КІБЕРБЕЗПЕКА ЕЛЕКТРОННИХ РЕСУРСІВ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ MOODLE

Полотай Орест
к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

В сучасних реаліях, заклади вищої освіти повинні відповідати певним критеріям якості, серед яких важливим є наявність електронного навчального середовища, яке дає змогу здобувачам по-перше мати під рукою портативну бібліотеку навчальних матеріалів, по-друге забезпечує альтернативну форму навчання .в умовах військового стану чи карантинних обмежень.

На щастя, інформаційні технології вже давно проникли в галузь освіти. Електронне навчання з використанням інтернет-технологій є сучасною формою одержання освіти, поряд з стаціонарною та заочною. Всесвітня мережа Інтернет надає великі можливості для установ освіти. У електронному освітньому процесі використовуються кращі традиційні й інноваційні методи, засоби і форми навчання, засновані на комп'ютерних і телекомунікаційних технологіях.

Однак, поряд із розвитком технологій електронного навчання, стрімко розвивається й інша сторона медалі – загрози інформаційної безпеки електронних ресурсів системи дистанційного навчання. Звідси випливає необхідність дотримання правил забезпечення кібербезпеки, використання технічних засобів захисту для захисту середовище дистанційного навчання та серверу, на якому воно розгорнуте [4].

Найкраще для цього підходить система дистанційного навчання Moodle [1, 3].

Для роботи з конкретними ресурсами електронного курсу в системі Moodle існує певна група налаштувань, від правильності налаштувань яких залежить, наскільки дані ресурси, будуть захищені насамперед від навмисного знищення чи модифікації [5].

Насамперед, як тільки електронний курс розроблений і готовий до використанням, обов'язковою умовою є створення резервної копії курсу. Резервна копія виконується в два етапи.

Першим етапом є вибір конкретної групи ресурсів курсу, які необхідно включити в резервну копію (рис. 1).

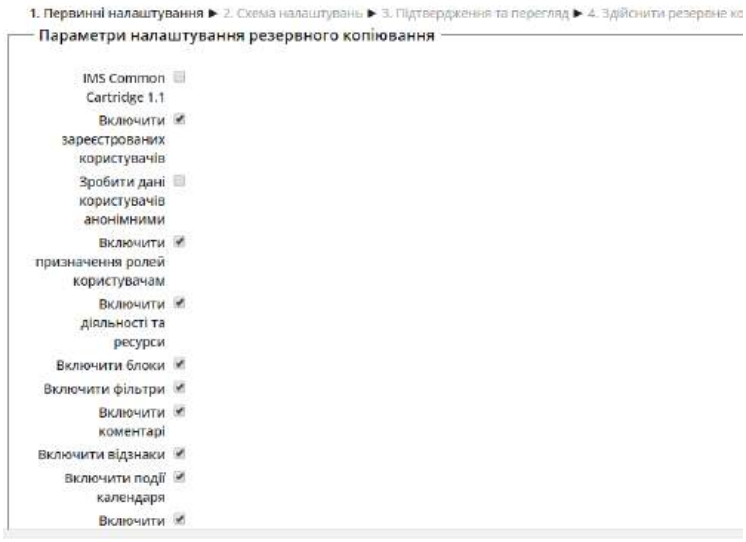

Рис. 1. Перший етап створення резервної копії курсу

На другому етапі вибираються конкретні ресурси з конкретної групи (рис. 2).

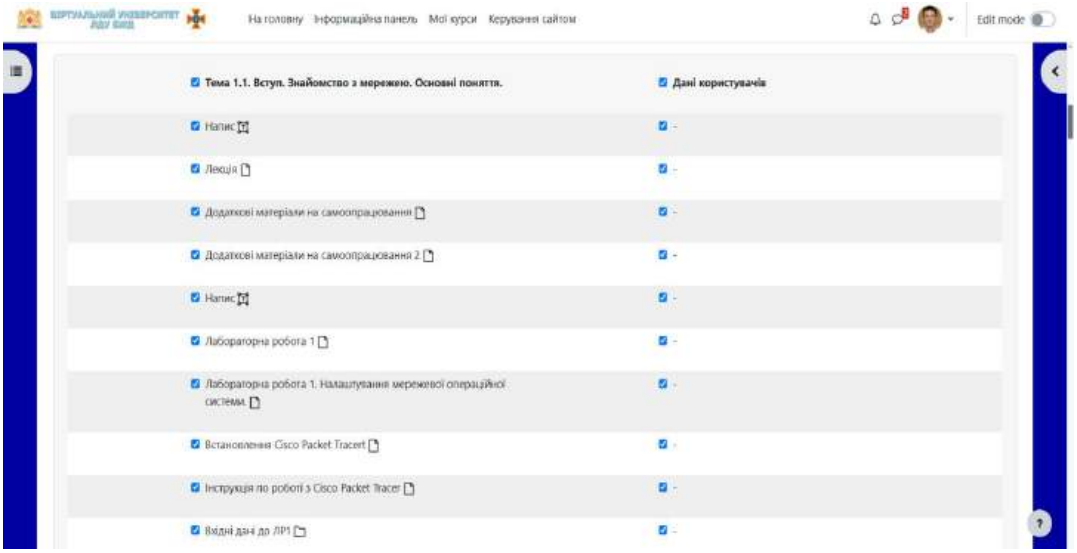

Рис. 2. Другий етап створення резервної копії курсу

Отже, курс готовий, резервна копія теж, тепер необхідно налаштувати безпеку ресурсів курсу, адже їхня втрата, навіть якщо вони продубльовані викличе чимало незручностей.

Найбільш цінними ресурсами в курсі є тести, лекції та завдання. Під час виконання дипломної роботи було налаштовано захищеність цих типів ресурсів в еталонному курсі.

На рис. 3 показано налаштування прав для різних типів користувачів на роботу з ресурсом типу тест.

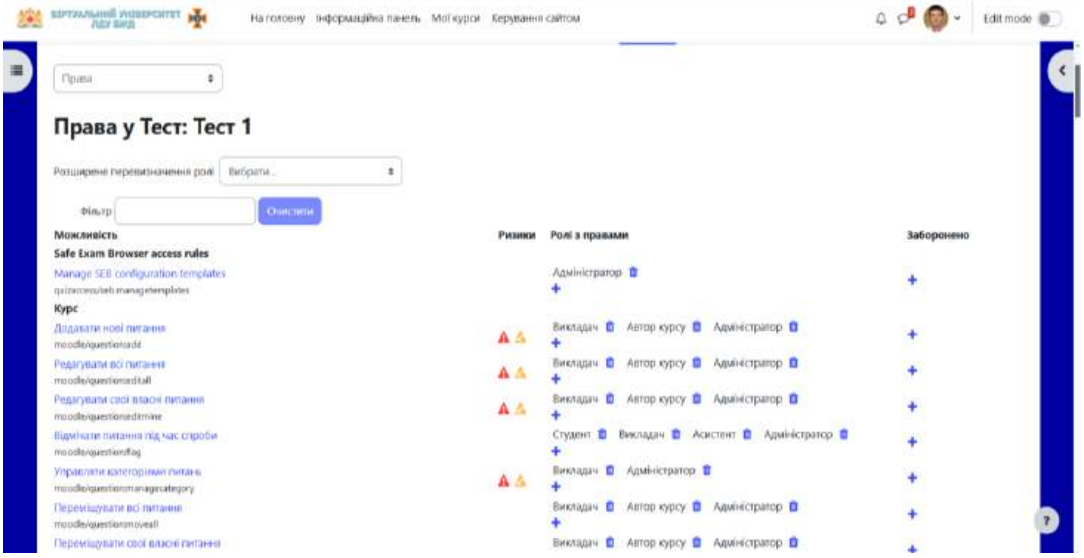

Рис. 3. Права на роботу з тестом

Здобувачу дозволено лише відмічати власні питання під час проходження тесту і власне лише проходити тест.

Також на окремий ресурс можна призначити локальну роль адміністратора, викладача чи студента. Це корисно для того, якщо необхідно тимчасово делегувати права на ресурс іншому учаснику курсу (рис 4).

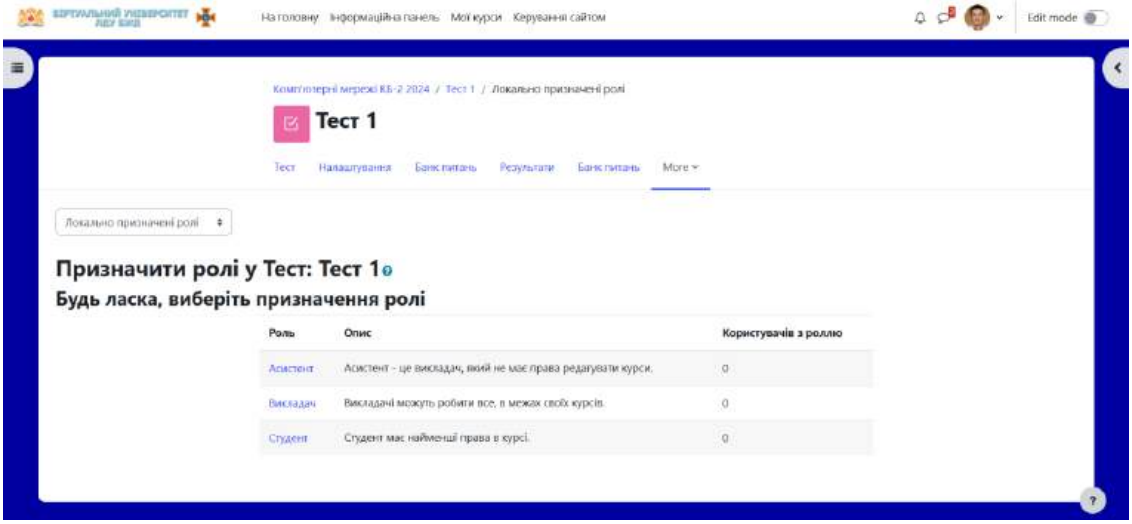

Рис. 4. Ролі на ресурс

Також здійснено налаштування доступу до тесту, а саме процедури тестування (рис. 5).

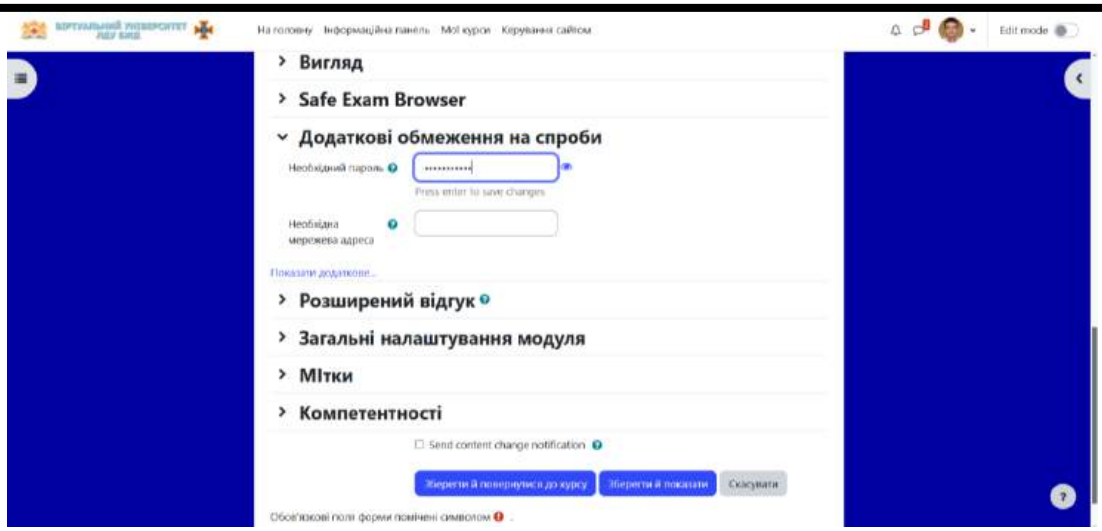

Рис. 5. Додаткові обмеження на тест

Аналогічним чином проведено налаштування прав на роботу з ресурсом типу завдання (рис. 6).

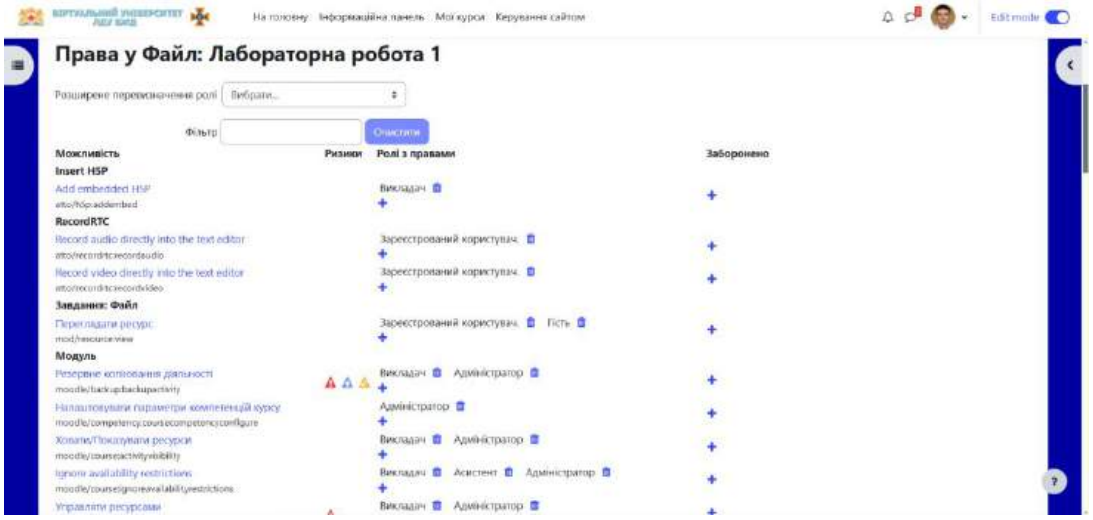

Рис. 6. Права на роботу з завданням

Здобувачу по замовчуванню дозволено тільки експортувати власні роботи.

І на завершення, цілий курс можна повністю приховати від студентів. Це корисно для того випадку, якщо курс вже розроблений, але час його використання ще не настав і доступ студентів до нього поки не бажаний (рис. 7).

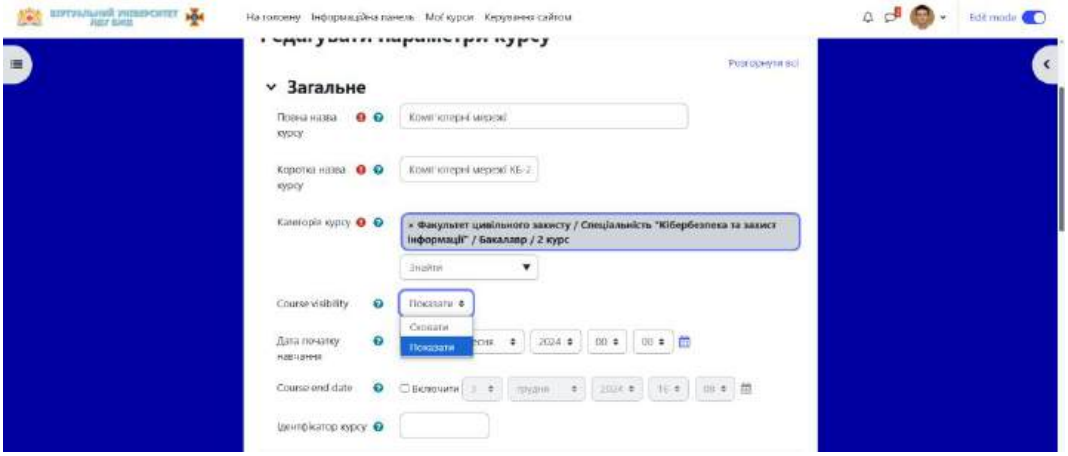

Рис. 7. Налаштування доступності курсу

Отже, правильне налаштування доступу до цілого електронного курсу та його ресурсів є основною вимогою для забезпечення кібербезпеки електронних ресурсів системи дистанційного навчання Moodle.

Список використаних джерел

1. Віртуальний університет Львівського державного університету безпеки життєдіяльності. URL: https://virt.ldubgd.edu.ua
2. Козяр М.М. Віртуальний університет: перспективи переходу на новий тип освіти / Козяр М.М. // Сучасні інформаційні технології та інноваційні методики навчання у підготовці фахівців: ме-тодологія, теорія, досвід, проблеми: зб. наук. праць. − Київ-Вінниця: ТОВ фірма "Планер", 2010. – Вип. 23. − С. 40-46.
3. Офіційний сайт розробників системи Moodle. URL: https://moodle.org
4. Полотай О.І., Бойко К. Програмно-технічний захист інформації за допомогою охоронної системи. Зб. тез. III Всеукр. наук.-практ. конф. молодих учених, студентів і курсантів “Захист інформації в інформаційно-комунікаційних системах” (м. Львів, 28 листопада 2019 р.). Львів : ЛДУБЖД, 2019. С. 76–78.
5. Полотай О.І., Кухарська Н.П. Розроблення електронних курсів у віртуальному навчальному середовищі. Львів : СПОЛОМ, 2021. 172 с.

ПРОПОЗИЦІЇ ЩОДО БЕЗПЕКИ ІНФОРМАЦІЙНИХ ПОТОКІВ ЗАКЛАДУ ВИЩОЇ ОСВІТИ

Полотай Орест
к.т.н., доцент
Львівський державний університет безпеки життєдіяльності
Пузир Андрій
здобувач вищої освіти
Національний університет Львівська політехніка

Загрози кіберзлочинності, такі як фішинг, вірусні атаки, порушення даних через вразливості системи та загрози інформації в локальній мережі закладу вищої освіти, загрожують не лише конфіденційності даних навчального процесу, але й безпеці всього закладу вищої освіти. Існує ціла низка загроз, які притаманні закладам вищої освіти [3], зокрема вони, як і будь які інші учасники бізнес процесів вразливі до витоку конфіденційних даних, які у вигляді інформаційних потоків циркулюють в межах організації та можуть вийти назовні. Така втрата даних може призвести до серйозних втрат, як фінансових так і втрат репутаційних.

Збереження конфіденційності даних стало не просто питанням безпеки, а й важливим елементом стратегії конкурентоспроможності організацій.

Одним із найбільш ефективних способів забезпечення безпеки конфіденційної інформації є використання закладами вищої конкретних систем