УДК 004.056

В.Ф. Чекурін, О.О. Будік
Національний університет «Львівська політехніка»,
кафедра «Захист інформації»
79013, м. Львів, вул. С. Бандери, 12

ПІДХІД ДО ФОРМУВАННЯ ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СИСТЕМ ЕЛЕКТРОННОГО НАВЧАННЯ

E-learning system classification and generalized structural model for information security analysis have been considered. On this basis an approach to security requirements for e-learning system forming has been suggested.

Keywords – E-learning system, virtual learning environment, ELS information security

У статті розглянуто класифікацію та узагальнену структурну модель системи електронного навчання, зорієнтовані на потреби аналізу інформаційної безпеки. В рамках розробленої моделі запропоновано підхід до формування вимог безпеки систем електронного навчання

Ключові слова: система електронного навчання, віртуальне навчальне середовище, інформаційна безпека СЕН

Вступ

На сьогодні широке застосування у вищій освіті здобули три класичні форми навчання — стаціонарна, заочна та дистанційна [1]. Кожна з них має свої переваги та недоліки. Разом із тим у Європі та США високого рівня розвитку досягли інформаційно-комунікаційні технології навчання [2]. Фактично виникла четверта форма — електронне навчання (E-Learning [3]). Із заочною її єднає можливість отримувати якісну професійну освіту без відриву від виробництва, а з дистанційною — можливість навчатися, перебуваючи на будь-якій відстані від навчального закладу, та самостійно планувати свою навчальну активність. Зі стаціонарною формою електронне навчання поєднує можливість безпосереднього спілкування у віртуальному просторі студента з викладачем як індивідуально, так і у складі навчальної групи. На сьогодні у світі вже створені віртуальні університети, які готують спеціалістів виключно за цією формою навчання [4].

Зрозуміло, що впровадження цієї форми навчання вимагає створення відповідної інфраструктури, яка включає апаратно-програмне комп'ютерне забезпечення, телекомунікаційні засоби, цифрові інформаційні ресурси тощо і створення на цій основі системи електронного навчання (СЕН). Теоретичні засади функціонування СЕН, розуміння її структури та підходів до побудови перебувають наразі у стадії розвитку. Проте, вже зараз можна аналізувати загрози безпеки інформації, що неминуче виникають за реалізації цієї надзвичайно ефективної і перспективної форми навчання.

Будь-яку СЕН можна класифікувати як відкриту інформаційно-комунікаційну систему, що й визначає частину можливих загроз, як зовнішніх, так і внутрішніх, а відтак — і допустимі методи та засоби убезпечення від них. Проте, при експлуатації СЕН виникатимуть і специфічні загрози, зумовлені їх областю застосування.

Метою цієї статті є класифікація систем електронного навчання, опрацювання узагальненої моделі СЕН, зорієнтованої на потреби аналізу інформаційної безпеки, та формулювання вимог безпеки для СЕН.

1. Класифікація систем електронного навчання

Перші системи електронного навчання, які використовували обчислювальні ресурси лише одного комп'ютера і не передбачали роботи в мережі, з'явилися ще на початку 60-х років минулого століття [5]. Пізніше були створені системи, що функціонували в локальних мережах навчальних закладів. Поява СЕН з підтримкою взаємодії користувачів та інтерактивного спілкування студентів і викладачів припадає на 70-80-ті роки. Основними центрами розвитку цих систем та піонерами галузі є США, Канада, Великобританія. В Україні та інших пострадянських країнах увага до цього напрямку й активне розроблення систем електронного навчання розпочалася з 90-х років минулого століття. Наразі ми не маємо сучасних СЕН із підтримкою усіх прогресивних технологій та інтегрованою системою захисту інформації, що пройшла сертифікацію на відповідність українським стандартам безпеки.

Виходячи з літературних джерел [6], [7], та беручи до уваги потреби аналізу інформаційної безпеки СЕН класифікуватимемо їх за наступними ознаками (рис.1).

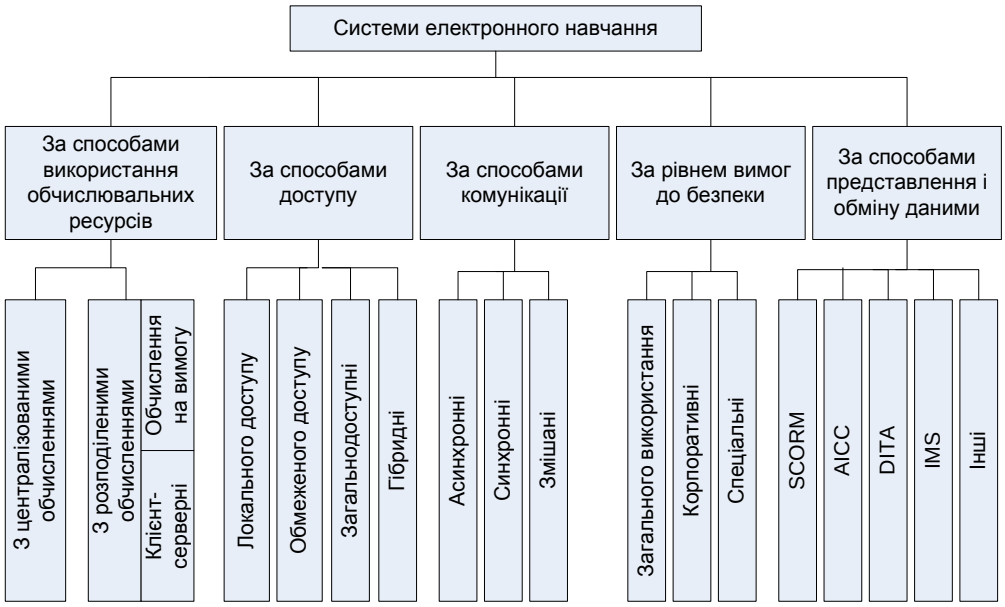

Рис. 1. Класифікація СЕН

За способом використання обчислювальних ресурсів СЕН поділяються на системи з централізованими та розподіленими обчисленнями. Перші передбачають централізоване використання обчислювальних ресурсів (ОР) лише одного комп'ютера, на якому встановлено навчальне ПЗ. Такі системи прості в реалізації, тож, незважаючи на їх архаїчність, їх продовжують використовувати в системі освіти України. Для СЕН, що базуються на розподілених обчисленнях, характерним є наявність обчислювальної мережі. Їх, у свою чергу, можна поділити на клієнт-серверні та системи, що надають ОР на вимогу. В перших використовуються фіксовані зв'язки між споживачами та постачальниками послуг, в других - методи динамічного розподілу ресурсів в мережі. До останніх слід віднести технології GRID та хмаркових обчислень (cloud computing).

За способами доступу до функцій системи та її контенту розрізнятимемо СЕН з локальним доступом, з обмеженим доступом, загальнодоступні та гібридні. До перших відноситимемо

системи, з доступом лише з конкретного захищеного від зовнішнього середовища сегмента локальної мережі (чи ізольованого комп'ютера. СЕН з обмеженим доступом є відкриті інформаційні системи, що можуть віддалено надавати послуги лише авторизованим користувачам. Загальнодоступні СЕН надають доступ до своїх функцій і контенту усім зареєстрованим користувачам. До гібридних відноситимемо СЕН, які можуть надавати різні види доступу (локальний, обмежений, загальнодоступний) до різних груп функцій та різних розділів контенту, залежно від прав користувачів.

За способом комунікації студентів і викладачів поділятимемо СЕН на асинхронні, які використовують обмін повідомленнями з використанням електронної пошти, форумів, блогів, синхронні, що забезпечують розмови в реальному часі, наприклад, з використанням клієнта миттєвих повідомлень, VoIP-телефонії, відео дзвінків, і змішані, які поєднують можливості синхронних і асинхронних методів комунікації.

За рівнем вимог до інформаційної безпеки розрізнятимемо СЕН загального використання без спеціальних вимог конфіденційності (до них можна віднести СЕН звичайних навчальних закладів), корпоративні СЕН та СЕН зі спеціальними вимогами секретності (СЕН навчальних закладів для системи оборони, спеціальних державних служб тощо) .

Розрізнятимемо також СЕН **за способами представлення і обміну даними.** На сьогодні використовуються декілька стандартів, які визначають представлення та обмін даних в системах електронного дистанційного навчання: SCORM (навчальний матеріал представлений окремими невеликими блоками, які можуть об'єднуватись у різні курси та використовуватись незалежно від того, ким, де та за допомогою яких засобів вони були створені) [8], AICC (описує спосіб обміну даними між навчальними матеріалами і системою управління навчанням, правила створення мета-даних) [9], IMS (специфікація метамови, яка призначена для моделювання навчальних процесів) [10], DITA (архітектура на основі стандарту XML, яка призначена для автоматизації збору документів із розрізнених фрагментів, оформлених згідно специфікації DTD, і їх публікації в різних форматах) [11].

2. Узагальнена структура системи електронного навчання та функції її компонент

Бачення структури, функцій та термінологія в області електронного навчання ще остаточно не усталені. Тому сформулюємо **узагальнену структуру СЕН**, яку ми будемо використовувати у подальших дослідженнях для оцінювання ступеня захищеності СЕН. Розглядатимемо СЕН як систему, що складається із обчислювальної інфраструктури, платформи СЕН та людських ресурсів (рис.2).

Завданням **обчислювальної інфраструктури** є надання обчислювальних ресурсів для функціонування СЕН. До її складу входить обчислювальна апаратура, системне програмне забезпечення, канали зв'язку. Ця платформа може функціонувати на окремому комп'ютері, в локальній обчислювальній мережі певної організаційної структури (кафедри, факультету, навчального закладу тощо), у корпоративній мережі (групи навчальних закладів, Міністерства освіти і т.д.), віртуальному середовищі Web-простору, віртуальних областях GRID- чи cloud computing-середовищ.

Платформа СЕН це комплекс програмних засобів та спеціалізованої апаратури, що формує відповідне віртуальне навчальне середовище. Воно містить операційне ядро системи — системне програмне забезпечення СЕН, яке підтримує функціонування усіх її складових, прикладне програмне забезпечення, яке надає навчальні та службові сервіси користувачам, інформаційних ресурсів, що містять навчальний контент та бази даних навчального та навчально-організаційного процесу.

Спеціалізована апаратура СЕН призначена для реалізації специфічних функцій системи електронного навчання у віртуальному просторі, зокрема, — запобігання загроз, пов’язаних з ідентифікацією та аутентифікацією користувачів.

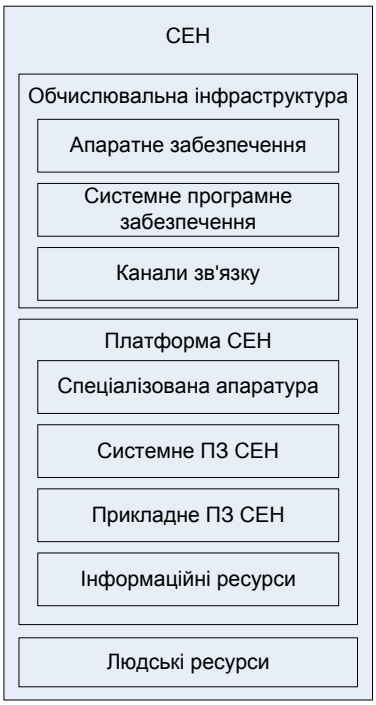

Рис. 2. Загальна структура СЕН

Системне програмне забезпечення СЕН включає (рис.3): інтерфейс користувача, систему управління навчанням LMS (Learning Management System), систему управління навчальним контентом LCMS (Learning Content Management System), систему комунікації.

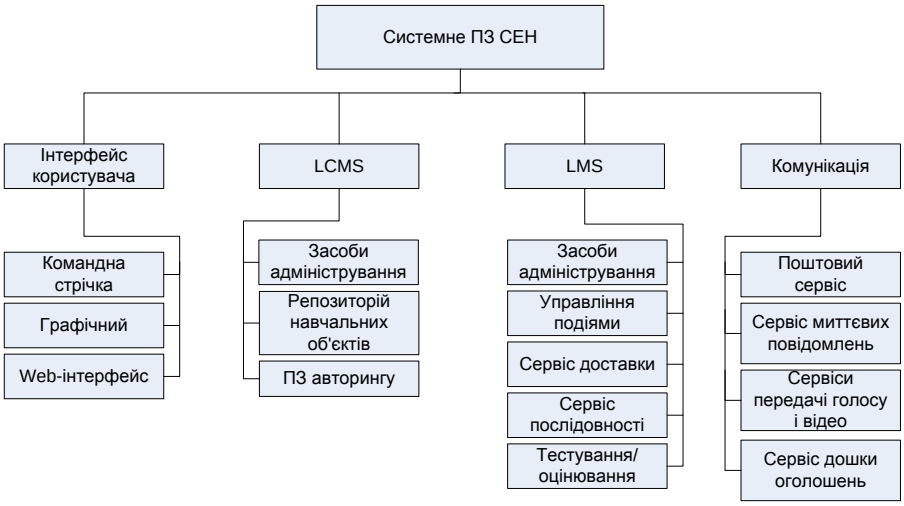

Рис. 3. Структура системного ПЗ СЕН

Інтерфейс користувача надає віддалений або локальний доступ користувачам до всіх функцій СЕН відповідно до їх прав. Залежно від типу СЕН та становища користувача це — інтерфейс командної стрічки, Web- чи графічний інтерфейс.

LMS в сукупності з **LCMS** являє собою ядро платформи СЕН. LMS реалізує такі функції: забезпечує запис студентів на курси; забезпечує користувачам доступ до каталогу інформаційних ресурсів та навчального контенту відповідно до їх привілеїв; відстежує успішність та активність студентів; генерує звіти; підтримує формування тестових та екзаменаційних завдань; здійснює автоматизоване оцінювання тестових і контрольних завдань. В загальному вона включає наступні компоненти: засоби адміністрування, систему управління подіями, сервіс доставки, система управління навчальними заходами, система автоматизованого оцінювання та тестування

Система адміністрування навчальним процесом здійснює контроль входу до СЕН та доступу до інформаційних ресурсів відповідно до привілеїв, керує обліковими записами користувачів різних груп, провадить списки студентів за видами, напрямками (спеціальностями) навчання, академічними групами, навчальними курсами в межах спеціальностей, встановлює відповідність між навчальними курсами та викладачами, які їх провадять, формує екзаменаційні відомості та розклад контрольних заходів тощо.

Система управління подіями формує плани навчальних заходів та активностей користувачів, реалізує функції нагадування, реєструє події, здійснює моніторинг реалізації запланованих подій.

Система доставки відповідає за формування порцій навчального контенту згідно планів навчальних заходів та подій і їх доставку користувачам.

Система тестування та оцінювання підтримує процеси формування тестових, екзаменаційних та інших контрольних завдань, керує ходом їх виконання, надає засоби для автоматизованої перевірки виконаних завдань.

LCMS використовується для створення навчальних матеріалів, курсів, тестів, редагування навчальних об’єктів, та дозволяє розміщувати все це у відповідній базі даних (навчальному репозиторії). До складу цієї системи входить також програмне забезпечення автоматизованого авторингу (для створення багаторазово використовуваних навчальних об’єктів, які будуть зберігатись у репозиторії);

Система комунікації забезпечує синхронну, асинхронну чи змішану комунікацію між викладачами і студентами за допомогою сервісів пошти, миттєвих повідомлень, передачі голосу і відео, дошки оголошень.

Прикладне програмне забезпечення складається (рис.4) із загальних інструментів та спеціалізованих навчальних середовищ.

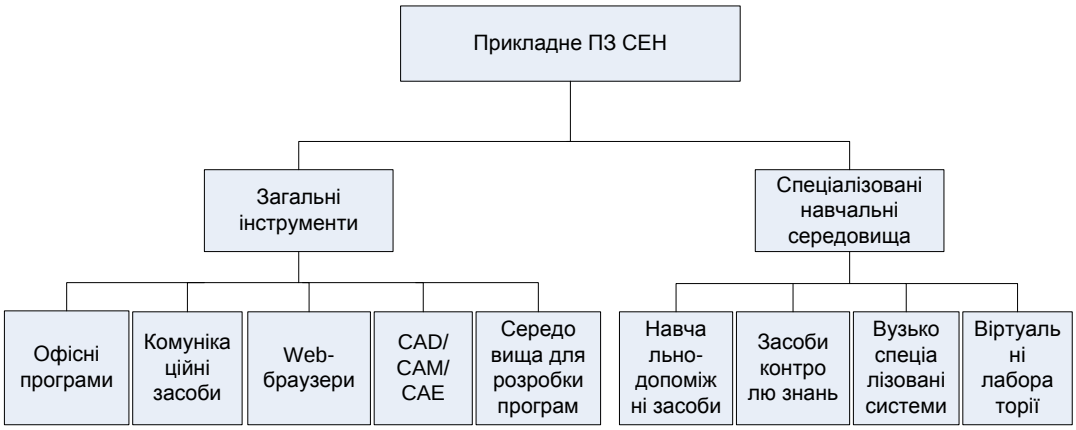

Рис.4. Структура прикладного ПЗ СЕН

До *загальних інструментів* відносимо ринкові програмні продукти, які використовують у навчальному процесі – пакети офісних програм (MS Office, Open Office, IBM Lotus тощо), комунікаційні засоби (Skype, ICQ, MSN Messenger), Web-браузери; системи автоматизованого проектування (AutoCad, TopoR, bCAD) та засоби математичного моделювання (MathCad, Matematica, Maple тощо), середовища для розроблення програм (C++, Java, Delphi тощо). *Спеціалізовані навчальні середовища* це — програмні засоби та програмно-апаратні комплекси, , які розроблені, як правило, силами ВНЗ чи на їх замовлення з урахуванням специфіки навчального закладу та профілів підготовки спеціалістів. Серед них — навчально-допоміжні (організаційні, демонстраційні) засоби, засоби контролю (перевірки) знань, вузькоспеціалізовані системи, призначенні для формування у студентів фахових знань, умінь та навичок з їх предметної області (емулятори, імітатори, тренажери тощо), а також віртуальні навчальні лабораторії.

Інформаційні ресурси поділяємо на такі категорії: адміністративно-господарську, навчально-організаційну та наукову частини і навчальний контент. До першої відносяться різні документи, що безпосередньо не стосуються навчального процесу. До навчально-організаційної віднесемо інформацію, яка є документальним забезпеченням навчального процесу, зокрема, особисті дані користувачів, відомості про успішність, розпорядчі документи, інші організаційні матеріали. Навчальний контент включає бази знань, електронні конспекти лекцій, фото/відео матеріали, навчальні об’єкти, курси, методичні матеріали, матеріали для контролю успішності. До наукової інформації віднесемо каталоги, тематичні картотеки, бібліотеку звітів виконаних досліджень, дані про актуальні дослідження, бази даних студентської та наукової бібліотек.

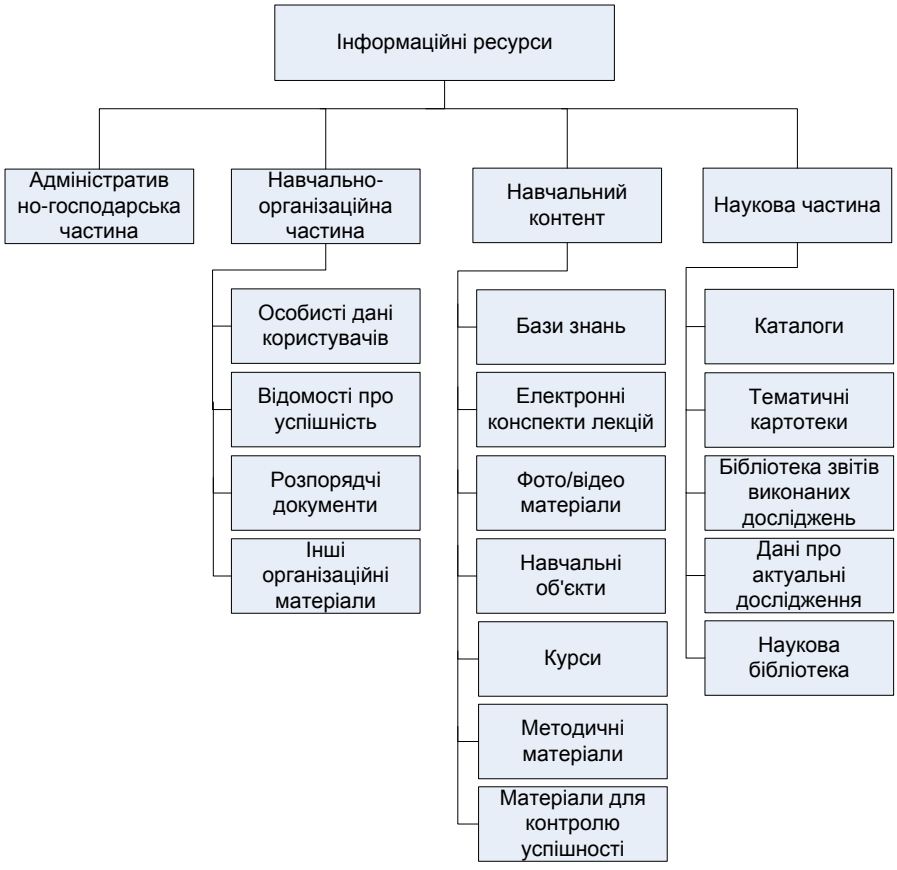

Рис. 5. Структура інформаційних ресурсів СЕН

Третьою складовою системи електронного навчання є людські ресурси. В контексті СЕН доцільно виділити такі типи користувачів: студенти (отримують освітні послуги), викладачі (надають освітні послуги), автори курсів (формують та оновлюють навчальний контент),

адміністратори освіти (адміністративний персонал ВНЗ) та системні адміністратори (відповідають за функціонування СЕН).

3. Формулювання вимог до безпеки системи електронного навчання

Формулювання вимог до інформаційної безпеки та визначення рівня захищеності СЕН слід здійснювати відповідно з міжнародними та внутрішніми державними і галузевими стандартами. Серед них найвідомішими є Критерії визначення безпеки довірених комп'ютерних систем, або Оранжева книга [12], Критерії оцінки безпеки інформаційних технологій, або Єдині критерії [13]. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України розробив власні «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» [14].

Система електронного навчання, що призначена для використння в Україні, повинна пройти сертифікацію на відповідність українським стандартам безпеки. Тому сформулюємо вимоги до безпеки СЕН на основі Критеріїв, розроблених ДСТСЗІ. Ці Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу і надають орієнтири для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного.

Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного з чотирьох основних типів. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять **загрози конфіденційності**. Загрози, що відносяться до несанкціонованої модифікації інформації, становлять **загрози цілісності.** Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять **загрози доступності**. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет послуг **спостереженості і керованості.**

Специфіка системи електронного навчання виявляється у платформі СЕН, тому застосуємо описані Критерії для формулювання вимог безпеки до кожного об'єкту платформи СЕН відповідно до розроблених у другому параграфі узагальненої структури СЕН, структури системного ПЗ СЕН та прикладного ПЗ СЕН. Для цього використовуємо таблиці, в яких визначимо необхідність реалізації послуги для кожного об'єкту платформи СЕН. Для прикладу побудуємо таблицю вимог до конфіденційності СЕН.

Таблиця 1.

Вимоги до конфіденційності СЕН

Об'єкт	Послуги конфіденційності				
	Довірча конфіден-ційність	Адміністра-тивна конфіденцій-ність	Повторне використання об'єктів	Аналіз прихованих каналів	Конфіден-ційність при обміні
Спеціалізована апаратура	+	+	-	+	-

Інтерфейс користувача	-	-	-	-	-
Засоби адміністрування LCMS	+	+	+	-	+
Репозиторій навчальних об’єктів	+	+	+	-	+
ПЗ авторингу	+	+	+	-	+
Засоби адміністрування LMS	+	+	+	-	+
Управління подіями	+	+	-	-	-
Сервіс доставки	+	+	-	+	+
Система тестування/оцінювання	+	+	+	+	+
Поштовий сервіс	+	+	-	-	+
Сервіс миттєвих повідомлень	+	+	-	-	+
Сервіси передачі голосу і відео	+	+	-	-	+
Сервіс дошки оголошень	+	+	-	-	+
Загальні інструменти	-	-	-	-	-
Спеціалізовані навчальні середовища	+	+	+	+	+

Спеціалізована апаратура може використовуватися для забезпечення довірчої конфіденційності, адміністративної конфіденційності та аналізу прихованих каналів. У відповідних клітинках ставим знак «+». Так само визначаємо послуги конфіденційності і для інших об’єктів платформи СЕН.

За таким самим принципом можна побудувати таблиці вимог до цілісності, доступності і спостереженості СЕН.

, Висновки

Запропоновано класифікацію систем електронного навчання і розроблено узагальнену структурну модель системи електронного навчання, зорієнтовану на потреби аналізу інформаційної безпеки, а також деталізовано структуру платформи СЕН. Запропоновано підхід до формування вимог до безпеки СЕН на основі «Критеріїв оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу».

Подальші дослідження слід спрямувати на Our future work will relate to developing method of security level evaluation for e-learning system, models of attackers for different user types – students, teachers, authors, learning and system administrators, and model of security system for e-learning system.

Список використаних джерел

1. Закон України Про вищу освіту. 2. V. Venugopal, Manjulika Srivastava. ICT & The Future of Distance. Turkish Online Journal of Distance Education, Vol. 4, 2003. 3. Сайт про e-Learning - http://www.e-learningconsulting.com/consulting/what/e-learning.html. 4. Canadian Virtual University - http://www.cvu-uvc.ca. 5. Oliver Boyd-Barrett. Computers and learning. Addison-Wesley, 1991. 6. Ляхов А.Л., Демиденко М.І. Основні властивості автоматизованих систем моделювання і управління навчальним процесом у ВНЗ. Математичні машини і системи, 2008. 7. Gabriela Hoppe. Classification and Sustainability Analysis of E-Learning Applications. Universitat Hannover, 2003. 8. Офіційний сайт SCORM - http://scorm.com. 9. Офіційний сайт AICC - http://www.aicc.org/joomla/dev. 10. Офіційний сайт IMS Global Learning Consortium - http://www.imsglobal.org/commoncartridge.html. 11. Сайт онлайн-спільноти DITA - http://dita.xml.org. 12. Trusted Computer System Evaluation Criteria, Department of Defense, 1985. 13. Офіційний сайт проекту The Common Criteria - http://www.niap-ccevs.org/cc-scheme/cc_docs. 14. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». ДСТСЗІ, 1999.

1. Інформаційна безпека в освітній галузі

1.5 Огляд міжнародних та внутрішніх стандартів інформаційної безпеки в освіті.