УДК **138.147:002.6**
№ держреєстрації **0109U002808**
Інв. №

МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ І СПОРТУ УКРАЇНИ
ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД

«НАЦІОНАЛЬНИЙ ГІРНИЧИЙ УНІВЕРСИТЕТ»

49000, м. Дніпропетровськ, пр. К.Маркса 19, тел./факс. (0562) 47-32-09
E-mail: HomenkoO@nmu.org.ua

З А Т В Е Р Д Ж У Ю

Проректор з наукової роботи
д-р техн. наук. проф.

О.С. Бешта

_____
“__”_____2010 р.

З В І Т

МОБІЛЬНІ СИСТЕМИ ВІДДАЛЕНОГО МОНІТОРИНГУ, УПРАВЛІННЯ Й ПЛАНУВАННЯ ВИРОБНИЧИМИ Й НАУКОВО-ОСВІТНІМИ ПРОЦЕСАМИ НА ОСНОВІ ПОРТАЛЬНИХ РІШЕНЬ

(заключний)

ГП-428

Начальник НДЧ,
канд. техн. наук, доцент — О.Є. Хоменко

Науковий керівник НДР,
д-р техн. наук.,
зав. кафедри ЕОТ — Г.В. Кузнецов

2010

Рукопис закінчено 5 грудня 2010 р

Результати цієї роботи розглянуто вченою радою Державного ВНЗ «НГУ», протокол від «_21_» грудня 2010 р. № 13

СПИСОК АВТОРІВ

Науковий керівник НДР, головний науковий співробітник	Г.В. Кузнецов (розд. 1-4, формування направлень досліджень)
Провідний науковий співробітник	О.П. Водовозов (вступ, розд. 1,2, аналіз результатів, висновки)
Провідний науковий співробітник	К.В. Соснін (вступ, розд. 2, 4)
Доцент кафедри електропривода, канд. техн. наук, доцент	О.О. Азюковський (розділ 2 - 4)
асистент кафедри ЕОТ	О.В. Пірожніков (розділ 4)

Нормоконтроль Л.С. Шломина

Р Е Ф Е Р А Т

Звіт про НДР: 188 с., 53 джерел, 4 додат.

Об'єкт дослідження – процеси у мобільних системах віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень.

Предмет дослідження – мобільні системи віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень.

Мета роботи підвищення ефективності управління і планування виробничими, науково-освітніми і бізнес – процесами шляхом створення та впровадження багатофункціональних порталів з можливістю організації каналів передачі даних між віддаленими об'єктами засобами мобільного зв'язку.

Наукова новизна роботи полягає у розробці, науковому обґрунтуванню методики використання віддаленого моніторингу стану об'єктів на основі web-орієнтованих технологій та інтрамережі вищого технічного навчального закладу.

Основні результати:

Сформульовано рекомендації щодо використання сучасних педагогічних технологій та методик підготовки фахівців вищих технічних заходів наукоємних спеціальностей. *Встановлено* пріоритетні побажання студентів вечірньої форми навчання щодо складових інформаційної Інтернет-підтримки дисциплін, що вивчаються. *Запропоновано* структуру та інтерфейс шаблону закритої частини портального рішення науково-освітнього забезпечення студентів вищого технічного закладу. *Розроблено* алгоритм дій при створенні шаблонів сторінок закритої частити порталу для різних категорій користувачів згідно визначених повноважень на базі новітніх програмних продуктів Microsoft.

Зазначено, що розподіл структури порталу на інформаційно-незалежні частини (відкриту та закриту) полегшує процеси пошуку потрібної інформації різними категоріями користувачів, зменшує їх витрати часу й спрощує

процедуру формулювання вимог до шаблонів інформаційних сторінок різного функціонального призначення.

Сформульовано вимоги до програмного забезпечення, що використовується при реалізації сучасних педагогічних технологій при підготовці фахівців наукоємних спеціальностей у вищих технічних університетах. Наведено перелік етапів щодо підготовки до проведення лекції:

- правильно формулювати цілі читаного курсу, лекції, фрагмента лекції;
- відбирати і структурувати учбовий матеріал, відповідний цілям заняття з урахуванням особливостей конкретної аудиторії тих, що навчаються; готувати якісні демонстраційні матеріали, включаючи мультимедійні, складати тексти лекцій і викладати матеріал коротко і зрозуміло;
- оцінювати адресатів, які повинні засвоїти учбовий матеріал. Ця оцінка повинна охоплювати не лише оцінку рівня їх знань але і облік психологічних і соціальних особливостей тих, що навчаються;
- вибирати технічні засоби навчання, відповідні цілям і завданням навчання, грамотно використовувати їх в учбовому процесі;
- вибирати методи навчання, що дозволяють найефективніше досягати намічених цілей;
- правильно організовувати контроль знань, умінь і навичок тих, що навчаються на усіх етапах учбового процесу, включаючи підготовку матеріалів для здійснення контролю і проведення аналізу ефективності занять;
- вибирати методи навчання, що дозволяють найефективніше досягати намічених цілей;
- правильно організовувати контроль знань, умінь і навичок тих, що навчаються на усіх етапах учбового процесу, включаючи підготовку матеріалів для здійснення контролю і проведення аналізу ефективності занять;
- користуватися технологіями створення учбових мультимедійних матеріалів.

Метод розробки – теоретичні і експериментальні дослідження.

Сформовано рекомендації по використанню програмно-апаратних комплексів віддаленого контролю та моніторингу освітньо-наукових процесів у підготовці фахівців наукоємних спеціальностей в технічних університетах.

ПЛАТФОРМИ WINDOWS SERVER 2008 ENTERPRISE, МЕРЕЖЕВА СТРУКТУРА, ОСВІТНЬО-НАУКОВИЙ ПОРТАЛ, ВЕБ СЛУЖБИ, MICROSOFT SQL SERVER 2005, ТЕХНОЛОГІЇ РЕПЛІКАЦІЇ БАЗ ДАНИХ, ПРОГРАМНО-ТЕХНІЧНІ КОМПЛЕКСИ МОБІЛЬНОГО ЗВ’ЯЗКУ.

З М І С Т

В С Т У П

Відомо, що не може бути однією єдиною моделі навчання, в тому числі і дистанційного. Важливо зрозуміти, які моделі можливі в організації дистанційного навчання, оскільки від цього буде залежати технологія організації і структурування змісту навчання і самого навчального процесу. Розглянемо ті моделі дистанційного навчання, які видаються найбільш перспективними.

Розглянемо дистанційне навчання як самостійну систему, одну з форм навчання. Розглянемо можливі умови та варіації організації дистанційного навчання, специфіку, для яких цілей той чи інший варіант може бути найбільш прийнятний і за яких Умовах. Існує багато визначень моделей для різних галузей діяльності. Найбільш прийнятним можна вважати наступне визначення: «... будь-який образ (уявний чи умовний: зображення, опис, схема, креслення, графік, план, карта і т. п.) будь-якого об'єкта, процесу або явища (оригіналу даної моделі), який використовується як його "заступника", "представника "...».

Розглянемо моделі дистанційного навчання за двома ознаками: з організації дистанційної системи освіти і з організації навчального процесу. У даний час існуюча мережа відкритого та дистанційної освіти у світовій практиці базується на шести відомих моделях, що використовують різні традиційні засоби нових інформаційних технологій: телебачення, відео-запису, друковані посібники, комп'ютерні телекомунікації і ін.

Навчання за типом екстернату

Навчання, орієнтоване на шкільні чи вузівські вимоги, призначається для учнів і студентів, які з якихось причин не можуть відвідувати очні учбові заклади. Модель передбачає можливість консультацій фахівців, тестування. *Університетське навчання (на базі одного університету)*

Це ціла система навчання для студентів, які навчаються дистанційно. Навчання проводиться з широким використанням нових інформаційних технологій, включаючи комп'ютерні телекомунікації. Створюються інформаційно-освітні середовища окремих університетів, де студенти можуть

отримувати величезний масив додаткової інформації до свого курсу. Такі програми для отримання різноманітних атестатів освіти розроблені в багатьох провідних університетах світу.

Навчання, що ґрунтується на співпраці декількох навчальних закладів

Співпраця декількох освітніх організацій у підготовці програм дистанційного навчання дозволяє зробити більш професійно якісними і менш дорогими. Подібна практика реалізована, наприклад, в міжуніверситетської телеосвітньої програмі Кепрікон (Capricorn Interuniversity Teleducation Program, 1990), у розробці якої взяли участь університети Аргентини, Болівії, Бразилії, Чилі та Парагваю. Перспективна мета даної програми - дати можливість кожному громадянинові країн співдружності отримати будь-яка освіта на базі функціонуючих у країнах співдружності коледжів і університетів, не залишаючи своєї країни, свого будинку.

Навчання в спеціалізованих освітніх установах

Спеціально створені для цілей дистанційного навчання освітні заклади орієнтовані на розробку мультимедійних курсів. У їх компетенцію входять також оцінка знань та атестація учнів. Найбільшим подібною установою є Відкритий університет в Лондоні (Великобританія), на базі якого в останні роки дистанційно проходять навчання велику кількість студентів не тільки з Великобританії, але і з багатьох країн співдружності. Оплата за навчання, як правило, здійснюється цілком тими організаціями, фірмами, де працюють їхні студенти.

Автономні навчальні системи

Традиційно в зарубіжній практиці цю модель також відносять до дистанційної моделі навчання, хоча, строго кажучи, вона може вважатися дистанційної тільки в тій її частині, яка передбачає можливість інтерактивності. Навчання в рамках подібних систем ведеться цілком за допомогою ТБ або радіопрограм, а також додаткових друкованих посібників.

1 АНАЛІЗ, ДОСЛІДЖЕННЯ ТА СИСТЕМАТИЗАЦІЯ СУЧАСНИХ ПЕДАГОГІЧНИХ ТЕХНОЛОГІЙ ТА МЕТОДИК ПІДГОТОВКИ ФАХІВЦІВ ВИЩИХ ТЕХНІЧНИХ ЗАХОДІВ НАУКОЄМНИХ СПЕЦІАЛЬНОСТЕЙ

1.1 Неформальне, інтегроване дистанційне навчання на основі мультимедійних програм

Рівень розповсюдженості сучасних інформаційно-комунікаційних технологій, їх вплив на ритми повсякденного життя у поєднанні зі значним розширенням можливостей у опрацюванні інформації, що вже існує та створенні нових знань зумовлює актуальність дослідження проблеми їх розгортання та інтеграції до освітнього процесу. Доступність окремих складових інформаційно-комунікаційних систем, у тому числі й мобільного зв’язку, зумовлює високу ступінь різноманітності, що певною мірою породжує проблему уніфікації та стандартизації рішень, щодо розгортання систем колективної роботи. Саме поняття «система колективної роботи» (СКР) є відносно нове й може бути розглянуте як сукупність сайтів, до яких (або до частини яких) здійснюється тільки авторизований доступ. Але не це є відмінністю СКР. Головною її метою є підвищення ефективності спільної роботи, що спрямована на досягнення єдиної мети (або групи цілей) за мінімально можливий проміжок часу при одночасному забезпеченні відповідної якості. Наявність у ВНЗ комп’ютерної техніки, яка об’єднана до єдиної мережі, що містить деякі вузли зберігання інформації організаційного та навчально-методичного спрямування не у всіх випадках надає можливість створення на її основі СКР. Під час розгортання СРК слід чітко формулювати мету, інтеграційні якості, складові елементи, компоненти. Встановлювати зв'язки і відношення між частинами і елементами, функціональні характеристики, спадкоємність та враховувати перспективу розвитку.

Слід також враховувати, що сьогодні представлено чимало програмних продуктів, мета яких - створення систем колективної роботи. І більшість з них

має істотний недолік. Зокрема, розробка порталу навчального закладу вимагає вузької спеціалізації. Тобто програмний продукт, розроблений для організації, що займається наприклад виробництвом чи бізнесом, не зможе бути без значної модифікації використаний для колективу, який працює в освіті. Незважаючи на те, що багато процесів у обох галузях містять схожі елементи.

Аналіз останніх досліджень і публікацій свідчить, що неповною мірою вирішено проблему структурування контенту сучасних систем, що забезпечують віддалений доступ до інформації освітньо-наукового характеру. Тому уточнення структурування змістовної частини СКР, її місце як складової педагогічної технології, що складається із сукупності прийомів, психолого-педагогічних установок, що визначають спеціальний набір і компонування форм є актуальною задачею.

Розгляд педагогічної технології можливо розпочати з моделі навчання. У ній як зазвичай виділяють два яруси. Верхній ярус – методи і форми – відноситься до дидактики, нижній ярус складає педагогічну техніку (засоби і прийоми). Інформаційно-комунікаційна система колективної роботи, що надає можливість під час організації навчального процесу мінімізувати вплив як географічного так і часового факторів, повинна органічно інтегруватись до існуючих педагогічних підходів, що отримали розповсюдження у вищих технічних навальних закладах. Під час викладання дисциплін, що відносяться до точних наук, слід акцентувати увагу на наявність завдань на усі поняття, що вивчаються, факти, способи діяльності, включаючи мотиваційні. Крім того, наявність ключових завдань, та їх угрупування у вузли навколо об'єднуючих логічних центрів. Спадкоємність матеріалу, що пропонується до вивчення. Зростання складностей у кожному рівні. Особливий акцент слід приділяти цільовій орієнтації. Кожен з наведених пунктів повинен бути повністю наповнений відповідною змістовною частиною, що його забезпечує.

Сучасні інформаційно-комунікаційні технології, що є основою для створення СКР у тому числі на основі портальних рішень. З розвитком веб-технологій призначення і можливості корпоративних порталів зазнали ряд

змін. Нижче наведені основні групи функціональних можливостей порталів організацій, які з'явилися в ході цього розвитку.

Внутрішній сайт. Початковим призначенням порталів є функції внутрішнього сайту організації:

- Публікація новин та інших матеріалів для співробітників
- Створення бази файлів і документів
- Форум для внутрішнього спілкування

Основною відмінністю таких порталів від публічних сайтів є система управління правами доступу, яка забезпечує безпеку комерційної інформації. Наступним етапом у розвитку корпоративних порталів стала поява в їх складі інструментів для спільної роботи. Як правило, сучасні корпоративні портали дозволяють створювати віртуальний робочий простір для окремих проектів або підрозділів організації. У такому робочому просторі співробітники можуть використовувати наступні інструменти:

- груповий календар
- файлове сховище з контролем версій
- система управління завданнями
- wiki-система

І, нарешті, останньою стадією еволюції корпоративних порталів стала їх роль як інструменту інтеграції корпоративних даних і додатків. Метою цієї інтеграції є надання користувачу єдиної точки доступу до інформаційної інфраструктури організації. Перевагою даної моделі є:

- можливість роботи з декількома корпоративними додатками в одному інтерфейсі
- персоналізація цього інтерфейсу для кожного окремого користувача
- прозора система аутентифікації користувачів
- можливість використання даних, що зберігаються в різних сховищах у мережі компанії.

Для інтеграції з іншими корпоративними додатками, портали використовують плагіни (засновані на Java технології) або віджети (засновані на технологіях HTML, JavaScript).

Через те, що процес передачі знань від їх носія (вчителя, тьютора) до студента (слухача) знаходиться під активним впливом всіх його учасників, системи колективної роботи, що спрямовані на надання найбільш зручних умов одночасної сумісної роботи без врахування географічного фактору, є найбільш ефективним інструментарієм, який базується на результатах розвитку інформаційно-комунікаційних технологій.

Розглядаючи процес інформатизації освіти як процес, розвиток якого спирається на основі реалізації нових можливостей сучасних інформаційно-комунікаційних технологій, і спрямований на забезпечення більш глибокої інтеграції з одного боку процесів пізнання закономірностей предметних областей і довкілля з іншого – поєднуючи їх з перевагами індивідуалізації і диференціації навчання на основі СКР. Проте, висока різноманітності платформ, на основі яких розгорнуті елементи (сегменти) інформаційного простору вищого навчального закладу, котрий до того ж, є значно обмеженим для зовнішнього доступу студентів та викладачів, створюють певні труднощі під час розгортання СКР. Наведемо перелік деяких платформ, на основі яких можуть бути розгорнуті СКР.

1. Workplace (O2Spaces). Система розрахована на роботу з офісними пакетами OpenOffice і StarOffice – і підтримує більшість їх функцій. Workplace виконана на основі платформи J2EE, контейнера Apache Tomcat та СУБД PostgreSQL.

До переваг системи слід віднести: підтримка роботи з будь-якими службами каталогів стандарту LDAP; система Workplace може працювати в Linux, Solaris і 32-розрядними версіями Windows; доступ до документів, що зберігається в системі, можна здійснювати з OpenOffice; вбудована пошукова система підтримує індексацію документів у форматах PDF, ODF і Microsoft Office; повідомлення про зміни документів, миттєвий обмін повідомленнями,

спільні календарі, управління потоками робіт і форуми; вбудована система контролю версій і механізм контролю прав використання документів.

Недоліками системи є висока вартість, необхідність значних комп'ютерних ресурсів для роботи платформи, необхідність наявності IT-фахівців високої кваліфікації, для коректної інсталяції та обслуговування системи.

Популярна open-source CMS система Drupal (GNU GPL) для створення порталів та спільнот. Відрізняється багатою функціональністю і високою безпекою. Перевагами системи є: open-source CMS, підтримка авторизації по LDAP, велика бібліотека додатків, система спільних публікацій, підтримка Open ID.

До недоліків слід віднести: малі можливості для здійснення функцій ERP (планування ресурсів підприємства); відсутність якісних модулів меню; відсутність використання API Drupal об'єктних можливостей PHP; відсутність зворотної сумісності API; відсутність необхідної гнучкості в налаштуванні системи під спеціальні завдання.

Microsoft SharePoint представлений у вигляді двох основних продуктів - Windows SharePoint Services (WSS) і Microsoft Office SharePoint Server (MOSS). Крім цього, пропонується інструментальний засіб Microsoft Office SharePoint Designer (SPD).

Windows SharePoint Services (WSS) – безкоштовний додаток до Windows Server. WSS надає базову інфраструктуру для спільної роботи - редагування, зберігання документів, контроль версій і т.п. Також він містить у собі таку функціональність, як «маршрути» руху документів (платформа для документообігу), списки завдань, нагадування, онлайн-дискусії.

Microsoft Office SharePoint Server (MOSS) - платний компонент для інтеграції функціональності SharePoint у роботу додатків MS Office. Він є надбудовою над WSS і розширює його можливості. Містить у собі інструменти для бізнес аналітики - Excel Services, Business Data Catalog. MOSS дозволяє отримати доступ до Microsoft Project Server і до форм Microsoft

Office InfoPath через браузер, централізовано, відповідно до концепції багатомодульним порталу. Підтримує спеціальні бібліотеки, такі як PowerPoint Template Libraries.

Microsoft Office SharePoint Designer (SPD) - HTML-редактор у стилі WYSIWYG, заточений під створення SharePoint-сторінок і управління документами для WSS сайтів. SPD дає можливість доступу до функціональності свого рендер-движка через Microsoft Expression Web і через середовище розробки Microsoft Visual Studio. Навесні 2009 року став безкоштовним продуктом.

SharePoint може бути використаний для створення сайтів, що надають користувачам можливість для спільної роботи (наприклад у системі викладач – студент). Створювані на платформі SharePoint сайти можуть бути використані як сховище інформації, знань і документів, а також використовуватися для встановлення веб-додатків, таких як вікі і блоги. Користувачі можуть керувати і взаємодіяти з інформацією, в списках і бібліотеках документів, використовуючи спеціальні плагіни, які називаються «веб-частини» (SharePoint WebParts)

Головними перевагами є універсальність. Немає різниці, займаєтеся ваша організація бізнесом або працює в сфері освіти – є певний робочий режим, що складається з неминучих і щоденних етапів. Простота інтерфейсу. Sharepoint розроблений корпорацією Microsoft, яка з самого початку орієнтує інтерфейс своїх продуктів на користувача з базовим рівнем підготовки у інформаційних технологіях. Інтеграція Office Groove 2007 з Windows SharePoint Services V3 і Office SharePoint Server 2007. До складу Office Groove 2007 входить засіб «Файли SharePoint», призначений для інтеграції бібліотеки документів з Windows SharePoint Services V3 і Office SharePoint Server 2007. З інструментів «Файли» і «Файли SharePoint» робочої області Office Groove 2007 можна ініціювати сеанс спільного перегляду презентації PowerPoint.

Недоліками є відсутність кросплатформеності, необхідність участі ІТ-фахівців високої кваліфікації під час налаштування системи під конкретні потреби корпорації.

Зважаючи на те, що у системі вищої освіти найбільше поширеною платформою є продукція Microsoft, найбільш прийнятним продуктом для розгортання на його основі є SharePoint. Доцільність впровадження та використання СКР у навчальному процесі очевидна та полягає у наступному:

- підвищення ефективності та інтенсифікація спільної роботи;
- виграш у часі: мінімізація витрачення часу на поширення необхідної інформації, оперативне її доведення до всіх учасників, що мають авторизований доступ;
- максимальний «охват» / «охоплення» учасників СКР у навчальному процесі;
- реалізація індивідуального підходу до учасників СКР: кожний працює відповідно до власного темпу та можливостей, з певним набором інформаційного наповнення.

В умовах сучасного інноваційного розвитку на перший план виходить необхідність випереджуючої підготовки фахівців з урахуванням вимог завтрашнього дня, що неможливо здійснити без запровадження та втілення новітніх освітніх технологій. Необхідність пошуку ефективних шляхів вдосконалення професійної підготовки обумовлена процесами автоматизації та комп'ютеризації, рівнем розвитку науки на сучасному етапі. До першочергових завдань відноситься впровадження інформаційних технологій у навчальний процес і в систему управління університетом. Також до важливих завдань слід віднести забезпечення функціонування інформаційних сайтів університетів, факультетів, кафедр.

Підвищення індивідуалізації освітнього процесу водночас з його безперервністю є однією з задач стратегії розвитку системи освіти в Україні, забезпечення її більш повної інтеграції до світового освітнього простору. Неперервний процес отримання нових знань, виділення й поява нових

професій, мінімізація часу від формування ідеї до її практичного втілення вимагають від фахівців миттєвого реагування на виклики. Також не повністю вирішеною лишається проблема актуалізації освітнього контенту, спрощення технічної частини процесу його створення та забезпечення вільного доступу до нього студентів.

Одним з варіантів вирішення поставлених задач є впровадження на основі сучасних інформаційно-комунікаційних технологій систем колективного доступу до інформації. Система колективної роботи (СКР) - це відносно нове поняття, під яким мається на увазі приватний, корпоративний сайт, до якого, як і до звичайного сайту у Всесвітній павутині, існує можливість підключатися за допомогою програми-браузера і захищеного https-протоколу. Незареєстровані користувачі не можуть отримати до нього доступ. Мета впровадження СКР – забезпечення одночасного доступу до процесу створення нових інформаційних ресурсів, що значно підвищує ефективність використання робочого часу, який витрачається на розробку навчально-методичного забезпечення освітнього процесу. Водночас, шляхом встановлення обмежень на доступ до відповідних частин навчального контенту можливо реалізувати адресність у поданні інформації, а крім того – надати можливість користувачеві (студентові) самостійно обирати ті частини структурованого контенту, які є необхідними з його точки зору.

Одним з шляхів реалізації СКР є мобільні системи віддаленого моніторингу, управління й планування науково-освітніми й виробничими процесами на основі портальних рішень «Microsoft» (http://mibo.nmu.org.ua/default.aspx). Використання сучасних мобільних технологій у поєднанні з сучасними портальними рішеннями розгорнутими на основі технології «Microsoft» дозволяє не тільки своєчасно отримати інформацію щодо особливостей організації освітнього процесу, але й забезпечити високу ступінь його індивідуалізації.

Актуальність дослідження впливу розвитку сучасних інформаційно-комунікаційних технологій на отримання додаткових можливостей у всіх

сферах діяльності людства з вирішення проблеми відповідності сучасним викликам зумовлюють динамічні зміни, що є наслідком розвитку тих самих технологій. До чинників, які повинні безпосередньо формувати, або як найменше, значно впливати на формування майбутнього безумовно відносяться освітні процеси. Проте сьогодні постає проблема, яка лишається вирішеною далеко неповною мірою, і пов'язана зі зменшенням актуалізації освітнього контенту, яка зумовлена швидким старінням цінності інформації. Водночас, сучасні технології дозволяють більш активно використовувати інтелектуальний потенціал суспільства зменшуючи обмеження, що викликані географічним фактором. Сучасні тенденції української вищої освіти свідчать про більш глибоку інтеграцію інформаційних технологій до освітнього процесу. Просте підвищення культури користування сучасними інформаційно-комунікаційними технологіями не вирішує проблеми підвищення ефективності їх використання, що є важливою науковою та практичною проблемою. Це підтверджує значна кількість публікації, спрямованих на формування та наукове обґрунтування пропозицій, впровадження яких забезпечує підвищення ефективність використання сучасних інформаційних технологій і підвищення якості освіти [1 - 3]. Сьогодні склалася ситуація, коли потенційна можливість, що надається рівнем розвитку інформаційно-комунікаційних технологій поєднується з практично відсутнім системним підходом до їх використання у освітній практиці. Відомий у світі стандарт SCORM (Sharable Content Object Reference Model), що розроблений для систем дистанційного навчання й передбачає розбиття матеріалу на невеликі, логічно завершені блоки які можуть бути пропонованими для навчання окремо, має бути адаптованим для освітніх реалій України. Серед яких слід відзначити як різноманітність платформ, що використовуються різними навчальними закладами для розгортання власного освітнього інформаційного простору так й значні відмінності у базовій інформаційній культурі користувачів.

Останні дослідження й публікації, що присвячені проблематиці аналізу впливів сучасних інформаційно-комунікаційних технологій на тенденції розвитку вітчизняної освіти свідчать про наявність значного потенціалу відкритих інформаційних систем. Вони надають додаткові ступені свободи системі вищої освіти й забезпечують можливість значно підвищити актуальність освітнього контенту, значно зменшуючи потреби у часі на методологічне перетворення нових знань, формування їх у освітній контент. Водночас, невирішеним лишається питання стандартизації вимог до створюваних відкритих освітніх просторів, вимог до освітньо-наукового контенту, що їх наповнює. Здійснення аналізу тенденцій розвитку сучасної української вищої технічної освіти з урахуванням впливу глобалізаційних та інформаційних чинників надає змогу спрогнозувати проблеми стратегічного характеру й сформулювати на цій основі завдання до сьогоденного виконання, що є частиною не повністю вирішеної загальної проблеми аналізу тенденцій розвитку сучасної української освіти й містить певну новизну отриманих результатів.

Встановлення можливостей та наслідків від впровадження нових сучасних інформаційно-комунікаційних технологій до освітнього процесу повинно спиратися на методологічне обґрунтовані засади їх використання. Вирішення проблеми забезпечення відповідного рівня якості вищої освіти в Україні нерозривно пов’язане з підвищенням актуалізації навчального контенту, його доступності для студентів і, як наслідок, що певною мірою сприяє формуванню майбутніх ознаків суспільства завтрашньої доби. Сучасне становище людського суспільства обумовлено його входженням у період «інформаційної цивілізації», що в свою чергу обумовлює необхідність здійснення реформаційних змін у сучасному суспільстві. Однією з вагомих складових реформаційних процесів є модернізація системи вищої освіти.

Здійснюючи аналіз сучасного стану освіти і науки у всьому світі і зокрема в Україні, хотілося б наголосити на тому, що в умовах розвитку інформаційної цивілізації обсяг наукової інформації подвоюється через кожні

2 – 5 років, виникають більш досконаліші технології виробництва. З метою забезпечення належної якості і європейського рівня навчання Україна має запровадити та дотримуватися завдань та принципів створення зони Європейської вищої освіти: введення двоциклового навчання; запровадження кредитної системи; формування системи контролю якості освіти; розширення мобільності студентів і викладачів; забезпечення працевлаштування випускників; привабливість європейської системи освіти. Основні завдання реформування вищої освіти зазначені у «Державній програмі розвитку освіти в Україні на 2005-2010 рр.» - інтеграція освіти і науки, інформатизація освіти, запровадження нових педагогічних технологій; підвищення якості навчання, виховання, кваліфікації, компетенції та відповідальності фахівців усіх напрямків, їхньої підготовки і перепідготовки; розвиток системи неперервної освіти впродовж життя та ін. Безумовно важливим завданням є розвиток безперервної освіти, оскільки технології дуже швидко застарівають, а тому необхідно змінити підхід до навчання – це не лише 5 студентських років у стінах вузу, а готовність самостійно набувати нові знання (вчитися) протягом усього життя.

Головним завданням університету є забезпечення високої якості освіти, інтеграції навчального, наукового та інноваційного процесів, запровадження нових технологій навчання, що дозволяє здійснювати підготовку конкурентоспроможних фахівців. Для розвитку вищої освіти в Україні необхідно більше використовувати можливості новітніх інформаційних та комунікативних технологій, запроваджувати інтерактивні моделі навчання, здійснювати перехід від розповідавчих до діяльнісних форм, не передавати знання, а організувати таким чином дослідницьку діяльність студентів, щоб вони самі знаходили ці знання, а викладачу залишається направляти та контролювати їх діяльність, спрямовувати їх не на отримання правильної відповіді, а на розуміння того, як цю відповідь отримано. Інноваційне навчання передбачає зміни системи організації освіти (децентралізація системи управління освітою, зміна системи фінансування вузів,

вдосконалення бази навчально-методичного забезпечення, запровадження інформаційних та комп'ютерних технологій).

В умовах сучасного інноваційного розвитку на перший план виходить необхідність випереджуючої підготовки фахівців з урахуванням вимог завтрашнього дня, що неможливо здійснити без запровадження та втілення новітніх освітніх технологій та інноваційних форм і методів навчання. Необхідність пошуку ефективних шляхів вдосконалення професійної підготовки обумовлена процесами автоматизації та комп'ютерізації, рівнем розвитку науки на сучасному етапі. До першочергових завдань відноситься впровадження інформаційних технологій у навчальний процес і в систему управління університетом. Наприклад, у Національному гірничому університеті введена система «Деканат», що дозволяє оперативно обробити та отримати інформацію щодо організації навчального процесу в університеті (навчальні плани, графіки, відомості тощо). Також до важливих завдань слід віднести забезпечення функціонування інформаційних сайтів університетів, факультетів, кафедр. Цей процес має обов'язково супроводжуватись створенням персональних сайтів викладачів, які в свою чергу мають пройти відповідну підготовку, наприклад, через проходження ними підвищення кваліфікації, що відповідає загальноєвропейському принципу «освіта через все життя». Процес підвищення кваліфікації може передбачати поглиблене вивчення іноземної мови, дидактики, психології, риторики та обов'язково опанування новітніх комп'ютерних технологій.

Використання комп'ютерів в системі освіти як об'єкта вивчення, як засіб навчання, як елемент методики досліджень, як складова системи управління освіти, дозволяє визначити його як одночасно і інформаційний, і навчальний, і контролюючий засіб. Завдяки ПК відкриваються «on-line» джерела інформації: електронні бібліотеки, публікації в Інтернеті, телеконференції, Web-форуми, Web-сайти університетів, кафедр, викладачів. На думку сучасних науковців, при використанні ПК технічні можливості дозволяють значно активізувати навчальний процес, підвищити наочність поданого матеріалу, отримувати не

лише теоретичні, а й практичні знання. Також до переваг комп'ютерної технології можна віднести її гнучкість, застосування при різних формах навчання та максимальна реалізація індивідуалізації навчання. Комп'ютерна технологія дозволяє підвищувати інтерес до навчання предметів. За результатами дослідження Рассела і Хейні, студенти дають значно більше правильних відповідей при розв'язанні задач на ПК, а не на паперових носіях. Слід зауважити, що вплив інформаційно-комунікаційних технологій не обмежується тільки системою освіти. Вони формують й постійно змінюють умови функціонування фахівців, з одного боку, полегшуючи умови праці й зменшуючи час на створенні нових інформаційних цінностей, з іншого значно ускладнюючи процес пошуку й орієнтування в надлишкових інформаційних потоках потрібної інформації. Водночас спостерігається зменшення впливів географічних факторів на доступність освіти.

Таким чином, у добу інформаційного суспільства необхідно більше використовувати можливості новітніх інформаційних та комунікативних технологій; необхідно зберегти власні традиції змістовної, ґрунтовної та широкої теоретичної підготовки фахівців з одночасним використанням інноваційних технологій у навчанні та відповідністю сучасним європейськими вимогами.

Проблема трансформації змісту навчальних дисциплін, що викладаються студентам у вищому навчальному закладі у формат, що є адаптованим до дистанційного до них доступу містить декілька складових: 1) забезпеченість всіх учасників інформаційного навчального середовища необхідним технічним інструментарієм (наявність у навчального закладу мережевої структури, що відповідає певним вимогам, вільний доступ до мережі Інтернет студентів та викладачів); 2) розміщений в локальній інформаційній мережі закладу певний інформаціно – науковий контент, що використовується під час навчального процесу; 3) володіння технічними інструментаріями інформаційно-комунікаційних технологій, на основі яких можливо розгортання портального рішення (хоча б на етапі створення так

званої «активної» веб-сторінки, що надає можливість користувачу декілька додаткових сервісів окрім вільного доступу до «відкритої» частини контенту); 4) наявність чітко сформованих критеріїв та вимог до змісту дисциплін, що пропонуються для дистанційного доступу.

Наявність вказаних складових зумовлює можливість створення елементів телекомунікаційної освітньо-наукової організаційної структури, мета якої є однаковою для різних форм навчання. Це зумовлює неможливість ізоляції вказаної структури від процесів, що протікають у всій системі освіти або її обмеженість тільки певною (однією) формою навчання. Тому, більш коректним є ведення розмови про створення інформаційно-комунікаційної системи *дистанційного доступу до навчального контенту*, на базі сучасних інформаційно-телекомунікаційних технологій для будь яких форм навчання. Безумовно, існують обмеження, які витікають з особливостей в організації форм навчання, які повинні враховуватися під час підготовки змісту дисциплін, що призначений для дистанційного доступу до нього. Тобто потрібно враховувати цільову аудиторію під час розробки нового (або трансформації існуючого) змісту дисципліни, що викладається. Таким чином можна стверджувати про можливість (у випадку орієнтації на широкий прошарок верст населення, з врахуванням великої розбіжності в базовій кваліфікації) існування декількох версій навчальних дисциплін в єдиній системі дистанційного доступу до освітно-наукового контенту вищого технічного навчального закладу. Сучасні інформаційно-комунікаційні технології забезпечують постійну доступність навчальних матеріалів, які раніше були обмеженими для використання, що в свою чергу викликає проблему надлишкового інформаційного забезпечення користувачів. Вказана проблема може бути вирішена шляхом чіткого проблемно-орієнтованого структурування контенту та наданням пошукових сервісів як у межах портального рішення так й по за ними.

З метою підвищення рівня керованості процесами формування освітнього контенту, унеможливлення надання прав різним категоріям

користувачів з однаковими можливостями щодо ступеню редагування змісту пропонується категорування користувачів освітньо-наукового порталу за рівнем доступу до інформації та її оновлення і корекції. Це адміністратори портального рішення, які мають повний доступ до всіх компонентів інформаційної системи й відносяться до першої групи користувачів (рис. 1.1). Друга група – це працівники деканатів, які відповідають за планування, організацію та контроль навчально-методичної, науково-методичної та науково-дослідницької діяльності структурного підрозділу вищого навчального закладу. До неї також можна віднести викладачів, які постійно працюють у запропонованому віртуальному середовищі. Користувачі, які входять до другої групи мають право створювати нові веб-частини на сторінці, здійснювати розсилку повідомлень користувачам (учасникам інформаційного обміну та обігу) які відносяться до інших груп (рівнів доступу).

Особливістю користувачів другої категорії є те, що вони мають можливість створювати облікові записи нових користувачів й призначати їм певні права доступу, але не вище ніж права доступу власної категорії. Категорію студентів які відносяться до третьої групи і об’єднані у академічні групи можна сформувати у так звану довгострокову групу користувачів. Відмінністю цієї групи є довгостроковий (у межах періоду навчання) доступ до інформаційного наповнення дисциплін, інформацію щодо змісту навчальних планів, графіку навчального процесу, розкладу занять та консультацій викладачів. Короткострокова група містить облікові записи тих користувачів, які з певних причин мають обмежений у часі доступ до наповнення порталу. Наприклад це можуть бути слухачі курсів підвищення кваліфікації, студенти, які проходять додатковий курс посиленої підготовки з певних дисциплін, викладачі, які залучені до процесу навчання на короткостроковий термін, керівники короткострокових проектів (студентські олімпіади, інженерні та наукові проекти, як правило міждисциплінарного характеру). Остання, четверта група користувачів – це незареєстровані користувачі для яких є доступною загальна інформація переважно рекламного характеру. Вказана група має

доступ тільки до переліку видів освітніх послуг, що надаються вищим навчальним закладом та анотованого опису спеціальностей.

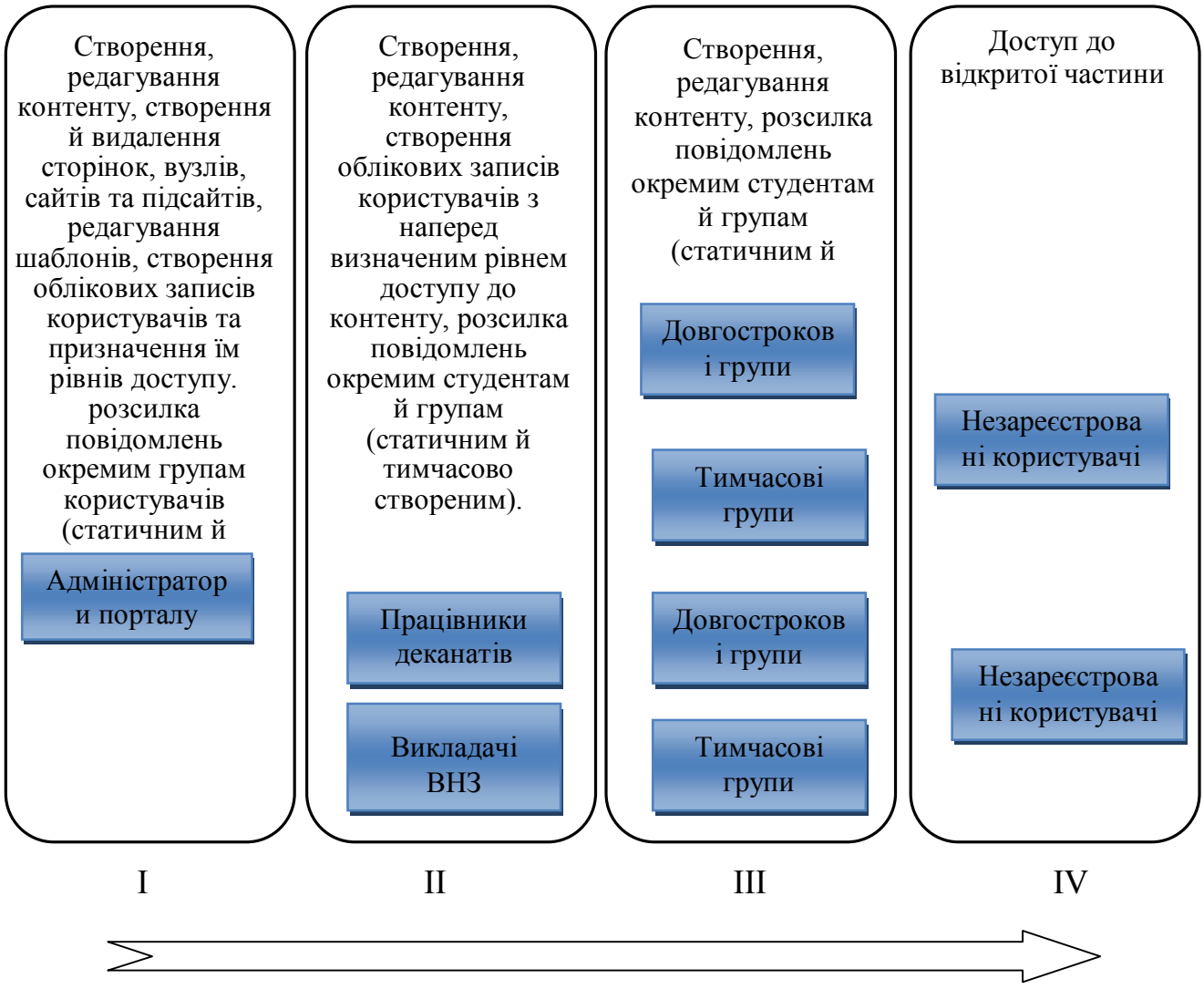


Рисунок 1.1 - Категорування користувачів освітньо-наукового порталу за рівнем доступу до інформації

Запропонований рівень категорування користувачів за рівнями доступу до інформаційного наповнення портального рішення, електронних ресурсів з одного боку не містить надлишкове дрібне розподілення прав та рівнів доступу між користувачами, з іншого надає змогу забезпечити певний рівень керованості процесами створення інформаційних потоків. Він відповідає необхідності створенню умов для задоволення інформаційних потреб навчальної діяльності вищих навчальних закладів.

Слід зауважити, що створення науково-освітнього порталу вищого технічного навчального закладу породжує не тільки проблему структурування контенту, який вже існує в переважній більшості випадків у цифровому вигляді й потребує тільки процедури узгодження форматів, але й розробки й підтримки процесів створення нової інформації, яка є необхідною для забезпечення освітнього процесу установи.

Програми самоосвіти при можливості консультацій орієнтовані на навчання дорослої аудиторії, тих людей, які з якихось причин не змогли закінчити шкільну освіту. Подібні проекти можуть як частина офіційної освітньої програми бути інтегрованими в цю програму.

Виходячи з викладеного вище, основні цілі всіх моделей освіти на відстані можна звести до наступних.

1. Дати можливість учнем удосконалювати, поповнювати свої знання в різних областях в рамках діючих освітніх програм.

2. Дати атестат про освіту, ту чи іншу кваліфікаційну ступінь на основі результатів відповідних іспитів (екстернат).

3. Дати якісну освіту за різними спрямування шкільних та вузівських програм.

При цьому використовуються як програми окремих університетів, де практикуються очні, заочні та дистанційні форми навчання, або їх поєднання, програми міжуніверситетські, розроблені і використовувані спільними зусиллями декількох освітніх установ, підтримуваних урядовими та діловими колами, так і автономні програми, що розробляються для самостійного використання учнями за певними напрямками. Однак про дистанційною формою навчання можна говорити лише в тих випадках, коли передбачається можливість інтерактивності на основі не тільки відповідних засобів навчання, але і контактів з викладачами, іншими студентами.

Розподілений клас

Ця модель будується на організації навчального процесу в режимі реального часу. Заняття ведеться з групою студентів очного відділення

одночасно з «віддаленими» студентами за допомогою інтерактивних телекомунікацій, відеоконференцій. Використання даної моделі припускає, що студенти збираються в призначений час перед своїми комп'ютерами або в аудиторіях, обладнаних засобами відеоконференцій.

Самостійна робота учнів

Ця модель розрахована на вільне розміщення учнів, можливість працювати в асинхронному режимі. Учні працюють самостійно. Їх забезпечують всім необхідним методичним та навчальним матеріалом, включаючи докладні навчальні програми. Вони мають можливість встановлювати контакт з консультантом інституту, який відповідає на питання, оцінює їхню роботу. Контакти можуть встановлюватися за допомогою телефону, голосової пошти, телеконференції, електронної пошти або звичайної пошти.

Відкрите освіта + клас

Модель передбачає використання традиційного друкованого матеріалу, інших засобів навчання (відеозапис, CD), які повинні забезпечити студентові можливість працювати в індивідуальному темпі, використовуючи при цьому в разі необхідності інтерактивні телекомунікаційні технології для групової роботи студентів.

1.2 Інтеграція очних і дистанційних форм навчання

Це найбільш перспективна модель, як показує вже накопичена практика, причому стосовно як до шкільної освіти (профільні курси, використання курсів дистанційного навчання, для поглиблення знань, ліквідації прогалин у знаннях), так і до вузівського.

Вочевидь, що при впровадженні в практику навчання в старших класах профільного навчання можливість створення фонду спеціалізованих або профільних курсів з особистих напрямками в межах загальноосвітньої програм школи могла б суттєво просунути вирішення проблеми профільного навчання.

У даний час в Україні офіційно намічено всього чотири напрями профільного навчання: гуманітарний , суспільно-наукове, соціально-економічне і технологічне. Це досить загальні напрямки, які не дозволяють у разі необхідності конкретизувати профільність навчання.

Зрозуміло, зазначеними напрямками не вичерпуються профорієнтаційні інтереси учнів. За допомогою курсів дистанційного навчання можливо значно урізноманітнити вказані напрями, даючи учням можливість більш чіткої професійної орієнтації та підготовки до вступу до відповідного вузу. Такі курси можна створювати на базі університетів, і вести їх могли б викладачі цих університетів на основі інтеграції з очною системою навчання вказана вище профілів. Причому розробка таких курсів могла б вестися на корпоративних засадах кількома вузами, де є аналогічні або близькі за профілем спрямування. У учнів є досить широкий вибір профільного напряму навчання в старших класах, а розробка і керівництво цих курсів провідними вузами країни гарантували б якість такого навчання. Відповідно можна говорити і про створення інформаційно-предметного середовища за даним профілем. Тоді й підготовка до державного тестування знайшла б більш значиму мотивацію. Поки всі ці ідеї можна викладати лише в умовному способі, оскільки ніхто ні на рівні міністерства, ні на рівні конкретних вузів не має ясно виробленої в цьому напрямку позиції, тим більше програми дій. Однак наше завдання - показати можливості, нехай і потенційні, використання різних моделей дистанційного навчання.

Інтеграція дистанційного та очного навчання дуже перспективна і в частині більш широкого використання учнівського компонента, навчання за індивідуальними програмами, яке останнім часом все більш широко поширюється в наших школах, особливо в старших класах.

Мережеве навчання

Мережеве навчання слід використовувати для тих випадків, коли виникають складнощі з якісним забезпеченням учнів очними формами

навчання, для студентів та дорослого населення, які бажають підвищити свій професійний рівень, змінити професію і т . д.

У цьому випадку створюються спеціальні, автономні курси дистанційного навчання, тобто за окремими навчальними дисциплінами, розділів чи тем програми, або цілі віртуальні школи, кафедри, університети. Слід зауважити, що будь-який курс дистанційного навчання - це повноцінний навчальний процес. Ця модель навчання може повністю замінити очну форму навчання і бути самодостатньою для отримання якісної освіти за умови грамотної її організації. Ця затребуваність з роками тільки зростає, оскільки все більша кількість людей бажають отримати повноцінну освіту або поглибити свої знання з окремих дисциплін, не маючи можливості відвідувати очні учбові заклади

Мережеве навчання і кейстехнології

Модель мережевого навчання і кейстехнологій призначена для диференціації навчання. Справа в тому, що у великій кількості випадків немає необхідності в створенні електронних мережевих підручників, якщо існують вже апробовані друковані посібники. Набагато ефективніше будувати навчання, спираючись на вже видані підручники та навчальні посібники і за допомогою додаткового матеріалу, що розміщується в мережі, або поглиблювати цей матеріал для просунутих учнів, або давати додаткові роз'яснення, вправи та ін. для слабких учнів. При цьому передбачаються консультації викладачів, система тестування і контролю, додаткові лабораторні та практичні роботи, спільні проекти та ін.

1.3 Інформаційно-комунікаційні технології та розвиток дистанційних методик підготовки фахівців вищих технічних заходів наукоємних спеціальностей

Оцінка потреб сучасного суспільства в галузі освіти показує, що в останні роки намітилася чітка тенденція у збільшенні попиту населення на отримання безперервної освіти та професійної перепідготовки. Це вимагає вже в найближчі роки вирішення двох проблем. По-перше, у зв'язку з появою великої

кількості нових освітніх установ все більш актуальною стає проблема перепідготовки викладачів. По-друге, підготовка і перепідготовка дорослих людей в силу їх соціального статусу вимагає використання форм і методів дистанційного навчання.

В останні кілька років термін "дистанційне навчання отримав широке розповсюдження. Слід зауважити, що забезпечити необхідну мобільність системи освіти в рамках традиційних форм буде досить важко навіть за істотні фінансові вливання, так як традиційні форми навчання зажадають істотного збільшення професорсько-викладацьких кадрів, підготовка яких відбувається досить повільно.

Реальною альтернативою екстенсивного розвитку традиційних форм освіти є формування системи дистанційної освіти (СДО). Окрім наведених вище обґрунтувань необхідності дистанційного навчання доцільно навести й глобальні причини, що викликають цю потребу в усьому світі.

За час навчання студента у ВНЗ кількість знань у світі практично подвоюється. Темпи технологічного і науково-технічного прогресу сьогодні такі, що багато знань застарівають вже протягом 1-3 років. Випереджаючий освіта вимагає, щоб нові знання надходили в систему освіти безпосередньо в процесі навчання. Тому виникла нова умова цивілізованого суспільства - перейти від освіти на все "життя" до "освіти через усе життя". Інформаційні ресурси знань сьогодні географічно розосереджені по всій земній кулі. Тому безперервну освіту, можна отримати лише шляхом дистанційного навчання. Ця проблема може бути вирішена шляхом формування Єдиної Системи дистанційної освіти.

Однак, становлення дистанційної освіти як інноваційного явища у галузі освіти, саме по собі знаходиться на стадії бурхливого і складного розвитку. При цьому механізми узагальнення, інтеграції всього кращого, конструктивного подолання суперечностей та ідеології розвитку ДО чітко все ще не сформульовані. Причина цьому - відсутність єдиного понятійного апарату, нормативно-правової бази, наукових досліджень в області ДО, узагальнення

вже наявного досвіду у вигляді науково-методичних посібників, аналітичних оглядів, регулярних семінарів і т.п.

Незважаючи на багаторічний вітчизняний і зарубіжний досвід з теорії та практиці ДО, все ще відсутня загальноприйняте його визначення. Такий стан справ можна вважати природним для досить нового напряму, а численність визначень підтверджує в цілому актуальність і новизну напрямків досліджень дистанційної освіти.

Дистанційна освіта - це синтетична, інтегральна гуманітарна форма навчання, що базується на використанні широкого спектру традиційних і нових інформаційних технологій та їх технічних засобів, які застосовуються для доставки навчального матеріалу, його самостійного вивчення, діалогового обміну між викладачем і навчаються, причому процес навчання в загальному випадку некритичний до їх розташування у просторі і в часі, а також до конкретного освітнього закладу.

До мети створення та розвитку єдиної системи дистанційної освіти в можна віднести надання школярам, студентам, цивільним і військовим фахівцям, найширшим верствам населення в будь-яких районах країни і за її рубежами рівних освітніх можливостей, а також підвищення рівня освіти за рахунок більш активного використання наукового освітнього потенціалу провідних університетів, академій, інститутів провідних галузевих центрів підготовки і перепідготовки кадрів, центрів підвищення кваліфікації та інших освітніх установ.

СДО повинна сприяти рішенню таких соціально значущих завдань як:

- підвищення рівня освіченості суспільства і якості освіти;
- реалізація потреб населення в освітніх послугах;
- задоволення потреб країни в якісно підготовлених фахівцях;
- підвищення соціальної і професійної мобільності населення, його підприємницької і соціальної активності, рівня самосвідомості, розширення кругозору;

- збереження і примноження знань, кадрового і матеріального потенціалу, накопичених вітчизняною сферою освіти;
- розвиток єдиного освітнього простору в рамках Росії, всього світового співтовариства.

Переваги дистанційного навчання стають очевидними, а розвиток СДО набуває особливої актуальності для освітньої системи країни під впливом наступних процесів:

- продовження економічних реформ, що висувають нові вимоги до освіти;
- формування нових потреб населення в сучасних змісті і технологіях освіти;
- політичні зміни, що сприяють зростанню міжнародних зв'язків, у тому числі в галузі освіти;
- поява і швидкий розвиток якісно нових технічних засобів обміну інформацією між учасниками освітнього процесу;
- зростання міжнародної інтеграції в освіті при посиленні конкуренції на світових ринках освітніх послуг.

В даний час створення і розвиток СДО стає особливо актуальним, тому що саме ця система може І найбільш адекватно і гнучко реагувати на потреби суспільства. СДО відповідає логіці розвинена І освіти і суспільства в цілому, де на перше місце ставляться потреби кожного окремого громадянина.

Основними завданнями, пов'язаними зі створенням СДО, є:

- визначення та закріплення принципів організації і функціонування єдиної СДО;
- формування організаційно-управлінської структури СДО і фінансових механізмів, що забезпечують її розвиток;
- розробка нормативно-правового забезпечення СДО;
- створення системи інформаційно-аналітичного та маркетингового забезпечення СДО;

– розробка теоретичних, науково-психологічних основ і конкретних методик дистанційного навчання з урахуванням соціо-культурної, професійної, етичної, віково-психологічної та іншої специфіки учнів;

– створення спеціалізованих інформаційно-освітніх середовищ і курсів ДО;

– розробка критеріїв, засобів і систем контролю якості ДО, розробки та репродукування

– методичних матеріалів, програм, курсів та їх супроводження;

– вдосконалення комунікаційної інфраструктури для реалізації освітніх технологій;

– створення системи підготовки, перепідготовки та підвищення кваліфікації кадрів СДО;

– розробка і здійснення програми проведення рекламно-пропагандистської компанії (з урахуванням специфіки регіонів і типів контингенту користувачів), спрямованої на ознайомлення населення з принципами функціонування, можливостями та перевагами СДО і на надання їй статусу високої престижності та соціальної значимості;

– розвиток міжнародного співробітництва в галузі дистанційної освіти.

Найважливішими пріоритетами розвитку СДО в період її створення та первинного функціонування є:

– Першочергове забезпечення широкомасштабної підготовки, перепідготовки та підвищення кваліфікації кадрів для конверсійних, освітніх, регіональних та інших державних і суспільних програм, які забезпечують розвиток пріоритетних галузей економіки і соціальної сфери;

– Якнайшвидше надання населенню освітніх послуг вищої школи з дисциплін, які користуються максимальним попитом, не задоволеним традиційними системами навчання;

– Безумовне забезпечення високих стандартів і якості освіти за рахунок реалізації комплексних освітніх програм, заснованих на кращих традиціях вітчизняної освіти, міжнародному досвіді, а також на використанні передових психолого-педагогічних, інформаційних, комунікаційних та інших технологій;

– Послідовне проведення принципу організації освіти, що полягає в тісному і безперервному взаємне впливі освіти, науки і виробництва, і використання переваг, створюваних такою організацією;

– Реалізація принципу конкретної адресності курсів і програм ДО залежно від соціальних та освітніх завдань та специфіки контингенту учнів;

– Формування сприятливої громадської думки про дистанційну освіту і створення умов для соціально-психологічної комфортності користування ДО;

– Забезпечення повноцінної оперативності (педагогічної) і відстроченою (освітньої та соціально-психологічної) зворотного зв'язку зі споживачами послуг СДО для визначення її дієвості в різних регіонах та ефективності дистанційного навчання різних категорій користувачів;

– Прискорений розвиток інфраструктури СДО, що надає можливість отримання освіти за місцем проживання широким верствам населення, і рішення, тим самим, соціальних проблем, пов'язаних з існуючою диспропорцією в розміщенні вищих та інших навчальних закладів на території країни ближнього зарубіжжя, з міграцією молоді у великі міста з метою отримання освіти в провідних вузах країни і викликаної цим додаткового соціального напруженістю у великих містах, з відставанням рівня та якості освіти в малих містах;

– Переважне розвиток форм дистанційної освіти, що створюють умови для якісно нової академічної мобільності студентів, надання їм можливості для переходу з однієї освітньої програми на іншу, з одного

навчального закладу до іншого для продовження освіти, одночасного навчання у різних навчальних закладах, у тому числі зарубіжних;

– Прискорений розвиток експорту освітніх послуг вищої школи з метою зміцнення її економічної бази і впливу країни на міжнародній арені.

З урахуванням результатів, отриманих на сьогоднішній день в Україні і в усьому світі, загальновизнаними є наступні основні характеристичні ознаки дистанційної освіти:

– комплекс освітніх послуг;

– охоплення широких верств населення в країні і за кордоном;

– використання спеціалізованої інформаційно - освітнього середовища;

– опора на сучасні засоби обміну навчальною інформацією на будь-якій відстані.

По-перше, дуже важливо те, що мова йде не просто про освітні послуги, а мається на увазі саме *комплекс освітніх послуг.*

По-друге, не менш важливо і те, що освіта повинна все більшою мірою формувати і задовольняти освітні потреби кожної конкретної людини з тим, щоб забезпечувати потреби суспільства і держави у професійно освічених кадрах. Ця умова повністю відповідає сучасній парадигмі освіти в світі.

По-третє, дистанційне навчання має проводитись у спеціально сформованої інформаційно-освітньому середовищі. Формування такого середовища є однією з істотних завдань, яка сьогодні стоїть перед світовою освітньою системою. Мета полягає в тому, щоб кожна людина змогла отримати доступ до цього середовища, до цього освітнього простору і за допомогою її здобути знання.

Використання у межах дистанційної освіти сучасних телекомунікаційних мереж і технічних засобів інформатики, особливо в інтерактивному режимі, дозволяє сьогодні говорити про необхідність створення особливої дидактики та спеціальної методології освіти.

Характеристичними рисами навчального процесу в СДН є:

- гнучкість;
- адаптивність;
- модульність;
- економічна ефективність;
- орієнтація на споживача;
- опора на передові комунікаційні та інформаційні технології.

Гнучкість СДО полягає у тому, що студенти в цій системі в основному не відвідують регулярних занять у вигляді лекцій і семінарів, а працюють в слушний для себе час в зручному місці. Це принципово важливо для тих, хто не може або не хоче змінити свій звичний уклад життя. Для вступу до вузу на дистанційне навчання студенту не вимагається якого-небудь освітнього і вікового цензу. Кожен може вчитися так довго, скільки йому особисто необхідно, для освоєння предмету і отримання необхідних залікових одиниць за обраними навчальних курсів.

Адаптивність СДО забезпечує кожному користувачеві вибір, створення і реалізацію індивідуальної траєкторії набуття освіти або набуття навичок і вмінь.

В основу програм дистанційної освіти покладено модульний принцип. Кожен окремий навчальний курс програми створює цілісне уявлення про певну наочну область. Це дозволяє з набору будь-якої кількості незалежних курсів-модулів формувати учбову програму, що відповідає індивідуальним і / або груповим потребам.

Економічна ефективність ДО визначається шляхом експертних оцінок і розрахунків. Середня оцінка світових освітніх систем говорить про те, що дистанційне навчання обходиться приблизно на 50% дешевше традиційних форм освіти. Досвід недержавних центрів дистанційного навчання показує, що їх витрати на підготовку фахівця складають приблизно 60% від витрат на підготовку фахівців за денною формою навчання.

Відносно низька собівартість ДО досягається за рахунок використання концентрованого уявлення і уніфікації змісту, орієнтованості технологій ДО на велику кількість учнів, а також за рахунок більш ефективного використання існуючих учбових площ і технічних засобів.

Орієнтація на споживача є одним з найбільш важливих факторів успіху розвитку дистанційної освіти, оскільки, з різних причин, не всі люди можуть регулярно відвідувати навчальні заняття у стаціонарі. Дистанційне навчання розширює доступ до якісної освіти. Опора на передові комунікаційні технології є найважливішою характеристикою СДО з визначення та коментарів тут не потрібно.

Слід зазначити, що єдина система дистанційної освіти будується "стільниковим" методом і тому проблема створення цієї системи вирішується на трьох рівнях:

- глобальні (міжнародні і федеральні) підсистеми ДН та їх забезпечення;
- регіональні та галузеві підсистеми ДН та їх забезпечення;
- локальні підсистеми ДО та їх забезпечення.

Проблеми власне організації дистанційного навчання вирішуються шляхом розподілу робіт за наступними напрямками:

- концептуальні моделі та дидактичні аспекти ДО;
- методичні та психолого-педагогічні основи ДО;
- система викладачів-консультантів і способи їх взаємодії з учнями;
- контроль якості та тестування в СДО;
- технології та інформаційно-освітні середовища;
- способи передачі освітньої інформації;
- типове оснащення регіональних центрів дистанційного навчання.

Різка зміна соціально-економічної ситуації у світі істотно знизило потенційну доступність навчання у провідних вузах країни для широких верст населення. У цій ситуації застосування дистанційних форм навчання дозволяє зробити важливий крок у напрямку відновлення порушених принципів соціальної рівності.

З урахуванням цього останнім часом низкою фахівців запропоновано поняття "ідеальної (або" оптимальної) моделі дистанційного навчання, яка включає у собі інтегровану навчальну середу з варіантним визначенням ролі різних компонентів - технологічних, педагогічних, організаційно-методичних. При цьому дистанційне навчання може забезпечити високу ефективність і досить низьку вартість курсу навчання для кожного студента при великому числі учнів за рахунок екстенсивного використання одного разу розроблених навчальних матеріалів (друкованих видань, аудіо-, відеокасет, телекомунікаційних та комп'ютерних навчальних програм, мультимедійних курсів на компакт-дисках і т.п.), ціна тиражування яких невелика.

У поєднанні з традиційними підручниками та методичними посібниками це і створює унікальну розподілену середу, доступну широкої аудиторії. Можна розділити використовувані сьогодні інформаційні технології дистанційного навчання за якісним пріоритетом реалізації взаємодії і ступеня комунікабельності учнів і викладачів на такі категорії:

- не інтерактивні (друковані матеріали, аудіо-, відеоносії);
- засоби комп'ютерного навчання (електронні підручники, новітні засоби мультимедіа, бази даних і знань, навчальні та контролюючі системи, електронні бібліотеки);
- відеоконференції - засоби телекомунікації з аудіо-, відеоканалами та комп'ютерних мереж.

Однак будь-які методи, технології, підходи мають свої обмеження. Ймовірно, обмеження інформаційних технологій усвідомлюються сьогодні недостатньо і досліджено далеко не повно. Так, незважаючи на величезну рекламу і вже проведені значні витрати, затребуваність "електронних підручників", "електронних журналів" тощо, виявляється невелика, коефіцієнт їх тиражування вкрай малий. Багато студентів пояснюють, що звичайний підручник все ще читати простіше, приємніше і комфортніше, а відеофільм простіше оцінити звичайному телевізорі.

У той же час є принципова особливість, що надає цим коштам великий сенс, - інтерактивність. Це вимагає створення електронних засобів навчання у стилі "навчальних ігор", "активного діалогу", "сценаріїв освітнього процесу". Їх продумування і розробка є головною частиною проблеми розвитку дистанційного навчання. Саме цій частині роботи ні в Росії, ні в світі належної уваги ще не приділяється.

У кожному конкретному випадку повинні застосовуватися ті методи, які найбільшою мірою відповідають цілям навчання. Так, якщо в результаті навчання передбачається видача деякого сертифіката або диплома, що має серйозне самостійне значення, то, безумовно, завершальна стадія навчання, а саме випускний іспит або захист диплома повинні здійснюватися очно. Те навчання, яке пов'язане з роботою на спеціальному обладнанні, також має здійснюватися в місці розташування цього обладнання. Однак підготовчі, теоретичні етапи цілком можуть здійснюватися дистанційно.

По суті, даний дистанційне навчання виникає при наявності дистанційної ж зворотного зв'язку. Цілком можна уявити собі організований на сучасному рівні письмовий обмін інформацією між учнями і викладачами. При цьому викладач зовсім не обов'язково повинен відповідати студенту на кожен лист. У принципі повинні бути визначені терміни виконання окремих завдань, форма подання матеріалів, форма організації консультацій, способи оцінки представлених результатів та інше. Кожен студент задає свої питання, але отримує повний перелік відповідей викладача для всіх студентів. Тут найбільш зручною визнається Телекомунікаційна система у вигляді електронної пошти або телеконференції.

Таким чином, складовою частиною інформаційно-освітнього середовища є як навчаються, так і викладачі, взаємодія яких здійснюється за допомогою сучасних інформаційно-обчислювальних засобів. Таке навчальне середовище надає унікальні можливості учням для здобуття знань як самостійно, так і під керівництвом викладачів або тьюторів.

При розробці навчальних курсів дистанційного навчання упор робиться на самостійну роботу учнів, їх індивідуальна творчість, проведення власних міні-досліджень різного рівня. Повинно передбачатися найбільшу кількість завдань, розрахованих на самостійну розробку, з можливістю отримання оперативних консультацій. Світовий досвід дистанційного навчання показує, що при такій організації навчального процесу взаємодія учнів і викладачів на індивідуальній основі відбувається набагато ефективніше, ніж при інших формах організації освітнього процесу.

Використання у дистанційному навчанні великої інформаційної бази потребує вирішення цілого ряду супутніх проблем, пов'язаних з дотриманням авторських і майнових прав розробників, захистом інформації, тестуванням і сертифікацією програмних та навчальних продуктів.

Таким чином, для успішної практичної реалізації дистанційного навчання необхідне здійснення наступного:

- оперативна доставка навчальної інформації навчається;
- здійснення зворотного зв'язку з викладачем;
- забезпечення дистанційної індивідуальної та / або групової роботи.

1.4 Мультімедіа технології в освіті

Практично всі класи інформаційних ресурсів використовують засоби мультимедіа.

Криза епохи аналогової інформації проявляється в трьох основних явищах:

- накопичену інформацію складно переробляти;
- складно забезпечити подальше збереження інформації;
- пристрої запису, зберігання та відтворення інформації надзвичайно різнорідні.

У сучасних глобальних інформаційних технологіях, технічної базою яких став комп'ютер, а методичною - цифрове представлення інформації, ці проблеми усунені, в результаті чого:

- інформація однорідна: текст, звукоряд, відеоряд представляються єдиним чином, у цифровому вигляді;
- інформацію легко зберігати:
  - по-перше, вона в цифровому вигляді не спотворюється при копіюванні;
  - по-друге, оптичні носії інформації мають тільки гарантійний термін зберігання десятки років;
- Інформацію легко переробляти: всі операції від рутинних (наприклад, пошук) до творчих (наприклад, перетворення) на комп'ютері проводяться або автоматично, або автоматизовані (за участю людини).

Цей перелом і явне окреслення меж двох інформаційних епох внесла поява мультимедійних технологій.

Саме ці технології об'єднали текст, звук, графіку, фото, відео в однорідному цифровому поданні. Відповідно і засоби обробки, зберігання та відтворення масивів інформації стали концептуально однаковими.

Мультимедіа зажадало створення ємних і довговічних носіїв інформації - оптичних компакт-дисків. Останній стандарт оптичного носія - DVD (Digital Versatile/Video Disk) зробив концепцію однорідності цифрової інформації зримою і відчутною - один пристрій замінює аудіоплейєр, відеомагнітофон, слайдер та інші пристрої відтворення.

Саме мультимедійним технологіям зобов'язаний Інтернет нинішнім розквітом (WWW-сервер, телефонія (відеотелефон), інтерактивне телебачення тощо). Стало очевидним, що саме широке впровадження мультимедійних технологій в освіту, де багато десятиліть панувала книга, сьогодні стало питанням існування освіти в новій інформаційній епосі.

Ще в 1992 році сам термін «мультимедіа» в Україні був мало кому відомий. Але саме тоді було розгорнуто першу міжвузівську науково-технічну програму «Мультимедіа технології», створено першу професійна кіно-фотостудію, розроблено перші мультимедійні продукти.

До найбільш важливих результатів шестирічної роботи з цим науково-технічним програм належать:

- виконано більше 60 мультимедіа розробок, з них понад 20 видані широким тиражем на CD-ROM, тобто представляють дійсно «продукти», виконані професійно і мають ринкову вартість і попит;
- в 1992-1997 рр.. мультимедійні продукти і технології, розроблені в українській вищій школі, представлялися більш ніж на 50 міжнародних і українських виставках і спеціалізованих тематичних конференціях. У тому числі, на найбільших у світі: CeBIT / 93, 94, 95, 96, 97 у Німеччині, Comdex Fall / 94, 95 у США, Milia / 94, 97 у Франції, ED-Media / 94, 95 в Канаді та Австрії, Worldclidac / 96 у Швейцарії та інших;
- мультимедійні продукти видані в Західній Європі (Швейцарія, Італія, Франція, Великобританія);

Досягнуті результати утворюють необхідний базис для вирішення нових завдань. Період розробки експериментальних зразків мультимедіа минув. Настав час повних з фізичного і функціональному обсягом мультимедіа продуктів, готових до видання на CD-ROM. Обсяги в 600 Мбайт мультимедіа інформації повинні методично «закривати» повний навчальний курс або його значну частину так, щоб можна було впевнено стверджувати, що студент або школяр, може підготуватися по конспекту, книзі або лазерному диску з однаковим успіхом.

Найбільш серйозну увагу слід приділити навчальних курсів середньої школи, оскільки раніше з різних причин цей найбільш широкий освітній простір розробками мультимедіа охоплювався слабо.

Мультимедіа технології стрімко розвиваються. Зазначений вище новий стандарт оптичного носія-DVD має ємність порядку одиниць і десятків Гбайт і замінює всі попередні: CD-ROM, Video-CD, CD-Audio. Він відкриває можливості не тільки збільшення кількості інформації, але і підвищення її якості до рівня, що перевищує аналогові подання. У сфері освіти виникає нова

важливе завдання - використати можливості DVD для розширення методичного спектру, наближаючи навчальні матеріали до рівня віртуальної реальності.

Свого часу винахід друкованого верстата зробило революцію в розповсюдженні інформації. Пізніше грамплатівка, кіноплівка, магнітна стрічка, аналоговий лазерний диск доповнили книгу. Власне процес поширення інформації полягав у поширенні носіїв. При цьому паралельно розвивалися телеграф, телефон, радіо, телебачення, що поширюють інформацію без носія.

Глобальні комп'ютерні технології розвиваються за тими ж принципами: поряд з поширенням носіїв, основним з яких став CD, все більшу роль відіграють глобальні комп'ютерні мережі. При цьому однорідність подання інформації в цифровому вигляді дає нові можливості поєднання, інтеграції інформаційних ресурсів. Так, наприклад, методично далеко не легко об'єднати в комплекс книгу, видану 5 років тому, і сьогоднішню телепередачу про останні досягнення в даній предметній області. А якщо уявити собі хороший методичний комплекс для студента-заочника, то він буде включати книги, відео і аудіо касети і вимагатиме цілої студії для використання, не кажучи вже про послуги пошти та транспорту для реалізації елементарного зворотного зв'язку з викладачами.

Все це легко замінюється одним мультимедіа компакт-диском і комп'ютером, включеним в мережу Інтернет. Диск містить мультимедіа інформацію, яку важко передати через мережу через досить великий розмір. У той же час мережа дає можливість, з одного боку, оновлювати інформацію, а з іншого - проводити в інтерактивному режимі тестування, співбесіду з викладачем, тобто по суті проводити в цьому інформаційному середовищі консультації та прийом іспитів.

Таке інтерактивне теле-навчання, технологічним базисом якого є мультимедіа технології, при сучасній популярності і потрібності дистанційного навчання, природним чином стає одним з предметів актуальних досліджень у галузі інформатизації галузі освіти.

В останні роки у світі широкого поширення набули «мультимедіа кіоски». Ці мультимедійні інформаційні системи, розташовані в громадських місцях, дають по запиту наочну інформацію відвідувачам, пасажирам, покупцям з найрізноманітніших питань - від фотографій і годин прийому потрібного посадової особи до зовнішнього вигляду і вартості товарів. Мультимедіа кіоск поєднує простоту звернення, який забезпечується сенсорним екраном, з фізичної міцністю конструкцій - гарантією стійкості при масовому використанні. Такі сучасні мультимедіа інформаційні системи будуть виключно корисними в освітніх установах, а також в інфраструктурі українських міст, інформаційних центрах, в організаціях тощо.

З метою подальшого викладу положень Концепції багатокомпонентну інформаційну мультимедіа середу зручно розділити на три групи: аудіо, відео, текстова інформація.

Аудіо. Серед компонентів інтерфейсу «учень-комп'ютер», що моделює природне для нас взаємодія «вчитель-учень», обов'язково присутні звичні звуки: мова, музика, ефекти, а також їх комбінації, наприклад музика / мова - спів. Ефекти включають звуки типу грім, шум і т.д. Такі природні звуки в мультимедіа мають позначення WAVE (хвиля). Їх цифровий запис і відтворення не є нині технічним нововведенням. Наприклад, добре відомі застосовувані в побуті аудіо компакт-диски.

Найбільш важливим питанням при використанні цього елемента мультимедійного середовища є інформаційний обсяг носія. Так, при частоті дискретизації 11 КГц і восьмирозрядному запису значення амплітуди в кожній точці відліку 1 хвилина звучання потребує 66 Кбайт пам'яті. Найкращий стандарт якості - стерео, 44 кГц і 16 біт вимагає вже пам'яті в 16 разів більше, тобто для запису однієї хвилини WAVE звуку вищої якості необхідна пам'ять порядку 10 Мбайт. Проблема поєднання високої інформаційної ємкості і низької вартості пам'яті (носія інформації) в даний час в Україні, як і в усьому світі, вирішується шляхом використання оптичних цифрових компакт-дисків (CD). Однак і стандартний обсяг CD (до 640 Мбайт) дозволяє записати не

більше години WAVE звука. В даний час розвиваються методи компресії звукової інформації. На світовому ринку з'являється все більше звукових карт, що використовують апаратні методи компресії/декомпресії, оскільки відомі програмні рішення вимагають значних ресурсів комп'ютера і не застосовні для простих CD-аудіоплейєрів.

Принципово інший тип звуків, що використовуються в мульті-середовищі - MIDI (Musical Instrument Digital Interface). У цьому випадку звуки музичних інструментів, звукові ефекти синтезуються програмно-керованими електронними синтезаторами. Необхідна корекція і цифровий запис MIDI звуків здійснюється за допомогою програм-секвенсорів (музичних редакторів).

MIDI звуки включають музику (одноголосний і багатоголосу, аж до звучання оркестру) і звукові ефекти, в тому числі не мають природних аналогів. Питання синтезу мови в даний час є предметом досліджень, їх результати поки не мають широкого застосування в мультимедіа. Величезною перевагою MIDI є порівняно малий обсяг необхідної пам'яті - 1 хвилина MIDI звуку займає в середньому 10 Кбайт.

Відео. Порівняно з аудіо відеоряд представляється значно більшою кількістю використовуваних елементів. Перш за все, сюди входять елементи статичного відеоряду, які можна розділити на дві групи: графіка (мальовані зображення) та фото. До першої групи належать різні малюнки, інтер'єри, поверхні, символи в графічному режимі. До другої - фотографії та скановані зображення.

Динамічний відеоряд практично завжди складається з послідовностей статичних елементів (кадрів). Тут виділяються три типових елементи: звичайне відео (life video), квазівідео, анімація. Перший елемент - це, по суті, послідовність фотографій (близько 24 фото в секунду), другий - сильно розріджена послідовність (6-12 фото в секунду), третій - послідовність мальованих зображень.

Використання відеоряду у складі мультимедійного середовища передбачає рішення значно більшої кількості проблем, ніж

використання аудіо. Перша з них - роздільна здатність екрану і кількість кольорів. Стандарт VGA дає розподільчу здатність 640 х 480 пікселів (точок) на екрані при 16 кольорах або 320 х 200 пікселів при 256 кольорах. У свою чергу стандарт SVGA (відеозапис 512 К, 8 біт / піксель) дає 640 х 480 при 256 кольорах, а 24-бітові відеоапарати (відеопам'ять 2 Мбайт, 24 біт / піксель) дозволяють мати на екрані 16 млн. кольорів.

Друга проблема - обсяг інформації. Для статичних зображень один повний екран у режимі 640 х 480, 16 кольорів потребує 150 Кбайт пам'яті, в режимі 320 х 200, 256 кольорів - 62,5 Кбайт, а в режимі 640 х 480, 256 кольорів -300 Кбайт. Такі значні обсяги одразу визначають високі вимоги до носія інформації, відеопам'яті і до швидкості передачі даних. Останнє особливо важливо при використанні динамічного відеоряду.

Текстова інформація (інформаційні ресурси). Характерною відмінністю мультимедіа продуктів інших видів інформаційних ресурсів є помітно більший інформаційний об'єм, тому в даний час основним носієм цих продуктів є оптичний диск CD-ROM стандартної ємністю 640 Мбайт. На світовому ринку сьогодні представлені тисячі найменувань мультімедіа продуктов на CD-ROM. Як правило, каталоги містять наступні розділи:

- енциклопедії та довідники;
- освіта;
- розваги;
- ігри;
- навчальні та розвиваючі ігри.

Поряд з продуктами, підготовленими до широкого використання, вже є значна кількість мультимедіа додатків, розроблених у ВНЗ для задоволення потреб навчального процесу. Ці програми найчастіше не мають товарних якостей, зате мають незаперечні переваги з точки зору методики, оперативності і задоволення потреб цього навчального закладу.

Бурхливо розвивається напрямок - мультимедіа в телекомунікаціях. Багато великих фірми активно ведуть розробки комунікацій

на основі волоконно-оптичних мереж стандарту ISDN. Канал в такій мережі має пропускну здатність 64 Кбіт / сек і користувачеві може бути надано одночасно кілька можливостей. Спектр пропонованих застосувань мультимедіа вельми широкий - від перегляду замовних телепередачі до вибору потрібної книги та участі у мультимедіа конференції. Такі розробки вже мають загальну назву Information Highway і передбачається їх об'єднання в рамках державних програм.

Активно популяризується ідея використання вже існуючих глобальних комп'ютерних мереж для потреб вищої освіти. З цією метою доцільне об'єднання зусиль світових університетів на базі гіпермедіа технологій. Тут головне полягає в наступному. Очевидний недолік університетських мультимедіа розробок - це недостатня якість виконання. Для створення ринкових CD-ROM продуктів залучаються професійні художники, музиканти, актори, аудіо/відео інженери, програмісти. У той же час університетська розробка виконується в кращому випадку професором якої-небудь кафедри і програмістом. Як правило, така розробка невелика за обсягом, зате її методичне якість і глибина подання предметної області - поза конкуренцією. У такій ситуації видається доцільним збирати невеликі мультимедіа фрагменти навчальних курсів на серверах мереж з тим, щоб кожен викладач університету при підготовці свого курсу міг отримати необхідний йому матеріал з мережі. Один з ідеологів цієї роботи - професор Маурер (м. Грац, Австрія) - стверджує, що, незважаючи на очевидні проблеми (низька для мультимедіа пропускна здатність мереж, проблеми авторського права та ін), ідея такого «світового університету» життєздатна.

Значним недоліком будь-якого навчального видання є його детермінованість. Кожен вчитель школи, викладач ВНЗ будує свої заняття з урахуванням сучасної ситуації, можливостей і цілей аудиторії, нюансів розвитку навчального процесу в конкретному навчальному закладі.

Мультимедіа технології в принципі дозволяють побудувати адаптивний навчальний курс, який визначається методикою, науковим потенціалом і світоглядом конкретного викладача. З іншого боку, ефективність самостійних занять значною мірою залежить від урахування смаків, інтересів, психофізичних особливостей учня. Дозвіл протиріч між життєвою динамікою і статикою канонічного подання є одним з найактуальніших предметів досліджень в області проблем інформатизації безпосередньо освітнього процесу.

Впровадження інтерактивних технологій в найпотужніше на сьогодні засіб масової інформації-телебачення - має величезні перспективи для розвитку освіти, освіти, культури та демократії в суспільстві. Комп'ютерні мультимедіа технології в поєднанні з сучасними засобами телекомунікацій дають принципово нові можливості як телепрограмі (її ведучим), так і телеглядачам (слухачам). Розвиток цього напрямку, дослідження та розробки, що випереджають світові досягнення, є одним з показників другого рівня української науки і технологій.

Сучасний період розвитку нашого суспільства характеризується швидким зростанням кількості мультимедійних електронних видань, в тому числі видань, яким самі автори визначають навчальний призначення. У цій ситуації необхідне втручання спеціалістів у галузі освіти, які, з одного боку, зобов'язані захистити інтереси покупця на новому ринку освітніх послуг, а з іншого боку - допомогти виробникам у створенні дійсно навчальних продуктів.

Добре відомо, що участь педагогів і вчених у створенні мультимедіа електронного видання анітрохи не поступається, більше того, перевершує за складністю і трудомісткості підготовку класичної монографії. Цілком очевидно, що настав час «зрівняти в правах» електронне і книжкове видання.

Розробка методології, документальної та технічної бази сертифікації та видача рекомендаційних грифів Міносвіти України мультимедіа електронним виданням навчального призначення є ще одним із завдань інформатизації сфери освіти.

1.5 Класифікація програмно-апаратного комплексу в освіті

У багатьох міжнародних і українських документах зафіксовано, що світова і вітчизняна системи освіти переживають кризу. Однією з основних причин цієї кризи є постійне відставання змісту і якості освіти від швидкості зміни сучасних технологій. Тому на порядку денному гостро стоїть питання про ліквідацію цієї кризи за рахунок створення нових інформаційних технологій та програмно-апаратних комплексів у вітчизняній сфері освіти.

Цей розділ концепції написаний на підставі матеріалів науково-технічного звіту «Класифікація та сучасний стан обчислювальних платформ та програмного забезпечення», який підготовлено відділенням «Обчислювальні платформи та програмне забезпечення» Науково-експертної ради з інформатизації сфери освіти.

Звіт містить виклад технічної політики з надання методичної допомоги в галузі обчислювальної техніки (ОТ) та програмного забезпечення (ПЗ) як колективним, так і індивідуальним користувачам і розробникам інформаційних технологій у сфері освіти.

Ці дві, здавалося б різні завдання вибору ОТ («HARD»), ПЗ («SOFT») насправді сильно взаємопов'язані. Зусилля фізиків і технологів в області мікро-і наноелектроніки призводять до перманентного ущільненню кількості транзисторів на одиницю площі або об'єму кристала, що призводить до створення все більш швидкодіючих процесорів. За законом, виведеним засновником компанії INTEL - основного розробника процесорів для персональних комп'ютерів Гордона Мура, кожні 18 місяців щільність транзисторів на кристалі подвоюється. Нові потужності процесорів дають можливості розробникам ПЗ створювати все більш інтелектуальні програми, які не можуть бути реалізовані на попередніх версіях Вт

Згідно з іншим законом про можливості споживчого ринку, покупець в основній своїй масі може заплатити за новий інструментарій не більше 2-3 тисяч доларів кожні, приблизно, 2-3 роки. Звідси випливає циклічний механізм гонки розвитку ОТ, ПЗ.

Необхідність регулярного збору і класифікації інформації про сучасні програмно-апаратних засобах не викликає сумнівів. На її основі є можливість проведення грамотного і науково-обгрунтованого аналізу отриманої інформації, використовуючи сучасні методи оцінки якості та класифікації програмно-апаратних засобів. Це, у свою чергу, дає можливість робити висновки на предмет доцільності впровадження різних програмно-апаратних комплексів у ВНЗ України. Такий підхід допомагає при розробці нових державних програм у системі освіти, дозволяючи забезпечити пошук нових методів навчання, знижує негативний ефект від традиційної інертність системи освіти.

Саме з цих міркувань до складу цієї Концепції включена справжня глава про програмно-апаратних комплексах в освіті.

Загальні положення класифікації програмно-апаратних комплексів (ПАК). Першим етапом побудови системи оцінки та вибору програмно-апаратного комплексу є вивчення всього спектру таких коштів. Це дозволяє розробити принципи побудови системи класифікаційних ознак ПАК і всієї системи класифікації в цілому. Інформація про результати локалізації в рамках безлічі класифікаційних ознак підмножини освітніх ПАК, введених в систему оцінки, використовується на наступному етапі оцінки - побудові системи характеристик якості. Ця інформація використовується також на етапі остаточного прийняття рішення для ідентифікації його переваг у стратегії вибору.

Виходячи з цих загальних положень класифікаційні ознаки освітніх ПАК представляють собою сукупність, засновану на таких передумовах:

- повнота охоплення - це означає, що на момент введення класифікації всі існуючі комплекси можуть бути класифіковані;
- інваріантність ядра системи класифікації - це означає, що поява в результаті науково-технічного прогресу нових комплексів не призводить до зміни верхніх рівнів класифікаційного дерева, а призводить або до зміни самого нижнього рівня, або до додавання нових гілок;

- взаємодоповнюваність різних систем класифікації - це означає, що одне і те ж засіб може бути класифікований у різних системах для одержання найбільш повної інформації про подальші шляхи використання системи оцінки якості і вибору.

На підставі цих передумов рекомендуються як концептуальних наступні класифікаційні ознаки:

- дидактична спрямованість;
- програмна реалізація;
- технічна реалізація;
- предметна область застосування.

Запропонована класифікація дозволяє комплексно розглядати програмні, методичні та технічні аспекти класифікації.

Класифікація за дидактичної спрямованості. У літературі зустрічається декілька підходів до класифікації компонентів програмно-апаратних комплексів по дидактичній спрямованості. Наприклад, пропонується, перш за все, класифікувати ЗНАННЯ, що передаються навчаються за допомогою комп'ютера, наступним чином. По-перше, існувало розподіл знань на явні і неявні. Надалі з розвитком досліджень в галузі штучного інтелекту ці знання стали називатися артикульованих і неартикульовані.

Артикульованих частина знань - це знання, які легко структуруються і можуть бути передані навчається за допомогою порцій інформації (текстової, графічної, відео тощо).

Неартикульована частина знань являє собою компонент знання, заснований на досвіді, інтуїції і т.п.

Ця частина знання охоплює вміння, навички, інтуїтивні образи та інші форми людського досвіду, які не можуть бути передані навчається безпосередньо, а «видобуваються» їм у ході самостійної пізнавальної діяльності при вирішенні практичних завдань. Спираючись на таку класифікацію знань, можна класифікувати освітні програмно-апаратні комплекси. Технології,

покладені в основу цих комплексів та застосовуються для підтримки процесу навчання артикульованих частини знань, є декларативними.

До них доцільно відносити:

- комп'ютерні підручники;
- навчальні бази даних;
- тестові і контролюючі програми та інші комп'ютерні засоби, що дозволяють зберігати, передавати і перевіряти правильність засвоєння навчаються інформації учбового призначення.

Технології, що використовуються при створенні ПАК, що підтримують процес освоєння неартикульованої частини знань, є процедурними. Комп'ютерні інформаційні технології (КІТ) цього класу не містять і не перевіряють знання у вигляді порцій інформації. Вони побудовані на основі різних моделей. У цьому випадку до КІТ цього класу відносяться:

- пакети прикладних програм (ППП);
- комп'ютерні тренажери (КТ);
- лабораторні практикуми;
- програми ділових ігор;
- експертно-навчальні системи (ЕОС) та інші комп'ютерні засоби, які дозволяють навчається у ході навчального дослідження одержувати (здобувати) знання з досліджуваної предметної області.

Не слід ототожнювати поняття артикульованих і неартікуліруемой частин знання з поняттям відповідно формалізованих і неформалізованих знань. Нерідко неформалізовані знання також можуть бути представлені в потрібному вигляді, наприклад, у вигляді евристичних правил і передані навчається за допомогою систем декларативного типу.

Наведена класифікація за ознакою декларативних і процедурних технологій є, як і будь-яка інша, умовною. Слід говорити лише про більш високий ступінь детермінованості процесу отримання знань в декларативних системах і свободи процесу їх освоєння у процедурних системах. Один і той же освітній програмно-апаратний комплекс може бути

використаний за першою або другою технології в залежності від застосовуваної методики. Наприклад, лабораторний практикум може бути забезпечений гнучкими інструкціями, що і в якій послідовності виконувати. У цьому випадку навчається отримує готову інформацію про процес і, відповідно, отримує декларативні знання. Якщо ж навчальна завдання поставлено таким чином, що навчається необхідно для її вирішення провести дослідження, то цей же програмно-апаратний комплекс дозволяє отримати деяку порцію процедурних знань.

Можливий і інший підхід до класифікації ПАК по дидактичній спрямованості. У цьому разі сучасні комп'ютерні технології навчання також діляться на два класи:

- системи програмованого навчання (СПО);
- інтелектуальні навчальні системи (ІНС).

Технологія програмованого навчання передбачає отримання навчаються порцій інформації (текстової, графічної, відео - все залежить від технічних можливостей) у певній послідовності і забезпечує контроль за засвоєнням в точках навчального курсу, визначених викладачем.

Інтелектуальні навчальні системи відрізняються такими особливостями, як адаптація до знань і особливостям учня, гнучкість процесу навчання, вибір оптимального навчального впливу, визначення причин помилок учня. Для реалізації цих особливостей ІНС застосовуються методи і технології штучного інтелекту.

Структура ІНС містить загальні та спеціальні знання трьох класів:

- про предметну область;
- про стратегії навчання;
- про учня (модель навчається).

В інтелектуальних навчальних системах ці знання представлені у відповідних базах знань за допомогою різних методів і засобів. При цьому в моделі учня виділяються три компоненти, кожен з яких

включає процедурну і декларативну складову. Це наступні компоненти:

- а) база знань учня;
- б) діагностика його знань і виконуваних завдань;
- в) алгоритм формування нових завдань.

Модель учня постійно оновлюється в ході навчання у відповідності зі змінами розкритих нею характеристик учня.

Розподіл технологій розробки програмно-апаратних комплексів на СПО і ІНС не може бути суворим, оскільки системи одного класу можуть включати в себе і елементи іншого.

Для реалізації ІНС використовуються такі засоби:

- експертні системи;
- гіпертекстові системи;
- системи мультимедіа;
- програми ділових ігор;
- мультфільми.

Наведений вище поділ технологій комп'ютерного навчання на процедурні й декларативні, а також на СПО і ІНС випливає з поділу цілей навчання на два класи:

- навчання навичкам використання конкретних методів в практичній діяльності, отримання і систематизація різних фактичних даних;
- навчання аналізу інформації, її систематизації, творчості, досліджень.

Системи другого класу (2) дозволяють проектувати навчальні курси значно складніші, ніж системи першого класу (1). Саме з їх допомогою можна навчити процесам проведення синтезу, аналізу, аналогії, порівняння, дедукції, індукції тощо Обидва класи технологій взаємно доповнюють один одного, тому в цілому ряді випадків невірним є відмова від систем першого класу на користь систем другого класу.

Слід постійно мати на увазі, що бурхливий розвиток засобів інформаційно-обчислювальної техніки надає сильний психологічний тиск на викладачів та розробників навчальних програм, змушуючи та / або

примушуючи робити крен у бік використання в першу чергу технічних досягнень, а не методичних знахідок.

Так, наприклад, це може мати місце при використанні таких сучасних засобів, як гіпертексти і мультимедійного середовища. З положень, викладених вище, випливає, що ці кошти можуть використовуватися і як системи першого (1) і як системи другого (2) класу. При цьому відомий підхід до розвитку гіпертексту не з точки зору нарощування його технічних можливостей (чому найчастіше приділяється увага в технологіях мультимедіа), а з точки зору посилення його інтелектуальних та партнерських якостей. Такі гіпертексти вважаються інтелектуальними. У цьому випадку з їх допомогою викладач повинен мати можливість:

- ідентифікувати проблему навчання (фрагмент предмета, курсу) або обмежити сферу інформаційних потреб учня;
- відібрати з гіпертексту підмножина конкретних вузлів, зміст яких відповідає інформаційним потребам навчається або є корисним при пошуку вирішення якої-небудь задачі;
- в безлічі вузлів виділити основні і допоміжні, деталізують кілька рівнів, і вирішувати проблему їх оформлення;
- забезпечити відібрані вузли необхідними зв'язками, відсікаючи непотрібні в даному контексті.

Вибір варіанта класифікації ПАК по діктатіческой спрямованості (див. вище п. 400 і п. 401) ВНЗ проводять виходячи зі своєї специфікації і досягнутого рівня інформатизації навчального процесу.

Класифікація за способом програмної реалізації. За способом програмної реалізації програмно-апаратні комплекси можна розділити на три класи:

- Створені за допомогою прямого програмування на мові високого рівня;

- Створені з використанням коштів об'єктного програмування;

- Створені за допомогою інструментальних авторських систем (ІАС).

Цей поділ також не є досить жорстким, тому що більшість авторських оболонок має вихід в середу прямого програмування. Це пояснюється тим, що

універсальні, а тим більш спеціалізовані інструментальні оболонки зазвичай не реалізують багато функцій, необхідні для створення освітніх програмно-апаратних комплексів по типу процедурної реалізації дидактичної складової. Наприклад, вони не мають коштів для математичного моделювання об'єктів.

Зазвичай дидактичні особливості, наприклад, програмування ділових ігор і ситуацій, здійснюються підключенням зовнішніх виконуваних модулів з наявністю або відсутністю одно-або двостороннім передачі даних. В якості мов програмування для виходів в зовнішнє середовище найчастіше використовувалися: C + +; Pascal; Prolog.

Останні досягнення в програмному забезпеченні дозволяють перейти до використання елементів об'єктно-орієнтованого програмування (наприклад, з використанням мов, що входять у програмний продукт Microsoft Visual Studio).

За принципами організації процесу навчання інструментальні авторські системи (ІАС) поділяються на традиційні та інтелектуальні.

Інтелектуальні ІАС спираються на останні досягнення в області штучного інтелекту і є, безумовно, передовими для розробки прикладних комп'ютерних навчальних програм (КУП), націлених на проблемно-орієнтований підхід до навчання.

Традиційні ІАС залежно від наявності у них тих чи інших функціональних можливостей доцільно розділяти на універсальні і спеціалізовані.

Універсальні ІАС повинні забезпечувати наступні функціональні можливості:

- введення і аналіз відповідей;
- формування логічної структури КУП;
- підтримку та формування текстового і графічного матеріалу;
- забезпечення динаміки зображень;
- математичне моделювання з візуалізацією результатів;
- організацію гіпертекстових структур;

- збір і обробку статистичної інформації;
- формування рейтингової оцінки рівня знань;
- можливість роботи в локальній обчислювальній мережі;
- функціонування КУП в автономному режимі.

В даний час існують десятки як зарубіжних, так і вітчизняних універсальних ІАС. В останні роки у зв'язку з розвитком технічних можливостей для створення програмно-апаратних комплексів на основі технологій мультимедіа до функціональних можливостей універсальних ІАС додалися ще дві: звуковий супровід і підтримка відеозображення.

Спеціалізовані ІАС комп'ютерних навчальних програм у залежності від їх цільового призначення доцільно поділяти на такі типи:

- гіпертекстове і гіпермедіа ІАС;
- моделюють ІАС;
- ІАС для контролю знань і педагогічного тестування;
- ІАС для організації лекційного супроводу.

Гіпертекстові і гіпермедіа ІАС (1) характеризуються такими можливостями:

- робота з такими фрагментами, як текст, графіка, звук і відео;
- наявність різних способів пошуку інформації (за ключовими словами і «гарячих точок» екрана, за функціональними кнопкам, по темах в багатовіконному режимі, по графічним картам вузлів та зв'язків);
- багатовіконний режим роботи;

різні способи навігації (наявність стандартних маршрутів і можливість фільтрації матеріалу);

наявність механізму «закладок»;

внесення і збереження коментарів;

- побудова нових гіпертекстових структур з множинною інтерпретацією матеріалу (збирання та збереження рефератів і конспектів);
- організація взаємодії із зовнішнім середовищем (підключення моделюючих програм і т.д.).

Моделюючі ІАС (2) використовуються для розробки програм моделювання процесів та об'єктів різної фізичної природи, а також створення різних комп'ютерних тренажерів (КГ), у тому числі в реальному масштабі часу, і повинні забезпечувати наступні функціональні можливості:

- моделювання процесів, описаних алгоритмічно, а також системами математичних рівнянь і нерівностей;
- забезпечення різних сценаріїв моделювання (крім жорстких, тобто сценаріїв з можливістю управління діями учня і самою моделлю);
- підтримку інтерактивного режиму розробки моделі з корекцією дій розробника;
- застосування різних процедур (рекурсивних, ітераційних і т.д.);
- наявність бібліотеки готових форм індикаторів і датчиків;
- забезпечення роботи в реальному масштабі часу;
- можливість підключення до реальних апаратних засобів;
- наявність достатньої кількості змінних і спецфункцій.

Контроль завдань та педагогічне тестування (3). Оскільки кінцевою метою контролю і тестування є визначення та наукове вимір ступеня засвоєння навчального матеріалу і оволодіння необхідними знаннями, вміннями і навичками, спеціалізовані АІС повинні підтримувати наступні функціональні можливості:

- широкий набір способів пред'явлення завдань (випадковий вибір, генерація завдань за шаблонами і т.д.);
- повний набір способів аналізу і введення відповідей;
- гнучкість у способах виставлення оцінки рівня навчальних досягнень учня;
- збір та обробку індивідуальної та групової статистичної інформації про результати контролю;
- можливість роботи в локальній обчислювальній мережі з метою автоматичного збору інформації про хід контролю та його результати з усіх комп'ютерів одночасно.

Для створення педагогічних тестів, які представляють собою сукупність взаємопов'язаних завдань зростаючої складності, що дозволяють на надійність і валідність оцінити знання та інші цікаві для педагога характеристики особистості, необхідно виконання ряду додаткових вимог. До таких вимог належать:

- наявність в АІС інструкції для викладача у вигляді специфікації тесту, що включає в себе загальний опис, приклад тестового завдання, характеристику форми і змісту завдань, характеристику відповідей і т.д.;
- Можливість складання тестових завдань усіх відомих типів (відкритих, з вибірковою відповіддю, на встановлення відповідності, контрольованих, включаючи і контрольоване конструювання графічних зображень);
- можливість створення адаптаційних тестів, в яких вибір наступного завдання визначається в залежності від результату виконання попереднього;
- наявність засобів аналізу педагогічного тесту на валідність;
- необхідність коштів збору статистики проходження тесту навчальними групами для інтерпретації тестових балів з урахуванням нормативно-орієнтованого підходу (порівняння окремих навчальних досягнень учнів) і критеріально-орієнтованого (ступінь оволодіння навчаються необхідного навчального матеріалу).

Супровід лекційного матеріалу (4). АІС, що використовуються для цих цілей, повинні підтримувати наступні функціональні можливості:

- створення і підключення динамічних зображень;
- створення власної та підключення якісної статистичної графіки (зчитується за допомогою сканера або створеної в інших графічних редакторів);
- оформлення тексту різноманітними стилями;
- звуковий супровід матеріалу.

Наступний спосіб класифікації методів реалізації навчальних комплексів здійснюється в межах класифікаційної ознаки «програмна реалізація» для:

а) операційної системи Windows;

б) операційної системи MS-DOS.

Спочатку більшість використовуваних в даний час КУП функціонувало під управлінням операційної системи MS-DOS. Однак в останні роки всі сучасні мультимедіа програми для обчислювальних платформ IBM орієнтовані на операційну систему Windows і ця тенденція буде зберігатися, тому що система Windows підтримує певний рівень стандартизації інтеРфейсу, що дуже важливо у навчанні. Це дозволяє студенту не витрачати час на вивчення особливостей роботи з програмою, а майже відразу ж приступити до змістовної частини навчання.

Необхідність створення авторських інструментальних систем не втратила своєї актуальності після впровадження в практику такої потужної оболонки, як Windows. Це пояснюється тим, що робота в Windows передбачає знання особливостей і стандартних угод операційного середовища Windows, що найчастіше недоступно викладачеві-непрограмістів.

Методичні можливості, інтелектуальність і ефективність комп'ютерного навчання багато в чому визначаються можливими видами відповідей учнів. Використання глобальних мереж для дистанційного навчання стало можливим завдяки бурхливому розвитку техніки і появи зручних і доступних технологій для роботи з розподіленими базами даних, таких як WWW-технології.

Ці можливості особливо привабливі для створення віддалених навчальних середовищ, побудованих за технологією гіпермедіа. В даний час комп'ютерні технології дозволяють транспортувати на віддалені комп'ютери будь-які навчальні і тестуючі системи. Такий досвід у світі є. Наприклад, відомі відкриті університети в Європі.

Класифікація комплексів за видами технічної реалізації і ступеня використання у різних предметних областях.

Технічна політика в частині апаратної реалізації ПАК є прерогативою кожного окремо взятого ВНЗ, оскільки централізовані закупівлі інформаційно-обчислювальної техніки в останні роки практично не проводяться.

Класифікація програмно-апаратних комплексів по предметним областям також проводиться ВНЗ самостійно на підставі класичного поділу предметних областей на природничо-наукові, загально-інженерні, спеціальні та гуманітарні.

Аналіз сучасного стану комп'ютерних інформаційних технологій у вищій школі показує, що з появою персональних комп'ютерів насамперед почали з'являтися тестуючі та контролюючі програми, що підтримують традиційні технології навчання, в першу чергу, в області природничих дисциплін, де методики навчання носять історично усталений характер. Потім із розвитком технічних можливостей персональних комп'ютерів КУП стали оснащуватися можливостями моделювання. Вище наводилися окремі приклади КУП, що ілюструють різні класифікаційні ознаки.

1.6 Розвиток інфраструктури та телекомунікацій сфери освіти

Під інфраструктурою в економіці розуміються структури, які забезпечують функціонування виробничих систем, і безпосередньо в технологічних процесах виробництва продукції не беруть участь. У їх число входять: дороги, лінії електропередачі, системи постачання ресурсами і т.п.

Під інфраструктурою інформатизації освіти зазвичай розуміють телекомунікаційні мережі і зв'язуються ними об'єкти: сервери, автоматизовані робочі місця, системи надання інформаційних ресурсів і т.п.

Одним з важливих досягнень виконання робіт з інформатизації освіти в попередні роки вважається створення в України мережі регіональних центрів інформатизації освіти та центрів нових інформаційних технологій. Структура цих центрів та її взаємодія з Міносвіти України і регіональними органами управління освітою.

В даний час створені організаційна інфраструктура, ресурси науково-освітніх мереж, а також досвід, набутий в ході їх створення та експлуатації, стали основою Міжвідомчої науково-технічної програми «Створення

національної мережі комп'ютерних телекомунікацій для науки і вищої школи (НСКТ НВШ) ».

Побудова, експлуатація та розвиток опорної інфраструктури НСКТ НВШ багато в чому буде залежати від того, наскільки ефективно в цих роботах буде акумульовано і врахований досвід становлення і розвитку мереж за кордоном, а також результати виконання вітчизняних телекомунікаційних проектів для середньої і вищої школи і науки.

Світове співтовариство в останні роки утворило світову інформаційну мережу на базі комп'ютерних телекомунікацій (Internet, Freenet, Runnet, Intranet тощо), що дало принципово новий рівень розвитку людського суспільства як такого, його економіки і забезпечують систем.

Зокрема, через ці мережі з будь-якого робочого місця, оснащеного сучасним комп'ютером (сьогодні вартість до 2000 доларів США), реалізується оперативний доступ до будь-якої інформації світового інформаційного простору (біржі, банки, транспортні та інші послуги, замовлення науково-технічної, рекламної, освітньої інформації і т.д.). Можливо при цьому надання різних взаємних послуг (роботодавець-виконавець), маніпулювання фінансовими, товарними потоками, здійснення покупок, електронні гроші, електронні мети платежів, управління проектами та системами.

На порядку денному стоїть об'єднання віртуальних об'єктів до системи моніторингу управління містами, територіями, регіонами.

Для розвитку інформаційних технологій у цих контекстах і їх впровадження необхідно розгортання:

- електронних експозицій моделей (формалізованого подання) знань, даних, документів, мультимедійних образів;
- просторово і тематично інтегрованих пошукових систем;
- тренажерних залів віртуального інформаційного простору;
- інфраструктури центрів навчання з використання інформаційних технологій та їх інструментарію, центрів сертифікації тощо

Це створює необхідні передумови для створення телекомунікаційної мережі, наповненою знаннями в формі моделей і образів. Саме це і має бути реалізацією сучасної інформаційного середовища, маючи на увазі побудова і корпоративне використання учасниками освітнього процесу:

- моделей навчальних дисциплін (структурні, математичні, інформаційні, образні, логічні конструкції тощо);
- моделей рівнів і типів освіти (гуманітарної, природної, загально-інженерної, технічної, спеціальної) з відстеженням міждисциплінарних зв'язків;
- моделей віртуального інформаційного простору (візуалізація, пошук інформації тощо);
- моделей власне навчання та управління освітнім процесом.

Соціальними ефектами вирішення зазначених завдань є:

- доступ користувачів до світових систем знань і культури, трансляція знань, вироблених людством, будь-якого суб'єкта єдиного інформаційного простору;
- необмежена свобода творчості;
- вільне формування людиною особистісно значущих поглядів на суспільство і навколишній світ;
- розвиток гуманітарної спрямованості освіти;
- реалізація тези «доступності освіти для всіх», поширення форм домашнього та дистанційної освіти;
- зміцнення морального статусу корпусу викладачів, скорочення відтоку їх з освітніх установ;
- формування передумов і умов до досягнення нової якості освіти і створення інформаційного суспільства, «суспільства знання»;
- адаптація особистості до динамічно мінливих умов економічного функціонування і життя в цілому, зниження соціальної напруженості в суспільстві;
- інтеграція наукового і педагогічного потенціалу України у світову інформаційну середовище;

- прискорення регіональних тенденцій розвитку, підвищення продуктивності праці в інтелектуальній сфері, на виробництві та в бізнесі;
- розвиток інформаційно-освітнього середовища регіонів і суб'єктів України;
- створення в регіонах «фабрик ідей» за системою «Технопарку» і т.п.

Незважаючи на різні стартові умови в створенні і розвитку телекомунікаційних мереж, пов'язані з певним відставанням України в цьому плані, ресурсно-адміністративне забезпечення цих робіт у нашій країні в даний час не тільки порівняти, але часто і перевершує аналогічні показники країн Європи. Враховуючи історію і досвід розвитку комп'ютерних телекомунікацій у цих країнах є можливість активно використовувати в повсякденній практиці результати аналізу діяльності транснаціональних цифрових мереж передачі даних. Ця стратегія реально відповідає терміну «наздоганяти, не наздоганяючи», а вчитися на чужих помилках і недоліках.

Одним з найважливіших напрямків реалізації такої стратегії відносяться:

- доцільність і співвідношення вкладень у розвиток сегмента опорної мережі до регіональної опорній точці доступу і в розвиток інфраструктури самої регіональної мережі;
- облік ресурсів, задіяних у розвитку опорної інфраструктури «НСКТ НВШ - Rbnet» в цілому і шлюзів у закордонні комп'ютерні мережі;
- стратегічний аналіз потоків і позаштатних ситуацій на сегментах опорної мережі в регіональні мережі, порівняння їх між собою і з аналогічними даними по закордонних мереж;
- аналіз еволюції організаційно-адміністративних структур провідних світових мереж і використання його результатів при створенні відповідних структур в України.

Вивчення та аналіз даних по цих напрямках дозволяють вибрати раціональні варіанти вирішення аналогічних проблем на шляху побудови і розвитку НСТК НВШ.

У даний час розвиток глобальної мережі Інтернет відбувається настільки швидко, що кількість матеріалів, що описують поточний стан мережі, застаріває вже до моменту публікації. Однак, «неточності» інформації, викликані даними обставиною, загальної картини стану справ не міняють.

Найбільш вузьким і вразливим на сьогоднішній день місцем у системі масового використання телекомунікаційних технологій в сфері освіти України є засоби зв'язку. Тому створення єдиної телекомунікаційної мережі у національній системі освіти є однією з найважливіших завдань цієї Концепції.

У провідних зарубіжних фірм - виробників мережевих програмно-апаратних комплексів (SUN, DEC, HP, Apple, IBM і ін) існує безліч освітніх програм, які допомагають університетам та навчальним інститутам набувати, освоювати і адаптувати сучасні засоби зв'язку та навчальні комплекси. При проведенні гнучкої політики з такими фірмами є реальна можливість оснастити освітні установи та регіони сучасними, конкурентоспроможними засобами зв'язку.

Поява нових технологій передачі даних, а також мережевих інформаційних технологій, відкриває нові горизонти у використанні мереж. Початкова фаза впровадження таких технологій на практиці є дуже складною. Причинами є брак досвіду їх технічної експлуатації та використання для навчальних цілей, а також відносно слабка їх сумісність і обмежений вибір обладнання. При цьому основний перепоною є спочатку слабкий користувальницький попит, що у разі комп'ютерних мереж виражається у відсутності додатків, адекватних пропонованим мережних технологій.

Таким чином, при створенні мереж передачі даних нового покоління виникає необхідність вирішення відразу комплексу завдань, що лежать як в області телекомунікацій, так і в області інформаційних технологій.

В якості базової технології передачі даних доцільно використовувати технологію ATM (Asynchronous Transfer Mode), яка, будучи порівняно новою мережевою технологією, вже досить добре стандартизована і реалізована в широкому спектрі обладнання різних фірм-користувачів. Є досить багато прикладів успішного застосування технології ATM як у пілотних, так і в продуктивних мережах передачі даних, починаючи від академічних комп'ютерних мереж і закінчуючи мережами великих телеоператорів. Найбільш яскравими з них є національна надшвидкісна магістраль vBNS в США, що фінансується Національним науковим фондом, академічна мережа FUNET у Фінляндії, мережа Super JANET у Великобританії, мережа WARMAN в Польщі. На базі технології ATM розгорнуто і успішно виконується європейський проект міжнаціональної магістралі.

Основними достоїнствами технології ATM є:

- Високі швидкості передачі. Характерні швидкості в мережах ATM складають сотні мегабіт в секунду, що є необхідним для додатків мультимедіа і працюють в режимі реального масштабу часу.
- Підтримка широкого спектру послуг. ATM - мережа є універсальним середовищем передачі, придатної для одночасної передачі синхронного та асинхронного трафіку з різними параметрами якості (телефонія, відео, комп'ютерні дані).
- Відносна простота і висока ефективність мультиплексування і маршрутизації, а також виділення повноти пропускання. Технологія ATM дозволяє виробляти надання і незалежну маршрутизацію потоків даних від декількох кілобіт на секунду до декількох десятків мегабіт в секунду. При цьому в груповому потоці може бути досягнута висока ступінь утилізації каналу.
- Підтримка сигналізації і виділення ресурсів на вимогу. Прийняті стандарти дозволяють використовувати технологію ATM як базової технології широкосмугових ISDN-мереж (B-ISDN).

- Можливість створення віртуальних мереж необхідної топології і якості. Передача комп'ютерних даних в АТМ-мережі відбувається у віртуальних мережах, які можуть бути створені на вимогу і на час фізичного використання (передачі даних), дозволяючи тим самим істотно оптимізувати витрати.

АТМ є вельми наукомісткої технологією, що вимагає великої дослідницької та організаційної роботи при впровадженні. Дуже важливим є максимально ефективне використання всіх потенційних можливостей АТМ-технології, в іншому випадку застосування цієї технології стає економічно і технічно недоцільне. Для вирішення частини завдань, що стосуються сумісності обладнання, підтримки сигналізації, наявності реалізованих об'єктів віртуальних мереж можуть знадобитися додаткові дослідження і розробки програмного забезпечення.

Розгорнута програма експериментів на обладнанні в мережі АТМ виробляється в реальному оточенні, тобто при наданні продуктивних сервісів мережі і додатків.

Особлива увага повинна бути приділена реалізації механізмів резервування ресурсів, сигналізації, відповідності «мережному контрактом» (chaping), передачі традиційного пакетного трафіку, боротьби з «витратами» в мережі.

На логічному рівні повинні бути налагоджені й досліджені різні способи створення віртуальних мереж, оцінені їхні параметри (необхідну якість, пропускна здатність), а також їхнє сполучення з різними додатками (реєстрація, приєднання і резервування).

У частині створення, впровадження, тестування і демонстрації високошвидкісних додатків, характер додатків має бути спрямований на забезпечення спільної роботи користувачів і груп та забезпечити вільний доступ до високопродуктивних обчислювальних ресурсів (в першу чергу - до суперкомп'ютерних центрах), а також доступ до мультимедіа даними, у тому числі спільно і в режимі реального масштабу часу.

Вирішення цієї підзадачі лежить як в області застосування традиційних додатків локальних мереж у середовищі мереж віртуальних, так і в галузі створення більш складних додатків нового покоління (медіа-сервери, відео на вимогу), заснованих на спеціальних архітектур та / або протоколах (зокрема, на рівні програмного інтеРфейсу ATM-API).

Третьою обов'язковою умовою для визнання (отримання) статусу «полігону» інформатизації є наявність у суб'єкта України ВУЗу, здатного бути ідеологічним лідером в області інформатизації сфери освіти, регіону і суспільства в цілому на всій території суб'єкта України. Цілком достатнім обгрунтуванням цього умови є корпоративні інтереси вищої школи в галузі інформатизації.

Вже сьогодні досить високі передумови для виконання всіх трьох наведених вище умов отримання статусу «полігону» інформатизації є, наприклад, в Київський області.

Метою програми є використання потенціалу вищої школи регіону для прискореної інформатизації суспільства, в першу чергу, сфери науки і освіти регіону, розробка та освоєння нових інформаційних та комп'ютерних технологій, формування єдиного інформаційного середовища.

Завдання програми - інтеграція зусиль ВНЗ регіону щодо створення розвиненої регіональної інформаційно-телекомунікаційної системи, що базується на передових технологіях. Система повинна забезпечити подальший розвиток освіти і науки в регіоні, створити конкурентоспроможні освітні та наукомісткі виробничі технології, науково-технічну продукцію та інші регіональні інформаційні ресурси і послуги.

Програма складається з двох розділів:

- системи віртуальної реальності, математичного моделювання та гнучкі освітні системи;
- інформаційно-телекомунікаційні мережі.

При вирішенні глобальної проблеми нинішнього освіти - підвищення якості функціонування освітньої системи, гарантованості цієї якості - особливу

актуальність набувають ідеї, пов'язані з об'єктивізацією оцінки не тільки досягнутих, а й очікуваних, планованих результатів освітньої діяльності.

Спроби реалізації цих ідей робилися і раніше. Розвиток будь-якої предметної людської області, в тому числі і сфери освіти, реалізується певними ідеалами і нормативами, виражають цілі й установки діяльності у конкретній предметній області. У більшості областей діяльності такі цілі й установки реалізуються через стандарти.

Попередниками державних освітніх стандартів у нашій країні були кваліфікаційні характеристики фахівців з вищою професійною освітою. Зокрема, був розроблений довідник кваліфікаційних вимог до підготовки з інформатики випускників середньої і вищої школи. У цьому довіднику для кожної спеціальності системи професійної освіти були вказані рекомендовані рівні базової та спеціальної підготовки за напрямками:

- мікропроцесорна техніка (МПТ);
- системи автоматизованого проектування (САПР);
- автоматизовані системи управління технологічними процесами (АСУТП);
- автоматизовані системи наукових досліджень (АСНИ). Для кожного рівня базової та спеціальної підготовки були розроблені:
- фрагменти діяльнісної характеристики (перелік знань, умінь і навичок, які повинен придбати навчається, отримуючи базову або спеціальну підготовку відповідного рівня);
- найменування і програми досліджуваних навчальних дисциплін, їх обсяг в годинах, рекомендації за обсягом та складом практичної роботи на комп'ютерах і в спеціалізованих лабораторіях;
- теоретичні і практичні навчальні посібники;
- рекомендації з технічного оснащення комп'ютерних навчальних класів та спеціалізованих обчислювальних лабораторій.

Таблиця 1.1

Корпоративні інтереси вищої школи в області інформатизації

Основні елементи інформаційного середовища			
Інтереси вищої школи	Інформаційні ресурси	Програмно-технічні засоби	Комунікаційні засоби
1. Духовні, інтелектуальні	Забезпечення повноти доступу до міжнародних та регіональних ресурсів	Використання в навчальній та науковій роботі новітніх інформаційних технологій	Забезпечення оперативності (в часі і просторі) доступу суб'єктів вищої школи регіону до телекомунікаційних систем
2. Політичні	Демократизація доступу до інформаційних ресурсів, забезпечення гласності та достовірності по суб'єктам політичної діяльності	Проведення єдиної науково-технічної політики у розвитку програмно-технічних засобів регіонального інформаційного середовища	Демонополізація комунікаційних систем в інтересах юридичних осіб регіону
3. Соціальні	Створення регіональних баз даних: - політика; - екологія; - культура; - споживчі; - інтереси; - працевлаштування; - охорону здоров'я;	Забезпечення інтелектуального, дружнього та безпечного інформаційного середовища	Розширення сфери застосування дистанційних форм освіти
4.Економічні	Реалізація на комерційній основі професійних баз знань та комп'ютерних фондів професійно-освітніх програм	Виконання НДР і ДКР, підготовка кадрів з експлуатації та розвитку програмно-технічних засобів інформаційного середовища	Виконання НДР і ДКР, участь у проектах зі створення і розвитку регіональних телекомунікаційних систем

Сьогодні стандартизація в освіті - це черговий етап у пошуках працездатного механізму надання освітньої діяльності більш чіткої цільової спрямованості, підвищення відповідальності за результати праці всіх учасників широкому розумінні освітнього процесу: від «сценаристів» - вчених, що розробляють навчально-програмну документацію, підручники та навчально-методичні посібники різного типу, - до «виконавців» - викладачів, які покликані творчо втілювати ці сценарні задуми в повсякденній педагогічній діяльності, що призводить, у кінцевому рахунку, до тих чи інших результатів.

Проблема полягає в тому, щоб розробити механізм порівняння очікуваних результатів освітньої діяльності з реальними і на цій основі з належною доказовістю судити не тільки про фактично досягнуті результати навчання з тих чи інших навчальних дисциплін, але і про ефективність запропонованих теоретичних концепцій, як навчально-програмних документів і методик, які використовуються в освітній практиці. Іншими словами, мова йде не тільки про констатацію досягнутого рівня та якості освіти як про одномоментної, суто контрольної акції адміністративно-управлінського характеру, а й про подальшої можливості корекції освітньої діяльності, її орієнтації на більш високий рівень відповідності, збігу цілей і результатів освіти за всіма їх структурним складовим.

Саме в цьому відповідно і складається істинний критерій ефективності освіти.

Проблема реалізації ідеї стандартизації полягає в тому, щоб надати цій ідеї належну технологічність і визначити необхідну і достатню зону стандартизації в освіті, не переходячи меж допустимого у вирішенні даного завдання і не надаючи цим рішенням характеру панацеї від усіх інших проблем, з якими доводиться стикатися в сфері освіти. Це все є складною комплексною проблемою, що вимагає концептуального обґрунтування.

Практична педагогіка - це багато в чому мистецтво, а мистецтво є продуктом творчої діяльності. У сфері освіти творча діяльність повинна

приводити до результату, що задовольняє тих чи інших суспільних, у тому числі і естетичним нормам, статистично загальноприйнятій очікуванню, які на даному етапі дозволяють оцінити отриманий результат.

Разом з тим при всій стійкості ці норми й очікування не є абсолютно стабільними в часі і навіть у просторі, маючи на увазі, скажімо, простір географічне. Звідси випливає висновок: будь-який стандарт рухливий і динамічний, він лише фіксує зовні і внутрішньо детермінуючі чинники і обставини , які так чи інакше впливають на оцінку результативності якої б то не було цілеспрямованої діяльності.

Наведені вище положення та міркування дозволяють сформулювати ключові поняття концепції стандартизації. До числа таких понять повинно бути віднесено поняття відповідності. Будь-який стандарт повинен бути встановлений і прийнятий на основі відповідних вимог до стандартизований об'єктах, на основі співвіднесення змістовних параметрів даних об'єктів з якимсь суспільно прийнятим еталоном. У цьому сенсі будь-який стандарт виступає і як мета, до досягнення якого слід прагнути, і як реально отриманий результат, який повинен бути зіставлений з метою. Разом з тим стандарт - це ще й потужний засіб підвищення якості предметної діяльності, що призводить до необхідного результату.

Стандартизація, таким чином, є процедурою, що супроводжує і етап цілепокладання, і етап оцінки результативності в будь-якій сфері, пов'язаній з організацією процесу руху від заданої мети до очікуваного результату.

При цьому стандартизація не повинна вбивати творчий початок у будь-якої цілеспрямованої діяльності, не зводитися до жорсткого регламентування й алгоритмізації всього і вся. Стандартизація повинна виступати лише як засіб організації діяльності А, що дозволяє розкласти системні якості об'єкта на складові елементи, конкретизувати властивості цих елементів у їх взаємозв'язках, своєчасно врахувати динаміку факторів, що детермінують пошук оптимального шляху Б до бажаного результату, ввести в якості обов'язкової процедуру співвіднесення цілей і результатів,

нарешті, сприяти корекції В, як цілей і результатів, так і процесу, як би «розташованого» між ними.

У кінцевому рахунку, стандартизація спрямована на досягнення належного рівня, якості і ефективності в будь-якій сфері людської діяльності. Причому перші два показники характеризують переважно змістовний бік цілепокладання та результативності, а третій - сторону процесуальну, діяльнісну.

У сфері освіти ці загальні методологічні положення концепції стандартизації знаходять втілення в найрізноманітніших аспектах. Однак ступінь можливої реалізованим ідей стандартизації стосовно до різних об'єктів і явищ дуже різна. По суті, мова повинна йти про саму можливість і необхідність стандартизації в освіті, а, кажучи більш конкретно, про тих реальних об'єктах, які піддаються стандартизації не тільки без шкоди для свого нормального функціонування, а й з метою істотного підвищення кінцевої ефективності тих чи інших освітньо-педагогічних акцій.

Взаємозв'язок і взаємозалежність всіх ланок і ступенів освіти дає підставу використовувати для характеристики цілісності освітньої сфери поняття система.

Тривалий період поняття «система освіти» трактувалося, головним чином, для позначення жорсткої, централізованої освітньої структури, однакової для всіх регіонів країни, з адміністративно-командної ієрархією управління. У такій системі цілі і зміст освіти були гіпертрофовано стійкими, навчально-програмна документація та підручники роками не змінювалися, а використовувані (точніше, нав'язані вчителю, викладачу) уніфіковані методи, засоби та організаційні форми виховно-освітньої діяльності відображали не стільки творчий початок у праці педагога , скільки сформовані стереотипи і канони догматичної педагогіки, що ілюструє у своєму найгіршому варіанті витрати обов'язковою, наказовій «стандартизації» у сфері освіти.

Нова парадигма освіти, заснована на індивідуалізації та диференціації освіти, варіативності і альтернативності освітніх систем і навчальних закладів,

гнучкості та динамічності навчально-програмної документації, її прогностичності та адаптивності до мінливих умов соціально-економічного середовища та індивідуальним інтересам і здібностям учнів, змушує по-новому оцінити можливості стандартизації стосовно до цілісної системи освіти і входять до неї компонентів.

У даному випадку мова повинна йти про справді динамічних стандартах, що визначають стратегію і тактику управління освітою на всіх рівнях:

- на рівні суспільства в цілому;
- на рівні регіону;
- на рівні галузі (стосовно до професійної освіти);
- на рівні навчального закладу;
- на рівні викладацької діяльності.

Сьогодні першочерговим кроком при здійсненні реформи змісту і якості освіти шляхом його інформатизації є розробка державних освітніх стандартів по всіх щаблях освіти.

Державні освітні стандарти покликані забезпечити збереження єдності освітнього простору, можливості безперервної освіти особистості, академічної мобільності, раціональної витрати фінансових і матеріально-технічних ресурсів.

При цьому стандарти повинні відповідати запитам особистості, суспільства і держави, можливостям їх реалізації.

Державні освітні стандарти з інформатики, у свою чергу, повинні бути забезпечені інструментально-технологічної організацією, що спирається на досить строго певні еталони, а не носити довільно-інтерпретований, словесно-декларативний характер. Тільки в такому вигляді вони будуть створювати умови для розвитку економіки та науково-технічного прогресу.

Стандарт не повинен обмежувати академічних свобод викладачів, учнів, студентів та наукових працівників, розвитку варіативних програм і розмаїття видів і типів освітніх установ.

Поряд з вирішенням проблеми державних освітніх стандартів необхідно:

- розробити пакети нових освітніх технологій, що включають проблемну форму організації педагогічної роботи вчителя на будь-якому навчальному матеріалі, що забезпечують формування, підтримку і розвиток навчальної діяльності учнів;
- провести комп'ютеризацію бібліотек навчальних закладів, активно впроваджувати в освітній процес нові інформаційні технології;
- забезпечити розробку нових освітніх технологій, орієнтованих на сільську, нечисленну і малокомплектну школу, визначити особливу роль нових інформаційних технологій в освітньому процесі.

Це має створити необхідні передумови для реалізації державних освітніх стандартів, які визначають сучасні вимоги підготовки фахівців для умов інформаційного суспільства.

З кінця 80-х років зазнає істотні зміни зміст курсів базової інформатики на всіх рівнях освіти. Зменшується кількість навчальних годин, відведених на вивчення програмування. Все більше уваги приділяється вивченню нових інформаційних технологій. Націленість на вивчення в курсах базової інформатики нових інформаційних технологій, визнання високого розвивального потенціалу інформатики та її особливої ролі у формуванні сучасного інформаційного суспільства стали вихідними положеннями при розробці сучасної концепції викладання базової інформатики в навчальних закладах України.

Відмінними рисами цієї концепції є:

- визнання високого розвивального потенціалу інформатики і надання їй статусу фундаментальної навчальної дисципліни;
- відповідне сучасним поглядам, уявлення про структуру предметної галузі інформатики;
- модульне подання досліджуваної предметної області на відміну від раніше використовувався дисциплінарного;

- використання сучасних інформаційних технологій системного модульного формування змісту підготовки, заснованих на діяльнісному підході і дозволяють, виходячи з державних освітніх стандартів, сформувати програму, орієнтовану на характеристики майбутньої професійної діяльності учня з урахуванням його особистісних інтересів та особливостей.

Справою першорядної ваги є прийняття та введення в дію державного освітнього стандарту з інформатики для загальної освіти. Це буде сприяти збереженню єдиного освітнього простору країни, визначенню того освітнього мінімуму знань і умінь з інформатики, який буде гарантований для кожного випускника середньої школи. Стандарт необхідний для підвищення об'єктивності перевірки та оцінки результатів навчання, атестації роботи вчителів і освітніх установ.

У стандарті з інформатики необхідно забезпечити дотримання наступних основних принципів:

- стандарт не повинен суперечити загальним принципам державних освітніх стандартів, прийнятих Міносвіти України;
- у ньому повинні бути задані функції, структура предметного стандарту, місце відповідної освітньої галузі (навчального предмета) в навчальному плані і т.д.;
- стандарт повинен відбивати лише мінімально необхідний набір вимог щодо змісту, а послідовність, логіка вивчення предмету визначається шкільною програмою навчання;
- стандарт не може включати в свій зміст навчальний матеріал, що не пройшов достатньої експериментальної перевірки в практиці масової школи.

Ефективність використання інформаційних технологій багато в чому визначається їх якістю і довірою до них користувачів. Якість виробів, процесів проектування, виробництва і послуг, відповідність їх вимогам, встановленим стандартами, є однією з вузлових проблем, що визначає рівень життя людини і стан народного господарства країни.

Це повністю відноситься і до області освітніх інформаційних технологій. У нові інформаційні технології входять наступні основні компоненти:

- апаратні засоби інформаційно-обчислювальної техніки;
- апаратні засоби телекомунікації;
- програмні засоби (ПС) реалізації функцій інформаційних технологій;
- бази даних і бази знань;
- експертні системи;
- документація, що регламентує функції та застосування всіх компонент інформаційних технологій.

Апаратні компоненти інформаційних технологій мають досить універсальний характер і відносно слабко залежать від функціонального призначення конкретної інформаційної технології. Водночас при їх первинному виборі завжди враховується ряд технічних характеристик інформаційних технологій. Аналіз та методики випробування цих компонентів не відрізняються новизною і можуть проводитися досить традиційними методами і засобами, розробленими в області складного приладобудування.

Інші компоненти інформаційних технологій складають їхню інтелектуальну частину, визначальну призначення ІТ, функції та якість вирішення завдань за допомогою конкретної інформаційної технології. Ці компоненти ІТ значно відрізняються принциповою новизною, великою різноманітністю характеристик, які важко формалізуються і вимагають глибокого дослідження методів перевірки їх значень у реальних освітніх інформаційних технологій. Тому основна увага повинна бути зосереджена на методах і засобах випробувань цих компонентів, а також на визначенні якості найбільш складних функціональних компонент інформаційних технологій.

З урахуванням специфіки контингенту користувачів інформаційних технологій в освіті абсолютно неприпустимі аномалії функціонування цих

ІТ при будь-яких спотвореннях вихідних даних, збої та часткових відмовах апаратури і в інших нештатних ситуаціях.

Для цього випробування інформаційних технологій повинні спеціально організуватися і документуватися, що об'єднується поняттям і процесом «сертифікація» ІТ.

Архітектурна, технічна та програмно-інформаційна сумісність різних інформаційних технологій може бути забезпечена тільки шляхом стандартизації і сертифікації програмно апаратних засобів відповідно до вимог державних та міжнародних стандартів. Для цього необхідне проведення стандартизації, сертифікації та каталогізації засобів, процесів та послуг, а також проведення єдиної технічної політики при створенні (придбанні) сумісних апаратних і програмних засобів, організації взаємодії та комплексування інформаційних технологій різних рівнів.

Це повинно бути забезпечено розвитком наступних основних напрямків в області стандартизації інформаційних технологій:

- розвиток і вдосконалення нормативно-технічної бази, що визначає всі види сумісності компонент ІТ, взаємодія і комплексування інформаційних систем, що регламентує найважливіші споживчі властивості ІТ та вимоги якості, безпеки та екології;
- створення і поетапне введення в дію в рамках реалізації цієї Концепції системи сертифікації ІТ, що забезпечує об'єктивну і незалежну оцінку їх споживчих властивостей і забезпечення якості;
- створення системи каталогізації вітчизняних та імпортних ІТ в освіті, організація на її базі їх класифікації та сертифікації з метою інформаційного забезпечення користувачів в системі Міносвіти України та інших зацікавлених відомств, організацій та фізичних осіб;
- створення довідкової служби про діють і розробляються державних і міжнародних стандартах в області інформатизації сфери освіти.

В даний час переважна більшість міжнародних та вітчизняних стандартів у галузі інформатики та інформаційних технологій, що забезпечують

можливість створення переносимих технологій, недоступні українським фахівцям з-за їх локального зберігання тільки в організаціях Держстандарту України, а також з-за недостатньої системної та програмістської культури фахівців і відсутності механізмів стимулювання професійного прагнення освоїти і використовувати сучасні стандарти.

Основою системи нормативно-технічної документації в будь-якій предметній області є стандарти термінів і визначень, які повинні з необхідною і достатньою повнотою несуперечливо описувати предметну область в її сучасному розумінні на момент прийняття стандарту. Іншими словами, термінологічні стандарти повинні забезпечувати суб'єктам, які обмінюються інформацією у даній предметній області, однакове й несуперечливе розуміння цієї інформації.

Особливо гостро стоїть проблема багатозначності понять у швидко розвиваються предметних областях, до яких і відноситься інформатика.

Усвідомлюючи важливість вищевикладеної ситуації міжнародні та вітчизняні органи стандартизації розробили і ввели в дію ряд основних нормативних документів, що регламентують створення систем термінологічних стандартів і тлумачних словників.

Базовим поняттям цих документів є поняття «гармонізація». При цьому гармонізація власне понять визначається як цілеспрямована діяльність, що дозволяє усунути або знизити до прийнятного рівня відмінності, пов'язані з різним понятійним системам, що описує один і той самий об'єкт стандартизації. Гармонізація понять здійснюється не тільки в рамках систем понять, виражених різними мовами, але і в межах однієї мови.

Під гармонізацією термінів розуміється цілеспрямована діяльність, в результаті якої одне поняття в різних мовах позначається термінами, що мають одні й ті ж або подібні ознаки поняття чи мають однакову або злегка розрізняються форму. Дане визначення наводиться в документах ISO / TC 37 наводиться ряд поправок, які повинні прийматися до уваги українськими розробниками.

По-перше, рекомендується розглядати гармонізовані терміни в більш широкому плані як терміни, що позначають гармонізовані поняття незалежно від того, збігаються чи ні терміни за формою та / або буквальному значенню.

По-друге, підкреслюється, що трактування ISO/TC37 може хибно орієнтувати на введення в українську термінологію гармонізованих термінів поряд із уже наявними термінами, що призведе до зростання синонімії.

Важливість термінології, використовуваної при створенні нових ІТ в освіті, підкреслена в Декларації II Міжнародного Конгресу ЮНЕСКО «Освіта й інформатика», де визнано за необхідне звернутися до Міжнародної організації стандартів з проханням перевірити, спростити і відредагувати термінологію в галузі нових інформаційних технологій, спільно з фахівцями з освіти.

В даний час в Міносвіти України діє галузевий стандарт «Інформаційні технології у вищій школі. Терміни та визначення. ОСТ ВШ 01.002-95 ». Розробником стандарту є Державний НДІ системної інтеграції.

При розробці цього галузевого стандарту методологічною основою послужили принципові положення вітчизняних нормативних документів, а також міжнародних стандартів, наприклад:

- «ІСО 860. Міжнародна гармонізація понять і термінів ».
- «ІСО 704-87.« Принципи та методи термінології ».

Нижче, як приклад, наводяться визначення бази даних, узяті з деяких джерел, які також використовувалися при розробці зазначеного галузевого стандарту ОСТ ВШ 01.002-95:

- База даних - сукупність даних, суттєвих для деякої діяльності (IBM: Термінологічний словник з обробки даних. 1971 р.);
- База даних - подання всієї інформації, оброблюваної в інформаційній системі (Технічний звіт ІСО 9007. Концепція та термінологія для концептуальної схеми та інформаційної бази, (Е), 1987 р.);
- База даних - організований набір фактів з даної предметної області, інформація, впорядкована у вигляді набору елементів записів однакової структури. Для обробки записів використовуються спеціальні програми, що

дозволяють їх впорядкувати, робити вибірки за вказаною правилом (Бази даних. Навчальний посібник, видавництво МАІ, 1993 р.);

- База даних - пойменована, цілісна, єдина система даних, орієнтована за певними правилами, які передбачають загальні принципи опису, зберігання і обробки даних (Галузевий стандарт «Інформаційні технології у вищій школі. Терміни та визначення. ОСТ ВШ 01.002-95». М., 1995 р., 24 с).

В останні роки в Міносвіти України проводиться успішна робота з розробки державних стандартів вищої освіти. Наявність таких стандартів дозволяє організувати роботу з моніторингу професійної підготовки з ключових напрямків, визначальним національний стратегічний освітній капітал. До таких, без сумніву відноситься і підготовка з сучасних інформаційних технологій.

У середньостроковій перспективі (2000-2005 рр..) В цілому по системі освіти доцільно також ввести національні стандарти інформатизації вищої професійної освіти, що відповідають прогресивним світовим тенденціям.

Багатофакторність і складність проблем стандартизації серйозно актуалізує проблему пошуку ефективних засобів практичної реалізації цієї багатопланової завдання. Такими засобами, безсумнівно, повинні служити технічні засоби комп'ютеризації та інформатизації, які б, з одного боку, автоматизації рутинних операцій пошуку, зберігання та виборчого подання необхідної для розробки стандартів інформації, а, з іншого боку, включає користувачів цієї інформації (не тільки розробників, але і «споживачів» стандартів) у творчий інтерактивний режим «спілкування» з «об'єктивним» комп'ютером, що виключає зайву суб'єктивність і емоційну забарвленість відповідних суджень.

Ідеологія комп'ютерної підтримки стандартизації у сфері освіти складається з ряду тезовий положень, що відносяться до різних етапів обґрунтування і використання освітніх стандартів.

Дані про світовий рівень освіти відповідного виду:

- перелік навчальних предметів;

- навчальні програми, кількість годин, що виділяються на ту чи іншу тему;
- перелік знань, умінь, навичок, що формуються в навчальних закладах відповідного типу за кордоном;
- статистичні відомості про рівні засвоєння різних навчальних предметів, найбільш типових утрудненнях у навчанні і т.п.;
- експертні оцінки зарубіжних і вітчизняних фахівців про якість освіти та їх пропозиції щодо його підвищення;
- дані про структури стандартів у навчальних закладах різних країн і експертні оцінки їх порівняння;

Статистичні і змістовні відомості:

- реальні види діяльності випускників після закінчення навчального закладу відповідного типу;
- результати експертних оцінок значущості придбаних знань, умінь, навичок, творчих якостей особистості, сформованих у навчальних закладах даного рівня, для подальшого навчання чи роботи випускників;
- відсутні і надлишкові знання, вміння, навички і т.д. (В якості експертів можуть виступати і випускники, що закінчили навчальний заклад у минулі роки);

Регіональні особливості роботи навчальних закладів:

- пріоритетні види діяльності випускників;
- основні напрямки подальшого навчання;
- підвищення кваліфікації;
- перепідготовка і т.п. з урахуванням специфіки регіону;
- можливості отримання паралельного додаткової освіти, що впливає на мінімально необхідний освітній стандарт в навчальних закладах розглянутого типу;
- відомості про реальні ресурсах реалізації запланованих і розроблюваних стандартів.

Педагогічна інформація:

- дані про структуру навчального плану та навчальних програм конкретного типу навчальних закладів з урахуванням їх екстраполяціонний динаміки;
- відомості про спадкоємність даного типу навчальних закладів з попередніми і наступними освітніми ланками (спадкоємність по вертикалі);
- інформація про навчальні заклади альтернативного типу, порівняльні дані про зміст освіти в цих типах навчальних закладів;
- інформація аналітичного характеру про співвідношенні компонентів логічної структури науки та відповідного навчального предмета (підстави, теорії, закони та закономірності, категорії, поняття, терміни, правила, постулати, принципи, ідеї, методи, факти);
- експертна оцінка структури світоглядних, поведінкових і творчих якостей особистості випускника, його найбільш істотних ментальних характеристик у їх нормативному варіанті (у плані очікування);
- експертна оцінка доступності планованого стандарту для реалізації з даним контингентом учнів (з урахуванням їх реальної підготовки, інтересів, здібностей, можливостей мотивації та стимулювання навчання тощо);
- відомості про навчальній літературі, матеріально-технічній базі, кадровому складі викладачів для навчальних закладів даного типу;
- аналітичні дані про віддалені результати роботи навчальних закладів даного типу (відомості про моральні та професійні якості випускників різних років, їх суспільній поведінці, вчинках тощо);
- інформація про підсумки дослідно-експериментальної роботи з перевірки працездатності запропонованих варіантів стандартів, що дозволяє внести необхідні корективи в стандарти, мінімізувати, оптимізувати або максимізувати їх.

Вже на етапі розробки стандартів комп'ютерні технології дозволяють створити необхідні бази даних по всіх видах означеної вище інформації і в режимі «запит-відповідь» забезпечувати розробників стандартів необхідними відомостями. У принципі, такі бази даних повинні бути періодично

оновлюваними, що свідчить про необхідність організації спеціальної постійно діючої служби комп'ютерної підтримки стандартизації на різних рівнях управління освітою.

Стандарт - не самоціль. Він повинен сприяти не тільки перевірку та контроль результатів освіти, але й пошуку оптимальних шляхів досягнення цих результатів. Тому повинні бути створені умови для інформаційного забезпечення споживачів на рівні країни в цілому, окремих регіонів та навчальних закладів, особливо. Останнє важливе тому, що при всій значимості загальнодержавних стандартів, вони носять лише характер нормативних орієнтирів, інваріантних стосовно до даного рівня освіти в цілому. В умовах же диференціації освітніх установ (навіть на одному і тому ж рівні освіти), появи альтернативних навчальних закладів, а також з урахуванням регіоналізації освіти і посилення самостійності кожного навчального закладу, особливу роль набувають стандарти освіти на більш конкретному рівні, яким і є рівень навчального закладу.

При цьому слід враховувати головна вимога: до однієї і тієї ж мети, до одного й того ж очікуваного результату можна прийти різним шляхом. У цьому і полягає ідея альтернативності та диференціації освіти, а освітні стандарти повинні сприяти творчому пошуку найбільш ефективних і в принципі різноманітних методів освітньої діяльності.

Якщо на етапах розробки стандартів та їх впровадження в практику комп'ютерна підтримка зводиться, головним чином, до інформаційного забезпечення, а технічна реалізація цих функцій зводиться до створення інформаційно-пошукових систем на основі банків даних і знань, то етап контролю виконання вимог освітніх стандартів відрізняється рядом специфічних особливостей.

Стандарт освіти за самою своєю ідеєю вводиться для оцінки планованого, і досягнутого рівня освіти, її якості як з боку держави і суспільства, так і з боку кожного зацікавленого в отриманні відповідної освіти людини. Отже, комп'ютерна система контролю повинна бути розрахована і на аналіз

статистично репрезентативної вибірки за результатами масових тестових досліджень, і на обслуговування індивідуальних користувачів за їх запитами (абітурієнтів, випускників навчальних закладів, їх батьків, представників підприємств, зацікавлених у високій якості підготовки своїх можливих працівників і т.д.).

У будь-якому випадку мова йде про порівняння отриманих результатів з еталонними з оптимального числа найбільш істотних параметрів. Їх кількість має бути достатньою для обґрунтованого судження про відповідність (або невідповідність) результатів контролю того чи іншого стандарту, але не надмірно великим, ускладнює процес оцінки результативності освіти.

У принципі, будь-яка система автоматизованого контролю являє собою людино-машинну систему, тому мова може йти тільки про ступінь автоматизації системи контролю. Роль людини зводиться до розробки та введення в комп'ютер системи тестів, а також засобів програмного забезпечення. Комп'ютер виконує функції порівняння та оперативного подання відповідних результатів і бере участь разом з людиною у виконанні експертних функцій. Останні орієнтовані на корекцію тих чи інших освітніх акцій як на рівні контролю ефективності функціонування системи освіти, так і на індивідуальному рівні (якщо це ще можливо). Крім того, за підсумками контролю можуть бути видані рекомендації про найбільш доцільних напрямках використання отриманої освіти в наступної навчальної чи трудової діяльності (при індивідуальному контролі). У цьому випадку мова йде про профорієнтаційному ефекті контролю.

Винятково важливою є також психолого-педагогічна завдання - обґрунтування системи параметрів контролю.

Можуть бути різні підходи до її вирішення. Один з можливих способів, орієнтованих переважно на індивідуальні потреби викладачів і учнів, зводиться до наступного.

Результати освіти можуть бути відображені у відповідному тезаурус, що включає в себе систему понять, адекватно і з належною повнотою характеризує рівень і якість отриманої освіти.

Очевидно, що еталонний тезаурус у тій чи іншій мірі відрізняється від того реального тезауруса, яким у результаті утворення опанував учень або випускник навчального закладу. Еталонний тезаурус завжди багатша індивідуального. Ступінь відмінності між ними, виражена відповідними кількісними характеристиками, і може бути основним показником виконання освітнього стандарту.

Процедура складання (і періодичного оновлення) еталонного тезаурусу - завдання, безсумнівно, трудомістка й у психолого-педагогічному відношенні творча. Всі інші процедури, порівняння і оцінки цілком піддаються формалізації і технічно дуже прості.

Завдання полягає в експериментальній апробації даного методу і його впровадження в масову практику.

Поєднання безперервно функціонуючих людино-машинних систем стандартизації, врешті-решт, має привести до організації спеціальної служби державного і громадського контролю за якісним рівнем освіти в країні.

Проблеми і перспективи сертифікації програмних засобів інформаційних технологій в освіті

Інформатизація суспільства значною мірою повинна базуватися на цілеспрямованої діяльності всіх груп населення з освоєння нових інформаційних технологій. При цьому особливий акцент повинен бути зроблений на впровадженні цих технологій в освітні структури (дошкільні установи, школи, середні спеціальні навчальні заклади, ВНЗ і фундаментальну наукову освіту).

В Україні за останні п'ять-сім років досягнуто значного прогресу в галузі забезпечення різних сфер інформатизації сучасним телекомунікаційним і мережним устаткуванням. Проте позитивний ефект при цьому часто

знижується через неякісне програмного забезпечення, а також застосування «піратських версій» останнього.

Робота на неякісних програмних продуктах призводить до «неповноцінності» створюваних на їх основі баз даних, інформаційних систем, предметних додатків і т.д. Актуальною є проблема якості програмного забезпечення і для освітньої сфери, в різних областях якої в масовому порядку використовуються програмні засоби, що мають в більшості випадків предметно-орієнтований характер і для створення яких гостро необхідні ліцензійні інструментальні засоби.

Галузева система сертифікації засобів інформаційних технологій у сфері освіти

(Галузева система) - передбачає створення в рамках Міносвіти України (на базі ВНЗ, науково-дослідних установ, центрів НІТ та регіональних центрів інформатизації) регіональної мережі випробувальних лабораторій і органів сертифікації, акредитованих в різних відомчих і позавідомчих системах сертифікації та забезпечують всебічну сертифікацію використовуються у сфері освіти засобів інформаційних технологій, до яких, в першу чергу, відносяться:

- телекомунікації, мережеве обладнання;
- сервери та персональні комп'ютери;
- мультимедійне і периферійне устаткування;
- операційні системи;
- текстові та графічні редактори;
- СУБД;
- інструментальні засоби розробки;
- спеціалізовані засоби навчального призначення (навчальні системи, електронні підручники, бази даних, електронні журнали та ін);
- засоби забезпечення інформаційної безпеки.

Метою створення Галузевий системи сертифікації є проведення єдиної політики в області інформатизації в частині ефективного застосування якісних засобів інформаційних технологій у сфері освіти, грунтуючись на системному

обліку вимог стандартів (міжнародних, державних і галузевих) і проведенні об'єктивної та незалежної оцінки споживчих властивостей окремих компонентів та інформаційних технологій як цілісної системи.

В аспекті розвитку Галузевий системи сертифікації необхідне рішення наступних перспективних завдань:

- розробка та реалізація галузевої політики стандартизації та сертифікації освітніх інформаційних технологій, що забезпечують ефективність процесу навчання та якості освіти;
- розробка та впровадження галузевих стандартів та нормативної бази для системної сертифікації засобів інформаційних технологій у сфері освіти;
- розвиток регіональної мережі випробувальних лабораторій та органів з сертифікації з акредитацією та ліцензуванням їх діяльності, а також організація регіональних навчально-наукових центрів, орієнтованих на діяльність у галузі стандартизації, сертифікації та консультаційних послуг;
- цілеспрямована підготовка кадрів для забезпечення потреб Галузевий системи сертифікації;
- розвиток матеріальної бази, включаючи програмно-апаратні комплекси для проведення випробувань та сертифікації основних засобів інформаційних технологій;
- проведення моніторингу для організації тестових випробувань та ведення галузевого реєстру сертифікованих засобів інформаційних технологій, включаючи ведення обліку розподілених баз даних на Web-серверах і організацію робіт в режимі віртуальної корпорації;
- залучення уваги науково-педагогічної громадськості до проблем сертифікації шляхом проведення виставок, конференцій, круглих столів, наукових публікацій тощо.

Принципи сертифікації. Відповідно до чинного законодавства України під сертифікацією розуміється дія третьої сторони, незалежною від виробника і споживача продукції, яка доводить, що належним чином ідентифікована

продукція відповідає конкретному стандарту (міжнародному, національному, галузевому) або іншому нормативному документу.

В основі сертифікації лежать випробування (тестування), тобто сукупність технічних процедур, що дозволяють адекватно визначити заявлену характеристику об'єкта сертифікації.

За результатами випробувань може бути оформлений сертифікат відповідності або висновок про невідповідність продукції, що сертифікується встановленим вимогам. Сертифікат є документом, виданим відповідно до правил Системи сертифікації і котрі засвідчують, що програмний продукт відповідає встановленим вимогам.

В ході сертифікації повинен бути вирішений цілий ряд найбільш загальних завдань оцінки якості програмного забезпечення. По-перше, повинна бути встановлена повнота вихідних даних і параметрів, що описуються в технічній і супровідній документації. По-друге, необхідно забезпечити застосування стандартних (атестованих) методик випробувань або розробку спеціальних методик, що враховують особливості конкретного продукту. По-третє, завданням є також проведення випробувань та оцінки достовірності їх результатів. По-четверте, заключній завданням є узагальнення результатів випробувань і отримання остаточної оцінки показників якості програмного продукту.

Необхідність сертифікації програмного забезпечення визначає замовник та відображає це в договорі на поставку продукції. Ринкові відносини змушують використовувати механізм незалежної оцінки якості програмного забезпечення. У цьому випадку добровільна сертифікація може проводитися за заявкою розробника.

Особливо ефективна сертифікація для програм масового користування, що випускаються великими тиражами, тому що в цьому випадку різко знижуються витрати, викликані претензіями споживачів. Разом з тим результати сертифікації повинні окупати витрати на її проведення, тому перед проведенням сертифікації необхідна детальна економічна оцінка.

Методичні основи випробувань і сертифікації представляють собою систему науково обґрунтованих процедур, об'єднаних в єдиний технологічний процес, на кожному етапі якого розробляються документи, що відображають стан і якість випробуваного програмного продукту.

Технологічний процес випробувань та сертифікації підтримується, як правило, досить ефективними інструментальними пакетами для автоматизації випробувань та методиками оцінки якості. Випробування унікального програмного забезпечення для цілей сертифікації вимагають попередніх досліджень як в системній, так і в предметній областях, тому в таких випадках потрібно більш високий рівень формалізації та документального оформлення всіх умов і результатів, ніж при звичайних випробуваннях.

Програмні засоби навчального призначення. В даний час у сфері освіти накопичено значне число програмних засобів, широко застосовуються на всіх етапах навчання. У більшості випадків предметно-змістовна частина цих програм є досить ефективною. Крім того, відсутність єдиного підходу та єдиних вимог до системного оформлення навчального програмного забезпечення, розробленого в одному із ВУЗів, робить скрутним або неможливим його використання в інших навчальних закладах.

Сертифікація програмних засобів телекомунікації є в достатній мірі відокремленої завданням, найтіснішим чином пов'язаної з апаратною частиною. Початкові витрати на сертифікацію цих засобів повинні нести як розробник програмного забезпечення, так і його споживачі, тому витрати на випробування і сертифікацію повинні включатися в продажну вартість програмного забезпечення.

При створенні програмного продукту масового застосування, особливо вимагає тривалого супроводу, необхідно більш тісну взаємодію між розробником та органом із сертифікації. Можуть, зокрема, укладатися довгострокові угоди, які регламентують періодичні випробування і надання оперативної інформації про виявлені помилки або дефектах з урахуванням претензій користувачів. У процесі супроводу програмного продукту,

наприклад, при його модернізації, розробник може вносити зміни, які можуть спричинити за собою нові помилки. Тому необхідно безперервне відстеження органом з сертифікації змін в програмному забезпеченні інформаційних технологій.

Процедури сертифікації. Відповідно до вимог, процедура сертифікації програмних засобів інформаційних технологій у сфері освіти сьогодні включає ряд етапів «Процедури сертифікації інформаційно-програмних засобів навчального призначення».

Для досягнення якісних результатів сертифікації ПС необхідно організувати взаємодію всіх учасників цієї процедури: Центрального органу з сертифікації та/або органу з сертифікації, випробувальної лабораторії та розробника програмного забезпечення. Протягом усього терміну дії сертифіката два рази на рік орган з сертифікації повинен проводити інспекційний контроль якості сертифікованого програмного продукту.

Найбільш відповідальним етапом сертифікації є розробка технічних умов, тобто вимог до характеристик програмного продукту, на які видається сертифікат відповідності. Від того, як складені технічні умови, залежить «вагомість» сертифіката.

Відповідно до складених технічними умовами розробляються методики випробувань. Випробування програмної частини можуть включати специфічні тести. У кожному конкретному випадку набір тестованих характеристик може варіюватися, однак завжди існує мінімальна програма випробувань, що реалізується, як правило, системами автоматизованого тестування.

У загальному вигляді система автоматизованого тестування являє собою універсальний пакет програм, що передбачає тестування графічного інтерфейсу, системне тестування, тестування при максимальному навантаженні та інші. Засоби автоматизованого тестування додатків клієнт/сервер як найбільш популярних програмних засобів дозволяє випробувальним лабораторіям багаторазово використовувати сценарії тестування і тестові дані, вести моніторинг помилок, емулювати необхідне число користувачів на

робочих станціях. Слід, однак, враховувати, що створення систем автоматизованого тестування вимагає дуже високих витрат їх на розробку.

Вирішення проблеми інформатизації сфери освіти України не є самоціллю. Взаємопов'язані і взаємовпливають процеси реформування та інформатизації освіти здійснюються в ім'я досягнення Україною інших, більш високих цілей. Виходячи з цього заключний розділ Концепції присвячений саме співвіднесенню проблем освіти та її інформатизації з глобальними проблемами сьогодення і майбутнього України.

Сьогодні світовий інформаційний простір (кіберпростір - по західній термінології) стає ареною боротьби за національні інтереси. Якщо на початку історії людства основною ареною протистояння держав і народів була суша, а метою - захоплення території та населення, то пізніше протистояння було перенесено на морські простори, потім у глибини океанів, в повітряний простір і, нарешті, в космос (концепція «зоряних воєн »Р. Рейгана).

Однією з головних сфер суперництва в XXI столітті стане і вже реально стає інформаційний простір. Цілі цієї боротьби - зміна шкали цінностей і поведінкових стратегій, підвищення стійкості власне розвитку держав.

Іншими словами можна сказати, що в кінці XX століття народився новий вельми ефективний метод управління суспільством - інформаційне управління. Програш у цій важливій сфері безумовно відкидає країну на задвірки історії.

Кількість невирішених проблем у цьому плані досягло в України своєї критичної маси. Якщо ситуація не зміниться, то всі наші діяння і благі наміри щодо виходу з існуючої кризи безглузді.

Суспільство майбутнього ніколи, ні в найменшій мірі не може бути суспільством людей, лише натискаючих кнопки. Воно має і буде суспільством організованих, висококваліфікованих працівників. Людина завжди був і буде єдиним суб'єктом творчої діяльності.

Щоб це дійсно стало фактом, реальністю обов'язково необхідні знання, освіту. Сьогодні розвиток науки і техніки поставило перед освітою ряд складних проблем. У системі навчання все важче враховувати наукові

досягнення, бо вони швидко "старіють", змінюються іншими. За висновками експертів кваліфікований робітник повинен протягом свого трудового життя п'ять-шість разів освоювати нову техніку (так швидко застарівають набуті знання). Половина технічних знань інженера старіє кожні п'ять-сім років, а вісімдесят відсотків всіх знань, які будуть потрібні майбутнім фахівцям (сьогодні ще студентам) протягом їх трудової діяльності ще нікому невідомо.

Все це означає, що система освіти, що орієнтується на фахівця, що володіє фіксованою сумою якихось знань у певній галузі науки, не може відповідати сучасним вимогам.

Головне у підготовці майбутніх фахівців полягає не стільки в тому, щоб дати їм якусь суму знань, скільки в тому, щоб озброїти їх умінням самостійно засвоювати нові знання, безперервно вдосконалюватися, творчо підходити до вирішення нових проблем.

Звідси випливає основне завдання сучасної освіти - сприяти оволодінню методологією формування системи знань. І основний принцип правильного вирішення цього завдання - упор на самостійну роботу учня, студента. Учень з самого першого класу має бути не об'єктом, що сприймає нові знання, а свого роду дослідником в осягненні основ наукових знань. Школа повинна бути лабораторією, в яку учень приходить, щоб робити відкриття. Природно, що ці відкриття будуть не для всього людства, а для нього самого.

Робота з реалізації проблеми інформатизації освіти повинна бути спрямована в основному на вирішення управлінських, організаційних, методологічних та інформаційних питань. Основні проблеми розвитку та інформатизації освіти необхідно вирішувати одночасно і взаємопов'язано, чітко координуючи вказані напрями робіт між собою.

Прогнозування розвитку сфери освіти необхідно проводити шляхом моделювання майбутнього. Результати моделювання можуть бути резюмовано так:

- Необхідно розуміти, за рахунок чого розвивається суспільство, в іншому випадку можливі проблеми і труднощі і швидко наростаючі кризи.

Якщо керівництво України вважає за необхідне зберегти позиції країни (як держави) у світовому співтоваристві, то повинні бути вкладені додаткові кошти у сферу освіти і науки, а головне - необхідно використовувати на ділі можливості, що надаються інтелектуальної сферою.

- Для подолання кризових ситуацій інтелектуальну сферу необхідно розвивати, використовуючи її як ресурс подальшого розвитку країни. Якщо цей ресурс не використовується, можливо тільки екстенсивний розвиток суспільства або його деградація.
- Існує пороговий рівень розвитку інтелектуальної сфери, нижче якого вона швидко втрачає здатність грати роль ресурсу розвитку суспільства. Експертні оцінки показують, що для України в нинішніх умовах цей рівень знаходиться вище 5% бюджету країни.

Сьогодні вважається загальновизнаним, що освіті відводиться вирішальна роль у відродженні та підтримку нової України, і що намічені реформи торкнуться питань освітньої політики, управління, змісту, оцінки, професійної освіти та підготовки, питання викладацького корпусу і т.п.

Необхідно виробити ієрархію пріоритетів щодо їх реалізації, виходячи з історичного і сьогоднішнього досвіду. При проведенні змін такого роду необхідно пам'ятати, що термінові, прилеглі й довгострокові цілі треба розглядати як невід'ємні частини широко спланованого процесу. Побудова нового освітнього майбутнього є тривалим процесом. Розробники цієї Концепції сподіваються, що багато рекомендації, положення та принципи, висловлені вище, виявляться корисними на всіх етапах цього шляху.

Дана заключна глава Концепції має на меті залучення особливої уваги до ряду насущних і ключових напрямків розвитку та інформатизації освіти. Деякі з них допоможуть посилити поточні реформи, інші - привернути увагу до окремих проблем і вказати нові шляхи їх вирішення. Необхідно прийняти практичні кроки по наростаючій, а не всеосяжного зміни сфери освіти. Настав час змістити акцент освітньої політики від задоволення потреб

виробників (навчальних закладів та шкіл) до задоволення потреб дітей, молоді, студентів, дорослих учнів і окремих груп населення країни.

Для досягнення суспільної мети освітня політика повинна віддавати перевагу спонукальним стимулам і ринковим механізмам, а не "декретів" і "указам". З метою стимулювання механізмів забезпечення реформи необхідно підкреслити роль недержавних організацій, об'єднань і асоціацій.

У той час, як Україна прагне привести свою систему освіти у відповідність з новими цілями, необхідно виробити більш скоординований і зв'язне визначення принципів і цінностей, що лежать в основі цієї нової політики. У ньому слід приділити велику увагу завданням освіти дорослих, випереджаючого та безперервної освіти, ролі та структурі вищої освіти, а також формам взаємозв'язку між системою освіти та її соціальними партнерами.

Посилення ролі індивідуального розвитку і самореалізації має бути урівноважене залученням уваги до цілей співробітництва, взаємодопомоги і групової роботи. Освіта повинна відігравати основну роль у створенні нової громадянської культури для демократичного суспільства, для цього доцільно залучати міжнародну допомогу і співпрацю.

Необхідно розробити і впровадити у життя процедури розпізнавання і зняття бар'єрів, що перешкоджають рівному доступу до освіти і успішністю учнів, що заважають їм у максимальній мірі розкрити свої здібності в реальних рамках наявних людських фінансових ресурсів.

Необхідно забезпечити стійкість процесів децентралізації. Слід внести більшу ясність у систему делегування прав і повноважень учасникам процесу управління. Необхідно також розширити практику укладання угод між Міносвіти України і суб'єктами і забезпечити умови для співпраці в їх рамках.

Необхідно приділяти особливу увагу створенню вітчизняної інформаційної бази з освітнім та навчальним системам як в горизонтальному, так і у вертикальному вимірі, щоб забезпечити зворотний зв'язок за напрямками, досягненням і проблемам в галузі освітньої політики.

Для забезпечення прозорості процесу розподілу та використання фінансових коштів доцільно провести реформу системи фінансування сфери освіти.

Центральна ідея реалізації цієї Концепції дуже проста. Ось вона:

Біологи назвали сучасної людини - Homo Sapiens-людина розумна, маючи на увазі його здатність забезпечити перевагу і стійке зростання свого виду. Зростаючу могутність, можливість швидко реалізувати плани, бажання, мрії планетарного масштабу дозволяють стверджувати, що виникає новий вид людини - Homo Ludenus - людина грає, що розвивається. Цей людина здатна змінювати світ у відповідності зі своєю віртуальною реальністю. Віртуальних реальностей існує багато, а значить і альтернатив на нинішньому рівні розвитку біосфери і техносфери є декілька. Наша віртуальна реальність стає фактором планетарного масштабу. Її вдосконалення є одним з головних ресурсів розвитку та джерелом найбільш серйозних ризиків і загроз. Людству кинутий історичний виклик. Країни, регіони, цивілізації, які не зможуть прийняти його, не мають майбутнього.

Україна багата своїми людьми. Значить є у такої країни можливість зробити багатство знань загальнонаціональним надбанням.

2 ФОРМУВАННЯ ВИМОГ ДО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, ЩО ВИКОРИСТОВУЄТЬСЯ ПРИ РЕАЛІЗАЦІЇ СУЧАСНИХ ПЕДАГОГІЧНИХ ТЕХНОЛОГІЙ ПРИ ПІДГОТОВЦІ ФАХІВЦІВ

2.1 Дотримання практики захисту інформації

Інноваційні процеси передбачають не тільки використання наукової,педагогічної та комерційної інформації, але й подальшу її обробку та конфіденційність. Тому правомірно протиставити два взаємовиключних чинники:

– чи повинні одні й ті ж заходи охорони конфіденційності інформації, що визначаються режимом комерційної таємниці, застосовуватись весь період, коли вони використовуються в управлінських або технологічних процесах;

– заходи повинні застосовуватися адекватно динаміці комерційної цінності інформації і тільки на період від появи до втрати цієї комерційної цінності, потенційної або дійсної.

Актуальність заходів означає їх модифікацію в залежності від особливостей поточного етапу інноваційних процесу, яка забезпечить реальну можливість запобігання несанкціонованого доступу до інформації, що має комерційну цінність. Значення принципу актуальності заходів з охорони випливає з тлумачення положень закону «Про комерційну таємницю» (КТ), згідно з яким право власника інформації, що складає КТ, виникає з моменту встановлення власником інформації стосовно режиму КТ. Для закріплення своїх прав, у відповідності з законом, володар інформації:

– визначає склад і перелік такої інформації (інформація про споживання електроенергії та фінансових розрахунках);

– визначає заходи з охорони конфіденційності інформації у формі режиму КТ (розмежування доступу).

Для адміністрування режиму КТ можливі актуальні заходи охорони конфіденційності:

– застосувати до інформації максимальний режим КТ;

– оцінити можливість охорони конфіденційності з використанням патенту, ліцензії, авторського права і т.ін.;

– зберігати рівень контролю над розповсюдженням і дотриманням заходів щодо захисту інформації в організації.

Використання підвищення режиму КТ випливає із закону «Про комерційну таємницю», що дозволяє власникові при необхідності поряд з заходами режиму КТ застосовувати засоби і методи технічного захисту конфіденційності, вважати прийнятною достатність заходів з охорони конфіденційності, ґрунтуючись на власній оцінці можливості доступу до інформації.

2.2 Аналіз та класифікація загроз

Для визначення методики розробки моделі загроз для захисту інформації з обмеженим доступом під час дистанційного управління технологічними, освітніми процесами по радіоканалу необхідно провести всебічний аналіз можливих загроз збереженню цілісності інформації. Цінність інформації, яка циркулює в системі дистанційного моніторингу складається з чотирьох складових: конфіденційність, цілісність, доступність, стійкість до помилок. Аналіз та класифікація загроз у приватних бездротових автоматизованих системах полягає в наступному – інформаційна система, яка аналізується, може розглядатися як взаємодія трьох компонентів: джерела інформації (лічильники), приймача інформації (модем-координатор) і середовища передачі інформації (Інтернет). Тому система захисту повинна

виконувати захист всіх компонентів. Завдання захисту інформації в мережі зводиться до захисту інформації кожного її компонента.

Під інформаційними загрозами розуміються шляхи реалізації впливів, які вважаються небезпечними. Наприклад, загроза знімання інформації й перехоплення випромінювання з модуля лічильника веде до втрати конфіденційності, загроза пожежі або механічного пошкодження веде до порушення цілісності інформації, а загроза розриву зв'язку може реалізувати небезпеку для доступності інформації. Загроза збою електропостачання може привести до небезпеки появи помилок в системі керування системи на верхньому рівні. Виходячи з цього аналіз небезпеки повинен показати де, коли і у якому місці системи інформація може втратити цінність. На об’єкті дослідження циркулює інформація що до освітніх та наукових процесів побутових.

2.2.1 Критерії класифікації загроз

Діяльність по забезпеченню інформаційної безпеки спрямована на те, щоб не допустити збитків від втрати конфіденційної інформації. Тож, до критерію класифікації загроз можна віднести:

- об'єкт загрози;
- фактор виникнення загрози;
- джерело виникнення загрози.

Об'єктом загрози може бути будь-який елемент, який входить до складу автоматизованої системи, а саме: пристрої збору даних, які формують сітку ZigBee за об’єктом; модем-координатор, який забезпечує зв’язок між ZigBee - середовищем та центральним сервером, системи за каналом GPRS; сервер системи, який забезпечує Веб-сервіси, сервер Бази даних (БД).

Фактором загрози можуть бути апаратні та програмні засоби автоматизованої системи. Джерелом виникнення загрози може бути людський фактор, який формується незгодою споживача с даними дистанційного

моніторингу його енергоспоживання, та технічний фактор, обумовлений незадовільним станом існуючих електричних мереж.

Усі джерела загроз зазвичай розподіляються на антропогенні, техногенні, стихійні. [1] Враховуючи малоймовірність стихійних факторів та їх вплив на цілісність інформації, цей фактор можливо не враховувати. Техногенні фактори також не мають критичного значення для системи в цілому. Це обумовлено тим, що пошкодження окремого модуля ПЗПД, або елемента системи інформаційного простору, не може привести до пошкодження усього масиву даних. Загубленою може бути інформація лише окремого користувача, а не об'єкту взагалі. Вихід з ладу модему-координатору також не приведе до пошкодження даних, тому що інформація зберігається не тільки в енергонезалежній пам'яті модему, а і в модулі ПЗПД також. Дані з модуля можуть бути зчитані локально за допомогою адаптера «USB-ZigBee». Тому основним фактором загроз є антропогенний.

Антропогенними джерелами загроз безпеки інформації є суб'єкти, дії яких можуть бути кваліфіковані як випадкові (ненавмисні) або навмисні злочини. Ненавмисні, або випадкові, дії в системі «Energy Web-XB» неможливі після вводу системи в дослідну або промислову експлуатацію, тому що система працює в автоматичному режимі.

Для бездротових мереж автоматизованих систем контролю і управління процесами надання послуг користувачам , визначені такі типи загроз [1]:

- загроза конфіденційності (К) – несанкціонований доступ до інформації;
- загроза цілісності (Ц) – несанкціонована модифікація інформації;
- загроза доступності (Д) – порушення можливості доступу абонентів і адміністраторів системи до інформації;
- загроза спостереженості (С) – порушення керованості системи.

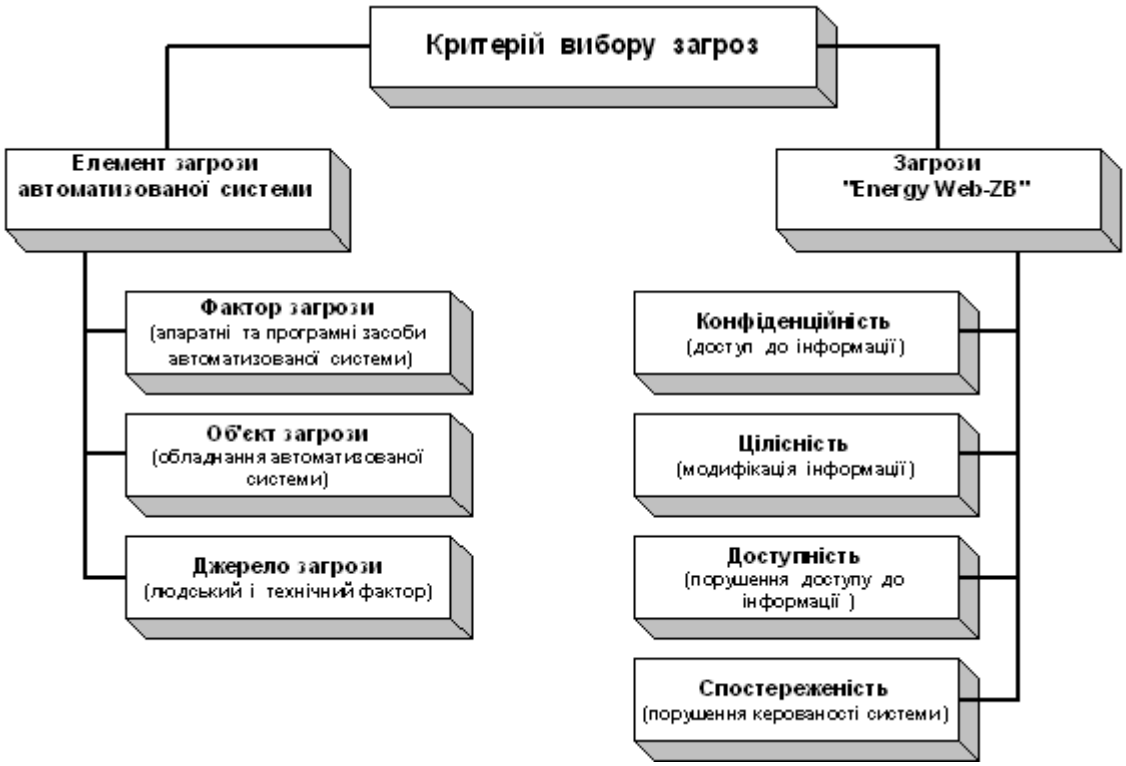


Рисунок 2.1 – Класифікатор критеріїв загроз

2.2.2 Класифікація загроз

Для безпеки інформації, що обробляється в бездротових автоматизованих системах збору даних («Energy Web-ZB»), визначені такі потенційні види загроз:

– збої в роботі програмних засобів;

– порушення технології збору, передачі даних та режиму обробки інформації;

– порушення фізичної цілісності;

– застосування комп'ютерних вірусів;

– наведень побічних електромагнітних випромінювань на пристрої збору і передачі даних.

Визначені загрози можуть призвести до порушення цінності інформації. Тому для унеможливлення дії цих загроз слід виділити об'єктивні та суб'єктивні фактори і розробити політику інформаційної безпеки компанії. Для цього слід мати на увазі, що реалізація загроз в системі можлива за допомогою:

– технічних каналів, що включають канали ZigBee сітки та GPRS/GSM мережі;

– підключення до технічних засобів (модем-координатор, сервер БД, сервер Веб-сервіс);

– застосування комп‘ютерних вірусів;

– подолання захисту за допомогою каналів спеціального впливу з метою руйнування системи збору/ передачі даних або порушення цілісності інформації.

2.2.3 Побудова моделі загроз для інформації з обмеженим доступом у бездротових автоматизованих системах збору даних

Метою побудови моделі загроз є визначення суттєвих загроз для інформації в автоматизованій системі обробки, передачі, аналізу та збереження інформації. Основними завданнями при побудові моделі загроз є:

– аналіз умов функціонування АС;

– визначення потенційних загроз для ІзОД в АС, їх аналіз та оцінка;

– визначення суттєвих загроз для ІзОД в АС.

Створення моделі загроз повинен базуватись на наступних законодавчих і нормативних документах:

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» (від 05.07.1994 №80/94-ВР, в редакції Закону від 31.05.2005 №2594-IV);

– РД 50-34.698-90 «Методичні вказівки. Інформаційна технологія. Комплекс стандартів і керівних документів на автоматизовані системи. Вимоги до змісту документів»;

– ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення» (затверджений наказом Держстандарту України від 11.10.1996 №423, чинний від 01.01.1997);

– ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт» (затверджений наказом Держстандарту України від 19.12.1996 №511, чинний від 01.07.1997);

– НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі» (затверджений наказом ДСТСЗІ СБ України від 08.11.2005 №125);

– НД ТЗІ 1.6-003-04 «Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації»;

– НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» (затверджений наказом ДСТСЗІ СБ України від 28.04.1999 №22, чинний від 01.07.1999);

– НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту в автоматизованій системі» (затверджений наказом ДСТСЗІ СБ України від 04.12.2000 №53, чинний від 15.12.2000);

– НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» (затверджений наказом ДСТСЗІ СБ України від 28.04.1999 №22, чинний від 01.07.1999);

– НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» (затверджений наказом ДСТСЗІ СБ України від 28.04.1999 №22, чинний від 01.07.1999);

– «Тимчасове положення про категоріювання об'єктів (ТПКО-95)» (затверджене наказом Державного комітету країни з питань державних секретів та технічного захисту інформації від 10.07.1995 №35, чинне від 01.08.1995);

– «Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітним випромінювань і наводок (ТР ЕОТ-95)» (затверджені наказом ДСТЗІ від 09.06.1995 №25, чинні від 01.07.1995);

– «Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ТЗІ-ПЕМВН-95)» (затверджені наказом ДСТЗІ від 09.06.1995 №25, чинні від 01.07.1995).

Побудова моделі загроз для інформаційних ресурсів є одним із головних етапів створення систем захисту і складається з опису сукупності суттєвих загроз для інформаційних ресурсів, способів та засобів їх здійснення в конкретних умовах застосування автоматизованої системи.

Схема інформаційних потоків, що циркулюють в об’єкті, може бути відображена наступною схемою:

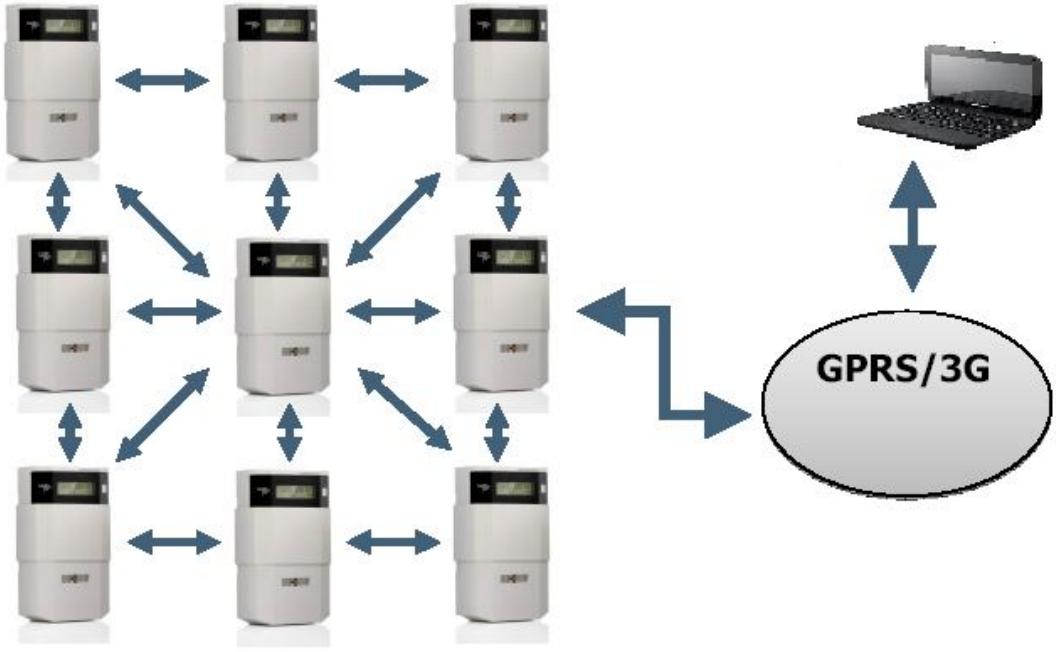


Рисунок 2.4 - Схема інформаційних потоків в середовищі ZigBee

Кожен елемент інформаційного середоваща, обладнаний ZigBee-пристроєм збору/передачі даних, входить в окремий кластер (об’єднання), у

якому зв'язки встановлюються між кожним лічильником групи. Згідно зі специфікацією ZigBee в автоматизованій системі дистанційного збору даних і управління енергоспоживанням використовується архітектура сітки, що побудована координатором та великим числом роутерів (маршрутизаторів). Програмування ПЗПД виконувалось під час монтажу і інсталяції системи на об'єкті. Кожному ПЗПД було призначено свій ідентифікаційний номер, за яким здійснюється доступ по мережі. Ця архітектура системи, що побудована за термінологією стандарту IEEE 802.15.4 без маяків (non-beacon enabled), дозволяє асинхронну роботу, і маршрутизатори (роутери) постійно прослуховують ефір на наявність завдань для виконання. В цьому випадку координатор постійно підтримує встановлену під час формування адресацію, та придатність системи до роботи. Згідно з цим алгоритмом найбільш вразливим є ланка мережі, що контролюється координатором. Проникнення зловмисника до даних системи можливо застосуванням паралельного координатора з перед встановленим діапазоном адрес та атрибутами модулів ПЗПД. Тому серед перших кроків що до захисту інформації на об'єкті є захист ідентифікаційних даних встановлених під час параметризації, а саме:

- код мережі;
- діапазон адрес сітки;
- коди абонентів;
- номер GSM-оператора для даного об'єкту.

На рисунку 2.5 зображена схема побудови системи дистанційного збору даних про режими роботи (параметри енергоспоживання, інші технологічні параметри). На ній зображені існуючі ПЗПД, модем-координатор та зв'язки між ними в мережі ZigBee.

Згідно цієї схеми другим етапом побудови системи інформаційної безпеки є впровадження технології захисту GSM/GPRS з'єднання модему «Сігма GSM-ZigBee» з сервером АС «Energy Web-ZB». GPRS (General Packet Radio Service) - послуга пакетної передачі даних по радіоканалу була

розроблена для можливості роботи в мережі Інтернет [5]. Загальний вигляд системи GPRS зображен на рисунку 2.6.

До GPRS- мережі входить 4 компонента:

- **мобильна станція** (Mobile Station, MS);
- **базова станція** (Base Station System, BSS);
- **вузол обслуговування абонентів** (Serving GPRS Support Node, SGSN);
- **вузол маршрутизації GPRS** (Gateway GPRS Support Node, GGSN).

Також до складу GPRS-мережі входить 3 типу реєстрів:

- **реєстр власних абонентів мережі** (Home Location Register, HLR);
- **реєстр переміщень** (Visitor Location Register, VLR)**;**
- **реєстр ідентифікаційних даних обладнання** (Equipment Identity Register, EIR).

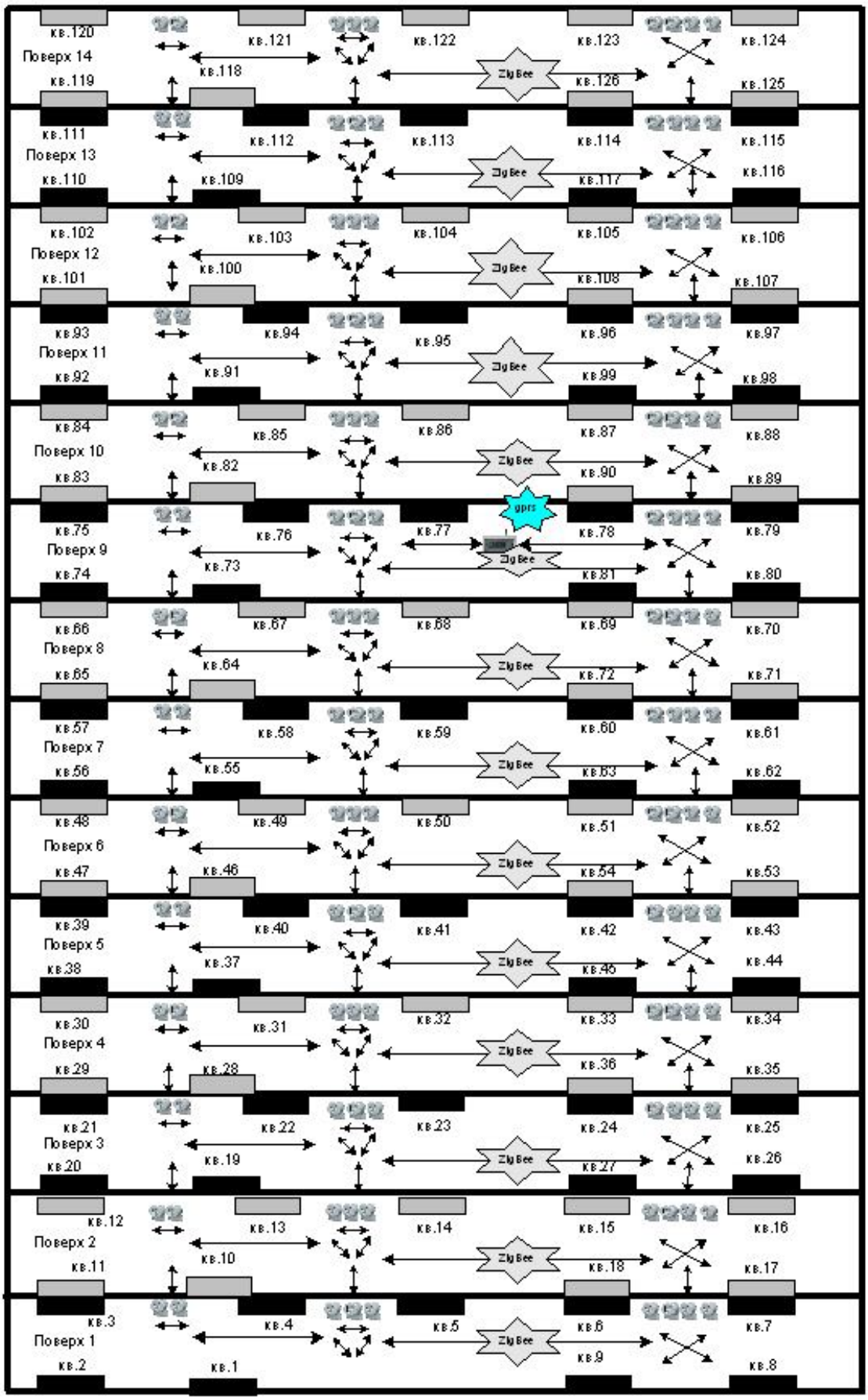


Рисунок 2.5 - Схема побудови системи

Вузол обслуговування абонентів GPRS SGSN - один з найважливіших елементів GPRS-мережі. SGSN за допомогою баз даних, які зберігаються в реєстрах HLR, VLR і EIR, забезпечують підключення абонентів до мережі; захист GPRS від таких атак, як несанкціоноване підключення до мережі.

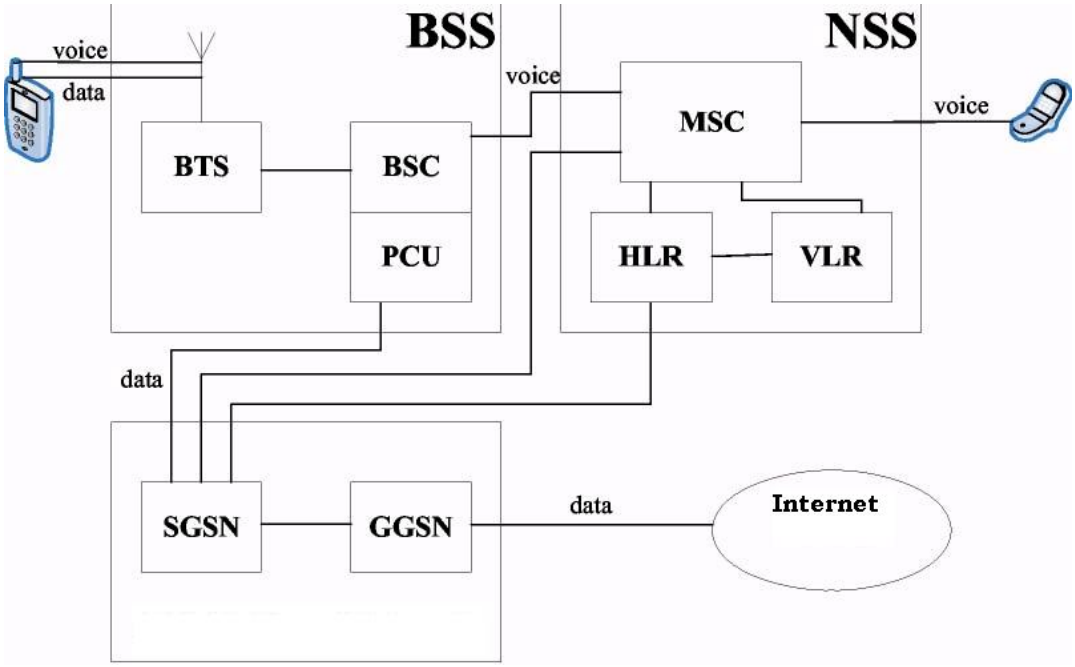


Рисунок 2.6 - Архітектура GPRS-мережі.

GGSN також як і SGSN є найважливішим елементом GPRS - мережі, як з точки зору функціонування мережі, так із точки зору забезпечення безпеки цього функціонування. З точки зору забезпечення функціонування мережі GPRS GGSN виконує такі важливі функції, як приймання та передача даних з зовнішніх мереж , призначення IP - адрес і таке інше. З точки зору забезпечення захисту інформації мережі GPRS, GGSN захищає мережу від зовнішніх загроз (атак) з Інтернету, або GPRS - мережі іншого оператора стільникового зв’язку.

У мережі GPRS, що використовується в даному випадку, рівні безпеки складаються з наступних складових:

- Безпеки MS;
- Безпеки каналу зв'язку MS і SGSN;
- Безпека передачі даних між SGSN і GGSN;
- Безпека передачі даних у відкритій мережі Інтернет.

Безпека MS забезпечується SIM-карткою (Subscriber Identity Module) та власно терміналом. SIM-картка має IMSI (International Mobile Subscriber Identity) ідентифікатор абонента, який включає тризначний код країни (для України – 380), двузнаковий код оператора (Київстар – 67), код абонента MSIN (Mobile Subscriber Identity Number), що має 10 розрядів. Власний індивідуальний ключ Ki зберігається в HLR і VLR. SIM-картка захищена 4-розрядним PIN-кодом (Personal Identification Number). Безпека термінала забезпечується 14-розрядним міжнародним ідентифікатором приладів стільникового зв'язку (IMEI, International Mobile Equipment Identity), який зберігається в регистрі EIR, що повністю відповідає вимогам безпеки бездротових персональних мереж контролю енергоспоживання.

Безпека з'єднання MS з вузлом SGSN забезпечується аутентифікацією абонента на рівні MSIN та аутентифікацією обладнання на рівні IMEI. Безпека передачі даних між MS і SGSN забезпечується алгоритмом шифрування A5, що використовує ключ Kc (64 біт), який генерується алгоритмом A8.

Безпека з'єднання між вузлами SGSN і GGSN забезпечується використанням протоколу GTP (GPRS Tunneling Protocol), який вбирає в себе протоколи користувача, наприклад, HTTP, FTP і т.ін.

Для зменшення можливості проникнення зловмисника з зовнішніх загальних мереж (наприклад, Інтернет), опорна мережа побудована на основі приватних (локальних) IP-адрес. Ще однією технологією захисту є використання шлюзів (Border Gateway), які виконують роль між мережевого екрану (Firewall). Під час роботи в мережі Інтернет вузол GGSN виконує основний захист. На рівні серверу системи захист забезпечується за допомогою Firewall. Для підвищення захищеності системи дистанційного збору даних про енергоспоживання і управляння станом підключення побутових абонентів необхідно використати технологію трансляції адрес (network address translation).

2.3 Визначення та оцінка загроз

Технічний захист інформації з обмеженим доступом в автоматизованих системах і засобах обчислювальної техніки, призначених для формування, пересилання, приймання, перетворення, відображення та зберігання інформації, забезпечується комплексом конструкторських, організаційних, програмних і технічних заходів на всіх етапах їх створення й експлуатації. Основними методами та засобами технічного захисту інформації з обмеженим доступом в автоматизованих системах і засобах обчислювальної техніки є:

- використання захищених засобів;
- регламентування роботи користувачів, технічного персоналу, програмних засобів, елементів баз даних і носіїв інформації з обмеженим доступом (розмежування доступу);
- регламентування архітектури автоматизованих систем і засобів обчислювальної техніки;
- інженерно-технічне оснащення споруд і комунікацій, призначених для експлуатації автоматизованих систем і засобів обчислювальної техніки; пошук, виявлення і блокування закладних пристроїв. [13].

Визначення загроз для ІзОД в АС проводилось за різними критеріями: джерелом виникнення, способом здійснення (технічними каналами, несанкціонованим доступом); результатами впливу на властивості АС (цілісності, доступності, спостереженості) [16].

Схематичний вигляд системи зображено на рисунку 2.7.

При розгляді антропогенних загроз розроблена модель порушника, яка визначає [18]:

- мету порушника та ступінь її небезпечності для інформації;
- категорії осіб, з числа яких може бути порушник;
- припущення щодо кваліфікації порушника;
- припущення щодо характеру його дій.

Порушник за нашим уявленням є кваліфікований спеціаліст (можливо бувший співробітник компанії) знайомий з технологією ZigBee, який має знання щодо програмування ПЗПД і модемів. Крім того порушник може мати досвід управління системою по Інтернету.[17]

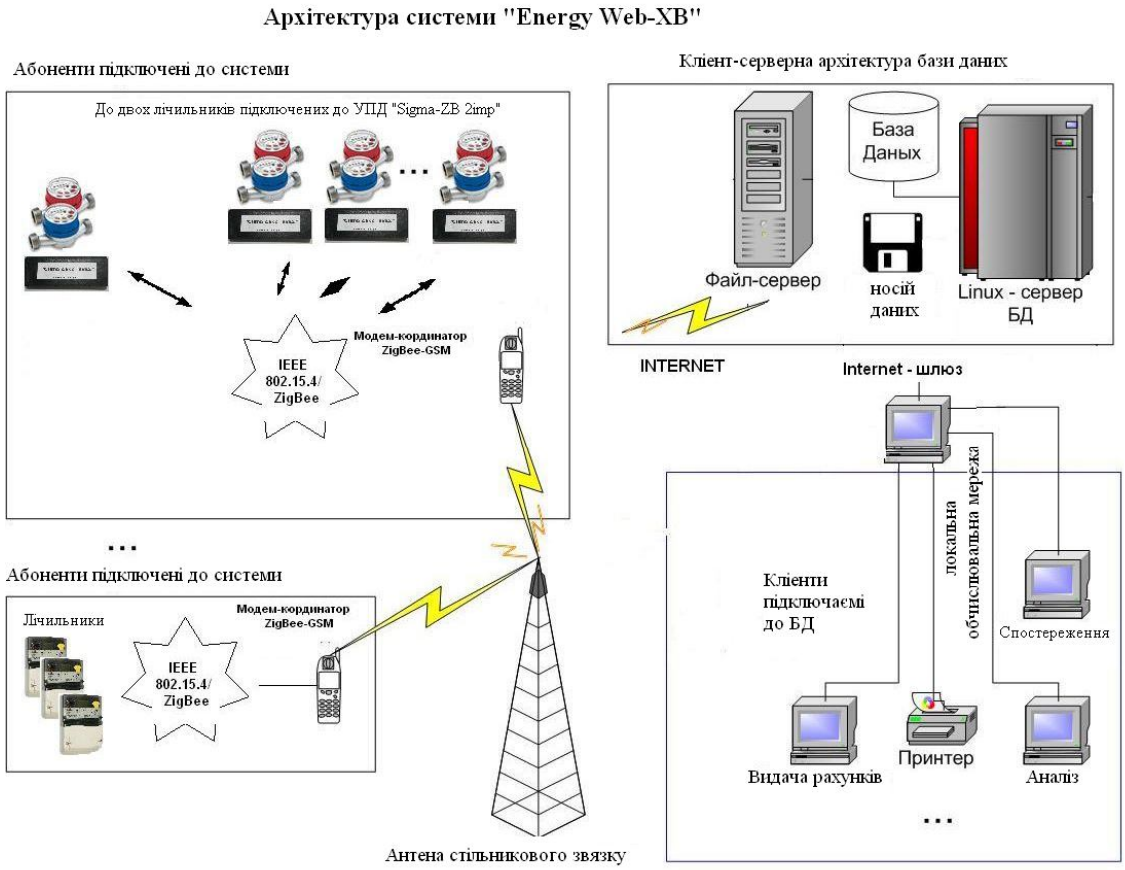


Рисунок 2.7 - Схема системи

Найбільшу небезпеку представляє кваліфікований порушник, який хоче отримати доступ до окремих модулів ПЗПД або модемів з метою трансформації даних. Крім того серед можливого сценарію нападу по мережі Інтернет, є вживання комп'ютерних вірусів або шпигунських програм з метою доступу до бази даних серверу системи. Тому під час побудови системи захисту інформації необхідно вжити як технічні, так і програмні та організаційні заходи щодо побудови ефективної комплексної системи захисту.

Організаційні заходи включають в себе розробку прав доступу до серверу баз даних для різних користувачів. Для доступу до серверу необхідно розділити право на доступ до інформації про енергоспоживання для ознайомлення, доступ для прав корекції показників щодо визначення абонентів, доступ до прав управління станом енергоспоживання (підключення/відключення). Розділення прав виконується шляхом призначення різних паролів та логинів користувачів. Найбільш важливим, з точки зору захисту, є доступ до прав управління. Тому в цьому разі існує необхідність дублювання процедури захисту за допомогою різних паролів кожної операції ідентифікації. Технічні заходи щодо побудови системи безпеки складаються з унеможливлення доступу до модему-координатору по мережі Інтернет з сторонніх місць а також зміна параметрів ПЗПД окремих активних елементів інформаційного простору. Для цього використана наступна процедура встановлення підключення між сервером та модемом. Під час параметризації модему задається фіксована IP-адреса серверу системи. Модем в автоматичному режимі по каналу GPRS звертається до серверу для отримання завдання на виконання. У разі відсутності такого модем відключається від мережі. Наступного разу під час звернення йому надається вже нова IP-адреса, тобто модем має динамічно змінну адресу, що унеможливлює втручання в роботу системи порушникам по мережі Інтернет. Захист ПЗПД здійснюється шляхом використання захищеного ZigBee - з'єднання, конфіденційного PAN***(Personal Area Network)*** ідентифікатора, якому належать модулі XBee, фірмового протоколу SCTM. Захист серверу системи від атак по Інтернет виконується шляхом встановлення мережевого екрану та розділення серверу Інтернет і серверу БД. Для унеможливлення дистанційного втручання в роботу системи та окремих її модулів необхідно заборонити несанкціонований GSM-доступ до модему. Для цього необхідно активацію GSM здійснювати з серверу по каналу GPRS.

Крім того для безпеки системи важливим засобом є протидія протиправним намаганням співробітників, невдоволених діями адміністрації володаря системи. У цьому випадку необхідно виконувати шифрування існуючих паролів, та забезпечувати їх заміну за таблицею шифрів, яка розробляється службою безпеки і зберігається в адміністратора системи. Тому можливо припустити, що динамічна зміна паролів доступу, які призначаються кодованим шифруванням, є найбільш ефективною системою захисту від протиправних посягань зловмисника.

3 АНАЛІЗ ІСНУЮЧИХ МЕТОДИК ВИКОРИСТАННЯ ЗАСОБІВ ВІДДАЛЕНОГО ДОСТУПУ Й КОНТРОЛЮ У ПРАКТИЦІ ПІДГОТОВКИ ФАХІВЦІВ

3.1 Побудова політики безпеки в персональних бездротових мережах дистанційного моніторингу

Основним питанням під час побудови бездротових мереж дистанційного моніторингу забезпечення необхідного рівня безпеки інформації, що передається каналами радіозв'язку. Це досягається за допомогою двох шляхів - технічними і організаційними засобами.

Серед технічних засобів маємо відокремити наступні [6]:

- Зменшити зону радіо покриття до зони окремої будівлі;
- Увести фільтрацію за MAC-адресами;
- Періодично змінювати ідентифікатор мережі (PAN ID).

Активувати функції AES-128 шифрування;

- Активувати фільтрацію трафіка на між мережевому екрані;
- Забезпечити активацію GSM-доступу по захищеному каналу GPRS;
- Встановити сервер контролю доступу з посиленою аутентифікацією абонентів-користувачів бездротової мережі.

Згідно стандарту 802.1x взаємодія клієнту мережі з сервером доступу здійснюється за схемою, зображеною на рисунку 3.1.

У системі «Energy Web-XB» реалізовано Internet Authentication Service (IAS). На стороні сітки ZigBee використано алгоритм AES (Advanced Encryption Standart - криптографічний протокол Rijndael) шифрування з 128-бітовим ключем, що є оптимальним з точки зору безпеки і навантаження на сервер.

Наступним рівнем є управлінський або адміністративний. Головне, що повинен забезпечити управлінський рівень,- це розробити політику забезпечення інформаційної безпеки на підприємстві по впровадженню і

експлуатації бездротових персональних мереж, побудованих по технології ZigBee.

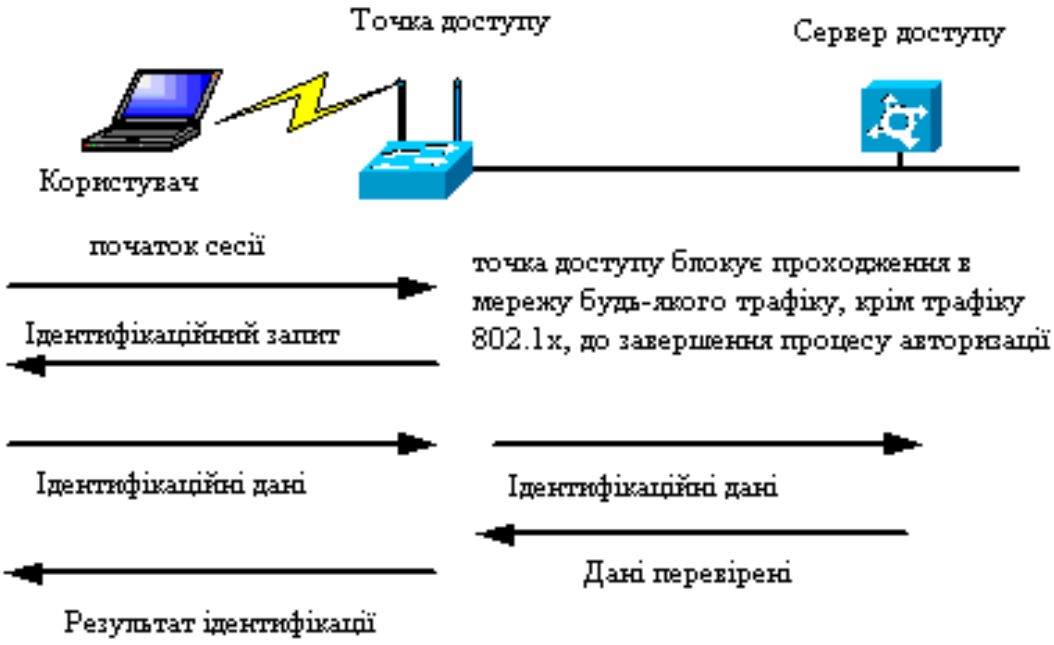


Рисунок 3.1 - Схема авторизації користувача в бездротовій мережі

Стосовно персоналу, що працює з інформаційними системами, використовуються організаційні і програмно-технічні засоби забезпечення інформаційної безпеки. До них відносяться [7]:

- Підбір персоналу;
- Його навчання;
- Забезпечення дисципліни;
- Засоби захисту «від дурня».

Важливим елементом також є засоби фізичного захисту поверхових розподільчих щитків та мережевого обладнання. Для підтримки режиму інформаційної безпеки насамперед найбільш важливими є програмно-технічні засоби, тому що збої обладнання, помилки програмного забезпечення, помилки користувачів несуть основну загрозу в інформаційних системах. Тому слід зазначити ключові механізми інформаційної безпеки [15]:

1. Ідентифікація і аутентифікація;
2. Управління доступом;
3. Аудит і протоколювання;
4. Криптографія;
5. Екранування.

На першому місті стоїть задача забезпечення конфіденційності і захисту від несанкціонованого доступу. Вона досягається шляхом виконання вказаних вище програмно-технічних і адміністративних заходів. Але, як вказано в «Помаранчевій книзі» [8], найбільшої шкоди задають некваліфіковані дії користувачів і адміністраторів, що обслуговують інформаційну систему. Іноді такі помилки стають загрозами: похибки в програмах, невірно введені дані, помилки в адмініструванні системи. Всі ці дії приводять до значних матеріальних втрат. Тому найбільш радикальним засобом боротьби з непрофесійними діями персоналу, що експлуатує автоматизовану систему, є, по можливості, її максимальна автоматизація та дійсний контроль за коректністю введення даних і експлуатацією системи.

Це є свідоцтвом того, що внутрішня загроза найбільш небезпечна у порівнянні з іншими загрозами. Велику небезпеку представляють «невдоволені» або «скривджені» співробітники. Як ті що працюють, так і ті що звільнені. У своїх діях вони керуються почуттям помсти організації-кривднику і можуть пошкодити обладнання, вмонтувати логічну «бомбу» в програмне забезпечення або базу даних, пошкодити БД і т.ін. Тому необхідно слідкувати за тим, щоб під час звільнення подібних співробітників були анульовані усі їх права доступу до критичних інформаційних ресурсів компанії. Особливу увагу слід звернути на комп’ютерні віруси. Тому правила комп’ютерної гігієни повинні впроваджуватись і контролюватись на кожному робочому місці, з якого здійснюється доступ до комп'ютерної мережі компанії.

3.1.1 Ідентифікація і аутентифікація

Ідентифікація і аутентифікація є основними програмно-технічними засобами безпеки, і виконують роль першої лінії захисту інформаційного простору фірми. Згідно [1] Ідентифікація (identification) — процедура присвоєння ідентифікатора об'єкту КС або встановлення відповідності між об'єктом і його ідентифікатором; впізнання. Аутентифікація (authentication) — процедура перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності.

Ідентифікація дозволяє користувачу зареєструватись в системі, а аутентифікація дозволяє системі підтвердити права доступу даного користувача.

Користувач має можливість підтвердити свої права наступними діями: ввести власний логін і пароль.

Головною перевагою парольної аутентифікації є її простота і приємність. Паролі використовуються в операційних системах і інших сервісах. Тому за виконання правил їх використування, вони забезпечують задовільний рівень захисту і безпеки. Слабкою стороною парольного захисту є можливість електронного перехвату. Це найбільш принципова вада цього методу, яку неможливо компенсувати навчанням персоналу або простим адмініструванням. Тому єдиний вихід з цієї ситуації – впровадження криптографічного захисту для шифрування паролів завчасно до передачі каналами зв'язку. Надійність парольного захисту системи «Energy Web-XB» забезпечена:

1. Технічними обмеженнями на кількість знаків і спроб вводу;
2. Періодична заміна паролів;
3. Обмеження доступу до файлу паролів;
4. Навчання і виховання користувачів;
5. Використання програмного генератору паролів.

Технічні обмеження полягають у встановлені спроб вводу «логіна користувача» та його паролю трьома спробами, а також в обмеженні (8 знаків) довжини парольного коду. Заміна паролів здійснюється щомісяця адміністратором системи. Пароль назначається директором за допомогою конфіденційної програми генератору паролів, що зберігається на твердому носії в сейфі компанії. Розроблена матриця заміни програмного коду генератора паролів, яка зберігається у керівництва компанії і тим самим унеможливлює несанкціоноване використання файлу паролів фірми. Ці заходи підвищують інформаційну безпеку і значно зменшують вплив людського фактору на безпечну і сталу роботу системи.

3.1.2 Управління доступом

Засоби управління доступом дозволяють контролювати діяльність користувачів під час роботи з системою. Мається на увазі логічне управління, що реалізовано на програмному рівні. Логічне управління - це головний механізм для систем з багатьма користувачами, який забезпечує конфіденційність і цілісність інформації, шляхом заборони доступу не авторизованим користувачам. В нашому випадку кожен користувач має свої, виключно обмежені права доступу для читання тільки до інформації, що призначена виключно їм. Права управління доступні тільки одному користувачу, визначеному керівництвом компанії власника системи. Задача логічного управління доступом полягає в тому, щоб для кожної пари (суб’єкт, об’єкт) визначити кількість можливих дій, які обмежені деякими умовами, і контролювати ці дії у встановленому порядку. Контроль прав доступу виконується різними компонентами програмного середовища, які не дозволяють користувачу уникнути відповідальності за можливі порушення правил користування і експлуатації системи.

3.1.3 Аудит і протоколювання

Протоколювання - це фіксування всіх подій, що трапляються в інформаційній системі під час її спостереження. Під час протоколювання визначаються користувач і фіксуються всі дії вчинені ним що до інформаційних ресурсів. Після протоколювання необхідно провести аудит, під час якого оперативно, або за розкладом, вивчити поведінку користувачів під час їх роботи з системою [9]. Проведення протоколювання і аудиту ставить за мету:

- Забезпечити прозорість дій користувачів і адміністратора під час роботи з системою;
- Забезпечення можливості реконструкції послідовності дій користувачів під час звернення до системи;
- Виявлення спроб порушення інформаційної безпеки;
- Представлення інформації для визначення та аналізу проблем.
- Розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля.
- Розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали.
- Розроблення, виробництво, впровадження, дослідження ефективності, супроводження засобів та комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу.
- Виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об'єктах інформаційної діяльності.

Основна форма організації інформаційних масивів в автоматизованій системі є база даних, яка представляє сукупність взаємозв'язаних даних, що зберігаються разом. БД існує незалежно від усіх інших програм і призначена для сумісного одночасного використування багатьма іншими користувачами. Така централізація і незалежність даних в технології БД потребує використання програмних засобів (СКБД), за допомогою яких здійснюється управління роботою додатків та забезпечується захист інформації від стороннього проникнення.

3.1.3.1 Система керування базами даних

Система керування базами даних (*СКБД*) — комп'ютерна програма чи комплекс програм, що забезпечує користувачам можливість створення, збереження, оновлення, пошук інформації та контролю доступу в базах даних.

- Основні характеристики СКБД
- Контроль за надлишковістю даних
- Непротирічність даних
- Підтримка цілісності бази даних (коректність та непротирічність)
- Цілісність (описується за допомогою обмежень)
- Незалежність прикладних програм від даних
- Спільне використання даних
- Підвищений рівень безпеки
- Можливості СКБД
- Дозволяється створювати БД (здійснюється за допомогою мови визначення даних DDL (Data Definition Language)).

Дозволяється додавання, оновлення, видалення та читання інформації з БД (за допомогою мови маніпулювання даними DML, яку часто називають мовою запитів). Можна надавати контрольований доступ до БД за допомогою:

1. Системи забезпечення захисту, яка запобігає несанкціонованому доступу до БД;

2. Системи керування паралельною роботою прикладних програм, яка контролює процеси спільного доступу до БД;

3. Система відновлення — дозволяє відновлювати БД до попереднього непротирічного стану, що був порушений в результаті збою апаратного або програмного забезпечення

Основні компоненти середовища СУБД

- Апаратне забезпечення;
- Програмне забезпечення;
- Дані;
- Процедури — інструкції та правила, які повинні враховуватись при проектуванні та використанні БД.

Користувачі :

- адміністратори даних(керування даними, проектування БД, розробка алгоритмів, процедур) та БД (фізичне проектування, відповідальність за безпеку та цілісність даних);
- розробники БД;
- прикладні програмісти;
- кінцеві користувачі.

3.2 Архітектура СУБД

Існує трирівнева система організації СУБД що забезпечує незалежний рівень ізоляції програми від особливостей представлення даних на нижчому рівні.

Рівні:

1. Зовнішній — представлення БД з точки зору користувача.
2. Концептуальний — узагальнене представлення БД, описує які дані зберігаються в БД і зв'язки між ними. Підтримує зовнішні представлення, підтримується внутрішнім рівнем.
3. Внутрішній — фізичне представлення БД в комп'ютері.

Логічна незалежність — повна захищеність зовнішніх моделей від змін, що вносяться в концептуальну модель.

Фізична незалежність — захищеність концептуальної моделі від змін, які вносяться у внутрішню модель.

В проекті системи «Energy Web-XB» використана вільна *СКБД* - **MySQL**. Дана система керування базами даних (СКБД) з відкритим кодом була створена як альтернатива комерційним системам. MySQL — одна з найпоширеніших систем керування базами даних. Вона використовується, в першу чергу, для створення динамічних веб-сторінок, оскільки має чудову підтримку з боку різноманітних мов програмування. MySQL – компактний багатопоточний сервер баз даних. Характеризується великою швидкістю, стійкістю і простотою використання. MySQL був розроблений компанією «TcX» для підвищення швидкодії обробки великих баз даних. MySQL вважається гарним рішенням для малих і середніх додатків. Вихідні коди сервера компілюються на безлічі платформ. Найбільш повно можливості сервера виявляються в UNIX-системах, де є підтримка багатопоточності, що підвищує продуктивність системи в цілому.Для некомерційного використання MySQL є безкоштовним. Можливості сервера MySQL:

- простота у встановленні та використанні;
- підтримується необмежена кількість користувачів, що одночасно працюють із БД;
- кількість рядків у таблицях може досягати 50 млн.;
- висока швидкість виконання команд;
- наявність простої і ефективної системи безпеки.

Сервера MySQL має свої недоліки, але вони не є критичними під час розробки і впровадження інформаційних систем для робочих груп.

Основні вимоги з безпеки даних для БД і СКБД співпадають з вимогами безпеки даних в комп'ютерних системах – контроль доступу, криптографічний захист, перевірка цілісності, протоколювання і т.ін. Управління цілісністю БД полягає в захисті БД від помилок, що приводять

до пошкодження бази. Підтримання цілісності забезпечується в кожний момент часу шляхом перевірки вірогідності усіх даних, взаємозв'язками між окремими складовими БД. З підтриманням цілісності зв'язані наступні вимоги:

1. Забезпечення вірогідності.
2. Управління паралелізмом.
3. Відновлення.

Більшисть систем БД представляє з себе середовище централізованого зберігання даних. Це значно зменшує надмірність даних, спрощує доступ до них і дозволяє більш ефективніше виконувати їх захист.

Більшість сучасних СКБД мають вбудовані засоби, що дозволяють адміністратору системи визначати права доступу користувачів до різних сегментів БД аж до конкретного елемента. При цьому є можливість не тільки надати доступ тому або іншому користувачеві, але й указати дозволений тип доступу: що саме може робити конкретний користувач із конкретними даними (читати, модифікувати, видаляти й т.п.), аж до реорганізації всієї БД Таблиці (списки) керування доступом широко використовуються в комп'ютерних системах, наприклад, в ОС для керування доступом до файлів. Особливість використання цього засобу для захисту БД полягає в тому, що в якості об'єктів захисту виступають не тільки окремі файли (області в мережних БД, відносини в реляційних БД), але й інші структурні елементи БД: елемент, поле, запис, набір даних.

Порушення цілісності даних може бути викликане рядом причин:

- збої обладнання, фізичні впливи або стихійні лиха;
- помилки санкціонованих користувачів або навмисні дії несанкціонованих користувачів;
- програмні помилки СКБД або ОС;
- помилки в прикладних програмах;
- спільне виконання конфліктних запитів користувачів і ін.

Порушення цілісності даних можливо й у добре налагоджених системах. Тому важливо не тільки не допустити порушення цілісності, але й вчасно виявити факт порушення цілісності й оперативно відновити цілісність після порушення.

Підтримка цілісності на основі наведених вище обмежень цілісності являє собою досить складну проблему в системі БД навіть із одним користувачем . У системах, орієнтованих на багатокористувацький режим роботи, виникає цілий ряд нових проблем, пов'язаних з паралельним виконанням конфліктуючих запитів користувачів .

Найважливішим засобом механізму захисту цілісності БД виступає об'єднання сукупності операцій, у результаті яких БД із одного цілісного стану переходить в інший цілісний стан, в один логічний елемент роботи, називаний транзакцією. Суть механізму транзакцій полягає в тому, що до завершення транзакції всі маніпуляції з даними проводяться поза БД, а занесення реальних змін у БД проводиться лише після нормального завершення транзакції . З погляду безпеки даних такий механізм відображення змін у БД дуже суттєвий . Якщо транзакція була перервана, то спеціальні вбудовані засоби СУБД здійснюють так званий «відкат» - повернення БД у стан, що передує початку виконання транзакції (насправді відкат звичайно полягає просто в невиконанні змін, обумовлених ходом транзакції, у фізичній БД). Якщо виконання однієї транзакції не порушує цілісності БД, те в результаті одночасного виконання декількох транзакцій цілісність БД може бути порушена .

Щоб уникнути подібного роду помилок, СУБД повинна підтримувати так звані механізми блокування, що забезпечують захоплення транзакціями елементів даних, що модифікуються, до моменту завершення модифікації. При цьому гарантується, що ніхто не одержить доступу до елемента даних, що модифікується, поки транзакція не звільнить його . Застосування механізму блокувань приводить до нових проблем управління паралелізмом, зокрема , до виникнення ситуацій клінчу двох транзакцій. Причому, якщо деяка транзакція намагається блокувати об'єкт, який уже блокований іншою транзакцією, то їй

доведеться чекати, поки не буде знято блокування об'єкта транзакцією, що встановила це блокування. Іншими словами, блокування об'єкта може виконувати тільки одна транзакція.

3.3 Управлінські заходи забезпечення інформаційної безпеки

Головна мета заходів, що вживають на управлінському рівні, - формування програми робіт в галузі інформаційної безпеки й забезпечення її виконання. У задачу управління входить виділення необхідних ресурсів і контроль стану справ. Підґрунтям програми є багаторівнева політика безпеки, що відображає підхід організації до захисту своїх інформаційних активів.

«Комплексні системи захисту інформації - є невід'ємною складовою частиною конкретного об'єкта інформаційної діяльності і поєднує організаційні та інженерні заходи, програмні й технічні засоби, призначені для попередження навмисних чи ненавмисних дій щодо блокування інформації, порушення її цілісності або конфіденційності».

Політика інформаційної безпеки — набір законів, правил і практичних рекомендацій і практичного досвіду, що визначають управлінські і проектні рішення в області ЗІ. На основі ПІБ будується керування, захист і розподіл критичної інформації в системі.

«Мета технічного захисту інформації з обмеженим доступом - своєчасне виявлення загроз та запобігання порушенню цілісності інформації з обмеженим доступом і витоку її технічними каналами.»

Наявний список подібних рішень може містити в собі наступні елементи:

- формування або перегляд комплексної програми забезпечення інформаційної безпеки, визначення відповідальних осіб за просування програми;
- формулювання цілей, які переслідує організація в області інформаційної безпеки, визначення загальних напрямків у досягненні цих цілей;
- забезпечення бази для дотримання чинних законів;

– формулювання управлінських рішень по тим питанням реалізації програм, які повинні розглядатись на рівні організації в цілому.

Для політики безпеки рівня керівництва організації цілі в галузі інформаційної безпеки формулюються в термінах цілісності, доступності й конфіденційності. Для організації відповідальної за підтримку критично важливих баз даних, на першому плані може стояти зменшення випадків втрат, пошкоджень або спотворення даних. Режимна організація в першу чергу опікується про захист від несанкціонованого доступу - конфіденційності.

На верхній рівень (рис.3.2) виноситься керування захисними ресурсами й координація використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем, підтримка контактів з іншими організаціями, що забезпечують або контролюють режим безпеки.

Політика верхнього рівня повинна чітко окреслювати сферу свого впливу. Можливо, це будуть усі комп'ютерні системи організації або навіть більше, якщо політика регламентує деякі аспекти використання співробітниками своїх домашніх комп'ютерів. Можлива, однак, і така ситуація, коли в сферу впливу включаються лише найбільш важливі системи. У політиці повинні бути визначені обов'язки посадових осіб по виробленню програми безпеки й по проведенню її в життя. У цьому змісті політика безпеки є основою підзвітності персоналу.

Політика верхнього рівня має справу із трьома аспектами виконавської дисципліни. По-перше, організація повинна дотримувати існуючих законів. По-друге, слід контролювати дії осіб, відповідальних за вироблення програми безпеки. Нарешті, необхідно забезпечити певний ступінь слухняності персоналу, а для цього потрібно виробити систему заохочень і покарань. На верхній рівень слід виносити мінімум питань. До середнього рівня можна віднести питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних систем, експлуатованих організацією.

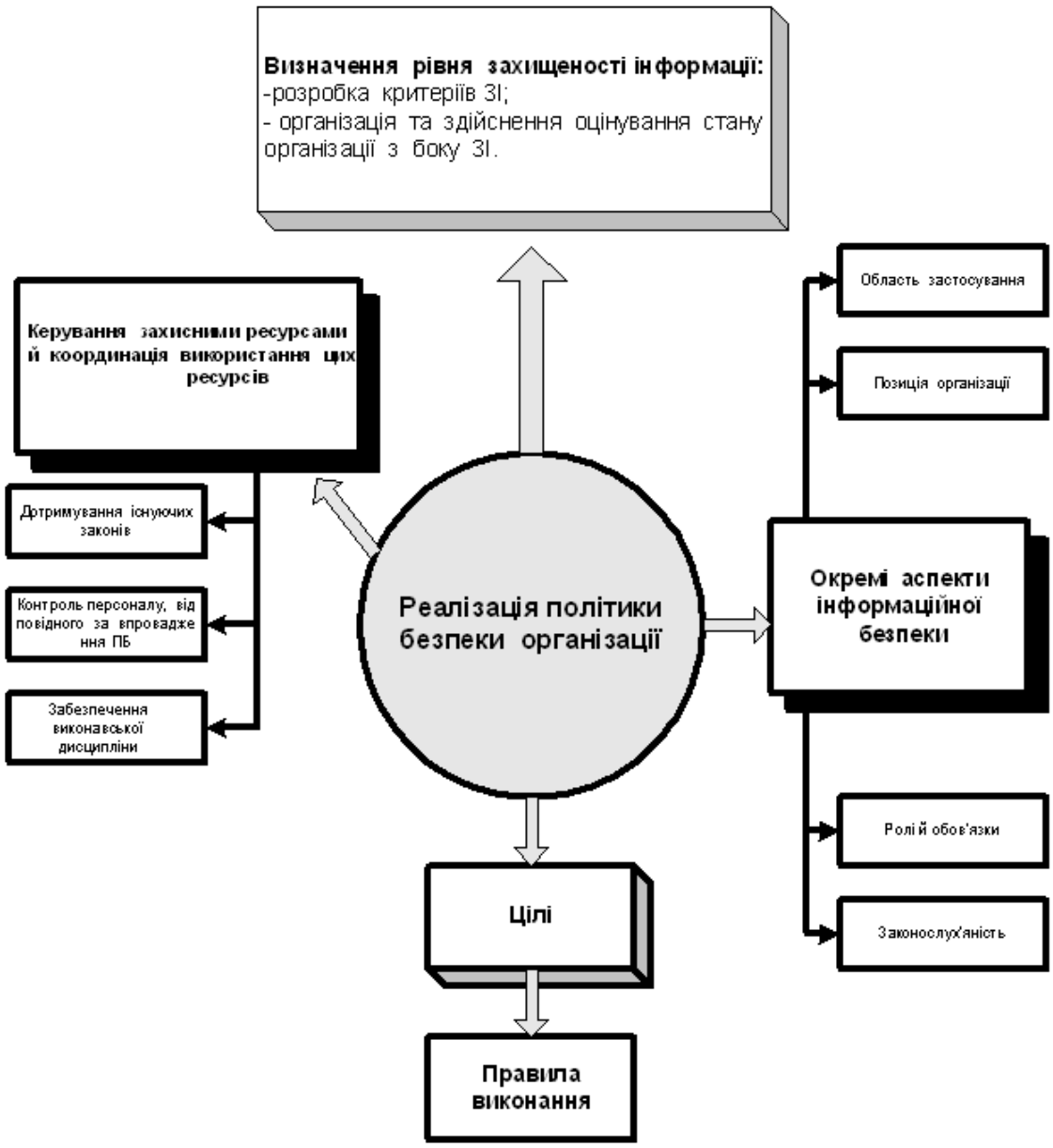


Рисунок 3.2 - Реалізація ПБ

Приклади таких питань - відношення до передових, але ще недостатньо перевіреним технологіям: доступ до Internet, використання домашніх комп'ютерів, застосування користувачами неофіційного програмного забезпечення і т.ін. Політика забезпечення інформаційної безпеки на середньому рівні повинна висвітлювати наступні теми:

– Область застосування. Випливає необхідність специфицікації в якій чітко формулюється - де, коли, як, стосовно кого й чому застосовується дана політика безпеки.

– Позиція організації полягає в повній забороні використання неліцензійного програмного забезпечення і в виробленні процедури приймання подібного забезпечення. Позиція може бути сформульована й у більш загальному виді, як набір цілей, які переслідує організація в даному аспекті. Взагалі, стиль документів по політиці безпеки, як і перелік цих документів, може бути суттєво різним для різних організацій.

– Ролі й обов'язки. В "політичний" документ необхідно включити інформацію про посадових осіб, відповідальних за проведення політики безпеки в життя. Наприклад, якщо для використання працівником іншого програмного забезпечення потрібно офіційний дозвіл, то повинно бути відомо, у кого і як його слід одержувати. Якщо повинні перевірятися носії, принесені з інших комп'ютерів, необхідно описати процедуру перевірки. Якщо неофіційне програмне забезпечення використовувати не можна, слід знати, хто стежить за виконанням даного правила.

– Законослухняна. Політика повинна містити загальний опис заборонених дій і покарань за них.

– Точки контакту. Повинне бути відомо, куди слід звертатися за роз'ясненнями, допомогою й додатковою інформацією. Звичайно "точкою контакту" є посадова особа, і це не залежить від того, яка конкретна людина займає в цей момент дану посаду

Політика безпеки нижнього рівня належить до конкретних сервісів. Вона містить у собі два аспекти - цілі й правила їх досягнення, тому її часом важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, розглянута політика повинна бути набагато детальніше. У той же час ці речі настільки важливі для забезпечення режиму безпеки, що рішення, що ставляться до них, повинні ухвалюватися на управлінському, а не технічному рівні. Питання, на які слід дати відповідь під час розробки політики безпеки нижнього рівня:

- хто має право доступу до об'єктів, підтримуваним сервісом?
- за яких умовах можна читати й модифікувати дані?
- як організований дистанційний доступ до сервісу?

При формулюванні цілей політика нижнього рівня може виходити з міркувань цілісності, доступності й конфіденційності, але вона не повинна на них зупинятися. Її цілі повинні бути конкретними. У більш загальному випадку цілі повинні зв'язувати між собою об'єкти сервісу й осмислені дії з ними. Із цілей виводяться правила безпеки, що описують, хто, що й при яких умовах може робити. Чим детальніше правила, чім більш формально вони викладені, тим простіше підтримати їхнє виконання програмно-технічними заходами. З іншого боку, занадто жорсткі правила можуть заважати роботі користувачів, імовірно, їх доведеться часто переглядати. Керівництву доведеться знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а працівники не виявляться надмірно заангажованими.

Звичайно ПБ складається із двох основних частин:

1. Політика для роботи в окремій мережі.
2. Політика для роботи в бездротовому середовищу.

У частині реалізації ПБ визначають рамки відповідальності. ПБ визначає відповідальних посадових осіб за реалізацію ПБ, до яких вона застосовна. Область дії ПБ застосовна до всіх підрозділів. Підрозділам рекомендується уточнити загальні рекомендації в тій мері, у якій вони застосовні до них, але доповнення до політики не повинні конфліктувати з основними рекомендаціями ПБ. У випадку суперечки відносно інтерпретації або реалізації локальної політики стосовно загальної ПБ, останнє слово - за відділом безпеки компанії. Відповідальність за виконання ПБ покладає на начальника служби безпеки й адміністратора компанії або на інших осіб верхньої ланки керування. Уточнення й інтерпретації ПБ можуть бути отримані у відділі безпеки у випадках очевидного конфлікту між локальними вимогами й різними тлумаченнями положень ПБ.

Галузь застосування.

У сферу дії політики забезпечення інформаційної безпеки попадають усі апаратні, програмні й інформаційні ресурси, що входять у мережу підприємства[14]. Політика орієнтована також на людей, що працюють із мережею, у тому числі на користувачів, субпідрядників і постачальників обладнання.

Позиція організації.

Метою організації є забезпечення цілісності, доступності й конфіденційності даних, а також їх повноти й актуальності.

Окремими цілями є:

– забезпечення рівня безпеки, відповідного до вимог нормативних документів [12];

– дослідження економічної доцільності у виборі захисних заходів (витрати на захист не повинні перевершувати передбачуваний збиток від порушення інформаційної безпеки);

– забезпечення безпеки в кожній функціональній області мережі;

– забезпечення підзвітності всіх дій користувачів з інформацією й ресурсами;

– забезпечення аналізу реєстраційної інформації;

– надання користувачам достатньої інформації для свідомої підтримки режиму безпеки;

– вироблення планів відновлення після аварій і інших критичних ситуацій для всіх функціональних областей з метою забезпечення безперервності роботи мережі;

– забезпечення відповідності з наявними законами політики безпеки підприємства.

Перераховані нижче групи людей відповідають за реалізацію сформульованих цілей:

– керівник організації відповідає за розробку відповідної політики забезпечення інформаційної безпеки й проведення її в життя;

– керівники підрозділів відповідають за доведення положень політики забезпечення інформаційної безпеки до користувачів і за контакти з ними.

– адміністратори мережі забезпечують безперервне функціонування мережі й відповідають за реалізацію програмних і технічних заходів, необхідних для проведення в життя політики забезпечення інформаційної безпеки.

– користувачі зобов'язані працювати з інформаційною мережею відповідно до політики безпеки, підкорятися розпорядженням осіб, відповідальних за окремі аспекти безпеки, доводити до відома керівництво про всі підозрілі ситуації.

Порушення політики забезпечення інформаційної безпеки може піддати локальну мережу й циркулюючу в ній інформацію неприпустимому ризику. Оскільки найбільш уразливою ланкою будь-якої інформаційної системи є людина, особливе значення набуває виховання законослух'яності співробітників стосовно законів і правилам інформаційної безпеки. Випадки порушення цих законів і правил з боку персоналу повинні розглядатися керівництвом для вживання заходів аж до звільнення.

Вочевидь, що забезпечення інформаційної безпеки є комплексним завданням. Це обумовлене тим, що інформаційне середовище є складним багатоплановим механізмом, у якім діють такі компоненти, як електронне встаткування, програмне забезпечення, персонал. Для розв'язку проблеми забезпечення інформаційної безпеки необхідне застосування комплексу законодавчих, організаційних і програмно-технічних заходів. Зневага хоча б одним з аспектів цієї проблеми може привести до втрати або витоку інформації, вартість і роль якої в житті сучасного суспільства здобуває усе більш важливе значення.

Кожна посадова особа й службовець компанії, який адмініструє або використовує мережеві й інші ресурси, відповідає за строге дотримання розробленої ПБ. Кожний користувач зобов'язано повідомляти про

підозрюваних або реальних уразливих місцях (погрозах) у безпеці системи своєму безпосередньому керівникові (менеджерові) або адміністраторові. У компанії є своя група улагоджування інцидентів з комп'ютерною безпекою (ГУІКБ), яка повинна повідомляти керівництво в обов'язковому порядку про основні інциденти, при яких відбулися компрометація, неправильне використання або псування інформаційних цінностей компанії. Підрозділам (відділам) рекомендується організувати свої локальні ГУІКБ для більш швидкого виявлення вразливих місць у захисті і їх усунення. Хоча співробітники, що входять у ГУІКБ, мають свої основні посадові обов'язки, питання безпеки мають пріоритет стосовно них. Керівники підрозділів повинні призначати своїх співробітників до складу ГУІКБ при виникненні інциденту, і звільняти від основних обов'язків до кінця розслідування.

У цій частині ПБ вказуються положення й критерії, які визначають її в тій мері, у якій вона застосовна до кого об'єкту й суб'єкта в Компанії. Частина, що відноситься до мереж, включає критерії, які повинні бути виконані для Інтернет з погляду безпеки.

Інтернет складається з мереж, тому ПБ, рівною мірою застосовується до всіх мережевих компонентів. Мережа, яка не є частиною Інтернет, не має засіб захисту, повинна дотримуватись вимог внутрішньої ПБ. Така мережа не містить точки ризику і є захищеною.

Мережеві ресурси компанії існують лише для того, щоб підтримувати її діяльність. У деяких випадках важко провести чорту між інтересами Компанії (службовими інтересами) і іншими інтересами. Система конференцій і електронної пошти Інтернет є прикладами змішання інтересів компанії й особистих інтересів співробітників по використанню цих ресурсів. Компанія розуміє, що спроби використання обмежень у цих випадках безглузді. Тому необхідно дати рекомендації, а не строгі вимоги відносно інформаційних ресурсів, які служать для розв'язку завдань, що стоять не тільки перед Компанією. Керівники відділів мають право ухвалити рішення щодо допустимості використання мережних ресурсів співробітниками для розв'язку

завдань, відмінних від службових, у тому випадку, якщо при цьому підвищується ефективність роботи даного співробітника. З іншої сторони менеджери повинні перешкоджати некоректному використанню мережних і інших ресурсів, як для особистих цілей, так і для цілей відпочинку й розваги співробітників. Сітьові адміністратори повинні повідомляти про інциденти керівнику відділу безпеки, пов'язаних з підозрюваним або доведеним використанням інформаційних ресурсів не по призначенню. Доступ до інформаційних цінностей Компанії не буде здійснений, якщо не виникне необхідності в такій інформації. Це значить, що критична інформація повинна бути захищена таким чином, щоб вона була невідома основній масі співробітників. У певних випадках може виявитися необхідним перетворити мережу таким чином, щоб навколо критичних інформаційних цінностей був створений периметр безпеки за допомогою технічних і організаційних заходів. Розробка ПБ ведеться тільки після виходу відповідного наказу в Компанії, де регламентуються права й можливості адміністратора на етапі розробки. При цьому, у наказі на розробку ПБ повинен вказуватися рівень доступу адміністратора до робочих місць користувачів і в інші приміщення, а також доступ до різних категорій інформації, наприклад, у режимі перегляду файлів і папок.

Увесь процес побудови ПБ можна розділити на 3 етапи:

1. Аналіз даних, інформації, цілей реалізації.

2. Власне розробка ПБ, результатом якої є створений юридичний документ.

3. Впровадження, зокрема , доведення обов'язків посадових осіб (під розпис), реєстрація у відділі кадрів і ін.

ПБ повинна реалізовуватися в не більш ніж двох екземплярах, які відповідно зберігаються в юриста і директора. На першому етапі, на кожному робочім місці користувача пропонується зібрати наступну інформацію:

1. Місце розташування або топологічна прив'язка вузлів мережі до схеми приміщень.

2. Характеристики приміщень, кімнат, будинків, поверхів і т.д.

3. Технологічні норми й нормативи по розміщенню робочого місця користувача.

4. Параметри й характеристики ПК.

5. Список користувачів, що працюють на ПК і їх права доступу.

6. Категорії інформації, використовувані на робочім місці, яка в підсумку повинна бути кваліфікована із прив'язкою до організаційно - штатної структури Компанії.

7. Типи груп користувачів, передбачуваних для використання в мережі, які обґрунтовуються й регламентуються в ПБ із обліком на подальше використання й розширення. При цьому, адміністраторові дозволяється додавання нових і зміна існуючих типів груп, пов'язаних з реорганізацією Компанії.

Уся термінологія в ПБ повинна бути описана заздалегідь грамотно з юридичної й технічної точки зору. У ПБ повинна бути регламентована в окремому пункті її доля у випадку звільнення адміністратора (ПБ втрачає свою юридичну чинність, оскільки адміністратор є її розроблювачем). Обов'язки посадових осіб, що охоплюють усі сфери діяльності співробітника, регламентуються в ПБ в окремих розділах для кожної категорії.

Тут вказуються права, обов'язки, перелік заборонених операцій і дій, а також можливі види санкцій, застосовуваних до співробітника. При цьому перелік останніх вказується в ПБ окремою статтею, з узгодженням у керівництва. Наприклад, це може бути список штрафних санкцій у вигляді втримання коштів , залежно від ваги порушення, а також вказівки на відповідні нормативні законодавчі акти для більш серйозних порушень. Таким чином, політика мережної безпеки в Компанії розподіляє відповідальність за її реалізацію й впровадження між конкретними посадовими особами Вона визначає обов'язки кожного службовця Компанії при використанні сітьових і інших ресурсів і необхідності повідомляти про вразливі місця в системі безпеки. Вона також встановлює, що загальною політикою є - заборонене все,

що явно не дозволене. Тобто , якщо діяльність або вид доступу не можуть бути знайдені або визначені в цьому документі, то вони заборонені. За доробку ПБ відповідає особу, що займається розробкою даного документа, у міру того, як потреба в безпеці й технології сітьової взаємодії змінюються. Директиви, що містяться в ПБ, повинні бути завжди інтерпретовані як наказ директора Компанії.

3.4 Розробка політики безпеки автоматизованої системи обробки конфіденційної інформації

Політика безпеки що розробляється застосовна до автоматизованої системи (АС) для обробки конфіденційної інформації, яка потребує особливої захисту (надалі АС, яка призначена для обробки конфіденційної інформації, що потребує особливого захисту, буде позначатися як АС.4).

Відповідно до НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» АС - це організаційно-технічна система, що реалізує інформаційну технологію і об'єднує ОС, фізичне середовище, персонал і інформацію, яка обробляється. Відповідальність за забезпечення захисту конфіденційної інформації, що потребує особливого захисту, покладається на керівника (заступника керівника) підприємства. Організація і проведення робіт по захисту конфіденційної інформації, що потребує особливого захисту, проводиться службою інформаційної безпеки, яка визначає вимоги до модернізації системи захисту інформації, виконання робіт з експлуатації та контроль за станом захищеності інформації. Служба інформаційної безпеки повинна створюватися наказом керівника підприємства. З огляду на штат співробітників, служба інформаційної безпеки має складатися з адміністратора інформаційної безпеки, обов'язки якого повинен виконувати адміністратор ІКС підприємства. У своїй діяльності адміністратор інформаційної безпеки має керуватися документом «Інструкція адміністратору інформаційної безпеки».

Для забезпечення створення, обробки та зберігання конфіденційної інформації, що потребує особливого захисту, на підприємстві необхідно виконати локалізацію такої інформації. Під час обробки конфіденційної інформації в АС.4 повинен забезпечуватися її захист від несанкціонованого і неконтрольованого ознайомлення, модифікації, знищення, копіювання і розповсюдження. Завдання та функції АС.4: забезпечити безпечну обробку, зберігання та створення конфіденційної інформації критичного характеру в електронному вигляді та на паперових носіях; забезпечити збереження властивостей конфіденційної інформації (конфіденційність, цілісність та доступність).

Об'єкти доступу.

До даних об’єктів відносяться текстові документи, представлені в електронному вигляді та на паперових носіях, які містять конфіденційну інформацію критичного характеру. Як раніше було зазначено, до конфіденційної інформації відносимо:

- комерційну інформацію (дані про витрату електроенергії за розрахунковий проміжок часу);
- інформацію про поточне споживання електроенергії окремим абонентом;
- інформацію про стан підключення абонента;
- інформацію про параметри точки обліку.
- Дані захисту: база даних захисту (перелік користувачів та їх атрибут доступу), журнал захисту, параметр та конфігурації КСЗ;
- Технічні засоби (сервер баз даних), в тому числі засоби захисту;
- Програмне забезпечення ПК (програмні засоби КСЗ, спільне, функціональне та спеціальне ПЗ та службові дані, необхідні для його роботи);
- Знімні носії, які містять критичну інформацію;
- Резервні копії критичною інформації.

Для встановлення правил розмежування доступу необхідно забезпечити виконання наступних умов:

– Абонент мережі отримує доступ до власних показників витрати електроенергії по мережі Інтернет. Система повинна забезпечити доступ користувачів тільки до тих даних, які відповідають їх ідентифікаторам.

– Службові користувачі отримують доступ до даних тільки за виконання умов розмежування.

Доступ до конфіденційної інформації повинен надаватися тільки користувачам, які пройшли ідентифікацію та аутентифікацію . Спроби доступу до такої інформації не ідентифікованих осіб чи користувачів з непідтвердженою під час аутентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися.

У випадку, якщо користувачеві за родом діяльності необхідний доступ до заборонених йому ресурсів, він може оформити тимчасовий доступ наказом керівника підприємства після згоди адміністратора інформаційної безпеки. Адміністратор інформаційної безпеки має право відмовити користувачеві в доступі до критичною інформації у випадку, якщо він не згоден з причинами, по яких користувачеві необхідно надати доступ.

Адміністратор інформаційної безпеки повинен регулярно проводити перевірку прав користувачів, виконуючи «Вимоги до перевірки прав користувачів».

Реалізація функції копіювання критичної інформації в електронному вигляді на змінні носії інформації повинна здійснюватися тільки в присутності адміністратора інформаційної безпеки підприємства. Цей процес повинен контролюватися шляхом реєстрації в системному журналі імені користувача, об'єкта копіювання, часу копіювання. Виведення критичною інформації в текстовому вигляді повинно здійснюватися тільки на принтері у виділеному приміщенні та в присутності адміністратора інформаційної безпеки. Цей процес

повинен фіксуватися в системному журналі: ім'я користувача, об'єкт друку, час друку.

Видалення критичною інформації, представленої в електронному вигляді та на паперовому носії, може виконувати тільки адміністратор інформаційної безпеки після дозволу директора підприємства. Всі інші користувачі не мають право на видалення інформації в АС.4. При спробі користувачем видалити інформацію, система повинна зареєструвати інформація про цей процес і заблокувати дію.

Доступ до даних захисту повинен надаватися відповідно до ролі користувача. Права на читання і запис даних у базу даних захисту і право на перегляд системного журналу безпеки повинен мати тільки користувач з роллю адміністратора безпеки.

Право на читання і зміни значень параметрів конфігурації КСЗ, безпосередньо пов'язаних з керівництвом доступу, а також права на читання і зміни значень інших параметрів конфігурації КСЗ, права на читання даних про поточну поведінку КСЗ і право на оперативне керівництво КСЗ повинен мати тільки користувач з роллю адміністратора безпеки.

У системі повинні бути чітко прописані обов'язки обслуговуючого персоналу і користувачів. Ведення переліку користувачів з його атрибутами доступу виконує адміністратор інформаційної безпеки. Адміністратор інформаційної безпеки має створити для кожного користувача АС.4 обліковий запис з наданням їм відповідних прав та дозволів у відповідності з групою та роллю користувача.

Коригування атрибутів доступу до об'єктів доступу виконує адміністратор інформаційної безпеки з вказівки керівника підприємства. Інсталяцію та оновлення всіх програмних засобів виконує системний адміністратор. Всі роботи, які прямо або безпосередньо можуть вплинути на захищеність інформації (у тому числі ті, які відносяться до програмних засобів КСЗ), виконуються за згодою адміністратора інформаційної безпеки. Щоденні зобов'язання адміністрування (відстеження потенційно небезпечних дій,

поновлення роботи в разі збоїв у системі) виконує адміністратор інформаційної безпеки.

Для надійності збереження критичною інформації адміністратор інформаційної безпеки повинен щодня в кінці робочого дня виконувати резервне копіювання критичною інформації. Резервна інформація повинна бути представлена в зашифрованому вигляді. Тривалість зберігання резервного диска повинна становити термін до дня зняття наступного балансу споживання електроенергії. Після закінчення цього терміну диск може повторно використовуватися для резервного копіювання. Цілісність і достовірність архівної інформації перевіряється адміністратором інформаційної безпеки. Ідентифікація та аутентифікація користувачів, надання та позбавлення їх прав доступу до критичною інформації та її обробка, контроль за цілісністю засобів захисту в АС.4 повинне здійснюватися автоматично. Усі користувачі АС.4 повинні бути навчені правилам роботи в АС.4 і під розписку ознайомлені з «Інструкцією користувачу АС.4», яка має регламентувати порядок доступу та правила поводження з захищеною інформацією.

Система захисту фізичного середовища АС.4 повинна складатися з:

- системи пожежної сигналізації;
- системи охоронної сигналізації;
- системи контролю доступу.

На підприємстві повинно бути організовано власну охорону всього фізичного середовища підприємства. Система охоронної сигналізації повинна забезпечувати захист фізичного простору АС.4 від можливого несанкціонованого проникнення зловмисника. Система контролю доступу повинна забезпечувати неможливість несанкціонованого проникнення осіб на територію функціонування АС.4 в робочий і неробочий час і неможливість несанкціонованого і неконтрольованого доступу до носіїв інформації та журналу подій.

Розробка системи захисту конфіденційної інформації виконується для автоматизованої системи (АС.4), призначеної для обробки конфіденційної

інформації, що потребує захисту, для вищого технічного навчального закладу. Результатом роботи має бути система захисту інформації (СЗІ), яка забезпечить можливість створення, обробки та зберігання конфіденційної інформації, представленої в електронному вигляді і в текстових документах.

Метою створення СЗІ є забезпечення захисту конфіденційної інформації. У АС.4 надаються особливі вимоги до конфіденційності, цілісності та доступності інформації. Відповідно до специфікацій, наведених у документі НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», комплекс засобів захисту (КСЗ) повинен надавати такі послуги безпеки: 1. Базова довірча конфіденційність - КД-2; 2. Повторне використання об'єктів - КВ-1; 3. Мінімальна довірча цілісність - ЦД-1; 4. Обмежений відкат - ЦО-1; 5. Модернізація - ДЗ-1; 6. Ручне відновлення - ДВ-1; 7. Захищений журнал - НР-2; 8. Окрема ідентифікація та автентифікація - НИ-2; 9. Відокремлення адміністратора - НО-1; 10. СЗІ з контролем цілісності - НЦ-1; 11. Самотестування під час старту - НТ-2.

Процес розробки КСЗ повинен відповідати рівню гарантій Г-2 (відповідні вимоги наведені в документі НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»). СЗІ розробляється як сукупність технічних і програмних засобів захисту та організаційних заходів, які забезпечать виконання загальних вимог до створення, обробки та зберігання конфіденційної інформації. СЗІ розробляється відповідно до вимог, які визначені в таких законодавчих та нормативних документах з питань охорони конфіденційної інформації та технічного захисту інформації:

Закон України «Про інформацію». Закон України «Про захист інформації в автоматизованих системах». Закон України «Про державну таємницю». НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

НД ТЗІ 2.5-006-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки.

НД ТЗІ 3.7-001-99 Методичні вказівки для розробки технічного завдання на створення комплексної систем захисту інформації в автоматизованій системі.

ДСТУ 3396.0-96. Технічний захист інформації. Основні положення.

ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт.

Технічні засоби (сервер баз даних) АС.4 розміщені в приміщенні ДВНЗ, який знаходиться в межах контрольованої зони. Приміщення облаштовані електромеханічним замком, системами пожежної та охоронної сигналізацій. Система пожежної сигналізації виконана з димових датчиків. Система охоронної сигналізації виконана з ІЧ-датчиків руху, акустичного датчика розбиття скла, контактного датчика відкриття дверей.

За рівнем повноважень доступу до інформації і характером робіт, які виконуються в процесі функціонування АС.4, особи, які мають доступ до АС.4, поділяються на наступні категорії: 1. Звичайні користувачі – студенти; 2. Користувачі, які забезпечують функціонування АС.4, адміністрування операційної системи; 3. Працівники служби інформаційної безпеки, які забезпечують функціонування СЗІ; 4. Технічний персонал, який обслуговує мережу енергоспоживання.

З метою забезпечення безпечної обробки конфіденційної інформації критичного характеру в АС.4 наказом керівника ДВНЗ створюється служба

інформаційної безпеки в АС.4, якій надаються повноваження організації та впровадження СЗІ, контроль за станом захищеності інформації. З огляду на штат співробітників підприємства, служба інформаційної безпеки має складатися з адміністратора інформаційної безпеки, обов'язки якого повинен виконувати системний адміністратор. У своїй діяльності адміністратор інформаційної безпеки має керуватися документом «Інструкція адміністратору інформаційної безпеки».

КСЗ повинен реалізовувати рівень КД-2 - Базова довірча конфіденційність.

Доступ до програмних засобів СЗІ:

КСЗ повинен надавати доступ до процесів, за допомогою яких обробляється конфіденційна інформація, тільки користувачам АС.4. КСЗ повинен надавати доступ до процесів, за допомогою яких виконується ведення бази даних захисту і перегляд системного журналу безпеки, тільки адміністратору інформаційної безпеки. КСЗ повинен надавати можливість змінювати атрибути доступу файлів тільки адміністратору інформаційної безпеки.

Доступ до даних захисту:

КСЗ повинен надавати можливість роботи з даними захисту тільки за допомогою призначеного для цього процесу;
КСЗ повинен реалізовувати правила розмежування доступу до даних захисту.

Повторне використання об'єктів

КСЗ повинен реалізувати рівень КВ-1 - повторне використання об'єктів. Політика повторного використання об'єкта, що реалізується КСЗ, відноситься до всіх об'єктів КС. Перед тим як користувач або процес може отримати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права до даного об'єкту повинні бути скасовані. Перед тим як користувач або процес може отримати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся

інформація, яка містилася в даному об'єкті, повинна стати недосяжною. *Доступ до програмних засобів СЗІ*

КСЗ повинен надавати доступ до процесів, за допомогою яких обробляється конфіденційна інформація, тільки користувачам АС.4. КСЗ повинен надавати доступ до процесів, за допомогою яких виконується ведення бази даних захисту і перегляд системного журналу безпеки, тільки адміністратору інформаційної безпеки. КСЗ повинен надавати можливість змінювати атрибути доступу файлів тільки адміністратору інформаційної безпеки.

Доступ до даних захисту:

КСЗ повинен надавати можливість роботи з даними захисту тільки за допомогою призначеного для цього процесу; КСЗ повинен реалізовувати правила розмежування доступу до даних захисту;

Відкат

КСЗ повинен реалізовувати рівень ЦО-1 - обмежений відкат. Відкат може здійснюватися у випадку видалення або модифікації об'єкта доступу. КСЗ повинен забезпечувати можливість адміністратору інформаційної безпеки відкоту дій за допомогою автоматизованих засобів. КСЗ повинен забезпечити фіксування відкату в системному журналі безпеки. Відміна операції не повинна призводити до видалення з системного журналу безпеки запису про операцію, яка була скасована.

Використання ресурсів

КСЗ повинен реалізовувати рівень ЦД-1 - квоти. Уві захищені об'єкти повинні ідентифікуватися і контролюватися диспетчером доступу шляхом накладення обмежень на максимальний обсяг денного ресурсу, який може бути виділений користувачу. Запити на зміну встановлених обмежень повинні оброблятися КСЗ тільки в тому випадку, якщо вони послані від адміністратора інформаційної безпеки.

Гаряча заміна

КСЗ повинен реалізовувати рівень ДЗ-1 - модернізація. Модернізацію або заміну окремих компонентів комп'ютерної системи може виконувати тільки системний адміністратор. Модернізація комп'ютерної системи повинна виконуватися у випадку порушення умов функціонування системи в цілому або окремих її компонентів.

Відновлення після збоїв

КСЗ повинен реалізовувати рівень ДВ-1 - ручне відновлення. В системі необхідно передбачити певний порядок обробки помилок, які з'являються під час роботи системи. Програмні засоби повинні надати адміністратору можливість вказати системі, яким чином вона повинна реагувати на помилку. Всі можливі помилки та способи їх усунення повинні бути документовані.

Реєстрація (аудит)

КСЗ повинен реалізовувати рівень НР-2 - захищений журнал. Для реєстрації подій в СЗІ слід передбачити журнал безпеки, який повинен бути захищений від несанкціонованого ознайомлення, модифікації і знищення. Адміністратору інформаційної безпеки необхідно надати засоби для зручної роботи з журналом, які також дозволяли створювати копії журналу і працювати з раніше створеними копіями. Засоби реєстрації КСЗ повинні забезпечувати реєстрацію таких подій: вхід / вихід користувачів у АС.4; ідентифікація та аутентифікація користувачів; створення / видалення або зміна облікових записів (у тому числі зміна паролів користувачів); зміна політики безпеки ОС; результати виконання користувачами операцій з обробки даних (копіювання інформації на знімні носії, резервне копіювання, друк, зміни інформації, спроби видалення інформації); спроби несанкціонованих дій над інформацією; факти надання та позбавлення користувачів прав доступу до критичною інформації та її обробки; зміни конфігурації КСЗ; результати перевірки цілісності засобів захисту інформації; початок і кінець роботи прикладних програм.

Усі записи про події повинні містити інформацію про дату, час і тип (у тому числі успішне або неуспішні) події, а для подій аудиту (відстеження дій

користувачів) так само про користувача, процес і об'єкти, пов'язані з подією. Слід надати адміністратору інформаційної безпеки можливість встановлювати політику аудиту, яка б визначала, які саме події реєструються засобами КСЗ.

Ідентифікація та аутентифікація

КСЗ повинен реалізовувати рівень НІ-2 - одноразова ідентифікація і аутентифікація. Кожен користувач повинен однозначно ідентифікуватися КСЗ на підставі свого імені. Перш ніж дозволити будь-якому користувачеві виконувати які-небудь контрольовані КСЗ дії, КСЗ повинен аутентифікувати цього користувача на основі введеного ним пароля. КСЗ повинен забезпечити захист даних аутентифікації від несанкціонованого ознайомлення, модифікації і руйнування.

Розподіл обов'язків

КСЗ повинен реалізовувати рівень НО-1 - виділення адміністратора. У відповідності з обмеження доступу визначається 3 ролі користувачів:

1. Звичайний користувач;
2. Адміністратор інформаційної безпеки;
3. Системний адміністратор.

Цілісність комплексу засобів захисту

КСЗ повинен реалізовувати рівень НЦ-1 - КСЗ з контролем цілісності. КСЗ повинен перевіряти цілісність таких об'єктів: програмні компоненти КСЗ, параметри і розділи системного реєстру, в яких зберігаються важливі для захисту дані. Всі помилки, які виникають під час перевірки цілісності, необхідно вважати порушенням цілісності. Необхідно сформулювати вимоги до налаштувань ОС, які гарантують, що послуги безпеки доступні тільки через інтерфейс КСЗ і всі запити користувачів на доступ до об'єктів захисту контролюються КСЗ. Відновлення програмних засобів КСЗ повинно проводитися системним адміністратором.

Самотестування

КСЗ повинен реалізовувати рівень НТ-2 - самотестування під час старту. КСЗ виконує перевірку і на підставі цього гарантує правильність функціонування і цілісність функцій КС.

Керованість КСЗ

Для проведення різних видів робіт необхідно передбачати кілька станів КСЗ: робочий стан для нормальної роботи та деякі службові стану, точніше, стан відновлення для проведення відновних робіт. Правом переведення КСЗ з одного стану в інший повинні володіти тільки адміністратор інформаційної безпеки або системний адміністратор.

Засоби адміністрування КСЗ повинні забезпечувати: ведення переліку користувачів АС.4, тобто введення, видалення користувачів та встановлення їх атрибутів доступу; настройка параметрів роботи КСЗ (параметри перевірки цілісності, параметри ведення журналу безпеки тощо); оперативне управління КСЗ (зміна стан КСЗ, проведення перевірок цілісності та ін.)

Вимоги до гарантій реалізації

Процес реалізації повинен відповідати рівню гарантій Г-2 у відповідності з НД ТЗІ 2.5-004-99. Наведені послуги безпеки реалізуються за допомогою програмного забезпечення. Програмне забезпечення КСЗ складається з таких частин:

- засоби захисту операційної системи;
- функціональне ПЗ (антивірусні програми);
- спеціальне ПЗ (програмні засоби, призначені для вирішення спеціальних задач захисту в АС.4).

Операційна система та програмне забезпечення повинні бути придбані в офіційного постачальника і мати ліцензії. В якості спеціального ПЗ повинні використовуватися програмні засоби з гарантією реалізації на рівні Г-2.

Архітектура

Спеціальне програмне забезпечення повинно складатися з таких частин:

- ПЗ, призначене тільки для захисту інформації та засоби, які виконують захист даних.

– Спеціальна ПО захисту повинно містити з своєму складі такі компоненти:

– сервер безпеки, який виконує функції ядра КСЗ;

– адміністративні утиліти - програмні засоби, призначені для адміністрування КСЗ, роботи з журналом безпеки й оперативного управління КСЗ;

– засоби захисту документів.

Послідовність розробки

У процесі розробки ПЗ повинні бути створені такі характеристики:

– Функціональні специфікації, які містять перелік послуг безпеки, що надаються КСЗ, правила і механізми надання послуг.

– Проект архітектури КСЗ з описом функціонування її компонентів та їх зовнішніх інтерфейсів; Повинно бути показана відповідність проекту архітектури моделі політики безпеки. На стадії розробки ескізного проекту необхідно розробити проект архітектури КСЗ. Представлений проект повинен містити перелік і опис усіх компонентів КСЗ і функцій, реалізованих ними. Повинні бути описані будь-які використовувані зовнішні політики безпеки. Зовнішні інтерфейси КСЗ повинні бути описані в термінах винятків, повідомлень про помилки і кодів повернення. Стиль специфікації проекту архітектури повинен бути неформалізованим.

– Детальний проект найбільш важливих для захисту інформації частин програмного забезпечення. Повинно бути показано відповідність детального проекту архітектурі. Необхідно привести перелік всіх компонентів КСЗ і точний опис функціонування кожного механізму, призначення і параметри інтерфейсів кожного компонента КСЗ. Стиль специфікації детального проекту повинен бути неформалізованим.

У вигляді окремих документів або підрозділів повинно бути наведено опис послуг безпеки, реалізованих КСЗ, настанови адміністратору інформаційної безпеки щодо послуг безпеки, настанови користувачам щодо

послуг безпеки (інструкції використання функцій безпеки звичайним користувачем). Настанови адміністратору повинні містити опис засобів інсталяції, генерації і запуску автоматизованої системи, опис усіх можливих параметрів конфігурації. Опис послуг безпеки може бути різним для адміністратора та користувача.

Експлуатаційні документи:

1. Інструкція адміністратора інформаційної безпеки;
2. Інструкція користувачеві АС.4;
3. Інструкція з організації антивірусного захисту в АС.4;
4. Інструкція з організації парольного захисту в АС.4;
5. Інструкція з ведення «Журналу подій»;
6. Вимоги при реєстрації користувачів АС.4;
7. Вимоги до перевірки прав користувачів АС.4.

З метою забезпечення режиму секретності під час обробки та зберігання критичною інформації в АС.4 наказом керівника ДВНЗ необхідно створити службу інформаційної безпеки підприємства. Служба інформаційної безпеки зобов'язана вести організацію та впровадження СЗІ, контроль стану захищеності інформації, вести журнал подій. З огляду на штат співробітників підприємства, служба інформаційної безпеки має складатися з адміністратора інформаційної безпеки, обов'язки якого повинен виконувати системний адміністратор підприємства. У своїй діяльності адміністратор інформаційної безпеки має керуватися документом «Інструкція адміністратору інформаційної безпеки».

Для обробки конфіденційної інформації в АС.4 необхідно встановити основні технічні засоби та програмне забезпечення, що задовольняють вимогам, висунутим в ПБ і ТЗ. В якості ОТС та програмного забезпечення для обробки критичною інформації необхідно використовувати тільки ліцензійне обладнання і ПЗ. Чинний сертифікат припускає, що компоненти ОТС та ПЗ, що випускаються виробником, пройшли спеціальну перевірку та спеціальні дослідження, мають однаковий склад, а розкид технічних параметрів і рівнів

побічних випромінювань знаходиться в межах ставляться до них вимог. Також роботу АС.4 забезпечує технічний персонал. Роботи технічного персоналу контролюються адміністратором інформаційної безпеки або співробітником, відповідальним за безпеку фізичної середовища АС.4.

Користувачі АС.4 повинні мати відповідним чином оформлені допуски до відомостями, що містять критичну інформацію. Допуск до АС.4 оформляється наказом керівника.

4 РОЗРОБКА Й НАУКОВЕ ОБҐРУНТУВАННЯ РЕКОМЕНДАЦІЙ ПО ВИКОРИСТАННЮ ПРОГРАМНО-АПАРАТНИХ КОМПЛЕКСІВ ВІДДАЛЕНОГО КОНТРОЛЮ ТА МОНІТОРИНГУ ОСВІТНЬО-НАУКОВИХ ТА ТЕХНОЛОГІЧНИХ ПРОЦЕСІВ

4.1 МОДЕМ-КООРДИНАТОР «СИГМА GSM-ZB»

Модем-координатор Сигма GSM-ZB розроблений для організації віддаленого дистанційного управління пристроями, що підтримують специфікацію ZigBee і являє собою міст між мережами ZigBee і GSM / GPRS.

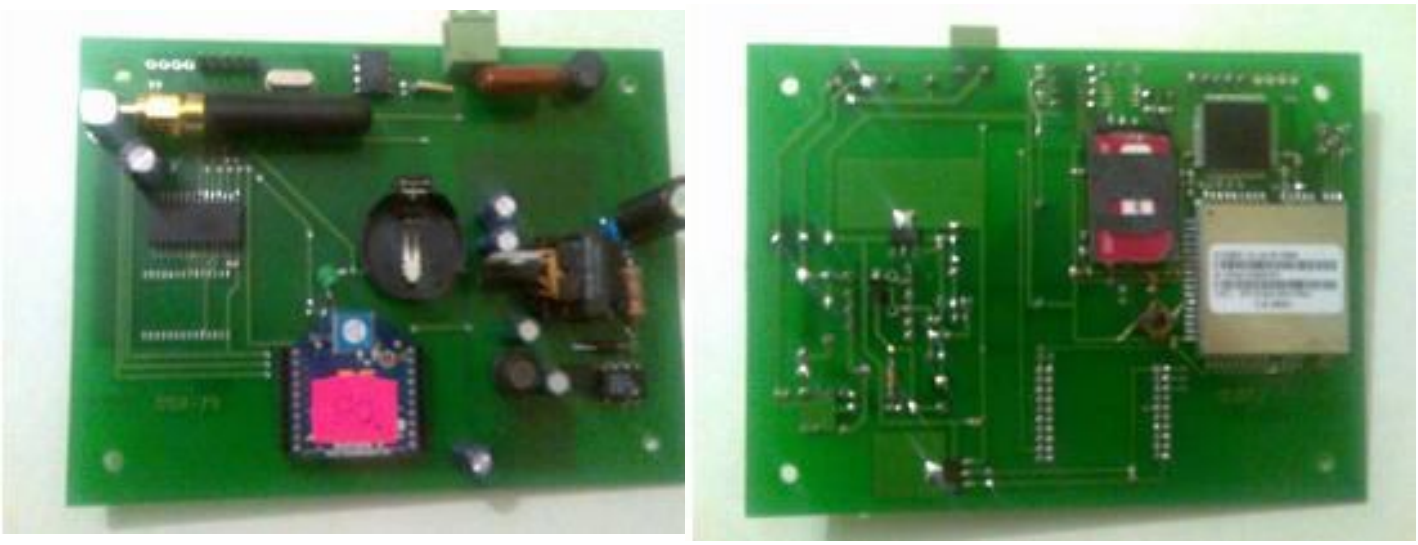


Рисунок 4.1 - Модем-координатор «Сигма GSM-ZB»

Технологія Servic Smart Energy Web-ZB (SSEW) є Internet-платформою для побудови інтелектуальних мереж (Smart Grid), на основі якої реалізовані різні інформаційно-керуючі програми, пов'язані з телекомунікаційних послуг у сфері розподілу та споживання ресурсів. Мережа збору та передачі даних, реалізована на базі даної технології, представляє собою комплекс апаратних і програмних засобів цифрового комунікаційного середовища, що функціонує в складі різних приватних мереж обліку та управління споживання енергоресурсів. Технологія SSEW володіє ширшою порівняно зі звичайними AMR/AMI/AMM системами функціональністю. Крім оптимального управління

та підвищеної оперативності система надає можливість вибірково регулювання окремих сегментів мережі аж до індивідуального розподілу ресурсів. При цьому використовуються RF канали (ieee802.15.4/ZigBee) і новітні технології зв'язку (gprs, 3G, 4G WiMAX), що дозволяє реалізовувати складні рішення для додатків будь-якої конфігурації в оптимальні терміни і при незначних витратах.

Технологія SSEW (Servic Smart Energy Web-ZB) заснована на дистанційному зборі даних і управлінні розподіленими пристроями, зв'язок між якими організована у відповідності зі специфікацією ZigBee / IEEE 802.15.4, з використанням протоколу TCP / IP.

Основними розробленими на цей момент додатками є:

– Система обліку інформаційних та ресурсних потоків та управління навантаженням «Smart Energy Web-ZB»;

– Система обліку та управління споживанням води «Smart Water Web-ZB»;

– Система обліку споживання газу «Smart Gaz Web-ZB».

Всі перераховані системи, організовані за принципом WPAN (персональних бездротових мереж), інтегровані в Інтернет і діють у відповідності з передовими принципами «хмарних» (cloud computing) або «сервісних» (SaaS) технологій. Дана архітектура забезпечує транзит інформаційних потоків між клієнтами мережі і клієнтськими виконавчими пристроями, наприклад, різними лічильниками, датчиками і т.п. (рис. 4.2). Завдання SSEW полягає в своєчасному, повному і достовірному інформаційному обміні між первинними пристроями і сервером Бази даних системи. Основне ядро системи забезпечує автоматичне функціонування віддалених ZigBee WPAN, їх конфігурування і керування, а так само підтримує інформаційний обмін між різними автономними додатками і об'єктами.

Основними функціями системи є:

– Збір, зберігання та передавання даних від первинних пристроїв.

– Управління мережею і контроль її працездатності.

– Формування даних для конвертації у зовнішню програму.

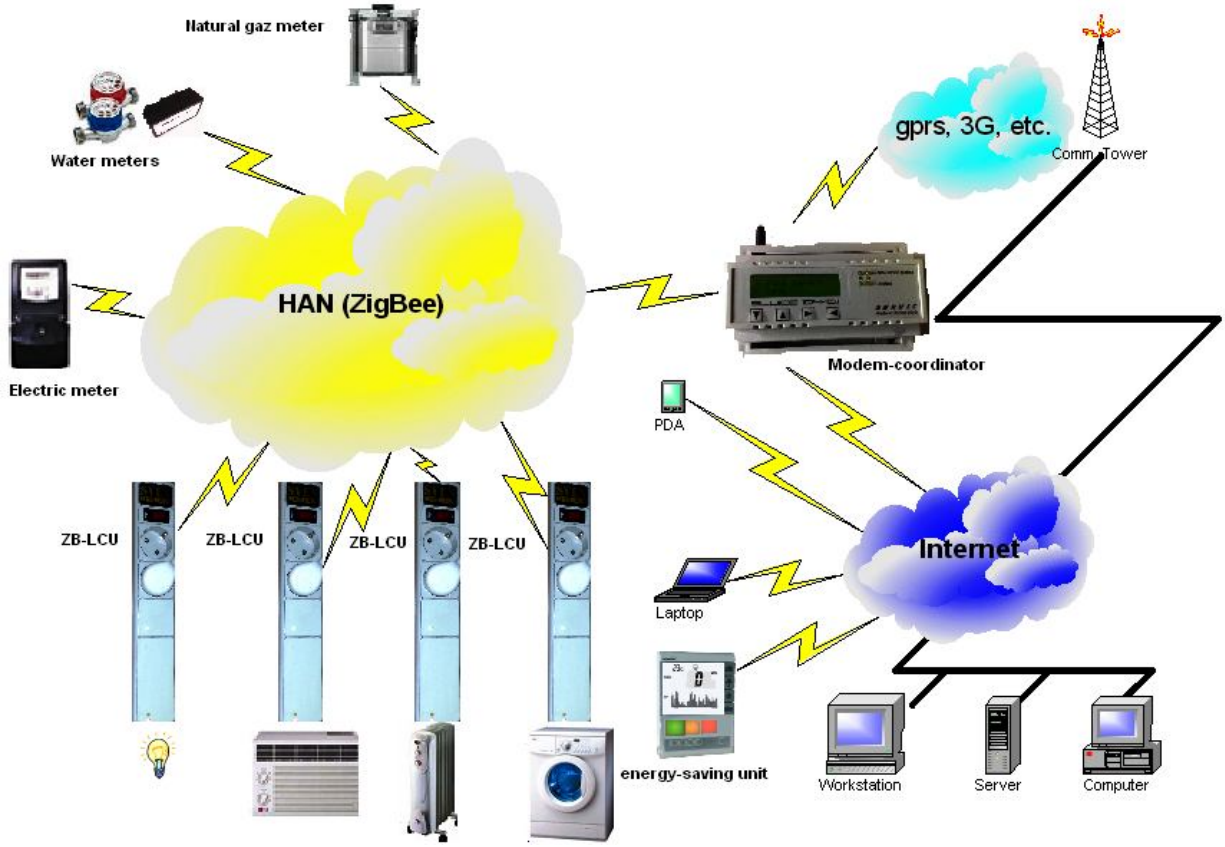


Рисунок 4.2 - Структура SSEW

Базове устаткування SSEW (ZigBee-плагіни) підключається до мереж, облік в яких здійснюється первинними пристроями, оснащеними цифровим (імпульсним) інтерфейсом, а управління - додатковими виконавчими механізмами (електромагнітні клапани або приводи, реле навантаження). Такими пристроями є, наприклад, лічильники електроенергії, води, газу, тепла і т.п. Передбачається, що використовуються для обліку лічильники оснащені імпульсним або цифровим виходом. Лічильники в сукупності з мережним устаткуванням SSEW (модем-координатор) представляють собою Систему обліку та регулювання. Дану систему слід розглядати як універсальний засіб побудови різних AMR / AMI / AMM систем на підставі того, що:

1. Використовуються інтерфейсні пристрої - ZigBee-плагіни, що дозволяють адаптувати широкий спектр оригінального обладнання різних виробників в єдину закінчену систему.

2. Використання «хмарної» (Saas) технології за допомогою Internet-з'єднання дозволяє здійснювати:

– Збір, зберігання і первинну обробку інформації.

– Управління мережею та всіма первинними пристроями мережі.

– Передачу інформації, адаптованої до прикладних задач клієнтів.

– Забезпечити взаємодію клієнтів зі звітними додатками.

Передача даних в SSEW здійснюється з використанням мережевих транзитних пристроїв - модем-координаторів, з одного боку, підтримують зв'язок з клієнтськими виконавчими пристроями, а з іншого - з Internet через різні канали зв'язку. Будучи майстром мережі, модем-координатор синхронізує календарний годинник всіх пристроїв, формує адресні інформаційні потоки, діагностує стан мережі.

4.1.1 Складові елементи системи

Серія виробів «Сигма-xZBx» призначена для передачі вимірювальної інформації з встановлених або знову встановлюваних приладів обліку енергоносіїв, обладнаних:

- імпульсними по МЕК 62053-31;

-інтерфейсними по МЕК 1107, 1142 або RS-485 виходами.

ПЗПД (пристрій збору і передачі даних) «Сигма-ZB» призначено для збору електричних імпульсів з приладів обліку, обробки, зберігання та передачі даних в форматованому вигляді по радіоканалу 2,4 ГГц ieee 802.15.4 / специфікація ZigBee. У залежності від інтерфейсного виходу приладів обліку енергоносіїв пристрій «Сигма-ZB» може виконувати функції:

– або власне ПЗПД з процедурами обробки, тарифікації, зберігання даних і їх конвертації в цифровий формат;

– або перетворювача інтерфейсу.

ZigBee-плагіни «Сигма-ZBx» є базовим елементом системи і призначені для виконання функцій обліку, управління та контролю первинними датчиками і пристроями систем збору даних. Модулі мають вбудований годинник реального часу, незалежну пам'ять, автономний блок живлення, керуючий мікроконтроллер, блок керування навантаженням і модуль XBee, що забезпечує формування бездротової персональної мережі відповідно до стандарту ieee802.15.4/ZigBee. Модулі мають два виконання, що відрізняються за живленням:

– Пристрої із зовнішнім живленням змінним струмом напругою ~ 110 - 240V;

– Пристрої з автономним живленням від батарей типу AA напругою 3 - 6V.

Група пристроїв із зовнішнім живленням, у свою чергу, підрозділяється на плагіни, що використовуються для роботи з найпростішими приладами обліку, обладнаними імпульсним виходом по МЕК 62053-31, і виконують роль повнофункціонального ПЗПД (пристрої збору та передачі даних), а також на пристрої, що працюють з багатофункціональними лічильниками, що підтримують обмін за числовим інтерфейсу. Вказані плагіни є інтелектуальними перетворювачами інтерфейсів RS 485, CL - ZigBee. Підтримувана топологія мережі - меш (mesh).

Пристрої збору та передачі даних «Сигма-ZBint» являє собою повнофункціональний пристрій - перетворювач інтерфейсу CL (RS485) / ZigBee, що дозволяє перетворити формовану вимірювальним приладом обліку послідовність форматованих команд в значення наприклад, спожитої енергії, потужності, миттевих виміряних значень, тарифних значень та інших функцій описуваних протоколом приладу, у формат протоколу ZigBee. Структура вимірювального каналу представлена на рис. 4.4. Пристрій має керуючий вихід (12V, 0,5 А) для комутації виконавчого механізму (реле навантаження).

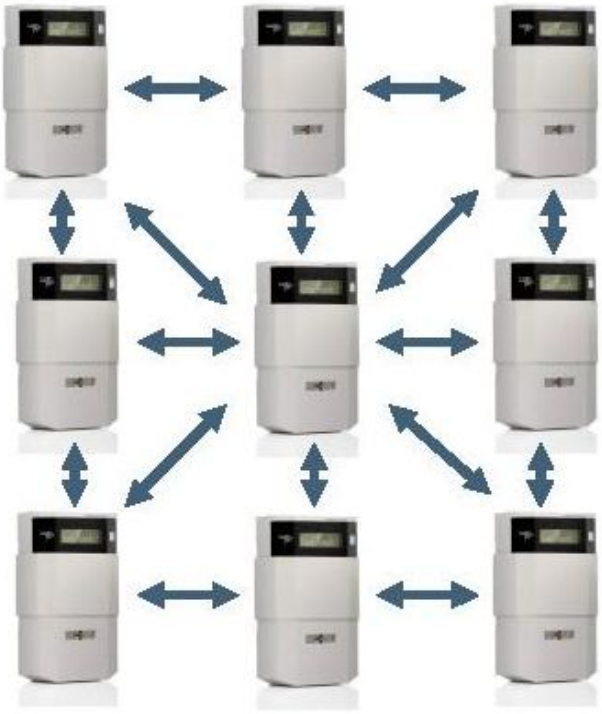
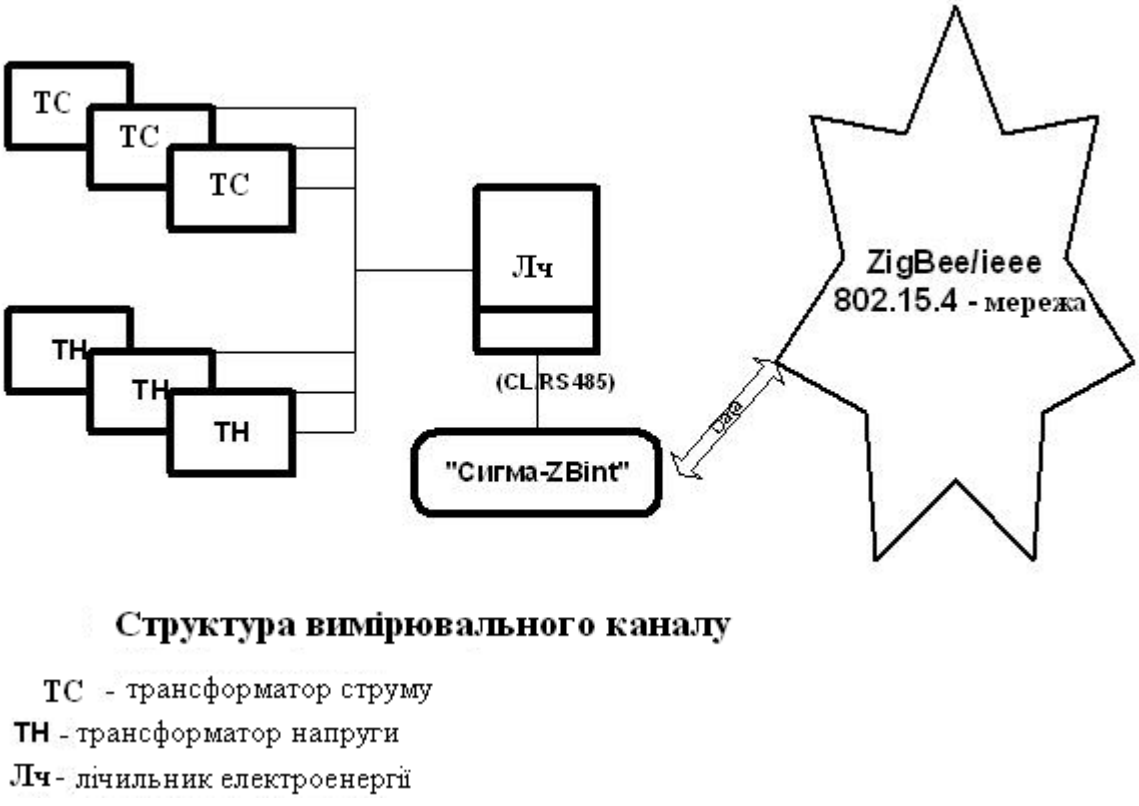


Рисунок 4.3 - Меш-топологія мережі WPAN



Структура вимірювального каналу

ТС - трансформатор струму
ТН - трансформатор напруги
Лч - лічильник електроенергії

Рисунок 4.4 - Вимірювальний канал перетворювача інтерфейсу

CS-вхід перетворювача підтримує такі стандарти і специфікації:

Таблиця 4.1 - Параметри CS - входу

CL	МЭК 61107-2001
CL	МЭК 61142-2001
RS485	EIA RS-485

Таблиця 4.2 - Параметри імпульсних входів S0

Параметри	**Значення параметрів**
Максимальна напруга	27 В (DC)
Максимальний струм у стані " ввімкнено "	27 мА
Мінімальний струм у стані "ввімкнено"	10 мА
Максимальний струм у стані "вимкнено"	1 мА
Константа імпульсів [імп/кВтч, імп/кВарч, імп/кВАч]	від 1 до 65530
Тривалість імпульсів, мс	від 1 до 250
Пауза між імпульсами, мс	від 1 до 250

Крім обліку енергії ПЗПД формує добовий 15,30,60-хвилинний графік навантаження, команди управління силовим реле, контролює мережеву активність ZigBee-мережі.

Плагін «Сигма-W (G) ZB» з автономним живленням призначений для роботи з лічильниками води і газу, обладнаними імпульсним виходом, в енергозберігаючому режимі. Основний час (99,7%) воно знаходиться в сплячому режимі (струм споживання 20 мкА) і прокидається під час вступу імпульсу на будь-який з 2-х входів для його підрахунку і запам'ятовування часу надходження (для входу сигналізації), а також періодично для читання часу. У

визначений розкладом час включається ZigBee модуль, час життя якого продовжується при отриманні будь-якої протокольної команди. Після закінчення цього часу ZigBee модуль відключається і пристрій переходить в сплячий режим. Максимальний час активного режиму на добу становить 5 хвилин. Пристрій має два імпульсних входу, які можуть використовуватися для підключення двох лічильників, наприклад, холодної та гарячої води, або для підключення лічильника та сигналізації. Пристрій також може бути обладнане силовим виходом для управління електро-виконавчим механізмом (електричний привід або клапан). Гарантований термін роботи від батарей - 4 роки. Зовнішній вигляд представлений на рис.4.5.

Рисунок 4.5 - Плагін «Сигма-W (G) ZB» з автономним живленням

Бездротовий адаптер управління навантаженням «ZB-LCU» розроблений на основі пристрою «Сигма-ZBimp» і є його спрощеним варіантом. Адаптер застосовується для віддаленого управління навантаженням побутових споживчих пристроїв (водонагрівач, пральна машина, посудомийна машина і інші потужні споживачі). Адаптер легко інсталюється в домашню мережу ZigBee і управляється як локально, так і дистанційно по мережі Інтернет. Використовується для оптимізації споживання, наприклад, в години максимуму навантаження і для аварійного управління. Загальний вигляд пристрою наведено на рисунку 4.6.

Рисунок 4.6 - ZB-LCU

Розроблено платформа для побудови шлюзу між мережею ZigBee і зовнішнім додатком з використанням прямого TCP / IP, WiMAX, 3G або GSM / gprs з'єднання. У розроблених версіях протоколів ZigBee закріплені механізми створення і розширення однієї персональна мережі PAN, і не розглядаються механізми створення мереж шляхом об'єднання різних PAN. Цю прогалину усунуто на апаратному рівні, що особливо важливо для додатків, що підтримують протокол HART.

IEEE 802.15.4 платформа доступу розроблена для створення користувацьких шлюзів і отримання доступу в мережі, утворені пристроями що підтримують даний стандарт. Дозволяє реалізацію 802.15.4 додатків, що використовують віддалений доступ з різних хост-систем. Можливі різноманітні варіанти підключення до хост-системі. Застосовуються радіомодулі XBee з вихідною потужністю 1, 2, 75, 100 мВт або модулі ServBee-v2.1.1.1R. Платформа дозволяє розширювати діапазон бездротової мережі з використанням дротових і бездротових TCP / IP мереж. (Рис.8). Особливості платформи:

– Зв'язок між собою двох 802.15.4 (у тому числі ZigBee) PAN сегментів разом.

– Підтримка мосту PAN ID1 - PAN ID2.

– Підтримка мосту PAN ID-gprs (GSM), 3G, 4G, WiMAX, Intenet.

– Дистанційне керування і параметризація через веб-інтерфейс.

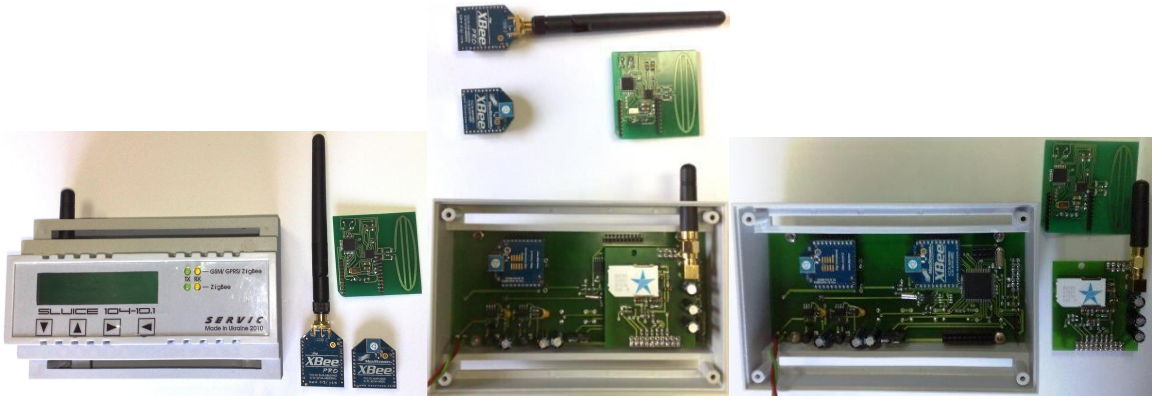


Рисунок 4.7 - Зовнішній вигляд приладу

USB-координатор мережі ieee 802.15.4/ZigBee дозволяє виконувати функції побудови та управління мережею, а також параметризації і зчитування показань з приладів обліку і датчиків,обладнаних пристроями «Сигма-ZBx».

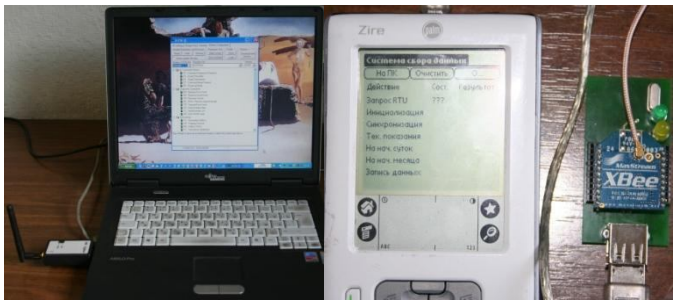


Рисунок 4.8 - Зовнішній вигляд пристрою

Призначений для збору, обробки та передачі вимірювальної інформації в персональних бездротових мережах з подальшою трансляцією цифрової інформації по глобальній мережі Інтернет. Всі вироби підтримують стандартний протокол IEEE 802.15.4 / Zigbee, дозволяє легко інтегрувати в мережу необмежену кількість пристроїв різних виробників.

Варіанти виконання пристроїв:

Прихована установка в приміщенні

Рисунок 4.9 - Модем-координатор

Установка в приміщенні з обмеженим доступом.

Рисунок 4.10 - Модем-координатор

Загальнодоступне місце для візуалізації показань приладів.

Рисунок 4.11 - Модем-координатор

ТЕХНІЧНІ ХАРАКТЕРИСТИКИ

1. Несуча частота -2,4 ГГц.
2. Повна відповідність стандарту IEEE 802.15.4 специфікація ZigBee.
3. Радіус дії в мережі ZigBee:
    - У приміщенні 10 - 40м;
    - На відкритій місцевості 30 - 1200м.
4. Швидкість передачі даних в мережі ZigBee до 115 Кб / с.
5. Джерело живлення: 220В змінного струму, 12В постійного струму.
6. Комунікаційний інтерфейс: GSM / GPRS, 3G, WiMAX.
7. Антенний інтерфейс: SMA.

Рисунок 4.12 - Загальний вигляд пристрою

Призначений для параметризації пристроїв «Сигма-xZBx» на місці установки приладів обліку. Підключення ZigBee-плагінів до автономного інсталлер здійснюється за допомогою інтерфейсного кабелю через роз'єм X1. Тим самим істотно спрощується процес інсталяції та включення пристроїв в мережу ZigBee, відпадає необхідність встановлення зв'язку через координатор мережі, полегшується виконання сервісних функцій обслуговуючим персоналом.

Програмне забезпечення.

«Smart Energy Web-ZB» - представляє собою апаратно-програмні засоби, що дозволяють будувати автоматизовані системи обліку і управління енергоспоживанням як сконцентрованих, так і віддалено розташованих промислових, побутових та дрібномоторних споживачів. Система містить потужні засоби побудови та управління бездротовими мережами (ieee802.15.4, ZigBee), допускає можливість дистанційного додавання нових об'єктів і користувачів, а також віддалену параметризацію приладів обліку.

Можливість інтеграції в Інтернет за допомогою GPRS, 3G, 4G WiMAX або прямого TCP / IP з'єднання істотно знижує вимоги до каналу передачі даних і капітальні витрати на побудову системи збору даних. Використання «Smart Energy Web-ZB» дозволяє добитися безпрецедентного зниження вартості обладнання та робіт з його інсталяції, часу монтажу системи, робіт з технічного обслуговування та експлуатації автоматизованої системи. Енергетичний WEB-сервер («Smart Energy Web-XB») дозволяє не тільки передавати дані про споживаної електроенергії в форматованому вигляді через

Internet, а й керувати підключенням абонентів. Web-сервер регулярно збирає дані з приладів обліку і зберігає їх у базі даних. Web-сервер постійно підключений до інформаційної мережі, і будь-який клієнт, що має доступ, може запросити в нього інформацію або виконати процедуру управління віддаленим об'єктом.

Програмне забезпечення параметризації пристроїв «Сігма-ZBx», «Сигма-xZB» і «Сігма-W (G) ZB» представлено програмами ZTS, SetParam, SCTM-dialog. Це ПЗ дозволяє виконувати функції програмування і управління пристроями, що підтримують специфікацію ZigBee. ZTS і SetParam використовуються локально поблизу встановлених пристроїв за допомогою адаптера «Сігма USB-ZigBee» або налагоджувальної плати комплекту розробника MaxStream. SCTM-dialog є вдосконаленою версією попередніх програм і крім локальної версії, підтримують дистанційну параметризацію і керування пристроями за допомогою прямого GSM / gprs - з'єднання.

Система дистанційного контролю та управління процесами моніторингу «Energy Web-ZB» заснована на передачі показань присторів і сигналів управління за існуючими каналами Інтернет. За допомогою такої системи енергопостачальні або енергосервісні компанії можуть дистанційно вести контрактні взаємини з абонентами, реалізовувати програми управління енергоспоживанням абонентів, надавати їм розширений пакет послуг. Архітектура системи є дворівневою і дозволяє підключати до віддаленого терміналу аналізу та управління необмежене число абонентів.

Система призначена в першу чергу для комунальних, енергопостачальних та енергосервісних організацій, що забезпечують постачання енергоресурсів й оптимізують їх споживання. Файл-сервер забезпечує дистанційний контроль і зчитування показань приладів обліку електричної і теплової енергії, а також газу і води, дистанційно керує всією системою. Двосторонній інформаційний потік містить свідчення обслуговуються лічильників і команди управління. Управління системою здійснюється з будь-якого пристрою, що має вихід в

Інтернет та встановлений веб-браузер. Ядро системи, що забезпечує працездатність системи, складається з основних модулів:

– Контроль та керування системою.
– Додавання абонентів і модулів в базу.
– Управління територіальними довідниками.

У базовий варіант поставки включені «Презентація» і дві звітні форми:

– Звітна форма для житлового сектора.
– Звітна форма для ТП.

Додаткові функції системи, що реалізують її додаткові можливості, реалізовані в програмах:

– Діагностика та аналіз роботи мережі ZigBee.
– Розподіл прав доступу для користувачів.
– Налагоджувальна форма.
– Оператор мереж ZigBee.
– Статистика.
– Контроль і керування сигналізацією.

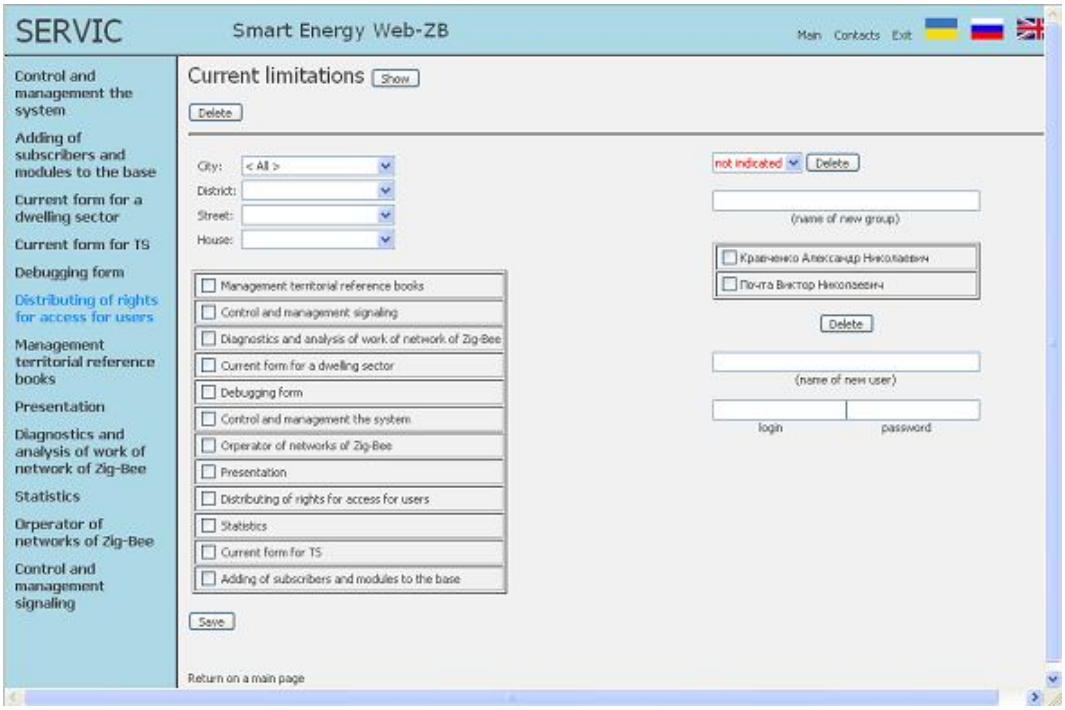


Рисунок 4.13 - Панель керування системою

Особливості системи «Smart Energy Web-ZB» на плагінах ZigBee «Сігма ZB»:

1. Віддалене конфігурування.
2. Ведення графіка навантаження (15, 30, 60хв.)
3. Тарифікація споживання (зонний облік).
4. Ведення астрономічного часу.
5. Кодування інформації та криптографічний захист.
6. Контроль поточного споживання.
7. Індикація поточних значень.
8. IEEE 802.15.4/ZigBee інтерфейс зв'язку із зовнішніми програмами.
9. Прямий доступ до Інтернет, додатковий канал зв'язку - GSM.
10. Стандартні протоколи обміну даними: МЕК 62053-31, 61107-2001, 61142-2001, 62056-21, ANSI C12.19
11. Програмоване обмеження навантаження споживання.
12. Дистанційне керування навантаженням (підключення / відключення). Модем - координатор мережі «Сигма-xZB» дозволяє організувати бездротову ZigBee / RF мережу практично будь-якої конфігурації. Є базовим елементом у побудові «розумної мережі» Smart Grid та організації взаємодії безлічі мереж (HAN). Має двонаправлений інтерфейс і підтримує віддалене параметрування і налаштування по Інтернет.

Принцип роботи заснований на передачі даних з GSM модему на xBee модуль і назад, дозволяє використовувати робочу плату як налагоджувальної. Замість xBee модуля може застосовуватися плата від Test ZigBee counter. Передача даних здійснюється з урахуванням сигналу CTS модуля xBee і GSM модему SIM300D.

Швидкість передачі між контролером і xBee модулем складає 115200 біт / сек. Порядок роботи з модем-координатором Сигма GSM-ZB.

- При включенні харчування, виконується переклад модему в повнофункціональний режим шляхом відсилання модулю SIM300 команди AT + CFUN = 1 через 2 секунди після того, як висновок STATUS модему встановиться в 1.
- При короткочасній установці виведення STATUS в 0, або не отриманні протокольної команди по GSM каналу протягом 60 хвилин (якщо канал GPRS відключений), а так само при відсутності зв'язку з сервером протягом 10 хвилин + 3 паузи, заданої командою G3 (якщо канал GPRS включений) буде виконана перезавантаження модему шляхом відсилання модулю S IM300 команди AT + CPOWD = 0

– GSM-ZigBee автоматично посилає в ZigBee мережа широкомовну команду (у полі адреси 00000) установки часу з паузою між посилками згідно змінної T5.

– Для відправки повідомлення GSM-ZigBee пристрою, в поле адреси повинно бути 00000. При будь-якому іншому адресу, повідомлення буде передано транзитом до ZigBee мережу.

– Для можливості віддаленої відправки широкомовної команди (у полі адреси 00000) в ZigBee мережу, передбачена команда TB (Transfer Broadcasting), після якої, будь-яке надіслане протокольне повідомлення по GSM каналу буде передано в ZigBee мережа (тільки 1 раз!)

– Для можливості місцевого управління ZigBee мережею передбачена команда B0 і B1 (Відключення і включення xBee модуля відповідно). Відключення провадиться шляхом установки виведення RESET xBee модуля в 0.

– GSM-ZigBee постійно, згідно встановленого часу (див. G3), звертається до сервера для отримання від нього команд. Для нормальної роботи, в комплекті з енергозберігаючими пристроями, в 23.57, 0.57,

1.57 і припиняється зв'язок з сервером на 10 хвилин для недопущення затримок, пов'язаних з GPRS.

– GSM-ZigBee постійно по колу перевіряє стан пристроїв сигналізації, згідно переліку адрес (див. функцію MW). При вичитування баз даних (див. далі), перевірка пристроїв сигналізації буде виконана в повному обсязі (згідно переліку адрес) після кожного запиту БД.

– GSM-ZigBee автоматично кожен день на годину ночі (або за запитом - команда DB READ) виробляє вичитування баз даних з ZigBee мережі і зберігати їх у своїй пам'яті. Адреси пристроїв ZigBee мережі можуть бути визначені двома способами:

  - а) автоматично, через команду ATND xBee модуля;
  - б) відповідно до заданого діапазону адрес (команда D5).

У першому випадку будуть витягнуті адреси з Node Identifier всіх видимих в мережі пристроїв (Максимум - 250), а в другому випадку з фіксованого діапазону адрес заданих через дефіс (Наприклад 00007-00123). Фіксований діапазон адрес так само повинен не перевищувати 250, а використовувані адреси можуть бути від 1 до 65535 включно.

Перемикання між режимами здійснюється за допомогою команд D0 і D1. Після отримання БД пристрою та її збереження в незалежній пам'яті, запит БД наступного устрою буде відправлений через 2 секунди. При відсутності (не отриманні) БД, адреси не відповіли пристроїв будуть збережені і після опитування інших адрес, GSM-ZigBee буде опитувати пристрою раніше не повернули БД за запитом. Опитування буде відбуватися до тих пір, поки всі БД не будуть отримані. Отримані БД зберігаються в незалежній пам'яті. Після отримання всіх БД в ZigBee мережа буде відіслана широкорозповсюджувана команда SL02, для переведення в режим зниженого енергоспоживання пристроїв, що працюють у цьому режимі.

Так само автоматично, кожен день в годину ночі, GSM-ZigBee перевіряє стан рахунку і терміну дії SIM карти і збереження результату в

енергонезалежній пам'яті. Для ручної ініціалізації перевірки рахунку застосовується команда SC. Відповідь оператора можна прочитати за допомоги команди S2.

У GSM-ZigBee передбачена можливість отримання і передачі даних по GPRS каналу. Команда G1 включає канал GPRS. У цьому режимі відразу, після отримання БД з ZigBee мережі, відбувається відкидання від отриманої інформації профілю навантаження (крім тих БД, адреси пристроїв яких занесені до списку адрес командою AW) і передача на сервер залишилися даних. Так само GSM-ZigBee буде знаходитися в режимі постійного опитування сервера на наявність команд для виконання.

Для захисту від несанкціонованого доступу до ресурсів даного пристрою передбачена команда CL, яка обмежує роботу модема по GSM каналу. Обмеження будуть введені на можливість зміни будь-яких настроювань GSM-ZigBee, а так само будь-яку передачу даних транзитом до ZigBee мережу. Залишаться доступними команди тільки на читання налаштувань GSM-ZigBee і збережених даних. При спробі виконати інші команди, буде повернуто повідомлення ACCESS DENIED. Зняти блокування для роботи по каналу GSM можна при допомоги команди CU, але відправити на модем її можна буде тільки по каналу GPRS. Виходячи з цього, перед тим, як використовувати команду CL, необхідно переконатися в правильності внесених налаштувань GPRS.

Кожна надійшла команда на GSM-ZigBee буде збережена в енергонезалежній пам'яті. Пам'ять GSM-ZigBee організована сторінками. Розмір сторінок і їх кількість для зберігання баз даних і надійшли команд можна отримати за допомогою команди DI і CI. Так само за допомогою цих команд можна отримати стан GSM-ZigBee (в частині роботи зі збору БД) і кількості прийнятих і не прийнятих БД з моменту початку збору даних, кількості не відправлених на сервер баз даних та стан блокування GSM каналу. Нумерація сторінок для БД та отриманих команд різна.

Читання БД збережених в GSM-ZigBee може бути здійснено чотирма способами:

а) за часом формування БД (місяць і дата в полі даних - 4 байта);

б) за адресою пристрої (у полі даних 5 байт);

в) за адресою і часу (в полі даних 9 байт);

г) за номером сторінки (в полі даних 7 байт).

При відсутності БД з заданими параметрами видається повідомлення - NO DATA BASE Повернення сторінок з БД по GSM каналу може супроводжуватися затримками в кілька секунд, в залежності від обсягу встановленої пам'яті.

Читання команд збережених в GSM-ZigBee може бути здійснено чотирма способами:

а) за часом надходження команди (місяць і дата в полі даних - 4 байта);

б) за адресою призначення (у полі даних 5 байт);

в) за адресою і часу (в полі даних 9 байт);

г) за номером сторінки (в полі даних 3 байт).

При відсутності збереженої команди з заданими параметрами видається повідомлення – NO DATA COMMAND.

Повернення сторінок з командами по GSM каналу може супроводжуватися затримками в кілька секунд, в залежності від обсягу встановленої пам'яті.

При зверненні до xBee модулю в разі його відключення відповідною командою або будь-який інший причиною непрацездатності видається повідомлення - THE MODULE XBEE DOES NOT ANSWER.

Для визначення адрес, видимих в ZigBee мережі координатором, передбачена команда NI, яка повертає перелік адрес - до 30 в одній відповіді по 5 символів на адресу. Якщо не знайдено жодного пристрою, тоді видається повідомлення - DEVICES ARE NOT FOUND

Команда VR повертає версію прошивки GSM-ZigBee.

Передача будь-яких даних від контролера до SIM300 або xBee модулю здійснюється з урахуванням сигналу CTS відповідного модуля. При установці високого рівня сигналу CTS протягом 10 секунд, щоб надіслати повідомлення за відповідним канал у скасовується. При програмуванні контролера автоматично встановлюються параметри (табл. 4.1)

Таблиця 4.1 - Автоматично встановлені параметри контролера

Функція	**Значення**	**Функція**	**Значення**
B2	1	I1	212.3.120.2
C2	0	I3	5115
CU		IW	0
D0		N1	www.kyivstar.net
D5	00001 - 00001	R1	00000
Last page DB	0	S1	* 111 #
Last page DC	0	T3	+0000000
No Send DB	0	T5	0001
GPRS	OFF	U1	115200
G3	060	U3	8N
G6			

Таблиця 4.2 - Функції модем-координатора Сигма GSM-ZB

Функція	**Опис**	**Поле**	**Поле даних відповіді, байт**	**Одиниці вимірювань**
AT	Передача команди xBee модулю	ні	Не визначено	
AC	Видалення адреси зі списку адрес, які повертаються БД з	5	-	
AW	Запис адреси в список адрес, що повертаються БД з профілем	5	-	

Продовження таблиці 4.2

AV	Перевірка адреси у списку адрес, які повертаються БД знавантаження	5	1	0 або 1
B0	Відключення xBee модуля	_		
B1	Включення xBee модуля	-	-	
B2	Читання стану підключення xBee модуля	-	1	0 або 1
C0	Відключення режиму налагодження	-	-	
C1	Включення режиму налагодження (передача отриманих даних)	-	-	
C2	Читання стану режиму налагодження	-	1	0,1 або 3
C3	Вмикання. режиму налагодження		_	
CI	Читання інформації про отримувані командах і їхні бази	-	Не визначено	
CL	Включення блокування виконання команд	-	-	
CU	Розблокувати виконання команд отриманих	-	-	
D0	Відключення режиму авто визначення пристроїв	-	-	
D1	Включення режиму авто визначення пристроїв	-	-	
D5	Установка діапазону адрес для скачування БД	11	-	
DB (4)	Читання БД всіх сторінок з вказаною датою	4	Не визначено	
DB (5)	Читання БД всіх сторінок з вказаною адресою	5	Не визначено	

Продовження таблиці 4.2

DB (7)	Читання БД однієї сторінки з вказаним номером	7	Не визначено	
DB (9)	Читання БД однієї сторінки з вказаною адресою і датою	9	Не визначено	
DBERASE	Стирання пам'яті з базами даних	5	Не визначено	%
DBREAD	Ініціалізація початку читання БД абонентів за ZigBee мережі	4	–	
DBSTOP	Зупинка читання БД абонентів за ZigBee мережі	4	-	
DC (3)	Читання однієї збереженої команди з вказаним номером	3	Не визначено	
DC (4)	Читання всіх збер. команд із зазначеною датою надходження	4	Не визначено	
DC (5)	Читання всіх збер. команд з вказаною адресою одержувача	5	Не визначено	
DC (9)	Читання всіх збер. команд з вказаною адресою одержувача та	9	Не визначено	
DQ (3)	Читання однієї команди з вказаним номером сторінки	3	Не визначено	
DQ (4)	Читання всіх команд із зазначеною датою надходження в черзі	4	Не визначено	
DQ (5)	Читання всіх команд з вказаною адресою у черзі команд	5	Не визначено	
DQ (9)	Читання всіх команд з вказаною адресою і датою надходження	9	Не визначено	
DI	Читання інф. про розмір устан. пам'яті	-	Не визначено	
G0	Відключення каналу GPRS	-	-	
G1	Включення каналу GPRS	-	-	
G3	Установка паузи між запитами по каналу GPRS	3		сек.
G5	Включення перевірки підтвердження відправки рядка на сервер	-	-	
G6	Вимкнення перевірки підтвердження відправки рядка	-	-	
GC	Пошук команди для запитуваної пристрою в пам'яті	-	Не визначено	
GI	Читання повної інф. про налаштування GPRS і GSM	-	Не визначено	
I1	Установка IP сервера	<=16	-	
I3	Установка номера порта сервера	<=8		
IW	Установка ідентифікатора модему	<=8	-	
MC	Видалення адреси зі списку адрес	5	-	

Продовження таблиці 4.2

MW	Запис адреси в список адрес, контрольованих сигналізацією	5	-	
MR	Читання списку адрес, контрольованих сигналізацією	-	<= 301	
N1	Установка точки входу (PN)	<=32	-	
NI	Читання переліку адрес всіх видимих в ZigBee мережі об'єктів	-	Не визначено	
QC	Видалення всіх кім. із зазначеним адр. і функцією з параметрами	Ні	Не визначено	
QD (3)	Видалення однієї команди з вказаним номером сторінки	3	-	
QD (4)	Видалення всіх команд із зазначеною датою надходження	4	Не визначено	
QD (5)	Видалення всіх команд з вказаною адресою у черзі команд	5	Не визначено	
QD (9)	Видалення всіх команд з вказаною адресою і датою	9	Не визначено	
R0	Обнулення лічильника скидання	_	_	
R1	Читання лічильника скидання	-	20	
RC	Перезавантаження контролера	-	-	
S1	Установлення телефонного номера для перевірки рахунку	<=8	-	
S2	Читання стану рахунку	-	<= 128	
SC	Ініціалізація дзвінка для перевірки стану рахунку	-	-	
SR	Передача команди модулю SIM300 з розривом зв'язку	Ні	-	
SW	Передача команди модулю SIM300 без розриву зв'язку	Ні	Не визначено	
T0	Читання часу	-	14	г.м.д.ч.м
T1	Встановлення часу	14	-	г.м.д.ч.м
T2	Читання паузи на підгонку годин на 1 секунду	-	8	сек.
T3	Установка паузи на підгонку годин на 1 секунду	8	-	сек.
T4	Читання періоду відправки широкомовної команди	-	4	хв.
T5	Установка періоду відправки широкомовної команди	4	-	хв.
TB	Встановлення прапора для передачі слід. одного повідомлення на xBee	-	-	
U1	Установка швидкості передачі US RT для xBee модуля	Ні	-	Біт / сек

Продовження таблиці 4.2

Установлення формату кадру US RT для xBee модуля	2	-	8N або
Читання інформації про налаштування US RT xBee модуля	-	Не визначено	
Читання версії прошивки	-	Не визначено	

Опис функцій

AT - передача команди xBee модулю (вхід в командний режим). Поля даних запиту і відповіді невизначені.

AC - видалення зі списку, а адрес, які повертаються БД з профілем навантаження. Поле даних відповіді відсутня. Поле даних запиту:

AAAA, де AAAA - видаляється адресу зі списку адрес.

AW - запис адреси в список адрес, що повертаються БД з профілем навантаження. Ост е виконання даної команди, всі відповіді на які надходять запити (з даними адресою) з читання БД будуть віз обертатися з профілем навантаження. Дана команда поширює ся і на щоденну автоматичну передачу БД, але не має впливу на транзитні запити в ZigBee мережу.

AV - перевірки а адреси в списку адрес, повернених БД з профілем навантаження. Формат поля даних запиту див. AC.

Поле даних відповіді:

– N, м де N - якщо 1, то адреса є у списку адрес, а якщо 0 - то відсутня.

– BO - відключення xBee модуля. Поле даних запиту і відповіді відсутня. B1 - включення xBee модуля. Поле даних запиту і відповіді відсутня.

– B2 - читання стану підключення xBee модуля. Поле даних запиту відсутня.

Формат поля даних відповіді:

– N, м де N - якщо 1, то модуль включений, а якщо 0 - то вимкнений.

– CO - відключення режиму відладки. Поле даних запиту і відповіді відсутня.

– C1 - включення режиму відладки. У цьому режимі дані, отримані від модему, передаються на xBee модуль. Поле даних запиту і відповіді відсутня.

– C2 - читання стану режиму відладки.

– N = 0 - режим відладки відключений

– N = 1 - включений режим налагодження

– N = 3 - включений режимналагодження

– 3C3 - ввімкнення режиму відладки.

У цьому режимі дані, отримані від модему, передаються на xBee модуль, а отримані від xBee модуля передаються на модем. Поле даних запиту і відповіді відсутня. CI - читання інформації про стать учаемих до омандах та їх бази. Поле даних запиту відсутня.

CL - включення блокування виконання команд отриманих за допомогою GSM. Після виконання даної команди, все що надійшли команди по канал у GSM не будуть працювати, крім деяких не критичних команд читання і включення канала GPRS. Перед тим, як використовувати дану до команду необхідно переконатися в правильності внесених налаштувань GPRS. Поле даних запиту і відповіді відсутня.

CU - вимикання блокування виконання команд підлогу вчених з GSM. Поле даних запиту і відповіді відсутня.

D0 - відключення режиму авто визначення адрес пристроїв в ZigBee мережі для завантаження та збереження баз даних. У даному режимі адреси будуть визначатися згідно заданого діапазону функцією D 5. Поле даних запиту і відповіді відсутня.

D1 - включення режиму авто визначення адрес пристроїв в ZigBee мережі для завантаження та збереження баз даних. У даному режимі адреси будуть визначені через до команду ATND координатора GSM-ZigBee. Максимально можливе кількість адрес - 250. Поле даних запиту і відповіді відсутня.

D5 - встановити діапазон адрес пристроїв в ZigBee мережі для скачування і збереження баз даних. Формат поля даних запиту:

SSSSS-EEEEE, де

SSSSS - початковий адресу

EEEEE - кінцевий адресу

DB - читання всіх збережених БД із зазначеними місяцем і датою формування

даної бази в кінцевому пристрої ZigBee мережі. Поле даних запиту:

ММДД, де

ММ - місяць DD – дата

Формат поля даних відповіді не визначений.

Rev.1.1 -2010

DB - читання всіх збережених БД із зазначеними адресою кінцевого пристрою ZigBee мережі.

ВИСНОВКИ

У роботі *сформульовано* рекомендації щодо використання сучасних педагогічних технологій та методик підготовки фахівців вищих технічних заходів наукоємних спеціальностей. *Встановлено* пріоритетні побажання студентів вечірньої форми навчання щодо складових інформаційної Інтернет-підтримки дисциплін, що вивчаються. *Запропоновано* структуру та інтерфейс шаблону закритої частини портального рішення науково-освітнього забезпечення студентів вищого технічного закладу. *Розроблено* алгоритм дій при створенні шаблонів сторінок закритої частити порталу для різних категорій користувачів згідно визначених повноважень на базі новітніх програмних продуктів Microsoft.

Зазначено, що розподіл структури порталу на інформаційно-незалежні частини (відкриту та закриту) полегшує процеси пошуку потрібної інформації різними категоріями користувачів, зменшує їх витрати часу й спрощує процедуру формулювання вимог до шаблонів інформаційних сторінок різного функціонального призначення.

Сформульовано вимоги до програмного забезпечення, що використовується при реалізації сучасних педагогічних технологій при підготовці фахівців наукоємних спеціальностей у вищих технічних університетах. Наведено перелік етапів щодо підготовки до проведення лекції:

- правильно формулювати цілі читаного курсу, лекції, фрагмента лекції;
- відбирати і структурувати учбовий матеріал, відповідний цілям заняття з урахуванням особливостей конкретної аудиторії тих, що навчаються; готувати якісні демонстраційні матеріали, включаючи мультимедійні, складати тексти лекцій і викладати матеріал коротко і зрозуміло;
- оцінювати адресатів, які повинні засвоїти учбовий матеріал. Ця оцінка повинна охоплювати не лише оцінку рівня їх знань але і облік психологічних і соціальних особливостей тих, що навчаються;

- вибирати технічні засоби навчання, відповідні цілям і завданням навчання, грамотно використовувати їх в учбовому процесі;
- вибирати методи навчання, що дозволяють найефективніше досягати намічених цілей;
- правильно організовувати контроль знань, умінь і навичок тих, що навчаються на усіх етапах учбового процесу, включаючи підготовку матеріалів для здійснення контролю і проведення аналізу ефективності занять;
- вибирати методи навчання, що дозволяють найефективніше досягати намічених цілей;
- правильно організовувати контроль знань, умінь і навичок тих, що навчаються на усіх етапах учбового процесу, включаючи підготовку матеріалів для здійснення контролю і проведення аналізу ефективності занять;
- користуватися технологіями створення учбових мультимедійних матеріалів.

Обґрунтована рекомендація по впровадженню методик використання засобів віддаленого доступу й контролю у практиці підготовки фахівців наукоємних спеціальностей у вищому технічному університеті.

Сформульовано рекомендації по використанню програмно-апаратних комплексів (ZigBee) віддаленого контролю та моніторингу освітньо-наукових та технологічних процесів у підготовці фахівців наукоємних спеціальностей в технічних університетах.

ПЕРЕЛІК ПОСИЛАНЬ

1. «Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ТЗІ-ПЕМВН-95)» (затверджені наказом ДСТЗІ від 09.06.1995 №25, чинні від 01.07.1995).

2. «Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітним випромінювань і наводок (ТР ЕОТ-95)» (затверджені наказом ДСТЗІ від 09.06.1995 №25, чинні від 01.07.1995);

3. IEEE TG 15.4. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE standard for Information Technology, IEEE-SA Standards Board, 2003.

4. Kyznetsov G. Pridneprovsk Regional Higher Educational Information Systems And Networks / G. Kyznetsov, O. Azukovskiy, T. Kalugna // Proceeding “Forum on Higher Education”. Congress of the Black Sea Universities Network. April 2-5 2008. – Kyiv, 2008. – 132 p. P – 96-97.

5. Microsoft Office Communicator 2005: http://www.microsoft.com/livecomm

6. Microsoft® Office Live Communications Server: http://www.microsoft.com/livecomm

7. Microsoft® Office System: http://www.microsoft.com/office/system

8. Microsoft® Windows Server: http://www.microsoft.com/windowsserversystem

9. Microsoft® Windows SharePoint Services и Microsoft® Office SharePoint Portal Server: http://www.microsoft.com/sharepoint

10. ZigBee Specification. ZigBee Alliance, 2006.

11. Алексеев Н. Г. Формирование осознанного решения учебной задачи //Педагогика и логика. —М.: Касталь, 1993.—С.385

12. Андрей Андрющенко. Цели и назначение ИБ. Политика ИБ. http://www.security.ukrnet.net/userinfo.php?uid=4

13. Г.В. Кузнецов / Інформаційна технологія «GRID» - можливості, розвиток і використання// Кузнецов Г.В., Азюковський О.О., Єфімєнко А.А. // Збірник наукових праць Національного гірничого університету, № 33, Т 2, - Дніпропетровськ: РВК НГУ, 2009.-312с. стор. 55-60

14. Г.В. Кузнецов / Підвищення рівня індивідуалізації освітніх процесів як елемент реалізації стратегії розвитку освіти. Кузнецов Г.В., Пазиніч Ю.М. Асєєв О.І., Пірожніков О.В.// Міжнародна науково-практична конференція «Релігія, релігійність, філософія та гуманітарні знання у сучасному інформаційному просторі: національні та інтернаціональні аспекти», 21-23 грудня 2010 року, Східноукраїнський національний університет імені Володимира Даля – м. Луганськ.

15. Г.В. Кузнецов / Портальне рішення дистанційного доступу до освітньо-наукового контенту вищого навчального закладу. Кузнецов Г.В., Азюковський О.О. // Праці Міжнародної наукової конференції «Традиції та інновації в науці та освіті XXI століття» (Південноукраїнський національний педагогічний університет імені К.Д. Ушинського) Одесса, 2010 р. С. 137-139.

16. Г.В. Кузнецов / Сучасні інформаційно-комунікативні технології як складова розвитку вищої освіти України. Кузнецов Г.В., Пазиніч Ю.М., Азюковський О.О. // Матеріали V Всеукраїнської науково-методичної конференції «Безперервна освіта: реалії та перспективи», 28-30 жовтня 2010 року. – Івано-Франківськ: ІФНТУНГ, 2010.

17. Г.В. Кузнецов /Особистісний підхід у вищій освіті на основі впровадження у освітній процес сучасних інформаційно-комунікаційних технологій. Кузнецов Г.В., Азюковський О.О. // Всеукраїнські педагогічні читання «Гуманна педагогіка у вищій школі» - Д.: Національний гірничий університет, 2010 – 88с.

18. Г.В. Кузнецов /Системи колективної роботи у навчальному процесі. Кузнецов Г.В., Пазиніч Ю.М. Азюковський О.О. Пірожніков О.В.// Вища освіта України Додаток 4, том 4 (22), 2010 р.- Тематичний випуск «Вища освіта України у контексті інтеграції до європейського освітнього простору» - 516 с.

19. ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення» (затверджений наказом Держстандарту України від 11.10.1996 №423, чинний від 01.01.1997);

20. ДСТУ 3396.1-96 «Захист інформації. Технічний захист інформації. Порядок проведення робіт» (затверджений наказом Держстандарту України від 19.12.1996 №511, чинний від 01.07.1997);

21. Закон України «Про захист інформації в автоматизованих системах» (від 05.07.1994 №80/94-ВР, в редакції Закону від 31.05.2005 №2594-IV);

22. И. Роберт Современные информационные технологии в образовании: дидактические проблемы; перспективы использования / Роберт И.// Москва "Школа-Пресс" 1994. – 55с.

23. Калюжна Т.М. Теоретико-методичні засади формування освітнього порталу / Т.М.Калюжна, О.О.Азюковський, О.М.Долгов // Вища освіта України. Додаток 3. том 2. Тематичний випуск «Вища освіта України у контексті інтеграції до Європейського освітнього простору». 2006.- С.204-209.

24. Картузов А.В. Вопросы профессиональной подготовки педагогов в области ИТ-управления учебным процессом / А.В. Картузов // Тезисы докладов 3-ей международной конференции «Функциональные пространства. Дифференциальные операторы. Общая топология. Проблемы математического образования», посв. 85-летию Л.Д. Кудрявцева.- М.: МФТИ, 2008.- С. 769-770.

25. Картузов А.В. Информационная система управления учебным процессом / Андреев В.В., Картузов А.В. / Информационные технологии глобального информационного общества, Тезисы докладов 6-й ежегодной международной научно-практической конференции, Казань, 4-5 сентября 2008 г., Казань: ООО «Центр оперативной печати», 2008.- С. 244-245.

26. Картузов А.В. Методика профессиональной подготовки специалиста в области применения информационных технологий для управления учебным процессом. Монография.- Чебоксары: ЧКИ РУК, 2007.– 292 с.

27. Климанов В. П., Солдатов А. В. Комплексная модель эффективности процессов жизненного цикла продукции // 4-я Всероссийская научно-

практическая конференция "Информационные технологии в управлении и учебном процессе вуза": Тез. докл. Владивосток, 2003.

28. Кузнецов Г. В. Соціально-педагогічні аспекти впливу інформаційно-комунікаційних технологій на якість безперервної фахової освіти / Г. В. Кузнецов, О. М. Долгов, Т. М. Калюжна // Збірник наукових праць Національної академії прикордонних військ України (педагогічні науки). – Хмельницький: 2006 – №36

29. Кузнецов Г. В. Сучасні інформаційно-комунікаційні технології як складова розвитку вищої освіти / Г. В. Кузнецов, Ю. М. Пазиніч, О. О. Азюковський // Науковий вісник НПУ ім. М. Драгоманова. – 2010

30. Кузнецов Г. В. Теоретико-методологічні засади формування освітнього порталу / // Вища освіта України. – 2006. – 2 Том (додаток 3)

31. Кузнецов Г. Портальне рішення дистанційного доступу до освітньо-наукового контенту вищого навчального закладу / Г.В. Кузнецов, О.О. Азюковський // Праці Міжнародної наукової конференції «Традиції та інновації в науці та освіті XXI століття» (Південноукраїнський національний педагогічний університет імені К.Д. Ушинського) Одесса, 2010 р.

32. Кузнецов Г.В. Сучасні інформаційно-комунікативні технології як складова розвитку вищої освіти України / Кузнецов Г.В., Пазиніч Ю.М., Азюковський О.О. // Матеріали V Всеукраїнської науково-методичної конференції «Безперервна освіта: реалії та перспективи», 28-30 жовтня 2010 року. – Івано-Франківськ: ІФНТУНГ, 2010.

33. Г.В. Кузнецов / Удосконалення можливостей використання науково-освітнього порталу та засобів мобільного зв’язку у технічному університеті. Кузнецов Г.В., Козлакова Г.О.// Вища освіта України: теоретичний та науково-практичний часопис / [за ред. В.І. Лугового, М.Ф. Степка] – К.: ; Запоріжжя: Класичний приватний університет, 2010 «1. – Тематичний випуск: «Наука і вища освіта: технології взаємодії». – 284с.

34. Кулагин В. Основные тенденции модернизации управления в сфере высшего образования // Высшее образование в России. – 2007. – № 3. – С. 156–164.

35. Максим М. Безопасность беспроводных сетей / Мерит Максим, Дэвид Полино; Пер. с англ. Семенова А.В. – М.: Компания АйТи; ДМК Пресс, 2004.-288с.

36. Максим Филиппов. «Вопросы обеспечения безопасности корпоративных беспроводных сетей стандарта 802.11.» http://www.osp.ru/os/2003/07/

37. Марат Давлетханов «Безопасность GPRS» http://infobez.ru/article.asp?ob_no=1740

38. Матеріал Wiki: http://uk.wikipedia.org/wiki

39. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» (затверджений наказом ДСТСЗІ СБ України від 28.04.1999 №22, чинний від 01.07.1999);

40. НД ТЗІ 1.6-003-04 «Створення комплексів технічного захисту інформації на об'єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації»;

41. О.О. Азюковський / Система автоматичного керування електротехнічними комплексами електрохімічного захисту від корозії. Азюковський О.О. // Міжнародна науково-практична конференція «Реалізація принципів Болонського процесу при підготовці фахівців і розвитку наукових досліджень у галузі електроенергетики та інформаційних технологій» 03 грудня 2010 року Дніпропетровськ, НГУ

42. Овчарук О. Тенденції інформатизації освіти й використання ІКТ для поліпшення якості освіти // Шлях освіти. – 2007. – № 2. – С. 19–22.

43. Пазиніч Ю.М. Світоглядні та організаційні засади реформування сучасної вищої освіти в Україні // Вища освіта України у контексті інтеграції до європейського освітнього простору / Теоретичний та науково-методичний часопис. Додаток 3. Том 1. – К., 2008 - С.317-322.

44. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб

45. Положення про технічний захист інформації в Україні

46. Развертывание и технические ресурсы для Microsoft® Office Live Communications Server: http://office.microsoft.com/en-us/FX011450741033.aspx

47. Рошан Педжман, Лиэри Джонатан. Основы постороения беспроводных локальных сетей стандарта 802.11. : Пер. с англ. - М.: Издательский дом «Вильямс», 2004. – 304 с.

48. С.В. Кавун, Г.В. Шубина. «Методика построения политики безопасности организации» УДК 681.3. Харьковский университет Воздушных сил., г. Харьков

49. Служба Public IM Connectivity для Live Communications Server 2005: http://www.microsoft.com/office/livecomm/prodinfo/publicim.mspx

50. Солдатов А. В. Эффективное управление ресурсами вуза в сфере образовательной деятельности // Международный форум информатизации - 2002: Доклады международной конференции "Информационные средства и технологии". 15-18 октября 2002 г.: В 3 т. Т. 1. М.: Янус-К, 2002.

51. Соломенцев Ю. М., Позднеев Б. М., Солдатов А. В. Эффективное управление ресурсами вуза // Информационно-коммуникационные технологии в управлении вузом: Материалы Всерос. науч.-практ. конф. 25-28 февр. 2003 г. / ПетрГУ. Петрозаводск, 2003.

52. Телекоммуникации. Руководство для начинающих. / Авторы: Мур М., Притеки Т., Риггс К., Сауфвик П. — СПб.: БХВ-Петербург, 2005. - 624 с.: ил.

53. Флоров С. Технологія побудови інформаційного науково-освітнього порталу вищого навчального закладу / С. Флоров, А. Старіков, Г. Кузнецов, Т. Калюжна // Праці Міжнародної наукової конференції «Досягнення та перспективи розвитку інформаційного суспільства в Україні» (Ганновер, Німеччина, CeBIT-2006). Спеціалізований додаток до загальногалузевого науково-виробничого журналу «Зв'язок» - К.:2006. – С. 64-74.

ВИТЯГ З ПРОТОКОЛУ № 4

засідання кафедри електроніки та обчислювальної техніки
Державного вищого навчального закладу «Національний гірничий університет»

м. Дніпропетровськ «19» жовтня 2010 р.

ПРИСУТНІ: завідувач кафедри професор Кузнецов Г.В., заступник завідувача кафедри доцент Корнієнко В.І., доценти кафедри: Галушко О.М., Школа М.І., Гусєв О.Ю., Куваєв Я.Г.; старші викладачі: Войцех С.І., Галушко С.О., Жукова О.А., Кручінін О.В., Тимофєєв Д.С., Святошенко В.О., Саксонов Г.М., Білий В.І.; асистенти: Гуліна І.Г., Мартиненко А.А., Рибальченко Ю.П., Соснін К.В., Баранов А.А., Мешков В.І., Пивоварова О.В., Начовний І.І., Нікітюк Є.О., Лізунова Т.Л., Сєчкін І.А., Пірожніков О.В., Потихенченко С.М., Притула Н.В.

СЛУХАЛИ: доповідь керівника теми ГП-428 кафедри електроніки та обчислювальної техніки професора Кузнецова Г. В. про виконання науково-дослідної роботи ГП-428 «Мобільні системи віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень» у 2010 році, етап 2 «Дослідження, розробка та впровадження технологій використання сучасних педагогічних підходів й методів при підготовці фахівців наукоємних спеціальностей за допомогою мобільних систем віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень». Доповідач виклав основні результати роботи по темі ГП-428 та повідомив, що робота виконана у повному обсязі згідно з календарним планом та технічним завданням.

Основними результатами роботи є:

- рекомендації щодо використання сучасних педагогічних технологій та методик підготовки фахівців вищих технічних заходів наукоємних спеціальностей;

- вимоги до програмного забезпечення, що використовується при реалізації сучасних педагогічних технологій при підготовці фахівців у вищих технічних університетах;
- обґрунтована рекомендація по впровадженню методик використання засобів віддаленого доступу й контролю у практиці підготовки фахівців наукоємних спеціальностей у вищому технічному університеті;
- рекомендації по використанню програмно-апаратних комплексів віддаленого контролю та моніторингу (ZigBee) освітньо-наукових та технічних процесів у підготовці фахівців.

ВИСТУПИЛИ: доценти – Школа М.І., Галушко О.М., старші викладачі – Кручінін О.В., Тимофєєв Д.С., Саксонов Г.М., Войцех С.І., які позитивно оцінили результати виконаної роботи за заключний етап, а також відзначили, що результати роботи відповідають вимогам технічного завдання.

Виступаючі рекомендували заключний звіт з НДР ГП-428 за 2010 рік затвердити.

ВИРІШИЛИ:

1. Робота виконана у повному обсязі згідно з календарним планом та технічним завданням.
2. Робота є актуальною, її науково-технічний рівень відповідає сучасному рівню науки, техніки та технологій, робота має теоретичне та практичне значення.
3. Звіт не містить відомостей, що можуть бути віднесені до винаходу або відкриття, а також відомостей, що становлять державну таємницю.
4. Заключний звіт з НДР ГП-428 ухвалити та рекомендувати до затвердження.

Завідувач кафедри електроніки та обчислювальної техніки д.т.н., професор — **Г. В. Кузнецов**

Секретар, ст. викладач — **С. О. Галушко**

ВИТЯГ З ПРОТОКОЛУ №2
засідання секції **«Інформаційні та телекомунікаційні системи»**
науково-технічної ради Національного гірничого університету

м. Дніпропетровськ «10» грудня 2010 р.

ПРИСУТНІ: голова секції – д.т.н., професор Кузнецов Г.В., заступник голови секції – д.т.н., професор Бусигін Б.С., к.т.н., професор Алексєєв М.О., д.т.н., професор Слєсарєв В.В., д.т.н., професор Ткачов В.В., асистент Іванов О.М.

СЛУХАЛИ: доповідь наукового керівника теми ГП-428 «Мобільні системи віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень» (етап 1 – «Розробка, наукове обґрунтування методики використання віддаленого моніторингу стану об'єктів на основі web-орієнтованих технологій та інтрамережі вищого технічного навчального закладу», етап 2 – «Дослідження, розробка та впровадження технологій використання сучасних педагогічних підходів й методів при підготовці фахівців наукоємних спеціальностей за допомогою мобільних систем віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень») завідувача кафедри електроніки та обчислювальної техніки професора Кузнецова Г.В. про виконану роботу по темі ГП-428 та основні положення заключного звіту НДР.

Доповідач відзначив, що робота виконана у повному обсязі згідно з технічним завданням та календарним планом. За результатами роботи всього опубліковано 8 наукових праць, у тому числі у 2010 році – 7 наукових праць.

ВИСТУПИЛИ: професор Бусигін Б.С., професор Алексєєв М.О., професор Ткачов В.В., які дали позитивну оцінку результатам виконаної роботи по темі ГП-428, відзначили, що робота виконана у повному обсязі згідно з календарним планом та технічним завданням. Виступаючі відзначили актуальність роботи, а також те, що результати роботи мають теоретичне та практичне значення, а їх науково-технічний рівень відповідає сучасному рівню вітчизняних і світових розробок. Виступаючі рекомендували заключний звіт НДР ГП-428 затвердити.

ВИРІШИЛИ:

1. Робота по темі ГП-428 виконана у повному обсязі згідно з календарним планом та технічним завданням.
2. Результати роботи по темі ГП-428 є актуальними, їх науково-технічний рівень відповідає сучасному рівню науки, техніки та технологій. Ці результати мають теоретичне та практичне значення.
3. Звіт по темам ГП-428 не містять відомостей, що можуть бути віднесені до винаходу або відкриття, а також відомостей, що становлять державну таємницю.
4. Заключний звіт НДР ГП-428 ухвалити та рекомендувати до затвердження.

Голова секції,
д.т.н., професор Г.В. Кузнецов

Вчений секретар секції О.М. Іванов

Р Е Ц Е Н З І Я

на звіт по науково-дослідній роботі ГП-428

МОБІЛЬНІ СИСТЕМИ ВІДДАЛЕНОГО МОНІТОРИНГУ, УПРАВЛІННЯ Й ПЛАНУВАННЯ ВИРОБНИЧИМИ Й НАУКОВО-ОСВІТНІМИ ПРОЦЕСАМИ НА ОСНОВІ ПОРТАЛЬНИХ РІШЕНЬ

Етап 2, заключний (2010рік)
«Дослідження, розробка та впровадження технологій використання сучасних педагогічних підходів й методів при підготовці фахівців наукоємних спеціальностей за допомогою мобільних систем віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень»

Робота, що рецензується, проведена у 2010 році, та спрямована на підвищення ефективності управління і планування виробничими, науково-освітніми і бізнес – процесами шляхом створення та впровадження багатофункціональних моніторингових систем з можливістю організації каналів передачі даних між віддаленими об'єктами засобами мобільного зв'язку.

Основні результати науково-дослідної роботи по темі ГП-428:

- рекомендації щодо використання сучасних педагогічних технологій та методик підготовки фахівців;
- вимоги до програмного забезпечення, що використовується при реалізації сучасних педагогічних технологій при підготовці фахівців;
- рекомендація по впровадженню методик використання засобів віддаленого доступу й контролю у практиці підготовки фахівців наукоємних спеціальностей у вищому технічному університеті;
- рекомендації по використанню програмно-апаратних комплексів віддаленого контролю та моніторингу освітньо-наукових процесів та параметрів технологічний процесів у підготовці фахівців.

Отримані результати містять наукову та практичну складові й можуть бути використаними під час розробки, проектування та розгортання мобільних

систем віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень.

Використання платформи SharePoint Server 2007 при створенні системи інформаційного забезпечення процесів різного призначення дозволяє прискорити інформаційний обмін при одночасному підвищенні якості управлінських рішень. Це досягається внаслідок своєчасного забезпечення користувачів необхідним інформаційним ресурсом з актуальним по відношенню до поточної ситуації контентом.

Використання технології спрощення процесів розміщення інформаційних ресурсів у Web значно зменшує час звернення інформаційних потоків, які є особливо актуальними для організацій, працюючих з великими об'ємами інформації. Наявність "єдиної точки входу" доступність до якої зумовлюється тільки можливістю підключення до Web, значно розширює інструментарій як управлінського, так і обслуговуючого персоналу що також сприяє поліпшенню показників режимів роботи будь-яких систем та організаційних структур (освітніх, виробничих, наукових тощо).

Використання модему-координатора Сигма GSM-ZB розробленого для організації віддаленого дистанційного управління пристроями, що підтримують специфікацію ZigBee і являє собою міст між мережами ZigBee і GSM / GPRS надає практично будь який інформаційній системі моніторингу параметрів процесів потрібне інформаційне насичення вектору стану.

Р е ц е н з е н т
докт. техн. наук,
професор **В.В. Слєсарєв**

ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД «НАЦІОНАЛЬНИЙ ГІРНИЧИЙ УНІВЕРСИТЕТ» КАНЦЕЛЯРІЯ

Підпис Слєсарєва В.В.
Зав. канцелярією
20 12 2010

«З А Т В Е Р Д Ж У Ю»

«06» грудня 2010

П е р ш и й п р о р е к т о р
Державного вищого навчального закладу
«Національний гірничий університет»,
д.т.н., професор **П.І. Пілов**

А К Т В П Р О В А Д Ж Е Н Н Я

результатів науково-дослідної роботи
«**Мобільні системи віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень**»
(тема ГП-428)

Результати досліджень, що отримані у межах виконання науково-дослідної роботи «Мобільні системи віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень» впроваджені у Міжгалузевому інституті безперервної освіти Національного гірничого університету при організації навчального процесу шляхом інтегрування наукового порталу (http://mibo.nmu.org.ua) до процесів інформаційного забезпечення в системі екстернатної підготовки фахівців, довузівської підготовки та підготовки за вечірньою формою. Результати наукового аналізу організаційно-педагогічних умов застосування системи віддаленого моніторингу, управління й планування виробничими й науково-освітніми процесами на основі портальних рішень у поєднанні з рівнем розповсюдженості сучасних інформаційно-комунікаційних технологій, їх впливом на ритми повсякденного життя підтверджують актуальність дослідження.

Доступність окремих складових інформаційно-комунікаційних систем, що вже існують у Державному ВНЗ «НГУ», розповсюдженість засобів мобільного зв'язку, зумовлює високу ступінь різноманітності, багатоваріантності рішень, що певною мірою породжує проблему уніфікації та стандартизації систем колективної роботи (СКР). Головною метою СКР є підвищення ефективності спільної роботи, що спрямована на досягнення єдиної мети (або групи цілей) за мінімально можливий проміжок часу при одночасному забезпеченні відповідної якості. У виконаній роботі запропоновано мете, інтеграційні якості, складові елементи, компоненти, які є необхідними під час розгортання СРК.

Впровадження у педагогічну діяльність запропонованої СКР у поєднанні з традиційними методами організації освітніх процесів дозволяє отримання в реальному часі параметрів процесів; візуалізацію інформації, дистанційний доступ до інформаційних ресурсів порталу; ведення баз даних, у тому числі – реального часу; підготовка довідкових і звітних документів; оперативне сповіщення та обмін даними між територіально розосередженими об'єктами (суб'єктами) системи; виконання розрахунків; дистанційне управління процесами і об'єктами.

П р о р е к т о р з навчальної роботи **Ю.Т. Хоменко**