

ІНСТРУКЦІЯ КОРИСТУВАЧА

щодо генерації ключів електронного цифрового
підпису за допомогою «Кабінету користувача»
центру сертифікації ключів
АТ «ПРАВЕКС БАНК»

1. ПЕРЕЛІК СКОРОЧЕНЬ

СМР – Certificate Management Protocol (протокол управління обслуговуванням посиленних сертифікатів).

LDAP – Lightweight Directory Access Protocol (протокол доступу до каталогу).

OCSP – Online Certificate Status Protocol (протокол визначення статусу посиленого сертифіката).

TSP – Time Stamp Protocol (протокол фіксування часу).

ЕЦП – Електронний цифровий підпис.

Кабінет користувача – Офіційний ресурс АТ «ПРАВЕКС БАНК» (<https://ca.pravex.com.ua:444/>).

НКІ – Носій ключової інформації.

ПЗ – Програмне забезпечення «ІТ Користувач ЦСК-1».

ПК – Персональна комп'ютер.

СВС – Список відкликаних сертифікатів.

ЦСК – Центр сертифікації ключів АТ «ПРАВЕКС БАНК».

Файлове сховище – Каталог (папка), призначений для зберігання посиленних сертифікатів та СВС.

2. ПРИЗНАЧЕННЯ КАБІНЕТУ КОРИСТУВАЧА

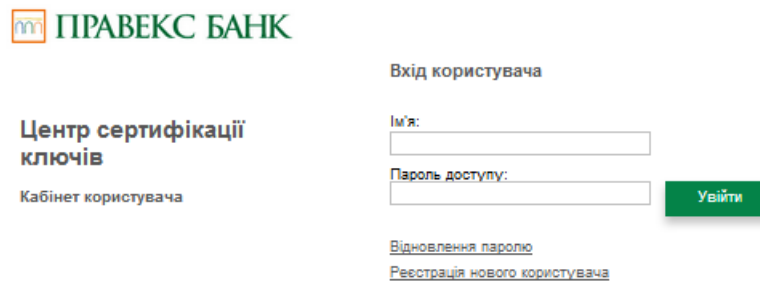
Кабінет користувача центру сертифікації ключів (надалі – Кабінет користувача) є офіційним ресурсом АТ «ПРАВЕКС БАНК», який забезпечує:

- реєстрацію користувачів;
- генерацію ключів ЕЦП користувачів;
- сертифікацію відкритих ключів ЕЦП користувачів.

3. РЕЄСТРАЦІЯ В КАБІНЕТІ КОРИСТУВАЧА

1. Для можливості генерації ключа ЕЦП ЦСК Банку необхідно зареєструватися в Кабінеті користувача за посиланням <https://ca.pravex.com.ua:444/>.

2. Стандартний вигляд головної сторінки Кабінету користувача наведено на [рис. 1](#).



ПРАВЕКС БАНК

Центр сертифікації
ключів

Кабінет користувача

Вхід користувача

Ім'я:

Пароль доступу:

Увійти

[Відновлення паролю](#)
[Реєстрація нового користувача](#)

Рис. 1. Головна сторінки Кабінету користувача

3. Для Клієнтів, які ще не зареєстровані в Кабінеті користувача, необхідно пройти процедуру реєстрації, натиснувши кнопку «Реєстрація нового користувача».

4. Після чого з'явиться форма реєстрації, яку необхідно заповнити реквізитами користувача. Приклад заповнення форми реєстрації наведено на [рис. 2](#).

5. Після введення необхідних даних натиснути кнопку [Зареєструвати](#)

Реєстрація користувача

Для реєстрації користувача кабінету ЦСК необхідно заповнити наступну форму заявки з інформацією про заявника (користувача)

Ім'я користувача *:

Адреса електронної пошти (e-mail) *:

Пароль *:

Пароль (підтвердження) *:

Прізвище *:

Ім'я та по батькові *:

Місто (нас. пункт) *:


Область (регіон) *:

Для міст Київ або Севастополь поле 'Область (регіон)' не заповнюється

Адреса :

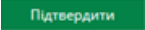
Телефон :

Код ДРФО **:

Я не робот  reCAPTCHA
Конфідційальність - Умовня використання

Зареєструвати

Рис. 2. Форма реєстрації користувача в Кабінеті користувача

6. Далі необхідно підтвердити коректність введених даних, натиснувши кнопку  (см. рис.3).

ПРАВЕКС БАНК КАБІНЕТ КОРИСТУВАЧА ЦСК

Реєстрація користувача

Перевірте дані що були введені. Для редагування необхідно перейти до попередньої форми.

Ім'я користувача: Тест4

Прізвище: Тест4

Ім'я та по батькові: Тест4

Місто (нас. пункт): Київ

Область (регіон):

Адреса:

Телефон:

Організація: Фізична особа

Підрозділ: Фізична особа

Посада: Фізична особа

Адреса електронної пошти: olga.dimpul@pravex.ua

Код ДРФО:

Рис. 3. Форма підтвердження реєстрації користувача

7. Після чого з'явиться повідомлення щодо необхідності підтвердження реєстрації користувача (см. рис.4):

Реєстрація користувача

Реєстрацію завершено успішно. Для підтвердження реєстрації перейдіть за посиланням, що наведено у електронному листі.

Рис. 4. Повідомлення щодо закінчення реєстрації користувача

8. На вказану при реєстрації користувача електрону адресу буде надіслано наступне повідомлення (см. рис. 5):

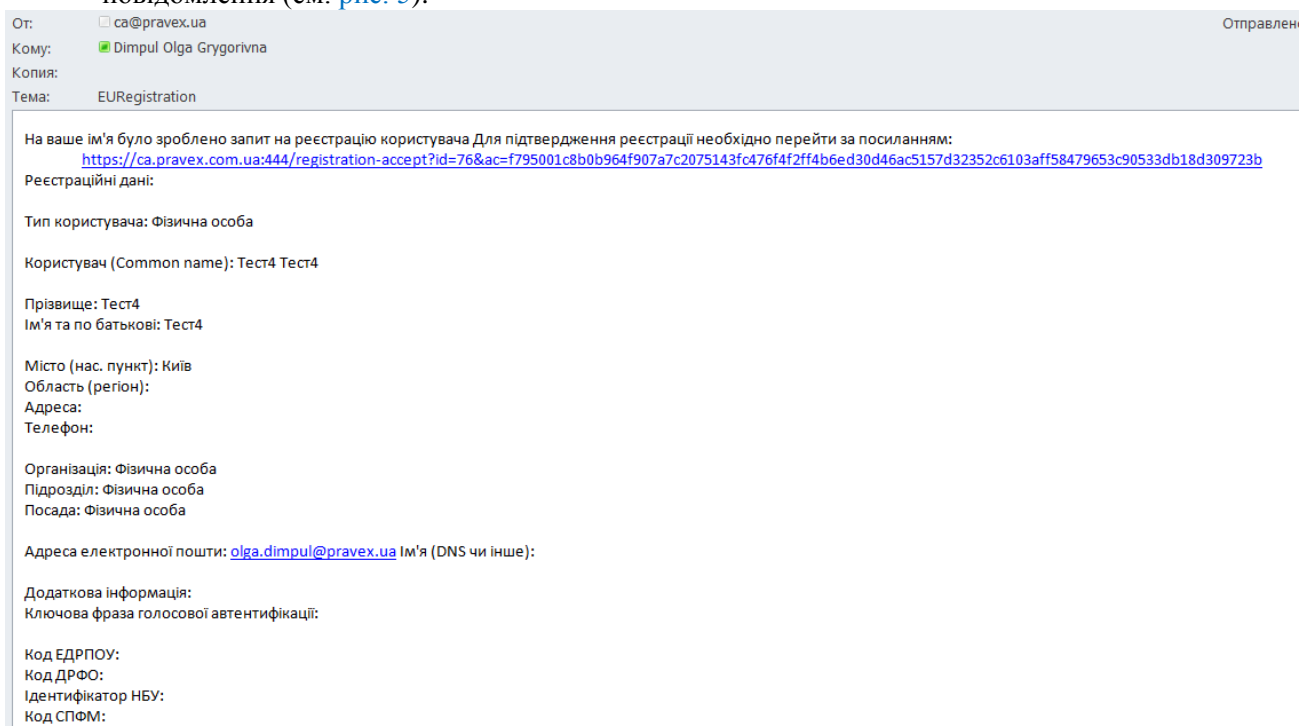


Рис. 5. Приклад електронного листа щодо підтвердження реєстрації

9. Для підтвердження реєстрації слід натиснути на посилання, після чого буде здійснено автоматичний перехід на сторінку з підтвердженням реєстрації (см. рис. 6).

Реєстрація користувача

Вашу реєстрацію підтверджено. Після перегляду ваших даних адміністратором безпеки ваш обліковий запис буде активовано.

Рис. 6. Сторінка підтвердження реєстрації в Кабінеті користувача

10. Після активації Адміністратором ЦСК облікового запису користувача, на електрону адресу користувача буде надіслано відповідне повідомлення (см. рис. 7).

From: ca
Sent: Tuesday, July 10, 2018 10:06 AM
To: Dimpul Olga Grygorivna
Subject: ЦСК АТ "ПРАВЕКС БАНК"

Користувача **Тест4** активовано.

<https://ca.pravex.com.ua:444/>

ЦСК

Адміністратор реєстрації



9/2, Klovsyy Uzviz, Kyiv, 01021, Ukraine

Tel: +38 044 5210251 (Int 49-81)

ca@pravex.ua

Follow PRAVEX BANK on:



Рис. 7. Приклад електронного листа з підтвердженням активації облікового запису користувача

11. При переході за посиланням, вказаним у електронному листі, відкривається головна сторінка ЦСК (см. [рис. 8](#)), на якій необхідно здійснити вхід в Кабінет користувача під ім'ям та паролем, зазначеним при реєстрації.

**Центр сертифікації
ключів**
Кабінет користувача

Вхід користувача

Ім'я:

Пароль доступу:

Увійти

[Відновлення паролю](#)
[Реєстрація нового користувача](#)

Рис. 8. Головна сторінка Кабінету користувача

4. ГЕНЕРАЦІЯ ОСОБИСТОГО КЛЮЧА

1. Стандартна сторінка Кабінету користувача наведена на [рис. 9](#).

Про кабінет користувача центру сертифікації ключів

Центр сертифікації ключів (ЦСК) забезпечує обслуговування сертифікатів відкритих ключів користувачів розробників та інших користувачів. Надає розробникам можливість створювати власний відокремлений пункт реєстрації ЦСК.

Центр сертифікації ключів забезпечує:

- обслуговування сертифікатів користувачів, що включає:
 - реєстрацію користувачів;
 - сертифікацію відкритих ключів користувачів;
 - розповсюдження сертифікатів через інформаційний ресурс - web-сайт та LDAP-каталог, а також за протоколом CMP;
 - управління статусом сертифікатів та розповсюдження інформації про статус сертифікатів через списки відкликаних сертифікатів на інформаційному ресурсі та за протоколом OCSP;
- фіксування часу (формування позначок часу).

У засобах ЦСК реалізуються наступні криптографічні алгоритми та протоколи:

- шифрування за ДСТУ ГОСТ 28147-2009, TDEA та AES за ISO/IEC 18033-3;
- ЕЦП за ДСТУ 4145-2002 та RSA за ISO/IEC 14888-2:2008 і PKCS#1;
- гешування за ГОСТ 34.311-95 та SHA за ISO/IEC 10118-3:2004;
- протокол розподілу ключових даних за ДСТУ ISO/IEC 15946-3 та вимог до форматів криптографічних повідомлень.

Засоби ЦСК підтримують наступні формати даних та операційні протоколи взаємодії:

- сертифікати та списки відкликаних сертифікатів (CVC) згідно ISO/IEC 9594-8 та державних вимог до надійних засобів ЕЦП;
- особисті ключі згідно PKCS#8 та PKCS#12;
- протокол OCSP (визначення статусу сертифіката) згідно RFC 2560 та державних вимог до надійних засобів ЕЦП;
- протокол TSP (фіксування часу) згідно RFC 3161 та державних вимог до надійних засобів ЕЦП;
- протокол CMP (управління сертифікатами);
- протокол LDAP (доступ до LDAP-каталогу);
- підписані дані (дані з ЕЦП) згідно ETSI TS 101 733 (CAAdES), RFC 5652 та державних вимог до надійних засобів ЕЦП;
- захищені дані (зашифровані дані) згідно RFC 5652 та державних технічних специфікацій.

Засоби кабінету користувача ЦСК забезпечують обслуговування тестових сертифікатів відкритих ключів користувачів. Надає можливість формувати тестові сертифікати користувачів, в т.ч. і з попередньою генерацією особистих ключів

Рис. 9. Кабінет користувача

2. Для генерації ключа ЕЦП необхідно обрати відповідний розділ - «Генерація ключів».
3. Для користувачів, які вперше здійснюють генерацію ключів ЕЦП в Кабінеті користувача, відобразиться наступне повідомлення (см. рис. 10):

Повідомлення оператора

Виникла помилка при взаємодії з криптографічною бібліотекою. Бібліотеку web-підпису не запущено або не інстальовано у системі. Для продовження необхідно запустити або інстальувати бібліотеку web-підпису.

- ➔ [Інсталяційний пакет web-бібліотеки підпису](#)
- ➔ [Інсталяційний пакет бібліотеки підпису \(web-розширення\)](#)
- ➔ [Настановна користувача](#)

ОК

Рис. 10. Повідомлення про необхідність запуску/інсталяції бібліотеки web-підпису

4. Необхідно обрати один із варіантів: «Інсталяційний пакет web-бібліотека підпису» або «Інсталяційний пакет бібліотеки підпису (web-розширення)».
5. Порядок дій в залежності від обраного варіанту:
 - 5.1. «Інсталяційний пакет web-бібліотека підпису» (см. рис. 11 (а), (б), (в), (г), (д), (е), (ж))
 - Закачати інсталяційний пакет

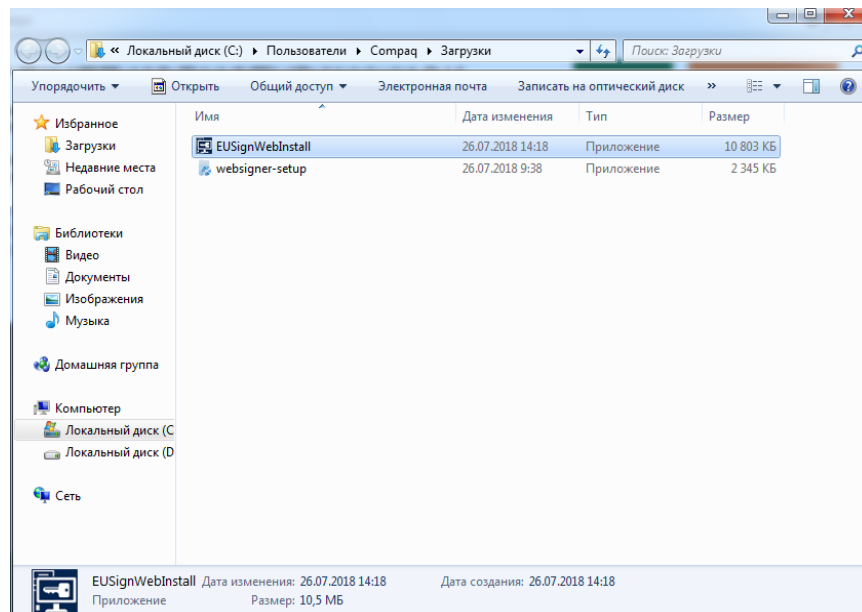


Рис. 11 (а)

- Встановити програму

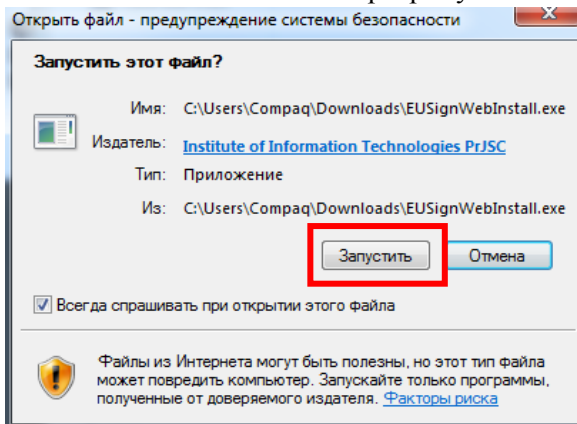


Рис. 11 (б)

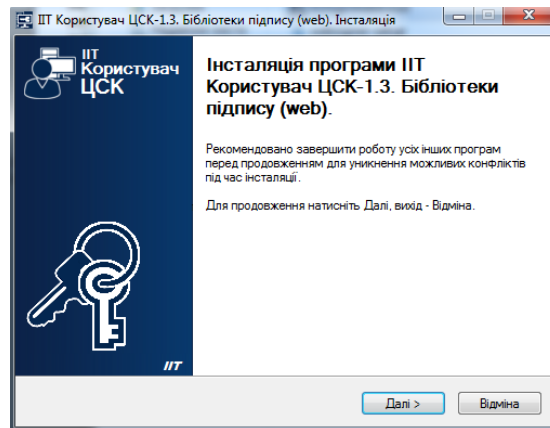


Рис. 11 (в)

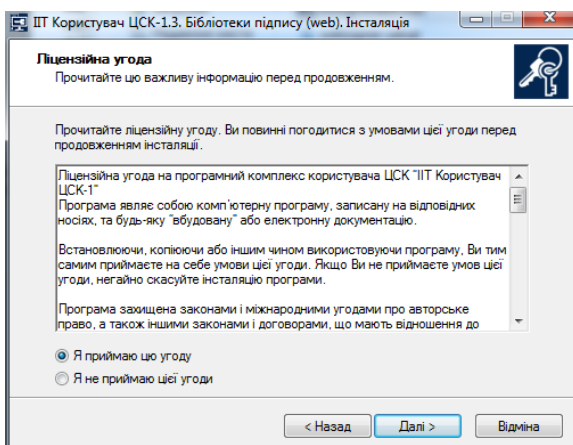


Рис. 11 (г)

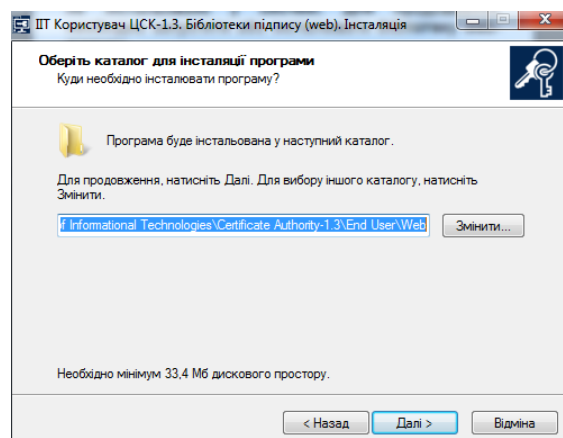


Рис. 11 (д)

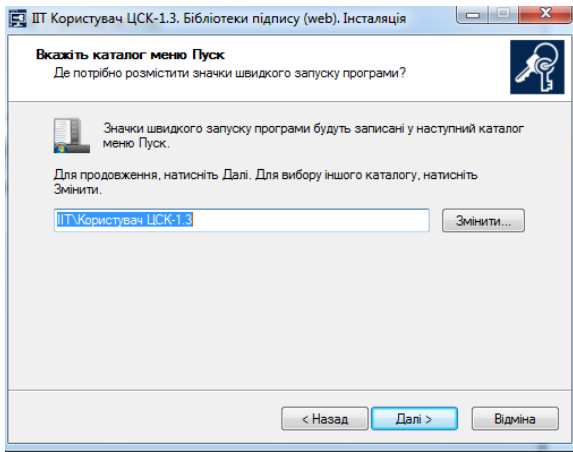


Рис. 11 (е)

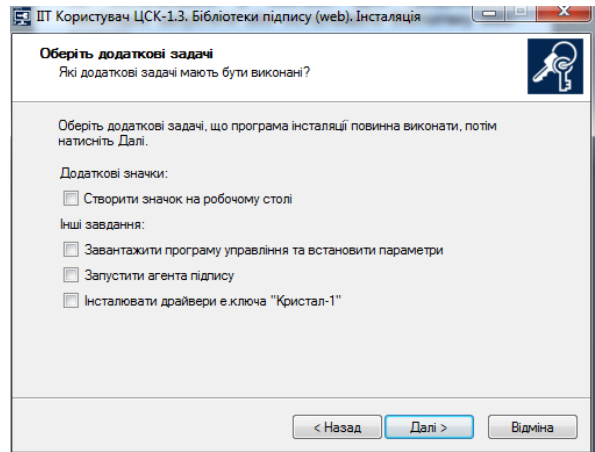


Рис. 11 (ж)

- Запустити програму

Після встановлення програми на робочому столі з'явиться ярлик з назвою «ІТ Користувач ЦСК-1.3. Агент підпису». Для продовження роботи з генерації ключа його потрібно запустити.

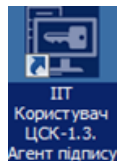


Рис. 11 (з)

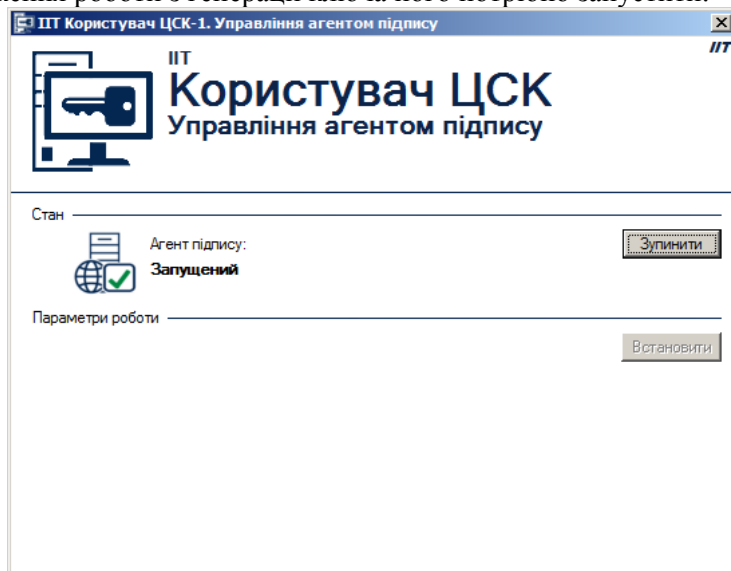


Рис. 11 (и)

5.2. «Інсталяційний пакет бібліотеки підпису (web-розширення)» (см. рис. 12 (а), (б), (в), (г))

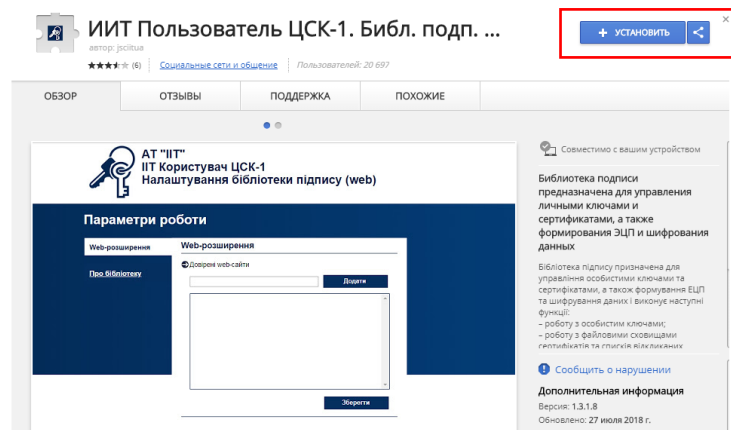


Рис. 12 (а)

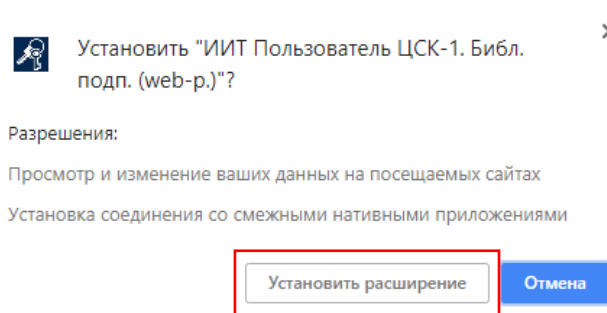


Рис. 12 (б)

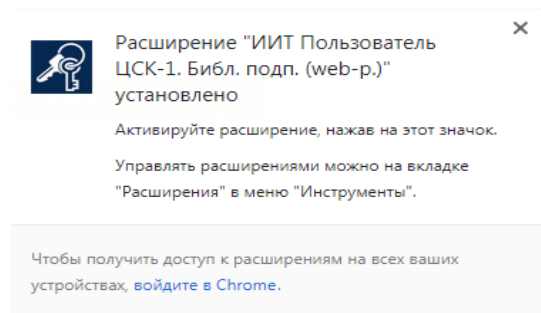


Рис. 12 (в)

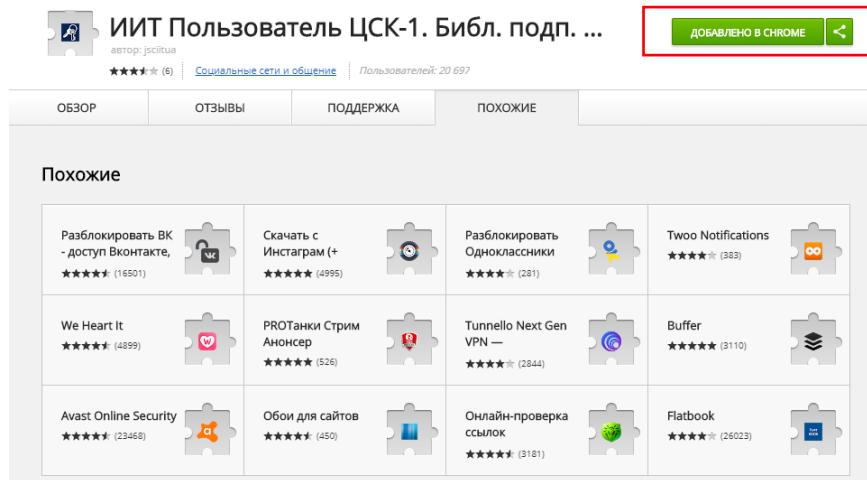


Рис. 12 (г)

6. Після інсталяції/запуску криптографічної бібліотеки необхідно перейти до генерації ключів ЕЦП.
7. Генерація ключів складається з двох кроків:
 - генерація особистого ключа
 - формування запиту на створення сертифікату.

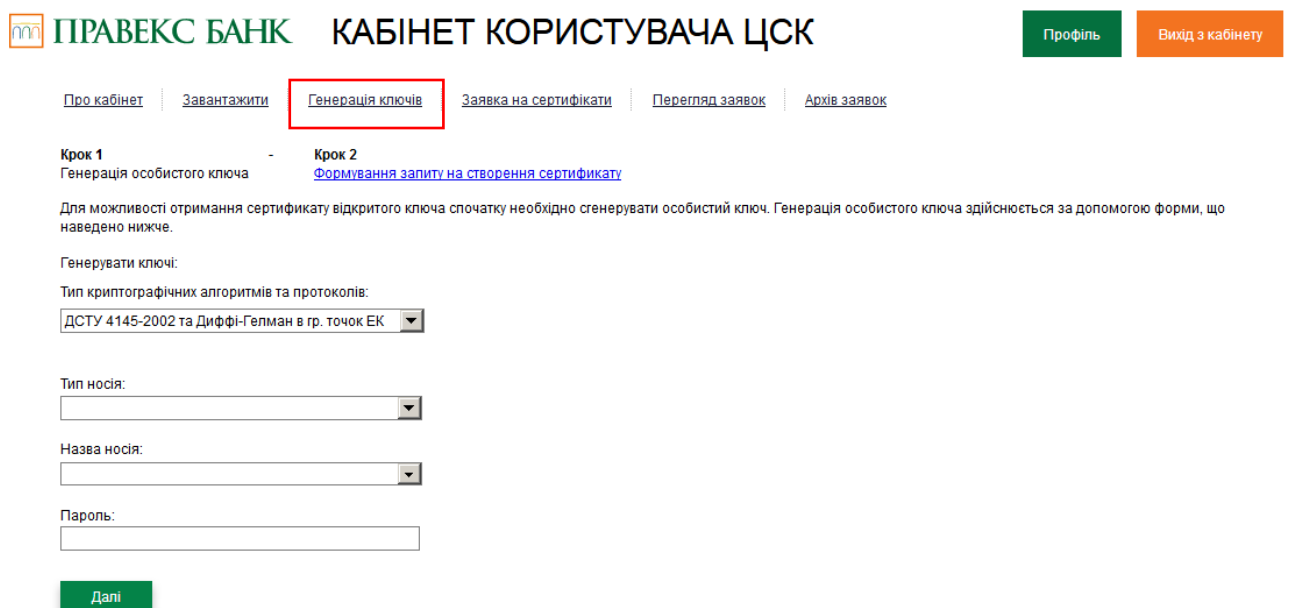


Рис. 10. Розділ «Генерація ключів»

8. На першому кроці необхідно вказати дані про носій, на якому ключ буде збережено: «Тип носія», «Назва носія», «Пароль» (см. рис. 11).

Тип носія:

Назва носія:

Пароль:

Далі

Рис. 11. Приклад заповнення даних про носій, на якому буде збережено особистий ключ

9. Після натискання кнопки **Далі** буде здійснено автоматичний перехід на сторінку формування запиту на створення сертифікату – крок 2 (см. рис. 12).

ПРАВЕКС БАНК КАБІNET КОРИСТУВАЧА ЦСК **Профіль** **Вихід з кабінету**

[Про кабінет](#) | [Завантажити](#) | [Генерація ключів](#) | [Заявка на сертифікати](#) | [Перегляд заявок](#) | [Архів заявок](#)

Подання заявки на сертифікати

Подання заявки на формування сертифікатів до ЦСК

Заявка на формування сертифікатів

Для формування сертифікатів необхідно заповнити наступну форму заявки з інформацією про заявника (користувача) та прикріпити файли із запитом на формування сертифікатів

Загальна назва *:

Адреса електронної пошти (e-mail) *:

Публікувати сертифікат:

Прізвище *:

Ім'я та по батькові *:

Місто (нас. пункт) *:

Область (region) *:

Для міст Київ або Севастополь поле 'Область (region)' не заповнюється

Адреса:

Телефон:

Організація:

Підрозділ:

Посада:

Код ДРФО *:

Запит *:

Запит *:

Повернутись **Подати**

Рис. 12. Сторінка «Подання заявки на сертифікати»

10. Вводимо дані в поля, обов'язкові для заповнення, і натискаємо **Подати**. В результаті відкриється вікно з переліком заявок, відправлених на обробку в Банк (см. рис. 13).

Подані заявки на формування сертифікатів

Список заявок на формування сертифікатів, що сформовані користувачем та вже оброблені ЦСК чи знаходяться на обробці

Всього заявок: 4



ПН	Сформовано	Заявник (загальне ім'я)	Статус обробки	Оброблено
9	11.07.2018 10:38	Тест4 Тест4	Не оброблений	
8	11.07.2018 10:37	Тест4 Тест4	Не оброблений	
7	11.07.2018 10:35	Тест4 Тест4	Не оброблений	
6	10.07.2018 18:19	Тест4 Тест4	Оброблений	10.07.2018 18:55

Видалити

Рис. 13. Розділ «Перегляд заявок»

11. Заявки можуть бути в декількох статусах:

- «Не оброблений» - на розгляді Адміністратора ЦСК;
- «Відхилений» - відхилений Адміністратором ЦСК;
- «Оброблений» - особистий ключ сертифіковано Адміністратором ЦСК.

12. Для сертифікації особистого ключа користувача необхідно роздрукувати «*Запит на додавання ключів АТ «ПРАВЕКС БАНК»*». Для цього навпроти заявки зі статусом «Не оброблений» необхідно натиснути кнопку  , далі у формі «Заявка на формування сертифікатів» (см. [рис. 14](#)) необхідно натиснути кнопку .

Заявка на формування сертифікатів

Інформація про стан обробки заявки на формування сертифікатів та інформація про користувача, який її сформував

Інформація про заявку

Сформована: 11.07.2018 15:34



Статус: Не оброблений

Інформація про користувача

Загальна назва (ім'я): Тест4 Тест4

Прізвище: Тест4

Ім'я та по батькові: Тест4

Місто (нас. пункт): Київ

Область (регіон):

Організація: Фізична особа

Підрозділ: Фізична особа

Посада: Фізична особа

Адреса:

Телефон:

Адреса електронної пошти: olga.dimpul@pravex.ua

Публікувати сертифікат: 

Код ДРФО: 5544332211

Рис. 14. Форма «Заявка на формування сертифікатів»

9. Роздрукований «Запит на додавання ключів АТ «ПРАВЕКС БАНК»» (в двох екземплярах) необхідно підписати та завірити печаткою уповноваженої особи Клієнта (см. [рис. 15](#)). *Після чого оригінали Запитів необхідно передати на обслуговуюче відділення.*

**Запит на додавання ключів АТ «ПРАВЕКС БАНК»
Замовлення на сертифікацію відкритої частини ключів ЕЦП
(Протоколу розподілу ключів)**

Прошу сертифікувати відкриту частину ключа ЕЦП (Протоколу розподілу ключів), параметри якого наведені нижче. Електронні платіжні документи, підписані за допомогою секретної частини даного ключа, вважатимуться дійсними.


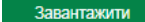
Номер запити	10
Дата створення запити	11.07.2018 15:34
Загальна назва (ім'я):	Тест4 Тест4
ПІБ власника ЕЦП	Тест4 Тест4
Населений пункт	Київ
Область	
Організація	Фізична особа
Підрозділ	Фізична особа
Посада	Фізична особа
Адреса електронної пошти	olga.dimrul@pravex.ua
Криптографічні алгоритми	ДСТУ 4145-2002 та Діффі-Гелман в гр. точок ЕК
Відкритий ключ	28 4B 73 D3 B1 40 6C 1A 7A 2E 6E D9 6B 43 68 28 FE 97 DB 7A FD 01 49 12 CE 01 E8 B7 6D 96 49 06 01
Відкритий ключ протоколу розподілу	36 DF 89 2F B5 6C 6D AC 6A 96 C6 61 4A C9 CF 60 09 F7 76 64 B4 FE EC 7E AE EA 4F 4C 5A FD 85 CE AF EE 25 48 63 F6 B5 7B 2C 33 62 35 32 06 6A C8 C4 DA 23 8B 0D 6B

Ідентифікаційний код	Серія: _____	Номер: _____
Документ, що посвідчує особу	Дата видачі: _____	
	Ким виданий: _____	
Номер договору/догоди, угоди на обслуговування в системі «PRAVEKBANK BIZ»	_____	
Особистий підпис власника ЕЦП	_____	
Достовірність приведених даних підтверджую	_____	
Керівник підприємства	_____	
Уповноважена особа банку	_____	
Дата прийому запити	_____	

Завіряється
Клієнтом

Рис. 15. Приклад Запиту на додавання ключів АТ «ПРАВЕКС БАНК»

10. Після сертифікації особистого ключа Адміністратором ЦСК, статус заявки буде змінено на «Оброблений».

11. Для подальшої роботи з особистим ключом, користувачеві необхідно зберегти сертифікат. Для цього навпроти заявки зі статусом «Оброблений» необхідно натиснути кнопку , після чого у формі «Заявка на формування сертифікатів» (см. рис. 16) необхідно натиснути кнопку . Сертифікат буде збережено в стандартне місце завантаження на ПК користувача. Для зручності використання його в роботі, рекомендуємо скопіювати сертифікат в папку з особистим ключем ЕЦП на раніше обраному носії.

Заявка на формування сертифікатів

Інформація про стан обробки заявки на формування сертифікатів та інформація про користувача, який її сформував

Інформація про заявку

Сформована: 10.07.2018 18:19

[Друкувати](#)

Статус: Оброблений

Час обробки: 2018-07-10 18:55:04

Сформовані сертифікати

Сертифікат ЕЦП:

[Завантажити](#)

[Друкувати](#)

Сертифікат протоколу розподілу: [Завантажити](#) [Друкувати](#)

Інформація про користувача

Загальна назва (ім'я): Тест4 Тест4

Прізвище: Тест4

Ім'я та по батькові: Тест4

Місто (нас. пункт): Київ

Область (регіон):

Організація: Фізична особа

Підрозділ: Фізична особа

Посада: Фізична особа

Адреса:

Телефон:

Адреса електронної пошти: olga.dimpul@pravex.ua

Публікувати сертифікат:

Код ДРФО: 5544332211

Рис.16. Завантаження сертифікату особистого ключа

РЕЗУЛЬТАТ:

- 1. Згенерований особистий ключ (файл Key-6.dat та технічний ключ Key-11.dat)*
- 2. Завантажений сертифікат особистого ключа*

Особистий ключ и сертифікат можливо використовувати для попередньої реєстрації нового клієнта або нового ключа в системі PRAVEXBANK BIZ !

Технічна підтримка здійснюється за телефоном (044) 521-02-70, а також на електронну адресу ICB-help@pravex.ua або cert_icb@pravex.ua (з 9:00 до 18:00 у робочі дні).