СЕКЦІЯ 7.

ІНФОРМАТИЗАЦІЯ СУСПІЛЬСТВА ТА ЗАХИСТ ІНФОРМАЦІЇ

Логінова Наталія Іванівна

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

НАПРЯМИ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМІ УПРАВЛІННЯ НАВЧАННЯМ MOODLE

Впровадження інформаційно-комунікаційних технологій (ІКТ) в системі вищої освіти дозволяє змінити та розширити традиційні форми навчального процесу: лекції, семінари та практичні заняття, вдосконалити самостійну підготовку. Також використання ІКТ в освіті привело до появи нових навчальних програмних засобів: комп'ютерних навчальних систем, електронних версій дисциплін, засобів контролю знань та ін., об'єднаних в єдиний електронний навчальний простір за допомогою систем управління навчанням Learning Management Systems (LMS).

Системи управління навчанням LMS – це прикладні програмні продукти для управління навчальною діяльністю. Вони дозволяють розробляти й поширювати навчальні матеріали, використовуючи комунікаційні мережі, забезпечувати доступ до інформації, організовувати навчальний процес і контролювати результати навчання. З їх допомогою організується централізоване та автоматизоване управління навчальним процесом. Системи LMS дозволяють швидко та зручно, у будь-який час сформувати та доставити навчальну інформації до студента за допомогою веб-технологій. Забезпечують підтримку мобільності навчання та відповідність всім стандартам вищої освіти.

Серед сучасних систем управління навчанням LMS, які ефективно доповнюють традиційне навчання електронним, найбільш поширеною є система управлінням навчанням Moodle, в якої містяться навчальні інформаційні ресурси та персональні дані користувачів. Тому сукупність внутрішніх і зовнішніх інформаційних загроз створює передумови для порушення безпечного функціонування системи [1].

Хоч в системі управління навчанням Moodle використовуються документи переважно без грифів секретності, навчальні інформаційні ресурси містять дані, що відносяться до інформації з обмеженим доступом та потребують захисту. До того ж забезпечення конфіденційності, цілісності та доступності інформації в таких системах потребує застосування різних заходів захисту [2].

Забезпечення інформаційної безпеки в системи управління навчанням Moodle повинно здійснюватися комплексно та включати до себе різні напрями захисту.

Захист інформації – це комплекс заходів, що проводяться власником інформації щодо забезпечення своїх прав на володіння інформацією і її поширення, створення умов, що обмежують її поширення і виключають або істотно ускладнюють несанкціонований, незаконний доступ до інформації та її носіїв.

Технічний напрям захисту інформації базується на використанні різноманітних апаратно-програмних і криптографічних засобів захисту. Заходи щодо технічного захисту інформації повинні враховувати вимоги до захисту і режиму доступу, відповідно до рівня конфіденційності інформації. Більш важлива за рівнем вимог до захисту інформація вимагає більш ретельних систем захисту.

До технічних засобів захисту інформації відносяться системи ідентифікації та аутентифікації користувачів, керування політиками безпеки, криптографічні перетворення інформації, антивірусний захист, системи керування доступом, аудит та моніторинг подій в системі.

Основою захисту інформації в системі управлінням навчанням Moodle є ідентифікація та аутентифікація користувачів, 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 здійснюється за деякими параметрами: ім'ям входу (логіном), паролем, персональними даними (ім'я, прізвище, адреса електронної пошти, місто, країна тощо). При використанні даної системи у навчальному процесі адміністратор визначає метод аутентифікації користувачів. Передбачено декілька варіантів запису на курс, але найбільш поширеними є ручна реєстрація та самостійна реєстрація по електронній пошті.

Для захисту інформаційних навчальних ресурсів від сторонніх користувачів, як правило, використовується ручна реєстрація, коли всі студенти автоматично додаються на сервер та викладачі видають їм логіни та паролі для доступу до навчальних ресурсів.

Цей спосіб є ефективним з точки зору безпеки системи. Реєстрація сторонніх користувачів буде не можлива.

Парольний захист є одним із поширених засобів захисту інформації в системі управління навчанням Moodle. Політикою безпеки сайту передбачена перевірка паролів користувачів на складності паролів, яка визначається наступними параметрами: довжина паролю, кількість цифр, букв в нижньому та верхньому регістрах, спеціальних символів та послідовність однакових символів.

Для захисту інформаційних 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.

Для перевірки знань студентів в системі передбачено комп'ютерне тестування, при якому виникають питання ідентифікації студентів та забезпечення доступу сторонніх користувачів. Для цього в системі передбачено використання IP-блокатора. Тобто доступ до системи можна здійснити лише в мережі навчального закладу. Система також передбачає заборону паралельного входу під одним обліковим записом, що не дає можливість виконати тест іншою особою.

В системі управління навчанням Moodle підтримується антивірусна перевірка завантажених файлів за допомогою вбудованою антивірусною програмою Clam Antivirus (AV), яку потрібно додатково встановити до системи.

До засобів захисту інформаційних ресурсів в системі відноситься моніторинг подій, який дозволяє адміністратору та викладачам отримувати повідомлення про події, які відбуваються в Moodle. Для викладачів доступна інформація про діяльність кожного студента або групи в курсах. Система моніторингу надає відомості про перегляд курсів, окремих елементів, активності студентів за певний проміжок часу. Адміністратор системи за допомогою моніторингу може відстежити коли та як здійснювався доступ до інформаційних ресурсів, відновити будь-який сценарій сеансу роботи зареєстрованого користувача, а саме: перелік сторінок, відвіданих за сеанс роботи; час, проведений на кожній сторінці; перелік файлів, які були скопійовані; час тестування тощо [3].

Крім вбудованих функцій захисту інформації та інформаційних ресурсів в системі управління навчанням Moodle передбачено використання різних плагінів, що надають можливість вдосконалити систему захисту окремих елементів курсів та користувачів системи.

Отже, захист навчальних інформаційних ресурсів в системі управління навчання Moodle є комплексним та дозволяє забезпечити безпеку інформації.

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. Будік О. О., Чекурін В. Ф. Специфічні загрози інформаційній безпеці систем електронного навчання. – [Електронний ресурс]. – Режим доступу: http://science.lp.edu.ua/uk/node/2044.
3. Герасименко І. В. Технології захисту даних у системі підтримки дистанційного навчання / І. В. Герасименко // Інформаційні технології і засоби навчання. – 2015. – Том 47. – № 3. – С. 150–159.

Kozin Oleksandr Borisovich

National University «Odessa Law Academy»
Associate Professor of the Department of Information Technologies
Ph.D of Physical-Mathematical Sciences, Associate Professor

Papkovskaya Olga Borisovna

Odessa National Polytechnic University
Associate Professor of the Department of Higher Mathematics
and Systems Modeling, Ph.D of Physical-Mathematical Sciences,
Associate Professor

TRENDS IN THE DEVELOPMENT OF E-GOVERNMENT AND E-TRUST SERVICES

E-government is one of the areas of organization of the state authorities through the system of local information networks and segments of the Internet on a single platform. This guarantees the activity of the authorities in real time and creates the most easy and accessible daily communication with them residents, legal entities, non-governmental institutions. The main element of online management is the e-government, as the general infrastructure of inter-agency computerized information interaction between government institutions and regional self-government bodies with residents, entrepreneurs and other businesses. This is an addition or analogue of the classical government. It only determines another way of interaction, relying on the active use of information and communication technologies to improve the performance of government services.

There are various approaches to determining the model of e-governance. A typical or classic approach describes the links between key e-government actors and includes components such as: «Government – Government» (G2G – «government to government»);