

Порядок

підключення до системи обміну повідомленнями спільноти
CSIRT-NBU Центру кіберзахисту Національного банку
України

версія 1.0



1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1 Порядок підключення до системи обміну повідомленнями спільноти CSIRT-NBU Центру Кіберзахисту Національного банку України (далі – Порядок) розроблений відповідно до вимог Порядку інформаційного обміну між банками України і Центром кіберзахисту Національного банку України з питань кіберзахисту в банківській системі України, що опубліковано у розділі "Нормативні документи" Порталу Центру кіберзахисту Національного банку України.

1.2 Порядок визначає процедуру підключення до системи обміну повідомленнями спільноти CSIRT-NBU Центру Кіберзахисту Національного банку України з урахуванням вимог конфіденційності, що зазначені у Порядку інформаційного обміну між банками України і Центром кіберзахисту Національного банку України з питань кіберзахисту в банківській системі України.

1.3 Терміни та скорочення в цьому Порядку вживаються в такому значенні:

адміністратор системи обміну повідомленнями – уповноважений представник Центру кіберзахисту, який відповідає за адміністрування спільноти CSIRT-NBU (облікові записи користувачів організації, канали обміну повідомленнями, тощо);

відповідальна особа організації – уповноважений представник банку, який відповідає за взаємодію із Центром кіберзахисту з організаційних питань;

користувач організації – уповноважений представник банку якому надано доступ до системи обміну повідомленнями спільноти CSIRT-NBU Центру кіберзахисту Національного банку України;

система обміну повідомленнями спільноти CSIRT-NBU (далі – система обміну повідомленнями) – спеціальна система для обміну інформаційними повідомленнями між учасниками інформаційного обміну, що створена на основі вільної системи обміну повідомленнями Mattermost, що розгорнута та функціонує на ресурсах Національного банку України, яка дозволяє отримувати і відправляти повідомлення, файли і зображення, відстежувати історію переговорів і отримувати повідомлення на смартфоні або персональному комп'ютері.

1.4 Користувачі організації підключаються до системи обміну повідомленнями відповідно до умов цього Порядку.

1.5 Для обміну повідомленнями між банками та Центром кіберзахисту створюються спеціальні канали обміну:

- приватні канали організації - призначені для обміну інформацією технічного характеру, доступний лише для користувачів організації та представників Центру кіберзахисту Національного банку України;

- загальний канал спільноти CSIRT-NBU: Town Square – для обміну повідомленнями загальноорганізаційного характеру, доступний для всіх користувачів спільноти.

1.6 Додавання та видалення користувачів організації здійснюється адміністратором системи обміну повідомленнями за погодженням відповідальної особи організації.

2. ПІДКЛЮЧЕННЯ КОРИСТУВАЧІВ ДО СИСТЕМИ ОБМІНУ ПОВІДОМЛЕННЯМИ

2.1. Для підключення користувачів організації до системи обміну повідомленнями відповідальна особа організації надсилає перелік користувачів, яким буде надано доступ, на електронну адресу: CSIRT-NBU@bank.gov.ua.

2.2. Представник Центру кіберзахисту надсилає запрошення на електронні адреси визначених користувачів організації у вигляді спеціального посилання для реєстрації: [https://mattermost.bank.gov.ua/\[param\]](https://mattermost.bank.gov.ua/[param]).

2.3. Для приєднання до системи обміну повідомленнями користувачу необхідно перейти за отриманим посиланням на сторінку реєстрації (рис. 1) та обрати спосіб реєстрації:

- за допомогою браузеру;

- за допомогою застосунку, який необхідно додатково завантажити на персональний комп'ютер або смартфон за вказаним на сторінці посиланням: <https://mattermost.com/download/#mattermostApps>.

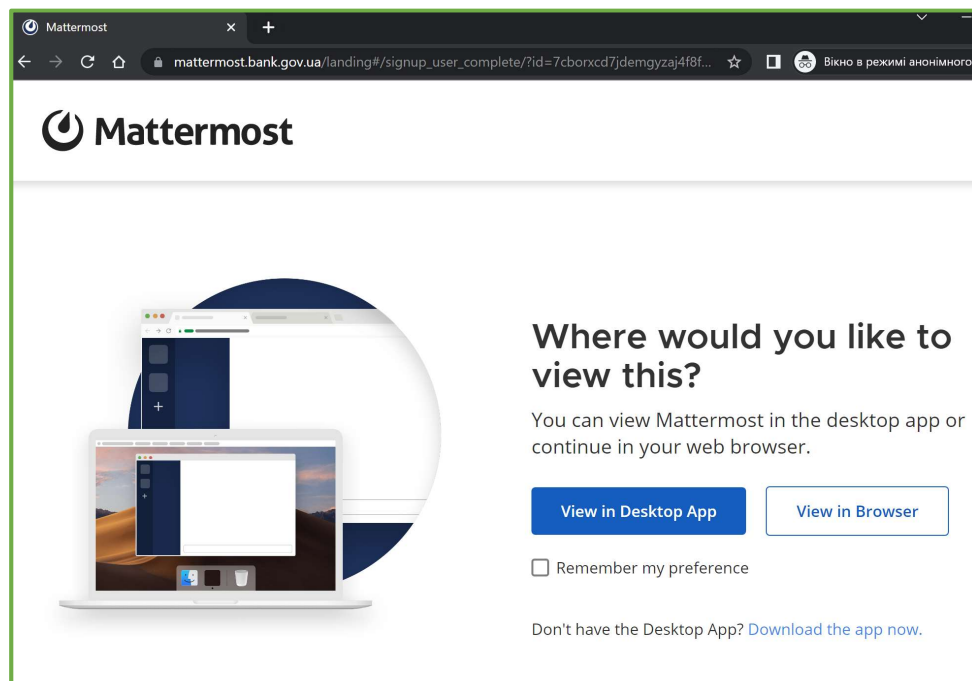


Рис.1 Початкова сторінка реєстрації

2.4. На наступному кроці реєстрації (рис.2) користувачу необхідно ввести:

- адресу корпоративної електронної пошти організації;

- username – доступно для використання такі символи: маленькі літери, цифри, крапка, тире та символ підкреслення;

- пароль – довжина від 12 до 64 символів, має містити принаймні одну маленьку літеру, одну велику літеру, одну цифру, один спеціальний символ.

Рис.2 Введення реєстраційних даних

Після введення всі даних необхідно натиснути на кнопку "Створити акаунт". Для завершення реєстрації необхідно підтвердити свій адрес електронної пошти (рис. 3) та тільки після цього користувачу буде доступна можливість для авторизації в системі обміну повідомленнями.

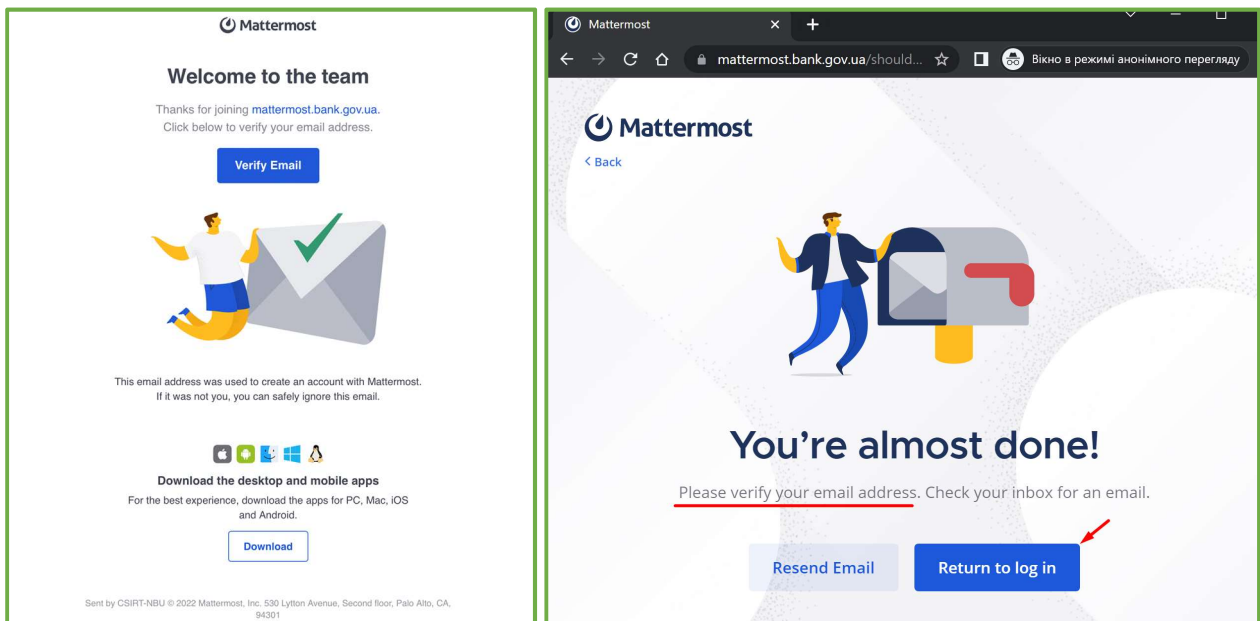


Рис.3 Підтвердження email адреси

В результаті вдалої авторизації відбудеться переадресація на головну сторінку спільноти CSIRT-NBU Mattermost (рис.4)

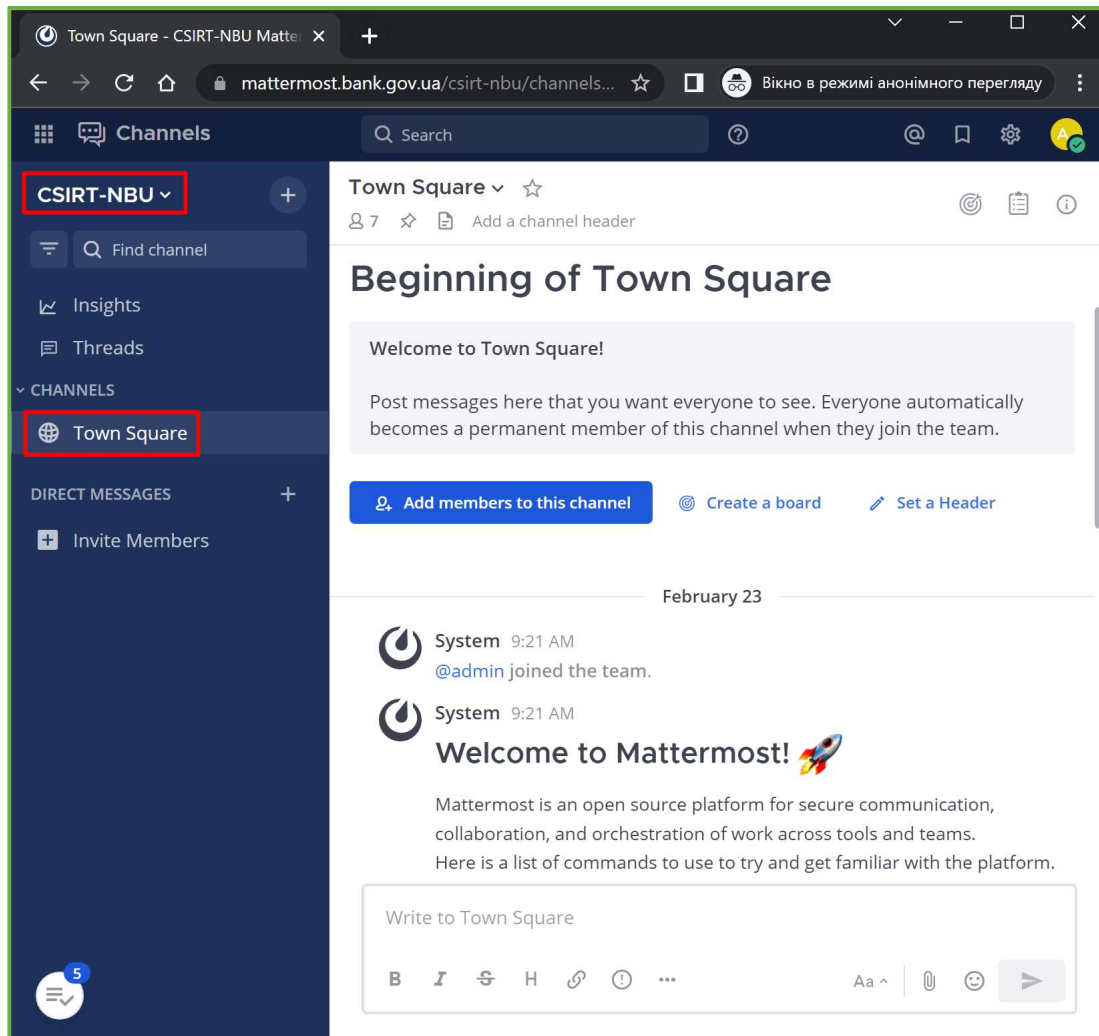


Рис.4 Головна сторінка спільноти CSIRT-NBU Mattermost

2.5. Відразу після реєстрації та приєднання до спільноти CSIRT-NBU Mattermost користувачу організації буде доступний для обміну повідомленнями загальний для всіх користувачів спільноти канал "Town Square".

2.6. Необхідною умовою завершення реєстрації для всіх користувачів є обов'язкове заповнення всіх полів свого профілю та налаштування параметрів безпеки (рис. 5). Лише після виконання цієї умови користувач організації буде доданий до приватного каналу організації.

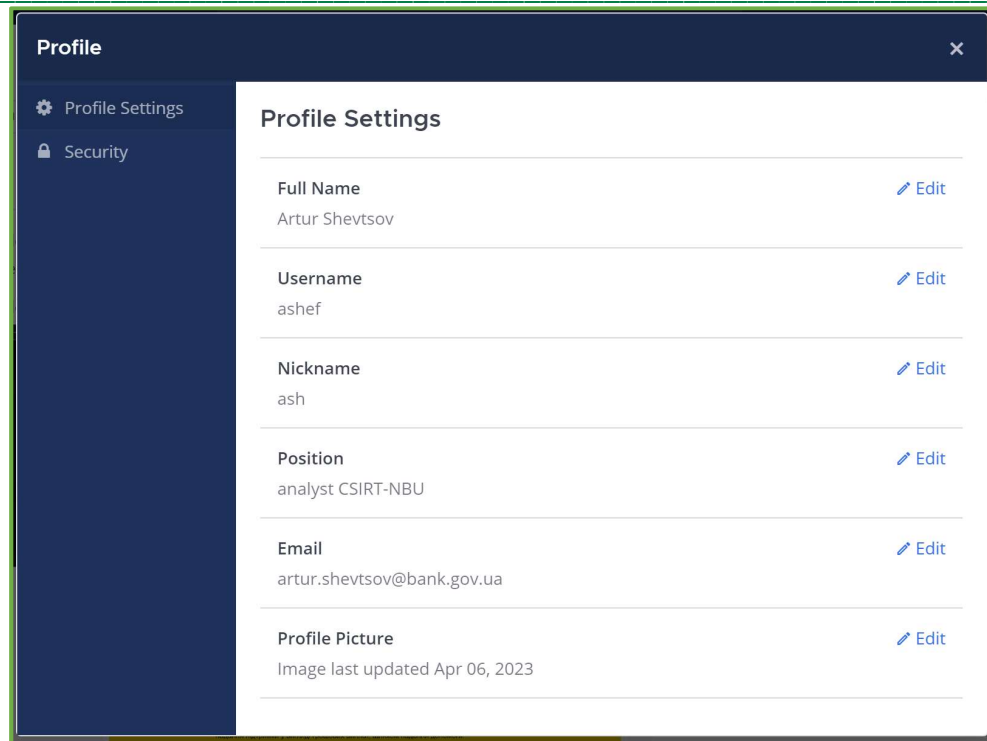


Рис.5 Профіль користувача

3. ПРОФІЛЬ КОРИСТУВАЧА, НАЛАШТУВАННЯ БЕЗПЕКИ ТА СПОВІЩЕНЬ СИСТЕМИ ОБМІНУ ПОВІДОМЛЕННЯМИ

3.1. Всі користувачі після першого входу в систему обміну повідомленнями спільноти CSIRT-NBU Mattermost повинні обов'язково заповнити "Профіль користувача системи" (рис.5) та включити двофакторну автентифікацію для входу до системи (рис.6).

3.2. Заповнення полів профілю користувача:

- обов'язкове для заповнення поле "Full Name" – повинно містити Прізвище та Ім'я користувача, буде відображатись при обміні повідомленнями в каналах спільноти;

- обов'язкове для заповнення поле "Username" – унікальне для всіх користувачів системи та заповнюється при реєстрації, доступне для подальшого редагування;

- необов'язкове для заповнення поле "Nickname" – заповнюється за бажанням користувача;

- обов'язкове для заповнення поле "Position" – вказується посада користувача організації, буде відображатись при обміні повідомленнями в каналах спільноти;

- обов'язкове для заповнення поле "Email" – заповнюється при реєстрації та доступне для подальшого редагування, не буде відображатись при обміні повідомленнями в каналах спільноти;

- необов'язкове для заповнення поле "Profile Picture" – додається за бажанням користувача.

3.3. Налаштування безпеки користувача системи обміну повідомленнями (рис. 6):

- поле "Password" – заповнюється при реєстрації та доступне для подальшої зміни паролю користувача;

- опція "Multi-factor Authentication" – обов'язково необхідно активувати опцію двофакторної автентифікації із використанням мобільного додатку Google Authenticator (рис.7 та рис.8).

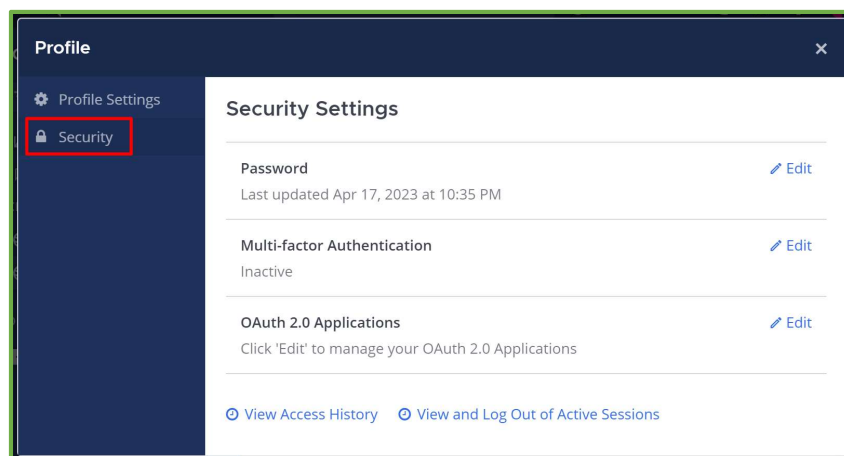


Рис.6 Налаштування безпеки

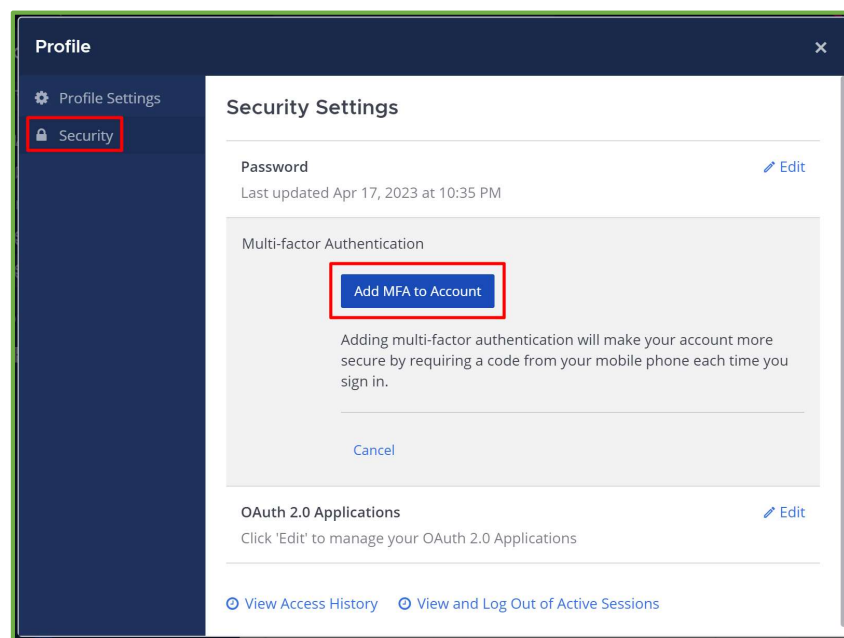


Рис.7 Налаштування двофакторної автентифікації

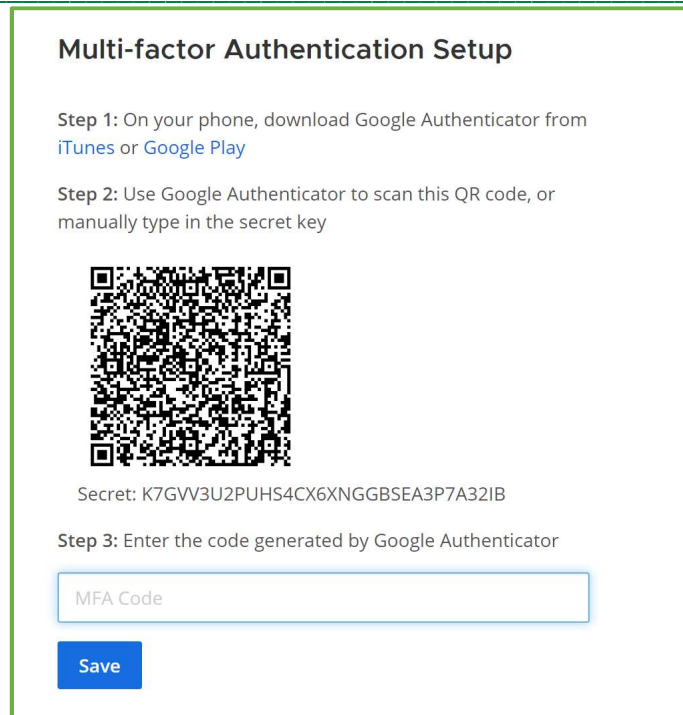


Рис.8 Налаштування Google Authenticator

3.4. Налаштування сповіщень системи обміну повідомленнями здійснюється в меню "Settings" (рис.9). Доступна можливість налаштувати (включати або виключати) сповіщення про нові повідомлення на вказану в профілі користувача адресу електронної пошти та push-сповіщення на мобільний або десктопний застосунок.

За замовчуванням активовані push-сповіщення та email-сповіщення лише для нових повідомлень в Direct Messages. Для отримання push-сповіщень або email-сповіщень про нові повідомлення в усіх доступних приватних та загальних каналах необхідно активувати відповідну опцію "For all activity" (рис. 10).

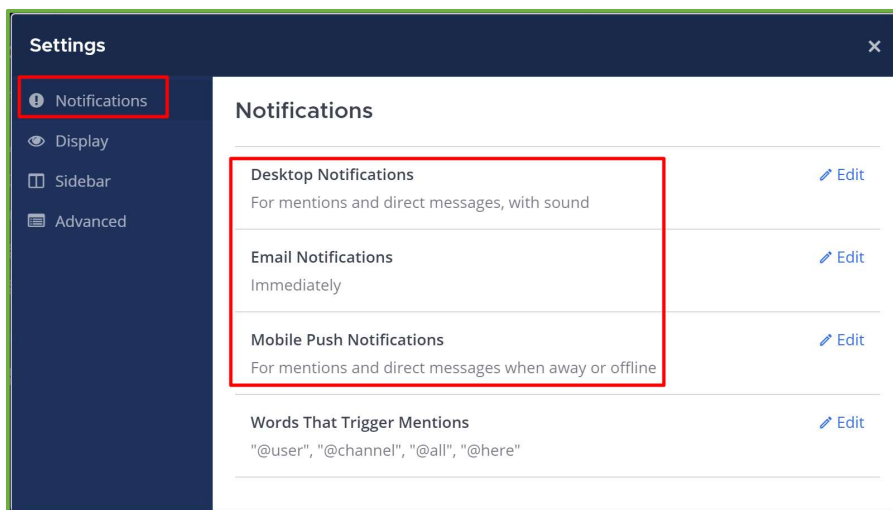


Рис.9 Налаштування сповіщень

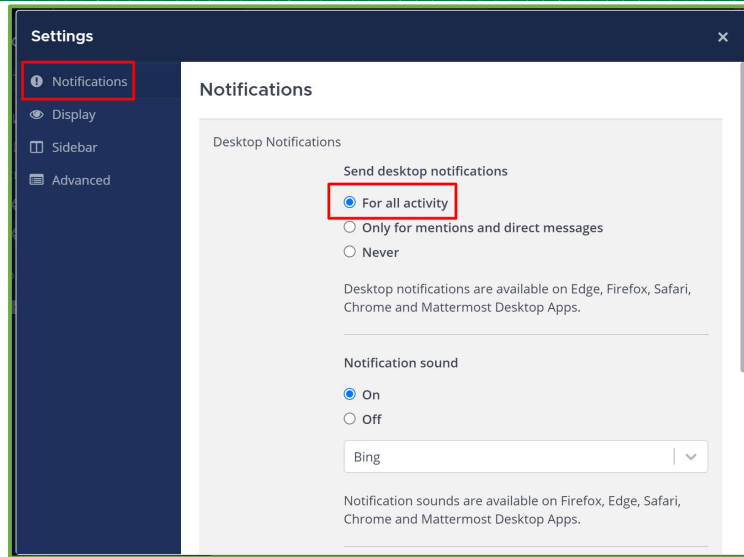


Рис.10 Налаштування сповіщень для всіх нових повідомлень

3.5. Всі користувачі системи обміну повідомленнями мають однакову роль та права по створенню, надсиланню, редагуванню, видаленню повідомлень (рис. 11).

Всім користувачам спільноти доступні для обміну повідомленнями канали:

- приватні канали організації – призначені для обміну інформацією технічного характеру, мають доступ лише користувачі організації та представники Центру кіберзахисту Національного банку України;

- загальний канал спільноти CSIRT-NBU: Town Square – для обміну повідомленнями загальноорганізаційного характеру.

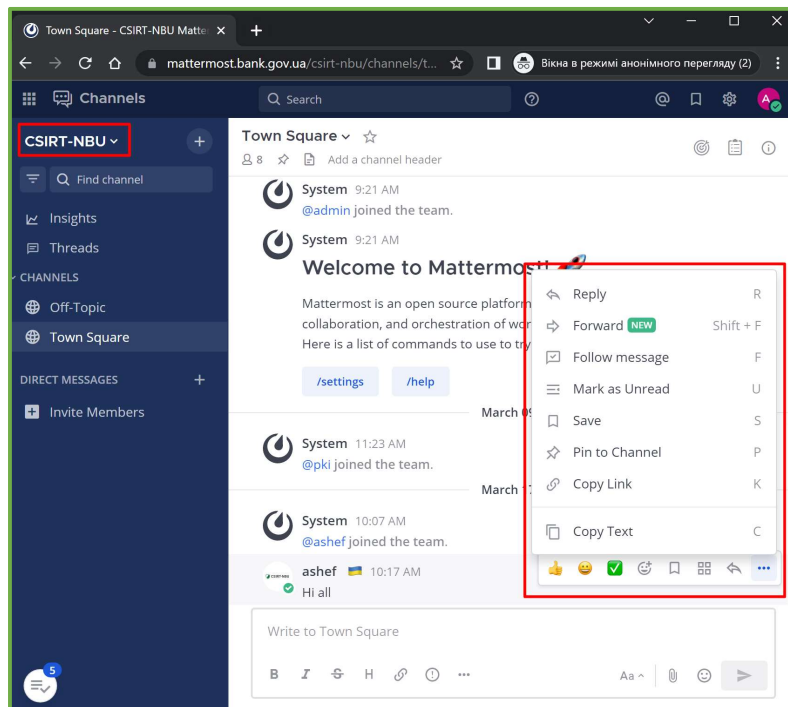


Рис.11 Основні функції при роботі із повідомленнями

4. ВАРІАНТИ ЕКСПЛУАТАЦІЇ СИСТЕМИ ОБМІНУ ПОВІДОМЛЕННЯМИ

4.1. Користування системою обміну повідомленнями спільноти CSIRT-NBU доступно:

- за допомогою одного із браузерів в яких підтримуються push-сповіщення (Edge, Firefox, Safari, Chrome);

- за допомогою застосунку для смартфона (Android, IOS) доступно для завантаження за посиланням: <https://mattermost.com/download/#mobile>;

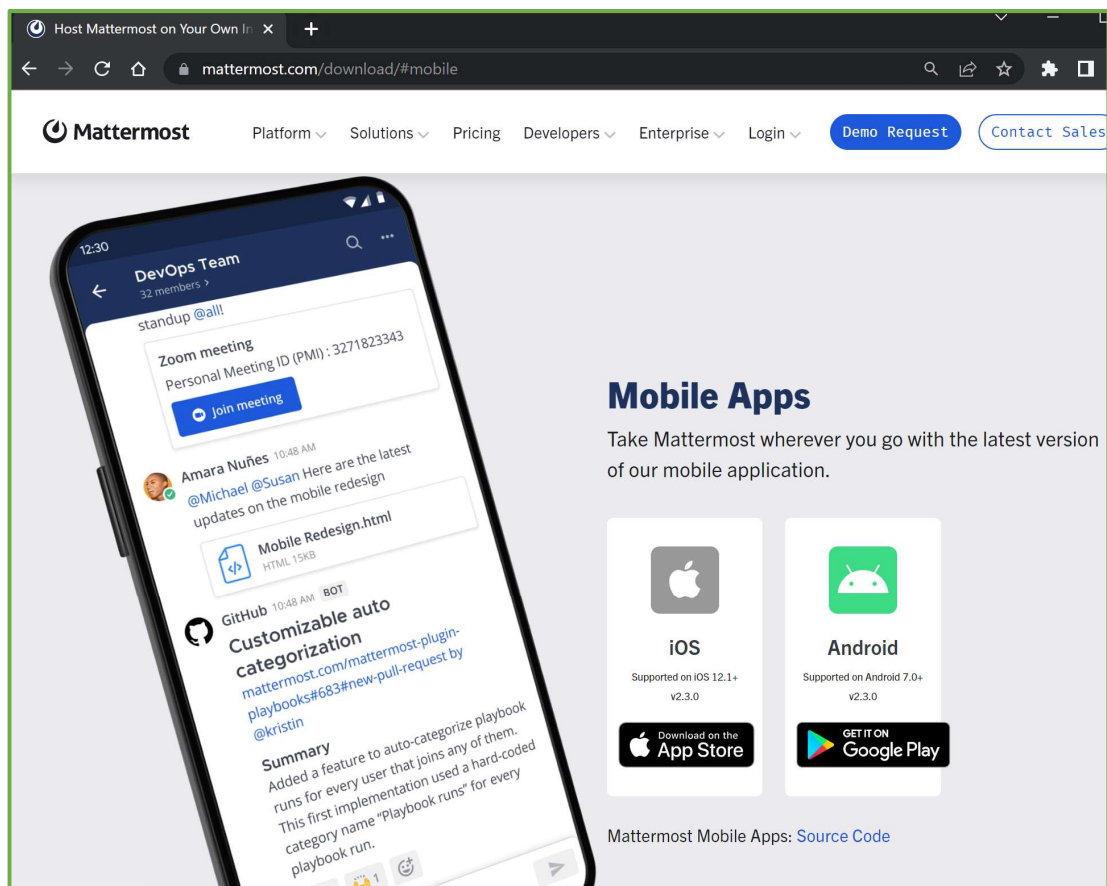


Рис.12 Мобільні застосунки

- за допомогою застосунку для персонального комп'ютера (Windows, MacOS, Linux), доступно для завантаження за посиланням: <https://mattermost.com/download/#desktop>.

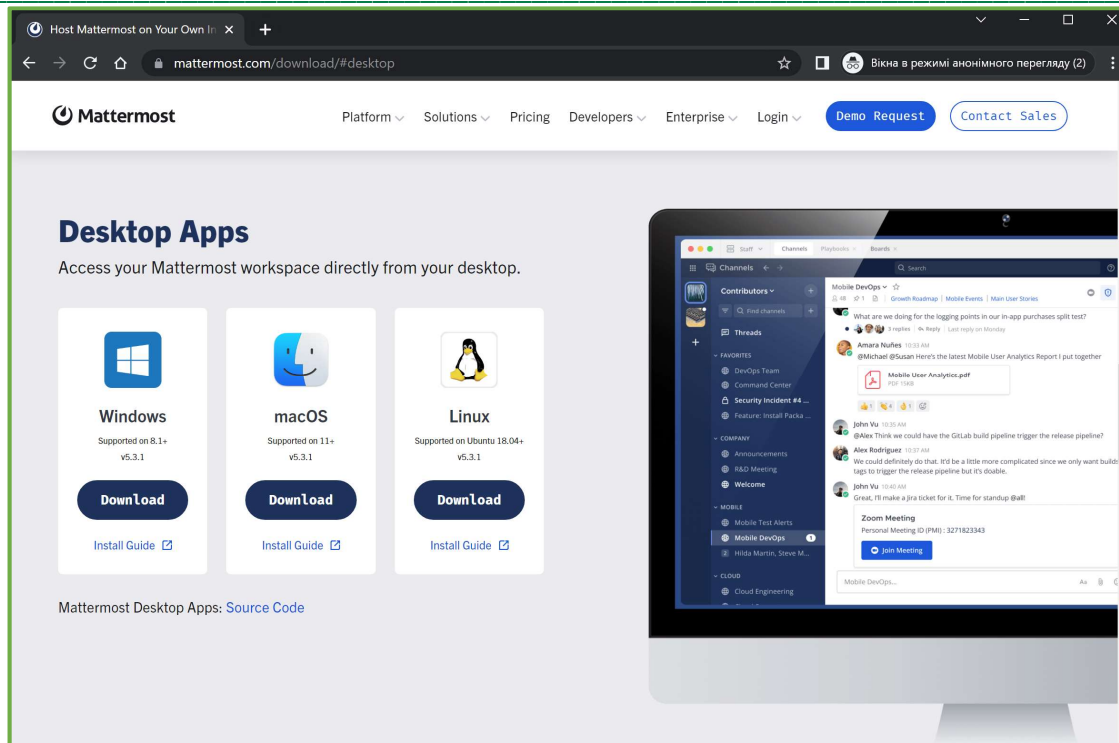


Рис.13 Десктопні застосунки

4.2. Довідкова інформація про систему обміну повідомлення Mattermost.

Mattermost – система обміну повідомленнями з відкритим вихідним кодом, орієнтована на забезпечення комунікації співробітників організації.

Вихідний код серверної частини проекту написаний мовою Go і поширюється під ліцензією MIT. Вебінтерфейс і мобільні застосунки написані на JavaScript з використанням React, десктоп-клієнт для Linux, Windows і macOS побудований на платформі Electron. Як СКБД можуть застосовуватися MySQL і PostgreSQL.

Mattermost позиціонується як альтернатива системі організації комунікацій Slack чи Microsoft Teams, і дозволяє отримувати і відправляти повідомлення, файли і зображення, відстежувати історію переговорів і отримувати повідомлення на смартфоні або ПК. Підтримуються підготовлені для Slack модулі інтеграції, а також надана велика колекція власних модулів для інтеграції з Jira, GitHub, IRC, XMPP, Hubot, Giphy, Jenkins, GitLab, Trac, BitBucket, Twitter, Redmine, SVN і RSS/Atom.