"ЗАТВЕРДЖУЮ"

Ректор

_____Володимир Мельник

Інструкція щодо використання онлайн-сервісів ЛНУ імені Івана Франка

1. Загальні положення

Ця інструкція встановлює загальні вимоги щодо використання онлайн-сервісів у ЛНУ імені Івана Франка (далі - заклад освіти).

Безпека і конфіденційність даних стають ключовими аспектами при роботі в інформаційному середовищі закладу вищої освіти. Цим документом формуються ключові інструкції та вказівки для безпечного використання внутрішніх (Microsoft 365, Деканат, Електронний документообіг, Moodle) та зовнішніх онлайн-сервісів Університету.

2. Інструкції та вказівки.

2.1. Захистіть свій обліковий запис.

Не розміщуйте в мережі персональні дані, такі як ваше ім'я, адреса, телефони тощо. Не надсилайте особисту та конфіденційну інформацію з мережі, якщо вона не зашифрована.

Використовуйте складні паролі, які включають букви, цифри та спеціальні символи. Не використовуйте легко вгадувані паролі, такі як "123456" або "password."
Важливо не зберігати свої паролі на комп'ютері. Краще використовуйте для цього зовнішні носії, тобто ту ж звичайний папір або блокнот, або ж зберігайте їх у спеціальних програмах, захищених від злому.

Двоетапна аутентифікація: Увімкніть двоетапну аутентифікацію (2FA), якщо ця опція доступна. Це зробить ваш обліковий запис набагато стійкішим до вторгнень.

2.2. Оновлюйте програмне забезпечення.

Регулярно оновлюйте операційну систему та програмне забезпечення до останніх версій, оскільки оновлення часто включають виправлення потенційних безпекових проблем.

2.3. Збереження та обмін даними.

Зберігайте конфіденційні дані в безпечних місцях, таких як хмарні сховища з шифруванням (One Drive, Google Drive, тощо). Робіть резервне копіювання важливої інформації.

2.4. Безпека відеоконференцій.

При використанні платформ для відеоконференцій (Zoom, MS Teams, тощо) перевірте налаштування приватності, не діліться посиланнями на зустрічі публічно та використовуйте паролі для входу.

2.5. Перевірка та фільтрування джерел інформації.

Будьте уважні до ненадійних листів або посилань, які можуть бути спамом чи фішингом. Не відкривайте додатки або файли від невідомих джерел.

Перевірте, чи ви на безпечному сайті, особливо, коли вводите конфіденційну інформацію.

2.6. Захист від вірусів та шкідливого ПЗ.
Встановіть або оновлюйте інтегроване антивірусне програмне забезпечення на вашому пристрої (на Windows 10/11 за замовчуванням вже присутній Windows Defender).

2.7. Контроль доступу.
Налаштуйте налаштування приватності в онлайн-сервісах так, щоб обмежити доступ до вашої інформації.

2.8. Повідомляйте про проблеми.
Якщо ви помітили будь-які підозрілі або безпекові проблеми, негайно повідомте про це адміністратора чи службу підтримки.

Проректор з науково-педагогічної роботи та інформатизації — Віталій КУХАРСЬКИЙ

Завідувач центру мережевих технологій та IT підтримки — Василь ПЕТРИШИН