***РЕЗОЛЮЦІЯ***

*Національна безпека є важливою складовою суверенної держави. Для України, що відносно недавно відновила незалежність, важливо забезпечити власний суверенітет в усіх сферах. У сучасному світі інформаційний простір відіграє основну роль як база даних та джерело воєнно-стратегічної інформації. В умовах повномасштабної збройної агресії інформаційна безпека набуває особливого значення.*

Концепція Цифрової трансформації освіти і науки на період до 2026 року передбачає досягнення таких стратегічних цілей:

– цифрове освітнє середовище є доступним та сучасним;

– працівники сфери освіти володіють цифровими компетентностями;

– зміст освіти в галузі ІКТ відповідає сучасним вимогам;

– послуги та процеси у сфері освіти і науки є прозорими, зручними та ефективними;

– дані у сфері освіти і науки є доступними та достовірними.

*Означено основні аспекти безпеки інформаційного простору освіти і науки:*

*1. Захист інформаційних ресурсів: конфіденційність; цілісність; доступність.*

*2. Захист інформаційної інфраструктури: захист мереж; захист серверів та обладнання; захист кінцевих пристроїв.*

*3. Захист користувачів: підвищення обізнаності; управління ідентифікацією та доступом; підтримка та реагування на інциденти.*

*4. Правові та регуляторні аспекти: дотримання законодавства; розробка та впровадження політик безпеки.*

*5. Специфічні загрози в освітньому та науковому середовищі: кібербулінг: захист студентів та викладачів від онлайн-цькування; плагіат та порушення авторських прав; витік наукових даних та інтелектуальної власності; вплив дезінформації та пропаганди.*

*Безпека інформаційного простору освіти і науки в умовах стрімкого розвитку технологій та зростання кіберзагроз потребує не просто реагування на поточні виклики, а й проактивного впровадження проективних змін, спрямованих на створення стійкої, безпечної та довірливої екосистеми для навчання, досліджень та інновацій у майбутньому.*

*(Н. Терентьєва, 2025)*