УДК 004.056.5 д.т.н., доц. **Оксіюк О.Г.** (КНУ)

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ УПРАВЛІННЯ НАВЧАННЯМ

У статті проаналізовано особливості забезпечення захисту інформації в системах управління навчанням, розглянуто можливості забезпечення санкціонованого доступу до матеріалів курсу за допомогою впровадження політики рольового розмежування доступу, показано основні загрози фальсифікації результатів навчання та можливі методи та моделі протидії цим загрозам. Визначенні особливості забезпечення інформаційної безпеки в системах управління навчанням. Розглянуто можливості забезпечення санкціонованого доступу до матеріалів курсу за допомогою впровадження політики рольового розмежування доступу до інформаційних ресурсів у систему дистанційного навчання. Проведений аналіз методів та підходів до побудови систем розпізнавання та ідентифікації користувачів комп'ютера на основі інформаційних моделей. Визначено особливості кожного із розглянутих методів, їх переваги, недоліки та напрями подальшого використання.

Ключові слова: система управління навчанням, захист інформації, інформаційна система, політика інформаційної безпеки, інформація.

Інформація – текстова, числова, графічна, звукова, незалежно від того, чи є вона власністю держави, суспільства або окремих організацій чи фізичних осіб, становить певну цінність. Тому навчальний інформаційний ресурс потребує постійного захисту від різних сторонніх впливів і джерел загроз, які можуть призвести до зниження їхньої цінності, порушення конфіденційності, цілісності та доступності. Розвиток інформаційних систем, їх ускладнення, взаємна інтеграція та відкритість призводять до появи нових джерел загроз інформації, зростання кількості зловмисників, котрі мають потенційну можливість здійснити вплив на неї.

Інформаційні технології як невід'ємна складова сучасного суспільства все глибше проникають практично в усі сфери діяльності людини. Водночас людство з кожним роком стало все інтенсивніше їх використовувати. Повсякденне застосування інформаційних технологій має значні переваги: підвищується ефективність процесу управління; значно збільшується швидкість оброблення та передачі даних; покращується захист інформації від зловмисних дій і т.п. Саме тому забезпечення безпеки не тільки самої інформації, але й безпосередньо інформаційних технологій є актуальною проблемою, яка вимагає нагального вирішення.

Метою статті є визначення особливостей забезпечення інформаційної безпеки в системах управління навчанням.

Система управління навчанням – система управління навчальною діяльністю, яка використовується для розробки, управління та поширення навчальних матеріалів із забезпеченням спільного доступу. Програмне забезпечення системи управління навчанням складається з двох частин: клієнтської і серверної.

До складу клієнтської частини входять два компоненти: підсистема навчання та підсистема діагностування. Серверна частина системи електронного навчання реалізується на основі спеціалізованого програмного забезпечення і являє собою систему управління навчальним процесом.

Використання систем управління навчанням передбачає доступність для студента навчальних матеріалів (тексти лекцій, завдання до практичних/лабораторних та самостійних робіт; додаткові матеріали (книги, довідники, посібники, методичні розробки) та засобів для спілкування і тестування протягом 24 годин 7 днів на тиждень.

Для захисту інформації у системах управління навчанням першочерговими завданнями є забезпечення санкціонованого доступу користувачів до матеріалів курсу, а також автентичності навчальної звітності. Розглянемо детальніше можливості забезпечення кожної з вимог.

Контроль за доступом. Умовою забезпечення надійного захисту інформації у системі управління навчанням є розроблення та впровадження політики інформаційної безпеки [1]. За її відсутності у аналогічній системі можуть виникати протиправні дії зловмисників щодо курсів навчальних програм загалом, так і кожного з користувачів (викладач, курсант/студент, ад'юнкт) зокрема [2].

Система керування процесом навчання передбачає управління великими базами даних (індивідуальні дані користувачів, навчальні програми, лекційні та лабораторні матеріали, репозитарій тощо) та надання доступу до певної інформації різним категоріям користувачів (адміністратори, педагогічний склад, курсанти/студенти, ад'юнкти) [3]. Основним завданням політики безпеки у системі є захист інформаційних активів від зовнішніх і внутрішніх навмисних і ненавмисних джерел загроз [4].

Проведений у [5] огляд ряду найпоширеніших політик безпеки, які можуть застосовуватися до різних інформаційних систем, показав, що найоптимальнішою для систем управління навчанням є політика рольового розмежування доступу (РРД) до інформаційних ресурсів.

Основними елементами моделі РРД до інформаційних ресурсів системи керування навчанням є:

– $U = \{u_i, i = \overline{1,n}\}$ – множина користувачів системи: педагогічний склад, курсанти/студенти, ад'юнкти та ін.;

– $R = \{r_i, \quad i = \overline{1,n}\}$ – множина ролей системи: manager – адміністратор; course creator – автор курсу; teacher – викладач; non-editing teacher – викладач без права редагування; student – курсанти/студенти; guest – відвідувач; authenticated user – авторизований користувач та ін.;

– $P = \{p_i, \quad i = \overline{1,m}\}$ – множина прав доступу до об'єктів системи: навчальні курси, науковий репозитарій, особисті дані користувачів та ін.;

– $S = \{s_i, \quad i = \overline{1,n}\}$ – множина сеансів роботи користувачів системи, статистика роботи користувачів;

– $PA: R \to 2^P$ – функція, яка визначає для кожної ролі системи множину прав доступу;

– при цьому для кожного $p \in P$ існує $r \in R$ така, що $p \in PA(r)$;

– $UA: U \to 2^R$ – функція, яка визначає для кожного користувача системи множину ролей, на які він може авторизуватися;

– $user: S \to U$ – функція, яка визначає для кожного сеансу відповідного користувача системи, від імені якого він активований;

– $roles: S \to 2^R$ – функція, яка визначає для користувача системи множину ролей, на які він авторизований в цьому сеансі; при цьому в кожен момент часу τ для кожного сеансу $s \in S$ має виконуватися умова $roles(S) \subseteq UA(user(s))$. Принципово можуть існувати ролі системи, на які не авторизований жоден користувач.

Загальна схема моделі РРД до інформаційних ресурсів зображена на рис. 1.

Модель рольового розмежування доступу дає змогу чітко встановити рівні доступу кожного користувача системи до тої чи іншої інформації, що міститься в навчальних програмах, репозитарії та ін., проводити статистику сеансів роботи користувача.

Чітко встановлені рівні доступу до інформаційних ресурсів запобігають діям зловмисників, спрямованим на зміну властивостей інформації – цілісність, доступність, конфіденційність [4].

Автентичність навчальної звітності. Однією з складових систем управління навчанням є підсистема діагностування, що призначена для перевірки рівня знань студентів. Наявність такої підсистеми, звичайно, передбачає процес оцінювання та необхідність ведення журналу успішності. Таким чином, після виконання студентом чергової роботи, у

спеціальному файлі звітності має бути зроблено відмітку, яку не можна імітувати власноруч. Це можливо, якщо зловмиснику невідомий:

• спосіб створення такого запису-відмітки (секретність алгоритму);

• масив деяких даних, що включаються у запис (секретність ключа).

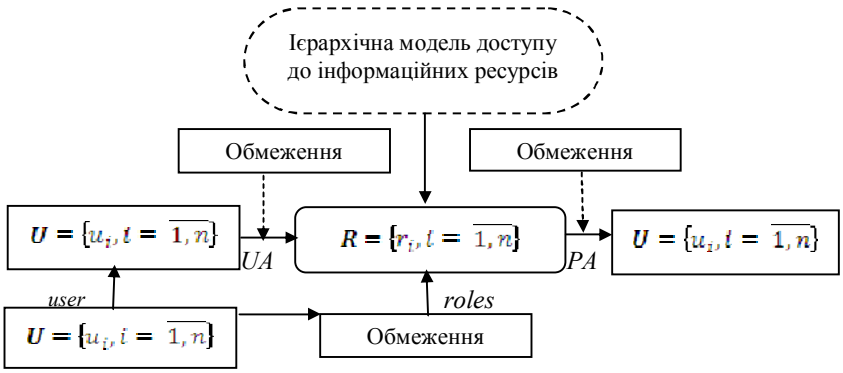

Рис. 1. Схема моделі РРД до інформаційних ресурсів системи управління навчанням

Обирати, що саме слід робити секретним: ключ чи алгоритм необхідно на основі аналізу трудомісткості злому відповідно секретного ключа та секретного алгоритму. Встановлено, що в даному випадку трудомісткість злому секретного алгоритму на порядок вища, ніж секретного ключа. Це пояснюється тим, що алгоритм захисту являє собою код, пов'язаний із іншою частиною ПЗ діалектичними зв'язками, тому зломщикові необхідно виконати великий обсяг роботи для аналізу цих посилань. В той же час, якщо алгоритм створення записів є відомим, то зломщикові достатньо віднайти статичні дані у коді ПЗ (ключ), що легко виконується шляхом трасування програми. Отже, використання секретного алгоритму в даному випадку є обґрунтованим.

Для виключення можливості видачі чужих результатів за свої у кожний запис файлу звітності слід вносити певну унікальну для даного i-того студента інформацію. В [6] було запропоновано шифрування запису за допомогою відкритого ідентифікатора студента e_i у якості ключа. Отриманий від студента результат на сервері розшифровується за допомогою секретного ідентифікатора студента d_i. e_i та d_i утворюють пару, і виступають відповідно відкритим та секретним ключами двохключової системи шифрування. Аналогічно результат виконання кожної роботи шифрується за допомогою відкритого ідентифікатора j-тої навчальної роботи w_j у якості ключа. На сервері результат розшифровуватиметься за допомогою відкритого ключа v_j.

Ще однією загрозою процесу електронного навчання є можливість підміни студента, коли працювати віддалено буде не сам студент, а його "довірена" особа. Для запобігання цієї ситуації слід впровадити біометричну автентифікацію особи студента [6]. Традиційні методи ідентифікації та аутентифікації, основані на використанні карток, електронних ключів чи інших переносних ідентифікаторів, а також паролів і кодів доступу, мають істотні недоліки. Головним недоліком таких методів є неоднозначність ідентифікованої особистості. Ще одним, не менш важливим недоліком традиційних методів ідентифікації є складність виявлення підміни ідентифікованого користувача.

Використання методів прихованого клавіатурного моніторингу дає змогу реалізувати процедури ідентифікації та аутентифікації. Підміну ідентифікованого користувача можна встановити на основі результатів процедури аутентифікації, що може провадитися безперервно. Крім цього, фактор прихованого спостереження допомагає виявити недозволених користувачів [7].

Висновки. У роботі проаналізовано особливості забезпечення захисту інформації в системах управління навчанням, розглянуто можливості забезпечення санкціонованого доступу до матеріалів курсу за допомогою впровадження політики рольового розмежування доступу, показано основні загрози фальсифікації результатів навчання та можливі методи протидії цим загрозам.

ЛІТЕРАТУРА:

1. Гайша О.О. Методики забезпечення захищеності систем дистанційної освіти : автореф. дис. на здобуття наук. ступеня канд. техн. наук : спец. 05.13.06 «Інформаційні технології» : захист 28.03.08 / Гайша Олександр Олександрович; Нац. ун-т кораблебудування ім. адм. Макарова – К., 2008. – 15 с.

2. Голубченко О.Л. Політика інформаційної безпеки / О.Л. Голубченко. – Луганськ : Вид-во СНК ім. В. Даля, 2009. – 300 с.

3. Заяць М.М. Аналіз методів та підходів до побудови систем розпізнавання та ідентифікації користувачів комп'ютера на основі інформаційних моделей / Заяць М.М., Заяць А.В. // Вісник Нац. ун-ту „Львівська політехніка" "Інформаційні системи та мережі". – 2011.– № 715. – С.114-122.

4. Сташевський З.П. Впровадження політики рольового розмежування доступу до інформаційних ресурсів у систему дистанційного навчання / Сташевський З.П., Лозинський О.І., Бурак Н.Є. // Вісник Львівського державного університету безпеки життєдіяльності : зб. наук. праць. – Львів: Вид-во ЛДУ БЖД. – 2012. – № 6. – С. 130-136.

5. Сташевський З.П. Політика інформаційної безпеки як один із методів забезпечення якості вищої освіти / Сташевський З.П., Бурак Н.Є., Грицюк Ю.І. // Проблеми інтеграції національних закладів вищої освіти до Європейського освітнього середовища: зб. мат. Міжнар. наук.-метод. конф. Том 2 "Проблеми взаємної адаптації системи вищої освіти". – Харків : Вид-во "Форт". – 2012. – С. 102-105.

6. С.В. Ленков, Д.А. Перегудов, В.А. Хорошко, Методы и средства защиты информации. В 2-х томах. –К.: Арий, 2008. – Том II.

7. Оксіюк О.Г. Проектування та застосування експертно-навчальних систем: Монографія / О.Г. Оксіюк, С.А. Шворов, Б.М. Герасимов. - Київ: Вид-во Європейського ун-ту, 2008. – 150 с.

Без рецензії.

д.т.н., проф. Оксиюк А.Г.

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ УПРАВЛЕНИЯ ОБУЧЕНИЯ

В статье проанализированы особенности обеспечения защиты информации в системах управления обучения, рассмотрены возможности обеспечения санкционированного доступа к материалам курса с помощью внедрения политики ролевого разграничения доступа, показаны основные угрозы фальсификации результатов учения и возможные методы и модели противодействия этим угрозам. Определении особенности обеспечения информационной безопасности в системах управления учебой. Рассмотрены возможности обеспечения санкционированного доступа к материалам курса с помощью внедрения политики ролевого разграничения доступа к информационным ресурсам в систему дистанционного обучения. Проведенный анализ методов и подходов к построению систем распознавания и идентификации пользователей компьютера на основе информационных моделей. Определены особенности каждого из рассмотренных методов, их преимущества, недостатки и направления дальнейшего использования.

Ключевые слова: система управления обучением, защита информации, информационная система, политика информационной безопасности, информация.

Ph.P. Oksiuk A.G.

FEATURES OF PROVIDING OF PRIV IN SYSTEMS MANAGEMENTS EDUCATING

In the article the features of providing of priv are analysed in control system of educating, possibilities of providing of the sanctioned access are considered to materials of course by means of introduction of politics of ролевого differentiation of access, the basic threats of falsification of results of studies and possible methods and models of counteraction to these threats are shown. Determination of feature of providing of informative safety in control system studies. Possibilities of providing of the sanctioned access are considered to materials of course by means of introduction of politics of ролевого differentiation of access to the informative resources in the controlled from distance departmental teaching. Conducted analysis of methods and going near the construction of the systems of recognition and authentication of computer users on the basis of informative models. The features of each are certain of the considered methods, their advantage, defects and directions of the further use.

Keywords: control system by studies, priv, informative system, politics of informative safety, information.