УДК 005.34:629.5.081.5:658.562
DOI 10.47049/2226-1893-2025-4-217-225

ОРГАНІЗАЦІЯ КІБЕРБЕЗПЕКИ СИСТЕМ УПРАВЛІННЯ ДИСТАНЦІЙНИМИ КУРСАМИ ТИПУ LMS MOODLE. КЕЙС ДЛЯ ОНМУ

М.Г. Ткаченко
к.ф.-м.н., доцент кафедри «Технічної кібернетики та інформаційних технологій імені професора Р.В. Меркта»
ORCID: https://orcid.org/0000-0002-3166-2627
e-mail: mashatk90@ukr.net

Одеський національний морський університет, Одеса, Україна

Є.О. Севастєєв
ст. викладач кафедри «Кібербезпеки та технічного захисту інформації»
ORCID: https://orcid.org/0000-0003-1165-1119
e-mail: seva.odessa@gmail.com

Державний університет інтелектуальних технологій і зв'язку

Анотація. *У сучасному світі цифрові технології відіграють ключову роль у сфері освіти, зокрема через широке використання систем управління навчанням (Learning Management Systems, LMS). Одеський національний морський університет (ОНМУ) активно застосовує платформу LMS Moodle для організації дистанційного навчання. Проте зростання кіберзагроз, таких як фішингові атаки, програми-вимагачі та витоки даних, підкреслює необхідність посилення кібербезпеки таких систем. Ця стаття розглядає підхід до організації кібербезпеки LMS Moodle в ОНМУ, базуючись на аналізі поточного стану захисту, виявленні вразливостей та розробці цільового профілю кіберзахисту.*

Ключові слова: *кіберзахист, кібербезпека, поточний профіль, цільовий профіль, LMS, Moodle.*

UDC 005.34:629.5.081.5:658.562
DOI 10.47049/2226-1893-2025-4-217-225

ORGANIZATION OF CYBERSECURITY OF DISTANCE COURSE MANAGEMENT SYSTEMS OF THE LMS MOODLE TYPE. CASE FOR ONMU

Mariia G. Tkachenko
c.phy.-mat.s., Docent, department «Technical Cybernetics and Information Technologies named after Professor R.V. Merkt»
ORCID: https://orcid.org/0000-0002-3166-2627
e-mail: mashatk90@ukr.net

Odesa National Maritime University, Odesa, Ukraine

Ievhen Sevastieiev
Senior Lecturer, Department of Cybersecurity and Technical Information Protection
ORCID: https://orcid.org/0000-0003-1165-1119
e-mail: seva.odesa@gmail.com

State University of Intellectual Technologies and Communications

Abstract. *In the modern world, digital technologies play a key role in the field of education, in particular through the widespread use of Learning Management Systems (LMS). Odessa National Maritime University (ONMU) actively uses the LMS Moodle platform to organize distance learning. However, the growth of cyber threats, such as phishing attacks, ransomware and data leaks, emphasizes the need to strengthen the cybersecurity of such systems. This article considers the approach to organizing the cybersecurity of LMS Moodle at ONMU, based on the analysis of the current state of protection, vulnerability identification and development of a targeted cybersecurity profile.*

Keywords: *Cybersecurity, current profile, target profile, LMS, Moodle.*

Актуальність проблеми. Зростання кількості кібератак на освітні установи зумовлює потребу в комплексних заходах захисту. За даними досліджень, освітній сектор є однією з найуразливіших цілей через великі обсяги конфіденційних даних (персональна інформація студентів, викладачів, фінансові дані) та часто недостатній рівень захисту. У контексті ОНМУ, LMS Moodle, як відкрита платформа, забезпечує гнучкість у налаштуванні, але також має вразливості, такі як міжсайтові сценарії (XSS), SQL-ін'єкції та віддалене виконання коду (RCE). Це вимагає системного підходу до кібербезпеки, що відповідає міжнародним стандартам, таким як NIST Cybersecurity Framework та ISO 27001. [1; 2]

Мета статті. Розробити системний підхід до підвищення кібербезпеки системи управління дистанційним навчанням (LMS) Moodle в Одеському національному морському університеті (ОНМУ) шляхом:

1. Аналізу поточного стану захисту платформи з використанням методології NIST Cybersecurity Framework.
2. Ідентифікації ключових вразливостей (відсутність 2FA, обмежений моніторинг, застарілі політики безпеки).
3. Розробки цільового профілю кібербезпеки з конкретними технічними та організаційними заходами (впровадження SIEM-систем, оновлення процедур резервного копіювання, навчання персоналу).
4. Демонстрації практичної цінності запропонованих рішень для захисту конфіденційних даних, відповідності міжнародним стандартам (ISO 27001) та покращення репутації університету.
5. Формування універсальної моделі, яка може бути адаптована іншими ЗВО, що використовують LMS Moodle. [3]

Наукова новизна. Інтеграція методології NIST CSF у контекст специфічних вимог української освітньої інфраструктури з акцентом на практичну реалізацію в умовах обмежених ресурсів.

Основний текст статті. Методологія **NIST Cybersecurity Framework (NIST CSF)**, розроблена Національним інститутом стандартів і технологій США (NIST), надає системний підхід до управління ризиками кібербезпеки. Методологія NIST CSF побудована на п'яти основних функціях:

1. Identify (Ідентифікація):
   - Інвентаризація IT-активів: систем, даних, користувачів.
   - Оцінка ризиків у різних підрозділах (адміністративні, дослідницькі, навчальні).
   - Визначення критичних ресурсів, наприклад: систем управління студентами (SIS), електронні платформи навчання (LMS).
2. Protect (Захист):
   - Впровадження контролів доступу: багатофакторна автентифікація для викладачів і студентів.
   - Шифрування даних, зокрема на мобільних пристроях і при передачі.
   - Розробка політик безпечного користування мережами (Bring Your Own Device, Wi-Fi).
3. Detect (Виявлення):
   - Встановлення систем виявлення вторгнень (IDS/IPS).
   - Моніторинг підозрілої активності (аналітика поведінки).
   - Інтеграція з Security Information and Event Management (SIEM).
4. Respond (Реагування)
   - План реагування на інциденти (IRP): чітко описані ролі, відповідальність.
   - Сповіщення користувачів і органів влади у випадку витоку даних.
   - Аналіз інцидентів для запобігання повторення.
5. Recover (Відновлення)
   - Плани відновлення після атак (DRP), резервне копіювання.
   - Комунікація зі студентами та персоналом.
   - Безперервне вдосконалення процесів безпеки.

NIST CSF є ефективним інструментом для структуризації підходів до кібербезпеки у сфері вищої освіти. Його застосування дозволяє установам бути більш стійкими до кіберзагроз, відповідати вимогам нормативних актів і підтримувати надійне середовище для навчання та досліджень. [1]

Методологія NIST CSF стала основою для створення і впровадження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601, які можна назвати національною адаптацією міжнародних стандартів. [4]. Окрім методології NIST CSF в Методичних рекомендаціях були враховані вимоги міжнародного стандарту ISO/IEC 27001:2022. *Information Security Management System — International Standard*., який застосовується для створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою (ISMS − Information Security Management System).

Виданий спільно **Міжнародною організацією зі стандартизації (ISO)** та **Міжнародною електротехнічною комісією (IEC)**, він є основою для управління ризиками інформаційної безпеки в будь-якій організації – від державних установ до приватних компаній, банків, університетів тощо. Основою для організації системи оцінювання та розвитку кібербезпеки в Методичних рекомендаціях, є модель з п'яти функціональних класів (категорій), що ґрунтується на структурі NIST CSF.

Кожен із цих 5 основних класів (функцій) містить підкатегорії – конкретизовані напрямки діяльності або очікувані результати. Саме підкатегорії деталізують, що саме потрібно зробити, щоб забезпечити кожну функцію. Підбір релевантних для закладу освіти категорій кожного класу стає основою для створення поточного і цільового профілей кіберзахисту, які відображають, відповідно, реальний стан справ на момент оцінки і бажаний стан, який має бути досягнуто.

Даний підхід було застосовано для аналізу стану кібербезпеки LMS Moodle в ОНМУ. Далі відображено результати аналізу.

Аналіз середовища Moodle в ОНМУ. Було ідентифіковано основні інформаційні активи, встановлено їх критичність та здійснено аналіз ризиків. [5].

Таблиця 1

Критично важливі функції LMS Moodle в ОНМУ

№	Актив	Критичність	Ризики
1	Безперебійний доступ до курсів	Підтримка навчального процесу	1. Втрата або спотворення доступу до навчання (DoS-атаки, блокування); 2. Неможливість проведення іспитів, заліків, оцінювання , зрив освітнього процесу; 3. Паніка серед студентів, масові скарги, відтік контингенту; 4. Підміна контенту, вставка шкідливих посилань або дезінформації; 5. Порушення внутрішніх нормативних документів ЗВО.
2	Захист персональних даних	Конфіденційність і відповідність	1. Порушення законодавства (штрафи, розслідування НАЗК, СБУ, Держспецзв'язку); 2. Репутаційні втрати, падіння довіри з боку абітурієнтів та партнерів; 3. Масове шахрайство на основі викрадених ПД (оформлення кредитів, доступ до інших сервісів).
3	Цілісність освітніх матеріалів	Достовірність навчального контенту	1. Порушення авторського права, судові позови від викладачів; 2. Втрати довіри до якості навчання (некоректні або сфальсифіковані тести); 3. Репутаційні наслідки в разі витоку/маніпуляцій зі змістом (особливо в міжнародних партнерських програмах).

Аналіз поточного стану кібербезпеки LMS ОНМУ. Поточний профіль кіберзахисту LMS ОНМУ виступає ключовим засобом для аналізу впроваджених заходів інформаційної безпеки у системі Moodle, яка забезпечує функціонування освітнього процесу. Цей документ фіксує фактичний стан реалізації захисних заходів, рівень їх відповідності чинним нормативним вимогам, а також визначає поточну здатність платформи протистояти кіберзагрозам.

Профіль має на меті:

- Визначення рівня імплементації механізмів кіберзахисту;
- Виявлення наявних недоліків у системі безпеки;
- Формування підґрунтя для створення цільового профілю кіберзахисту.

Область охоплення включає всі компоненти інформаційної безпеки платформи Moodle, зокрема:

- Забезпечення конфіденційності персональних даних здобувачів освіти й викладачів;
- Гарантування постійного доступу до освітніх матеріалів;
- Збереження цілісності даних та ведення системних журналів.

Таблиця 2

Поточний профіль кіберзахисту LMS ОНМУ

Клас заходів	Категорія	Опис заходу	Статус	Примітка
Ідентифікація ризиків (ID)	Управління активами (ID.AM)	Ідентифіковано фізичне обладнання та системи LMS	Реалізовано	Потребує регулярного оновлення інвентаризаційних даних
	Управління політиками (ID.GV)	Політики кібербезпеки задокументовано	В процесі реалізації	Необхідне узгодження з нормативними вимогами
Захист (PR)	Контроль доступу (PR.AC)	Впроваджено ідентифікацію користувачів із використанням паролів	Реалізовано	Відсутня багатофакторна автентифікація (2FA)
	Захист даних (PR.DS)	Налаштовано резервне копіювання даних	Реалізовано	Резервні копії тестуються щоквартально
Виявлення інцидентів (DE)	Моніторинг (DE.CM)	Впроваджено базовий моніторинг активності користувачів	В процесі реалізації	Потрібне впровадження аналітики для виявлення аномальної поведінки
Реагування (RS)	Комунікації (RS.CO)	Описані сценарії реагування на кіберінциденти	Розглядається	Відсутні практичні симуляції та тренування для персоналу
Відновлення (RC)	Планування відновлення (RC.RP)	Створено базовий план відновлення після інцидентів	В процесі реалізації	Потребує інтеграції з планами реагування університету

Для оцінки рівня захисту LMS Moodle в ОНМУ було проведено аналіз поточного профілю кіберзахисту, використовуючи методологію NIST Cybersecurity Framework. Цей підхід передбачає класифікацію заходів за п'ятьма класами: Ідентифікація (ID), Захист (PR), Виявлення (DE), Реагування (RS) та Відновлення (RC). Основні результати аналізу представлені в таблиці нижче. Ключові вразливості включають недостатній контроль доступу, обмежений моніторинг, застаріле програмне забезпечення та низьку обізнаність користувачів щодо кібергігієни. Ці недоліки підвищують ризик несанкціонованого доступу та втрати даних, що вимагає негайних заходів для їх усунення.

Цільовий профіль кіберзахисту. Цільовий профіль кіберзахисту LMS ОНМУ окреслює бажаний рівень інформаційної безпеки, до якого має прагнути університет для забезпечення надійного захисту освітньої платформи Moodle. Цей профіль формується на основі аналізу фактичного стану кіберзахисту, а також враховує рекомендації щодо усунення виявлених уразливостей.

Цільовий профіль має на меті:

- Підвищення загального рівня кіберстійкості системи;
- Усунення слабких місць, зафіксованих у поточному стані;
- Досягнення відповідності чинному законодавству та міжнародним стандартам у сфері інформаційної безпеки.

У межах цільового профілю передбачено модернізацію безпекових заходів у таких ключових сферах:

- Ідентифікація активів, користувачів і пов'язаних ризиків;
- Захист конфіденційності, цілісності та доступності інформації;
- Виявлення підозрілих дій та потенційних загроз;
- Оперативне реагування на кіберінциденти;
- Швидке відновлення функціональності після інцидентів.

На основі аналізу було розроблено цільовий профіль кіберзахисту, який визначає бажаний рівень безпеки LMS Moodle. Він охоплює п'ять ключових напрямків покращення, кожен із яких включає конкретні заходи, терміни реалізації та відповідальних осіб. Основні рекомендації представлені в таблиці нижче. Реалізація цих заходів передбачає 12-18 місяців і потребує координації між ІТ-відділом, адміністрацією та зовнішніми експертами. Кожен захід супроводжується документальним оформленням, технічним забезпеченням та, за потреби, навчанням персоналу.

Практична значущість. Запропоновані заходи мають високу практичну цінність для ОНМУ. Впровадження цільового профілю дозволить:

- Захистити конфіденційні дані студентів і викладачів;
- Знизити ризик кібератак і несанкціонованого доступу;
- Забезпечити відповідність міжнародним стандартам кібербезпеки;
- Підвищити репутацію університету в сфері дистанційної освіти.

Таблиця 3

Поточний профіль кіберзахисту LMS ОНМУ

Клас заходів	**Категорія**	**Цільовий показник**	**Опис заходів**	**Термін реалізації**	**Очікуваний результат**
Ідентифікація ризиків (ID)	Управління активами (ID.AM)	Розширення інвентаризації активів	Регулярне оновлення списку серверів, програмного забезпечення та мережевого обладнання	До 3 місяців	Оновлений реєстр активів
	Управління політиками (ID.GV)	Оновлені політики кібербезпеки	Розробка нових політик із врахуванням стандартів ISO 27001	До 6 місяців	Політики, що відповідають міжнародним стандартам
Захист (PR)	Контроль доступу (PR.AC)	Впровадження багатофакторної автентифікації (2FA)	Забезпечення додаткового рівня захисту для всіх користувачів LMS	До 4 місяців	Захищений доступ до системи
	Захист даних (PR.DS)	Автоматичне резервне копіювання з щотижневим тестуванням	Розширення системи резервування та впровадження автоматичних тестів	До 2 місяців	Надійне відновлення даних
Виявлення інцидентів (DE)	Моніторинг (DE.CM)	Встановлення SIEM-системи	Впровадження системи для аналізу логів та виявлення аномалій у реальному часі	До 5 місяців	Виявлення загроз у реальному часі
Реагування (RS)	Комунікації (RS.CO)	Проведення тренувань на основі кіберінцидентів	Моделювання інцидентів для покращення готовності персоналу	До 6 місяців	Підготовлений персонал
Відновлення (RC)	Планування відновлення (RC.RP)	Оновлення плану відновлення із включенням зовнішніх партнерів	Інтеграція плану відновлення LMS з університетськими планами	До 3 місяців	Працездатний план відновлення

Ці рекомендації можуть бути адаптовані для інших закладів освіти, які використовують LMS Moodle, що робить кейс ОНМУ універсальним прикладом для освітнього сектору.

Підвищення кібербезпеки дозволить ОНМУ розширити використання LMS для міжнародних студентів, що зміцнить його позиції на глобальному освітньому ринку. [6; 7]

Висновки. Організація кібербезпеки LMS Moodle в ОНМУ є комплексним завданням, що вимагає системного підходу. Аналіз поточного стану показав прогрес у базових заходах захисту, але виявив критичні вразливості, які потребують негайного усунення. Розроблений цільовий профіль кіберзахисту пропонує чіткий план дій, який поєднує технічні, організаційні та освітні заходи. Реалізація цього плану не лише підвищить безпеку освітнього середовища ОНМУ, але й стане прикладом для інших закладів освіти в Україні. Подальші дослідження можуть бути спрямовані на оцінку ефективності впроваджених заходів та адаптацію до нових кіберзагроз.

СПИСОК ЛІТЕРАТУРИ

1. NIST Special Publication 800-53: *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, 2020, 492 p.
2. ISO/IEC 27001:2022. *Information Security Management System – International Standard*, 26 p.
3. Ткаченко М.Г., Севастєєв Є.О. Аналіз методів підвищення кібербезпеки LMS ОНМУ. IV Міжнародна науково-практична конференція «Проєктний та логістичний менеджмент: нові знання на базі двох методологій», 2024., с. 25-28.
4. Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури, затверджені наказом Адміністрації Держспецзв'язку від 06.10.2021 № 601.
5. Ian Wild. *Moodle 4 Security*. Pub.: de Gruyter GmbH, Walter, 2024, 288 p.
6. Постанова КМУ від 16.05.2023 р. № 497 « Про затвердження Порядку пошуку та виявлення потенційної вразливості інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж».
7. ENISA. *Cybersecurity in Education: Challenges and Soluti*ons, 2022, 29 p.

REFERENCES

1. NIST Special Publication 800-53: *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, 2020, 492 p.
2. ISO/IEC 27001:2022. *Information Security Management System – International Standard*, 26 p.

3. Tkachenko M.G., Sevasteev E.O. Analysis of methods of improving cyber security of LMS of ONMU. IV International scientific and practical conference "Project and logistics management: new knowledge based on two methodologies", 2024., p. 25-28.
4. Methodological recommendations for increasing the level of cyber protection of critical information infrastructure, approved by the order of the State Special Communications Administration No. 601 dated October 6, 2021.
5. Ian Wild. *Moodle 4 Security*. Pub.: de Gruyter GmbH, Walter, 2024, 288 p.
6. Decree of the CMU of May 16, 2023 No. 497 «On approval of the Procedure for searching and identifying potential vulnerabilities of information (automated), electronic communication, information and communication systems, electronic communication networks».
7. ENISA. *Cybersecurity in Education: Challenges and Solutions*, 2022, 29 p.

Стаття надійшла до редакції 15.09.2025

Посилання на статтю: Ткаченко М.Г., Севастєєв Є.О. Організація кібербезпеки систем управління дистанційними курсами типу lms moodle. кейс для ОНМУ // *Вісник Одеського національного морського університету:* Зб. наук. праць, 2025. № 4 (78). С. 217-225. DOI 10.47049/2226-1893-2025-4-217-225.

Article received 15.09.2025

Reference a Journal Artic: M. Tkachenko, I. Sevastieiev. Organization of cybersecurity of distance course management systems of the lms moodle type. case for onmu // *Herald of the Odesa National Maritime University*: Coll. scient. works, 2025. № 4 (78). P. 217-225. DOI 10.47049/2226-1893-2025-4-217-225.