

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)

Кафедра Інформаційних управляючих систем
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження методів оцінювання ефективності функціонування ІС
центрів сертифікації електронно-цифрових підписів
(тема)

Виконав:

студент 2 курсу, групи ІУСТМ-22-1
Соловійова Єлизавета Ігорівна
(прізвище, ім'я, по батькові)

Спеціальність 122 Комп'ютерні науки
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційні управляючі системи та технології
(повна назва освітньої програми)

Керівник доц. каф. ІУС Аліна МІХНОВА
(посада, власне ім'я, ПРІЗВИЩЕ)

Допускається до захисту

Зав. кафедри


(підпис)

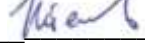
Костянтин ПЕТРОВ
(власне ім'я, ПРІЗВИЩЕ)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
 Кафедра Інформаційних управляючих систем
 Рівень вищої освіти другий (магістерський)
 Спеціальність 122 Комп'ютерні науки
 (код і повна назва)
 Тип програми освітньо-професійна
 (освітньо-професійна або освітньо-наукова)
 Освітня програма Інформаційні управляючі системи та технології
 (повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри 
 (підпис)

« 20 » листопада 20 23 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ


студентові Соловйовій Єлизаветі Ігорівні
 (прізвище, ім'я, по батькові)


- Тема роботи Дослідження методів оцінювання ефективності функціонування ІС центрів сертифікації електронно-цифрових підписів
 затверджена наказом університету від 16 листопада 2023 р. № 1359 Ст.
- Термін подання студентом роботи до екзаменаційної комісії 18 січня 2024 р.
- Вихідні дані до роботи матеріали звіту з передатестаційної практики, опис процесу обліку видачі сертифікатів електронно-цифрових підписів, науково-технічна література та інтернет джерела щодо методів оцінювання ефективності функціонування інформаційних систем, існуючих інформаційних систем центрів сертифікації ключів, класифікацій інформаційних систем, нормативно-правові акти, які діють в рамках закону про електронні довірчі послуги.
- Перелік питань, що потрібно опрацювати в роботі дослідження сучасного стану інформаційних систем центрів сертифікації ключів; дослідження існуючих методів оцінювання ефективності функціонування інформаційних систем; методика використання методів оцінювання ефективності функціонування інформаційних систем центрів сертифікації ключів; апробація результатів дослідження.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Дослідження діяльності центрів сертифікації ключів та особливостей інформаційних систем центрів сертифікації ключів як предметної області	20.11.2023 – 28.11.2023	Виконано
2	Аналіз існуючих методів оцінювання ефективності функціонування інформаційних систем	29.11.2023 – 08.12.2023	Виконано
3	Формування вимог до інформаційних систем із урахуванням особливостей функціонування центрів сертифікації ключів	09.12.2023 – 13.12.2023	Виконано
4	Розробка методу оцінювання ефективності функціонування інформаційних систем центрів сертифікації ключів	14.12.2023 – 20.12.2023	Виконано
5	Формування критерію оцінювання ефективності функціонування інформаційних систем центрів сертифікації ключів	21.12.2023 – 25.12.2023	Виконано
6	Обґрунтування вибору інформаційних системах в залежності від класів центрів сертифікації ключів	26.12.2023 – 30.12.2023	Виконано
7	Проведення апробації результатів досліджень	31.12.2023 – 03.01.2024	Виконано
8	Оформлення пояснювальної записки	04.01.2024 – 08.01.2024	Виконано
9	Захист кваліфікаційної роботи	19.01.2024	Виконано

Дата видачі завдання 20 листопада 2023 р.

Студент 
(підпис)

Керівник роботи 
(підпис)

доц. каф. ІУС Аліна МІХНОВА
(посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи містить: 88 с., 20 рис., 9 табл., 16 джерел, 1 додаток.

ЕЛЕКТРОННО-ЦИФРОВИЙ ПІДПИС, ІНФОРМАЦІЙНА СИСТЕМА, КРИТЕРІЙ, МЕТОД ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ, СЕРТИФІКАТ, СУКУПНА ВАРТІСТЬ ВОЛОДІННЯ, ТЕХНІЧНІ ХАРАКТЕРИСТИКИ, ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ, ЦЕНТР СЕРТИФІКАЦІЇ КЛЮЧІВ.

Метою кваліфікаційної роботи є дослідження методів оцінювання ефективності функціонування інформаційних систем центрів сертифікації ключів з метою вибору найефективнішої інформаційної системи для роботи з електронно-цифровими підписами.

Об'єктом дослідження в рамках цієї магістерської кваліфікаційної роботи є інформаційні системи центрів сертифікації ключів.

Предметом дослідження є методи оцінювання ефективності функціонування інформаційних систем центрів сертифікації ключів.

В ході дослідження отримані такі результати: проаналізовано центри сертифікації ключів та особливості їх інформаційних систем, проведено аналіз існуючих методів оцінювання ефективності функціонування інформаційних систем центрів сертифікації ключів із вибором тих, що найкраще підходять для роботи в галузі електронно-цифрових підписів, сформовано критерій оцінювання ефективності функціонування інформаційних систем центрів сертифікації ключів, запропоновано метод оцінювання ефективності функціонування інформаційних систем центрів сертифікації ключів, було наведено методику використання запропонованого методу та проведено його апробацію.

ABSTRACT

The explanatory note to the qualification work contains: 88 pages, 20 figures, 9 tables, 16 sources, 1 appendix.

ELECTRONIC-DIGITAL SIGNATURE, INFORMATION SYSTEM, CRITERION, PERFORMANCE ASSESSMENT METHOD, CERTIFICATE, TOTAL COST OF OWNERSHIP, TECHNICAL CHARACTERISTICS, FUNCTIONAL CAPABILITIES, KEY CERTIFICATION CENTER.

The purpose of the qualification work is to study the methods of evaluating the effectiveness of the functioning of information systems of key certification centers with the aim of choosing the most effective information system for working with electronic digital signatures.

The object of research within the framework of this master's qualification work is information systems of key certification centers.

The subject of the study is methods of evaluating the effectiveness of the functioning of information systems of key certification centers.

During the investigation, the following results were obtained: the key certification centers and the features of their information systems were analyzed, and the analysis of other methods for assessing the effectiveness of information management functions was carried out. Of these key certification center systems, from the selection of those that are most suitable for working in the field of electronic digital signatures, a criterion has been formed for assessing the effectiveness of the operation information systems of key certification centers, a method for assessing the effectiveness of the functioning of information systems of key certification centers was established, a method for revising the established method was established, and testing was carried out.

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ДПС – державна податкова служба

ІС – інформаційна система

ЕЦП – електронно-цифровий підпис

КНЕДП – кваліфікований надавач електронних довірчих послуг

ЦСК – центр сертифікації ключів

ЗМІСТ

Скорочення та умовні позначки	6
Вступ.....	9
1 Огляд та аналіз існуючих ІС ЦСК та методів оцінювання їх функціонування	10
1.1 Опис предметної області.....	10
1.2 Огляд та аналіз особливостей ІС ЦСК.....	16
1.3 Аналіз існуючих методів оцінювання ефективності функціонування ІС.....	19
1.4 Постановка задачі дослідження.....	22
2 Проведення дослідження методів оцінювання функціонування ІС ЦСК	23
2.1 Формування вимог до ІС з урахуванням особливостей функціонування ЦСК.....	23
2.2 Формування критерію оцінювання ефективності функціонування ІС ЦСК.....	25
2.3 Побудова методу оцінювання ефективності ІС ЦСК на основі існуючих методів.....	28
3 Методика використання запропонованого методу оцінювання функціонування ІС ЦСК.....	31
3.1 Відмінності в ІС в залежності від класу ЦСК.....	31
3.2 Формування алгоритмів використання запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу або при впровадженні нової ІС) з урахуванням особливостей для певних ЦСК.....	38
4 Апробація запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу)	46
4.1 Опис діяльності ЦСК та визначення його типу за запропонованою класифікацією.....	46

4.2 Формування варіантів проєктних рішень для реінжинірингу ІС.....	51
4.3 Обґрунтування вибору варіанту проєктного рішення для реінжинірингу ІС.....	57
Висновки	66
Перелік джерел посилання	67
Додаток А Графічний матеріал.....	70

ВСТУП

Ключовим словом сучасності без сумнівів є слово «спрощення». Люди прагнуть спростити все – від прослуховування музики до розробки нових технологій. Люди прагнуть вирішувати поточні питання та проблеми сидячі за монітором комп'ютера або ноутбука, та зайвий раз нікуди не ходити.

Цей факт торкається й людей, що працюють із електронно-цифровими підписами, що означає, що більшість документів вже підписуються саме в електронному вигляді. Саме тому центри сертифікації ключів зараз активно проводять дослідження по поліпшенню, модернізації інформаційних систем, впровадженню нових інформаційних систем, усуненню недоліків роботи з видачею сертифікатів електронно-цифрових підписів тощо.

В такій ситуації просто необхідно знаходити найкращі варіанти, що принесуть максимальну ефективність при мінімальних витратах. Тому оцінювання ефективності інформаційних систем – одна із найпоширеніших потреб в галузі електронних довірчих послуг.

Саме в цьому і полягає актуальність кваліфікаційної роботи – дослідження методів оцінювання ефективності інформаційних систем центрів сертифікації ключів принесе вигоду для багатьох підприємств, що хочуть провести реінжиніринг старої інформаційної системи або провести впровадження нової інформаційної системи.

1 ОГЛЯД ТА АНАЛІЗ ІСНУЮЧИХ ІС ЦСК ТА МЕТОДІВ ОЦІНЮВАННЯ ЇХ ФУНКЦІОНУВАННЯ

1.1 Опис предметної області

Центр сертифікації ключів – це кваліфікований надавач електронних довірчих послуг, що має розгалужену мережу представництв у багатьох регіонах України [1].

Це підприємство, що виконує багато функцій, серед яких створення, перевірка та підтвердження електронно-цифрового підпису чи печатки; формування, перевірка та підтвердження чинності сертифіката електронно-цифрового підпису (ЕЦП) чи печатки; формування, перевірка та підтвердження кваліфікованої електронної позначки часу.

Сертифікати електронно-цифрового підпису надаються у вигляді окремих апаратних чи апаратно-програмних засобів ЕЦП, які є частиною програмно технічного комплексу, а також окремих програмних додатків або програмних модулів [2].

ЕЦП може використовуватися в наступних ситуаціях:

- для підписання звітності до контролюючих органів;
- для обміну електронними документами з контрагентами (М.Е.Дос, тощо);
- для отримання державних електронних послуг громадян України у веб-сервісах та порталах.

На рисунку 1.1 показано спрощене зображення варіантів документів для підписання ЕЦП.



Рисунок 1.1 – Спрощене зображення варіантів документів для підписання
ЕЦП

Усього в Україні працює тридцять акредитованих центрів сертифікації ключів, більшість з яких є державними.

Як показові центри сертифікації ключів (ЦСК) були обрані такі: ЦСК «Україна», кваліфікований надавач електронних довірчих послуг (КНЕДП) Державної податкової служби (ДПС) України, «Дія.Підпис», «SmartID», КНЕДП «Банк Альянс». Для даних ЦСК необхідно провести детальний огляд та порівняльний аналіз особливостей функціонування з урахуванням використання в них інформаційних систем ЦСК.

ЦСК «Україна» – кваліфікований надавач електронних довірчих послуг, що має розгалужену мережу представництв у всіх регіонах України [1].

Згідно до законодавства, цей КНЕДП, як і більшість інших, здійснює первинне отримання сертифікату ЕЦП лише в особистій присутності за наявності усіх потрібних документів. Але ЦСК «Україна» має інформаційну систему, що дозволяє автоматично продовжити діючі сертифікати онлайн.

Кроки, які потрібно пройти клієнту, для автопродовження:

- вхід до особистого кабінету в програмі «MEDOC»;
- вхід на сторінку підгружених діючих сертифікатів;
- натискання кнопки «Автопродовжити»;

- вибір сертифікатів для автопродовження;
- натискання кнопки «Робити»;
- очікування повідомлення про успішне автопродовження.

Переваги: зручне відображення діючих сертифікатів, серед яких можна легко вибрати потрібні для автопродовження, також можна вибрати термін дії ЕЦП – 1 або 2 роки і вибрати спосіб зберігання – файловий або захищений носій.

До недоліків можна віднести доволі низьку швидкість генерації сертифікату відносно інших КНЕДП, бо тут процес створення сертифікату ЕЦП відбувається вручну відповідними робітниками ЦСК «Україна». Крім того, програма «MEDOC» немає мобільного аналогу, через що автопродовження можна замовляти лише при наявності комп'ютеру.

КНЕДП Державної податкової служби України є акредитованим центром сертифікації ключів, де можна отримати як первинні електронно-цифрові підписи, так і повторні.

Отримання перших проводиться лише в особистій присутності клієнта в одному із відділень із певним переліком документів на руках. А повторне отримання можна замовити на офіційному сайті при умові, що термін дії сертифікату, який буде продовжено, ще не закінчився. Проходить процедура таким чином [3]:

- зчитування діючого електронно-цифрового підпису за допомогою вивантаження відповідного файлу;
- підписання договору із заповненням особистих даних;
- створення нового сертифікату ЕЦП.

На сторінці присвяченій автопродовженню сертифікатів ЕЦП на офіційному сайті ДПС присутня відповідна форма для заповнення даних, а також інструкція, скрін якої наведено на рисунку 1.2.

Повторне (дистанційне) формування сертифікатів за електронним запитом



Рисунок 1.2 – Інструкція для процесу автопродовження ЕЦП в КНЕДП ДПС

КНЕДП ДПС – один із найзручніших центрів сертифікації ключів, що має велику кількість переваг. Серед них: безкоштовність, безпечність, швидкість, декілька варіантів вибору носія сертифікату ЕЦП – файловий або захищений та інші.

Але все ж є декілька вагомих недоліків. Наприклад, відсутність мобільної версії, через яку процес автопродовження полегшився би в разі, відсутність вибору терміну дії сертифікату ЕЦП – можна створити лише на 2 роки та відсутність відображення діючих сертифікатів, серед яких можна би було вибрати потрібний замість особистого вивантаження файлу.

«Дія.Підпис» – це зручний та надійний інструмент роботи з інформацією в електронному вигляді [4]. Отримання електронно-цифрового підпису через державний портал здійснюється за допомогою декількох кроків:

- авторизація у застосунку «Дія»;
- перехід «Меню» → «Дія.Підпис»;
- натискання кнопки «Створити Дія.Підпис»;
- підтвердження особи через камеру у реальному часі;
- створення особистого п'ятизначного пінкоду;

– отримання електронно-цифрового підпису.

На рисунку 1.3 представлено приклад отримання електронно-цифрового підпису в графічному вигляді.

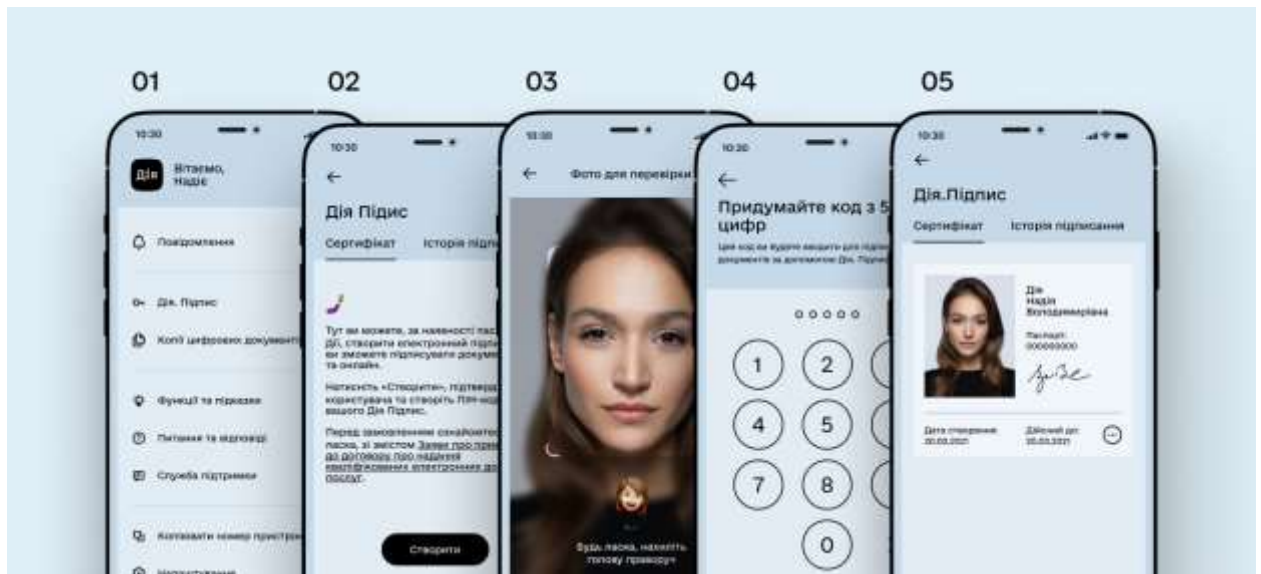


Рисунок 1.3 – Приклад створення ЕЦП в «Дія.Підпис»

Великою перевагою інформаційної системи «Дія.Підпис» є можливість отримання первинного електронно-цифрового підпису онлайн, а не офлайн, як в більшості інших ЦСК. Причиною тому є наявність підтверджених документів у самому застосунку «Дія», що миттєво генерує сертифікат ЕЦП після проходження деяких обов'язкових кроків, описаних вище. Крім того, отримати ЕЦП можна безкоштовно, що приваблює користувачів.

Із недоліків можна визначити термін дії сертифікату та недосконалу систему перевірки особи через фото. Система перевірки особи через камеру може сильно помилятися. Програма може довгий час не підтверджувати особу, як би людина не тримала телефон, а також навпаки може підтверджувати особистість, коли шахраї користуються програмами, що здатні змінювати обличчя.

«SmartID» – це кваліфікований електронний підпис від «ПриватБанку», який можна отримати у додатку «Приват24». Кроки для генерації ЕЦП:

- авторизація у комп'ютерній версії додатку «Приват24»;
- «Усі послуги» → «Бізнес» → «Завантажити сертифікат»;
- перевірка коректності особистих даних;
- введення паролю до сховища ключів;
- введення коду, що прийшов у SMS за особистим номером, або підтвердження у мобільній версії додатку «Приват24»;
- отримання файлу з ключем та завантаження його у комп'ютер.

На рисунку 1.4 показано, де в комп'ютерній версії додатку «Приват24» можна знайти послугу створення сертифікатів ЕЦП.

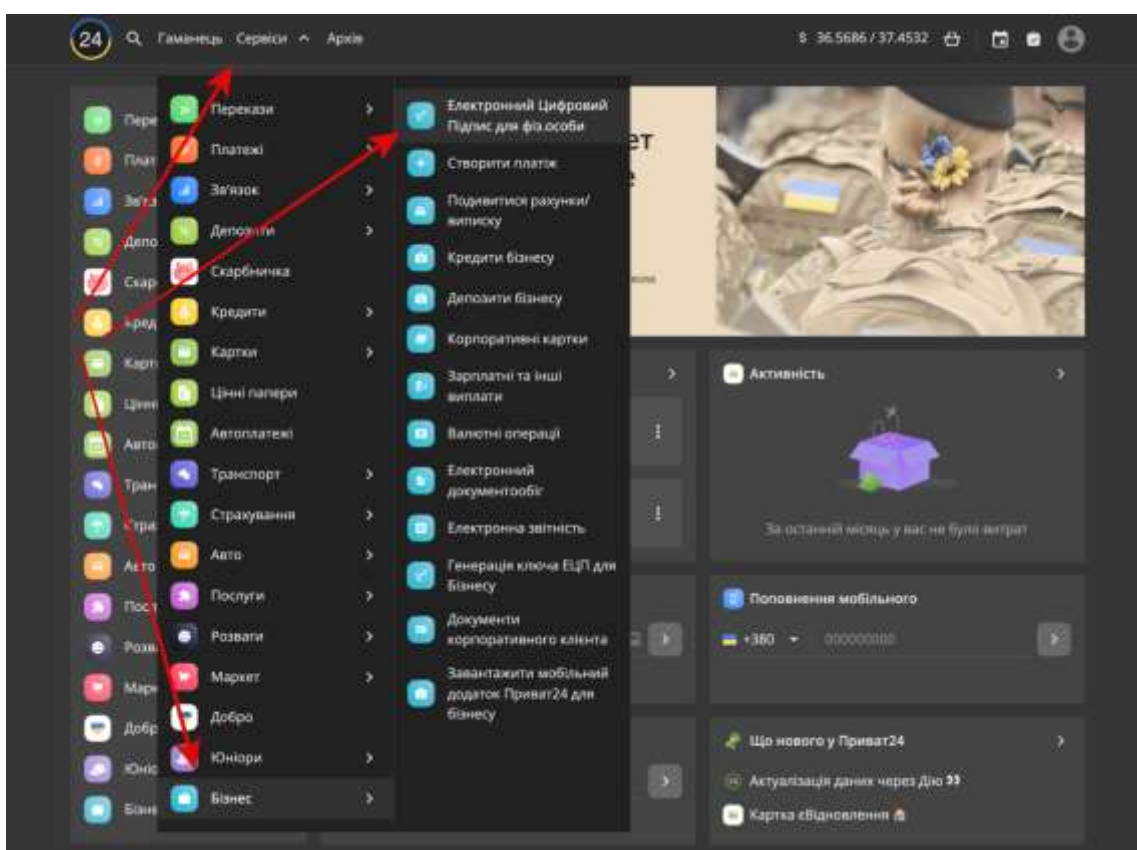


Рисунок 1.4 – Місцезнаходження послуги створення «SmartID»

Із плюсів можна визначити можливість отримання ЕЦП у файловому форматі, безкоштовність послуги та, звісно, можливість отримання первинного сертифікату через інтернет, а не за фізичною присутністю.

Головні недоліки: обмежена варіація термінів дії сертифікату ЕЦП – лише один рік, як і в «Дія.Підпис», та проблеми з генерацією ЕЦП через додаток «Приват24» у смартфоні.

КНЕДП «Банк Альянс» – кваліфікований надавач електронних довірчих послуг, що підтримує використання користувачами КНЕДП електронно-цифрового підпису [5].

Інформаційна система КНЕДП «Банк Альянс» є найнедосконалішою та найневигіднішою серед усіх представлених ІС. Через неї можна лише сформувавши заявку на продовження сертифікату ЕЦП, з друківкою якої треба особисто приходити до будь-якого центру реєстрації КНЕДП для генерації нових ключів та формування сертифікату [5].

Так процес продовження ЕЦП відрізняється від процесу первинного отримання лише кількістю документів, які треба мати з собою (в першому випадку потрібен тільки паспорт/ ID-картка).

1.2 Огляд та аналіз особливостей ІС ЦСК

Як було сказано вище, в Україні існує тридцять акредитованих організацій, що займаються видачею сертифікатів електронно-цифрових підписів, і кожна з них має власну інформаційну систему зі своїми недоліками і перевагами.

Для директорів нових компаній, які тільки вливаються у потік роботи із електронним документообігом, важливо обрати найкращу ІС, яку можна було би взяти за основу при розробці своєї власної. Нижче описано переваги і недоліки інформаційних систем обраних центрів сертифікації ключів.

Інформаційна система ЦСК «Україна»:

– переваги: зручний користувацький інтерфейс, а саме – відображення діючих сертифікатів, серед яких можна легко вибрати потрібні

для автопродовження; пропускна здатність, масштабованість, гнучкість, надійність і захищеність ІС на високому рівні;

- недоліки: відсутність мобільного аналогу, через що автопродовження можна замовляти лише при наявності комп'ютеру.

Інформаційна система КНЕДП ДПС:

- переваги: високий рівень захищеності даних, надійності, масштабованості і зручний інтерфейс;

- недоліки: відсутність мобільної версії, через яку процес автопродовження полегшився би в разі, а також пропускна здатність і гнучкість середнього рівня.

Інформаційна система «Дія.Підпис»:

- переваги: високого рівня пропускна здатність, надійність, масштабованість, гнучкість і зручний інтерфейс;

- недоліки: захищеність даних, а саме – недосконала система перевірки особи через фото.

Інформаційна система «SmartID»:

- переваги: великого рівня захищеність даних, надійність, масштабованість, гнучкість і зручний інтерфейс;

- недоліки: проблеми з генерацією ЕЦП через додаток «Приват24» у смартфоні, а також доволі середня пропускна здатність.

Інформаційна система КНЕДП «Банк Альянс»:

- переваги: достатньо великого рівня захищеність даних та надійність;

- недоліки: відсутність мобільного додатку, низького рівня гнучкість, масштабованість, пропускна здатність, а також поганий інтерфейс.

В таблиці 1.1 проводиться порівняння ІС обраних ЦСК за такими показниками: «пропускна здатність», «захищеність даних», «надійність», «масштабованість», «гнучкість», «зручний інтерфейс» по п'ятибальній шкалі:

5 – найвищий бал (або є така послуга), 1 – найнижчий бал, 0 – немає такої послуги.

Таблиця 1.1 – Порівняльна таблиця існуючих інформаційних систем для видачі сертифікатів ЕЦП

Показники \ ІС ЦСК	ЦСК «Україна»	КНЕДП ДПС України	«Дія.Підпис»	«SmartID»	КНЕДП «Банк Альянс»
Пропускна здатність	5	3	4	3	2
Захищеність даних	5	5	2	4	4
Надійність	4	4	4	4	4
Масштабованість	5	4	4	4	3
Гнучкість	5	3	5	4	1
Зручний інтерфейс	4	4	5	5	1

Проведений аналіз щодо можливостей інформаційних систем, за допомогою яких здійснюється видача сертифікатів електронно-цифрових підписів, показав, що кожна з систем має свої переваги та недоліки.

Найбільш широкий функціонал показали інформаційні системи ЦСК «України» та «Дія.Підпис», які користуються найбільшою популярністю серед клієнтів. А найвужчий функціонал показала ІС КНЕДП «Банк Альянс», яка наразі немає більшості характеристик, які мають її конкуренти.

Ефективність функціонування ІС ЦСК можливо дослідити з використанням відповідних методів.

1.3 Аналіз існуючих методів оцінювання ефективності функціонування ІС

Існує безліч методів оцінювання ефективності функціонування інформаційних систем, кожен із яких має різний підхід, показники, а також сферу використання. Як показникові, були вибрані такі: «стандарт-кост», «функціонально-вартісний аналіз», «внутрішня норма прибутку», «бенчмаркінг», «перевірка забезпечення якості», «аналіз економічної ефективності» та «аналіз охоплення даних».

Огляд та аналіз існуючих методів оцінювання ефективності функціонування інформаційних систем представлений в таблиці 1.2.

Таблиця 1.2 – Аналіз існуючих методів оцінювання ефективності функціонування ІС

Методи оцінювання	Опис	Характеристика	Показники
Стандарт-кост (облік нормативних витрат)	Основним завданням, яке ставить перед собою ця методика, є облік відхилень від стандартів (норм) і аналіз причин їх виникнення [6].	Метод спрямований на усунення проблем або недоліків, а також на удосконалення при прийнятті управлінських рішень.	Фактичні затрати, затрати в межах норм, відхилення внаслідок їх змін і відхилення внаслідок технічних, технологічних, організаційних та інших причин.
Функціонально-вартісний аналіз	Ставиться питання, наскільки виправдані витрати з урахуванням отриманих властивостей ІС, що задовольняють ті чи інші запити і потреби [7].	Точне знання вартості продукції дає змогу приймати правильні стратегічні рішення та сприяє якісній реалізації управлінських функцій [8].	Ефективність (пропускна здатність, безпека, надійність, інтерфейс і тощо), ціна.

Продовження таблиці 1.2

Методи оцінювання	Опис	Характеристика	Показники
Внутрішня норма прибутку	Характеризується максимально допустимий відносний рівень витрат, які можуть бути здійснені під час реалізації проекту [9].	Можливість порівняння різних інвестиційних проектів між собою з метою визначення найбільш економічно ефективних за наявним капіталом.	Внутрішня норма прибутку, часовий період, чистий приплив грошових коштів за часовий період, загальна вартість початкових інвестицій.
Бенчмаркінг	За допомогою порівняльного аналізу виявляються альтернативні рішення, серед яких обираються ті, що принесуть найкращий результат з точки зору майбутньої перспективи [10].	Виявлення сильних і слабких сторін ІС в залежності від зміни попиту, пропозиції та ринкового середовища, визначення об'єктивного рівня продуктивності.	Будь-які (пропускна здатність, безпека, надійність, інтерфейс і тощо).
Перевірка забезпечення якості	Визначаються показники програмної якості ІС [11].	Відстежуючи показники контролю якості, можна визначати сфери вдосконалення, приймати рішення на основі даних і гарантувати, що програмне забезпечення відповідає бажаним стандартам якості.	Помилки, виявлені в одному тесті, загальна кількість помилок, знайдених у тестах і після випуску.

Кінець таблиці 1.2

Методи оцінювання	Опис	Характеристика	Показники
Аналіз економічної ефективності	Визначаються найбільш ефективні втручання шляхом порівняння вартості різних втручань з їхніми результатами або впливом [12].	Визначаючи найбільш економічно ефективні втручання, особи, які приймають рішення, можуть досягти максимального впливу з мінімальними ресурсами [12].	Вартість втручання, ефект з втручання (підвищення пропускної здатності, покращення безпеки і тощо).
Аналіз охоплення даних	Використовуються математичні моделі для порівняння відносної ефективності кожної програми або втручання шляхом порівняння його входів і результатів [12].	Може вміщувати кілька входів і виходів і не потребує попередньо визначеного їх зважування, використовується для визначення найкращих практик і контрольних показників продуктивності програми [12].	Вхідна інформація (технічне забезпечення, робота працівників і тощо), вихідна інформація (сама програма), ваги кожної інформації.

Серед методів оцінювання ефективності функціонування ІС, представлених в таблиці 1.2, найкращими для галузі електронно-цифрових підписів вважаються «перевірка забезпечення якості» та «функціонально-вартісний аналіз».

Перший був обраний тому, що в ньому визначаються показники програмної якості ІС, які є дуже важливими для розуміння технічних і програмних характеристик ІС. А другий – допомагає зіставити кошти із функціональними характеристиками, що просто необхідно для розуміння вигоди від певної ІС.

1.4 Постановка задачі дослідження

В першому розділі проведено огляд та аналіз особливостей інформаційних систем центрів сертифікації ключів із визначенням їх переваг та недоліків, а також проведено порівняння ІС між собою із подальшим визначенням найкращих і найгірших.

Наведено аналіз деяких існуючих методів оцінювання ефективності функціонування, де було визначено їх опис, характеристики, а також основні показники.

В результаті проведеного дослідження було виявлено два методи, які є найкращими в галузі електронного документообігу: «перевірка забезпечення якості» та «функціонально-вартісний аналіз».

На підставі вищезазначеного можна наступним чином сформулювати постановку задачі дослідження:

- формування вимог до ІС з урахуванням особливостей функціонування ЦСК;
- формування критерію оцінювання ефективності функціонування ІС ЦСК;
- побудова методу оцінювання ефективності функціонування ІС ЦСК;
- проведення аналізу відмінностей в ІС в залежності від класу ЦСК;
- формування алгоритмів використання запропонованого методу оцінювання ефективності функціонування ІС ЦСК з урахуванням особливостей для певних ЦСК;
- апробація запропонованого методу оцінювання ефективності функціонування ІС ЦСК «Харків».

2 ПРОВЕДЕННЯ ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНЮВАННЯ ФУНКЦІОНУВАННЯ ІС ЦСК

2.1 Формування вимог до ІС з урахуванням особливостей функціонування ЦСК

Процес вибору інформаційної системи проводиться дуже великим числом показників у кожному конкретному випадку, щоб можна було говорити про якісь рекомендації загального характеру. В даному випадку – ІС ЦСК – ці показники будуть формуватися із різноманітних вимог до інформаційної системи.

Основна вимога, якої слід керуватися при виборі найвигіднішої інформаційної системи, – це задоволення потреб бізнесу підприємства. В галузі електронно-цифрових підписів задоволення потреб бізнесу – це ефективна робота в сфері електронних довірчих послуг, яка і приносить прибуток ЦСК. При розгляданні задоволення потреб бізнесу доцільно розглядати три групи вимог:

- ІС має задовольняти функціональним вимогам, які висуває підприємство;
- ІС має задовольняти технічним вимогам, які висуває підприємство;
- витрати на ІС мають не перевищувати зазначений бюджет.

Таким чином, кожна вищеприсана вимога перекривається відповідною множиною показників, що складається із багатьох показників, які використовуються в оцінюванні ефективності функціонування ІС ЦСК. Відповідні множини показників:

- функціональні можливості (F);
- технічні характеристики (Т);
- сукупна вартість володіння (С).

На рисунку 2.1 показано вимоги до ІС ЦСК, а також відповідні їм множини показників.

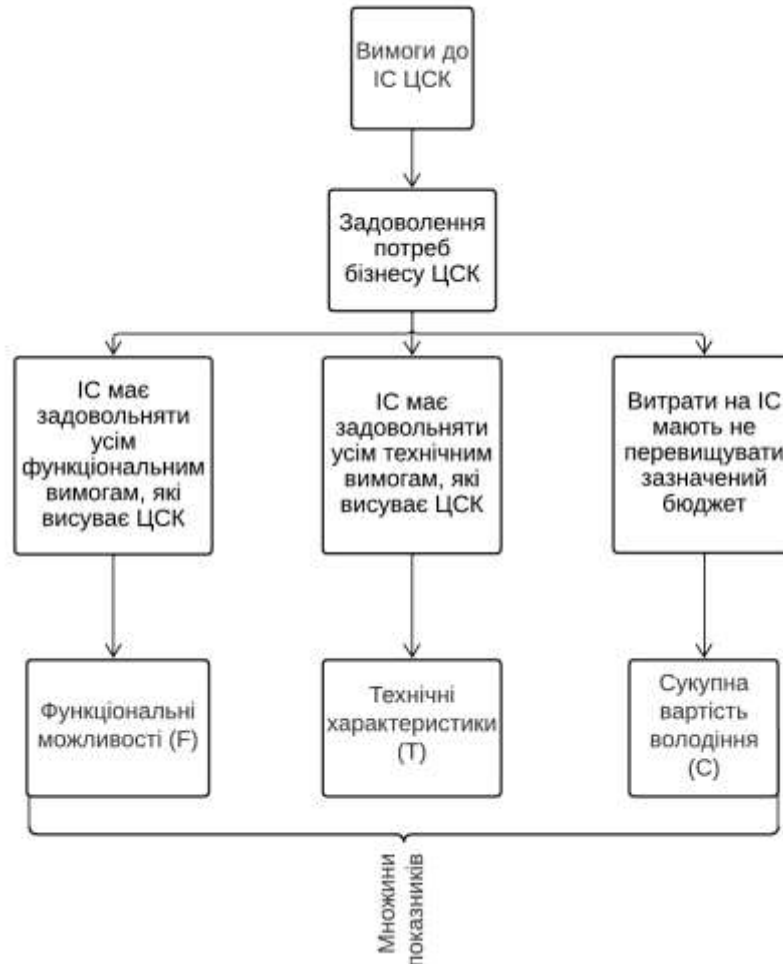


Рисунок 2.1 – Вимоги до ІС ЦСК і відповідні їм множини показників

Множина показників функціональних можливостей позначають відповідність ІС основним бізнес-процесам, що упроваджуються підприємством. Множина показників функціональних можливостей складається із багатьох показників в залежності від детальних вимог підприємства, клієнта, тощо.

Для представлення множини показників технічних характеристик використовуються деякі технічні показники, яких повинна дорівнювати ІС, або входити в діапазон певних значень, або просто мати наявності, тощо.

Множина показників технічних характеристик також складається із багатьох показників, численність яких може змінюватися відповідно до побажань/вимог підприємства, клієнта, тощо.

Множина показників сукупної вартості володіння позначає суму прямих і непрямих витрат, які несе власник системи за період життєвого циклу ІС [13]. Множина показників сукупної вартості володіння також складається із декількох показників, які в свою чергу задає підприємство, директор, тощо.

Опираючись на вищеописані множини показників функціональних можливостей, технічних та сукупної вартості володіння, потрібно сформулювати критерій оцінювання ефективності функціонування ІС ЦСК.

2.2 Формування критерію оцінювання ефективності функціонування ІС ЦСК

Критерій оцінювання ефективності функціонування ІС ЦСК використовується для оцінювання ефективності функціонування ІС ЦСК за річний період із застосуванням фактичних розрахунків.

Він складається із показників, що в свою чергу складають множини показників. В пункті 2.1 було визначено три множини показників: функціональні можливості (F), технічні характеристики (T) та сукупна вартість володіння (C).

При розрахунку критерію оцінювання кожному із показників відповідає експертно встановлений коефіцієнт важливості. Коефіцієнт важливості показників – це коефіцієнт, фактичне значення якого відповідає ступеню важливості певного показника із множини показників. Зазвичай кожному з показників у множині надають такі значення, які в сумі складаються в одиницю.

В більшості випадків коефіцієнти важливості показників визначаються за результатами експертного оцінювання. Але в деяких актуальних галузях є вже фіксовані фактичні значення коефіцієнтів важливості, що відповідають певним показникам, тому новий процес проведення експертного оцінювання не є потрібним. До таких галузей відноситься і оцінювання ефективності функціонування ІС ЦСК.

Нижче приведено літерні позначення множин показників, а також показників із відповідними коефіцієнтами важливості.

Кожному із показників із множини показників функціональних можливостей F_i відповідає коефіцієнт важливості b_i , де i – це порядковий номер показника та коефіцієнта важливості. Наприклад, $F_1 - b_1, F_2 - b_2, F_i - b_i$ тощо.

Кожному із показників із множини показників технічних характеристик T_j відповідає коефіцієнт важливості k_j , де j – це порядковий номер показника та коефіцієнта важливості. Наприклад, $T_1 - k_1, T_2 - k_2, T_j - k_j$ тощо.

Кожному із показників із множини показників сукупної вартості володіння C_z відповідає коефіцієнт важливості l_z , де z – це порядковий номер показника та коефіцієнта важливості. Наприклад, $C_1 - l_1, C_2 - l_2, C_z - l_z$ тощо.

При формуванні узагальненого критерію для оцінювання ефективності функціонування ІС ЦСК враховуються множини показників, описані вище. Критерій оцінювання ефективності функціонування може бути розрахованим за наступною формулою:

$$E = \frac{F+T}{C} \rightarrow \max,$$

$$C \leq C_{const} \quad (2.1)$$

де E – критерій оцінювання ефективності функціонування ІС ЦСК;

F – множина показників функціональних можливостей;

T – множина показників технічних характеристик;

C – множина показників сукупної вартості володіння;

C_{const} – значення фіксованого бюджету.

Нижче детальніше розглянуто кожний окремий елемент формули критерія оцінювання ефективності функціонування (2.1):

$$F = \sum_{i=1}^I b_i F_i, \quad (2.2)$$

де F – множина показників функціональних можливостей;

F_i – показник функціональних можливостей;

b_i – коефіцієнт важливості показників функціональних можливостей;

I – кількість показників.

$$T = \sum_{j=1}^J k_j T_j, \quad (2.3)$$

де T – множина показників технічних характеристик;

T_j – показник технічних характеристик;

k_j – коефіцієнт важливості показників технічних характеристик;

J – кількість показників.

$$C = \sum_{z=1}^Z l_z C_z, \quad (2.4)$$

де C – множина показників сукупної вартості володіння;

C_z – показник сукупної вартості володіння;

l_z – коефіцієнт важливості показників сукупної вартості володіння;

Z – кількість показників.

З використанням сформованого критерію оцінювання ефективності функціонування ІС ЦСК буде побудовано метод оцінювання ефективності функціонування ІС ЦСК.

2.3 Побудова методу оцінювання ефективності ІС ЦСК на основі існуючих методів

Процес оцінювання ефективності функціонування ІС ЦСК проводиться на основі спеціального методу, що складається із декількох кроків. Але кроки можуть відрізнятися в залежності від мети використання методу – так процес оцінювання ефективності функціонування ІС ЦСК проводиться по одній з двох причин:

- якщо потрібно оцінити ефективність функціонування інформаційних систем для впровадження в ЦСК;
- якщо потрібно оцінити ефективність функціонування вже існуючої в ЦСК ІС із процесом реінжинірингу [14].

Запропонований метод оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу або при впровадженні нової ІС) є гібридом двох, обраних у підрозділі 1.3 методів – «функціонально-вартісного аналізу» та «перевірки забезпечення якості». Так як результатом першого є зниження витрат на кожну одиницю ефективності, а результатом другого – виявлення прогалин у функціональних можливостях і технічних характеристиках, то результатом нового методу повинні бути обидва результати.

Запропонований метод оцінювання ефективності функціонування ІС ЦСК (при впровадженні нової ІС):

- крок 1. Сбір даних про діяльність ЦСК, що має бути супроводженою за допомогою ІС;
- крок 2. Формування вимог з метою впровадження нової ІС з урахуванням класифікації ЦСК та його особливостей;
- крок 3. Запропонування декількох варіантів ІС для проведення впровадження в ЦСК;

- крок 4. Аналіз поточних показників функціональних можливостей та технічних характеристик. Відсіювання ІС, чий показники не відповідають вимогам;
- крок 5. Формування показника сукупної вартості володіння;
- крок 6. Проведення процесу порівняння показника сукупної вартості із фіксованим бюджетом (константою). Якщо перевищує бюджет, то перехід на крок 3;
- крок 7. Проведення оцінювання ефективності функціонування ІС ЦСК з використанням критерію ефективності, описаного у формулах 2.1 – 2.4. Перехід на крок 3, якщо не всі варіанти оцінені;
- крок 8. Вибір кращого варіанту за розрахунком проведення впровадження ІС в ЦСК.

Запропонований метод оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу):

- крок 1. Сбір даних про функціонування ІС в ЦСК;
- крок 2. Формування вимог з метою реінжинірингу існуючої ІС ЦСК з урахуванням класифікації ЦСК та його особливостей;
- крок 3. Аналіз поточних показників функціональних можливостей та технічних характеристик для оцінки можливостей реінжинірингу за допомогою проведення тестування для виявлення невідповідностей;
- крок 4. Формування висновків щодо того, чи може ІС ЦСК взагалі бути зміненою, щоб відповідати визначеним вимогам;
- крок 5. Запропонування декількох варіантів проведення реінжинірингу;
- крок 6. Формування показника сукупної вартості володіння;
- крок 7. Проведення процесу порівняння показника сукупної вартості із фіксованим бюджетом (константою). Якщо перевищує бюджет, то перехід на крок 5;

– крок 8. Проведення оцінювання ефективності функціонування ІС ЦСК з використанням критерію ефективності, описаного у формулах 2.1 – 2.4. Перехід на крок 5, якщо не всі варіанти оцінені;

– крок 9. Вибір кращого варіанту за розрахунком проведення реінжинірингу ІС ЦСК.

Таким чином, було сформовано запропонований метод оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу або при впровадженні нової ІС).

В цілому метод є майже однаковим для двох ситуацій, але все одно є деякі важливі відмінності. В методі при впровадженні нової ІС в ЦСК процес запропонування декількох варіантів впровадження проходить майже на початку, після формування вимог до впровадження. А в методі при реінжинірингу ІС ЦСК запропонування варіантів реінжинірингу проходить після аналізу поточних показників функціональних можливостей і технічних характеристик, а також після формування висновків щодо доцільності проведення процесу реінжинірингу взагалі (на основі проведеного аналізу показників).

Хоча запропонований метод оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу або при впровадженні нової ІС) можна використовувати однаково для обох випадків, найкращих результатів можна досягнути розрізливши їх.

3 МЕТОДИКА ВИКОРИСТАННЯ ЗАПРОПОНОВАНОГО МЕТОДУ ОЦІНЮВАННЯ ФУНКЦІОНУВАННЯ ІС ЦСК

3.1 Відмінності в ІС в залежності від класу ЦСК

Центр сертифікації ключів – це кваліфікований надавач електронних довірчих послуг [1], що, крім основної – видачі сертифікатів електронно-цифрових підписів, виконує дуже багато функцій. Але навіть сам процес видачі сертифікатів ЕЦП може проходити за абсолютно різними сценаріями із абсолютно різними результатами.

Усі центри сертифікації ключів мають відмінності у бізнес-процесах, від яких залежать функціональні можливості, технічні характеристики та сукупна вартість володіння. В залежності від цих відмінностей проводиться розділення ЦСК на різні класи по певним категоріям, які комбінуються, що утворює унікальний ЦСК із відповідно унікальною інформаційною системою.

Існують такі категорії відмінностей в ЦСК:

- потреба в фізичній присутності клієнта;
- область застосування сертифікату ЕЦП;
- категорії клієнтів;
- різноманітність термінів дії;
- різноманітність способів зберігання сертифікатів ЕЦП.

Нижче приведено класифікації ЦСК за різними категоріями відмінностей, а також кругові діаграми відсоткового співвідношення різних класів ЦСК із значеннями, що є у відкритому доступі в Інтернеті.

Категорія «потреба в фізичній присутності» розділяє ЦСК на два класи:

- ЦСК, які потребують фізичного принесення документів при первинному отриманні сертифікату ЕЦП;
- ЦСК, які можуть генерувати сертифікати ЕЦП онлайн без первинного фізичного надання документів.

На рисунку 3.1 представлена кругова діаграма, що відображає відсоткове співвідношення класів ЦСК в категорії «потреба в фізичній присутності».

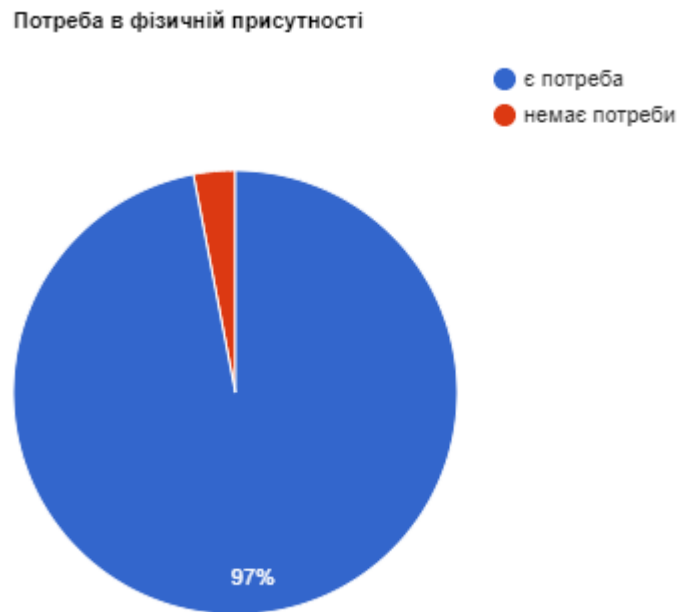


Рисунок 3.1 – Кругова діаграма класів ЦСК в категорії «потреба в фізичній присутності»

Категорія «область застосування сертифікату ЕЦП» розділяє ЦСК на два класи:

- ЦСК, що надають сертифікати ЕЦП, які можуть діяти тільки в рамках поточного ЦСК;
- ЦСК, що надають сертифікати ЕЦП, якими можна підписувати будь-який документ в будь-якій організації.

На рисунку 3.2 представлена кругова діаграма, що відображає відсоткове співвідношення класів ЦСК в категорії «область застосування сертифікату ЕЦП».

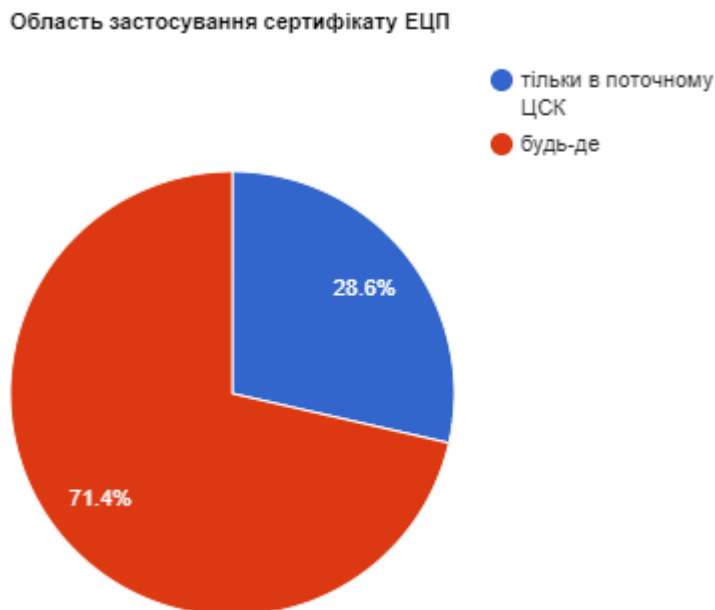


Рисунок 3.2 – Кругова діаграма класів ЦСК в категорії «область застосування сертифікату ЕЦП»

Категорія «категорії клієнтів» розділяє ЦСК на три класи:

- ЦСК, що можуть надавати сертифікати ЕЦП і фізичним особам, і юридичним особам;
- ЦСК, що можуть надавати сертифікати ЕЦП тільки фізичним особам;
- ЦСК, що можуть надавати сертифікати ЕЦП тільки юридичним особам.

На рисунку 3.3 представлена кругова діаграма, що відображає відсоткове співвідношення класів ЦСК в категорії «категорії клієнтів».

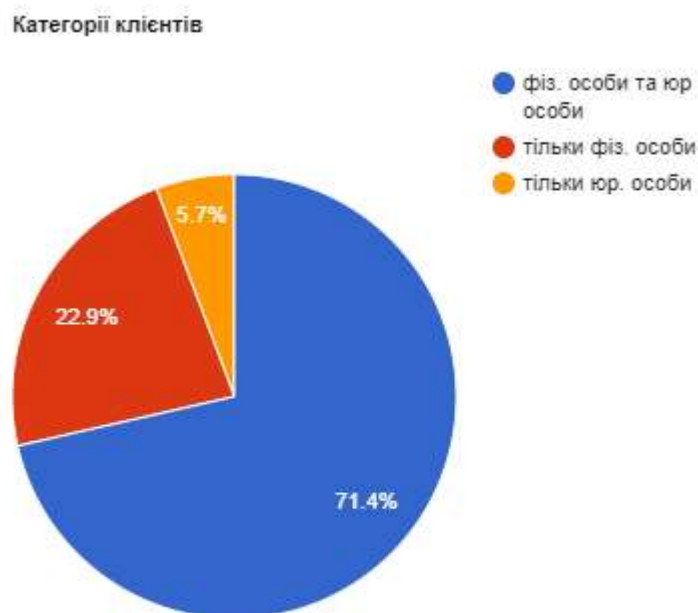


Рисунок 3.3 – Кругова діаграма класів ЦСК в категорії «категорії клієнтів»

Категорія «різноманітність термінів дії» розділяє ЦСК на три класи:

- ЦСК, що можуть надавати сертифікати ЕЦП, які є дійсними на 1 рік/2 роки/5 років;
- ЦСК, що можуть надавати сертифікати ЕЦП, які є дійсними на 1 рік/2 роки;
- ЦСК, що можуть надавати сертифікати ЕЦП лише на 1 рік.

На рисунку 3.4 представлена кругова діаграма, що відображає відсоткове співвідношення класів ЦСК в категорії «різноманітність термінів дії».

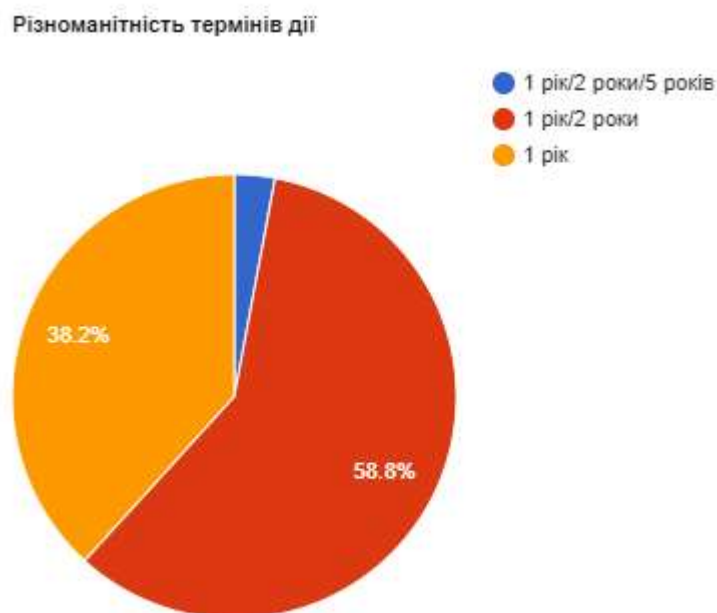


Рисунок 3.4 – Кругова діаграма класів ЦСК в категорії «різноманітність термінів дії»

Категорія «різноманітність способів зберігання сертифікатів ЕЦП» розділяє ЦСК на три класи:

- ЦСК, що мають два варіанти зберігання сертифікату ЕЦП – файловий та на токен;
- ЦСК, що мають один варіант зберігання сертифікату ЕЦП – файловий;
- ЦСК, що надають сертифікати ЕЦП тільки у додатку без можливості завантажити його на свій носій.

На рисунку 3.5 представлена кругова діаграма, що відображає відсоткове співвідношення класів ЦСК в категорії «різноманітність способів зберігання сертифікатів ЕЦП».

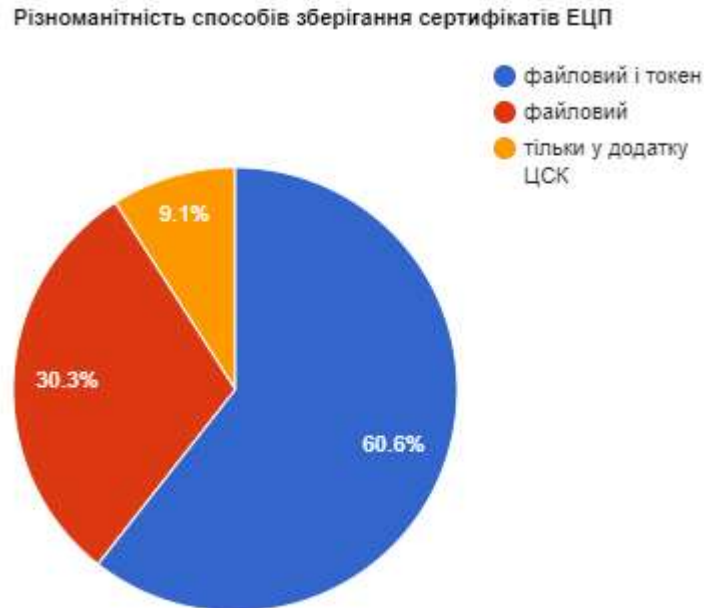


Рисунок 3.5 – Кругова діаграма класів ЦСК в категорії «різноманітність способів зберігання сертифікатів ЕЦП»

Наявність класів ЦСК впливає на оцінювання ефективності функціонування ІС ЦСК в двох ситуаціях:

- приналежність до конкретних класів впливає на побудову ІС, а саме на показники в множинах показників функціональних можливостей, технічних характеристик та сукупної вартості володіння, які впливають на розрахунок критерію оцінювання ефективності функціонування ІС ЦСК;
- вибір ІС серед різноманіття існуючих систем є складною задачею через специфіку предметної галузі [15]. Тому при пошуку інформаційної системи, що планується бути впровадженою в ЦСК, приналежність до певних класів облегшує процес відбору ІС на основі сформованих вимог. Таким чином, якщо ІС належить одному із секторів на кругових діаграмах (тобто належить певному класу), то вона пройде відбір або буде відсіяна згідно з певних вимог до ІС.

Приклад для другої ситуації: потрібно знайти варіанти інформаційних систем для впровадження в новий ЦСК, який належить до таких класів

(приналежність було виявлено на основі проведеного аналізу діяльності самого ЦСК):

- категорія «потреба в фізичній присутності»: ЦСК, які потребують фізичного принесення документів при первинному отриманні сертифікату ЕЦП;
- категорія «область застосування сертифікату ЕЦП»: ЦСК, що надають сертифікати ЕЦП, якими можна підписувати будь-який документ в будь-якій організації;
- категорія «категорії клієнтів»: ЦСК, що можуть надавати сертифікати ЕЦП тільки фізичним особам;
- категорія «різноманітність термінів дії»: ЦСК, що можуть надавати сертифікати ЕЦП, які є дійсними на 1 рік/2 роки;
- категорія «різноманітність способів зберігання сертифікатів ЕЦП»: ЦСК, що мають два варіанти зберігання сертифікату ЕЦП – файловий та на токен.

Далі проводиться порівняння функціональних можливостей та технічних характеристик варіантів ІС із їх потенційним задоволенням потреб класів, до яких входить ЦСК. Якщо ІС підходить під усі класи, то вона проходить на етап формування критерію до оцінювання ефективності функціонування ІС ЦСК, а якщо не підходить, то відсіюється з вибірки варіантів.

Приклад відбору ІС для впровадження в ЦСК показано в таблиці 3.1, де класи – це перелік класів, до яких належить ЦСК, описані вище, ІС – це варіанти ІС для впровадження в ЦСК з порядковим номером від першої до n-ї, а символи «+» та «-» – це відповідність функціоналу ІС класу ЦСК.

Таблиця 3.1 – Приклад відбору ІС для впровадження в ЦСК з урахуванням класів, до яких входить цей ЦСК

Класи \ ІС	1	2	3	4	5	6	n
а	+	+	+	–	+	+	+
б	+	+	+	+	–	+	–
в	–	+	+	+	+	+	+
г	–	+	+	–	+	+	+
д	+	+	+	+	+	+	+

На основі таблиці 3.1 можна зробити висновки, що інформаційні системи 2, 3 та 6 підходять під усі класи, а значить стають головними претендентами на впровадження в ЦСК.

Таким чином, можна сформувати безліч комбінацій класів, за котрими буде проводитися відбір інформаційних систем для впровадження.

Далі потрібно сформувати алгоритм використання запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу ІС або при впровадженні нової ІС) з урахуванням класів в категоріях.

3.2 Формування алгоритмів використання запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу або при впровадженні нової ІС) з урахуванням особливостей для певних ЦСК

3.2.1 Алгоритм використання запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при впровадженні нової ІС)

Алгоритм застосування запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при впровадженні нової ІС) зображено на рисунку 3.6, а детальний опис наведено нижче.



Рисунок 3.6 – Блок-схема алгоритму застосування запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при впровадженні нової ІС)



Рисунок 3.6, аркуш 2

На початку збираються дані про діяльність ЦСК, що має бути супроводженою за допомогою ІС. Визначаються класи, до яких належить ЦСК. Після цього проводиться аналіз вимог, на основі яких формується звіт із підсумковими вимогами для проведення впровадження ІС в ЦСК.

Надалі проводиться формування декількох варіантів ІС для впровадження ІС в ЦСК.

Наступні кроки – це аналіз показників в множинах показників функціональних можливостей та технічних характеристик.

До показників функціональних можливостей в ІС ЦСК в залежності від класів в категоріях можуть відноситися різні позиції. Наприклад:

- електронна ідентифікація та автентифікація користувачів на вході в веб-додаток ЦСК;
- автоматична перевірка повноти заповнення текстової форми/ форми документів);
- автоматична перевірка наявності у зазначених заявах граматичних помилок;
- передача/прийняття та оброблення інформації у режимі реального часу;
- безперервність роботи веб-порталу;
- розмежування та контроль доступу до інформації, яка міститься на веб-порталі/ перевірка повноважень користувачів і надання їм права на виконання певних дій із захищеними ресурсами, тощо.

До показників технічних характеристик ІС ЦСК зазвичай відносяться:

- пропускна здатність – це максимальна швидкість передачі даних по певному каналу;
- надійність – це спроможність ІС виконувати зазначені функції в заданих режимах та умовах експлуатації; ця характеристика має властивості безвідмовності, ремонтпридатності, а також довговічності;

- захищеність даних – це забезпечення конфіденційності, доступності і цілісності даних;
- зручний користувацький інтерфейс – одна із найважливіших вимог, яка, зазвичай, визначає задоволеність користувачів;
- масштабованість – це здатність системи легко адаптуватися до збільшеного навантаження;
- гнучкість – це здатність легко та швидко перевлаштовуватися на новий склад завдань, які вирішуються.

На основі даних аналізу показників функціональних можливостей та технічних характеристик відсіюються ті ІС, чії показники не відповідають сформованим вимогам.

Після цього формується значення множини показників сукупної вартості володіння, який порівнюється із зазначеним фіксованим бюджетом. До складу множини показників сукупної вартості володіння ІС ЦСК входять такі показники:

- адміністрування ІС ЦСК;
- розробка і впровадження нових елементів в ІС ЦСК;
- підтримка технічного обладнання ІС ЦСК;
- заробітна плата робітників;
- підтримка апаратно-програмних засобів ІС ЦСК.

Якщо перевищує бюджет, то береться інший варіант ІС для проведення впровадження в ЦСК.

Якщо не перевищує бюджет, то проводиться розрахування значення множини показників функціональних можливостей за формулою (2.2), значення множини показників технічних характеристик за формулою (2.3) та значення множини показників сукупної вартості володіння за формулою (2.4). Далі проводиться розрахування критерію оцінювання ефективності функціонування ІС ЦСК за формулою (2.1). Після цього проводиться

оцінювання варіанту проведення впровадження ІС в ЦСК за розрахованим критерієм.

Якщо ще не всі варіанти оцінені, то береться наступний варіант впровадження ІС в ЦСК. Якщо усі варіанти вже оцінені, то проводиться вибір найкращого варіанту впровадження ІС ЦСК.

3.2.2 Алгоритм використання запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу)

Алгоритм застосування запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу) зображено на рисунку 3.7, а детальний опис наведено нижче.



Рисунок 3.7 – Блок-схема алгоритму застосування запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу)

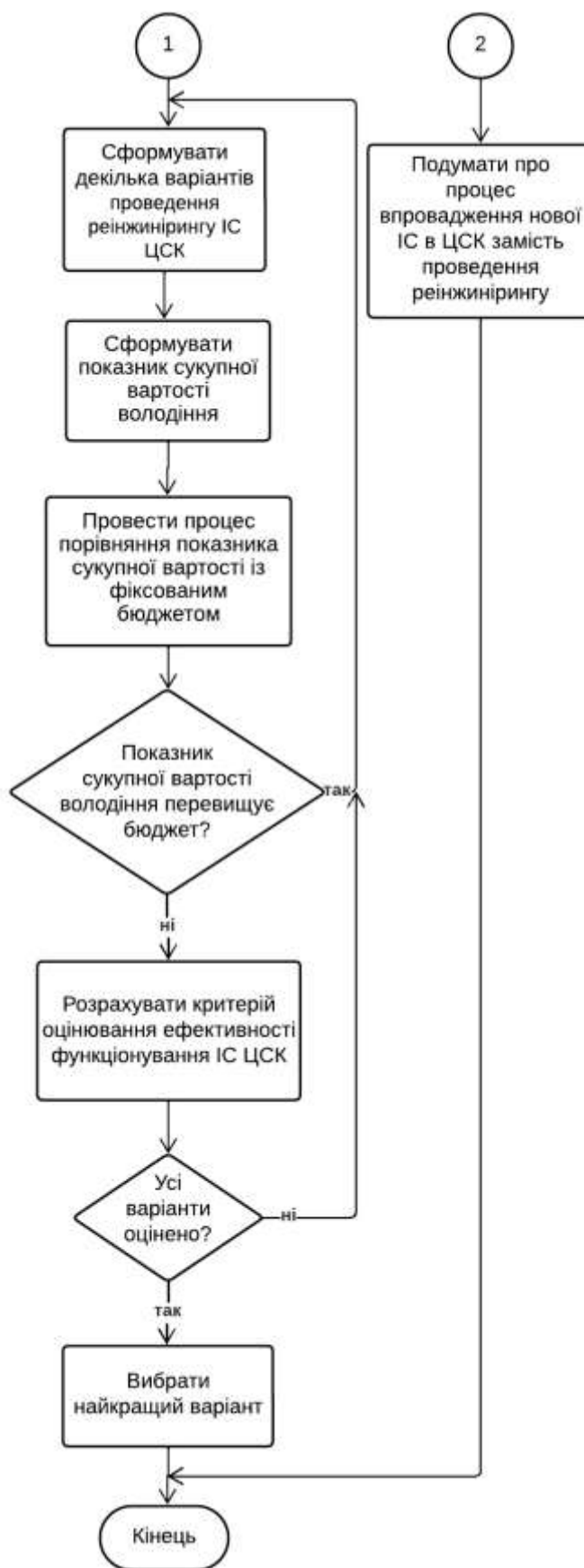


Рисунок 3.7, аркуш 2

На початку збираються дані про функціонування ІС в ЦСК. Визначаються класи, до яких належить ЦСК. Після цього проводиться аналіз вимог для проведення реінжинірингу ІС ЦСК.

Наступні кроки – це аналіз показників в множинах показників функціональних можливостей та технічних характеристик за допомогою проведення тестування для виявлення невідповідностей. Приклади показників в множинах показників функціональних можливостей та технічних характеристик описані у підпункті 3.2.1.

На основі даних аналізу показників функціональних можливостей та технічних характеристик стає зрозумілим, чи має сенс взагалі проводити реінжиніринг ІС ЦСК. Якщо ні, то проводяться роздуми щодо впровадження нової ІС в ЦСК замість проведення реінжинірингу старої. Якщо так, то формується декілька варіантів проведення реінжинірингу ІС ЦСК.

Після цього формується значення множини показників сукупної вартості володіння, який порівнюється із зазначеним фіксованим бюджетом. Приклад показників сукупної вартості володіння описано у підпункті 3.2.1.

Якщо показник перевищує бюджет, то береться інший варіант проведення реінжинірингу ІС ЦСК. Якщо не перевищує бюджет, то проводиться розрахування значення множини показників функціональних можливостей за формулою (2.2), значення множини показників технічних характеристик за формулою (2.3) та значення множини показників сукупної вартості володіння за формулою (2.4). Далі проводиться розрахування критерію оцінювання ефективності функціонування ІС ЦСК за формулою (2.1). Після цього проводиться оцінювання варіанту проведення реінжинірингу ІС ЦСК за розрахованим критерієм.

Якщо ще не всі варіанти оцінені, то береться наступний варіант проведення реінжинірингу ІС ЦСК. Якщо усі варіанти вже оцінені, то проводиться вибір найкращого варіанту проведення реінжинірингу ІС ЦСК.

Далі проводиться апробація запропонованого методу оцінювання ефективності функціонування ІС ЦСК.

4 АПРОБАЦІЯ ЗАПРОПОНОВАНОГО МЕТОДУ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ІС ЦСК (ПРИ РЕІНЖИНІРИНГУ)

4.1 Опис діяльності ЦСК та визначення його типу за запропонованою класифікацією

Апробація запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу) буде проводитися на прикладі ІС такого ЦСК, як ТОВ «Центр сертифікації ключів «Харків».

ТОВ «Центр сертифікації ключів «Харків» – це український кваліфікований надавач електронних довірчих послуг, що створює сучасні рішення для ведення електронного документообігу відповідно до державних стандартів криптографічного захисту інформації [16].

ТОВ «Центр сертифікації ключів «Харків» керує адміністрація, на чолі якої стоїть директор. Йому підпорядковуються заступник директора та секретарі [16].

Адміністрація керує п'ятьма відділами:

- відділом реєстрації, де працюють адміністратори реєстрації;
- відділом сертифікації, де працюють адміністратори сертифікації;
- відділом безпеки, яким керує начальник безпеки, а йому підпорядковуються заступник начальника безпеки, системні адміністратори та охоронці;
- архівом, де працюють архіваріуси;
- бухгалтерією, якою керує головний бухгалтер, а йому підпорядковуються бухгалтера.

Схема організаційної структури центру сертифікації ключів представлена на рисунку 4.1.

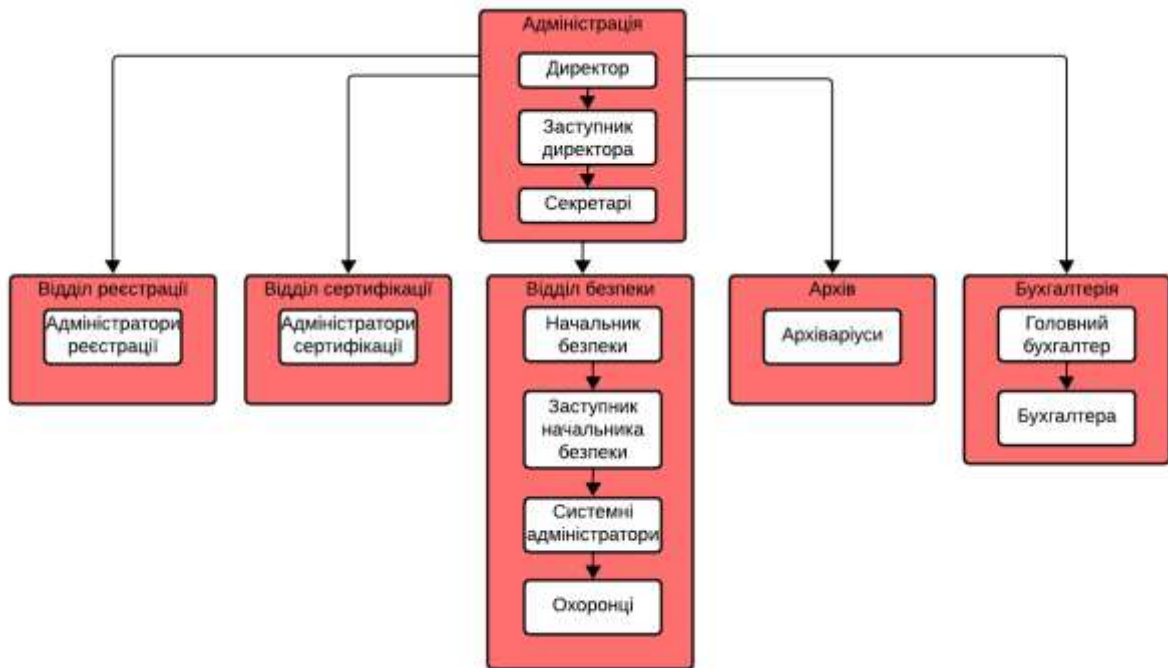


Рисунок 4.1 – Схема організаційної структури ТОВ «Центр сертифікації ключів «Харків»»

Інформаційна система ЦСК «Харків» містить шість підсистем [16]:

- адміністрування – займається роботою із програмним забезпеченням та містить модуль «Розробка та оновлення програмного комплексу видачі сертифікатів ЕЦП»;
- бухгалтерія – містить модулі «Облік податків та звітність» та «Облік оплати сертифікатів»;
- керівництво – займається загальним оглядом діяльності ЦСК та його перспективністю, має модуль «Аналітичні результати діяльності ЦСК»;
- відділ кадрів – займається роботою із працівниками, містить модуль «Облік кадрових ресурсів»;
- навчання – має модуль «Навчання та підвищення кваліфікації робітників»;
- сертифікація – містить модулі «Видача сертифікатів ЕЦП ЦСК», «Блокування та відкликання сертифікатів ЕЦП» та модуль «Облік видачі сертифікатів електронно-цифрових підписів».

На рисунку 4.2 зображена схема функціональної структури інформаційної системи ЦСК «Харків».



Рисунок 4.2 – Схема функціональної структури інформаційної системи «Центр сертифікації ключів»

Головним бізнес-процесом ЦСК «Харків» є первинна видача сертифікатів електронно-цифрових підписів та їх автопродовження. В ІС цей бізнес-процес відноситься до модулю «Обліку видачі сертифікатів електронно-цифрових підписів», що входить до складу підсистеми «Сертифікації».

Схеми потоків даних процесу «Облік видачі сертифікатів ЕЦП при первинному отриманні» і декомпозиції потоків даних цього процесу представлені на рисунках 4.3 та 4.4.

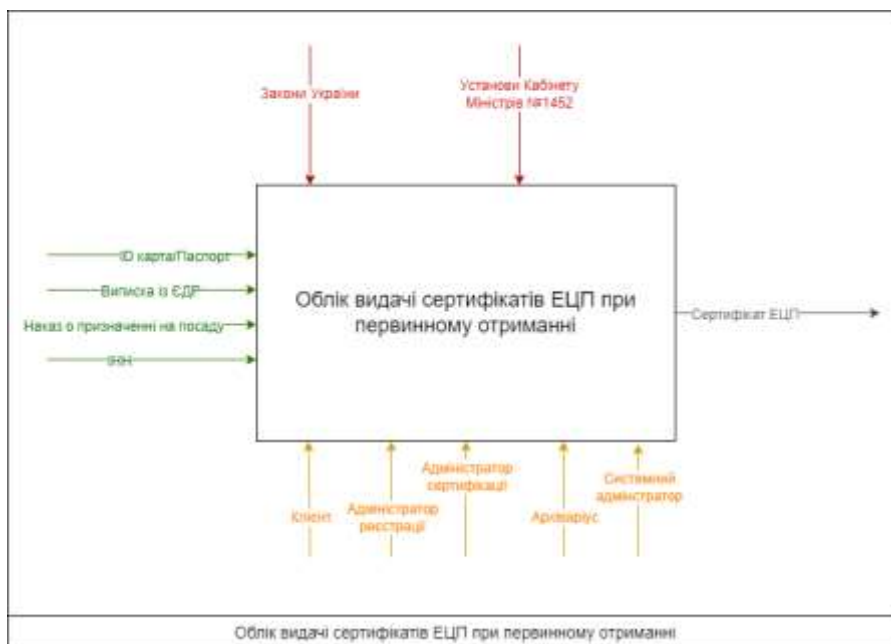


Рисунок 4.3 – Схема потоків даних процесу «Облік видачі сертифікатів ЕЦП при первинному отриманні»

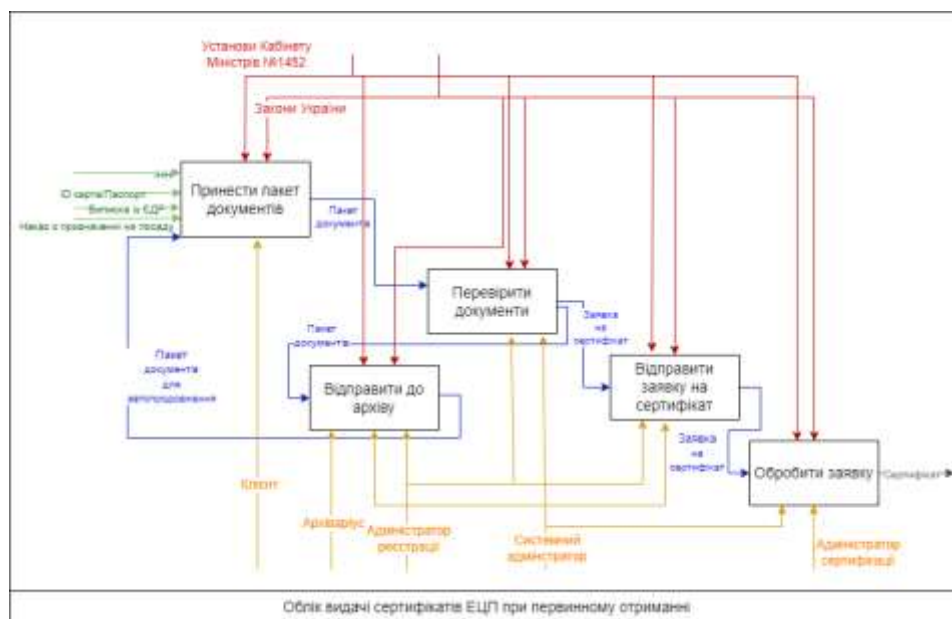


Рисунок 4.4 – Схема декомпозиції потоків даних процесу «Облік видачі сертифікатів ЕЦП при первинному отриманні»

Схеми потоків даних процесу «Облік видачі сертифікатів ЕЦП при автопродовженні» і декомпозиції потоків даних цього процесу представлені на рисунках 4.5 та 4.6.

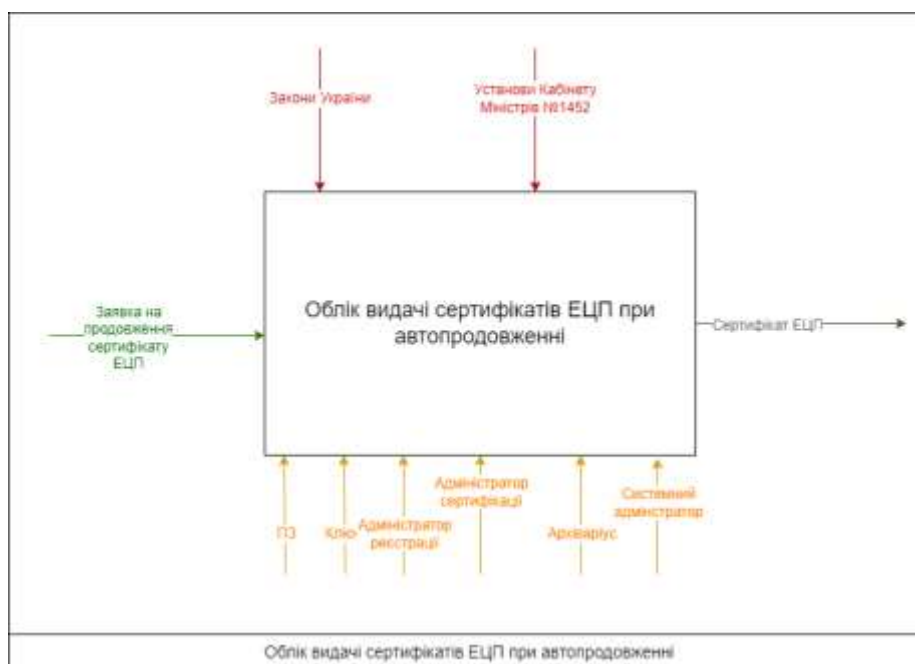


Рисунок 4.5 – Схема потоків даних процесу «Облік видачі сертифікатів ЕЦП при автопродовженні»

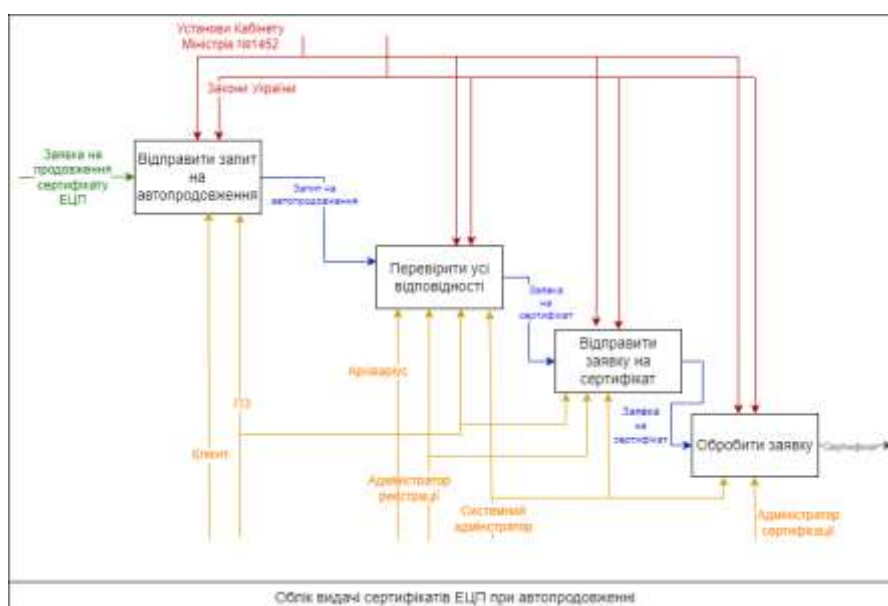


Рисунок 4.6 – Схема декомпозиції потоків даних процесу «Облік видачі сертифікатів ЕЦП при автопродовженні»

На основі проведеного аналізу діяльності ЦСК «Харків» було виявлено, до яких класів в категоріях (описаних у пункті 3.1) він належить:

- категорія «потреба в фізичній присутності»: клас – ЦСК, які потребують фізичного принесення документів при первинному отриманні сертифікату ЕЦП;
- категорія «область застосування сертифікату ЕЦП»: клас – ЦСК, що надають сертифікати ЕЦП, якими можна підписувати будь-який документ в будь-якій організації;
- категорія «категорії клієнтів»: клас – ЦСК, що можуть надавати сертифікати ЕЦП і фізичним особам, і юридичним;
- категорія «різноманітність термінів дії»: клас – ЦСК, що можуть надавати сертифікати ЕЦП, які є дійсними на 1 рік/2 роки;
- категорія «різноманітність способів зберігання сертифікатів ЕЦП»: клас – ЦСК, що мають два варіанти зберігання сертифікату ЕЦП – файловий та на токен.

Далі будуть сформовані вимоги для реінжинірингу ІС ЦСК «Харків», будуть проаналізовані значення показників в множинах показників функціональних можливостей та технічних характеристик, а далі будуть сформовані варіанти проектних рішень для реінжинірингу ІС.

4.2 Формування варіантів проектних рішень для реінжинірингу ІС

Як показано на схемі декомпозиції потоків даних процесу «Облік видачі сертифікатів ЕЦП при первинному отриманні», що на рисунку 4.4, першим кроком первинного отримання сертифікату ЕЦП є принесення документів до адміністратора реєстрації. Це потрібно для того, щоб робітник на основі даних документів заповнив спеціальну форму, після чого клієнт вводить персональний пароль та генерує ключі, потрібні для подальшого створення сертифікатів ЕЦП.

Наразі цей процес забирає багато часу як у клієнтів, так і у адміністраторів реєстрації. Тому основною метою проведення процесу реінжинірингу є спрощення процесу перенесення особистих даних клієнта з документів до спеціальної форми на первинне отримання сертифікату ЕЦП.

Вимоги для проведення процесу реінжинірингу ІС ЦСК «Харків»:

- апгрейд існуючого веб-додатку для автоматизації процесу перенесення особистих даних;
- застосування зрозумілих та зручних для користувачів інтерфейсів;
- контроль доступу до інформації, яка міститься на веб-порталі, з урахуванням апгрейду веб-додатку;
- бюджет – 102 000 \$.

Для того, щоб мати можливість провести реінжиніринг за висунутими вимогами, існуюча ІС ЦСК «Харків» має задовольняти таким вимогам:

- існуюча ІС ЦСК «Харків» має задовольняти деяким показникам із множини показників функціональних можливостей;
- значення деяких поточних показників із множини показників технічних характеристик мають входити в певний діапазон значень.

Виявлення наявності потрібних для проведення реінжинірингу функціональних можливостей серед існуючих в ІС ЦСК «Харків» продемонстровано в таблиці 4.1.

Таблиця 4.1 – Відповідність наявних функціональних можливостей ІС ЦСК «Харків» потрібним для проведення реінжинірингу

Наявні показника із множини показників функціональних можливостей	Показники функціональних можливостей ІС ЦСК «Харків»
Потрібні показники функціональних характеристик	
Електронна ідентифікація та автентифікація користувачів на вході в веб-додаток ЦСК	+
Розмежування та контроль доступу до інформації, яка міститься на веб-порталі	+

Кінець таблиці 4.1

Наявні показники із множини показників функціональних можливостей	Показники функціональних можливостей ІС ЦСК «Харків»
Потрібні показники функціональних характеристик	
Передача/прийняття та оброблення інформації у режимі реального часу	+
Безперервність роботи веб-порталу	+
Перевірка повноважень користувачів і надання їм права на виконання певних дій із захищеними ресурсами	+

Для того, щоб мати можливість оцінити рівень показників технічних характеристик відносно того рівня, який повинен бути для проведення реінжинірингу ІС ЦСК «Харків», було проведено нормалізацію значень технічних характеристик.

Значення поточних показників технічних характеристик ІС ЦСК «Харків» обчислювалися в процесі тестування ІС та надавалися із порівнянням до «ідеального» для цього показника технічних характеристик значення. Таким чином, максимальне значення «1» – можливий ідеал технічної характеристики в ІС, мінімальне значення «0» – повна неідеальність.

Відповідність значень показників технічних характеристик ІС ЦСК «Харків» діапазнам потрібних для проведення реінжинірингу показано в таблиці 4.2.

Таблиця 4.2 – Відповідність значень показників технічних характеристик ІС ЦСК «Харків» діапазнам потрібних для проведення реінжинірингу

Показники технічних характеристик	Задовільні діапазони значень показників	Значення поточних показників технічних характеристик ІС ЦСК «Харків»
Пропускна здатність	0,5 – 1	0,7
Надійність	0,7 – 1	0,75

Кінець таблиці 4.2

Показники технічних характеристик	Задовільні діапазони значень показників	Значення поточних показників технічних характеристик ІС ЦСК «Харків»
Захищеність даних	0,9 – 1	0,95
Зручний користувацький інтерфейс	0,4 – 1	0,6
Масштабованість	0,6 – 1	0,7
Гнучкість	0,5 – 1	0,6

В результаті аналізу поточних показників функціональних можливостей та технічних характеристик було виявлено, що має сенс проводити процес реінжинірингу ІС ЦСК «Харків».

Таким чином, було сформовано два варіанту проведення реінжинірингу ІС ЦСК «Харків», що задовольняють вимогам до реінжинірингу.

Перший. В веб-додатку створюється нова сторінка, де знаходиться спеціальна форма. Клієнт заповнює цю форму особистими даними та на основі цієї форми на персональні носії автоматично генеруються ключі, потрібні для подальшого створення сертифікатів ЕЦП.

Вже потім клієнт приходить до адміністратора реєстрації із носієм та оригіналами документів. А далі проходить звичний процес первинного отримання сертифікатів ЕЦП.

На рисунку 4.7 представлена контекстна діаграма прецедентів для клієнтів першого варіанту проведення реінжинірингу.

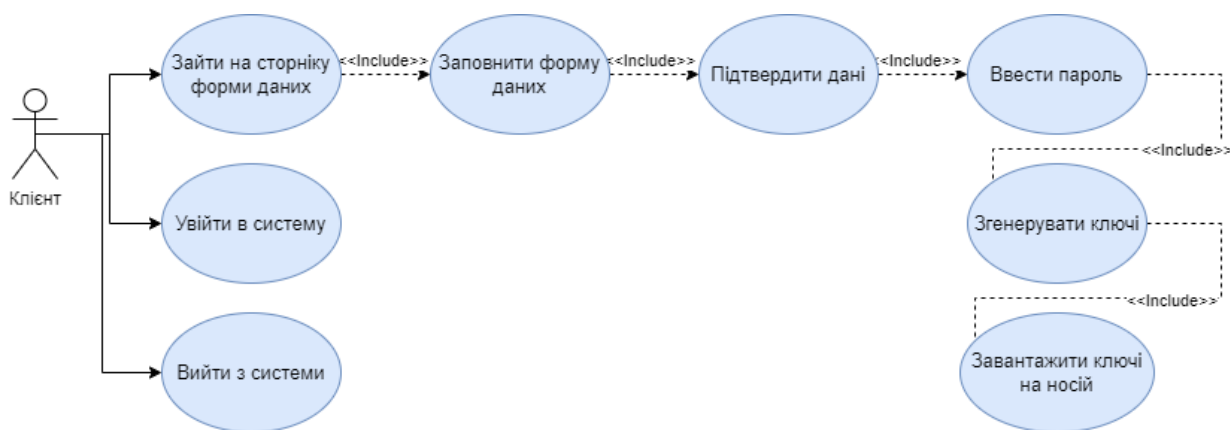


Рисунок 4.7 – Контекстна діаграма прецедентів для клієнтів першого варіанту проведення реінжинірингу

Перший варіант проведення реінжинірингу ІС ЦСК «Харків» додає такі показники в множину показників функціональні можливості:

- заповнення форми на генерацію ключів клієнтом за допомогою програмних засобів веб-порталу;
- автоматична перевірка повноти заповнення форми;
- автоматична перевірка наявності у зазначених заявах граматичних помилок;
- автоматична генерація ключів на основі заповненої форми;
- завантаження згенерованих ключів на персональний пристрій.

Перший варіант проведення реінжинірингу ІС ЦСК «Харків» таким чином впливає на показники в множині показників технічних характеристик:

- пропускна здатність – старий показник: 0,7; новий показник: 0,7;
- надійність – старий показник: 0,75; новий показник: 0,75;
- захищеність даних – старий показник: 0,95; новий показник: 0,98;
- зручний користувацький інтерфейс – старий показник: 0,6; новий показник: 0,8;
- масштабованість – старий показник: 0,7; новий показник: 0,7;
- гнучкість – старий показник: 0,6; новий показник: 0,75.

Другий. В веб-додатку створюється спеціальна сторінка, на яку клієнт завантажує документи, потрібні для первинного отримання сертифікатів ЕЦП.

Окрім того, створюється спеціальна програма, яка автоматично обробляє документи, бере з них потрібні дані та самостійно заповнює форму. Після закінчення заповнення форми клієнт автоматично отримує інформацію про завершення заповнення форми.

Потім клієнт приходять до адміністратора реєстрації, на основі цієї форми генерує файли із даними, потрібними для подальшого створення сертифікатів ЕЦП. А далі проходить звичний процес первинного отримання сертифікатів ЕЦП.

На рисунку 4.8 представлена контекстна діаграма прецедентів для клієнтів другого варіанту проведення реінжинірингу.



Рисунок 4.8 – Контекстна діаграма прецедентів для клієнтів другого варіанту проведення реінжинірингу

Другий варіант проведення реінжинірингу ІС ЦСК «Харків» додає такі показники в множину показників функціональні можливості:

- прикріплення документів за допомогою програмних засобів веб-порталу;

- автоматична перевірка повноти заповнення форми прикріплених документів;
- автоматичне заповнення форми на генерацію ключів за допомогою програмних засобів;
- автоматичне інформування клієнта після закінчення заповнення форми;
- автоматична перевірка на недостатність/ некоректність даних.

Другий варіант проведення реінжинірингу ІС ЦСК «Харків» таким чином впливає на показники в множині показників технічних характеристик:

- пропускна здатність – старий показник: 0,7; новий показник: 0,7;
- надійність – старий показник: 0,75; новий показник: 0,75;
- захищеність даних – старий показник: 0,95; новий показник: 0,9;
- зручний користувацький інтерфейс – старий показник: 0,6; новий показник: 0,7;
- масштабованість – старий показник: 0,7; новий показник: 0,7;
- гнучкість – старий показник: 0,6; новий показник: 0,8.

Далі буде проведено розрахування критеріїв оцінювання ефективності функціонування ІС ЦСК «Харків» при двох варіантах проведення реінжинірингу. На їх основі буде вибрано найкращий варіант проведення реінжинірингу ІС ЦСК «Харків».

4.3 Обґрунтування вибору варіанту проєктного рішення для реінжинірингу ІС

Для того, щоб мати можливість провести реінжиніринг ІС ЦСК «Харків», потрібно сформулювати показник сукупної вартості володіння для

обох варіантів проведення реінжинірингу, а потім провести порівняння його із фіксованим бюджетом.

Формування значення множини показників сукупної вартості володіння для двох варіантів проведення реінжинірингу представлено в таблиці 4.3.

Таблиця 4.3 – Формування значення множини показників сукупної вартості володіння для двох варіантів проведення реінжинірингу

Показник із множини показників сукупної вартості володіння	Значення показника для першого варіанту	Значення показника для другого варіанту
Розробка і впровадження нових елементів в ІС ЦСК «Харків»	12 430 \$	15 713 \$
Адміністрування ІС ЦСК «Харків» з урахуванням результатів реінжинірингу	13 180 \$	14 000 \$
Підтримка апаратно-програмних засобів ІС ЦСК «Харків» з урахуванням результатів реінжинірингу	35 082 \$	38 360 \$
Підтримка технічного обладнання ІС ЦСК «Харків» з урахуванням результатів реінжинірингу	5 500 \$	5 500 \$
Заробітна плата робітників з урахуванням результатів реінжинірингу	26 360 \$	26 000 \$
Усього	92 552 \$	99 573 \$

Таким чином, значення множини показників сукупної вартості володіння для першого варіанту проведення реінжинірингу – 92 552 \$, для другого – 99 573 \$. Як було сказано у пункті 4.2, фіксований бюджет – 102 000 \$, а значить жоден із варіантів його не перебільшив.

Для розрахунку критерію оцінювання ефективності функціонування ІС ЦСК потрібно провести нормалізацію значень показників, що входять у формулу, а також надати їм відповідні коефіцієнти важливості.

Як було сказано у підрозділі 2.2, в галузі оцінювання ефективності функціонування ІС ЦСК представлені фіксовані фактичні значення коефіцієнтів важливості, що відповідають показникам із множин показників функціональних можливостей, технічних характеристик та сукупної вартості володіння, тому новий процес проведення експертного оцінювання не є потрібним.

В кожному з варіантів реінжинірингу ІС ЦСК «Харків» нормалізація показників із множин показників функціональних можливостей, технічних характеристик та сукупної вартості володіння ІС ЦСК «Харків» проходила таким чином:

- для множини показників функціональних можливостей значення показників обчислювалися відповідно до програмної реалізації та її порівняння із «ідеальною» програмною реалізацією для цієї функціональної можливості;
- для множини показників технічних характеристик, як було сказано у підрозділі 4.2, значення показників обчислювалися в процесі тестування ІС та надавалися із порівнянням до «ідеального» для цієї технічної характеристики значення;
- для множини показників сукупної вартості володіння значення показників обчислювалися відносно «максимальної» вартості, можливої для кожного із показників.

Порівняння нормалізованих значень показників із множини показників функціональних можливостей в двох варіантах проведення реінжинірингу представлено в таблиці 4.4.

Таблиця 4.4 – Порівняння нормалізованих значень показників із множини показників функціональних можливостей в двох варіантах проведення реінжинірингу

Коефіцієнт важливості	Показник із множини показників функціональних можливостей	Нормалізовані значення показника для першого варіанту	Нормалізовані значення показника для другого варіанту
0,15	Електронна ідентифікація та автентифікація користувачів на вході в веб-додаток ЦСК	0,9	0,9
0,2	Розмежування та контроль доступу до інформації, яка міститься на веб-порталі/ перевірка повноважень користувачів і надання їм права на виконання певних дій із захищеними ресурсами	1	1
0,15	Передача/прийняття та оброблення інформації у режимі реального часу	0,85	0,85
0,1	Безперервність роботи веб-порталу	0,7	0,7
0,1	Заповнення форми на генерацію ключів клієнтом за допомогою програмних засобів веб-порталу	0,9	0
0,05	Автоматична перевірка повноти заповнення текстової форми/ форми документів	0,9	0,8

Кінець таблиці 4.4

Коефіцієнт важливості	Показник із множини показників функціональних можливостей	Нормалізовані значення показника для першого варіанту	Нормалізовані значення показника для другого варіанту
0,05	Автоматична перевірка наявності у зазначених заявах граматичних помилок	0,95	0
0,1	Автоматична генерація ключів на основі заповненої форми	1	0
0,1	Завантаження згенерованих ключів на персональний пристрій	0,9	0
0,1	Прикріплення документів за допомогою програмних засобів веб-порталу	0	1
0,15	Автоматичне заповнення форми на генерацію ключів за допомогою програмних засобів	0	0,95
0,05	Автоматичне інформування клієнта після закінчення заповнення форми	0	0,8
0,05	Автоматична перевірка на недостатність/некоректність даних	0	0,75

На основі таблиці 4.4 можна провести розрахування значення множини показників функціональних можливостей по формулі 2.2.

Перший варіант проведення реінжинірингу:

$$F = 0,15 * 0,9 + 0,2 * 1 + 0,15 * 0,85 + 0,1 * 0,7 + 0,1 * 0,9 + \\ + 0,05 * 0,9 + 0,05 * 0,95 + 0,1 * 1 + 0,1 * 0,9 \approx 0,905, \quad (4.1)$$

Другий варіант проведення реінжинірингу:

$$F = 0,15 * 0,9 + 0,2 * 1 + 0,15 * 0,85 + 0,1 * 0,7 + 0,05 * 0,8 + \\ + 0,1 * 1 + 0,15 * 0,95 + 0,05 * 0,8 + 0,05 * 0,75 \approx 0,893, \quad (4.2)$$

Порівняння значень показників із множини показників технічних характеристик в двох варіантах проведення реінжинірингу представлено в таблиці 4.5.

Таблиця 4.5 – Порівняння нормалізованих значень показників із множини показників технічних характеристик в двох варіантах проведення реінжинірингу

Коефіцієнт важливості	Показник із множини показників технічних характеристик	Нормалізовані значення показника для першого варіанту	Нормалізовані значення показника для другого варіанту
0,15	Пропускна здатність	0,7	0,7
0,2	Надійність	0,75	0,75
0,3	Захищеність даних	0,98	0,9
0,05	Зручний користувачський інтерфейс	0,8	0,7
0,2	Масштабованість	0,7	0,7
0,1	Гнучкість	0,75	0,8

На основі таблиці 4.5 можна провести розрахування значення множини показників технічних характеристик по формулі 2.3.

Перший варіант проведення реінжинірингу:

$$T = 0,15 * 0,7 + 0,2 * 0,75 + 0,3 * 0,98 +$$

$$+0,05 * 0,8 + 0,2 * 0,7 + 0,1 * 0,75 \approx 0,8, \quad (4.3)$$

Другий варіант проведення реінжинірингу:

$$T = 0,15 * 0,7 + 0,2 * 0,75 + 0,3 * 0,9 + \\ +0,05 * 0,7 + 0,2 * 0,7 + 0,1 * 0,8 \approx 0,78, \quad (4.4)$$

Порівняння значень показників із множини показників сукупної вартості володіння в двох варіантах проведення реінжинірингу представлено в таблиці 4.6.

Таблиця 4.6 – Порівняння нормалізованих значень показників сукупної вартості володіння в двох варіантах проведення реінжинірингу

Коефіцієнт важливості	Показник із множини показників сукупної вартості володіння	Нормалізовані значення показника для першого варіанту	Нормалізовані значення показника для другого варіанту
0,25	Розробка і впровадження нових елементів в ІС ЦСК «Харків» (одноразово)	0,65	0,85
0,25	Адміністрування ІС ЦСК «Харків» з урахуванням результатів реінжинірингу (за рік)	0,88	0,9
0,2	Підтримка апаратно-програмних засобів ІС ЦСК «Харків» з урахуванням результатів реінжинірингу (за рік)	0,76	0,8

Кінець таблиці 4.6

Коефіцієнт важливості	Показник із множини показників сукупної вартості володіння	Нормалізовані значення показника для першого варіанту	Нормалізовані значення показника для другого варіанту
0,2	Підтримка технічного обладнання ІС ЦСК «Харків» з урахуванням результатів реінжинірингу (за рік)	0,9	0,9
0,1	Заробітна плата робітників з урахуванням результатів реінжинірингу (за рік)	0,81	0,8

На основі таблиці 4.6 можна провести розрахування значення множини показників сукупної вартості володіння по формулі 2.4.

Перший варіант проведення реінжинірингу:

$$C = 0,25 * 0,65 + 0,25 * 0,88 + 0,2 * 0,76 + 0,2 * 0,9 + 0,1 * 0,81 \approx 0,8, \quad (4.6)$$

Другий варіант проведення реінжинірингу:

$$C = 0,25 * 0,85 + 0,25 * 0,9 + 0,2 * 0,8 + 0,2 * 0,9 + 0,1 * 0,8 \approx 0,86, \quad (4.5)$$

Таким чином, за сформованими значеннями показників в множинах показників функціональних можливостей, технічних характеристик та сукупної вартості володіння можна розрахувати критерій оцінювання ефективності функціонування ІС ЦСК по формулі 2.1.

Перший варіант проведення реінжинірингу:

$$E = \frac{0,905+0,8}{0,8} \approx 2,13, \quad (4.7)$$

Другий варіант проведення реінжинірингу:

$$E = \frac{0,893+0,78}{0,86} \approx 1,95, \quad (4.8)$$

Таким чином, за сформованим критерієм оцінювання ефективності функціонування ІС ЦСК можна зробити висновок, що перший варіант проведення реінжинірингу є більш ефективним, ніж другим. Тому саме він повинен бути використаним для проведення реінжинірингу ІС ЦСК «Харків».

ВИСНОВКИ

За результатами виконання кваліфікаційної роботи було досліджено методи оцінювання ефективності функціонування інформаційних систем центрів сертифікації ключів з метою вибору найефективнішої інформаційної системи для роботи з електронно-цифровими підписами.

Спочатку було детально проаналізовано предметну область, а саме центри сертифікації ключів, а також було проаналізовано особливості інформаційних систем центрів сертифікації ключів. Крім того, було проведено аналіз існуючих методів оцінювання ефективності функціонування ІС ЦСК із вибором тих, що найкраще підходять для роботи в галузі електронно-цифрових підписів. Було сформовано постановку задачі.

Наступним кроком було формування вимог до інформаційної системи з урахуванням особливостей функціонування ЦСК. Далі було сформовано критерій оцінювання ефективності функціонування ІС ЦСК, а також було побудовано метод оцінювання ефективності функціонування ІС ЦСК для двох варіантів – впровадження нової ІС та реінжиніринг ІС.

Далі було проаналізовано відмінності в інформаційних системах в залежності від того, до яких класів в певних категоріях належать ЦСК. Потім було сформовано алгоритми використання запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу або при впровадженні нової ІС).

Останнім кроком була апробація запропонованого методу оцінювання ефективності функціонування ІС ЦСК (при реінжинірингу) на прикладі інформаційної системи ТОВ «Центр сертифікації ключів «Харків».

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. ЦСК «Україна» [Електронний ресурс] // uakey.com.ua: портал послуг. URL: <https://uakey.com.ua/>.
2. Акредитований центр сертифікації ключів [Електронний ресурс] // acsk.privatbank.ua: портал державних послуг. URL: <https://acsk.privatbank.ua/main>.
3. Повторне (дистанційне) формування сертифікатів за електронним запитом [Електронний ресурс] // ca.tax.gov.ua: портал державних послуг. URL: <https://ca.tax.gov.ua/manage-certificates>.
4. Як отримати Дія.Підпис? [Електронний ресурс] // paperless.dii.gov.ua: портал державних послуг. URL: <https://paperless.dii.gov.ua/instruction/yak-otrimati-diyapidpis>.
5. Alliance Bank [Електронний ресурс] // [AllianceBank.ua](https://ca.bankalliance.ua/uk): офіційний сайт. URL: <https://ca.bankalliance.ua/uk>.
6. Чичуліна К., Міщук Є., Арзуманян А. Сучасні методи обліку витрат. Економіка і суспільство. 2017. № 13. 8 с.
7. Функціонально-вартісний аналіз як метод удосконалення об'єкту. [Електронний ресурс] // osvita.ua: інформаційно-довідковий портал. URL: https://osvita.ua/vnz/reports/econom_pidpr/18693.
8. Федоронько Н., Гнатюк І. Використання функціонально-вартісного аналізу для підвищення ефективності зовнішньоекономічної діяльності підприємств. Глобальні та національні проблеми економіки. 2018. 3 с.
9. Метод внутрішньої норми прибутку. [Електронний ресурс] // pidru4niki.com: інформаційно-довідковий портал. URL: https://pidru4niki.com/1279091240741/buhgalterskiy_oblik_ta_audit/metod_vnutri_shnoyi_normi_pributku.

10. Гончарова О. Реінжиніринг бізнес-процесів як метод процесного управління. Вісник Київського національного університету імені Тараса Шевченка. Економіка. 2013. Вип. 10 (151). 78–82 с.

11. Evaluation of MIS (Management Information System) [Електронний ресурс] // IncludeHelp.com: інформаційно-довідковий портал. URL: <https://www.includehelp.com/MIS/evaluation-of-mis.aspx>.

12. Efficiency Evaluation: Methods to Optimize Program Resources [Електронний ресурс] // EvalCommunity.com: інформаційно-довідковий портал. URL: <https://www.evalcommunity.com/career-center/efficiency-evaluation>.

13. Підходи щодо оцінки сукупної вартості володіння [Електронний ресурс] // irbis-nbu.gov.ua: інформаційно-довідковий портал. URL: <http://www.irbis-nbu.gov.ua/>.

14. Чиркова К. С., Міхнова А. В., Міхнов Д. К. Розробка технології реінжинірингу спеціалізованих інформаційних систем. International Academy Journal Web of Scholar. 2021.

15. Чиркова К. С., Міхнова А. В., Міхнов Д. К. Критерій вибору структури інформаційної системи закладів служби крові. Біоніка інтелекта.. 2017.

16. Соловйова Є. І. Модуль «Облік видачі сертифікатів електронно-цифрових підписів» ІС «Центр сертифікації ключів». 2022. Кваліфікаційна робота.

17. Методичні вказівки щодо розробки та оформлення кваліфікаційної роботи (для студентів усіх форм навчання другого (магістерського) рівня вищої освіти спеціальності 122 Комп'ютерні науки освітньо-професійної програми «Інформаційні управляючі системи та технології») / Упоряд.: Петров К.Е., Левикін В.М., Чалий С.Ф., Євланов М.В., Саєнко В.І., Міхнов Д.К., Міхнова А.В., Чала О.В. – Харків: ХНУРЕ, 2021. – 30 с.

18. ДСТУ 3008:2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. Чинний від 22-06-2015. Вид. офіц. Київ : УкрНДНЦ, 2016. 31 с.