МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА ГВАРДІЯ УКРАЇНИ
КИЇВСЬКИЙ ІНСТИТУТ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

ПОЛОЖЕННЯ
про порядок використання цифрових інструментів здобувачів вищої освіти у освітньому процесі в Київському інституті Національної гвардії України

Схвалено вченою радою
Київського інституту
Національної гвардії України
Протокол від 26.02.2026 № 12

Київ-2026

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Положення про порядок використання цифрових інструментів здобувачів вищої освіти у освітньому процесі (далі – Положення) є нормативним документом Київського інституту Національної гвардії України (далі – Інститут), що регламентує правила, обмеження та механізми використання програмного забезпечення здобувачами вищої освіти.

1.2. Положення розроблено відповідно до законів України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про державну таємницю», наказів Міністерства внутрішніх справ України та Командувача Національної гвардії України з питань кібербезпеки та технічного захисту інформації, Статуту внутрішньої служби Збройних Сил України, а також відповідно до положень про організацію освітнього процесу в Інституті й про академічну доброчесність в Інституті.

1.3. Мета Положення – впровадження сучасних технологій управління знаннями в освітній процес при безумовному дотриманні вимог інформаційної безпеки та кібергігієни.

1.4. Положення поширюється на всіх здобувачів вищої освіти Інституту, які використовують особисті технічні засоби (ноутбуки, планшети, смартфони) в навчальних цілях.

2. ВИКОРИСТАННЯ СИСТЕМИ УПРАВЛІННЯ ЗНАННЯМИ

2.1. Програмне забезпечення «Obsidian» дозволяється використовувати як інструмент для ведення особистих електронних конспектів, структурування навчального матеріалу з відкритих джерел, планування самостійної роботи та створення персональної бази знань.

2.2. Вимоги до інформаційної безпеки:

забороняється вносити, зберігати, обробляти в системі «Obsidian» будь-які відомості, що становлять державну таємницю, службову інформацію (гриф «Для службового користування»), персональні дані військовослужбовців (окрім загальнодоступних), зміст бойових розпоряджень та інформацію про систему охорони об’єктів;

дозволяється використання виключно матеріалів з відкритих джерел, підручників, статутів та незасекречених методичних матеріалів;

з метою унеможливлення витоку даних на сервери третіх сторін, рекомендовано зберігати базу знань (Vault) виключно локально на жорсткому диску особистого пристрою; використання сторонніх хмарних сервісів синхронізації (Obsidian Sync, iCloud, Google Drive тощо) допускається лише під особисту відповідальність користувача та виключно для баз даних, що не містять службової інформації;

дозволяється встановлення лише перевірених плагінів (Community Plugins) з офіційного репозиторію розробника;

користувач зобов'язаний критично оцінювати ризики встановлення додаткового програмного забезпечення, що має доступ до файлової системи.

2.3. Академічне використання:

науково-педагогічним працівникам дозволяється надавати навчальні матеріали (лекції, опорні конспекти) у форматі Markdown (.md) для інтеграції в особисті бази знань здобувачів.

3. ПРАВА ТА ОБОВ'ЯЗКИ КОРИСТУВАЧІВ

3.1. Здобувач вищої освіти має право:

використовувати «Obsidian» для покращення власної успішності та самоорганізації.

3.2. Здобувач вищої освіти зобов'язаний:

дотримуватися правил кібергігієни, використовувати складні паролі та двофакторну аутентифікацію (2FA) для захисту своїх облікових записів;

негайно повідомляти встановленим порядком про спроби сторонніх осіб отримати несанкціонований доступ до пристроїв або підозрілу активність;

на вимогу прямих командирів, посадових осіб вузла зв’язку Інституту та інших посадових осіб надати доступ до пристрою для перевірки відсутності на ньому інформації з обмеженим доступом у рамках чинного законодавства.

4. ВІДПОВІДАЛЬНІСТЬ

4.1. Порушення вимог цього Положення, зокрема пункту 2.2 (вимоги до інформаційної безпеки) тягне за собою дисциплінарну відповідальність згідно з Дисциплінарним статутом Збройних Сил України.

4.2. У разі виявлення фактів витоку інформації, що спричинили тяжкі наслідки, винні особи можуть бути притягнуті до адміністративної або кримінальної відповідальності згідно з чинним законодавством України.

5. ПРИКІНЦЕВІ ПОЛОЖЕННЯ

5.1. Встановлення та використання програмного забезпечення «Obsidian» на службових комп'ютерах (автоматизованих робочих місцях) Інституту, які підключені до внутрішніх мереж або використовуються для обробки службової інформації, категорично заборонено.

5.2. Контроль за виконанням Положення покладається на начальника вузла зв’язку Інституту.