ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут інформаційних технологій

Кафедра системного аналізу

Пояснювальна записка

до кваліфікаційної роботи
на ступінь вищої освіти бакалавр
на тему: «**РОЗРОБКА КОМПОНЕНТ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ В ОСВІТІ**»

Виконав: студент 4 курсу, групи САД-41
спеціальності 124, Системний аналіз
Сологуб Я. Д.

Керівник Штіммерман А. М.
(прізвище, ініціали)

Рецензент Литвинчук А. О.
(прізвище, ініціали)

Нормоконтроль Ставицька Ю. В.
(прізвище, ініціали)

Київ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Системного аналізу
Ступінь вищої освіти бакалавр
Спеціальність 124, Системний аналіз

ЗАТВЕРДЖУЮ
Завідувач кафедри
системного аналізу
_____ О.А.Золотухіна
"____" _____2020 року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ РОБОТУ СТУДЕНТУ

Сологуб Ярослав Дмитрович
(прізвище, ім'я, по батькові)

1.Тема роботи: Розробка компонент інформаційних систем управління в освіті

Керівник роботи Штіммерман Аксенія Миколаївна Старший викладач кафедри
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від ___ 2020 року№____

2.Строк подання студентом робот 08.05.2020-10.06.2020

3.Вхідні дані до роботи: Науково-методична та науково-технічна література з питань розбудови, функціонування, розвитку та модернізації баз даних інформаційних систем управління освітою в Україні та зарубіжних країнах
Звіт про НДР «Розробка та введення в дослідну експлуатацію ІТС «Державна інформаційна система освіти»; Технічне завдання на розробку інтегрованої інформаційної системи управління освітою (EMIS) – програмування та розробка баз даних (TFSCB-CQ-01)

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити).
4.1.Зарубіжний досвід функціонування інформаційних систем управління освітою (EMIS)
4.2.Функціонування інформаційних систем управління освітою в Україні
4.3.Програмно-апаратне забезпечення функціонування інформаційно-телекомунікаційної системи «Державна інформаційна система освіти»
4.4.Автоматизація процесів обробки інформації в базі даних (інтерактивний прототип системи)
4.5.Організація безпеки та захист інформації в інформаційній системі управління в освіті
4.6.Модель загроз функціонування інформаційної системи управління в освіті

5.Перелік графічного матеріалу

1.	Обєкт, предмет, мета роботи
2.	Завдання роботи
3.	Схема функціонування EMIS
4.	Порівняння функціоналу різних інформаційних систем у сфері освіти
5.	Схема програмно-апарвтного забеспечення
6.	Функціональна схема ІТС
7.	Принципова схема бізнес-процесу ІТС ДІСО
8.	Програмно-апарвтна архітектура ІТС ДІСО
9.	Управління обліковими записами та правами доступу користувачив інформації
10.	Ризики загроз ІТС ДІСО
11.	Класифікація внутрішніхпорушників в компонентах ІТС
12.	Основний результат роботи
13.	Практична значущість результатів дослідження
14.	Висновки

6. Дата видачі завдання ____08.05.2020_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Аналіз науково-технічної літератури з питань становлення, розвитку, функціонування та модернізації інформаційних систем управління освітою. Опис предметної області, постановка задачі, визначення об'єкта, предмета, мети та завдань роботи	08.05-15.05.2020	
2	Вивчення зарубіжного досвіду функціонування інформаційних систем управління освітою (EMIS). Проведення системного аналізу функціонування інформаційних систем управління освітою в Україні	15.05.-22.05.2020	
3	Аналіз програмно-апаратного забезпечення та автоматизація процесів обробки інформації в базі даних інформаційно-телекомунікаційної системи «Державна інформаційна система освіти»	22.05.-01.06.2020	
4	Аналіз ефективності функціонування інформаційно-телекомунікаційної системи «Державна інформаційна система освіти»	22.05.-01.06.2020	
5	Розробка компонент інформаційно-телекомунікаційної системи «Державна інформаційна система освіти» за результатами системного аналізу ефективності функціонування	10.05.-20.05.2020	
6	Розробка обов'язкових демонстраційних матеріалів	01.06.-04.06.2020	
7	Попередній захист роботи	05.06.2020	
8	Здача роботи в деканат	10.06.2020	

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Бакалаврська робота: 70 с., 24 рис., 14 табл., 42 джерела, 1 додаток.

ІНФОРМАЦІЙНА СИСТЕМА УПРАВЛІННЯ ОСВІТОЮ, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА ДЕЖАВНА ІНФОРМАЦІЙНА СИСТЕМА ОСВІТИ, БАЗИ ДАНИХ, ЗАХИСТ ІНФОРМАЦІЇ

Об’єкт дослідження – функціонування та розвиток інформаційних систем управління освітою. Предмет дослідження – розробка компонент інформаційних систем управління в освіті.

Мета роботи – дослідити функціонування та проаналізувати ефективності функціонування інформаційної системи управління освітою в Україні.

Методи дослідження – загальнонаукові емпіричні (статистичний опис, порівняльний аналіз); теоретичні (аналіз, синтез, узагальнення, індукція, дедукція, пояснення, класифікація); формальні та якісні методи системного аналізу.

Результати дослідження та їх новизна полягає у здійсненні ґрунтовного аналізу функціонування зарубіжних та українських інформаційних систем управління освітою та розроблено компоненти посилення інформаційної безпеки ІТС «ДІСО», зокрема: досліджено архітектуру БД та функціонал інформаційних систем управління освітою зарубіжних країн в контексті визначення напрямів розвитку української ІСУО; здійснений порівняльний аналіз переваг та недоліків функціонуючих інформаційних систем у сфері освіти та здійснено оцінку функціонуванню ІТС «ДІСО»; визначено напрями посилення інформаційної безпеки, зокрема розроблено компонент інформаційної безпеки ІТС «ДІСО» в частині управління обліковими записами та правами доступу користувачів до інформації; визначено ступінь загрози з боку зовнішніх та внутрішніх порушників, зокрема встановлено, що в контексті загрози цілісності та доступності інформаційних ресурсів системи внутрішні порушники можуть розташовуються в певному порядку зменшення ступеня небезпеки.

ЗМІСТ

Стор.

ВСТУП

1 ДОСЛІДЖЕННЯ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ ОСВІТОЮ

1.1. Зарубіжний досвід функціонування інформаційних систем управління освітою (EMIS)

1.2. Функціонування інформаційних систем управління освітою в Україні

2 АНАЛІЗ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ «ДЕРЖАВНА ІНФОРМАЦІЙНА СИСТЕМА ОСВІТИ»

2.1. Програмно-апаратне забезпечення функціонування інформаційно-телекомунікаційної системи «Державна інформаційна система освіти»

2.2. Автоматизація процесів обробки інформації в базі даних (інтерактивний прототип системи)

3 АНАЛІЗ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1. Організація безпеки та захист інформації в інформаційній системі управління в освіті

3.2. Модель загроз функціонування інформаційної системи управління в освіті

ВИСНОВКИ

ПЕРЕЛІК ПОСИЛАНЬ

ДОДАТКИ

ПЕРЕЛІК СКОРОЧЕНЬ

АРМ	- Автоматизоване робоче місце
ОТГ	- Об’єднана територіальна громада
АЦСК	- Акредитований центр сертифікації ключів
БД	- База даних
ДССУ	- Державна служба статистики України
ЕЦП	- Електронний цифровий підпис
ЄДЕБО	- Єдина державна електронна база освіти
ЕОМ	- Електронно-обчислювальної машини
ЗО	- Заклади освіти
КСЗІ	- Комплексна система захисту інформації
КЗЗ	- Комплекс засобів захисту
КНОІ	- Канали несанкціонованого отримання інформації
ОС	- Операційна система
МОН	- Міністерство освіти і науки України
ДНУ «ІОА»	- ДНУ «Інститут освітньої аналітики»
ІКТ	- Інформаційно-комунікаційні технології
ІСУО	- Інформаційні системи управління освітою
ІСУО «НВ»	- Інформаційна система управління освітою ТОВ «Нові знання»
ІТС ДІСО	- Інформаційно-телекомунікаційна система «Державна інформаційна система освіти»
ПБ	- Політики безпеки
ПЗ	- Програмне забезпечення
ПК	- Персональний комп’ютер
ПП	- Програмний продукт
СБ	- Світовий банк
СКБД	- Система керування базами даних
ТЗ	- Технічне завдання
ТЗІ	- Технічний захист інформації
УЦОЯО	- Український центр оцінки якості освтіи
EMIS	- Education Management Information System
KPI	- Ключові показники ефективності (англ. Key Performance Indicators, KPI)

ВСТУП

1. Обґрунтування вибору теми і її актуальність. Актуальність дипломної роботи зумовлена передусім необхідністю в аналізі функціонування інформаційної системи управління освітою з метою розробки напрямів удосконалення. Функціонування розрізнених баз даних не відповідають вимогам Міністерства освіти і науки України. На сьогоднішній момент однією із гострих проблем в Україні є забезпечення органи державного управління та усіх зацікавлених осіб достовірною інформацією про стан розвитку системи освіти в Україні. З огляду на вищезазначене дослідження розбудови та розвитку сукупності апаратно-програмних засобів для формування єдиного інформаційного простору освітньої статистики і аналітики в Україні є вкрай актуальним.

2. Ступінь вивченої проблеми. Проблема становлення та розвитку інформаційних систем управління освітою досліджена більшою мірою у зарубіжних країна, зокрема фахівцями Світового банку. Серед вітчизняних науковців, які вивчали проблеми функціонування інформаційних систем у сфері освіти доцільно виділити Лондара С., Литвинчука А., Ракова С. та інших дослідників. Проте питання розвитку ІСУО в Україні залишається актуальним.

3. Специфіка джерельної бази. Джерельна база переважно представлена інтернет-ресурсами, з огляду на специфіку предмету дослідження. ІСУО, як правило, містять відкриті портали даних в мережі інтернет.

4. Об'єкт дослідження – функціонування та розвиток інформаційних систем управління освітою.

5. Предмет дослідження – розробка компонент інформаційних систем управління в освіті.

6. Мета і завдання роботи. *Мета* – дослідити функціонування та проаналізувати ефективності функціонування інформаційної системи управління освітою в Україні. *Завдання*: проаналізувати теоретичні основи функціонування інформаційних систем управління освітою; вивчити зарубіжний та український досвід функціонування інформаційних систем управління освітою; проаналізувати ефективність функціонування інформаційно-телекомунікаційної системи «Державна інформаційна система освіти»; оцінити

організацію інформаційної безпеки.

7. Методика дослідження. Методи дослідження – загальнонаукові емпіричні (статистичний опис, порівняльний аналіз) та теоретичні (аналіз, синтез, узагальнення, економіко-математичне моделювання, індукція, дедукція, пояснення, класифікація).

8. Наукова новизна роботи полягає у здійсненні системного аналізу функціонування ІТС «ДІСО», що дозволило визначити напрями підвищення ефективності в частині посилення інформаційної безпеки, зокрема: розроблено компонент інформаційної безпеки ІТС «ДІСО» в частині управління обліковими записами та правами доступу користувачів до інформації, що зберігається в БД; визначено ступінь загрози з боку зовнішніх та внутрішніх порушників.

9. Практична значущість результатів дослідження. Практичне значення дипломної роботи полягає у можливості використання висновків та рекомендацій, які отримані у процесі дослідження у практичну роботу організацій. Зокрема розроблення компоненту інформаційної безпеки ІТС «ДІСО» використано в практичній діяльності ДНУ «Інститут освітньої аналітики» (довідка від 26.05.2020 № 04-14/154, див. додаток).

Також результати дослідження пройшли апробацію на науково-практичних конференціях: І Міжнародна науково-практична конференція «Реформа освіти в Україні інформаційно-аналітичне забезпечення», 29 листопада 2017 року, м.Київ, ДНУ «ІОА» (тези: Кир’янов А., Сологуб Я. Основна мета та завдання інформаційної системи освіти); Науково-практична конференція «Системний аналіз в бізнесі та управлінні», 17 квітня 2020 року, м.Київ, ДУТ (тези: Литвинчук А.О., Терещенко Г.М., Сологуб Я.Д. Розвиток інформаційних систем освітнього менеджменту).

1 ДОСЛІДЖЕННЯ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ ОСВІТОЮ

1.1. Зарубіжний досвід функціонування інформаційних систем управління освітою (EMIS)

Інформатизація суспільства стрімко розвивається, пронизуючи усі сфери. Світова спільнота обговорює актуальні питання розбудови інформаційного суспільства, зокрема у 2018 році в Женеві обговорювались питання запровадження інформаційно-комунікаційних технологій (ІКТ) у різні сфери життя, і насамперед в систему освіти [1]. У світі функціонує безліч інформаційних систем, які мають свої ознаки та класифікацію [2]. Інформаційні системи для обслуговування потреб організацій або органів влади визначають як інформаційно-аналітичні системи управління[3]. До таких систем відносять і управлінські інформаційно-аналітичні системи в освіті [4].

Відзначимо, що останні десятиріччя за підтримки впливових міжнародних організацій активно розвиваються інформаційні системи управління освітою (ІСУО) (Education Management Information System (EMIS)). Це такі бази даних (БД), які містять різноманітні освітні показники.

Інформаційна система управління освітою – це організована група інформаційних та документаційних служб, що забезпечують збір, зберігання, обробку, аналіз та розповсюдження інформації стосовно планування й управління системою освіти, зазначають міжнародні аналітики [5]. Українські аналітики зазначають, що ІСУО (EMIS) – це набір компонентів, що охоплює, зокрема, процеси вводу та виводу інформації та зворотний зв’язок, поєднаних з метою досягнення певної мети, а саме, для управління великими обсягами даних та інформації, які можна легко отримати, обробити, проаналізувати та зробити доступними для використання й поширення. EMIS є інструментом, який застосовує системну теорію та досягнення комп’ютеризації для розробки всебічного підходу до збирання й використання значних обсягів інформації у системі освіти і навчання. У результаті потенційним користувачам на систематичній основі надається точна та своєчасна інформація для забезпечення процесу прийняття рішень, планування, розробки проектів і виконання інших

управлінських функцій та операцій [6]. Загальну схему функціонування EMIS, яка притаманна для усіх країн світу наведено на рис.1.1.

Рис. 1.1. Схема функціонування EMIS

Джерело: [7]

На рисунку схематично зображено функціональні та ієрархічні взаємозв'язки між постачальниками та споживачами інформації. Окреслено напрями інформаційних потоків.

Аналіз міжнародного досвіду функціонування ІСУО дозволяє говорити, що кожна країна будує власні системи. Слід відзначити, що в розвинених країнах такі системи функціонують досить давно, водночас в країнах, що розвиваються ІСУО знаходяться на стадії становлення та розвитку. Основним фінансовим та консультаційним донором процесу розбудови ІСУО в світі є Світовий банк (СБ).

Експерти СБ виділяють такі принципи функціонування ІСУО для країн: 1) забезпечення підзвітності/відповідальності; 2) управління інформаційними потоками; 3) інтелектуальність/інтегрованість інформаційних систем[8]. Слід зауважити, що майже кожна країна світу дотримується цих принципів.

Принцип «підзвітність/відповідальність» реалізується через збір простих показників про кількість учнів місцевих шкіл (як правило зазначається вік, стать, рік прибуття/вибуття тощо) (рис. 1.2).

Рис. 1.2. **Первинний збір даних (підзвітність/відповідальність)**

Джерело: побудовано автором

Цей процес не потребує застосування ІКТ технологій, а в багатьох випадках дані в школах про учнів збираються на паперових носіях (як правило із підписом відповідальної особи) та передаються до місцевих органів влади, і потім вручну вводять дані до ІСУО.

Управління інформаційними потоками, передусім, використовується з метою здійснення оцінки усіпшності учнів, аналізу ефективності роботи вчителя тощо (рис. 1.3).

Рис. 1.3. **Первинний збір даних (управління інформаційними потоками)**

Джерело: побудовано автором

Рисунок демонструє, що забезпечується зворотний зв’язок між закладом освіти та органами місцевої влади. Місцеві органи влади використовують дані

про процес навчання для прийняття рішень в процесі управлянні освітою.

Стосовно інтелектуальності/інтегрованості EMIS відзначимо, що інформаційні потоки використовуються у цілях управління навчальним процесом. Застосовуються бізнес-аналітика, аналітичні звіти, які надаються зацікавленим стейкхолдерам.

Коротко зупинимося на описанні ІСУО в зарубіжних країнах.

Так, у Великобританії інформаційна система у сфері освіти функціонує за принципом агрегування даних. Через засоби EMIS у 2015 р. забезпечено функціонування єдиної БД, в якій міститься низка показників про кількість учнів, їхню успішність, обсяги шкільних витрат на забезпечення матеріально-фінансовими ресурсами закладів освіти тощо. Також забезпечено портал відкритих даних в мережі Інтернет, адміністратором якого є Департамент освіти Великобританії[9]. В британській EMIS та на сайті міститься наступна інформація: заяви, консультації та оцінки; інформація про успішність школи; зарахування до школи; шкільні показники; випускники шкіл; дані про відвідування учнями шкіл; виключення учнів зі школи; дані про шкільне харчування; кількість вчителів, вакансії вчителів та співвідношення учнів-вчителів; заробітна плата вчителів; довідник шкіл та шкільної інфраструктури та багато іншої корисної інформації для стейколдерів[10].

Схожа система функціонує майже у всіх країнах ЄС. Наприклад, у Франції забезпечується функціонування ІСУО на регіональному та загальнонаціональному рівнях. В французькій ІСУО міститься широкий перелік показників про стан розвитку освіти: кількість шкіл; кількість класів; розподіл по класах; кількість учнів у розрізі статі та віку; кількість школярів, які користуються їдальнею; дані про педагогічний і не педагогічний персоналі; розподіл учителів за рівнем кваліфікації та сертифікації за класами; розподіл учителів за віком і статтю; кількість класних кімнат; кількість класних кімнат для ремонту; кількість шкільних їдалень та багато інших відомостей.

Поряд із широким набором даних інформаційні системи Франції містять набори демографічних даних та даних про міграційні потоки населення, що є важливими для прогнозування потреби у кількості шкіл та педагогічних працівниках.

Досить розвинена ІСОУ функціонує у США, проте управління системою освіти забезпечується на рівні штатів, що обумовлює місцеву специфіку. Фактично у всіх штатах функціонує розвинена інформаційна система освіти із широким переліком показників розвитку. В деяких штатах такі системи є більш розвиненими і поряд із набором даних в інформаційних системах там розраховуються індекси та інтегральні показники. Наприклад, в штаті Меріленд США (округ Сесіл) розраховується академічний індекс (Academic index), який є комплексним показником для відображення успішності учнів того чи іншого навчального закладу. Академічний індекс враховується при вступі до коледжів та університетів, а його результати щорічно оприлюднюються у відповідних збірниках [11].

В Австралії також на рівні кожного штату збирається, обробляється та оприлюднюється великий масив даних стан розвитку освіти. Доступність цієї інформації забезпечує Департамент освіти і професійної підготовки штатів (наприклад штат Квінсленд)[12]. Ознайомитися з інформацією можна через інформаційні системи Myskills[13] (портал відкритих даних); Career development, skills and qualifications[14] (ІСУО про варіанти професійної підготовки та навчання; перелік вимог, необхідних для подальшого навчання або кар'єрного розвитку тощо). ; інформація про національні рівні кваліфікацій та як вони співвідносяться один з одним й часові рамки, необхідні для кожного кваліфікаційного рівня.

Для України також цікавим є становлення EMIS у країнах, що розвиваються, зокрема у найближчих сусідів. Зауважимо, що в Російські Федерації та в Республіці Білорусь відсутні ІСУО. Про розбудови таких систем тільки розпочинають говорити. Наприклад, в Республіці Білорусь ухвалено Концепцію інформатизації системи освіти[15], в які одним з важливих напрямків визначено впровадження республіканських інформаційно-аналітичних систем (аналог EMIS). Поряд з цим в Білорусі функціонує інформаційно-аналітичний центр Міністерства освіти Республіки, який займається збором та обробкою даних про освіту[16].

У той же час у Таджикистані за підтримки Світового банку відбувається розбудова ІСУО (EMIS), основною метою якої є інтегрування інформації у сферу

управління освітою та зробити її доступною для всіх користувачів (учителів, керівників, посадових осіб, політичних лідерів, батьків, учнів тощо)[17]. EMIS Таджикистану дозволяє вирішити такі задачі: розширити можливості обробки, зберігання в БД, аналізу інформації для органів управління у сфері освіти; забезпечувати прозорість функціонування системи освіти через надання доступу до БД для різних установ та окремих осіб на всіх рівнях для більш ефективного управління у сфері освіти; забезпечувати оптимізацію потоку інформації для прийняття рішень через скорочення і видалення повторів, а також заповнення інформаційних «дір» тощо.

В Таджикистані EMIS функціонує як підсистема державної політики у сфері освіти в частині управління та планування фінансових та матеріальних ресурсів через обмін і потік інформації. EMIS пов'язує міністерство освіти з іншими інституціями, що причетні до освітньої діяльності. В інформаційній системі обробляється широкий спектр показників, серед яких: кількість учнів; кількість викладачів; ставки викладачів; кількість класів; показники наповнюваності класів; кількість років навчання до закінчення[10]. Також в інформаційній системі Таджикистану обробляються й дані аналітики та моніторингів: готовність випускників до роботи; як праця випускників максимізує економічне зростання; підвищення кваліфікації в соціальній сфері; чи надала система освіти школярам життєві навики; рівень заробітку випускників; досвід роботи випускників тощо.

Також Світовий банк активно сприяє розвитку EMIS у країнах Африки[18-20]. Зокрема, в Судані Світовий банк разом з ЮНІСЕФ (дитячий фонд ООН – United Nations Children's Fund) та у співпраці з Африканським освітнім фондом (AET) забезпечили становлення EMIS [21]. Першим завданням було те, щоб зібрати якомога повніший список шкіл з різних джерел. У 2015-2016 рр. уперше аналіз даних був проведений командою EMIS у Судані. Зібрані та проаналізовані дані засобами інформаційної системи дозволили покращити процес розроблення планів та прогнозів щодо розвитку та фінансово-матеріального забезпечення системи освіти у цій африканській країні.

Проведений аналіз функціонування інформаційних систем та думки аналітиків (фахівців у цій сфері) дозволяють стверджувати, що характерними для

всіх країн є принципи побудови EMIS: 1) дані EMIS мають задовольняти потреби планування освітніх показників та бюджетування; 2) інформація повинна відповідати потребам логістики забезпечення освітніх послуг;3) дані EMIS мають відповідати потребам моніторингу та оцінки освіти; 4) інформація EMIS має сприяти міжнародному співробітництву та комунікаціям[22].

Для проведення порівняльного аналізу функціонування ІСУО в різних країнах варто застосувати методику СБ (рис. 1.4, 1.5), з огляду на те, що ця міжнародна організація забезпечує розбудову та розвиток інформаційних систем у сфері освіти по всьому світу.

Сфери політики	Важелі політики
СПРИЯТЛИВЕ СЕРЕДОВИЩЕ	ЗАКОНОДАВЧА БАЗА, ОРГАНІЗАЦІЙНА СТРУКТУРА ТА ІНСТИТУЦІОНАЛІЗОВАНІ ПРОЦЕСИ, ЛЮДСЬКІ РЕСУРСИ, ІНФРАСТРУКТУРНА СПРОМОЖНІСТЬ, БЮДЖЕТ, КУЛЬТУРА УХВАЛЕННЯ РІШЕНЬ НА ОСНОВІ ДАНИХ
АКТУАЛЬНІСТЬ СИСТЕМИ	АРХІТЕКТУРА ДАНИХ, ОХОПЛЕННЯ ДАНИХ, АНАЛІТИЧНА ОБРОБКА ДАНИХ, ДИНАМІЧНА СИСТЕМА, ЛЕГКІСТЬ ОБСЛУГОВУВАННЯ
ЯКІСНІ ДАНІ	АКТУАЛЬНІСТЬ МЕТОДОЛОГІЇ, ТОЧНІСТЬ І НАДІЙНІСТЬ, ЦІЛІСНІСТЬ, ЦИКЛІЧНІСТЬ ТА СВОЄЧАСНІСТЬ
ВИКОРИСТАННЯ ДЛЯ УХВАЛЕННЯ РІШЕНЬ	ВІДКРИТІСТЬ ДЛЯ КОРИСТУВАЧІВ ІСУО, ВИКОРИСТАННЯ В РОБОТІ, ДОСТУПНІСТЬ, ЕФЕКТИВНІСТЬ ПОШИРЕННЯ РЕЗУЛЬТАТІВ

Рис.1.4. Сфери та важелі політики SABER-ІСУО

Джерело: складено авторам за даними [23]

Рис. 1.5. Оцінка згідно із SABER та стан розвитку ІСУО

Джерело: [23]

Таблиця 1.1

Аналіз інформаційних систем управління освітою (EMIS) в країнах

Країна	Сприятливе середовище				Актуальність системи				Якісні дані				Використання для ухвалення рішень				Портал відкритих даних (інформаційні сайти)			
Оцінка згідно із SABER та стан розвитку ІСУО	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Україна	+	+	+		+	+	+		+	+	+		+	+	+		+	+		
РФ	+				-	-	-	-	+				+				+			
Республіка Білорусь	+				-	-	-	-	+				+				+			
Великобританія	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Франція	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
США	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Австралія	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Таджикистан	+	+			+	+			+	+			+				+			
Судан	+				+				+				+	+			-	-	-	-

Джерело складено автором

Проведений аналіз зарубіжного досвіду функціонування інформаційних систем управління освітою (EMIS) дозволив визначити місце України у питаннях розвитку ІСУО. Наша інформаційна система є досить розвиненою за критеріями оцінки СБ. Однак порівнюючи наші результати із ІСУО розвинених країн, можна стверджувати, що нам доцільно продовжувати розвиток інформаційних систем у сфері освіти. Детально функціонування інформаційних систем управління освітою в Україні будо досліджено в п.1.2.

1.2. Функціонування інформаційних систем управління освітою в Україні

В Україні функціонує низка інформаційних освітніх системи, втім більшість з них не відповідають світовим критеріям. Відповідно основних компонентів та побудовою програмного забезпечення до EMIS можна віднести тільки три інформаційні системи: програмний комплекс «КУРС: Освіта», Єдина державна електрона база освіти (ЄДЕБО), інформаційно-телекомунікаційна система «Державна інформаційна система освіти» (ІТС «ДІСО»).

До складу програмного Комплексу Проєкт «КУРС: Освіта» входять наступі ключові складові:

1. Комп'ютерна програма «КУРС: Школа»; «КУРС: Школа +»; портал

інформаційна система управління освітою ТОВ «Нові знання» (ІСУО «НВ»); портал «NZ.UA» це – публічний сайт для всіх учасників освітнього процесу: учнів, батьків, вчителів та інших працівників освіти; комп'ютерна програма «КУРС:Дошкілля»[24-27]. Усі структурні елементи Комплексу «КУРС: Освіта» є незалежними, проте взаємопов'язаними та функціонують з єдиною структурованою інформацією рис. 1.6.

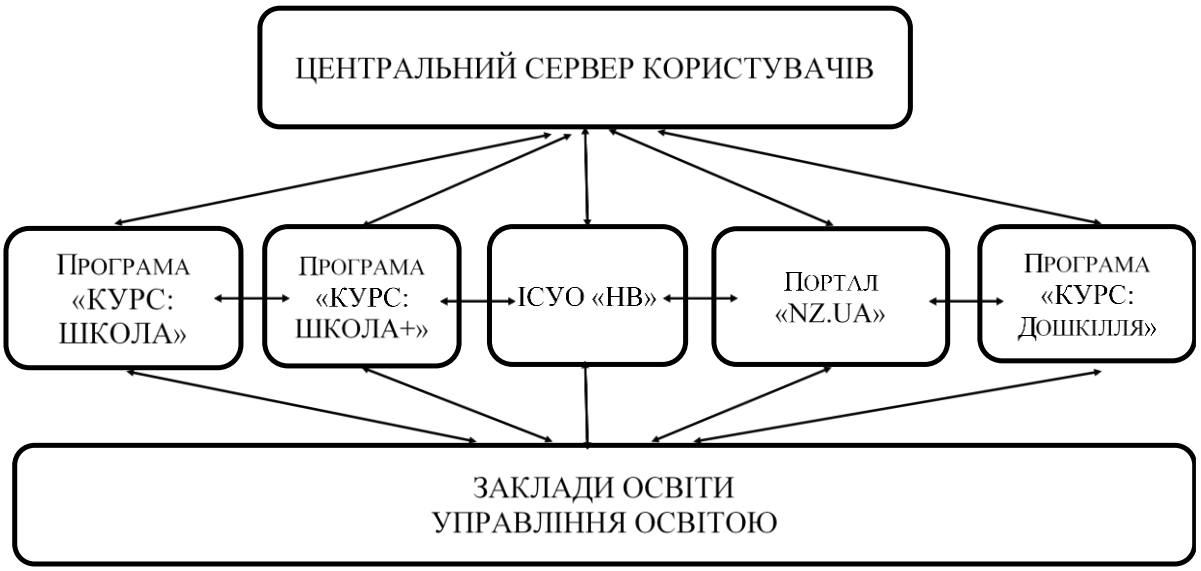


Рис. 1.6. **Структура програмного комплексу «КУРС: Освіта»**

Програмний комплекс «КУРС: Освіта» розроблено на основі дворівневої архітектури. У школах встановлюється програма «КУРС: Школа», яка є автономною із застосуванням клієнт-серверних технологій, а потрібна інформація через відповідне програмно-апаратне забезпечення передається на WEB-сервер, доступ до якого здійснюється через браузер. Функціонал системи дозволяє ведення баз даних у школах та департаментах/управліннях освіти навіть і без тимчасового доступу до мережі Інтернет з подальшим доповненням внесених даних до загальнообласної бази.

Сайт «Мої знання» є інтернет порталом, контент, що розміщено на сайті представлено на рисунку 1.7.

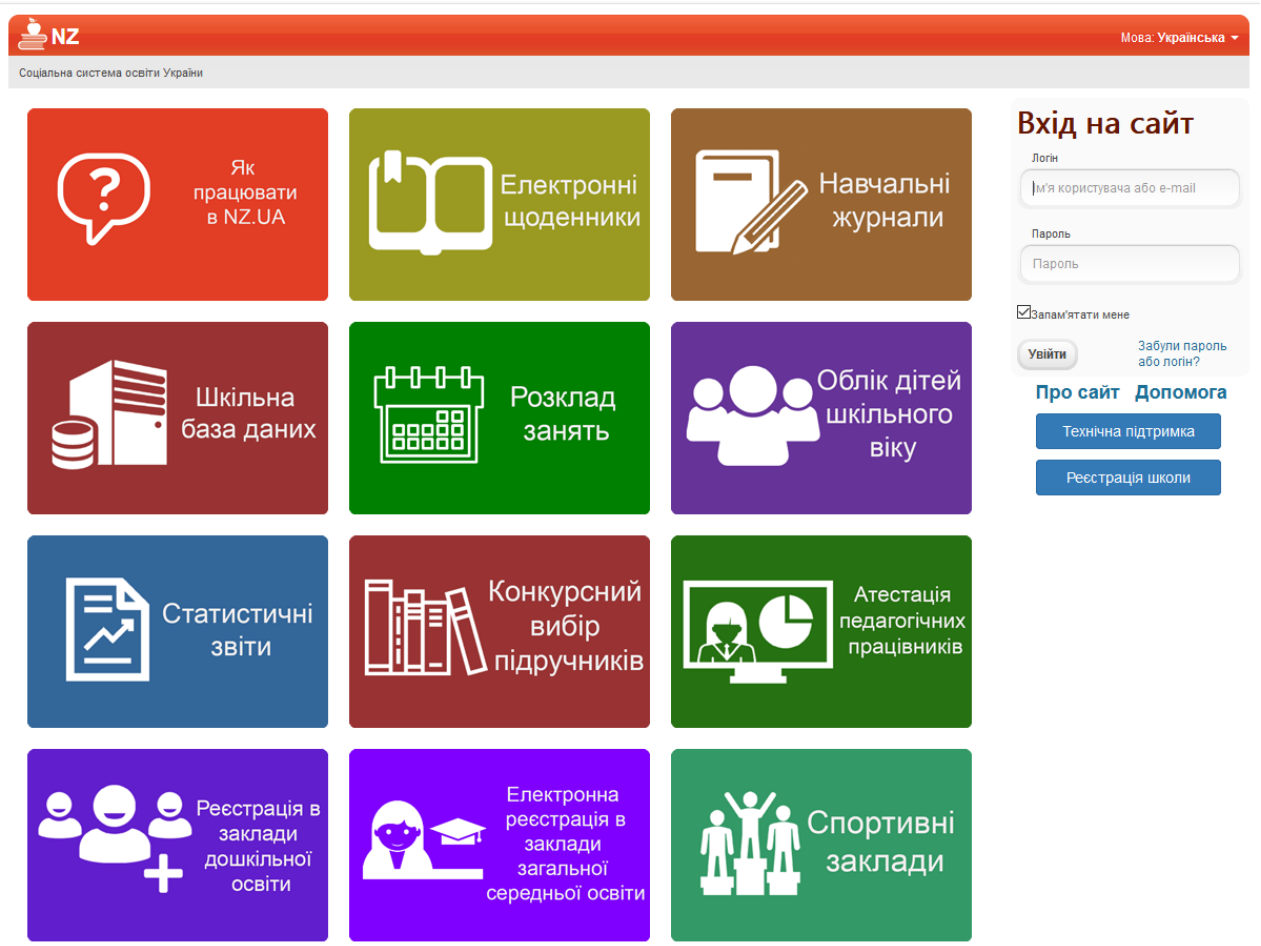


Рис. 1.7. Інтернет портал – сайт «Нові знання»

Джерело: [25]

Програма «КУРС: Школа» забезпечує автоматизацію та керування навчальними процесами: встановлює навантаження вчителям; складає розклади занять як у ручному, так і в автоматичному режимі; має модуль електронних класних журналів тощо.

ІСУО «НВ» формує статистичні форми звітності ЗНЗ-1, 76-РВК, 77-РВК, 83-РВК, Д-4, Д-5, Д-6, Д-7, Д-8, та пересилає їх електронні версії відповідно до ієрархії; забезпечує пошук необхідної інформації та полегшує вибірку даних і складання звітів тощо. Кожен регіон України має власне доменне ім’я і, відповідно, власну Систему управління освітою регіону, склад і функціонал якої може доповнюватися і нарощуватися залежно від завдань і потреб (рис.1.8).

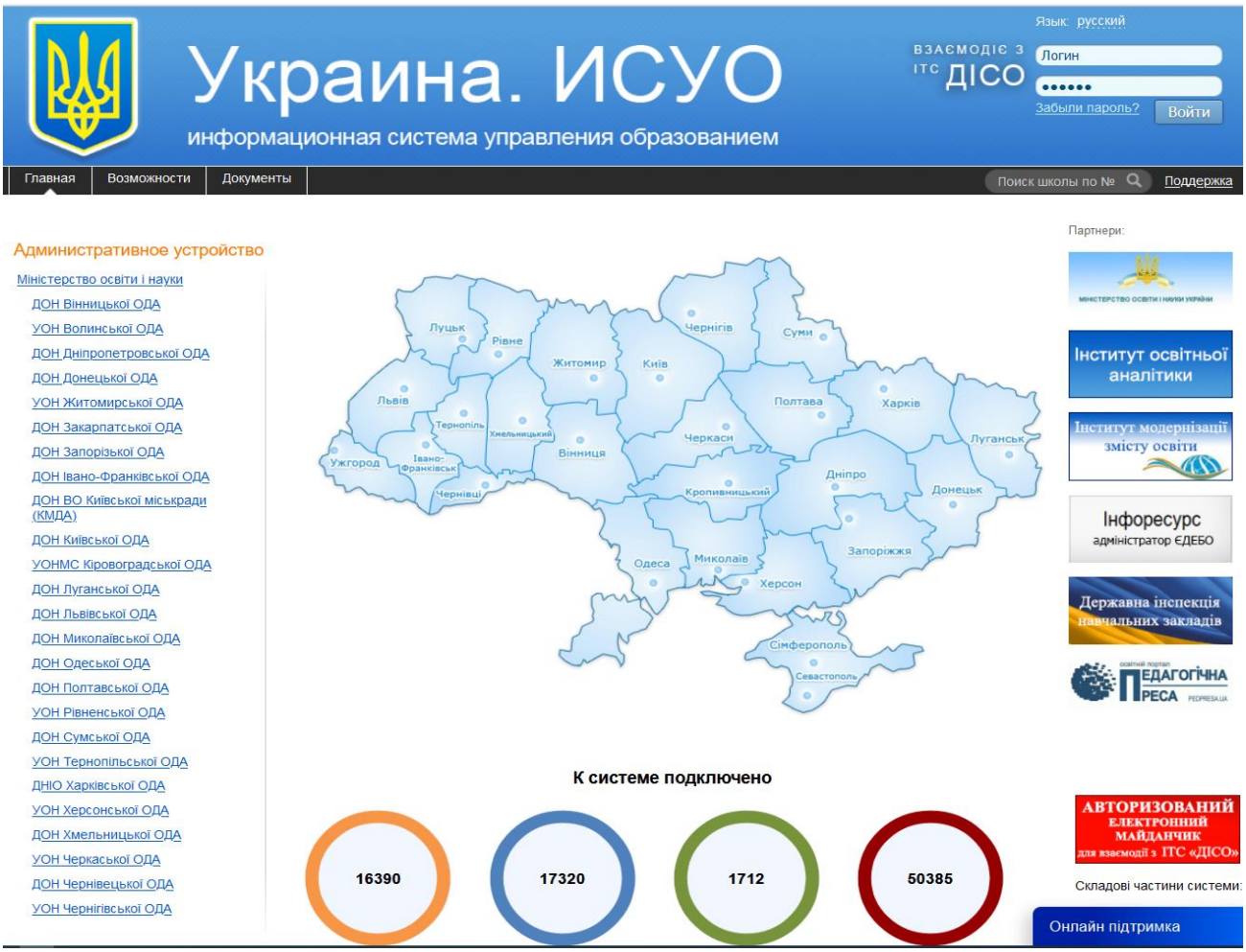


Рис. 1.8. Сайт ІСУО ТОВ «Нові знання»

Джерело: [26]

Структура ІСУО «НВ» функціонує відповідно до принципів певної ієрархії у сфері управління системою освіти: Міністерство освіти і науки України; обласні департаменти/управління освіти і науки; районні та міські відділи/управління освіти; школи. Згідно ієрархії розподіляються права доступу користувачів до функціональних можливостей та обсягу інформації в системі. Масштабованість ІСУО «НВ» забезпечує включення інших даних, у т.ч. про фінансування шкіл та потреби у підручниках. Також розроблено додатковий функціонал «Конструктор форм». ІСУО «НВ» має масштабовану архітектуру, що не залежить від архітектури апаратного забезпечення і типу операційної системи. Це дозволяє збільшити кількість користувачів та обсяг даних без втрати працездатності під час інтенсивного навантаження. ІСУО базується на платформі MySQL 5.7 DBMS та Apache web server.

Комп'ютерна програма «КУРС: Дошкілля» використовується для

адміністрування єдиної БД закладів дошкільної освіти; керування процесами обліку дітей дошкільного віку та автоматичного складання обов'язкового статистичного звіту за формою 85-к. Програма «КУРС: Дошкілля» містить інформації про склад педагогічних працівників, вихованців, батьків або опікунів. Програма забезпечує спрощення ведення контролю відвідуваності у бідь-який проміжок часу (тиждень, місяць, рік) у розрізі визначених дитячих груп, аба усього закладу. Програма загалом покликана підвищити ефективність роботи закладу дошкільної освіти та створити комфортні умови для результативної роботи педагогічних працівників та вихователей. Програма забезпечує підтримку двох мов (російської та української), розділяє права та рівні доступу до інформації, що зберігається в БД. Надає можливість роботи в розрахованому на одного користувача і мережевому режимі з підтримкою персоналізації інтерфейсу [24].

У 2011 року створено Єдину державну електронну базу з питань освіти (ЄДЕБО). ЄДЕБО – автоматизована система збору, реєстрації, обробки, зберігання та захисту відомостей і даних з питань освіти (рис. 1.9).

Рис. 1.9. Єдина державна електронна база з питань освіти

Джерело: [28]

Власником ЄДЕБО є держава, розпорядником – Міністерство освіти і науки, а технічним адміністратором – державне підприємство «Інфоресурс»

(ДП «Інфоресурс»). Основними задачами ДП «Інфоресурс» є: забезпечення функціонування ЄДЕБО (збирання, реєстрація, накопичення, зберігання, адаптування, внесення змін, поновлення, використання, поширення (розповсюдження, передача), оброблення та захист даних, що містяться в ЄДЕБО); організація замовлення, видачі та обліку документів про освіту державного зразка. Уся інформація, що міститься в ЄДЕБО, за виключенням персональних даних та інформації з обмеженим доступом, є доступною у форматі відкритих даних, зокрема з урахуванням потреб осіб з порушенням зору. Будь-яка особа може користуватися повним доступом до усієї інформації, що міститься в ЄДЕБО. Доступ до БД ЄДЕБО забезпечується через офіційний вебсайт [29].

ДП «Інфоресурс» забезпечує збір форми державного статистичного спостереження № 2-3 нк. Станом на 01 січня 2020 року до ЄДЕБО підключено: 1 475 закладів вищої освіти; 1505 закладів професійної (професійно-технічної) освіти; 777 обласних, районних, місцевих органів управління у сфері освіти [28].

Найпотужнішою інформаційною системою є інформаційно-телекомунікаційна система «Державна інформаційна система освіти» (ІТС «ДІСО»)[30], основною метою створення якої було необхідність забезпечення органів освіти достовірною статистичною інформацією. ІТС «ДІСО» було створено за фінансово-інформаційної підтримки Світового банку. Експерти Світового зокрема забезпечували консультування щодо функціоналу системи, переліку показників, які найповніше відображають стан розвитку освіти (рис.1.10) [17].

Підтримка Світовим банком розбудови ІТС ДІСО забезпечила відповідність системи світовим стандартам інформаційних систем управління освітою, зокрема: розширений обсяг даних (персонал, результати навчання, фінансові дані); посилений статистичний та аналітичний потенціал; забезпечення інтеграції ІТС ДІСО з іншими системами даних; посилення перевірки даних та стандартів якості; резервування даних для забезпечення їх безпеки у випадку форс-мажорних обставин; створення можливостей для використання освітніх даних усіма зацікавленими сторонами (своєчасність подання, відкритий доступ тощо); покращення стратегій поширення та адаптація

цих даних до потреб різних груп зацікавлених сторін.

Рис. 1.10. Інформаційно-телекомунікаційна система «Державна інформаційна система освіти»

Джерело: [30]

Адміністратором ІТС ДІСО є Державна наукова установа «Інститут освітньої аналітики» (ДНУ «ІОА») [31]. Функціонування ІТС ДІСО було затверджено відповідними наказами Міністерства освіти і науки України (МОН) [32].

ІТС «ДІСО» – це сукупність апаратно-програмних засобів, що використовується для формування єдиної інформаційної системи статистики і аналітики закладів загальної середньої, дошкільної та позашкільної освіти України. Головною метою ІТС «ДІСО» є удосконалення діяльності системи органів управління освітою на всіх функціональних рівнях в умовах децентралізації і становлення державно-громадської моделі управління освітою, забезпечення національної і регіональних статистичних служб якісними даними для бюджетного процесу (формування бюджету та оцінки ефективності його

виконання), створення відкритих інформаційних аналітичних систем на принципах Open Data для інформування освітянської спільноти, широких кіл громадськості про стан і результати освіти на всіх рівнях управління за критеріями якості, забезпечення передумов для переходу до електронного врядування в системі освіти [33].

Аналіз ІТС «ДІСО» показав, що інформаційна система є взаємопов'язаною системою автоматизованих процесів збору, обробки та верифікації статистичної інформації на всіх рівнях управління освітою. Система спроектована таким чином, щоб охоплювати усі заклади освіти на рівні середньої та дошкільної освіти, проте архітектура і структура даних дозволяє у майбутньому розвиток системи задля охоплення інших закладів освіти (вищої, професійної та інших). Спрощено схему функціонування ІТС «ДІСО» наведено на рис.1.11.

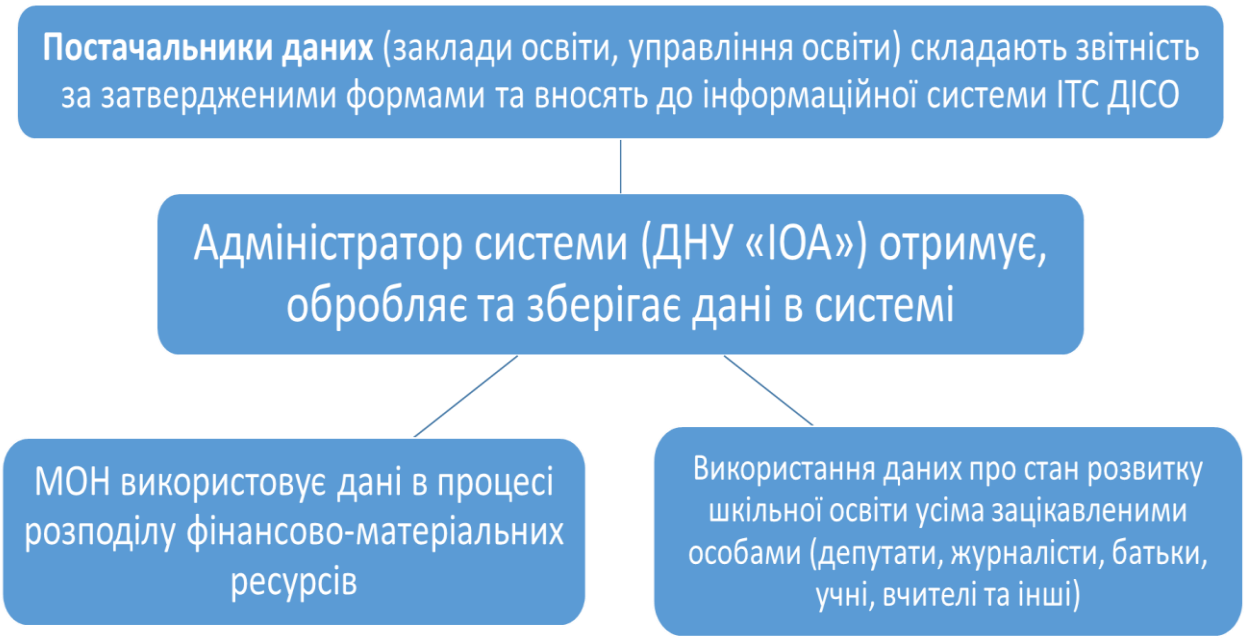


Рис. 1.11. Функціонування ІТС «ДІСО»

Джерело: побудовано автором на основі аналізу функціонування ІТС «ДІСО»

Аналіз ІТС «ДІСО» виявив наступні характеристики:

1. Наявність єдиного автоматизованого інформаційного середовища зі збору, обробки та верифікації даних;
2. Якість та оперативність роботи з обробкою інформації;
3. Наявність спеціальних механізмів захисту інформації;
4. Потенційна можливість забезпеченням сумісності та інтегрованості з іншими

інформаційними системами у сфері освіти.

Аналіз функцій ІТС «ДІСО» та завдань, які вирішує система представлено на рис. 1.12.

Рис.1.12. Функції та завдання, які виконує ІТС ДІСО

Джерело: побудовано автором на основі аналізу функціонування ІТС ДІСО

Також аналіз ІТС ДІСО показав, що система містить засоби налаштування для адаптації до змін статистичних форм та розширення переліку статистичної

інформації. Тобто будь-які зміни з боку МОН у формах статистичної звітності не вплинуть на ефективність функціонування ІТС ДІСО.

Визначено, що робота інформаційної системи базується на однорідному інтерфейсі, із використанням загальноприйнятих і загальнозрозумілих термінів, мнемонічних і графічних позначень.

Функціонал ІТС ДІСО представлено на рисунку 1.13.

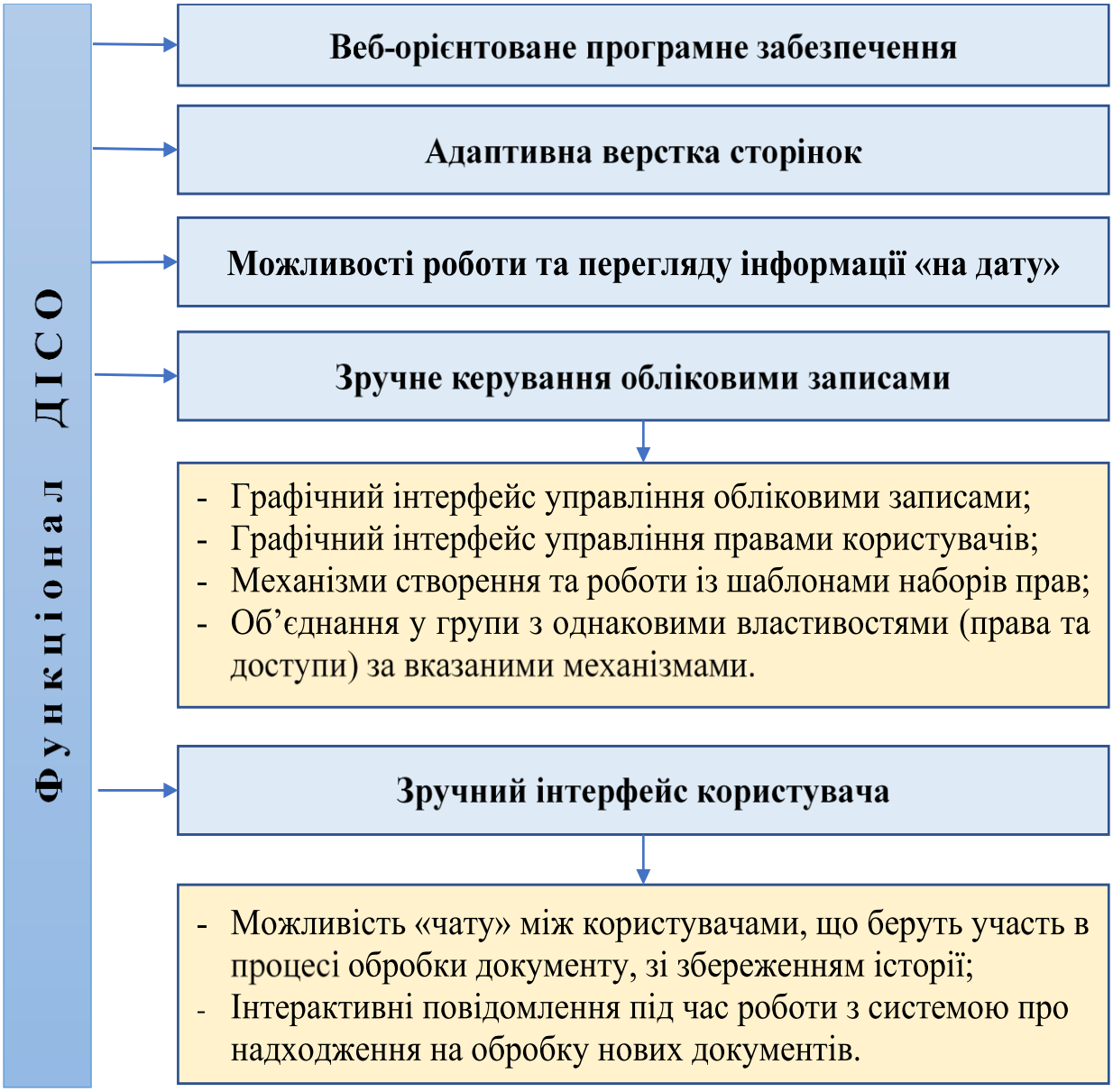


Рисунок 1.13. Функціонал ІТС ДІСО

Джерело: побудовано автором на основі аналізу функціонування ІТС ДІСО

Презентація та представлення інформації в системі здійснюється наступним чином (див. рис.1.14).

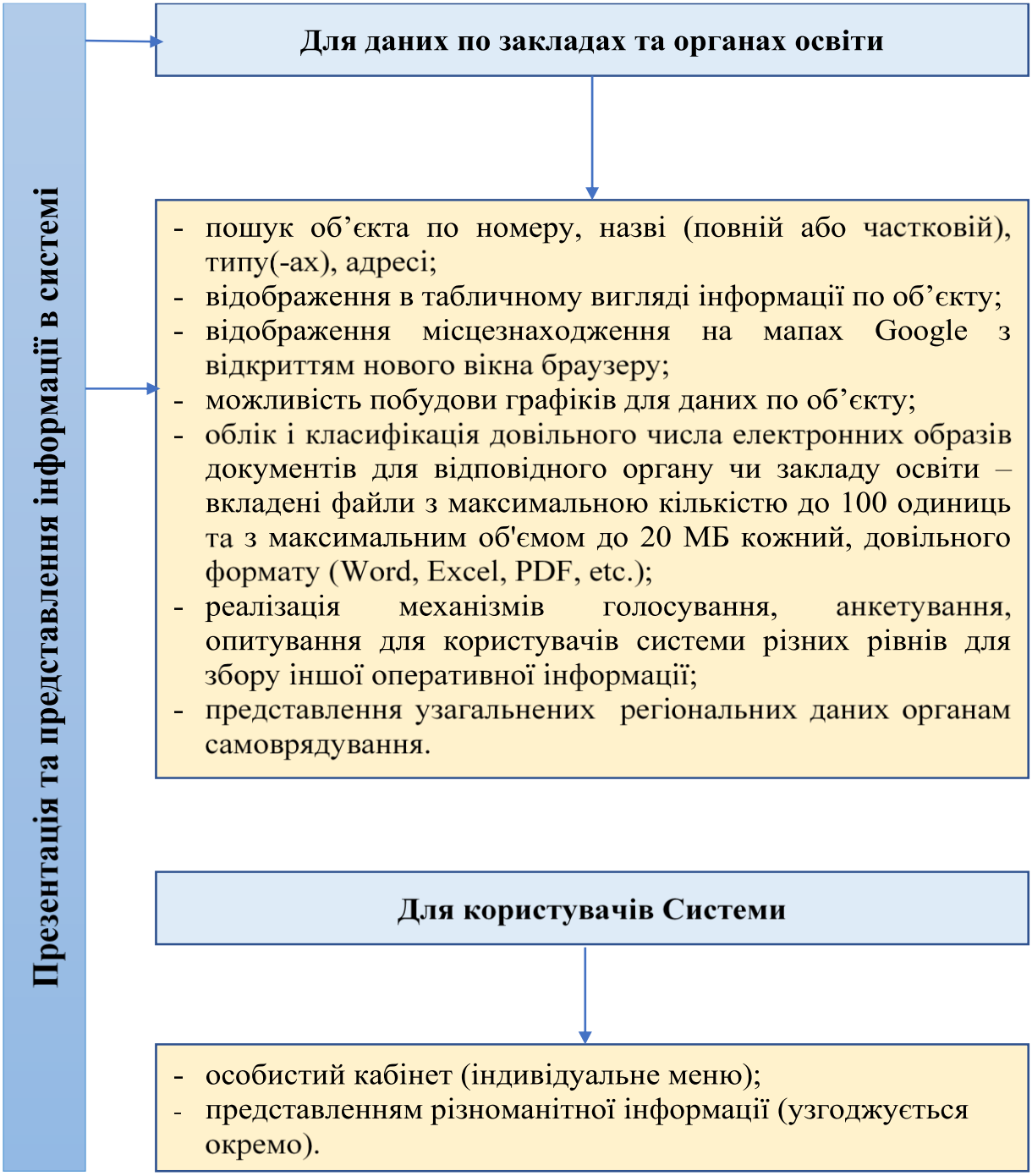


Рис.1.14. Презентація та представлення інформації в ІТС ДІСО

Джерело: побудовано автором на основі аналізу функціонування ІТС ДІСО

Система архівного зберігання інформації забезпечується через архівацію інформації засобами СУБД. Забезпечено можливість запису на змінні носії; зберігання в поточній базі даних з особливими політиками доступу.

Порівняльний аналіз функціонування інформаційних систем у сфері освіти дозволив визначити функціонал кожної з них (див. табл.1.2).

Таблиця 1.2

Порівняння функціоналу різних інформаційних систем у сфері освіти

Інформаційні системи освіти в Україні		Значення для системи освіти	Охоплення території	Фінансова доступність	Масштабованість	Додатковий функціонал
ІТС «ДІСО»		Державне значення (здійснення розподілу освітньої субвенції за інформацією, яка міститься в БД)	Усі заклади загальної середньої та дошкільної освіти	Безкоштовно	Є можливість забезпечувати розподіл будь-яких фінансово-матеріальних ресурсів	Має конструктор форм. Містить засоби налаштування для адаптації до змін статистичних форм та розширення переліку показників статистичної інформації. Містить технічну можливість для проведення опитувань за вимогою МОН.
Проект «КУРС: Освіта»	ІСУО«НВ»	Локальне значення	Заклади загальної середньої та дошкільної освіти, які уклали договори з ТОВ «Нові знання»	Платне	Частково має можливості забезпечувати розподіл підручників	Має конструктор форм. Містить засоби налаштування для адаптації до змін статистичних форм.
	КУРС: Школа					
	КУРС:Школа +					
	КУРС:Дошкілля					
	портал «NZ.UA»					
ЄДЕБО		Локальне значення. Передусім ведення реєстрів.	Усі заклади освіти	Частково платне	Не має можливостей розподілу ресурсів	Не має конструктору форм

Джерело: складено автором за даними проведеного аналізу

2 АНАЛІЗ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ «ДЕРЖАВНА ІНФОРМАЦІЙНА СИСТЕМА ОСВІТИ»

2.1. Програмно-апаратне забезпечення функціонування інформаційно-телекомунікаційної системи «Державна інформаційна система освіти»

Спрощена схема програмно-апаратного забезпечення представлена на рисунку 2.1.

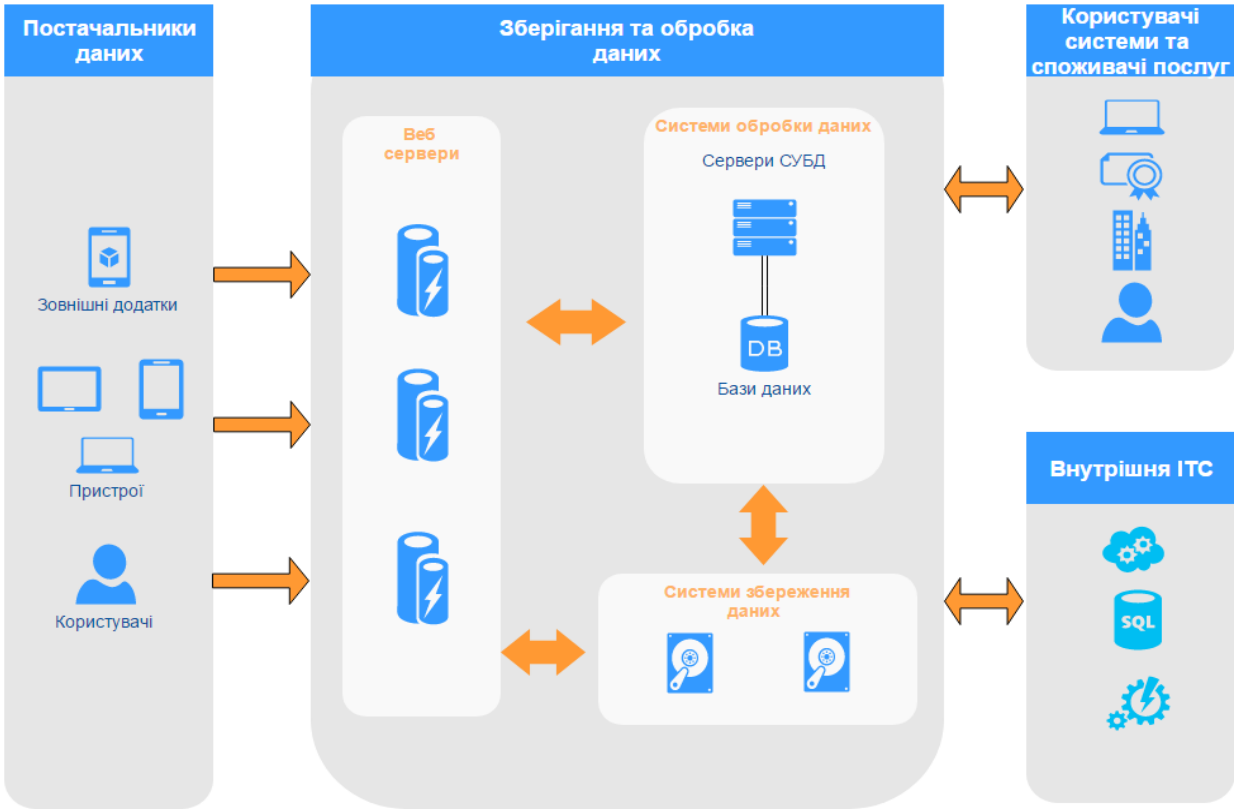


Рис.2.1. Схема програмно-апаратного забезпечення.

Джерело: побудовано автором на основі аналізу функціонування ІТС ДІСО[34]

Апаратне забезпечення (АП) містить засоби мережевої безпеки – кластер мережевої безпеки, високопродуктивний комплексний міжмережевий екран, антивірусне ПЗ, захист від несанкціонованих проникнень і від витоку даних; резервне джерело живлення – рішення для забезпечення відмовостійкості мережевого обладнання; комутатор – пристрій, який дозволяє розподілити навантаження між портами та надавати максимально швидкий доступ користувача до необхідної інформації, що зберігається в системі зберігання даних (Комутатори відповідного рівня повинні гарантувати відмовостійкість

рішення на базі стека; система зберігання даних – система, яка підтримує функції автоматичного багаторівневого зберігання даних та інтелектуальної ідентифікації «гарячих» даних, що значно підвищують ефективність використання ресурсів зберігання); сервери кластеру віртуалізації складаються з трьох серверів, що мають у складі модуль з ліцензіями керування сервером; сервер Управління (один сервер для підтримки не більше двох віртуальних серверів та модуль керування з ліцензіями керування сервером).

Для забезпечення мережевого зв'язку серверу використовується відповідне комутаційне обладнання (в тому числі, міжмережевий екран) зі складу центру обробки даних ТОВ «Адамант» (далі – ЦОД). Функціональна схема ІТС «ДІСО» наведена на рис.2.2.

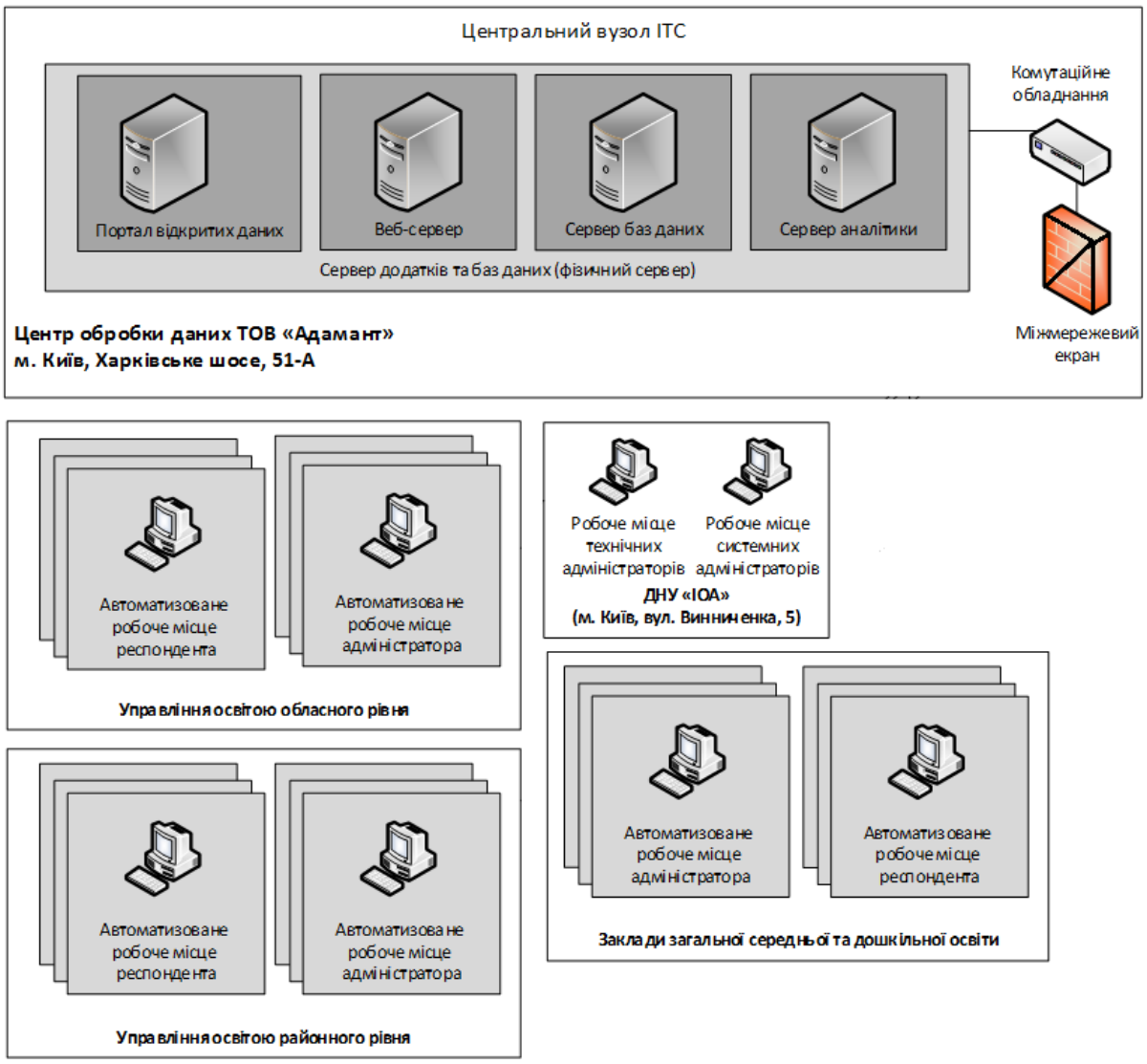


Рис. 2.2. Функціональна схема ІТС

Джерело: складено автором за даними [35]

Сервер додатків та БД призначений для забезпечення графічного інтерфейсу для користувачів системи. Це передбачено функціональними завданнями ІТС «ДІСО» з обробки інформації для розміщення та управління БД інформаційних об’єктів, що зберігаються та обробляються в системі, для забезпечення функціонування прикладного програмного забезпечення (ПЗ). Веб-сервер, сервер баз даних, сервер аналітики, портал відкритих даних розгорнуті на сервері додатків та баз даних в якості окремих компонентів прикладного програмного забезпечення.

Робочі місця системних адміністраторів призначені для: централізованого управління налаштуваннями програмного та апаратного забезпечення серверу ІТС та комутаційного обладнання; управління обліковими записами обслуговуючого персоналу на технічних засобах ІТС, а також для перегляду протоколів подій в ІТС.

Робочі місця технічних адміністраторів призначені для: управління налаштуваннями прикладного програмного забезпечення, обліковими записами адміністраторів та респондентів управлінь освітою обласного рівня та їх правами доступу до БД; формування інформаційних звітних даних з використанням прикладного ПЗ відповідно до покладених функціональних обов’язків.

Автоматизовані робочі місця адміністраторів управлінь освітою обласного рівня призначені для: управління обліковими записами респондентів власного управління освітою, адміністраторів управлінь освітою районного рівня (відповідно до адміністративної підпорядкованості) та їх правами доступу до БД; подання інформаційних звітів на основі даних, сформованих респондентами власного управління освітою, та звітів, поданих адміністраторами управлінь освітою районного рівня (відповідно до адміністративної підпорядкованості) з використанням прикладного ПЗ згідно з функціональних обов’язків, що на них покладені.

Автоматизовані робочі місця респондентів управлінь освітою обласного рівня призначені для формування статистичної звітної інформації на обласному рівні для подальшої подачі відповідних інформаційних звітів адміністратором

свого управління освітою до ДНУ «ІОА».

Автоматизовані робочі місця адміністраторів управлінь освітою районного рівня призначені для: управління обліковими записами респондентів власного управління освітою, адміністраторів закладів освіти (відповідно до адміністративної підпорядкованості) та їх правами доступу до БД; подання інформаційних звітів на основі даних, сформованих респондентами власного управління освітою, та даних, поданих адміністраторами закладів освіти (відповідно до адміністративної підпорядкованості) з використанням прикладного ПЗ згідно з функціональних обов'язків, що на них покладені.

Автоматизовані робочі місця респондентів управлінь освітою районного рівня призначені для формування статистичної звітної інформації на районному рівні для подальшої подачі відповідних інформаційних звітів адміністратором свого управління освітою до управління освітою обласного рівня (відповідно до адміністративної підпорядкованості).

Автоматизовані робочі місця адміністраторів закладів освіти призначені для: управління обліковими записами респондентів власного закладу освіти та їх правами доступу до інформаційних об'єктів; подання інформаційних звітів на основі даних, сформованих респондентами власного закладу освіти з використанням прикладного ПЗ згідно з функціональних обов'язків, що на них покладені.

Автоматизовані робочі місця респондентів закладів освіти призначені для формування статистичної звітної інформації на рівні закладу освіти для подальшої подачі відповідних інформаційних звітів адміністратором свого закладу освіти до управління освіти районного рівня (відповідно до адміністративної підпорядкованості).

Всі наведені автоматизовані робочі місця адміністраторів та респондентів являють собою окремі ЕОМ, що підключені до Інтернет мережі.

ПЗ, яке встановлено на сервери кластеру віртуалізації під керуванням операційної системи, ліцензованої на необмежену віртуалізацію. Для використання цих сервісів є ліцензії користувачів відповідного рівня. На кластер встановлено такі компоненти:

1. Поштова система – платформа для обміну повідомленнями, яка допомагає підвищити продуктивність користувачів за допомогою повсюдного доступу до електронних комунікацій і знизити ризики за допомогою засобів контролю та захисту інформації. Система складається з двох серверів та базується на відповідних ліцензіях. Перевагами рішення є можливість забезпечити відмовостійкість Баз Даних поштових скриньок. Суть роботи полягає в створенні копії бази і при виході з ладу одного сервера, база автоматично активується на іншому сервері;

2. Платформа для колективної роботи складається з сімох віртуальних серверів, робота яких забезпечується відповідними ліцензіями, використовується як безпечна БД, що забезпечує систематизацію та зберігання даних, а також спільного використання інформації та забезпечення доступу до них з ПК та будь-якого іншого пристрою, на якому встановлено прикладне ПЗ;

3. Для надання послуг ЕЦП використовується центр (центри) сертифікації ключів;

4. Встановлювання оновлення операційної системи, прикладного та серверного ПЗ на всіх комп'ютерах у мережі, за допомогою Служби оновлення.

Збереження даних і налаштування середовища в централізованій базі даних. Здійснення управління і моніторинг сервісів, додатків, серверів. Консолідування інформації про функціонування різних компонентів ІТ-інфраструктури, забезпечення її узагальненого подання до єдиної консолі. Пакет складається з двох віртуальних машин.

Для управління ІТ-інфраструктурою, інформаційна система дозволяє: оновлювати та встановлювати нове прикладне ПЗ і ОС; здійснювати інвентаризацію апаратного і ПЗ, віддалено керувати віртуальними та мобільними системами. Для управління і моніторингу ІТ-сервісів, консолідування інформації про функціонування різних компонентів ІТ-інфраструктури, забезпечуючи її узагальнене подання до єдиної консолі. Ліцензування зазначених віртуальних машин забезпечується для трьох серверів з необмеженою віртуалізацією.

На центральному вузлі ІТС використовується таке ПЗ: ОС серверу – Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-145-generic x86_64); операційні системи

робочих місць адміністраторів ДНУ «ІОА» – сімейства Microsoft Windows; операційні системи робочих місць адміністраторів та респондентів управлінь освітою та закладів освіти – сімейства Microsoft Windows; прикладне програмне забезпечення: прикладне програмне забезпечення веб-серверу nginx 1.10.3; СУБД Mysql 5.7.26; прикладне ПЗ «Державна інформаційна система освіти»; антивірусне ПЗ ESET File Security для Linux/BSD/Solaris версії 4, яке отримало експертний висновок відповідно до результатів державної експертизи в сфері технічного захисту інформації № 726 від 15.05.2017.

Операційні системи, прикладне та антивірусне ПЗ містять програмні механізми захисту інформації, які використовуються для захисту інформації, що міститься ІТС «ДІСО».

В якості комутаційного обладнання в ІТС використовуються відповідні мережеві комутатори.

Для мережевого захисту центрального вузлу ІТС використовується апаратний міжмережевий екран (зі складу ЦОД), який забезпечує наступні функції: фільтрація та аналіз трафіку на рівнях L3- L7 моделі OSI; розмежування доступу між ІТС та зовнішніми мережами; інспекція мережевого трафіку та блокування пакетів або сесій, що є підозрілими; маскування топології і мережевих адрес ІТС від публічного перегляду; контроль інформаційних потоків між ІТС та Інтернет з метою виявлення спроб мережевих вторгнень та несанкціонованого доступу до мережевих ресурсів, в т.ч. атак типу «відмова в обслуговуванні», забезпечення реєстрації, попередження та протидії таким спробам; виявлення і протидія мережевим атакам і несанкціонованій мережевій активності; фільтрація та аналіз мережевого трафіку за протоколами, портами і IP-адресами відправника й одержувача; переривання з’єднання, якщо відбудеться «атака»; протоколювання (реєстрація) подій, які стосуються безпеки системи; тощо.

Живлення всіх серверів та комутаційного обладнання здійснюється від джерел безперебійного живлення. При відключенні електроживлення налаштоване автоматичне коректне завершення роботи серверу за відповідною програмною командою джерела безперебійного живлення.

Апаратне забезпечення серверу та робочих місць не містять штатних апаратних та апаратно-програмних засобів захисту інформації.

2.2. Автоматизація процесів обробки інформації в базі даних (інтерактивний прототип системи)

Розпочнемо із загального опису бізнес процесу. Модератор закладу освіти вносить дані в форму подання звітності (дані розподілені на розділи за типом інформації). При створенні форми звітності нового року є можливість використання даних попереднього року для спрощення та оптимізації процесу внесення даних. При внесенні даних відображається релевантна довідка та відбувається перевірка коректності заповнення інформації (автоматичні правила перевірки).

При збереженні форми здійснюється перевірка на коректність введення розрахункових даних, повноту заповнення всіх полів та своєчасність їх заповнення. Після заповнення форми подання інформації, Модератор формує єдиний звіт «пакетом», підписує його за допомогою ЕЦП та відправляє «вгору».

Модератор на рівні районних та ОТГ управлінь освітою формує, підписує ЕЦП в електронному вигляді звіти за формами ДССУ та відправляє «вгору».

Модератори обласного рівня формують, підписують та відправляють як в електронному, так і паперовому вигляді (відповідно до чинного законодавства) звіти за формами ДССУ. Електронний формат подання звітності повинен бути підписаний ЕЦП.Принципову схему бізнес-процесу ІТС ДІСО наведено на рисунку 2.3.

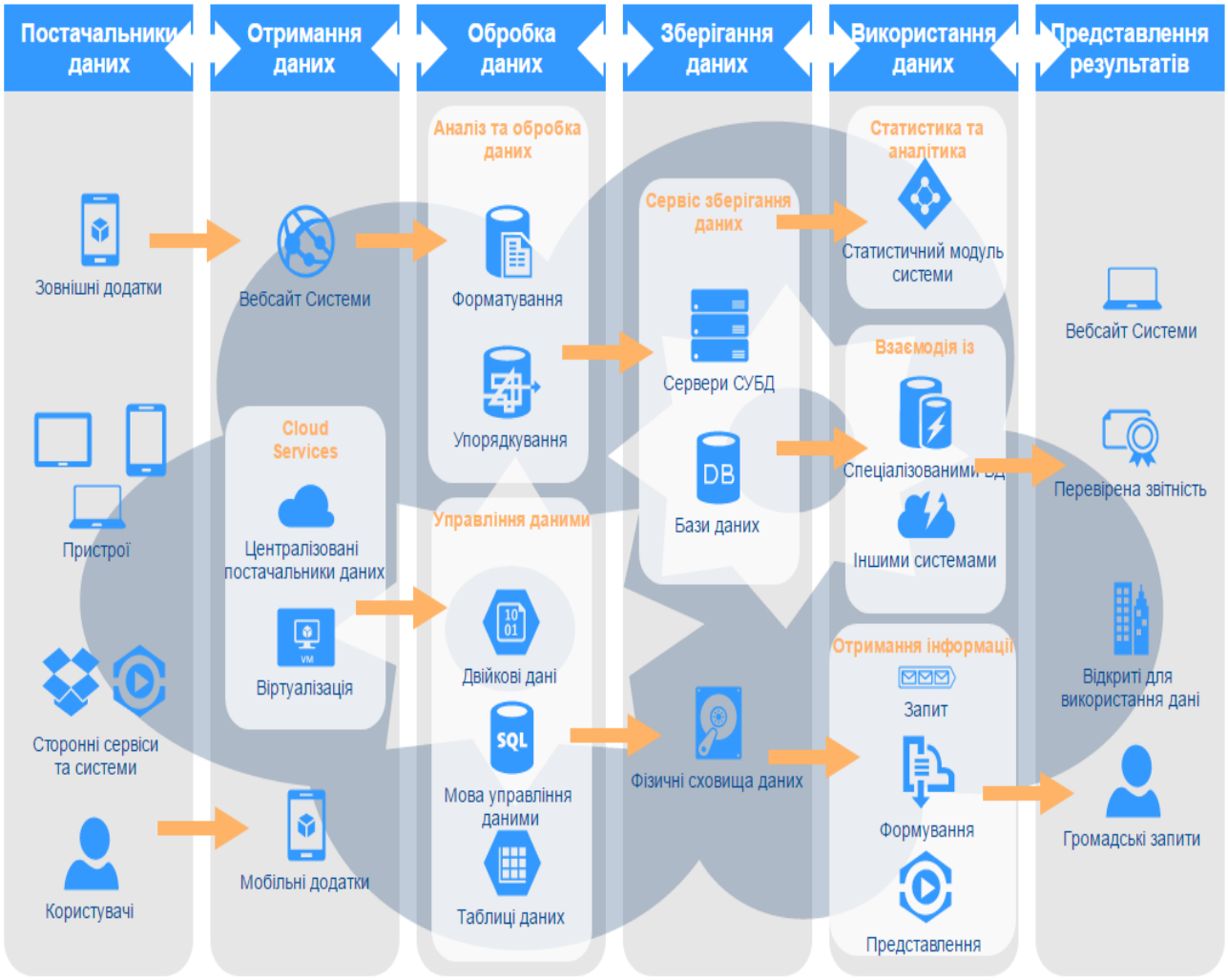


Рис. 2.3. Принципова схема бізнес-процесу ІТС ДІСО

Джерело: побудовано автором на основі аналізу функціонування ІТС ДІСО[34]

Постачальник даних – модератор закладу освіти вносить дані в форму подання звітності (дані розподілені на розділи за типом інформації). При створенні форми звітності нового року є можливість використання даних попереднього року для спрощення та оптимізації процесу внесення даних. При внесенні даних відображається релевантна довідка та відбувається перевірка коректності заповнення інформації (автоматичні правила перевірки)).

При збереженні форми здійснюється перевірка на коректність введення розрахункових даних, повноту заповнення всіх полів та своєчасність їх заповнення. Після заповнення форми подання інформації, Модератор формує єдиний звіт «пакетом», підписує його за допомогою ЕЦП та відправляє «вгору».

Модератор на рівні районних та ОТГ управлінь освітою формує, підписує

ЕЦП в електронному вигляді звіти за формами ДССУ та відправляє «вгору».

Модератори обласного рівня формують, підписують та відправляють як в електронному, так і паперовому вигляді (відповідно до чинного законодавства) звіти за формами ДССУ. Електронний формат подання звітності повинен бути підписаний ЕЦП.

Далі наводимо детальний перелік сценаріїв використання в рамках процесу (табл. 2.1, 2.2, 2.3, 2.4).

Таблиця 2.1

Сценарій «Заповнення форми звітності»

Атрибут	Опис
Ціль	Заповнення форми звітності
Учасники	Модератор закладу
Початок, вхід	Користувач входить в систему, розділ «Звітність».
Сценарій	Відкриває форму «Подання звітності», має можливість: Скопіювати дані попереднього періоду. Переглянути дані попереднього періоду (якщо у попередньому періоді за атрибутом не було значення або не було такого атрибуту, то комірка залишається пустою). Заповнити дані вручну та виконати одну з дій: - Виконує дію «Зберегти», форма не закривається, дані зберігаються, форма подання звітності доступна для подальшого заповнення. - Виконує дію «Скасування», форма не закривається, незбережені дані видаляються. - Виконує дію «Закрити», форма закривається, дані не зберігаються. Збереження даних в системі відбувається за всіма розділами одночасно, а не окремими формами розділів. Форма «Подання звітності» використовується лише для зручності заповнення даних.
Результат	Форма подання звітності заповнена, доступна для формування звіту згідно з правами доступу.

Джерело: складено автором на основі аналізу функціонування ІТС ДІСО

Таблиця 2.2

Сценарій «Формування та відправлення звіту»

Атрибут	Опис
Ціль	Відправлення звіту
Учасники	Адміністратор закладу
Початок, вхід	Користувач входить у систему, розділ «Звітність».
Сценарій	Формує звіт та підписує його, для цього виконує дію «Підписати». Звітом закриваються дані, не доступні для подальшого редагування. Генерується документ, підписання відбувається за допомогою ЕЦП, система повинна забезпечувати збереженість цілісності поданих даних. Після чого відправляє до «свого» управління освітою. Сформований та підписаний за допомогою ЕЦП звіт можливо роздрукувати. При внесенні будь-яких змін у документ, на який було накладено ЕЦП, чинність такого підпису втрачається. Після підпису дані відображаються у вищих адміністраторів та підлягають їх погодженню.
Результат	Подання звітності відправлено.

Джерело: складено автором на основі аналізу функціонування ІТС ДІСО

Таблиця 2.3

Сценарій «Відкликання форми «Подання звітності»»

Атрибут	**Опис**
Ціль	Редагування даних у формі «Подання звітності», яка пройшла кроки узгодження.
Учасники	Адміністратор закладу
Початок, вхід	Користувач входить у систему, розділ «Звітність».
Сценарій	Обирає заповнену форму «Подання звітності», має можливість виконати дію «Відкликати» та заповнити коментар на підставі чого виконується відкликання затвердженої форми «Подання звітності». Форма не закривається, доступна для подальшого редагування. Статус змінюється на «Відкликана». Відповідальним з вищих органів надходить інформація про факт відкликання. Після редагування потрібно повторно виконати дію «Підпис» (см. Сценарій 2.4.4). Інформація про зміну даних атрибутів зберігається в системі у вигляді історії, доступна при формуванні звіту за редагуванням, в якому відображається: 1. Попереднє значення 2. Нове значення 3. Хто змінив 4. Коли змінив
Результат	Форма «Подання інформації» відкликана.

Джерело: складено автором на основі аналізу функціонування ІТС ДІСО

Таблиця 2.4

Сценарій «Редагування/видалення даних у формі «Подання звітності»

Атрибут	Опис
Ціль	Редагування даних у формі «Подання звітності»
Учасники	Модератор закладу
Початок, вхід	Якщо звітність була повернута на доопрацювання, користувач входить у систему, розділ «Звітність».
Сценарій	Обирає заповнену форму «Подання звітності», має можливість відредагувати/видалити дані в комірках атрибутів. Після чого має можливість: Виконати дію «Зберегти», форма не закривається, дані зберігаються, форма звітності доступна для подальшого редагування. Виконати дію «Скасування», форма не закривається, дані не зберігаються. Виконати дію «Закрити», форма закривається, дані не зберігаються. Після цього повторно відправляє звітність. Інформація про зміну даних атрибутів зберігається в системі в вигляді історії, доступна при формуванні звіту за редагуванням, в якому відображається: 1. Попереднє значення 2. Нове значення 3. Хто змінив 4. Коли змінив Можливість редагування даних у даних звітності – лише в статусах звітності: 1. Чернетка 2. Нова 3. Відхилена 4. Відкликана
Результат	Дані в формі звітності відредаговані та відправлені повторно.

Джерело: складено автором на основі аналізу функціонування ІТС ДІСО

Звіти закладів освіти відразу формують національну базу освітніх даних ДНУ «ІОА» та агрегуються у загальні звіти Державної служби статистики України (ДССУ) вищими органами освітнього управління в електронному вигляді.

Далі детальний перелік сценаріїв використання у рамках процесу наведено в табл. 2.5, 2.6.

Таблиця 2.5

Сценарій «Перегляд та прийняття звітності»

Атрибут	Опис
Ціль	Перегляд та прийняття звітності
Учасники	Модератор (райони, ОТГ, обласного рівня, ІОА)
Початок, вхід	Користувач входить у систему, розділ «Звітність»
Сценарій	Модератор району/міста має доступ до відповідного переліку закладів та статус поданої звітності та може: ● Переглянути подану звітність; ● Прийняти подану звітність; ● Відхилити прийняття поданої звітності при наявності помилок з обов'язковим коментарем причини відхилення. Якщо звітність з усіх закладів прийнята, змінюється статус звітності району, ОТГ. Модератор обласного рівня має доступ до відповідного переліку районів та статусів поданої звітності району та може: ● Переглянути подану звітність; ● Прийняти подану звітність; ● Відхилити прийняття поданої звітності за наявності помилок з обов'язковим коментарем причини відхилення Якщо звітність зі всіх районів прийнята, змінюється статус звітності на обласному рівні. Модератор ІОА має доступ до обласного рівня, статусів поданої звітності та може: ● Переглянути подану звітність; ● Формувати зведені звіти усіх рівнів.
Результат	Форма звітності переглянута та перевірена.

Джерело: складено автором на основі аналізу функціонування ІТС ДІСО

Таблиця 2.6

Сценарій «Формування звіту»

Атрибут	Опис
Ціль	Формування звітності.
Учасники	Адміністратор (район, ОТГ, обласний рівень, ІОА).
Початок, вхід	Користувач входить у систему, розділ «Звітність».
Сценарій	Модератор має можливість формування звітів, які доступні на цьому рівні, а також: ● Переглянути обраний сформований звіт; ● Роздрукувати обраний сформований звіт.
Результат	Звіт сформовано.

Джерело: складено автором на основі аналізу функціонування ІТС ДІСО

ДНУ «ІОА», як технічний адміністратор системи, має можливість налаштування складної логіки валідації даних (внутрішніх перевірок та взаємозв'язків між блоками даних) за допомогою коду.

Також ФТС «ДІСО» має можливість конфігурування та редагування візуальної схеми звіту. Технічний адміністратор може моделювати та створювати варіанти шаблону звіту, шаблони за замовчуванням. Технічний адміністратор системи має можливість розширити модель даних, що використовується в шаблоні для формування звітності.

Для візуалізації даних повинна бути можливість обирати оптимальний засіб її відображення: візуалізація у вигляді табличних даних або форм, адаптованих для друку; візуалізація у вигляді динамічної панелі показників (наприклад, KPI) з можливістю доступу до деталізації обраного показника; різні типи графіків, різні типи діаграм тощо. Сформовані панелі з індикаторами та візуалізацією даних мають бути доступними через декілька шляхів та адаптовані для перегляду на мобільних пристроях.

Архітектура БД системи повинна бути налаштована з урахуванням прав доступу до інформації на відповідних рівнях управління освітою: центральна БД усіх закладів освіти використовується задля аналізу звітності на національному рівні та прийняття раціональних і результативних управлінських рішень органів управління освітою; деталізовані до закладу освіти обласні, районні, ОТГ бази даних доступні для органів управління освітою відповідного рівня.

Для захисту інформації використовуються механізми розмежування доступу за принципом обмеження повноважень. Тобто, кожний користувач має доступ лише до тих даних, що необхідні йому для виконання відповідних завдань. Різні користувачі можуть мати однакові права доступу до ресурсів ІТС ДІСО. Такі користувачі утворюють групу користувачів з однаковими правами. В системі є можливість розділити права доступу користувачів та категорій користувачів для розділення прав доступу по групах та дозволів (гнучке налаштування зміни користувачів у групах, гнучке визначення складу учасників процесу). Ідентифікація користувачів відбувається за логіном і паролем. Після автентифікації через веб-інтерфейс користувач потрапляє до ІТС «ДІСО». Є

також можливості блокування облікового запису на основі аудиту дій користувачів системи.

В межах процесів надання інформації та генерації звітності формуються завдання щодо редагування даних у формах подання інформації або агрегації звітів. ІТС «ДІСО» веде облік завдань користувачів зі збереженням поточного статусу, історії операцій, логу, тощо. Завдання можуть автоматично формуватися в системі через пов’язані ланцюжки бізнес-процесів, наприклад, при відправці звіту школою формується завдання на його модерування, а при відхиленні модератором звіту - формується повторне завдання на редагування.

Користувачі проінформовані про призначення завдання за допомогою електронної пошти або інших засобів. Інформування користувачів ІТС «ДІСО» та інших визначених осіб щодо стану звітів, завдань та про інші події, які можуть контролюватися ІТС «ДІСО», можливе з використанням внутрішньої функції відправки повідомлень платформи (див. рис.2.4).

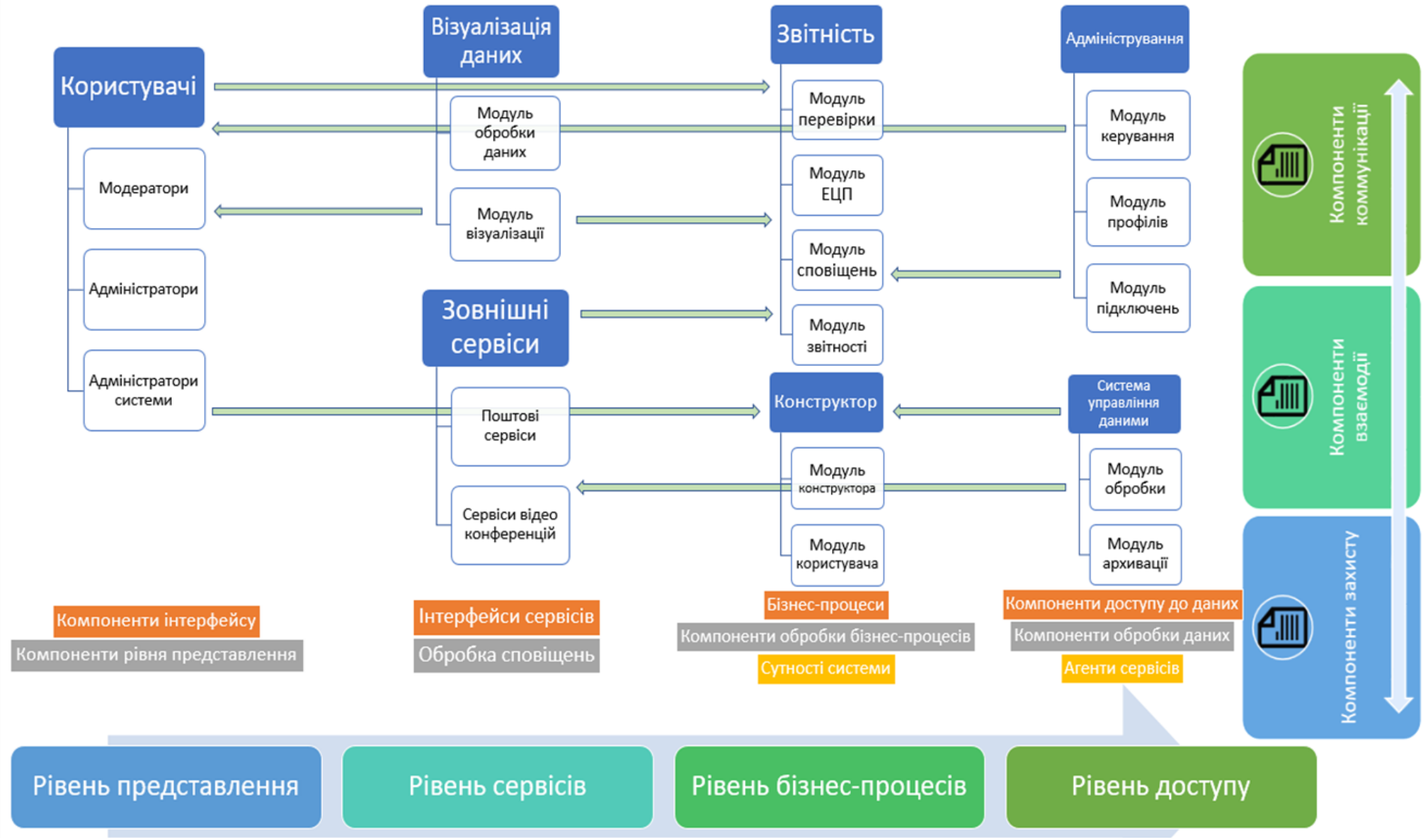


Рис.2.4. Програмно-апаратна архітектура ІТС ДІСО

Джерело: складено автором на основі аналізу функціонування ІТС ДІСО

ІТС ДІСО повинен дозволяти гнучко налаштовувати інформування електронною поштою з гіперпосиланням до ІТС ДІСО: хто та коли буде отримувати повідомлення; графік повідомлення, а також відгуки процесу для визначення одержувача повідомлення без втручання в програмний код системи. Повідомлення повинні створюватися на базі шаблонів, що визначають їх структуру та вміст.

Реалізація можливості інтероперабельності ІТС ДІСО з різними освітніми системами та базами даних (ЄДЕБО, БД УЦОЯО, органи управління освітою, проекти дослідження якості освіти, тощо). Також має бути передбачена можливість розширення функціоналу щодо інтеграції з іншими системами за відповідними вимогами.

3 АНАЛІЗ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1. Організація безпеки та захисту інформації в інформаційній системі управління в освіті

Проведений у 2-му розділі дипломної роботи системний аналіз функціонування ІТС «ДІСО» дозволив визначити напрями організації безпеки та захисту інформації в системі. Важливим аспектом функціонування будь-якої інформаційної системи є ефективна організація безпеки та захисту інформації. Так для забезпечення захищеності даних, що зберігають в БД ІТС «ДІСО», розроблено комплексну система захисту інформації (КСЗІ). Дані БД ІТС «ДІСО» становлять цінність і мають буди захищені відповідно до українського законодавства із застосуванням відповідних технічних засобів. Інформаційна безпека – це насамперед інформації, яка зберігається в БД системи.

Безпека показує ступінь захищеності системи. Характеристики безпеки й рівень захищеності оцінюються по цілому ряду факторів, наприклад: можливості несанкціонованого доступу до персональної інформації (конфіденційних даних); можливості використання важливих ресурсів; криптографічному захисту; характеристикам доступу в Інтернет; можливості проникнення в систему через Інтернет; антивірусному захисту; підготовленості персоналу тощо [36].

Відзначимо, що КСЗІ визначається цілою низкою законодавчих актів у сфері технічно-криптографічного захисту даних. Перелік яких визначений Державною службою спеціального зв’язку та захисту інформації України[37].

Основними законодавчими актами у сфері захисту інформації є Закони України «Про захист інформації в інформаційно-телекомунікаційних системах»[38], «Про захист персональних даних»[39] та постанова Кабінету Міністрів України від 29.03.06 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»[40].

Основною ціллю забезпечення інформаційної безпеки ІТС «ДІСО» є запобігання загрозам втрати та несанкціонованого розповсюдження

конфіденційних даних. Захист інформації, яка зберігається в БД системи має супроводжуватися на всіх етапах збору, обробки та зберігання даних, а також у різних режимах функціонування ІТС «ДІСО». Зокрема усі запроси на отримання доступу до інформаційної системи мають контролюватися комплексом засобів захисту (КЗЗ).

Для реалізації безпеки має бути забезпечено ізоляцію об'єктів усередині сфери управління КСЗІ та гарантовано розмежування запитів доступу та управління потоками інформаційних даних між об'єктами. Для цього кожний об'єкт повинен мати певний набір атрибутів доступу, які включають унікальний ідентифікатор та іншу інформацію, що дозволяють перевіряти легальність запитів доступу та визначати його права доступу або права доступу до нього [41].

Для того, щоб забезпечити ізоляцію об'єктів інформаційної системи та гарантувати розмежування запитів доступу та управління потоками інформації між цими об'єктами необхідно скласти переліки доступу, що визначать права доступу інших об'єктів мережі до нього. Права доступу мають бути надані мінімальній кількості осіб. Безумовним є адміністративне управління доступом з використанням паролів та призначеного для користувача унікального ідентифікатора.

Щоб захистити інформацію під час її обробки та зберігання створюється КСЗІ, що є сукупністю організаційно-інженерних заходів та програмно-апаратних засобів.

Також зазначимо, що операційні системи (ОС), системи управління базами даних (СУБД), прикладне та антивірусне ПЗ, мережеве обладнання, які забезпечують функціонування ІТС «ДІСО», повинні містити інтегровані системи захисту інформації, що контролюватиме управління доступу до системи.

Компоненти інформаційної системи, які забезпечують захист інформації мають забороняти використання локальних та мережевих ресурсів ІТС «ДІСО» без відповідного дозволу. Насамперед КСЗІ інформаційної системи має виконувати низку функцій, що представлено на рис.3.1.

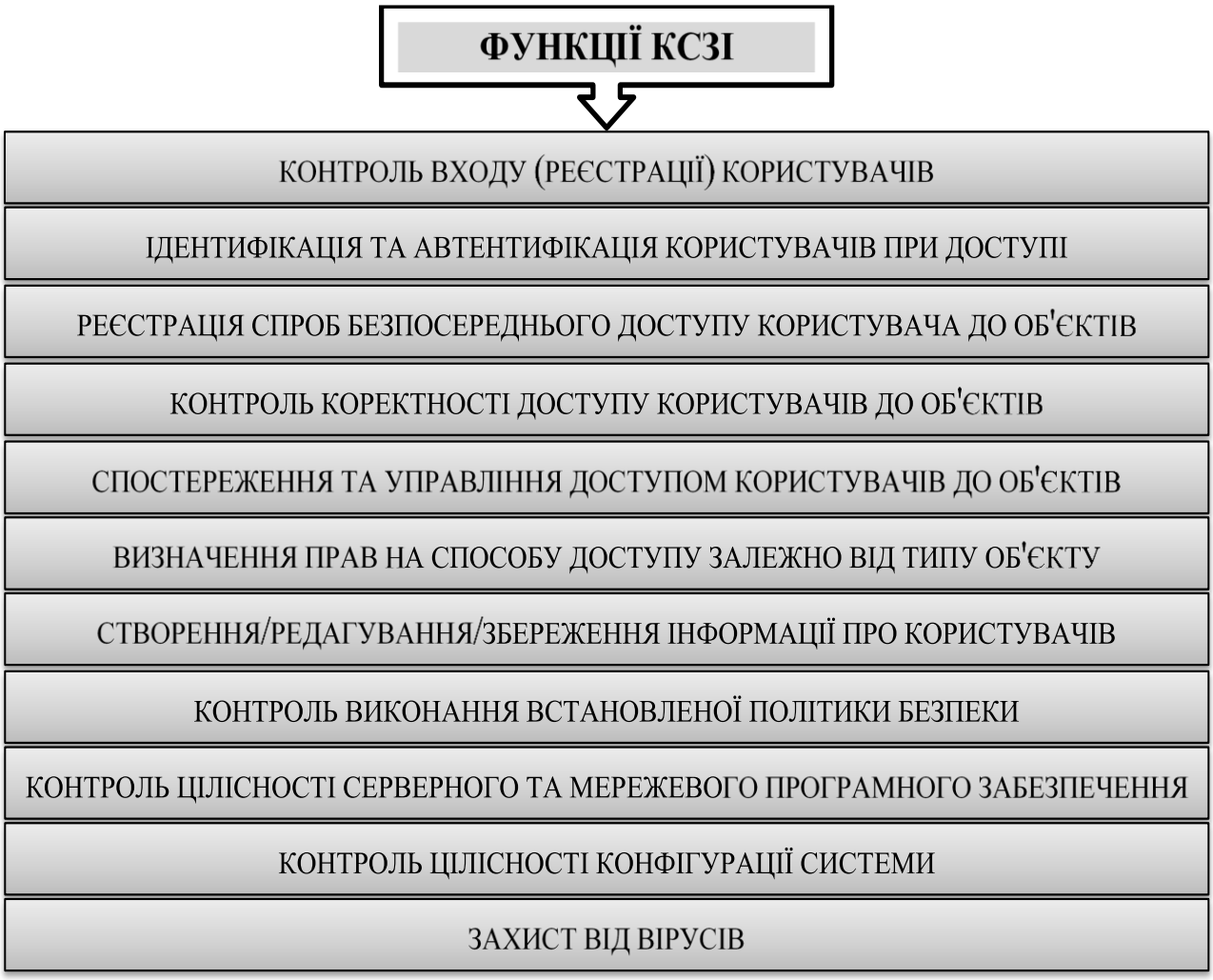


Рис. 3.1. Функції КСЗІ

Джерело: побудовано автором

Наголосимо, що складові компоненти інформаційної системи мають взаємодіяти виключно у межах, що необхідні для забезпечення функціонування. Так, міжмережевий екран системи має забезпечувати певний функціонал (рис.3.2).

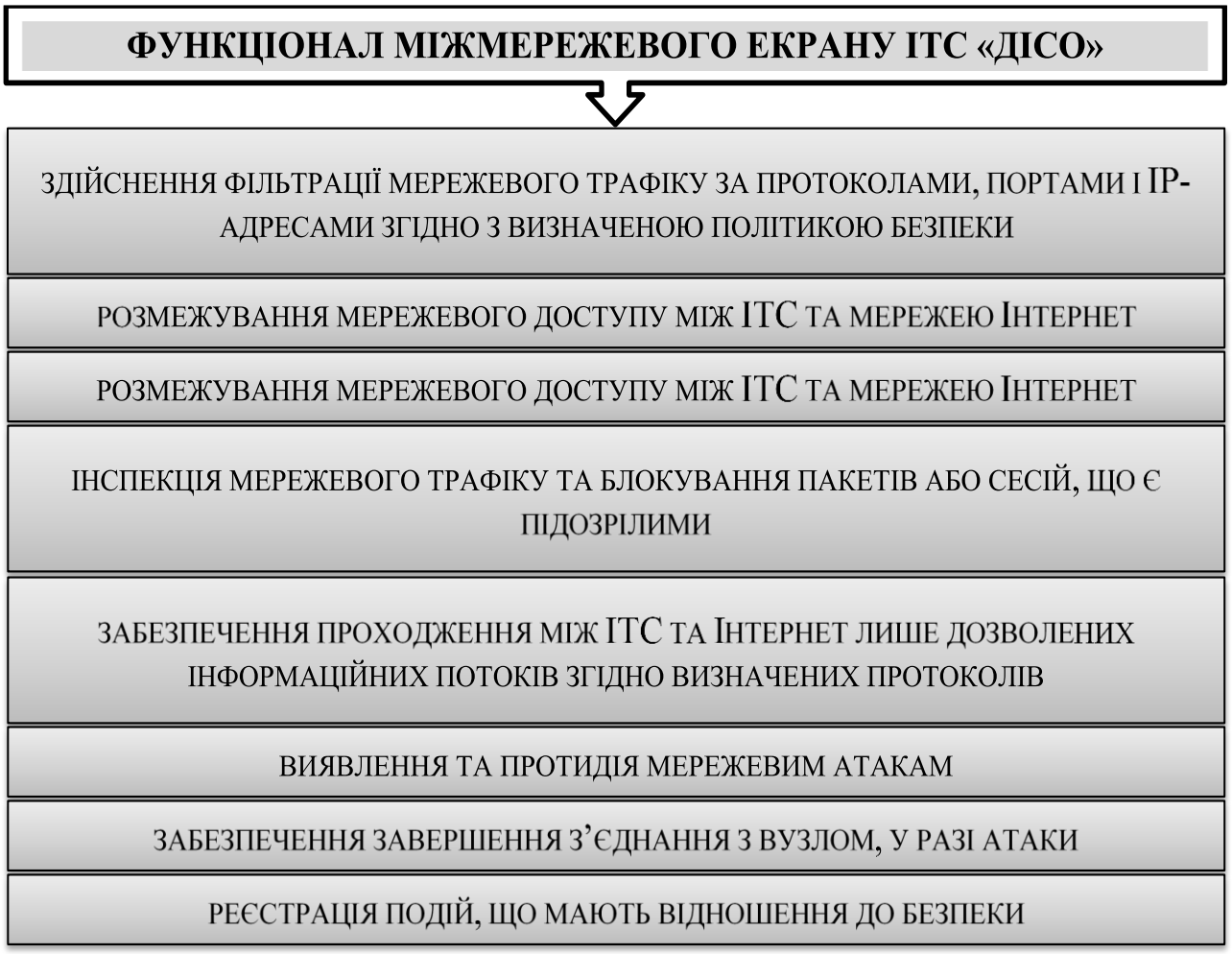


Рис. 3.2. Функціонал міжмережевого екрану ІТС «ДІСО»

Джерело: побудовано автором

Аналітики відзначають, що параметри робочого середовища будь-якого технічного засобу інформаційної системи мають визначатися профілем користувача, а кожному обліковому запису користувача (або групі користувачів) має відповідати його профіль [24; 42]. Тому, управління обліковими записами та правами доступу користувачів (або груп користувачів) до мережевих та локальних ресурсів ІТС «ДІСО» має здійснюватися виключно системним адміністратором (адміністратором БД).

Схематично управління обліковими записами та правами доступу користувачів інформації наведено на рис. 3.3.

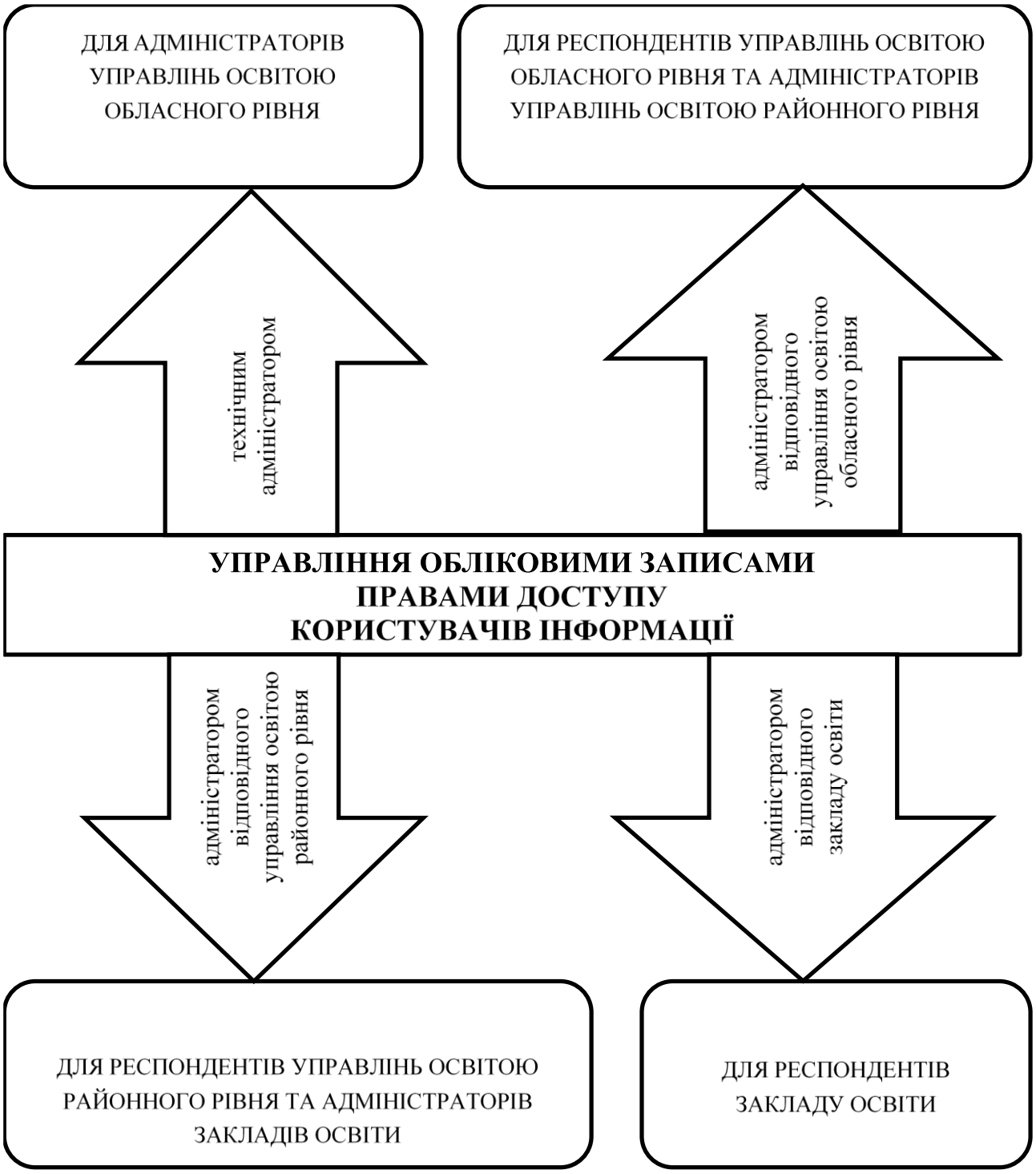


Рис.3.3. Управління обліковими записами та правами доступу користувачів інформації, що зберігається в БД

Джерело: побудовано автором

Для прикладу наведемо прототип кабінету адміністратора відповідного управління освітою районного рівня (рис. 3.4).

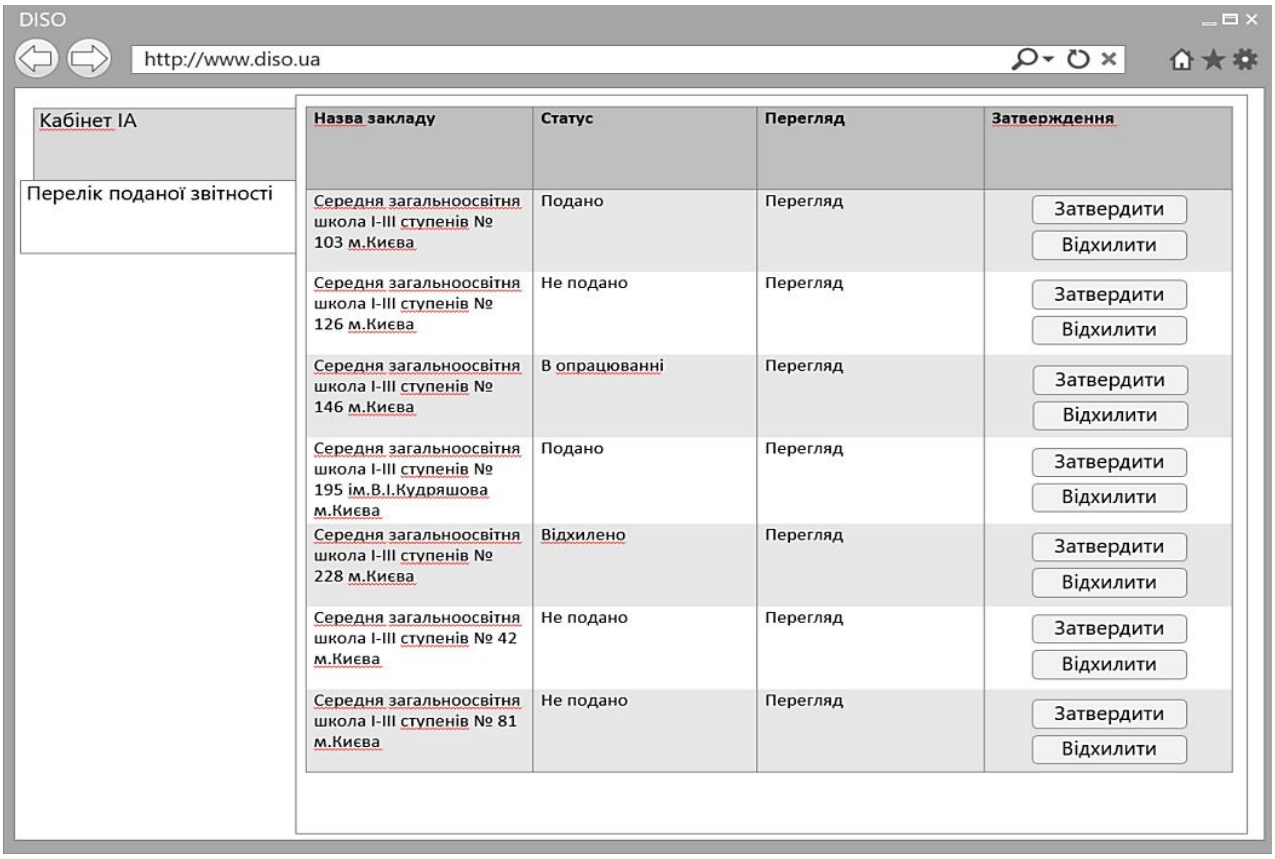


Рис. 3.4. Кабінет адміністратора відповідного управління освітою районного рівня

Джерело: побудовано автором на основі [30].

Так, усі намагання будь-якого суб'єкта одержати доступ до інформаційної системи має оброблятися КЗЗ. Надання доступу користувачам до ІТС «ДІСО» загалом має бути чітко регламентовано. Права доступу до інформації, що зберігається в БД системи надаються у разі підключення користувачів до засобами ІТС «ДІСО». Дозволяти мережевий доступ користувачів до серверів інформаційної системи виключно у випадку якщо вони спільно використовуються. Коли надаються однакові права доступу до інформації, яка зберігається в БД можна об'єднувати користувачів у локальні групи, також один користувач може одночасно бути у декількох групах. Вищезазначені правила розповсюджуються на такі інформаційні потоки: внутрішні (між активними і пасивними об'єктами всередині однієї персональної ЕОМ); локальні (обмін між робочими станціями і серверами всередині ІТС), зокрема, локальні інформаційні потоки з інформацією, що обробляється в системі, мають бути відокремлені від інформаційних потоків технологічної інформації; міжмережеві (обмін між

самою системою та користувачами ІТС). Розділ інформаційних потоків має забезпечуватися на прикладному рівні через різних ідентифікатори, мережеві портів та інше. Вихідний/вхідний міжмережевий обмін має відбуватися виключно через міжмережевий екран.

Ідентифікатор безпеки користувача або групи користувачів ІТС «ДІСО» має бути унікальним. При створенні нового облікового запису КЗЗ ІТС повинен автоматично генерувати новий унікальний ідентифікатор, який має застосовуватися як ідентифікатор облікового запису користувача.

Перед тим як отримати доступ до різних об’єктів інформаційної системи та прикладного ПЗ кожен користувач має ідентифікуватися, а КЗЗ ІТС «ДІСО» використовуватиме цю унікальну ідентифікацію для контролю дій користувачів.

Щодо переліку інформації, яка потребує особливого захисту, її наведено в табл. 3.1.

До програмно-інформаційних ресурсів інформаційної системи, що підлягають захисту, відноситься сукупність даних певної логічної структури (файл, база даних), які містяться в ІТС «ДІСО».

Об’єкти доступу, види інформації, які мають захищатися засобами КЗЗ ІТС наведені в табл.3.2. Суб’єкти доступу, як вже зазначалося є: системний адміністратор; технічний адміністратор; адміністратор управління освітою обласного рівня; респондент управління освітою обласного рівня; адміністратор управління освітою районного рівня; респондент управління освітою районного рівня; адміністратор закладу освіти; респондент закладу освіти; користувачі мережі Інтернет.

Взаємодія суб’єктів доступу і об’єктів захисту інформації в БД відбувається відповідно до адміністративного принципу керування доступом. Принципи розділення доступу користувачів до БД наведено в табл. 3.3.

Таблиця 3.1

Інформація, яка підлягає захисту з використанням КСЗІ

№ з/п	Вид інформації	Ступінь обмеження доступу інформації	Вид представлення даних
1	Журнали реєстрації подій, що ведуться апаратними та програмними засобами ІТС	конфіденційна (технологічна)	у вигляді файлів
2	Файли конфігурації програмного та апаратного забезпечення, що необхідні для коректної роботи ІТС	конфіденційна (технологічна)	у вигляді файлів
3	Інформація, що зберігається в базі даних ІТС		
3.1	Довідник закладів освіти	відкрита (державні інформаційні ресурси)	у вигляді об’єктів бази даних
3.2	Кількісні показники контингентів учнів за класами		
3.3	Відомості про мову навчання та мову, що вивчається як предмет		
3.4	Відомості про змінність навчання та групи продовженого дня		
3.5	Відомості про розподіл учнів за профілем навчання та поглибленим вивченням предметів		
3.6	Статистичні відомості про віковий склад учнів		
3.7	Відомості про учнів, які закінчили клас і переведені до наступного класу або закінчили заклад освіти, або переведені до іншого закладу		
3.8	Відомості про класи та класи-комплекти		
3.9	Відомості про гуртки, секції, організовані закладом		
3.10	Відомості про приміщення та матеріальну базу закладу освіти		
3.11	Кількісні показники педагогічних працівників	відкрита (державні інформаційні ресурси)	у вигляді об’єктів бази даних
3.12	Кількісні показники розподілу учителів, які викладають окремі предмети (включаючи директорів закладів та їх заступників)		
3.13	Дані щодо фінансування загальної середньої освіти за визначений МОН період		
3.14	Кількісні дані щодо діяльності дошкільних закладів освіти		
3.15	Відомості про стан комп’ютеризації шкіл та охоплення сучасними інформаційними технологіями		
3.16	Відомості щодо обліку фінансових даних про заклад освіти		
3.17	Відомості про ліцензування та аудит закладу освіти		
3.18	Персональні дані педагогічних працівників	конфіденційна (персональні дані)	
3.19	Загальнодоступна інформація про дошкільні, середні, позашкільні та професійно-технічні навчальні заклади та статистичні відомості щодо їх діяльності	відкрита (державні інформаційні ресурси)	
4	Резервна копія інформації, що зберігається в базі даних	конфіденційна (персональні дані)	у вигляді файлів

Джерело: складено автором

Таблиця 3.2

Властивості із захисту інформації, які повинні забезпечуватись для відповідних об’єктів захисту

Вид інформації	Вимоги щодо забезпечення властивостей інформації			
	конфіденційність	цілісність	доступність	спостережність
журнали реєстрації подій системного програмного забезпечення та мережевого обладнання центрального вузла ІТС в електронній формі	+	+	+	+
журнали реєстрації подій прикладного програмного забезпечення в електронній формі	+	+	+	+
довідники закладів освіти	-	+	+	+
кількісні показники контингентів учнів за класами	-	+	+	+
відомості про мову навчання та мову, що вивчається як предмет	-	+	+	+
Відомості про змінність навчання та групи продовженого дня	-	+	+	+
відомості про розподіл учнів за профілем навчання та поглибленим вивченням предметів	-	+	+	+
статистичні відомості про віковий склад учнів	-	+	+	+
відомості про учнів, які закінчили клас і переведені до наступного класу або закінчили заклад освіти, або переведені до іншого закладу	-	+	+	+
відомості про класи та класи-комплекти	-	+	+	+
відомості про гуртки, секції, організовані закладом	-	+	+	+
відомості про приміщення та матеріальну базу закладу освіти	-	+	+	+
кількісні показники педагогічних працівників	-	+	+	+
кількісні показники розподілу учителів, які викладають окремі предмети	-	+	+	+
дані щодо фінансування загальної середньої освіти за визначений МОН період	-	+	+	+
кількісні дані щодо діяльності дошкільних закладів освіти	-	+	+	+
відомості про стан комп’ютеризації шкіл та охоплення сучасними інформаційними технологіями	-	+	+	+
відомості щодо обліку фінансових даних про заклад освіти	-	+	+	+
відомості про ліцензування та аудит закладу освіти	-	+	+	+
персональні дані педагогічних працівників	+	+	+	+
загальнодоступна інформація про дошкільні, середні, позашкільні та професійно-технічні навчальні заклади та статистичні відомості щодо їх діяльності	-	+	+	+
резервна копія інформації, що зберігається в базі даних	+	+	+	+
конфігураційні та системні об’єкти компонентів ІТС	+	+	+	+
конфігураційні та системні об’єкти системи управління базами даних ІТС, що визначають параметри конфігурації, функціонування та правила розмежування доступу	+	+	+	+

Джерело: складено автором

Таблиця 3.3

Взаємодія об’єктів та суб’єктів захисту інформації в ІТС «ДІСО»

Об’єкт захисту	системний адміністратор	технічний адміністратор	адміністратор управління освітою обласного рівня	респондент управління освітою обласного рівня	адміністратор управління освітою районного рівня	респондент управління освітою районного рівня	адміністратор закладу освіти	респондент закладу освіти	користувачі мережі Інтернет
довідники закладів освіти		+	+	+	+	+	+	+	
кількісні показники контингентів учнів за класами		+	+	+	+	+	+	+	
відомості про мову навчання та мову, що вивчається як предмет		+	+	+	+	+	+	+	
відомості про змінність навчання та групи продовженого дня		+	+	+	+	+	+	+	
відомості про розподіл учнів за профілем навчання та поглибленим вивченням предметів		+	+	+	+	+	+	+	
статистичні відомості про віковий склад учнів		+	+	+	+	+	+	+	
відомості про учнів, які закінчили клас і переведені до наступного класу або закінчили заклад освіти, або переведені до іншого закладу		+	+	+	+	+	+	+	
відомості про класи та класи-комплекти		+	+	+	+	+	+	+	
відомості про гуртки, секції, організовані закладом		+	+	+	+	+	+	+	
відомості про приміщення та матеріальну базу закладу освіти		+	+	+	+	+	+	+	
кількісні показники педагогічних працівників		+	+	+	+	+	+	+	
кількісні показники розподілу учителів, які викладають окремі предмети		+	+	+	+	+	+	+	
дані щодо фінансування загальної середньої освіти за визначений МОН період		+	+	+	+	+	+	+	
кількісні дані щодо діяльності дошкільних закладів освіти		+	+	+	+	+	+	+	
відомості про стан комп’ютеризації шкіл та охоплення сучасними інформаційними технологіями		+	+	+	+	+	+	+	
відомості щодо обліку фінансових даних про заклад освіти		+	+	+	+	+	+	+	
відомості про ліцензування та аудит закладу освіти		+	+	+	+	+	+	+	
персональні дані педагогічних працівників		+	+	+	+	+	+	+	
загальнодоступна інформація про дошкільні, середні, позашкільні та професійно-технічні навчальні заклади та статистичні відомості щодо їх діяльності		+	+	+	+	+	+	+	+
резервна копія інформації, що зберігається в базі даних	+								
конфігураційні та системні об’єкти компонентів ІТС	+								
конфігураційні та системні об’єкти системи управління базами даних ІТС, що визначають параметри конфігурації, функціонування та правила розмежування доступу		+							

Джерело: складено автором

Користувачі інформаційної системи отримують доступ до даних відповідно до їхніх функціональних обов'язків.

Загальні підходи до інформаційної безпеки ІТС «ДІСО» забезпечуються поетапно (рис.3.5).

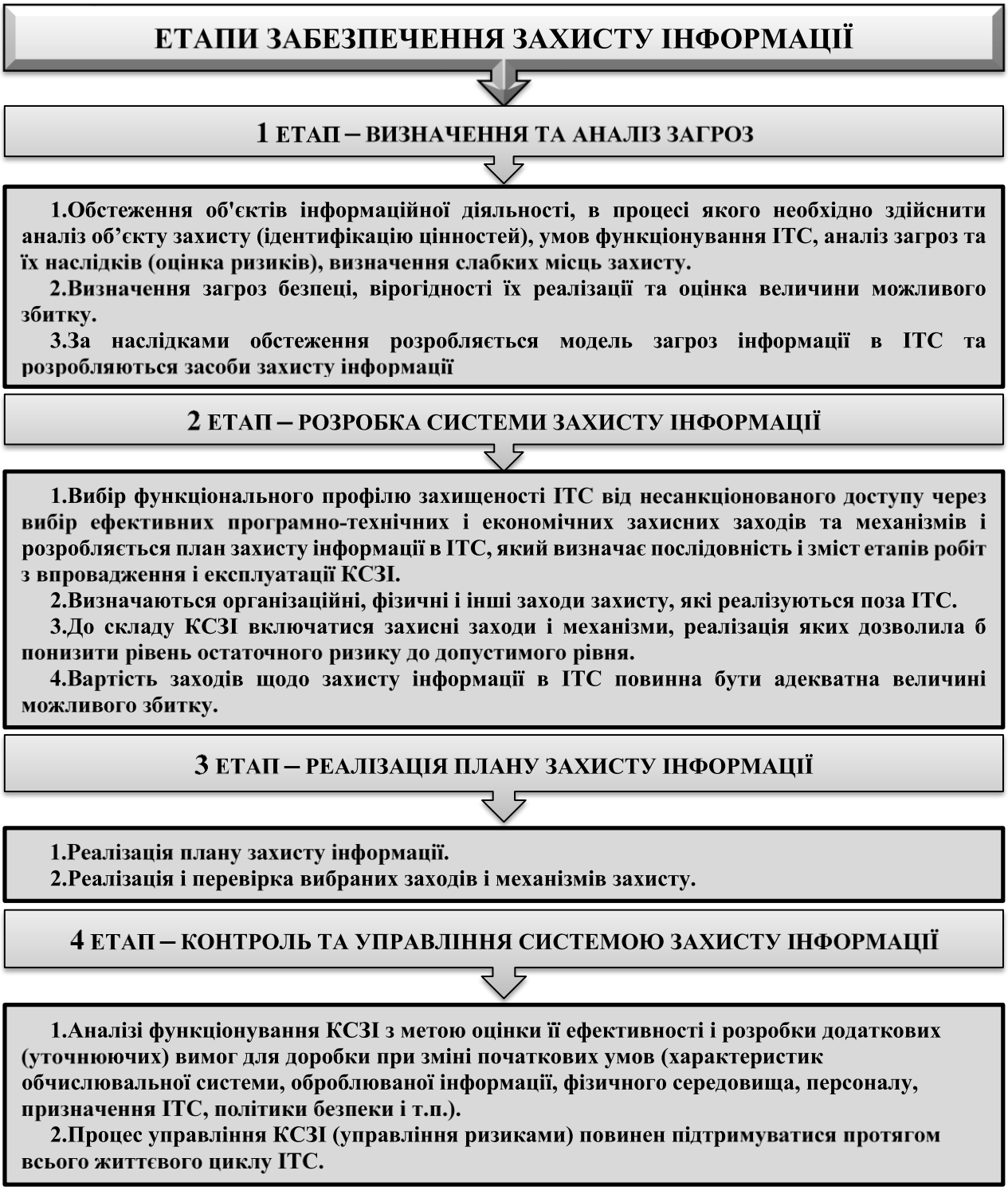


Рис. 3.5. Етапи забезпечення захисту інформації

Джерело: побудовано автором

Задачі КСЗІ мають бути реалізовані через комплексне використання

методів і засобів криптографічного і технічного захисту інформації. За умов порушення правил інформаційної безпеки (порушення конфіденційності, доступності, цілісності даних та інше) необхідно: негайно припинити процес збору, обробки та передачі інформації; блокувати програмно-апаратні засоби доступу в систему; доповісти про факт порушення системному адміністратору та керівнику функціонального підрозділу, де мав місце факт порушення.

3.2. Модель загроз функціонування інформаційної системи управління в освіті

Системний аналіз ефективності функціонування ІТС «ДІСО» дозволив розробити модель загроз, що враховує вихідні дані, які містяться в матеріалах обстеження середовищ функціонування системи. При оцінці функціонування ІТС та розробці моделі загроз було враховано вимоги державного стандарту України[37][1].

Модель загроз ІТС розроблена за результатами аналізу архітектури та компонентів системи, класифікації ресурсів і її складових частин; аналізу неформальної моделі можливих інформаційних потоків у функціональних підсистемах, складових частинах і ІТС загалом; визначення і аналізу інформаційних ресурсів компонентів ІТС загалом, що підлягають захисту (об'єктів захисту); визначення переліку загроз та можливих каналів витоку інформації з оцінкою можливих втрат у разі здійснення загроз.

Модель загроз визначає їхній склад і джерела, оцінку можливості їх прояву, шляхи здійснення, оцінку очікуваного збитку. Передусім, модель загроз має на

1 ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення; ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт; ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни і визначення; НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації н комп'ютерних системах від несанкціонованого доступу; НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації віл несанкціонованого доступу; НД ТЗІ 1.1-002-98. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу; НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі; НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2; НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

меті аналіз ризиків, визначення політики безпеки інформації і вимог до КСЗІ ІТС, формування планів технічного захисту інформації (ТЗІ), реалізації організаційних, первинних і основних технічних заходів захисту інформації і контролю функціонування КСЗІ ІТС.

ІТС «ДІСО» пов’язана з іншими інформаційними системами і наявність таких інформаційних зв’язків може зумовлювати виникнення загроз інформаційній безпеці. Загрози для інформаційної безпеки, загалом, залежать від багатьох чинників, зокрема від характеристик обчислювальної системи, фізичного середовища, персоналу, технологій обробки інформації, що збирається, обробляється та передається. Загрози можуть мати об'єктивну або суб’єктивну природу. Загрози, які мають суб'єктивну природу, можуть бути випадковими (ненавмисними) або навмисними.

Системна класифікація загроз для ІТС «ДІСО» дозволила визначити відповідні критерії:

1.Загрози відповідно місця зберігання інформаційних ресурсів в частині автоматизованого процесу збору та обробки даних, зокрема: загрози, що виникають незалежно від процесів обробки даних, тобто такі загрози зумовлені власне функціонуванням ІТС як такої; загрози, які містяться виключно у процесі збору та обробки даних;

2. Загрози відповідно до джерел виникнення стосовно компонентів системи та їхньої взаємодії: зовнішні джерела – загрози, що є поза межами компонентів системи; внутрішні джерела, що містяться в самих компонентах системи, у т.ч. дії обслуговуючого ІТ-персоналу;

в) Загрози відповідно до взаємодії джерел загроз з компонентами системи: без змін у компонентах системи; з ненавмисним або навмисним внесенням змін у компоненти системи.

Схематично ризики настання загроз відповідно до природи походження загрози представлено на рис. 3.6.

ЗАГРОЗИ СУБ'ЄКТИВНОЇ ПРИРОДИ	ЗАГРОЗИ ОБ'ЄКТИВНОЇ ПРИРОДИ
□ випадкові зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту), такі як стихійні лиха і аварії, землетрус, повінь, пожежа або інші випадкові події; □ випадкові зміни умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони) такі, як аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, затоплення приміщень унаслідок аварії інж енерних комунікацій водопостачання та опалення, пожежа та інші випадкові події; □ випадкові збої і відмови в роботі оснащення і технічних засобів компонентів ІТС.	□ навмисні зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту), такі як впливи (аварії, пожежі або інші навмисні події) на комутаційні вузли і канали (тракти) передачі первинної мережі зв'язку і т.п.; □ навмисна зміна умов внутрішнього фізичного середовища (усередині будівлі бо контрольованої зони), такі як аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, затоплення приміщень унаслідок аварії інженерних комунікацій водопостачання та опалення, пожежа або інші навмисні події; □ наслідки помилок під час проектування і розробки компонентів ІТС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо); □ помилки п ерсоналу (користувачів) ІТС під час експлуатації обладнання і технічних засобів компонентів ІТС; □ навмисні дії (спроби) потенційних порушників під час експлуатації обладнання і технічних засобів компонентів ІТС.

Рис. 3.6. Ризики загроз ІТС «ДІСО»

Джерело: побудовано автором

В табл. 3.4 представлено перелік суттєвих загроз (каналів несанкціонованого отримання інформації (КНОІ)) відповідно до класів загроз. Під КНОІ розуміються такі можливі канали несанкціонованого отримання інформації, засобами яких відбувається здійснення загроз, а наслідком яких може бути отримання (або небезпека отримання) інформації, що захищається,

особами або процесами, що не мають на це повноважень.

Таблиця 3.4

Структура і перелік потенційних каналів несанкціонованого отримання інформації в ІТС

Клас КНОІ	Фактори, наслідком яких може бути отримання (або небезпека отримання) інформації, що захищається, особами або процесами, які не мають на це повноважень,
КНОІ 1-го класу – канали виявляються безвідносно до обробки інформації і без доступу порушника до елементів складових частин ІТС	помилки і системні неузгодженості при проектуванні архітектури ІТС, технології обробки інформації, розробці прикладних програм; розголошування, передача або втрата атрибутів розмежування доступу (паролів, ідентифікаційних карток тощо); викрадання носіїв інформації з місць зберігання; підслуховування розмов осіб, що мають відношення до вирішення функціональних задач ІТС; провокація на розмови осіб, які мають відношення до вирішення функціональних задач ІТС; використання порушником оптичних засобів; використання порушником акустичних засобів.
КНОІ 2-го класу – канали виявляються в процесі обробки інформації без доступу порушника до елементів складових частин ІТС	збої і помилки в роботі апаратно-програмних засобів ІТС в процесі обробки інформації; помилки в програмах обробки інформації, які можуть привести до витоку інформації; передача даних за помилковою адресою абонента (помилкова зміна маршруту); підключення апаратури реєстрації.
КНОІ 3-го класу – канали виявляються безвідносно до обробки інформації з доступом порушника до елементів складових частин ІТС, але без зміни останніх	копіювання бланків з вихідними даними; копіювання магнітних носіїв; копіювання з пристроїв відображення; копіювання вихідних документів; копіювання інших документів; розкрадання виробничих відходів; підкуп, шантаж користувачів ІТС.
КНОІ 4-го класу – канали, що виявляються в процесі обробки інформації з доступом порушника до елементів складових частин ІТС, але без зміни останніх	запам'ятовування інформації з паперових носіїв інформації; запам'ятовування інформації з пристроїв відображення; запам'ятовування службових даних; копіювання (фотографування) інформації з пристроїв відображення в процесі обробки; отримання доступу до ІТС в обхід засобів захисту; читання залишкової інформації з оперативної пам'яті і зовнішніх запам’ятовуючих пристроїв; використання програмних «пасток»; використання недоліків мов програмування; використання недоліків операційних систем; використання зараженого «вірусом» ПЗ; несанкціонована зміна особистих повноважень або повноважень інших користувачів на відправлення і отримання повідомлень; маскування під зареєстрованого користувача або запити компонентів ІТС; видача одного об'єкту за іншого з метою використання його повноважень для формування помилкової інформації або команд управління; видача одного об'єкту або суб'єкта за іншого для того, щоб зняти з себе відповідальність за реалізовані або спроби реалізувати певні загрози; санкціонування помилкових обмінів повідомленнями або їх підтвердження.
КНОІ 5-го класу – канали, що виявляються безвідносно до обробки інформації з доступом порушника до елементів складових частин ІТС зі зміною останніх	підміна бланків, магнітних носіїв, вихідних документів, елементів програм, елементів баз даних; викрадання бланків з вихідними даними, магнітних носіїв, вихідних документів, інших документів; несанкціонований доступ (далі – НСД) з метою використання апаратних пристроїв і ПЗ (у тому числі баз даних); зміна режимів технічних засобів або ПЗ; впровадження і використання несанкціонованого ПЗ; некомпетентне використання, настройка або неправомірне відключення засобів захисту користувачами ІТС; впровадження апаратник і програмних «закладок» і «вірусів»;

Клас КНОІ	Фактори, наслідком яких може бути отримання (або небезпека отримання) інформації, що захищається, особами або процесами, які не мають на це повноважень,
	зчитування залишкової інформації з оперативних запам'ятовуючих пристроїв після виконання санкціонованих запитів.
КНОІ 6-го класу – канали, що виявляються в процесі обробки інформації з доступом порушника до елементів складових частин ІТС зі зміною останніх	незаконне підключення до апаратури; НСД з метою підключення, зміни до пристроїв інформаційно-програмного забезпечення (у тому числі до баз даних); незаконне підключення до ІТС; отримання атрибутів доступу в ІТС з наступним їх використанням для маскування під зареєстрованого користувача («маскарад»); впровадження і застосування ПЗ забороненого політикою безпеки або несанкціоноване використання ПЗ, за допомогою якого можна отримати доступ до критичної інформації.

Джерело: складено автором за [35]

В табл. 3.5 наведено канали несанкціонованого порушення цілісності або доступності інформації (КНЦД) відповідно до класів загроз. КНЦД – канали порушення властивостей інформації, через які здійснюються загрози, які впливають негативно на інформацію в системі особами або процесами, що не мають на це повноважень.

Таблиця 3.5

Структура і перелік каналів несанкціонованого порушення цілісності або доступності інформації в ІТС

Клас КНЦД	Фактори, наслідком прояву яких може бути порушення особами або процесами, що не мають на це повноважень, фізичної і логічної цілісності або доступності інформації
КНЦД 1-го класу – канали виявляються безвідносно до обробки інформації і без доступу порушника до елементів складових частин ІТС	випадкове або навмисне знищення носіїв інформації в місцях зберігання; випадкові зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту) такі як: стихійні лиха і аварії, землетрус, повінь, пожежа або інші випадкові події; випадкові зміни умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони) такі як: аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, затоплення приміщень внаслідок аварії інженерних комунікацій водопостачання, опалювання, пожежа або інші випадкові події; випадкові збої (неправильне виконання функцій) і відмови (повний вихід з ладу) в роботі обладнання і технічних засобів компонентів ІТС; відмови та збої у роботі технічних засобів ІТС; невиконання вимог до організаційних заходів захисту діючих в ІТС розпорядчих документів.
КНЦД 2-го класу – канали виявляються в процесі обробки інформації без доступу порушника до елементів складових частин ІТС	випадкові зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту) такі як: стихійні лиха і аварії, землетрус, повінь, пожежа або інші випадкові події); випадкові або навмисні зміни умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони) такі як: аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, затоплення приміщень внаслідок аварії інженерних комунікацій водопостачання, опалювання, пожежа або інші випадкові події; випадкові збої і відмови в роботі обладнання і технічних засобів компонентів ІТС; відмови і збої у роботі технічних засобів ІТС;

Клас КНЦД	Фактори, наслідком прояву яких може бути порушення особами або процесами, що не мають на це повноважень, фізичної і логічної цілісності або доступності інформації
	невиконання вимог діючих розпорядчих документів щодо організаційних заходів захисту.
КНЦД 3-го класу – канали виявляються безвідносно до обробки інформації з доступом порушника до елементів складових частин ІТС, але без зміни останніх	неправомірна зміна режимів роботи елементів складових частин ІТС (окремих компонентів, обладнання, ПЗ тощо); запуск тестових або технологічних процесів, які здатні привести до незворотних змін в системі (наприклад, форматування носіїв інформації); наслідки некомпетентного застосування засобів захисту.
КНЦД 4-го класу – канали виявляються в процесі обробки інформації з доступом порушника до елементів складових частин ІТС, але без зміни останніх	неправомірна зміна режимів роботи елементів складових частин (окремих компонентів, обладнання, ПЗ тощо); запуск тестових або технологічних процесів, які здатні привести до незворотних змін в системі (наприклад, форматування носіїв інформації); випадкові збої і відмови в роботі обладнання і технічних засобів компонентів ІТС; невиконання вимог діючих розпорядчих документів щодо організаційних заходів захисту; наслідки некомпетентного застосування засобів захисту; помилки під час введення даних в ІТС, виведення даних за помилковими адресами пристроїв, внутрішніх і зовнішніх абонентів тощо; неправомірне впровадження і використання забороненого політикою безпеки ПЗ (наприклад, учбові та ігрові програми, системне і прикладне забезпечення тощо); отримання інформації про відмову одержувача (відправника) від факту прийому (передачі) інформації або твердження, що вона прийнята (передана) в інший час; факт формування одержувачем помилкової інформації, нібито отриманої від відправника; отримання інформації про те, що повідомлення або запит передавалися, хоча насправді вони не передавалися або передавалися в інший час; отримання інформації про те, що повідомлення або запит отримано від певного користувача, хоча насправді вони сформовані одержувачем (порушником); навмисна зміна одержувачем повідомлень з метою порушення їх цілісності і автентичності; формування відправником помилкового підтвердження отримання інформації, нібито прийнятого від одержувача.
КНЦД 5-го класу – канали, що виявляються безвідносно до обробки інформації з доступом порушника до елементів складових частин ІТС зі зміною останніх	ненавмисне зараження «вірусами»; невиконання вимог діючих в ІТС розпорядчих документів щодо організаційних заходів захисту; помилки під час введення даних в ІТС, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо; неправомірне впровадження і використання забороненого політикою безпеки ІТС (наприклад, учбові та ігрові програми, системне і прикладне забезпечення тощо); видача одного об'єкту або суб'єкту за іншого для того, щоб зняти з себе відповідальність за реалізовані або спроби реалізувати певні загрози.
КНЦД 6-го класу – канали, що виявляються в процесі обробки інформації з доступом порушника до елементів складових частин ІТС із зміною останніх	пошкодження апаратури, програм, елементів баз даних, носіїв даних, вихідних документів; дії, які приводять до відмови окремих компонентів ІТС, порушення апаратних, програмних інформаційних ресурсів (обладнання, каналів зв'язку, віддалення даних, програм тощо); НСД з метою підключення, зміни до пристроїв та програмного забезпечення (у тому числі баз даних); порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації); порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, вентиляція тощо); порушення режимів функціонування ІТС (обладнання і ПЗ); впровадження і застосування комп'ютерних вірусів, закладних (апаратних і програмних) пристроїв;

Клас КНЦД	Фактори, наслідком прояву яких може бути порушення особами або процесами, що не мають на це повноважень, фізичної і логічної цілісності або доступності інформації
	впровадження і застосування ПЗ забороненого політикою безпеки або несанкціоноване використання ПЗ, за допомогою якого можна отримати доступ до критичної інформації; проходження (обхід) порушником реалізованих організаційних заходів та технічних засобів захисту.

Джерело: складено автором за даними [35]

В результаті проведеного аналізу моделей загроз можна визначити загрози на рівні компонентів системи.

На рівні окремих апаратно-програмних засобів складових частин ІТС (системний блок ПЕОМ, принтер, дисплей, модем, абонентська лінія, ОС, файл, каталог, база даних тощо) суттєвими є наступні загрози: несанкціонований доступ до програмно-апаратного забезпечення БД; несанкціонована зміна режимів роботи компонентів системи, обладнання, ПЗ та інше; неправомірне одержання даних з системи; зчитування залишкової інформації з оперативної пам'яті ПК та зовнішніх накопичувачів; несанкціоноване порушення цілісності інформації в системі, зокрема через внесення вірусів, апаратно-програмних закладок у пристроях тощо; викрадення носіїв інформації або копіювання даних; фізичне порушення цілісності окремих компонентів системи (носіїв інформації, обладнання, пристроїв тощо); виведення з ладу обладнання та його невірне застосування.

Також у додаток до вище перелічених загроз на рівні компонентів системи, досить істотними є такі загрози: неправомірне виключення штатних і/або підключення додаткових апаратно-програмних компонентів; навмисне виведення з ладу компонентів системи; порушення функціоналу компонентів системи (віруси, програмно-апаратні закладки та ін.); порушення функціональних режимів системи (відключення електроенергії, вентиляції та ін.); отримання несанкціонованих атрибутів доступу до компонентів системи із застосуванням маскування під зареєстрованого користувача («маскарад»); несанкціоноване використання ПЗ, що є забороненим.

В результаті проведеного системного аналізу архітектури компонентів системи, моделі інформаційних потоків у функціональних підсистемах та

визначення можливих каналів витоку інформації, було розроблено модель порушника ІТС «ДІСО». Основне призначення розробленої модель порушника – це здійснення системної оцінки ризиків та визначення інструментів політики безпеки (ПБ) згідно з КСЗІ.

Стосовно компонентів системи, загалом, порушники можуть бути внутрішніми (обслуговуючий ІТ-персонал) або зовнішніми (будь-хто за межами компонентів ІТС «ДІСО»).

Згідно з критеріями, за якими ми здійснювали класифікацію, в основу моделі зовнішніх порушників було покладено такі припущення:

1) Рівень знань та кваліфікації порушників: високий рівень володіння знаннями у сфері ІКТ та ПЗ; високий рівень володіння знаннями про функціонал операційних систем, мережевих протоколів та СУБД; обізнаність про особливості функціонування інформаційних систем та закономірності формування в ІТС масивів даних, інформаційних потоків тощо.

2) Рівень функціональних можливостей порушників: здатність запуску фіксованого набору задач (ПЗ), що здійснюють функції обробки інформації; здатність розробки та запуску власного ПЗ новими нетиповими функціями обробки даних; здатність керування функціонуванням компонентів системи.

3) Рівень способів/методів, які використовують порушники: агентурні способи одержання даних; пасивні технічні методи перехоплення інформаційних сигналів; засоби та методи активного впливу на компоненти системи, що можуть вплинути на каналів передачі інформації тощо.

Стосовно зовнішніх порушників можна перелічити наступне: злочинна діяльність, що спрямована на протиправне заволодіння конфіденційними даними з метою отримання фінансово-матеріальної вигоди; міжнародні системи передачі інформації (глобальні мережі); 3) національні/корпоративні системи передачі інформації, що керуються сторонніми організаціями; 4) діяльність організацій та/або окремих осіб, яка спрямована на одержання конкурентних переваг.

На основі проведеного системного аналізу ми виявили потенційних внутрішніх порушників: системні адміністратори; технічні адміністратори;

користувачі інформаційних послуг ІТС «ДІСО»; розробники прикладного ПЗ для ІТС «ДІСО»; постачальники (продавці) обладнання і технічних засобів та спеціалісти, які здійснюють їх монтаж, поточне гарантійне і післягарантійне обслуговування; технічний персонал, який забезпечує обслуговування будівель та електрообладнання. Внутрішні порушники мають можливість реалізувати в складових частинах і ІТС в цілому по каналах несанкціонованого отримання інформації наступні класи загроз – 3, 4, 5 і 6, за винятком порушників зі складу технічного персоналу, які можуть реалізувати КНОІ 1-го і 2-го класів. Також внутрішні порушники мають нагоду реалізувати в складових частинах і ІТС в цілому по каналах потенційно можливих причин несанкціонованого порушення цілісності БД або доступності даних наступні класи загроз – 3, 4, 5 і 6, за винятком порушників зі складу технічного персоналу, які можуть реалізувати КНЦД 1-го і 2-го класів (див. табл.3.4, 3.5)[35].

Відповідно до ступеня небезпеки та критеріїв класифікації, внутрішніх порушників в компонентах ІТС «ДІСО» представлено в табл. 3.6.

Таблиця 3.6

Класифікація внутрішніх порушників в компонентах ІТС

Ступінь небезпеки	**Групи внутрішніх порушників**	**Критерії класифікації**																
		Рівні можливостей				**Рівні знань про ІТС**				**Методи і способи порушень**				**Місце здійснення дії**				
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	5
1	Системні адміністратори				+				+				+			+	+	+
2	Технічні адміністратори			+					+				+			+	+	+
3	Користувачі	+				+				+				+		+		
4	Розробники прикладного ПЗ		+*		+*	+	+	+	+	+	+	+	+			+	+	+
5	Постачальники обладнання технічних засобів				+			+		+	+	+	+			+	+	
6	Технічний персонал									+	+				+			

*Примітка. * можливості визначені для розробників апаратних засобів і прикладного ПЗ ІТС.*

Джерело: складено автором за даними [35]

Представлена в таблиці 3.6 класифікація внутрішніх порушників у

компонентах ІТС здійснена у відповідності до функціональних можливостей реалізації загроз. Проте слід відзначити, що в контексті загрози цілісності та доступності інформаційних ресурсів системи внутрішні порушники можуть розташовуються в наступному порядку зменшення ступеня небезпеки:

1 місце – системні адміністратори;

2 місце – розробники прикладного ПЗ;

3 місце – технічні адміністратори;

4 місце - користувачі;

5 місце – постачальники обладнання і технічних засобів для функціонування системи;

6 місце – технічний персонал.

В кінці зауважимо, що модель порушника підлягає перегляду при будь-яких змінах розміщення, функціонування та технічних характеристик ІТС «ДІСО».

ВИСНОВКИ

1. Функціонування інформаційних систем управління освітою в зарубіжних країнах дозволив визначити, що кожна країна має свої особливості у побудові БД інформаційних систем у сфері освіти. Проведений аналіз зарубіжного досвіду функціонування інформаційних систем управління освітою (EMIS) дозволив визначити місце України у питаннях розвитку ІСУО. Наша інформаційна система є досить розвиненою за критеріями оцінки СБ. Однак порівнюючи наші результати із ІСУО розвинених країн, можна стверджувати, що нам доцільно продовжувати розвиток інформаційних систем у сфері освіти. ІСУО розвинених країн є масштабованими, із значним функціоналом та великим переліком даних, які знаходяться у відкритому доступі.

2. В Україні функціонує низка інформаційних освітніх системи, втім більшість з них не відповідають світовим критеріям. Відповідно основних компонентів та побудовою програмного забезпечення до EMIS можна віднести тільки три інформаційні системи: програмний комплекс «КУРС: Освіта», Єдина державна електрона база освіти (ЄДЕБО), інформаційно-телекомунікаційна система «Державна інформаційна система освіти» (ІТС «ДІСО»). Проведений порівняльний аналіз функціонування інформаційних систем в Україні показав, що найбільш функціональною та масштабною є ІТС «ДІСО».

3. Засобами ІТС «ДІСО» є можливість організовувати збір, обробку та зберігання даних закладів освіти у цифровому форматі, включаючи створення електронного архіву даних, автоматизованого управління процедурами збору інформації, контролю виконавської дисципліни, а також управління бізнес-процесами опрацювання інформації. ІТС «ДІСО» забезпечує якісний інформаційний супровід МОН в процесі ухвалення управлінських рішень на основі використання оперативних, аналітичних, нормативно-довідкових, експертних даних, в тому числі, які утворюються при взаємодії систем та баз освітніх даних, сумісності інформації внаслідок використання єдиних стандартів та процедур побудови баз даних та обміну інформації.

4. Аналіз ІТС ДІСО виявив недоліки системи, що зумовлює необхідність передбачити комплексну систему захисту інформації, зокрема: розмежування доступу користувачів і програм користувачів до інформації; виявлення та реєстрацію спроб порушення розмежування доступу; автоматизовану ідентифікацію користувачів і експлуатаційного персоналу при зверненні до ресурсів ІТС ДІСО; реєстрацію фактів порушення доступу; протоколювання дій користувачів, включаючи доступ із зовнішніх систем; заборону на несанкціоновану зміну конфігурації ІТС ДІСО; виявлення, ідентифікацію та видалення комп'ютерних вірусів на серверах системи; зхист БД, звітної, архівної інформації від несанкціонованого доступу та фізичного руйнування; захист інформації від спотворення та несанкціонованого використання при взаємодії структурних складових ІТС «ДІСО» через канали зв'язку; захист цілісності даних від руйнувань при аварійних режимах і збоях в електроживленні ІТС ДІСО.

5. Визначено, що КСЗІ інформаційної системи має виконувати низку функцій: контроль входу (реєстрації) користувачів в ІТС; ідентифікація та автентифікація користувачів при доступі в ІТС; реєстрація спроб безпосереднього доступу користувача до об'єктів ІТС; контроль коректності доступу користувачів до об'єктів ІТС; спостереження та управління доступом користувачів до об'єктів ІТС; визначення прав та способу доступу залежно від типу об'єкту ІТС; створення, редагування та збереження облікової інформації про користувачів, групи (ролі) користувачів та об'єкти; спостереження та реєстрацію як системних подій (використання системи або індивідуальних програмних додатків), так і подій, пов'язаних з безпекою ІТС; контроль виконання встановленої політики безпеки; аналіз та уточнення політики безпеки; контроль цілісності серверного та мережевого програмного забезпечення; контроль цілісності конфігурації ІТС; захист від вірусів; управління логічною структурою ІТС.

6. Розроблено компоненти ІТС «ДІСО», що повинні взаємодіяти тільки в межах, необхідних для функціонування ІТС. Зокрема розроблено компонент управління обліковими записами та правами доступу користувачів щодо доступу

до інформації, що зберігається в базі даних здійснюється: для адміністраторів управлінь освітою обласного рівня – технічним адміністратором; для респондентів управлінь освітою обласного рівня та адміністраторів управлінь освітою районного рівня – адміністратором відповідного управління освітою обласного рівня (в межах закладів освіти своєї області); для респондентів управлінь освітою районного рівня та адміністраторів закладів освіти – адміністратором відповідного управління освітою районного рівня (в межах закладів освіти свого району); для респондентів закладу освіти – адміністратором відповідного закладу освіти в межах свого закладу освіти.

ПЕРЕЛІК ПОСИЛАНЬ

1. МІП представляє Україну на Всесвітньому саміті з питань інформаційного суспільства у Женеві. Міністерство інформаційної політики. URL: https://mip.gov.ua/news/2305.html.
2. Types of Information System URL: http://www.chris-kimble.com/Courses/World_Med_MBA/Types-of-Information-System.html
3. Золотухіна О.А. Функціональне моделювання інформаційної системи управління ресурсами підприємства в умовах невизначеності або недостовірності даних / Золотухіна О.А., Шушура О.М. // Зв'язок. 2017. - № 6. С. 52–57.
4. Лондар С.Л. Міжнародний досвід розвитку сучасних освітніх інформаційних систем. Освітня аналітика України. 2019. №1(5). С.5-19.
5. Виллануева Ч. Информационная система управления образованием (ИСУО) и формулирование плана действий по образованию для всех (ОДВ) на период с 2002 по 2015 гг. URL: https://unesdoc. unesco.org/ark:/48223/pf0000156818_rus
6. Лєснікова М.В. Аналіз міжнародного досвіду формування інформаційної системи управління освітою у сфері професійної (професійно-технічної) освіти. СОЦІАЛЬНА СТАТИСТИКА. 2019. №2. С.49-60.
7. Education Management Information Systems (EMIS): a guide for young managers URL: https://unesdoc.unesco.org/ark:/48223/pf0000220621
8. Husein Abdul-Hamid, Namrata Saraogi, Sarah Mintz. Lessons Learned from World Bank Education Management Information System Operations. Portfolio Review, 1998–2014 URL: https://openknowledge.worldbank.org/bitstream/handle/10986/26330/9781464810565.pdf?sequence=2&isAllowed=y.
9. Department of education United Kingdom and Northern Ireland. URL: https://www.education-ni.gov.uk/ topics/statistics-and-research/statistic.

10. Розвиток інформаційних систем управління освітою як інструмент реалізації державної освітньої політики: монографія / за ред. С. Л. Лондара ; ДНУ «Інститут освітньої аналітики». Київ, 2020. 248 с.
11. Progress on Implementing College and Career Readiness and College Completion Strategies in Maryland. URL: https://www.dllr.state.md.us/p20/p20ccrccarep2016.pdf.
12. Queensland Government. Education and training. URL: https://www.qld.gov.au/education/further-ed/vet.
13. Myskills. Training Provider Search. URL: https://www.myskills.gov.au/RegisteredTrainers/Search.
14. Career development, skills and qualifications. URL: https://www.qld.gov.au/education/career/qualifications.
15. Концепция информатизации системы образования Республики Беларусь на период до 2020 года. URL: https://edu.gov.by/statistics/informatizatsiya-obrazovaniya/.
16. Главный информационно-аналитический центр Министерства образования Республики Беларусь. URL: http://www.giac.by/o-tsentre/history.php.
17. Republic of Tajikistan. Education management information systems. URL: http://documents.vsemirnyjbank.org/curated/ru/261831500373515546/pdf/117550-WP-SABER-EMIS-Tajikistan-Country-Report-Final-2017.pdf.
18. Education Management Information System: A Short Case Study of Mozambique. *WORKING PAPER.* February. 2006. №.3. 30 p.;
19. Education Management Information System: A Short Case Study of Ghana. *WORKING PAPER.* February. 2006. №.4. 24 p.;
20. Education Management Information System: A Short Case Study of Nigeria. *WORKING PAPER*. February. 2006. №.5. 23 p.;
21. Education in the Republic of South Sudan. URL: https://www.basicknowledge101.com/pdf/Education%20South%20Sudan.pdf.
22. Haiyan Hua, Jon Herstein. Education Management Information System (EMIS): Integrated Data and Information Systems and Their Implications In Educational Management. USA. March 2003. 26 p.

23. EDUCATION MANAGEMENT INFORMATION SYSTEMS. Ukraine. SABER Country Report 2017. 45 p. http://documents.vsemirnyjbank.org/curated/ru/242991505976233066/SABER-education-management-information-systems-country-report-Ukraine-2017

24. Проєкт «КУРС: Освіта» http://ekyrs.org/ua/project/

25. Інтернет портал – сайт «Нові знання» https://nz.ua/

26. Сайт ІСУО ТОВ «Нові знання» https://isuo.org/ru/

27. Проект «КУРС: Освіта» http://dnz.ekyrs.org/ua/project/

28. Єдина державна електронна база з питань освіти https://info.edbo.gov.ua/about/

29. Актуальні питання реформування освіти в Україні : монографія / за ред. С. Л. Лондара ; ДНУ «Інститут освітньої аналітики». Київ, 2018. 246 с.

30. Офіційний сайт ІТС «ДІСО» http://diso.gov.ua/

31. Офіційний сайт Інституту освітньої аналітики [Електронний ресурс] – Режим доступу: http://iea.gov.ua/

32. Про введення в дослідну експлуатацію інформаційно-телекомунікаційної системи державної наукової установи «Інститут освітньої аналітики» «Державна інформаційна система освіти»: наказ МОН від 31.08.2016 №1054 http://diso.gov.ua/upload/Nakaz_1054.PDF;

33. Про затвердження Положення про інформаційно-телекомунікаційну систему державної наукової установи «Інститут освітньої аналітики»: Наказ МОН від 24.03.2016 №320 https://mon.gov.ua/ua/npa

34. Лондар С. Завдання модернізації державної інформаційної системи освіти (ДІСО). Освітня аналітика України. 2018. №1(2). – С.11-22.

35. Розробка та введення в дослідну експлуатацію інформаційно-телекомунікаційної системи «Державна інформаційна система освіти» [Текст]: звіт про НДР (закл.) / ДНУ «Інститут освітньої аналітики»; керівн. А. О. Литвинчук; викон.: А. В. Кир'янов [та ін.]. – К., 2019. – 162 с. – № держреєстрації 0117U003335.

36. БурячокВ.Л., ТолюпаС.В., АносовА.О., КозачокВ.А., Лукова-ЧуйкоН.В. Системнийаналізтаприйняттярішеньвінформаційнійбезпеці: підручник. / В.Л.

Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

37. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України http://www.dsszzi.gov.ua

38. Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 05.07.1994 № 80/94-ВР https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

39. Про захист персональних даних: закон України від 01.06.2010 № 2297-VI https://zakon.rada.gov.ua/laws/show/2297-17

40. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України від 29.03.06 № 373 https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF

41. Ватковська М. Формування інформаційної системи управління освітою як етап модернізації інформаційного забезпечення державного управління у галузі освіти України. Актуальні проблеми державного управління : зб. наук. пр. Харків, 2015. № 1 (47). 420 с.

42. Гришина Т. В. Освітня технологія як професійний пріоритет учителя. Харків : Основа, 2007. 153 с.

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ ОСВІТНЬОЇ АНАЛІТИКИ»
STATE SCIENTIFIC INSTITUTION «INSTITUTE OF EDUCATIONAL ANALYTICS»
вул. Володимира Винниченка, 5, м. Київ, 04053, тел. (044) 486 98 70
info@iea.gov.ua, http://iea.gov.ua/, СДРПОУ 39817791

26.05.2020 № 04-14/154
На № ___від __.__.2020

Державний університет телекомунікацій

Щодо впровадження результатів дослідження

Висновки та результати дипломної роботи Сологуба Я. Д. «РОЗРОБКА КОМПОНЕНТ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ В ОСВІТІ» використані при підготовці науково-дослідної роботи «Розробка та введення в дослідну експлуатацію інформаційно-телекомунікаційної системи «Державна інформаційна система освіти» (№ держреєстрації 0117U003335); рекомендації щодо розробки компонента інформаційної безпеки використано при підготовці Технічного завдання на модернізацію інформаційно-телекомунікаційної системи «Державна інформаційна система освіти».

Директор **Сергій ЛОНДАР**

Литвинчук А. 068-354-76-83

Додаток Б

Міністерство освіти і науки України
Державний університет телекомунікацій
Навчально-науковий інститут інформаційних технологій
Кафедра системного аналізу

«Розробка компонент інформаційних систем управління в освіті»

Виконав: студент групи САД-41
Сологуб Ярослав Дмитрович
Науковий керівник:
ст. викладач кафедри Системного аналізу, Штіммерман А.М

Київ-2020

1

Об'єкт дослідження – функціонування та розвиток інформаційних систем управління освітою.

Предмет дослідження – розробка компонент інформаційних систем управління в освіті.

Мета – дослідити функціонування та проаналізувати ефективності функціонування інформаційної системи управління освітою в Україні.

2

Завдання

- Проаналізувати теоретичні основи функціонування інформаційних систем управління освітою
- Вивчити зарубіжний та український досвід функціонування інформаційних систем управління освітою
- Проаналізувати ефективність функціонування інформаційно-телекомунікаційної системи «Державна інформаційна система освіти»
- Здійснити системній аналіз організації інформаційної безпеки

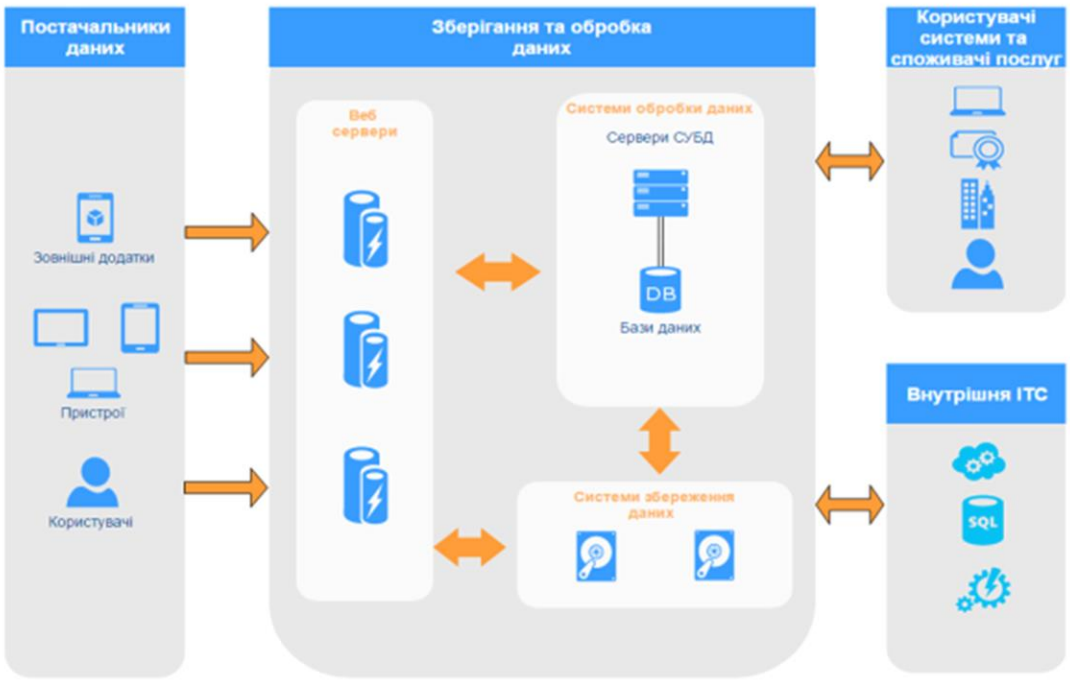
Схема функціонування EMIS

Порівняння функціоналу різних інформаційних систем у сфері освіти

Інформаційні системи освіти в Україні		Значення для системи освіти	Охоплення території	Фінансова доступність	Масштабованість	Додатковий функціонал
ІТС «ДІСО»		Державне значення (здійснення розподілу освітньої субвенції за інформацією, яка міститься в БД)	Усі заклади загальної середньої та дошкільної освіти	Безкоштовно	Є можливість забезпечувати розподіл будь-яких фінансово-матеріальних ресурсів	Має конструктор форм. Містить засоби налаштування для адаптації до змін статистичних форм та розширення переліку показників статистичної інформації. Містить технічну можливість для проведення опитувань за вимогою МОН.
Проект «КУРС: Освіта»	ІСУО«НВ» КУРС: Школа КУРС:Школа + КУРС:Дошкілля портал «NZ.UA»	Локальне значення	Заклади загальної середньої та дошкільної освіти, які уклали договори з ТОВ «Нові знання»	Платне	Частково має можливості забезпечувати розподіл підручників	Має конструктор форм. Містить засоби налаштування для адаптації до змін статистичних форм.
ЄДЕБО		Локальне значення. Передусім ведення реєстрів.	Усі заклади освіти	Частково платне	Не має можливостей розподілу ресурсів	Не має конструктору форм

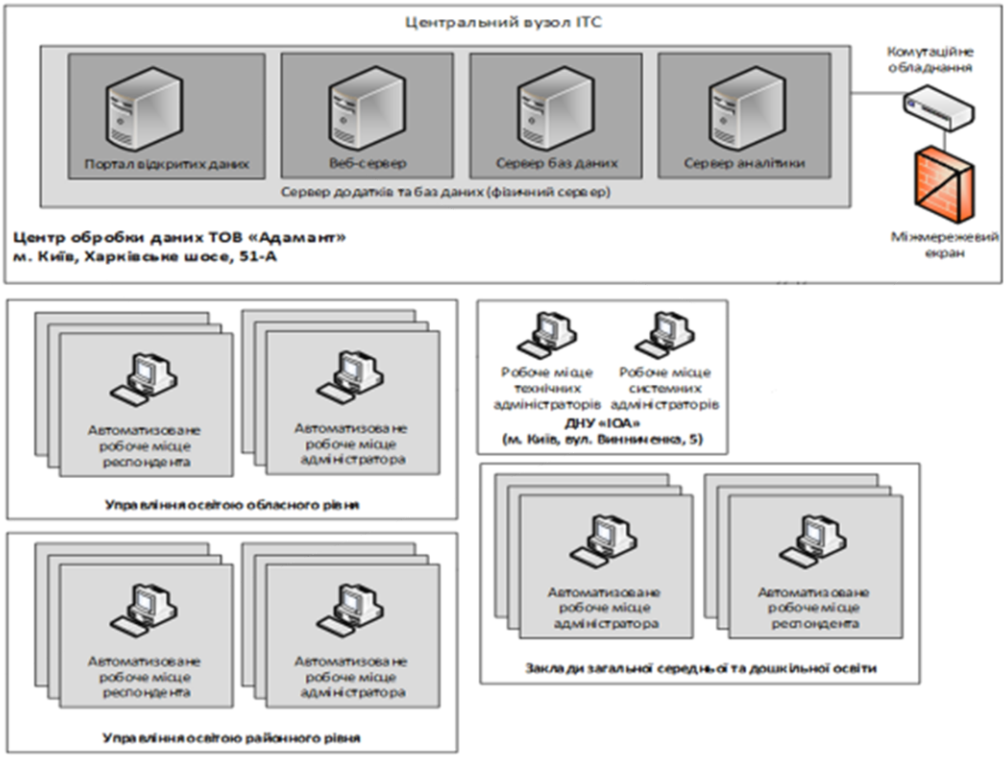
5

Схема програмно-апаратного забезпечення

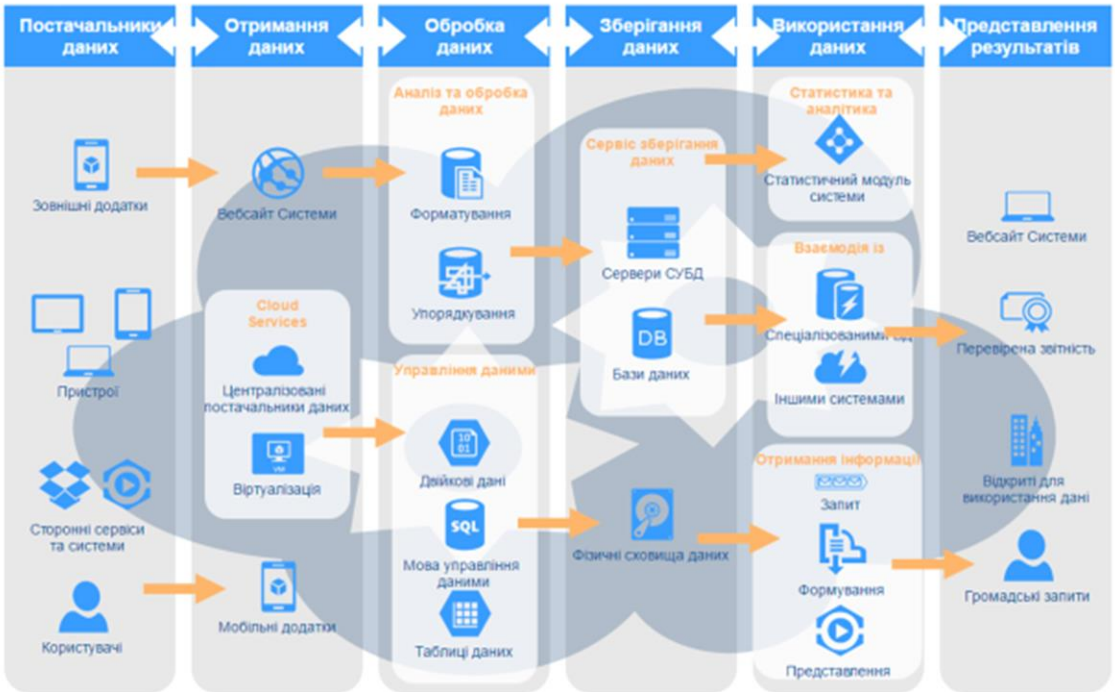


6

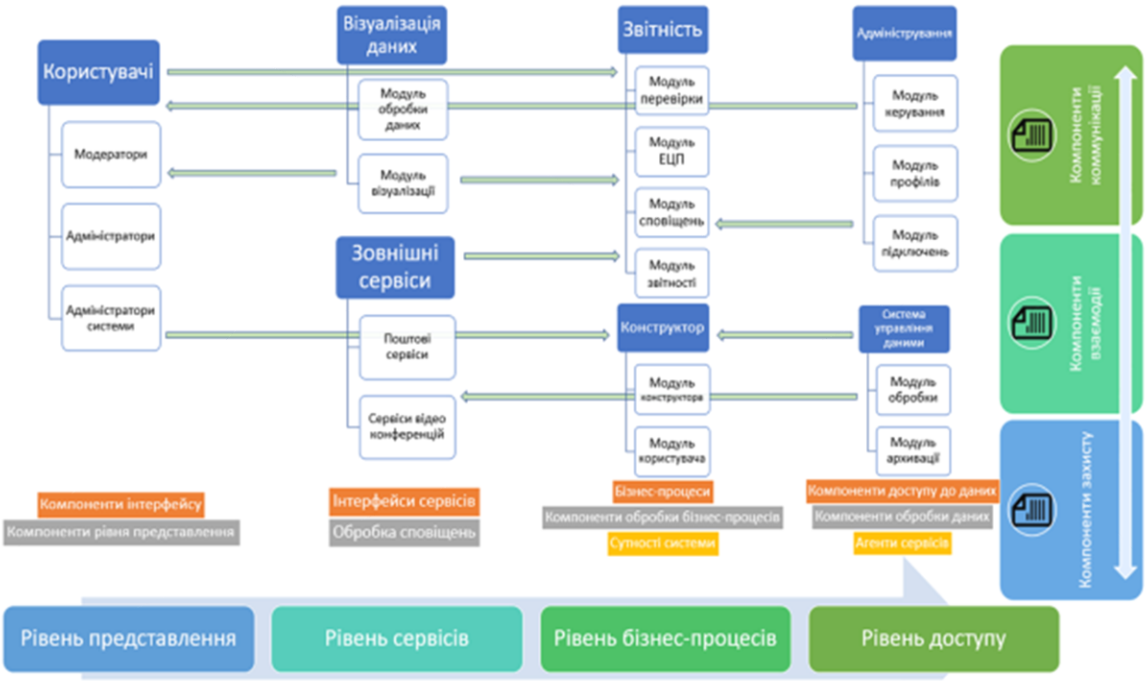
Функціональна схема ІТС



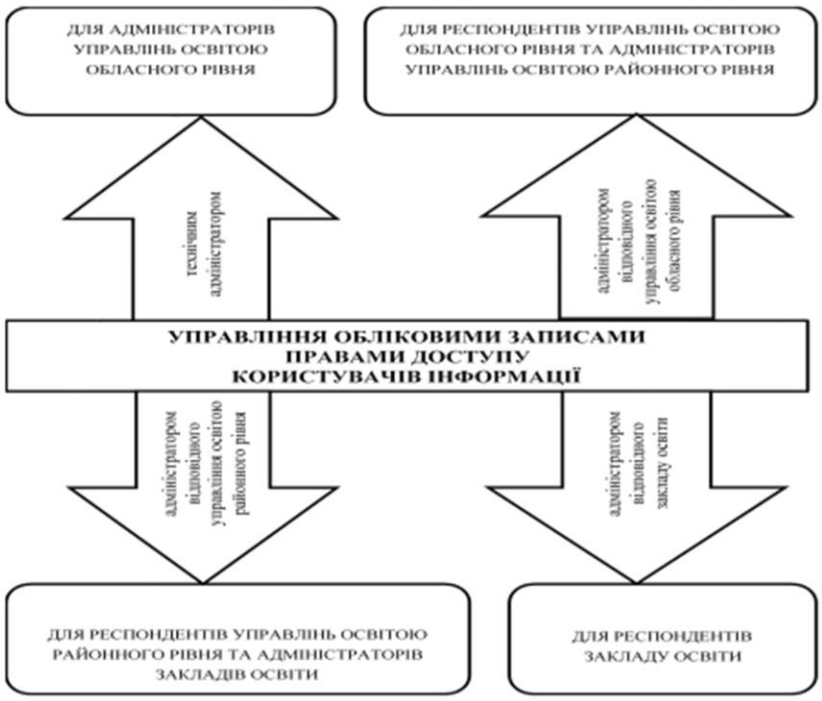
Принципова схема бізнес-процесу ІТС ДІСО



Програмно-апаратна архітектура ІТС ДІСО



Управління обліковими записами та правами доступу користувачів інформації, що зберігається в БД



Ризики загроз ІТС «ДІСО»

ЗАГРОЗИ СУБ'ЄКТИВНОЇ ПРИРОДИ

- випадкові зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту), такі як стихійні лиха і аварії, землетрус, повінь, пожежа або інші випадкові події;
- випадкові зміни умов внутрішнього фізичного середовища (усередині будівлі або контрольованої зони) такі, як аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, затоплення приміщень унаслідок аварії інж енерних комунікацій водопостачання та опалення, пожежа та інші випадкові події;
- випадкові збої і відмови в роботі оснащення і технічних засобів компонентів ІТС.

ЗАГРОЗИ ОБ'ЄКТИВНОЇ ПРИРОДИ

- навмисні зміни умов зовнішнього фізичного середовища (за межами будівлі або контрольованої зони об'єкту), такі як впливи (аварії, пожежі або інші навмисні події) на комутаційні вузли і канали (тракти) передачі первинної мережі зв'язку і т.п.;
- навмисна зміна умов внутрішнього фізичного середовища (усередині будівлі бо контрольованої зони), такі як аварія системи електропостачання приміщень будівлі, руйнування будівельних конструкцій приміщень будівлі, затоплення приміщень унаслідок аварії інженерних комунікацій водопостачання та опалення, пожежа або інші навмисні події;
- наслідки помилок під час проектування і розробки компонентів ІТС (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);
- помилки п ерсоналу (користувачів) ІТС під час експлуатації обладнання і технічних засобів компонентів ІТС;
- навмисні дії (спроби) потенційних порушників під час експлуатації обладнання і технічних засобів компонентів ІТС.

Класифікація внутрішніх порушників в компонентах ІТС

Ступінь небезпеки	Групи внутрішніх порушників	Критерії класифікації																
		Рівні можливостей				Рівні знань про ІТС				Методи і способи порушень				Місце здійснення дії				
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	5
1	Системні адміністратори				+				+				+			+	+	+
2	Технічні адміністратори			+					+				+			+	+	+
3	Користувачі	+				+				+				+		+		
4	Розробники прикладного ПЗ		+*		+*	+	+	+	+	+	+	+	+			+	+	+
5	Постачальники обладнання технічних засобів				+			+		+	+	+	+			+	+	
6	Технічний персонал									+	+				+			

Основний результат роботи

Здійсненні системного аналізу функціонування ІТС «ДІСО», що дозволило визначити напрями підвищення ефективності в частині посилення інформаційної безпеки, зокрема: розроблено компонент інформаційної безпеки ІТС «ДІСО» в частині управління обліковими записами та правами доступу користувачів до інформації, що зберігається в БД; визначено ступінь загрози з боку зовнішніх та внутрішніх порушників.

Практична значущість результатів дослідження.

Практичне значення роботи передусім полягає у розробленні компоненту інформаційної безпеки ІТС «ДІСО» ДНУ «Інститут освітньої аналітики» (довідка від 26.05.2020 № 04-14/154).

Також результати дослідження пройшли апробацію на науково-практичних конференціях: І Міжнародна науково-практична конференція «Реформа освіти в Україні інформаційно-аналітичне забезпечення», 29 листопада 2017 року, м.Київ, ДНУ «ІОА» (тези: Кир'янов А., Сологуб Я. Основна мета та завдання інформаційної системи освіти); Науково-практична конференція «Системний аналіз в бізнесі та управлінні», 17 квітня 2020 року, м.Київ, ДУТ (тези: Литвинчук А.О., Терещенко Г.М., Сологуб Я.Д. Розвиток інформаційних систем освітнього менеджменту).

Висновки

1. Системний аналіз функціонування ІСУО в зарубіжних країнах дозволив визначити переваги та недоліки систем та визначити напрями розвитку для України
2. Проведений порівняльний аналіз функціонування ІСУО в Україні показав розрізненість БД та обмеженість функціоналу у переважній більшості систем
3. Встановлено, що найбільш функціональною та масштабною є ІТС «ДІСО», що забезпечує якісний інформаційний супровід МОН в процесі ухвалення управлінських рішень
4. Системний аналіз ІТС «ДІСО» виявив недоліки захисту інформації в системі
5. Розроблено компонент ІТС «ДІСО» в частині управління обліковими записами та правами доступу користувачів щодо доступу до інформації, що зберігається в базі даних

Дякую за увагу!