***La bibliographie:***

1. Кібербулінг: загроза XXI століття [Електронний ресурс] – Режим доступу : https://naurok.com.ua/post/kiberbuling-zagroza-hhi-stolittya. – Дата звернення: 07.04.2019 р.
2. Кібербулінг: новітні небезпеки в інтернет-просторі [Електронний ресурс] – Режим доступу https://t-pravda.net/society/other/210137-kberbulng-novtn-nebezpeki-v-nternet-prostor.html?lang=ru. – Дата звернення: 07.04.2019 р.

**Key words:** Cyber-bullying, Internet – mobing, cyberbullying, trolling, harassment, aggression, ways of protection.
**Ключові слова:** кібербулінг, тролінг, переслідування, агресія, способи захисту.
**Ключевые слова:** кибербуллинг, троллинг, преследования, агрессия, способы защиты.

***ЛОГІНОВА НАТАЛІЯ ІВАНІВНА***

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

## АНАЛІЗ ВРАЗЛИВОСТЕЙ ІНФОРМАЦІЇ В СИСТЕМІ УПРАВЛІННЯМ НАВЧАННЯМ MOODLE

Інформатизація вищої освіти за допомогою інформаційно-комунікаційних технологій (ІКТ) є одним з пріоритетних напрямів розвитку сучасного інформаційного суспільства. Для вдосконалення традиційного навчального процесу, забезпечення доступності та ефективності навчання використовуються системи управління навчанням, які дозволяють створити єдиний інформаційний навчальний простір, використовуючи комунікаційні мережі, комп'ютери та мобільні пристрої. Системи управління навчанням забезпечують доступ студентів до навчальної інформації, зручно та швидко, у будь-який час надають можливість отримати консультацію викладача в електронному вигляді за допомогою ІКТ.

Сьогодні існує багато систем управління навчанням, які дозволяють здійснювати електронне навчання, організують інтерактивну взаємодію викладачів та студентів за допомогою засобів ІКТ. Найбільш поширеною є система управління навчанням Moodle, яка розповсюджується вільно з відкритим кодом, яка дає можливість створювати та публікувати навчальні курси, засновані на ІКТ. Курси є вмістом навчальних дисциплін, а також містять засоби, що дозволяють реалізувати різні форми і методи навчання та здійснювати контроль знань [1].

Moodle – це веб-додаток, який розміщено на персональному комп'ютері або віртуальному хостингу та підключено до мережі інтернет. Для роботи системи використовується веб-сервер, сервер бази

даних та додаток. Кожний з цих компонентів може бути використаний для незаконного доступу комп'ютерних зловмисників з метою отримання інформації про користувачів і навчальні контенти, а також для розповсюдження вірусів, піратських кодів тощо. Тому для даної системи актуальні наступні питання інформаційної безпеки: захист інформаційних ресурсів системи; захист від мережевих атаки; захист від комп'ютерних вірусів; захист проти злому паролів користувачів тощо.

Інформаційні ресурси системи містять персональну інформацію користувачів та навчальний контент (курси), які можуть захищатися безпосередньо засобами Moodle.

Кожний користувач системи управління навчанням Moodle має свій профіль, який містить персональну інформацію. Рівень доступу до такої інформації визначається політикою конфіденційності. В системі виконується ідентифікація та аутентифікація користувачів, оскільки всі сучасні механізми захисту інформації розраховані на роботу з іменованими суб'єктами та об'єктами. Суб'єктами в Moodle є користувачі та процеси навчання, а об'єкти – персональна інформація та навчальні інформаційні ресурси [2].

Захист інформації, яка міститься в курсах здійснюється за допомогою резервного копіювання, що забезпечує захист навчального контенту від помилок та збоїв обладнання.

Доступ до системи управління навчанням Moodle здійснюється за допомогою мережі інтернет, тому для неї актуальні проблеми захисту від мережевих атак.

Наприклад, міжсайтова вразливість (XSS – Cross Site Scripting) – вважається найбільш безпосередньою шкодою для конфіденційності користувачів і поширення вірусів. XSS – це тип атаки на веб-додатки, що впроваджує в веб-браузери користувачів шкідливий код, який виконується на комп'ютері при відкритті веб-сторінки та взаємодії з веб-сервером зловмисника. Існує декілька типів таких вразливостей:

– постійні XSS-атаки – виникають коли зловмисник впроваджує шкідливі дані до веб-додатку та вони постійно зберігаються в базі даних та забезпечують несанкціонований доступ до системи;

– непостійні XSS-атаки – тип мережевої атаки, коли впроваджений код відправляє відвідувачу сайту повідомлення про помилку, що включає деякі або всі вхідні дані, відправленні на сервер як частина запиту;

– DOM-атаки – це атаки на основі об'єктної моделі документу (Document Object Model) та вони відбуваються, якщо JavaScript на сторінці отримує доступ до параметрів URL і використовує його для запису HTML на сторінку [3].

Система управління навчання Moodle як веб-додаток піддається також зараженню комп'ютерними вірусами та троянськими програмами, SQL ін'єкціям, злому паролів користувачів системи тощо.

Однак, не зважаючи на існуючи вразливості система управління навчанням Moodle є безпечної для організації навчального процесу засобами ІКТ. Для протидії існуючим вразливостям в системі управління навчанням Moodle передбачено постійне оновлювання версій програм,

оскільки кожна нова версія містить виправлення та захист від сучасних комп'ютерних вірусів і троянських програм. Для безпечної роботи системи необхідно періодично змінювати паролі адміністраторів. Вживати заходи протидії впровадженню SQL ін'єкцій. Використовувати антивірусні програми тощо. Безпека системи полягає в постійному адмініструванні веб-сервера та бази даних, захисту від перенавантажень, а також вирішення технічних та організаційних питань.

***Список використаної літератури:***


1. Логінова Н.І. Забезпечення інформаційної безпеки в системі управління навчанням MOODLE / Н. І. Логінова // Правові та інституційні механізми забезпечення розвитку України в умовах європейської інтеграції: матер. міжнар. наук.-практ. конф. (18 травня 2018 р.): у 2 т. – Т. 1. – Одеса: Видавничий дім «Гельветика», 2018. – С. 598–600.
2. Логінова Н.І. Напрями захисту інформації в системі управління навчанням MOODLE / Н. І. Логінова // // Правове життя сучасної України: матер. міжнар. наук.-практ. конф. (17 вересня 2018 р.). – Одеса: Видавничий дім «Гельветика», 2018. – С. 188–191.
3. Tawfiq S. Barhoom, Rola J. Azaiza. Enhance MOODLE Security Against XSS Vulnerabilities // International Journal of Computing and Digital Systems. – № 5. – 2016.



**Ключові слова**: система управління навчанням Moodle, інформаційна безпека, вразливість інформації.

**Ключевые слова**: система управления обучением Moodle, информационная безопасность, уязвимость информации.

**Key words**: learning management systems Moodle, information security, information vulnerability



***ТРОФИМЕНКО ОЛЕНА ГРИГОРІВНА***

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент


## МОНІТОРИНГ СТАНУ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Під час становлення інформаційного суспільства інформаційно-комунікаційні технології (ІКТ) – інтернет, новітні технології, цифрові послуги і пристрої – стають невід'ємною частиною нашого сьогодення. Разом з усіма перевагами від впровадження ІКТ вкрай небезпечно не враховувати можливі кіберзагрози світовому співтовариству як зворотній бік цього процесу. Останнім часом дедалі частіше суспільство стикається з різноманітними видами кібератак: збої при наданні електронних послуг, блокування роботи державних органів, фішингові атаки електронною поштою, кіберзлочини, порушення цілісності та