УДК 004.056

В.Ф. Чекурін, О.О. Будік

Національний університет «Львівська політехніка», Львів

МОДЕЛЬ СИСТЕМИ ЕЛЕКТРОННОГО НАВЧАННЯ ДЛЯ АНАЛІЗУ ЗАГРОЗ ЇЇ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

В роботі запропоновано модель системи електронного навчання (СЕН), яка зорієнтована на потреби аналізу загроз її інформаційній безпеці. Особливостями моделі є чіткий поділ СЕН на компоненти, врахування структури сучасних СЕН, включення в модель, крім програмної, також і апаратної частини, що дозволяє проводити комплексний аналіз загроз. Структура СЕН включає комп'ютерну інфраструктуру, платформу електронного навчання, інформаційні ресурси та людські ресурси. Платформу електронного навчання як специфічну складову СЕН розглянуто детальніше. Також проведено огляд специфічних загроз інформаційній безпеці СЕН.

Ключові слова: *електронне навчання, система електронного навчання, інформаційна безпека, захист інформації, загрози, вразливості.*

Вступ

Постановка проблеми. З початку впровадження інформаційних технологій в навчання дуже мало уваги присвячувалося проблемам інформаційної безпеки. Як наслідок, загальним недоліком більшості сучасних систем електронного навчання (СЕН), в тому числі, впроваджуваних в Україні [1], є слабо розвинені або взагалі відсутні механізми захисту інформації.

Для аналізу загроз інформаційній безпеці систем електронного навчання необхідно створити відповідну модель СЕН. На сьогоднішній день існує велика кількість моделей СЕН, зорієнтованих на конкретну реалізацію, проте узагальнена модель з урахуванням потреб аналізу інформаційної безпеки ще не створена. Тому розроблення такої моделі ***є актуальним завданням.***

Кожна СЕН може розглядатися як відкрита інформаційна система. Таким чином, як і будь-яка відкрита система, вона характеризується загальновідомими внутрішніми і зовнішніми загрозами. Для протистояння цим загрозам використовується загальна система захисту інформації. Для захисту СЕН від специфічних загроз, зумовлених областю застосування, необхідно ***визначити та класифікувати ці загрози, а також створити відповідні механізми захисту.***

Метою даної роботи є розроблення моделі системи електронного навчання для аналізу загроз її інформаційній безпеці, а також огляд деяких специфічних загроз.

Аналіз останніх досліджень. Є велика кількість поглядів на структуру систем електронного навчання. В роботі [2] запропоновано структурну модель системи навчання на базі Web-технологій. СЕН розглядається як сукупність трьох взаємопов'язаних видів ресурсів: технологічної інфраструктури, навчальних ресурсів і людських ресурсів. Недоліками цієї моделі є спрямованість на використанням веб-технологій, відсутність деяких важливих компонентів сучасних СЕН, зокрема, системи управління навчальним контентом (LCMS, Learning Content Management System). Чітко не виділені підсистеми СЕН, що не дозволяє аналізувати загрози інформаційної безпеки.

В британському стандарті UKeU eLearning Framework [3] описується каркас для систем електронного навчання. В ньому чітко виділяються компоненти СЕН, проте він також орієнтований на вебсистеми. Виділена окремо система адміністрування, яка чомусь знаходиться на одному рівні з системою управління навчанням (LMS, Learning Management System) і LCMS. З нашого погляду, це невірно, оскільки LMS та LCMS мають свої власні підсистеми адміністрування, які є важливими для виділення з позиції аналізу інформаційної безпеки. Цей каркас розглядає лише програмну складову СЕН і не бере до уваги апаратне забезпечення, що не дозволяє комплексно розглядати загрози.

Стандарт LTSA IEEE P1484-1 [4] розглядає СЕН як п'ятирівневу систему. Перевагою запропонованої моделі СЕН є чіткий опис компонентів на різних рівнях абстракції і взаємодії між ними, незалежність від конкретної технології реалізації. Але ця модель також охоплює лише програмну частину СЕН.

В Концепції інформаційної системи вищих навчальних закладів Хорватії [5] акцентується увага на інформаційних потоках в ВНЗ. Навчальна частина не розглядається.

Загальним недоліком розглянутих вище моделей СЕН з позиції аналізу інформаційної безпеки є виключення апаратної частини, а також відсутність

вираженої системи захисту інформації (СЗІ). Також в більшості моделей чітко не виділені основні компоненти, які використовуються в сучасних СЕН, а самі моделі, крім LTSA, пов'язані на конкретних технологіях. Запропонуємо модель СЕН, в якій усунено описані вище недоліки і яку можна використати для загального аналізу загроз.

1. Модель системи електронного навчання

Розглядаємо СЕН як масштабовану систему, яка може функціонувати на окремому комп'ютері, в локальних і/або глобальних мережах в середовищах Web, GRID і хмаркових технологій. Беручи до уваги розглянуті вище моделі СЕН та потреби аналізу інформаційної безпеки, представляємо СЕН у вигляді каркасу, який складається з чотирьох основних частин – комп'ютерної інфраструктури (КІ), платформи електронного навчання (ПЕН), інформаційних ресурсів (ІР) та людських ресурсів (ЛР) (див. рис. 1).

1.1. Комп'ютерна інфраструктура. Призначенням КІ є надання обчислювальних ресурсів для підтримки функціонування СЕН. Вона включає комп'ютерне апаратне забезпечення, системне програмне забезпечення, комунікаційне обладнання і систему захисту інформації КІ. КІ можуть формувати, в залежності від масштабу СЕН, окремий комп'ютер, локальна мережа факультету, корпоративна мережа університету з віддаленим доступом, віртуальна область середовищ GRID чи хмаркових обчислень. В складі КІ слід виділити загальну СЗІ, яка протистоїть типовим загрозам.

3.2. Платформа електронного навчання. ПЕН включає сукупність програмних і апаратних засобів, які формують відповідне віртуальне навчальне середовище з використанням інформаційних ресурсів і механізмів політики безпеки ПЕН, - апаратура спеціального призначення, системне і прикладне програмне забезпечення ПЕН, система захисту інформації ПЕН.

Апаратура спеціального призначення включає обладнання, яке безпосередньо використовується в навчальному процесі. Це може бути обладнання для симуляції фізичних процесів, лабораторне обладнання, дослідницьке обладнання з віддаленим доступом тощо.

Системне програмне забезпечення ПЕН забезпечує функціонування усіх її частин. Воно включає інтерфейс користувача, LCMS, LMS та комунікаційний модуль (рис. 2).

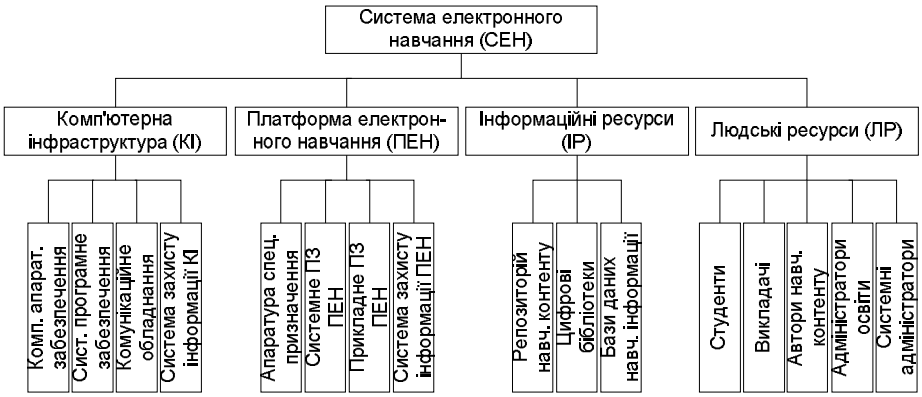

Рис. 1. Структурна модель СЕН

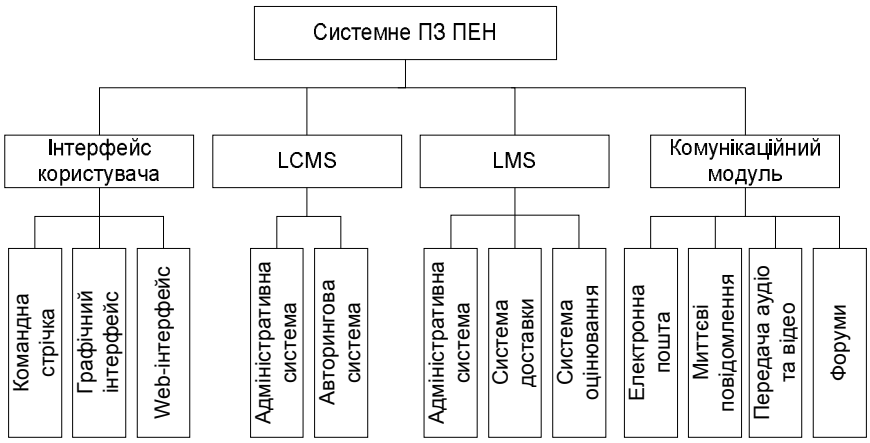

Рис. 2. Структурна модель системного програмного забезпечення ПЕН

Інтерфейс користувача надає користувачам локальний чи віддалений доступ до функцій ПЕН відповідно до їх прав. В залежності від типу СЕН і ролі користувача це може бути командна стрічка, графічний чи Web-інтерфейс.

LCMS призначена для забезпечення створення, модифікації, управління навчальним контентом. Вона складається з адміністративної і авторингової систем, які взаємодіють з навчальним репозиторієм і LMS.

LMS є ядром ПЕН. Вона виконує такі типові для неї функції: реєстрацію студентів на курси, надання доступу до інформаційних каталогів і навчального контенту відповідно до прав користувачів, відстеження активності і навчального прогресу студентів, формування звітів, тестових та екзаменаційних завдань, автоматизоване оцінювання знань. В загальному вона складається з адміністративної системи, систем доставки та оцінювання.

Адміністративна система LMS реалізує в віртуальному навчальному середовищі функції деканату. Вона відповідає за управління всіма учбовими заходами, навчальними процесами, планування активності студентів, контроль, реєстрацію та моніторинг користувачів, надає функції календаря тощо.

Система доставки відповідає за формування порцій навчального контенту відповідно до навчальних планів і заходів та доставку їх користувачу.

Система оцінювання надає засоби для автоматизованої перевірки знань студентів та вимірювання ефективності роботи викладачів.

Комунікаційний модуль підтримує обмін інформацією між користувачами в рамках навчальних чи/і адміністративних процесів. Він реалізує функції синхронної, асинхронної чи змішаної комунікації з використанням доступних комунікаційних засобів: електронна пошта, миттєві повідомлення, передача аудіо та відео, форуми тощо.

Прикладне програмне забезпечення надає користувачам операційні сервіси загального і спеціального призначення. Воно складається з інструментальних засобів загального і спеціального призначення. Засоби загального призначення це сукупність серійних програмних продуктів, що використовуються в навчальному процесі. Ними можуть бути офісні пакети (MS Office, IBM Lotus, OpenOffice), комунікаційні засоби (ICQ, Skype, MSN Messenger), Web-браузери, CAD/CAM-системи (AutoCad, MathCad, Maple), середовища для розробки програм (C++ Visual Studio, Eclipse, Delphi).

Інструменти спеціального призначення це програмні і апаратні продукти, призначені для задоволення специфічних потреб навчального процесу. Серед них можуть бути навчальні інструменти, інструменти оцінювання знань, високо спеціалізовані системи, віртуальні лабораторії, симулятори різних типів, емулятори, тренінгові системи тощо.

Ми пропонуємо окремо виділити СЗІ платформи електронного навчання, яка захищає віртуальне навчальне середовище від специфічних загроз, які не можуть буди подолані загальною СЗІ КІ. Вона включає технічні і організаційні механізми безпеки для реалізації політики безпеки віртуального навчального середовища. Ця СЗІ забезпечує управління профілями користувачів СЕН, ідентифікацію, автентифікацію і авторизацію користувачів в навчальному віртуальному середовищі, реєструє події для аудиту інформаційної безпеки, захищає інформаційні ресурси і СЕН від специфічних внутрішніх і зовнішніх загроз.

1.3. Інформаційні ресурси. Інформаційні ресурси поділяються на три частини – репозиторій навчального контенту, цифрові бібліотеки, та бази даних навчальної інформації. Навчальний контент включає навчальні програми, розклади, бази знань, мультимедійні лекції, навчальні курси, електронні методики, тестові завдання тощо. Бази даних зберігають структуровану інформацію, яка відноситься до всіх членів системи людських ресурсів СЕН, про всі події, їх наслідки і задіяних у них користувачів, адміністративну ін формацію.

3.4. Людські ресурси. Людські ресурси СЕН об'єднують усіх учасників навчального процесу, які отримують і надають навчальні сервіси, а також підтримують функціонування СЕН. Це є студенти, викладачі, автори навчального контенту, адміністратори освіти, системні адміністратори. Людські ресурси є структурованою ієрархічною динамічною системою, члени якої розрізняються за ролями і привілеями.

2. Специфічні загрози інформаційній безпеці СЕН

Для кожної складової СЕН (КІ, ПЕН, ІР, та ЛР) характерний набір специфічних загроз. Типові загрози, які виявляються в КІ, визначаються в політиці безпеки КІ і можуть бути усунені загальною СЗІ. СЗІ ПЕН призначена для протистояння специфічним загрозам, які виявляються в ПЕН, ІР і ЛР. До створення СЗІ ПЕН необхідно розробити політику безпеки для ПЕН, сформувати вимоги безпеки і специфікації, вибрати відповідні механізми безпеки. Але перед цим потрібно визначити особливості СЕН з позицій інформаційної безпеки і виявити специфічні загрози.

2.1. Особливості СЕН з позицій інформаційної безпеки. Покоління електронних компонент для комп'ютерів змінюються кожні 5-7 років. Але навчальні заклади України зазвичай не мають достатньо фінансових ресурсів для оновлення усієї інфраструктури. В цих умовах типова навчальна інформаційна система є великою гетерогенною системою

і завдання забезпечити цілісність інформації є нетривіальним. Наприклад, інформаційна система Сумського державного університету включає 2143 комп'ютера [6]. Інформаційна система Київського політехнічного університету включає 23500 програмних продуктів, 17600 з яких належать до навчальних. Не кожна корпоративна бізнес-система включає таке різноманіття апаратних і програмних засобів. Для забезпечення цілісності інформації в СЕН необхідно створити комплексні механізми безпеки. Ще одна проблема – управління ліцензіями в великій гетерогенній системі. Територіальна розпорошеність компонентів СЕН ставить проблеми при організації належної автентифікації та ідентифікації користувачів. Ще одна важлива риса СЕН – неперервне оновлення інформаційних ресурсів.

Описані вище специфічні властивості СЕН призводять до неконтрольованого росту вразливостей, загроз від внутрішніх і зовнішніх зловмисників, а також складностей в прогнозуванні потенційних матеріальних, фінансових, моральних та інших збитків. Специфіка освітніх закладів створює багато проблем для управління ризиками.

2.2. Деякі специфічні загрози. Кожна складова системи електронного навчання має свої вразливості і викликані ними загрози. Більшість специфічних проблем виникає на рівні платформи СЕН. Окремо слід виділити загрозу добровільної передачі ідентифікаційних та автентифікаційних даних, яка не зустрічається в інших інформаційних системах. В більшості сучасних СЕН передбачена лише парольна автентифікація, яка не може протидіяти цій загрозі. Студент може свідомо передати свої логін і пароль сторонній особі, щоб вона здала за нього іспит чи пройшла тестування.

Для опису специфічних загроз використаємо таблицю, в якій вкажемо назву загрози, її опис та вразливі до неї компоненти СЕН (табл. 1).

Таблиця 1

Специфічні загрози інформаційній безпеці СЕН

Загроза	Опис	Вразливий компонент СЕН
Фальшивий контент	Зловмисник може отримати неавторизований доступ до системи і завантажити фальшивий контент, якщо СЕН має вразливості в механізмах ідентифікації, автентифікації та авторизації	Адміністративна система LCMS, Авторингова система LCMS, Адміністративна система LMS
Екзамен може бути переглянутий до дати складання	Зловмисник може отримати неавторизований доступ до системи і переглянути завантажені екзамени до дати складання іспиту, якщо СЕН має вразливості в механізмах ідентифікації, автентифікації, авторизації та конфіденційності	Адміністративна система LCMS, Навчальний репозиторій, Адміністративна система LMS
Екзамен може бути видалений	Зловмисник може отримати неавторизований доступ до системи і видалити завантажені екзаменаційні файли, якщо СЕН має вразливості в механізмах ідентифікації, автентифікації, авторизації, цілісності та доступності	Адміністративна система LCMS, Навчальний репозиторій, Адміністративна система LMS
Іспит може бути складений іншою особою	Студент може свідомо передати свої ідентифікаційні і автентифікаційні дані неавторизованій особі, яка може скласти іспит замість студента. Для СЕН є проблемою визначення, авторизований чи неавторизований користувач склав іспит	Система оцінювання LMS
Зміна дати екзамену	Зловмисник може отримати неавторизований доступ до системи і змінити дату складання іспиту, якщо СЕН має вразливості в механізмі цілісності	Адміністративна система LMS, Система оцінювання LMS
Неавторизоване перехоплення результату	Зловмисник може отримати неавторизований доступ до системи, перехопити результати інших студентів і представити їх як свою власну роботу	Комунікаційний модуль, Система оцінювання LMS, Система адміністрування LMS
Доступ до ресурсів без оплати за них	Студент може передати свої персональній ідентифікаційні та автентифікаційні дані неавторизованій особі, яка отримає доступ до навчального контенту без оплати за нього	Система адміністрування LMS
Неавторизований доступ до навчального контенту	Зловмисник може використати «дірки» в системі безпеки СЕН для неавторизованого доступу до навчального контенту, до яких він не має прав доступатися	Адміністративна система LCMS, Навчальний репозиторій, Адміністративна система LMS

Як видно з поданої таблиці, більшість специфічних загроз виникає на рівні платформи електронного навчання. Критичними компонентами з точки зору захисту інформації є адміністративні системи LCMS та LMS, навчальний репозиторій, система оцінювання LMS, комунікаційний модуль.

В режимі оцінювання знань критичним є підтвердження особи користувача. Для вирішення цієї проблеми використовуються біометричні технології, технології автентифікації на основі смарт-карт [7]. Проте наявні рішення не дозволяють повністю усунути дану загрозу і необхідно проводити подальші дослідження в цьому напрямі.

Більшість загроз на рівні LCMS мають зв'язок з проблемами захисту інтелектуальної власності. Щоб усунути їх необхідно створити та інтегрувати в СЕН інфраструктуру захисту від несанкціонованого копіювання.

Відомі технології, такі як DRM [], не відповідають потребам СЕН, тому необхідно розробити специфічне рішення.

Як і в інших інформаційних та телекомунікаційних системах, користувачі СЕН розглядаються як потенційні зловмисники. Необхідно розробити моделі порушників для всіх типів користувачів - студентів, викладачів, авторів контенту, адміністраторів освіти та системних адміністраторів.

Висновки

Ми розробили модель системи електронного навчання, зорієнтовану на потреби аналізу ін формаційної безпеки. Її особливістю є чіткий поділ на компоненти, врахування структури сучасних СЕН, включення в модель, крім програмної, також і апаратної частини. Цю модель потрібно розвинути, використовуючи одну з методологій моделювання, наприклад, UML чи IDEF. Тоді можна буде застосувати формальні підходи до аналізу загроз інформаційній безпеці СЕН.

Подальші дослідження можна спрямувати на розроблення класифікації загроз інформаційній безпеці СЕН, моделей порушників, політики безпеки, специфікацій та механізмів захисту інформації в СЕН.

Список літератури

1. Web-сайт Українського інституту інформаційних технологій в освіті [Електронний ресурс]. – Режим доступу до ресурсу: http://uiite.kpi.ua/ua/about-dl/regions.html

2. Retalis Symeon. Modelling Web-based Instructional Systems / Symeon Retalis, Paris Avgeriou. – Journal of Information Technology Education. – 2002. – Volume 1.

3. UK e-Universities Worldwide. Principles and Practice in e-Learning platform architecture. – UKeU, 2002.

4. Learning Technology Systems Architecture, Draft 5. – IEEE, 1999.

5. Edgar Frackmann. Proposal for an overall Concept for Higher Education Information Systems in Croatia / Edgar Frackmann. – Zagreb, 2007.

6. Мишко Сергій. Індустріалізація в масштабах країни / Сергій Мишко. – PCWeek/UE, 2009.

7. Использование смарт-карт для защиты информации в процессе дистанционного обучения / М.И. Спирягин, В.И. Спирягин, С.А. Клюев, Е.А. Валуйский, Ф.П. Усенко // Проблеми програмування. – 2006. – № 2-3, спеціальний випуск.

Надійшла до редколегії 27.04.2011

Рецензент: д-р техн. наук, проф. В.А. Лужецький, Вінницький національний технічний університет, Вінниця.

МОДЕЛЬ СИСТЕМЫ ЭЛЕКТРОННОГО ОБУЧЕНИЯ ДЛЯ АНАЛИЗА УГРОЗ ЕЁ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.Ф. Чекурин, А.А. Будик

В работе предложено модель системы электронного обучения (СЕО), которая ориентирована на потребности анализа угроз её информационной безопасности. Особенностями модели являются четкое деление СЕО на компоненты, учет структуры современных СЕО, включение в модель, кроме программной, также и аппаратной части, что позволяет проводить комплексный анализ угроз. Структура СЕО включает компьютерную инфраструктуру, платформу электронного обучения, информационные ресурсы, и человеческие ресурсы. Платформу электронного обучения как специфичную составляющую СЕО рассмотрено детальнее. Также проведено обзор специфических угроз информационной безопасности СЕО.

Ключевые слова: *электронное обучение, система электронного обучения, информационная безопасность, защита информации, угрозы, уязвимости.*

MODEL OF E-LEARNING SYSTEM FOR THE ANALYSIS OF ITS INFORMATION SECURITY THREATS

V.F. Chekurin, O.O. Budik

The model of the e-learning system (ELS) for the analysis of its information security threats is proposed in the paper. Peculiar properties of this model are well-defined division of ELS into the components, taking into account the structure of modern e-learning systems, inclusion of the hardware part besides the software one, which allow carrying out a complex threat analysis. The ELS structure includes computer infrastructure, e-learning platform, information resources and human resources. E-learning platform as a specific ELS part is considered in detail. Also particular threats to ELS information security are reviewed.

Keywords: *e-learning, e-learning system, information security, information protection, threats, vulnerabilities.*