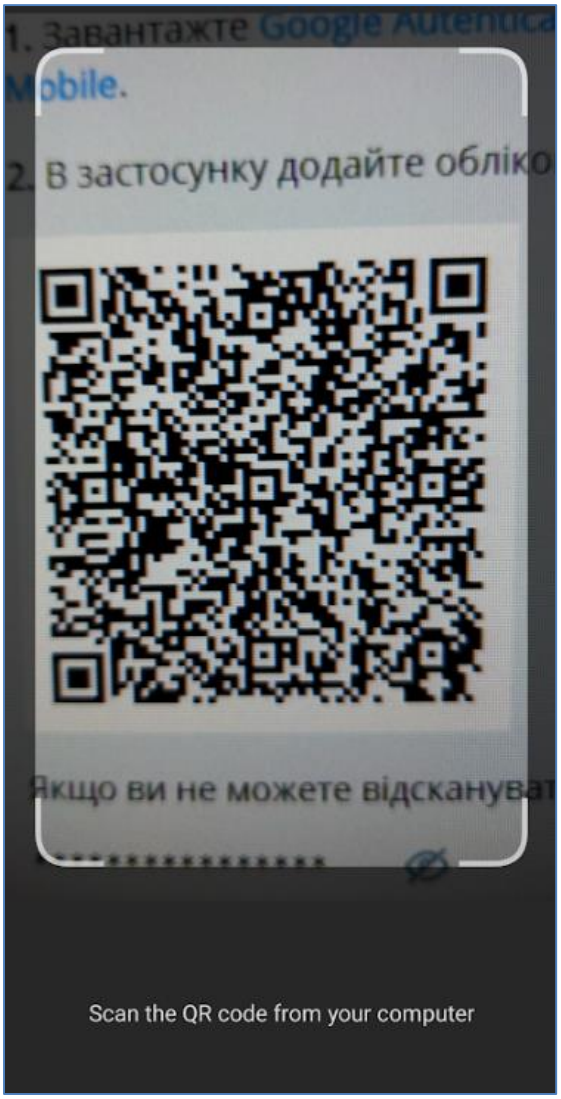


**Рисунок 16 - Сканер QR-коду**

Після успішного зчитування QR-коду для згенерованого коду безпеки АСКОД створюється новий обліковий запис (account) у переліку акаунтів застосунку DUO Mobile (Мал.16).

У вікні інформації нового акаунту DUO Mobile, який створено для коду безпеки АСКОД, необхідно виконати збереження такого акаунту кнопкою “Save” (Рисунок 17).

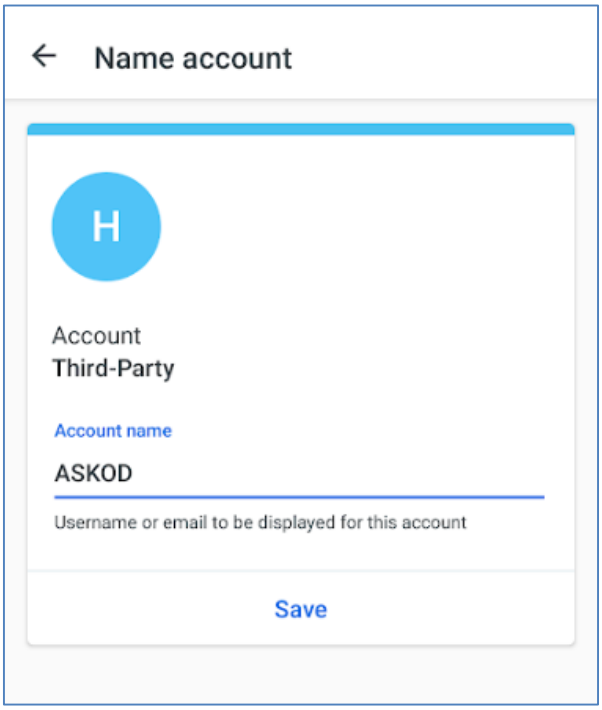


**Рисунок 17 - Вікно збереження інформації нового аккаунту DUO Mobile, який створено для коду безпеки АСКОД**

Після збереження нового акаунту коду безпеки АСКОД такий акаунт активується і для такого акаунту починається циклічна генерація шестизначних кодів, які змінюються кожні 30 секунд (Рисунок 18).

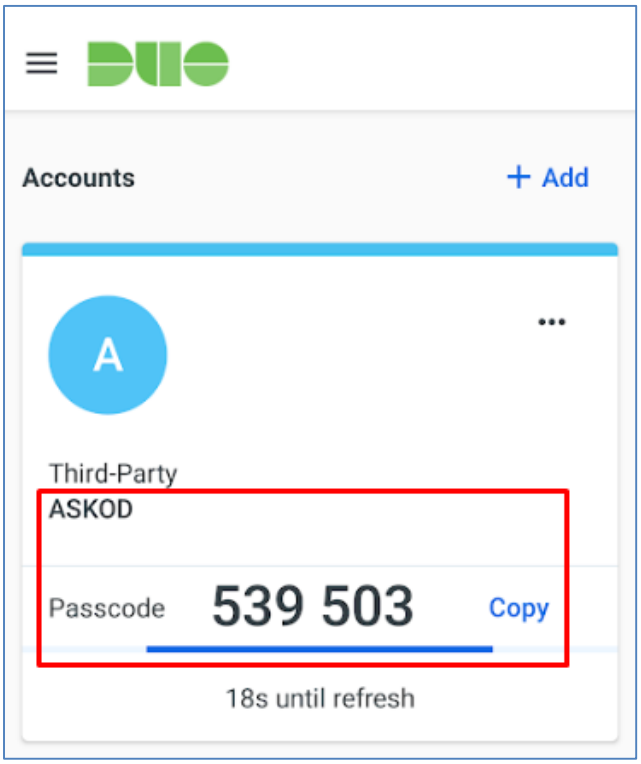


**Рисунок 18 - Циклічна генерація шестизначних кодів для акаунту коду безпеки АСКОД**