

## ЗАХИСТ ОСВІТНІХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Савенко С.О.

e-mail: stepan.savenko@nure.ua

Науковий керівник – к.т.н., проф. Милютченко І.О.

Харківський національний університет радіоелектроніки, каф. КРiСТЗi  
м. Харків, Україна

The work examines electronic information resources (EIR) intended for use in the educational process. The specified types and advantages of educational EIRs, requirements and recommendations for their use. The main threats to educational EIRs and areas of protection are formulated: organizational, technical, legal. The essence of EIR determines the specificity of their protection.

Інформаційні ресурси [1], зокрема, електронні інформаційні ресурси (ЕІР) [2] мають ключове значення у сучасному навчально-методичному забезпеченні освітнього процесу. Освітні ЕІР надають доступ до різноманітної інформації, сприяють активному навчанню та розвитку навичок, необхідних для успіху в цифровому світі.

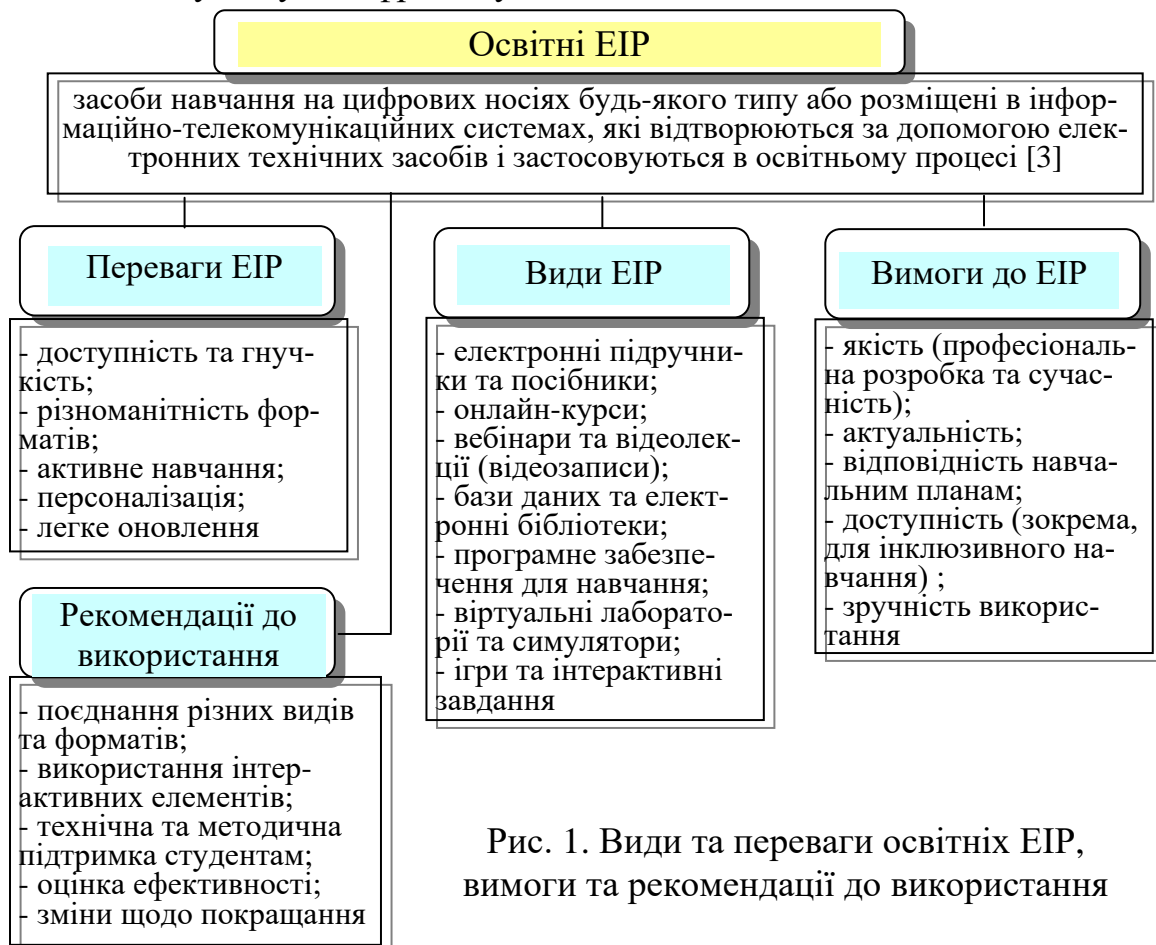


Рис. 1. Види та переваги освітніх ЕІР, вимоги та рекомендації до використання

Освітні ЕІР мають низку переваг порівняно з традиційними навчаль-

но-методичними матеріалами. Види та переваги освітніх ЕІР, вимоги та рекомендації до використання узагальнено на рис.1.

Використання ЕІР є важливим кроком до модернізації освітнього процесу та підвищення його якості. За умови правильного підходу, ЕІР є потужним інструментом для забезпечення успіху кожного студента.

Захист освітніх ЕІР є критично важливим для забезпечення безпеки даних, академічної доброчесності та стабільної роботи закладу освіти. Освітні ЕІР можуть включати персональні дані студентів, викладачів та працівників, результати досліджень, фінансову інформацію, навчально-методичні матеріали, адміністративну документацію та ін.

Основними загрозами для освітніх ЕІР є:

- кіберзлочинність (хакерські атаки, віруси, шкідливе програмне забезпечення, фішинг, DDoS-атаки, зловживання інсайдерами);
- втрата даних через випадкове видалення, пошкодження обладнання, стихійні лиха;
- несанкціонований доступ (злом акаунтів, використання слабких паролів, недостатній захист мережі);
- академічний плагіат та порушення авторських прав.

Для протидії загрозам освітнім ЕІР застосовують такі напрямки захисту (рис.2).

Організаційні заходи:

- впровадження політики інформаційної безпеки, що передбачає правила та процедури щодо захисту ЕІР, відповідальність персоналу, реагування на інциденти;
- регулярні тренінги для студентів, викладачів та працівників щодо загроз, методів захисту, правил безпечної роботи з інформацією;
- застосування системи ідентифікації та аутентифікації користувачів, розмежування прав доступу до різних видів інформації;
- управління ризиками через ідентифікацію та оцінку потенційних загроз, розробку планів дій для мінімізації негативних наслідків.

Технічні заходи:

- використання між мережних екранів (файрволів), систем виявлення вторгнень, віртуальних приватних мереж (VPN);
- захист кінцевих точок (антивірусне програмного забезпечення, оновлення операційних систем та програм, контроль за використанням зовнішніх носіїв інформації);
- використання криптографічних методів для захисту конфіденційної інформації, особливо під час передачі через мережу;
- створення резервних копій даних та їх безпечне зберігання;
- обмеження доступу до серверів та іншого обладнання, забезпечення їх охорони та захисту від стихійних лих.

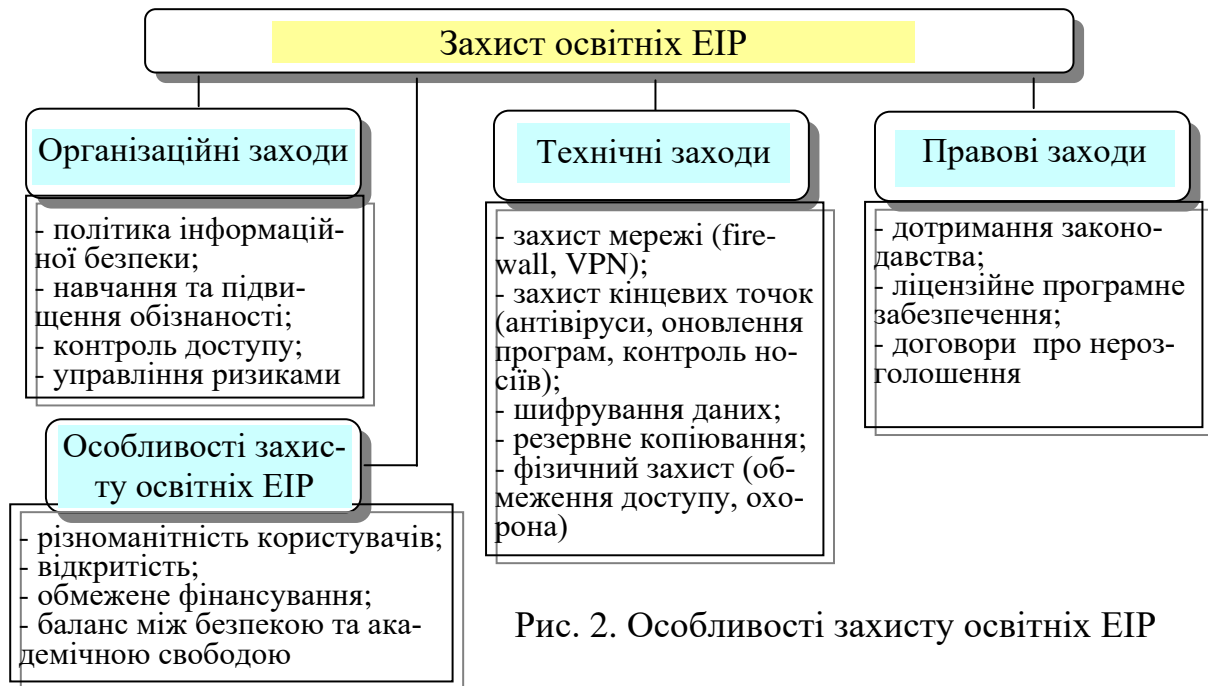


Рис. 2. Особливості захисту освітніх ЕІР

#### Правові заходи:

- виконання вимог законодавства у сфері захисту персональних даних, авторських прав та інших нормативних актів;
- використання лише ліцензійного програмного забезпечення;
- укладення договорів з працівниками та партнерами про нерозголошення конфіденційної інформації.

Захист освітніх ЕІР має певні особливості: велика кількість студентів, викладачів, працівників з різними рівнями технічної підготовки; забезпечення доступу до інформації для широкого кола користувачів, зокрема зовнішніх; недостатнє фінансування для придбання сучасних засобів захисту; необхідність балансу між безпекою та академічною свободою.

Отже, захист освітніх ЕІР є складним та багатогранним завданням, яке потребує комплексного підходу та постійної уваги. Керівництво та персонал повинні забезпечити створення ефективної системи захисту інформації, яка б враховувала можливі загрози та особливості закладу освіти.

**Список використаних джерел:** 1. Милютченко І.О., Онопко Б.В. Інформаційні ресурси: аналіз категорії та класифікація // Радіотехніка: Всеукр. міжвід. наук.-техн. зб.. Харків, 2018. Вип.192. С. 157–161. 2. Милютченко І.О., Кулько П.О. Електронні інформаційні ресурси: визначення та класифікація // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2023. Вип. 213. С. 65 – 69. 3. Положення про Електронні освітні ресурси. Затверджено Наказом МОНМС України від 01.10.2012 № 1060 (редакція від 19.07.2019). URL: <http://zakon.rada.gov.ua/laws/show/z1695-12#Text> (дата звернення 20.02.2025).