

ІНФОРМАЦІЙНА БЕЗПЕКА В ДИСТАНЦІЙНОМУ НАВЧАННІ

Ясько А.О., Горелов Ю.П.

Харківський національний університет внутрішніх справ, м. Харків

Зростаючий інтерес до ДН з боку потенційних споживачів освітніх послуг привів до того, що багато навчальних закладів прагнуть самостійно розробляти й впроваджувати комп'ютерні системи ДН. Однак, поширення ДН неможливо без рішення цілого ряду проблем, одна з яких - забезпечення інформаційної безпеки.

Забезпечення інформаційної безпеки в даному контексті може розглядатися у двох аспектах:

1. Забезпечення конфіденційності, цілісності та готовності інформації в процесі навчання.
2. Захист студентів від недостовірної, перекрученої та шкідливої інформації.

У першому випадку ми маємо справу з технічною проблемою захисту інформації від таких погроз, як несанкціонований доступ до цифрового контенту, порушення цілісності й неадекватність навчальних ресурсів, порушення нормального функціонування сервісних служб і ресурсів, порушення безпеки процедур тестування.

Комплексний похід до рішення проблеми захисту інформації в ДН передбачає реалізацію цілого ряду процедур. При цьому використовуються реєстрація й аутентифікація користувача, здійснення контролю доступу, моніторинг і виявлення вторгнення, захист мережних комунікацій, захист сховищ цифрових даних. Це дозволяє реалізувати захист на всіх етапах взаємодії користувача з навчальним матеріалом.

Друга проблема – захист користувача від шкідливого контенту – стала особливо актуальною з появою концепції Веб 2.0, що у значній мірі змінює модель взаємодії користувача з мережею. До основних особливостей нової концепції можна віднести синдикацію, соціалізацію, співробітництво, інтерактивність та відкритість. Інтернет із засобу доступу до навчальних ресурсів, що розроблені викладачем, стає засобом взаємодії й спілкування, створення співтовариств, реалізації доступності всього спектра сервісів у процесі навчання. Користувачеві стають доступні блогі та мікроблогі, соціальні мережі та системи соціальних презентацій, вики-проекти, соціальні закладки, мультимедійні системи поширення інформації, системи спільних редакторських офісів, технології синдикації та нотифікації інформації, підкастинг та ін.

У цих умовах рішення проблеми інформаційної безпеки багато в чому залежить від медіаосвіти, професійної компетентності викладача, аналізу, відбору, підготовки й систематичної перевірки інформаційно-освітніх ресурсів, організації й керування взаємодією студентів. Викладач повинен вміти реалізовувати педагогічні технології засобами інформаційно-комунікативних технологій, забезпечуючи цілісність та результативність процесу навчання.