ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ЗАСОБІВ НАВЧАННЯ НАПН УКРАЇНИ

Аналітична записка

ПРОЕКТИ НОРМАТИВНИХ ДОКУМЕНТІВ ПРОЦЕСУ СЕРТИФІКАЦІЇ ЕЛЕКТРОННИХ ЗАСОБІВ НАВЧАЛЬНОГО ПРИЗНАЧЕННЯ

Автори: Дем'яненко В.М., Запорожченко Ю.Г., Лаврентьєва Г.П., Лапінський В.В., Морзе Н.В., Шишкіна М.П.

2014

Рекомендовано до друку Вченої радою Інституту інформаційних технологій і засобів навчання НАПН України (протокол № 6 від 26 червня 2014 року)

Авторський колектив:
Дем'яненко В. М. (розділ I, V), Запорожченко Ю. Г. (розділ I), Лапінський В. В. (розділ I), Лаврентьєва Г.П. (розділ I, III, IV), Морзе Н.В. (розділ VI), Шишкіна М. П. (розділ I, II, III)

Проекти нормативних документів процесу сертифікації електронних засобів навчального призначення : аналітична записка / [Дем'яненко В. М. , Запорожченко Ю. Г. , Лапінський В. В., Лаврентьєва Г.П., Морзе Н.В., Шишкіна М. П.]; – К. : ІІТЗН, 2014. – 160 с., іл.

До аналітичної записки вміщено проекти нормативних документів процессу сертифікації і оцінювання якості електронних ресурсів навчального призначення, розроблені у межах виконання науково-дослідної роботи «Система психолого-педагогічних вимог до засобів інформаційно-комунікаційних технологій навчального призначення», ДР№0112U000281.

УДК 373.3/.5.091.64:(0.034.2)].015.3.02

ЗМІСТ.

І. ПРОЕКТ ПОЛОЖЕННЯ
ПРО ЕЛЕКТРОННІ ОСВІТНІ РЕСУРСИ

(Лист № 29_від 27.09.2012 р.)

1. Загальні положення

1.1. Положення про електронні освітні ресурси (далі – Положення) розроблене згідно Національного плану дій на 2012 рік (пунктів 5.1.1. – 5.1.3. Плану-графіка реформ на 2012 рік) щодо впровадження Програми економічних реформ на 2010 - 2014 роки "Заможне суспільство, конкурентоспроможна економіка, ефективна держава", затвердженого Указом Президента України від 12 березня 2012 року № 187/2012, Державної цільової програми впровадження у навчально-виховний процес загальноосвітніх навчальних закладів інформаційно-комунікаційних технологій "Сто відсотків" на період до 2015 року, затвердженої постановою Кабінету Міністрів України від 13 квітня 2011 р. № 494, і визначає поняття електронних освітніх ресурсів (далі - ЕОР), їх види, принципи класифікації, порядок розроблення, експертизи і розповсюдження.

1.2. Положення ґрунтується на положеннях і нормах Законів України «Про освіту», «Про вищу освіту», «Про професійно-технічну освіту», «Про загальну середню освіту», «Про позашкільну освіту», «Про видавничу справу», «Про наукову і науково-технічну експертизу», «Про авторське право і суміжні права», Державних стандартів України: ДСТУ 3017-95 «Видання. Основні види. Терміни та визначення»; ДСТУ 7157:2010 «Видання електронні. Основні види та вихідні відомості»; ДСТУ ISO/IEC 12119:2003 Інформаційні технології. Пакети програм. Тестування і вимоги до якості; ДСТУ ISO/IEC 2382-5:2005 Інформаційні технології. Словник термінів; ДСТУ IEEE Std 1484.12.1:2006 Інформаційні технології. Метадані навчальних об`єктів; чинних державних і освітніх стандартів з урахуванням вимог Державних санітарних правил і норм, інших нормативно-правових актів, що регламентують діяльність МОНмолодьспорту щодо науково-методичного і матеріально-технічного забезпечення системи освіти.

1.3. ЕОР, а також їх певні сукупності за допомогою комп'ютерних засобів використовуються для реалізації основних функцій системи освіти (навчальної,

наукової, управлінської); для інформаційно-процесуального забезпечення виконання різних завдань (або їх фрагментів): дидактичних завдань, завдань з ІКТ-підтримки наукових досліджень й розробок та управління системою освіти на всіх її організаційних рівнях.

1.4. Розроблення Положення сприятиме уточненню місця ЕОР у складі освітнього середовища, ролі, яка відводиться цим інформаційним ресурсам у його структурі. Це розвиває методологію створення ЕОР, їх індустріального виробництва та ефективного використання в освітній практиці.

2. Основні терміни та поняття

Електронні освітні ресурси – це вид засобів освітньої діяльності (навчання та ін.), які існують в електронній формі, розміщуються і подаються в освітніх системах на запам'ятовуючих пристроях електронних даних, є сукупністю електронних інформаційних об'єктів (документів, документованих відомостей та інструкцій, інформаційних матеріалів, процесуальних моделей та ін.)

ЕОР: *відображують* змістовно-технологічні компоненти освітніх методичних систем, *формують* предметно-інформаційні складові освітнього середовища (закритого і відкритого), *утворюють* наповнення освітніх електронних інформаційних систем, *призначені* для різнобічного цілеспрямованого використання учасниками освітнього процесу з метою інформаційно-процесуальної підтримки навчальної, наукової та управлінської діяльності, інформаційного забезпечення функціонування та розвитку освітніх систем.

Електронні ресурси навчального призначення (ЕРНП) – сукупність ЕОР, що застосовуються для інформаційно-процесуального забезпечення виконання дидактичних завдань (або їх фрагментів), спрямовані на реалізацію навчальної функції системи освіти.

Електронні ресурси управлінського призначення (ЕРУП) – сукупність ЕОР, що застосовуються для інформаційно-процесуального забезпечення

виконання завдань управління системою освіти (або їх фрагментів), спрямовані на реалізацію управлінської функції системи освіти.

Електронні ресурси для підтримки наукових досліджень (ЕРНД) – сукупність ЕОР, що застосовуються для інформаційно-процесуального забезпечення виконання завдань ІКТ-підтримки наукових досліджень та розробок, спрямовані на реалізацію наукової та проектувальної функції системи освіти.

Дані та їх сукупності (окремі дані та / або бази даних) – певним чином структурована, упорядкована і закодована сукупність статичних і динамічних інформаційних об'єктів, що містять аудіо- та відео- або символьні відомості чи їх комбінації (числа, тексти, таблиці, цифрові моделі, графіка, звук, фото, відео та ін.), які можуть бути застосовані для вирішення комп'ютерно орієнтованих завдань (задач) різного освітнього призначення.

Комп'ютерна програма – поданий мовою програмування закодований опис задачі (задач), що підлягає вирішенню за допомогою комп'ютера. Цей опис є інструкцією, де вказується, у якій послідовності (за яким алгоритмом), над якими даними, які операції необхідно виконати й у якій формі видати результат. Тобто, комп'ютерна програма містить опис:

• вбудованих даних (значень елементів даних, відомостей про їх склад і структуру) та їх сукупностей (баз даних), у тому числі всіх або деяких параметрів задачі (задач), а також спеціальних додаткових даних, які підлягають введенню, телекомунікаційному отриманню і / або передаванню, опрацюванню, зберіганню, відображенню;

• способів розв'язування задачі (задач деякого класу);

• адрес мережних ЕОР (даних та інших комп'ютерних програм);

• типу пристрою, з якого можуть вводитися (отримуватися) і на який має видаватися (передаватися) результат розв'язування задачі (задач, виконання програм).

Електронний документ – ідентифікований елемент контенту електронних інформаційних систем.

Освітній контент – структурований предметний зміст, що

використовується в освітньому процесі

Електронне видання – електронний документ, що пройшов редакційно-видавниче опрацювання і призначений для розповсюдження у незмінному вигляді за допомогою носіїв електронних даних та інформаційно-комунікаційних мереж.

Електронний аналог друкованого видання – електронне видання, що за змістом і формою подання в основному відтворює відповідне друковане видання (із збереженням розташування на сторінці тексту, ілюстрацій, посилань, приміток і т.ін.).

Електронні дидактичні демонстраційні матеріали – електронні дані, що призначені для демонстрації (наочного подання, візуалізації, візуально-звукового подання) окремих явищ, об’єктів, процесів, що вивчаються, з метою поглиблення їх розуміння за рахунок надання можливості їх спостереження учневі.

Інформаційна система – система, яка забезпечує ідентифікацію, зчитування, подання і зберігання, оброблення, передавання і доступ користувачів до даних в електронно-цифровій формі.

Депозитарій електронних ресурсів – комплексна інформаційна система, що забезпечує реєстрацію, зберігання, поновлення, індексацію, пошук і доступ до електронних інформаційних ресурсів та (або) їх описів за допомогою телекомунікаційних мереж та інформаційних технологій.

Комп'ютерний тест – набір стандартизованих завдань, представлених в електронній формі, що призначені для оцінювання рівня навчальних досягнень учнів (рівня оволодіння навчальним матеріалом) .

Електронний довідник – електронне навчальне видання, призначене для надання, отримання коротких наукових і прикладних відомостей довідкового характеру, може використовуватись для розвитку навичок пошуку та систематизації навчальних відомостей.

Електронний навчальний посібник – навчальне електронне видання, що доповнює або частково (повністю) замінює підручник. Посібник може охоплювати не всю дисципліну, а лише один або декілька розділів навчальної

програми. Однак матеріал має бути поданий у руслі фундаментальних знань, поданих у підручнику.

Електронний підручник – це електронне навчальне офіційно затверджене видання з систематизованим викладом дисципліни (її розділу, частини), що відповідає навчальній програмі з даної дисципліни. Призначене для формування знань, умінь і навичок навчальної і практичної діяльності, забезпечення необхідного рівня засвоєння навчального матеріалу.

Електронні навчально-методичні матеріали – матеріали по методиці навчання певної дисципліни (її розділу, частини) або виховання, що містять методичні рекомендації, вказівки до певної теми, розділу або питання, до виконання окремих завдань, практичних робіт.

Електронні програмно-методичні матеріали – матеріали, що визначають зміст, обсяг, порядок навчання певної дисципліни, її розділу, теми (навчальні програми, плани; плани занять).

Додаткові науково-навчальні матеріали – матеріали, що сприяють доповненню і розширенню уявлень про об’єкти і процеси, що є предметом вивчення (хрестоматії, статті, монографії, книги і т.ін.).

Курс дистанційного навчання – комплекс навчально-методичних матеріалів та освітніх послуг, створених в електронному освітньому середовищі, для організації переважно індивідуалізованої взаємодії учасників і організаторів навчального процесу на відстані (екстириторіально) із переважним і принциповим використанням інформаційних і комунікаційних технологій та засобів інформаційно-комунікаційних мереж для постачання навчальних матеріалів та інших інформаційних об’єктів.

Електронний практикум – комп’ютерна програма (або програмне середовище) призначена для формування і закріплення умінь, практичних навичок, використання теоретичних знань для вирішення практичних завдань і вправ).

Комп’ютерно-орієнтована навчальна лабораторія – комп’ютерна програма (або програмне середовище), що може застосовуватись при проведенні лабораторних і практичних занять, для здійснення експериментальних

досліджень безпосередньо з фізичними об'єктами і (або) математичними, інформаційно-описовими, імітаційними наочними моделями, представленими на екрані ЕОМ.

Імітаційно моделюючі програми (видання) навчального призначення – призначені для дослідження та вивчення окремих аспектів (явищ) реальності, поданих засобами комп'ютерного моделювання, за допомогою яких учень отримує можливість зміни (керування) окремими структурними і функціональними характеристиками моделі.

Моделюючі програми (видання) навчального призначення – призначені для моделювання об'єктів, явищ і процесів, що є предметом вивчення, або надання засобів для побудови і дослідження моделей.

Програми-тренажери – комп'ютерні програми, що призначені для формування і закріплення умінь та практичних навичок, опанування методів, процедур виконання певних видів навчальної або професійної діяльності, а також для здійснення самопідготовки.

Предметний пакет прикладних програм (ППП) - комплекс взаємопов'язаних прикладних програм для розв'язання задач певного класу із предметної галузі, що вивчається, призначений для автоматизації різноманітних розрахунків або інших операцій, що виникають у цій галузі.

Електронний навчально-методичний комплекс (ЕНМК) – структурована сукупність ЕОР, що містять взаємопов'язаний освітній контент і призначені для спільного використання в освітньому процесі. Типова структура ЕНМК охоплює: електронні навчально-методичні матеріали; теоретичний матеріал (електронний курс лекцій або електронний підручник); електронний практикум; навчальні пакети прикладних програм; програмні засоби контролю знань; додаткові навчально-довідкові матеріали.

Програмні засоби оцінювання знань – засоби ІКТ, які дають можливість автоматизації процесів визначення рівня навчальних досягнень учня, призначені для підтримування процесів оцінювання та само оцінювання у навчанні.

3. Класифікація ЕОР

3.1. З*а галуззю призначення* (спрямованості використання) ЕОР діляться

відповідно на:

• *електронні ресурси навчального призначення* (ЕРНП),

• *електронні ресурси для підтримки наукових досліджень* (ЕРНД),

• *електронні ресурси управлінського призначення* (ЕРУП).

3.2. Незалежно від напряму використання ті чи інші ЕОР можуть відображати різні складові розв’язуваних задач, які мають певне змістовно-процесуальне застосування (призначення). Тому за характером *змістовно-процесуального застосування* ЕОР можна розділити на *дані і комп'ютерні програми*.

3.3. Фізично ЕОР тимчасово або постійно розташовуються й існують на різних типах виокремлених (існуючих окремо від інших) запам'ятовуючих пристроях - носіях електронних даних: мобільних пристроях пам'яті: дискетах, оптичних дисках, флеш-пам'яті, а також на вбудованих пристроях зберігання електронних даних: відповідних пристроях персональних комп'ютерів, універсальних і спеціалізованих ЕОМ, відповідних засобах кластерів пам'яті ІКМ, які самі собою є інваріантними щодо свого інформаційно-змістовного наповнення, переважно передбачають багаторазову його заміну (окрім спеціальних пристроїв з одноразовим записом цифрових даних).

Не мережні ЕРНП за видами носіїв, на яких вони розміщені - відповідних видах технічних засобів навчання, існують у вигляді:

• *дискет;*

• *оптичних дисків;*

• *флеш-пам'яті.*

3.4. Залежно від *середовища фізичного існування*, ЕОР можуть бути розміщені:

• *на виокремлених пристроях зберігання електронних даних*;

• *на вбудованих пристроях зберігання електронних даних*.

3.5. В залежності від *мережної орієнтації* середовища використання ЕОР можуть бути:

• *не мережними*, які призначені (придатні) для використання спільно з локальними комп'ютерними та комп'ютерно орієнтованими засобами;

• *мережними*, які призначені (придатні) для використання в ІКМ.

3.6. В залежності від рівня *обмеження користувацького простору* ЕОР можуть бути:

• *з обмеженим доступом* (обмежено доступними) - з наперед визначеними умовами доступу,

• *загальнодоступними* - з не обмеженими умовами доступу.

3.7. За *масштабом користувацької доступності* (масштабу обмеження кола користувачів) ЕОР *з обмеженим доступом* можуть бути:

• *персональними*, які використовуються індивідуально тільки одним конкретним користувачем;

• *корпоративними (груповими)*, з частково обмеженим (в межах корпорації, для визначених груп користувачів) колом користувачів.

3.8. ЕРНП прикладного використання *за складовою в організації процесу навчання* поділяються на: навчальні та забезпечувальні.

Навчальні (безпосередньо для реалізації процесу навчання):

- *Е-видання навчальні*;
- *Програмні засоби оцінювання навчальних досягнень*;
- *Комп'ютерно орієнтовані навчальні лабораторії;*
- *Е-видання довідкові;*
- *Е-видання демонстраційні;*
- *Е-видання моделюючі;*
- *Електронні тренажери;*
- *Електронні практикуми;*
- *Навчальні пакети прикладних програм;*
- *Електронні навчально-методичні комплекси*

Забезпечувальні (для забезпечення процесу навчання):

- *Електронні дані навчального призначення*;
- *Електронні навчально-методичні матеріали;*
- *Електронні програмно-методичні матеріали;*
- *Електронні додаткові науково-навчальні матеріали*

3.9. *Навчальні програми за рівнем групування* діляться на:

• *окремі навчальні програми*;

• *системні сукупності (колекції) навчальних програм*.

Навчальні дані *за рівнем групування* їх поділяють на:

• *окремі дані*;

• *бази даних*.

3.10. Для підвищення дидактичної ефективності застосування ЕРНП ці засоби навчання використовуються в навчально-виховному процесі спільно з іншими навчально-методичними матеріалами (наприклад, підручниками та посібниками, методичними рекомендаціями для вчителів, учнів, розміщеними на папері), формуючи такою сукупністю комп'ютерно орієнтовані *програмно-методичні комплекси* .

4. Загальні вимоги до ЕОР

ЕОР повинні відповідати таким вимогам:

відповідність чинному державному освітньому стандарту;

відповідність програмі з навчального предмета, для вивчення якого розроблено ЕОР;

дотримання чинних санітарних норм та правил щодо використання комп’ютерної техніки і режиму праці учнів на персональних комп’ютерах;

дотримання техніко-технологічних, психолого-педагогічних, навчально-методичних та дизайн-ергономічних вимог до ЕОР;

дотримання законодавства України щодо захисту авторських прав.

5. Розроблення ЕОР

5.1. Розроблення ЕОР здійснюється автором (викладачем, вчителем, іншою фізичною особою) або авторським колективом у процесі виконання передбаченої індивідуальним планом методичної роботи, в результаті спеціального замовлення, з ініціативи фізичної чи юридичної особи.

5.2. У розробленні ЕОР можуть брати участь як окремі вчителі (викладачі, співробітники навчальних закладів), так і творчі колективи педагогів і співробітників, а при необхідності і сторонні виконавці.

5.3. Розроблення ЕОР може бути здійснено: вчителями (викладачами) у межах методичної роботи, передбаченої їх індивідуальними планами роботи;

педагогами та співробітниками науково-навчальних закладів та установ на основі типових договорів на оплачуване надання освітніх послуг

6. Експертиза ЕОР

6.1. Доцільність використання ЕОР у навчально-виховному процесі визначається за результатами відповідної експертизи, проведеної згідно зі встановленим Міністерством освіти і науки, молоді та спорту України порядком.

6.2. Психолого-педагогічна експертиза визначає повноту викладення змісту предметної галузі та відповідність загальним і специфічним психолого-педагогічним вимогам.

6.3. Техніко-технологічна експертиза визначає працездатність ЕОР як програмного продукту і його сумісність з апаратно-програмними комплексами різної конфігурації; визначає стійкість до помилкових та некоректних дій користувачів.

6.4. Дизайн-ергономічна експертиза оцінює психологічні, ергономічні та художні якості ЕОР та його компонентів

6.5. ЕОР, які створюються і використовуються в межах одного навчального закладу, мають пройти внутрішню експертизу, яку проводять відповідні спеціалісти цього навчального закладу.

7. Поширення ЕОР

Зберігання, поширення, забезпечення доступу до ЕОР та їх описів здійснюється за допомогою їх тиражування на різних типах носіїв електронних даних, а також шляхом їх реєстрації і розміщення в електронних депозитаріях, інших фондах та організаціях, які надають доступ до ЕОР усім учасникам освітнього процесу, а також інших локальних і мережевих інформаційних ресурсах.

ІІ. ПРОПОЗИЦІЇ ДО ПРОЕКТУ ПОЛОЖЕННЯ ПРО ДЕПОЗИТАРІЙ ЕЛЕКТРОННИХ ОСВІТНІХ РЕСУРСІВ

(Лист № 29 від 28.01.2013 р., Додаток 2, Додаток 3.)

Додаток 2. Пропозиції до Положення про депозитарій електронних ресурсів

До п.1.3. розділу І. «Загальні положення» пропонується наступні тлумачення наведених у ньому термінів.

Інтернет – глобальна комп'ютерна мережа, що використовує стандартизовані протоколи і об'єднує десятки тисяч інших мереж.

Інтернет-ресурс - інтернет-сторінка, електронний ресурс, що розміщено в Інтернет.

URL – уніфікований покажчик інформаційного ресурсу, адреса, використовувана веб-браузером (програма перегляду веб-сторінок) для пошуку ресурсу в Інтернеті. Стандартизований рядок символів URL вказує місцезнаходження ресурсу, документа чи його частини в Інтернеті.

Веб-сторінка – веб-документ, HTML-документ, доступний через веб-броузер. Кожна веб-сторінка складається з HTML-файлів, зображень у графічному форматі тощо, а також має власний URL. Веб-сторінка може містити посилання на інші веб-сайти.

Веб-браузер – програма веб-перегляду, навігатор. Програма з графічним інтерфейсом, використовувана для навігації і перегляду різноманітних інтернет-ресурсів.

Метадані – набір допустимих структурованих описів, що є характеристиками об'єктів, даних чи ресурсів для цілей їх ідентифікації, пошуку, оцінювання та управління ними.

Електронний освітній контент - структурований предметний зміст, що має освітнє призначення.

Депозит - внесення інформаційних ресурсів разом з їх описами у процесі різні аспекти фактичних елементів даних, наприклад, ім.'я, формат, вміст.

До п.2.1 розділу ІІ. «Мета і завдання» пропонується врахувати наступні принципи створення депозитарію.

Метою створення депозитарію є забезпечення користувачів вільним Інтернет-доступм до науково-освітніх електронних ресурсів, підвищення ефективності інформаційного забезпечення навчального процесу

До п.2.2 розділу ІІ. «Мета і завдання» пропонується врахувати наступні принципи створення депозитарію.

Універсальний підхід до роботи з ресурсами (мультисорсинг) передбачає реалізацію універсальних підходів до цілеспрямованої актуалізації, генерації і багаторазового використання інформаційних ресурсів, поданих у вигляді електронного контенту.

Вільний мережний доступ – необхідні ресурси і сервіси доступні по мережі через стандартні механізми, що підтримують використання гетерогенних платформ (наприклад, мобільних телефонів, ноутбуків, кишенькових на тастільних комп'ютерів тощо).

Неперервність постачання послуг – забезпечення постачання сервісів інформаційних технологій на максимальному рівні якості в умовах постійної зміни платформ електронного навчання, виникнення нових рішень, зміни технологічної бази клієнтських місць і т.п.

Уніфікована інфраструктура (єдина платформа доступності фізичних і віртуальних серверів) дає можливість управляти ресурсами і розподіляти їх по необхідності з можливістю динамічного призначення і перепризначення різноманітних фізичних і віртуальних ресурсів у відповідності з потребами користувача. Особливе значення має незалежність розміщення ресурсів, коли замовник, у загальному випадку, не знає і не контролює точне фізичне розташування ресурсів, що постачаються, але може визначити їх розташування на більш високому рівні абстракції (наприклад, країна, штат, центр обробки даних)

Інтероперабельність і масштабованість – створення і забезпечення стійкого функціонування надійних платформ, сервісних оперативних динамічних середовищ, на основі яких обчислювальні потужності можуть

гнучко надаватися і вивільнюватись, у ряді випадків автоматично, для забезпечення потреб у споживанні, зберіганні і постачанні необхідних сервісів.

До п.4.3. розділу IV. «Фонд депозитарію», пропонується врахувати наступну класифікацію електронних ресурсів, які можуть зберігатися в Депозитарії:

4.3. Електронні ресурси, які можуть зберігатися в Депозитарії:

Навчальні матеріали

Навчально-методичні матеріали

Довідкові матеріали

Ілюстративні і демонстраційні матеріали

Додаткові інформаційні матеріали

Нормативні документи

Наукові матеріали

Програмні продукти

Програмні комплекси

Інструментальні засоби для створення програмних засобів навчання

До п.4.5. розділу IV. «Фонд депозитарію», пропонується врахувати наступні розділи, з яких складається зміст Депозитарію:

Інструменти навчальної діяльності

Інструменти організації навчального процесу

Електронні видання

Колекції

До п.5.5.2. розділу IV. «Фонд депозитарію», пропонується структурувати наступним чином:

Інструменти навчальної діяльності:

Програмні засоби оцінювання;

Електронні тренажери;

Електронні практикуми;

Електронні підручники, посібники;

Електронні довідники, енциклопедії;

Імітаційні моделі

Навчальні пакети прикладних програм;

Електронні навчально-методичні комплекси

Інструменти організації навчального процесу:

Електронні мультимедійні матеріали;

Електронні навчально-методичні матеріали;

Електронні програмно-методичні матеріали;

Електронні додаткові науково-навчальні матеріали

Електронні видання:

Е-видання наукові

Е-видання літературно художні

Е-аналоги друкованих видань

До п.4.5.1. розділу IV. «Фонд депозитарію», пропонується врахувати наступні вимоги до електронних матеріалів, що входять до складу електронних колекцій.

Синтезований візуальний ряд має містити 2-х, 3-х вимірні статичні і динамічні моделі об'єктів, керовані моделі.

Символьні електронні матеріали мають містити: пояснювальні тексти, заголовки, формули, таблиці.

Графічні електронні матеріали можуть охоплювати схеми, діаграми, карти, графіки, генеалогічні дерева та ін.

Тематичні колекції аудиозаписів охоплюють записи виступів, музичних творів, звуків природи та ін.

Відео-електронні матеріали містять відеофрагменти процесів і явищ, демонстрації дослідів, відео екскурсії та ін.

Фотографічні електронні матеріали містять фотографії експонатів, об'єктів предметної галузі, портрети, ілюстрації та ін..

Додаток 3. Методичні рекомендації щодо класифікації навчальних матеріалів у депозитаріях електронних освітніх ресурсів

З*а галуззю призначення* (спрямованості використання) електронні освітні ресурси (ЕОР) діляться відповідно на:

• *електронні ресурси навчального призначення* (ЕРНП),

• *електронні ресурси для підтримки наукових досліджень* (ЕРНД),

• *електронні ресурси управлінського призначення* (ЕРУП).

Електронні ресурси навчального призначення (ЕРНП) – сукупність ЕОР, що застосовуються для інформаційно-процесуального забезпечення виконання дидактичних завдань (або їх фрагментів), спрямовані на реалізацію навчальної функції системи освіти.

Електронні ресурси управлінського призначення (ЕРУП) – сукупність ЕОР, що застосовуються для інформаційно-процесуального забезпечення виконання завдань управління системою освіти (або їх фрагментів), спрямовані на реалізацію управлінської функції системи освіти.

Електронні ресурси для підтримки наукових досліджень (ЕРНД) – сукупність ЕОР, що застосовуються для інформаційно-процесуального забезпечення виконання завдань ІКТ-підтримки наукових досліджень та розробок, спрямовані на реалізацію наукової та проектувальної функції системи освіти.

Незалежно від напряму використання ті чи інші ЕОР можуть відображати різні складові розв’язуваних задач, які мають певне змістовно-процесуальне застосування (призначення). Тому за характером *змістовно-процесуального застосування* ЕОР можна розділити на *дані і комп'ютерні програми*.

Дані та їх сукупності (окремі дані та / або бази даних) – певним чином структурована, упорядкована і закодована сукупність статичних і динамічних інформаційних об'єктів, що містять аудіо- та відео- або символьні відомості чи їх комбінації (числа, тексти, таблиці, цифрові моделі, графіка, звук, фото, відео та ін.), які можуть бути застосовані для вирішення комп'ютерно орієнтованих завдань (задач) різного освітнього призначення.

Комп'ютерна програма – поданий мовою програмування закодований опис задачі (задач), що підлягає вирішенню за допомогою комп'ютера. Цей опис є інструкцією, де вказується, у якій послідовності (за яким алгоритмом), над якими даними, які операції необхідно виконати й у якій формі видати результат. Тобто, комп'ютерна програма містить опис:

• вбудованих даних (значень елементів даних, відомостей про їх склад і структуру) та їх сукупностей (баз даних), у тому числі всіх або деяких параметрів задачі (задач), а також спеціальних додаткових даних, які підлягають введенню, телекомунікаційному отриманню і / або передаванню, опрацюванню, зберіганню, відображенню;

• способів розв'язування задачі (задач деякого класу);

• адрес мережних ЕОР (даних та інших комп'ютерних програм);

• типу пристрою, з якого можуть вводитися (отримуватися) і на який має видаватися (передаватися) результат розв'язування задачі (задач, виконання програм).

Фізично ЕОР тимчасово або постійно розташовуються й існують на різних типах виокремлених (існуючих окремо від інших) запам'ятовуючих пристроях - носіях електронних даних: мобільних пристроях пам'яті: дискетах, оптичних дисках, флеш-пам'яті, а також на вбудованих пристроях зберігання електронних даних: відповідних пристроях персональних комп'ютерів, універсальних і спеціалізованих ЕОМ, відповідних засобах кластерів пам'яті ІКМ, які самі собою є інваріантними щодо свого інформаційно-змістовного наповнення, переважно передбачають багаторазову його заміну (окрім спеціальних пристроїв з одноразовим записом цифрових даних).

Не мережні ЕРНП за видами носіїв, на яких вони розміщені - відповідних видах технічних засобів навчання, існують у вигляді:

• *дискет;*

• *оптичних дисків;*

• *флеш-пам'яті*.

Залежно від *середовища фізичного існування*, ЕОР можуть бути розміщені:

• *на виокремлених пристроях зберігання електронних даних*;

• *на вбудованих пристроях зберігання електронних даних*.

В залежності від *мережної орієнтації* середовища використання ЕОР можуть бути:

• *не мережними*, які призначені (придатні) для використання спільно з локальними комп'ютерними та комп'ютерно орієнтованими засобами;

• *мережними*, які призначені (придатні) для використання в ІКМ.

В залежності від рівня *обмеження користувацького простору* ЕОР можуть бути:

• *з обмеженим доступом* (обмежено доступними) - з наперед визначеними умовами доступу,

• *загальнодоступними* - з не обмеженими умовами доступу.

За *масштабом користувацької доступності* (масштабу обмеження кола користувачів) ЕОР *з обмеженим доступом* можуть бути:

• *персональними*, які використовуються індивідуально тільки одним конкретним користувачем;

• *корпоративними (груповими)*, з частково обмеженим (в межах корпорації, для визначених груп користувачів) колом користувачів.

ЕРНП прикладного використання *за складовою в організації процесу навчання* поділяються на: навчальні та забезпечувальні.

Навчальні (безпосередньо для реалізації процесу навчання):

- *Е-видання навчальні*;
- *Програмні засоби оцінювання навчальних досягнень*;
- *Комп'ютерно орієнтовані навчальні лабораторії;*
- *Е-видання довідкові;*
- *Е-видання демонстраційні;*
- *Е-видання моделюючі;*
- *Електронні тренажери;*
- *Електронні практикуми;*
- *Навчальні пакети прикладних програм;*
- *Електронні навчально-методичні комплекси*

Забезпечувальні (для забезпечення процесу навчання):

- *Електронні дані навчального призначення*;
- *Електронні навчально-методичні матеріали;*
- *Електронні програмно-методичні матеріали;*
- *Електронні додаткові науково-навчальні матеріали*

Навчальні програми за рівнем групування діляться на:

• *окремі навчальні програми*;

• *системні сукупності (колекції) навчальних програм*.

Навчальні дані *за рівнем групування* їх поділяють на:

• *окремі дані*;

• *бази даних*.

Для підвищення дидактичної ефективності застосування ЕРНП ці засоби навчання використовуються в навчально-виховному процесі спільно з іншими навчально-методичними матеріалами (наприклад, підручниками та посібниками, методичними рекомендаціями для вчителів, учнів, розміщеними на папері), формуючи такою сукупністю комп'ютерно орієнтовані *програмно-методичні комплекси* .

Проект

ПОЛОЖЕННЯ

про психолого-педагогічні вимоги до якості електронних освітніх ресурсів

(Лист № 28.01.2013 р. № 30, Додаток 1)

1. Загальні положення

1.1. Положення про психолого-педагогічні вимоги до якості електронних освітніх ресурсів (далі – Положення) розроблене згідно Національного плану дій на 2012 рік (пунктів 5.1.1. – 5.1.3. Плану-графіка реформ на 2012 рік) щодо впровадження Програми економічних реформ на 2010 - 2014 роки "Заможне суспільство, конкурентоспроможна економіка, ефективна держава", затвердженого Указом Президента України від 12 березня 2012 року № 187/2012, Державної цільової програми впровадження у навчально-виховний процес загальноосвітніх навчальних закладів інформаційно-комунікаційних технологій "Сто відсотків" на період до 2015 року, затвердженої постановою Кабінету Міністрів України від 13 квітня 2011 р. № 494, і визначає психолого-педагогічні вимоги до електронних освітніх ресурсів (далі - ЕОР).

1.2. Положення ґрунтується на положеннях і нормах Законів України «Про освіту», «Про вищу освіту», «Про професійно-технічну освіту», «Про загальну середню освіту», «Про позашкільну освіту», «Про видавничу справу», «Про наукову і науково-технічну експертизу», Положення про електронні освітні ресурси; чинних державних і освітніх стандартів з урахуванням вимог Державних санітарних правил і норм, інших нормативно-правових актів, що регламентують діяльність МОН щодо науково-методичного і матеріально-технічного забезпечення системи освіти.

1.2. Під вимогами до ЕОР розуміють: психолого-педагогічні чинники, умови або можливості, необхідні користувачеві ЕОР для вирішення навчальних завдань або досягнення освітніх цілей.

1.3. Розроблення Положення сприятиме уточненню психолого-педагогічних вимог до якості ЕОР. Це розвиває методологію проведення експертизи якості

ЕОР, сприяє підвищенню якості ЕОР у процесі їх створення, індустріального виробництва та ефективного використання в освітній практиці.

2. Психолого-педагогічні вимоги до якості ЕОР

ЕОР мають відповідати стандартним дидактичним вимогам, що подаються до навчальних видань, таких як підручники, навчальні та методичні посібники. Дидактичні вимоги відповідають специфічним закономірностям навчання і, відповідно, дидактичним принципам навчання.

Загальні дидактичні вимоги до якості ЕОР

Вимога *науковості* навчання означає необхідність забезпечення достатньої глибини, коректності та наукової вірогідності викладу змісту навчального матеріалу, що поданий у компонентах електронного засобу або ресурсу, з урахуванням останніх наукових досягнень. Процес засвоєння навчального матеріалу має будуватися відповідно до сучасних методів наукового пізнання: експеримент, порівняння, спостереження, абстрагування, узагальнення, конкретизація, аналогія, індукція і дедукція, аналіз і синтез, методи моделювання, в тому числі й математичного, а також методу системного аналізу. Відповідно і добір засобу має проводитися із урахуванням можливості реалізації цих функцій на належному науковому рівні.

Вимога *доступності* навчання, здійснюваного з використанням електронного засобу навчального призначення, пов’язана з необхідністю забезпечення відповідності ступеня теоретичної складності й глибини вивчення матеріалу віковим і індивідуальним особливостям учнів. Неприпустима надмірна ускладненість і перевантаженість навчального матеріалу, при якій оволодіння ним стає непосильним для того, кого навчають.

Вимога забезпечення *проблемності* процесу навчання обумовлена самою сутністю і характером навчально-пізнавальної діяльності. Коли учень стикається з навчальною проблемною ситуацією, що вимагає вирішення, його розумова активність зростає. Рівень виконання даної дидактичної вимоги за допомогою електронного засобу або ресурсу може бути значно вищим, ніж при використанні традиційних підручників і посібників. Відповідно до цього, добір і

застосування електронного засобу має відбуватися таким чином, щоб можна було реалізувати всі потенційні можливості активізації навчальної діяльності.

Вимога *наочності* навчання пов’язана з урахуванням особливостей чуттєвого сприйняття властивостей досліджуваних об'єктів і забезпечення можливості їх спостереження учнем. У випадку використання електронних засобів та ресурсів у навчанні ця вимога може бути реалізовано на принципово новому, більш високому рівні. Через це добір засобу має здійснюватися таким чином, щоб сприяти якомога більш повному сприйняттю та розкриттю властивостей об’єктів вивчення. Поширення систем віртуальної реальності дозволить у найближчому майбутньому поліпшити не лише наочність, а і полісенсорність навчання.

Вимога *свідомості* навчання, *самостійності й активізації* діяльності передбачає забезпечення учнів навчальним матеріалом для самостійних дій та здійснення свідомого вибору на шляху досягнення кінцевих цілей і завдань. При цьому предметом усвідомлення постає той зміст, на який спрямована діяльність, що може бути поданий як стисло, так і в розгорнутому вигляді. Учні самі дозують обсяг і глибину матеріалу, необхідного для осягнення сутності явища. Для активізації діяльності учня за допомогою електронних засобів та ресурсів необхідно добирати ті, в яких передбачено генерування різноманітних навчальних ситуацій, формулювання питань, надання можливості вибору тієї чи іншої траєкторії навчання, керування ходом подій.

Вимога *систематичності та послідовності* навчання означає необхідність забезпечення наступності засвоєння учнями визначеної системи знань у певній предметній галузі. Знання, уміння і навички мають формуватися у визначеній системі, в чіткому логічному порядку. Для цього важливо, щоб навчальний матеріал було подано у структурованому вигляді, враховуючи як ретроспективи, так і перспективи формування знань, умінь і навичок при компонуванні кожної частки навчального матеріалу й створенні міжпредметних зв'язків. Порядок подання змісту і прогнозування навчальних впливів має бути ретельно продуманим, обумовленим логікою процесу навчання. Забезпечення зв'язку відомостей, що містять електронні засоби або ресурси, із практикою має

відбуватися за рахунок добору прикладів, створення змістовних ігрових моментів, постановки завдань практичного характеру, експериментів, моделей реальних процесів і явищ.

Специфічні дидактичні вимоги

Вимога *інтерактивності* навчання стосується, зокрема, організації зворотного зв'язку при роботі учня з засобом ІКТ. За допомогою зворотного зв'язку здійснюється контроль і корегуються дії учня, надаються рекомендації для подальшої роботи, забезпечується постійний доступ до супровідної довідки. В результаті контролю та діагностики помилок за підсумками навчальної діяльності проводиться аналіз роботи з рекомендаціями щодо підвищення рівня знань.

Вимога *адаптивності* ЕОР передбачає можливість адаптації процесу навчання з цим засобом до рівня знань і вмінь, психологічних особливостей того, кого навчають. Розрізняють три рівні адаптації ЕЗНП: першим рівнем адаптації вважається можливість вибору учнем найпридатнішого для нього індивідуального темпу вивчення матеріалу; другий рівень адаптації передбачає діагностику стану того, кого навчають, на підставі результатів якої пропонується зміст і методика навчання; третій рівень адаптації базується на відкритому підході, коли користувачеві надається можливість вибору із значного числа варіантів, придатних для якомога більшого контингенту тих, кого навчають.

Вимога *розвитку інтелектуального потенціалу* того, хто навчається, полягає у тому, що використання засобів ІКТ має сприяти формуванню стилів мислення (алгоритмічного, наочно-образного, теоретичного), умінню оптимізувати рішення в складній ситуації, опрацьовувати інформацію (на основі використання систем опрацювання даних, інформаційно-пошукових систем, баз даних тощо).

Вимога *забезпечення повноти (цілісності) і безперервності* дидактичного циклу означає, що зміст електронного засобу або ресурсу передбачає структурно-функціональну зв'язаність навчального матеріалу, можливість виконання всіх ланок дидактичного циклу в межах одного сеансу роботи.

Вимога *системності та структурно-функціональної зв'язаності* подання навчального матеріалу в ЕОР. Тобто потрібно, щоб зміст електронного засобу навчального призначення мав достатню глибину, коректність, добір матеріалу здійснювався структуровано, логічно, послідовно, відповідно до вікових та індивідуальних особливостей учня. Неприпустима надмірна ускладненість і перевантаженість навчального матеріалу.

Специфічні дидактичні вимоги до якості ЕОР.

1. Вимога адаптивності передбачає здатність пристосовуваності ЕОР до індивідуальних можливостей учня. Ця вимога означає адаптацію процесу навчання до рівня знань і умінь, психологічних особливостей того, хто навчається. Розрізняють три рівні адаптації ЕОР. Першим рівнем адаптації вважається реалізація можливості вибору учнем найбільш підходящого для нього індивідуального темпу вивчення матеріалу. Другий рівень адаптації передбачає діагностику стану учня, на підставі результатів якої, пропонується зміст і методика навчання. Третій рівень адаптації базується на відкритому підході, який спрямований на класифікацію можливих користувачів і полягає в тому, що автори програми прагнуть розробити якомога більше варіантів її використання для якомога ширшого контингенту тих, хто навчається.

2. Вимога інтерактивності навчання означає, що в процесі навчання має мати місце взаємодія учня з ЕОР. ЕОР мають забезпечувати інтерактивний діалог і зворотний зв'язок. Важливою складовою частиною організації діалогу є реакція ЕОР на дії користувача. Зворотний зв'язок дозволяє здійснювати контроль і коригувати дії учня, видавати рекомендації щодо подальшої роботи, здійснювати постійний доступ до довідкової та роз'яснювальної інформації. При контролі з діагностикою помилок за результатами навчальної роботи зворотний зв'язок видає результати аналізу роботи з рекомендаціями з підвищення рівня знань.

3. Вимога реалізації комп'ютерної візуалізації навчальної інформації, що подається в ЕОР. Вимога передбачає аналіз технічних можливостей використання сучасних засобів подання навчальної інформації (комп'ютерів,

мультимедіа проекторів, засобів віртуальної реальності та сучасного програмного забезпечення) і якість подання навчальної інформації в ЕОР.

4. Вимога розвитку інтелектуального потенціалу учня при роботі з ЕОР передбачає формування різноманітних стилів мислення (алгоритмічного, наочно-образного, рефлексивного, теоретичного), вміння приймати раціональні або варіативні рішення в складних ситуаціях, умінь з опрацювання і набування інформації (на основі використання систем обробки даних, інформаційно-пошукових систем, баз даних тощо).

5. Вимога системності та структурно-функціональної зв'язаності подання навчального матеріалу в ЕОР.

6. Вимога забезпечення повноти (цілісності) і безперервності дидактичного циклу навчання означає, що при роботі з ЕОР має забезпечуватись можливість виконання всіх ланок дидактичного циклу в межах одного сеансу роботи з інформаційною і комунікаційною технікою (на це і націлені ЕОР, наприклад, електронні підручники та електронні навчальні посібники, комплексно реалізують відразу кілька дидактичних функцій).

Психологічні вимоги до якості ЕОР

- Відповідність вербально-логічному та сенсорно-перцептивним рівням когнітивного процесу;
- орієнтація на особливості сприйняття (переважно зорового, а також слухового, дотикового);
- врахування особливостей уваги (стійкість, концентрація, здатність переключатися, розподіл і обсяг);
- розвиток мислення (наочно-дійове образне, словесно-логічне, понятійне, конкретно-понятійне, абстрактно-понятійне або теоретичне);
- розвиток уяви (мимовільна , довільна, репродуктивна, творча);
- розвиток пам’яті (миттєва, довгострокова, короткострокова, оперативна);
- орієнтація на словниковий запас та вербально-лінгвістичні можливості певного рівня знань та підготовки дітей, доступність викладення відповідно до віку;

- врахування «зони найближчого розвитку», тобто сприяння розвитку дитини.

3. Психолого-педагогічна експертиза якості ЕОР

3.1. Доцільність використання ЕОР у навчально-виховному процесі визначається за результатами відповідної експертизи, проведеної згідно зі встановленим Міністерством освіти і науки України порядком.

3.2. Психолого-педагогічна експертиза визначає повноту викладення змісту предметної галузі та відповідність загальним і специфічним психолого-педагогічним вимогам.

Методичні рекомендації з комплексного оцінювання якості електронних освітніх ресурсів

(Лист № 28.01.2013 р. № 30, Додаток 2)

Під *комплексним оцінюванням якості електронних освітніх ресурсів (ЕОР)* розуміється оцінювання якості ЕОР за сукупністю параметрів: змістовних, дидактичних, психологічних, техніко - технологічних, методичних та дизайн-ергономічних.

Змістовне оцінювання якості ЕОР.

Зміст ЕОР має відповідати вимогам Державних освітніх стандартів України за відповідними напрямами підготовки фахівців, навчальним програмам, затвердженим МОН України, Положенням щодо якості ЕОР, затвердженими МОН України.

Відповідність ЕОР вимогам Державних освітніх стандартів може підтвердити експертиза Міністерства освіти і науки України по відповідному напрямку.

ЕОР, використовувані для самостійного вивчення певної навчальної дисципліни, мають охоплювати повну сукупність освітніх ресурсів, засоби для реєстрації учнів, вивчення теоретичних матеріалів, комп'ютерного моделювання та експериментального дослідження досліджуваних об'єктів, включаючи засоби опрацювання і відображення результатів моделювання і експериментів, а також інтерактивні навчальні завдання для тренінгу та засоби контролю знань і умінь.

Техніко-технологічне оцінювання якості ЕОР.

ЕОР можуть бути розміщені в мережі Інтернет (портали, сайти), локальних мережах і на CD- ROM.

Для ЕОР на CD- ROM рекомендується використовувати наступні мультимедіа компоненти:

Macromedia Flash-формат представлення анімованої графіки, розроблений фірмою Macromedia і широко підтримуваний різними програмними продуктами (передбачуваний обсяг - 100-150 Мб);

AVI- формат представлення відеоінформації з використанням відеокодеків MPEG- 4 (передбачуваний обсяг - 200-300 Мб);

JPG-формат представлення графічної інформації (передбачуваний обсяг - 50-70 Мб);

GIF - економічний формат представлення графічної інформації (передбачуваний обсяг - 10-20 Мб);

WAV- стандартний формат представлення аудіоінформації в системі Microsoft Windows.

Зміст ЕОР має відповідати сучасним науковим розробкам у відповідних предметних галузях і достовірності подання фактографічних матеріалів.

ЕОР має забезпечувати широке подання структурних компонентів освітнього процесу – надання інформації (навчання), практичні заняття (тренування і закріплення знань, умінь і навичок), атестація (контроль отриманих знань, умінь і навичок), можливість підсумкового контролю отриманих знань сучасними методами комп'ютерної атестації.

Розробник мережних ЕОР має забезпечити стабільну роботу в мережі Інтернет на основі каналу цілодобового доступу до сегменту мережі Інтернет з пропускною здатністю не менше 2 Мбіт/с. Застосування ЕОР не має вимагати підвищених показників продуктивності комп'ютерної техніки та спеціального програмного забезпечення для робочих місць учасників навчального процесу.

Програмна реалізація ЕОР має дозволяти роботу з ними через звичайний-браузер. Технічні та програмні засоби забезпечення ЕОР мають володіти достатньою пропускною здатністю для одночасної роботи не менше однієї навчальної групи студентів в режимі віддаленого доступу з комп'ютерних мереж.

Для розробників ЕОР порталів пропонується враховувати наступні вимоги до ЕОР:

1. Функціонування ЕОР у відповідних порталу телекомунікаційних середовищах, операційних системах і платформах.

2. Максимального використання сучасних засобів мультимедіа та телекомунікаційних технологій.

3. Надійності та стійкої працездатності.

4. Гетерогенності (стійкої роботи на різних комп'ютерних та інших аналогічних їм засобах, передбачених специфікацією ЕНМК).

5. Стійкості до дефектів.

6. Наявності захисту від несанкціонованих дій користувачів.

7. Ефективного та виправданого використання ресурсів.

8. Тестованості.

9. Простоти, надійності та повноти інсталяції і деінсталяції.

Програмно-технологічною платформою для побудови та підтримки системи освітніх порталів є програмно-апаратний комплекс, що дозволяє будувати і підтримувати портали різного призначення і архітектури та забезпечувати виконання наступного набору функцій:

• виконання програмних додатків;

• можливість спільної роботи;

• управління контентом;

• управління користувачами;

• контроль і управління продуктивністю;

• управління знаннями;

• підтримування комунікацій;

• персоніфікація;

• профілювання;

• пошук;

• забезпечення безпеки;

• стандартний www -доступ до порталу.

Психолого-педагогічне оцінювання якості ЕОР.

Психолого-педагогічне оцінювання якості електронних освітніх ресурсів автори досліджень здебільшого пропонують здійснювати за сукупністю показників: змістовних, дидактичних, методичних та дизайн-ергономічних [1, 2, 3, 4, 5, 6]. Зокрема, виокремлюють дидактичні показники, що поділяються на суто дидактичні і специфічні. Суто дидактичні вимоги спільні як для електронних, так і інших видів засобів навчання, наприклад, підручників,

навчальних та методичних посібників тощо. Дидактичні вимоги зумовлені загальними закономірностями і принципами процесу навчання. Специфічні вимоги стосуються суто електронних засобів і ресурсів навчального призначення.

Дидактичні вимоги до якості ЕОР.

Далі розглянуто дидактичні вимоги до ЕОР, що реалізуються у навчально-виховному процесі [3, 4, 5].

Суто дидактичні вимоги

Вимога *науковості* навчання означає необхідність забезпечення достатньої глибини, коректності та наукової вірогідності викладу змісту навчального матеріалу, що поданий у компонентах електронного засобу або ресурсу, з урахуванням останніх наукових досягнень. Процес засвоєння навчального матеріалу має будуватися відповідно до сучасних методів наукового пізнання: експеримент, порівняння, спостереження, абстрагування, узагальнення, конкретизація, аналогія, індукція і дедукція, аналіз і синтез, методи моделювання, в тому числі й математичного, а також методу системного аналізу. Відповідно і добір засобу має проводитися із урахуванням можливості реалізації цих функцій на належному науковому рівні.

Вимога *доступності* навчання, здійснюваного з використанням електронного засобу навчального призначення, пов’язана з необхідністю забезпечення відповідності ступеня теоретичної складності й глибини вивчення матеріалу віковим і індивідуальним особливостям учнів. Неприпустима надмірна ускладненість і перевантаженість навчального матеріалу, при якій оволодіння ним стає непосильним для того, кого навчають.

Вимога забезпечення *проблемності* процесу навчання обумовлена самою сутністю і характером навчально-пізнавальної діяльності. Коли учень стикається з навчальною проблемною ситуацією, що вимагає вирішення, його розумова активність зростає. Рівень виконання даної дидактичної вимоги за допомогою електронного засобу або ресурсу може бути значно вищим, ніж при використанні традиційних підручників і посібників. Відповідно до цього, добір і

застосування електронного засобу має відбуватися таким чином, щоб можна було реалізувати всі потенційні можливості активізації навчальної діяльності.

Вимога *наочності* навчання пов’язана з урахуванням особливостей чуттєвого сприйняття властивостей досліджуваних об'єктів і забезпечення можливості їх спостереження учнем. У випадку використання електронних засобів та ресурсів у навчанні ця вимога може бути реалізовано на принципово новому, більш високому рівні. Через це добір засобу має здійснюватися таким чином, щоб сприяти якомога більш повному сприйняттю та розкриттю властивостей об’єктів вивчення. Поширення систем віртуальної реальності дозволить у найближчому майбутньому поліпшити не лише наочність, а і полісенсорність навчання.

Вимога *свідомості* навчання, *самостійності й активізації* діяльності передбачає забезпечення учнів навчальним матеріалом для самостійних дій та здійснення свідомого вибору на шляху досягнення кінцевих цілей і завдань. При цьому предметом усвідомлення постає той зміст, на який спрямована діяльність, що може бути поданий як стисло, так і в розгорнутому вигляді. Учні самі дозують обсяг і глибину матеріалу, необхідного для осягнення сутності явища. Для активізації діяльності учня за допомогою електронних засобів та ресурсів необхідно добирати ті, в яких передбачено генерування різноманітних навчальних ситуацій, формулювання питань, надання можливості вибору тієї чи іншої траєкторії навчання, керування ходом подій.

Вимога *систематичності та послідовності* навчання означає необхідність забезпечення наступності засвоєння учнями визначеної системи знань у певній предметній галузі. Знання, уміння і навички мають формуватися у визначеній системі, в чіткому логічному порядку. Для цього важливо, щоб навчальний матеріал було подано у структурованому вигляді, враховуючи як ретроспективи, так і перспективи формування знань, умінь і навичок при компонуванні кожної частки навчального матеріалу й створенні міжпредметних зв'язків. Порядок подання змісту і прогнозування навчальних впливів має бути ретельно продуманим, обумовленим логікою процесу навчання. Забезпечення зв'язку відомостей, що містять електронні засоби або ресурси, із практикою має

відбуватися за рахунок добору прикладів, створення змістовних ігрових моментів, постановки завдань практичного характеру, експериментів, моделей реальних процесів і явищ.

Специфічні дидактичні вимоги

Вимога *інтерактивності* навчання стосується, зокрема, організації зворотного зв'язку при роботі учня з засобом ІКТ. За допомогою зворотного зв'язку здійснюється контроль і корегуються дії учня, надаються рекомендації для подальшої роботи, забезпечується постійний доступ до супровідної довідки. В результаті контролю та діагностики помилок за підсумками навчальної діяльності проводиться аналіз роботи з рекомендаціями щодо підвищення рівня знань.

Вимога *адаптивності* ЕОР передбачає можливість адаптації процесу навчання з цим засобом до рівня знань і вмінь, психологічних особливостей того, кого навчають. Розрізняють три рівні адаптації ЕЗНП: першим рівнем адаптації вважається можливість вибору учнем найпридатнішого для нього індивідуального темпу вивчення матеріалу; другий рівень адаптації передбачає діагностику стану того, кого навчають, на підставі результатів якої пропонується зміст і методика навчання; третій рівень адаптації базується на відкритому підході, коли користувачеві надається можливість вибору із значного числа варіантів, придатних для якомога більшого контингенту тих, кого навчають.

Вимога *розвитку інтелектуального потенціалу* того, хто навчається, полягає у тому, що використання засобів ІКТ має сприяти формуванню стилів мислення (алгоритмічного, наочно-образного, теоретичного), умінню оптимізувати рішення в складній ситуації, опрацьовувати інформацію (на основі використання систем опрацювання даних, інформаційно-пошукових систем, баз даних тощо).

Вимога *забезпечення повноти (цілісності) і безперервності* дидактичного циклу означає, що зміст електронного засобу або ресурсу передбачає структурно-функціональну зв'язаність навчального матеріалу, можливість виконання всіх ланок дидактичного циклу в межах одного сеансу роботи.

Вимога *системності та структурно-функціональної зв'язаності* подання навчального матеріалу в ЕОР. Тобто потрібно, щоб зміст електронного засобу навчального призначення мав достатню глибину, коректність, добір матеріалу здійснювався структуровано, логічно, послідовно, відповідно до вікових та індивідуальних особливостей учня. Неприпустима надмірна ускладненість і перевантаженість навчального матеріалу.

Серед психолого-педагогічних вимог до якості ЕОР важливе місце займає група *методичних* вимог. Показникам цього типу надають особливої уваги з точки зору добору і виявлення місця конкретного засобу в навчальному процесі, його позиціонування відносно певної предметної галузі, врахування методів й специфіки використання цієї галузі.

Серед показників даного типу деякі автори [3, 5] виокремлюють наступні:

1. Подання навчального матеріалу має спиратися на вербально-понятійні, наочно-образні та діяльнісні компоненти свідомості.

2. Необхідно, щоб зміст електронного засобу навчального призначення адекватно відтворював систему понять навчальної дисципліни.

3. При роботі з засобом навчання учневі надається можливість закріплювати різноманітні вміння зі здійсненням контролю на різних етапах засвоєння матеріалу на рівні, достатньому для реалізації алгоритмічної та евристично-пошукової діяльності.

При оцінюванні аспектів якості відносно методичних вимог до електронного засобу навчального призначення варто звертати увагу також на такі показники [2, 3, 5]:

- Якість методичних рекомендацій з використання засобу.
- Відповідність системи завдань, вправ, практичних та лабораторних робіт вимогам до вмінь та навичок, що мають бути сформовані на певному етапі.
- Можливість вибору учнем рівня складності при опануванні змісту.
- Можливість вибору варіанту змісту в залежності від профілю навчання.
- Наявність проміжних форм контролю вивчення матеріалу.
- Наявність підсумкових форм контролю вивчення матеріалу.
- Збалансованість подання теоретичного і практичного матеріалу.

- Врахування рівня інформаційно-комунікаційної підготовки учня.

Психологічні вимоги до якості ЕОР.

Відповідність психолого-педагогічним вимогам подання навчального матеріалу в ЕОР має враховувати можливий вік учнів, на навчання яких розрахований ЕОР; відповідність психолого-педагогічному потенціалу учнів; можливість варіативності навчання. До них тісно примикає група здоров'язбережувальних вимог.

Психологічні вимоги характеризуються наступними показниками [2, 3]:

- відповідність вербально-логічному та сенсорно-перцептивним рівням когнітивного процесу;
- орієнтація на особливості сприйняття (переважно зорового, а також слухового, дотикового);
- врахування особливостей уваги (стійкість, концентрація, здатність переключатися, розподіл і обсяг);
- розвиток мислення (наочно-дійове образне, словесно-логічне, понятійне, конкретно-понятійне, абстрактно-понятійне або теоретичне);
- розвиток уяви (мимовільна , довільна, репродуктивна, творча);
- розвиток пам'яті (миттєва, довгострокова, короткострокова, оперативна);
- орієнтація на словниковий запас та вербально-лінгвістичні можливості певного рівня знань та підготовки дітей, доступність викладення відповідно до віку;
- врахування «зони найближчого розвитку», тобто сприяння розвитку дитини.

Вимоги *здоров'язбережувального характеру*, що пред'являються до освітніх електронних видань і ресурсів, стосуються гігієнічних вимог, санітарних норм і правил роботи з комп'ютерною технікою. Слід зазначити, що відповідність освітніх електронних видань і ресурсів віковим особливостям учнів і санітарним нормам роботи з комп'ютерною технікою є одним з основних умов ефективності інформатизації навчального процесу. Невідповідність цим вимогам призведе або до не сприйняття учнями частини інформації або до погіршення їх здоров'я [1, 4, 5].

Для аналізу освітніх електронних видань і ресурсів велике значення мають вимоги до режиму праці й відпочинку школярів під час роботи з персональними комп'ютерами: використовувані засоби ІКТ мають бути розроблені так, щоб час їх функціонування не перевищував санітарних норм роботи з комп'ютерною технікою.

Ергономічні вимоги до якості ЕОР.

Ергономічні вимоги до ЕОР будуються з урахуванням вікових особливостей учнів, забезпечують підвищення рівня мотивації до навчання, стосуються показників, що характеризують подання зображення на екрані та режимів роботи з ЕОР.

Основною ергономічною вимогою є забезпечення гуманного ставлення до учня, організації в ЕОР і його компонентах дружнього інтерфейсу, забезпечення можливості використання учнями необхідних підказок і методичних вказівок, вільної послідовності і темпу роботи, що дозволить уникнути негативного впливу на психіку, створить доброзичливу атмосферу на заняттях.

Ергономічні вимоги, пропоновані до ЕЗНП, діляться на такі групи [2, 3, 5]: вимоги до колірних характеристик; вимоги до просторового розміщення інформації на екрані монітора; вимоги до організації діалогу; вимоги до буквено-цифрового символіки і знаків; вимоги до звукового супроводу.

1. *Вимоги до колірних характеристик*.

Параметр якості: відповідність колірної палітри відносній видимості предметів зображення [2].

- Неприпустима наявність колірних гомогенних полів. Оптимальність контрасту зображення по відношенню до фону. Для графічної інформації необхідно використання прямого контрасту, для текстової - зворотного.
- Постійність використовуваних кольорів. Одні й ті ж об'єкти позначені однаковими кольорами.
- Відповідність кольорів стійким зоровим асоціаціям: червоний - небезпека, жовтий - увага, стеження, зелений - дозволяючий і т.д.
- Яскравість кольорів об'єктів по відношенню до тла. Необхідний рівномірний розподіл яскравості, контраст яскравості не менш, ніж 60 %.

- Оптимальність вибору кольорів для смислового протиставлення об'єктів: червоний - зелений, синій - жовтий, білий - чорний.
- Оптимальність поєднання кольору і яскравості зображення: червоний - при високій яскравості; зелений - в середньому діапазоні яскравості; жовтий - в широкому діапазоні, синій - при малої яскравості.

2. *Вимоги до просторового розміщення інформації на екрані монітора*. Параметр якості: відповідність форм об'єктів стійким зоровим асоціаціям: форми об'єктів на екрані схожі на форми реальних об'єктів [2, 5].

- Використання логічних наголосів: обов'язкове використання для графічної, бажано і для текстово-графічної інформації.
- Оптимальність використання логічних наголосів: наявність не більше одного логічного наголосу в кожен момент часу. Виділення логічним наголосом головного об'єкта.
- Відповідність послідовності логічних наголосів оптимальному порядку вивчення інформації: послідовність логічних наголосів відповідає оптимальному порядку вивчення інформації.
- Відповідність просторового розташування інформації на екрані оптимальному порядку вивчення.
- Ступінь засміченості поля головного об'єкта - не більше 4-6 другорядних об'єктів в полі головного об'єкта.

3. *Вимоги до організації діалогу* формуються з умов максимальної природності взаємодії учня з програмним засобом.

Параметри якості: доступність для учнів, відповідність тезаурусу та лінгвістичної композиції [2].

- Час реакції на відповідь або управлінський вплив: 2 - 3 секунди, 3-10 секунд, більше 10 секунд;
- Число варіантів відповідей у питаннях типу «меню»: 4 – 6;
- Правдоподібність відповідей у питаннях типу «меню»: один - найбільш правдоподібна;
- Наявність інструкції або підказки, зручність роботи з нею: є (у явному або неявному вигляді) у програмному засобі: зручна в роботі

4. Вимоги до буквено-цифрової символіки і знаків.

Формуються з умов максимальної ефективності зчитування буквено-цифрового інформації з екрана монітора, розділяються на вимоги до розбірливості зображення і вимоги до параметрів тексту [2].

5. *Вимоги до звукового супроводу* розроблені, виходячи з умов максимальної природності сприйняття людиною звукової інформації з урахуванням специфіки використання ЕОР у навчальному процесі.

Параметри якості: комфортність сприймання звукової інформації [2].

- Відповідність амплітудно-частотних характеристик ЕОР області комфортного сприйняття.
- Відсутність негативних реакцій на звукову інформацію.
- Звукові характеристики ЕЗНП відповідають природним звукам.
- Залежність максимальної розбірливості від рівня гучності: для демонстраційних ЕОР максимальна розбірливість при великій гучності. Для ЕОР для індивідуальної роботи на уроці: максимальна розбірливість при малій гучності. Для ЕОР для самостійної роботи в домашніх умовах: максимальна розбірливість між низьким і середнім рівнем гучності.
- Відповідність звукової інформації стійким звуковим асоціаціям: характеристики окремих фрагментів звукового супроводу близькі до характеристик реальних процесів або об'єктів;
- Ступінь засміченості звукового супроводу: найбільш оптимально використання одночасно 1-2 звукових фрагментів, що характеризують різні процеси або об'єкти. Можливо використання 3 фрагментів; використання більш 3 звукових фрагментів одночасно - не доцільно.
- Оптимальність темпу звукового супроводу: темп звукового супроводу повинен відповідати оптимальній швидкості роботи учнів з ЕОР.

Список використаних джерел.

1. Дем’яненко В.М. Методичні рекомендації з оцінювання якості електронних засобів та ресурсів у навчально-виховному процесі / В.М.Дем’яненко, М.П.Шишкіна // Інформаційні технології і засоби навчання [Електронний ресурс]. - 2011. №6 (26). - Режим доступу:

http://journal.iitta.gov.ua/index.php/itlt/article/view/589/462.

2. Вострокнутов И.Е. Теория и технология оценки качества программных средств образовательного назначения / И.Е.Вострокнутов. – М.: Госкоорцентр информационных технологий, 2005. – 300 с.

3. Григорьев С.Г. Информатизация образования. Фундаментальные основы / С.Г. Григорьев, В.В.Гриншкун. – Томск: Изд-во «ТМЛ-Пресс», 208. – 286 с.

4. Жалдак М.І. Комп'ютерно-орієнтовані засоби навчання математики, фізики, інформатики / М.І.Жалдак, В.В.Лапінський, М.І.Шут. – Київ: Дініт, 2004.

5. Роберт И.В. Теория и методика информатизации образования (психолого-педагогический и технологический аспекты) / И.В. Роберт. – М.: ИИО РАО, 2008. – 274 с.

6. Черткова Е.А. Разработка спецификации требований к компьютерным обучющим системам / Е.А.Черткова, И.В.Ретинская, К.К. Дауренбеков // Качество, Инновации, Образование. – 2009. - №3. – с.63-67.

V. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАВЧАЛЬНОГО КОМП'ЮТЕРНОГО КОМПЛЕКСУ

(Лист № 28.01.2013 р. № 30)

ЗМІСТ

1. Інформаційна безпека дітей
в умовах загальноосвітнього навчального закладу.
Основні загрози для дітей та підлітків у сфері ІКТ.

Використання комп'ютерів у навчальному процесі є необхідною умовою сучасного навчання та виховання підростаючого покоління. Однак, в даному розділі, зосередимо свою увагу на негативних наслідках інформатизації та поширення інформаційних технологій у шкільних умовах. З усіх негативних впливів інформаційного середовища і можливих негативних наслідків впливу комп'ютерної техніки на дітей і підлітків ми виділимо ті, які підпадають під визначення інформаційної безпеки несформованої особистості.

Можемо сказати, що інформаційна безпека – це стан захищеності, тобто вона є властивістю системи мінімізувати інформаційні загрози. В першу чергу треба говорити про загрози, вони є первинними по відношенні до захисту від загроз. Для окремої особистості існують одні загрози, для суспільства інші, для держави – ще інші. Поширивши цю тезу вглиб, можемо вказати, що для дітей і молоді існують інші види загроз з огляду на вікові та психологічні особливості. Що для сформованої, зрілої особистості, не несе загрози, те для дитини може виявитися небезпечним. Несформованість психічної, вольової, емоційної сфери, недостатній рівень розвитку критичного мислення дітей і підлітків з одного боку, і часто вільний, неконтрольований доступ їх до джерел інформації, веде до підпадання їх під негативний інформаційний вплив, котрий може проявитися, як у деструктивних діях, так і в формуванні морально спотвореної особистості. Настільки людина сприйнятлива до психологічних впливів, загроз інформаційного середовища, наскільки в неї розвинені особистісні якості: психологічна стійкость, сила власних переконань, сила волі, критичне мислення. Однак, можна сказати, що несформована дитяча особистість, в силу її психічних особливостей, є найбільш уразливою до таких впливів.

Під **шкідливою** ми розуміємо інформацію, яка здатна негативно вплинути на особистість людини, її психіку, на прийняття нею рішень, загалом на поведінкові моделі та зміщувати ціннісно-орієнтаційні настанови в бік негативно оцінюваних у соціумі. Загалом шкідлива інформація, особливо у

випадку дитини чи молодої людини, може нанести шкоду людині як цілісній особистості, що формується. Загроза шкідливої інформації, в основному, лежить не в площині фізичної шкоди, а в площині психологічного впливу на ціннісні орієнтири і самовизначення особистості у соціумі.

Отже, можемо дати визначення інформаційної безпеки особистості дитини. Основною відмінністю є те, що процес формування особистості у них ще не є закінченим, і саме вплив інформації, інформаційного середовища на формування даної особистості є в даній постановці питання вирішальним. Під інформаційною безпекою особистості, що формується, ми будемо розуміти, з одного боку, стан захищеності її життєво важливих інтересів, а з іншого – процес набуття особистістю таких якостей (вольових, інтелектуальних, емоційних), за наявності яких ніякі інформаційні впливи на неї неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху її стійкого прогресивного розвитку. Нове розуміння інформаційної безпеки вимагає переосмислення ролі освіти в процесі виховання нового покоління, здатного адекватно вписатися в новий інформаційний світ. Саме педагог, вчитель повинен стати основною ланкою у системі формування захисту молодої особистості від негативних інформаційних впливів. Потребують більш детальної розробки такі аспекти захисту особистості, що формується: правові, психологічні, педагогічні.

Зауважимо, що оскільки людина визначається найбільшою цінністю педагогіки гуманізму, то й інформаційно-психологічна безпека учнів є основною домінантою інформаційної безпеки особистості.

Розглянемо докладніше, які види загроз породжує новітній інформаційний простір для людини. Хоча найбільш серйозні небезпеки підстерігають наших дітей за межами моніторів, існує чимало серйозних ризиків, з якими діти зіштовхуються онлайн. Можемо сказати, що існує настільки великий спектр загроз для дітей і підлітків, що вони вимагають класифікації. Виходячи з аналізу [42], виділимо такі види загроз:

1) Загрози для особистісної безпеки

- Загроза ознайомлення з матеріалами небажаного змісту(порнографія, ненормативна лексика, суіцидального характеру, сектантські, расистські та ненависницькі, вибухові речовини, хакерські сайти)
- Загроза отримання недостовірної інформації
- Загроза залежностей (комп'ютерної, ігрової, Інтернет і т.ін.)
- Загроза спілкування з небезпечними людьми (шахраями, збоченцями , гриферами і т.ін)
- Загрози вчинення протиправних дій (хакерство, порушення авторських прав і т.ін.)

2) Загрози витоку персональної інформації
   - Загроза розголошення конфіденційних даних (фамілії, імені, адреси, номерів кредитних карток, телефону і т.ін).
3) Загрози для персональних комп'ютерів
   - Загроза проникнення вірусів, черв'яків
   - Загроза завантаження шкідливого активного коду
   - Загроза завантаження програм з прихованими функціями: троянів, клавіатурних шпигунів і т.ін.

Основні методи попередження доступу учнів до небажаного змісту. Контент-фільтри.

Основні види небажаних Інтернет-ресурсів

Інтернет є могутнім інструментом навчання. Однак, окрім корисної інформації, учні можуть зустрітися з небажаним контентом. Наприклад, одержуючи доступ до невідповідної інформації на сайтах, присвячених злочинній діяльності або заходячи на сайти, що піддають ризикові їхню конфіденційність. Хоча нашу заклопотаність, у першу чергу, викликає порнографічний і інший сексуальний контент, існують інші види неприйнятної доступної інформації, що може бути наджвичайно шкідливою для наших дітей. Останнє можна розділити на дві групи:

Заборонений контент для будь-якого віку та небажаний для дітей та підлітків. До ресурсів першого роду відносяться:

- Сайти з дитячою порнографією.
- Сайти терористів.
- Сайти, що розпалюють національну та расову ворожнечу.

До сайтів небажаних для дітей (крім вище згаданих) відносяться ті, які діти не повинні відвідувати за віковим обмеженням:

- Жорстокі ігри.
- Он-лайнові казино.
- Порнографія.
- Сайти, що пропагують насилля.
- Сайти сексуальних меншин.
- Сайти магазинів інтим-послуг.

Наявність у внутрішній мережі навчального закладу подібної інформації може викликати не лише претензії до учнів, які подібний контент скачують на робочу станцію мережі, але й карне переслідування адміністрації школи, яка допустила зберігання подібних матеріалів.

Відмітимо, що небажаним контентом може являтися також той, який відволікає дітей від учбового процесу. Діти можуть замість виконання навчального завдання в Мережі Інтернет, займатися переглядом дозволених матеріалів, але таких, що не мають безпосереднього відношення до учбового процесу.

Види контент фільтрації.

Проблема доступу дітей до небажаного змісту не може бути вирішена єдиним методом, а сукупністю програмних, виховних та організаційних заходів. Розглянемо основні з них:

Контент-фільтр – це система, що блокує доступ до небажаних ресурсів Інтернету, виходячи з тих або інших критеріїв. Контент фільтри можуть бути реалізовані в різних програмних комплексів або як самостійний програмний продукт. Наприклад, в складі мережних екранів чи проксі-серверів. Мережні екрани призначені для обмеження доступу між різними мережами, вони перевіряють весь трафік, що минають їх, і блокують заборонений.

Обрані сайти – заздалегідь строго визначається сукупність сайтів, до яких буде дозволений доступ дітей. Найчастіше використовується при неможливості прямого доступу НКК до мережі Інтернет.

Дитячі пошукові машини – це такі, що створені на базі існуючих пошукових машин спеціально для школярів і здійснюють фільтрацію посилань, що видаються користувачеві виходячи з вікових обмежень.

На базі Гуглу вчителі можуть створювати свої власні тематичні пошукові машини для того, щоб школярі, не "перелопачували" весь Інтернет у пошуку необхідної інформації. Будь-які користувачі, зареєстровані в офісі Гуглу, можуть колективно редагувати і поліпшувати ці пошукові машини.

У такий спосіб може бути вирішена проблема захисту школярів від нерелевантної інформації, яку вони можуть одержати, направляючи запити в пошукові машини "загального користування".

Інші методи захисту неповнолітніх користувачів.

Спостереження за використанням чатів. Використання чату в навчальних цілях завжди повинне проводитися під спостереженням учителя.

Спеціально набудована система електронної пошти. Це поштовий сервер шкільного призначення з налаштованими обмеженнями щодо того, кому і як можна відправляти електронні повідомлення. Школи можуть обмежити поштовий зв'язок тільки внутрішніми користувачами, а зовнішній дозволяти винятково через учителя. Деяким учням може бути дозволено, посилати пошту на зовнішні адреси, але тільки за заздалегідь визначеним їх списком.

Використання систем спостереження. Для моніторингу найкраще використовувати програми, які дозволяють спостерігати за діями учнів з учительського комп’ютера. Обов’язковим є ведення журналів, що протоколюють дії дітей в Інтернеті.

Проблема проникнення/витоку контенту з навчального закладу. Трафікоємні процедури

Дотепер ми говорили про те, що в навчальному закладі є проблема проникнення небажаного контенту усередину навчальної мережі. Але існує також проблема

витоку контенту. У даному випадку, по-перше, мова йде про витік приватних персональних даних. У сучасному суспільстві існує проблема викрадення дітей, сексуальні домагання і ін. Тому особиста інформація про дитину (її фотографія, розклад уроків, e-mail, телефон) не повинні вивішуватися в Мережі для вільного доступу.

При розміщенні фотографій у Мережі (наприклад, на шкільному Web-сайті) бажано розміщати фотографії дітей тільки за згодою батьків або тільки групові. Не варто вказувати імена дітей і іншу особисту інформацію.

Друга проблема – це розсилання поштою або розміщення на шкільному (або іншому) сайті забороненого контенту. Розсилання піратського ПО, порнографії і т.п.

Небажаний контент потрапляє в мережу навчального закладу переважно по двох каналах: через Web-трафік і через поштовий трафік.

Проблема фільтрації поштового трафіку широко відома як проблема спаму. У якості спама можуть поширюватися повідомлення образливого характеру, заклики до насильства і т.п. Крім усіх перерахованих вище проблем, спам до того ж генерує зайвий трафік, відволікає користувачів.

Звичайно, важливим є запобігання розповсюдженню та вилучення подібного контенту з flash-нагромаджувачів, CD, DVD дисків та жорстких дисків НКК.

Трафікоємні процедури – скачування відеофільмів, музики, файлових архівів програмного забезпечення ведуть до різкого збільшення трафіку, що може сповільнювати роботу мережі і збільшувати витрати на оплату трафіку. Більшість програм, що блокують доступ до заборонених Web-сайтів, забезпечують і контроль трафікоємних процедур.

Насамперед , варто сказати, що проблема захисту від шкідливого контенту далеко не тільки шкільна проблема. Використання інтернету співробітниками або учнями, не зв'язане з навчальною або службовою діяльністю, одержало назву "киберслэкинг" (від англ. cyberslacking - дослівно на російській "кибербездельничание").

Навчальні заклади аж ніяк не першими стали намагатися вирішити проблему фільтрації Інтернету. Це, з одного боку, говорить про те, що проблема глобальна

і просто не вирішується, а з іншої, що навчальним закладам у ряді випадків можуть підійти рішення, створені для організацій широкого профілю. Відзначимо також, що віруси, трояни, шпигунські програми й інші шкідливі коди теж можуть легко передаватися через Web.

Боротьба з небажаним контентом.

У боротьбі можна виділити організаційні заходи (призначення відповідальних осіб, створення режиму доступу в комп'ютерний клас, доведення до відома учнів норм поводження у Мережі, відповідальності за протиправні дії і т.п.) і технічні. До технічних заходів відносяться фільтрація трафіку і моніторинг дій учнів.

Наявність моніторингу (навіть без фільтрації) уже може стати ефективним заходом. Якщо учень буде знати, що за його діями (усіма відвідуваннями ведеться постійний моніторинг і всі його дії записуються в log-файлах із вказівкою того, хто, коли і що відвідував), то це вже в істотній мері обмежить імовірність відвідування небажаних сайтів.

Варіанти фільтрації контенту.

Контент може фільтруватися на рівні провайдеру, на рівні шлюзу в Інтернет мережі, що захищається, і на рівні клієнтської станції.

Фільтрація може бути побудована на основі зовнішньої оновлюваної бази даних заборонених ресурсів і може бути побудована на основі локальної програми, що діє по власних принципах фільтрації ("чорні", "білі" списки, ключові слова і т.п.).

При цьому в принципі фільтрація може бути побудована за принципом:

1. "Забороняємо все, крім того, що можна" 2. "Можна все, крім того, що заборонено"

Звичайно, реалізувати фільтрацію за принципом "Забороняємо все, крім того, що можна", побудувати досить просто, подібна форма, можливо, має сенс для молодших школярів, але в цьому випадку Інтернет утрачає багато своїх функцій. Другий варіант вимагає побудови і постійного оновлення величезної бази даних (підтримувати її повинен провайдер сервісу), що постійно поповнює базу забороненого контенту.

Для повноцінної реалізації другого виду фільтрації необхідно проіндексувати мільярди Web-сторінок, і це під силу тільки великим провайдерам подібного сервісу, наприклад, таким як iSS, Proventia Web Filter. Чим більше база, тим якісніше і дорожче рішення.

Складності фільтрації контенту в школах.

Щодня в Інтернеті з'являються тисячі нових сайтів, тому, навіть використовуючи відновлення баз даних з небажаними ресурсами, домогтися 100%-ної фільтрації неможливо. Окрема проблема - це недостатня фільтрація російськомовного та україномовного контенту західними продуктами. Можливі помилки, коли фільтр буде відсівати сайти корисного змісту. Загалом, чим більш інтелектуальний фільтр і чим більша база, на яку він спирається, тим дорожче рішення і тим воно менш доступне для шкіл.

Часто в школах встановлено різне комп'ютерне устаткування і програмні продукти фільтрації контенту (Web і e-mail), що працюють на різних платформах. Адміністратори в школах мають різний досвід роботи з комп'ютерами, і навіть непрофесіонал повинен мати можливість створювати і підтримувати політику фільтрації. Освітній процес включає безліч різних областей науки, і фільтрація повинна бути всеосяжною, що набудовується, а також забезпечувати захист від новітніх погроз.

Моніторинг Інтернет активності.

Моніторинг і протоколювання - це в багатьох випадках перший і найважливіший крок у контролюванні Інтернет доступу. Дана функція наочно показує серфінг-профіль користувача. Учитель може перевірити, де знаходився учень, що переглядав, у який час і як довго. Моніторинг дає швидку і точну картину Web серфінгу. Дані про Інтернет-активність захищені криптографічно і зберігаються в недоступному для неавторизованого перегляду вигляді. Будь-який відвіданий ресурс може бути переглянутий, і згодом доданий у список дозволених або заборонених сайтів. Звіти моніторингу (Monitoring Reports) чітко показують, які Web-сторінки відвідувалися, час візиту, Web-адресу, і іншу інформацію.

Комплекс заходів для захисту учнів від загроз ІКТ

Організаційні, програмно-апаратні та виховні заходи. Правила інформаційної безпеки для учнів

Політика інформаційної безпеки по відношенню до користувачів-учнів повинна бути вироблена у кожному навчальному закладі і конкретизована у вигляді правил з ІБ (див. Додаток С). Вкажемо, що основними *принципами політики безпеки* повинні бути: послідовність, обов'язковість, карність.

Необхідні заходи захисту НКК від навмисних та ненавмисних дій учнів: контроль з боку вчителя, персоналізація та обмеження доступу до критичних ресурсів, контроль і реагування на НСД програмних засобів захисту, реагування персоналу, вчителя і застосування відповідних виховних заходів.

Основна мета політики безпеки НКК – це забезпечення виконання учнями-користувачами правил інформаційної безпеки, які унеможливлюють чи зводять до мінімуму шкоду, яку вони можуть спричинити своїми діями, навмисними чи ненавмисними, програмному компоненту НКК. Ця мета реалізується організаційними, програмно-апаратними та виховними заходами.

Комплексний підхід до інформаційної безпеки вимагає поєднання таких заходів по відношенню до користувачів-учнів: контроль з боку вчителя (перш за все візуальний), контроль і реагування на несанкціоновані дії (НСД) програмних засобів захисту, реагування персоналу, вчителя при виникненні НДС і застосування відповідних виховних заходів. Під несанкціонованими, ми будемо розуміти дії, що заборонені політикою безпеки і конкретизовані у правилах користувачів.

До **організаційних** заходів належать перш за все розробка, впровадження та контроль за виконанням політики безпеки СІБ НКК по відношенню до користувачів-учнів. Контроль за виконанням покладено на вчителів та обслуговуючий персонал.

Особливої уваги потребує проблема доступу дітей до Інтернету.

Правила щодо доступу в Інтернет, встановлені в школі, повинні бути формалізовані, тобто мати вигляд обов'язкового документа. Відповідно до світового досвіду, можливою формою цього документу є підписана учнями, їхніми батьками і вчителями письмова угода, що визначає порядок використання

Інтернету - тобто формалізовані правила для Мережі набувають рис "колективного договору". Ці правила повинні обов’язково включати інструкцію з публікації в Інтернету особистих даних учнів, їхніх фотографій, аудіо- і відеоматеріалів і тощо.

Частина правил політики безпеки, що стосується доступу учнів до Інтернету, повинна бути повідомлена перед початком відповідних занять. Найкращий варіант - коли учитель виконує роль не доглядача, а консультанта. Цього можна спробувати досягти, провівши бесіду з дітьми, де їм буде докладно розказано про небезпеки, що існують в Інтернеті, необхідно навчити їх правильно виходити з неприємних ситуацій. Інструкції з безпечного використання Інтернету повинні бути роз'яснені учнем до того, як вони одержать доступ до Інтернету або їм нададуть індивідуальні адреси електронної пошти. На закінчення бесіди поясніть обмеження на використання Інтернету й обговоріть їх з дітьми. Спільно збільшити безпеку використання Мережі набагато простіше.

Програмно-апаратні засоби прийнятої політики безпеки реалізуються через систему управління (контролю) доступу користувачів до ресурсів, яка включає ідентифікацію та автентифікацію користувачів, управління (контроль) доступу до ресурсів, протоколювання та аудит дій користувачів. Програмно-апаратні засоби повинні гарантувати захищеність критично важливих компонентів ПЗ НКК від несанкціонованих і помилкових дій користувачів. В правилах розмежування доступу необхідно заборонити доступ цих користувачів до системних областей диску, а також заборонити модифікацію ними програмного забезпечення, навчальної та іншої важливої інформації. Рекомендується забезпечити доступ в Інтернет тільки з тих комп'ютерів, що постійно знаходяться в полі зору вчителя. Також варто використовувати програми, що дають можливість відображати вміст екранів усіх комп'ютерів на моніторі вчителя і тим самим дозволяють стежити за діяльністю учнів.

Основними в реалізації політики безпеки НКК є *виховні* заходи. Оскільки вони використовуються як для попередження НСД, так і для впливу на порушників правил безпеки з метою їх перевиховання. Дуже важливо встановити правила покарання тих, хто зловживає доступом; порушення можуть бути і не настільки

значними, але повинні бути обговорені, а за серйозні провини повинні бути передбачені серйозні заходи покарання.

Не слід забувати, що основним завданням школи є виховання майбутнього громадянина. З кожним роком зростає кількість працівників, які тим чи іншим чином використовують у своїй повсякденній роботі інформаційні технології. Також, безсумнівно, зростає роль інформаційної безпеки як неодмінної складової будь-якої інформаційної системи. Найуразливішою ланкою будь-якої системи безпеки були і будуть люди. Тому майбутнього кваліфікованого працівника неможливо уявити без необхідних базових знань з інформаційної безпеки. Важливу роль тут грає не лише навчання, але й виховання, оскільки лише воно забезпечує засвоєння морально-етичних норм в галузі інформаційних технологій.

Політика безпеки роботи з користувачами-учнями, з педагогічної точки зору, повинна сприяти вихованню учнів, зокрема преміювати (розширювати права) за хорошу поведінку і «карати» за погану. Основні методи, які використовують для безумовного виконання політики безпеки користувачами є інформування, контроль, спонукання, попередження, тимчасова заборона (відмова в доступі), зменшення наданих прав і привілеїв (як користувача НКК) та інші.

Головна мета виховних заходів є усвідомлення учнями відповідальності за свої дії навіть у «віртуальному» середовищі, засвоєння етичних норм поводження в цьому середовищі, результатом чого є формування в учнів компетентності з інформаційної безпеки.

Питання інформаційної безпеки в шкільному курсі інформатики.

В шкільному курсі інформатики є достатньо резервів для внесення основних питань інформаційної безпеки до змісту навчального курсу основи інформатики. Так, пропонується доповнити шкільний курс такими питаннями:

1) Інформація в Інтернет: чи завжди вона є правдивою?
2) Поняття про загрози. Загрози для особистості в Інтернеті.
3) Поняття про кіберзалежності і їх основні ознаки.
4) Основні закони в сфері захисту інформації.

5) Основні поняття про захист інформації, захист персональних даних. Права власності в Інтернеті.
6) Основні правила етичного спілкування в Інтернеті. Питання комп'ютерної етики.
7) Основи безпечної роботи в мережі Інтернет. Поняття про між- мережний екран та захист ПК.

Просвіта батьків з питань інформаційної безпеки

Враховуючи розширення змісту діяльності вчителя інформатики, необхідності розвитку його компетентності, що стосується наданням інформаційно-консультаційних послуг учителям, батькам, учням, а також широкого розповсюдження домашніх ПК, слід розвивати їхнє уміння переконувати батьків у необхідності захисту дітей від шкідливої інформації. З відомостями про небезпеки онлайнового середовища необхідно ознайомити не лише учнів, але й батьків. До того ж одним з основних завдань вчителя інформатики є потреба навчити дітей і підлітків уникати небезпек Мережі. Як утримати учнів від доступу до веб-сайтів, що містить непристойні матеріали, і від контакту з особами, що представляють для них загрозу? Щоб захистити учнів і переконати в необхідності цього їхніх батьків, необхідно прийняти заходи, спрямовані на запобігання будь-яких несанкціонованих вторгнень в інформаційний простір школи. Варто одержати згоду батьків на прийняття рішень, що можуть викликати ризик для дітей, і спробувати зробити їх учасниками прийняття рішень. Для цього учителі повинні розповісти батькам, у яких цілях вони використовують Інтернет у школі, які можуть бути небезпеки і як вони контролюють ризики. Повідомлення повинне бути ясним і чітким (закінченим), і викладати усю важливу інформацію так, що навіть самий необізнаний у комп'ютерному відношенні батько міг би її зрозуміти.

Необхідність консультації батьків про можливості програмного забезпечення і технічної реалізації, не допущення доступу дітей до шкідливої інформації через домашнє ПК вимагає отримання майбутніми вчителями компетенції з питань інформаційної безпеки.

Рекомендації по захисту дітей від доступу до інформації, що не сумісна з завданнями навчання

Знаходячись в комп'ютерному класі з групою учнів, що досліджують Інтернет, - непроста задача. У Вас виникають сумніви, чи проводять вони свій час з користю або дарма його витрачають? От деякі дії, що може почати вчитель, щоб збільшити безпеку учнів в Інтернеті.

1) Розберіться в основних питаннях безпеки Інтернету, перш ніж ввійти в клас.
2) Упевніться, що Ви, по можливості, інформовані про ті функції, що виконують шкільні комп'ютери.
3) Довідайтеся, чи встановлені на шкільних комп'ютерах фільтри або програмне забезпечення для захисту дітей; якщо встановлені, з'ясуєте, яке саме.
4) На початку уроку, коли комп'ютери ще не включені, обговоріть з дітьми, що можна чекати від дослідження Інтернету.
5) Нагадайте учням про техніку безпеки і правила користування Інтернетуом.
6) Не дозволяйте учням блукати по Мережі - вони можуть потрапити в небезпечну зону; виберіть декілька сайтів, що викликають інтерес, і зосередьте на них увагу дітей.
7) Стежте за тими учням, що швидко виключають монітори, сміючись над побаченим на екрані, групуються навколо одного комп'ютера або виглядають збентеженими - це попереджувальні знаки потенційної неприємності.
8) Винагородіть тих учнів, що поводяться відповідально в Інтернеті; зробіть їх прикладом наслідування для іншої частини класу.
9) З амість того щоб забороняти улюблені заняття учнів в Інтернеті (чати, електронна переписка), досліджуйте можливості використання цих технологій для розширення навчання й одержання знань.[44]

Організаційні та процедурні заходи з інформаційної безпеки. Програмно-апаратні засоби

Організація роботи кабінету інформатики з урахуванням заходів з інформаційної безпеки.

Окремо взяті технічні чи програмні засоби не можуть діяти без організованої і спрямованої діяльності всіх учасників інформаційних взаємодій, без регламентації, розробки і впровадження правил інформаційної безпеки (політики безпеки), постійного керівництва обслуговуючим персоналом і керуванням системою безпеки НКК. «Всі зусилля по забезпеченню внутрішньої безпеки комп'ютерних систем фокусуються на створенні надійних і комфортних механізмів регламентації дій всіх законних користувачів і обслуговуючого персоналу та присилування до безумовного виконання встановленого в навчальному закладі режиму доступу до ресурсів системи. Організаційні заходи необхідні для забезпечення ефективного виконання інших заходів захисту в частині, що стосується регламентації дій людей». [12, с.31] Оскільки, на даному етапі інформатизації загальноосвітніх навчальних закладів є труднощі з виділенням коштів на закупівлю чи оновлення саме програмно-апаратних засобів, то для захисту НКК можемо використовувати лише наявні їх можливості. Тому найбільш перспективним вбачається максимальне використання організаційних та виховних заходів для підвищення ефективності СІБ НКК, впровадження яких не вимагає витрати додаткових коштів. Саме комплексний підхід до інформаційної безпеки НКК, усвідомлення необхідності таких заходів на всіх рівнях управління освітою, навчанням та підвищенням компетентності обслуговуючого персоналу та вчителів інформатики, є запорукою успішної реалізації вимог висунутих до надійності програмної складової НКК.

Методи оптимізації і підвищення надійності роботи КІТК.

Робота кабінету інформатики має свою специфіку порівняно з іншими лабораторіями та кабінетами школи. Для того щоб підвищити ефективність

роботи обслуговуючого персоналу, необхідно розробити нові підходи до організації роботи НКК. Використання цих підходів дозволить застосувати методи інформаційної безпеки для підвищення надійності програмного компоненту НКК, зменшити витрати робочого часу на відновлення його працездатності під час програмних збоїв, підвищить захищеність ПЗ НКК.

Серед основних методів, що використовуються для підвищення захищеності і відновлюваності програмної складової інформаційної системи (ІС), є резервування та періодична перевірка його цілісності. Ці методи можуть реалізовуватися системними утилітами, що входять до складу операційної системи або іншими програмами, наприклад, антивірусними. При першому запуску цих програм створюється база відповідних значень незмінних файлів, зокрема системних (наприклад, контрольних сум); при повторному запуску здійснюється перевірка всіх незмінних файлів на модифікацію. Якщо така модифікація здійснена, то це може свідчити про наявність вірусів або може бути результатом дій недосвідчених користувачів. Програми-ревізори, як правило, можуть відновлювати пошкоджені файли. Однак, якщо ці пошкодження достатньо значні чи зачіпають критично важливі файли операційної системи, то для їх відновлення необхідно мати резервну копію системної області жорсткого диску. Системні утиліти, що створюють архіви-образи логічних дисків допомагають швидко відновити роботу пошкодженої операційної системи не перевстановлюючи її. Необхідною умовою використання цих засобів є чітке планування і виконання регламентних робіт персоналом. Наприклад, образ системного диску обов’язково робиться, як мінімум раз на навчальний рік після відповідних підготовчих робіт, а перевірка файлів на цілісність має проводитися за визначеним періодом.

Резервування.

Резервування є основним методом боротьби із наслідками збоїв та підвищення надійності ІС. Воно буває як програмне так і апаратне. В умовах школи мова може йти лише про резервування системного програмного забезпечення, та іншої важливої інформації. Пропонується проводити резервування системної області жорсткого диску принаймні на початку кожного навчального року.

Питання про необхідну кількість резервних копій (чи така копія робиться для кожного комп'ютера учня окремо чи одна для всіх КУ) вирішується проведенням уніфікації. Див. далі.

Уніфікація

Як правило, програмно-апаратне забезпечення кожного робочого місця учня є стандартним. Тобто на них встановлено однакові операційні системи, інші прикладні програми. Однак під часом експлуатації дана ідентичність щезає, змінившись різнорідністю, яка збільшує затрати часу на обслуговування КУ.
Для того щоб забезпечити ідентичність КУ під час експлуатації, пропонуються такі заходи.

Первинна уніфікація.

Якщо апаратні складові КУ є однаковими чи з незначними відмінностями, то можливе створення єдиної резервної копії для всіх комп'ютерів учнів. Для цього на одній машині перевстановлюється все програмне забезпечення, виконуються відповідні налаштування, а потім на базі його створюється резервна копія системного розділу диску. На базі цієї копії може бути відновлена працездатність будь-якого комп'ютера учня.

Вторинна уніфікація.

Якщо переустановлення програмного забезпечення повністю «з нуля» за якихось причин є неможливою, то проводиться створення резервної копії на кожному КУ(після відповідних підготовчих робіт: повної перевірки на віруси, дефрагментації і т.ін.). Цей спосіб вимагає збереження резервних копій залежно від кількості робочих місць.

Управління СІБ НКК та контроль за виконанням правил.

Системні утиліти, які забезпечують спостереження за роботою на комплекті учня (КУ) і керування КУ з комплекту вчителя (КВ), можуть бути використані як засоби централізованого управління безпекою. Вони дозволяють з одного комп'ютера виконувати більшість регламентних робіт СІБ (наприклад, запускати оновлення антивірусних баз, антивірусну перевірку жорстких дисків,

перевірку програмного забезпечення (ПЗ) на цілісність і т. ін.). Деякі програми містять внутрішній планувальник або ж можна скористатися планувальником операційної системи (ОС) для запуску програм СІБ, що економить час обслуговуючого персоналу.

Для чіткої організації робіт і підвищення надійності СІБ необхідно розробити і впровадити цілий ряд задокументованих процедур, які визначають обов'язки, відповідальність персоналу при виконані регламентованих періодичних процедур, перетбачити реакцію і дії у випадку інцидентів порушення правил безпеки та захисту НКК. Згідно визначення, інцидент – це будь-яке порушення правил інформаційної безпеки, всановлених в навчальному закладі. До таких інцидентів належать:

- Програмно-апаратний збій чи відмова, які викликані:
- Несанкціонованими чи помилковими діями користувачів;
- Проникненням вірусу у систему (чи інших АШК);
- Відмовою чи поломкою обладнання.
- Протоколювання, виявлення частоти і видів даних інцидентів.

Останній пункт необхідний, для прийняття обґрунтованого рішення про необхідну модифікацію СІБ НКК.

Документи (журнали обліку). Всі документи можуть вестися як електронному, так і в паперовому вигляді.

Журнал обліку програмно-апаратних збоїв та відмов.

Форма №1.

Дата	№ комп'ютера	Опис проблем, що виникли	Дата виконання	Опис виконаних дій та причин проблеми

Журнал може заповнюватися вчителями, що проводять уроки в НКК, а виконуватися лаборантом чи іншими відповідальними особами, контроль за виконанням лежить на зав.лабораторією.

Журнал самостійної роботи учнів в КІІКТ.

Форма №2.

Дата	Час початку роботи	№ комп'ютера	Які завдання виконувалися	Час закінчення роботи

Організаційні основи антивірусного захисту НКК.

Для ефективного захисту НКК необхідна не лише наявність антивірусного пакету на кожному комп'ютері, але й правильна організація роботи по антивірусному захисту.

До цього можемо включити такі пункти:

- Обов'язкова наявність антивірусу-резидента в оперативній пам'яті.
- Неможливість зміни налаштувань антивірусного захисту користувачами.
- Обов'язкова перевірка всіх переносних носіїв.
- Обов'язкове сканування і лікування всіх жорстких дисків.

Якнайчастіше встановлення оновлень ОС та антивірусних баз, що ліквідує знайдені уразливості.

При організації антивірусного захисту необхідно передбачити періодичність і дати антивірусної перевірки та оновлення баз. Автоматизація цього процесу вимагає залучення програми-планувальника (наприклад, Scheduled Tasks Explorer в Windows XP, Windows Server 2003) для перевірок. Періодичність антивірусних заходів встановлюється календарним планом регламентних робіт, що є обов'язковим для виконання.

При виборі та налаштуванні програмного антивірусного комплексу для НКК, корисно брати до уваги такі міркування.

- Можливості оновлення антивірусних баз: частоту, простоту встановлення і можливість оновлення по мережі.
- Вимогливість до системних ресурсів.
- Можливості віддаленого керування та сканування по мережі.
- Наявність вбудованого планувальника.
- Надійність у роботі і простота експлуатації.

- Необхідність обов’язкової перевірки з’ємних носіїв.

Якщо ми розглянемо мал. 2 (с.25), то побачимо, що основними «входами» для шкідливого ПЗ, до якого належать віруси, черв’яки, трояни, є з’ємні носії та мережа Інтернет. Якщо з взяти до уваги наявність локальної мережі, то будь-який вірус, проникнувши в мережу, буде розповсюджений по всіх робочих станціях. Для попередження зараження необхідно ввести строгі правила антивірусного захисту.

На кожній робочій станції НКК має бути встановлений антивірусний пакет, який проводить сканування на віруси в реальному часі. Всі системи, що підключені до мережі організації, повинні підлягати періодичній загальній перевірці, щоб виявляти заражені вірусами ОС та допоміжне програмне забезпечення.

Перевірка на віруси жорстких дисків та оновлення антивірусних баз має проводиться з визначеним періодом.

Обов’язок користувачів полягає у сприянні заходам антивірусного захисту. Користувачі повинні перевіряти всі дані при кожному їх завантаженні з будь-якого джерела. Також необхідно перевіряти будь-який з’ємний носій перед його відкриттям на наявність вірусів. Користувачі повинні сприяти оновленню антивірусних баз, а також ніколи не перешкоджати та не вивантажувати з оперативної пам’яті антивірусні програми.

На сервері Інтернету навчального закладу повинен бути встановлений антивірусний пакет, що проводить сканування вхідного трафіку на наявність вірусів та шпигунських програм. Виконання активного вмісту web-сторінок має бути обмежено. Завантаження будь-якого програмного забезпечення з Інтернету користувачам заборонено.

Навчальний заклад повинен проводити сканування кожного повідомлення електронної пошти на наявність вірусів, черв’яків і інших файлів, що виконуються, які становлять загрозу безпеці. Інфікована електронна пошта не повинна доставлятися користувачу.

Сторонні данні чи ПЗ повинні спочатку завантажуватися в ізольовану систему, на якій можна проводити опробування та тестування на наявність вірусів,

помилок, закладок і інших проблем (наприклад проблем сумісності) при завантаженні цих даних чи встановленні цього ПЗ на інші системи в мережі.

Програмно-апаратні засоби захисту КІКТ.

Переходячи до програмно-апаратного рівня реалізації системи захисту НКК, ми розглянемо основні напрямки його захисту і особливості програмного забезпечення, які ці функції реалізують.

«Найбільш значимими для захисту автоматизованих систем є програмні засоби захисту, що дозволяють створювати модель захищеної автоматизованої системи з побудовою правил розмежування доступу, централізовано управляти процесами захисту, інтегрувати різні механізми і засоби захисту в єдину систему».[30, с.10].

Однак саме програмна частина ННК є найбільш уразливою до помилкових дій великої кількості недосвідчених користувачів і саме вона, поряд з апаратною, створює передумови безперебійної роботи всього комплексу. Тобто, об'єктом захисту виступає не стільки інформація, в класичному розумінні інформаційної безпеки, скільки асоційовані з нею інформаційні ресурси.

Аналіз наявного програмно-апаратного забезпечення.

Виходячи з нормативних документів, а також реалій сьогодення, можемо зазначити, що програмне забезпечення НКК є недостатнім для реалізації СІБ у повному обсязі. До того ж в багатьох школах є застарілим не лише обладнання, а й програмне забезпечення. Тому, розробляючи алгоритм створення СІБ НКК, будемо враховувати значну різницю в програмному забезпеченні, а також неможливість його негайного оновлення.

Проведений аналіз наявного у школах ПЗ дає можливість виділити такі його класи:

- Windows 95/98/Me
- Windows 2000/ XP

Наприклад, ось що говорить Крисін А.В. [19, с.38], порівнюючи цих два класи.

«Не секрет, що в Windows 2000/ NT/XP існує ціла система безпеки, яка дозволяє захистити ваш комп'ютер майже від будь-якої несанкціонованої дії. На жаль,

багато користувачів вимушені працювати під Windows 95/98/Me, які є абсолютно беззахисні. Особливо страждають від цього комп’ютери в учбових закладах, доступ до яких зовсім не обмежений».

Щодо лінійки Windows, то з кожною версією вбудовані засоби захисту і безпечність ОС зростають. Ми надалі будемо орієнтуватися на однорангову мережу, побудовану на базі Windows XP Pro, оскільки такі вимоги не тільки зазначені в нормативних документах, але й є найбільш розповсюдженими у даний час.

При побудові СІБ, ми повинні, в основному, спиратися на можливості ОС, то для кожного варіанту опишемо відповідну **стратегію** захисту. Стратегія захисту складається з стратегії адміністрування користувачів (яка залежить від можливостей ОС) та програмно-апаратних засобів захисту.

Для цього опишемо більш детально стратегію безпеки Windows 2000/XP, використавши матеріали з книжки Крисіна А.В. [19, с.56-65].

Модель безпеки Windows 2000/XP заснована на поняттях аутентифікації й авторизації. У Windows 2000/XP також існують технології шифрування, що захищають конфіденційні дані на диску й у мережі:наприклад. EFS (Encrypting File System) - технологія відкритого ключа.

Windows XP. Аутентифікація.

Реєструючи на комп'ютері для одержання доступу до ресурсів локального комп'ютера або мережі, користувач повинен увести своє ім'я і пароль. У Windows 2000/XP можлива єдина реєстрація для доступу до всіх мережних ресурсів. Таким чином, користувач може ввійти в систему з клієнтського комп'ютера по єдиному паролі або смарт-карті й одержати доступ до інших комп'ютерів домену без повторного введення ідентифікаційних даних.

Головний протокол безпеки в доменах Windows 2000 – Kerberos 5. Для аутентифікації на серверах під керуванням Windows NT 4.0 і доступу до ресурсів доменів Windows NT, клієнти Windows 2000/XP використовують протокол NTLM. Комп'ютери з Windows 2000/XP, що не належать до домену, також застосовують для аутентификации протокол NTLM.

Використовуючи Windows 2000/XP у мережі з активним каталогом (Active Directory), можна керувати безпекою реєстрації за допомогою параметрів політики груп, наприклад, обмежувати доступ до комп'ютерів і примусово закінчувати сеанси роботи користувачів через заданий час. Можна застосовувати попередньо сконфігуровані шаблони безпеки, що відповідають вимогам безпеки даної робочої станції або мережі. Шаблони являють собою файли з попередньо сконфігурованими параметрами безпеки, які можна застосовувати на локальному комп'ютері або імпортувати у групові політики активного каталогу. Ці шаблони використовуються в незмінному виді або налаштовуються для визначених уразливостей.

Windows XP. Авторизація.

Авторизація дозволяє контролювати доступ користувачів до ресурсів. Застосування списків керування доступом (access control list, ACL) і прав доступу NTFS гарантує, що користувач одержить доступ тільки до потрібних йому ресурсів, наприклад, до файлів, дисків (у тому числі мережних), принтерів і додатків. За допомогою груп безпеки, прав користувачів і прав доступу можна одночасно керувати безпекою як на рівні ресурсів, так і на рівні файлів, папок і прав окремих користувачів.

Windows XP. Групи безпеки.

Групи безпеки спрощують керування доступом до ресурсів. Можна приписувати користувачів до груп безпеки, а потім надавати цим групам права доступу. Можна додавати користувачів до груп безпеки і видаляти їх звідти відповідно до потреб цих користувачів.

Оснащення MMC Computer Management дозволяє створювати облікові записи користувачів і поміщати їх у локальні групи безпеки. Можна надавати користувачам права доступу до файлів і папок і визначати дії, що користувачі можуть виконувати над ними. Можна дозволити і спадкування прав доступу. При цьому права доступу, визначені для каталогу, застосовуються до всіх його підкаталогів і файлів, що знаходиться в них.

Серед груп безпеки, локальних для домену і комп'ютера, існує ряд попередньо сконфігурованих груп, у які можна включати користувачів :

Адміністратори (Administrators) мають повний контроль над локальним комп'ютером і правами на здійснення будь-яких дій. При установці Windows 2000/XP для цієї групи створюється і призначається убудований обліковий запис Адміністратор (Administrator). Коли комп'ютер приєднується до домену, за замовчуванням до групи Адміністратори додається група Адміністратори домену (Domain Administrators).

Досвідчені користувачі (Power Users) мають права на читання і запис файлів не тільки в особистих папках, але і за їхніми межами. Вони можуть установлювати додатки і виконувати багато адміністративних дій.

Користувачі (Users) у відношенні до більшої частини системи мають тільки право на читання. У них є право на читання і запис тільки файлів їх особистих папок. Користувачі не можуть читати дані інших користувачів (якщо вони не знаходяться в загальній папці), установлювати додатка, що вимагають модифікації системних каталогів або реєстру, і виконувати адміністративні дії.

Гості (Guests) можуть реєструватися по убудованому обліковому записі Guest і виконувати обмежений набір дій, у тому числі виключати комп'ютер. Користувачі, що не мають облікового запису на цьому комп'ютері, або користувачі, чиї облікові записи відключені (але не вилучені), можуть зареєструватися на комп'ютері по обліковому записі Guest. Можна встановлювати права доступу для цього облікового запису, що за замовчуванням входить в убудовану групу Guests. За замовчуванням обліковий запис Guest відключений.

Можна сконфігурувати списки керування доступом для груп ресурсів або груп безпеки і в міру необхідності додавати/видаляти з них користувачів або ресурси, що полегшує керування правами доступу і їхній аудит. Можна надати користувачам права на доступ до файлів і папок і вказати дії, які можна виконувати з ними. Можна також дозволити спадкування прав доступу; при цьому вказані права до деякої папки застосовуються і до її підкаталогів і файлів, що знаходиться в них.

Windows XP. Політика груп.

Параметри політики груп дозволяють призначати ресурсам права доступу, а також надавати права доступу користувачам. Це потрібно для того, щоб вимагати запуску визначених додатків тільки в заданому контексті безпеки (тим самим знижуючи ризик впливу на комп'ютер небажаних додатків, наприклад, вірусів) і конфігурувати різні права доступу для безлічі клієнтських комп'ютерів. Можна зконфігурувати права доступу на еталонному комп'ютері, що буде використаний як базовий образ для установки цих прав на інші робочі станції, гарантуючи, таким чином, стандартизоване керування безпекою навіть під час відсутності Active Directory.

Функції аудита дозволяють виявляти спроби відключити або обійти захист ресурсів. Можна задіяти попередньо сконфігуровані шаблони безпеки, що відповідають вимогам безпеки для даної робочої станції або мережі. Шаблони безпеки - це файли з попередньо встановленими параметрами безпеки, що застосовують до локального комп'ютера або імпортують у групові політики активного каталогу (Active Directory). Шаблони безпеки використовуються в незмінному виді або набудовуються у відповідності з визначеними завданнями.

Windows XP. Шифрування.

Шифрована файлова система (EFS) дозволяє користувачам зашифрувати і розшифровувати файли. EFS використовується для захисту файлів користувачів від зловмисників, що можуть одержати несанкціонований фізичний доступ до збережених конфіденційних даних (наприклад, викравши переносної комп'ютер або зовнішній диск).

Користувачі працюють із зашифрованими файлами і папками так само, як і з іншими файлами і папками. Шифрування прозоре. Якщо користувач EFS є особою, що зашифрувала файл або папку, система автоматично розшифровує їх при наступному доступі. Однак для зловмисників зашифровані файли і папки недоступні.

Шифрована файлова система (EFS) забезпечує ядро технології шифрування файлів, що використовуються для збереження шифрованих файлів на томах файлової системи NTFS. Після того як файл або папка зашифровані, з ними

працюють так само, як і з іншими файлами або папками. Шифрування є прозорим для користувача, що зашифрував файл. Це означає, що перед використанням файл не потрібно розшифровувати. Файл можна відкрити і змінювати, як це робиться звичайно. Однак зловмисникові, що намагається одержати доступ до зашифрованих файлів або папок, не зможе це зробити. Зловмисник одержить повідомлення про відмовлення в доступі, якщо він спробує відкрити, скопіювати, перемістити або перейменувати зашифрований файл або папку.

Шифрування і розшифровування файлів виконується установкою властивостей шифрування для папок і файлів, як встановлюються й інші атрибути, наприклад, "тільки читання", "стиснутий" або "схований". Якщо шифрується папка, усі файли і підпапки, створені в зашифрованій папці, автоматично шифруються. Рекомендується використовувати шифрування на рівні папки. Файли і папки можуть також бути зашифровані або розшифровані з допомогою функції командного рядка cipher.

Windows XP. Рекомендації з використання EFS.

Зашифруйте папку "Мої документи", тому що в ній автоматично зберігається більшість документів. Це гарантує шифрування особистих документів за замовчуванням.

Зашифруйте папку Temp, щоб будь-які тимчасові файли, створювані програмами, шифрувалися автоматично. Шифруйте папки замість окремих файлів, щоб тимчасові файли, що створюються програмами-додатками в процесі редагування, також були зашифровані.

За допомогою команди Експорт з об'єкта MMC "Сертифікати", зробіть на гнучкому диску резервні копії сертифіката шифрування файлів і пов’язаного з ним закритого ключа. Зберігаєте гнучкий диск у безпечному місці. Якщо сертифікат шифрування файлів буде загублений (через збій диска або по якій-небудь іншій причині), за допомогою команди імпорт з об'єкта MMC "Сертифікати" сертифікат і пов'язаний з ним закритий ключ можуть бути відновлені з гнучкого диска, а зашифровані файли - відкриті.

Безпека Інтернету.

Очевидно, що можливість виходу у глобальну мережу є важливим і необхідним чинником підвищення ефективності навчального процесу для кожного навчального закладу. Однак, не слід забувати, що це нововведення несе низку загроз.

Зауважимо, що на даний час приблизно 70% шкільних комп'ютерних класів підключенні до Інтернету. Найчастіше це є Dial-Up з'єднання за допомогою телефонної лінії. Таке з'єднання, як правило, використовується для виходу в Інтернет з одного (учительського) комп'ютера. Всі проблеми аналогічні з тими, що виникають при підключення до Інтернету одиничного персонального комп'ютера.

Однак технології не стоять на місці. Тому кількість шкіл для яких є технічно можливою організація колективного доступу до Інтернету, з кожним роком збільшується. Проблеми безпечного колективного доступу до Інтернету ми розглянемо другій частині даного розділу.

Розглянемо основні з них.

Проблема 1. Можливість розголошення даних користувача.

Проблема 2. Вона стосується, на нашу думку, підключення до Інтернету НКК. Робить освітню локальну мережу більш уразливою до віддалених атак, а також є додатковим джерелом проникнення шкідливих програм.

Освітні мережі цілком можуть стати об'єктом ненаправлених атак (наприклад, хакерських), хоча і не завжди містять цінну інформацію. Останнім часом спостерігається тенденція на проведення атак, які захоплюють контроль над віддаленою системою, перетворюючи її на «зомбі». Тобто, можливість використання ресурсів «захопленої» системи є достатнім стимулом для проведення атак хакерами.

Також при доступі неповнолітніх до Інтернету слід враховувати необхідність їхнього захисту від аморальної та іншої шкідливої інформації. Тобто крім проблем адміністрування доступу до Інтернету користувачів-учнів, виникає також необхідність заборони доступу цієї групи користувачів до вищезгаданої інформації.

Основні фактори, що сприяють уразливості освітніх мереж є: застарілість програмного забезпечення, а саме його недостатня оновлювальність в плані ліквідації уразливостей ОС, проблеми з оновленням антивірусних баз, недостатня обізнаність персоналу. Тому, завданням даного розділу вбачається, розглянути освітні мережі з точки зору безпеки підключення до Інтернету, та подати основні теоретичні відомості та практичні рекомендації вчителям інформатики з вищезгаданих питань.

Завдання КСІБ, при наявності підключення НКК до Інтернету - доповнити цю систему необхідними засобами захисту внутрішньої мережі від віддалених атак та шкідливих програм. Це можливо лише при вірному поєднанні антивірусного захисту комп'ютера-шлюзу при його роботі в Інтернет, а також при встановленні на ньому відповідного програмного забезпечення, наприклад, міжмережного екрану (firewall).

Питання безпеки.

Система Internet при проектуванні не планувалася як захищена мережа, тому її проблемами є*:*

- *легкість перехоплення даних* і фальсифікація адрес у мережі. Основна частина трафіку Internet - це нешифровані дані. E-mail, паролі і файли можуть бути перехоплені шляхом використання доступних програм;
- *вразливість засобів TCP/IP* - ряд засобів TCP/IP спроектовано незахищеними, і це може бути скомпрометовано кваліфікованими зловмисниками; засоби, що використовуються для тестування, особливо вразливі;
- *відсутність політики* - багато сайтів сконструйовані так, що надають широкий доступ до себе з боку Internet, не враховуючи можливості зловживання цим доступом; багато сайтів дозволяють роботу більшій кількості сервісів TCP/IP, ніж їм необхідно для роботи, і не намагаються обмежити доступ до інформації про свої комп'ютери,якою можуть скористатися зловмисники; [20, с.103]

При підключенні локальної мережі до Інтернету, безперечно, ризики зростають. Необхідно обов'язково приймати заходи для захисту локальної мережі. Основні вимоги до захисту:

- Захист локальної мережі від віддаленого НСД з боку глобальної мережі;
- Втаємничення інформації про структуру внутрішньої мережі і її компонентів від користувачів глобальної мережі;
- Розмежування доступу в захищену мережу і із захищеної мережі в глобальну.

Підключення локальної мережі до Інтернету.

Для підключення локальної мережі використовуються два основних методи підключення: постійне та тимчасове. Постійне вимагає швидкісного каналу зв'язку з провайдером, а також наявності маршрутизатора та спеціального модему. Тимчасове є більш дешевим та найчастіше використовується в умовах навчальних закладів: за допомогою звичайного модему та телефонного кабелю. При підключенні локальної мережі до Інтернету один з комп'ютерів виступає в якості **шлюзу:** через модем чи іншим способом зв'язується з Internet, а інші комп'ютери з'єднуються з Інтернетом через нього. Для повноцінної роботи в Інтернеті шлюз повинен мати реальний IP-адрес, в іншому випадку він не отримає ззовні ні одного IP-пакету. Як правило, реальний IP-адрес виділяється лише комп'ютеру-шлюзу, що має безпосереднє з'єднання з Інтернетом. При підключенні через модем IP-адреса призначається йому динамічно, з пулу провайдера. При постійному з'єднані він постійний.

Після підключення різниця між статичними і динамічними адресами щезає. На комп'ютері-шлюзі будуть працювати як програми-клієнти, так і програми-сервери. Причому програми-сервери будуть доступними з обох мереж – як із Internet, так і із локальної мережі. (Небажані з'єднання ззовні можуть бути відключені засобами безпеки, які ми розглянемо далі). Це відбувається тому, що у комп'ютера- шлюзу принаймні два мережних інтерфейси: наприклад, модем і мережна карта. І відповідно дві IP-адреси одна «реальна», що призначається контролеру віддаленого доступу, друга внутрішня, що призначається мережній

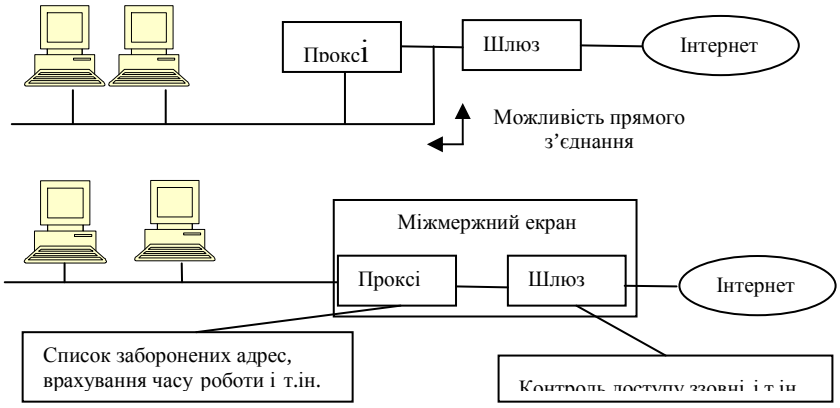
карті у локальній мережі. Така конфігурація доступу до Інтернет, вирішує відразу два завдання:

- Економляться дефіцитні IP-адреси;
- Забезпечується захист комп'ютерів локальної мережі (крім комп'ютера шлюзу)

Організація безпечного колективного доступу до Інтернету.

Однак така архітектура не дозволяє іншим комп'ютерам в мережі з'єднуватися з Інтернетом. Для того щоб таке з'єднання стало можливим, необхідне використання спеціальної програми-посередника, яка носить назву проксі-сервер.

Проксі-сервер (від анг. Proxy – замісник, уповноважений) – це сервер-посередник, до чиїх завдань входить обробка запитів, що приходять від комп'ютерів своєї мережі, на отримання інформації, розміщеної зовні неї.



Мал.5. Проксі-сервер та міжмережний екран.

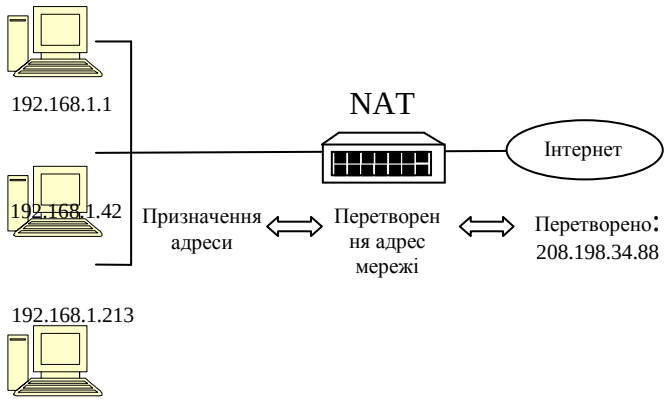
Кешування.

Якщо документ чи зображення повністю передані по мережі від www-серверу програмі-браузеру, то браузер зберігає їх в своєму кеші (кеш знаходиться в окремому підкалозі браузера на диску). Якщо користувач в подальшому запитає той самий документ, то перед тим як заново перекачувати файл по мережі, браузер перевірить, чи є він в кеші. Якщо документ на сервері не новіший ніж документ у кеші, то користувачу буде запропоновано документ з кешу, що суттєво збільшить швидкість роботи. Розмір кешу обмежений. Він

встановлюється користувачем в налаштуваннях браузера. Нові документи витісняють старі. Однією з функцій проксі-сервера є кешування web-сторінок.

Перетворення мережних адрес.

Одним з найрозповсюдженіших способів сховати конфігурацію внутрішньої мережі є використання одних адрес для внутрішніх систем і перетворення їх при зв'язку з Інтернетом. Такий механізм носить назву перетворення мережних адрес (NAT – Network Address Translation). Необхідність в NAT виникла внаслідок швидкого розвитку Інтернет і неспроможності забезпечити всі системи в Інтернеті унікальною адресою.



Мал.6.Перетворення мережних адрес.

Тому для внутрішніх мереж використовується зарезервований простір IP-адрес.

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Не кожній організації є потреба застосовувати NAT. Однак якщо NAT буде використовуватися, необхідно включити відповідне формулювання в правила політики в найбільш загальному вигляді.

Адреси внутрішньої мережі мають залишатися схованими. Коли системи запитують доступ до інших мереж, сховані адреси повинні перед передачею бути перетворенні в легальні зареєстровані адреси.

Міжмережний екран (Firewall).

Міжмережний екран (МЕ) – це спеціалізований комплекс міжмережного захисту, який також називають брандмауером чи системою firewall. Зазвичай

МЕ захищає внутрішню мережу організації від «вторгнення» із глобальної мережі. Тоді він має розміщуватися між мережею, яку захищає, та потенційно ворожою мережею. Для більшості організацій МЕ є необхідною умовою забезпечення безпеки внутрішньої мережі.

Можна класифікувати МЕ за такими ознаками.

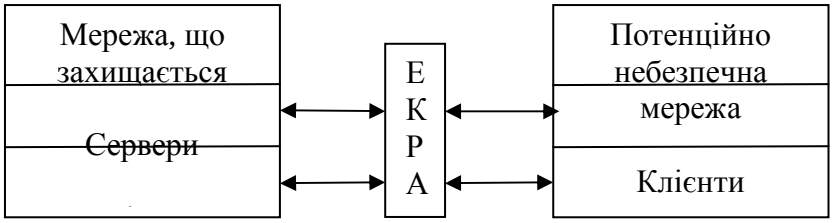
За функціонуванням на рівнях моделі OSI:

- Пакетний фільтр (екрануючий маршрутизатор – screening router);
- Шлюз сеансового рівня (екрануючий транспорт)
- Прикладний шлюз (application gateway)
- Шлюз експертного рівня (statefull inspection firewall)

За виконанням:

- Апаратно-програмний
- Програмний.
- Фільтрування трафіку.
- Фільтрування інформаційних потоків.

При розгляді будь-якого питання, що стосується мережних технологій, основою служить еталонна модель ISO/OSI. Міжмережеві екрани також доцільно класифікувати по тому, на якому рівні виробляється фільтрація - канальному, мережному, транспортному чи прикладному. Відповідно, можна говорити про концентратори, що екранують, (рівень 2), маршрутизатори (рівень 3), про транспортне екранування (рівень 4) і про прикладні екрани (рівень 7). Існують також комплексні екрани, що аналізують інформацію на декількох рівнях.



Мал.7. Екран як засіб розмежування доступу.

Міжмережевий екран - це напівпроникна мембрана, що розташовується між що захищається (внутрішньою) мережею і зовнішнім середовищем (зовнішніми мережами чи іншими сегментами корпоративної мережі) і контролює всі інформаційні потоки у внутрішню мережу і з неї (Мал. 7). Контроль

інформаційних потоків складається в їхній фільтрації, тобто, у вибірковому пропущенні через екран, можливо, з виконанням деяких перетворень і повідомленням відправника про те, що його даним у пропуску відмовлено. Фільтрація здійснюється на основі набору правил, попередньо завантажених в екран і мережні аспекти, що є вираженням політики безпеки організації.

Політика безпеки Інтернет.

Мета політики безпеки для Internet - прийняти рішення про те, як організація передбачає захищатися. Політика інформаційної безпеки, зазвичай, складається з двох частин - загальних принципів і конкретних правил роботи. Загальні принципи визначають підхід до безпеки в Internet. Правила ж визначають, що дозволено, а що заборонено. Правила можуть бути доповнені конкретними процедурами та різними рекомендаціями.

Політика безпеки Інтернет повинна передбачувати:

- Ліміти об’єму інформації для кожного користувача.
- Правила антивірусного захисту, які неможливо минути. Наприклад заборона завантаження активного коду.
- Ввести правила змістовного фільтрування запитів користувачів, щоб заборонити доступ неповнолітніх до деяких сайтів, що містять шкідливу інформацію.
- Ввести правила фільтрування вхідного трафіку, захисту топології внутрішньої мережі, захисту портів Інтернет-шлюзу.

Захист внутрішнього навчального веб-сервера.

Особливої уваги потребує інформація навчального призначення, що подається у вигляді внутрішнього web-серверу. Цей веб-сервер може бути розроблений для організації учбового процесу з багатьох предметів. А тому важливо, щоб був визначений працівник, який несе відповідальність за загальну політику безпеки веб-сервера, займається вставкою документів у корпоративне дерево, їхньою корекцією і видаленням. Крім того, автори окремих розділів (вчителі з конкретних предметів) не повинні мати прав на модифікацію корпоративного дерева. Важливим, з точки зору безперервності учбового процесу, є захист

вихідних документів від модифікації учнями-користувачами, що не забороняє їх копіювання.

Інформація про дітей на шкільних веб-сайтах.

Кількість шкільних веб-сайтів з кожним роком зростає, та, не зважаючи на це, багато вчителів ще недостатньо розуміють, яку саме інформацію про дітей можна розміщувати на них. Реалії сьогодення показують, що особисті дані учнів (і не тільки в електронному вигляді) можуть бути використані зловмисниками, що ставить під загрозу особисту безпеку дітей. Тому краще на шкільних вебсайтах розміщати фотографії дітей тільки за згодою батьків і тільки групові. Якщо на шкільному веб-сайті розміщена інформація про учнів, то варто вказувати лише загальні факти з життя дитини (його інтереси, хобі, заслуги) не вказуючи його фізичну адресу, адресу електронної пошти (без дозволу батьків), телефон, повне ім'я й іншу особисту інформацію.

Посилання на інші ресурси на шкільному веб-сайті.

Якщо школа на своєму веб-сайті розміщає посилання на будь-який інший, нешкільний сайт, потрібно обов'язково перевірити, чи є цей сайт прийнятним для відвідування його учнями. Корисним в такому випадку є використання «спливаючих вікон», які попереджують про перехід в небезпечну зону: це убезпечить вас від ситуації, коли зміст ресурсу змінився на неприйнятний. Навіть якщо керівництво Вашої школи вирішить, що таке спливаюче вікно з попередженням не потрібно, учителі повинні розповісти батькам, що дітям можуть бути доступні нешкільні сайти і, незважаючи на те, що керівництво школи рахувало, що сайти підходили для відвідування їхніми учнями в той час, коли в минулому були встановлені посилання, зміст сайтів може змінитися або вони можуть більше не діяти, тобто, школа не взмозі контролювати те, що відбувається на цих сайтах. Учитель повинен пояснити батькам і дітям, що вони відвідують такі сайти на свій страх і ризик. Тому, якщо школа не має наміру регулярно перевіряти посилання, імовірно, краще не розміщати посилання на нешкільні сайти на веб-сайті школи.[44]

Додаток А. Глосарій основних термінів.*

Автентифікація (authentication) – процедура перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності.

Авторизація (authorization) – надання повноважень; встановлення відповідності між повідомленням (пасивним об'єктом) і його джерелом (створене його користувачем або процесом).

Авторизація (authorization) – надання повноважень; встановлення відповідності між повідомленням(пасивним об'єктом) і його джерелом (створене його користувачем або процесом).

Авторизований користувач (authorized user) – користувач, що володіє певними повноваженнями.

Адміністратор (administrator, administrative user) – користувач; роль якого включає функції керування КС/або КЗЗ.

Адміністратор безпеки (security administrator) – адміністратор, відповідальний за дотримання політики безпеки.

Аналіз ризику (risk analysis) – процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеня їх прийнятності для експлуатації АС.

Атака (attack) – спроба реалізації загрози.

Вразливість системи (system vmneraMity) – нездатність системи протистояти реалізації певної загрози або сукупності загроз.

Втрата інформації (information leakage) – неконтрольоване поширення інформації, що веде до її несанкціонованого одержання.

Доступність (availability) – властивість ресурсу системи (КС, послуги, об'єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному

користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому потрібний.

Журнал реєстрації (audit trail) – упорядкована сукупність реєстраційних записів, кожен з яких заноситься КЗЗ за фактом здійснення контрольованої події.

*Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу. Навч. посібник /За ред. С.Г.Лаптева. - К.: Вид-во Європ. ун-ту, 2001. - С.155-173.

Загроза (threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Запит на доступ (access request) – звернення одного об'єкта КС до іншого з метою отримання певного типу доступу.

Засоби захисту (protection facility) – програмні, програмно-апаратні та апаратні засоби, що реалізують механізми захисту.

Захист від несанкціонованого доступу; захист від НСД (protection from unauthorized access) – запобігання або істотне утруднення несанкціонованого доступу до інформації.

Заходи забезпечення безпеки (safeguards) – послуги, функції, механізми, правила і процедури, призначені для забезпечення захисту інформації.

Ідентифікація (identification) – процедура присвоєння ідентифікатора об'єкту КС або встановлення відповідності між об'єктом і його ідентифікатором; упізнання.

Інцидент – будь-яке порушення правил інформацыйної безпеки, встановленої в організації.

Комплекс засобів захисту; КЗЗ (trusted computingbase; TCB) – сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Захищена комп'ютерна система; захищена КС (trusted computer system, trusted computer product) – комп'ютерна система, яка здатна забезпечувати захистоброблюваної інформації від певних загроз.

Квота (quota) – обмеження можливості використання певного ресурсу КС користувачем або процесом.

Керування доступом (access control) – сукупність заходів з визначення повноважень і прав доступу, контролю за дотриманням ПРД.

Ключ (key) – конкретний стан деяких параметрів алгоритму криптографічного перетворення, що забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму.

Комплексна система захисту інформації; КСЗІ – сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Компрометація (compromise) – порушення політики безпеки; несанкціоноване ознайомлення.

Комп'ютерний вірус (computer virus) – програма, що має здатність до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування КС і/або зумовити порушення політики безпеки.

Конфіденційність інформації (information confidentiality) – властивість інформації, яка полягає в тому, що вона не може бути отримана неавторизованим користувачем і/або процесом.

Криптографічне перетворення – перетворення даних, яке полягає в їх шифруванні, вироблення імітовставки або цифрового підпису.

Люк (trap door) – залишені розробником недокументовані функції, використання яких дає можливість обминути механізми захисту.

Механізми захисту (security mechanism) – конкретні процедури і алгоритми, що використовуються для реалізації певних функцій і послуг безпеки.

Міжмережний екран (firewall) – комплекс програмно-апаратних засобів, які здійснють весь комплекс захисту внутрішньої мережі від іншої (потенційно ворожої).

Модель порушника (user violator model) – абстрактне формалізоване або неформалізоване описання порушника.

Модифікація (modification) – зміна користувачем або процесом інформації, що міститься в об'єкті.

Несанкціонований доступ до інформації; НСД до інформації (unauthorized access to information) – доступ до інформації, здійснюваний з порушенням ПРД.

Ознайомлення (disclosure) – одержання користувачем або процесом інформації, що міститься в об'єкті.

Пароль (password) - секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до КС або до інформації.

Повноваження (privilege) – права користувача або процесу на виконання певних дій, зокрема, на одержання певного типу доступу до об'єктів.

Політика безпеки інформації (information security policy) – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Порушник (user violator) – користувач, який здійснює несанкціонований доступ до інформації.

Правила розмежування доступу; ПРД (access mediation rules) – частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів.

Право доступу (access right) – дозвіл або заборона здійснення певного типу доступу.

Програмна закладка (program bug) – потайно впроваджена програма або недокументовані властивості програмного забезпечення, використання яких може призвести до обходу КЗЗ і/або порушення політики безпеки.

Проникнення (penetration) – успішне подолання механізмів захисту системи.

Проксі-сервер(proxy) – це сервер-посередник, до чиїх завдань входить обробка запитів, що приходять від комп’ютерів своєї мережі, на отримання інформації, розміщеної зовні неї.

Реєстрація (audit, auditing) – послуга, що забезпечує збирання й аналіз інформації щодо використання користувачами і процесами функцій і об'єктів, контрольованих КЗЗ.

Ризик (risk) – функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Розмежування доступу (access mediation) – сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі ПРД можливості надання доступу.

Розшифрування даних (data decryption) – процес перетворення шифртексту у відкритий текст.

Санкціонований доступ до інформації (authorized access to information) – доступ до інформації, що не порушує ПРД.

Список доступу (access control list) – перелік користувачів і/або процесів з зазначенням прав доступу їх до об'єкта КС, з яким пов'язаний цей перелік.

Список повноважень (privilege list, profile) – перелік об'єктів з зазначенням прав доступу до них з боку користувача або процесу, з яким пов'язаний цей перелік.

Стійкість до відмов (fault tolerance) – послуга, що забезпечує здатність КС продовжувати функціонування в умовах виникнення збоїв і відмов окремих компонентів.

Тип доступу (access type) – суттєвість доступу до об'єкта, що характеризує зміст здійснюваної взаємодії, а саме: проведені дії, напрям потоків інформації, зміни в стані системи (наприклад, читання, запис, запуск на виконання, видаляння, дозапис).

*Троянський кін*ь (Trojan horse) – програма, яка, і будучи авторизованим процесом, крім виконання документованих функцій, здатна здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми.

Цілісність інформації (information integrity) – властивість інформації, яка полягає в тому, що вона не може бути модифікована неавторизованим користувачем і/або процесом.

Цілісність системи (system integrity) – властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

Шифрування даних – процес зашифрування або розшифрування.

Додаток В. Схеми.

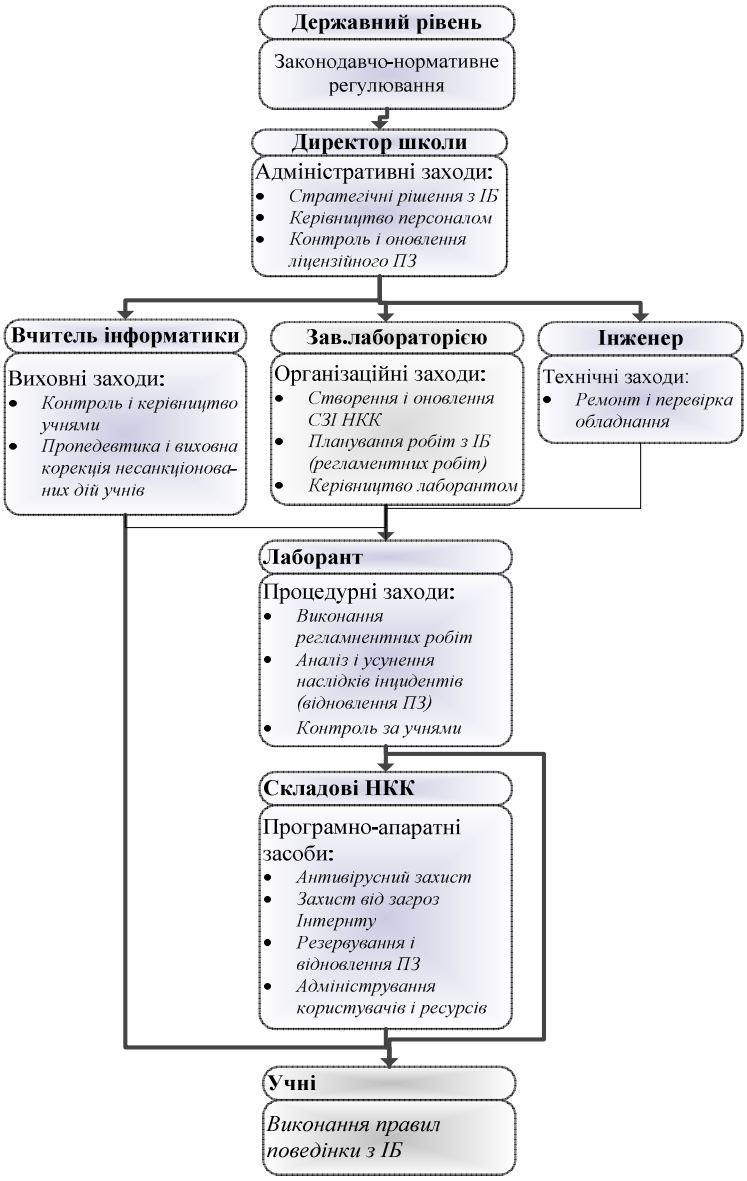


Схема 1. Розподіл заходів з інформаційної безпеки серед персоналу

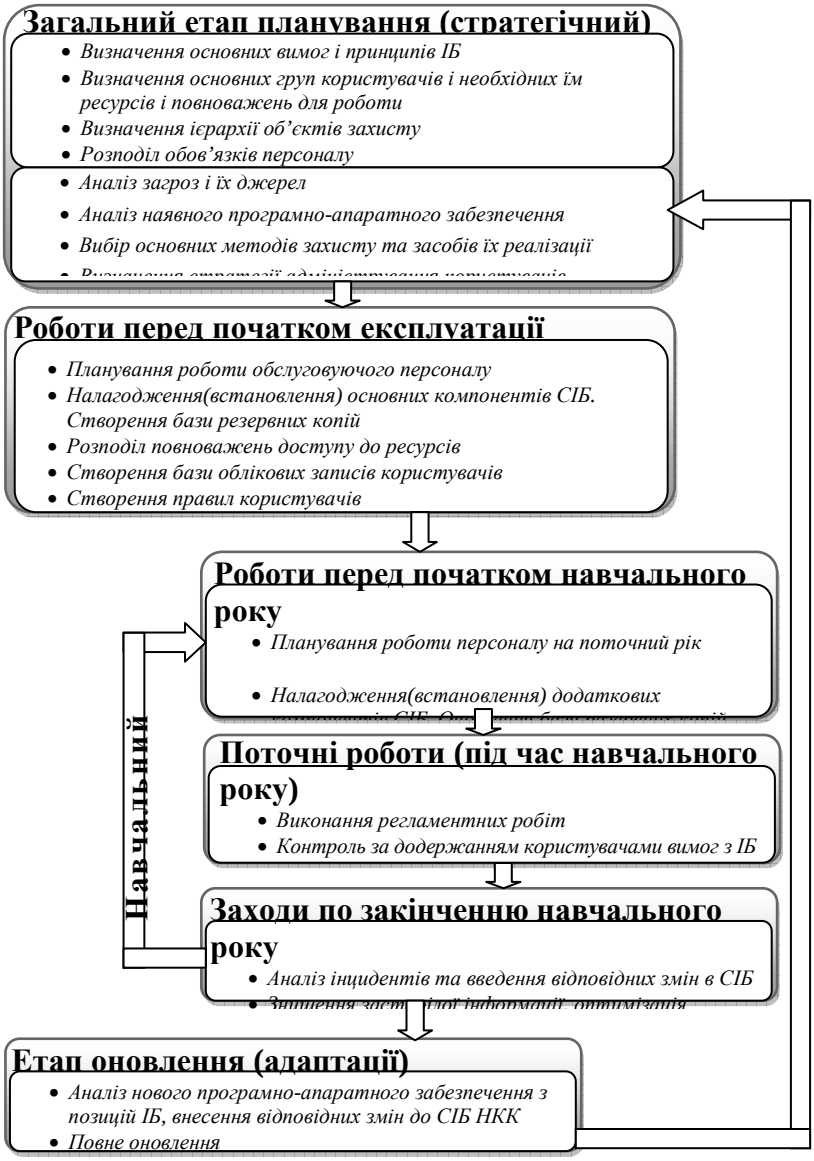


Схема 2. Планування заходів з ІБ на всіх етапах життєвого циклу СІБ НКК.

Додаток С. Приклади правил інформаційної безпеки.

Правила роботи учнів у кабінеті інформаційно-комунікаційних технологій (доповнення правилами інформаційної безпеки)

Обов'язки користувачів по реєстрації в системі:

1. Для реєстрації в системі ми повинні ввести по запиту своє користувацьке ім'я (логін) та пароль;
2. Якщо ви ввели некоректно пароль три рази, то ваш обліковий запис буде заблоковано, розблокувати її може лише лаборант (вчитель інформатики);
3. Ви ніколи не повинні записувати свій пароль;
4. Ви ніколи не повинні повідомляти будь-кому свій логін чи пароль;
5. Якщо ви забули свій пароль, необхідно особисто отримати новий у лаборанта.

Робота в комп'ютерному класі:

1. Комп'ютерне обладнання та програмне забезпечення класу призначене лише для навчальних цілей і повинно використовуватися лише для цього;
2. Не можна приносити на носіях та завантажувати на жорсткі диски комп'ютерів заборонену інформацію (порнографію, що демонструє жорстокість), стороннє програмне забезпечення.
3. У класі підтримується стандартна конфігурація всіх робочих станцій, користувачам забороняється змінювати цю конфігурацію, якщо дана зміна не передбачена навчальним завданням.

Обов'язки користувача Internet:

1. Підключення школи до Інтернету повинно використовуватися лише для навчання;
2. Забороняється використання комп'ютерів шкільного класу та підключення до Інтернету для ігор, отримання та збереження забороненої інформації (порнографії, що демонструє жорстокість), стороннього програмного забезпечення.
3. Користувачі повинні знати що комунікації Internet не є конфіденційними. Користувачі не повинні передавати по мережі інформацію, яка містить їх

конфіденційну інформацію: прізвище, адреса, телефон, особисті фотографії та іншу інформацію, розголошення якої може нанести їм шкоду.

4. Користувачі не повинні завантажувати з Internet програмне забезпечення та активні компоненти web-сторінок, а всі дані що завантажуються ними з Internet повинні пройти антивірусну перевірку. Дані, що завантажуються учнями з Internet повинні бути навчального призначення і мати розмір, що не перевищує встановлений у навчальному закладі ліміт.

Контроль та дослідження мережних даних.

1. Керівництво школи попереджує, що воно має право досліджувати і знищувати будь-які дані, що зберігаються на комп'ютерах та мережних системах. Також введеться контроль за діями учнів: візуальний і електронний. Якщо зібрані факти будуть свідчити про порушення користувачем правил інформаційної безпеки чи законів, то вони можуть бути використані як підстава для дисциплінарного покарання.

Правила антивірусного захисту:

1. На всіх комп'ютерах встановлено антивірусне програмне забезпечення. Обов'язок користувачів полягає у сприянні заходам антивірусного захисту.
2. Користувачі повинні перевіряти всі дані при кожному їх завантажені з будь-якого джерела. Також необхідно перевіряти будь-який переносний носій перед його відкриттям на наявність вірусів.
3. Користувачі повинні сприяти оновленню антивірусних баз, а також ніколи не перешкоджати та не вивантажувати з оперативної пам'яті антивірусні програми.
4. Користувачі не повинні створювати, запускати, передавати чи демонструвати ніяких комп'ютерних кодів, які можуть нанести шкоду системам обробки даних чи інформації, що в них зберігається.

Кодекс моральної поведінки у віртуальному середовищі:

1. Не можна поширювати інформацію, що може містити наклеп, образу будь-якої людини за національними, расовими, статевими, фізичними та іншими прикметами.

Список використаних джерел

Нормативні документи та закони.

1. Положення про кабінет інформатики та інформаційно-комунікаційних технологій навчання загальноосвітніх навчальних закладів // Інформатика. - 2005. - №2-3. - С. 3-8.
2. Методичні рекомендації щодо облаштування і використання кабінету інформатики та інформаційно-комунікаційних технологій навчання загальноосвітніх навчальних закладів // Інформатика. - 2005. - №2-3. - С. 9-32.
3. Правила безпеки під час навчання в кабінетах інформатики навчальних закладів системи загальної середньої освіти // Інформатика. - 2005. - №2-3. - С. 33-37.
4. Вимоги до специфікації навчальних комп'ютерних комплексів // Комп'ютер у школі та сім'ї. - 2007. - №4. - С. 50-51.
5. Правила використання комп'ютерних програм у навчальних закладах. Затверджено наказом Міністерства освіти і науки України від 2 грудня 2004 року N 903.
6. Державна програма “ Інформаційні та комунікаційні технології в освіті і науці ” на 2006–2010 роки. Затверджено постановою кабінету міністрів від 7 грудня 2005 р. № 1153.
7. Закон України "Про інформацію" від 02.10.1992р. - №2657-XII.
8. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 № 2594-IV
9. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9.01.2007 № 537-V.

Навчальні посібники з інформаційної безпеки.

10. Анин Б. Защита компьютерной информации СПБ: БХВ – СПб.; 2000. – 368с.

11. Бармен С. Разработка правил информационной безопасности: Пер. с анг. – М.: «Вильямс», 2002. – 208 с.: ил. – ISBN 5-8459-0323-8
12. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. Учебное пособие/ Моск.гос.инженер.физ.ин-т (техн.ун.) – М.Изд-во МИФИ, 1995. –93с.
13. Галатенко В.А. Основы информационной безопасности // Интернет-университет информационных технологий [Електронный ресурс]. – Режим доступа: – http://www.intuit.ru
14. Глосарій з курсу «Захист інформації в інформаційних системах» для студентів спеціальності 7.080401 усіх форм навчання. – Харьків: ХДЕУ, 2004. – 16 с.
15. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – Киев: “Корнійчук”, 2000 – 152 с.
16. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.; Издательство “Диа-Софт”, 1999. – 480 с.
17. Корченко О.Г., Морозов А.С. Захист та зламування програм.: Навчальний посібник. К.: НАУ, 2001. – 84 с. Библ.81.
18. Косарев В.М., Петренко А.Н. Информационная безопасность: организация защиты програм и даннях. Учебное пособие. – Днепропетровск: Изд. ДУЭП, 2003. –152 с.
19. Крысин А. В. Информационная безопасность. Практическое руководство.: - М.: СПАРРК, К.: ВЕК+, 2003. – 320 с.
20. Лужецький В.А., Северин Л.І., Гульчак П.Ю., Кожухівський А.Д. Основи організаційного захисту інформації. Навчальний посібник. – Вінниця: ВНТУ, 2005. – 148 с.
21. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с.: ил.
22. Мамаев М., Петренко С. Технологии защиты информации в интернете. Специальный справочник. – СПб.: Питер, 2002. – 848 с.

23. Медведев Н.Г., Москалюк Д.В. Аспекти информационной безопасноети виртуальних частных сетей. Учебное пособие. - К.: Изд-во Европ.ун-та, 2002. - 95 с
24. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика; Электроинформ, 1997. – 368 с.
25. Михаэль А. Бэнкс. Информационная защита ПК: Пер. с анг.. – К.: ВЕК+, М.: Энтроп, Спб.: Корона-Принт 2001. –272 с.
26. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия - Телеком, 2006. – 544 с.: ил.
27. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов среднего професионального образования. – М.; Форум-Инфра-М, 2002. –368 с.
28. Петраков А.В. Основы практической защиты информации. 3-е изд. Учебн. Пособие. М.: Радио и связь, 2001. – 368 с.;ил.
29. Пономаренко В.С., Журавльова І.В., Туманов В.В. Основи захисту інформації. Навчальний посібник. – Харьків: Вид.ХДЕУ, 2003. – 176 с.
30. Устенко І.В. Системи захисту інформації: Навч.посібник. Миколаїв: НУК, 2006. – 68 с.
31. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001, 352 с., ил.
32. Великий тлумачний словник сучасної української мови / Укладач і головний редактор В.Т.Бусел. – К.; Ірпінь: ВТФ «Перун», 2004. – 1440 с.

Програмне забезпечення.

33. Андреев А.В. и др. Microsoft Windows Server. Русская версия / Под общ. ред. А.Н. Чекмарева и Д.Б. Вишнякова. – Спб.: БХВ – Санкт-Петербург, 2000. – 960 с.: ил.
34. Виллеттт Эдвард, Каммингс Стив. Office XP. Библия пользователя. «Вильямс», 2002. – 848 с.: ил.
35. Мінухін С В. Лабораторний практикум з навчальної дисципліни "Комп'ютерні мережі". Навчально-практичний посібник для студентів

напряму підготовки 0804 "Комп'ютерні науки" всіх форм навчання / С. В. Мінухін, В. Ю. Жукарєв; [Заг. редакція докт екон. наук, професора. С. Пономаренка. – Харків: Вид. ХНЕУ, 2007. – 212 с (Укр. мов.)

36. Пєтух А.М., Войтко В.В., Бевз С.В., Яремко С.А. Мережі ЕОМ. Лабораторний практикум. -Вінниця: ВНТУ, 2003 - 125 с.
37. Сетевые операционные системы/ В.Г. Олифер, Н.А. Олифер. – Спб.: Питер, 2002. – 544 с.: ил.
38. Симпсон Алан, Андердал Брайан Windows XP. Библия пользователя. Пер. с англ.: – М.: Издательский дом «Вильямс», 2004. – 704 с.: ил.
39. Уильям Р. Станек Microsoft Windows XP Professional. Справочник системного администратора. Пер. с англ.: М.: Издательский дом «Русская редакция», 2002. –448 с.: ил.
40. Эффективная работа: Windows XP / Э. Ботт, К. Зихерт. – СПб.: Питер, 2003. – 1069 с: ил.

Проблеми інформаційної безпеки в школі.

41. Інформаційна безпека України: сутність та проблеми. [Електронный ресурс]. – Режим доступа: http://bezpeka.com/ru/lib/spec/art12.html
42. Безопасность детей в Интернете. Microsoft, 2006. – [Електронный ресурс]. – Режим доступа: http://www.microsoft.com/rus/athome/security/children/default.mspx
43. Серебреникова М. Компьютерная этика. – [Електронный ресурс]. – Режим доступа: http://www.ourtx.com/?a=289
44. Личный интернет. Учителям о проблемах информационной безопасности в образовании. [Електронный ресурс]. – Режим доступа: http://www.content-filtering.ru
45. Прохоров А. «Приличный» Интернет в школе и дома // КомпьютерПресс. – №2. – 2007. [Електронный ресурс].– Режим доступа: http://www.compress.ru/article.aspx?id=17262&iid=799
46. Полат Е.С. Проблема информационной безопасности в образовательных сетях рунет. [Електронный ресурс].– Режим доступа: http://www.ioso.ru/distant/library/publication/infobez.htm

47. Поляков В.П. Аспекты информационной безопасности в курсе информатики и информационных технологий // Школьные технологии. – 2006. – №6 – С.177-179.
48. Мошкин В.Н., Чередниченко А.И. Проблема информационной безопасности в содержании школьного образования [Електонный ресурс]. – Режим доступа: http://www.uni-altai.ru/engine/download.php?id=502
49. Ершов Д.А.Информационная безопасность личности как цель социально-педагогической деятельности // Учитель Российской школы – ключевая фигура модернизации образования, интернет конференция 1 марта – 1 июня 2008 г. [Електонный ресурс]. – Режим доступа: http://modern-obraz08.livejournal.com/2634.html
50. Давлетханов М. Статья про Интернет в школе. [Електонный ресурс]. – Режим доступа: http://www.guru-soft.ru/entensysarticles
51. Онландия. [Електонный ресурс]. – Режим доступа: http://www.onlandia.org.ua
52. Журин А.А. Информационная безопасность как педагогическая проблема // Педагогика. – 2001.– №4. – С.49-54.
53. Чусавитина Н.Г. Элективный курс «Основы информационной безопасности» // Информатика и образование. - 2007. - N 4. - С. 41-56.

ПРОЕКТ ПОЛОЖЕННЯ

про сертифікацію електронного навчального курсу

1. Загальна частина

1.1. Одним із завдань Болонського процесу є створення глобального міжнародного освітнього середовища, головною перевагою якого є представлення навчального матеріалу в дидактично уніфікованому й формалізованому вигляді та надання можливості його використання у будь-якому місці і у будь-який час незалежно від форми навчання студента.

1.2. Електронний навчальний курс (ЕНК) - це комплекс навчально-методичних матеріалів та освітніх послуг, створених для організації індивідуального та групового навчання з використанням дистанційних технологій (ДТ). *Дистанційні технології навчання* складаються з інноваційних педагогічних та інформаційно-комунікаційних технологій дистанційного навчання (ДН). *Інноваційні педагогічні технології дистанційного навчання* це технології опосередкованого активного спілкування викладачів зі студентами, студентів між собою з використанням телекомунікаційного зв'язку та методології індивідуальної роботи студентів зі структурованим навчальним матеріалом, який подається у електронному вигляді та зберігається на спеціальному навчальному порталі, з урахуванням компетентністного та особистісно-орієнтованого підходу, проектної методики навчання. *Інформаційно-комунікаційні технології дистанційного навчання* - це технології створення, передавання і зберігання навчальних матеріалів, організації і супроводу навчального процесу дистанційного навчання за допомогою телекомунікаційного зв'язку, зокрема, електронних локальних, регіональних та глобальних (Інтернет) мереж.

1.3. Особливість електронного навчального курсу (ЕНК) полягає у тому, що такий електронний навчальний засіб передбачений для оволодіння студентами навчальним матеріалом під керівництвом викладача. Основними характеристиками ЕНК є:

- структурованість навчально-методичних матеріалів;

- логіка вивчення навчального курсу;
- чіткий графік виконання студентами навчального плану;
- налагоджена система інтерактивної взаємодії викладача і студента, студентів між собою, засобами ресурсів ЕНК та дистанційних технологій, протягом усього часу вивчення дисципліни;
- якісно виконані навчальні матеріали, які дозволяють набути компетентностей, задекларованих у робочій програмі;
- система контролю та оцінювання виконання всіх видів навчальної діяльності студентів.

1.4. Електронні навчальні курси розміщуються на навчальному порталі. Робота порталу повинна бути організована на основі використання системи дистанційного навчання, наприклад, Moodle, ATutor ILIAS, Прометей тощо. За допомогою цієї системи студент може дистанційно, через Інтернет, ознайомитися з навчальним матеріалом, який може бути представлений у вигляді різнотипних інформаційних ресурсів (текст, відео, анімація, презентація, електронний посібник), виконати завдання та відправити його на перевірку, пройти електронне тестування. Викладач має змогу самостійно створювати дистанційні електронні курси і проводити навчання на відстані, надсилати повідомлення студентам, розподіляти, збирати та перевіряти завдання, вести електронні журнали обліку оцінок та відвідування, налаштовувати різноманітні ресурси курсу і т.д.

1.5. Доступ до ресурсів навчального порталу– персоніфікований. Логін та пароль доступу студенти та науково-педагогічні працівники (НПП) отримують у адміністратора сервера. Правила отримання доступу подаються на сайті навчального порталу. Кожний студент та НПП має доступ лише до тих електронних навчальних курсів, на яких він зареєстрований для участі у навчальному процесі. Реєстрація студентів на електронному навчальному курсі здійснюється викладачем цього курсу. По закінченні навчання за програмою курсу викладач відраховує студентів з числа його учасників.

1.6. Електронні навчальні курси можуть бути використані як засоби навчання

для студентів денної, заочної, дистанційної форм навчання та регіональних вищих навчальних закладів на всіх етапах навчальної діяльності студентів під час вивчення відповідних дисциплін.

1.7. Електронні навчальні курси складаються з електронних ресурсів двох типів: а) ресурси, призначені для подання студентам змісту навчального матеріалу, наприклад, електронні конспекти лекцій, мультимедійні презентації лекцій, методичні рекомендації тощо; б) ресурси, що забезпечують закріплення вивченого матеріалу, формування вмінь та навичок, самооцінювання та оцінювання навчальних досягнень студентів, наприклад, завдання, тестування, анкетування, форум тощо). Всі електронні навчальні курси, розміщені на навчальному порталі, повинні мати уніфіковану структуру (див. рис.1), яка включає:

- загальну інформацію про навчальну дисципліну (робоча програма, календарний план, критерії оцінювання, друковані та Інтернет-джерела, глосарій, оголошення);
- навчально-методичні матеріали з кожного модуля:
  - o теоретичний матеріал (мультимедійні презентації лекцій, структуровані електронні навчальні матеріали, електронний конспект лекцій, аудіо-, відео-, анімаційні навчальні ресурси, список друкованих та Інтернет-джерел);
  - o практичні (семінарські, лабораторні) роботи (зміст, методичні вказівки щодо їх виконання, список індивідуальних завдань, форма подання результатів виконання, критерії оцінювання);
  - o завдання для самостійної роботи студентів (додатковий теоретичний матеріал, завдання, методичні вказівки щодо їх виконання, список індивідуальних завдань, форма подання результатів виконання, критерії оцінювання);
  - o модульний контроль (контрольні запитання, завдання з критеріями оцінювання та формою подання результатів виконання, тести для самоконтролю та контролю);
- матеріали для проведення підсумкової атестації (контрольні запитання, тест для самоконтролю, підсумковий тест для атестації студента з

дисципліни);

- додаткові матеріали.

2. Етапи розробки та сертифікації електронного навчального курсу

2.1. Процес створення ЕНК передбачає п’ять послідовних етапів:

Етап 1 - навчання науково-педагогічних працівників (НПП) по створенню електронного навчального курсу.

Етап 2 – наповнення ЕНК електронними навчально-методичними ресурсами в повному обсязі відповідно до критеріїв структурно-функціональної, науково-змістовної та методичної експертизи.

Етап 3 - апробація ЕНК протягом одного навчального семестру. На цьому етапі викладач реєструє студентів на курсі та використовує матеріали ЕНК для навчання студентів. Результати навчання студентів зберігаються на порталі.

Етап 4 – сертифікація електронного навчального курсу на рівні ВНЗ. Процедура сертифікації описана в п.4 даного Положення. Лише сертифікований ЕНК має право на його використання на всіх етапах навчального процесу (в т.ч. на етапі підсумкової атестації).

Етап 5 – сертифікація ЕНК на рівні Міністерства освіти і науки України з наданням рекомендації щодо використання у навчальному процесі з «грифом МОН». Процедура сертифікації описана в п.5 даного Положення.

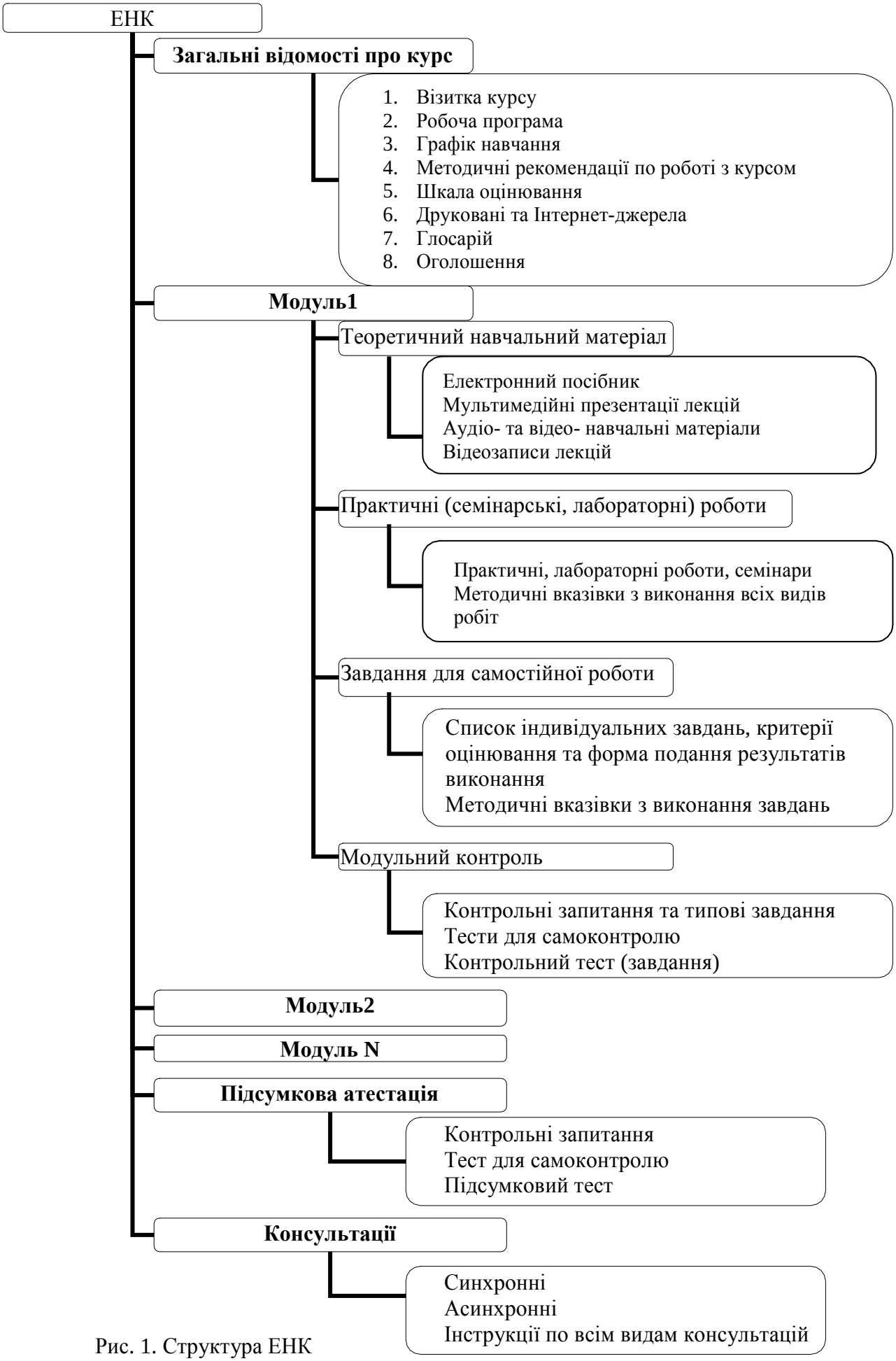


Рис. 1. Структура ЕНК

3. Зміст електронного навчального курсу

3.1. Навчально-методичні матеріали ЕНК з дисциплін мають бути структурованими відповідно до схеми, наведеної на рис.1.

Приклад структури ЕНК, розробленого на базі платформи дистанційного навчання Moodle, наведено у додатку 1.

3.2. Складові частини електронного навчального курсу повинні містити такі навчально-методичні матеріали:

Загальна інформація про курс:

Робоча програма. У робочій програмі зазначається мета та завдання вивчення курсу, його зміст, у якому відображаються назви тем кожного модуля з анотаціями, кількість годин на вивчення кожного модуля.

Приклад ресурсу «Робоча програма» наведено у додатку 2.

Календарний план. Відображає потижневий план проведення лекційних та практичних (семінарських, лабораторних) занять, а також виконання студентами завдань для самостійної роботи.

Шаблон та приклад календарного плану наведено у додатку 3.

Критерії оцінювання. Містить інформацію щодо системи оцінювання навчальних досягнень студентів з дисципліни, як поточних, так і підсумкових. З кожного модуля вказується розподіл балів за виконання завдань та шкала оцінювання.

Приклад оформлення такого ресурсу наведено у додатку 4.

Друковані та Інтернет-джерела. У цьому ресурсі пропонуються основні, додаткові друковані джерела з дисципліни та Інтернет-ресурси (додаток 5).

Глосарій. Містить основні терміни навчального курсу та їх означення, (додаток 6).

Оголошення. Оголошення використовуються НПП для анонсування подій, повідомлень про зміни у навчальному курсі тощо.

Зразок оголошення наведено у додатку.

Зміст модуля включає такі матеріали:

Теоретичний навчальний матеріал. Містить обов'язкові навчальні ресурси: 1) структуровані електронні матеріали, зміст яких відображає логіку навчання за курсом і надає студенту теоретичні відомості з модуля у повному обсязі (додаток 8); 2) мультимедійні презентації лекцій (додаток 9), 3) додаткові електронні навчальні матеріали: електронні конспекти лекцій, флеш-ролики; аудіо і відео матеріали; довідкові та нормативні документи (форми, шаблони, стандарти, нормативні акти, закони тощо).

Практичні (семінарські, лабораторні) роботи. У матеріалах курсу обов'язково має бути перелік лабораторних (практичних, семінарських) робіт у вигляді окремих ресурсів. До кожної роботи потрібно сформулювати мету та завдання, які забезпечують формування вмінь та навичок, необхідних для засвоєння теми, надати методичні рекомендації з їх виконання, форму подання результатів виконаної роботи, критерії оцінювання кожної роботи, список індивідуальних завдань, завдань для виконання у парах та групами. Лабораторні роботи, для виконання яких необхідно спеціальне обладнання та реальні об'єкти, виконуються в аудиторних умовах, про що зазначається при формулюванні завдання. Навчально-методичні матеріали з практичних (семінарських, лабораторних) робіт потрібно оформляти у вигляді: веб-сторінки (сторінок), посилань на файли різних форматів та завдань (додаток 10). Результат виконання лабораторної (практичної) роботи студенти можуть надсилати викладачеві в електронній формі до навчального порталу, подавати у паперовому вигляді або усно. Після перевірки та оцінювання виконаних завдань, викладач має виставити бали до електронного журналу ЕНК (див. рис. додаток 11).

Завдання для самостійної роботи. Значна частина навчальних годин при вивченні кожної дисципліни відводиться на самостійне опрацювання. У матеріалах електронного навчального курсу необхідно розмістити додатковий теоретичний матеріал, завдання для самостійного виконання та методичний матеріал, який забезпечить його якісне виконання студентами. Завдання формулюється у такій формі: текст завдання, форма

подання результатів виконання, критерії оцінювання, термін виконання, список додаткових друкованих та Інтернет-джерел. (додаток 12). Результати виконання завдання можна надсилати викладачеві в електронній формі до навчального порталу, подавати у паперовому вигляді або усно.. Після перевірки та оцінювання виконаних завдань, викладач має виставити бали до електронного журналу ЕНК (див. рис. додаток 11).

Модульний контроль. Для оцінювання знань, умінь та навичок, набутих під час вивчення кожного модуля курсу, використовуються індивідуальні завдання, тести та опитування за допомогою контрольних запитань. Платформа Moodle дозволяє створювати тестові завдання 10 різних типів. Методика розробки тестових завдань та формування тесту наведена у додатках 13 та 14. Кожний модуль має містити тест для самоконтролю, контрольні запитання та контрольний тест. Результати оцінювання навчальних досягнень кожного студента автоматично заносяться до електронного журналу після тестування (див. рис. додаток 11).

Підсумкова атестація – передбачає наявність матеріалів для підготовки студентів до складання заліків та іспитів (наприклад, контрольні запитання, типові завдання) та підсумковий тест. Методика створення підсумкового тесту та оформлення результатів у вигляді атестаційної відомості наведена у додатках 14 та 15.

3.3. Результати навчання студентів фіксуються у журналі оцінок ЕНК. У електронному журналі оцінок викладачем задаються категорії для оцінювання всіх видів навчальної діяльності та визначається їх обсяг (у відсотках) по відношенню до підсумкової оцінки з дисципліни.

Наприклад:

Категорії	Обсяг
Модуль 1 – Модуль 2 – Модуль 3 –	15% 20 % 20 %
Підсумкова атестація –	30%
Всього	100 %

Приклад журналу оцінок та розрахунку обсягу кожного модуля наведено у додатку 11.

4. Порядок внутрішньої сертифікації ЕНК

4.1. Внутрішня сертифікація ЕНК на рівні ВНЗ здійснюється студентами, колегами – співробітниками та спеціально створеною комісією.

4.2. Студенти, зареєстровані на курсі, та колеги – співробітники заповнюють анкету (додаток 16), у якій висловлюють своє відношення до розробленого електронного курсу. Результати анкетування складають j загальної оцінки за електронний навчальний курс.

4.3. Комісія по сертифікації ЕНК очолюється проректором відповідальним за даний напрям роботи у ВНЗ, її склад затверджується відповідним наказом ректора університету. Рішення комісії щодо можливості сертифікації ЕНК складає s загальної оцінки за ЕНК і ґрунтується на трьох видах експертиз: структурно-функціональної, змістовно-наукової та методичної.

Структурно-функціональна експертиза передбачає аналіз виконання загальносистемних вимог до ЕНК (додаток 17, табл.1), наявності обов'язкових складових ЕНК та визначення відповідності кожної складової вимогам, визначеним у додатку 17 (табл. 2, 3).

Змістовно-наукова експертиза передбачає аналіз науковості матеріалів курсу, відповідності змісту державним стандартам освіти, цілям і завданням дистанційного курсу. Оцінюється актуальність змісту, новизна матеріалу, що подається, його завершеність і логічна узгодженість (додаток 17, табл.4).

Методична експертиза передбачає оцінювання методичних аспектів організації дистанційного курсу, педагогічно-психологічних засад організації навчальної діяльності студентів та НПП, їх взаємодії, організації системи контролю. Різнобічність цієї експертизи вимагає залучення для її проведення спеціалістів з питань тестування, використання інтерактивних методів, сучасних інформаційно-освітніх технологій (додаток 17, табл.5).

4.4. Експертиза ЕНК здійснюється групою фахівців, які призначаються рішенням комісії із сертифікації ЕНК, до якої входять: фахівець з предметної області для здійснення змістовно-наукової експертизи – експерт зі змісту;

фахівець з методики організації дистанційного навчання для здійснення структурно-функціональної та методичної експертизи - експерт з методики дистанційного навчання. Кожний експерт, залучений до експертизи, оцінює ЕНК за критеріями, наведеними у додатку 17, складає експертний висновок за формою (додаток 18) і подає його для розгляду комісії університету із сертифікації ЕНК. Комісія приймає ЕНК для сертифікації за умови, що висновки експертів носять позитивний характер і по кожному виду експертизи набрано не менше 80 балів.

4.5. Порядок проведення сертифікації ЕНК у ВНЗ: проведення анкетування студентів і колег;

призначення експертів для здійснення експертизи ЕНК здійснюється на підставі рішення комісії з сертифікації ЕНК;

проведення експертизи відбувається згідно з Положенням, затвердженим ректором університету;

висновки експерта зі змісту розглядаються та затверджуються на засіданні відповідної кафедри університету, яка несе відповідальність за якість змісту електронного навчального курсу.

рішення комісії університету з сертифікації ЕНК, яке формується на основі висновків експертів та презентації ЕНК автором,

затвердження рішення комісії із сертифікації ЕНК Вченою радою університету щодо рекомендації до використання ЕНК у навчальному процесі з грифом Університету «сертифіковано».

5. Порядок сертифікації ЕНК на рівні Міністерства освіти і науки України

5.1. Сертифікація ЕНК з наданням грифу МОН здійснюється у відповідності до наказу Міністерства освіти і науки України №537 від 17.06.2008 р., згідно з яким грифи МОН надають електронним засобам навчального призначення (засоби навчання, що зберігаються на цифрових або аналогових носіях даних і відтворюються на електронному обладнанні: комп'ютерні програми загально-дидактичного спрямування, електронні таблиці, електронні бібліотеки, слайдтеки, тестові завдання, віртуальні лабораторії тощо).

5.2. Організація проведення експертизи електронних навчальних курсів покладається на Інститут інноваційних технологій і змісту освіти та Головний центр сертифікації та акредитації МОН України на базі УкрНЦРІТ.

5.3. Для одержання грифа МОН автор ЕНК проходить внутрішню сертифікацію ЕНК відповідно до прийнятого Положення у ВНЗ і після успішної сертифікації звертається з листом-клопотанням до Інституту. У листі-клопотанні зазначають: повну назву електронного навчального курсу, URL-адресу розміщення електронного навчального курсу та необхідні дані для доступу до нього; автора (авторів), кому адресований електронний навчальний курс, тип навчального закладу відповідно до освітнього чи освітньо-кваліфікаційного рівня, відповідність ЕНК навчальній програмі із зазначенням предмета чи курсу (дисципліни), результати внутрішньої сертифікації ЕНК (експертні висновки з трьох видів експертиз та витяг з рішення Вченої ради ВНЗ), інструкцію користувача електронного навчального курсу.

5.3. Подані матеріали реєструють в Інституті (за адресою 04070, м. Київ, вул. Сагайдачного, 37). Науково-методичною радою з питань освіти МОН визначаються експерт з науково-змістовної експертизи.

Головний центр сертифікації та акредитації МОН України на базі УкрНЦ РІТ здійснює структурно-функціональну та методичну експертизу ЕНК.

5.4. Експерти в термін до двох місяців дають оцінку якості електронного

навчального курсу, відповідності вимогам галузевих та державних стандартів, та критеріям, визначеним у даному Положенні.

5.5. Висновок науково-змістовної розглядається відповідною комісією Науково-методичної ради з питань освіти МОН, яка виносить рішення про можливість надання електронному навчальному курсу відповідного грифа МОН та у тижневий термін повертає до Інституту розглянуті матеріали разом із випискою з протоколу засідання комісії.

5.6. експертизи та виносить рішення про можливість надання електронному навчальному курсу відповідного грифа МОН. Після прийняття рішення директор центру у тижневий термін повертає до Інституту розглянуті матеріали разом із випискою з протоколу засідання Центру.

5.7. Узагальнені матеріали та пакет необхідних документів щодо надання грифа МОН не пізніше ніж 14 робочих днів передаються Інститутом до МОН для затвердження відповідного рішення Колегією.

5.8. Після затвердження рішення про надання грифа МОН, у десятиденний термін надсилає лист про надання грифа МОН автору ЕНК або ВНЗ, який звертався з клопотанням щодо надання грифу МОН.

Додаток 1

Приклад структури ЕНК на базі платформи Moodle

На рис.3 наведено приклад структури ЕНК з дисципліни «Техніка презентації та Web-дизайн». Кожна складова частина ЕНК повинна мати заголовок і відповідати структурі, наведеній на рис.1. У заголовку кожного модуля наводиться його вага у загальній рейтинговій оцінці.

Розрахунок «ваги» кожного модуля можна виконати за формулою

$V_i = \frac{0.7 * k_i}{\Sigma k_i} * 100\%$, *де* k_i *- кількість кредитів з модуля*, Σk_i *загальна кількість кредитів з дисципліни*.

Наприклад, на вивчення дисципліни «Техніка презентації і Web-дизайн» відводиться 54 год., або 1,5 кредитів, з них - для вивчення 1 модуля – 0,65 кредитів, 2 модуля – 0,85 кредитів. Тоді вага 1 модуля буде $V_1 = \frac{0.7 * 0.65}{1.5} * 100\% = 30\%$, $V_2 = \frac{0.7 * 0.85}{1.5} * 100\% = 40\%$, вага атестації – 30%, всього 100 %.

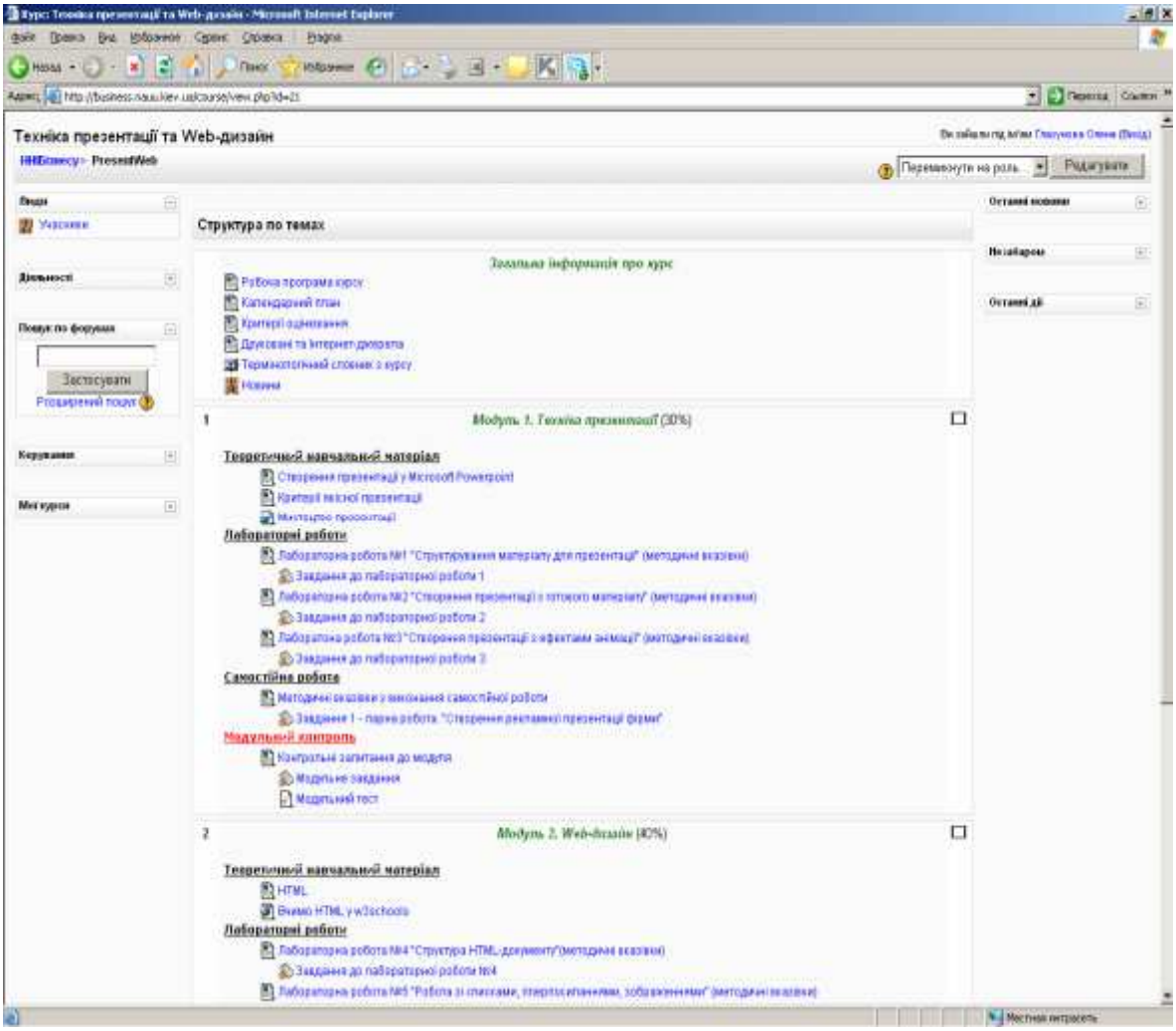

Техніка презентації та Web-дизайн
Структура по темах
Загальна інформація про курс
Робоча програма курсу
Календарний план
Критерії оцінювання
Дружові та Інтернет-дискусія
Термінологічний словник з курсу
Новини
Модуль 1. Техніка презентацій (30%)
Теоретичний навчальний матеріал
Створення презентації у Microsoft Powerpoint
Критерії якісної презентації
Методичні рекомендації
Лабораторні роботи
Лабораторна робота №1 "Структурування матеріалу для презентації" (методичні вказівки)
Завдання до лабораторної роботи 1
Лабораторна робота №2 "Створення презентації з готового матеріалу" (методичні вказівки)
Завдання до лабораторної роботи 2
Лабораторна робота №3 "Створення презентації з ефектами анімації" (методичні вказівки)
Завдання до лабораторної роботи 3
Самостійна робота
Методичні вказівки з виконання самостійної роботи
Завдання 1 – парна робота "Створення рекламної презентації фірми"
Модульний контроль
Контрольні запитання до модуля
Модульне завдання
Модульний тест
Модуль 2. Web-дизайн (40%)
Теоретичний навчальний матеріал
HTML
Вчимо HTML у w3schools
Лабораторні роботи
Лабораторна робота №4 "Структура HTML-документу"(методичні вказівки)
Завдання до лабораторної роботи №4
Лабораторна робота №5 "Робота зі списками, гіперпосиланнями, зображеннями" (методичні вказівки)

Рис.3

Додаток 2

Приклад подання ресурсу «Робоча програма», який входить до ЕНК «Економетрія»

На рис.5 наведено приклад робочої програми з дисципліни «Економетрія». Ресурс «Робоча програма» розміщується у секції «Загальна інформація про курс» (1). В робочій програмі наводиться: назва дисципліни, назва спеціальності, курс, семестр, кількість тижнів, кількість годин лекційних, практичних, для самостійної роботи, форма контролю (залік, іспит) (2); мета та задачі, вимоги до знань і вмінь, знання і вміння, яких студент набуде після вивчення дисципліни (3), короткі анотації щодо змісту кожної теми в модулі та кількість годин(кредитів), що відводяться на їх вивчення (4).

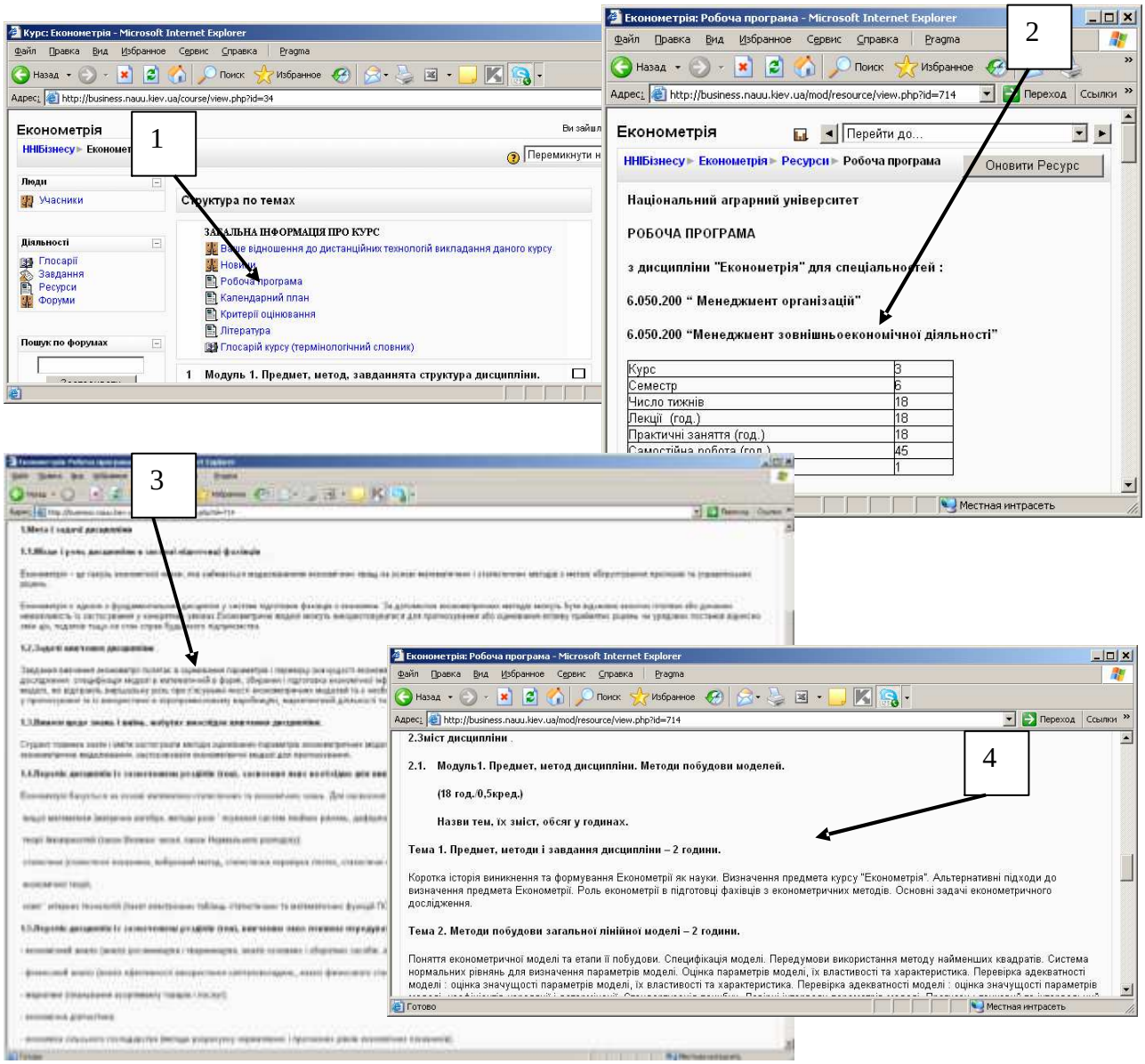
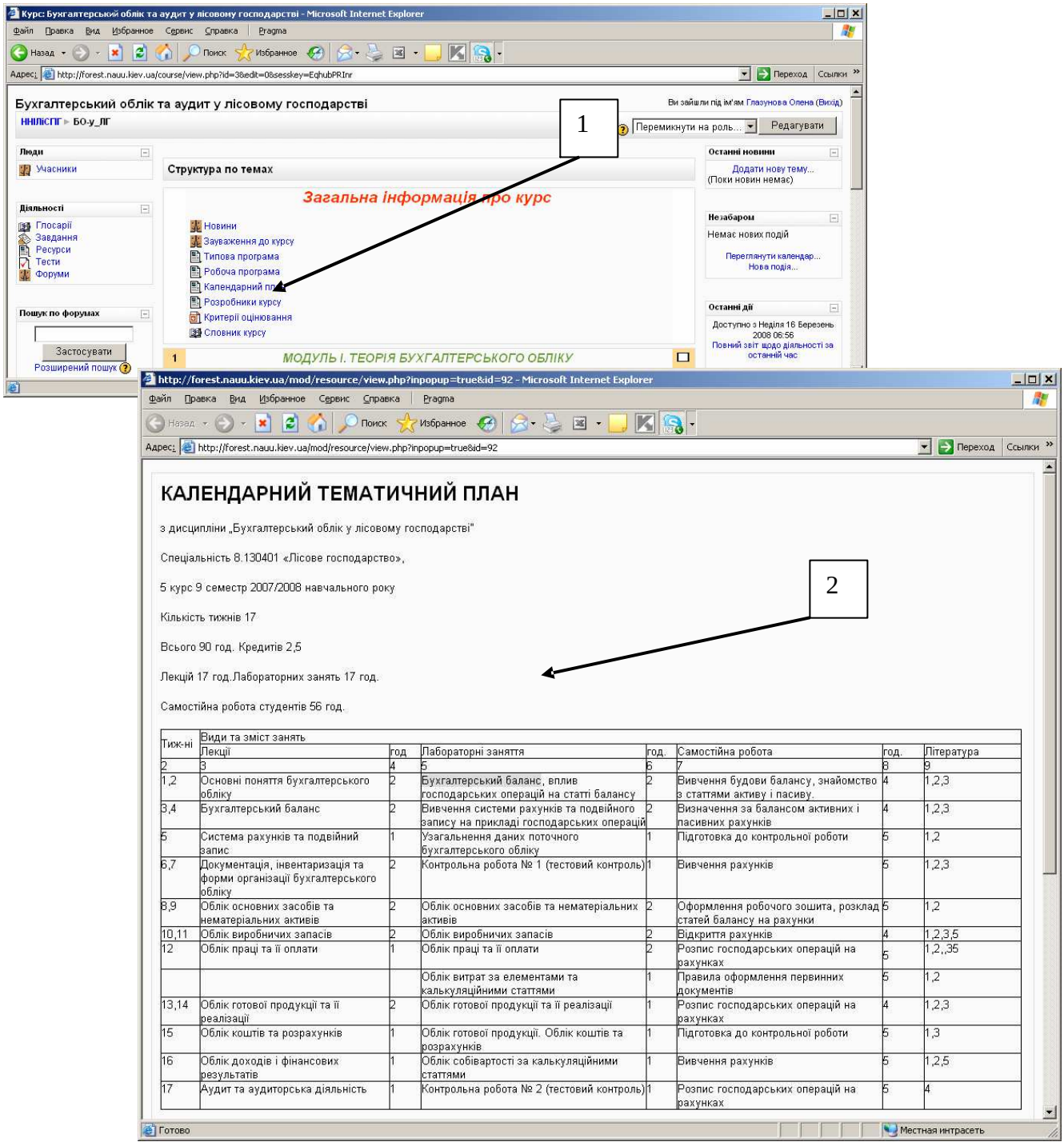


Рис.5

Додаток 3

Приклад подання ресурсу „Календарний план”, який входить до ЕНК з дисципліни «Бухгалтерський облік у лісовому господарстві»

На рис.6 подано приклад календарного плану з дисципліни «Бухгалтерський облік у лісовому господарстві». Ресурс «Календарний план» розміщується у секції «Загальна інформація про курс» (1). У ньому відображається потижневе планування усіх видів навчальної діяльності (2).



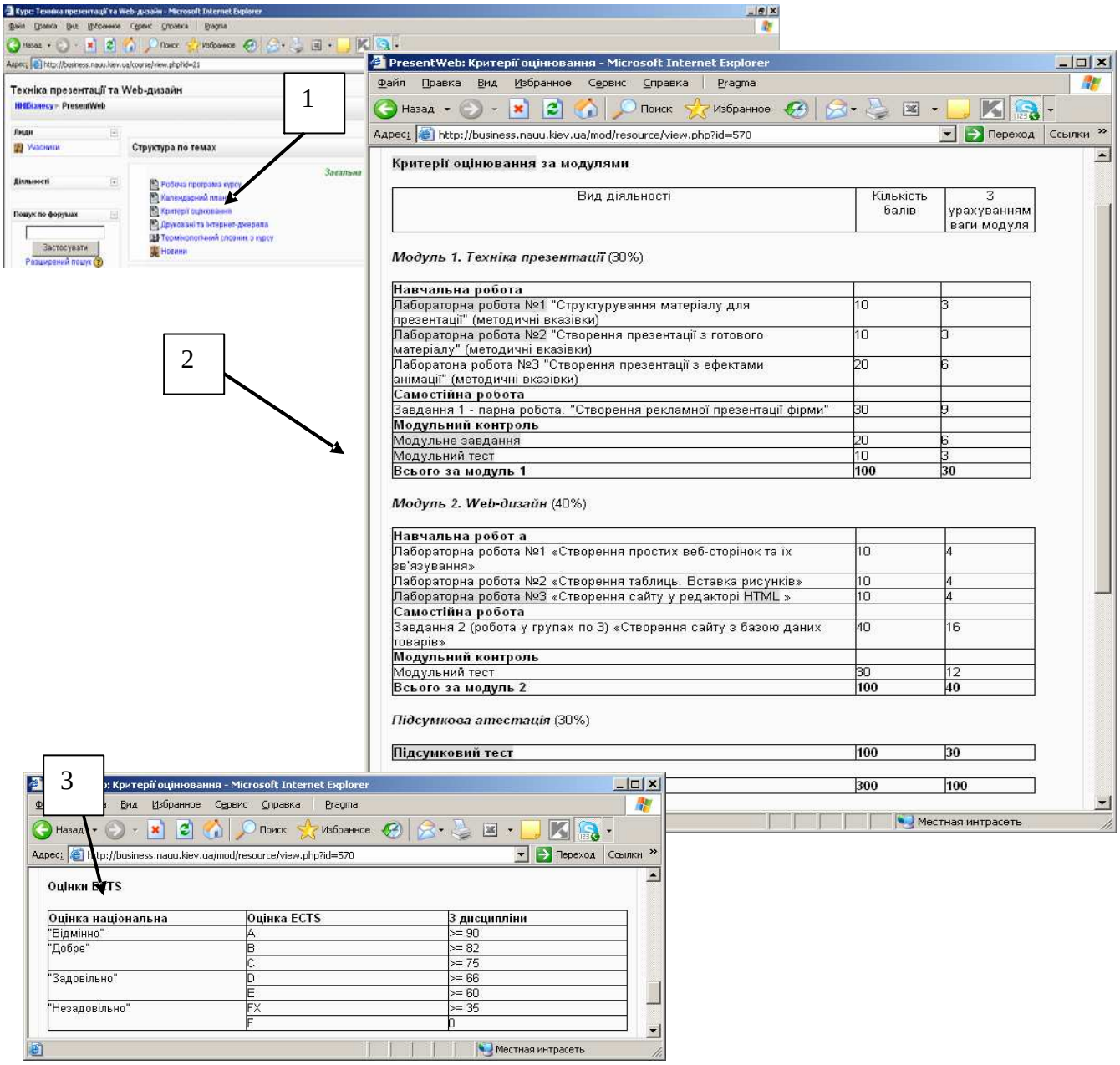
Тиж-ні	Види та зміст занять							
	Лекції	год.	Лабораторні заняття	год.	Самостійна робота	год.	Література	
2	3	4	5	6	7	8	9	
1,2	Основні поняття бухгалтерського обліку	2	Бухгалтерський баланс, вплив господарських операцій на статті балансу	2	Вивчення будови балансу, знайомство з статтями активу і пасиву.	4	1,2,3	
3,4	Бухгалтерський баланс	2	Вивчення системи рахунків та подвійного запису на прикладі господарських операцій	2	Визначення за балансом активних і пасивних рахунків	4	1,2,3	
5	Система рахунків та подвійний запис	1	Узагальнення даних поточного бухгалтерського обліку	1	Підготовка до контрольної роботи	5	1,2	
6,7	Документація, інвентаризація та форми організації бухгалтерського обліку	2	Контрольна робота № 1 (тестовий контроль)	1	Вивчення рахунків	5	1,2,3	
8,9	Облік основних засобів та нематеріальних активів	2	Облік основних засобів та нематеріальних активів	2	Оформлення робочого зошита, розклад статей балансу на рахунки	5	1,2	
10,11	Облік виробничих запасів	2	Облік виробничих запасів	2	Відкриття рахунків	4	1,2,3,5	
12	Облік праці та її оплати	1	Облік праці та її оплати	2	Розпис господарських операцій на рахунках	5	1,2,,35	
			Облік витрат за елементами та калькуляційними статтями	1	Правила оформлення первинних документів	5	1,2	
13,14	Облік готової продукції та її реалізації	2	Облік готової продукції та її реалізації	1	Розпис господарських операцій на рахунках	4	1,2,3	
15	Облік коштів та розрахунків	1	Облік готової продукції. Облік коштів та розрахунків	1	Підготовка до контрольної роботи	5	1,3	
16	Облік доходів і фінансових результатів	1	Облік собівартості за калькуляційними статтями	1	Вивчення рахунків	5	1,2,5	
17	Аудит та аудиторська діяльність	1	Контрольна робота № 2 (тестовий контроль)	1	Розпис господарських операцій на рахунках	5	4	

Рис.6

Додаток 4

Приклад оформлення критеріїв рейтингового оцінювання знань студентів з дисципліни

На рис.7 наведено приклад ресурсу «Критерії оцінювання» з дисципліни «Техніка презентації та Web-дизайн». Ресурс «Критерії оцінювання» розміщується у секції «Загальна інформація про курс» (1). У цьому ресурсі відображається розподіл оціночних балів за кожний вид навчальної діяльності при вивченні модулів з дисципліни (2) та відповідність національних оцінок з оцінками ECTS (3). [1]



Вид діяльності	Кількість балів	З урахуванням ваги модуля
Модуль 1. Техніка презентації (30%)		
Навчальна робота		
Лабораторна робота №1 "Структурування матеріалу для презентації" (методичні вказівки)	10	3
Лабораторна робота №2 "Створення презентації з готового матеріалу" (методичні вказівки)	10	3
Лабораторна робота №3 "Створення презентації з ефектами анімації" (методичні вказівки)	20	6
Самостійна робота		
Завдання 1 - парна робота. "Створення рекламної презентації фірми"	30	9
Модульний контроль		
Модульне завдання	20	6
Модульний тест	10	3
Всього за модуль 1	**100**	**30**
Модуль 2. Web-дизайн (40%)		
Навчальна робот а		
Лабораторна робота №1 «Створення простих веб-сторінок та їх зв'язування»	10	4
Лабораторна робота №2 «Створення таблиць. Вставка рисунків»	10	4
Лабораторна робота №3 «Створення сайту у редакторі HTML »	10	4
Самостійна робота		
Завдання 2 (робота у групах по 3) «Створення сайту з базою даних товарів»	40	16
Модульний контроль		
Модульний тест	30	12
Всього за модуль 2	**100**	**40**
Підсумкова атестація (30%)		
Підсумковий тест	**100**	**30**
	300	**100**

Оцінка національна	Оцінка ECTS	З дисципліни
"Відмінно"	A	>= 90
"Добре"	B	>= 82
	C	>= 75
"Задовільно"	D	>= 66
	E	>= 60
"Незадовільно"	FX	>= 35
	F	0

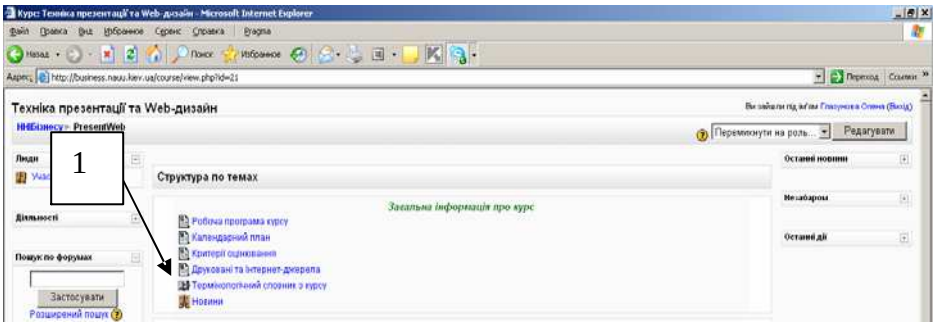
Рис.7

[1] Якщо під час вивчення модуля різні види аудиторної та самостійної навчальної діяльності не оцінюються, то можна навести лише критерії оцінювання для модульного контролю

Додаток 5

Приклад подання ресурсу „Друковані та Інтернет-джерела”

На рис.8 наведено приклад ресурсу «Друковані та Інтернет-джерела» з дисципліни «Техніка презентації та Web-дизайн». Ресурс «Друковані та Інтернет-джерела» розміщується у секції «Загальна інформація про курс» (1). У цьому ресурсі необхідно навести основні друковані джерела (2), які студенти повинні використовувати при вивченні дисципліни, додаткові друковані джерела (3) та Інтернет-джерела (4).



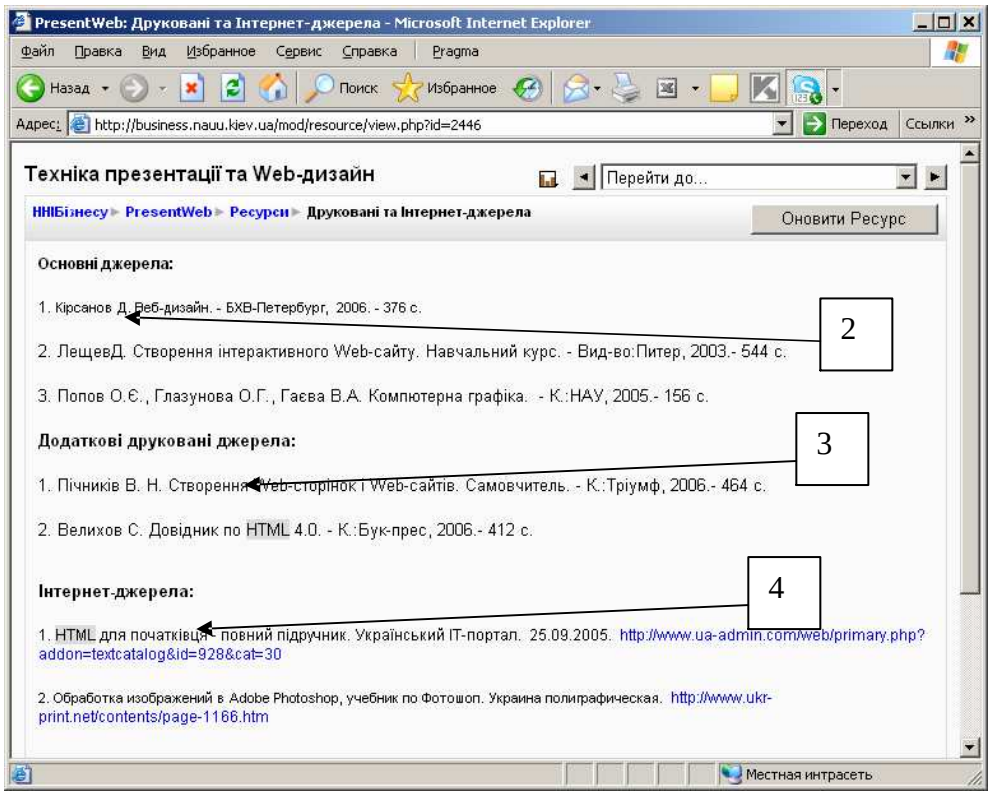


Рис.8

Додаток 6

Приклад подання термінологічного словника, створеного для ЕНК «Економічна інформатика» на базі платформи Moodle

Термінологічний словник або глосарій – активний ресурс ЕНК. Всі терміни та поняття, які потребують визначення, заносяться до глосарію (рис.9).

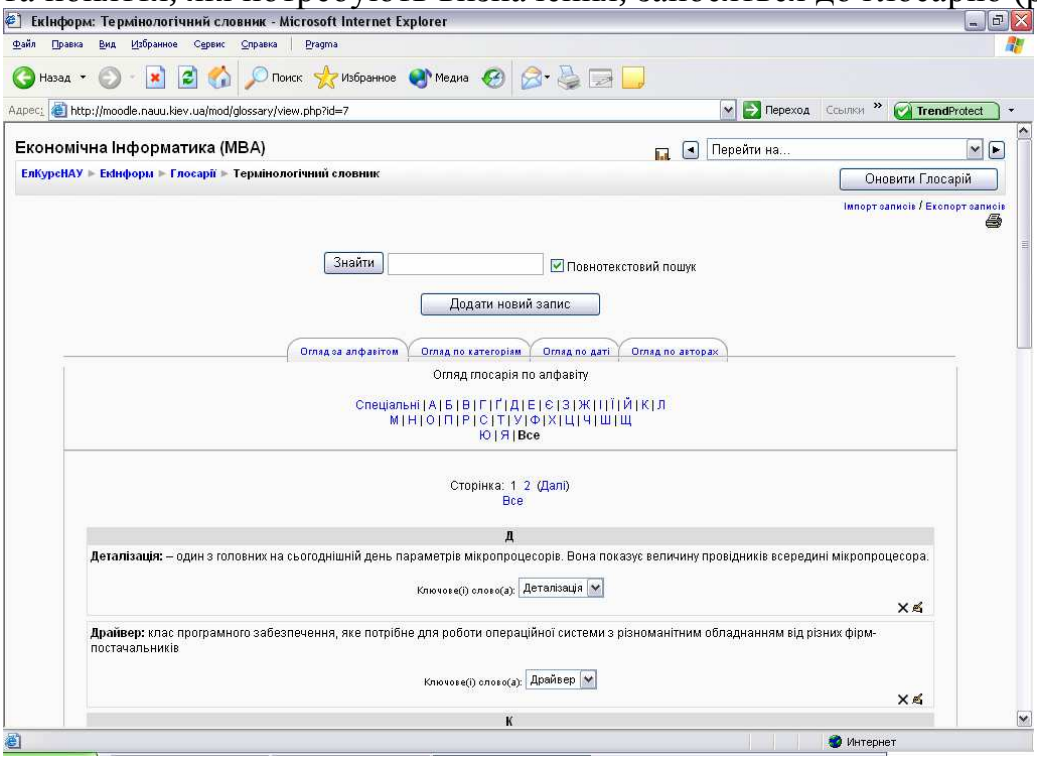


Рис.9

Занесені до глосарію терміни виділяються кольором у інших ресурсах ЕНК (рис.10). Клацнувши мишею по виділеному терміну у навчальному ресурсі (1), на екрані ПК отримаємо вікно з його означенням, яке наведене у глосарії (2).

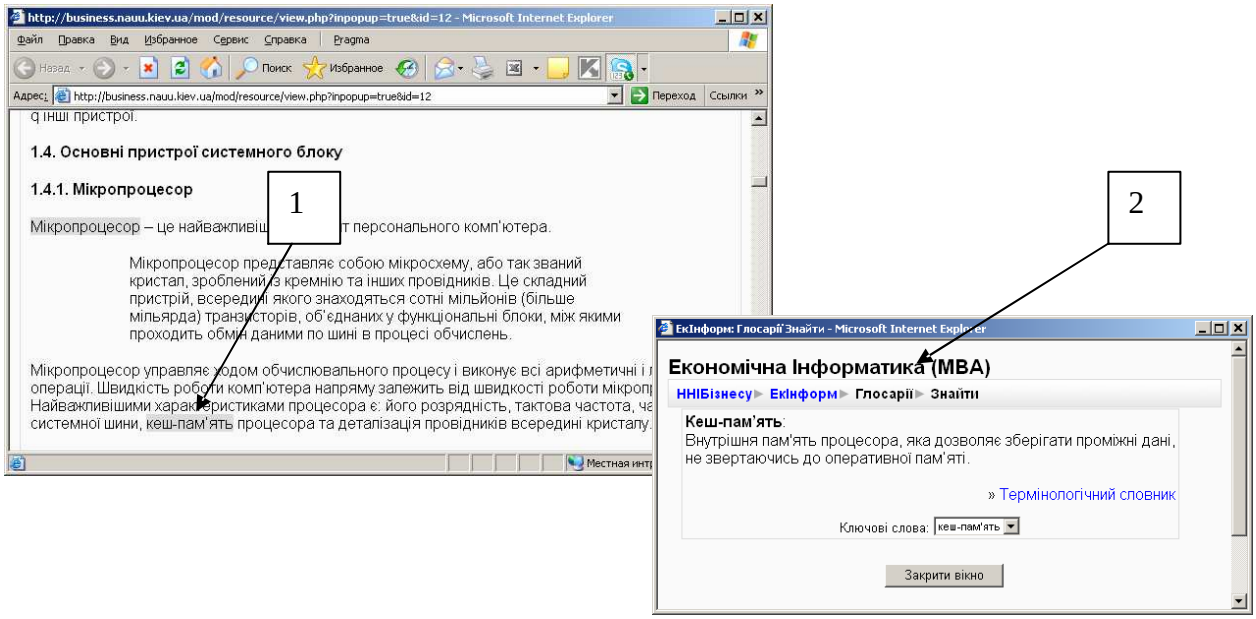


Рис.10

Додаток 7

Приклад подання оголошень у матеріалах електронного навчального курсу, створеного на платформі Moodle

У матеріалах курсу є можливість розміщувати оголошення. Викладач може розмістити оголошення (рис.11), наприклад, про проведення студентської конференції (1), а студент може прийняти участь у обговоренні, наприклад, написати тему доповіді, з якою він виступить на конференції. Крім того, можна розміщувати оголошення, що безпосередньо стосуються навчальної діяльності, наприклад, про виконання самостійної роботи (2).

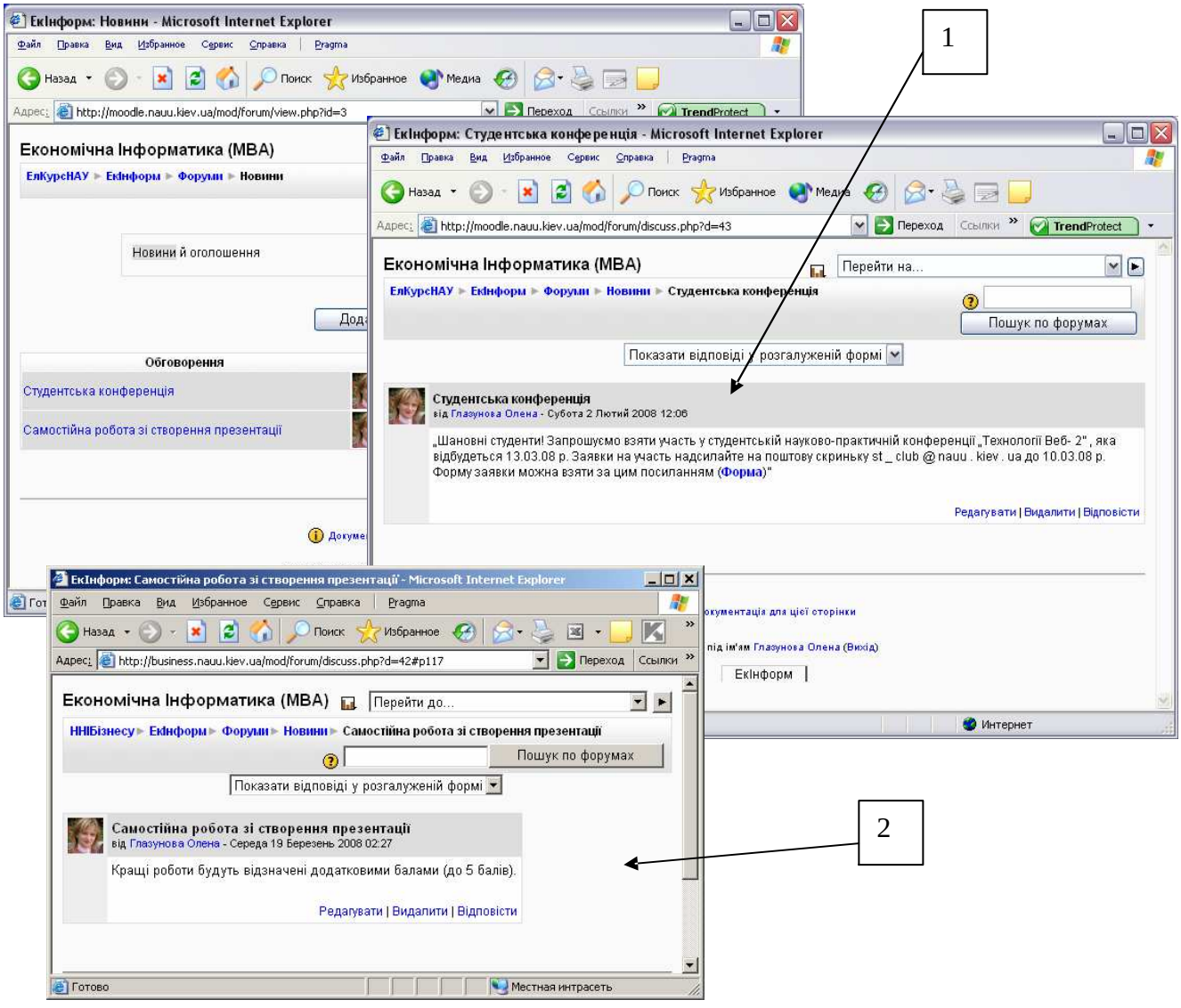


Рис.11

Додаток 8

Приклади подання структурованих електронних навчальних матеріалів в ЕНК, створеному на базі платформи Moodle

Структуровані електронні навчальні матеріали можна подати як ресурс типу „Веб-сторінка” (рис.12). У цьому ресурсі виводиться зміст теми. Кожний елемент змісту є гіперпосиланням на іншу веб-сторінку або на закладку цієї ж сторінки, де і розкривається зміст питання.

Наприклад, у розділі «Теоретичний матеріал» створено ресурс типу «Веб-сторінка» - «Структура інформаційної системи» (1). Цей ресурс відкриває головну сторінку зі змістом теми (2). З цієї сторінки можна перейти до будь-якого питання, що розкривається у темі.

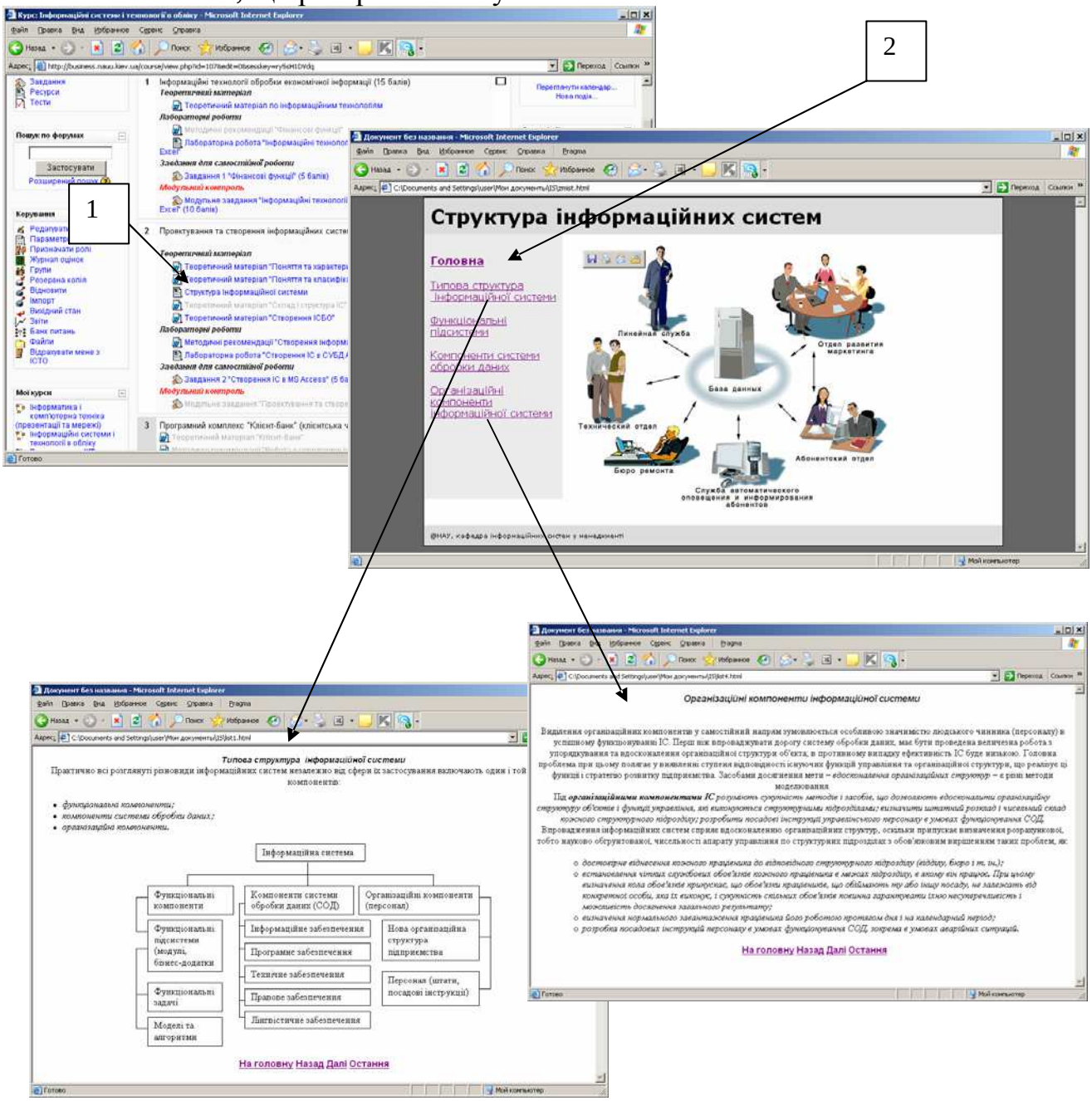


Рис.12

Додаток 9

Приклади подання презентацій лекцій в ЕНК, створеному на базі платформи Moodle

Навчальний ресурс у вигляді презентації подається як посилання на відповідний файл (рис.13). Студент має змогу відкрити його для перегляду або зберегти на своєму носії інформації.

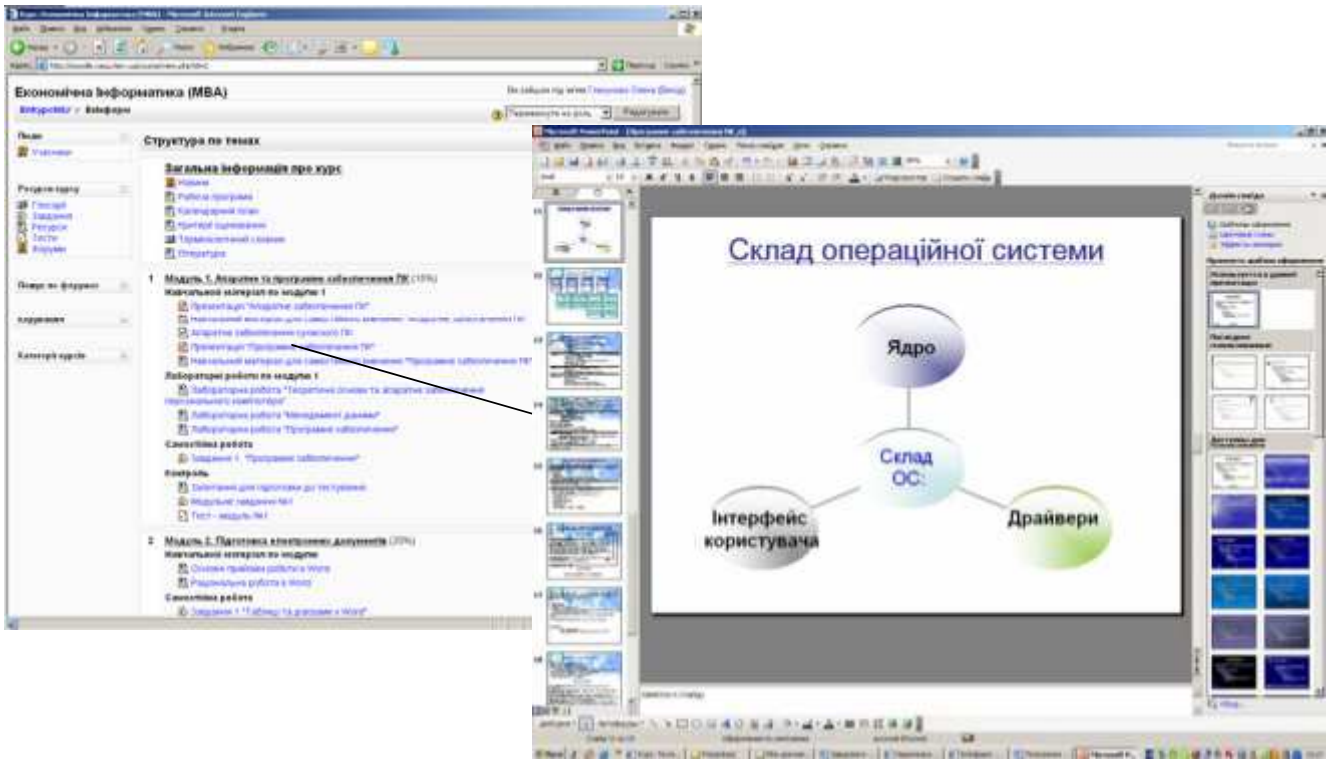


Рис.13

При створенні презентації потрібно дотримуватися таких основних правил:

- використовуються ключові слова і фрази, а не речення;
- на одному слайді виводиться одне ключове поняття;
- цифрові дані подаються у вигляді діаграм;
- теоретичний матеріал структурується та подається у схемах та організаційних діаграмах;
- теоретичний матеріал підкріплюється графічними зображеннями та відео-фрагментами;
- основний зміст подається логічно та грамотно;
- діаграми і графічні зображення використовуються відповідно до поставленої мети;
- ефекти анімації застосовуються для акцентування уваги на визначених моментах, поетапного виведення вмісту слайду на екран, для демонстрації руху або послідовності дій;
- для подання текстового матеріалу використовується шрифт з мінімальним розміром – 20 пт;
- фон, колір тексту та діаграм відповідають правилу 3-х кольорів та їх відтінків (у презентації використовувати 3 основні кольори та їх відтінки);
- презентація носить проблемний характер, не є точною копією друкованого підручника.

Додаток 10

Приклади подання навчально-методичних матеріалів для лабораторних (практичних) робіт

У цьому ресурсі потрібно розмістити: мету роботи; зміст роботи; завдання для індивідуального виконання; методичні вказівки щодо виконання завдань; форму подання результатів виконаної роботи; критерії оцінювання; термін, до якого потрібно подати звіт про виконане завдання.

Ресурс «Лабораторна робота» може бути поданий одним ресурсом типу «Завдання» або двома окремими ресурсами: «Лабораторна робота (методичні вказівки)» типу «веб-сторінка» і «Завдання до лабораторної роботи» типу «Завдання».

Наприклад (рис.14), у ЕНК «Техніка презентації та Web-дизайн», кожна лабораторна робота представлена за допомогою двох ресурсів. У першому (1) наводиться тема, мета, зміст та методичні вказівки до виконання роботи. У другому (2) – індивідуальні завдання, форма представлення результатів виконання, критерії оцінювання та термін подачі результатів виконання роботи.

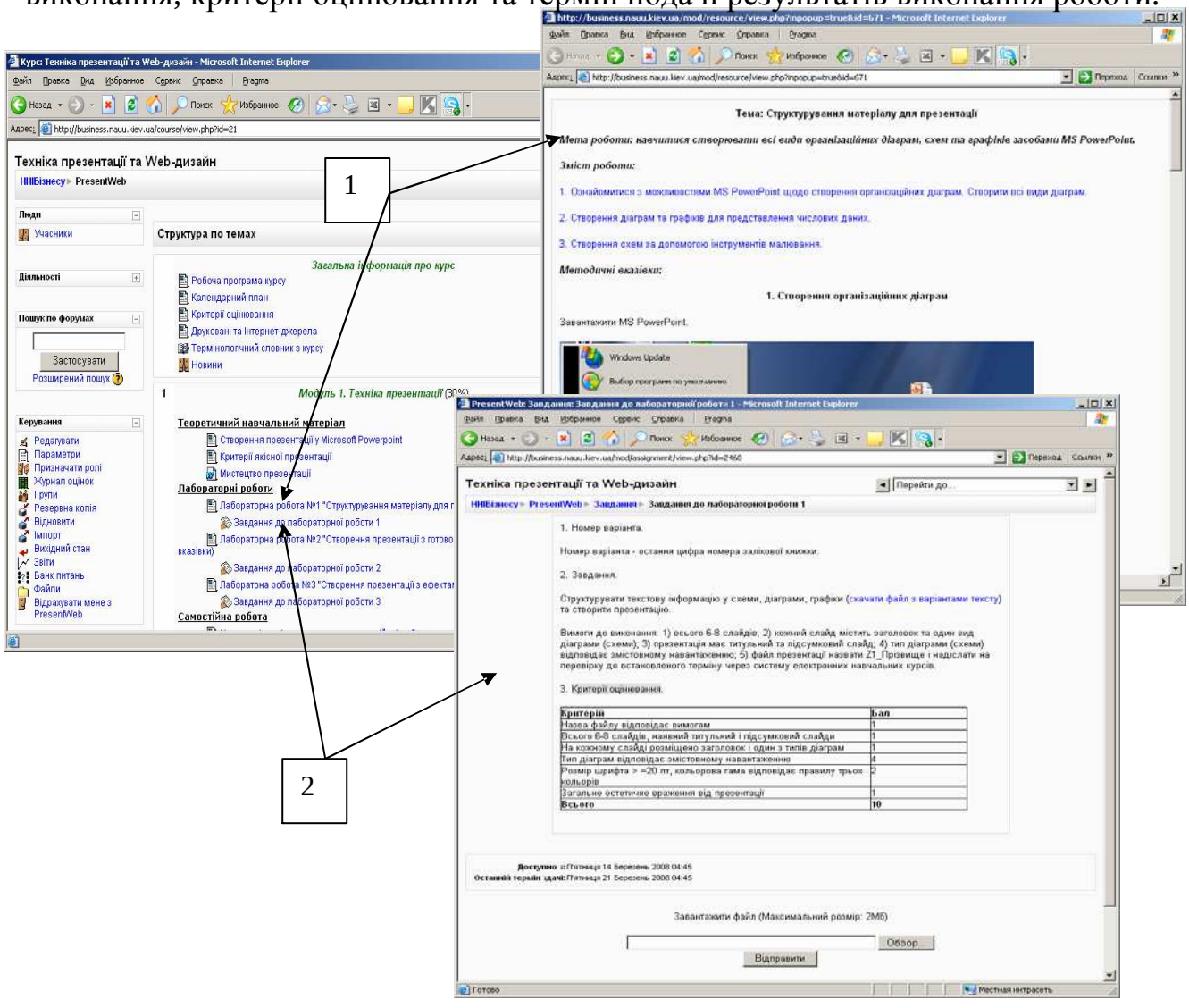


Рис. 14

Додаток 11

Приклад оформлення журналу оцінок у ЕНК на базі платформи Moodle

Щоб оформити журнал оцінок, необхідно знати «вагу» кожного модуля у загальній структурі оцінки з дисципліни.

Журнал оцінок відкривається кнопкою „Журнал оцінок” на панелі керування ресурсами курсу.

У журналі оцінок (рис.15) задаються категорії (1) для оцінювання (наприклад: модуль 1, модуль 2, атестація). В кожну категорію потрібно помістити завдання та тести, за якими здійснюється оцінювання навчальних досягнень (2). Оцінювання навчальних досягнень студентів з усіх модулів та підсумкової атестації здійснюється за 100-бальною шкалою. У журналі оцінок переглянути бали за кожне завдання та підсумкову оцінку з модуля (4) або лише підсумкову оцінку з модуля (5).

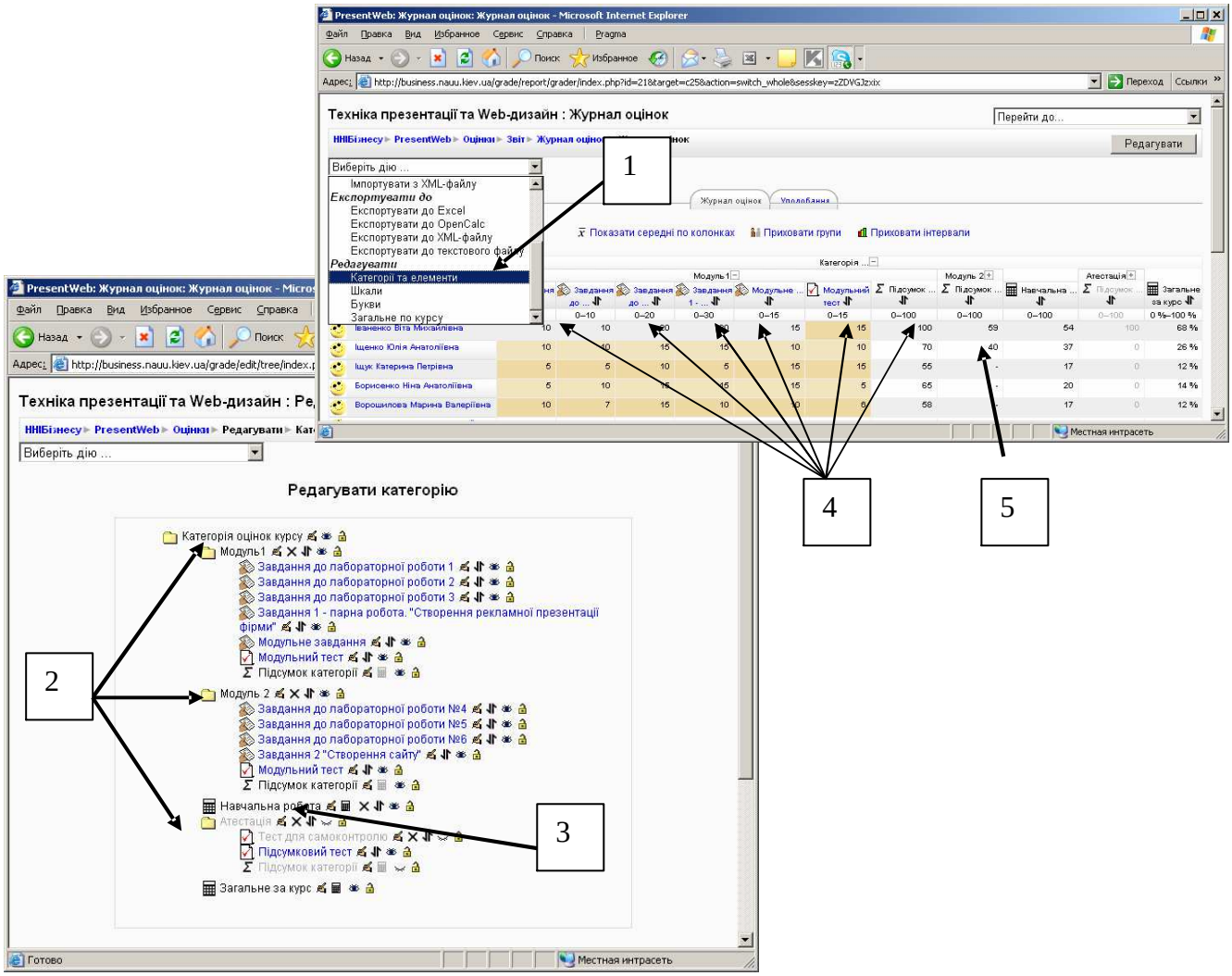


Рис.15

Додаток 12

Приклад подання навчального ресурсу типу „Завдання” для організації самостійної роботи студентів

Обов’язкові елементи при формулюванні завдання для самостійного виконання: текст завдання, вимоги до виконання та подачі результатів виконання, критерії оцінювання, термін подачі результатів виконання.

Платформа Moodle дозволяє створювати завдання різного типу для самостійної роботи студентів. Можна сформулювати завдання, відповіддю на яке буде файл. Студент формує відповідь на завдання у вигляді файлу і через навчальний ресурс „Завдання” відправляє його на сервер (див. рис.14, 2).

Інший тип завдань, який можна використати при роботі з платформою Moodle, - завдання з відповіддю у вигляді тексту (рис.16). Студент вводить відповідь у вікні завдання, відкривши текстовий редактор (рис.16 - 1).

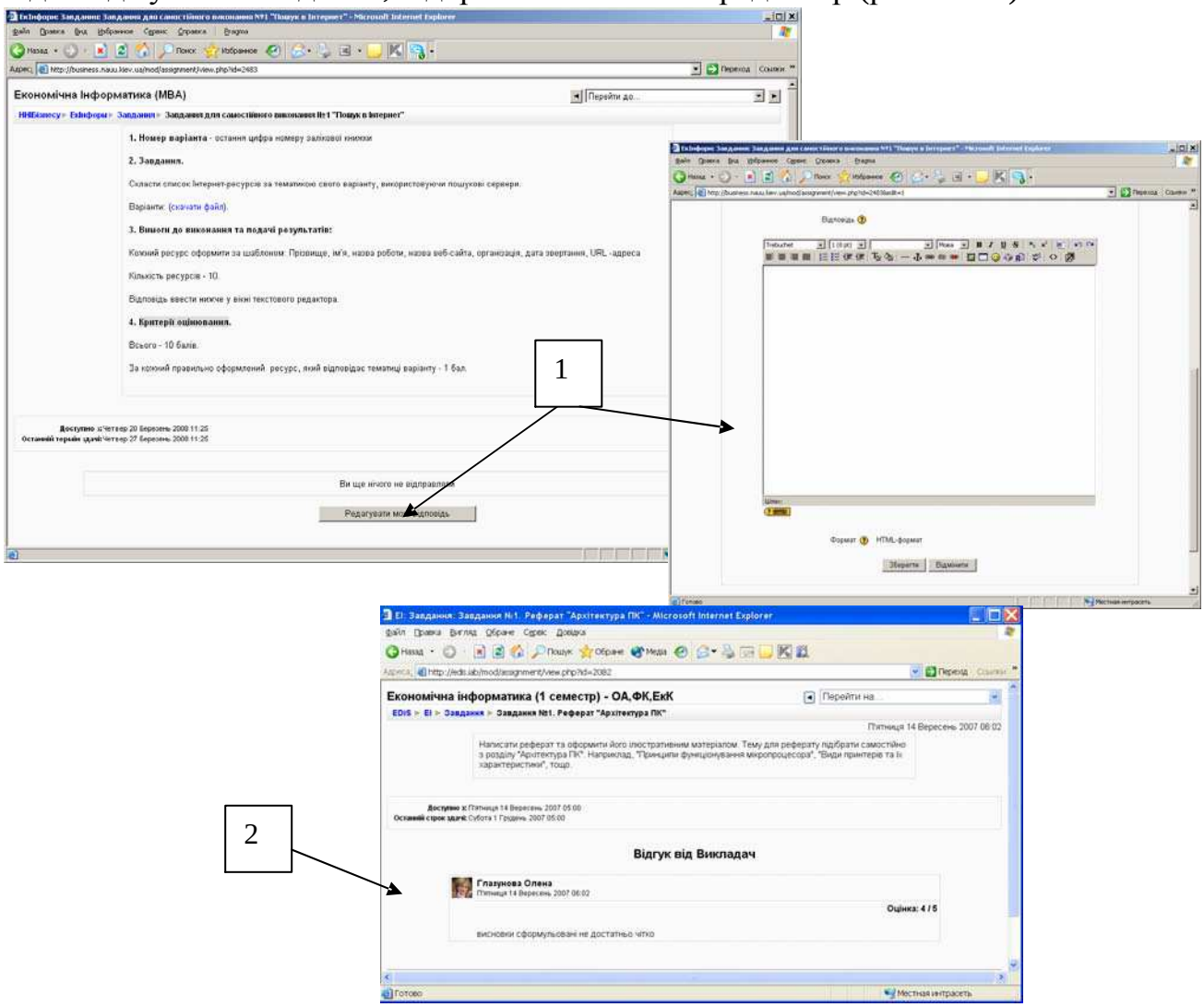


Рис.16

Викладач оцінює надіслані на сервер відповіді та надсилає студентам коментарі з приводу результатів виконаного завдання. На рис.16 -2 наведено відгук викладача на роботу студента.

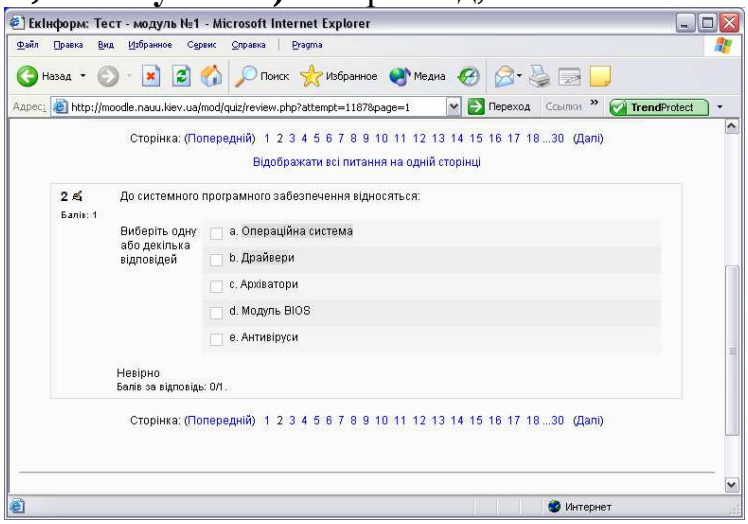
Додаток 13

Приклади тестових завдань, які можна сформувати у ЕНК на базі платформи Moodle:

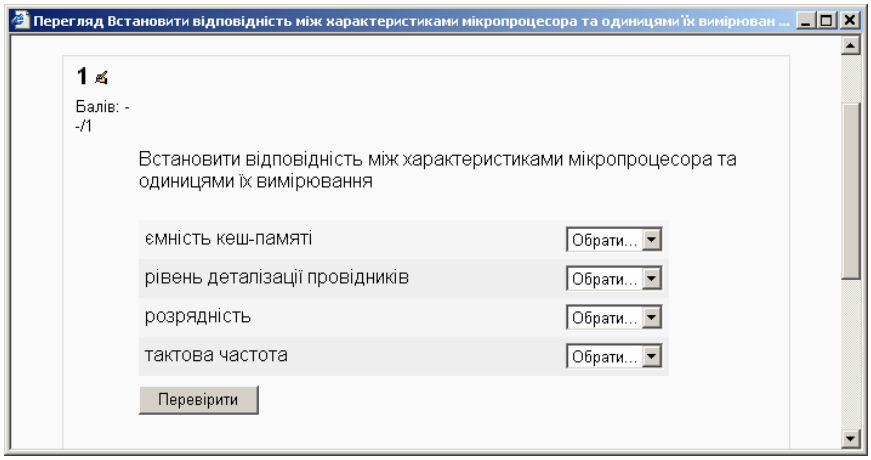
У ЕНК створюється банк тестових завдань за категоріями складності. У ЕНК на базі платформи Moodle можна створити тестові завдання різних типів, в тому числі, з використанням графічних зображень.

1. Завдання з вибором однієї правильної відповіді (допомагає діагностувати рівні засвоєння навчального матеріалу: **знання, розуміння, застосування** - за Б.Блумом**).** Наприклад,

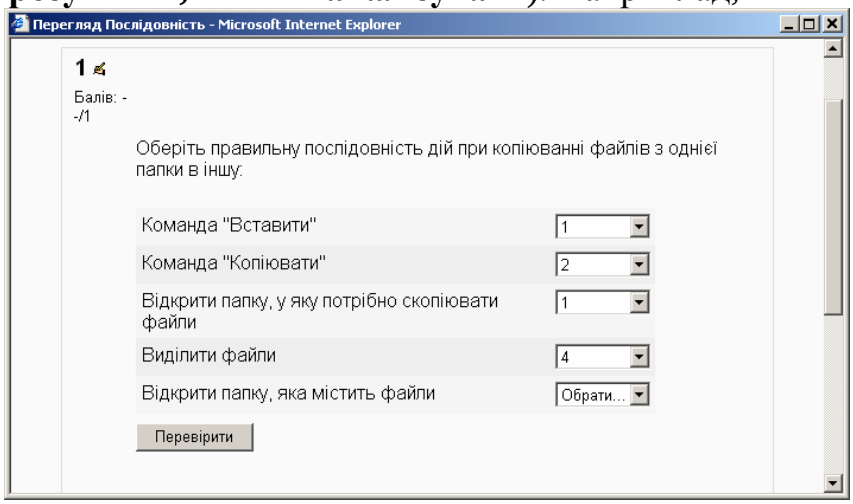
2. Завдання з можливістю множинного вибору (дозволяє діагностувати рівні: **знання, розуміння, застосування)**. Наприклад,



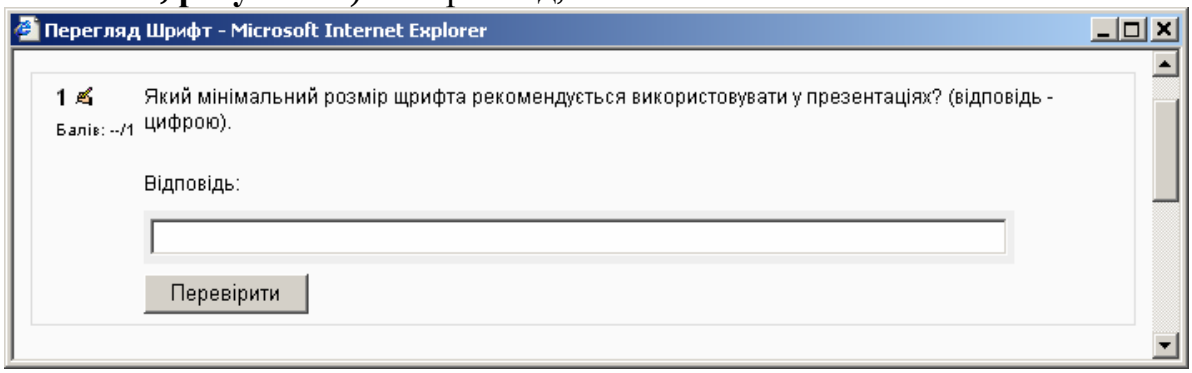
3. Завдання на визначення відповідності (дозволяє діагностувати рівні: **знання, розуміння**). Наприклад,



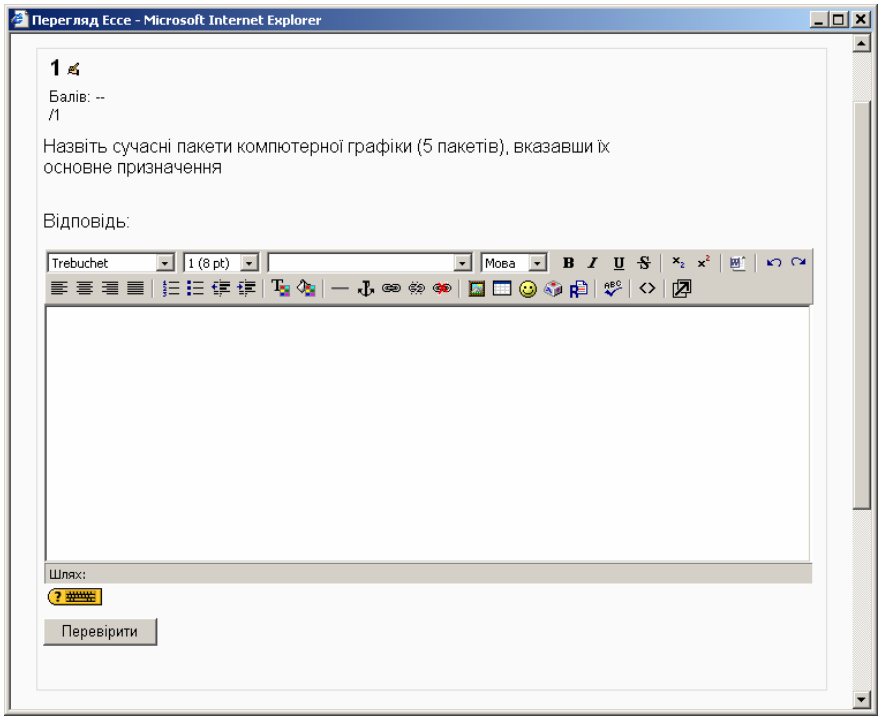
4. Завдання на встановлення правильної послідовності (дозволяє діагностувати рівні: **знання, розуміння, вміння аналізувати**). Наприклад,



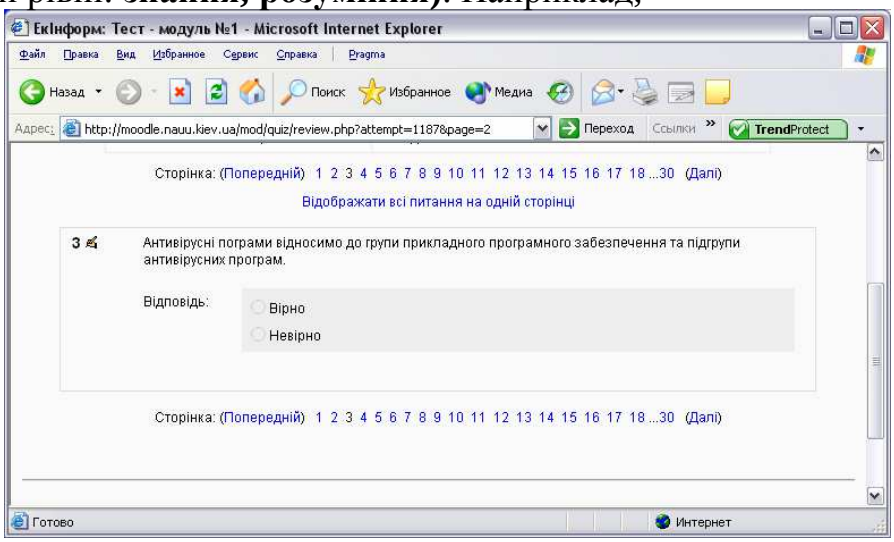
5. Завдання відкритого типу: коротка відповідь (дає можливість діагностувати рівні: **знання, розуміння**)*:* Наприклад,



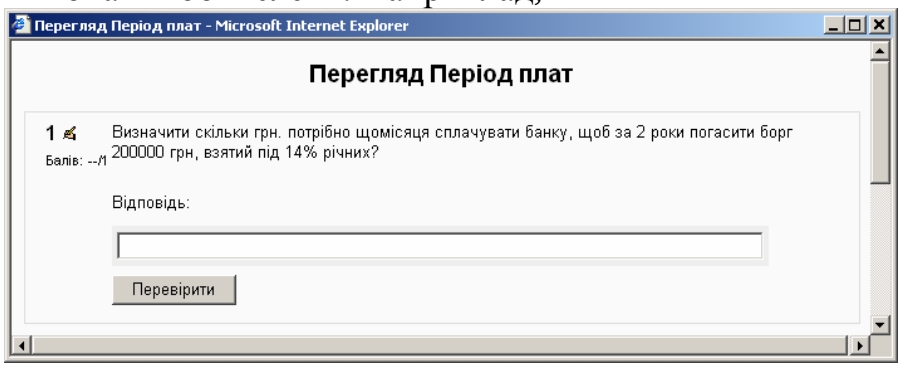
6. Завдання відкритого типу: есе (дозволяє діагностувати рівні: **знання, розуміння, аналіз, синтез, оцінювання**). Наприклад:



7.Завдання типу True/False (правильно/неправильно) (дає можливість діагностувати рівні: **знання, розуміння)**. Наприклад,



8. Завдання на отримання числової відповіді (допомагає діагностувати рівні: **знання, розуміння, застосування).** Такий тип питання передбачає допустиму похибку при виконанні обчислень. Наприклад,



Додаток 14

Приклад формування підсумкового тесту

Тест для підсумкової атестації створюється з використанням технологічної матриці, за якою визначається кількість тестових завдань з різних тем (модулів) для перевірки всіх рівнів засвоєння студентами навчального матеріалу.

Всі тестові завдання слід поділити на 2(3) категорії: „прості” та „складні” („прості”, „середньої складності”, „складні”). До категорії „простих” відносяться завдання на знання, розуміння, застосування за класифікацією таксономії Б.Блума. До категорії „складних” – завдання на синтез, аналіз, оцінювання. Для кожної категорії встановлюється відсоток використання тестових завдань при формуванні підсумкового тесту (наприклад, 70% завдань з категорії «прості», 30% завдань з категорії «складні»).

Визначивши «вагу» кожного модуля (наприклад, 35, 35, 30), визначаємо кількість тестових завдань, які потрібно взяти для перевірки знань з кожного модуля (в даному випадку 11, 10, 9). При цьому 70 % відводимо на оцінювання навичок мислення низького рівня за таксономією Б.Блума: знання, розуміння, застосування (відповідно 35, 25. 20), решта 30 % - на оцінювання вищих когнітивних рівнів: аналіз, синтез, оцінювання (відповідно 10,5,5). В результаті зазначених розрахунків створюється технологічна матриця розподілу тестових завдань у тесті за рівнями оцінювання та модулями.

	Категорія «Прості»			Категорія «Складні»				
	Знання	Розуміння	Застосу-вання	Аналіз	Синтез	Оцінювання	Вага модуля, %	Кількість тестів з модуля
Модуль 1	4	3	2	1	0	1	35	11
Модуль 2	4	3	2	1	1	0	35	10
Модуль 3	3	2	2	1	0	0	30	9
%	35	25	20	10	5	5	100	

Кількість завдань = 30

Додаток 15

Приклад формування атестаційної відомості у ЕНК

За результатами тестування формується підсумкова атестаційна відомість (рис.17). Платформа Moodle дозволяє переглянути результати тестування студентів по кожній групі (1), зберегти їх у форматі таблиці Excel (2), оформити у вигляді атестаційної відомості та вивести на друк .

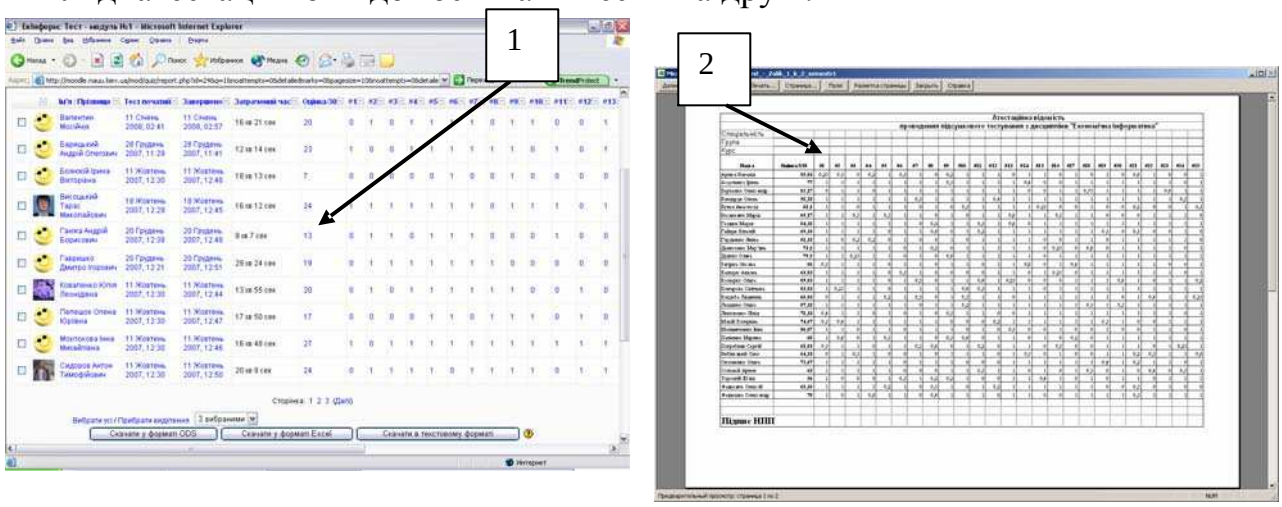


Рис.17

Оскільки тестування проводиться в електронному вигляді, то від студентів вимагається поставити свій підпис під отриманими результатами. Всі результати тестування студентів після проведення підсумкової атестації зберігаються в електронному вигляді на сервері разом з атестаційною відомістю протягом 1 навчального року. Результат кожного тестування при потребі може бути виведений на друк (рис.18).

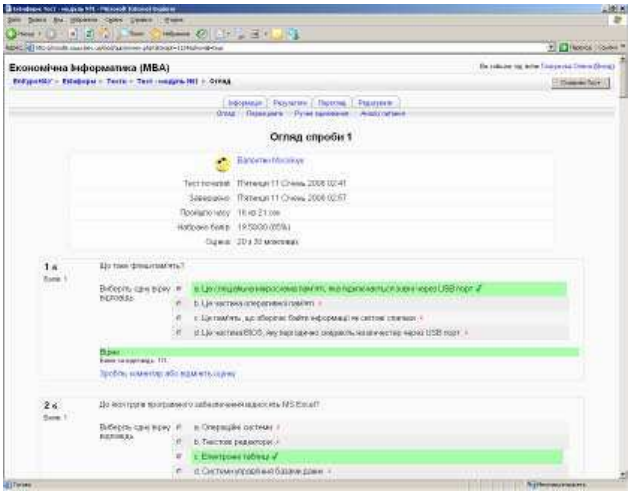


Рис.18

Додаток 16

Анкета «ЕНК очима студентів і співробітників»

Питання анкети	Повністю погоджуюсь	Погоджуюсь	Частково погоджуюсь	Не погоджуюсь	Категорично не згоден
1. Програма курсу чітко представлена, у зрозумілій формі подано план проведення занять і контрольних заходів					
2. Достатньо роз'яснені критерії проміжної та підсумкової атестації по дисципліні					
3. У оголошеннях та форумах подані актуальні питання для обговорення					
4. Запропоновані друковані та Інтернет джерела містять основні та додаткові навчально-методичні матеріали з дисципліни					
5. Зміст курсу добре структурований					
6. Ключові терміни достатньо пояснені					
7. Викладений матеріал актуальний і достатньо підкріплений графікою, мультимедіа, відео та аудіофрагментами					
8. Навчальний матеріал у електронному посібнику викладено у логічній послідовності, на доступному рівні, в обсязі достатньому для оволодіння навчальним матеріалом					
9. Навчальний матеріал викладено професійною мовою, грамотно					
10. В курсі реалізовано інтерактивний самоконтроль пройденого матеріалу					
11. Викладач використовує ефективні методи викладання, володіє матеріалом, викладає матеріал зрозумілою мовою					
12. Викладач представляє матеріал в цікавій манері стимулює активність студентів творче мислення студентів					
13. Ступінь трудомісткості самостійних робіт відповідає ресурсу часу					
14. Наявні теоретичні відомості щодо змісту, послідовності та методики виконання роботи, графічні зображення, приклад виконання завдань, індивідуальні завдання подані в обсязі достатньому для самостійного оволодіння студентами навчальним матеріалом					
15. Критерії оцінювання кожної практичної (самостійної) роботи дозволяють чітко зрозуміти границі якісного виконання завдання для отримання позитивної оцінки					
16. Тестові завдання охопюють навчальний матеріал, висвітлений у матеріалах курсу					
17. Забезпечується он-лайн та оф-лайн спілкування для проведення консультацій					
18. Постійне оцінювання (семінари, тести, анкети і ін.) відображає зміст курсу та здійснюється вчасно і об'єктивно					
19. Задоволений(а) якістю викладання дисципліни					
20. Задоволений(а) відповідністю предмету вибраній спеціальності					

Додаток 17

Критерії структурно-функціональної експертизи

Таблиця 1.

Загально системні критерії (структурно-функціональна експертиза)

№	Критерій	Характеристика	Так	Ні
Загально системні критерії (всього)			**100**	
1.	Відповідність стандартам	Платформа для розробки ЕНК підтримує стандарти IMS, SCORM	10	0
2.	Простота і надійність роботи з курсом	Робота з курсом здійснюється за допомогою звичайних браузерів Інтернету, без спеціального програмного забезпечення	10	0
3.	Кількість користувачів	Забезпечення можливості одночасної роботи групи користувачів з курсом	10	0
4.	Стійкість роботи з курсом	Забезпечення стійкої роботи на комп'ютерах різної конфігурації;	10	0
5.	Персоніфікація користувачів	Можливість зареєструватися для проходження курсу	10	0
6.	Збереження результатів	Фіксація і збереження результатів тестування та виконаних завдань	10	0
7.	Використання технологій Веб 2.0	Підтримка Вікі, блогів, форумів	10	0
8.	Керування ресурсами	Можливість керувати ресурсами курсу	10	0
9.	Забезпечення інтерактиву	Забезпеченя інтерактивного спілкування викладач-студент у режимі оф-лайн	10	0
10.		Забезпеченя інтерактивного спілкування викладач-студент у режимі он-лайн	10	0

Таблиця 2.

Критерії повноти (структурно-функціональна експертиза)

№	Розділ курсу	Елемент	**Тип1**	**Тип2**	**Тип3**
Повнота структури (всього)			100	100	100
1.	Загальна інформація про курс	Візитка курсу	2	2	2
2.		Робоча програма	4	4	4
3.		Графік навчання	2	2	2
4.		Методичні рекомендації по роботі з курсом	2	2	2
5.		Шкала оцінювання	2	2	2
6.		Друковані та Інтернет-джерела	2	2	2

7.		Глосарій	4	4	4
8.		Оголошення	2	2	2
9.	Навчальні матеріали з модулів	Електронний посібник до кожної теми відповідно до тематики робочої програми	10	10	10
10.		Презентації до усіх лекцій	10	5	5
11.		Відеозаписи усіх лекцій	10	5	5
12.		Практичні (лабораторні) роботи з тематикою відповідно до робочої програми	10	10	5
13.		Методичні рекомендації з виконання практичних (лабораторних) робіт	0	5	5
14.		Віртуальні лабораторні роботи	0	5	10
15.		Завдання для самостійної роботи	5	5	5
16.		Контрольні запитання (завдання)	5	5	5
17.		Тест для самоконтролю	5	5	5
18.		Контрольний тест	10	10	10
19.	Підсумкова атестація	Питання для підготовки	5	5	5
20.		Атестаційний тест	10	10	10

Колонки: Тип 1, Тип 2, Тип 3 - визначають тип дисципліни, для якої створюється ЕНК. Тип 1 – дисципліни теоретичного складу, які передбачають вивчення теоретичних положень, без практичних або лабораторних робіт, які не потребують розміщення у ЕНК відео фрагментів, методичних рекомендацій до виконання практичних робіт, наприклад, філософія, теорія економічних вчень, історія тощо. Тип 2 – технологічні дисципліни, матеріали до яких повинні включати і навчальні відео фрагменти, і графічні зображення, і ресурси для виконання практичних (лабораторних) робіт, можливо також віртуальні лабораторні роботи, наприклад, статистика, інформатика, основи агрономії тощо. Тип 3 – навчальні дисципліни для вивчення яких необхідно виконувати лабораторні досліди, а тому необхідно щоб ЕНК обов’язково містив віртуальні лабораторні практикуми. Прикладом дисциплін 3-го типу є фізика, хімія, біохімія, хірургія тощо.

Таблиця 3.

Критерії відповідності елементів курсу визначеній структурі та форматам (структурно-функціональна експертиза)

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень 2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
1.	Візитка курсу	Подано у форматі Веб-сторінки; вказана категорія студентів, для яких підготовлений курс, відомості про авторів курсу, коротка характеристика курсу (ключові теми курсу)	2	1	1	0	0
2.	Робоча програма	Подано у форматі Веб-сторінки; наявність мети та завдань вивчення курсу; наявність вимог до знань, умінь та навичок (вхідних та вихідних); вказано кількість годин на вивчення кожного модуля; відображаються назви тем з анотаціями	2	1	1	0	0
3.	Графік навчання	Подано у форматі Веб-сторінки, наявність потижневого планування проведення лекційних та практичних (семінарських, лабораторних)	2	1	1	0	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень 2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
		занять у формі таблиці, наявність потижневого планування виконання студентами завдань для самостійної роботи, вказується розподіл оціночних балів за виконання різних видів навчальної діяльності з кожного модуля					
4.	Методичні рекомендації по роботі з електронним курсом	Подано у форматі Веб-сторінки; даються чіткі інструкції студентам щодо вивчення теоретичного матеріалу, виконання практичних завдань, самостійної роботи, тестів	2	1	1	0	0
5.	Шкала оцінювання	Подається у форматі Веб-сторінки, наведена таблиця співвідношень національних оцінок та оцінок ECTS	2	1	1	0	0
6.	Друковані та Інтернет джерела	Подано у форматі Веб-сторінки, вказуються основні та додаткові друковані джерела з дисципліни, наводяться	2	1	1	0	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень 2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
		Інтернет-джерела з активними гіперпосиланнями					
7.	Термінологічний словник	Подано у форматі глосарія, означення наводяться до всіх термінів у словнику	2	1	1	0	0
8.	Оголошення	Подано у форматі форуму	1	1	1	0	0
9.	Теоретичний матеріал	Електронні навчальні матеріали представлені у вигляді окремих тем. Кожна тема подається у вигляді електронного посібника з розвиненою системою навігації	10	7	4	2	0
10.		Додаткові мультимедійні навчально-методичні матеріали (відео, підкасти, аудіо, …) подані у рекомендованих форматах, відкриваються без додатково встановлених спеціальних програмних засобів	5	4	3	1	0
11.		Презентацій до всіх лекцій (тем) відповідають структурі - слайд 1 – тема, автор; - слайд 2 – план; - слайд 3 –	10	7	4	2	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень 2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
		інформаційні джерела; - слайди 4-19 – розкриття змісту лекції; - слайд 20 – висновки, завдання;					
12.		Презентації подані у одному з форматів: ppt, pps, pdf	5	4	3	1	0
13.	Практичні (лабораторні) роботи	Наявність окремих ресурсів для кожної практичної (лабораторної) роботи,	5	4	3	1	0
14.		Кожна робота містить основні структурні елементи: - тема, мета, методичні рекомендації, список завдань, форма подання результатів виконаної роботи, критерії оцінювання, термін виконання (для всіх робіт)	10	7	4	2	0
15.		Віртуальний лабораторний практикум завантажується на ПК стандартної конфігурації і пристосований до роботи у мережі	5	4	3	1	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень 2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
16.	Завдання для самостійної роботи	Наявність окремих ресурсів із завданнями для самостійного виконання, які містять основні структурні елементи: зміст завдання, хід виконання, список індивідуальних завдань, інформаційні джерела,форма подання результатів виконаного завдання, критерії оцінювання, термін виконання	5	4	3	1	0
17.		Наявність методичних рекомендацій з виконання завдань або додаткових навчально-методичних ресурсів для самостійного опрацювання або посилань на зовнішні інформаційні ресурси	5	4	3	1	0
18.		Завдання передбачає можливість відправки студентом відповіді з виконаним завданням	5	4	3	1	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень 2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
		викладачеві на перевірку					
19.	Модульний контроль	Навчальний тест для самоконтролю (5-10 тестових завдань) містить розширені коментарі до відповідей студентів	5	4	3	1	0
20.		Інтерактивний тест або/і завдання для модульного контролю виконуються за індивідуальними варіантами	10	7	4	2	0
21.	Підсумкова атестація	Тест для підсумкової атестації містить необхідну кількість тестових запитань	5	4	3	1	0

Таблиця 4.

Критерії науково-змістовної експертизи

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
	Візитка курсу	Анотація дисципліни, наведена у візитці курсу змістовно відповідає описанню ключових тем курсу	1	0	0	0	0
	Робоча програма	Відповідає типовій навчальній програмі або анотації освітнього стандарту	1	1	0	0	0
	Графік навчання	Відповідає робочій навчальній програмі	1	0	0	0	0
	Друковані та Інтернет джерела	Запропоновані друковані та Інтернет джерела містять основні та додаткові навчально-методичні матеріали з дисципліни	1	1	0	0	0
		Запропоновані джерела є актуальними та сучасними	1	1	0	0	0
	Термінологічний словник	Основні терміни з дисципліни подані у глосарії до курсу	1	1	0	0	0
		Усі означення термінів у глосарії до курсу подано у коректній формі	1	1	0	0	0
	Оголошення	У оголошеннях та форумах подані	1	1	0	0	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
		актуальні питання для обговорення					
	Теоретичний матеріал	Кожна тема, що подається у електронному посібнику, висвітлена в обсязі достатньому для оволодіння студентами навчальним матеріалом	4	2	0	0	0
		Зміст навчального матеріалу відповідає освітнім стандартам, робочій навчальній програмі	4	2	0	0	0
		Навчальний матеріал у електронному посібнику викладено у логічній послідовності, на доступному рівні для студентів ВНЗ	4	2	0	0	0
		Кожна тема містить актуальну наукову інформацію щодо предметної області вивчення	4	3	2	0	0
		Навчальний матеріал, викладений у електронних посібниках має практичне значення,	3	3	2	1	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
		пов'язаний з майбутньою професією					
		Матеріал викладено грамотно, лінгвістично чисто	3	1	0	0	0
		Графічні зображення та підкасти якісно доповнюють навчальний матеріал	4	3	2	1	0
		Текстовий навчальний матеріал достатньо підкріплений графікою, мультимедіа, відео та аудіофрагментами	4	3	2	1	0
		Графічні зображення, моделі, відеофрагменти, розміщені у навчальних ресурсах, доречні, коректно виконані, відповідають змісту навчального матеріалу та меті їх використання	4	3	2	1	0
		Мультимедійні презентації відповідають змісту лекційного матеріалу, графічні	4	3	2	1	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
		зображення, схеми, діаграми містять сучасну актуальну інформацію щодо предмету вивчення					
		Відеозаписи лекцій містять записи лекцій, які відповідають за змістом необхідному рівню подання навчального матеріалу для студентів ВНЗ з відповідних тем курсу	4	3	1	0	0
	Практичні (лабораторні) роботи	Зміст практичних (лабораторних) робіт відповідає необхідному рівню оволодіння вміннями та навичками, які зазначаються у робочій програмі	4	2	0	0	0
		Методичні вказівки з виконання практичної (лабораторної) роботи дають повне пояснення щодо порядку виконання роботи	4	3	2	1	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
		Віртуальні лабораторні роботи дозволяють виконати необхідні досліди та набути необхідних навичок з їх виконання. Програмне забезпечення відповідає сучасному рівню розвитку науки	4	3	2	1	0
	Завдання для самостійної роботи	Додаткові навчальні матеріали або методичні вказівки з виконання завдань для самостійної роботи або посилання на зовнішні інформаційні ресурси подані в обсязі достатньому для самостійного оволодіння студентами навчальним матеріалом	4	3	2	1	0
		Завдання для самостійної роботи відповідають змісту вмінь та навичок, які необхідно набути або удосконалити	4	2	0	0	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
		Завдання для самостійного виконання передбачають дослідницьку навчальну діяльність студентів, використання світових інформаційних ресурсів	4	3	2	1	0
	Модульний контроль	Контрольні запитання відповідають рівню засвоєння знань з модуля	4	2	0	0	0
		Навчальний тест містить завдання з ключових питань модуля	3	2	1	0	0
		Коментарі до запитань навчального тесту дають повну підказку студенту щодо виправлення помилок	3	2	1	0	0
		Завдання або тест охоплює весь матеріал з модуля та відповідає вимогам до знань, умінь та навичок, якими необхідно оволодіти під час вивчення модуля	4	2	0	0	0

№	Елемент курсу	Характеристика	Дотримано повністю (рівень 1)	Дотримано більше ніж на половину (рівень2)	Не виконується більше половини визначених вимог (рівень3)	Не дотримуються вимоги взагалі (рівень4)	Елемент відсутній
	Підсумкова атестація	Зміст контрольних запитань відповідає вихідним вимогам до знань, умінь та навичок	4	2	0	0	0
		Тестові завдання сформовані у тест таким чином, щоб охопити навчальний матеріал всіх модулів курсу (повнота контролю)	4	2	0	0	0
		Тест відповідає умовам валідності (об’єктивність контролю)	4	2	0	0	0
	Всього		**100**				

Таблиця 5

Критерії методичної експертизи

№	Елемент курсу	Характеристика	Рівень 1	Рівень2	Рівень3	Рівень4	Відсутній
	Візитка курсу	Викладач має досвід у використанні дистанційних технологій навчання (достатній показник - 3 роки)	5	4	3	2	1
	Робоча програма	Наявність рекомендацій методичної ради ВНЗ до використання у навчальному процесі	1	0	0	0	0
	Графік навчання	Структура електронного журналу оцінок повністю відповідає задекларованому розподілу оціночних балів	5	3	1	0	0
	Друковані та Інтернет джерела	Коректно працюють гіперпосилання на Інтернет-джерела	1	1	0	0	0
	Термінологічний словник	У навчальних ресурсах виділяються терміни, занесені до глосарію, та працюють посилання на глосарій	5	3	1	0	0
	Організація інтерактиву	Наявність можливості он-лайн спілкування для проведення консультацій	5	4	3	1	0
		Активність на форумі більше 1 разу на тиждень	3	2	1	0	0
		Затримка при обміні повідомленнями оф-лайн з боку викладача не більше 1 доби	5	4	3	1	0
	Теоретичний матеріал	Навчальний матеріал структурований, розбитий на порції, працюють гіперпосилання, наявні графічні зображення, матеріал, призначений для запам’ятовування	4	3	2	1	0

№	Елемент курсу	Характеристика	Рівень 1	Рівень2	Рівень3	Рівень4	Відсутній
		виділяється (кольором, іншим типом шрифту тощо), використовується інтерактивний самоконтроль пройденого матеріалу;					
		Навчальний матеріал не перевантажений надмірною кількістю текстової інформації	4	3	2	1	0
		Для подання навчального матеріалу у електронній формі використовується	4	3	2	1	0
		колір тексту, фону, графічних зображень у відповідності до правила 3-х кольорів та їх відтінків					
		Відео-фрагменти використовуються для демонстрації понять, явищ, процесів тощо і тривають в середньому 3-5 хв., доповнюються необхідним аудіосупроводом	4	3	2	1	0
		Графічні зображення якісно виконані та подані для підкріплення текстового матеріалу наочними засобами методично грамотно	4	3	2	1	0
		Дотримуються вимоги до подання мультимедійних презентацій: використовуються ключові слова і фрази, а не речення;- на одному слайді виводиться одне ключове поняття;- теоретичний матеріал структурується та подається	4	3	2	1	0

№	Елемент курсу	Характеристика	Рівень 1	Рівень2	Рівень3	Рівень4	Відсутній
		у схемах та організаційних діаграмах, цифрові дані подаються у вигляді таблиць та діаграм; ефекти анімації застосовуються для акцентування уваги на визначених моментах, поетапного виведення вмісту слайду на екран, для демонстрації руху або послідовності дій; презентація носить проблемний характер, не є точною копією друкованого посібника					
	Практичні (лабораторні) роботи	Наявні теоретичні відомості щодо змісту, послідовності та методики виконання роботи, графічні зображення, приклад виконання завдань, індивідуальні завдання	5	3	2	1	0
		Критерії оцінювання кожної роботи дозволяють чітко зрозуміти границі якісного виконання завдання для отримання позитивної оцінки	5	4	3	2	0
		У практичних (лабораторних) роботах використовується розгляд проблемних ситуацій, що потребують вирішення	5	4	2	1	0
	Завдання для самостійної роботи	Всі обрані типи завдань доцільно використовувати для перевірки необхідних вмінь та навичок; у коментарях до результатів за виконане завдання чітко описуються помилки та	5	4	2	1	0

№	Елемент курсу	Характеристика	Рівень 1	Рівень2	Рівень3	Рівень4	Відсутній
		даються рекомендації щодо їх виправлення					
		При виконанні завдань передбачається використання сучасних методів наукового пізнання: експеримент, порівняння, спостереження, абстрагування, узагальнення, конкретизація, аналогія, індукція та дедукція, аналіз та синтез, моделювання, системний аналіз тощо)	5	4	2	1	0
		У завданні з деталізовано форму подачі результатів, з критеріями оцінювання, терміном виконання	5	4	2	1	0
	Модульний контроль	Більше 150 питань у банку тестових питань на всі теми модуля; наявність різних категорій складності (знання, розуміння, використання, синтез, аналіз) у банку питань, в кожній категорії не менше 10 тестових завдань;	4	3	2	1	0
		Використовується не менше 5 різних типів тестових завдань	4	3	2	1	0
		У формулюванні тестових завдань використовуються графічні зображення та відеофрагменти	4	3	2	1	0

№	Елемент курсу	Характеристика	Рівень 1	Рівень2	Рівень3	Рівень4	Відсутній
		Випадкова вибірка запитань з банку тестових запитань при формуванні тесту з різних категорій складності у заданому співвідношенні;	4	3	2	1	0
	Підсумкова атестація	Тестові завдання, що використовуються у підсумковому тесті, містять завдання на різні рівні складності та різні типи тестових завдань	4	3	2	1	0
	Всього		100				

Таблиця 5

Додаток 18

Експертний висновок

Діючи на основі Положення про електронний навчальний курс, затвердженого "___"_____20__ р., експерт

(прізвище, ім'я, по-батькові)

здійснив (структурно-функціональну, змістовно-наукову, методичну) експертизу електронного навчального курсу:

(назва ЕНК)

Розробленого для студентів _____курсу, факультету _____, напряму підготовки_____

авторами якого є:

(прізвище, ім'я, по-батькові)

у відповідності до критеріїв, викладених у додатку 17 вказаного Положення.

Висновок експерта:
_____
____
_____
____ _____

Сума балів _____

Підпис
експерта_____
"___"_____200_
_ р.

[1]Розглянуто та затверджено на засіданні кафедри _____, протокол № ____ від "___"_____200__р.
Завідувач кафедри_____

_____

[1] Лише для змістовної експертизи