МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ, КОМП'ЮТЕРНОЇ ТА ПРОГРАМНОЇ ІНЖЕНЕРІЇ
КАФЕДРА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри ЗЗІ
_____ В.В. Козловський

«____»_____ 2020 р.

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Захищеність кваліфікованого надавача електронних довірчих послуг

Автор: В.О. Приходько

Науковий керівник: д.т.н., професор М.О. Шутко

Нормоконтролер: д.т.н., професор М.О. Шутко

Київ 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Засобів захисту інформації

Освітнього ступеня: «Магістр»

Спеціальність: 125 Кібербезпека

Освітньо-професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»

ЗАТВЕРДЖУЮ
Завідувач кафедри ЗЗІ

_____ В.В. Козловський

«____»_____ 2020 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
студента Приходька Віталія Олеговича

1. Тема: Захищеність кваліфікованого надавача електронних довірчих послуг
затверджена наказом ректора від 13.10.2020 р. № 1994/ст.
2. Термін виконання: з 05 жовтня 2020р. по 27 грудня 2020р.
3. Вихідні дані: аналіз діяльності Центрального засвідчувального органу; дослідження всіх розробок, які є на ринку в Україні; забезпечення захищеності кваліфікованого надавача електронних довірчих послуг.
4. Зміст пояснювальної записки (перелік питань, що підлягають розробці):
1. Центральний засвідчувальний орган
2. Розробки, які є на ринку України
3. Здійснення захищеності кваліфікованого надавача електронних довірчих послуг

КАЛЕНДАРНИЙ ПЛАН
виконання кваліфікаційної роботи

№ п/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі		Виконано
2.	Аналіз літературних джерел		Виконано
3.	Обґрунтування рішення		Виконано
4.	Збір інформації		Виконано
5.	Центральний засвідчувальний орган		Виконано
6.	Розробки, які є на ринку України		Виконано
7.	Здійснення захищеності кваліфікованого надавача електронних довірчих послуг		Виконано
8.	Оформлення і друк пояснювальної записки		Виконано
9.	Оформлення презентації		Виконано
10.	Отримання рецензій від опонентів		Виконано
11.	Захист в ЕК		

Дипломник В.О. Приходько

(підпис, дата)

Дипломний керівник М.О. Шутко

(підпис, дата)

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальний обсяг роботи складає 68 сторінок, має 4 рисунки, 3 таблиці. Список використаних джерел містить 53 найменування і займає 7 сторінок.

Метою кваліфікаційної роботи є забезпечення захищеності кваліфікованого надавача електронних довірчих послуг.

В кваліфікаційній роботі проведено аналіз існуючих розробників на ринку України.

Підсумком роботи є застосування мережного криптомодуля для підвищення захищеності кваліфікованого надавача електронних довірчих послуг.

Ключові слова: ЦЕНТРАЛЬНИЙ ЗАСВІДЧУВАЛЬНИЙ ОРГАН; КВАЛІФІКОВАНИЙ НАДАВАЧ ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУЛ; СИСТЕМА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ, ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ, САЙФЕР.

ЗМІСТ

СПИСОК ВИКОРИСТАНИХ СКОРОЧЕНЬ

PGP – Pretty Good Privacy

PKI – Public key infrastructure

SDSI – Simple Distributed Security Infrastructure

SET – Secure Electronic Transaction

SPKI – Simple Public Key Infrastructure

TSA – Time Stamping Authority

БД – База даних

ДССЗЗІ – Державна служби спеціального зв’язку та захисту інформації України

ЕДП – Електронні довірчі послуги

КЕП – Кваліфікований електронний підпис

КМУ – Кабінет Міністрів України

КНЕДП – Кваліфікований надавач електронних довірчих послуг

КСЗІ – Комплексна система захисту інформації

ПЗ – Програмне забезпечення

СВС – Списки відкликаних сертифікатів

СКЗІ – Система криптографічного захисту інформації

ТЗІ – Технічний захист інформації

ЦЗО – Центральний засвідчувальний орган

ЦР – Центр реєстрації

ЦСК – Центр сертифікації ключів

ВСТУП

Кваліфікований надавач електронних довірчих послуг (КНЕДП) – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа-підприємець, яка надає одну чи більше електронних довірчих послуг (ЕДП), діяльність якої відповідає вимогам Закону України «Про електронні довірчі послуги» та відомості які внесені до Довірчого списку, тому дана тематика щодо їх захисту є **актуальною** [41].

Відповідальність за дотриманням вимог покладено на Міністерство цифрової трансформації України – це є головний орган у системі центральних органів виконавчої влади, котрий забезпечує формування та реалізує політику у сфері ЕДП та здійснює функції центрального засвідчувального органу (ЦЗО) [41].

Інфраструктура відкритих ключів (Public key infrastructure – PKI) – інтегрований комплекс методів та засобів, який призначається для впровадження та експлуатації криптографічних систем з відкритими ключами [41].

Система кваліфікованого електронного підпису (КЕП) від Інституту інформаційних технологій (згідно PKI) – організаційно-технічна система, котра інтегрує сертифікати відкритих ключів, засоби КЕП, центри сертифікації ключів (ЦСК) та власників сертифікатів як єдину структуру [41].

Система криптографічного захисту інформації «Шифр-Х.509» (СКЗІ «Шифр-Х.509») призначена для створення PKI (створення ЦСК, у тому числі КНЕДП, центрів реєстрації (ЦР) у рамках відповідності ЦСК, наданих користувачам засобів управління ключами), забезпечення послугами КЕП органів державної влади, місцевого самоврядування, підприємств, установ та організацій будь-якої форми власності, фізичних осіб [41].

Метою є забезпечення захищеності кваліфікованого надавача електронних довірчих послуг.

У процесі підготовки кваліфікаційної роботи були поставлені наступні **задачі**:

- Аналіз діяльності Центрального засвідчувального органу;
- Дослідження всіх розробок, які є на ринку в Україні;
- Забезпечення захищеності кваліфікованого надавача електронних довірчих послуг.

Об’єкт дослідження. Кваліфікований надавач електронних довірчих послуг.

Предмет дослідження. Методи та способи для захисту КНЕДП.

Новизна роботи. Застосування мережного криптомодуля для підвищення захищеності кваліфікованого надавача електронних довірчих послуг.

Практична цінність. Результати досліджень можна використовувати для підвищення захищеності, швидкості здійснення операції, спрощення процесу використання ключів для користувачів.

РОЗДІЛ 1 ЦЕНТРАЛЬНИЙ ЗАСВІДЧУВАЛЬНИЙ ОРГАН

1.1 Про Центральний засвідчувальний орган

Відповідальність за дотриманням вимог покладено на Міністерство цифрової трансформації України – це є головний орган у системі центральних органів виконавчої влади, котрий забезпечує формування та реалізує політику у сфері ЕДП та здійснює функції ЦЗО [25].

Функції та повноваження ЦЗО визначено у Статті 7 ЗУ «Про ЕДП», відповідно до якої Мінцифри [25]:

- Визначає повноваження у сфері ЕДП та електронної ідентифікації;
- Надає адміністративну послугу шляхом внесення юридичних осіб та фізичних осіб-підприємців, які мають намір надавати ЕДП до Довірчого списку;
- Узгоджує розроблені надавачами ЕДП порядки синхронізації часу із Всесвітнім координованим часом (UTC);
- Узгоджує плани припинення діяльності КНЕДП;
- Приймає та зберігає документовану інформацію, сформовані сертифікати відкритих ключів, реєстри чинних, блокованих та скасованих сертифікатів відкритих ключів у разі припинення діяльності КНЕДП;
- Розглядає пропозиції суб’єктів відносин у сфері ЕДП щодо удосконалення державного регулювання сфери ЕДП;
- Надає суб’єктам відносин у сфері ЕДП консультації з питань, пов’язаних з наданням ЕДП;
- Інформує відповідно до ЗУ «Про ЕДП» про обставини, які перешкоджають діяльності ЦЗО;
- Здійснює оцінку стану розвитку сфери ЕДП за результатами проведення аналізу інформації про діяльність постачальників ЕДП та ЦЗО;
- Забезпечує взаємне визнання українських та іноземних сертифікатів відкритих ключів та КЕП, які застосовуються у процесі надання юридично значущих ЕДП;

- Здійснює інші повноваження у сферах ЕДП та електронної ідентифікації;
- Технічне та технологічне забезпечення виконання функцій ЦЗО здійснюється адміністратором інформаційно-телекомунікаційної системи ЦЗО.

Згідно ЗУ «Про ЕДП» до складу ЕДП входять [25]:

- створення, перевірка та підтвердження КЕП чи електронної печатки;
- формування, перевірка та підтвердження чинності сертифіката КЕП чи електронної печатки;
- формування, перевірка та підтвердження чинності сертифіката автентифікації веб-сайту;
- формування, перевірка та підтвердження електронної позначки часу;
- реєстрована електронна доставка;
- збереження удосконалених електронних підписів, печаток, електронних позначок часу та сертифікатів.

Суб'єктами відносин у сфері ЕДП є [25]:

- користувачі ЕДП;
- надавачі ЕДП;
- органи з оцінки відповідності;
- засвідчувальний центр;
- ЦЗО;
- контролюючий орган.

ЕДП надаються на договірних засадах КНЕДП, де ЕДП надається як окремо, так і в сукупності [25].

Кваліфікований надавач електронних довірчих послуг (КНЕДП) – юридична особа незалежно від організаційно-правової форми та форми власності, фізична особа-підприємець, яка надає одну чи більше електронних довірчих послуг (ЕДП), діяльність якої відповідає вимогам Закону України

«Про електронні довірчі послуги» та відомості які внесені до Довірчого списку [25].

1.2 Електронний реєстр чинних, блокованих та скасованих сертифікатів відкритих ключів

Реєстр – електронна база даних (БД), куди входять відомості щодо самопідписані сертифікати електронної печатки ЦЗО, сертифікати ЦЗО для та дані в протоколі визначення статусу сертифіката у реальному часі, сертифікати КНЕДП, сформовані з використанням самопідписаного сертифікату електронної печатки ЦЗО, статус та обмеження у використанні таких сертифікатів, списки відкликаних сертифікатів (СВС) ЦЗО [9].

Станом на 05.11.2018 існує наступний список КНЕДП, які внесені до Довірчого списку [9]:

- Центральний засвідчувальний орган
- Міністерство цифрової трансформації України
- Засвідчувальний центр
- Національний банк України
- Кваліфіковані надавачі електронних довірчих послуг
- Акціонерне товариство комерційний банк «ПРИВАТБАНК»
- Військова частина 2428
- Генеральний штаб Збройних Сил України
- Офіс Генерального прокурора
- Державна казначейська служба України
- Державне підприємство «Оператор ринку»
- Державне підприємство «ДІЯ»
- Державне підприємство «Український інститут інтелектуальної власності»
- Державне підприємство «Українські спеціальні системи»
- Інформаційно-довідковий департамент ДПС

- Міністерство внутрішніх справ України
- Національний банк України
- Публічне акціонерне товариство «Державний ощадний банк України»
- Публічне акціонерне товариство «Національний депозитарій України»
- Акціонерне товариство «УкрСиббанк»
- Товариство з обмеженою відповідальністю «Алтерсайн»
- Товариство з обмеженою відповідальністю «Арт-мастер»
- Товариство з обмеженою відповідальністю «Інтер-Метл»
- Товариство з обмеженою відповідальністю «Центр сертифікації ключів «Україна»
- Філія «Головний інформаційно-обчислювальний центр» публічного акціонерного товариства «Українська залізниця»
- Товариство з обмеженою відповідальністю «ДЕПОЗИТ САЙН»

Інформація щодо КНЕДП разом з інформацією про КНЕДП надають у вигляді, яке придатне для автоматичної обробки та міститься у Довірчому списку.

1.3 Нормативно-правові акти [26]

- Указ Президента України від 22.05.1998 № 505/98 «Про Положення про порядок здійснення криптографічного захисту інформації (КЗІ) в Україні»
- ЗУ від 22.05.2003 № 851-IV «Про електронні документи та електронний документообіг»
- ЗУ від 05.10.2017 № 2155-VIII «Про ЕДП»
- Постанова Кабінету Міністрів України (КМУ) від 27.01.2010 № 55 «Про впорядкування транслітерації українського алфавіту латиницею»

- Постанова КМУ від 16.12.2015 № 1057 «Про визначення сфер діяльності, в яких центральні органи виконавчої влади здійснюють функції технічного регулювання»
- Постанова КМУ від 10.05.2018 № 356 «Про внесення змін та визнання такими, що втратили чинність, деяких актів Кабінету Міністрів України у зв'язку з прийняттям ЗУ «Про електронні довірчі послуги»
- Постанова КМУ від 19.09.2018 № 749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності»
- Постанова КМУ від 26.09.2018 № 775 «Про затвердження обов'язкових вимог до Довірчого списку»
- Постанова КМУ від 10.10.2018 № 821 «Про затвердження Порядку зберігання документованої інформації та її передавання центральному засвідчувальному органу в разі припинення діяльності КНЕДП»
- Постанова КМУ від 07.11.2018 № 992 «Про затвердження вимог у сфері ЕДП та Порядку перевірки дотримання вимог законодавства у сфері ЕДП»
- Постанова КМУ від 18.12.2018 № 1215 «Про затвердження Порядку проведення процедури оцінки відповідності у сфері ЕДП»
- Постанова КМУ від 23.01.2019 № 60 «Про затвердження Порядку взаємного визнання українських та іноземних сертифікатів відкритих ключів, електронних підписів, а також використання інформаційно-телекомунікаційної системи ЦЗО для забезпечення визнання в Україні ЕДП, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб'єктами різних держав»
- Постанова КМУ від 19.06.2019 № 546 «Про затвердження Положення про інтегровану систему електронної ідентифікації»

- Постанова КМУ від 18.09.2019 № 856 «Питання Міністерства цифрової трансформації»
- Постанова КМУ від 11.12.2019 № 1068 «Про внесення змін до деяких постанов КМУ»
- Постанова КМУ від 03.03.2020 № 193 «Про реалізацію експериментального проекту щодо забезпечення можливості використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів»
- Постанова КМУ від 29.04.2020 № 345 «Про реалізацію експериментального проекту щодо забезпечення безперервного надання кваліфікованих ЕДП у разі заміни надавача таких послуг»
- Постанова КМУ від 02.09.2020 № 785 «Про реалізацію експериментального проекту щодо використання віддаленого КЕП Смарт-Дія»
- Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ) від 20.07.2007 № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів КЗІ»
- Наказ Адміністрації ДССЗЗІ України від 23.06.2008 № 100 «Про затвердження Положення про державну експертизу у сфері криптографічного захисту інформації»
- Роз'яснення Міністерства юстиції України щодо порядку обчислення геш-значення, викладені у Листі Міністерства юстиції України від 15.10.2012 № 12776-026-12/133
- Наказ Адміністрації ДССЗЗІ від 18.12.2012 № 739 «Про затвердження Вимог до форматів криптографічних повідомлень»
- Наказ Державного агентства з питань електронного урядування України від 27.11.2018 № 86 «Про встановлення Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування»

- Про позначку кваліфікованого сертифіката відкритого ключа, затверджені Наказом Міністерства юстиції України, Адміністрації ДССЗІ України від 01.02.2019 № 316/5/57
- Наказ Міністерства юстиції України від 04.11.2019 № 3398/5 «Про затвердження Порядку подання до ЦЗО інформації про діяльність надавачів ЕДП та засвідчувального центру»
- Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання ЕДП, затверджені Наказом Міністерства юстиції України, Адміністрації ДССЗЗІ України від 18.11.2019 № 3563/5/610
- Регламент роботи ЦЗО, затверджений наказом Міністерства цифрової трансформації України від 19.12.2019 за №27
- Наказ Міністерства юстиції України від 17.01.2020 № 173/5 «Про визнання такими, що втратили чинність наказів Міністерства юстиції України»
- Наказ Міністерства цифрової трансформації України від 08 липня 2020 року № 104 «Про затвердження Порядку ведення Довірчого списку»
- Наказ Міністерства цифрової трансформації України від 20 липня 2020 року № 107 «Про затвердження інформаційної та технологічної карток адміністративної послуги внесення Міністерством цифрової трансформації України юридичних осіб та фізичних осіб-підприємців, які мають намір надавати ЕДП, до Довірчого списку»
- Наказ Міністерства цифрової трансформації України від 28 липня 2020 року № 112 «Про затвердження Порядку ведення реєстру чинних, блокованих та скасованих сертифікатів відкритих ключів»
- Наказ Міністерства цифрової трансформації України від 25 серпня 2020 року № 125 «Про затвердження форми плану припинення діяльності з надання кваліфікованих ЕДП, Вимог до формату реєстрів сформованих кваліфікованих сертифікатів відкритих ключів, а також носіїв інформації та порядку запису на них документів в електронній формі»

1.4 Регламент роботи ЦЗО

Відповідно до ЗУ «Про ЕДП», ЦЗО надає кваліфіковану ЕДП формування, перевірки та підтвердження чинності кваліфікованого сертифіката КЕП чи електронної печатки КНЕДП із застосуванням самопідписаного сертифіката відкритого ключа ЦЗО [12].

Організаційно-методологічні, технічні та технологічні умови діяльності ЦЗО у процесі надання ним кваліфікованої ЕДП формування, перевірки та підтвердження чинності сертифіката КЕП чи електронної печатки, порядок взаємодії надавачів ЕДП з ЦЗО у процесі надання ним кваліфікованої ЕДП формування, перевірки та підтвердження чинності сертифіката КЕП чи електронної печатки встановлюються Регламентом роботи ЦЗО [12].

Регламент роботи ЦЗО є обов'язковим для юридичних осіб та фізичних осіб-підприємців, які мають намір надавати ЕДП та для КНЕДП [12].

Дія Регламенту роботи ЦЗО не поширюється на надавачів ЕДП, що не мають наміру надавати кваліфіковані ЕДП та КНЕДП у банківській системі та під час здійснення переказу коштів [12].

Відповідно до вимог законодавства Регламент містить [13]:

- загальні відомості про надавача ЦЗО;
- перелік кваліфікованих ЕДП, надання яких забезпечує ЦЗО;
- перелік посад найманих працівників, обов'язки яких безпосередньо пов'язані з наданням кваліфікованих ЕДП, та функції таких працівників;
- політику сертифіката та положення сертифікаційних практик;
- опис процедур та процесів, які виконуються під час надання кваліфікованих ЕДП, що не передбачають формування та обслуговування кваліфікованих сертифікатів відкритих ключів.

Регламент роботи затверджується керівником ЦЗО – Міністром цифрової трансформації України та погоджується із контролюючим органом – Адміністрацією ДССЗЗІ.

1.5 Висновки до першого розділу

У першому розділі кваліфікаційної роботи було проаналізовано основний орган – ЦЗО, який є регулятором законодавства у сфері надання ЕДП.

Також, визначено основні нормативно-правові акти, які стосуються даної сфери, без яких не можна здійснювати регуляцію, але на жаль даний перелік є не повний, так як необхідно ЦЗО та суміжним органам державної влади розробляти додаткові документи для вдосконалення захисту КНЕДП.

Зафіксовано перелік установ, які входять до Довірчого списку.

Регламент роботи ЦЗО є обов’язковим для юридичних осіб та фізичних осіб-підприємців, які мають намір надавати ЕДП та для КНЕДП.

РОЗДІЛ 2 РОЗРОБКИ, ЯКІ Є НА РИНКУ УКРАЇНИ

2.1 Інфраструктура відкритих ключів

PKI – комплекс методів та засобів, які призначені забезпечувати впровадження та експлуатацію криптографічних систем з відкритими ключами [29].

PKI включає у собі ПЗ, криптографічні технології та служби, котрі надають можливість установам захищати канали зв'язку в комп'ютерних мережах. PKI включає у собі сертифікати, асиметричні алгоритми шифрування та ЦСК до єдиної мережевої архітектури [29].

PKI ґрунтується на криптосистемах з відкритим ключем та має певний набір властивостей, які є невід'ємними для захисту даних у розподілених системах. Дані властивості перераховані нижче [29]:

- один сертифікат (відкритий) застосовується для зашифрування повідомлення, для розшифрування необхідна наявність ключа, який містить перший сертифікат;
- через відкритий сертифікат не можна отримати доступ до ключа. Тобто, один із ключів відкритий для всіх, а другий є особистим та зберігається у захищеному місці. Такі ключі використовуються для формування КЕП та автентифікації.

Задачею PKI є створення сертифікатів КЕП, збереження сертифікатів та ключів, забезпечення резервних копій та відновлення ключів, взаємна сертифікація, ведення списків відкликаних сертифікатів (СВС) та автоматичного відновлення ключів та сертифікатів після завершення строку дії [29].

Підходи для реалізації PKI [29]:

- PKI, ґрунтується на сертифікатах у форматі X.509 – PKIX.
- проста PKI Simple Public Key Infrastructure/Simple Distributed Security Infrastructure (SPKI/SDSI).

Задача простої PKI SPKI – поширення сертифікатів для авторизації. Підґрунтям – проста розподілена інфраструктури безпеки SDSI. За допомогою

ключів і здійснюється об’єктів [15].

Мета сертифікату SPKI – авторизація дій, надання дозволів та прав власнику ключа. Сертифікати для авторизації генеруються власником ключа, який надає можливість застосовувати глобальне сховище інформації [15].

Сертифікат SPKI порівнюється зі звичайним ключем, де власник генерує сертифікати із заповненням обов’язкових полів. Прикладом для застосування: таємне голосування [15].

- захищена система доменних імен DNS.

Доменна система імен Domain Name System (DNS) є розподіленою БД з децентралізованим керуванням та зберігає інформацію щодо ресурси мережі та вказує схему іменування, що ґрунтується на доменних іменах [42].

Для захисту інформації (ЗІ) при передачі даних застосовується механізм TSIG, який автентифікує повідомлення DNS (передачі зони, динамічне оновлення та звичайні запити й відповіді) [42].

Для забезпечення коректної передачі даних DNS в рамках мережі Інтернет застосовується розширення протоколу – DNSSEC. Мета – застосування криптографії з відкритими ключами для додавання КЕП до даних. Секретний ключ відомий лише адміністратору, КЕП додається до БД у вигляді запису спеціального типу SIG. Дані передаються у відкритому вигляді, де відкритий ключ з пари ключів доступний всім охочим [42].

Для реалізації механізму DNSSEC використовуються наступні типи записів: KEY, SIG та NXT. Запис типу KEY містить відкритий ключ зони, а SIG – КЕП для набору записів [42].

- система захищеної електронної пошти Pretty Good Privacy (PGP).

Система PGP формується для захисту таємниці повідомлень електронної пошти в інформаційному середовищі. PGP це гібридна система, котра застосовує переваги криптографічних алгоритмів (симетричних чи асиметричних). Для користувача, система візуально має вигляд, як система з відкритим ключем, котра здійснює безпечний обмін повідомленнями відкритими каналами зв’язку без захищеного каналу. PGP виконує наступні

задачі: зашифровувати, формувати КЕП, розшифровувати, здійснювати перевірку повідомлень, які надійшли електронною поштою [44].

Для початку користувач генерує ключі (відкритий та особистий). Відкритий ключ передається іншому користувачу через електронну пошту. Другий користувач перевіряє чинність відкритого ключа, далі підтверджує безпеку та ступінь довіри до нього [44].

Система PGP виступає посередником для розповсюдження інформації щодо ступеню довіри до ключів. Загальна модель PGP підтримує централізований сценарій (сертифікати ключів засвідчує – засвідчувальний центр). Система PGP пропонує інтегровані засоби для поширення та пошуку ключів на серверах ключів [44].

- система захищених електронних транзакцій Secure Electronic Transaction (SET).

Протокол SET ґрунтується на технічному стандарті та забезпечує безпеку розрахунків за картками через мережу Інтернет (гарантує конфіденційність та цілісність інформації щодо платежі, автентифікацію рахунку власника картки та надає можливість підтвердити право продавця здійснювати фінансові операції) [46].

У середовищі SET – PKI є основою автентифікації користувачів для розрахунків. Конфіденційність та цілісність повідомлень забезпечується завдяки механізму подвійних підписів. Повідомлення зашифровується завдяки випадково згенерованого симетричного ключа шифрування, далі здійснюється зашифрування повідомлення. Як результат – конверт із зашифрованим повідомленням. Другий користувач – завдяки власному ключу розшифровується повідомлення відправника [46].

Протокол SET надає послугу автентифікації для учасників завдяки застосування сертифікатів формату X.509 та має засоби відкликання, реалізовані у вигляді списку відкликаних сертифікатів. В SET визначаються власні специфічні доповнення сертифікатів, які мають підтримку лише в SET-сумісних системах [46].

Основними складовими РКІ є ЦСК, центри реєстрації, репозиторії та архіви сертифікатів. Основними користувачами РКІ є: держателі та користувачі сертифікатів [46].

ЦСК – юридична особа незалежно від форми власності чи фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги щодо сертифікації відкритих ключів. ЦСК включає у себе апаратне та ПЗ, обслуговування їх. ЦСК здійснюють наступні задачі [28]:

- видача сертифікатів;
- оброблення статусу сертифікатів та підтримання списків відкликаних сертифікатів;
- поширення поточного списку дійсних та відкликаних сертифікатів для перевірки стану сертифікату;
- підтримка архівних даних щодо сертифікатів та їх стан.

Центр реєстрації – об'єкт, який відповідає за ідентифікацію та автентифікацію суб'єктів сертифікатів, але не підписує і не випускає сертифікати [28].

Архів – це БД, котра містить інформацію, яку зберігає та захищає інформацію для розв'язання різних суперечок, які можуть виникнути у майбутньому. Задачею архіву – безпечне збереження інформації для встановлення вірності давно зроблених КЕПів [28].

ЦСК формує сертифікати ключа КЕП, який включає відкритий ключ, основні реквізити підписувача, термін дії сертифікату, найменування та реквізити КНЕДП та КЕП самого ЦСК. Сертифікат включає і іншу інформацію про КНЕДП, власника сертифіката, чи інформацію про способи використання відкритого ключа. Користувачами РКІ є організації та фізичні особи, які користуються послугами РКІ, але не видають сертифікати КЕП.

Побудова ЦСК-доменів ґрунтується на таких типах ЦСК [28]:

- Ізольований/Одноранговий ЦСК;
- Кореневий ЦСК;
- Підпорядкований ЦСК;

- Шлюзовий ЦСК.

РКІ окремого підприємства, відомства тощо може бути побудована за однією з відомих моделей [28]:

- Одноранговий ЦСК-домен;
- Ієрархічний ЦСК-домен.

Реалізації таких моделей часто утворюють замкнену групу, утворену в межах одного організації та призначену для відокремленого від інших ЦСК застосування локальної інфраструктури КЕП [21].

Архітектура КЕП для об'єднання окремих ЦСК-доменів підприємств, відомств тощо в єдину довірчу інфраструктуру може бути за однією з відомих моделей [21]:

- Ієрархічна модель.

Ієрархічна модель об'єднує ЦСК-домени в структуру зв'язного графа у вигляді дерева, де вершина Кореневий ЦСК. Він не генерує ключі для користувачів, лише Підпорядкованим ЦСК, і вже саме вони видають ключі користувачам. Довірчі відносини формується лише від вищого рівня до нижчого рівня ЦСК [21].

Переваги Ієрархічної моделі [21]:

- простота її початкової побудови;
- видає сертифікати лише Підпорядкованим ЦСК;
- розмежовує доступ груп користувачів до сервісів;
- додає нові довірчі групи видавців сертифікатів шляхом підключення нового Підпорядкованого ЦСК;

Недоліки Ієрархічної моделі [21]:

- Компрометація Кореневого ЦСК – компрометація Ієрархічного «дерева», що призводить до заміни усіх без винятку ключів держателів;
- Єдиний Кореневий ЦСК може бути неможливим – конкуренція, міжвідомчі перепони;

- Перехід як від Ізольованих ЦСК до єдиної Національної ієрархічної моделі РКІ КЕП є логічно непрактичним.

В ієрархічній структурі при перевірці ланцюжків сертифікатів не передбачана перевірка сертифікату – самопідписаний, при компрометації ключа кореня публікація списку відкликаних сертифікатів є неможливою, так як список підписується скомпрометованим ключем [21].

- Мережена модель.

Мережена модель – модель встановлення довірчих відносин між окремими Ізольованими та Ієрархічними ЦСК.

Переваги мереженої моделі [3]:

- простота встановлення довірчих відносин;
- гнучка структура;
- компрометація окремого ЦСК не може скомпрометувати всю структуру;
- відновлення після компрометації простіше за використання попередньої моделі;
- легко формується з набору Ізольованих ЦСК.

Недоліки мереженої моделі [3]:

- при компрометації, має повідомити всіх;
- складніше процес розширення сертифікації;
- не детермінована, що ускладнює встановлення шляху сертифікації.

- Шлюзова модель.

Включає у собі кілька незалежних ізольованих та ієрархічних доменів та інших структур з даною моделлю, і саме вони об’єднуються довірчими відносинами через довірчого посередника. Шлюзовий ЦСК завдяки механізму кросс-сертифікації [37].

Особливість, які притаманна даній моделі – можливість додавання нових доменів через довірчого посередника, Шлюзовий ЦСК поєднує у собі переваги Ієрархічної та Мереженої моделей [37].

Переваги шлюзової моделі [37]:

- застосування процедури реєстрації учасників;
- ЦСК інформує Шлюзовий ЦСК;
- без складнощів можна підключити новий ЦСК;
- держателі та користувачі сертифікатів не змінюють свої ключі;
- компрометація окремого ЦСК, не може скомпрометувати усю структуру;
- відновлення після компрометації простіше в шлюзовій моделі.

Недоліки шлюзової моделі схожі до мереженої моделі.

- Одноранговий ЦСК

Одноранговий ЦСК-домен має ЦСК з автопідписаним сертифікатом, який не засвідчується іншим ЦСК. Одноранговий ЦСК-домен входить до ізольованого ЦСК та користувачів сертифікатів [23].

Приєднати ізольований ЦСК-домен до іншого ЦСК можна кількома способами [23]:

- Через ієрархічні відносини, як підпорядкований ЦСК – перевипуск ЦСК сертифікату, і у результаті перевипуск всіх сертифікатів користувачів.
- Через відносини рівноправних ЦСК – всі сертифікати користувачів залишаються чинними після приєднання Ізольованого ЦСК.

Переваги Однорангового ЦСК: мінімальна вартість та простота впровадження [23].

Недоліки Однорангового ЦСК [23]:

- Всі користувачів є рівними по відношенню до довірчих відносин та з одним і тим же профілем сертифікату;
- Не відрізняються довірчі сертифікати, є важливим з боку безпеки домену;
- Компрометація сертифікату чи приєднання Ізольованого ЦСК до Ієрархічного домену призводить до повного перевипуску всіх сертифікатів цього ЦСК;

- Стандарти PKI не допускають видачу сертифікатів клієнтам Ізольованими ЦСК.

2.2 Розробка Інституту інформаційних технологій

Система КЕП – організаційно-технічна система, котра здатна інтегрувати сертифікати відкритих ключів, засоби КЕП, ЦСК та власників сертифікатів в єдину структуру [14].

Головними елементами системи КЕП є ЦСК та їх користувачі. Система КЕП є сукупність взаємодіючих між собою ЦСК та кінцевих користувачів [14].

КНЕДП державних органів [14]:

- Центральний засвідчувальний орган;
- Державної податкової служби України (кваліфікований);
- Міністерства внутрішніх справ України (кваліфікований);
- Міністерство оборони України (Збройних сил України-акредитований);
- Державної прикордонної служби України (кваліфікований);
- ДП «Дія» України (органів юстиції – кваліфікований);
- ДП «Українські спеціальні системи» (кваліфікований);
- Державна адміністрація залізничного транспорту України (Укрзалізниця – кваліфікований);
- Українські спеціальні системи (кваліфікований);
- ДП «Енергоринок» (ринку електричної енергії – кваліфікований).

КНЕДП банків:

- Національний банк України;
- АТ «УкрСиббанк» (кваліфікований);
- АТ КБ «Приватбанк» (кваліфікований);
- ТОВ «Арт-мастер» (кваліфікований) і ін.

ЦСК призначений для обслуговування сертифікатів та надання інших послуг (КЕП, електронна позначка часу та ін.).

ЦСК забезпечує [14]:

- обслуговування сертифікатів відкритих ключів користувачів до яких входять:
    - реєстрація користувачів;
    - сертифікація відкритих ключів користувачів;
    - розповсюдження сертифікатів;
    - управління статусом сертифікатів;
- надання послуг електронної позначки часу.

Здійснюється підтримки носіїв ключової інформації [14]:

- Електронний ключ «Кристал-1»,
- Електронний ключ «Алмаз-1К»,
- Захищений носій Avest AvestKey,
- Захищений носій Aladdin eToken/JaCarta,
- Захищений носій Автор SecureToken,
- Захищений носій Технотрейд uaToken,
- Захищений носій SafeNet iKey,
- Захищений носій Giesecke&Devrient StarSign,
- Захищений носій БІФІТ iBank Key,
- Смарт-карта «Карта-1»,
- Смарт-карта Техноконсалтинг TEllipse,
- Смарт-карта Aladdin eToken/JaCarta,
- Смарт-карта Автор CryptoCard,
- Смарт-карта Giesecke&Devrient StarSign,
- Смарт-карта БІФІТ Інтегра,
- Криптомодуль «Гряда-61»,
- Мережний криптомодуль «Гряда-301».
- Інші носії та криптомодулі з бібліотеками підтримки, які відповідають вимогам до алгоритмів, форматам та інтерфейсам, які реалізуються у засобах шифрування та надійних засобах КЕП з інтерфейсом PKCS#11.

1 Початкові та передпроектні роботи перед розгортання ЦСК [48]:

- Категоріювання та обстеження ЦСК.
- Підготовка початкової організаційно-розпорядчої документації.

2 Проектні роботи [48]:

- Розробка технічного завдання на комплексну систему захисту інформації (КСЗІ) ЦСК.
- Погодження технічного завдання на КСЗІ ЦСК з ДССЗЗІ України.
- Розробка вимог до будівельно-монтажних робіт у частині ЗІ.
- Розробка робочого проекту ЦСК.
- Розробка експлуатаційної документації на ЦСК.
- Погодження інструкцій з КЗІ з ДССЗЗІ України.
- Розробка організаційно-розпорядчої документації.
- Погодження регламенту з ДССЗЗІ України чи іншим вповноваженим органом.

3 Створення та впровадження [48]:

- Участь у проведенні будівельно-монтажних робіт.
- Постачання та монтаж обладнання, інсталяція ПЗ.
- Розробка програми внутрішніх випробувань.
- Навчання обслуговуючого персоналу.
- Супровід проведення внутрішніх випробувань та проведення дослідної експлуатації.

4 Експертизи та акредитація [48]:

- Отримання експертного висновку на ПТК ЦСК в галузі КЗІ ДССЗЗІ України.
- Підготовка документів до атестації КСЗІ в Держспецзв’язку України.
- Підготовка документів до кваліфікації чи реєстрації у ЦЗО.
- Супровід проведення експертних робіт під час кваліфікації чи реєстрації.

Як результат виконання робіт – формування кваліфікації ЦСК та отримання дозвільних документи [48]:

- експертний висновок у галузі КЗІ на програмно-технічний комплекс;
- атестат відповідності КСЗІ;
- свідоцтво про кваліфікацію чи посвідчення про реєстрацію.

Бібліотеки користувача ЦСК, які інтегруються у сторонні системи, наприклад [48]:

- системи електронної пошти: Microsoft Outlook, IBM Lotus Notes і т.д.;
- офісні пакети: Microsoft Office, Adobe Acrobat і т.д.;
- системи електронного документообігу: АСКОД, ДокПроф, Мегаполіс і т.д.;
- системи подання звітності у електронному вигляді до Державної податкової служби України, Пенсійного фонду України, МВС України і т.д.;
- автоматизовані та інтегровані банківські системи: SAP for Banking, Oracle і т.д.;
- автоматизовані інформаційні системи бюро кредитних історій;
- корпоративні та внутрішньовідомчі системи;
- власні засоби та комплекси КЗІ.

2.3 Розробка Сайферу

Система криптографічного захисту інформації «Шифр-Х.509» (СКЗІ «Шифр-Х.509») призначена для створення РКІ (створення ЦСК, у тому числі кваліфікованих, центрів реєстрації у рамках відповідності ЦСК, наданих користувачам засобів управління ключами), забезпечення послугами КЕП органів державної влади, місцевого самоврядування, підприємств, установ та організацій будь-якої форми власності, а також фізичних осіб [40].

Експертні висновки [40]

- Криптографічне ядро СКЗІ «Шифр-Х.509» є програмний виріб «Шифр+» (бібліотеки криптографічних перетворень), яке має чинний позитивний експертний висновок ДССЗЗІ України.
- СКЗІ «Шифр-Х.509» має чинний експертний висновок в області КЗІ, наданий ДССЗЗІ України.

Система «Шифр-Х.509» успішно інтегрується з наступними системами [40]:

- eFOUR, iFOBS, B2, EMOS.
- Nimbus.
- IB Pentagy.
- ProFIX/Bank.
- Ensemble.

Шифр-Х.509 підтримує роботу із носіями ключової інформації за інтерфейсом PKCS#11, табл.2.1.

Таблиця 2.1 – Підтримувані захищені носії

№	Виробник	Модель	Тип
1	ТОВ Автор, Україна	Author Secure Token-337	Token
2	ТОВ Автор, Україна	Author Secure SmartCard-336	SmartCard
3	ТОВ Мікрокрипт, Україна	Armorino	Token + Flash
4	Giesecke & Devrient, Німеччина	StarSign Crypto USB Token	Token, Token + Flash
5	Giesecke & Devrient, Germany	StarSign Crypto SmartCard	SmartCard
6	Технотрейд, Україна	uaToken	Token
7	ТОВ Авест Україна, Україна	Avest UA	Token
8	SafeNet, США	SafeNet Crypto eToken	Token
9	Gemalto, США	Gemalto ID Prime Series	Token, SmartCard

СКЗІ «Шифр Х.509» працює в комплексі та містить наступні компоненти [34]:

ПЗ ЦСК [34]:

- Сервер застосувань ЦСК.

- Поштовий модуль ЦСК.
- АРМ Адміністратора безпеки та аудиту ЦСК.
- АРМ Адміністратора сертифікації ЦСК.
- БД ЦСК.
- Довідник сертифікатів на базі LDAP-каталогу.

ПЗ центру реєстрації [34]:

- АРМ Адміністратора реєстрації.
- АРМ Віддаленого адміністратора реєстрації.
- АРМ Оператора реєстрації.
- АРМ оператора Центру прийому дзвінків.
- Комунікаційний модуль ЦР.
- БД ЦР.
- Модуль генерації ключів користувачів.

Серверне ПЗ [34]:

- Сервер OCSP.
- Сервер TSP.
- БД сервера TSP.
- Модуль обробки журналів сервера TSP.
- Веб-сайт ЦСК.
- Proxy-сервер.

ПЗ користувачів [34]:

- АРМ Модуля управління ключами.
- Java-застосування захисту даних та управління ключами.

Додаткові інструменти [34]:

- АРМ Системного адміністратора.
- АРМ Звітності ЦСК.
- Модуль роботи з ключовим контейнером.
- Модуль перегляду журналів.
- Модуль перегляду об’єктів PKI.

- Модуль сповіщення про статус сертифікатів.
- Модуль гарантованого видалення ключових контейнерів.

Бібліотеки функцій реєстрації та сертифікації для наступних платформ [34]:

- Win32.
- JRE.
- Android OS.

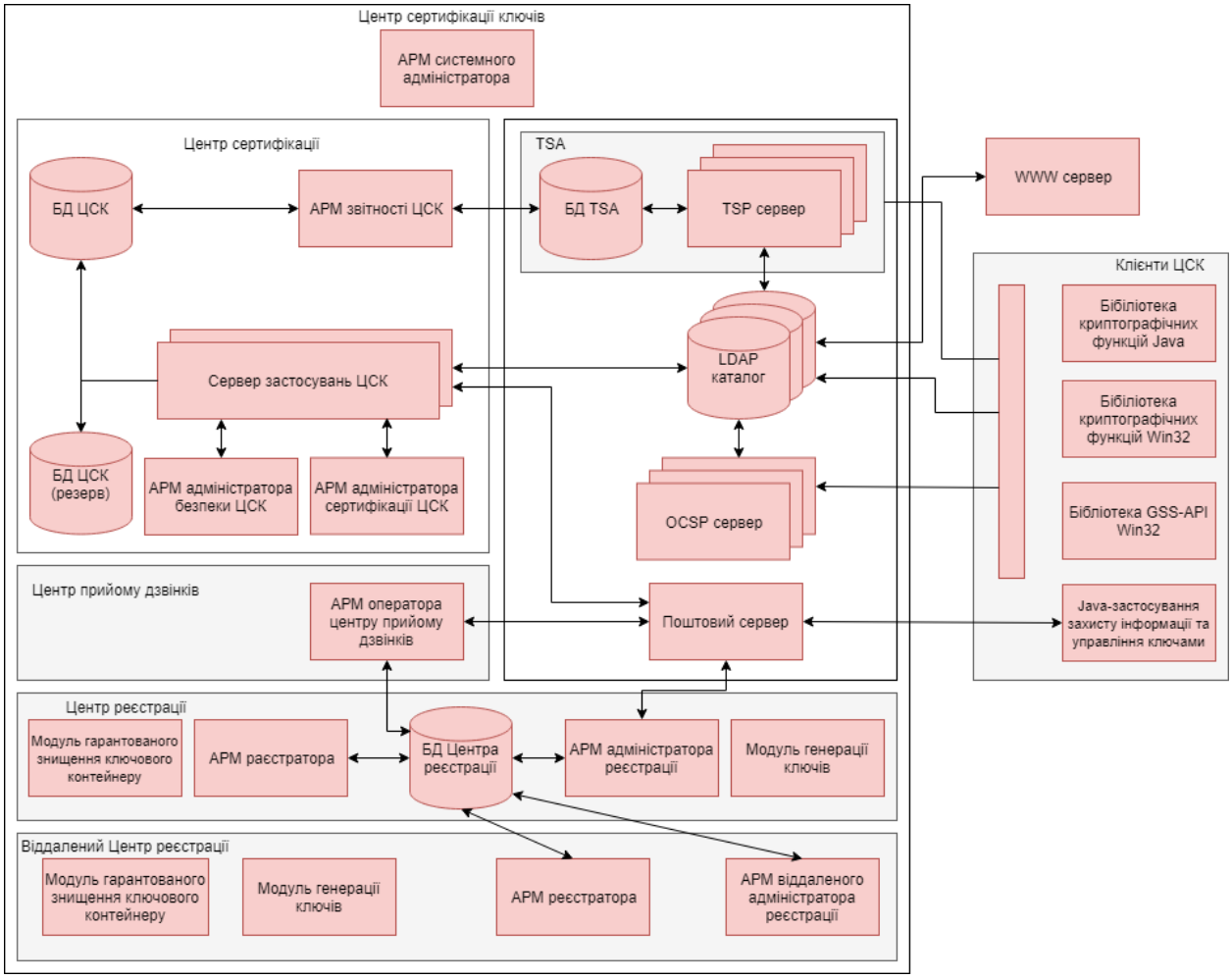


Рисунок 3.1 – Функціональна схема роботи СКЗІ «Шифр-Х.509»

ЦСК головним елементом СКЗІ «Шифр-Х.509», який здійснює управління ключами, видачу та відкликання сертифікатів, формування та видача списків відкликаних сертифікатів [20].

Складові елементи є [20]:

- Сервер застосувань
- АРМ Адміністратора безпеки та аудиту

- АРМ Адміністратора сертифікації
- Поштовий модуль ЦСК
- БД ЦСК

Програмні засоби центру реєстрації мають ідентифікувати, зареєструвати користувача для одержання сертифікату та надання послуг з генерації ключів користувачам, які хочуть одержати послугу безпосередньо в Центрі реєстрації (ЦР) [20].

Засоби ЦР складаються з наступних програмних засобів [20]:

- АРМ адміністратора реєстрації;
- АРМ реєстратора (оператора реєстрації);
- Комунікаційний модуль ЦР;
- БД ЦР;
- АРМ оператора ЦПД;
- АРМ віддаленого адміністратора реєстрації;
- Модуль генерації ключів;
- Модуль гарантованого знищення ключового контейнера;
- Модуль імпорту запитів у форматі PKCS#10;
- Довідник сертифікатів на базі LDAP-сервера.

Основними функціями ЦР є наступними [20]:

- Розмежування доступу до функцій та даних ЦР;
- Управління ключами адміністратора реєстрації;
- Управління ключами операторами реєстрації;
- Управління ключами оператора ЦПД;
- Управління ключами віддаленого адміністратора реєстрації;
- Ідентифікація та реєстрація користувачів;
- Видача стартових сертифікатів користувачів;
- Генерація робочих ключів для користувачів, які хочуть одержати робочі сертифікати безпосередньо в ЦР, формування запитів на сертифікати;

- Гарантоване знищення ключового контейнера, як на файловому носії, так і на носії ключової інформації;
- Прийом та перевірка автентичності запитів на сертифікати користувачів;
- Прийом та перевірка автентичності запитів на блокування/відновлення/скасування сертифікатів користувачів;
- Засвідчення запитів на сертифікати користувачів за підписом оператора реєстрації;
- Засвідчення запитів на сертифікати користувачів за підписом адміністратора реєстрації;
- Засвідчення запитів на блокування/відновлення/скасування сертифікатів користувачів за підписом адміністратора реєстрації;
- Засвідчення запитів на сертифікати користувачів за підписом віддаленого адміністратора реєстрації;
- Засвідчення запитів на блокування/відновлення/скасування сертифікатів користувачів за підписом віддаленого адміністратора реєстрації;
- Засвідчення запитів на блокування/відновлення/скасування сертифікатів користувачів за підписом оператора ЦПД;
- Передача запитів на сертифікати до ЦСК електронною поштою чи експорт в заданий каталог у вигляді файлу чи на носій ключової інформації;
- Передача запитів на блокування/відновлення/скасування сертифікатів в ЦСК електронною поштою чи експорту заданий каталог у вигляді файлу чи на носій ключової інформації;
- Прийом та контроль автентичності сертифікатів користувачів та СВС;
- Видача сертифікатів користувачам, які забажали отримати їх безпосередньо на ЦР чи віддаленому ЦР;
- Передача сертифікатів та СВС на адресу користувача, який генерує свої ключі самостійно;

- Введення та аудит локальної БД сертифікатів ЦР чи віддаленого ЦР, а також запитів на сертифікат та запитів на відкликання сертифікатів;
- Управління локальним довідником сертифікатів: розміщення, видалення сертифікатів у LDAP-каталозі.

Серверне ПЗ у структурі ЦСК складається з [11]:

- Сервер інтерактивного визначення статусу сертифікату (сервер OCSP).
- Інфраструктура сервісу надання електронних позначок точного часу (Time Stamping Authority – TSA), яка складається з:
    - Сервер точного часу (сервер TSP).
    - БД сервера TSP.
    - Планувальник обробки журналів сервера TSP.
    - Веб-сайт ЦСК.
    - Proxy-сервер.

У складі СКЗІ «Шифр-Х.509» використовують наступні додаткові інструменти [11]:

- АРМ Системного адміністратора.
- АРМ звітності ЦСК.
- Перегляд об’єктів та звітів роботи ЦСК:
    - Модуль перегляду журналів;
    - Модуль роботи з ключовим контейнером;
    - Модуль перегляду PKI-об’єктів;
- Модуль сповіщення про статус сертифікату;
- Модуль гарантованого видалення ключового контейнера.

Набір розширень для захисту документів за допомогою [11]:

- КЕП.
- Електронна позначка часу.

Набір розширень для захисту електронних повідомлень за допомогою [11]:

- зашифрування.
- КЕП.
- Електронної позначки часу.

Підтримуються наступні протоколи роботи з поштовими повідомленнями [11]:

- SMTP.
- POP3/IMAP.

Повідомлення, як на стороні сервера, так і на локальному комп’ютері.

Для роботи всіх розширень необхідна наявність доступу до всіх службових серверів ЦСК [11]:

- За спеціалізованими протоколами:
  - OCSP.
  - LDAP.
  - TSP.
- За єдиним протоколом:
  - HTTP/HTTPS.

Всі розширення, працюють з ключовими контейнерами, які знаходяться [19]:

- На файловому носії.
- На носії ключової інформації з підтримкою інтерфейсу PKCS#11.

Вся функціональність по роботі з сертифікатами, списком відкликаних сертифікатами, КЕП та електронними позначками часу реалізується у бібліотеках функції реєстрації та сертифікації. Для інтеграції в інші системи документообігу та захисту даних, дані бібліотеки надаються для наступних платформ [19]:

- Win32.
- JRE.
- Android OS.

2.4 Висновки до другого розділу

У ході підготовки другого розділу кваліфікаційної роботи було досліджено визначення інфраструктури відритих ключів, які притаманні їй властивості, варіанти реалізації.

Визначено задачі, які стоять перед ЦСК

- видача сертифікатів;
- оброблення статусу сертифікатів та підтримання списків відкликаних сертифікатів;
- поширення поточного списку дійсних та відкликаних сертифікатів для перевірки стану сертифікату;
- підтримка архівних даних щодо сертифікатів та їх стан.

Виявляється, що ЦСК-домени ґрунтуються на типах ЦСК, які описано у даному розділі:

- Ізольований/Одноранговий ЦСК;
- Кореневий ЦСК;
- Підпорядкований ЦСК;
- Шлюзовий ЦСК.

Додатково проаналізовано два фундатори апаратного та програмного забезпечення для побудови ЦСК: Інститут інформаційних технологій та Сайфер.

Де, перший пропонує організаційно-технічну систему, котра здатна інтегрувати сертифікати відкритих ключів, засоби КЕП, ЦСК та власників сертифікатів в єдину структуру. Та надає послуги для великої кількості державних органів влади та банківських установ.

А другий пропонує – СКЗІ «Шифр-Х.509», яка призначена для створення РКІ, забезпечення послугами КЕП органів державної влади, місцевого самоврядування, підприємств, установ та організацій будь-якої форми власності, а також фізичних осіб.

Розділ 3 ЗДІЙСНЕННЯ ЗАХИЩЕННОСТІ КВАЛІФІКОВАНОГО НАДАВАЧА ЕЛЕКТРОННИХ ДОВІРЧИХ ПОСЛУГ

3.1 Вибір моделі побудови інфраструктури відкритих ключів

Важливим елементом інтеграції РКІ є вибір її архітектури та проектування. РКІ допускає легкість проектування. Така архітектура починатися з боку ієрархії ЦСК. Кількість та рівні ЦСК залежать від вимог до безпеки та доступності [7].

Але застосування одного ЦСК як кореневого та видає конфігурацію небажаної з точки зору безпеки та масштабованості інфраструктури [7].

За потреби в наборі криптографічних сервісів та кількості облікових записів невелике, тому важливо використати однорівневу ієрархію [7].

Кореневий ЦСК не видаляється з мережі та повинен бути доступний для видачі сертифікатів. Управління однорівневою ієрархією не є складною, так як застосовується схема лише з одним сервером. Недоліки є низька відмовостійкість та неналежний рівень безпеки. Поломка серверу призводить до не здатності обробки запитів на видачі, відновлення, відкликання сертифікатів [7].

Компрометація серверу сертифікатів, призводить до втрати всієї РКІ, тобто вважаються не чинними сертифікати всієї РКІ [7].

Ієрархія, котра полягає у двох рівнях, котрі представляють собою відключений кореневий сервер та один чи кілька серверів, які генерують сертифікати (рис. 3.2.) [7].

Генеруючи сертифікати ЦСК можливості з управління політиками сертифікатів. Для забезпечення безпеки інфраструктури, кореневий центр – окремий та автономний, який не входить до вмісту домену, і не підключається до локальної обчислювальної мережі, який постійно знаходиться у відключеному стані. Таким чином, уникається можливість виникнення атак на кореневий сервер [39].

Для підвищення рівня доступності та відмовостійкості сервісу важливо розгорнути більше за один сервер, тобто повинен бути резервний ЦСК.

Кількість таких центрів, які генерують, то вони визначають функціональні вимоги, які покладені на ІТС [39].

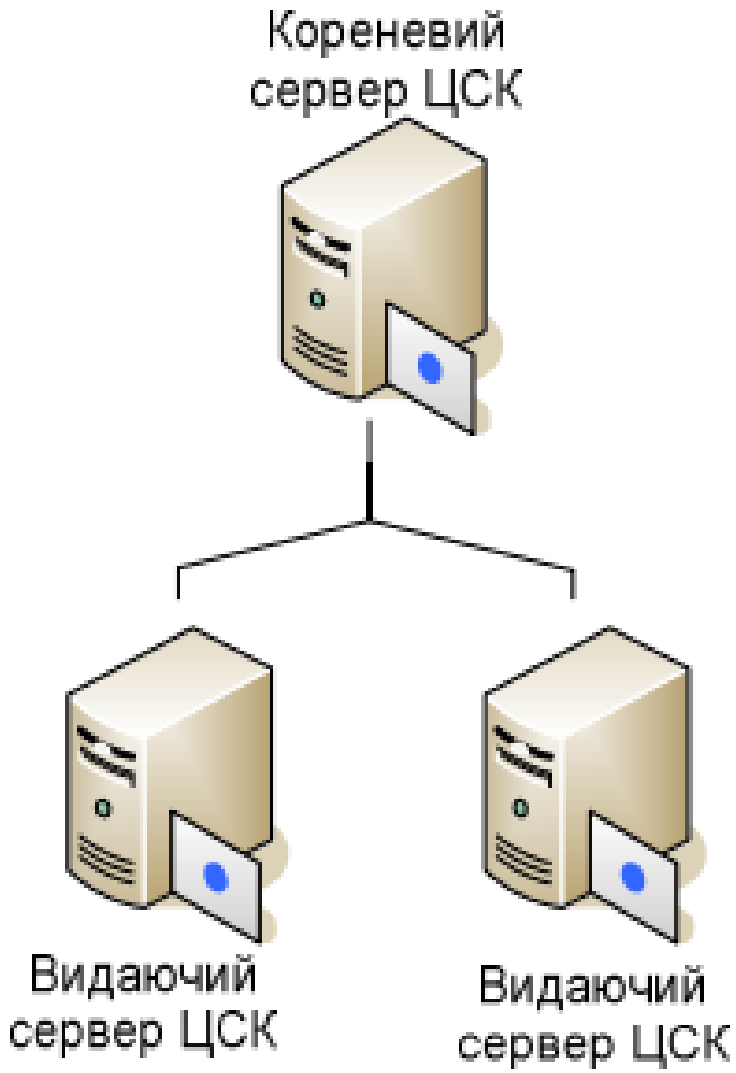


Рисунок 3.2 – Дворівнева ієрархія PKI

Трирівнева архітектура гарантує захист та масштабованість інфраструктури. Тоді здійснюється розгортання кореневого центру на іншому сервері, які не входять до складу корпоративної мережі [39].

Окремо здійснюється інтеграції серверів політик, які є підпорядкованими до кореневого ЦСК. Сервери не входять до складу корпоративної мережі та є окремими. Кореневий та підпорядковані сервери політик – відключені. Сервери, які генерують сертифікати – підпорядковуються серверам політик та можуть бути і корпоративними і окремими (рис. 3.3) [39].

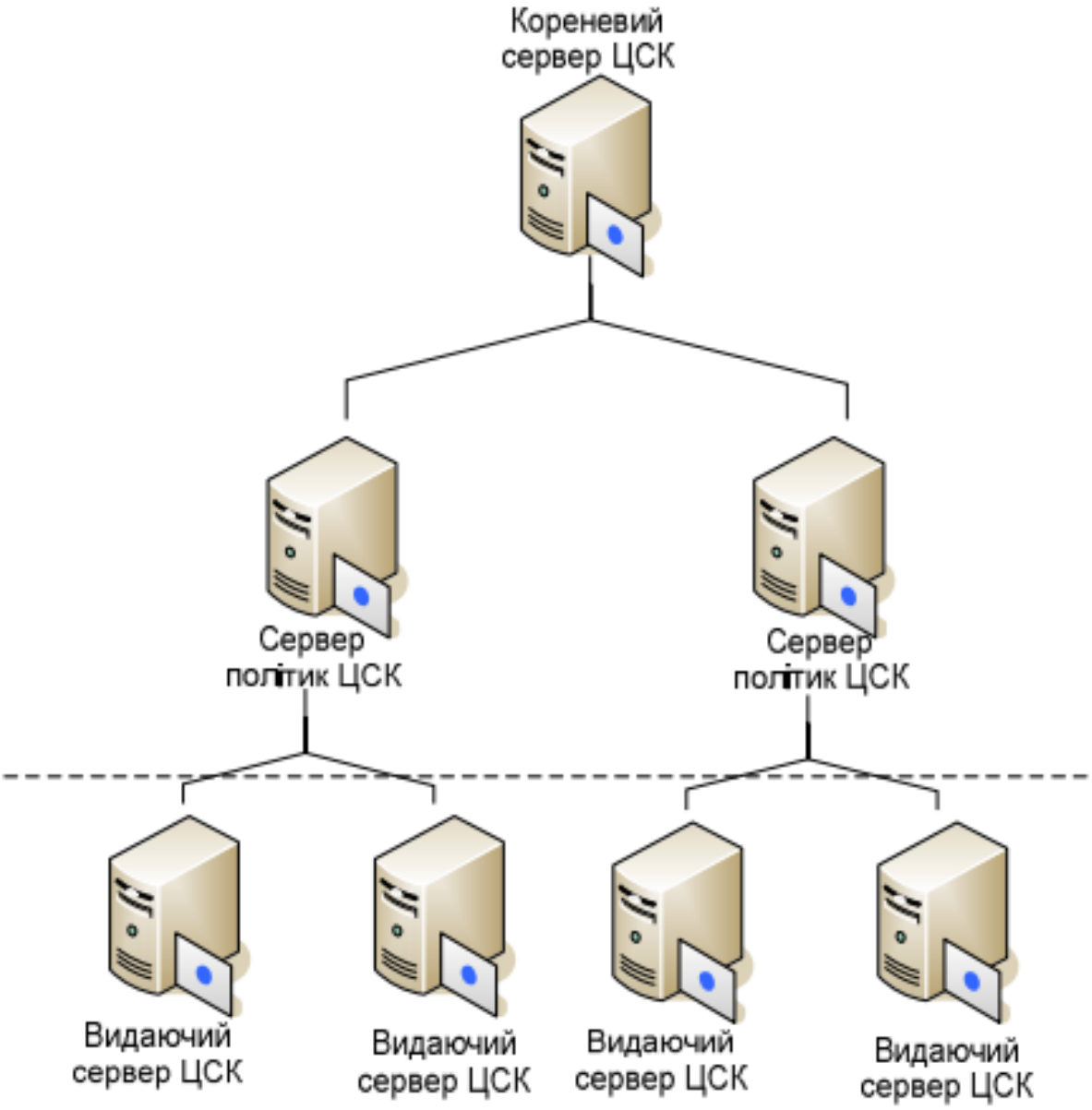


Рисунок 3.3 – Трирівнева ієрархів PKI

Пропонується застосовувати трирівневу архітектуру де [35]:

- Вимагаються високі вимоги до безпеки;
- Виникає потреба у політиках сертифікатів та пред’являються різні вимоги до використовуємих сертифікатів;
- Виникає необхідність у роздільному керуванні.

У інших випадках, варто використовувати чотирирівнева ієрархія PKI, зображена на рис. 3.4. Дана ієрархів є досить складною, більше за 4 рівні, застосовувати не рекомендується через її складність та сумнівну користь [35].

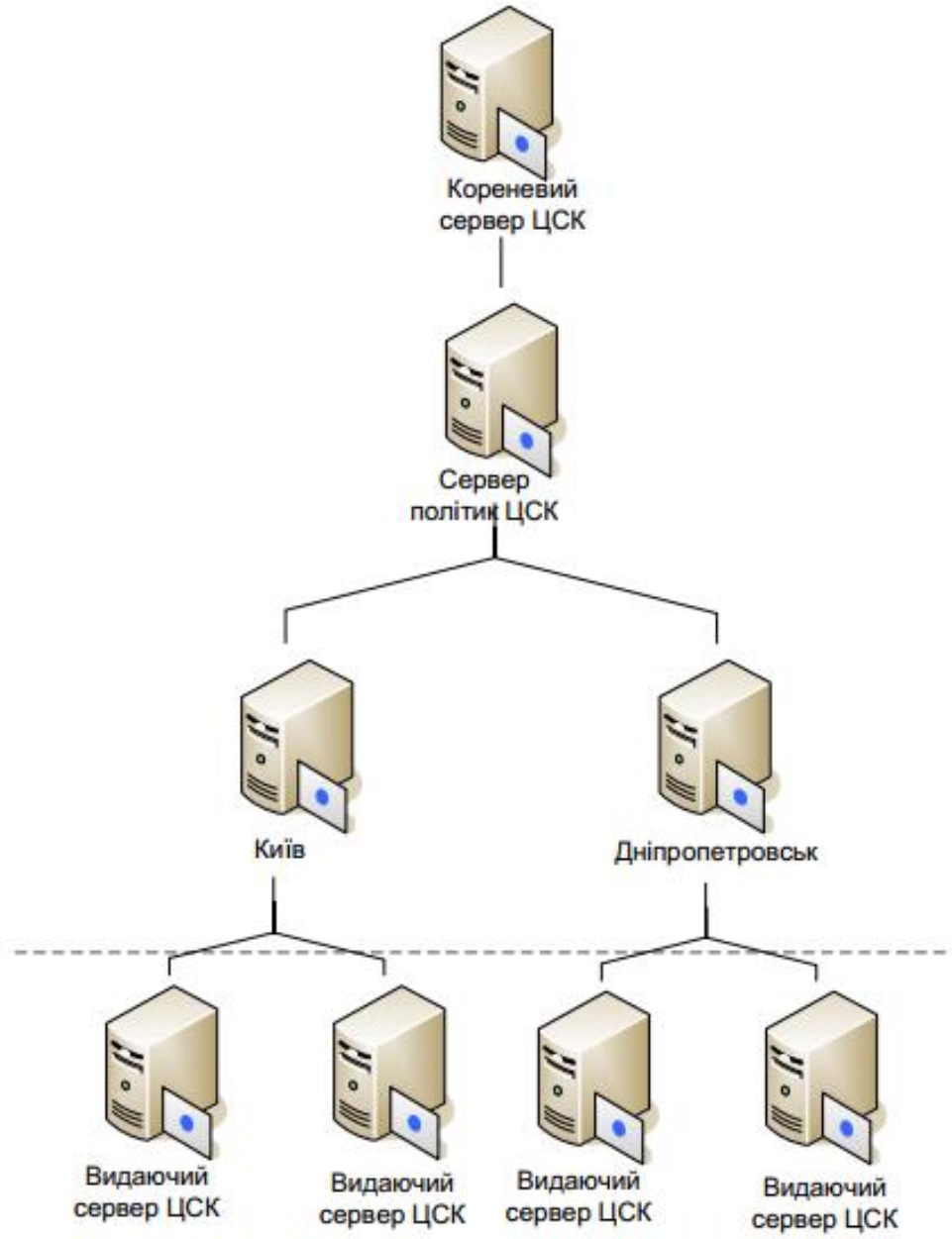


Рисунок 3.4 – Чотирирівнева ієрархів PKI

Вибір архітектури PKI визначається з кроків [35]:

- кількість сертифікатів, які генеруються;
- вимоги доступності для користувачів;
- модель адміністрування PKI;
- організаційна структура.

Інтеграція PKI може надати наступні можливості [35]:

- впровадження новітних інформаційних технології електронного документообігу;

- розширення можливостей інтеграції існуючих інформаційно-телекомунікаційних систем;
- гарантують цілісність та автентичність інформації, яка є в електронному вигляді;
- забезпечення легітимного електронного документообігу та реалізація правових відносин.

3.2 Вимоги до центрів сертифікації ключів

Відповідно Закону України «Про електронну комерцію» № 675-VIII від 03 вересня 2015 р., виникає проблематика можливостей ефективного застосування КЕП для здійснення приватноправових електронних правочинів, і в мережі Інтернет також [17].

Основні нормативно-правові акти є які регламентують використання у Законі України «Про електронні довірчі послуги» та Законі України «Про електронні документи та електронний документообіг». Прийняття цих законів однозначно позитивно впливає на впровадження та застосування КЕПу у різних сферах діяльності [17].

Відповідно Закону України «Про електронні довірчі послуги» – Кваліфікований електронний підпис прирівнюється до власноручного підпису (печатки) у випадку, якщо [17]:

– кваліфікований електронний підпис підтверджено з використанням кваліфікованого сертифіката ключа завдяки надійних засобів електронного підпису;

– під час перевірки використовувався кваліфікований сертифікат ключа, чинний на момент створення кваліфікованого електронного підпису;

– особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті».

У даному випадку, вимогами до суб’єктів є забезпечення можливостей застосування КЕП.

У країнах Європейського Союзу вимогами для надавачів електронних

довірчих послуг у сфері КЕП описуються у Директиві Європейського Союзу «Про порядок використання електронних підписів в Європейському Співтоваристві» 1999/93/ЕС [49].

Принципом надавачів електронних довірчих послуг у Європейському Союзі є дотримання п. 12 Преамбули Директиви 1999/93/ЕС можливості надання послуг КЕП особами публічного та приватного права. Країни ЄС зобов'язуються не забороняти провайдерам послуг в сфері використання КЕП без обмежень, застосовуючи схеми кваліфікації. Країни Європейського Союзу не мають мати обмеження про схеми кваліфікації [49].

У п. 16 Преамбули Директиви Європейського Союзу направлений застосування та визнання КЕП, нормативно-правова база не має застосовуватися за для обмежень для КЕП, та ґрунтується на добровільній згоді учасників даної системи, гарантується визнання КЕПів у якості доказів у процесі вирішення суперечок [49].

Визначені технічні вимоги в Європейському Союзі відносяться до посилених сертифікатів ключів, котрі застосовуються в сфері публічно-правових відносин. Регламент щодо КЕП у будь-яких відносинах залишається для учасників відносин. Європейський Союз застосовує КЕП за диспозитивним принципом, де регулююче втручання держав обмежується, це надає розвитку та не змушує обмежувати їх [49].

На відміну від ЄС чинне законодавство України містить диференційовані вимоги до учасників відносин у сфері застосування КЕП та їх діяльності. Виділяються наступних суб'єктів цих відносин [49]:

1) Підписант;

2) Користувач;

3) ЦСК;

4) КНЕДП.

На жаль, наразі не розроблено вимог до підписанта та користувача КЕП, тобто підпис документів та перевірка КЕП, за умови підписання іншими особами, без дотримання будь-яких адміністративних процедур [49].

Здійснення адміністративних процедур потребується лише від таких суб'єктів відносин, які пов'язані з КЕП як ЦСК та КНЕДП [32].

Аналіз ЗУ «Про електронні довірчі послуги» дозволяє сформулювати наступні основні відмінності ЦСК від КНЕДП [32]:

1) ЦСК може надавати послуги КЕП та обслуговувати звичайні сертифікати КЕП;

2) КНЕДП надає послуги КЕП та обслуговує лише удосконалені сертифікати ключів.

Різницею є у наданні послуг КЕП органам державної влади та місцевого самоврядування. Вдосконалені сертифікати ключів може видавати ЦЗО, функції покладаються на Міністерство цифрової трансформації та ЦЗО.

Для формування та діяльності ЦСК мають висуватися вимоги [32]:

1) Кваліфікаційні вимоги – до керівництва та/або персоналу ЦСК не встановлено.

2) Організаційні вимоги:

– Юридична особа будь-якої організаційно-правової форми чи приватний підприємець-фізична особа.

– Засвідчення власного відкритого ключа в ЦЗО, Міністерство цифрової трансформації або КНЕДП.

– Збереження особистих ключів підписантів та ознайомлення з ними в ЦСК забороняються.

– Про рішення щодо припинення діяльності ЦСК повинен сповістити підписантів за три місяці, якщо інше не визначено законодавством. Після повідомлення про припинення діяльності ЦСК не має жодного законного права видавати нові ключі та обслуговувати раніше видані.

– ЦСК, який сповістив щодо припинення діяльності, зобов'язується забезпечити захист прав споживачів повернувши кошти за надані послуги.

Деякі вимоги відповідають Директиві ЄС 1999/93/ЕС.

3) Технологічні та інші вимоги:

– ЦСК має забезпечити ЗІ у автоматизованих системах згідно чинного

законодавства. Тобто, щодо дотримання численних вимог до ЗІ в автоматизованих системах.

– ЦСК має забезпечити захист персональних даних, які отримані від підписанта, згідно чинного законодавством. Тобто, мається на увазі, відповідність Закону України «Про захист персональних даних» та технічних та організаційних вимог щодо ЗІ в автоматизованих системах.

– ЦСК має забезпечити у процесі генерації ключа відповідність відкритого ключа та відповідного особистого ключа підписанту.

– ЦСК має забезпечити своєчасне скасування, блокування та поновлення сертифікати ключів.

– ЦСК має забезпечити своєчасне сповіщення підписанта та додавання у сертифікат відкритого ключа підписанта інформації щодо обмеження застосування КЕП, котрі встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку ЦСК;

– ЦСК має забезпечити перевірку законності звернення користувача щодо скасування, блокування та поновлення сертифікатів ключів та збереження документів, згідно яких були скасовані, блоковані та поновлені сертифікати;

– ЦСК має забезпечити цілодобовий прийом заяв щодо скасування, блокування та поновлення сертифікатів ключів;

– ЦСК має забезпечити електронний перелік чинних, скасованих і блокованих сертифікатів ключів;

– ЦСК має забезпечити цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних списків сертифікатів через веб-сайт ЦСК;

– ЦСК має забезпечити збереження сформованих сертифікатів ключів впродовж строку;

– ЦСК має забезпечити надання консультації з питань, пов’язаних з КЕП.

Подібні вимоги є у в Директиві ЄС, але є певні відмінності: підвищенні вимоги щодо ЗІ в ІТС, які стосуються лише чинності осіб, котрі забезпечують обіг вдосконалених сертифікатів ключів – в Україні це КНЕДП [24].

Тому, є важливим розробити документи для ЦСК та КНЕДП [24]:

1) Засвідчення власного відкритого ключа в ЦЗО чи КНЕДП, де необхідно мати при собі документи:

2) Копія сертифікату відповідності на засоби КЗІ, що використовуються.

3) Копія сертифікату відповідності на засоби ТЗІ, що використовуються.

ЦСК застосовує засоби криптографічного та ТЗІ, розробляються та інтегруються сторонньою особою, котра має ліцензію та експертні висновки на розробку та впровадження у сфері криптографічного та/чи ТЗІ [24].

Процес формування та впровадження ЦСК є досить вартісною та займає багато часу на підготовку та підтримку його, тому деякі організації відмовляються від власного ЦСК, а зручніше користуватися ключами вже існуючих КНЕДП [24].

Відповідно вищевказаної Директиви, не мається вимагати здійснення адміністративних процедур для початку проведення діяльності у ЦСК. Вимагати можна лише у випадку, якщо це КНЕДП, який видає кваліфіковані сертифікати, тому надання адміністративних процедур здійснюється лише на принципах об’єктивності, прозорості, пропорційності та недискримінаційності. Важливим є застосування КЕП, які видаються КНЕДП інших країн. Відповідно ЗУ «Про ЕДП» вважається, КЕП, котрий отримано лише в Україні. У такому випадки, учасники правовідносин у сфері КЕП позбавляються можливості застосування послуг міжнародних компанії [24].

Згідно Директиви ЄС 1999/93/ЕС передбачається визнання сертифікатів ключів, які видані КНЕДП інших країн, якщо сертифікат дотримується хоча б однієї вимог [10]:

(a) надавач довірчих послуг відповідає вимогам Директиви, та кваліфікованій у системі добровільної кваліфікації, яка ґрунтується в державічлені ЄС;

(b) надавач довірчих послуг у країні-члені ЄС та гарантує відповідності своїх сертифікатів вимогам цієї Директиви;

(c) сертифікат чи надавач довірчих послуг визнається за двосторонньою або багатосторонньою угодою між ЄС та третіми країнами чи міжнародними

організаціями.

Як результат, нормативно-правові акти, Закони та постанови, формування та діяльність ЦСК є надмірним у порівнянні з ЄС. На відміну від ЄС, вимоги законодавства України до створення та діяльності ЦСК викладені у бланкетних та відсилочних нормах ряду нормативно-правових актів [10].

Тобто, це вимагає зробити висновок, що нормативно-правова база в Україні знижує розвиток у сфері застосування КЕП [10].

Недоліки законодавства не можуть бути вирішені у вигляді внесення незначних коректив, рішенням може бути лише перероблення чинного законодавства під рівень Європейського Союзу та в першу чергу відповідати Директиві ЄС «Про порядок використання електронних підписів в Європейському Співтоваристві» 1999/93/ЕС, для спрощення відповідних адміністративних процедур. Оптимальним є викладення всіх вимог у окремому нормативно-правовому акті [10].

3.3 Моделі побудови інфраструктури ЦСК та їх ризики

Програма щодо формування єдиної електронної інформаційної системи на державному рівні визначається важливою задачею для розвитку інформаційного суспільства України. Програма визначає надання послуг для громадян та юридичних осіб застосовуючи інформаційні системи, котрі забезпечують взаємодію органів виконавчої влади, з громадянами та юридичними особами на основі сучасних інформаційних технологій. Технології у різних системах потребують ідентифікації суб’єктів правових відносин та забезпечення цілісності та достовірності інформації із застосування КЕП [53].

Законодавством України визначено правовий статус КЕП та електронного документу. Для забезпечення застосування КЕП важливо сформувати інфраструктуру ЦСК – PKI. У ЗУ «Про електронні довірчі послуги» та постанові Кабінету Міністрів України, яка визначає функції та вимоги до ЦСК, КНЕДП, ЦЗО, засвідчувального центру органів виконавчої влади чи іншого державного органу [53].

При побудові Національної інфраструктури ЦСК необхідним є вибір варіанту моделі створення сертифікаційних шляхів між різними державними відомствами, комерційними та банківськими організаціями, тобто забезпечити надійність та високий рівень ЕДП відносин, інтеграцію та криптографічну незалежність кожного з організацій [53].

Побудова Національної інфраструктури КЕП не є лише технічним питання, але і питання національної безпеки. Тому, варто сформувати Національну інфраструктуру КЕП, де діючі системи різних форм власності та фінансові організації, мають працювати стабільно, не зазнавати збитків. Аналізуючи варіанти побудови Національної інфраструктури КЕП, варто врахувати наявність необхідних міжнародних технічних стандартів та діючих структур, які застосовують дані системи, чи їх компоненти [53].

ЦСК-домен – об’єкти певного ЦСК, яким видається сертифікат цим ЦСК [50].

Модель архітектури КЕП – модель об’єднання довірчими відносинами різних ЦСК-доменів [50].

Кросс-сертифікація – процес, який застосовується в РКІ, котрий встановлює довірчі відносини. Даний процес взаємної сертифікації двох рівноправних ЦСК-доменів, котрий застосовується одним ЦСК, для сертифікації іншим, окрім суміжного ЦСК. Це налає можливість отримувачам сертифікатів таких ЦСК-доменів перевіряє легальність сертифікатів одне одного. Механізм кросс-сертифікації встановлює довірчі відносини між рівноправними ЦСК доменами через незалежну взаємну кросс-сертифікацію адміністраторів Основних ЦСК у цих доменах [50].

Користувач сертифікату – суб’єкт чи об’єкт, котрі перевіряють чинність КЕП підписанта та низки сертифікатів. Власники сертифікатів отримують власні сертифікати у різних ЦСК, у залежності від організації чи товариства, членами якого вони є [22].

Інфраструктура КЕП містить кілька ЦСК, які пов’язуються довірчими шляхами, який дозволяє користувачеві сертифіката перевірити чинність КЕП та

низки сертифікатів, користувач має бути впевнений у чинності та законності сертифікату при його застосуванні. Отримувач підписаного документу, який немає власного ключа КЕП, має право перевірити чинність сертифікат підписанта, застосовуючи довірчий шлях сертифікату [22].

Задачею Національної інфраструктури КЕП – об'єднати PKI у єдину довірчу структуру, створивши довірчі шляхи сертифікації [22].

Для організації документообігу варто врахувати необхідність взаємозв'язку користувачів ЦСК за різної форми власності, у тому числі міжнародними організаціями та громадянами, які застосовують у своїй практиці міжнародні технічні стандарти та правила. Варто врахувати досвід країн, який є в рекомендаціях та стандартах EuroPKI Європейського Співтовариства, Федерального PKI Національного Інституту Стандартів і Технології США тощо [22].

3.4 Захищеність кваліфікованого надавача електронних довірчих послуг

Назва виробу: криптомодуль мережний «Гряда-301» чи «ІІТ МКМ Гряда-301» [4].

Виріб здійснює функції [4]:

– автентифікація комп'ютеру при доступі до криптомодуля;

– генерація особистих та відкритих ключів для алгоритмів КЕП;

– генерація особистих та відкритих ключів для протоколів розподілу ключів;

– генерація ключів для алгоритмів шифрування та генерацію випадкових послідовностей на основі апаратного генератора;

– зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД;

– створення та перевірка КЕП;

– обчислення геш-функції;

– розподіл ключових даних на основі асиметричних протоколів

розподілу;

– збереження даних у внутрішній пам’яті та захист їх від НСД;

– резервне копіювання ключів на зовнішні носії та відновлення ключів з носіїв;

– контроль цілісності та працездатності вбудованого ПЗ та ін.

Область застосування: апаратно-програмні засоби та комплекси КЗІ типу «П», «Ш» та «Р», які призначаються для захисту ІзОД, вимога щодо ЗІ яка встановлюється чинним законодавством, окрім інформації, яка становить державну таємницю та конфіденційної інформації [4].

Конструкція та технічні характеристики виробу [4]:

- Пристрій реалізується як окремий мережний вузол.
- Мережний криптомодуль являє собою сервер, висота – 1U та встановлюється у 19-ти дюймову стійку.
- Пристрій реалізується у кліматичному виконанні групи 2 відповідно стандарту ГОСТ 21552-90. Мережний криптомодуль входить до групи 1 технічних засобів, які призначені для експлуатації в наземних стаціонарних приміщеннях та спорудах.
- Електроживлення пристрою – 220В.
- Пристрій має 2 USB-розетки типу А для під’єднання носіїв ключової інформації (для керування та збереження резервних копій особистих ключів). У якості носіїв ключової інформації ля керування та збереження резервних копій особистих ключів застосовуються електронні ключі «КРИСТАЛ-1».
- Маса, не більше – 6.7 кг.
- Споживана потужність, не більше – 260 Вт.
- Зовнішні інтерфейси – 2 x Ethernet 10/100/1000.
- 2 x USB 2.0.

Криптографічні алгоритми та протоколи [4]:

Мережний криптомодуль «Гряда-301» реалізує криптографічні алгоритми та протоколи:

– шифрування за ДСТУ ГОСТ 28147:2009;

– КЕП за ДСТУ 4145-2002, RSA за PKCS#11 та ECDSA за ДСТУ ISO/IEC 14888-3:2014;

– гешування за ГОСТ 34.311-95;

– протоколи розподілу ключів за ДСТУ ISO/IEC 15946-3 та RSA за PKCS#11.

Генерація ключових даних здійснюється відповідно методики генерації ключових даних, яка погоджується Адміністрацією ДССЗЗІ.

Таблиця 3.1 – Дані, щодо швидкості формування КЕП

Швидкість формування КЕП за ДСТУ 4145-2002, поле 257	
час формування КЕП-0,64 мс	кількість формувань КЕП-1560 формувань/с
Швидкість формування спіл. секрету за ДСТУ ISO/IEC 15946-3, поле 431	
час формування спільного секрету-5,12 мс	кількість формувань спільного секрету (державного): 196 формувань/с
Швидкість формування КЕП за RSA, 2048 біт	
час формування КЕП-18 мс	кількість формувань КЕП-55 формувань/с
Швидкість формування КЕП за ECDSA, NIST P-256, 256 біт	
час формування КЕП-1,3 мс	кількість формувань КЕП-770 формувань/с
Швидкодія протоколу розподілу ключів за RSA	
час розшифрування даних-18 мс	кількість розшифрувань даних-55 розшифрувань/с
Швидкодія протоколу розподілу ключів за ECDH	
час формування спільного секрету-21 мс	кількість формувань спільного секрету-47 формувань/с

Кількість ключів – 12 288.

До комплекту входить наступний перелік експлуатаційних документів та пристроїв, табл.3.2

Таблиця 3.2 – Перелік експлуатаційних документів та пристроїв

Назва	Кількість
ЄААД.469535.049. Мережний криптомодуль "Гряда-301"	1
ЄААД.469535.040. Електронний ключ "Кристал-1"	2
Кабель електроживлення	1
Електричний кабель мережі, 3м	1
Електричний кабель мережі, 1м	1
Комплект кріплення в 19-ти дюймову стійку	1
ЄААД.00049-01 97 01-1. Носій інформації з інсталяційним пакетом програм	1
ЄААД.469535.049 ЕД. Комплект експлуатаційних документі	1
Комплект тари та упакування	1

Ресурс виробу до першого ремонту має бути – 15000 годин впродовж терміну служби, термін зберігання – 1 рік [45].

Міжремонтний ресурс – 8500 годин при ремонті за технічним станом впродовж терміну служби [45].

Пристрій підтримує цілодобову чи змінну роботу [45].

Гарантії підприємства-виробника: за умови коректної експлуатації виробу, відповідно документації, яка надається до виробу, то гарантія складає 1 рік. Варто зауважити, що гарантійні зобов’язання поширюються лише на пристрої, які вказані у гарантійному талоні [45].

Виробник знімає з себе гарантійні зобов’язання, якщо пристрій відкривався самостійно без представників виробника, чи підлягав переробці, чи має механічні пошкодження. Після завершення гарантійного терміну, ремонт чи заміна пристрою проводиться за додаткову оплату [45].

Мережний криптомодуль «Гряда-301» з заводським номером та носії

ключової інформації «Кристал-1» з заводським номером виготовляються та приймаються згіднох вимог державних стандартів, технічної документації, котрі діють та визнані придатним для експлуатації [45].

Слід зауважити, що корпус пристрою має бути заземлений.

Обслуговування пристрою має здійснюватися згідно до технічних умов.

Пристрій експлуатується у приміщеннях з нормальними кліматичними умовами [30]:

– температура навколишнього повітря – $(15...35)^0$C;

– відносна вологість навколишнього повітря – (40...75) %;

– атмосферний тиск – 86-104 кПа (650-808 мм. рт. ст.).

Пристрій в упакованому вигляді транспортується – зберігається, зовнішній вигляд та працездатність після впливу кліматичних факторів з шестигодинною витримкою в нормальних кліматичних умовах [30]:

– температура навколишнього повітря – $(1...40)^0$C;

– відносна вологість навколишнього повітря 80% при температурі плюс 25^0C;

– атмосферний тиск – 86-104 кПа.

Відновлення працездатності пристрою після видалення особистих ключів має здійснюватися шляхом завантаження на спеціалізованому технологічному стенді підприємства-виробника [30].

Що стосується утилізації мережного криптомодулю, то він має бути надісланий відправлений підприємству-виробнику, лише після видалення особистих ключів, програмного забезпечення та інших критичних даних у ПЗП внутрішнього криптомодуля [30].

3.5 Висновки до третього розділу

У ході підготовки третього розділу кваліфікаційної роботи було проаналізовано та запропоновано вибір моделі побудови інфраструктури відкритих ключів. Проаналізовано ключовий аспект при впровадженні РКІ – вібір її архітектури та ризики при її реалізації.

Визначено, які постають вимоги до центру сертифікації ключів. Недоліки законодавства не можуть бути вирішені у вигляді внесення незначних коректив, рішенням може бути лише перероблення чинного законодавства під рівень Європейського Союзу та в першу чергу відповідати Директиві ЄС «Про порядок використання електронних підписів в Європейському Співтоваристві» 1999/93/ЕС, для спрощення відповідних адміністративних процедур. Оптимальним є викладення всіх вимог у окремому нормативно-правовому акті.

Розглянуто потенційні та фактичні моделі побудови інфраструктури ЦСК та їх ризики.

Для організації документообігу варто врахувати необхідність взаємозв'язку користувачів ЦСК за різної форми власності, у тому числі міжнародними організаціями та громадянами, які застосовують у своїй практиці міжнародні технічні стандарти та правила. Варто врахувати досвід країн, який є в рекомендаціях та стандартах EuroPKI Європейського Співтовариства, Федерального PKI Національного Інституту Стандартів і Технології США тощо.

Проаналізовано та запропоновано застосування мережного криптомодуля для підвищення захищеності кваліфікованого надавача електронних довірчих послуг. Таким чином, захищеність підвищується, збільшується швидкість здійснення операції, спрощується процес використання ключів для користувачів.

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи були виконані наступні **задачі**:

- Аналіз діяльності Центрального засвідчувального органу;
- Дослідження всіх розробок, які є на ринку в Україні;
- Забезпечення захищеності кваліфікованого надавача електронних довірчих послуг.

У першому розділі кваліфікаційної роботи було проаналізовано основний орган – ЦЗО, який є регулятором законодавства у сфері надання ЕДП.

Також, визначено основні нормативно-правові акти, які стосуються даної сфери, без яких не можна здійснювати регуляцію, але на жаль даний перелік є не повний, так як необхідно ЦЗО та суміжним органам державної влади розробляти додаткові документи для вдосконалення захисту КНЕДП.

Зафіксовано перелік установ, які входять до Довірчого списку.

Регламент роботи ЦЗО є обов’язковим для юридичних осіб та фізичних осіб-підприємців, які мають намір надавати ЕДП та для КНЕДП.

У ході підготовки другого розділу кваліфікаційної роботи було досліджено визначення інфраструктури відритих ключів, які притаманні їй властивості, варіанти реалізації.

Визначено задачі, які стоять перед ЦСК

- видача сертифікатів;
- оброблення статусу сертифікатів та підтримання списків відкликаних сертифікатів;
- поширення поточного списку дійсних та відкликаних сертифікатів для перевірки стану сертифікату;
- підтримка архівних даних щодо сертифікатів та їх стан.

Виявляється, що ЦСК-домени ґрунтуються на типах ЦСК, які описано у даному розділі:

- Ізольований/Одноранговий ЦСК;
- Кореневий ЦСК;

- Підпорядкований ЦСК;
- Шлюзовий ЦСК.

Додатково проаналізовано два фундатори апаратного та програмного забезпечення для побудови ЦСК: Інститут інформаційних технологій та Сайфер.

Де, перший пропонує організаційно-технічну систему, котра здатна інтегрувати сертифікати відкритих ключів, засоби КЕП, ЦСК та власників сертифікатів в єдину структуру. Та надає послуги для великої кількості державних органів влади та банківських установ.

А другий пропонує – СКЗІ «Шифр-Х.509», яка призначена для створення РКІ, забезпечення послугами КЕП органів державної влади, місцевого самоврядування, підприємств, установ та організацій будь-якої форми власності, а також фізичних осіб.

У ході підготовки третього розділу кваліфікаційної роботи було проаналізовано та запропоновано вибір моделі побудови інфраструктури відкритих ключів. Проаналізовано ключовий аспект при впровадженні РКІ – вібір її архітектури та ризики при її реалізації.

Визначено, які постають вимоги до центру сертифікації ключів. Недоліки законодавства не можуть бути вирішені у вигляді внесення незначних коректив, рішенням може бути лише перероблення чинного законодавства під рівень Європейського Союзу та в першу чергу відповідати Директиві ЄС «Про порядок використання електронних підписів в Європейському Співтоваристві» 1999/93/ЕС, для спрощення відповідних адміністративних процедур. Оптимальним є викладення всіх вимог у окремому нормативно-правовому акті.

Розглянуто потенційні та фактичні моделі побудови інфраструктури ЦСК та їх ризики.

Для організації документообігу варто врахувати необхідність взаємозв’язку користувачів ЦСК за різної форми власності, у тому числі міжнародними організаціями та громадянами, які застосовують у своїй практиці міжнародні технічні стандарти та правила. Варто врахувати досвід

країн, який є в рекомендаціях та стандартах EuroPKI Європейського Співтовариства, Федерального PKI Національного Інституту Стандартів і Технології США тощо.

Проаналізовано та запропоновано застосування мережного криптомодуля для підвищення захищеності кваліфікованого надавача електронних довірчих послуг. Таким чином, захищеність підвищується, збільшується швидкість здійснення операції, спрощується процес використання ключів для користувачів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. D.R. Kuhn, V.C. Hu, W.T. Polk, S.J. Chang. Introduction to Public Key Technology and the Federal PKI Infrastructure.-NIST SP 800-32, February 2001

2. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [Електронний ресурс]. – Режим доступу: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093.

3. EuroPKI Certificate Policy, Version 1.1 (Draft 4), October 2000, OID: 1.3.6.1.4.1.5255.1.1.1

4. Tatu Ylonen «Introduction to Cryptography» [Електронний ресурс] – Режим доступу: http://www.cs.hut.fi/ssh/crypto/intro.html.

5. William T. Polk, Nelson E. Hastings. Bridge Certification Authorities: Connecting B2B Public Key Infrastructures.-NIST, 03/08/2004.

6. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування: монографія / І. Д. Горбенко , Ю. І. Горбенко // Харк. нац. ун-т радіоелектрон., ЗАТ «Ін-т інформ. технологій». – Х.: Форт, 2012. – 868 с.

7. Горбенко Ю. І. Інфраструктури відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія / Ю. І. Горбенко, І. Д. Горбенко // Харк. нац. ун-т радіоелектрон., ЗАТ Інт інформ. технологій. – Х.: Форт, 2010. – 593.

8. М.Ф. Бондаренко, И.Д. Горбенко, С.П. Черных, А.В. Потий Инфраструктура открытых ключей как основа обеспечения информационной безопасности национальных, ведомственных и коммерческих систем информационных технологий. [Режим доступу] http://www.bezpeka.com/files/lib_ru/239_bgchpopenkey.zip

9. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України (ДССЗЗІ) від 20.07.2007 № 141 «Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів КЗІ» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

10. Наказ Адміністрації ДССЗЗІ від 18.12.2012 № 739 «Про затвердження Вимог до форматів криптографічних повідомлень» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

11. Наказ Адміністрації ДССЗЗІ України від 23.06.2008 № 100 «Про затвердження Положення про державну експертизу у сфері криптографічного захисту інформації» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

12. Наказ Державного агентства з питань електронного урядування України від 27.11.2018 № 86 «Про встановлення Вимог до засобів електронної ідентифікації, рівнів довіри до засобів електронної ідентифікації для їх використання у сфері електронного урядування» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

13. Наказ Міністерства цифрової трансформації України від 08 липня 2020 року № 104 «Про затвердження Порядку ведення Довірчого списку» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

14. Наказ Міністерства цифрової трансформації України від 20 липня 2020 року № 107 «Про затвердження інформаційної та технологічної карток адміністративної послуги внесення Міністерством цифрової трансформації України юридичних осіб та фізичних осіб-підприємців, які мають намір надавати ЕДП, до Довірчого списку» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

15. Наказ Міністерства цифрової трансформації України від 25 серпня 2020 року № 125 «Про затвердження форми плану припинення діяльності з надання кваліфікованих ЕДП, Вимог до формату реєстрів сформованих кваліфікованих сертифікатів відкритих ключів, а також носіїв інформації та порядку запису на них документів в електронній формі» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

16. Наказ Міністерства цифрової трансформації України від 28 липня 2020 року № 112 «Про затвердження Порядку ведення реєстру чинних,

блокованих та скасованих сертифікатів відкритих ключів» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

17. Наказ Міністерства юстиції України від 04.11.2019 № 3398/5 «Про затвердження Порядку подання до ЦЗО інформації про діяльність надавачів ЕДП та засвідчувального центру» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

18. Наказ Міністерства юстиції України від 17.01.2020 № 173/5 «Про визнання такими, що втратили чинність наказів Міністерства юстиції України» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

19. Постанова Кабінету Міністрів України (КМУ) від 27.01.2010 № 55 «Про впорядкування транслітерації українського алфавіту латиницею» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

20. Постанова КМУ від 02.09.2020 № 785 «Про реалізацію експериментального проекту щодо використання віддаленого КЕП Смарт-Дія» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

21. Постанова КМУ від 03.03.2020 № 193 «Про реалізацію експериментального проекту щодо забезпечення можливості використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

22. Постанова КМУ від 07.11.2018 № 992 «Про затвердження вимог у сфері ЕДП та Порядку перевірки дотримання вимог законодавства у сфері ЕДП» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

23. Постанова КМУ від 10.05.2018 № 356 «Про внесення змін та визнання такими, що втратили чинність, деяких актів Кабінету Міністрів України у зв’язку з прийняттям ЗУ «Про електронні довірчі послуги» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

24. Постанова КМУ від 10.10.2018 № 821 «Про затвердження Порядку зберігання документованої інформації та її передавання центральному

засвідчувальному органу в разі припинення діяльності КНЕДП» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

25. Постанова КМУ від 11.12.2019 № 1068 «Про внесення змін до деяких постанов КМУ» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

26. Постанова КМУ від 16.12.2015 № 1057 «Про визначення сфер діяльності, в яких центральні органи виконавчої влади здійснюють функції технічного регулювання» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

27. Постанова КМУ від 18.09.2019 № 856 «Питання Міністерства цифрової трансформації» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

28. Постанова КМУ від 18.12.2018 № 1215 «Про затвердження Порядку проведення процедури оцінки відповідності у сфері ЕДП» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

29. Постанова КМУ від 19.06.2019 № 546 «Про затвердження Положення про інтегровану систему електронної ідентифікації» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

30. Постанова КМУ від 19.09.2018 № 749 «Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

31. Постанова КМУ від 23.01.2019 № 60 «Про затвердження Порядку взаємного визнання українських та іноземних сертифікатів відкритих ключів, електронних підписів, а також використання інформаційно-телекомунікаційної системи ЦЗО для забезпечення визнання в Україні ЕДП, іноземних сертифікатів відкритих ключів, що використовуються під час надання юридично значущих електронних послуг у процесі взаємодії між суб’єктами різних держав» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

32. Постанова КМУ від 26.09.2018 № 775 «Про затвердження обов'язкових вимог до Довірчого списку» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

33. Постанова КМУ від 29.04.2020 № 345 «Про реалізацію експериментального проекту щодо забезпечення безперервного надання кваліфікованих ЕДП у разі заміни надавача таких послуг» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

34. Постанови КМУ «Порядок засвідчення наявності електронного документа (електронних даних) на певний момент часу» №680 від 26.05.2004 р., «Порядок акредитації центру сертифікації ключів» №903 від 13.07.2004 р.

35. Про встановлення вимог до технічних засобів, процесів їх створення, використання та функціонування у складі інформаційно-телекомунікаційних систем під час надання ЕДП, затверджені Наказом Міністерства юстиції України, Адміністрації ДССЗЗІ України від 18.11.2019 № 3563/5/610 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

36. Про електронний цифровий підпис [Текст]: Закон України від 22.05.2003 р. №852-IV // Голос України. – 2003. – №119.

37. Про електронні документи та електронний документообіг [Текст]: Закон України від 22.05.2003 р. №851-IV // Голос України. – 2003. – №119.

38. Про електронну комерцію [Електронний ресурс]: проект Закону України від 17.06.2013 р. № 2306а. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=47409.

39. Про затвердження Вимог до форматів криптографічних повідомлень: наказ Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

40. Про затвердження Положення про центральний засвідчувальний орган [Текст]: Постанова Каб. Міністрів України від 28.10.2004 р. №1451 // Уряд. кур'єр. – 2004. – №214.

41. Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності [Текст]: Постанова Каб. Міністрів України від 28.10.2004 р. №1452 // Уряд. кур'єр. – 2004. – №214.

42. Про затвердження Правил посиленої сертифікації: наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 13.01.2005 № 3 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

43. Про затвердження Регламенту роботи центрального засвідчувального органу: наказ Міністерства юстиції України від 29.01.2013 № 183/5 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

44. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

45. Про захист персональних даних [Текст]: Закон України від 01.10.2010 р. №2297-VI // Голос України. – 2010. – №172.

46. Про позначку кваліфікованого сертифіката відкритого ключа, затверджені Наказом Міністерства юстиції України, Адміністрації ДССЗІ України від 01.02.2019 № 316/5/57 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

47. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.1998 № 505/98 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

48. Про систему електронних підписів, що застосовується в межах Співтовариства: Директива Європейського Парламенту та Ради Європейського Союзу від 13.12.1999 № 1999/93/ЄС [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

49. Регламент роботи ЦЗО, затверджений наказом Міністерства цифрової трансформації України від 19.12.2019 за №27 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

50. Роз'яснення Міністерства юстиції України щодо порядку обчислення геш-значення, викладені у Листі Міністерства юстиції України від 15.10.2012 № 12776-026-12/133 [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

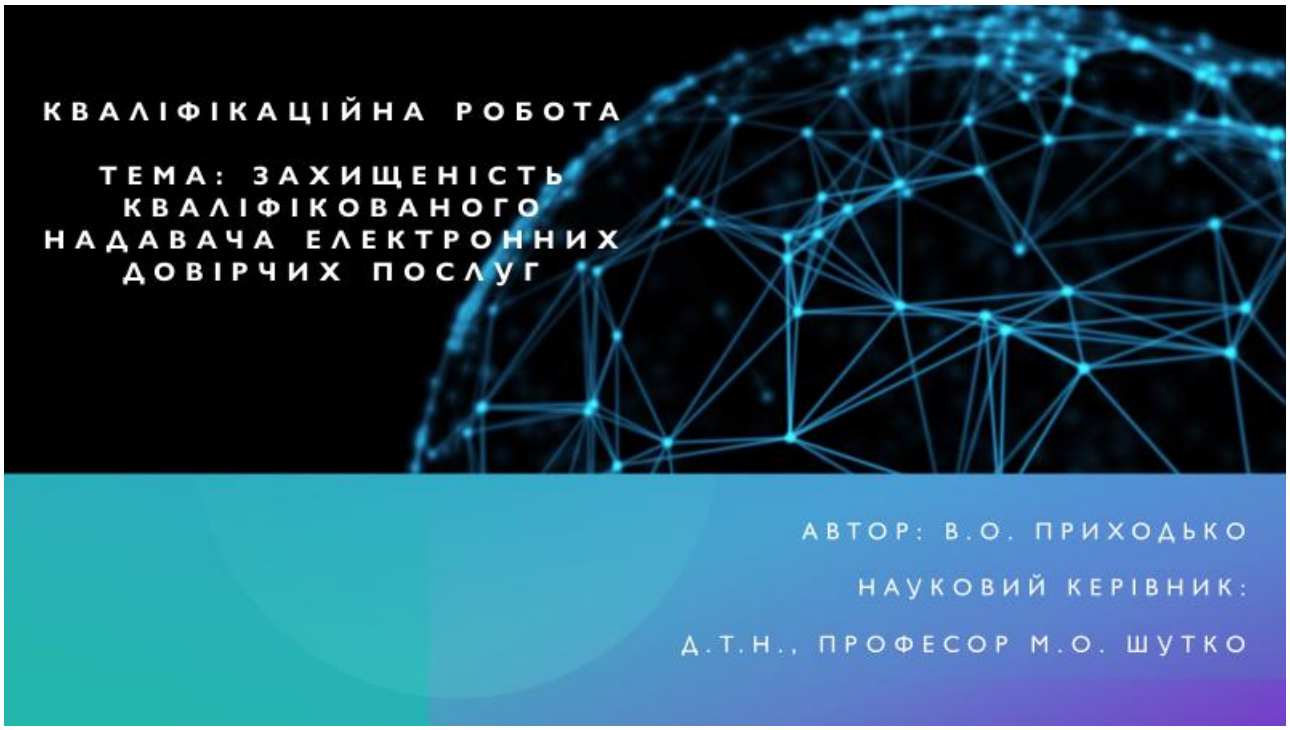
51. С. В. Бєлов, С. В. Мартиненко Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики [Режим доступу] http://www.itsway.kiev.ua/pdf/ModelCA_Risks.pdf

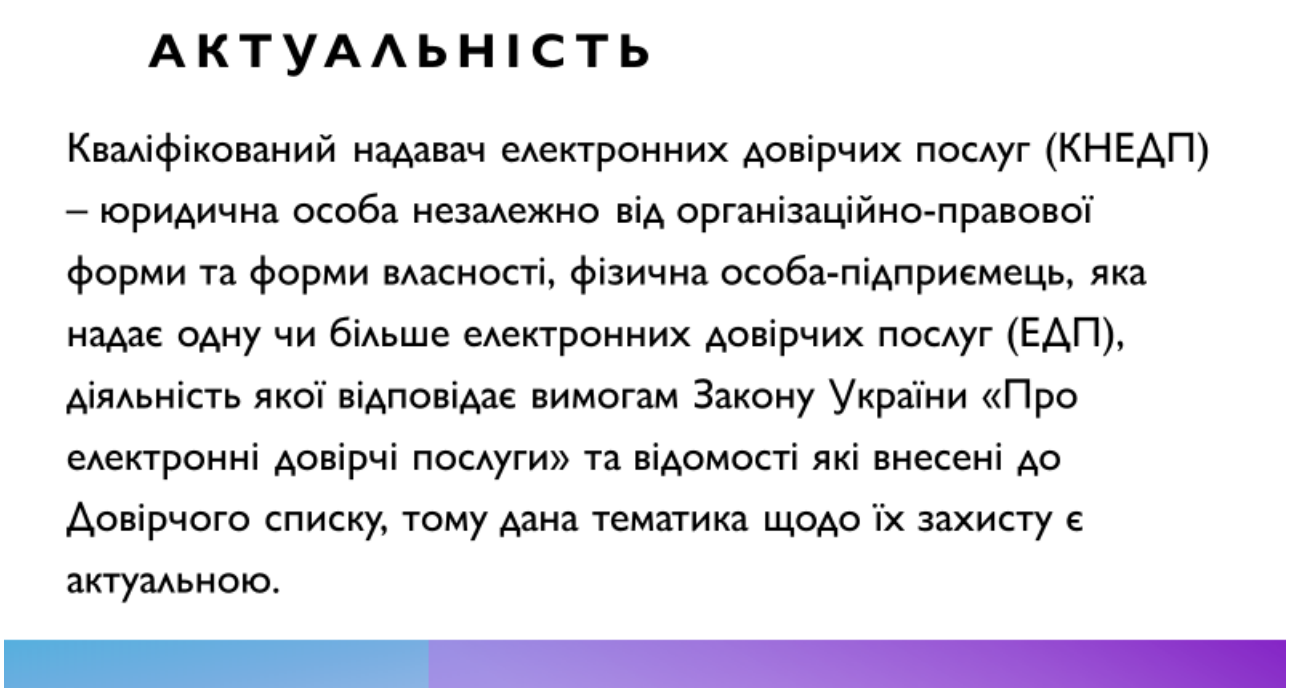
52. Терехов А. Н. Криптография с открытым ключом: от теории к стандарту. / А. Н. Терехов, А. В. Тискин // Программирование РАН. – 1994. – № 5. – С. 17–22.

53. Указ Президента України від 22.05.1998 № 505/98 «Про Положення про порядок здійснення криптографічного захисту інформації (КЗІ) в Україні» [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.

ДОДАТОК А

Оформлення слайдів та роздаткового матеріалу





МЕТА ТА ЗАДАЧІ РОБОТИ

Метою є забезпечення захищеності кваліфікованого надавача електронних довірчих послуг.

У процесі підготовки кваліфікаційної роботи були поставлені наступні задачі:

- Аналіз діяльності Центрального засвідчувального органу;
- Дослідження всіх розробок, які є на ринку в Україні;
- Забезпечення захищеності кваліфікованого надавача електронних довірчих послуг.

ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

- Об'єкт дослідження. Кваліфікований надавач електронних довірчих послуг.
- Предмет дослідження. Методи та способи для захисту КНЕДП.

НОВИЗНА ТА ПРАКТИЧНА ЦІННІСТЬ

Новизна роботи. Застосування мережного криптомодуля для підвищення захищеності кваліфікованого надавача електронних довірчих послуг.

Практична цінність. Результати досліджень можна використовувати для підвищення захищеності, швидкості здійснення операції, спрощення процесу використання ключів для користувачів.

РОЗДІЛ 1 ЦЕНТРАЛЬНИЙ ЗАСВІДЧУВАЛЬНИЙ ОРГАН

Функції та повноваження ЦЗО:

- Визначає повноваження у сфері ЕДП та електронної ідентифікації;
- Надає адміністративну послугу шляхом внесення юридичних осіб та фізичних осіб-підприємців, які мають намір надавати ЕДП до Довірчого списку;
- Узгоджує розроблені надавачами ЕДП порядки синхронізації часу із Всесвітнім координованим часом та припинення діяльності КНЕДП;
- Приймає та зберігає документовану інформацію, сформовані сертифікати відкритих ключів, реєстри чинних, блокованих та скасованих сертифікатів відкритих ключів у разі припинення діяльності КНЕДП;
- Розглядає пропозиції суб'єктів відносин у сфері ЕДП щодо удосконалення державного регулювання сфери ЕДП;
- Надає суб'єктам відносин у сфері ЕДП консультації з питань, пов'язаних з наданням ЕДП;
- Інформує відповідно до ЗУ «Про ЕДП» про обставини, які перешкоджають діяльності ЦЗО;
- Здійснює оцінку стану розвитку сфери ЕДП за результатами проведення аналізу інформації про діяльність постачальників ЕДП та ЦЗО;
- Забезпечує взаємне визнання українських та іноземних сертифікатів відкритих ключів та КЕП, які застосовуються у процесі надання юридично значущих ЕДП;
- Технічне та технологічне забезпечення виконання функцій ЦЗО здійснюється адміністратором інформаційно-телекомунікаційної системи ЦЗО.

РОЗДІЛ 2 РОЗРОБКИ, ЯКІ Є НА РИНКУ УКРАЇНИ

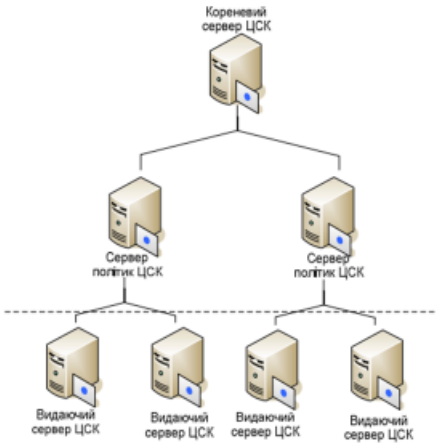
Розробка Інституту інформаційних технологій.
Система КЕП – організаційно-технічна система, котра здатна інтегрувати сертифікати відкритих ключів, засоби КЕП, ЦСК та власників сертифікатів в єдину структуру.
1 Початкові та передпроектні роботи перед розгортання ЦСК
2 Проектні роботи
3 Створення та впровадження
4 Експертизи та акредитація
Як результат виконання робіт – формування кваліфікації ЦСК та отримання дозвільних документи:

- експертний висновок у галузі КЗІ на програмно-технічний комплекс;
- атестат відповідності КСЗІ;
- свідоцтво про кваліфікацію чи посвідчення про реєстрацію.

РОЗДІЛ 2 РОЗРОБКИ, ЯКІ Є НА РИНКУ УКРАЇНИ

Розробка Сайферу.
СКЗІ «Шифр-X.509» призначена для створення PKI (створення ЦСК, у тому числі кваліфікованих, центрів реєстрації у рамках відповідності ЦСК, наданих користувачам засобів управління ключами), забезпечення послугами КЕП органів державної влади, місцевого самоврядування, підприємств, установ та організацій будь-якої форми власності, а також фізичних осіб.
ЦСК головним елементом СКЗІ «Шифр-X.509», який здійснює управління ключами, видачу та відкликання сертифікатів, формування та видача списків відкликаних сертифікатів.
Програмні засоби центру реєстрації мають ідентифікувати, зареєструвати користувача для одержання сертифікату та надання послуг з генерації ключів користувачам, які хочуть одержати послугу безпосередньо в Центрі реєстрації (ЦР).

РОЗДІЛ 3 ЗДІЙСНЕННЯ ЗАХИЩЕННОСТІ КНЕДП



Трирівнева ієрархів PKI

Назва виробу: криптомодуль мережний «Гряда-301» чи «ІІТ МКМ Гряда-301».
Виріб здійснює функції:

– автентифікація комп'ютеру при доступі до криптомодуля;
– генерація особистих та відкритих ключів для алгоритмів КЕП;
– генерація особистих та відкритих ключів для протоколів розподілу ключів;
– генерація ключів для алгоритмів шифрування та генерацію випадкових послідовностей на основі апаратного генератора;
– зберігання особистих ключів у внутрішній пам'яті та захист їх від НСД;
– створення та перевірка КЕП;
– обчислення геш-функції;
– розподіл ключових даних на основі асиметричних протоколів розподілу;
– збереження даних у внутрішній пам'яті та захист їх від НСД;
– резервне копіювання ключів на зовнішні носії та відновлення ключів з носіїв;
– контроль цілісності та працездатності вбудованого ПЗ та ін.

ВИСНОВКИ

У процесі підготовки кваліфікаційної роботи були виконані наступні задачі:

- Аналіз діяльності Центрального засвідчувального органу;
- Дослідження всіх розробок, які є на ринку в Україні;
- Забезпечення захищеності кваліфікованого надавача електронних довірчих послуг.

Проаналізовано та запропоновано застосування мережного криптомодуля для підвищення захищеності кваліфікованого надавача електронних довірчих послуг. Таким чином, захищеність підвищується, збільшується швидкість здійснення операції, спрощується процес використання ключів для користувачів.