Національний університет «Одеська юридична академія»
Факультет кібербезпеки та інформаційних технологій
Наукове товариство молодих вчених, аспірантів і студентів

ВСЕУКРАЇНСЬКА
НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

м. Одеса

29 листопада 2019 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАУКОВЕ ТОВАРИСТВО МОЛОДИХ ВЧЕНИХ,
АСПІРАНТІВ ТА СТУДЕНТІВ

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ
Всеукраїнської науково-практичної конференції

29 листопада 2019 року

Одеса
2019

УДК 004.056(063)
К38

Друкується за наказом ректора
Національного університету «Одеська юридична академія»
В. Є. Загороднього
(наказ №2410-62 від 2 жовтня 2019 року)

Відповідальний редактор – в.о. декана факультету кібербезпеки та інформаційних технологій, доцент О. В. Дикий.

Укладачі:
Кузьма Яна Іванівна – диспетчер деканату факультету кібербезпеки та інформаційних технологій.
Стоянова Тетяна Федорівна – диспетчер деканату факультету кібербезпеки та інформаційних технологій.
Пастернак Юрій Юрійович – студент 3 курсу факультету кібербезпеки та інформаційних технологій.

Кібербезпека в сучасному світі: матеріали всеукраїнської науково-практичної конференції (м. Одеса, 29 листопада 2019 р.) / за ред. О.В. Дикого ; уклад.: Я.І. Кузьма, Т.Ф. Стоянова, Ю.Ю. Пастернак. – Одеса: Видавничий дім «Гельветика», 2019.–332 с.

ISBN 978-966-916-949-5

У збірнику містяться матеріали доповідей, присвячених актуальним проблемам кібербезпеки в сучасному світі.
Подані матеріали конференції відповідають сучасним тенденціям розвитку кібербезпеки в Україні та можуть бути корисним и як у навчальному процесі, так і при проведенні наукових досліджень студентами та молодими вченими, а також для практичних працівників у зазначеній сфері

УДК 004.056(063)

ISBN 978-966-916-949-5

Логінова Н. І.

Національний університет «Одеська юридична академія», в.о. завідувача кафедри інформаційних технологій , кандидат педагогічних наук, доцент

ДЕЯКІ ПИТАННЯ КІБЕРБЕЗПЕКИ В СИСТЕМІ УПРАВЛІННЯ НАВЧАННЯМ MOODLE

Згідно до ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Кіберпростір – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних [1].

Використання кіберпростору в навчальному процесі є необхідною умовою для створення єдиного інформаційного навчального простору, що дозволяє забезпечити доступність та ефективність навчання за допомогою систем управління навчанням. Найбільш поширеною з яких є система управління навчанням Moodle, що використовує кіберпростір для розміщення навчальної інформації та персональних даних користувачів, які можуть стати об'єктами протиправних дій комп'ютерних зловмисників. Отже, кібербезпека систем управління навчанням в сучасних умовах інформатизації освіти є одним з пріоритетних питань.

Система управління навчанням Moodle являє собою розподілений додаток, який побудований на базі інформаційної системи, що використовує веб-ресурси для організації інтерактивної взаємодії викладачів та студентів. Під час функціонування система піддається низки негативних впливів випадкового та навмисного характеру, що може привести до порушення кібербезпеки не тільки самої системи, але й користувачів.

Найбільш ймовірними каналами витоку інформації в системі управління навчанням Moodle є:

- несанкціонований доступ до інформації, що зберігається та обробляється в системі;
- несанкціонований вплив на програмні засоби з метою порушення цілісності, доступності та конфіденційності інформації;
- міжсайтова вразливість та зараження комп'ютерними вірусами, троянськими програмами тощо.

Для запобігання несанкціонованому доступу до інформації в системі управлінням навчанням Моосіїе є ідентифікація та аутентифікація, оскільки всі сучасні механізми захисту інформації розраховані на роботу з іменованими суб'єктами та об'єктами. Суб'єктами в LMS Moodle є користувачі та процеси навчання, а об'єкти – персональна інформація та навчальні інформаційні ресурси. Для доступу до ресурсів системи управління навчанням Moodle необхідно пройти

аутентифікацію, яка здій снюється за деякими параметрами: ім'ям входу (логіном), паролем, персональними даними (ім'я, прізвище, адреса електронної пошти, місто тощо). Для захисту інформацій них ресурсів у системі використовуються політики користувачів, які зазначають набор визначених прав у межах системи (менеджер, автор курсу, викладач, асистент, студент, гість та інші). За цими правами налаштовуються розмежування доступом – користувачі отримують тільки той рівень доступу, який їм необхідний при роботі в системі [2].

Най більш поширені ризики безпеки пов'язані з несанкціонованому впливу на програмні засоби з метою порушення цілісності, доступності та конфіденцій ності інформації. До них відносяться завантаження підроблених завдань або видалення деяких навчальних контентів (тестів, матеріалів іспитів тощо). Можливе передача прав користувачів, коли студенти передають свої персональні дані аутентифікації з метою проходження тестів з інших точок доступу. Для запобігання цього в системі передбачено блокування доступу по IP-адресам та налаштування одноразового входу в систему.

Міжсай това вразливість – це порушення кібербезпеки через веб-додатки, вчинення протиправних дій спрямованих на отримання персональної інформації користувачів системи, блокування доступом до навчальних контентів, виведення з ладу програмного забезпечення. Най поширенішою (до 78%) є міжсай тове виконання сценаріїв (Cross Site Scripting), що дозволяє атакуючому впливати на вміст веб-сторінки, яка відображається в браузері користувача, з метою поширення шкідливого коду або отримання облікових даних користувача.

Останнім часом спостерігається збільшення числа DDos-атак на комп'ютерні навчальні ресурси в різних університетах світу. Як правило , ці атаки виникають в період сесій та їх дії спрямовані на зриві заходів по оцінці рівнів знань здобувачів освіти. Фахівці в галузі кібербезпеки стверджують, що в мережевому андеграунді існує низка сай тів, які готові виконати замовлену DDos-атаку за помірну плату, яка по кишен і навіть студенту [3].

Забезпечення кібербезпеки системи управління навчанням Moodle має бути комплексним: необхідно вдосконалювати вже наявні засоби щодо безпеки інформацій них ресурсів самої системи та вдосконалювати системи захисту хостингів, на яких застосовуються веб-додатки та баз и даних Moodle.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 08.07.2018 р. // Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403.
2. Логінова Н.І. Напрями захисту інформації в системі управління навча нням Moodle // Правове життя сучасної України: матер, міжнар. наук.-практ. конф. (17 вересня 2018 р.). – Одеса: Видавничий дім «Гельве тика», 2018. – С. 598-600.
3. DDos во время экзаменационной сессии. URL: https://threatpost.ru/ddos_vo_vremja_ekzamenatsionnoj_sessii/ 8466/ (дата звернення 1.11.2019).

Наукове видання

КІБЕРБЕЗПЕКА В СУЧАСНОМУ СВІТІ: АКТУАЛЬНІ ВИКЛИКИ

МАТЕРІАЛИ Всеукраїнської науково-практичної конференції

29 листопада 2019 року, м. Одеса

Верстка – О. С. Данильченко

Підписано до друку 7.10.2019. Формат 60х84/16. Папір офсетний . Гарнітура Cambria. Цифровий друк. Умовно-друк. арк. 19,30. Тираж 150. Замовлення № 1119-229. Ціна договірна. Віддруковано з готового оригінал-макета.

Видавництво і друкарня – Видавничий дім «Гельветика» 65101, Україна, м . Одеса, вул. Інглезі, 6/1 Тел.: + 38 (095) 934 48 28, + 38 (097) 723 06 08 E-mail: mailbox@helvetica.com.ua Свідоцтво суб'єкта видавничої справи ДК № 6424 від 04.10.2018 р.