DOI: https://doi.org/10.36910/6775-2524-0560-2025-58-13
UDC 681.326.74
Віталій Дмитрович Назарук, к.т.н., старший викладач
https://orcid.org/0000-0002-7579-9190
Костянтин Сергійович Шайнюк, аспірант
https://orcid.org/0009-0003-6523-940X
Національний університет водного господарства та природокористування, м. Рівне, Україна

МОДЕЛЬ ЗАГРОЗ ДЛЯ ІНФОРМАЦІЇ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ MOODLE

Назарук В.Д., Шайнюк К.С. Модель загроз для інформації системи дистанційного навчання Moodle. В роботі розглянуто загрози інформаційної безпеки системи дистанційного навчання Moodle, як найбільш поширеної системи в закладах вищої освіти України. Описано основні категорії загроз, які можуть виникнути в ході впровадження та експлуатації зазначеної системи в навчальному процесі, деталізовано окремі аспекти і підготовлено детальний аналіз загроз за рахунок несанкціонованого фізичного доступ до технічних засобів оброблення та зберігання інформації, порушення встановлених правил управління і розмежування ролевим доступом, помилок та відмов (збоїв) у функціонуванні програмного забезпечення, впровадження комп'ютерних вірусів та закладних програм, неправильних навмисних або ненавмисних дій персоналу, а також надзвичайних ситуацій. Визначено та зведено в таблицю вплив зазначених загроз на основні безпекові характеристики інформації (конфіденційність, цілісність, доступність та спостережність). Задля запобігання інцидентів інформаційної безпеки в системі по кожному виду загроз розроблено та надано рекомендації щодо протидії існуючим загрозам. Розроблена модель загроз для інформації в системи дистанційного навчання Moodle може бути використана при підготовці технічного завдання для побудови комплексної системи захисту інформації (далі - КСЗІ) системи дистанційного навчання, або проведення аудиту інформаційної безпеки відповідно до положень міжнародних стандартів. В свою чергу, впровадження КСЗІ чи проведення аудиту відкриває можливість безпечно і надійно використовувати зазначену інформаційну систему в навчальному процесі закладів вищої освіти із дотриманням вимог чинного законодавства України.
Ключові слова: системи дистанційного навчання, загрози безпеки інформації, модель загроз, засоби та заходи захисту.

Nazaruk V., Shayniuk K. Threat model for the information security of the moodle distance learning system. This paper examines the information security threats faced by Moodle, the most widely used distance learning system in Ukrainian higher education institutions. The study outlines the primary categories of threats that may arise during the implementation and operational use of this system in academic settings. Key areas of analysis include unauthorized physical access to data processing and storage equipment, breaches in access control and role-based management policies, software errors and malfunctions, introduction of computer viruses and malware, as well as both intentional and unintentional actions by personnel, and emergency situations. Each threat's impact on critical security attributes – confidentiality, integrity, availability, and observability – is detailed and summarized in tabular form. To prevent information security incidents within the system, the authors offer targeted recommendations to counteract each identified threat. The developed threat model for Moodle-based distance learning systems can serve as a foundation for creating a comprehensive information security system (CISS) or conducting security audits in line with international standards. Implementing a CISS or conducting an audit enhances the security and reliability of this educational platform in academic environments, ensuring compliance with Ukrainian legislation.
Keywords: remote learning systems, information security threats, threat model, security measures and protection methods.

Вступ.

Системи дистанційного навчання стають в даний час невід'ємною частиною освітнього процесу закладів вищої освіти усіх рівнів. Зумовлено це передусім їх функціоналом, який надає можливості зосередження в одному місці необхідних матеріалів навчальних курсів, інструментів контролю отриманих знань та інтерактивного діалогу здобувачів освіти з науково-педагогічними працівниками. Особливо затребуваними системи дистанційного навчання стали в період карантинних обмежень та в умовах воєнного часу, проте і після завершення зазначених обмежень їх популярність буде зростати, враховуючи опції економії часу на пересування до навчального закладу здобувачів вищої освіти і викладацького складу, можливості виконання завдань у зручний час, наявності інструментів неупередженої оцінки знань у вигляді тестів.

Така трансформація освітнього процесу вимагає детального аналізу стану кібербезпеки та захисту інформації впроваджених у навчальних закладах систем дистанційного навчання та вироблення рекомендацій щодо локалізації можливих вразливостей та загроз.

Постановка завдання.

Захисту підлягають наступні групи інформації системи дистанційного навчання:

- дані та програмні коди у вигляді файлів різних форматів, записів баз даних та інших структур машинного представлення;
- бази даних захисту (списки зареєстрованих користувачів, їх ідентифікаторів, повноважень користувачів, права доступу, журнали реєстрації подій та ін.);
- дані загального користування (в тому числі, – навчальні матеріали, дані тестів та оцінювання знань).

Особлива увага з точки зору захисту має бути приділена даним оцінювання знань, які використовуються в різного роду рейтингуваннях, призначенні стипендій та документах про отримання вищої освіти і, згідно Закону України Про захист інформації в інформаційно-комунікаційних системах [1], повинні оброблятися в системі із застосуванням комплексної системи захисту інформації, або при підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою.

Під час створення комплексної системи захисту інформації необхідно визначити переліків відомостей, які підлягають захисту в процесі обробки, інших об'єктів захисту в АС, класифікувати інформацію за вимогами до її конфіденційності або важливості для організації, необхідних рівнів захищеності інформації, визначення порядку введення (виведення), використання та розпорядження інформацією в автоматизованій системі (далі – АС), а також розробити та коригувати періодично моделі загроз і моделі захисту інформації в АС.

Задля впровадження достатніх і ефективних засобів захисту необхідно систематизувати існуючі загрози. Результат такої систематизації викладається у вигляді моделі загроз, яка, в свою чергу, служитиме вихідними даними для розроблення та впровадження комплексу засобів і заходів захисту.

Огляд джерел

Правові, та організаційні засади функціонування системи вищої освіти в Україні встановлено Законом України Про вищу освіту [2], рекомендації щодо навчально-методичного та інформаційного забезпечення навчального процесу за дистанційною формою навчання визначені Положенням про дистанційне навчання [3], відносини у сфері захисту інформації в інформаційно-комунікаційних системах врегульовано Законом України Про захист інформації в інформаційно-комунікаційних системах [1], правові та організаційні основи захисту життєво важливих інтересів суспільства та держави, національних інтересів України у кіберпросторі визначено Законом України Про основні засади забезпечення кібербезпеки України.[4].

В [5] надана оцінка загроз, викликів і можливостей запровадження дистанційного навчання внаслідок пандемії. Автори [6] звертають увагу на недосконалість політик безпеки існуючих систем дистанційного навчання. Як стверджено в [7], за результатами дослідження систем дистанційного навчання Sakai, Moodle, Atutor, ILIAS, Canvas, Blackboard, Webtutor на наявність механізмів захисту, найбільш захищеною є система Moodle (7 балів), а найменш захищеною – Webtutor (3 бали). Одночасно, система Moodle є і найбільш використовуваною в закладах вищої освіти України.

Рекомендації стосовно створення моделі загроз приведені в п.п. 4.2 – 4.3 додатку «Методичні вказівки щодо структури та змісту Плану захисту інформації в автоматизованій системі» до нормативного документу з технічного захисту інформації НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» [8]. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу визначено в [9].

Згідно [10] із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто, в нашому випадку, порушення цілісності і доступності інформації.

Виклад основного матеріалу.

Однією із найбільш поширених в Україні систем дистанційного навчання є Moodle (Modular Object-Oriented Dynamic Learning Environment — модульне об'єктно-орієнтоване динамічне навчальне середовище). Її популярність обумовлена такими факторами, як модульність, масштабованість і функціональність, а також наявністю відкритої (публічної) ліцензії GPL - General Public License. Разом з тим, така система потребує ретельного і зваженого підходу до виділення апаратного ресурсу, налаштування компонентів, впровадження заходів безпеки та адміністрування в цілому. Враховуючи важливість застосування системи в навчальному процесі

закладу вищої освіти, особливу увагу необхідно приділити загрозам інформаційній безпеці та впровадженню дієвих заходів та засобів захисту.

В свою чергу, впровадження засобів та заходів захисту проектується за відповідним технічним завданням, розробка якого виконується на підставі певних вихідних даних. Такі вихідні дані згідно [8], рекомендовано описати в ***моделі загроз*** та ***моделі порушника*** для кожної конкретної автоматизованої системи (АС). Предметом даного дослідження є модель загроз для інформації системи дистанційного навчання.

Модель загроз для інформації системи дистанційного навчання Moodle

Усі загрози та можливі кіберінциденти щодо інформації, яка створюється, обробляється та зберігається у зазначеній інформаційній системі, можна поділити на наступні категорії:

- несанкціонований фізичний доступ до серверного та мережевого обладнання;
- порушення встановлених правил розмежування та управління доступом;
- помилки у програмному забезпеченні (далі - ПЗ) та відмови (збої) у функціонуванні ПЗ та технічних засобів;
- впровадження шкідливого програмного забезпечення;
- неправильні та зловмисні дії користувачів;
- надзвичайні ситуації.

В таблиці 1 представлено перелік загроз інформації, де використовуються наступні скорочення для позначення тих характеристик інформації, на які впливає та або інша загроза: К - конфіденційність, Ц – цілісність, Д - доступність, С - спостережність. В стовпцях графи «Наслідки» знаком «+» відмічається можливість виникнення зазначеної загрози.

Табл. 1 Перелік загроз інформації

з/п	Тип та визначення загроз	Джерело загроз	Наслідки			
Загрози несанкціонованого фізичного доступу до обладнання						
	Пошкодження, знищення або викрадення обладнання.	Людина	+			
	Несанкціоноване копіювання інформації.	Людина	+			
	Внесення несанкціонованих змін в ПЗ та бази даних.	Людина	+			
	Внесення несанкціонованих змін в конфігурацію мережевої інфраструктури.	Людина	+			
Порушенням встановлених правил розмежування та управління доступом						
	Підключення порушника до системи під ідентифікатором або паролем зареєстрованого користувача	Людина	+			
	Переповнення таблиці логування зареєстрованих користувачів	ПЗ, обладнання				
	Неспроможність обробки процедури аутентифікації через недостатню продуктивність ядра системи	Обладнання				

	Відсутність доступу за рахунок аварій та несправностей мережевого обладнання	Людина, обладнання				
	Відсутність доступу, спричинена Dos та DDos атаками	Людина, ПЗ, обладнання				
	Помилки у ПЗ та відмови (збої) технічних засобів					
0	Збої, викликані використанням застарілих версій операційної системи, кластеру віртуалізації та ПЗ LMS Moodle	ПЗ				
1	Переповнення таблиць баз даних через обмежений ресурс пам'яті	ПЗ, обладнання				
2	Вихід з ладу обладнання, в т.ч через фізичний знос компонентів	Обладнання				
3	Відсутність електроживлення	Обладнання, середовище				
	Впровадження шкідливого програмного забезпечення					
4	Ураження програмного забезпечення комп'ютерними вірусами	Людина, ПЗ				
5	Шифрування баз даних та ПЗ за допомогою шкідливого програмного забезпечення	Людина, ПЗ				
6	Перехоплення паролів програмою-імітатором, включення в програми програмних закладок типу «троянський кінь», «бомба» тощо	Людина, ПЗ				
7	Використання «вад» мов програмування, операційних систем, мережевої інфраструктури (у тому числі параметрів системи захисту, встановлених «за умовчанням»).	Людина, ПЗ				
	Неправильні та зловмисні дії користувачів					
8	Випадкові помилки користувачів, обслуговуючого персоналу, помилкове конфігурування та адміністрування системи.	Людина				
9	Цілеспрямовані дії щодо неправомірного впливу на оброблювану інформацію та ПЗ	Людина				
0	Цілеспрямовані дії щодо зміни режимів роботи системи	Людина, ПЗ, обладнання.				
1	Викрадення в корисливих цілях інформації з ознаками інтелектуальної власності та екзаменаційних тестів користувачами з привілейованими правами доступу.	Людина				

	Надзвичайні ситуації					
2	Аварія систем життєзабезпечення (електроживлення, охолодження та вентиляції, ліній зв'язку тощо)	Середовище				
3	Фізичне зруйнування системи (внаслідок вибуху, пожежі, затоплення тощо) пошкодження всіх або окремих найбільш важливих компонентів системи (пристроїв, носіїв важливої інформації).	Середовище				

Згідно наданих в [8] рекомендацій, протидіяти наведеним вище загрозам доцільно із використанням наступних засобів та заходів захисту.

Загрози несанкціонованого фізичного доступу до обладнання.

Несанкціонований фізичний доступ до технічних засобів може реалізовуватися шляхом проникнення порушника у приміщення, де такі засоби розташовано. У випадку реалізації цієї загрози створюються передумови для порушення цілісності, конфіденційності і доступності інформації.

Заходи та засоби протидії:

- визначення порядку фізичного доступу співробітників та відвідувачів у приміщення, де розташовано серверне та мережеве обладнання (шляхом затвердження переліку осіб, яким дозволено знаходитись у приміщенні);
- розробка та дотримання регламенту розкриття та опечатування приміщень, постановки та зняття їх з охоронної сигналізації;
- забезпечення охорони приміщення, де розташовано обладнання у неробочий час;
- регламентування порядку дій персоналу та охорони у випадку реалізації спроб несанкціонованого фізичного доступу.

Порушення встановлених правил розмежування та управління доступом

Несанкціонований доступ до інформації здійснюється з порушенням встановлених правил управління доступом, а саме підключення порушника до системи під ідентифікатором або паролем зареєстрованого користувача з подальшим використанням забороненого програмного забезпечення для отримання доступу до інформаційних ресурсів в обхід системи управління доступом. У випадку реалізації цієї загрози створюються передумови для порушення цілісності, конфіденційності і доступності інформації.

Заходи та засоби протидії:

- надання привілейованих прав доступу користувачам з необхідним рівнем знань, та належною репутацією;
- обмеження доступу, надання користувачам доступу тільки до необхідних ресурсів та функціоналу. Використання принципу найменших привілеїв (Least Privilege Principle.
- реєстрація дій користувачів у захищеному журналі аудиту;
- впровадження двофакторної аутентифікації усіх, без виключення користувачів системи;
- логування і сповіщення про вхід до системи користувачів з розширеними правами доступу, автоматизоване віддалене блокування засобами системи у разі сповіщення про несанкціонований вхід;

Відсутність доступу користувачів до системи може бути спричинена переповненням таблиці логування, або зовнішніми DoS/DDoS атаками. Згідно проведених в ході дослідження спостережень, активність надмірного доступу до системи фіксується у період заліково - екзаменаційних сесій. Така активність зумовлена як об'єктивними факторами необхідності доступу здобувачів вищої освіти до освітніх матеріалів, так і зловмисними діями з метою перешкоджанню навчальному процесу.

Заходи та засоби протидії:

- виділення достатнього апаратного ресурсу для ведення таблиць логування та періодичне очищення їх адміністратором системи;

- аналіз трафіку на кількох рівнях інфраструктури: для першого рівня може бути використано мережеве обладнання (маршрутизатор), другий рівень - операційна система, третій рівень - додаткові налаштування прикладного програмного забезпечення або самої навчальної платформи та її модулів.

- фіксація IP-адрес пристроїв, які приймають або приймали участь в DoS/DDoS атаках та внесення їх в адрес-листи з обмеженим доступом або блокування їм окремих IP протоколів для запобігання надання відповіді на отримані від них запити;

Неправильні та зловмисні дії персоналу

Неправильні дії персоналу трапляються внаслідок його низької кваліфікації, недбалого ставлення до своїх службових обов'язків або свідомого завдання шкоди. У випадку реалізації цієї загрози створюються передумови для порушення цілісності, конфіденційності і доступності інформації.

Внаслідок таких дій персоналу можуть трапитись:

- відмови окремих компонентів, руйнування технічних засобів АС, програмних ресурсів (обладнання, каналів зв'язку, втрата даних, програм та ін.);

- ненавмисне пошкодження носіїв інформації;

- неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації або знищення окремих інформаційних ресурсів);

- ненавмисне зараження ПЗ комп'ютерними вірусами;

- неконтрольоване поширення інформації з АС, паролів та ідентифікаторів користувачів, іншої інформації щодо режимів роботи АС;

- неправомірне впровадження і використання стороннього ПЗ (наприклад, навчальних та ігрових програм, несанкціонованого системного і прикладного ПЗ та ін.).

Заходи та засоби протидії:

- організація професійної підготовки;
- розмежування прав доступу та привілеїв;
- впровадження політик та інструкцій безпеки;
- моделювання неправильних дій персоналу;
- ведення журналів аудиту дій користувачів у АС;
- регламентація порядку допуску користувачів до роботи з АС.

Зловмисні дії користувачів можуть бути спрямовані на несанкціоновану модифікацію результатів оцінювання знань (оцінки), викрадення інформації з ознаками інтелектуальної власності та викрадення інформації із вмістом підсумкових тестів з корисливими мотивами. В першу чергу це стосується користувачів з привілейованим доступом. Наприклад, користувач із роллю "менеджер кафедри" має технічну можливість відібрати курс, розроблений одним викладачем і закріпити за цим курсом іншого викладача без відома першого. Інша загроза може бути реалізована користувачами із роллю "модератор центру оцінювання знань", які мають доступ до всіх, без виключення, тестових завдань, розроблених викладачами з відміченими правильними відповідями на кожне питання. Саме ця категорія користувачів має технічну можливість копіювати зазначену інформацію і розпоряджатись нею на власний розсуд.

Заходи та засоби протидії:

регламентування дій користувачів із привілейованим доступом, яке унеможливлює певні зловживання;

мінімізація кількості користувачів з привілейованим доступом;

налаштування доступу до тестових завдань таким чином, щоб право на копіювання та модифікацію мав лише розробник цих завдань чи гарант освітньої програми.

Надзвичайні ситуації

Надзвичайні події (пожежа, затоплення, землетрус, військові дії, виникнення радіаційної та хімічної небезпеки) можуть бути причиною порушення конфіденційності, цілісності і доступності інформації.

Заходи та засоби протидії:

- проведення учбових занять з користувачами системи щодо їх дій на випадок виникнення надзвичайних ситуацій;
- організація системи оповіщення;
- впровадження технічних засобів протидії (мінімізації шкоди) від загрози, які включають протипожежне обладнання, систему оповіщення персоналу, резервного електропостачання;
- створення запасних комплектів технічних засобів, резервних копій ПЗ та інформаційних ресурсів системи дистанційного навчання;
- забезпечення резервних копій за принципом 3 – 2 – 1.

Висновки

Приведений в роботі аналіз загроз для інформації в системі дистанційного навчання Moodle може бути використаний при створенні технічного завдання для побудови комплексної системи захисту інформації, а також розробникам та адміністраторам, які працюють над супроводом та експлуатацією зазначеної системи.

Предметом подальших досліджень можуть стати модель порушника системи дистанційного навчання та розробка технічного завдання на побудову системи захисту.

Список бібліографічного опису

1. Про захист інформації в інформаційно-комунікаційних системах [Електронний ресурс]. – Закон України № 31. – 1994. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
2. Про вищу освіту: Закон України [Електронний ресурс] . – № 34. – 2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1556-18#Text
3. Про затвердження Положення про дистанційне навчання [Електронний ресурс]. – Наказ МОН № 466. – 2013. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0703-13#Text
4. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] . – Закон України № 45. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. *Панасенко І. В*. Дистанційне навчання в Україні: аналіз загроз і викликів. [Електронний ресурс]. – Бізнес Інформ. – 2021. – Режим доступу до ресурсу: https://www.business-inform.net/main/
6. *Yong Chen, Wu He*. Security Risks and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning. – IRRODL. – 2013. – №14. – С. 108–127.
7. *Гарасимчук О. І.* Організація захисту результатів контролю знань в системах дистанційного навчання. Кібербезпека: освіта, наука, техніка // Київський університет імені Бориса Грінченка. – 2020. – № 2(10). – С. 122–157.
8. Типове положення про службу захисту інформації в автоматизованій системі. НД ТЗІ 1.4-001-2000
9. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. НД ТЗІ 2.5-010-03
10. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-002-99

References

1. Verkhovna Rada of Ukraine. (2014). On Higher Education: Law of Ukraine No. 34 [Electronic resource]. Retrieved from https://zakon.rada.gov.ua/laws/show/1556-18#Text
2. Ministry of Education and Science of Ukraine. (2013). On the Approval of the Regulation on Distance Learning: Order No. 466 [Electronic resource]. Retrieved from https://zakon.rada.gov.ua/laws/show/z0703-13#Text
3. Verkhovna Rada of Ukraine. (1994). On the Protection of Information in Information and Communication Systems: Law of Ukraine No. 31 [Electronic resource]. Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
4. Verkhovna Rada of Ukraine. (2017). On the Basic Principles of Ensuring Cybersecurity of Ukraine: Law of Ukraine No. 45 [Electronic resource]. Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. *Panasenko, I. V.* (2021). Distance Learning in Ukraine: Analysis of Threats and Challenges [Electronic resource]. Business Inform. Retrieved from https://www.business-inform.net/main/
6. *Chen, Y., & He, W.* (2013). Security Risks and Protection in Online Learning: A Survey. The International Review of Research in Open and Distance Learning, 14, 108–127.
7. *Harasymchuk, O. I.* (2020). Organization of Protection of Knowledge Assessment Results in Distance Learning Systems. Cybersecurity: Education, Science, Technology, 2(10), 122–157. Kyiv: Borys Grinchenko Kyiv University.
8. Standard Regulation on the Information Protection Service in an Automated System. ND TZI 1.4-001-2000.
9. Requirements for Information Protection of Web Pages from Unauthorized Access. ND TZI 2.5-010-03.