УКРАЇНА
ДНІПРОВСЬКА РАЙОННА В МІСТІ КИЄВІ ДЕРЖАВНА АДМІНІСТРАЦІЯ
УПРАВЛІННЯ ОСВІТИ
проспект Миру, 6-А, м. Київ, 02105, тел/факс: (044) 332-46-70,
E-mail: dniprosvita@kmda.gov.ua, сайт: www.uosvitydnr.gov.ua, код згідно з ЄДРПОУ 37397216

15.04.2025 № 103/44-1071
На № _____ **від** _____

Керівникам закладів освіти
Дніпровського району

Управління освіти Дніпровської районної в місті Києві державної адміністрації на виконання листа Департаменту інформаційно-комунікаційних технологій виконавчого органу Київської міської ради (Київської міської державної адміністрації) від 10.04.2025 № 075-837 надсилає пам'ятку щодо посилення безпекових заходів під час використання месенджерів (на прикладі месенджера Signal) для використання у роботі.

Додаток: на 4 арк.

Заступник начальника Галина ТОДОСОВА

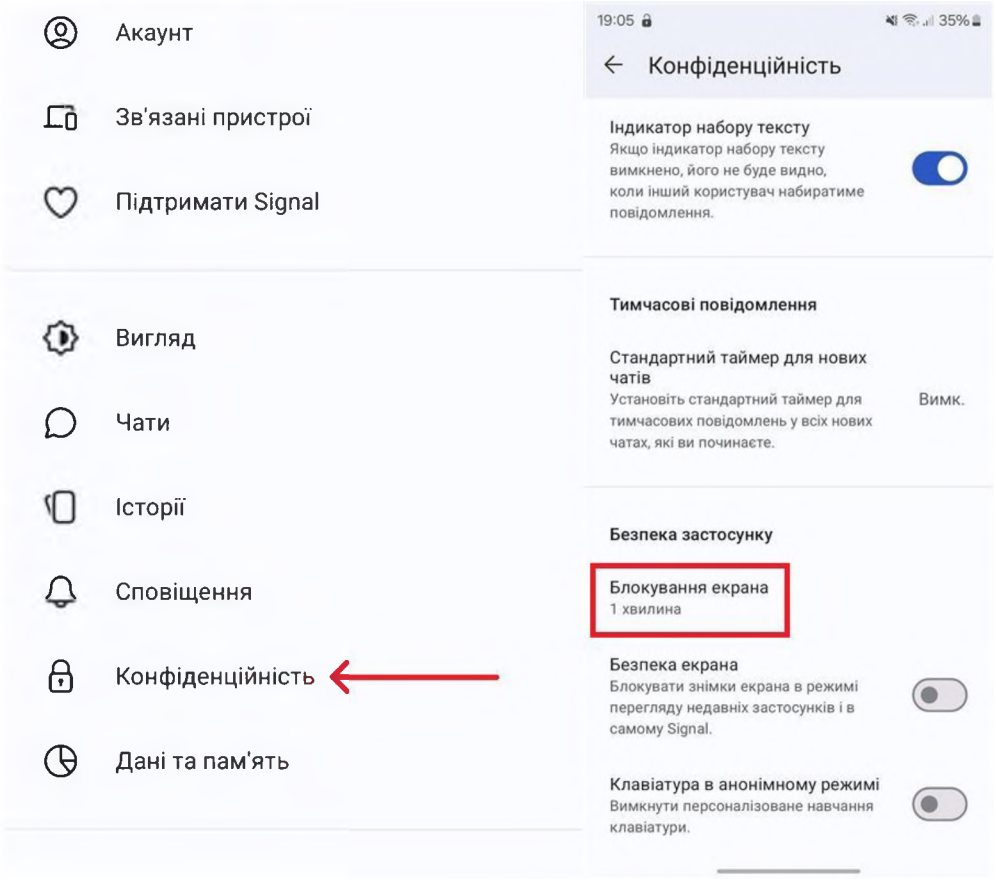
Дмитро Павлігин 093-99-444-99

Додаток 1

Пам’ятка щодо посилення безпекових заходів під час використання месенджерів. На прикладі месенджеру Signal.

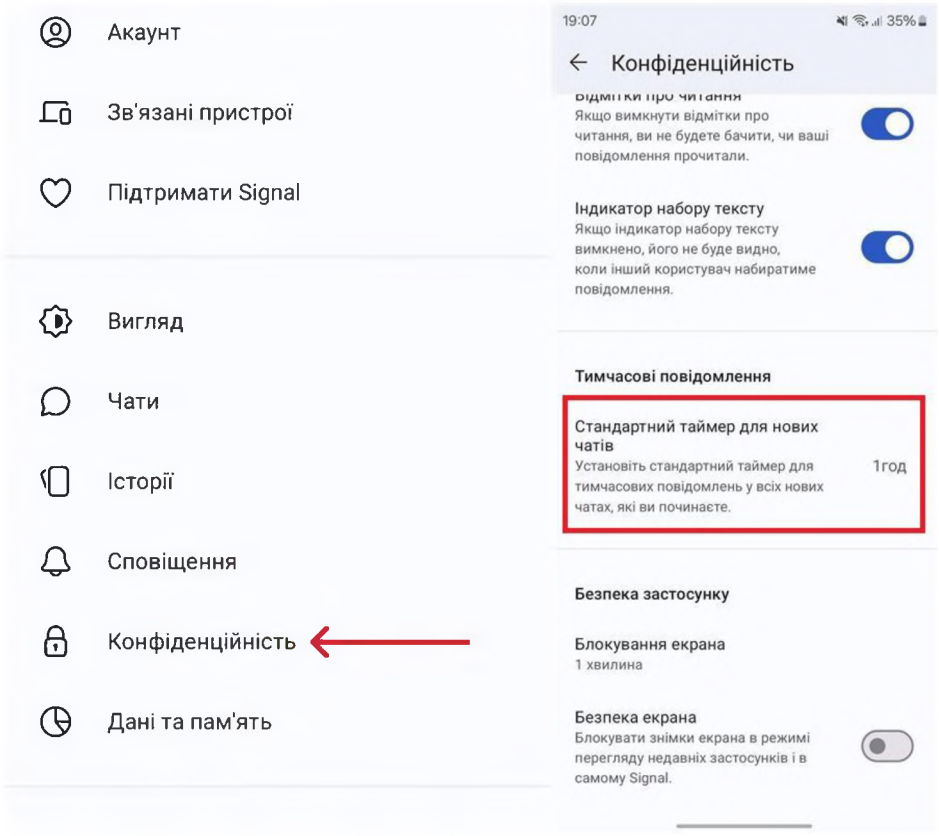
1. **Не додавати невідомих та неперевірених контактів.** Не приймати і не довіряти незнайомим контактам, їх потрібно відразу блокувати. При цілеспрямованих атаках проти конкретних керівників та офіцерів – зловмисники проводять деталізований збір інформації та мають достатньо контактів знайомих і друзів, прикидаючись якими, просять вчинити певні дії.
2. **Не завантажувати та не запускати файли від невідомих осіб.** Найпопулярнішим способом є злом через комп'ютерну версію Signal – через надсилання документу Word / Excel або інших файлів у архіві. При відкритті зараженого файлу, зловмисники зможуть приховано стежити за екраном, робити скріншоти, перехоплювати натискання клавіш на клавіатурі, викрасти сесію комп'ютерної версії Signal та приховано стежити за повідомленнями в обліковому записі та групах.
3. **Не сканувати QR-коди відправлені невідомими особами як «запрошення» до групи або чату**.
4. Ввімкнути розблокування Signal PIN-кодом або через розпізнавання обличчя / пальців. **Налаштування → Конфіденційність → Блокування екрана**

   (рекомендовані налаштування та кроки виділені червоним)



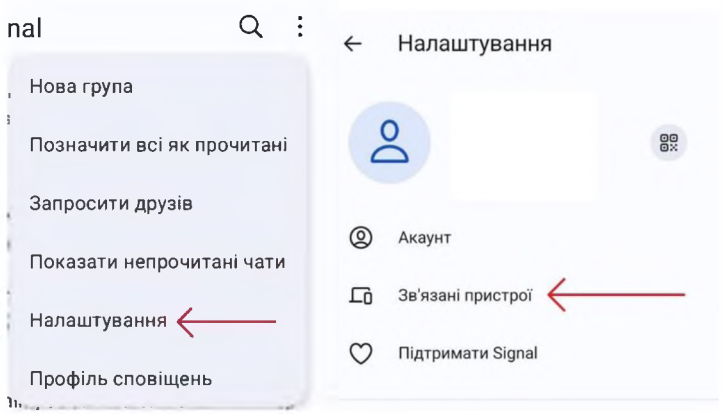
5. Налаштувати видалення повідомлень за годину або один день, залежно від ваших потреб. Для обмеження інформації, яку можуть отримати зловмисники при компрометації. **Налаштування → Конфіденційність → Стандартний таймер для нових чатів**

   (рекомендовані налаштування та кроки виділені червоним)



6. Перевіряти підключені пристрої. **Налаштування → Зв’язані пристрої**.

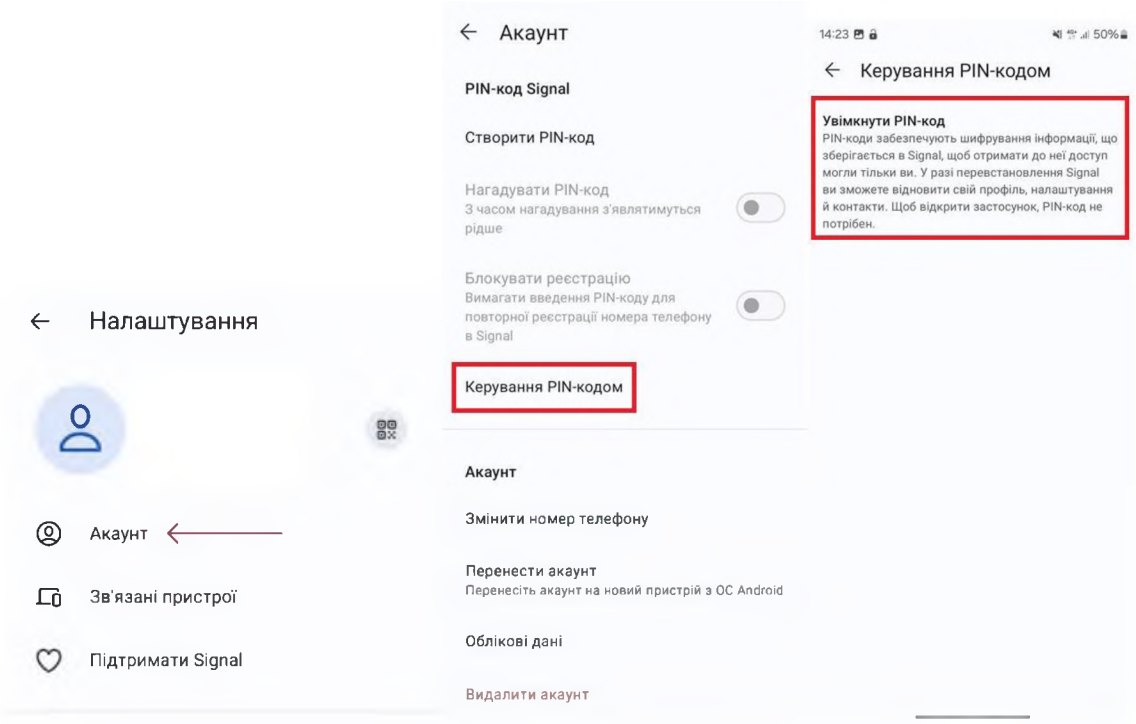
   (рекомендовані налаштування та кроки виділені червоним)



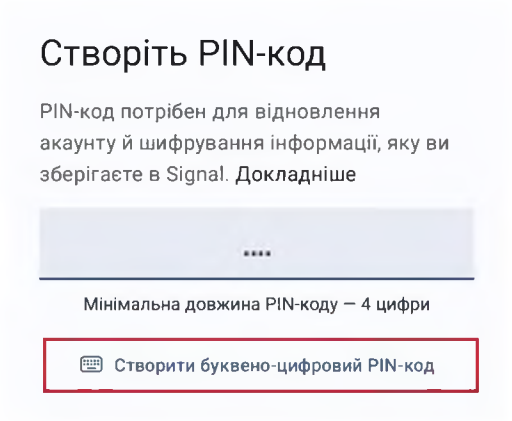
7. У випадку використання месенджерів на ПК, обов'язково ввімкнути/встановити антивірусний захист на Windows / Linux / MacOS .

8. Зайти в налаштування Signal та активувати PIN. **Налаштування → Акаунт → Керування PIN-кодом → Увімкнути PIN-код**.

   (рекомендовані налаштування та кроки виділені червоним)

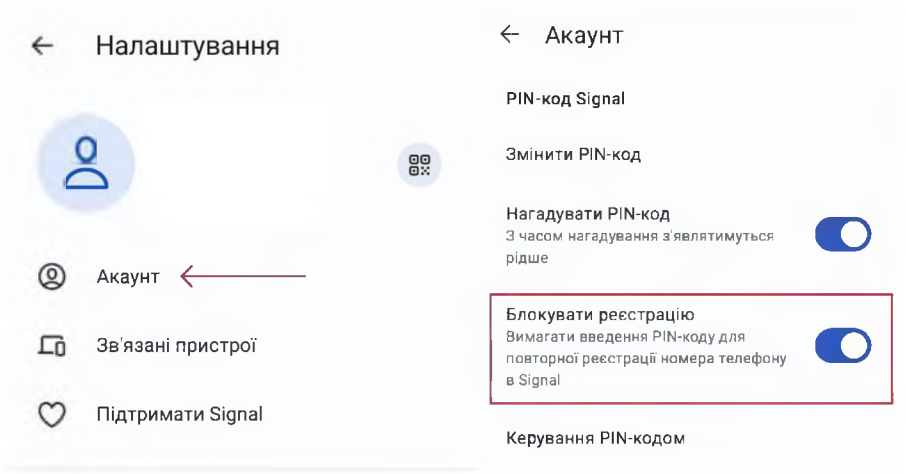


Для підвищеної безпеки **рекомендовано** використовувати буквено-цифровий PIN-код.



9. Для захисту від атаки з отриманням доступу до вашого номеру телефону (наприклад, через шахрайство з перенесенням SIM-карти) рекомендовано увімкнути функцію **Блокувати реєстрацію**. **Налаштування → Акаунт → Блокувати реєстрацію**.’

   (рекомендовані налаштування та кроки виділені червоним)


Налаштування
Акаунт
Зв'язані пристрої
Підтримати Signal
Акаунт
PIN-код Signal
Змінити PIN-код
Нагадувати PIN-код
З часом нагадування з'являтимуться рідше
Блокувати реєстрацію
Вимагати введення PIN-коду для повторної реєстрації номера телефону в Signal
Керування PIN-кодом