НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ННК "Інститут прикладного системного аналізу"
(повна назва інституту/факультету)

Кафедра Системного проектування
(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри
_____ А.І.Петренко
(підпис) (ініціали, прізвище)

"___"_____2015 р.

Дипломна робота

першого (бакалаврського) **рівня вищої освіти**
(першого (бакалаврського), другого (магістерського))

зі спеціальності 7.050102, 8.050102 Інформаційні технології проектування
7.050103, 8.050103 Системне проектування
(код та назва спеціальності)

на тему: Забезпечення інформаційної безпеки при використанні системи дистанційного навчання LON-CAPA в локальній мережі кафедри

Виконав (-ла): студент (-ка) 4 курсу, групи ДА-12
(шифр групи)

Куліш Златослава Ігорівна _____
(прізвище, ім'я, по батькові) (підпис)

Керівник доцент, к.т.н Кисельов Г.Д. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант Охорона праці доцент, к.б.н. Гусєв А.М. _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент доцент, к.т.н. Тимощук О.Л. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Нормоконтроль ст.. викладач Бритов О.А. _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2015 року

Національний технічний університет України
«Київський політехнічний інститут»

Факультет (інститут) ННК "Інститут прикладного системного аналізу"
(повна назва)

Кафедра Системного проектування
(повна назва)

Рівень вищої освіти Перший(Бакалаврський)
(перший (бакалаврський)

Спеціальність 7.050103, 8.050103 Системне проектування
(код і назва)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ А.І.Петренко
(підпис) (ініціали, прізвище)
«___»_____2015 р.

ЗАВДАННЯ
на дипломну роботу студентці
Куліш Златославі Ігорівні
(прізвище, ім'я, по батькові)

1. Тема роботи Забезпечення інформаційної безпеки при використанні системи дистанційного навчання LON-CAPA в локальній мережі кафедри

керівник роботи Кисельов Геннадій Д, к.т.н., доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «02» квітня 2015 р. № 30/1-ст

2. Строк подання студентом роботи 16.06.2015

3. Вихідні дані до роботи _____

Система дистанційного навчання LON-CAPA;

Методи захисту інформації - управління доступом, регламентація;

Структуктура забезпечення інформаційної безпеки локальної мережі кафедри.

4. Зміст розрахунково-пояснювальної записки (перелік завдань, які потрібно розробити)

1. Інформаційна безпека систем дистанційного навчання
2. Групи систем дистанційного навчання. LON-CAPA
3. Забезпечення інформаційної безпеки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслеників, плакатів тощо)

1.Функціональна система інформаційної безпеки, групи систем дистанційного навчання – плакат.
2. Поширення системи LON-CAPA, вплив онлайн навчання на успішність студентів – плакат.
3. Загальна схема доступу до навчальних матеріалів, методи та засоби інформації – плакат.
4. Діаграми прецедентів – плакат.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Гусєв А.М., доцент		
Основна частина	Кисельов Г.Д., доцент		

7. Дата видачі завдання 01.02.2015

Календарний план

№ з/п	Назва етапів виконання дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Отримання завдання	01.02.2015	
2	Збір інформації	15.02.2015	
3	Аналіз систем дистанційного навчання	28.02.2015	
4	Дослідження LCMS систем	10.03.2015	
5	Вивчення особливостей LON-CAPA	15.03.2015	
6	Аналіз проблем впровадження СДН	25.03.2015	
7	Дослідження та аналіз методів захисту	25.04.2015	
8	Реалізація методів у LON-CAPA	30.04.2015	
9	Оформлення дипломної роботи	05.05.2015	
10	Отримання допуску до захисту та подача роботи в ДЕК	16.06.2015	

Студент _____ З.І. Куліш
(підпис) (ініціали, прізвище)

Керівник роботи _____ Г.Д, Кисельов
(підпис) (ініціали, прізвище)

АНОТАЦІЯ

Бакалаврської дипломної роботи Куліш Златослави Ігорівни

на тему: " Забезпечення інформаційної безпеки при використанні системи дистанційного навчання LON-CAPA в локальній мережі кафедри "

Дипломна робота присвячена дослідженню методів захисту інформації і використанню їх в системі дистанційного навчання.

Актуальність теми зумовлена широким використанням систем дистанційного навчання у сучасному світі. Тому вибір методів захисту для забезпечення конфіденційності і захищеності інформації, є першочерговим завданням при використанні систем дистанційного навчання.

Цілю дипломної роботи є проаналізувати існуючі методи захисту інформації, аргументовано обравши з урахуванням вимог та особливостей системи дистанційного навчання декілька з них та реалізувати методи захисту у системі LON - CAPA.

В роботі проведено експериментальне впровадження методу до СДН, під час якого були створені умови максимальної безпеки для інформації, яка зберігається у системі.

В ході виконання дипломної роботи були запропоновані методи для забезпечення інформаційної безпеки системи.

В результаті роботи були реалізовані методи захисту, а саме: метод управління доступом та регламентації доступу.

Загальний обсяг роботи – 74 сторінок, 24 рисунка, 1 таблиця, 26 бібліографічних найменувань.

Ключові слова: інформаційна безпека, методи захисту, система дистанційного навчання, LON-CAPA, LCMS системи.

АННОТАЦИЯ

Бакалаврской дипломной работи Кулиш Златославы Игоревны

на тему: "Обеспечение информационной безопасности при использовании системы дистанционного обучения LON-CAPA в локальной сети кафедры"

Дипломная работа посвящена исследованию методов защиты информации и использованию их в системе дистанционного обучения.

Актуальность темы обусловлена широким использованием систем дистанционного обучения в современном мире. Поэтому выбор методов защиты для обеспечения конфиденциальности и защищенности информации, является первоочередной задачей при использовании систем дистанционного обучения.

Целю работы является проанализировать существующие методы защиты информации, аргументировано выбрав с учетом требований и особенностей системы дистанционного обучения несколько из них и реализовать методы защиты в системе LON - CAPA.

В работе проведено экспериментальное внедрение метода в СДО, в ходе которого были созданы условия максимальной безопасности для информации, которая хранится в системе.

В ходе выполнения дипломной работы были предложены методы для обеспечения информационной безопасности системы.

В результате работы были реализованы методы защиты, а именно: метод управления доступом и регламентации доступа.

Общий объем работы - 74 страниц, 24 рисунка, 1 таблица, 26 библиографических наименований.

Ключевые слова: информационная безопасность, методы защиты, система дистанционного обучения, LON-CAPA, LCMS системы.

ANNOTATION

For the bachelor's degree work of Kulish Zlatoslava Igorivna
on " Information security when using e-learning system LON-CAPA in the local network of the department "

This work is devoted to research methods to protect the information and use them in distance learning.

Actuality caused extensive use of distance learning in the modern world. Therefore, the choice of methods to protect the privacy and security of information is a priority in the use of distance learning.

Aim of the thesis is to analyze the existing methods of protecting information by choosing reasonably meet the requirements and characteristics of distance learning several of them and implement methods to protect the system LON - CAPA.

In work the experimental introduction to the DLS method in which conditions were created for maximum security of information stored in the system.

In the course of the thesis have been proposed methods for ensuring information security system.

As a result of protection methods have been implemented, namely the method of access control and regulation control.

The total amount of work - 74 pages, 24 figure, 1 table, 26 bibliographic titles.

Keywords: information security, protection methods, distance learning system, LON-CAPA, LCMS system.

ЗМІСТ

ВСТУП

Сучасні методи обробки, передачі та накопичення інформації сприяли появі загроз, пов'язаних з можливістю втрати, перекручування та розкриття даних, які адресовані або належать кінцевим користувачам. Тому забезпечення інформаційної безпеки комп'ютерних систем і мереж є одним з провідних напрямків розвитку IT.

Комп'ютерні інформаційні технології швидко розвиваються та вносять помітні зміни в наше життя. Інформація стала товаром, який можна придбати, продати, обміняти. При цьому вартість інформації часто в сотні разів перевершує вартість комп'ютерної системи, в якій вона зберігається.

Інформаційна безпека комп'ютерних систем досягається забезпеченням конфіденційності, цілісності та достовірності даних, що обробляються, а також доступності та цілісності інформаційних компонентів і ресурсів системи.

При розробці комп'ютерних систем, вихід з ладу або помилки в роботі можуть призвести до тяжких наслідків, питання комп'ютерної безпеки стають першочерговими. Відомо багато заходів, спрямованих на забезпечення комп'ютерної безпеки, основними серед них є технічні, організаційні та правові.

Захищеність інформаційної системи від випадкового або навмисного втручання, що завдає шкоди власникам або користувачам інформації, залежить, в основному, від доступності (можливість за розумний час отримати необхідну інформаційну послугу); цілісності (актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованого зміни); конфіденційності (захист від несанкціонованого прочитання).

Сучасна інформаційна система являє собою складну систему, що складається з великого числа компонентів різного ступеня автономності, які пов'язані між собою і обмінюються даними. Практично кожен компонент може піддатися зовнішньому впливу або вийти з ладу.

1 ІНФОРМАЦІЙНА БЕЗПЕКА СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ

1.1 **Інформаційна безпека сьогодення**

На сьогоднішній день однією з основних ознак науково-технічного прогресу є стрімкий розвиток інформаційних технологій. Однак, при їх широкому використанню у повсякденному житті та у професійній сфері, постає питання захищеності і безпеки таких технологій.

Інформаційна безпека - це стан захищеності інформаційного середовища, захист інформації являє собою діяльність щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається, тобто процес, спрямований на досягнення цього стану. Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова системи забезпечення інформаційної безпеки даного об'єкту [4].

Для побудови та ефективної експлуатації СЗІБ (система забезпечення інформаційної безпеки) необхідно:

- виявити вимоги захисту інформації, специфічні для даного об'єкта захисту;
- врахувати вимоги національного та міжнародного законодавства;
- використовувати напрацьовані практики (стандарти, методології) побудови подібних СЗІБ;
- визначити підрозділи, відповідальні за реалізацію та підтримку СЗІБ;
- рас проділити між підрозділами області відповідальності у здійсненні вимог СЗІБ;
- на базі управління ризиками інформаційної безпеки визначити загальні положення, технічні та організаційні вимоги, складові політики інформаційної безпеки об'єкта захисту;

- реалізувати вимоги політики інформаційної безпеки, впровадивши відповідні програмно-технічні засоби і способи захисту інформації;

- реалізувати систему менеджменту (управління) інформаційної безпеки (СМІБ);

- використовуючи систему управління організувати регулярний контроль ефективності СЗІБ і при необхідності перегляд і коригування СЗІБ .

Під системою безпеки будемо розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз (рис. 1.) [2].

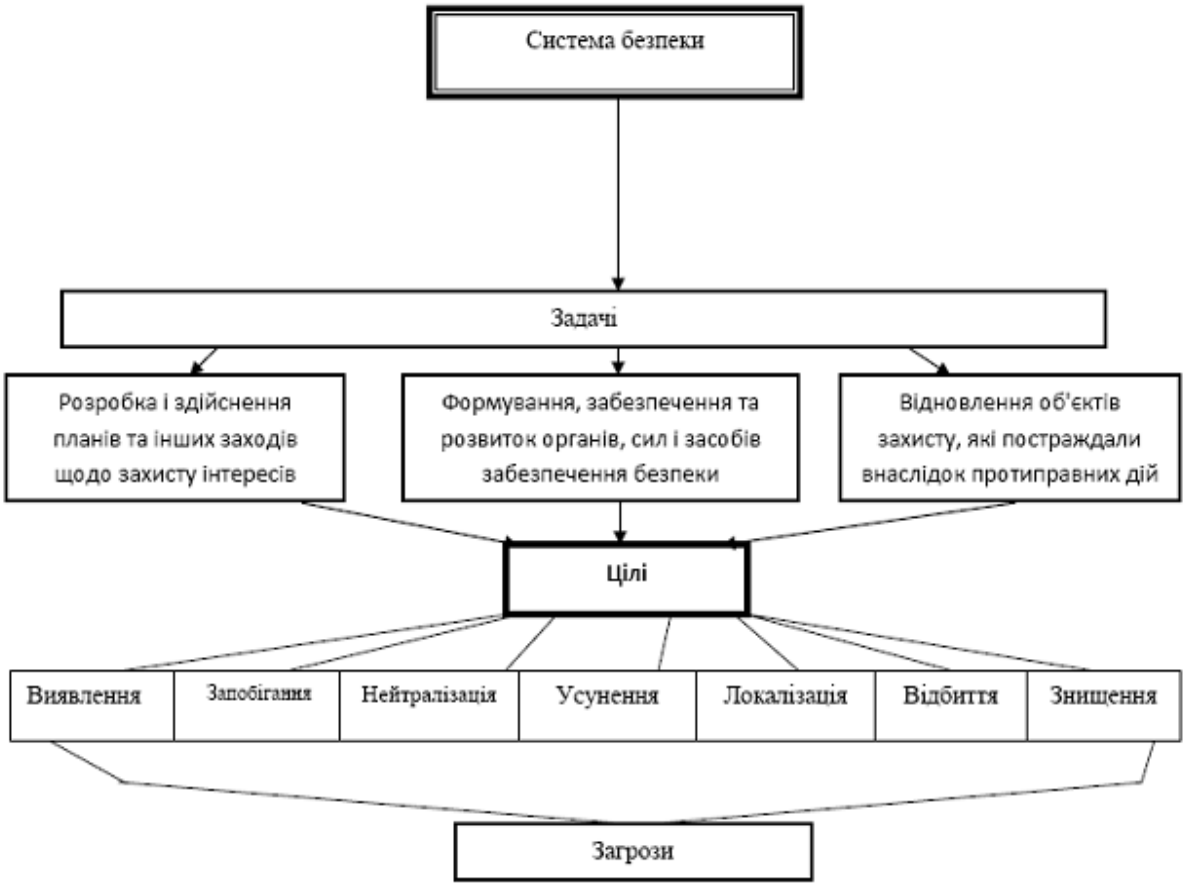

Рисунок 1 - Функціональна система інформаційної безпеки

Загроза являє собою сукупність певних факторів та умов, які виникли в процесі взаємодії об'єкта безпеки з іншими об'єктами, а також його компонентів між собою, які здатні негативно впливати на об'єкт.

Між загрозою і небезпекою нанесення шкоди існують певні відносини заподіяння цієї шкоди, які визначаються зв'язок між явищами, при якій одне явище, зване причиною, за наявності певних умов неминуче породжує інше явище, зване слідством. Загроза завжди породжує небезпеку. Небезпека може бути визначена як стан, в якому знаходиться об'єкт внаслідок появи загрози. Відмінність між ними полягає в тому, що небезпека є властивістю об'єкта безпеки, а загроза - властивістю об'єкта взаємодії. Очікуваним результатом загрози є шкода - наслідок негативної зміни умов існування об'єкту [3] .

Загрози інформаційній безпеці - це можливі дії або події, які можуть вести до порушень ІБ. Види загроз інформаційної безпеки дуже різноманітні і мають безліч класифікацій:

- За характером порушення:
  1. Порушення конфіденційних даних
  2. Порушення працездатності системи
  3. Незаконне втручання в функціонування системи
- За тяжкістю порушення:
  1. Незначні помилки
  2. Дрібне хуліганство
  3. Серйозний злочин
- За мотивацією:
  1. Зловмисне
  2. Незловмисне
- За місцем виникнення:
  1. Зовнішні загрози
  2. Внутрішні загрози(зі сторони інсайдерів)
- За об’єктом впливу:

1. Загрози, націлені на всю інформаційну систему
2. Загрози, націлені на окремі компоненти інформаційної системи

- За причиною виникнення:

1. Загрози, що виникли в результаті недостатніх засобів технічного захисту
2. Загрози, що виникли через брак організаційних мір

- За каналом проникнення:

1. Через слабкість програмного забезпечення
2. Через прогалини в системі авторизації та недоліки системи зберігання документів

Згідно представленої класифікації загроз за видом об'єкта впливу вони поділяються на: загрози інформації, загрози персоналу об'єкта та загрози власне забезпеченню інформаційної безпеки об'єкта.

При розробці необхідних, засобів, методів і заходів, що забезпечують захист інформації, необхідно враховувати велику кількість різних факторів.

Інформація, яка у даному випадку є предметом захисту, може бути представлена на різних технічних носіях, а також її носіями можуть бути користувачі і обслуговуючий персонал. Вона може піддаватися обробці в комп'ютерних системах, передаватися по каналах зв'язку і відтворюватись різними пристроями. Таким чином, для забезпечення інформаційної безпеки існують наступні принципи [5]: системність, комплексність та безперервність захисту інформації; гнучкість управління і застосування; відкритість алгоритмів і механізмів захисту; простота застосування захисних засобів і заходів.

За способами здійснення всі заходи забезпечення безпеки комп'ютерних систем підрозділяють на:

- правові(діючі закони, укази та нормативні акти);
- морально-етичні(норми поведінки);

- організаційно-адміністративні(регламентація процесів функціонування інформаційних систем - ІС);
- апаратно-програмні.

Особливу увагу необхідно приділити *апаратно-програмним заходам* захисту. До них відносяться електронні пристрої та спеціальні програми, які реалізуються самостійно або в комплексі з іншими. Можна виділити такі основні способи захисту[5]:

- ідентифікацію та аутентифікацію суб'єктів ІС;
- розмежування доступу до ресурсів ІС;
- контроль цілісності даних;
- забезпечення конфіденційності даних;
- аудит подій, що відбуваються в ІС;
- резервування ресурсів і компонентів ІС.

1.2 Системи дистанційного навчання

Система дистанційного навчання (СДН) - інформаційна система, яка представляє собою складний комплекс програм і рішень та призначена для планування, проведення та управління всіма навчальними заходами в організації (включаючи навчання, що проводиться як в очній, так і в дистанційній формі) [11].

Сучасна система дистанційного навчання повинна забезпечувати:

- централізоване автоматизоване управління навчанням;
- швидке і ефективне розміщення та надання навчального контенту учнем;
- єдину платформу для вирішення основних завдань у рамках планування, проведення та управління всіма навчальними заходами;
- підтримку сучасних стандартів у сфері технологій дистанційного навчання;

- персоналізацію навчального контенту і можливість його багаторазового використання;
- широкий діапазон засобів взаємодії між усіма учасниками навчального процесу.

Основними цілями використання, в рамках побудови корпоративного навчання, системи дистанційного навчання є:

- підвищення ефективності організації навчання;
- скорочення витрат на навчання за рахунок впровадження сучасних технологій електронного навчання;
- прискорення процесів навчання;
- спростити процедуру оцінки ефективності навчання.

Весь функціонал, який реалізований у сучасних системах дистанційного навчання умовно можна розділити на три основні блоки: управління навчанням, забезпечення взаємодії учасників навчального процесу та розробка навчального контенту.

В рамках управління навчанням СДН надають наступні основні функціональні можливості:

- управління компетенціями;
- автоматизоване формування навчальних програм;
- управління профілями користувачів;
- управління доступом до дистанційних курсів та тестів;
- внесення до журналу діяльності користувачів;
- забезпечення технічної та методичної підтримки користувачів;
- формування звітів;
- аналіз процесу навчання.

Для забезпечення взаємодії учасників навчального процесу, СДН надають наступні основні засоби організації спілкування користувачів:

- форум;
- чат;

- відеоконференція;
- блог;
- Wiki;
- віртуальна класна кімната.

Розробка навчального контенту містить набір інструментів, які вирішують широкий спектр завдань. Від створення простих тестів для проведення тестування слухачів, до розробки складних мультимедійних курсів. Однак, слід зазначити, що не всі системи включають в себе засоби розробки навчального контенту, справедливо припускаючи, що в якості засобів розробки можуть використовуватися програмні продукти сторонніх виробників.

Для цілковитої експлуатації функцій системи дистанційного навчання(СДН) необхідна досконала організація ефективної служби підтримки. Відсутність якісної технічної підтримки слухачів дистанційного навчання може значно знизити його ефективність.

Побудова ефективної системи підтримки системи дистанційного навчання вимагає:

- впровадження ефективної системи моніторингу стану СДН;
- використання засобів для контролю параметрів та стану облікових записів користувачів;
- використання засобів, що забезпечують швидку ідентифікацію причин виникнення збоїв у роботі СДН;
- створення Service Desk;
- вибудовування ефективного процесу підтримки користувачів.

Також необхідною умовою для побудови максимально ефективної і універсальної системи дистанційного навчання є її відповідність найбільш поширеному стандарту SCORM.

Поняття SCORM є акронімом від Sharable Content Object Reference Model, що означає: зразкова модель об'єкта вмісту для спільного використання.

SCORM визначає технічну основу для середовища навчання, побудованого з використанням Web-технологій. SCORM об'єднує безліч взаємопов'язаних технічних вимог, стандартів і нормативів. SCORM описує модель агрегації змісту (Content Aggregation Model) і середовище виконання (Run-Time Environment) для навчальних об'єктів, забезпечуючи адаптивне навчання, засноване на навчальних цілях, пріоритетах, продуктивності та інших факторах. SCORM також описує модель послідовності і навігації (Sequencing and Navigation) для динамічного відображення вмісту в залежності від потреб учнів.

SCORM базується на таких основних принципах:

- СДН повинна використовувати навчальний контент, розроблений з використанням засобів розробки, створених різними виробниками;
- СДН, створені різними виробниками, повинні мати можливість використовувати один і той же навчальний контент;
- СДН повинні мати можливість звернення до загального сховища навчального контенту і використовувати навчальний контент, що там зберігається.

Отже, підтримка стандарту SCORM дозволяє використовувати в системі дистанційного навчання дистанційні курси, розроблені різними виробниками, у випадку, якщо вони в свою чергу теж розроблені відповідно до стандарту SCORM.

Необхідно зазначити, що успішне впровадження електронного навчання ґрунтується на правильному виборі програмного забезпечення, яке відповідає конкретним вимогам, цілям і завданням, що висуває до нього організація.

До основних критеріїв вибору засобів організації електронного навчання можна віднести наступні:

- Функціональність.

Розуміє під собою наявність в системі набору функцій різного рівня, таких як форуми, чати, аналіз активності учнів, управління курсами і учнями та інше;

- Надійність.

Цей параметр характеризує зручність адміністрування і простоту оновлення контенту системи на базі існуючих шаблонів. Комфортабельність управління та захист від зовнішніх впливів істотно впливають на ставлення користувачів до системи та ефективності її використання;

- Стабільність.

Означає безперебійність та стійкість роботи системи по відношенню до різних режимів роботи і ступеня активності користувачів;

- Вартість.

Складається з вартості самої системи, а також з витрат на її впровадження, розробку курсів і супровід, наявність або відсутність обмежень по кількості ліцензій на слухачів (студентів);

- Наявність засобів розробки контенту.

Вбудований редактор навчального контенту не тільки полегшує розробку курсів, але і дозволяє інтегрувати в єдиній формі освітні матеріали різного призначення;

- Підтримка SCORM.

Стандарт SCORM є міжнародною основою обміну електронними курсами і відсутність в системі його підтримки знижує мобільність і не дозволяє створювати курси, які потім можна переносити та модифікувати;

- Система перевірки знань.

Дозволяє в режимі онлайн оцінювати знання учнів. Зазвичай така система включає в себе тести, завдання і контроль активності учнів на форумах;

- Зручність використання.

При виборі нової системи необхідно забезпечити зручність її використання. Це важливий параметр, оскільки потенційні учні ніколи не стануть використовувати технологію, яка здається громіздкою або створює труднощі при навігації. Технологія навчання повинна бути інтуїтивно зрозумілою. У навчальному курсі має бути максимально просто знайти меню допомоги, легко переходити від одного розділу до іншого і спілкуватися з інструктором.

- Модульність.

У сучасних системах електронного навчання курс може являти собою набір мікромодулів або блоків навчального матеріалу, які можуть бути використані в інших курсах.

- Забезпечення доступу.

Учні не повинні мати перешкод для доступу до навчальної програми, пов'язаних з їх розташуванням в часі і просторі, а також з можливими факторами, що обмежують можливості учнів (обмежені функції організму, ослаблений зір). Також використання технологій «завтрашнього дня», які підтримуються обмеженим колом програмного забезпечення, істотно знижує коло потенційних користувачів.

- 100% мультимедійність.

Можливість використання в якості контенту не тільки текстових, гіпертекстових і графічних файлів, але і аудіо, відео, gif- і flash-анімації, 3D-графіки різних файлових форматів.

- Масштабованість і розширюваність.

Можливість розширення кола учнів по СДН і додавання програм, і курсів навчання та освіти.

- Перспективи розвитку платформи.

СДН повинна бути розвивається середовищем, повинні виходити нові, поліпшені версії системи з підтримкою нових технологій, стандартів і засобів.

- Крос-платформність СДН.

В ідеалі система дистанційного навчання не повинна бути прив'язана до якої-небудь операційної системи або середовища, як на серверному рівні, так і на рівні клієнтських машин. Користувачі повинні використовувати стандартні засоби без завантаження додаткових модулів, програм і т.д.

- Якість технічної підтримки.

Можливість підтримки працездатності, стабільності СДН, усунення помилок і вразливих місць як із залученням фахівців компанії розробника СДН, так і фахівцями власної служби підтримки.

- Наявність (відсутність) російської локалізації продукту.

Локалізована версія продукту більш дружня як для адміністрування, розробки курсів, так і для кінцевих споживачів освітніх послуг.

Слідуючи даним критеріям можна максимально вигідно і ефективно підібрати систему дистанційного навчання, яка б задовольняла усі вимоги організації, де вона буде впроваджена і була б зрозумілою та доступною для усіх користувачів. Така система буде ефективною та затребуваною, якщо вона буде реалізована відповідно всім вимогам до СДН.

1.3 Інформаційна безпека у системах дистанційного навчання

Забезпечення інформаційної безпеки - одне з найважливіших завдань організацій при проведенні дистанційного навчання.

Говорячи про інформацію як про ресурс систем управління, можна зазначити, що для забезпечення його безпеки потрібен комплексний підхід, який дозволить різнобічно забезпечити, по-перше, цілісність, по-друге, доступність, по-третє, конфіденційність. Різноманіття і широке застосування систем дистанційного навчання в різних сферах людської діяльності, а також їх залежність від безпеки інформаційного ресурсу підсилюють значимість і актуальність дослідження СДН.

Актуальність питання інформаційної безпеки таких систем обумовлена проблемами забезпечення цілісності, доступності та конфіденційності

паралельно з питаннями забезпечення - сумісності, розширюваності та масштабованості цих систем.

Також необхідно зазначити, що існують комерційні та системи з відкритим кодом. Налаштування інформаційної безпеки таких систем дещо різниться між собою з очевидних причин, проте ключові моменти їх адміністрування – однакові.

Плюси комерційного програмного забезпечення широко відомі: в більшості своїй це надійні продукти (особливо ті, які прижилися на ринку), з належним рівнем підтримки користувачів, регулярними апгрейдами і новими версіями.

Однак, є й мінуси. Так, наприклад, існує проблема «закритих дверей» при використанні СДН на закритих платформах. По-перше, код джерела недоступний технічній підтримці організації, тому навіть невеликі зміни на рівні користувача не є можливими. Організація може спробувати вийти на контакт з компанією-виробником, якщо у нього з'явилися пропозиції про вдосконалення, але дуже малоймовірно, що його ідеї будуть втілені в короткий проміжок часу, якщо взагалі будуть. Крім цього до мінусів можна віднести високу вартість будь-якого комерційного продукту, регулярні виплати за ліцензію, за збільшення кількості користувачів (що взагалі-то є обов'язковим фактором будь-якої мережевої систем) та інше.

Системи з відкритим кодом дозволяють вирішувати ті ж завдання, що і комерційні системи, але при цьому у користувачів є можливість доопрацювання і адаптації конкретної системи до своїх потреб і поточної освітньої ситуації.

Більшість систем з відкритим кодом є крос-платформними рішеннями і не прив'язані ні до конкретних операційним системам, ні до конкретних Web-браузерів.

Сучасні тенденції розвитку OpenSource LCMS спрямовані в бік універсалізації та збільшення функціональності систем. За своїми

можливостями найбільш просунуті системи не поступаються комерційним аналогам, а деякі навіть перевершують.

СДН з відкритим вихідним кодом дозволяють реалізувати той же набір функціональних можливостей, що і комерційні рішення, але з істотно меншими економічними витратами.

Отже, аналіз та застосування засобів безпеки СДН є першочерговим завданням для досягнення максимального рівня безпеки.
До них, зокрема, відносяться інструменти адміністрування СДН. З їх допомогою, завдяки гнучкій системі налаштувань, можна забезпечити максимальну приватність користувачам та конфіденційність інформації, яка зберігається в навчальній базі системи. Для здійснення налаштувань всієї системи є адміністратор(у випадку налаштування курсу його роль може виконувати викладач), якому необхідно:

- створити облікові записи та призначити їм ролі.

Тут можна реєструвати, видаляти і редагувати облікові записи користувачів системи. Також є форма, в якій зберігаються особисті дані цього користувача, його блог, повні звіти про діяльність, його повідомлення. В налаштуваннях можна призначити роль користувачеві.

(Роль - це сукупність прав (дозволів), визначених в цілому для сайту, які можуть бути призначені певним користувачам в заданому контексті.)

- налаштувати курс.

Мається на увазі, можливість як створення нового курсу, так і використання вже існуючого, іншими словами є функція клонування курсів та налаштувань. А також контроль доступу користувачів до навчальних ресурсів системи.

- наповнити курс навчальними матеріалами.

У розпорядженні системи є велика різноманітність модулів (елементів курсу), які можуть бути використані для створення курсів будь-якого типу. Залежно від змісту курсу і концепції викладання, адміністратор включає найбільш підходящі елементи і ресурси, що надаються системою.

- адмініструвати процес навчання.

Зокрема, до цієї функції можна віднести вчасне оновлення і/або видалення облікових записів, перевірка актуальності даних (інформація про користувачів, навчальних матеріалів), що зберігаються в системі. Зміна прав доступу та переназначення ролей для учасників учбового процесу.

Таким чином, адміністратор - користувач з максимально широкими правами, основною метою якого є підтримка стабільної роботи системи, управління користувачами, налаштування основних параметрів системи, інформаційна безпека курсу та особистих даних користувачів, резервне копіювання і багато іншого. Саме від його продуманої та, як наслідок, ефективної роботи буде залежати робота всієї системи дистанційного навчання.

1.4 Висновки

На сьогоднішній день одним з головних завдань при використанні СДН є забезпечення інформаційної захищеності адміністратором, який повинен цю систему впровадити для використання та надалі, забезпечувати повне її обслуговування та підтримку.

Однак, при адмініструванні віртуального навчального середовища постає проблема вибору платформи, на якій буде побудована СДН. Цей вибір залежить від цілого ряду чинників: які вимоги пред'являються до середовища, які функціональні характеристики повинні бути присутніми, на яких користувачів орієнтована середовище та які налаштування в ній можна виконувати.

Комерційні системи дистанційного навчання у більшості випадків більш надійні, але вони майже не піддаються модифікаціям та змінам, які часто вносять адміністратори.

Безперечні переваги використання СДН на OpenSource, тому що такі системи є найбільш логічним вибором для освітніх проектів, оскільки основна його ідея полягає в співпраці, і сама ідеологія дозволяє об'єднати таланти і

досвід великої кількості користувачів у розвитку та вдосконаленні освітніх програмних продуктів. Більш того, таке навчальне програмне забезпечення може функціонувати як інструмент, орієнтований на учня, як основа для гнучкого та придатного для змін адміністратором навчання, адаптованого для будь-якої навчальної програми.

Отже**,** в умовах сучасного світу надійна безпека інформаційних ресурсів СДН може бути забезпечена тільки певним рядом заходів, таких як

1. Обміркований вибір програмного та апаратного забезпечення,
2. Ефективне адмініструванням таких систем,
3. Комплексний підхід до захисту інформації.

В свою чергу, комплексна система захисту інформації повинна бути:

- безперервною
- плановою
- цілеспрямованою
- конкретною
- активною
- надійною

2 ГРУПИ СИСТЕМ ДИСТАНЦІЙНОГО НАВЧАННЯ. LON-CAPA

2.1 LCMS системи.

На сьогоднішній день серед великого різноманіття засобів організації електронного навчання можна виділити такі групи:

- авторські програмні продукти (Authoring Packages),
- системи управління контентом (Content Management Systems - CMS),
- системи управління навчанням (Learning Management Systems - LMS),
- системи управління навчальним контентом (Learning Content Management Systems - LCMS)[12].

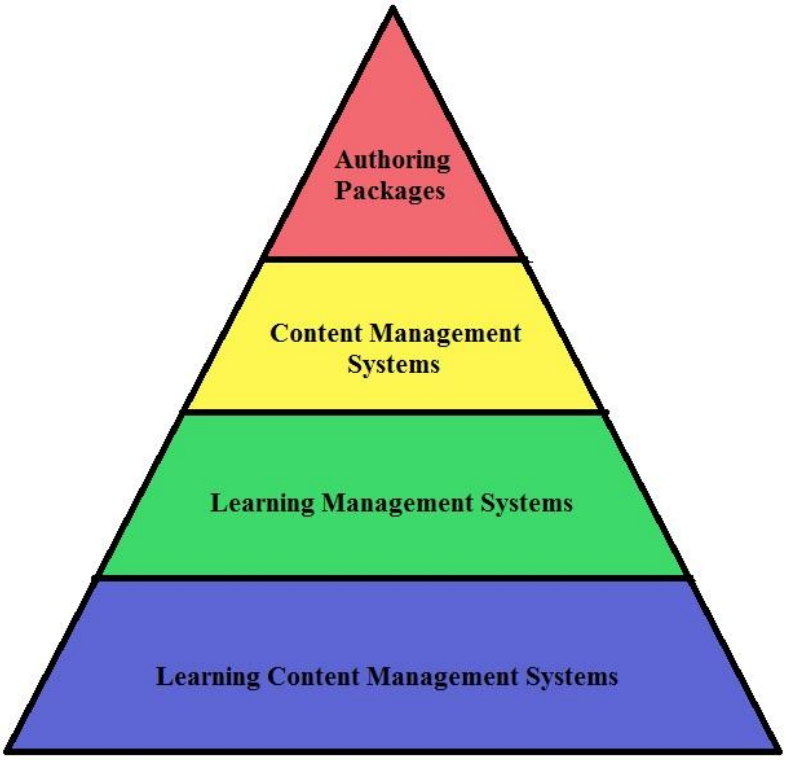

Рисунок 2 - Групи систем дистанційного навчання

Кожна з цих систем призначена для вирішення свого сегменту завдань, однак у зв'язку з їх стрімким розвитком більшість виробників намагаються включати функціональні можливості однієї системи в іншу. Це явище найбільш поширене в LCMS (виробники додають функціональність загального управління навчанням) та LMS (виробники реалізують можливість управління навчальним контентом) системах.

Так як деякі з цих систем можуть виконувати функції один одної, їх необхідно детальніше розглянути, щоб розмежувати, адже кожна система має свої особливості і чітко поставлені завдання, для яких вона була розроблена.

- Авторські програмні продукти (Authoring Packages):

Авторські продукти спеціально розроблені для подолання тих труднощів, з якими стикаються викладачі при використанні мов програмування. Ці програми зазвичай дозволяють викладачеві самостійно розробляти навчальний контент на основі візуального програмування. Викладач повинен піклуватися тільки про те, щоб помістити необхідну інформацію в потрібне місце. Ця інформація у вигляді фрагмента тексту, ілюстрації або відеофрагменту поміщається на екран.

Недоліком таких продуктів є відсутність можливості відстежувати і контролювати у часі процес навчання і успішність великої кількості учнів. Як правило, вони розроблені для створення уроків з негайним зворотним зв'язком з учнем, а не для зберігання інформації про навчальний процес протягом тривалого часу.

Крім того, велика частина таких програм не має коштів для забезпечення контакту між учнями в реальному часі. Зазвичай, там неможливо організувати чати, дискусії або двосторонній аудіо обмін. Інтерактивність також зазвичай обмежена.

Таким чином можна зробити висновок що, такі системи не є затребуваними через локальність своїх можливостей і лише частково вирішують проблеми організації електронного навчання.

- Системи управління контентом (CMS):

Системи управління контентом дозволяють створювати каталоги графічних, звукових, аудіо- , відео-, текстових та ін. файлів і керувати ними. Така система являє собою базу даних, забезпечену механізмом пошуку за ключовими словами, що дозволяє викладачеві або розробнику курсів швидко знайти те, що йому потрібно.

Системи управління контентом особливо ефективні в тих випадках, коли над створенням курсів працює велика кількість викладачів, яким необхідно використовувати одні й ті ж фрагменти навчальних матеріалах в різних курсах. Це скорочує час на розробку курсів, оскільки, наприклад, замість створення нового зображення, викладач може просто знайти і використовувати одне з вже існуючих.

Подібні системи швидше підходять для створення Web-сайтів, порталів з розміщеними на них освітніми матеріалами, однак для повноцінної організації дистанційної системи навчання вони не підходять.

- Системи управління навчанням (LMS):

Електронне навчання, як і будь-який навчальний процес, крім змістовної частини обов'язково включає організаційний компонент. Елементи управління процесом проходження курсів присутні в розвинених електронних бібліотеках, але для реалізації великої системи e-Learning цієї функціональності буде недостатньо. Знадобиться автоматизація таких завдань, як надання навчального контенту користувачам в потрібний час, контроль використання навчальних ресурсів, адміністрування окремих слухачів і груп, організація взаємодії з викладачем, звітність і т.д. Ці функції реалізують системи управління навчанням LMS, які являють собою платформу для розгортання e-Learning, але в ряді випадків можуть використовуватися і для адміністрування традиційного навчального процесу.

Система LMS, в ідеалі, повинна надавати кожному студенту персональні можливості для найбільш ефективного вивчення матеріалу, а менеджеру навчального процесу - необхідні інструменти для формування навчальних програм, контролю їх проходження, складання звітів про результативність навчання, організації комунікацій між студентами і викладачами. Студент отримує від LMS можливості доступу до навчального порталу, який є відправною точкою для доставки всього навчального контенту, вибору відповідних навчальних курсів на основі попереднього і проміжних тестувань, використання додаткових матеріалів за допомогою спеціальних посилань.

Адміністративні функції LMS охоплюють декілька базових областей. Управління студентами включає в себе реєстрацію та контроль доступу користувачів до системи і до навчального контенту, організацію слухачів в групи для надання їм загальних курсів і складання звітності, управління аудиторними і викладацькими ресурсами. LMS відповідає також за інтеграцію додаткових елементів навчального процесу (практичні заняття, лабораторні роботи, тести, засоби спільної роботи, посилання на зовнішні матеріали та ін.).

Крім того, LMS відповідає за розподіл і використання навчального контенту. У числі таких завдань - організація зручних для пошуку каталогів курсів, виділення груп курсів для обов'язкового вивчення і вивчення «за бажанням», розробка індивідуальних навчальних курсів, інші механізми цільового надання навчального контенту, підтримка синхронних і асинхронних режимів взаємодії з викладачем. Найважливішим елементом LMS є звітність по навчальному процесу, яка дозволяє, зокрема, робити висновки про ефективність вкладень в електронне навчання. У LMS повинні бути механізми контролю і складання звітів про те, наскільки успішно просувається слухач (або група) у вивченні певних тем, чи відповідає підвищення рівня професійної кваліфікації заданим на початку навчання цілям, наскільки отримані знання знаходять застосування у практичній роботі і впливають на її результативність.

Дуже важливо для LMS забезпечувати активну підтримку широкого кола курсів від сторонніх виробників. Деякі LMS сумісні з інструментом розробки

тільки власного виробництва, а інші дуже обмежено сумісні зі стандартами навчального контенту.

LMS повинна підтримувати стандарти, такі як SCORM і AICC. Підтримка стандартів означає, що LMS може імпортувати і управляти контентом і курсами, які скомпільовані у відповідності зі стандартами, незалежно від засобів розробки, які були використані.

Для LMS обов'язкова наявність модулів оцінки та тестування, при цьому найбільш сервісний підхід, коли

а) надається можливість включення тесту (модуля оцінки) як частини кожного розділу курсу (мережевого уроку);

б) є самостійний модуль тестування (і модуль оцінки), наприклад, за результатами вивчення окремого розділу та / або курсу в цілому.

Модуль управління знаннями дозволяє організації визначити необхідність у навчанні та ідентифікувати область докладання зусиль, яка базується на компетенції робочого колективу в конкретній області.

LMS забезпечує і механізми захисту, необхідні для мережевого середовища e-Learning, а також, у разі масштабних навчальних проектів, підтримує інтеграцію з системами планування ресурсів підприємства та управління персоналом.

LMS, будучи рішенням для управління навчальним процесом, підтримує, як мінімум, використання електронних курсів з різних джерел; найбільш розвинені системи пропонують спеціальні модулі для розробки власного навчального контенту.

Для того щоб LMS-платформи мали можливість «програвати» різні готові курси, створені стандарти інтероперабельності. Так, Airline Industry CBT Committee описує взаємодію комп'ютерних тренінгів з системами управління і служить основою для розвитку аналогічних стандартів інтероперабельності для Web-курсів. Широко відомі стандарти ISM для платформ навчання, а також Sharable Content Object Reference Model (SCORM) - сукупність технічних

специфікацій для створення навчального Web-контенту, розроблених в рамках програми Advanced Distributed Learning Міністерства оборони США.

- Системи управління навчальним контентом (LCMS):

Останні роки активно розвивається новий клас систем, що реалізують управління навчальним контентом (Learning Content Management System, LCMS). Подібні системи концентруються на управлінні змістом навчальних програм які орієнтовані на розробників контенту, фахівців з методологічної компонування курсів і керівників проектів навчання. В основі LCMS лежить концепція подання змісту навчання як сукупності багаторазово використовуваних навчальних об'єктів зі своєю цільовою аудиторією і певним контекстом використання.

Незважаючи на численні варіації можливостей LCMS, вона повинна включати наступні ключові компоненти:

- Репозитарій навчальних об'єктів.

Репозитарій навчальних об'єктів - це центральна база даних, яка зберігає і управляє навчальним контентом. З цієї точки окремі навчальні об'єкти доступні користувачам або як окремі елементи або як частина в складі більш великого навчального модуля, який у свою чергу може бути частиною повного курсу, цей процес визначається залежно від індивідуальних вимог до навчання. Кінцевий продукт може бути доступний через Web, CD-ROM, або в паперовому вигляді. Кожен об'єкт, залежно від вимог, може бути використаний кілька разів і з різними цілями. Інтегрованість контенту забезпечується незалежно від методу доставки.

- Програмне забезпечення автоматизованого аутсорсинга.

Це ПЗ використовується для створення багаторазово використовуваних навчальних об'єктів, які потім будуть доступні в репозитарії. Додаток автоматизує розробку, надаючи авторам шаблони і архівні зразки, що містять основні принципи дизайну навчального контенту. Використовуючи ці шаблони, автори можуть розробляти курси, застосовуючи наявні об'єкти з репозиторію, створюючи нові об'єкти, або використовуючи комбінацію з нових і старих

об'єктів. Авторами можуть бути експерти з тематики, дизайнери навчальних курсів, творці медіа-продукції і так далі. Цей інструмент також може бути використаний для швидкої конвертації існуючих в організації бібліотек навчального контенту, таких як додаткові аудіовізуальні матеріали, спеціальні інтерфейси і методики навчання.

- Інтерфейс відображення (програвання контенту).

Для представлення навчальних об'єктів відповідно до профілю навчання, для попереднього тестування і / або відповідно до запитів користувачів, є необхідним інтерфейс відображення матеріалів. Цей компонент також забезпечує трекінг результатів, посилання на відповідні джерела інформації та різні варіанти оцінки і зворотного зв'язку від користувачів. Цей інтерфейс може бути налаштований для конкретної організації, що використовує LCMS. Для прикладу, контент може бути представлений на веб-сторінках, що містять емблему організації та елементи оформлення прийняті в поточному корпоративному стилі. Крім цього, елементи управління та оформлення можуть бути локалізовані під необхідний регіон.

- Засоби адміністрування.

Ця програма використовується для управління обліковими записами учнів, запуском курсів з каталогу, відстеження результатів, складання звітів про процес навчання та інших простих адміністративних функцій.

Тіньова сторона застосування LCMS в тому, що вона дозволяє дати великий поштовх плануванню та отриманню навичок дизайну ефективних навчальних об'єктів - оскільки надає для використання шаблони і приклади. Дизайнери повинні мислити нелінійно і добре розуміти всі різні варіанти контенту, для якого об'єкт буде необхідний або може бути використаний.

Ринок LCMS поки ще досить фрагментований, що свідчить про його незрілость, проте він швидко розвивається; системи цього класу стають все більш затребуваними і розглядаються не просто як необхідна інфраструктура для e-Learning, але - принаймні, західними компаніями - і як частина загальної корпоративної IT-інфраструктури. Підтвердженням тому є інтерес, який

проявляють до рішень з управління навчанням виробники систем загального управління, в тому числі, компанії SAP (SAP Learning Solution), Oracle (iLearning), PeopleSoft (Enterprise Learning Management).

2.2 LON-CAPA – платформа для організації дистанційного навчання

Для реалізації дистанційного навчання сьогодні розроблено багато платформ, однак вони мають характерні особливості та відмінності. Саме тому для вибору однієї з них необхідним детальний аналіз їх функціональних можливостей.

Проаналізуємо найбільш поширені та відомі платформи:

- Платформа дистанційного навчання Moodle:

Moodle (модульне об'єктно-орієнтоване динамічне навчальне середовище), яке може використовуватися як платформа для електронного, в тому числі дистанційного навчання. Вона орієнтована насамперед на організацію взаємодії між викладачем та учнями, хоча підходить і для організації традиційних дистанційних курсів, а також підтримки очного навчання.

- Платформа дистанційного навчання ATutor:

ATutor є веб - орієнтованою системою керування навчанням. Програмний продукт є простим у встановленні, налаштуванні та підтримці для системних адміністраторів; викладачі (інструктори) можуть досить легко створювати та переносити навчальні матеріали та запускати свої онлайн-курси. А оскільки система є модульна, тобто складається з окремих функціональних одиниць — модулів, то вона відкрита для модернізації і розширення функціональних можливостей.

- Платформа дистанційного навчання Dokeos:

Dokeos – платформа побудови сайтів дистанційного навчання, заснована на гілці (fork) Claroline(версії 1.4.2.). Гілка являє собою клон вільно поширюваного програмного продукту, створений з метою змінити додаток - оригінал в тому чи іншому напрямку.

Dokeos безкоштовна і залишиться такою, оскільки ліцензія Claroline (GNU/GPL) припускає, що гілки підпадають під ту ж ліцензію. Оскільки гілка була виділена недавно, обидва додатки зараз відносно схожі один на одного, хоча деякі відмінності в ергономіці, побудові інтерфейсу, функціоналі вже починають проявлятися.

- Платформа дистанційного навчання LON-CAPA:

LON-CAPA (Learning Online Network with Computer-Assisted Personalized Approach) це безкоштовна платформа з відкритим вихідним кодом (Open Source). Вона не має ліцензійних зборів або обмежень, і всі компоненти системи є відкритими. Система була розроблена університетами та за підтримки приватних фондів.

LON-CAPA орієнтована на взаємодію між користувачами. Це стабільна, легко масштабована система, яка зайняла своє місце у світі серед багатьох віртуальних університетських курсів.

Для більш наочного порівняння систем, результати були зведені у таблицю 1.

Таблиця 1 - Порівняльна характеристика СДН [9]

	Инструменты коммуникации							Обучающие объекты					Управление данными пользователей				Удобство использования				Адаптация				Технические аспекты				Администрирование			Управление курсами			Итоговые баллы
	Форумы	Чаты	Внутренняя почта/сообщения	Оповещения	Конференции	Сотрудничество	Синхронные и асинхронные инструменты	Тесты	Обучающие материалы	Упражнения	Другие создаваемые обучающие объекты	Импортируемые обучающие объекты	Отслеживание	Статистика	Идентификация онлайн-пользователей	Персональные профили пользователей	Дружественность пользователю	Поддержка	Документация	Содействие	Адаптируемость	Персонализация	Расширяемость	Адаптивность	Стандарты	Системные требования	Безопасность	Масштабируемость	Управление пользователями	Управление авторизацией	Установка платформы	Управление курсами	Оценивание тестов	Организация объектов курса	
Максимальное значение	4	4	1	2	2	2	4	4	4	3	2	4	4	2	2	3	3	3	2	2	4	3	4	4	3	2	4	2	3	4	1	2	3	3	**99**
Moodle	4	4	0	2	0	2	4	4	4	3	2	4	4	1	2	2	3	3	2	2	3	2	4	1	3	2	2	2	1	1	1	1	1	1	**77**
ILIAS	2	4	1	0	0	0	4	4	1	0	2	4	1	1	2	2	1	1	2	0	2	3	4	0	3	2	4	0	3	4	1	2	2	2	**64**
Dokeos	2	4	0	1	2	0	4	4	4	0	2	4	2	1	0	1	2	3	2	2	1	0	4	2	2	2	0	0	3	0	1	1	1	3	**60**
LON-CAPA	2	4	1	1	0	0	4	2	1	1	1	4	1	1	0	2	0	3	0	2	2	3	3	1	3	2	2	1	2	2	1	1	3	3	**59**
ATutor	1	3	1	1	0	0	4	1	4	0	2	4	4	2	1	1	2	1	2	2	1	3	3	1	2	2	0	0	0	1	1	1	1	3	**55**
Sakai	3	4	0	1	0	0	4	0	4	3	1	4	4	0	1	1	3	1	1	0	0	0	4	0	0	2	2	2	0	2	1	2	0	0	**50**
OpenUSS	3	4	0	2	0	1	4	0	1	0	2	3	0	0	2	2	2	2	1	2	3	3	3	0	0	2	1	2	0	0	0	0	1	3	**49**
Spaghettilearning	1	4	1	1	0	0	4	2	0	0	1	4	4	2	2	1	2	2	1	2	2	3	2	0	0	2	2	0	1	0	1	1	1	0	**49**
dotLRN	3	0	1	2	0	0	0	1	0	0	2	1	0	0	2	1	1	1	2	0	2	2	4	0	2	2	4	2	1	3	0	2	0	2	**43**

Слід зазначити, що дослідження систем проводилося більше трьох років тому і за цей час багато з них пройшли ряд удосконалень.

Згідно результатам дослідження провідні позиції займають п'ять систем. Для реалізації цілі дипломної роботи була обрана платформа LON-CAPA. По даним таблиці вона займає не перше місце, але такий вибір зумовлений тим, що функції адміністрування LON-CAPA краще збалансовані у порівнянні з іншими системами та є більш наочними. Крім цього, однією з причин вибору цієї системи був надійний спосіб забезпечення інформаційної цілісності та конфіденційності навчальних матеріалів і особистих даних користувачів.

LON-CAPA це повнофункціональна система для управління курсами, навчальним контентом та системою оцінок.

До функцій управління курсами входять:

- розміщення матеріалів
- обговорення навчального процесу
- оголошення
- лабораторія планування
- створення простору для портфоліо

До функцій управління навчальним контентом відносять:

- зберігання онлайн контенту для повторного використання в інших курсах і семестрах
- управління правами доступу

Оцінка виставляється за результатами:

- домашнього завдання
- тестів та екзаменів

Ви можете запустити LON-CAPA безкоштовно на свій власний виділений сервер, або ви можете отримати хостинг і підтримку за окрему плату.

Кількість установ, які використовують LON-CAPA неухильно росте протягом багатьох років. На сьогоднішній день система тільки у США з`єднує між собою більш ніж 60 університетів і таку ж кількість старших шкіл. Крім

того, у цій мережі задіяні 10 коледжів, різні грантові проекти та, навіть, комерційні видавничі компанії.

На рис.3 можемо спостерігати як розповсюджувалось використання системи LON-CAPA [13]:

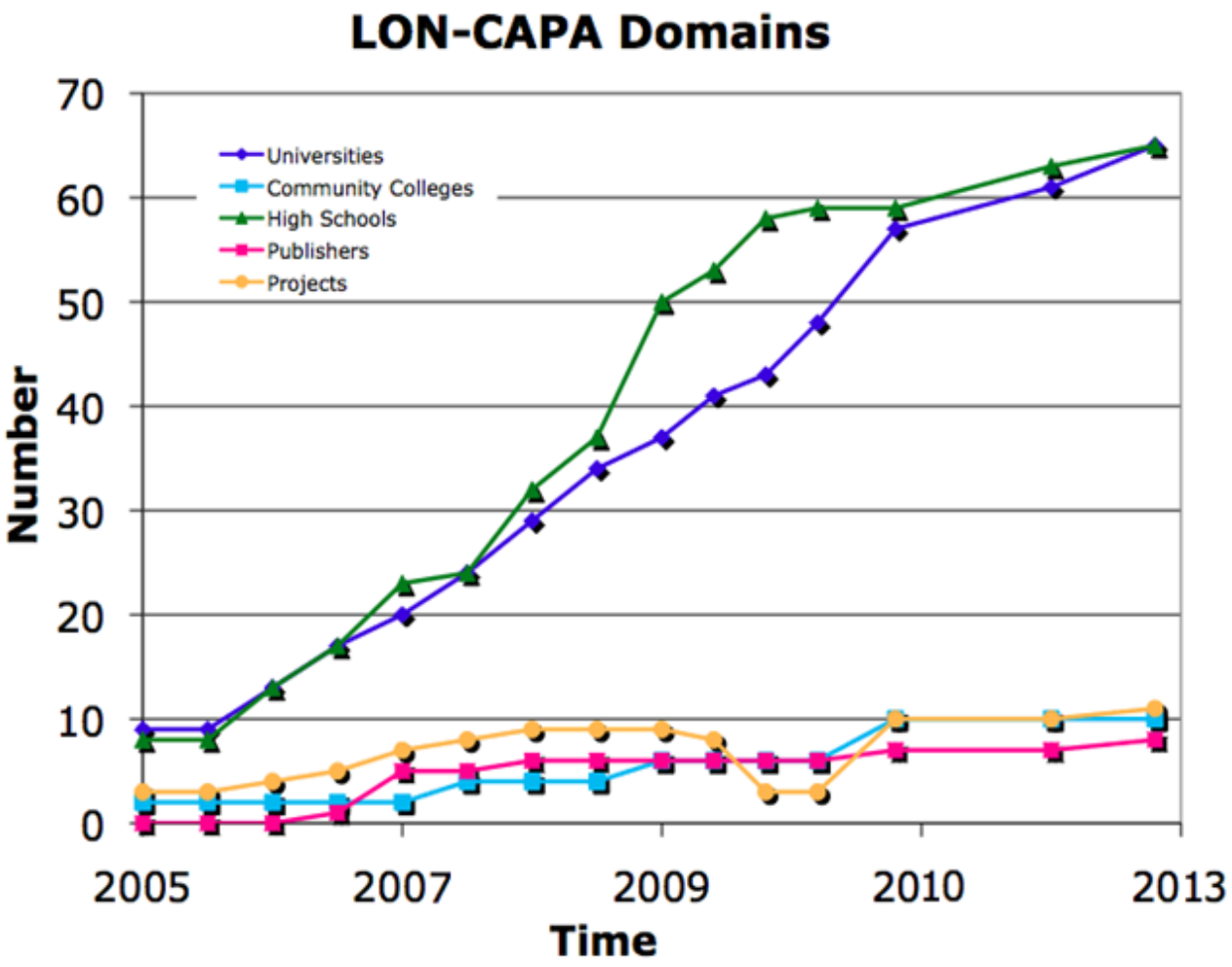

Рисунок 3 - Поширення системи LON-CAPA

На графіку чітко проілюстрована тенденція збільшення кількості організацій, які використовують LON-CAPA. Також не можна залишити без уваги і те, що така система організації навчання є дуже зручною і корисною для студентів. Розробниками LON-CAPA було проведено дослідження як впровадження онлайн навчання вплине на оцінки.

Щодо інших країн, там LON-CAPA ще не набула провідних позицій, але з кожним роком кількість установ, які оцінили її функціональні можливості і використовують систему збільшується.

На рис.4 можемо побачити, як поширюється система між різними установами у всьому світі.

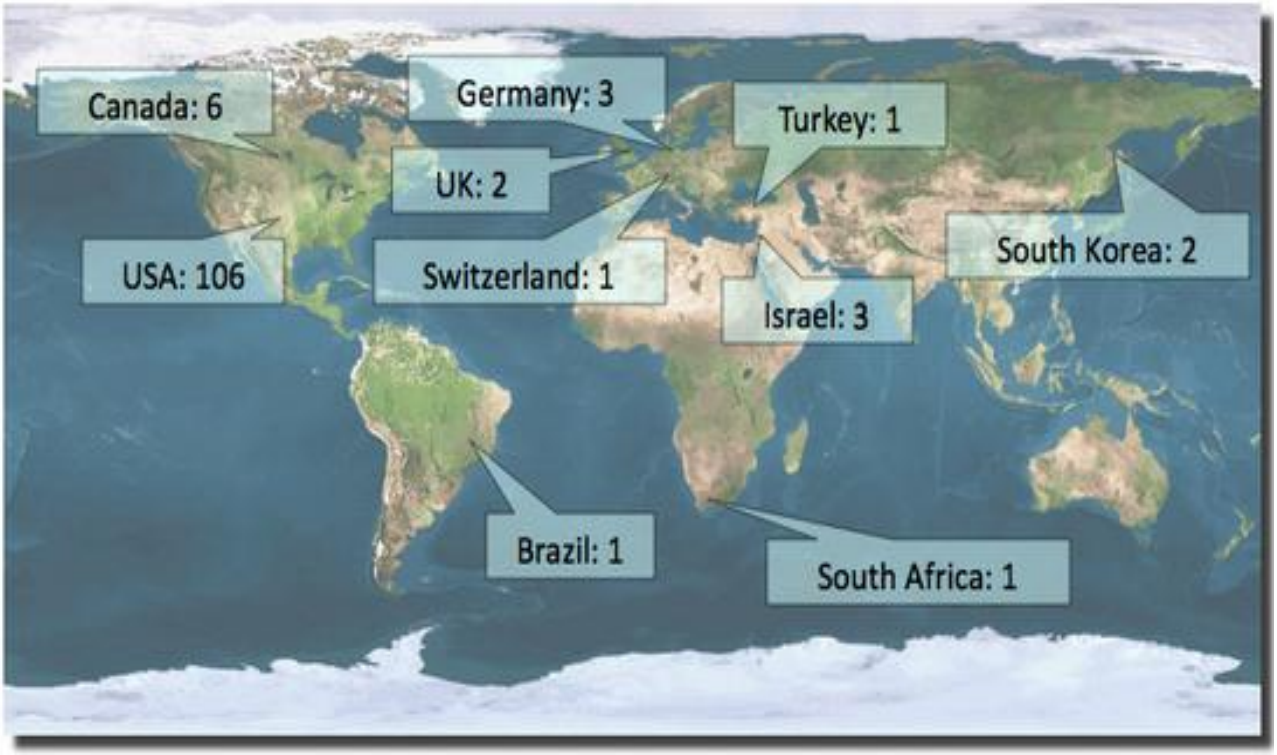

Рисунок 4 - Поширення системи у світі

Здатність практикувати роз’вязання, можливість мати декілька спроб для отримання правильного рішення, негайна допомога в освоєнні матеріалу – ці чинники значно вплинули на якість самостійного навчання студентів і, як наслідок, це призвело до загального покращення оцінок.

Стовпчики помилок вказують коливання по всій семестрам. Найкращою оцінкою є 4.0, і студенти, оцінка яких нижче 2.0 не можуть бути допущені до наступного курсу. Онлайн домашнє завдання значно знижує відсоток студентів, які знаходяться на межі провалу курсу, і значно збільшує відсоток студентів з оцінкою 3,5 і 4,0.

У порівнянні з іншими онлайн системами, LON-CAPA є безкоштовною для студентів.

На рис.5 можемо спостерігати позитивний вплив онлайн навчання на загальну успішність студентів з курсу фізики (чорним кольором позначена залежність до впровадження системи, а зеленим - після)[14]:

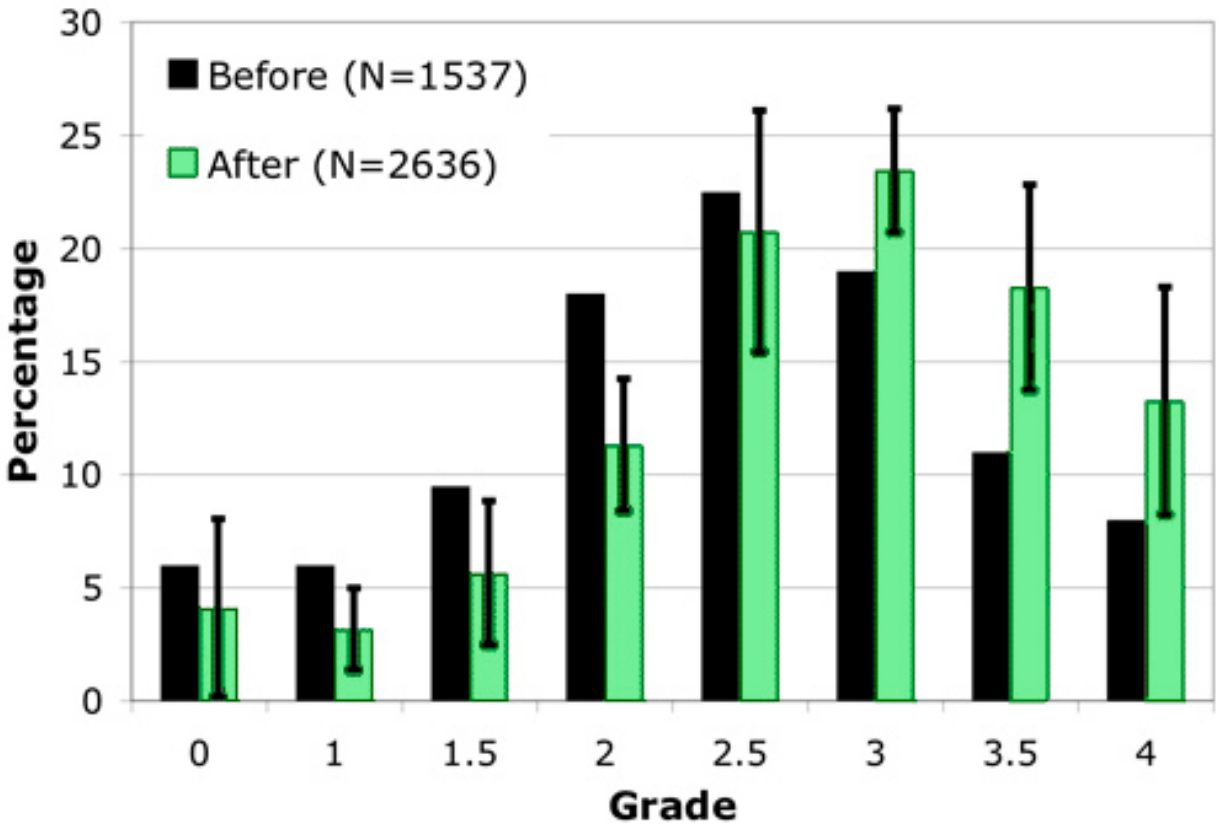

Рисунок 5 - Вплив онлайн навчання на успішність студентів

LON-CAPA це система, яка працює на Intel / AMD-апаратному програмному забезпеченні згідно з різними Linux-дистрибутивами. Система легко масштабується, так як обидва додаткових модуля і сесії машини можуть бути додані в будь-який час з мінімальним часом простою. LON-CAPA також працює на віртуальних машинах і в SAN середовищах.

Треба зазначити, що масштабованість системи забезпечується з однієї сторони мережею двох класів серверів:

- Сервери бібліотеки (Library Servers):

створюють копії контенту ресурсів та даних користувача. Таким чином, можна запустити будь-яку кількість машин з цією бібліотекою і користувачі можуть

бути переміщенні між ними з декількома годинами простою. Дані сервери потребують резервного копіювання.

- Сервери доступу (Access Servers)

працюють тільки з сесіями користувачів і не потребують резервного копіювання. Вони можуть бути реалізовані як онлайн так і оффлайн з мінімальним часом простою.

А з іншої сторони, у функціоналі LON-CAPA є передбаченим збалансування навантаження по всій мережі, це означає, що сесія (якщо вона так налаштована) може навіть бути розвантажена до інституційних меж. Це може бути реалізовано на рівні peer-to-peer (рівний до рівного), де один сервер розвантажує сесії до іншого, або в інтерфейсі LON-CAPA за допомогою балансування навантаження (рис.6)[15].

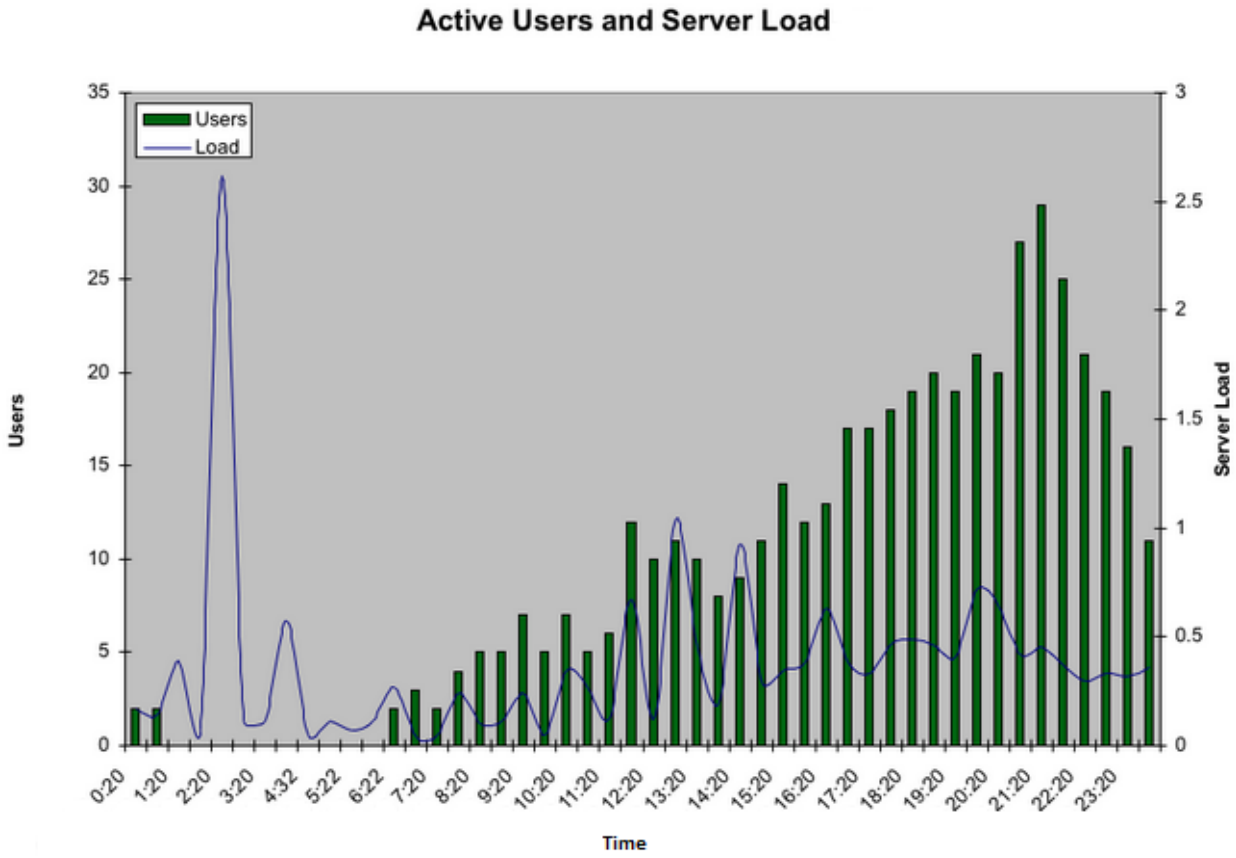

Рисунок 6 - Графік розподілу навантаження від кількості користувачів

Створення навчальних матеріалів вимагає затрат часу та коштів, тому однією із значних переваг системи LON-CAPA є можливість спільного доступу до навчального контенту. Таким чином розроблені навчальні матеріали

системи використовуються у рамках багатьох курсів. Можна сказати, що створюється певний навчальний об`єкт, який може бути повторно використаний на різних рівнях курсів, дисциплін і навіть інститутів – вбудований цифровий менеджер прав гарантує, що всі дії відбуваються згідно прав користування викладених авторами (рис. 7)[16].

Рисунок 7 - Загальна схема доступу до навчальних матеріалів

Для цього, в архітектурі LON-CAPA передбачений загальний пул ресурсів (сховище), що охоплюють декілька установ на найнижчому рівні. Факультет може зібрати ресурси з цього пулу на різних рівнях (наприклад, модулі, розділи, уроки і т.д.), і використовувати таку збірку в своїх курсах, а також зберігати їх знову в пул ресурсів для повторного використання. На найвищому рівні, LON-CAPA включає в себе повну систему управління для того, щоб ефективно та без втрат даних розгорнути ці ресурси в курсах системи.

Таке повторне використання зображена на рис.8: модулі на індивідуальні теми з фізики, які пишуть в двох різних закладах, збірка модулів у третьому та повторне використання в четвертому створюють єдину “мережу” в дистанційному навчанні[16].

Рисунок 8 - Спільне використання ресурсів різними закладами

Отже, LON – CAPA це система дистанційного навчання, використання якої значно полегшує процес навчання для користувачів та розробників курсу, завдяки доступності платформи, широким можливостям масштабування та повторного використання ресурсів у різних курсах.

З кожним роком система набуває все більшої популярності та поширення в усьому світі, що доводить, що функціонал системи добре розвинений і піддається модифікаціям (OpenSource).

2.3 Проблеми впровадження LON-CAPA в навчальний процес

Хотілося б відзначити проблеми, з якими належить зіткнутися при впровадженні будь - якої системи дистанційного навчання, а зокрема і LON-CAPA. До них слід віднести необхідність авторам курсів самостійно структурувати навчальний матеріал, неминуче адаптувавши його до вимог персонального комп'ютера. Для багатьох цей процес не є очевидним і надзвичайно хворобливий.

Консерватизм викладацького складу - не менше важка проблема. Вона відноситься до числа організаційних і може призвести до фатальних наслідків для впровадження системи дистанційного навчання в рамках навчального закладу.

Недостатня обізнаність технічного персоналу, в чиї обов'язки входить розгортання системи дистанційного навчання. Буває так, що особи, в чию компетенцію входять технологічні питання, приділяють невиправдано багато часу обговоренню варіантів, замість того, щоб зайняти активну позицію. Тому для розгортання системи дистанційного навчання потрібна компетентна людина.

Протидія тих, кому доручено запровадження дистанційного навчання. Якщо викладач впроваджує окремі компоненти дистанційного навчання, то йому можуть сказати, що це слід робити в рамках корпоративного стандарту навчального закладу (а коли з'явиться цей стандарт, нікому не відомо!), або що це методологічно спірно.

Необхідність постійного супроводу курсу. Існує думка, що після впровадження системи дистанційного навчання, її супроводу не буде потрібно. Це далеко не так. Тому що СДН потрібно постійно адмініструвати на наявність порушень доступу, підтримки навчальних курсів, створення все нових і нових користувачів.

Тим не менш, вже сьогодні існує достатня кількість впроваджених систем дистанційного навчання. Яким чином вдалося впровадити їх? Вдалим і гармонійним поєднанням потенціалу, можливостей і правильного розуміння ролі і місця дистанційного навчання в традиційному навчальному процесі.

Найбільш поширений спосіб впровадження СДН – це придбання вже готового рішення з документованими можливостями, на базі якого організація-замовник вирішує завдання розгортання дистанційного навчання. У вартість програмного забезпечення зазвичай входить докладна документація, методична та технічна підтримка. При цьому, організація-замовник самостійно вводить систему в експлуатацію.

Однак, готове рішення, значно дорожче за розгортання вільно-поширюваної СДН силами організації. Такий шлях дозволяє значно знизити витрати на реалізацію проекту розгортання СДН, «заточити» систему під свої потреби і вимоги, але майже вся тяжкість впровадження системи лягає на IT - службу організації. Також проект по впровадженню може затягнутися по часу, внаслідок відсутності оперативної технічної підтримки OpenSource співтовариства.

Таким чином впровадження OpenSource системи LON-CAPA дозволяє налаштувати її так, як необхідно організації (створення довільної кількості курсів, користувачів) та значно зменшує витрати на організацію дистанційного навчання, але велика частина обов’язків по впровадженню, а надалі й підтримки такої платформи, залишається на відділ адміністрування компанії.

2.4 Висновки

У сучасному світі існує вже багато рішень для організації дистанційного навчання, а ще більше систем, які керують ним, як от, наприклад:

- авторські програмні продукти (Authoring Packages),
- системи управління контентом (Content Management Systems - CMS),
- системи управління навчанням (Learning Management Systems - LMS),

- системи управління навчальним контентом (Learning Content Management Systems - LCMS).

Першочергове завдання організації, яка хоче впровадити СДН, визначити, які функції ця система має виконувати та для чого слугувати.

Останнім часом все більшої популярності та поширення набувають LCMS системи, хоча вони досить нові, але такий інтерес до них цілком виправданий, адже в них вдало поєднано багато функцій і при використанні стандартів XML, інформація може бути легко переміщена в LMS на рівні навчальних об’єктів.

Крім того, LCMS може керувати контентом на рівні грануляції нижче навчального об'єкта, що дозволяє організації більш просто здійснювати реструктуризацію та перенацілювання онлайн - контенту. Додатково, просунуті LCMS вміють динамічно будувати навчальні об'єкти відповідно до профілів користувачів або стилів навчання.

3 ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Засоби інформаційного захисту системи LON-CAPA

Для того, щоб зрозуміти як забезпечити максимальну інформаційну безпеку системі LON-CAPA необхідно з'ясувати, які засоби захисту є у самій системі дистанційного навчання.

Першим ступенем захисту такої системи є LDAP (Lightweight Directory Access Protocol — «полегшений протокол доступу до каталогів»). Це протокол прикладного рівня для доступу до служби каталогів, він є досить простим і дозволяє проводити операції аутентифікації, а також додання, зміни та видалення користувачів з каталогу.

У випадку СДН, поняття аутентифікація – це перевірка достовірності користувача шляхом порівняння введеного ним паролю з паролем, збереженим в базі даних користувачів.

Кожен запис в LDAP має своє унікальне ім'я, внаслідок чого на одному рівні каталогу не може існувати двох однакових записів. Таким чином ми можемо уникнути повторного створення користувачів з однаковим іменем та їх заміни записів один одним.

Використання такої системи як LDAP посилює інформаційну безпеку та забезпечує конфіденційність інформації, що зберігається у СДН, тому що користувачі, які внесені до каталогу LDAP мають пройти попередню аутентифікацію, щоб потрапити до системи LON-CAPA.

У дипломній роботі LDAP був використаний для зберігання у його каталозі даних координатора домену та для подальшої його аутентифікації у LON-CAPA, де користувач (координатор домену) надалі зможе створювати нові облікові записи користувачів системи та надавати їм права та ролі.

Слід зазначити, що і в самій системі LON-CAPA для збереження цілісності та конфіденційності ресурсів розробниками передбачено використання протоколу Kerberos, що орієнтований в основному на клієнт-

серверну архітектуру. Він реалізований на механізмі взаємної аутентифікації двох співрозмовників перед встановленням зв'язку між ними в умовах незахищеного каналу.

Іншими словами Kerberos базується на симетричних алгоритмах шифрування та для своєї роботи потребує довірену третю сторону. У ролі довіреної третьої сторони виступає Центр Розподілу Ключів, що складається із двох логічно розділених частин: Сервера Аутентифікації і Сервера Видачі Квитків. Отож, Kerberos працює на основі "квитків", які використовуються для підтвердження ідентичності користувачів.

ЦРК зберігає базу даних закритих ключів; закритий ключ учасника мережі відомий лише йому та ЦРК. Знання цього ключа є підтвердженням ідентичності учасника. Для з’єднання двох учасників, ЦРК генерує ключ сесії, який забезпечує безпеку повідомлень. Безпека протоколу сильно залежить від синхронізації часу учасників мережі та від обмеження часу придатності квитків.

Отже, протокол Kerberos забезпечує високий рівень захисту системі LON-CAPA, тому що пароль користувача не зберігається у незашифрованому вигляді навіть у базі даних аутентифікації, а після завершення етапів аутентифікації та авторизації, клієнт та сервер встановлюють зашифрований зв'язок (з допомогою генерації та обміну ключами шифрування).

3.2 Аналіз методів захисту інформації

Забезпечення інформаційної безпеки передбачає створення системи захисту інформаційних ресурсів від зловмисників, які схочуть ці ресурси використовувати, модифікувати або просто знищити.

Під інформаційною безпекою розуміється "стан захищеності інформації (даних), при якому забезпечені її конфіденційність, доступність та цілісність"[17]. При цьому:

- Конфіденційність – це забезпечення доступу до інформації тільки авторизованим користувачам.
- Цілісність – це забезпечення достовірності та повноти інформації та методів її обробки.
- Доступність – це забезпечення доступу до інформації авторизованим користувачам по мірі необхідності.

Комплексний характер, проблеми захисту говорить про те, що для її вирішення необхідне поєднання законодавчих, організаційних і програмно-технічних заходів.

Знання можливих загроз, а також вразливих місць інформаційної системи, необхідне для того, щоб вибирати найефективніші засоби забезпечення безпеки.

Одними з найнебезпечніших та найчастіших є ненавмисні помилки користувачів, операторів, системних адміністраторів і інших осіб, обслуговуючих інформаційні системи. Іноді такі помилки приводять до прямого збитку (неправильно введені дані, помилка в програмі, що викликала зупинку або руйнування системи). Іноді вони створюють слабкі місця (найчастіше через помилки адміністрування), якими можуть скористатися зловмисники.

На другому місці за розмірами збитку розташовуються крадіжки і фальсифікації. В більшості випадків винуватцями виявлялися штатні співробітники організацій, чудово знайомі з режимом роботи і захисними заходами.

Ключовим етапом для побудови надійної інформаційної системи є вироблення політики безпеки.

Політика безпеки – це набір документованих норм, правил та практичних прийомів, що регулюють управління, захист та розподіл інформації обмеженого доступу[18].

З практичної точки зору політику безпеки доцільно розділити на три рівні:

- Рішення, що зачіпають організацію в цілому. Вони носять досить загальний характер і, як правило, йдуть від керівництва організації.
- Питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних систем, експлуатованих організацією.
- Конкретні методи для забезпечення інформаційної безпеки системи.

Для дипломної роботи ключовим моментом політики безпеки для системи є методи і засоби забезпечення захисту інформації та їх аналіз.

Методи можна класифікувати наступним чином:

- Перешкода;
- Управління доступом ;
- Маскування ;
- Регламентація ;
- Примус ;
- Спонукання.

Для аналізу цих методів необхідно детально зупинитися на кожному з них. Таким чином,

1. Перешкода - метод фізичного перешкоджанню шляху зловмиснику до інформації, що захищається (сигналізація, замки і т.д.).

2. Управління доступом - метод захисту інформації, пов'язаний з регулюванням використання всіх ресурсів інформаційної системи (елементів баз даних, програмних і технічних засобів).

Управління доступом включає наступні функції захисту:

- ідентифікацію співробітників і ресурсів інформаційної системи;
- аутентифікацію (встановлення автентичності) об'єкту по пред'явленому їм ідентифікатору (імені). Як правило, до таких засобів відносяться паролі;
- перевірку повноважень - авторизація користувачів;

3. Маскування - метод захисту інформації шляхом її криптографічного закриття. Цей метод захисту широко застосовується за кордоном, як при

зберіганні інформації, так і при обробці. При передачі інформації по каналах зв'язку великої протяжності цей метод дійсно надійним.

4. Регламентація - метод захисту інформації, що створює певні умови автоматизованої обробки, зберігання та передачі інформації, при яких можливість несанкціонованого доступу до неї (мережевих атак) зводилася б до мінімуму.

5. Примус - метод захисту, при якому користувачі системи змушені дотримуватися правил обробки, передачі і використання інформації (яка захищається) під загрозою матеріальної, адміністративної та кримінальної відповідальності.

6. Спонукання - метод захисту інформації, який мотивує користувачів не порушувати встановлені правила за рахунок дотримання сформованих моральних і етичних норм.

Всі перераховані методи інформаційної безпеки реалізуються за допомогою основних засобів захисту: фізичних, апаратних, програмних, апаратно-програмних, криптографічних, організаційних, законодавчих та морально-етичних.

Засоби забезпечення безпеки процесів переробки інформації, що використовуються для створення механізму захисту, поділяються на:

1. Формальні (виконують захисні функції по заздалегідь передбаченій процедурі без безпосередньої участі людини). До них входять:

- Фізичні засоби захисту, які призначені для зовнішньої охорони території об'єктів і захисту компонентів інформаційної системи організації (механічні, електричні, електромеханічні, електронні, електронно-механічні пристрої та системи, які функціонують автономно).
- Апаратні засоби захисту - це пристрої, вбудовані в блоки інформаційної системи (сервери, комп'ютери і т.д.) або сполучаються з нею спеціально для вирішення завдань захисту інформації. Вони

призначені для внутрішнього захисту елементів обчислювальної техніки та засобів зв'язку.

- Програмні засоби захисту, що призначені для виконання функцій захисту інформаційної системи за допомогою програмних засобів (антивірусний захист, міжмережеві екрани і т.д.).

2. Неформальні (визначаються цілеспрямованою діяльністю людини або регламентують цю діяльність). До них входять:

- Організаційні засоби - організаційно-технічні заходи, спеціально передбачаються в технології функціонування системи з метою вирішення завдань захисту інформації.
- Законодавчі засоби - нормативно-правові акти, за допомогою яких регламентуються права та обов'язки, а також встановлюється відповідальність всіх осіб і підрозділів, що мають відношення до функціонування системи, за порушення правил обробки інформації, наслідком чого може бути порушення її захищеності. Морально-етичні засоби - склалися в суспільстві або даному колективі моральні норми або етичні правила, дотримання яких сприяє захисту інформації, а порушення їх прирівнюється до недотримання правил поведінки в суспільстві або колективі.

Графічно така класифікація представлена на рис. 9:

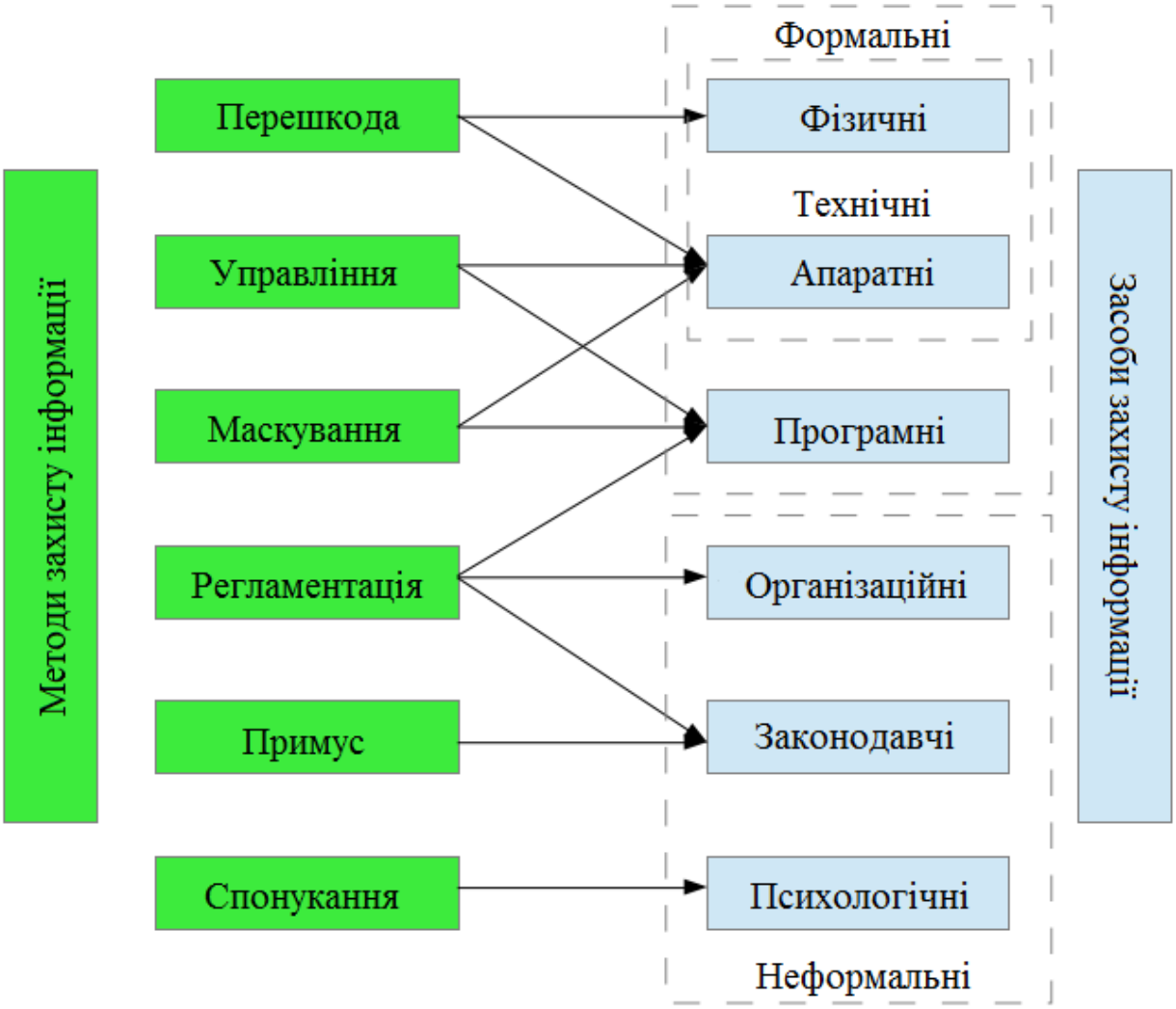

Рисунок 9 – Методи та засоби захисту інформації

Серед усіх розглянутих методів, для впровадження у систему LON-CAPA, були обрані методи управління доступом та регламентації доступу. Такий вибір обумовлений тим, що метод маскування вже частково реалізований при використанні протоколу Kerberos у самій системі, а інші методи більш орієнтовані на фізичне перешкоджання крадіжки інформації та залежать від морально - етичних норм людей.

Хоча тут, необхідно зазначити, що методи управління доступом та регламентації доступу також були обрані, тому що є одними з найбільш дієвих та гнучких для налаштування у СДН. Адже вони напряму взаємодіють з

користувачами, визначаючи їхні ролі та права у системі та доступ до інформаційних ресурсів. Такі методи дають змогу забезпечити конфіденційність даних користувачів системи та розміщених матеріалів.

Оскільки, однією з особливостей системи LON-CAPA є можливість повторного використання розроблених навчальних ресурсів в інших курсах, ці методи дуже важливі, зокрема для координаторів та викладачів навчальних курсів, які можуть надати доступ до їхніх матеріалів іншим викладачам, і заборонити – для гістьових облікових записів.

Гнучкість методів забезпечується можливістю створення, реструктуризації та зміни курсів та навчальних матеріалів, а також створення нових ролей для користувачів, щоб забезпечити мінімізацію повноважень. Під мінімізацією повноважень мається на увазі, що використовуючи методи захисту інформації , для реалізації безпеки системи, користувачам необхідно надавати мінімальні права доступу до інформації (чи курсу/групи) у відповідності до службової необхідності (викладачі, студенти і т.д.), аби уникнути несанкціонованого доступу до зміни навчальних курсів та матеріалів і крадіжки та поширення особистої та навчальної інформації в мережі Інтернет.

Отже, застосування додаткових методів захисту є необхідною умовою для покращення функціонування системи LON-CAPA, її захищеності від викрадання інформаційних ресурсів та для забезпечення доступу до її курсів тільки користувачів, які мають такі права.

3.3 Реалізація методів захисту у системі LON-CAPA

Таким чином, для реалізії методів захисту LON-CAPA у самій системі необхідно налаштувати ролі та повноваження, а також визначити та регламентувати користувачів та групи користувачів, які матимуть доступ до курсу та навчальних ресурсів.

Налагодження методу управління доступом в СДН показано на наступних рисунках:

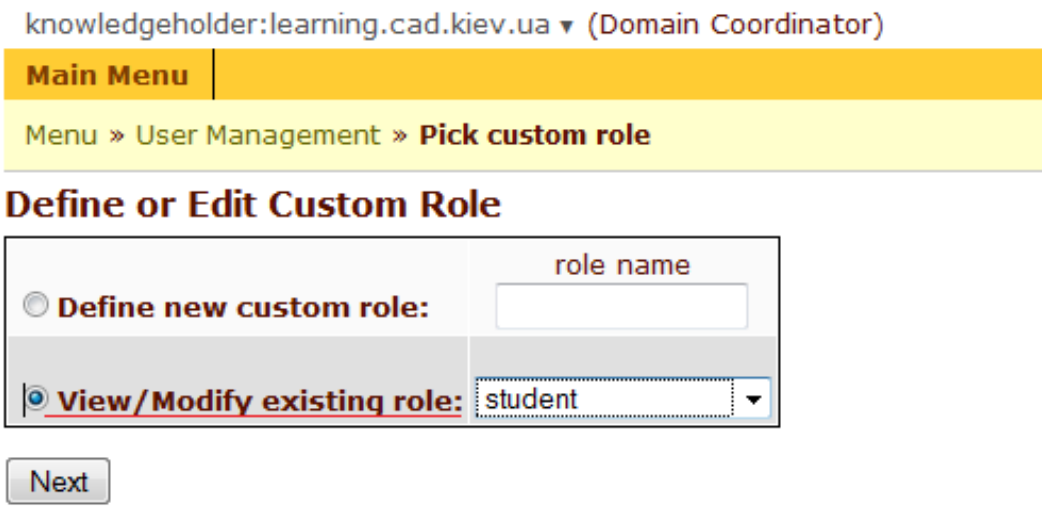

Рисунок 10 – Перегляд та модифікація ролей користувача

Рисунок 11 – Додати нову роль, для налаштування особливих прав користувачу

- При створенні нової ролі або модифікуванні вже існуючої, можна обрати серед вже доступних шаблонів і додати/відмінити права, які там присутні. Також можна вибрати, які права будуть в цієї ролі в контексті курсу чи спільноти.

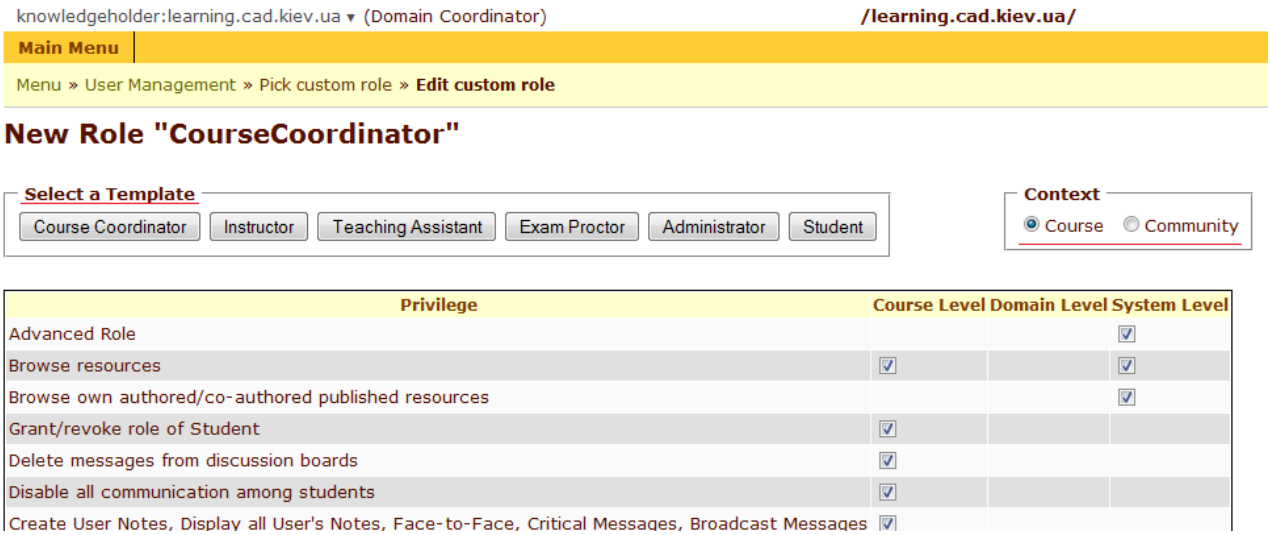

Рисунок 12 – Вибір шаблону та курсу

- Безпосередній вибір прав для ролі користувача:

Privilege	Course Level	Domain Level	System Level
Advanced Role			☑
Browse resources	☑		☑
Browse own authored/co-authored published resources			☑
Grant/revoke role of Student	☑		
Delete messages from discussion boards	☑		
Disable all communication among students	☑		
Create User Notes, Display all User's Notes, Face-to-Face, Critical Messages, Broadcast Messages	☑		
Evade communication blocking	☑		
Generate anonymous statistics	☑		
Lock and unlock assessments	☑		
Edit course contents	☑		
Modify grade queue	☑		
Modify grades	☑		
Grade items in grading queue	☑		
Set assessment parameters	☑		
Post anonymously	☑		
Advanced printing options (with answers, discussions, all foils, ...)	☑		
Post discussion on course resources	☑		
Print for other users and entire course	☑		
Post to chat rooms	☑		
Get identity behind anonymous postings	☑		
Send internal message		☑	
Send broadcast and receipt-required message	☑		
View grades	☑		
Access to What's New Page	☑		

- При створенні або редагуванні користувача, можна регламентувати його ролі (видаляти/додавати), такі як:
  1. Роль автора
  2. Роль на рівні домену
  3. Роль у навчальному курсі(надання доступу користувачам).

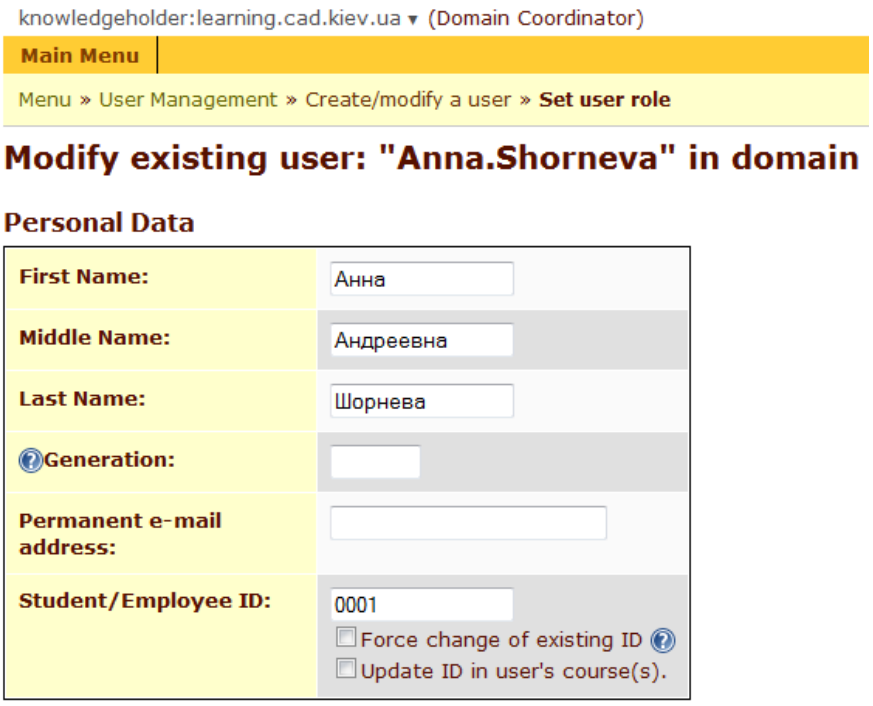

Рисунок 14 – Модифікування користувача

Також можна вибрати належність до курсу та часові рамки для ролей створюваного користувача:

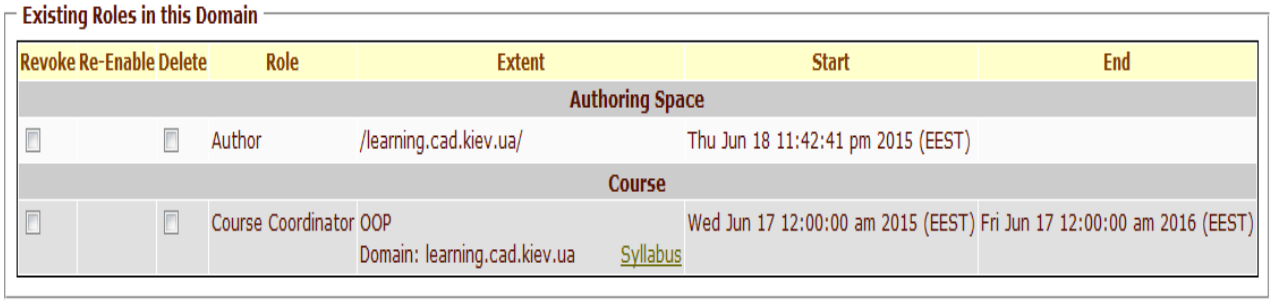

Рисунок 15 – Часові рамки

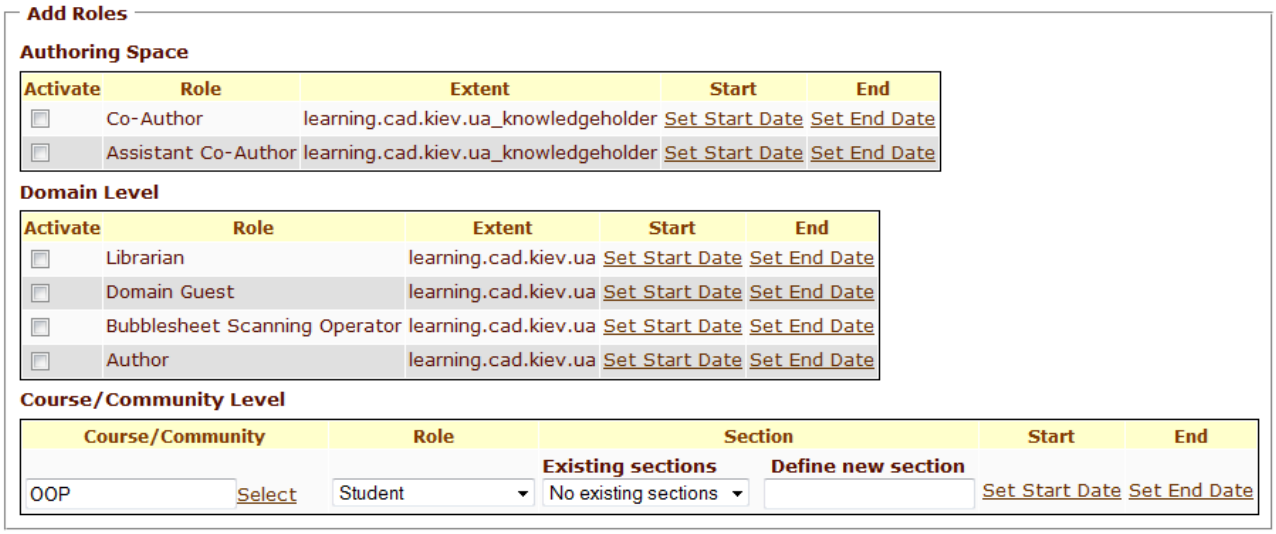

Рисунок 16 – Додання студента до курсу на рівні управління координатора домену

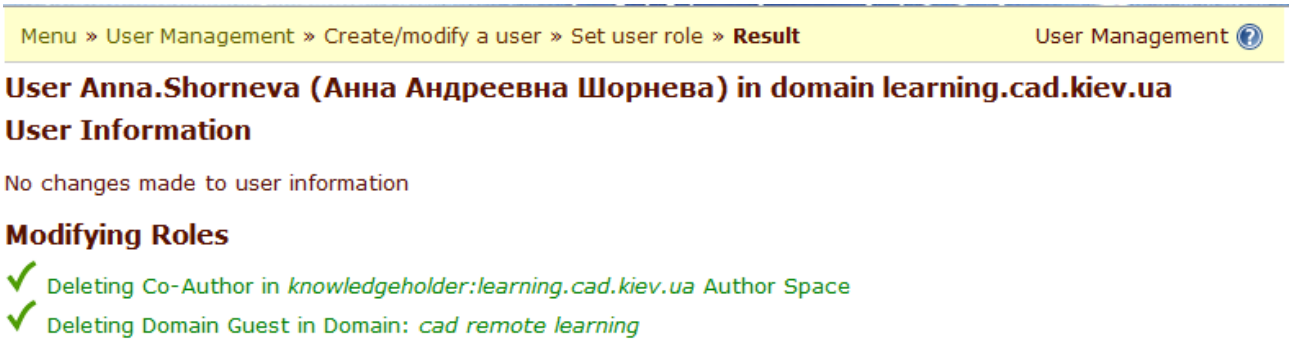

Рисунок 17 – Видалення ролей користувача

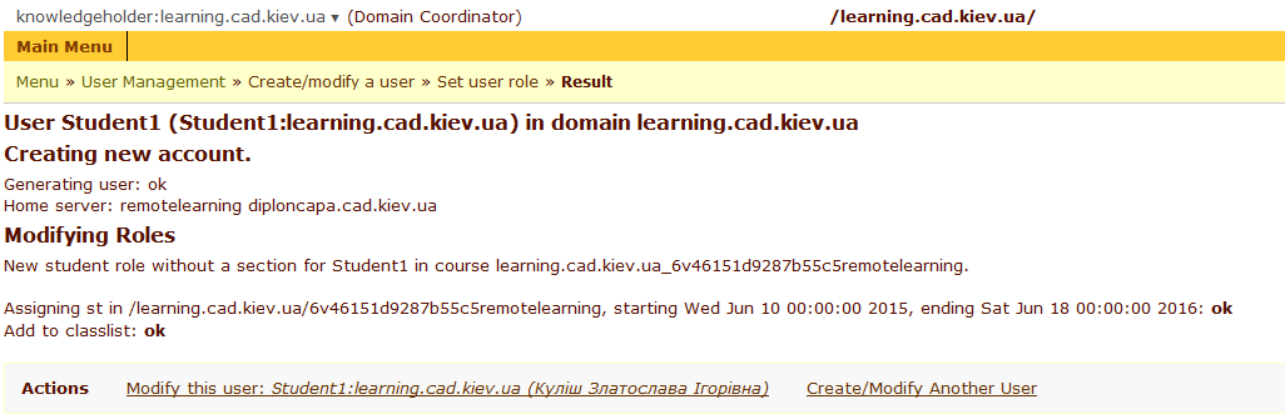

Рисунок 18 – Успішне створення студента, з зазначенням терміну дії його облікового запису

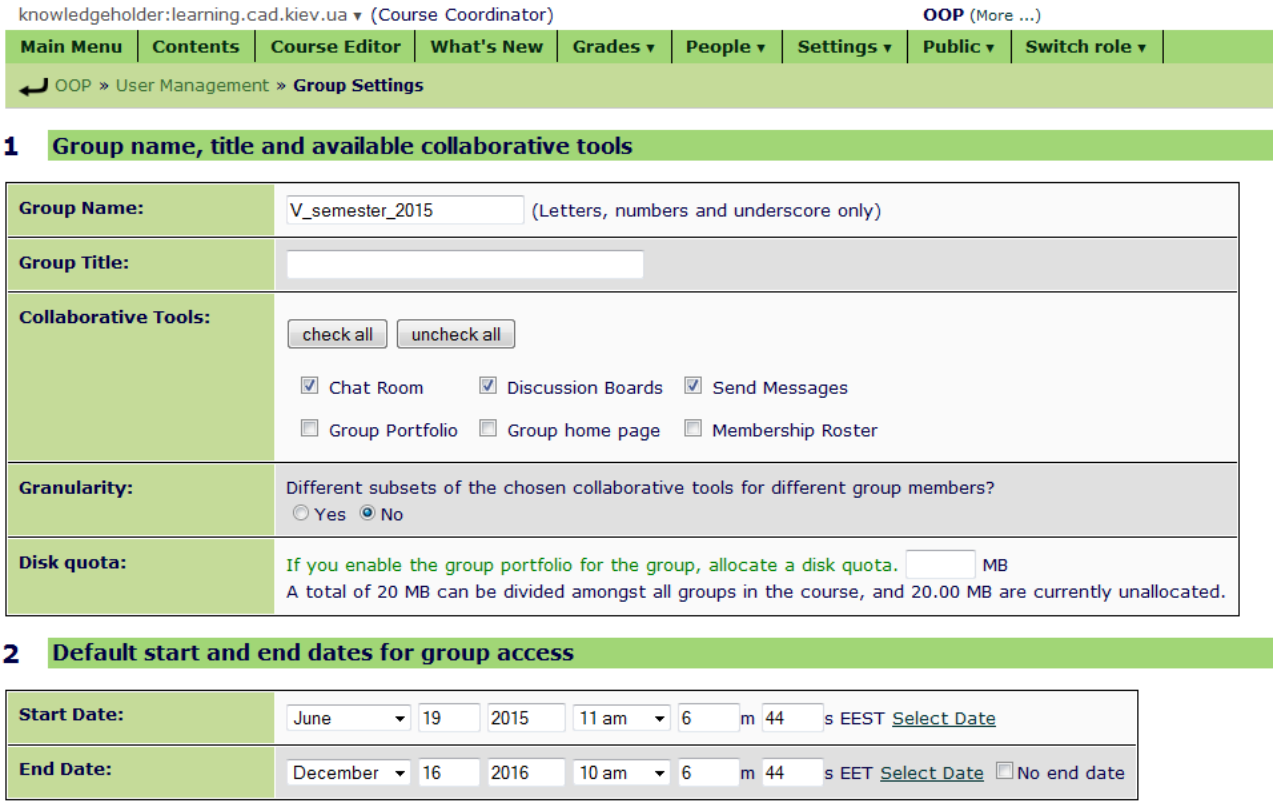

Рисунок 19 – Створення групи та визначення спільних засобів роботи, зокрема назначити термін дії для доступу до групи

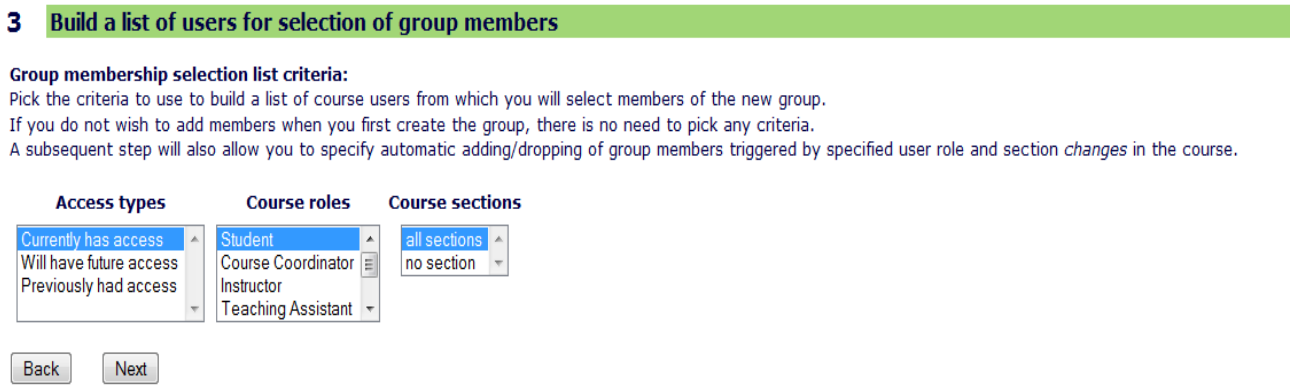

Рисунок 20 – Назначення користувачам доступу та ролей у курсі

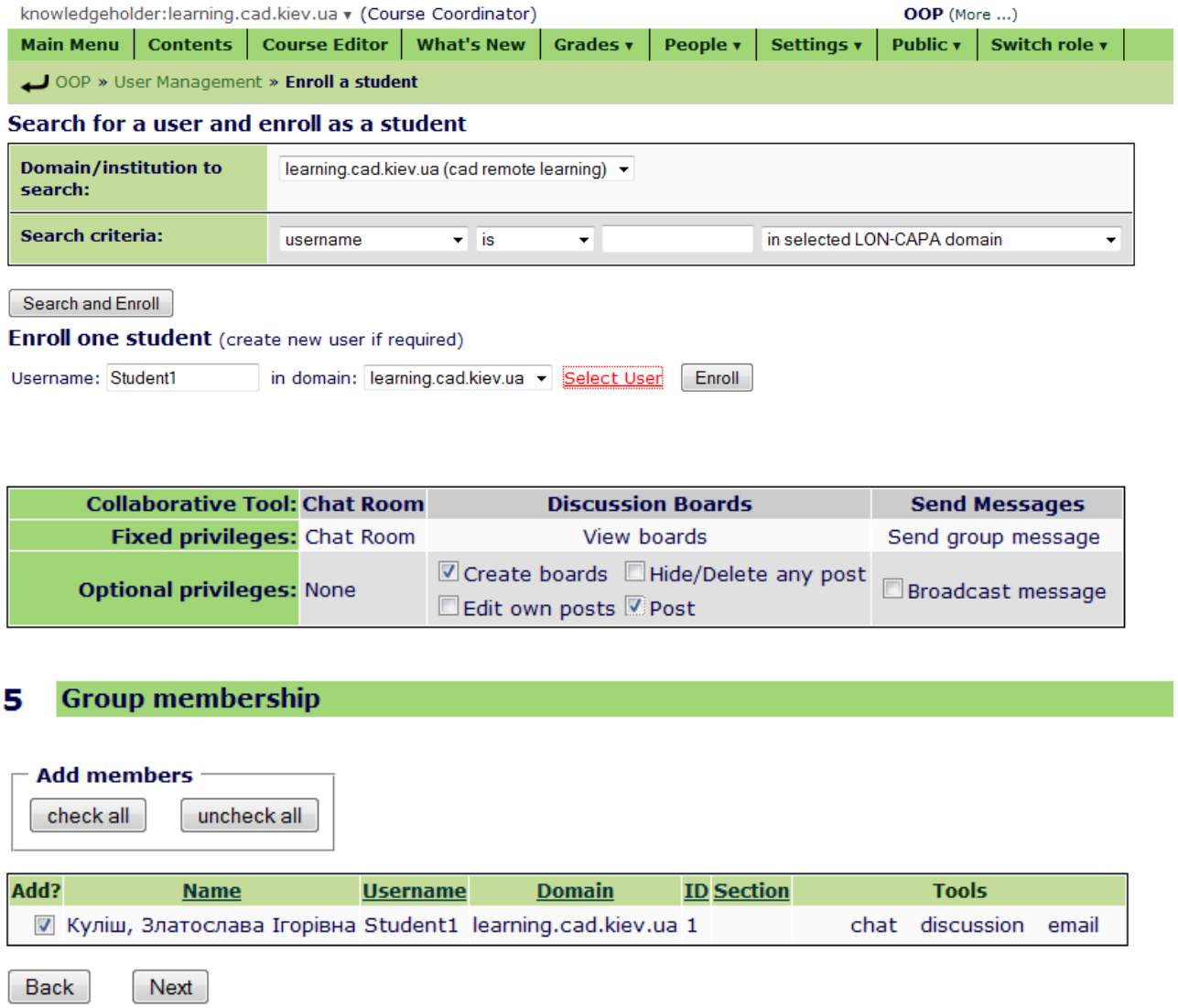

Рисунок 21 – Реєстрація користувача в групі

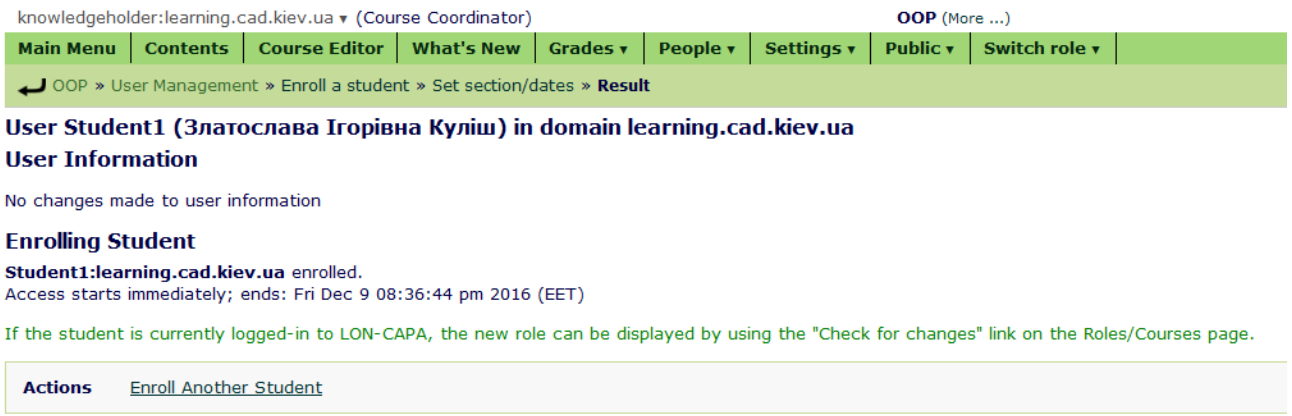

Рисунок 22 – Збереження всіх налаштувань користувача та добавлення його до курсу

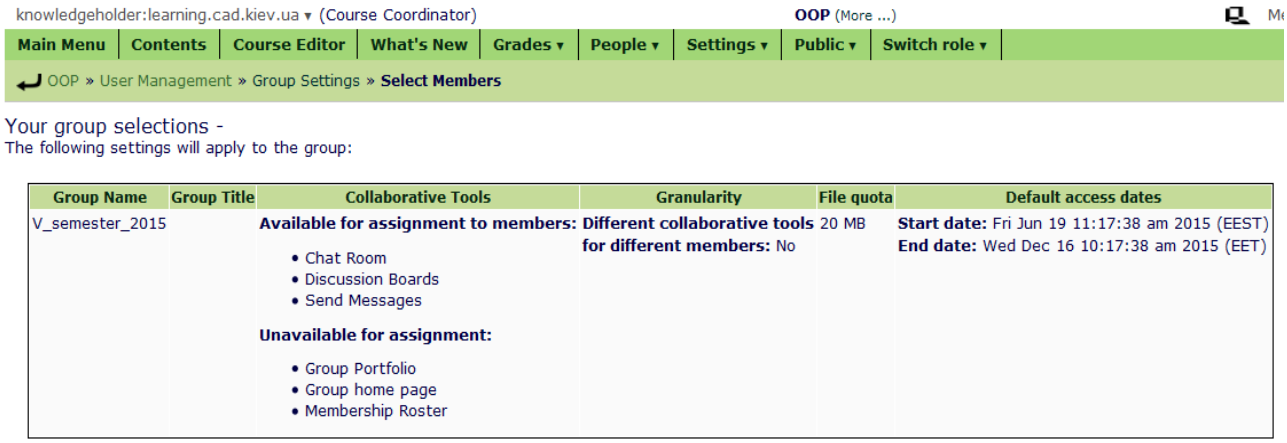

Рисунок 23 - Додавання усіх налаштувань групи

3.4 Висновки

У даному розділі були розглянуті методи забезпечення захисту для систем дистанційного навчання. Провівши детальний їх аналіз, для реалізації в системі LON-CAPA були вибрані методи управління доступом та регламентації.

Ці методи доповнюють інформаційну безпеку системи LON-CAPA, а саме її протоколів захисту – LDAP та Kerberos. Вони були обрані, тому що є одними з найбільш дієвих та гнучких для налаштування у СДН. Адже вони напряму взаємодіють з користувачами, визначаючи їхні ролі та права у системі та доступ до інформаційних ресурсів. Такі методи дають змогу забезпечити конфіденційність даних користувачів системи та розміщених матеріалів.

Оскільки, однією з особливостей системи LON-CAPA є можливість повторного використання розроблених навчальних ресурсів в інших курсах, ці методи дуже важливі, зокрема для координаторів та викладачів навчальних курсів, які можуть надати доступ до їхніх матеріалів іншим викладачам, і заборонити – для гістьових облікових записів.

Гнучкість методів забезпечується можливістю створення, реструктуризації та зміни курсів та навчальних матеріалів, а також створення нових ролей для користувачів, щоб забезпечити мінімізацію повноважень.

Отже, застосування додаткових методів захисту є необхідною умовою для покращення функціонування системи LON-CAPA, її захищеності від викрадання інформаційних ресурсів та для забезпечення доступу до її курсів тільки користувачів, які мають такі права.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Вступ

Метою охорони праці є науковий аналіз умов праці, технологічних процесів, апаратури та обладнання з точки зору можливості виникнення появи небезпечних факторів, виділення шкідливих виробничих речовин. На основі такого аналізу визначаються небезпечні ділянки виробництва, можливі аварійні ситуації та розробляються заходи щодо їх усунення або обмеження наслідків.

На всіх підприємствах мусять бути створені здорові і безпечні умови праці, встановлені правові засади регулювання відносин у галузі охорони праці між роботодавцями і працівниками, а також створені умови праці, що відповідають вимогам збереження життя і здоров'я працівників у процесі трудової діяльності (згідно закону України « Про охорону праці»).

Власник підприємства (або уповноважений орган) повинен забезпечувати працівників сучасними засобами техніки безпеки, які запобігають виробничому травматизмові, і організувати санітарно-гігієнічні умови, що попереджають виникнення професійних захворювань. Він не має права вимагати виконання роботи, що пов’язана з явною небезпекою для життя, а також при умовах, які не відповідають законодавству про охорону праці. Працівник має право відмовитися від дорученої роботи, якщо створилася виробнича ситуація, небезпечна для його життя чи здоров'я чи для людей, які його оточують, і навколишнього середовища.

4.2 Аналіз умов праці

Завданням даної дипломної роботи було дослідження бази даних LON-CAPA та налаштування її таким чином, щоб забезпечити максимальну безпеку

та цілісність інформації. В подальшому з її допомогою можна буде спростити та вдосконалити доступ студентів до навчальних матеріалів.

Робота з базою даних проходитиме в приміщенні відповідної установи(університет, технікум тощо). Стабільність та наповненість даної бази даних мають забезпечувати дві людини, для яких надано робоче місце з стаціонарним комп'ютером.

4.3 Опис приміщення

Згідно правил охорони праці робоче місце користувача ПЕОМ повинне займати площу не менш 6 м², висота приміщення повинна бути не менш 3 м, а об'єм - не менш 20 $м^3$ на одну людину[19]. Висота робочої поверхні, повинна бути 700 мм, а оптимальні розміри 1900 х 900 кв. мм. Відстань між очима користувача й екраном повинна складати 400 – 800 мм. Робочий стілець користувача ПЕОМ повинен бути оснащений підйомно-поворотним механізмом.

Для дотримання вимог пожежної безпеки встановлено систему автоматичної пожежної сигналізації та вогнегасник. А також, для забезпечення потрібного рівня мікроклімату у приміщенні, встановлено кондиціонер та систему опалення. Для забезпечення потрібного рівного освітленості кімната має два вікна та систему загального рівномірного освітлення, що встановлена на стелі. Схема робочого приміщення зображена на рис. 4.1

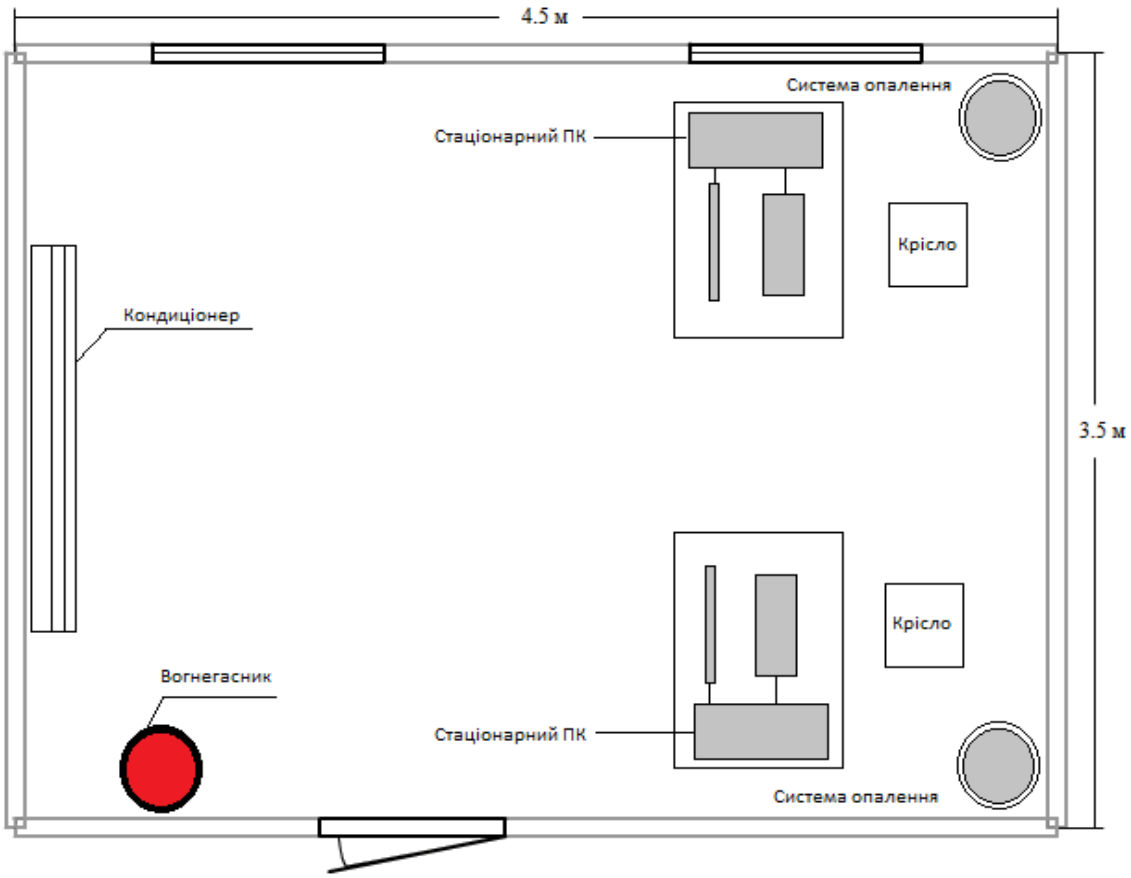

Рисунок 24 – Схема робочого приміщення

4.4 Аналіз шкідливих та небезпечних чинників

При використанні обчислювальної техніки слід дотримуватись правил безпеки та користування, оскільки при неправильному застосуванні вона має шкідливі та небезпечні чинники, а також може негативно впливати на здоров’я людини.

Небезпечні чинники – це чинники, у результаті яких людина може втратити працездатність або навіть втратити своє життя.

Шкідливі чинники можуть призвести до погіршення стану здоров’я людини, а в результаті довгого впливу до виникнення професійних захворювань.

До таких чинників відносяться:

- підвищений рівень шуму, вібрації, ультра- та інфразвука;
- недостатня освітленість робочої зони;
- підвищена чи знижена температура, вологість і рухомість повітря та інші;

4.4.1 Шум та вібрація

Приміщення, що розглядається, не межує з жодним іншим приміщенням, де рівні шумів та вібрацій перевищують норму.

Рівні звукового тиску в октавних смугах частот приміщення, рівні звуку та еквівалентні рівням звуку на робочих місцях, мають відповідати санітарним нормам виробничого шуму, ультразвуку та інфразвуку[20].

Обладнання, що є джерелом шуму (АЦП, принтери тощо), слід розташовувати у приміщеннях, де відсутні робочі місця.

Щоб забезпечити допустимий рівень шуму на робочих місцях, вибір засобів звукопоглинання має обґрунтовуватись спеціальними інженерно-акустичними розрахунками.

Значення характеристик вібрації на робочих місцях мають не перевищувати допустимих (відповідно до санітарних норм)[20].

У приміщеннях з ЕОМ коректований рівень звукової потужності не перевищує допустимої норми і становить 45 дБА.

4.4.2 Освітленість

Приміщення, в яких встановлені персональні комп’ютери, повинні мати природне та штучне освітлення відповідно до Національних стандартів України[21].

Природне освітлення має здійснюватись через світлові прорізи, орієнтовані переважно на північ чи північний схід і забезпечувати коефіцієнт природною освітленості (КПО) не нижче ніж 1,5%.

Штучне освітлення в приміщеннях з робочими місцями має здійснюватись системою загального рівномірного освітлення. У разі переважної роботи з документами, допускається застосування системи комбінованого

освітлення (крім системи загального освітлення додатково встановлюються світильники місцевого освітлення). Зазначення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300-500лк. Якщо ці значення освітленості неможливо забезпечити системою загального освітлення, допускається використовувати місцеве освітлення. При цьому світильники місцевого освітлення слід встановлювати таким чином, щоб не створювати відблисків на поверхні екрана, а освітленість екрана не має перевищувати 300 лк. Як джерела світла в разі штучного освітлення мають застосовуватись переважно люмінесцентні лампи типу ЛБ.

Допускається застосування ламп розжарювання у світильниках місцевого освітлення. Система загального освітлення має становити суцільні або переривчасті лінії світильників, розташовані збоку від робочих місць (переважно ліворуч), паралельно лінії зору працюючих[22].

Отже, в даному приміщенні передбачається використання комбінованого природного (верхнє освітлення поєднується з боковим), та комбінованого штучного (загальне і місцеве освітлення робочих місць світильниками) і суміщеного освітлення. У світильниках місцевого освітлення використовуються люмінесцентні лампи.

Заміну перегорілих ламп потрібно виконувати по мірі виходу їх із ладу, а також проводити чистку шибок і світильників не менше двох разів на рік.

4.4.3 Мікроклімат

Робота, яка виконується в офісі, відповідає до категорії - легка 1а, оскільки вона виконується сидячи і не вимагає фізичного навантаження. Мікроклімат в приміщенні відповідає наступним показникам: [23]

- для холодної пори року:

– температура: 22 – 24°С ;

– відносна вологість: 40 – 60%;

– швидкість руху повітря: 0,1м/с.

- для теплої пори року:

– температура: 23 – 25°С ;

– відносна вологість: 40 – 60%;

– швидкість руху повітря: 0,1м/с.

Для забезпечення оптимальних показників мікроклімату потрібно проводити планове провітрювання приміщення, а в літній період необхідно вмикати кондиціонер. Також бажаним є використання приладів зволоження повітря.

4.4.4 Пожежна безпека

У приміщенні знаходяться тверді горючі та важкозаймисті речовини та матеріали, отже дане приміщення відноситься до категорії В. Це обумовлено тим, що простір, у якому розташовані ЕОМ, повинні мати не нижче II ступеня вогнестійкості. Для гасіння пожеж в офісних приміщеннях слід використовувати порошкові вогнегасники, так як вони є універсальними для більшості типів пожеж. Всі заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), мають бути надійно захищені діелектричними щитками або сітками з метою недопущення потрапляння працівника під напругу [22].

Основними причинами займання в будівлі можуть бути:

– перевантаження обладнання,

– великі перехідні опори,

– зіпсованість електроустаткування,

– коротке замикання,

– порушення протипожежного режиму.

Щоб запобігти займанню або вчасно його зупинити, приміщення має бути оснащено системою автоматичної пожежної сигналізації, мати 1 вогнегасник ВП-5 із зарядом вогнегасної речовини 8-12 кг, відповідно до вимог чинного законодавства України. Проходи до засобів пожежогасіння мають бути вільними.

У будівлі шляхи евакуації мусять відповідати нормативним вимогам [24], а саме: коридори поверхів за довжиною поділені протипожежними перегородками; висота шляхів евакуації становить 3м, а ширина 1,5м. Крім того, на кожному поверсі будівлі та в кожному її кабінеті має бути план-схема евакуації на випадок пожежі.

4.5 Рекомендації щодо поліпшення умов праці

Внаслідок проведеного аналізу санітарно-гігієнічних умов праці, умов електробезпеки і пожежної безпеки приміщення, де виконуються роботи з використанням ЕОМ, було зроблено висновок про відповідність переважної більшості чинників нормативним вимогам.

Таким чином, було виявлено, що:

- умови роботи з відеотермінальними пристроями відповідають нормам;
- потрібно приділити особливу увагу організації відпочинку та перервам працюючого персоналу;
- об’єм приміщення, з розрахунку на одну людину відповідає нормативному значенню;
- фактичні показники мікроклімату цілком відповідають допустимим значенням;
- параметри природного освітлення відповідають нормі;
- рівень електробезпеки та пожежної безпеки знаходиться у відповідності нормативним вимогам.

Загалом умови праці в приміщенні, що розглядалося, є задовільними. Хоча в результаті проведеного аналізу виробничого приміщення були виявлені

деякі невідповідності умов праці нормативним (зокрема забезпечення відпочинку персоналу).

У зв’язку зі специфікою робот з ЕОМ також можна рекомендувати виконання комплексів вправ для фізичного і психічного розвантаження, які наведено у [25].

При вводі даних, редагуванні програм, читанні інформації з екрану безперервна тривалість роботи з відеотерміналом не повинна перевищувати 4-х годин (при 8-годинному робочому дні). Для зниження напруженості праці необхідно, якщо це можливо, рівномірно розподіляти навантаження і раціонально чергувати характер діяльності.

Щогодини треба робити перерву на 15 хвилин. Один або кілька разів у годину необхідно виконувати серію легких вправ на розтягування та розслаблення, що можуть зменшити напругу, що накопичується в м'язах при тривалій сидячій роботі за комп'ютером.

З метою профілактики й усунення перевтоми і перенапруги бажано після закінчення робочого дня і під час великих перерв проводити сеанси психофізіологічного розвантаження і зняття утоми.

З інших рекомендацій щодо поліпшення умов праці відповідно до [25] можна навести наступні:

- у приміщенні слід щоденно проводити вологе прибирання та провітрювання;
- у приміщенні повинні бути медичні аптечки першої допомоги.

Висновки до розділу 4

В результаті роботи був проведений детальний аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник.

Були визначені основні положення, які задовольняють норми та стандарти охорони праці, а саме: яким повинне бути приміщення для функціонування програмного продукту дипломної роботи, описані заходи, які є необхідними для того, щоб дане приміщення відповідало встановленим правилам і було комфортним для працівника.

Була наведена схема, розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри значення яких впливає на умови праці робітника, а також – наведені рекомендації щодо поліпшення цих умов.

ВИСНОВКИ

На сьогоднішній день одним з головних завдань при використанні СДН є забезпечення інформаційної захищеності адміністратором, який повинен цю систему впровадити для використання та надалі, забезпечувати повне її обслуговування та підтримку.

Однак, при адмініструванні віртуального навчального середовища постає проблема вибору платформи, на якій буде побудована СДН. Цей вибір залежить від цілого ряду чинників: які вимоги пред'являються до середовища, які функціональні характеристики повинні бути присутніми, на яких користувачів орієнтована середовище та які налаштування в ній можна виконувати.

Комерційні системи дистанційного навчання у більшості випадків більш надійні, але вони майже не піддаються модифікаціям та змінам, які часто вносять адміністратори.

Безперечні переваги використання СДН на OpenSource, тому що такі системи є найбільш логічним вибором для освітніх проектів, оскільки основна його ідея полягає в співпраці, і сама ідеологія дозволяє об'єднати таланти і досвід великої кількості користувачів у розвитку та вдосконаленні освітніх програмних продуктів. Більш того, таке навчальне програмне забезпечення може функціонувати як інструмент, орієнтований на учня, як основа для гнучкого та придатного для змін адміністратором навчання, адаптованого для будь-якої навчальної програми.

Отже**,** в умовах сучасного світу надійна безпека інформаційних ресурсів СДН може бути забезпечена тільки певним рядом заходів, таких як

- Обміркований вибір програмного та апаратного забезпечення,
- Ефективне адмініструванням таких систем,
- Комплексний підхід до захисту інформації.

В свою чергу, комплексна система захисту інформації повинна бути:

- Безперервною (постійний контроль за можливими порушеннями)
- Плановою (перевірка системи за заздалегідь визначеним планом)
- Цілеспрямованою (забезпечувати тільки ті заходи безпеки, які дійсно необхідні користувачам)
- конкретною (застосовувати перевірені методи та засоби забезпечення інформаційної безпеки)
- активною (щоб як найменше чинників могли вивести її з ладу)
- надійною (така система не повинна викликати підозр, щодо її надійності)

У сучасному світі існує вже багато рішень для організації дистанційного навчання, а ще більше систем, які керують ним, як от, наприклад, CMS, LMS, LCMS.

Першочергове завдання організації, яка хоче впровадити СДН, визначити, які функції ця система має виконувати та для чого слугувати.

Останнім часом все більшої популярності та поширення набувають LCMS системи, хоча вони досить нові, але такий інтерес до них цілком виправданий, адже в них вдало поєднано багато функцій та на їх основі реалізовано багато СДН, зокрема і система LON-CAPA.

У дипломній роботі було проаналізовано існуючі методи та засоби захисту інформації, серед них аргументовано вибрано тільки два методи – управління доступом до інформації та регламентації доступу. Дані методи були впровадженні в систему LON-CAPA для підвищення її інформаційної захищеності.

Надалі, ці методи можна використовувати для налаштування інших систем дистанційного навчання, використовуючи досвід впровадження їх у системі LON-CAPA.

ЛІТЕРАТУРА:

1. Семененко В.А. Информационная безопасность: учебное пособие. 2-е изд., стереот. - М.: МГИУ, 2005. - 215 с.

2. Корнюшин, П.Н. Информационная безопасность / П.Н. Корнюшин, С.С. Костерин. – Владивосток: ТИДОТ ДВГУ, 2003. – 154 с.

3. Конев И. Р. Информационная безопасность предприятия / И. Р. Конев, А. В. Беляев. – СПб. : БХВ-Петербург, 2003. – 747 с.

4. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1/ С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

5. Теория информационной безопасности и методология защиты информации: учебное пособие. / И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина - Казань: Изд-во Казан. гос. техн. ун-та, 2008. – с. 358.

6. Сороковская А. А. Информационная безопасность предприятия : новые угрозы и перспективы [Электронный ресурс]. – Режим доступа : http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf. — Дата доступу : 08.06.2015

7. Курушин В. Д. Компьютерные преступления и информационная безопасность / В. Д. Курушин, В. А. Минаев. – М. : Новый юрист, 2012.– 256 с.

8. Гатчин Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат. – СПб. : СПбГУ ИТМО, 2010. – 98 с.

9. Вишнівський В.В. Організація дистанційного навчання.Створення електронних навчальних курсів та електронних тестів.Навчальний посібник./ Вишнівський В.В., Гніденко М.П.,Гайдур Г.І., Ільїн О.О. – Київ: ДУТ, 2014. – 140с

10. Гайворонський М.В. Безпека інформаційно-комунікаційних систем./ Гайворонський М.В., Новіков О.М. – К.: Видавнича група BHV, 2009. – 608 с.

11. Дронь М.М., Малайчук В.П., Петренко О.М. Основи теорії захисту інформації: Навч. посібник. – Д.: Вид-во Дніпропетр. ун-ту, 2001. – 312 с.

12. Гильмутдинов А.Х. Электронное образование на платформе Moodle/ Гильмутдинов А.Х., Ибрагимов Р.А., Цивильский И.В. – Казань: КГУ, 2008. – с.169

13. Программное обеспечение для дистанционного обучения – Режим доступу: http://tutorsupport.narod.ru/index/0-13 – Дата доступу : 01.06.2015

14. Офіційний сайт системи LON-CAPA. – Режим доступу: http://www.lon-capa.org/institutions.html – Дата доступу : 05.06.2015

15. Офіційний сайт системи LON-CAPA. – Режим доступу: http://www.lon-capa.org/students.html– Дата доступу : 05.06.2015

16. Офіційний сайт системи LON-CAPA. – Режим доступу: http://www.lon-capa.org/scalability.html– Дата доступу : 05.06.2015

17. Офіційний сайт системи LON-CAPA. – Режим доступу: http://www.lon-capa.org/sharing.html– Дата доступу : 05.06.2015

18. Офіційний сайт системи LON-CAPA. – Режим доступу: http://bezopasnik.org/article/1.htm– Дата доступу :

19. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. Пособие для студ. Высш.учеб. заведений – М.: Издательский центр “Академия”, 2005. – 8с.

20. Правила охорони праці під час експлуатації електронно-обчислювальних машин : НПАОП 0.00.-1.31-10. – [Чинний від 2010-03-26]. – К. : Держнагляд охорон праці України, 2010. – 7 с. – (Національні стандарти України).

21. Санітарні норми виробничого шуму, ультразвуку та інфразвуку : ДСН 3.3.6.037-99. – [Чинний від 2000-01-01]. – К. : МОЗ України, 2000. – 37 с. – (Національні стандарти України).

22. Природнє і штучне освітлення : ДБН В.2.5-28:2015 – [Чинний від 2015-01-01]. – К. : Міністерство будівництва, архітектури та житлово-комунального господарства України, 2015. – 171 с. – (Національні стандарти України).

23. Охорона праці в офісі. Вимоги до робочого місця офісного працівника – [Електронний ресурс] . - Режим доступу: http://gc.ua/business-news/oxorona-praci-v-ofisi-vimogi-do-robochogo-miscya-ofisnogo-pracivnika/

24. Санітарні норми мікроклімату виробничих приміщень : ДСН 3.3.6.042-99. – [Чинний від 2000-01-01]. – К. : МОЗ України, 2000. – 42 с. – (Національні стандарти України).

25. Типові норми належності вогнегасників (затверджено наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 2 квітня 2004 р. N 151).

26. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПіН 3.3.2.007-98 (затверджено Постановою Головного державного санітарного лікаря України від 10.12.1998 р. № 7).