Шифр-CaaS. Настанова з установки та експлуатації Агенту ЄСКО (Java)

Вступ

В цьому документі описано порядок дій користувача для використання програмного комплексу «Шифр-CaaS», а саме Агенту ЄСКО (Java), його функціональні можливості та необхідні відомості для роботи з ним.

Системні вимоги

Перед початком встановлення та роботи з програмним застосуванням необхідно переконатися, що програмне та апаратне забезпечення відповідає рекомендаціям розробника. Мінімальні вимоги до апаратного забезпечення:

- Оперативна пам'ять: 512 МБ та вище;
- Процесор 1,2 ГГц;
- LAN: 10 Мбіт/с.

Мінімальні вимоги до програмного забезпечення:

- Вимоги до ОС:
 - OC Windows (Windows XP і вище, Windows Server 2008 R2 з SP1 і вище)
 - OC Linux (Ubuntu Linux 12.04 і вище, CentOS 6 і вище та ін.)
 - OC MacOS X (10.7.3 і вище)
- Браузери, що підтримуються:
 - Internet Explorer 11;
 - Mozilla Firefox;
 - Google Chrome.
- Java:
 - OC Windows XP (лише 8u111).
 - OC Windows 7/8/10 (8u152 і вище).
 - OC Linux (8u25 вище та ін.)

Підготовка робочого місця для роботи з сервісом

Встановлення середовища Java

Програмний комплекс «Агент Єдиного сервісу криптографічних операцій» реалізований мовою програмування Java, що дозволяє виконувати запуск на таких платформах:

- OC Linux.
- OC Windows.
- OC MacOS.

Детальніше про встановлення Java на вищевказані ОС є окрема Настанова користувача.

Налаштування проксі-сервера

Вступ

У випадку, **якщо доступ до мережі Інтернет з робочого місця користувача здійснюється за допомогою проксі-сервера**, то Агент «Шифр-CaaS» у вигляді Java Web Start Application використовує в своїй роботі проксісервер, який вказаний в налаштуваннях браузера, з якого був виконаний запуск програми. Якщо запуск програми проводиться за допомогою jnlp-файлу з файлової системи (локальної або мережевої), то буде використаний проксі-сервер, який вказаний в системних налаштуваннях.

Сучасні браузери підтримують три способи роботи з проксі:

- 1. Автоматичне налаштування. За допомогою DNS-сервера або DHCP-сервера вказується адреса скрипта (файлу) з налаштуваннями (детальніше тут). Цей спосіб є досить складним для пересічного користувача, тому слід звернутись до системного адміністратора або адміністратора мережі організації.
- 2. Задання скрипта з налаштуваннями проксі вручну аналогічне п.1, але адреса скрипта (файлу) вказується вручну.
- 3. Задання параметрів роботи проксі-сервера вручну.

Для вибору зазначених вище способів роботи з налаштування проксі-сервера всі сучасні браузери (IE, Firefox, Chrome, Opera, Safari) мають відповідний призначений для користувача інтерфейс.

У разі використання проксі (незалежно від способу його налаштування) для коректної роботи Агенту «Шифр-CaaS» необхідно:

- Додати в список адрес, для яких не слід використовувати проксі, адресу local.cipher.kiev.ua. Виконати можливо за допомогою відповідного призначеного для користувача інтерфейсу або через вказівку параметрів командного рядка при старті браузера. Відомості про доступні параметри командного рядка наведено в документації браузера.
- Налаштування доступу через проксі в конфігурації середовища Java.

Якщо ж цей спосіб налаштування не вирішив проблему доступу через проксі, потрібно:

• Додати в файл hosts ім'я

```
127.0.0.1 local.cipher.kiev.ua
```

У разі, якщо використовується мережа з доменом Microsoft Windows Server (2008, 2012 2016), можливе налаштування проксі для робочих станцій користувача здійснюється через налаштування групової політики. Групові політики оперують тими ж самими параметрами, які доступні користувачеві локально через призначений для користувача інтерфейс (вибір способу або параметрів вручну). В такому випадку потрібно звернутися до системного адміністратора або адміністратора мережі Вашої організації.

Нижче послідовно розглянуто варіанти налаштувань.

Браузер Firefox

Для зміни налаштувань проксі потрібно в браузері Firefox обрати розділ «Настройки», Рис. 1.





Далі послідовно обрати Налаштування: «Дополнительные->Сеть->Настроить», Рис. 2.

	Просмотр сайтов
	✓ Использовать автоматическую прокрутку
	Использовать плавную прокрутку
	При необходимости отображать сенсорную клавиатуру
	Всегда использовать клавиши курсора для навигации по страницам
	Искать текст на странице по мере его набора
	Включить управление видео «картинка в картинке» Подробнее
	Рекомендовать расширения при просмотре Подробнее
	Рекомендовать функции при просмотре Подробнее
	Параметры сети
^у асширения и темы	Настроить, как Firefox соединяется с Интернетом. Подробнее На <u>с</u> троить

Рис. 2. Додаткові мережеві налаштування браузера

У вікні «Параметры соединения» в полі «Не использовать прокси для:» потрібно вказати адресу local.cipher.kiev.ua, Рис. 3.

		Параметры соединения			
Настроика прокс	и для дост	упа в Интернет			
Б <u>е</u> з прокси					
Автоматически	определять і	настройки прокси для этой сети			
Испо <u>л</u> ьзовать с	системные на	стройки прокси			
• Ручная настрой	іка прокси				
НТТР прок <u>с</u> и	Адреса прок	ксі Вашої організації		П <u>о</u> рт	ПОРТ
	Также исп	ользовать этот прокси дл <u>я</u> FTP и HTTPS			
<u>Н</u> ТТРЅ прокси				По <u>р</u> т	0
ЕТР прокси				Порт	0
in upoke <u>n</u>					
У <u>з</u> ел SOCKS			 	Порт	0
	SOCKS 4				
	еской настро	ики прокси			
				О <u>б</u> н	ОВИТЬ
Не использовать про	окси для			О <u>б</u> н	ОВИТЬ
Не использовать про local.cipher.kiev.ua,	окси <u>д</u> ля ;127.0.0.1			О <u>б</u> н	ОВИТЬ
Не использовать про local.cipher.kiev.ua,	окси <u>д</u> ля ;127.0.0.1			О <u>б</u> но	ОВИТЬ
Не использовать про local.cipher.kiev.ua, Пример: .mozilla-rus	окси для ;127.0.0.1 :sia.org, .net.n	ız, 192.168.1.0/24		О <u>б</u> н	овить
He использовать про local.cipher.kiev.ua, Пример: .mozilla-rus Соединения с localho	окси <u>д</u> ля ;127.0.0.1 ;sia.org, .net.n ost, 127.0.0.1	ız, 192.168.1.0/24 и ::1 никогда не проксируются.		О <u>б</u> н	ОВИТЬ
Не использовать про local.cipher.kiev.ua, Пример: .mozilla-rus Соединения с localho	окси <u>д</u> ля ;127.0.0.1 ;sia.org, .net.n ost, 127.0.0.1	іг, 192.168.1.0/24 и ::1 никогда не проксируются.		О <u>б</u> н	овить
He использовать про local.cipher.kiev.ua, Пример: .mozilla-rus Соединения с localho Не запра <u>ш</u> ивать	окси <u>д</u> ля ;127.0.0.1 ;sia.org, .net.n ost, 127.0.0.1 ь аутентифик	иz, 192.168.1.0/24 и ::1 никогда не проксируются. ацию (если был сохранён пароль)		О <u>б</u> н	овить
He использовать про local.cipher.kiev.ua, Пример: .mozilla-rus Соединения с localho Не запра <u>ш</u> ивать Отправл <u>я</u> ть DNS	окси для ;127.0.0.1 sia.org, .net.n ost, 127.0.0.1 ь аутентифик S-запросы че	иz, 192.168.1.0/24 и ::1 никогда не проксируются. ацию (если был сохранён пароль) ерез прокси при использовании SOCKS 5		О <u>б</u> н	овить
Не использовать про local.cipher.kiev.ua; Пример: .mozilla-rus; Соединения с localho Не запра <u>ш</u> ивать Отправл <u>я</u> ть DNS Вк <u>л</u> ючить DNS ч	окси <u>д</u> ля ;127.0.0.1 sia.org, .net.n ost, 127.0.0.1 ь аутентифик S-запросы че через HTTPS	иz, 192.168.1.0/24 и ::1 никогда не проксируются. ацию (если был сохранён пароль) ерез прокси при использовании SOCKS 5		О <u>б</u> н	овить
Не использовать про local.cipher.kiev.ua, Пример: .mozilla-rus Соединения с localho Не запра <u>ш</u> ивать Отправл <u>я</u> ть DNS Вк <u>л</u> ючить DNS ч Ис <u>п</u> ользуемый п	окси <u>д</u> ля ;127.0.0.1 ssia.org, .net.n ost, 127.0.0.1 ь аутентифик S-запросы че через HTTPS провайдер	иz, 192.168.1.0/24 и ::1 никогда не проксируются. ацию (если был сохранён пароль) ерез прокси при использовании SOCKS 5 Cloudflare (По умолчанию)		О <u>б</u> н	овить

Рис. З. Додаткові параметри з'єднання

Браузери Google Chrome та Internet Explorer

Для зміни налаштувань проксі-сервера потрібно в браузері Google Chrome обрати розділ «Настройки», пункт «Система» та натиснути «Настройки прокси-сервера», Рис. 4.

Система	
Не отключать работающие в фоновом режиме сервисы при закрытии браузера	-
Использовать аппаратное ускорение (при наличии)	-
Открыть настройки прокси-сервера для компьютера	

Рис. 4 Налаштування браузера Google Chrome

Для браузера Internet Explorer потрібно обрати «Свойства браузера», Рис. 5.

	- ۵	60 %	¢
Печать			>
Файл			>
Масштаб (100%)			>
Безопасность			>
Открыть с помощью Microsoft Edge	CTR	L+SHIFT+E	
Добавить сайт в список приложений			
Просмотреть загрузки		CTRL+J	
Настроить надстройки			
Средства разработчика F12			
Перейти к закрепленным сайтам			
Параметры просмотра в режиме совместимости			
Свойства браузера			
О программе			

Рис. 5 Налаштування браузера Internet Explorer

Обрані налаштування для обох браузерів є системними. Тому подальший сценарій налаштувань мережі є стандартним для ОС Windows.

Системні налаштування проксі в мережі

У відкритому системному вікні «Свойства: Интернет» у вкладці «Подключение» потрібно натиснути «Настройка сети», Рис. 6.

Свойства браузе	epa				?	×
Общие	Безопасность		Кон	юнденци	альность	
Содержание	Подключения	Пр	ограммы	Доп	олнител	ьно
💨 Для у к Инто	становки подключен ернету щелкните эту	ия ко кноп	мпьютер ку.	а Уст	ановить	
Настройка ком частных сетей	мутируемого соедин 1	ения	и виртуа	льных		_
				Доб	авить	
				Добав	ить VPN	
				Уда	алить	
Щелкните кн прокси-серве	опку "Настройка" для ра для этого подклю	я пара чения	аметры я.	Ha	стройка	
Настройка пар Параметры л для подключ параметры к щелкните кн расположенн	раметров локальной (окальной сети не при ений удаленного до оммутируемого соеди опку "Настройка", ную выше.	сети именя ступа нени	ются . Для я	Настр	ойка сет	ги
	Oł	ĸ	От	мена	Приме	нить

Рис. 6. Системні налаштування мережі

В налаштуваннях параметрів локальної мережі зазначені параметри проксі-сервера, що використовується. Слід вказати опцію «Не использовать прокси-сервер для локальных адресов», Рис. 7.

Настройка параметров локальной сети Х
Автоматическая настройка Чтобы использовать установленные вручную параметры, отключите автоматическую настройку. Использовать сценарий автоматической настройки
Адрес
Прокси-сервер Использовать прокси-сервер для локальных подключений (не
применяется для коммутируемых или VPN-подключений).
Адрес: Адреса проксі Порт: ПОРТ Дополнительно
Не использовать прокси-сервер для локальных адресов
ОК Отмена

Рис. 7. Налаштування параметрів локальної мережі

Далі у наступному системному вікні потрібно натиснути в розділі «Проксі-сервер» опцію «Дополнительно» та вказати адреси – виключення у полі «Исключения», Рис. 8.

Парамет	ры прокси-	сервера	×
Сервер	ы		
	Тип	Адрес прокси-сервера	Порт
	<u>1</u> . HTTP:	Адреса проксі	: Nopt
	2. Secure:	Адреса проксі	: NOPT
	<u>3</u> . FTP:	Адреса проксі	: ПОРТ
	<u>4</u> . Socks:		:
	✓ Один пр	окси-сервер для всех протоколов	
Исключ	ения		
\$	<u>Н</u> е использ начинающи	овать прокси-сервер для адресов, ихся с:	
	127.0.0.1;	local.cipher.kiev.ua; localhost	<u>^</u>
	Адреса раз	деляются точкой с запятой (;).	~
		ОК	Отмена

Рис. 8. Параметри проксі-сервера

Середовище Java

Для запуску Java Web Start Application застосувань з урахуванням проксі-сервера у мережі – потрібно внести зміни в налаштуваннях Java, Рис. 9.



Рис. 9. Конфігурування јаva-середовища

У відкритій «Панелі управління Java» у вкладці «General» потрібно натиснути кнопку «Network Settings», Рис. 10.

🛃 Java Control Panel		_		×
General Update Java Security Advanced				
Aliant				
About				
View version information about Java Control Panel.				
			A <u>b</u> out	
Network Settings				
Network settings are used when making Internet connections. By settings in your web browser. Only advanced users should modif	/ default, Ja y these set	ava will u tings.	se the net	work
	[Netwo	rk Settings	
Temporary Internet Files		Mo	dify Interr	net conne
Files you use in Java applications are stored in a special folder for advanced users should delete files or modify these settings.	r quick exe	cution lat	er. Only	
	<u>S</u> etting	s	<u>V</u> iew	
Java in the browser is enabled.				
See the Security tab				
	OK	Cano	el	Apply

Рис. 10. Панель управління Java

Якщо в мережі використовується проксі-сервер – вказані на Рис. 11 поля будуть заповнені. Щоб додати певні ресурси у виключення – потрібно натиснути «Advanced».

Network Settings	\times
Override browser proxy settings.	
○ Use <u>b</u> rowser settings	
Use proxy server	
Address: Address: Address: Port: NOPT Advanced	
Bypass proxy server for local addresses	
O Use automatic proxy configuration script	
Script location:	
O Direct connection	
OK Cance	el

Рис. 11. Налаштування мережі

У розширених налаштуваннях проксі-серверів потрібно записати перелік адрес-виключень, тобто, доступ до яких буде здійснюватись без використання проксі, Рис. 12.

Advanced I	Network Settings			Х
Туре	Proxy Address		Port	
Http:	Адреса проксі	:	ΠΟΡΤ	
Secure:	Адреса проксі	:	ΠΟΡΤ	
Ftp:	Адреса проксі	:	ПОРТ	
Socks:		:		
E	<mark>∕</mark> <u>U</u> se same proxy server for all pr	oto	cols	
Do not 127.0.0	use proxy server for addresses beg 0.1;local.cipher.kiev.ua; localhost	jinn	ing with ^	
Use ser	micolon (;) to separate entries.		~	
	OK		Cance	

Рис. 12. Налаштування адрес-виключень

Системні налаштування hosts

Для остаточного результату потрібно відредагувати системний файл hosts, саме який відповідає у системі за взаємозв'язок між іменами хостів (сайтів, вузлів тощо) та визначення їх IP-адрес для забезпечення кінцевому користувачеві доступ до ресурсу.

Файл розташований в:

- OC Windows: C:\Windows\System32\drivers\etc\hosts.
- OC Linux: /etc/hosts.

Для внесення змін – у файлі hosts додати рядок:

```
127.0.0.1 local.cipher.kiev.ua
```

Зберегти зміни в документі.

Слід зауважити, що перед рядком, який необхідно додати немає необхідності додавати знак «решітки» - #, оскільки це є знак коментаря.

Робота із захищеними носіями

Агент Єдиного сервісу криптографічних операцій підтримує роботу із захищеними носіями.

Захищений апаратний носій у пасивному режимі – підтримує збереження особистого ключа у захищеному ключовому контейнері. Доступ до ключа здійснюється за допомогою інтерфейсу PKCS#11.

До таких носіїв відносяться:

• Author Secure Token-337 Series, Author Smart Card-337 Series (обов'язкове розміщення бібліотеки у залежності від розрядності Java).

- SafeNet|Gemalto|Thales eToken.
- IIT Алмаз-1К (обов'язкове встановлення ПЗ: EKAlmaz1CInstall.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- IIT Кристал-1 (обов'язкове встановлення ПЗ: EKeyCrystal1Install.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- Avest AvestKey.
- Efit Key.

Захищений апаратний носій у активному режимі – самостійно здійснює створення ЕП за допомогою особистого ключа у захищеному контейнері. Виконання операції з ЕП здійснюється за допомогою PKCS#11 інтерфейсу.

До таких носіїв відносяться:

- Author Secure Token-337 Series, Author Smart Card-337 Series (обов'язкове розміщення бібліотеки у залежності від розрядності Java).
- Plasticard TEllipse 3/4 (обов'язкове встановлення ПЗ та розміщення бібліотеки у залежності від розрядності Java).
- SafeNet|Gemalto|Thales eToken.
- IIT Алмаз-1К (обов'язкове встановлення ПЗ: EKAlmaz1CInstall.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- IIT Кристал-1 (обов'язкове встановлення ПЗ: EKeyCrystal1Install.exe та EUInstall.exe, також необхідно перед генерацією ключа ініціалізувати носій у PKCS#11 сумісному режимі).
- Avest AvestKey.
- Efit Key.

Операційна система Windows

Застосування захищеного носія Avtor Secure Token - 337

Для роботи із захищеними носіями Avtor Secure Token у Агенті Єдиного сервісу криптографічних операцій, необхідні додаткові бібліотеки **Av337CryptokiD.dll** (x32/x64 у залежності від розрядності Вашої операційної системи та розрядності Java). Є кілька варіантів її розміщення.

Варіант 1-й - розмістити вручну бібліотеку у папку Java, каталог bin.

Додатковий .dll файл можна отримати у розробника захищеного носія, компанії Автор, або завантажити за посиланням, вказаним нижче та розмістити за шляхом:

• Для ОС Windows x86 та Java RE x32. Бібліотеку слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: *C:\Program Files (x86)\Java\jre1.8.0_271\bin.*

Завантажити архів можна за посиланням - Avtor_Windows_x32.zip

 Для ОС Windows x64 та для Java RE x64. Бібліотеку слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: *C:\Program Files\Java\jre1.8.0_271\bin.*

Завантажити архів можна за посиланням - Avtor_Windows_x64.zip

Варіант 2-й - задати змінну середовища РАТН.

Як це зробити, необхідно перейти у "Пуск" - "Панель управління" - "Система" - обрати розділ "Додаткові параметри системи" - у вікні, що відкриється на вкладці "Додатково" - натиснути кнопку "Змінні середовища", Рис. 13.

Свойства системы					×
Имя компьют	гера		Оборудова	ние	
Дополнительно	Защита сис	темы	Удаленн	ный доступ	
Необходимо иметь пр перечисленных парам	оава администр иетров.	атора для	изменения	большинств	a
Быстродействие					
Визуальные эффект виртуальной памяти	ты, использован I	ние процен	ссора, опера	тивной и	
			<u>П</u> ара	метры	
— Профили пользоват Параметры рабочег	елей о стола, относя	щиеся ко	входу в сист П <u>а</u> ра	ему метры	
Загрузка и восстано Загрузка и восстано	овление овление систем	ы, <mark>отлад</mark> о	чная информ Пара	ация метр <u>ы</u>	
			Переменны	е среды	
	ОК		Отмена	При <u>м</u> ени	ть

Рис. 13. Властивості системи

У розділі "Змінні середовища" натиснути двічі на полі "Path", Рис. 14. У відкритому вікні натиснути кнопку "Створити", прописати "C:\Program Files (x86)\Av337CryptokiD.dll" та натиснути Ок, Рис. 15. Далі, у цей же каталог розмістити необхідну бібліотеку, у залежності від розрядності Java, Рис. 16.

Переменная	Значение
JAVA_OPTIONS	-Djava.net.preferlPv4Stack=true
MOZ_PLUGIN_PATH	C:\PROGRAM FILES (X86)\FOXIT SOFTWARE\FOXIT READER\plugins\
OneDrive	C:\Users\Admin\OneDrive
Path	C:\Users\Admin\AppData\Local\Microsoft\WindowsApps;C:\Users
TEMP	C:\Users\Admin\AppData\Local\Temp
ТМР	C:\Users\Admin\AppData\Local\Temp
	Создать Изменить Удадить
истемные переменные	
истемные переменные Переменная	Значение
истемные переменные Переменная ComSpec	Значение C:\WINDOWS\system32\cmd.exe
астемные переменные Переменная ComSpec DriverData	Значение C:\WINDOWS\system32\cmd.exe C:\Windows\System32\DriverData
истемные переменные Переменная ComSpec DriverData NUMBER_OF_PROCESSORS	Значение C:\WINDOWS\system32\cmd.exe C:\Windows\System32\DriverS\DriverData 4
астемные переменные Переменная ComSpec DriverData NUMBER_OF_PROCESSORS OS	Значение C:\WINDOWS\system32\cmd.exe C:\Windows\System32\DriverS\DriverData 4 Windows_NT
истемные переменные Переменная ComSpec DriverData NUMBER_OF_PROCESSORS OS Path	Значение C:\WINDOWS\system32\cmd.exe C:\Windows\System32\Drivers\DriverData 4 Windows_NT C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Pro
истемные переменные Переменная ComSpec DriverData NUMBER_OF_PROCESSORS OS Path PATHEXT	Значение C:\WINDOWS\system32\cmd.exe C:\Windows\System32\Drivers\DriverData 4 Windows_NT C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Pro .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC
истемные переменные Переменная ComSpec DriverData NUMBER_OF_PROCESSORS OS Path PATHEXT PROCESSOR ARCHITECTURE	Значение C:\WINDOWS\system32\cmd.exe C:\Windows\System32\Drivers\DriverData 4 Windows_NT C:\Program Files (x86)\Common Files\Oracle\Java\javapath;C:\Pro .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC AMD64

Рис. 14. Змінні середовища

C:\Program Files (x86)\Common Files\Oracle\Java\javanath	Cozast
C\ProgramData\Oracle\Java\iavapath	Создать
%SystemRoot%\system32	Изменить
%SystemRoot%	
%SystemRoot%\System32\Wbem	Обзор
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\	
%SYSTEMROOT%\System32\OpenSSH\	Удалить
C:\Program Files (x86)\Armorino Cryptoki Module	
C:\Program Files (x86)\Armorino Cryptoki Module	
C:\Program Files (x86)\Armorino Cryptoki Module	Вверх
C:\Program Files\Git\cmd	
C:\Program Files (x86)\Av337CryptokiD.dll	Вниз
	Изменить текс
	VISMENTIB TEKC

Рис. 15. Додавання змінної середовища

📙 🛃 📙 🖛 Prog	ram Files (x86)						- 0	\times	
Файл Главная	Поделиться Вид							^ ()
Закрепить на панели К быстрого доступа	опировать Вставить Вставить ярлык	Переместить Копировать Уда	х — алить Переименовать	<mark>І</mark> Новая папка	Свойства свойства	рыть ▼ енить нал	Выделить все Снять выделение Обратить выделен	ние	
	Буфер обмена	Упорядочи	ть	Создать	Открыть		Выделить		
← → • ↑ <mark> </mark> ;	 Этот компьютер > Локальный диск (С:) 	> Program Files (x86) ⇒			~ Ū	Поиск:	Program Files (x86)	<i>م</i>	
	Имя	Дата изменения	Тип	Размер				-	^
🖈 Быстрый доступ	active and a second participation of the second participat	15.09.2018 10:31	Параметры конф	1 КБ					
a OneDrive	Av337CryptokiD.dll	18.06.2013 17:37	Расширение при	390 KE					
🔲 Этот компьютер		27.07.2018 12:42	Папка с файлами						
		10.09.2018 11:54	Папка с файлами						
💣 Сеть		15.09.2018 10:33	Папка с файлами						
	<u> </u>								1

Рис. 16. Розміщення змінної середовища

Для продовження роботи необхідно повернутися до «Клієнту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.
- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».
- Вказати РІМ-код до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Застосування захищеного носія AvestKey

Для роботи із захищеними носіями AvestKey у Агенті Єдиного сервісу криптографічних операцій, необхідні додаткові бібліотеки **avcryptokinxt.dll** (x32/x64 у залежності від розрядності Вашої операційної системи та розрядності Java). Є кілька варіантів її розміщення.

Додатковий .dll файл можна отримати у розробника захищеного носія, компанії Автор, або завантажити за посиланням, вказаним нижче та розмістити за шляхом:

 Для ОС Windows x86 та Java RE x32. Бібліотеку слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: *C:\Program Files (x86)\Java\jre1.8.0_271\bin.*

Завантажити архів можна за посиланням - Avest-Win32.zip

 Для ОС Windows x64 та для Java RE x64. Бібліотеку слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: *C:\Program Files\Java\jre1.8.0_271\bin.*

Завантажити архів можна за посиланням - Avest-Win64.zip

Для продовження роботи необхідно повернутися до «Агенту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.
- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».
- Вказати **PIN-код** до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Застосування захищеного носія "EFIT KEY"

Необхідно завантажити за посиланням та встановити програмне забезпечення для роботи з захищеними носіями EFIT KEY.

Для продовження роботи необхідно повернутися до «Клієнту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.
- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».
- Вказати РІМ-код до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Застосування електронного ключа "Алмаз-1К"

Необхідно завантажити за посиланням та встановити програмне забезпечення для роботи з електронним ключем «Алмаз-1К», так як дане застосування допомагає керувати електронним ключем.

А також встановити програмне забезпечення "IIT Користувач ЦСК" з сайту розробника, яке доступне за посиланням.

Слід зауважити, що носій має бути ініціалізований у PKCS#11-сумісному режимі за допомогою програмного забезпечення "Алмаз-1К". А вже ключі на даному захищеному носії повинні бути згенеровані у режимі сумісності з PKCS#11 (якщо генерувати ключа за допомогою "IIT Користувач ЦСК", то це має бути обраний рядок "Алмаз-1К, PKCS#11, віртуальний". Це необхідно для роботи носія у Агенті Єдиного сервісу криптографічних операцій, якщо виникають помилки при роботі з носієм чи ключами, то слід звернутися до вашого КНЕДП/АЦСК та здійснити перегенерацію ключа у режимі сумісності з PKCS#11 для роботи в активному режимі.

Для продовження роботи необхідно повернутися до «Клієнту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.
- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».

- Вказати **PIN-код** до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Застосування електронного ключа "Кристал-1"

Відеоінструкція по роботі із застосуванням електронного ключа "Кристал-1" доступна за посиланням.

Для роботи з електронним ключем Кристал-1 у Агенті Єдиного сервісу криптографічних операцій, виконати наступні дії:

- завантажити за посиланням та встановити програмне забезпечення для роботи з електронним ключем Кристал-1, так як дане застосування допомагає керувати електронним ключем;
- встановити програмне забезпечення "IIT Користувач ЦСК" з сайту розробника, яке доступне за посиланням.
- завантажити додаткові .dll файли розробника електронного ключа Кристал-1, за посиланнями, вказаними нижче, та розмістити за шляхом у залежності від розрядності Вашої операційної системи та розрядності Java:
- для ОС Windows x86 та Java RE x32. Бібліотеки слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: *C:\Program Files (x86)\Java\jre1.8.0_271\bin.*

Завантажити архів можна за посиланням – EkeyCrystal1x86.zip

 для ОС Windows x64 та для Java RE x64. Бібліотеки слід розмістити у директорії, де інстальоване середовище Java в каталог bin, скоріше за все шлях буде таким: *C:\Program Files\Java\jre1.8.0_271\bin.*

Завантажити архів можна за посиланням - EkeyCrystal1x64.zip

• запустити програмне забезпечення "IIT Користувач ЦСК", у розділі Особистий ключ обрати пункт Зчитати, Рис. 17;



Рис. 17. Стартове вікно ПЗ "ІІТ Користувач ЦСК"

• обрати носій, ввести пароль та зчитати, Рис. 18;

Зчитування особистого ключа	
Встановіть носій ключової інформації чи підклю модуль та вкажіть параметри	чіть криптографічний
 гнучкий диск з'ємний диск оптичний диск е.ключ Aladdin e Token R2 е.ключ Aladdin e Token PRO е.ключ Aladdin e Token PRO е.ключ Aladdin e Token PRO (PKCS#11) смарт-карта BIFIT Integra 1.0 е.ключ BIFIT iToken е.ключ IIT Алмаз-1К е.ключ IIT Алмаз-1К (носій) е.ключ IIT Кристал-1 40413 е.ключ IIT Кристал-1 (носій) закордонний біометричний паспорт (ел. паспорт) файлова система (каталоги системи) файлова система (каталоги користувача) ID-карта громадянина (БЕН) криптомод. IIT Гряда-61 (PKCS#11) 	 Інформація про носій: Тип: е.ключ ІІТ Кристал-1 Назва: 40413 Перезаписуємий, потребує автентифікації, тільки повна очистка, електронний ключ, апаратний ГВП Апаратний криптомодуль Поновити Ключ у файлі (на диску)
	Зчитати Відміна

Рис. 18. Діалогове вікно зчитування особистого ключа

 далі з'явиться помилка про пошук власного сертифіката (Рис. 19) з пропозицією його завантаження з СМРсервера ЦСК, Рис. 20;





Рис. 20. Повідомлення з пропозицією завантаження сертифіката з СМР-сервера ЦСК

• їх необхідно імпортувати (Рис. 22, Рис. 23, Рис. 24), попередньо завантаживши з сайту КНЕДП, Рис. 21;

	*		*	
ГОЛОВНА СТОРІНКА	НОРМАТИВНА БАЗА	КОНТАКТИ	ВАКАНСІЇ	
Новини	*			
Регламент роботи	Пошук серти	ифікатів та	СПИСКИ	
Отримання електронних довірчих послуг, у тому числі для програмних РРО	ыдкликаних	сертифіка		
Дистанційне формування сертифікатів для програмних РРО (юр.особи)	Пошук сертифікаті	в Сертифікати	Надавача СВС	
Підпис даних	Власник	Видавник	PH	
Перевірка підписаних даних	Державна податкова служба	*		
Повторне (дистанційне) формування сертифікатів за епектронним запитом	України. "ОТРИМАНО (2019)-2"	кнедп ідд - дпс	36	2
Пошук сертифікатів та СВС	Державна податкова служба України.	кнедп ідд - дпс	35	đ
Скасування, блокування, поновлення сертифікатів	(2019)-1"			
Системи, акі підтримують	СМР - 2 сервер КНЕДП - ІДД ДПС	кнедп - ідд дпс	34 🔺	1
використання сертифікатів Кваліфікованого налавача ЕЛІ	СМР - 1 сервер КНЕДП - ІДД ДПС	КНЕДП - ІДД ДПС	33	đ
ІДД ДПС	ОСЅР-сервер КНЕДП - ІДД ДПС	кнедп - ідд дпс	32	2
	ТЅР-сервер КНЕДІ - ІДД ДПС	Центральний засвідчувальний орган	31	d
	кнедп - ідд дпс	Центральний засвідчувальний	30	đ

Рис. 21. Список сертифікатів Надавача на саиті КНЕДІ І ІДД-ДІ ІС

dР-сервера ЦСК	n	шук за власникож
UCK	Cepithush Horkep	T.
	ИР-сервера ЦСК ЦСК	MP-cepsepo LICK Cepifrosh novep

Рис. 22. Вікно Сертифікати

ООО № Локальный диск (D:) ► Download ▼ 4+ Поиск: Download Упорядочить ▼ Новая папка III ■ III ■ № Недавние места Имя Дата изменения Ти № Рабочий стол □ сыси провос этомо 1000000000000000000000000000000000000	р n ртификат
Упорядочить • Новая папка III • П У Недавние места • Имая • Дата изменения Ти Рабочий стол	п ртификат
Эдине места Имая Дата изменения Ти Дата изменения Ца Дата изменения Ти Дата изм На позвения Ти Дата изменения Ти Дат	n ртификат
📃 Рабочий стол	ртификат
CMP1-IDD0P5-250919 16.01.2021 12:54 Ce	
СМР2-1000Р5-250919 16.01.2021 12:34 Се	ртификат
🛃 Видео	
💽 Документы	
изображения	
🚽 Музыка 🗉	
Домашняя группа	
🖳 Компьютер	
🏭 Локальный дися	
👝 Локальный дися	
👝 Локальный дися	
* *	
Имя файла: Файли з сертифікатами (*.«	er; •
Открыть Отме	на

Рис. 23. Процесс імпортування сертифікатів

ертифікати			×
Сертифікати Кількість: 2, тип власни	іків: 🏕 користувачі ЦСК 🛛 🔻	Пошук з	за власником:
Власник 🔻	ЦСК	Серійний номер	Чинний до
	КНЕДП - ІДД ДПС КНЕДП - ІДД ДПС	58E2D9E7F900307B040000005EF03000DF6A8 58E2D9E7F900307B040000005EF03000E06A8E	15.01.2023 00 15.01.2023 00
•	m		4
Імпортувати			ОК

Рис. 24. Результат імпортування сертифікатів

 Повторно зчитуємо ключ, де автоматично починається завантаження сертифікатів: власника ключа, СМР, OCSP, TSP – серверів, КНЕДП, ЦЗО до каталогу C:\My Certificates and CRLs 13\, Рис. 25.

Завантажені сертифікати	
Завантажені з СМР-серв Ана СМР-сервер КНЕДП - СМР-сервер КНЕДП - ОСЅР-сервер КНЕДП - КНЕДП - ІДД ДПС ТЅР-сервер КНЕДП - І, ОСЅР-сервер КНЕДП - І, ОСЅР-сервер КНЕДП - І, ОСЅР-сервер Централ ТЅР-сервер АЦСК ІДД Центральний засвідчу	зера ЦСК сертифікати: атолійович ІДД ДПС ІДД ДПС - ІДД ДПС ДД ДПС дальний засвідчувальний орган ДФС /вальний орган атолійович не сховище сертифікатів?
	Да <u>Н</u> ет

Рис. 25. Повідомлення про результат завантаження сертифікатів

Для продовження роботи необхідно повернутися до «Клієнту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.
- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».
- Вказати **PIN-код** до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Застосування захищеного носія Avtor Secure Token - 337

Додатковий .dylib файл можна отримати у розробника захищеного носія, компанії Автор, або завантажити за посиланням, вказаним нижче та розмістити за шляхом:

• Бібліотеку слід розмістити у директорії, де інстальоване середовище Java, скоріше за все шлях буде таким: /Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/.

Завантажити архів можна за посиланням - Avtor_MacOS_x64.zip

Для продовження роботи необхідно повернутися до «Клієнту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.
- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».
- Вказати РІМ-код до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Застосування захищеного носія AvestKey

Необхідно завантажити архів з драйвером за посиланням - Avest-MacOS.zip

Після його розархівування та встановлення, яка розміщується за шляхом **/usr/local/lib** буде розміщена бібліотека libavcryptokinxt.dylib, дану бібліотеку необхідно скопіювати до папки за шляхом: **/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/.**

Окремо встановлюється утіліта для управління avtoksvc, яка розміщується за шляхом: /usr/local/bin.

Для перевірки працездатності необхідно:

- Вставити захищений носій AvestKey в USB-порт ПК.
- Відкрити термінал на ПК та ввести команду:

avtoksvc info

• Утіліта повинна відобразити інформацію про захищений носій AvestKey.

Для продовження роботи необхідно повернутися до «Клієнту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.
- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».
- Вказати **PIN-код** до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Застосування електронного ключа "Алмаз-1К"

Для роботи з електронним ключем Алмаз-1К у Агенті Єдиного сервісу криптографічних операцій, виконати наступні дії:

- встановити програмне забезпечення "IIT Користувач ЦСК" з сайту розробника, яке доступне за посиланням.
- завантажити додаткові .dylib файли розробника електронного ключа Алмаз-1К можна за посиланням та розмістити за шляхом /Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/.

Для продовження роботи необхідно повернутися до «Клієнту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.

- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».
- Вказати РІМ-код до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Застосування електронного ключа "Кристал-1"

Для роботи з електронним ключем Кристал-1 у Агенті Єдиного сервісу криптографічних операцій, виконати наступні дії:

- встановити програмне забезпечення "IIT Користувач ЦСК" з сайту розробника, яке доступне за посиланням.
- завантажити додаткові .dylib файли розробника електронного ключа Кристал-1 можна за посиланням та розмістити за шляхом /Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/bin/.

Для продовження роботи необхідно повернутися до «Клієнту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.
- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».
- Вказати РІМ-код до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Операційна система Linux

Операційна система Linux Ubuntu (Mint, Debian)

Застосування захищеного носія Avtor Secure Token - 337

Перш за все необхідно інсталювати в ОС середовище Java, процес встановлення наведено у відповідному розділі Встановлення Java. Операційна система Linux Ubuntu.

Пристрої Avtor Secure Token 337 та Avtor SC Reader 371 працюють через стандартні інтерфейси CCID та бібліотеки РКСS#11. Перед інсталяцією РКСS#11 бібліотеки в ОС повинні бути встановленні наступні пакети:

- pcscd (версії 1.4 чи вище)
- libccid (версії вище 1.0)
- libpcsclite1 (версії 1.4 чи вище)
- pcsc_tools (опціонально, для перевірки зв'язку з токеном)

1. Інсталяція оновлень та пакетів залежностей.

Інсталювати доступі пакети можна з консолі, почергово виконуючи команди:

```
sudo apt-get update
sudo apt-get install libpcsclite1
sudo apt-get install libccid
sudo apt-get install pcscd
sudo apt-get install pcsc-tools
```

Примітка. Необхідна наявність доступу до мережі Інтернет, для завантаження пакетів.

Перевірити наявність пакету у системі можна за допомогою команди:

```
dpkg -s <имя пакета>
```

Також, для перевірки наявності пакетів можна використовувати файловий менеджмер Synaptic. Встановити такий менеджмер можна, виконавши наступну команду

```
sudo apt-get install synaptic
```

Synaptic Package Manager						
Reload Mark All Upgrad	des	Apply Properties	ick filter	Q Search		
All	S	Package	Installed Version	Latest Version	Description	
libccid		libacr38u		1.7.11-1	PC/SC driver for t	
libpcsclite1		libacsccid1		1.0.2-3	PC/SC driver for /	
pcscd		libasedrive-serial		3.7-2	PC/SC driver for t	
		libasedrive-usb		3.7-2	PC/SC driver for t	
		libccid	1.4.5-1	1.4.5-1	PC/SC driver for l $^{\lor}$	
		libgempc410		1.0.6-4	PC/SC driver for t	
	1					
	PC/SC driver for USB CCID smart card readers					
	Get Screenshot Get Changelog					
	This library provides a PC/SC IFD handler implementation for the USB smart					
Sections	card	d drivers compliant to the CCID	protocol.		Ξ	
Status	This	package is needed to commu	nicate with the CCID	smartcard readers	through	
	the	PC/SC Lite resource manager (pcscd).			
Origin)	-, <u>-</u>	/-			
Custom Filters	For	an exhaustive list of supported	d reader see			
Search Results	http	o://pcsclite.alioth.debian.org/s	section.html			
Architecture) <u>.</u>	· · · ·				
8 packages listed, 1411 install	ed, 0 b	roken. 0 to install/upgrade, 0 t	oremove			

2. Встановлення PCSC#11

Після інсталяції залежностей, необхідно розмістити РКСЅ#11 бібліотеку, дані міститься у пакетах:

- для Java з розрядністю x86 Avtor_Linux_x32.zip (розмістити за шляхом /usr/lib/pkcs11/libav337p11d.so)
- для Java з розрядністю x64 Avtor_Linux_x64.zip (розмістити за шляхом /usr/lib/libav337p11d.so)

3. Перевірка підключеного пристрою

Для того щоб, перевірити коректність роботи пристрою в ОС необхідно, після інсталяції пакету бібліотек (необхідної розрядності), підключити носій до ПК та в консолі ввести команди:

• запуску pcscd-демона

sudo systemctl start pcscd

• додати його до автозапуску ОС

sudo systemctl enable pcscd

• перегляду інформації про носій

pcsc_scan

У консолі отримаємо інформацію про пристрій:

```
😑 🔲 user@testubuntu: ~
user@testubuntu:~$ pcsc_scan
PC/SC device scanner
V 1.4.18 (c) 2001-2011, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.7.4
Mon May 20 11:50:05 2013
Reader 0: Avtor SecureToken 00 00
  Card state:
  ATR: 3B 98 18 81 31 FE 43 30 41 56 54 00 00 00 07 F9
ATR: 3B 98 18 81 31 FE 43 30 41 56 54 00 00 00 07 F9
+ TS = 3B --> Direct Convention
  T0 = 98, Y(1): 1001, K: 8 (historical bytes)
  TA(1) = 18 --> Fi=372, Di=12, 31 cycles/ETU
 TD(1) = 81 --> Y(i+1) = 1000, Protocol T = 1
 TD(2) = 31 --> Y(i+1) = 0011, Protocol T = 1
  TA(3) = FE --> IFSC: 254
  TB(3) = 43 --> Block Waiting Integer: 4 - Character Waiting Integer:
```

Після завершення перегляду інформації про пристрій, натискаємо клавіші Ctrl+C.

Також можна перевірити коректність роботи пристрою через саму бібліотеку pkcs11, командами:

```
sudo apt install opensc
pkcs11-tool -module /usr/lib/pkcs11/libav337p11d.so -L (для x86)
pkcs11-tool -module /usr/lib/libav337p11d.so -L (для x64)
```

```
🔵 🔲 user@testubuntu: ~
  token manuf: AVTOR Ltd.
  token model:
                CC-337 RSA DSTU
 token flags: rng, login required, PIN initialized, token initialized, other
flags=0x200
 serial num : 141e40ba160d0000
user@testubuntu:~$ pkcs11-tool --module=/usr/lib/pkcs11/libav337p11d.so -L
Available slots:
Slot 0 (0x0): Avtor SecureToken 00 00
  token label:
               CC337
  token manuf:
              AVTOR Ltd.
 token model:
                CC-337 RSA DSTU
 token flags: rng, login required, PIN initialized, token initialized, other
flags=0x200
 serial num : 141e40ba160d0000
user@testubuntu:~$ pkcs11-tool --module=/usr/lib/pkcs11/libav337p11d.so -L
Available slots:
Slot 0 (0x0): Avtor SecureToken 00 00
 token label: CC337
  token manuf: AVTOR Ltd.
  token model: CC-337 RSA DSTU
 token flags: rng, login required, PIN initialized, token initialized, other
flags=0x200
  serial num : 141e40ba160d0000
user@testubuntu:~$
```

У випадку, якщо необхідна робота зі старими моделями захищеного носія, необхідно додати іd пристрою у Info.plist

У каталозі зі встановленням рссс (у даному випадку, вказано відносний шлях):

drivers/ifd-ccid.bundle/Contents/Info.plist

Для продовження роботи, необхідно повернутися до «Клієнту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний чи Пасивний режим.
- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».
- Вказати РІМ-код до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Якщо захищений носій не виявлено, зверніться до:

- Постачальника захищених носіїв.
- Розробника захищених носіїв.
- Розробника «Агенту Єдиного сервісу криптографічних операцій».

Подальша робота «Агенту Єдиного сервісу криптографічних операцій» з РКСЅ#11 пристроями можлива тільки після повного усунення питань, пов'язаних з правильною роботою захищених носіїв.

Після встановлення програмного забезпечення для роботи із захищеними носіями, слід переконатися, що операційна система виявила їх та відображає в «Диспетчере устройств». Для перевірки необхідно перейти «Пуск» -> «Панель управления» -> «Диспетчер устройств» -> «SmartCard Reader».

Операційна система Oracle Linux

Застосування захищеного носія Avtor Secure Token – 337

Перш за все необхідно інсталювати в ОС середовище Java, процес встановлення наведено у відповідному розділі Встановлення Java. Операційна система Oracle Linux.

1.Встановлення пакетів залежностей

Пристрої Avtor Secure Token 337/338 та Avtor SC Reader 371 працюють через стандартні інтерфейси CCID та бібліотеки PKCS#11. Перед інсталяцією PKCS#11 бібліотеки в OC повинні бути встановленні наступні пакети:

- pcsc-lite
- pcsc_tools (опціонально, для перевірки зв'язку з токеном)

Примітка. Необхідна наявність доступу до мережі Інтернет для завантаження пакетів.

Для інсталювання пакетів необхідно запустити програму «Термінал» (Ctrl+Alt+T) та в командному рядку терміналу ввести команду:

sudo yum install pcsc-lite

2. Для завантаження бібліотеки для носія Avtor Secure Token – 337/338 необхідно перейти в браузер та завантажити відповідні файли з ресурсу:

- для Java з розрядністю x86 Avtor Linux x32.zip (розмістити за шляхом /usr/lib/pkcs11/libav337p11d.so)
- для Java з розрядністю x64 Avtor_Linux_x64.zip (розмістити за шляхом /usr/lib/libav337p11d.so)

Після цього зберегти файл на ПК

Вы собираетесь	открыть:	
🗎 Avtor_Linux	κ_x64.zip	
являющийся из https://de Как Firefox след	я: Архив ZIP (229 КБ) ocs.cipher.kiev.ua цует обработать этот файл?	
О <u>т</u> крыть в	Менеджер архивов (по умолчанию)	~
01	файл	
 Сохранить 		

Та розархівувати в каталог Downloads/ Linux_x64

	домашняя папка Downloads	Linux_x64 ▶	Q := ≡ ×
 ⊘ Недавние ★ Избранные ☆ Домашняя папка ○ Documents ↓ Downloads ↓ Music 	Avtor_Linux_x64.zip	Linux_x64	
© Pictures ► Videos © Kopзина • VBox_GAs_7 ▲			
+ Другие места			Выделен объект «Linux_x64» (внутри 1 объект)

Перейти в програму «Термінал» (Ctrl+Alt+T) та в командному рядку ввести команду для розміщення його за шляхом /usr/lib/libav337p11d.so (на прикладі Java x64):

sudo cp /home/xxx/Downloads/Linux_x64/libav337p11d.so /usr/lib/

Але замість:

/home/xxx/Downloads/Linux_x64/ – вказати розміщення раніше збереженого файла libav337p11d.so.

Для продовження роботи, необхідно повернутися до «Клієнту Єдиного сервісу криптографічних операцій» та заповнити всі поля:

- Завантажити Агент ЄСКО.
- Вказати АЦСК/КНЕДП.
- Вказати Активний режим.
- Обрати захищений носій, натиснувши на кнопку «Вибрати токен».
- Вказати *PIN-код* до носія.
- Натиснути кнопку Розпочати роботу з ключем.

Якщо захищений носій не виявлено, зверніться до:

- Постачальника захищених носіїв.
- Розробника захищених носіїв.
- Розробника «Агенту Єдиного сервісу криптографічних операцій».

Подальша робота «Агенту Єдиного сервісу криптографічних операцій» з РКСЅ#11 пристроями можлива тільки після повного усунення питань, пов'язаних з правильною роботою захищених носіїв.

Після встановлення програмного забезпечення для роботи із захищеними носіями, слід переконатися, що операційна система виявила їх та відображає в «Диспетчере устройств». Для перевірки необхідно перейти «Пуск» -> «Панель управления» -> «Диспетчер устройств» -> «SmartCard Reader».

Робота з Клієнтом Єдиного сервісу криптографічних операцій

Запуск Агента ЄСКО

У веб-браузері перейти за посиланням - https://cryptocenter.cipher.kiev.ua/ до Клієнту Єдиного сервісу криптографічних операцій.

Покрокова інструкція та ознайомлення з інтерфейсом програмного комплексу:

• Стартове вікно Клієнту Єдиного сервісу криптографічних операцій у веб-браузері показано на Рис. 29.

Клієнт єдиного сервісу криптографічних операцій			Агент ЄСКО запустити	ЄСКО підключено	
				JKP RUS ENG	G
Особистий ключ Перевірити ЕП					
Параметри сесії	Параметри ключа				
Період активації ключа, хв:	КНЕДП/АЦСК:		Тестовий ЦСК Сайф	ep 🔻	
	Тип ключа:		[Файл на диску]	T	
	Шлях до контейнеру:			Вибрати файл	
	Пароль:			۲	
	Розпочати роботу з кл	ючем	Очистити форму		

Рис. 29. Стартове вікно ЄСКО

• Наступним кроком слід відкрити Агент ЄСКО, натиснувши у правому верхньому куті під написом Агент ЄСКО кнопку «запустити», Рис. 30.

Клієнт єдиного сервісу криптографічних		Агент ЄСКО	ECKO)
операцій		запустити	підключено	
ТОВ Сайфер БІС				
			JKP RUS EN	١G
Особистий ключ Перевірити ЕГ	I			
Параметри сесії	Параметри ключа			
Період активації ключа, хв:	КНЕДП/АЦСК:	Тестовий ЦСК Сай	фер 🔻	

Тип ключа:

Пароль:

Шлях до контейнеру:

15

Рис. 30. Запуск Агенту ЄСКО

Розпочати роботу з ключем

 Далі відкривається вікно Агенту Єдиного сервісу криптографічних операцій, Це означає що Агент запущено, все працює коректно, його слід згорнути та повернутися до веб-браузера, Рис. 31.

۳

۲

Вибрати файл

[Файл на диску]

Очистити форму

🔋 Агент єдиного сервісу крип	тографічних операцій		- [×
С Аге Про	ент єдиного се програму	рвісу криптографічн	ИХ ОГ Україн	тера нська	цій •
Дії		Стан			
Перезавантажити серві Очистити журнал подій Завершити роботу серв	c ica				
Журнал подій 11:50:33.770 - [INFO] - Серві 11:50:34.666 - [INFO] - REST 11:50:35.481 - [INFO] - 1.22.1	ic операцій успішно запу Web-сервис успішно заг I.1166	/щений. лущений.			

Рис. 31. Вікно «Агенту Єдиного сервісу криптографічних операцій»

• У веб-сторінці одразу помітні зміни. Статус Агенту ЄСКО змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 32.

Клієнт єдиного сервісу криптографічних		Агент ЄСКО	€C)	
операцій			підключено		підключ	ено
ТОВ Сайфер БІС						
				У	KP RUS	ENG
Особистий ключ Перевірити ЕП Параметри сесії	Генерація ключів Параметри ключа					
Період активації ключа, хв:	КНЕДП/АЦСК:		Тестовий ЦСК Сай	фер		¥
	Тип ключа:		[Файл на диску]		¥

Розпочати роботу з ключем

Рис. 32. Стартове вікно Клієнту ЄСКО

• На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа,

Вибрати файл

Очистити форму

۲

- за замовчуванням 15 хв. • На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати:
- АЦСК/КНЕДП, у якому було отримано ключ;

Перелік АЦСК/КНЕДП, які підтримуються «Агентом Єдиного сервісу криптографічних операцій»:

Шлях до контейнеру:

Пароль:

- 1. АЦСК/КНЕДП Національного банку України;
- 2. КНЕДП ІДД ДПС;
- 3. КНЕДП "ДІЯ";
- 4. АЦСК/КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- 5. АЦСК/КНЕДП АТ «КБ «Приватбанк»;
- 6. АЦСК/КНЕДП ПАТ «УкрСиббанк»;
- 7. АЦСК/КНЕДП «Masterkey» ТОВ «Арт-мастер»;
- 8. АЦСК/КНЕДП Збройних Сил;
- 9. АЦСК/КНЕДП Міністерства внутрішніх справ України;
- 10. КНЕДП Державної прикордонної служби;
- 11. АЦСК/КНЕДП Укрзалізниці;
- 12. КНЕДП "АЦСК ринку електричної енергії";
- 13. КНЕДП ДП «Українські спеціальні системи»;
- 14. АЦСК/КНЕДП Генеральної прокуратури України;
- 15. АЦСК/КНЕДП АТ «Ощадбанк»;
- 16. КНЕДП Казначейства (з ключами, які отримано після 31.01.2020);
- 17. КНЕДП ТОВ "ДепозитСайн".
- 18. КНЕДП АТ "КРЕДІ АГРІКОЛЬ БАНК".
- 19. АЦСК ПАТ "Альфа-Банк".

• Тип ключа:

- 1. файл на диску;
- 2. РКСЅ#11 пристрої активний режим;
- 3. РКСЅ#11 пристрої пасивний режим;
- 4. МКМ Шифр-HSM.
- 5. Хмарний сервіс Depositsign.
- Шлях до контейнеру;
- Пароль до ключа чи PIN до захищеного носія, Рис. 33.

Клієнт єдиного сервісу криптографічних			Агент ЄСКО	ЄСКО
			підключено	підключено
тов сайфер ыс				JKP RUS ENG
Особистий ключ Перевірити ЕП	Генерація ключів			
Параметри сесії	Параметри ключа			
Період активації ключа, хв:	КНЕДП/АЦСК:		Тестовий ЦСК Сайф	ep 🔻
15	Тип ключа:		[Файл на диску]	T
	Шлях до контейнеру:	C:\Users\Ad	min\Desktop\tomat	Вибрати файл
	Пароль:	•••••		۲
	Розпочати роботу з кл	ючем	Очистити форму	,

Рис. 33. Заповнення розділу «Параметри ключа»

 Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу створюється криптографічний контекст, де відкривається робоча область, в якій стають доступні всі функції та операції Клієнту ЄСКО, Рис. 34.



Клієнт єдиного сервісу криптографічних операцій

ТОВ Сайфер БІС

00:14:11

Особистий ключ Перевірити ЕП	Створити ЕП Зашифр	увати Розшифрувати Генерація ключів
Дії	Загальна інформація	про ключ ЕП
Загальна інформація	Повне ім'я	Чумак Торчин Помідор
Сертифікат ключа підпису	Серійний номер сертифікату	DA76B92DE30F63F8
Сортифікат каюца шифрурацца	Початок дії	11.02.2019, 10:35:46 GMT+2
Сертифікат ключа шифрування	Закінчення дії	11.02.2020, 00:00:00 GMT+2
Завершити роботу з ключем	Посилений	Hi
	Стартовий	Hi

Загальна інформація про ключ шифрування

Повне ім'я	Чумак Торчин Помідор
Серійний номер сертифікату	2C52794E9D4EA6A
Початок дії	11.02.2019, 10:35:45 GMT+2
Закінчення дії	11.02.2020, 00:00:00 GMT+2
Посилений	Hi
Стартовий	Hi

Агент ЄСКО

підключено

ECKO

підключено

RUS

ENG

УКР

Рис. 34. Робоча область Клієнту ЄСКО

Службові функції та опції ЄСКО

Після завантаження даних ключового контейнеру у вікні «Клієнту Єдиного сервісу криптографічних операцій» з'являються такі поля та відповідні опції, Рис. 35:

1.Вкладка «Особистий ключ», яка містить кнопки:

- «Загальна інформація» коротка інформація про ключів.
- «Сертифікат ключа ЕП» повна інформація про сертифікат ключа ЕП.
- «Сертифікат ключа шифрування» повна інформація про сертифікат ключа шифрування.
- «Завершити роботу з ключем» завершується сесія.

2.Вкладка «Перевірити ЕП».

На даній вкладці є можливість здійснити перевірку ЕП, доступні такі розділи:

- «Параметри перевірки ЕП» включає в себе:
 - Можна вказати Тип ЕП (Вбудований чи Відкріплений).
 - Режим перевірки електронної позначки часу для ЕП (Ігнорувати електронну позначку часу чи перевіряти електронну позначку часу, якщо вона присутня чи повертати помилку, якщо вона відсутня).
 - Режим перевірки електронної позначки часу для даних (Ігнорувати електронну позначку часу чи перевіряти електронну позначку часу, якщо вона присутня чи повертати помилку, якщо вона відсутня).
 - Розширення ЕП.
 - Генерація QR.
- «Файл» включає в себе 2 поля, якщо:

- Тип ЕП Відкріплений: файл для перевірки (файл на який було створено підпис) та файл з підписом (файл, який містить підпис).
- Тип ЕП Вбудований: файл з підписом (файл який містить підпис).
- «Текстові дані» включає в себе 2 поля, якщо:
 - Кодування UTF-16LE та UTF-8.
 - Тип ЕП Відкріплений: текстові дані для перевірки (текст на який було створено підпис) та підпис у кодуванні Base64 (текст, який містить підпис).
 - Тип ЕП Вбудований: підпис у кодуванні Base64 (текст, який містить підпис) та дані з електронного підпису (виведення даних без підпису).

	Клієнт єдиного сервісу криптографічних	Агент ЄСКО		f	еско	
	операцій	підключено		підя	ключе	ено
	ТОВ Сайфер БІС					
00:14:11			7	/KP	RUS	ENG

Особистий ключ	Перевірити ЕП	Створити ЕП Заши	ифрувати Розшифрувати Генерація ключів
Дії		Загальна інформац	ація про ключ ЕП
Загальна ін	формація	Повне ім'я	Чумак Торчин Помідор
Сертифікат кл	юча підпису	Серійний номер сертифікату	DA76B92DE30F63F8
Consultivos voco		Початок дії	11.02.2019, 10:35:46 GMT+2
Сертифікат ключ	ча шифрування	Закінчення дії	11.02.2020, 00:00:00 GMT+2
Завершити роб	оту з ключем	Посилений	Hi
		Стартовий	Hi

Загальна інформація про ключ шифрування	Загальна	а інформаці	я про ключ	шифрування
---	----------	-------------	------------	------------

Повне ім'я	Чумак Торчин Помідор
Серійний номер сертифікату	2C52794E9D4EA6A
Початок дії	11.02.2019, 10:35:45 GMT+2
Закінчення дії	11.02.2020, 00:00:00 GMT+2
Посилений	Hi
Стартовий	Hi

Рис. 35. Робоча область Клієнту ЄСКО

3.Вкладка «Створити ЕП».

На даній вкладці є можливість здійснити створення ЕП, доступні такі розділи:

- «Параметри створення ЕП» включає в себе:
 - Тип ЕП (Вбудований чи Відкріплений), за необхідності вказати позначку «Додати підпис до вже існуючого» (таким чином, можуть підписувати один файл кілька осіб).
 - Формат ЕП (CAdES-BES чи CAdES-X Long).
 - Генерація QR.
 - «Файл». Включає в себе 2 поля:
 - Файл/Файли для підпису (файл, який необхідно підписати).
 - Додатковий опис (назва файлу підпису).
 - «Текстові дані». Включає в себе поля:
 - Кодування UTF-16LE та UTF-8.
 - Текстові дані для підпису (текст, який необхідно підписати).
 - Додатковий опис (назва тексу підпису).

• Підпис у кодуванні Вазе64.

4.Вкладка «Зашифрувати».

На даній вкладці є можливість здійснити зашифрування даних, доступні такі розділи:

- «Параметри зашифрування». Слід визначитися з параметром, який слід додати при зашифруванні:
 - Сертифікат відправника та сертифікати видавців.
 - Сертифікат відправника.
 - Не додавати сертифікат відправника та сертифікати видавців.
 - «Сертифікат отримувача». Поле, де слід вказати сертифікат отримувача зашифрованих даних.
- «Файл». Поле, де слід вказати файл/файли для зашифрування.
- «Текстові дані»:
 - Кодування UTF-16LE та UTF-8.
 - «Текст для зашифрування». Поле, де слід вказати текст для зашифрування.
 - «Зашифровані дані у кодування Base64». Виведення зашифрованої інформації.

5.Вкладка «Розшифрувати».

На даній вкладці є можливість здійснити розшифрування даних, доступний такий розділ:

- «Файл». Слід вказати файл, який необхідно розшифрувати.
- «Текстові дані»:
 - Кодування UTF-16LE та UTF-8.
 - «Зашифровані дані у кодування Base64». Поле, де слід вказати зашифрований текст.
 - «Розшифрований текст». Виведення розшифрованої інформації.

6.Вкладка «Генерація ключів».

На даній вкладці є можливість здійснити генерацію ключів попередньо обравши відповідний профіль генерації ключів.

Профілі генерації ключів:

- Співробітник банку.
- Технолог.
- Посадова особа клієнта iFOBS.
- Клієнт iFOBS (ФОП).
- Користувач ЦСК.
- Організація.

Генерація ключів відбувається як файл на диску так і на захищений носій.

- 1. Час до кінця сесії відлік у реальному часі до закінчення сесії (знаходиться у лівому верхньому куті).
- 2. Статус роботи програмного комплексу «Агенту ЄСКО» знаходиться у правій верхній частині вікна. За допомогою «Агент ЄСКО» є можливість працювати не лише із файлами на диску, але із захищеними носіями.

7. Можливі статуси «Агенту ЄСКО»:

- «Запустити». Для початку роботи із «Агентом ЄСКО», необхідно натиснути дану кнопку та для подальшої роботи слід відкрити іншу інструкцію «Агент Єдиного сервісу криптографічних операцій. Настанова з установки та експлуатації».
- «Підключено». Працює у звичайному режимі.
- «Відключено». Слід звернутися до системного адміністратора.

8.Статус роботи програмного комплексу «ЄСКО» - знаходиться у правій верхній частині вікна.

Можливі статуси ЄСКО:

- «Підключено». Працює у звичайному режимі.
- «Відключено». Слід звернутися до системного адміністратора.

9.3міна мови - знаходиться у правій верхній частині вікна можна змінити мову веб-інтерфейсу ЄСКО. Доступні мови: українська, російська та англійська.

Основна форма «Агенту Єдиного сервісу криптографічних операцій» містить такі поля та відповідні опції, Рис. 36.

員 Агент єдиного сервіс	у криптографічних операцій		_	×		
	Агент єдиного се Про програму	ервісу криптографіч	НИХ ОПЕРа Українська	ацій •		
Дії		Стан				
Перезавантажити Очистити журнал г Завершити роботу	сервіс подій сервіса	E				
Журнал подій 11:56:44.733 - [INFO] - Запит на встановлення налаштувань сесії SessionUuid:145a9ce5-cbdc-4595-8c2^ 11:56:44.733 - [INFO] - Значення параметру "cald" встановено в "testCipherCa" SessionUuid:145a9ce5- 11:56:44.734 - [INFO] - Запит на встановлення налаштувань сесії виконано SessionUuid:145a9ce5-cbdc 11:56:44.774 - [INFO] - Дані ключового контейнера успішно завантажені SessionUuid:145a9ce5-cbdc-4 11:56:44.794 - [INFO] - Запит на перевірку ключового контейнера SessionUuid:145a9ce5-cbdc-4 11:56:46.893 - [INFO] - Запит на видалення сесії ClientURI:[https://ccs-dev.cipher.kiev.ua] 11:56:46.893 - [INFO] - Видалена сесія SessionUuid:145a9ce5-cbdc-4595-8c21-80a2d60ecf7e;ClientURI:[I						
Рис	с. 36. Агент Єдиного серві	су криптографічних операцій	 			

Даний розділ містить:

- назву Програмного комплексу.
- гіперпосилання «Про програму», яке відкриває нове вікно з інформацією про розробників, версію продукту, Рис. 37.
- Випадаючий список зі зміною мови, доступні мови: Українська, Англійська, Російська.

月 Про програму		Х
	Агент єдиного сервісу криптографічних операцій 1.0.3 Build #48 Copyright (c) 2006-2019 ООО Сайфер БИС	
	Агент єдиного сервісу криптографічних операцій криптографічної системи захисту інформації "Шифр X.509"	
	https://www.cipher.kiev.ua	
	ОК	

Рис. 37. Вікно «Про програму»

а.Розділ «Дії» містить гіперпосилання:

- «Перезавантажити сервіс».
- «Очистити журнал подій».
- «Завершити роботу сервісу».

b.Розділ «Стан» містить інформацію про стан роботи сервісу, що він працює.

с.Розділ «Журнал подій» містить повну інформацію про дії, які виконуються у веб-браузері, під час роботи з Агентом ЄСКО.

Вибір ключа ЕП – файл

Відеоінструкція знаходиться за посиланням.

Стартове вікно Клієнту Єдиного сервісу криптографічних операцій у веб-браузері показано на Рис. 38.

Клієнт єдиного се	Агент ЄСКО	ECKO	
🥑 операцій	запустити	підключенс	
ТОВ Сайфер БІС			JKP RUS EI
собистий ключ Перевірити ЕП			
Іараметри сесії	Параметри ключа		
lepioд активації ключа, хв:	КНЕДП/АЦСК:	Тестовий ЦСК Сайф	ep 🔻
15	Тип ключа:	[Файл на диску]	•
	Шлях до контейнеру:		Вибрати файл
	Пароль:		۲
	Розпочати роботу з ключем	Очистити форму	

Рис. 38. Стартове вікно ЄСКО

Наступним кроком слід відкрити Агент ЄСКО, натиснувши у правому верхньому куті під написом Агент ЄСКО кнопку «запустити», Рис. 39.

Клієнт єдиного сери операцій		вісу криптографічних		Агент ЄСКО		ECKO	
				запустити	підключено		чено
	ТОВ Сайфер БІС						
					У	KP RUS	ENG
Особис	гий ключ Перевірити EП						
Параме	етри сесії	Параметри ключа					
Період	активації ключа, хв:						

ріод активації ключа, хв:	КНЕДП/АЦСК:	Тестовий ЦСК Сайфер	
5	Тип ключа:	[Файл на диску]	
	Шлях до контейнеру:	Вибрати файл	
	Пароль:	۲	
	Розпочати роботу з кли	ючем Очистити форму	

Рис. 39. Запуск Агенту ЄСКО

Далі відкривається вікно Агенту Єдиного сервісу криптографічних операцій, його слід згорнути та повернутися до веб-браузера, Рис. 40.

🗐 Агент єдиного сервісу криптографічних операцій —				\times
Q	Агент єдиного се Про програму	ервісу криптографічн	НИХ ОПЕРа Українська	ацій •
Дії		Стан		
Перезавантажити Очистити журнал Завершити роботу	сервіс подій / сервіса			
Журнал подій 11:50:33.770 - [INFO] - 11:50:34.666 - [INFO] - 11:50:35.481 - [INFO] -	- Сервіс операцій успішно зап - REST Web-сервис успішно за - 1.22.1.1166	ущений. пущений.		

Рис. 40. Агент Єдиного сервісу криптографічних операцій

У веб-сторінці одразу помітні зміни. Статус Агенту ЄСКО змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 41.
Клієнт єдиного сервісу криптографічних			Агент ЄСКО		ECKC)
операцій			підключено		підключ	ено
ТОВ Сайфер БІС						
				2	/KP RUS	ENG
Особистий ключ Перевірити Е	П Генерація ключів					
Параметри сесії	Параметри ключа					
Період активації ключа, хв:	КНЕДП/АЦСК:	-	Тестовий ЦСК Сай	фер		¥
15	Тип ключа:		[Файл на диску]		¥

Розпочати роботу з ключем

Рис. 41. Стартове вікно Клієнту ЄСКО

• На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа,

Вибрати файл

Очистити форму

۲

Шлях до контейнеру:

Пароль:

Перелік АЦСК/КНЕДП, які підтримуються «Агентом Єдиного сервісу криптографічних операцій»:

На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати:

1. АЦСК/КНЕДП Національного банку України;

• АЦСК/КНЕДП, у якому було отримано ключ;

- 2. КНЕДП ІДД ДПС;
- 3. КНЕДП "ДІЯ";
- 4. АЦСК/КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- 5. АЦСК/КНЕДП АТ «КБ «Приватбанк»;
- 6. АЦСК/КНЕДП ПАТ «УкрСиббанк»;
- 7. АЦСК/КНЕДП «Masterkey» ТОВ «Арт-мастер»;
- 8. АЦСК/КНЕДП Збройних Сил;

за замовчуванням 15 хв.

- 9. АЦСК/КНЕДП Міністерства внутрішніх справ України;
- 10. КНЕДП Державної прикордонної служби;
- 11. АЦСК/КНЕДП Укрзалізниці;
- 12. КНЕДП "АЦСК ринку електричної енергії";
- 13. КНЕДП ДП «Українські спеціальні системи»;
- 14. АЦСК/КНЕДП Генеральної прокуратури України;
- 15. АЦСК/КНЕДП АТ «Ощадбанк»;
- 16. КНЕДП Казначейства (з ключами, які отримано після 31.01.2020);
- 17. КНЕДП ТОВ "ДепозитСайн".
- 18. КНЕДП АТ "КРЕДІ АГРІКОЛЬ БАНК".
- 19. АЦСК ПАТ "Альфа-Банк".

• Тип ключа:

- 1. файл на диску;
- 2. РКСЅ#11 пристрої активний режим;
- 3. РКСЅ#11 пристрої пасивний режим;
- 4. МКМ Шифр-HSM.
- 5. Хмарний сервіс Depositsign.
- Шлях до контейнеру;
- Пароль до ключа, Рис. 42.

Клієнт єдиного сервісу криптографічних			Агент ЄСКО	ECKO	
операціи	операцій			підключен	но
ТОВ Сайфер БІС					
				JKP RUS	ENG
Особистий ключ Перевірити ЕП	Генерація ключів				
Параметри сесії	Параметри ключа				
Період активації ключа, хв:	КНЕДП/АЦСК:		Тестовий ЦСК Сайф	ep	•
15	Тип ключа:		[Файл на диску]		•
	Шлях до контейнеру:	C:\Users\Ad	min\Desktop\tomat	Вибрати файл	n
	Пароль:			۲	>
	Розпочати роботу з кл	ючем	Очистити форму		

Рис. 42. Заповнення розділу «Параметри ключа»

Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу створюється криптографічний контекст, де відкривається робоча область, де стають доступні всі функції та операції в Клієнті ЄСКО, Рис. 43.



ТОВ Сайфер БІС

00:14:11

Особистий ключ	Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів	
Дії		Загальна інс	формація про клі	оч ЕП		
Загальна інформація		Повне ім'я Ч		Чумак Торчин Помідор		
Сертифікат ключа підпису		Серійний номер сертифікату		DA76B92DE30F63F8		
Consulting		Початок ді	ї 11	11.02.2019, 10:35:46 GMT+2		
Сертифікат ключ	а шифрування	Закінчення	Закінчення дії 11.0		MT+2	
Завершити роботу з ключем		Посилений	i Hi	Hi		
		Стартовий	H			

Загальна інформація про ключ шифрування

Повне ім'я	Чумак Торчин Помідор
Серійний номер сертифікату	2C52794E9D4EA6A
Початок дії	11.02.2019, 10:35:45 GMT+2
Закінчення дії	11.02.2020, 00:00:00 GMT+2
Посилений	Hi
Стартовий	Hi

Агент ЄСКО

підключено

єско

підключено

RUS

УКР

ENG

Рис. 43. Робоча область Клієнту ЄСКО

Вибір ключа ЕП – захищений носій

Відеоінструкція знаходиться за посиланням.

Стартове вікно Клієнта Єдиного сервісу криптографічних операцій у веб-браузері показано на Рис. 44.

	Клієнт єдиного сервісу криптографічних		Агент ЄСКО		€CKO)		
	опера	цій			запустити		пі	дключ	ено
	ТОВ Сайфе	ер БІС							
						2	УКР	RUS	ENG
Особис	тий ключ	Перевірити ЕП							
Параме	етри сесії		Параметри ключа						
Період	активації к	люча, хв:	КНЕДП/АЦСК:	-	Тестовий ЦСК Сай	фер			•

Тип ключа:

Пароль:

Шлях до контейнеру:

Ŧ

۲

Вибрати файл

[Файл на диску]

Очистити форму

15

Рис. 44. Стартове вікно ЄСКО

Розпочати роботу з ключем

Наступним кроком слід відкрити Агент ЄСКО, натиснувши у правому верхньому куті під написом Агент ЄСКО кнопку «запустити», Рис. 45.

Клієнт єдиного сервісу криптографічних	Агент ЄСКО		ECKO		
операцій	запустити		підклю	чено	
ТОВ Сайфер БІС					
		У	RUS	ENG	

Особистий ключ Перевірити ЕП		
Параметри сесії	Параметри ключа	
Період активації ключа, хв:	КНЕДП/АЦСК:	Тестовий ЦСК Сайфер 🔻
15	Тип ключа:	[Файл на диску]
	Шлях до контейнеру:	Вибрати файл
	Пароль:	۲
	Розпочати роботу з кл	ючем Очистити форму



Далі відкривається вікно Агенту Єдиного сервісу криптографічних операцій, його слід згорнути та повернутися до веб-браузера, Рис. 46.

🗐 Агент єдиного сервісу криптографічних операцій		_		×
Агент єдиного се Про програму	ервісу криптографічн	IИХ ОПЄ Українсь	рац ка	цій •
Дії	Стан			
Перезавантажити сервіс Очистити журнал подій Завершити роботу сервіса				
Журнал подій 11:50:33.770 - [INFO] - Сервіс операцій успішно зап 11:50:34.666 - [INFO] - REST Web-сервис успішно за 11:50:35.481 - [INFO] - 1.22.1.1166	ущений. пущений.			

Рис. 46. Агент Єдиного сервісу криптографічних операцій

У веб-сторінці одразу помітні зміни. Статус Агенту ЄСКО змінено на «підключено» та став доступний для змін пункт «Тип ключа», Рис. 47.

Клієнт єдиного сервісу криптографічних операцій			Агент ЄСКО	ECKO
			підключено	підключено
ТОВ Сайфер БІС				
				JKP RUS ENG
Особистий ключ Перевірити ЕП	Генерація ключів			
Параметри сесії	Параметри ключа			
Період активації ключа, хв:	КНЕДП/АЦСК:		Тестовий ЦСК Сай	фер 🔻
15	Тип ключа:		[Файл на диску]	•
	Шлях до контейнеру:			Вибрати файл
	Пароль:			۲
	Розпочати роботу з кл	ючем	Очистити форм	У

Рис. 47. Стартове вікно Клієнту ЄСКО

- На вкладці «Особистий ключ» у розділі «Параметри сесії» слід вказати у хвилинах період активації ключа, за замовчуванням 15 хв.
- На вкладці «Особистий ключ» у розділі «Параметри ключа» слід вказати:
- АЦСК/КНЕДП, у якому було отримано ключ;

Перелік АЦСК/КНЕДП, які підтримуються «Агентом Єдиного сервісу криптографічних операцій»:

- 1. АЦСК/КНЕДП Національного банку України;
- 2. КНЕДП ІДД ДПС;
- 3. КНЕДП "ДІЯ";
- 4. АЦСК/КНЕДП ТОВ «Центр сертифікації ключів «Україна»;
- 5. АЦСК/КНЕДП АТ «КБ «Приватбанк»;
- 6. АЦСК/КНЕДП ПАТ «УкрСиббанк»;
- 7. АЦСК/КНЕДП «Masterkey» ТОВ «Арт-мастер»;
- 8. АЦСК/КНЕДП Збройних Сил;
- 9. АЦСК/КНЕДП Міністерства внутрішніх справ України;
- 10. КНЕДП Державної прикордонної служби;
- 11. АЦСК/КНЕДП Укрзалізниці;
- 12. КНЕДП "АЦСК ринку електричної енергії";
- 13. КНЕДП ДП «Українські спеціальні системи»;
- 14. АЦСК/КНЕДП Генеральної прокуратури України;
- 15. АЦСК/КНЕДП АТ «Ощадбанк»;
- 16. КНЕДП Казначейства (з ключами, які отримано після 31.01.2020);
- 17. КНЕДП ТОВ "ДепозитСайн".
- 18. КНЕДП АТ "КРЕДІ АГРІКОЛЬ БАНК".
- 19. АЦСК ПАТ "Альфа-Банк".
- Тип ключа:
- 1. файл на диску;
- 2. РКСЅ#11 пристрої активний режим;
- 3. PKCS#11 пристрої пасивний режим;
- 4. МКМ Шифр-HSM;
- 5. Хмарний сервіс Depositsign.
- Шлях до контейнеру, Рис. 48;

[PKCS#1	11 пристрої] – активни	й режим
@. Avt	or SecureToken 0	
Ок	Відміна	

Рис. 48. Вказівка «Шлях до контейнера»

• PIN до захищеного носія, Рис. 49.

Клієнт єдиного сервісу криптографічних			Агент ЄСКО	ЄСКО	
операци			підключено	підключено	
ТОВ Сайфер БІС					
				JKP RUS ENG	
Особистий ключ Перевірити ЕП Г	енерація ключів				
Параметри сесії	Параметри ключа				
Період активації ключа, хв:	КНЕДП/АЦСК:	Тестовий ЦСК Сайфер			
15	Тип ключа:	[PKCS#1	1 пристрої] – актив	вний режим 🔻	
	Шлях до контейнеру:	@. Avtor Sec	cureToken 0	Вибрати токен	



Розпочати роботу з ключем

.....

Очистити форму

۲

Пароль:

Після заповнення всіх полів, слід натиснути кнопку «Розпочати роботу з ключем» та одразу створюється криптографічний контекст, де відкривається робоча область, де стають доступні всі функції та операції в Клієнті ЄСКО, Рис. 50.

Ð

Клієнт єдиного сервісу криптографічних операцій

ТОВ Сайфер БІС

00:14:11

Особистий ключ	Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів	
Дії		Загальна інфо	рмація про клю	эч ЕП		
Загальна інформація		Повне ім'я		Чумак Торчин Помідор		
Сертифікат ключа підпису		Серійний номер сертифікату		DA76B92DE30F63F8		
Contuctivat valous		Початок дії	11	11.02.2019, 10:35:46 GMT+2		
Сертифікат ключа	Сертифікат ключа шифрування		Закінчення дії 11.02.2020, 00:00:00 GMT+2		MT+2	
Завершити роботу з ключем		Посилений	Посилений Ні			
		Стартовий	Hi			

Загальна інформація про ключ шифрування

Повне ім'я	Чумак Торчин Помідор
Серійний номер сертифікату	2C52794E9D4EA6A
Початок дії	11.02.2019, 10:35:45 GMT+2
Закінчення дії	11.02.2020, 00:00:00 GMT+2
Посилений	Hi
Стартовий	Hi

Агент ЄСКО

підключено

ECKO

підключено

RUS

ENG

УКР

Рис. 50. Робоча область Клієнту ЄСКО

Створення ЕП

Вкладка «Створення ЕП» містить розділи: Параметри створення ЕП, Текстові дані та Файл, Рис. 51.

Розділ «Параметри створення ЕП», який у свою чергу включає:

1.Поле «Тип ЕП», яке містить:

- Вбудований;
- Відкріплений.

2.Поле «Формат ЕП«, яке містить:

- CAdES-BES. Або «Базова ЕП» використовується для автентифікації підписанта та перевірки цілісності електронного документа в період чинності сертифіката відкритого ключа (сертифікат). Формат «Базовий ЕП» не надає можливості встановити дійсність підпису у випадку, якщо ЕП перевіряється після закінчення строку чинності сертифіката або скасування сертифіката після формування ЕП;
- CAdES-X Long. Або «ЕП з повним набором даних перевірки» можливість встановлення дійсності ЕП у довгостроковому періоді (після закінчення строку чинності сертифікату).

3.Поле «Додати підпис до вже існуючого» (накладається підпис на файл, на який вже попередньо накладено ЕП).

4.Поле «Генерація QR».

5.Розділ «Файл», який у свою чергу включає:

- Файл для підпису (перетягнути файл(и) з Провідника на область «Перетягніть файл(и) чи огляд» або обрати необхідний файл(файли) для підпису, натиснувши на цю область);
- Додатковий опис (назва файлу з яким буде зберігатися файл з підписом, заповнюється автоматично, але можна змінити назву);
- Кнопка «Створити ЕП» (здійснює накладання ЕП на файл, який завантажено);
- Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

6.Розділ «Текстові дані», який у свою чергу включає:

- Кодування UTF-16LE та UTF-8.
- Текстові дані для підпису (у поле слід внести текстові дані);
- Додатковий опис (опис до текстових даних);
- Кнопка «Створити ЕП» (здійснює накладання ЕП на текстові дані, який завантажено);
- Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.
- Підпис у кодування Base64 (виведення підписаних текстових даних).



ТОВ Сайфер БІС

00:38:42

Агент ЕСКО 🚯	ECKO 🔮
підключено	підключе

9 но

ENG

RUS

УКР

Особистий ключ Перевірити ЕП	Створити ЕП Зашифрувати Розшифрувати Генерація ключів
Параметри створення ЕП	✓ Файл
🗸 Тип підпису	
О Вбудований	перетягніть файл(и) чи
🔍 Відкріплений	
🗸 Формат підпису	
🖲 Базовий (CAdES-BES)	
 О 3 повними даними для перевірки (CAdES-X Long) 	
🗆 Додати підпис до вже існуючого	
🛛 Генерація QR	Створити ЕП Очистити форму
	✓ Текстові дані
	Кодування: 🖲 UTF-16LE O UTF-8
	Текстові дані для підпису:
	Скопіювати
	Додатковий опис:
	Створити ЕП Очистити форму
	Підпис у кодуванні Base64:
	Скопіювати

Рис. 51. Вкладка «Створення ЕП»

Створення ЕП за типом «Вбудований» на файл

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Вбудований» та Формат ЕП (CAdES-BES чи CAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 52. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об'єм всіх файлів не повинен перевищувати 100Мб.

Клієнт єдиного сері	Клієнт єдиного сервісу криптографічних операцій					ECKO 🤇	•
ТОВ Сайфер БІС					ено	підключено	
00:37:42						ykp rus	ENG
Особистий ключ Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація	а ключів		
Параметри створення ЕП	🗸 Файл	I					
✔ Тип підпису	202012	09_135149.jpg		Û	Перетя	сніть файл(и) ч	и
Вбудований	log-tes	log-test.txt			nepen	огляд	
○ Відкріплений	log-tes	log-test.txt.png		ŵ			
🗸 Формат підпису							
○ Базовий (CAdES-BES)							
 З повними даними для перевірки (CAdES-X Long) 							
🗆 Додати підпис до вже існуючого							
🗆 Генерація QR	C	створити ЕП	Очистити ф	орму			
	▲ Текс	гові дані					

Рис. 52. Створення ЕП

Після натискання на кнопку «Створити ЕП» з'являється вікно із запитом дозволу на використання ЕП, для того, щоб дати дозвіл необхідно натиснути «ОК», Рис. 53. Якщо натиснути кнопку «Відміна», підпис не буде створено та операція буде завершена.

Після натискання кнопки «ОК» з'являється вікно про успішне створення електронного підпису, Рис. 54.

月 Агент єдиного сервісу криптографічних операцій	x
Pecypc [https://ccs-dev.cipher.kiev.ua] запитує дозвіл на використання ЕП в кількості 1 раз(у,ів).	?
Інформація про дані, що підписуються:	
20201209_135149.jpg	
Щоб дати дозвіл на використання особистого ключа натисніть кнопку "Ok". У разі відмови натисніть кнопку "Відміна".	
ОК Відг	иіна

Рис. 53. Дозвіл на використання ЕП



Рис. 54. Повідомлення про створення електронного підпису

Далі зберігається файл з підписом за допомогою кнопки «стрілки вниз», яка з'являється біля кожного файлу на який накладено підпис, Рис. 55.

💼 Клієнт єдиного се	Клієнт єдиного сервісу криптографічних операцій				CKO 🚯	ECKO 🚯		
ТОВ Сайфер БІС				підклю	учено	підключено		
00:36:34						JKP RUS ENG		
Особистий ключ Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерац	ія ключів			
Параметри створення ЕП	🗸 Фай.	л						
🗸 Тип підпису	20201	209_135149.jpg		ô 🕹	Dapat			
🔍 Вбудований	log-te:	log-test.txt		ŵ 🕹	Tieper	огляд		
○ Відкріплений	log-te	st.txt.png		ŵ 🕹				
🗙 Формат підпису	5	1.5						
○ Базовий (CAdES-BES)								
З повними даними для перевірки (CAdES-X Long)								
🗆 Додати підпис до вже існуючого								
🗆 Генерація QR		Створити ЕП	Очистити ф	форму				
	▲ Текс	тові дані						

Рис. 55. Збереження підпису у файл

За необхідності вказуємо шлях для збереження та очищаємо форму, Рис. 56.

💿 Сохранение							×
$\leftarrow \rightarrow \checkmark \land$	» Этот компьютер »	Загрузки > New			~ Ū	Поиск: New	م
Упорядочить 🔻	Новая папка						EE • ?
🖈 Быстрый досту	Имя п	^	Дата изменения	Тип	Размер		
OneDrive			нет элементов, удовлетв	оряющих условия	м поиска.		
💻 Этот компьюте	P						
🥔 Сеть							
Имя файла:	ECKO.txt.p7s						~
Тип файла:	PKCS #7 Signature (*.p7s	.)					~
 Скрыть папки 						Сохранить	Отмена

Рис. 56. Збереження файлу

Створення ЕП за типом «Відкріплений» на файл

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Відкріплений» та Формат ЕП (CAdES-BES чи CAdES-X Long), обирається файл для підпису, натискаємо кнопку «Створити ЕП», Рис. 57. За необхідності можна змінити файл. За необхідності можна видалити файл натиснувши відповідну кнопку та додати ще, але слід зауважити, що максимальний об'єм всіх файлів не повинен перевищувати 100Мб.

📻 Клієнт єдиного се	Клієнт єдиного сервісу криптографічних операцій						ECKO 🕄			
ТОВ Сайфер БІС				підключе	ено	підключен	o			
00:35:24						УКР RUS	ENG			
Особистий ключ Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація	ключів					
Параметри створення ЕП	🗸 Файл	η								
🗸 Тип підпису	202012	209_135149.jpg		Ŵ	Перета	гніть файл(и) ци	٦			
○ Вбудований	log-tes	st.txt		ŵ	огляд					
Відкріплений	log-tes	st.txt.png		Û						
🗙 Формат підпису										
🖲 Базовий (CAdES-BES)										
 З повними даними для перевірки (CAdES-X Long) 										
🗆 Додати підпис до вже існуючого										
🗆 Генерація QR	(Створити ЕП	Очистити ф	орму						
	▲ Текс	тові дані								

Рис. 57. Створення ЕП

Після натискання на кнопку «Створити ЕП» з'являється вікно із запитом дозволу на використання ЕП, для того, щоб дати дозвіл необхідно натиснути «ОК», Рис. 58. Якщо натиснути кнопку «Відміна», підпис не буде створено та операція буде завершена.



Рис. 58. Дозвіл на використання ЕП

Після натискання кнопки «ОК» з'являється вікно про успішне створення електронного підпису, Рис. 59.



Рис. 59. Повідомлення про створення електронного підпису

Далі зберігається файл з підписом за допомогою кнопки «стрілки вниз», яка з'являється біля кожного файлу на який накладено підпис, Рис. 60.



ТОВ Сайфер <mark>Б</mark>ІС

00:34:57

∆гент	ECKO	6
AICHI	CCRO	

підключено

ECKO 🕄 підключено ENG

RUS

УКР

Особистий ключ Перевірити ЕП	Створити ЕП Зашифрувати Ро	зшифрувати Генерація ключів	
Параметри створення ЕП	✔ Файл		
 Тип підпису Вбудований Відкріплений Формат підпису Базовий (CAdES-BES) З повними даними для перевірки (CAdES-X Long) Додати підпис до вже існуючого Генерація QR 	20201209_135149.jpg log-test.txt log-test.txt.png Створити ЕП		и
	▲ Текстові дані		

Рис. 60. Збереження підпису у файл

Далі обираємо шлях збереження файлу та очищаємо форму, Рис. 61.

гот компьютер 🔸	Paratana - Nati					>
гот компьютер 🔸	Zarmana & Naw					
	загрузки > ivew			~ Ū	Поиск: New	م
ая папка						= - ?
Имя	^	Дата изменения	Тип	Размер		
	ŀ	leт элементов, удовлетво	ряющих условиям п	оиска.		
0.txt.p7s						
#7 Signature (*.p7s))					`
					Сохранить	Отмена
	ая папка Имя О.tot.p7s ; #7 Signature (*.p7s)	iaя nanka Имя 	ая папка Имя Дата изменения Нет элементов, удовлетво O.txt.p7s ; #7 Signature (*.p7s)	вая папка Имя ^ Дата изменения Тип Нет элементов, удовлетворяющих условиям п О.txt.p7s 5 #7 Signature (*.p7s)	аая папка Имя Дата изменения Тип Размер Нет элементов, удовлетворяющих условиям поиска. О.bd.p7s ;#7 Signature (*.p7s)	аая папка Имя Дата изменения Тип Размер Нет элементов, удовлетворяющих условиям поиска. О.tot.p7s ; #7 Signature (*.p7s)



Створення ЕП за типом «Вбудований» на текстові дані

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Вбудований» та Формат ЕП (CAdES-BES чи CAdES-X Long), тип кодування, вказується текст для підпису, натискаємо кнопку

«Створити ЕП», Рис. 62.

Після натискання на кнопку «Створити ЕП» з'являється вікно із запитом дозволу на використання ЕП, щоб дати дозвіл необхідно натиснути кнопку «Ок». Якщо натиснути «Відміна», підпис не буде створено та операція буде завершена, Рис. 63.

👝 Клієнт єдиного сер	овісу крипт	су криптографічних операцій			€C	ЕСКО 🚯		
ТОВ Сайфер БІС			-	підключено	підкл	іючено		
00:34:12					УКР F	RUS ENG		
Особистий ключ Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів				
Параметри створення ЕП	∧ Файл	л						
✓ Тип підпису	🗸 Текс	тові дані						
 Відкріплений Формат підпису Базовий (CAdES-BES) 	Кодува Текстов 123	ння: 🖲 UTF-16LE 🔿 U	ITF-8					
 З повними даними для перевірки (CAdES-X Long) Додати підпис до вже існуючого Генерація ОВ 								
		Скопіювати						
	Додатк	овий опис:						
	(Створити ЕП	Очистити ф	орму				
	Підпис	у кодуванні Base64:						
		Скопіювати						

Рис. 62. Створення ЕП



Рис. 63. Дозвіл на використання ЕП

Після натискання кнопки «ОК» з'являється вікно про успішне створення електронного підпису, Рис. 64.



Далі у полі «Підпис у кодуванні Base64» з'являється текст з підписом, Рис. 65, далі за необхідності очищаємо форму.

📄 Клієнт єдиного сервісу криптографічних операцій			Агент ЄСКО 🚯	ECKO (ECKO 🚯	
ТОВ Сайфер БІС				підключено	підключ	ено
0:33:29					YKP RUS	ENG
Особистий ключ Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів		
Параметри створення ЕП	\land Файл	n				
✓ Тип підпису Вбудований	🗸 Текс	тові дані				
 Відкріплений 	Кодува	ння: 🖲 UTF-16LE 🔿 U	JTF-8			
✓ Формат підпису	Текстов	зі дані для підпису:				
О Базовий (CAdES-BES)	123					
 З повними даними для перевірки (CAdES-X Long) 						
🗆 Додати підпис до вже існуючого						
🗆 Генерація QR						
		Скопіювати				
	Додатк	овий опис:				
	(Створити ЕП	Очистити ф	орму		
	Підпис	у кодуванні Вазеб4:				
	MIIgn SIb3D LKoYk dGE0I QkdC	nAYJKoZIhvcNAQcCoJ QEHAaAIBAYxADIAM AgEBAQEDAQEwgcs> LXRgCDQkdCG0KEiM G0KEiMTkwNwYDVQ	IgiTCCIIUCAQExD wCgggagMIIGnD (LDAqBgNVBAMM SUwIwYDVQQKDE QLDDDQptC10L3F	jAMBgoqhiQCAQEBAQ CCBkSgAwIBAgIINwzda 119Cm0KHQmiDQotCe 12QotCe0JIgItCh0LDQu 13gtGAINGB0LXRgNGC0	QIBMBUGCSqG AC65LAcwDQY 0JIgItCh0LDQu ıdGE0LXRgCD DLJRhNGW0LrQ	•
		Скопіювати				

Рис. 65. Результат підпису тестових даних

Створення ЕП за типом «Відкріплений» на текстові дані

Відеоінструкція знаходиться за посиланням.

Процес Створення ЕП починається з того, що вказуються «Параметри для створення ЕП», Тип ЕП «Відкріплений» та Формат ЕП (CAdES-BES чи CAdES-X Long), тип кодування, вказується текст для підпису, натискаємо кнопку «Створити ЕП», Рис. 66.

👝 Клієнт єдиного сер	овісу криптографічних	Агент ЄСКО	сско
операцій		підключено	о підключено
ТОВ Сайфер БІС 02:03:26			JKP RUS ENG
Особистий ключ Перевірити ЕП	Створити ЕП Зашифрувати Р	озшифрувати Гене	рація ключів
Параметри створення ЕП	Файл		
✓ Тип підпису О Вбудована	Текстові дані		
 воудована Відкріплена Додати підпис до вже 	Кодування:		
існуючого • Формат підпису	123		
Базовий (CAdES-BES)			
 З повними даними для перевірки (CAdES-X Long) 			
	Скопіювати		
	Додатковий опис:		
	Створити ЕП Оч	истити форму	
	Підпис у кодуванні Base64:		
	Скопіювати		

Рис. 66. Створення ЕП

Після натискання на кнопку «Створити ЕП» з'являється вікно із запитом дозволу на використання ЕП, щоб дати дозвіл необхідно натиснути кнопку «Ок». Якщо натиснути «Відміна», підпис не буде створено та операція буде завершена, Рис. 67.

🔋 Агент єдиного сервісу криптографічних операцій	×
Pecypc [https://ccs-dev.cipher.kiev.ua] запитує дозвіл на використання ЕП в кількості 1 раз(у,ів).	?
Щоб дати дозвіл на використання особистого ключа натисніть кнопку "Ok". У разі відмови натисніть кнопку "Відміна". ОК	Зідміна

Рис. 67. Дозвіл на використання ЕП

Після натискання кнопки «ОК» з'являється вікно про успішне створення електронного підпису, Рис. 68.



Рис. 68. Повідомлення про створення електронного підпису

Далі у полі «Підпис у кодуванні Base64» з'являється текст з підписом, Рис. 69. Далі за необхідності очищаємо форму.



Агент ЄСКО 🚯

00

УКР

підключено

ЄСКО 🚯 підключено

RUS

ENG



ТОВ Сайфер БІС

00:29:06

Особистий ключ Перевірити ЕП	Створити ЕП Зашифрувати Розшифрувати Генерація ключів
Параметри створення ЕП	▲ Файл
✓ Тип підпису	✔ Текстові дані
О воудовании	
• ыдкріплении	
 Вазовии (САССЭ-БСЗ) З повними даними для перевірки (CAdES-X Long) 	123
🗆 Додати підпис до вже існуючого	
🗆 Генерація QR	
	Скопіювати
	додатковии опис:
	Створити ЕП Очистити форму
	Підпис у кодуванні Base64:
	MIIgjgYJKoZIhvcNAQcCoIIgfzCCIHsCAQExDjAMBgoqhiQCAQEBAQIBMAsGCSqGSI b3DQEHAaCCBqAwggacMIIGRKADAgECAgg3DN0ALrksBzANBgsqhiQCAQEBAQM BATCByzEsMCoGA1UEAwwj0KbQodCaINCi0J7QkiAi0KHQsNC50YTQtdGAINCR0Ib QoSIxJTAjBgNVBAoMHNCi0J7QkiAi0KHQsNC50YTQtdGAINCR0IbQoSIxOTA3BgN VBAsMMNCm0LXQvdGC0YAg0YHQtdGA0YLQuNGE0ZbQutCw0YbRltGXINC60LvRj
	Скопіювати

Рис. 69. Результат підпису тестових даних

Створення мобільного ЕП

За аналогією, як і при створенні звичайного підпису (за допомогою файлового контейнеру), необхідно завантажити файл/файли/текстові дані та натиснути кнопку «Створити ЕП», Рис. 70.



Особистий ключ Перевірити ЕП	Створити ЕП		
Параметри створення ЕП	✔ Файл		
 Тип підпису Вбудований Відкріплений Формат підпису Базовий (CAdES-BES) З повними даними для перевірки (CAdES-X Long) 	log-test.txt	û Ç	Перетягніть файл(и) чи огляд
 Додати підпис до вже існуючого Генерація QR 	Створити ЕП 🏠	Очистити форму	
	🔺 Текстові дані		

Рис. 70. Створення мобільного ЕП

На телефон приходить повідомлення про підтвердження створення ЕП та введення ПІН-коду, Рис. 71-Рис. 72. Про успішне створення мобільного ЕП повідомляється у відповідному повідомлені, Рис. 73.



Рис. 71. Підтвердження створення мобільного ЕП



Рис. 72. Введення ПІН-коду



Рис. 73. Повідомлення про створення ЕП

Перевірка ЕП

Дана функція є доступною і без ключа.

Варто зазначити! Кваліфікований електронний підпис вважається тоді, якщо сертифікат отриманий у Кваліфікованого надавача електронних довірчих послуг та ключ згенеровано на захищеному носії чи мережному криптомодулі чи у "хмарі". Якщо, хоча б одна умова не виконується, то підпис не є Кваліфікованим.

Вкладка «Перевірити ЕП» містить розділи: Параметри перевірки ЕП, Текстові дані та Файл, Рис. 74-Рис. 75.



Агент ЄСКО **()** підключено

	ТОВ Сайфер	ыс
00.28.20		

(еско 🤅)
під	цключе	но
УКР	RUS	E

ENG

Особистий ключ	Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів		
Параметри переві	рки підпису	🗸 Файл					
✓ Тип підпису ○ Вбудований		Файл дл	я перевірки:				
🖲 Відкріплений			Перетягніть файл чи огляд				
 Режим перевірк позначки часу для 	ки електронної підпису	Файл з г	ідписом:				
 Ігнорувати еле часу 	ектронну позначку			Перетягніть ф	райл чи огляд		
 Перевіряти ел позначку часу присутня 	ектронну 7, якщо вона		Перевірити Е	Π	Очистити форму		
 Перевіряти ел позначку часу помилку, якщо 	ектронну і повертати о вона відсутня	◆ Текст	ові дані				
Режим перевіркі позначки часу для	и електронної даних	Кодуван Текстові	іня: 🖲 UTF-16LE 〇 і дані для перевірк	UTF-8 :и:			
О Розширення ЕП							
🗆 Генерація QR							
		Електро	нний підпис в код	уванні Base64:			
			Перевірити Е	Π	Очистити форму		

Рис. 74. Вкладка «Перевірити ЕП»

Розділ «Параметри перевірки ЕП», який у свою чергу включає:

1.Поле «Тип ЕП», яке містить:

- Вбудований;
- Відкріплений;

2.Режим перевірки електронної позначки часу для ЕП, який вказується за необхідності ігнорувати, перевіряти її наявність, чи повертати помилку за її відсутності.

3. Режим перевірки електронної позначки часу для даних, який вказується за необхідності ігнорувати, перевіряти її наявність, чи повертати помилку за її відсутності.

4.Позначка «Розширити ЕП».

5.Позначка «Генерація QR-коду».

Розділ «Файл», який у свою чергу включає:

Якщо перевіряється файл за типом ЕП – Вбудований.

- 1. Поле «Файл з підписом» (обирається файл, який містить підпис за типом ЕП Вбудований).
- 2. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
- 3. Кнопка «Зберегти підписані дані» (дозволяє зберегти дані без підпису);
- 4. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

📻 Клієнт єдиного сервісу криптографічних операцій			Агент ЄСКО 🚯	ECK	ECKO 🚯	
ТОВ Сайфер БІС				підключено	підкл	ючено
00:24:37					JKP RI	US ENG
Особистий ключ Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів		
Параметри перевірки підпису	🗸 Файл					
✓ Тип підпису	Файл дл	я перевірки:				
 Вбудований Відкріплений 			Перетягніть фай	йл чи огляд		
 Режим перевірки електронної позначки часу для підпису 	Файл з г	ідписом:				
 Ігнорувати електронну позначку часу 			Перетягніть фай	йл чи огляд		
 Перевіряти електронну позначку часу, якщо вона присутня 		Перевірити El	1	Очистити ф	орму	
 Перевіряти електронну позначку часу і повертати 	▶ Текст	ові дані				
помилку, якщо вона відсутня > Режим перевірки електронної	Кодуван	іня: 🖲 UTF-16LE О	UTF-8			
позначки часу для даних	Текстов	дані для перевіркі	И:			
 Розширення ЕП Генерація QR 						
	Електро	нний підпис в коду	ванні Base64:			
		Перевірити El	1	Очистити ф	орму	
			Скопіювати розши	ирений підпис		

Рис. 75. Вкладка «Перевірити ЕП» зі вказівкою позначки «Розширення ЕП»

Якщо перевіряється файл за типом ЕП – Відкріплений.

- 1. Поле «Файл для перевірки» (обирається файл, який не містить підпис початковий файл);
- 2. Поле «Файл з підписом» (обирається файл, який містить підпис за типом ЕП Відкріплений);
- 3. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису за допомогою завантаженого файлу з підписом для файлу для перевірки);

4. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

3.Розділ «Текстові дані», який у свою чергу включає:

Якщо перевіряється файл за типом ЕП – Вбудований.

- 1. Кодування: UTF-16LE та UTF-8.
- 2. Поле «Підпис у кодування Base64» (вказується текст, який містить підпис за типом ЕП Вбудований).
- 3. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
- 4. Поле «Дані з електронного підпису» (виведення текст без підпсиу);
- 5. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Якщо перевіряється файл за типом ЕП – Відкріплений.

- 1. Кодування: UTF-16LE та UTF-8.
- 2. Поле «Текстові дані для перевірки» (вказуються текстові дані, який не містить підпис початкові дані);
- 3. Поле «Підпис у кодуванні Base64» (вказуються текстові дані з підписом, за типом ЕП Відкріплений);
- 4. Кнопка «Перевірити ЕП» (перевіряє дійсність електронного підпису);
- 5. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Процес Перевірки ЕП починається з того, що обираються «Параметри перевірки ЕП», обирається файл з підписом, натискаємо кнопку «Перевірити ЕП». За необхідності можна змінити файл.

Перевірка ЕП за типом «Вбудований», файл

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Вбудований» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Вбудований, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо файл з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 76.

Клієнт єдиного сер	Агент ЄСКО 🚯	ECKO 🚯	
ТОВ Сайфер БІС	підключено	підключено	
00:22:21			YKP RUS ENG
Особистий ключ Перевірити ЕП	Створити ЕП Зашифрувати Розшифрувати	Генерація ключів	3
Параметри перевірки підпису	✔ Файл		
✓ Тип підпису	Файл з підписом:		
 Вбудований Відкріплений 	log-test.txt.p7s		Очистити
Режим перевірки електронної позначки часу для підпису	Зберегти підг	исані дані	
Режим перевірки електронної позначки часу для даних	Перевірити ЕП	Очистити	і форму
О Розширення ЕП			
🗆 Генерація QR	 Текстові дані 		



Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 77.



Рис. 77. Повідомлення про дійсність електронного підпису

Після натискання «OK», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дату підпису, Рис. 78. За необхідності зберегти первинні дані (без підпису), натиснувши на кнопку «Зберегти підписані дані». Також можна сформувати та зберегти Протокол створення та перевірки кваліфікованого ЕП, натиснувши на Протокол перевірки (файл буде збережено на ПК з розширенням .pdf) або скопіювати результат перевірки у буфер обміну, натиснувши на Скопіювати. Після чого, натискаємо кнопку «Очистити форму».

📻 Клієнт єдиного сервісу криптографічних операцій			Агент ЄСКО 🚯	ECKO (0		
тов Сайф	þер БIC				підключено	підключе	ено
0:20:14						YKP RUS	ENG
Особистий ключ	Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів		
Параметри переві	ірки підпису	🗸 Файл	1				
✔ Тип підпису		Файл з	підписом:				
 Вбудований Візмої волий 		log-te	est.txt.p7s			Очисти	ти
 Відкріплений Режим перевірк 	и електронної	Проток	ол перевірки			Скопію	вати
позначки часу для	а підпису	Пілли	ıc 1	Підписувач: Пупкин	Сергій Петрович		
Режим перевірк позначки часу для	ки електронної аданих	Дійсн	ий	Організація: ТОВ «С РНОКПП: 123456789	айфер PRO» Ю		
О Розширення ЕГ]	Неква	аліфікований	ЄДРПОУ: 33349855 КНЕДП/АЦСК: ЦСК	ТОВ "Сайфер БІС"		
🗆 Генерація QR				Серійний номер сер Дата підпису: 09.12.	ртифікату підписанта: 370СС 2020, 16:32:46 GMT+2	DD002EB92C07	
				Електронна познач Серійний номер сер	ка часу підпису: дійсна; 09.12 ртифікату електронної позн	2.2020, 16:32:30 GMT іачки часу ЕП:	+2
				F2C0270A527AD965 Кваліфікований сер	тифікат: Ні		
				Тип засобу КЕП: е. к	люч Авест AvestKey		
				26anarry piar			
				зоеренти піді	исані дані		
			Перевірити	EU	Очистити	форму	
		∧ Текс	тові дані				

Рис. 78. Результат перевірки

Перевірка ЕП за типом «Відкріплений», файл

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Відкріплений» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Відкріплений, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо файл з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 79. Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 80.

Клієнт єдиного сер	Агент ЄСКО 🚯	ECKO 🚯			
ТОВ Сайфер БІС	ТОВ Сайфер БІС				
00:13:32			JKP RUS ENG		
Особистий ключ Перевірити ЕП	Створити ЕП Зашифрувати Розшифрувати	Генерація ключів			
Параметри перевірки підпису	🗸 Файл				
 Тип підпису Вбудований Відкріплений 	Файл для перевірки: log-test.txt		Очистити		
Режим перевірки електронної позначки часу для підпису	Файл з підписом:				
Режим перевірки електронної позначки часу для даних	log-test.txt.p7s		Очистити		
 Розширення ЕП Генерація QR 	форму				
	 текстові дані 				

Рис. 79. Перевірка ЕП



Рис. 80. Повідомлення про дійсність електронного підпису

Після натискання «OK», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дата підпису, Рис. 81. Також можна сформувати та зберегти Протокол створення та перевірки кваліфікованого ЕП, натиснувши на Протокол перевірки (файл буде збережено на ПК з розширенням .pdf) або скопіювати результат перевірки у буфер обміну, натиснувши на Скопіювати. Після чого, натискаємо кнопку «Очистити форму».



ТОВ Сайфер БІС

00:13:12

Агент ЄСКО 🚯	
підключено	

ЄСКО 🕄 підключено

ENG

RUS

УКР

Особистий ключ	Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифруват	и Генерація ключів	
Параметри переві	рки підпису	🗸 Файл				
 Тип підпису Вбудований Відкріплений Режим перевірки електронної позначки часу для підпису Режим перевірки електронної позначки часу для даних Розширення ЕП Генерація QR 		Файл для log-tes Файл з п log-tes Протоко Підпис Дійсни Неквал	я перевірки: st.txt iiдписом: st.txt.p7s ол перевірки с 1 ій ліфікований	Підписувач: Пупи Організація: ТОВ РНОКПП: 123456 ЄДРПОУ: 3334983 КНЕДП/АЦСК: Ц Серійний номер Дата підпису: 09, Електронна позн Серійний номер F2C0270A527AD94 Кваліфікований Засіб КЕП: Так Тип засобу КЕП:	кин Сергій Петрович «Сайфер PRO» 7890 55 СК ТОВ "Сайфер БІС" сертифікату підписанта: 370CDD002EI 12.2020, 16:51:06 GMT+2 качка часу підпису: дійсна; 09.12.2020, 1 сертифікату електронної позначки ч 65 сертифікат: Ні е. ключ Авест AvestKey	Очистити Очистити Скопіювати 892С07 16:50:49 GMT+2 асу ЕП:
			Перевірити І	in	Очистити форм	у
		▲ Тексто	ові дані			

Рис. 81. Результат перевірки

Перевірка ЕП за типом «Вбудований», текстові дані

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Вбудований» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Вбудований, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо текст з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 82.

Клієнт єдиного о тов Сайфер БІС	Агент ЄСКО 🚯 підключено	ЄСКО 🚯 підключено					
00:12:10			YKP RUS ENG				
Особистий ключ Перевірити Е	Створити ЕП Зашифрувати Розшифрувати	Генерація ключів	3				
Параметри перевірки підпису	∧ Файл						
 Тип підпису Вбудований Відкріпдений 	✓ Текстові дані Колування: ● UTE-16LE O UTE-8						
 Режим перевірки електронної позначки часу для підпису 	Електронний підпис в кодуванні Base64: hAgkA8sAnClJ62WUwDQYLKoYkAgEBAQEDA	Електронний підпис в кодуванні Base64: hAgkA8sAnClJ62WUwDQYLKoYkAgEBAQEDAQEEQqD9htp8vJpqtk7XfxTMNJIZ2U					
 Режим перевірки електронної позначки часу для даних Розширення ЕП Генерація QR 	gfOmxIn3165J3Dx10MALTgu7GJmCJszor/ZfC = Дані з електронного підпису:	66SAbt3QZ7rOofFSb	2ANaZu3RcAA=				

Рис. 82. Перевірка ЕП

Перевірити ЕП

Очистити форму

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 83.



Рис. 83. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дату підпису, Рис. 84.

Після чого, натискаємо кнопку «Очистити форму».



ТОВ Сайфер БІС

ECKO 🚯

підключено підключено 00:11:35 ENG УКР RUS Особистий ключ Перевірити ЕП Створити ЕП Зашифрувати Розшифрувати Генерація ключів Параметри перевірки підпису ∧ Файл Тип підпису Текстові дані Вбудований Відкріплений Кодування: 🔍 UTF-16LE 🔿 UTF-8 Електронний підпис в кодуванні Base64: Режим перевірки електронної позначки часу для підпису - -۰ hAgkA8sAnClJ62WUwDQYLKoYkAgEBAQEDAQEEQqD9htp8vJpqtk7XfxTMNJIZ2U Режим перевірки електронної gfOmxIn3165J3Dx10MALTgu7GJmCJszor/ZfG6SAbt3QZ7rOofFSb2ANaZu3RcAA= позначки часу для даних = О Розширення ЕП Дані з електронного підпису: Пенерація QR 123 Підпис 1 Підписувач: Пупкин Сергій Петрович Організація: ТОВ «Сайфер PRO» Дійсний РНОКПП: 1234567890 Некваліфікований **ЄДРПОУ:** 33349855 КНЕДП/АЦСК: ЦСК ТОВ "Сайфер БІС" Серійний номер сертифікату підписанта: 370CDD002EB92C07 Дата підпису: 09.12.2020, 16:55:45 GMT+2 Електронна позначка часу підпису: дійсна; 09.12.2020, 16:55:28 GMT+2 Серійний номер сертифікату електронної позначки часу ЕП: F2C0270A527AD965 Кваліфікований сертифікат: Ні **Baci6 KEII:** Tak Тип засобу КЕП: e. ключ Aвест AvestKey

Перевірити ЕП

Очистити форму



Перевірка ЕП за типом «Відкріплений», текстові дані

Відеоінструкція знаходиться за посиланням.

Для перевірки ЕП за типом «Відкріплений» необхідно у розділі «Параметри перевірки ЕП» вказати Тип ЕП – Відкріплений, та вказати параметр для Режиму перевірки електронної позначки часу для ЕП та Режиму перевірки електронної позначки часу для даних, обираємо текст з підписом, натискаємо кнопку «Перевірити ЕП», Рис. 85.



ТОВ Сайфер БІС

00:10:43

Агент ЄСКО 🚯 підключено

ЄСКО 🚯 підключено

ENG

RUS

УКР

Особистий ключ Перевірити ЕП	Створити ЕП Зашифрувати Розшифрувати Генерація ключів
Параметри перевірки підпису	木 Файл
✓ Тип підпису	✓ Текстові дані
 воудовании Відкріплений 	Кодування: 🖲 UTF-16LE 〇 UTF-8
> Режим перевірки електронної	Текстові дані для перевірки:
позначки часу для підпису Режим перевірки електронної позначки часу для даних	123
О Розширення ЕП	
Генерація QR	
	Електронний підпис в кодуванні Base64:
	OTTRICCYINIKEWDWYDVQQHDAJQITIC402IQSJEZIVIBCGA10EBKIVIQV0EtiVIZIVIZIVDK4 NTUtMDAwMjELMAkGA1UEBhMCdWECCQDywCcKUnrZZTANBgsqhiQCAQEBAQ MBAQRCM2110QzUaWjWmYQ+hFzNmpg5EEx5IAps4njV3CYfmQYA/8jLeMyAwm a5ReLCTFrBnEtcby5qw+wW5T1Vi43fMUAA
	Перевірити ЕП Очистити форму

Рис. 85. Перевірка ЕП

Після натискання кнопки «Перевірити ЕП», з'являється повідомлення з результатами перевірки електронного підпису, Рис. 86.



Рис. 86. Повідомлення про дійсність електронного підпису

Після натискання «ОК», з'являється інформація про дійсність підпису, вказується інформація про підписанта та дата підпису, Рис. 87.

Після чого, натискаємо кнопку «Очистити форму».



ТОВ Сайфер БІС

00:10:25

підключено

Електронна позначка часу підпису: дійсна; 09.12.2020, 16:58:59

Серійний номер сертифікату електронної позначки часу ЕП:

Очистити форму

ЄСКО 🕄 підключено

ENG

RUS

УКР

Особистий ключ	Перевірити ЕП	Створити ЕП Зашифруват	ги Розшифрувати	Генерація ключів	
Параметри переві	рки підпису	\land Файл			
 Тип підпису О Вбудораций 		🗸 Текстові дані			
 воудовании Відкріплений 		Кодування: 🔍 UTF-16	LE O UTF-8		
> Режим перевірк	и електронної	Текстові дані для пере	евірки:		
 позначки часу для Режим перевірк позначки часу для 	а підпису ки електронної а даних	123			
О Розширення ЕП	1				
🗆 Генерація QR					
		Електронний підпис в отклісуічіке wow to NTUtMDAwMjELMA MBAQRCM2110QzU a5ReLCTFrBnEtcby5q	кодуванні Base64: vqqnDajqmtc402rqsji «GA1UEBhMCdWECCQE aWjWmYQ+hFzNmpg58 w+wW5T1Vi43fMUAA	EX5IAps4njV3CYfmQYA/8jLeMyAwm	
		Підпис 1 Дійсний Некваліфікований	Підписувач: Пупк Організація: ТОВ РНОКПП: 1234567 ЄДРПОУ: 3334985 КНЕДП/АЦСК: ЦС Серійний номер (Дата пілагису: 0-1	ин Сергій Петрович «Сайфер PRO» 890 5 К ТОВ "Сайфер БІС" :ертифікату підписанта: 370CDD002EB92C07 12,2020, 16:59:15 GMT+2	

Рис. 87. Результат перевірки

Перевірити ЕП

GMT+2

F2C0270A527AD965 Кваліфікований сертифікат: Ні

Тип засобу КЕП: е. ключ Авест AvestKey

Засіб КЕП: Так

Розширення ЕП

Вкладка «Перевірити ЕП» містить додаткову позначку «Розширити ЕП», при її вказівці, зовнішній вигляд сторінки видозмінюється та стають доступні нові кнопки, Рис. 88.



Агент ЄСКО **()** підключено ЄСКО 🚯 підключено

ENG

RUS

УКР

00:09:43

ТОВ Сайфер БІС

Особистий ключ Перевірити ЕП	Створити ЕП Зашифрувати Розшифрувати Генерація ключів		
Параметри перевірки підпису	🗸 Файл		
 Тип підпису Вбудований Відкріплений 	Файл з підписом: Перетягніть файл чи огляд		
Режим перевірки електронної позначки часу для підпису	Зберегти підписані дані		
Режим перевірки електронної позначки часу для даних	Перевірити ЕП Очистити форму		
Розширення ЕП			
П Генерація QR Текстові дані			
	Кодування: • UTF-16LE O UTF-8 Електронний підпис в кодуванні Base64: 		
	Перевірити ЕП Очистити форму Скопіювати розширений підпис		

Рис. 88. Вкладка «Перевірити ЕП» з позначкою «Розширення ЕП»

Розширення ЕП для файлу

Відеоінструкція знаходиться за посиланням.

На прикладі вбудованого електронного підпису, який отримано раніше. Слід обрати файл та натиснути кнопку «Перевірити ЕП», Рис. 89.

Клієнт єдиного серв	Агент ЄСКО 🚯 підключено	ЄСКО 🚯	
00:07:56			JKP RUS ENG
Особистий ключ Перевірити ЕП	Створити ЕП Зашифрувати Розшифрувати	Генерація ключів	
Параметри перевірки підпису	✔ Файл		
 Тип підпису Вбудований Відкріплений 	Файл з підписом: log-test.txt.p7s		Очистити
Режим перевірки електронної позначки часу для підпису	Зберегти підп	исані дані	
Режим перевірки електронної позначки часу для даних	Перевірити ЕП Очистити форму		
✓ Розширення ЕП			
Пенерація QR	 Текстові дані 		

Рис. 89. Розширення вбудованого ЕП

Отримати повідомлення про успішне розширення підпису, Рис. 90.



Рис. 90. Повідомлення про результат перевірки та розширення ЕП

Отримати результат перевірки електронного підпису, Рис. 91.



ТОВ Сайфер БІС

1.1

Агент ЄСКО **()** підключено ECKO 🚯

ENG

підключено

RUS

УКР

Особистий ключ	Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів	
Параметри переві	оки підпису	🗸 Φai	йл			
 Тип підпису Вбудований Відкріплений Режим перевірки електронної 		Файл : log-1 Прото	з підписом: test.txt.p7s кол перевірки			Очистити Скопіювати
 Режим перевірки електронної позначки часу для підпису Режим перевірки електронної позначки часу для даних ☑ Розширення ЕП □ Генерація QR 		Підп Дійс Нек	пис 1 гний валіфікований	Підписувач: Пупкин Організація: ТОВ «С РНОКПП: 123456789 ЄДРПОУ: 33349855 КНЕДП/АЦСК: ЦСК Серійний номер сер Дата підпису: 09.12. Кваліфікований сер Засіб КЕП: Так Тип засобу КЕП: е. к	Сергій Петрович айфер PRO» 10 ТОВ "Сайфер БІС" этифікату підписанта: 370CDD002E 2020, 17:06:05 GMT+2 этифікат: Ні элюч Авест AvestKey	B92C07
				Зберегти підг	исані дані	
			Перевірити ЕП Очистити форм Зберегти розширений підпис			У
		▲ Тек	стові дані			

Рис. 91. Розширення вбудованого ЕП

За умови, якщо було завантажено файл вже з повними даними для перевірки, то з'явиться повідомлення про це, Рис. 92.


ТОВ Сайфер БІС

Агент ЄСКО 🚯 підключено

ECKO 🚯

ENG

підключено RUS

УКР

Особистий ключ Перевірити ЕП Створити ЕП Зашифрувати Розшифрувати Генерація ключів Параметри перевірки підпису 🗸 Файл Тип підпису Файл з підписом: Вбудований log-test.txt.p7s Очистити Відкріплений Протокол перевірки Скопіювати Режим перевірки електронної позначки часу для підпису Підпис містить повні дані для перевірки (CAdES-X Long). Розширювати Режим перевірки електронної електронний підпис непотрібно. позначки часу для даних Розширення ЕП Підпис 1 Підписувач: Пупкин Сергій Петрович Пенерація QR Організація: TOB «Сайфер PRO» Дійсний РНОКПП: 1234567890 Некваліфікований **ЄДРПОУ:** 33349855 КНЕДП/АЦСК: ЦСК ТОВ "Сайфер БІС" Серійний номер сертифікату підписанта: 370CDD002EB92C07 Дата підпису: 09.12.2020, 17:10:15 GMT+2 Електронна позначка часу підпису: дійсна; 09.12.2020, 17:09:59 GMT+2 Серійний номер сертифікату електронної позначки часу ЕП: F2C0270A527AD965 Кваліфікований сертифікат: Ні **Bació KEII:** Tak Тип засобу КЕП: e. ключ Aвест AvestKey Зберегти підписані дані Перевірити ЕП Очистити форму Зберегти розширений підпис Текстові дані



Розширення ЕП для текстових даних

Відеоінструкція знаходиться за посиланням.

На прикладі відкріпленого електронного підпису, який отримано раніше. Слід вказати підписані дані та натиснути кнопку «Перевірити ЕП», Рис. 93.



ТОВ Сайфер БІС

00:03:54

Агент ЄСКО 🚯 підключено ECKO 🚯

RUS

ENG

підключено

УКР

OK

Особистий ключ Перевірити ЕП	Створити ЕП Зашифрувати Розшифрувати Генерація ключів
Параметри перевірки підпису	木 Файл
✓ Тип підпису	✓ Текстові дані
 воудовании відкріплений 	Кодування: 🖲 UTF-16LE 🔿 UTF-8
Режим перевірки електронної позначки часу для підпису	Текстові дані для перевірки:
Режим перевірки електронної позначки часу для даних	123
Розширення ЕП	
🗆 Генерація QR	
	Електронний підпис в кодуванні Base64: DKITIGWOZCGOLI Qu9GOUTIKICYINKEWDWTDVQQHDAJQITIC40ZIQSJEZIVIBCGATOE BRMQVUEtMzMzNDk4NTUtMDAwMjELMAkGA1UEBhMCdWECCDcM3QAuuSwH MA0GCyqGJAIBAQEBAwEBBECeN+I/kWESJM7wuvtakhOMEe4PNq1GT0kro9VCWI r6WKypUu1N2RCeTDxiVLsW3oZOLnDddXncXNEA31ZAXvMI
	Перевірити ЕП Очистити форму
	Скопіювати розширений підпис

Рис. 93. Розширення відкріпленого ЕП

Отримати повідомлення про успішне розширення підпису, Рис. 94.

Подтвердите действие на странице ccs-dev.cipher.kiev.ua

Електронний підпис успішно перевірено. Електронний підпис успішно розширено.

Рис. 94. Повідомлення про перевірку та розширення підпису

Отримати результат перевірки електронного підпису, Рис. 95.



ТОВ Сайфер БІС

00:03:34

ECKO 🚯

підключено

ЄСКО 🕄 підключено

ENG

RUS

УКР

Особистий ключ Пе	еревірити ЕП	Створити ЕП Зашифрувати Розшифрувати Генерація ключів
Параметри перевірки п	підпису	🛧 Файл
 Тип підпису Вбудований 		✓ Текстові дані
 Відкріплений 		Кодування: 🖲 UTF-16LE О UTF-8
Режим перевірки еле позначки часу для підпі	ектронної 1ису	Текстові дані для перевірки:
Режим перевірки еле позначки часу для дани	ектронної их	123
Розширення ЕП		
∪ Генерація QR		
		Eлектроннии підпис в кодуванні Base64: DKnitowozcgociQuagocomkitcyiwikewowrovQQHDAjQmitc4oziQsjeziwibcGATOE BRMQVUEtMzMzNDk4NTUtMDAwMjELMAkGA1UEBhMCdWECCDcM3QAuuSwH MA0GCyqGJAIBAQEBAwEBBECeN+l/kWESJM7wuvtakhOMEe4PNq1GT0kro9VCWl r6WKypUu1N2RCeTDxiVLsW3oZOLnDddXncXNEA31ZAXvMI
		Підпис 1 Підписувач: Пупкин Сергій Петрович Дійсний Організація: ТОВ «Сайфер PRO» РНОКПП: 1234567890 РНОКПП: 1234567890 Некваліфікований ЄДРПОУ: 33349855 КНЕДП/АЦСК: ЦСК ТОВ "Сайфер БІС" Серійний номер сертифікату підписанта: 370CDD002EB92C07 Дата підпису: 09.12.2020, 17:12:15 GMT+2 Кваліфікований сертифікат: Ні Засіб КЕП: Так Тип засобу КЕП: е. ключ Авест AvestKey
		Перевірити ЕП Очистити форму
		Скопіювати розширений підпис

Рис. 95. Результат розширення та перевірки ЕП

За умови, якщо було завантажено текстові дані вже з повними даними для перевірки, то з'явиться повідомлення про це, Рис. 96.



ТОВ Сайфер БІС

00:02:46

Агент	ECKO	0	
-------	-------------	---	--

підключено

ЄСКО 🚯 підключено

ENG

RUS

УКР

Особистий ключ Перевірити ЕП Створити ЕП Зашифрувати Розшифрувати Генерація ключів	
Параметри перевірки підпису 🔨 Файл	
 Тип підпису Вбудований Відкріплений Відкріплений Відкріплений Кодування: © UTF-16LE O UTF-8 Текстові дані для перевірки: Режим перевірки електронної позначки часу для даних Розширення ЕП Генерація QR Електронний підпис в кодуванні Вазеб4: QntCSICLQodCw0LnRhNC10YAg0JHQhtChIjE5MDcGA1UECwww0KbQtd(CDRgdC10YDRgtC40YTRitc60LDRhtGW0Zcg0LrQu9GO0YfRitcyMREwDwHDAjQmtC40ZfQsjEZMBcGA1UEBRMQVUEtMzMzNDk4NTUtMDAwMjELI Підпис містить повні дані для перевірки (CAdES-X Long). Розширюва електронний підпис непотрібно. 	С90YLRg YDVQQ MAkGA1 ▼
Підпис 1 Підписувач: Пупкин Сергій Петрович Дійсний Організація: ТОВ «Сайфер PRO» РНОКПГ: 1224567890 РНОКПГ: 1224567890 Некваліфікований ЄДРПОУ: 33349855 КНЕДП/АЦСК: ЦСК ТОВ "Сайфер БІС" Серійний номер сертифікату підписанта: 370СDD00 Дата підпису: 09.12.2020, 17:14:25 GMT+2 Електронна позначка часу підпису: 09.12.202 GMT+2 Серійний номер сертифікату електронної позначка F2C0270A527AD965 Кваліфікований сертифікат: Ні Засіб КЕП: Так Тип засобу КЕП: е. ключ Авест AvestKey	2EB92C07 0, 17:14:09 4 масу ЕП:
Перевірити ЕП Очистити форм	ý

Рис. 96. Результати розширення підпису з повними даними для перевірки

Зашифрувати

Процес зашифрування здійснюється із застосуванням захищеного носія (в активному та пасивному режимі) чи файлового ключового контейнеру.

За умови, якщо генерація ключа здійснювалася за допомогою Агенту ЄСКО у активному режимі – процес зашифрування здійснюється коректно, або самостійний запис ключа за допомогою «Модуля роботи з ключовим контейнером» у пасивному режимі.

Вкладка «Зашифрувати» містить такі розділи: Параметри шифрування, Сертифікат отримувача, Текстові дані та Файл, Рис. 97.

Розділ «Параметри зашифрування», який включає:

- Додати при зашифруванні:
- 1. Сертифікат відправника та сертифікати видавців;
- 2. Сертифікат відправника;
- 3. Не додавати сертифікат відправника та сертифікати видавців.

Розділ «Сертифікат отримувача», який включає:

• Поле «Сертифікат отримувача зашифрованих даних» (завантажуємо файл-сертифікат отримувача).



ТОВ Сайфер БІС

00:53:14

Агент ЄСКО 🚯	
підключено	r

ЄСКО 🚯 підключено

RUS

ENG

УКР

Особистий ключ	Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів
Параметри зашифр	рування	Сертиф	ікат отримувача		
 Додати при заш Сертифікат від сертифікати ві Сертифікати від 	ифруванні: правника та идавців правника	Сертиф	ікат отримувача за	шифрованих даних: Перетягніть файл	і чи огляд
Не додавати с відправника та видавців	ертифікат а сертифікати	🗸 Файл	I		
		3	ашифрувати	Очистити фо	Перетягніть файл(и) чи огляд рму
		⊷ Текс	гові дані		
		Кодува Текст д	ння: 🖲 UTF-16LE О ля зашифрування:	UTF-8	
		3	ашифрувати	Очистити фо	рму
		Зашифр	оовані дані у кодув	анні Base64:	
			Скопіювати		

Рис. 97. Вкладка «Зашифрувати»

- Розділ «Файл», який включає:
- 1. Поле «Файл для шифрування»;
- 2. Кнопка «Зашифрувати» (здійснює зашифрування файлу);
- 3. Кнопка «Зберегти шифровані дані у файл» (зберігає шифровані дані у файл);
- 4. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час

останньої сесії.

- Розділ «Текстові дані», який включає:
- 1. Тип кодування UTF-16LE та UTF-8.
- 2. Поле «Текст для зашифрування»;
- 3. Кнопка «Зашифрувати» (здійснює зашифрування тексту);
- 4. Кнопка «Очистити форму» (здійснює очищення всієї форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.
- 5. Поле «Зашифровані дані у кодуванні Base64».

Процес зашифрування файлу

Відеоінструкція знаходиться за посиланням.

Для того, щоб зашифрувати файл, у розділі «Параметри зашифрування», обрати один з пунктів (сертифікат відправника та сертифікати видавців чи сертифікат відправника чи не додавати сертифікат відправника та сертифікати видавців), у розділі «Сертифікат отримувача» додати сертифікат отримувача зашифрованих даних, у розділі «Файл» обрати файл для шифрування, натиснути кнопку «Зашифрувати», Рис. 98.

📻 Клієнт єдиного сервісу криптографічних операцій				Агент ЄСІ	(0 🚯	ECKO 🕻	ECKO 🚯	
ТОВ Сайфер БІС				підключ	ено	підключе	но	
00:48:50						YKP RUS	ENG	
Особистий ключ Перевірити ЕП С	Створити ЕП	Зашифрувати	Розшифрувати	Генерація	а ключів			
Параметри зашифрування	Сертиф	ікат отримувача						
✓ Додати при зашифруванні:	Сертиф	ікат отримувача з	ашифрованих даних	75 14				
 Сертифікат відправника та сертифікати видавців 	ДМС	TEST-KEP.cer				Очистит	ти	
О Сертифікат відправника								
 Не додавати сертифікат відправника та сертифікати видавців 	🗸 Файл	1						
	logo.pr	ng		Û	Перет	ягніть файл(и) ч	и	
						огляд		
	3	ашифрувати	Очистити ф	орму				
	▲ Текс	тові дані						

Рис. 98. Процес зашифрування

Після натискання на кнопку «Зашифрувати» з'являється вікно з повідомленням з результатом зашифрування, Рис. 99.



Після, зберігаємо зашифровані дані у файл та очищаємо форму.

Після, за допомогою відповідної кнопки «стрілка вниз» можна зберегти зашифрований файл та очищаємо форму, Рис. 100.

📀 Сохранение								×
	» Этот компьютер » Загру	/зки > New			~ ē	Поиск: New	,	p
Упорядочить 🔻	Новая папка						≣ ≣ ▼ (?
📌 Быстрый досту	Имя /п	^	Дата изменения	Тип	Размер			
OneDrive		Нет	элементов, удовлетво	ряющих условиям по	иска.			
🛄 Этот компьюте	ep							
💣 Сеть								
Mua daŭ ast	logo ppg p7e							~
имя файла. Тур файла:	D75 5ile (* e7e)							
гип файла:	Promie (".pre)							v
 Скрыть папки 					[Сохранить	Отмена	

Рис. 100. Збереження зашифрованого файлу

Процес зашифрування текстових даних

Відеоінструкція знаходиться за посиланням.

Для того, щоб зашифрувати текстові дані, у розділі «Параметри шифрування», обрати один з пунктів (сертифікат відправника та сертифікати видавців чи сертифікат відправника чи не додавати сертифікат відправника та сертифікати видавців), у розділі «Сертифікат отримувача» додати сертифікат отримувача зашифрованих даних, у розділі «Текстові дані» вказати текст для шифрування, натиснути кнопку «Зашифрувати», Рис. 101.



00:42:41

Особистий

ТОВ Сайфер БІС			підключено	підк.	лючено	
:42:41				УКР	RUS ENG	G
Особистий ключ Перевірити ЕП Ство	рити ЕП Зашифрувати	Розшифрувати	Генерація ключів			
Параметри зашифрування	Сертифікат отримувача					
 Додати при зашифруванні: Сертифікат відправника та сертифікати видавців Сертифікат відправника 	Сертифікат отримувача за ДМС TEST-KEP.cer	ашифрованих даних	X	Ou	истити	
 Не додавати сертифікат відправника та сертифікати 	∧ Файл					
видавців	🗸 Текстові дані					
	Кодування: • UTF-16LE С Текст для зашифрування: 123) UTF-8				
	Зашифрувати	Очистити ф	орму			
	Зашифровані дані у кодуг	занні Base64:				
	Скопіювати					

Агент ЄСКО 🚯

ECKO 🕄

Рис. 101. Процес зашифрування

Після натискання на кнопку «Зашифрувати» з'являється у полі «Зашифровані дані у кодуванні Base64», Рис. 102.



Створити ЕП

ТОВ Сайфер БІС

Перевірити ЕП

00:42:41

Особистий ключ

ацій	Агент ЄСКО 🚯	ЄСКО 🚯
	підключено	підключено
		YKP RUS ENG
ифрувати	Генерація ключів	

Параметри зашифрування	Сертифікат отримувача	
 Додати при зашифруванні: Сертифікат відправника та сертифікати видавців Сертифікат відправника 	Сертифікат отримувача зашифрованих даних: ДМС TEST-KEP.cer	Очистити
 Не додавати сертифікат відправника та сертифікати 	▲ Файл	
видавців	✓ Текстові дані	
	Кодування: UTF-16LE O UTF-8 Текст для зашифрування: 123	
	Зашифрувати Очистити форму	
	Зашифровані дані у кодуванні Base64: MIIMowYJKoZIhvcNAQcDollMIDCCDJACAQKgggm6ollJtjCCA3Ewg MCAQICCES/YMW6IFFxMA0GCyqGJAIBAQEBAwEBMIHLMSwwKgY DCPQptCh0Jog0KLQntCSICLQodCw0LnRhNC10YAg0JHQhtChljEIM 1UECgwc0KLQntCSICLQodCw0LnRhNC10YAg0JHQhtChljE5MDcGA ww0KbQtdC90YLRgCDRgdC10YDRgtC40YTRitC60LDRhtGW0Zcg0L	gMZoA DVQQD ICMGA x1UECw rQu9G
	Скопіювати	

Зашифрувати

Розш

Рис. 102. Повідомлення про успішне зашифрування даних

Розшифрувати

Процес розшифрування здійснюється із застосуванням захищеного носія (в активному та пасивному режимі) чи файлового ключового контейнеру.

За умови, якщо генерація ключа здійснювалася за допомогою Агенту ЄСКО у активному режимі – процес розшифрування здійснюється коректно, або самостійний запис ключа за допомогою «Модуля роботи з ключовим контейнером» у пасивному режимі.

Дана вкладка містить розділ Файл.

Розділ «Файл», який включає, Рис. 103:

- 1. Поле «Файл для розшифрування» (обирається файл, який необхідно розшифрувати);
- 2. Кнопка «Розшифрувати» (Здійснює дешифрування файлу);
- 3. Кнопка «Зберегти розшифровані дані у файл» (здійснює збереження розшифрованих даних у файл);
- 4. Кнопка «Очистити форму» (здійснює очищення форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

Розділ «Текстові дані», який включає, Рис. 103:

- 1. Тип кодування: UFT-16LE та UTF-8.
- 2. Поле «Зашифровані дані у кодуванні Ваѕе64» (вказується текст, який необхідно розшифрувати);
- 3. Кнопка «Розшифрувати» (здійснює дешифрування текстових даних);
- 4. Кнопка «Очистити форму» (здійснює очищення форми). Очищення форми щоразу не є обов'язковим, так як після завершення сесії, автоматично будуть очищені всі форми, які використовувалися під час останньої сесії.

📄 Клієнт єдиного сервісу криптографічних операцій		Агент ЄСКО 🚯	ECK	ECKO 🚯		
ТОВ Сайфер БІС	В Сайфер БІС			підключено	підклю	чено
00:37:38					JKP RU	S ENG
Особистий ключ Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів	3	
✔ Файл						
Файл для розшифрування:			Перетягніть фай	л чи огляд		
Розшифрувати		Зберегти да	ні у файл	Оч	истити форму	
✓ Текстові дані						
Кодування: 🖲 UTF-16LE 🔿 UTF-8 Зашифровані дані у кодуванні Base64:						
Розшифрувати		Очистити форм	ý			
Розшифрований текст:						
Скопіювати						

Рис. 103. Вкладка «Розшифрувати», розділ «Файл» та «Текстові дані»

Процес розшифрування файлу

Відеоінструкція знаходиться за посиланням.

Для того, щоб розшифрувати файл, у розділі «Файл», необхідно вказати файл для розшифрування та натиснути кнопку «Розшифрувати», Рис. 104.

Після натискання на кнопку «Розшифрувати» з'являється вікно з повідомленням з результатом зашифрування, Рис. 105, де слід натиснути кнопку «ОК» та зберегти розшифровані дані у файл та очистити форму.

Клієнт єдиного сервісу	криптографічних операцій	Агент ЄСКО 🚯	ЄСКО 🚯
ТОВ Сайфер БІС		підключено	підключено
00:34:58			YKP RUS ENG
Особистий ключ Перевірити ЕП Створ	оити ЕП Зашифрувати Розшифрувати	Генерація ключів	
🗸 Файл			
Файл для розшифрування:	logo.png.p7e		Очистити
Розшифрувати	Зберегти дані у файл	Очист	ити форму
Текстові дані			

Рис. 104. Процес розшифрування

Подтвердите действие на странице ccs-dev.cipher.kiev.ua Розшифровані дані успішно отримані. Ок

Процес розшифрування текстових даних

Відеоінструкція знаходиться за посиланням.

Для того, щоб розшифрувати текст, у розділі «Текстові дані», необхідно вказати текст для розшифрування та натиснути кнопку «Розшифрувати», Рис. 106.

Клієнт єдиного сервісу кри	птографічних	Are	нт ЕСКО	ECKO
операцій		підк	лючено	підключено
10В Саифер ЫС 01:32:27			[YKP RUS ENG
Особистий ключ Перевірити ЕП Створити Е	П Зашифрувати	Розшифрувати	Генерація к	лючів
Файл				
Текстові дані				
Кодування:	/vkGSmO9MV8LDTtryM 1utF8TxwgoDEInsjH16ts	It3ISeVeBWMu6YpZ 9JjrpMA3KR042Ww	TIwcAYJKoZIhv vJcpOF/jpcg3Gl	cNAQcBM FbQ6KJdfC
Розшифрувати	Очистити форму			
Розшифрований текст:				
Скопіювати				

Рис. 106. Процес розшифру

Після натискання на кнопку «Розшифрувати» з'являється розшифровані текстові дані у полі «Розшифрований текст», Рис. 107 та очистити форму.

Клієнт єдиного серв	ісу криптографічних			Агент ЄСКО		€C	KO
операцій		підклі	ючено	підкль	очено		
ТОВ Сайфер БІС							
01:32:00						YKP RUS	S ENG
Особистий ключ Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифру	вати	Генерація	ключів	
Файл							
Текстові дані							
Кодування: © UTF-16LE © UTF-8 Зашифровані дані у кодуванні Base64: ggCxSeU6dTqagQsKbn/WGzYMdfreQG1 FsGCyqGJAIBAQEBAQEDMEwECC5vRD6 8Heo2Q4tWTqLBef0BI+bbj6xXkEgAawls	15CVze4RW/vkG 14+ez1BECp1utF8 Zfh9s=	SmO9MV8LDTtryM 3TxwgoDEInsjH16t9	It3ISeVeBWM NjrpMA3KR04	lu6YpZTI 42WvwJo	wcAYJKoZlh pOF/jpcg30	vcNAQcBM 5FbQ6KJdfC	*
Розшифрувати	Очи	стити форму					
Розшифрований текст:							
123							
Скопіювати							



Генерація ключів

Дана функція є доступною і без ключа.

Відеоінструкція знаходиться за посиланням.

Генерація ключів відбувається як у файл на диску так і на захищений носій.

На Рис. 108 показано вкладку «Генерація ключів», а саме вибір профілю. Дана вкладка містить розділ Профіль генерації ключів, які включає у себе:

- Співробітник банку.
- Технолог.
- Посадова особа клієнта iFOBS.
- Клієнт iFOBS (ФОП).
- Користувач ЦСК.
- Організація.

Дані профілі відрізняються один від одного полями та обов'язковими полями.

Клієнт	г єдиного сервісу кр	иптографічних операцій	Агент ЄСКО 🚯	ECKO 🚯
ТОВ Сайф	ер БІС		підключено	підключено
00:32:44				YKP RUS ENG
Особистий ключ	Перевірити ЕП Створити	ЕП Зашифрувати Розшифрувати	Генерація ключів	
	Профіль генерації ключів			
		За замовчуванням		~
	Країна*:	UA		
		Не обов'язкові поля для зап	овнення 🔻	
	CAPTCHA*:			
		Згенерувати ключі Очистити поля		

Рис. 108. Вкладка «Генерація ключів»

Після вибору з переліку необхідного профілю, Рис. 109 (у даному випадку буде розглядатися варіант генерації ключа для співробітника банку).

📻 Клієнт єдиного сервісу криптографічних операцій					Агент ЄСКО 🚯		ЕСКО 🄇	3
ТОВ Сай	фер БІС				підключено	п	ідключе	ено
00:30:20						УКР	RUS	ENG
Особистий ключ	Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів			
	Профіль генераці	ї ключів						
			За замовчуван	ням		~		
	За замовчуванн	ям						
	Співробітник ба	анку						
	Технолог							
	Посадова особа	а клієнта iFOBS						
	Клієнт iFOBS (ФО	ОП)						
	Користувач ЦС	<						
	Організація							

Рис. 109. Вибір профілю генерації ключів

Відкривається форма для заповнення персональних даних власника ключа. Слід звернути увагу, що є обов'язкові поля, якщо їх не вказати буде помилка, і підпис не буде створено. Форма профілю генерації ключів для Співробітника банку для заповнення персональних даних показана на Рис. 110.

Для профілю «Співробітник банку» необхідно вказати логін та пароль до MS Active Directory та натиснути кнопку «Отримати дані з корпоративного каталогу MS Active Directory». За умови, якщо дані не вірні чи не отримані з системи – слід звернутися до адміністратора системи (про це буде повідомлено у вікні).

Після уважного заповнення всіх полів, необхідно звернути увагу на САРТСНА, яку теж необхідно вказати, якщо вона є не розбірливою, праворуч від поля для її введення, є кнопка для її зміни. Наступним кроком є натискання на кнопку «Згенерувати ключі», Рис. 111.

Клієнт	єдиного сервісу к	криптографічних операцій	Агент ЄСКО 🚯	ЕСКО 🚯
ТОВ Сайфе	ер БІС		підключено	підключено
00:13:46				JKP RUS ENG
Особистий ключ	Перевірити ЕП Створ	ити ЕП Зашифрувати Розшифрувати	Генерація ключів	
	Профіль генерації ключів			
		Співробітник банку	```	•
	Користувач	omborchuk		
	Пароль		۲	
	Отримати	и дані з корпоративного каталогу MS Active Di	rectory	
	Повне ім'я*:			
	Прізвище*:			
	Ім'я, по батькові*:			
	РНОКПП*:			
	Країна*:	UA		
	Область*:			
	Населений пункт*:	Львів		
	Адреса*:	вул.Сахарова, 78		
	Організація*:	Банк «Захід»		
	Код ЄДРПОУ*:	33224434]
	Ел.адреса*:			
		Не обов'язкові поля для запо	овнення 🔻	
	CAPTCHA*:	NAIZZ	2	

Рис. 110. Форма для персональних даних

Очистити поля

Згенерувати ключі

👘 Клієнт	т єдиного сер	вісу і	криптогр	афічн	их		Агент ЕСКО		ECK	0
опера	перацій				підключено		підключ	ено		
ТОВ Сайф	ep BIC							ī.,		
									YKP RUS	ENG
Особистий ключ	Перевірити ЕП	Генер	зація ключів							
	Профіль генерації к	лючів								
			Cnispo6	ітник бан	вку			•]	
	Дані з MS AD отр	имано					0			
	Повне іл	via*:	Лось Олег 1	Миколай	ович					
	Kpai	іна*:	UA							
	Ім'я, по батько	osi*:	Олег							
	Населений пу	OCT*:	м.Львів							
	Облас	сть*:	Львівська							
	Адре	sca*:	вул. Сахаро	ова, 78						
	Прізви	ще*:	Лось							
	Зовніш ідентифікат	ний ор*:	omborchuk							
	Поса	цда*:	Начальник	відділу						
	Організа	ція*:	Банк							
	Підроз,	діл*:	Відділ мере	жевої бе	зпеки					
	Паспо	орт*:								
	Еладре	sca*:	omborchuk	@bank.co	om.ua					
			He	е обов'яз	кові поля д	ия запо	внення 🔺			
	Код ДР	ФО:								
	№ запи демографічн рес	су в юму стрі:	0000000-0	0000						
	CAPTCI	HA*:	dren			\odot				
			Згенерувати	ключі	Очистити	поля				

З'являється нове вікно з параметрами нового ключового контейнеру, у залежності від того куди буде збережено ключ, то слід звернути увагу на різницю у параметрах, якщо:

• Збереження відбувається у файл на диску.

Необхідно для поля Тип вказати Файл на диску, для поля Шлях до контейнеру вказати місцерозташування для збереження файлу, для цього слід натиснути «…» та вказати шлях, двічі вказати пароль та натиснути «ОК», Рис. 112.

🖡 Параметри нового ключового контейнера 🛛 🗙 🗙							
Для генерації ключії ключового контейне	в необхідно вибрати тип носія, вказати шлях до ера і пароль						
Тип:	[Файл на диску] 🔹						
Шлях до контейн	C:\Users\Admin\Desktop\Ivanov1990.pfx						
Пароль:	•••••••						
Повторіть пароль:	•••••						
	Пароль повинен містити не менше 8 символів						
	ОК Відмі	іна					

Рис. 112. Збереження ключа у файл на диску

• Збереження відбувається на захищений носій

Необхідно для поля Тип вказати активний чи пасивний режим, для поля Шлях до контейнеру вказати під'єднаний носій для збереження файлу, для цього слід натиснути «…», двічі вказати пароль та натиснути «OK», Рис. 113.

🗐 Параметри нового к	лючового контейнера	×
Для генерації ключів ключового контейне	з необхідно вибрати тип носія, вказати шлях до ера і пароль	
Тип:	[PKCS#11 пристрої]-пасивний режим 🔹	
Шлях до контейн	#. Avtor SecureToken 0	
Пароль:	••••••	
Повторіть пароль:	•••••	
	Пароль повинен містити не менше 8 символів	
	ОК Відмін	на

Рис. 113. Збереження ключа на захищений носій

Після коректного введення всіх даних у вікно «Параметри нового ключового контейнеру» з'являється віно з повідомлення про успішну генерацію ключів, Рис. 114.



Рис. 114. Повідомлення про успішну генерацію ключів

Зміна ключів

Зміна ключів, до закінчення строку дії яких менше 14 днів

Для зміни ключів обов'язкове завантаження Агенту ЄСКО. Далі слід вказати КНЕДП/АЦСК, тип ключа, шлях до контейнера та пароль, Рис. 115.

Після завантаження ключа з'являється повідомлення про виконання зміни ключа, у повідомленні вказано кількість днів до завершення дії ключів, пропонується одразу виконати зміну, Рис. 116.

Клієнт єдиного сер операцій ТОВ Сайфер БІС	Агент ЄСКО підключено	ЄСКО підключено		
Особистий ключ Перевірити ЕП	Генерація ключів			YKP RUS ENG
Параметри сесії	Параметри ключа			
Період активації ключа, хв:	КНЕДП/АЦСК:	Тесто	овий ЦСК Сайфер (п	роксі) 🔻
15	Тип ключа:		[Файл на диску]	Ŧ
	Шлях до контейнеру:	C:\Users\Ad	min\Desktop\zlatar	Вибрати файл
	Пароль:	•••••		۲
	Розпочати роботу з к	лючем	Очистити форму	



Слід зауважити, якщо до звершення строку дії ключів залишається один день, то здійснюється примусова зміна ключів, тобто повідомлення, яке зображене на Рис. 116 не виникає, однак пропонується зміна паролю до ключового контейнеру.

月 Агент єдиного сервісу криптографічних операцій	×
До закінчення дії ключів залишилося менше 7 днів	?
Виконати зміну ключів зараз?	
OK	Відміна

Рис. 116. Повідомлення про закінчення строку дії ключів

Пропонується вказати пароль до ключа двічі до ключового контейнеру, Рис. 117.

Агент єдиного сервісу криптогр	афічних операцій 🛛 🗙
Зміна пароля ключово	ого контейнера
Новий пароль:	Новий пароль
Повторіть новий пароль:	Повторіть новий пароль
	Пароль повинен містити не менше 8 символів
	Змінити пароль Відміна

Рис. 117. Введення паролю до ключового контейнеру

Після вказівки паролю до ключового контейнеру з'являється повідомлення про відправлення запиту на зміну ключа ЕП та шифрування до Центру сертифікації, Рис. 118 та Рис. 119.



Рис. 118. Запит на зміну ключів ЕП успішно відправлений до Центру сертифікації

戻 Агент єдиного сервісу криптографічних операцій	×
Запит на зміну ключів зв'язку успішно відправлений до центру сертифікації	i
	OK

Рис. 119. Запит на зміну ключів зв'язку успішно відправлений до Центру сертифікації

Далі створюється контекст, Рис. 120, з ключем строк дії, якого ще не закінчився, після того як у Центрі сертифікації буде засвідчено запити, то дати до ключа зміняться та не будуть з'влятися повідомлення про повторне відправлення запиту на зміну ключів.

Клієнт єдиного сере		вісу криптографіч	су криптографічних		ECKO			
опера	цій			підключено	підключено			
ТОВ Сайф	ер БІС							
00:14:32					YKP RUS ENG			
Особистий ключ	Перевірити ЕП	Створити ЕП Зашифру	увати Розшифр	увати Генерац	ція ключів			
Дії		Загальна інформація і	про ключ ЕП					
Загальна ін	формація	Повне ім'я	Ібрагімовіч Зл	атан <mark>І</mark> ванович				
Сертифікат кл	юча підпису	Серійний номер 21С40А сертифікату		21C40A52E4D14B5C				
Contubirat valo			11.09.2019, 10					
Сертифікат ключ	Сертифікат ключа шифрування		Закінчення дії 14.09.2019, 00:					
Завершити роб	Завершити роботу з ключем		Посилений Ні					
		Стартовий	Hi					
		Загальна інформація і	про ключ шифрува	ння				
		Повне ім'я	Ібрагімовіч Зл	атан <mark>І</mark> ванович				
		Серійний номер сертифікату	5D6CDB8FE4B	80CB2				
		Початок дії	11.09.2019, 10	9.2019, 10:36:10 GMT+2				
		Закінчення дії	14.09.2019, 00	19, 00:00:00 GMT+2				
		Посилений	Hi					
		Стартовий	Hi					

Рис. 120. Створення контексту з ключем

Зміна стартових ключів

Для зміни ключів обов'язкове завантаження Агенту ЄСКО. Далі слід вказати КНЕДП/АЦСК, тип ключа, шлях до контейнера та пароль, Рис. 121.

Після завантаження ключа з'являється повідомлення про виконання зміни ключа, у повідомленні вказано, що ключі є стартовими, пропонується одразу виконати зміну, Рис. 122.

	Клієнт єдиного сервісу криптографічних	Агент ЄСКО		ECKO		
Le la	операцій	підключено		підключ	ено	
	ТОВ Сайфер БІС					
			УКР	RUS	ENG	

Особистий ключ	Перевірити ЕП	Генерація ключів		
Параметри сесії		Параметри ключа		
Період активації к	люча, хв:	КНЕДП/АЦСК:	Тестовий ЦСК Сайфер (п	роксі) 🔻
15		Тип ключа:	[Файл на диску]	Ŧ
		Шлях до контейнеру:	C:\Users\Admin\Desktop\zlatar	Вибрати файл
		Пароль:	•••••	۲
		Розпочати роботу з кл	ючем Очистити форму	

Рис. 121. Завантаження ключа



Рис. 122. Повідомлення про те, що ключі є стартовими

Пропонується вказати пароль до ключа двічі до ключового контейнеру, Рис. 123.

Агент єдиного сервісу криптогр	афічних операцій	\times
Зміна пароля ключово	ого контейнера	
Новий пароль:	Новий пароль	
Повторіть новий пароль:	Повторіть новий пароль	
	Пароль повинен містити не менше 8 симво	лів
	Змінити пароль Відміна	

Рис. 123. Введення паролю до ключового контейнеру

Після вказівки паролю до ключового контейнеру з'являється повідомлення про відправлення запиту на зміну ключа ЕП та шифрування до Центру сертифікації, Рис. 124 та Рис. 125.

肩 Агент єдиного сервісу криптографічних операцій	×
Запит на зміну ключів ЕП успішно відправлений до центру сертифікації	i
	OK
Рис. 124. Запит на зміну ключів ЕП успішно відправлений до Центру сертиф	кації



Рис. 125. Запит на зміну ключів зв'язку успішно відправлений до Центру сертифікації

Після засвідчення запитів у Центрі сертифікації, можна створювати контекст та працювати з ключем у звичному режимі.

QR-код

QR-код дає можливість отримати результати перевірки ЕП. Для того, щоб отримати код, слід створити ЕП чи перевірити ЕП. Це не залежить від типу підпису чи формату. Для конверту, який містить більше, ніж один підпис формується окремий QR-код.

Створення ЕП

Відеоінструкція доступна за посиланням.

Процес створення ЕП починається з того, що вказуються параметри створення ЕП, обов'язково вказати позначку «Генерація QR», далі завантажується файл для підпису та натискається кнопка «Створити ЕП», Рис. 126.

Клієнт єдиного сер	вісу криптографічних операцій			Агент ЄСКО 🚯		ECKO 🕻	
ТОВ Сайфер БІС				підключено		підключе	но
00:58:56						УКР RUS	ENG
Особистий ключ Перевірити ЕП Параметри створення ЕП	Створити ЕП 🗸 Фай,	Зашифрувати л	Розшифрувати	Генерація клі	ючів		
 Тип підпису Вбудований Відкріплений Формат підпису Базовий (CAdES-BES) З повними даними для перевірки (CAdES-X Long) Додати підпис до вже існуючого Генерація QR 	logo.p	ng Створити ЕП	t Очистити ф	рорму	Теретягн	ніть файл(и) чн огляд	и
	▲ Текс	тові дані					



	Клієнт єдиного сервісу криптографічних операцій	Агент ЄСКО 🚯	ECKO 🄇)
L.	ТОВ Сайфер БІС	підключено	підключе	но
00:58:09			УКР RUS	ENG

Особистий ключ Перевірити ЕП	Створити ЕП 3а	ашифрувати	Розшифрувати	Генерац	ія ключів
Параметри створення ЕП	🗸 Файл				
 Тип підпису Вбудований Відкріплений Формат підпису Базовий (CAdES-BES) З повними даними для перевірки (CAdES-X Long) Додати підпис до вже існуючого Генерація QR 	logo.png Створи	ити ЕП 🎲	Очистити фо	орму	Перетягніть файл(и) чи огляд
	▲ Текстові	дані			

Процес створення підпису відображений на Рис. 127, завершенням процесу є повідомлення про його успішне створення, Рис. 128. У повідомленні зазначається «Електронний підпис успішно створено для 1 файлу».

Ссобистий ключ Пере	Подтвердите действи Електронний підпис успі	іе на странице ccs шно створено для 1	-dev.cipher.kiev.ua файлу(ів). ОК	р	ЄСКО 🛈 підключено УКР RUS ENG
Параметри створення ЕП	👽 Файл	1			
 Тип підпису Вбудований Відкріплений Формат підпису Базовий (CAdES-BES) З повними даними для перевірки (CAdES-X Lo Додати підпис до вже іси 	I одо.рг пд) нуючого	пд	0чистити форму	Перетя	гніть файл(и) чи огляд
Тенерація QK					
	▲ Текс	гові дані			

Рис. 128. Результат створення підпису

Після завершення створення підпису стають доступні позначки, окрім видалення та завантаження підпису, позначка QR-коду, Рис. 129.

Натиснувши на яку відкривається вікно із самим кодом для зчитування та завантаження картинки самого коду, Рис. 130.

Клієнт єдиного сервісу криптографічних операцій			Агент ЄСК	00	ECKO 🚯	
ТОВ Сайфер БІС				підключ	ено	підключено
00:56:19						YKP RUS ENG
Особистий ключ Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація	а ключів	
Параметри створення ЕП	🗸 Файл	л				
 Тип підпису Вбудований Відкріплений Формат підпису Базовий (CAdES-BES) З повними даними для перевірки (CAdES-X Long) Додати підпис до вже існуючого 	logo.p	пд	Очистити ф		Перетя	ягніть файл(и) чи огляд
Генерація QK	л Текс	тові дані				



Рис. 130. QR-код

Перевірка ЕП

Відеоінструкція доступна за посиланням.

Варто зазначити! Кваліфікований електронний підпис вважається тоді, якщо сертифікат отриманий у Кваліфікованого надвача електронних довірчих послуг та ключ згенеровано на захищеному носії чи мережному криптомодулі чи у "хмарі". Якщо, хоча б одна умова не виконується, то підпис не є Кваліфікованим.

Для перевірки заповнюються параметри перевірки ЕП та обов'язкова вказівка позначки «Генерація QR».

При успішній перевірці ЕП з'являється картинка QR-коду (Рис. 131), при натисканні на яку відкривається вікно з кодом для зчитування та завантажування (Рис. 132).



ТОВ Сайфер БІС

00:53:49

Аген	π ECKO 🚯	ECKO 🚯)
під	ключено		ni,	дключе	но
			УКР	RUS	ENG

Особистий ключ	Перевірити ЕП	Створити ЕП	Зашифрувати	Розшифрувати	Генерація ключів	
Параметри переві	рки підпису	🗸 Файл				
 Тип підпису Вбудований Відкріплений Режим перевірк позначки часу для Режим перевірк позначки часу для Режим перевірк Розширення ЕГ Генерація QR 	и електронної підпису и електронної даних	Файл з г Іодо.р Протоко Підпи Дійсни Неква	підписом: ng.p7s ол перевірки с 1 ліфікований	Підписувач: Пупкин (Організація: ТОВ «Са РНОКПП: 1234567890 ЄДРПОУ: 3349855 КНЕДП/АЦСК: ЦСК ТІ Серійний номер сер Дата підпису: 10.12.2 Електронна позначкі Серійний номер сер F2C0270A527AD965 Кваліфікований серт Засіб КЕП: Так Тип засобу КЕП: е. кл	Сергій Петрович йфер PRO») ОВ "Сайфер БІС" гифікату підписанта: 370CDD002E 020, 12:18:45 GMT+2 а часу підпису: дійсна: 10.12.2020, гифікату електронної позначки ч ійфікат: Ні юч Авест AvestKey	Очистити Скопіювати 892С07 12:18:41 GMT+2 насу ЕП:
				Зберегти підпі	исані дані	
			Перевірити В	п	Очистити форм	у

Рис. 131. Результати перевірки ЕП

∧ Текстові дані



Рис. 132. QR-код

Проблемні питання

Очистка кешу у Јаva

Application En	or	×
Unable to	launch the application.	
Name:	Агент единого сервісу криптографічни	
Publisher	Cipher	
Location:	http://caas.infotech.gov.ua	
		Ok Detais

Рис. 133. Помилка при запуску Агента

1 крок - Очистка кешу. Для очистки кешу у середовищі Java необхідно натиснути кнопку «Пуск» та перейти в конфігурування Java-середовища, Рис. 134.

Программы (1)
🕌 Configure Java
Документы (33)
hardware_settings_config
Config.DPLUser
hardware_settings_config
Config.NFS13Save
config.cfg
config.cfg
config_local.cfg
Config
game
🗱 filemappings
DishonoredDLC07
DishonoredDLC06
DishonoredPlayerState
DishonoredAILocomotion
Файлы (2)
ј лог
📋 лог
🔎 Ознакомиться с другими результатами
Confl
Сопії х завершение работы к

Рис. 134. Конфігурування Java-середовища

У відкритій «Панелі управління Java» у вкладці «General» потрібно натиснути кнопку «View», Рис. 135.

🕌 Java Control Panel		_		\times
General Update Java Security Advanced				
About				
View version information about Java Control Panel.				
			A <u>b</u> out.	
Network Settings				
Network settings are used when making Internet connections. By settings in your web browser. Only advanced users should modif	y default, Jav y these settir	a will us ngs.	e the netv	vork
		<u>N</u> etwork	Settings.	
Temporary Internet Files				
Files you use in Java applications are stored in a special folder for advanced users should delete files or modify these settings.	r quick execu	tion late	r. Only	
	Settings.		<u>V</u> iew	
Java in the browser is enabled.			Show t	a lava Ci
See the Security tab			SHOW U	ie Java Ca
	OK	Cance	el <u>k</u>	Apply

Рис. 135. Панель управління Java

Та очистити всі рядки, виділивши їх та натиснути "Delete", Рис. 136.

🕌 Java Cache Viewer					×
Show: Applications V		🔀 🏫 🛛 In	stalled Size: 0.0	0 KB - Cached Siz	e: 216078 KB
Application	Vendor	Remove selected items	Date	Size	Status
Агент единого сервісу крипто	Cipher	Application	10.11.2020	15001 KB	-13-
Агент єдиного сервісу крипто	Cipher	Application	10.11.2020	14995 KB	-10-
Агент единого сервісу крипто	Cipher	Application	10.11.2020	15002 KB	-13-
					Close
					CIOSC

Рис. 136. Видалення кешу

Підтвердити свої дії натисканням «ОК» у «Панелі управління Java».

2 крок - Відключення кешу. Для відключення збереження тимчасових файлів у середовищі Java необхідно натиснути кнопку «Пуск» та перейти в конфігурування Java-середовища, Рис. 137.

Программы (1)
🙆 Configure Java
Документы (33)
hardware_settings_config
Config.DPLUser
hardware_settings_config
config.NFS13Save
Config.cfg
config.cfg
config_local.cfg
🔒 Config
game
i filemappings
DishonoredDLC07
DishonoredDLC06
DishonoredPlayerState
DishonoredAILocomotion
Файлы (2)
П лог
П лог
🔎 Ознакомиться с другими результатами
conf × Завершение работы ►

Рис. 137. Конфігурування Java-середовища

У відкритій «Панелі управління Java» у вкладці «General» потрібно натиснути кнопку «Setting», Рис. 138.

🛓 Java Control Panel		x
General Update Java Security Advanced		
About		
View version information about Java Control Panel.		
	A <u>b</u> out.	
Network Settings		
Network settings are used when making Internet connections. By default, Java will settings in your web browser. Only advanced users should modify these settings.	use the net	twork
Netwo	rk Settings	
Temporary Internet Files		
Files you use in Java applications are stored in a special folder for quick execution advanced users should delete files or modify these settings.	ater. Only	
<u>S</u> ettings	<u>V</u> iew	
Java in the browser is enabled.		
See the Security tab		
OK	el A	pply

Рис. 138. Панель управління Java

Після цього необхідно зняти відмітку з пункту «Keep temporary files on my computer», Рис. 139. Натиснути «OK».

Temporary Files Settings
Keep temporary files on my computer.
Location
Select the location where temporary files are kept:
C:\Users\x\AppData\LocalLow\Sun\Java\Deployment\cache Change
Disk Space Select the compression level for JAR files: None Set the amount of disk space for storing temporary files: 32768 ★
Delete Files Restore Defaults
OK Cancel

Рис. 139. Панель Temporary Files Setting

Підтвердити свої дії натисканням «ОК» у «Панелі управління Java», Рис. 140.

🛃 Java Control Panel	
General Update Java Security Advanced	
About	
View version information about Java Control Panel.	
	About
Network Settings	
Network settings are used when making Internet connections. By default, Java wil settings in your web browser. Only advanced users should modify these settings.	use the network
Netwo	rk Settings
Temporary Internet Files	
Files you use in Java applications are stored in a special folder for quick execution l advanced users should delete files or modify these settings.	later. Only
<u>S</u> ettings	<u>V</u> iew
Java in the browser is enabled.	
See the Security tab	
OK Can	el Apply

Рис. 140. Панель управління Java

Не відображається захищений носій в ОС Windows

Рішення проблеми:

Для роботи с операційними системами, починаючи з Windows 7 (Windows 8, 10, Server 2008) і вище, зазвичай не потрібні додаткові драйвери, вони вже додані в систему за замовчуванням. Про те, в деяких випадках, операційна система некоректно встановлює драйвери для носія. В цьому випадку їх необхідно інсталювати самостійно.

Для цього, необхідно вставити захищенний носій в USB-роз'єм комп'ютера.

Після того, як операційна система визначить новий пристрій, він відобразиться в «Диспетчере устройств» як «Другое устройство».

Для встановлення драйверу, необхідно натиснути правою кнопкою миші на пристрої (для приклада наведений носій Avtor SecureToken) та обрати пункт меню «Обновить драйвер...», Рис. 141.



Рис. 141. Панель «Диспетчер устройств» ОС Windowc XP

У вікні "Мастер обновления оборудования", яке відкриється, необхідно обрати пункт меню «Нет, не в этот раз» та натиснути «Далее», Рис.142.



Рис. 142. Вікно "Мастер обновления оборудования"

В наступному вікні необхідно обрати «Установка из указанного места», натиснути «Далее», Рис.143.


Рис. 143. Вікно "Мастер обновления оборудования"

Після цього потрібно обрати директорію, де знаходиться каталог з драйвером для носія (заздалегідь архів з драйверами driver_for_XP-7-10.zip необхідно завантажити на ПК та розархівувати), Рис. 144.

🚇 Диспетчер устройств		
Консоль Действие Вид	Справка	
	🗉 🙁 🕿 😹	
Мастер обновления о	борудования	
Задайте параметры	Обзор папок 🔹 🔀 🌄	
	Выберите папку, содержащую драйверы для этого оборудования.	
📀 Выполнить поис		
Используйте фл	😰 Рабочий стол 🔉 🕅	
по умолчанию ло подходящий дра	🗄 🛄 Мои документы 🛛 🗧 Ве	
🗹 Поиск на (🟵 🕺 Сетевое окружение	
🗹 Включить	😂 x86	
C:\Docum		
О Не выполнять п		
Этот переключа	A	
Windows не мож подходящим доя	для просмотра подпалок щелкните по плюсику.	
	ОК Отмена _	
	 < Назад Далее > Отмена 	

Рис. 144. Вибір каталогу, в який розархівовано драйвери для носія

Після цього необхідно натиснути «Далее». Майстер налаштування обладнання ОС автоматично встановить драйвера для захищего носія, Рис. 145-147.



Рис. 145. Процес автоматичного пошуку драйверів для носія



Рис. 146. Процес встановлення драйверів для носія



Рис. 147. Завершення процесу встановлення драйверів для носія

Далі необхідно натиснути «Готово». Після цього, у вікні «Диспетчер устройств» повинен відобразитись носій, Рис. 148.



Рис. 148. Вікно «Диспетчер устройств»

Також необхідно перевірити роботу служби «Смарт-карта». Для цього необхідно натиснути правою кнопкою миші на «Этот компьютер» та обрати пункт меню «Управление», Рис. 149.



Рис. 149. Вікно «Диспетчер устройств»

У вікні «Управление компьютером», Рис. 150. необхідно обрати розділ «Службы и приложения», далі перейти в розділ «Службы», Рис. 151.



Рис. 150. Вікно «Управление компьютером»

Управление компьютером							-		×
<u>Фаил Деиствие вид с</u> прав	ka								
🗢 🔿 🖾 🚾 😣 🖬 🛛									
🌆 Управление компьютером (л	О. Службы							Дейст	яия
 Служебные программы Планировщик заданий Просмотр событий Просмотр событий Общие папки Локальные пользоватк Производительность Диспетчер устройст Запоминающие устройст Службы Службы Управлянощий элемен 	Чтобы просмотреть описание элемента, выделите его.	Имя Agent Activation Runtime_40146 AnyDesk Service BranchCache CaptureService_40146 Cisco AnyConnect Secure Mobili CorsentUX_40146 Corel License Validation Service V Corelexes Validation Service V CoredentialEnrollmentManagerUs DeviceAssociationBroker_40146 DevicePicker_40146	Описание Runtime fo AnyDesk s Эта служб Включает Cisco Any Позволяет This servic Manages c Диспетчер Enables ap Эта польз	Состояние Выполняется Выполняется Выполняется Выполняется Выполняется	Тип запуска Вручную Автоматиче Вручную Вручную Автоматиче Вручную Автоматиче Вручную Вручную Вручную	Вход от имени Локальная сис Локальная сис Сетевая служба Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис	^	Служб Дс	a A
		Q. DevicesFlow_40146 Q. DHCP-клиент Q. DialogBlockingService Q. DialogBlockingService Q. DialogBlockingService Q. ESET HTTP Server Q. ESET SHA Service Q. ESET SHA Service Q. Google Chrome Elevation Service Q. Google Undate Service (audate)	Позволяет Регистрир Еxecutes di Служба б Служба D ESET MTTP ESET Service ESET Syste Keeps your	Выполняется Выполняется Выполняется	Вручную Автоматиче Вручную (ак Отключена Автоматиче Вручную Автоматиче Вручную Автоматиче	Локальная сис Локальная слу Локальная сис Оскальная сис Сетевая служба Сетевая служба Локальная сис Локальная сис Локальная сис			
	Decumentary of Contract, of	Gogle Update Service (gupdate GraphicsPerfSvc GraphicsPerfSvc Intel(R) Content Protection HDC Intel(R) Content Protection HECI Intel(R) Dynamic Application Loa Intel(R) Graphics Command Cent	Keeps your Graphics p Version: 1.6 Intel(R) Co Intel(R) Co Intel(R) Dy Service for	Выполняется Выполняется Выполняется Выполняется	Вручную Вручную (ак Вручную Автоматиче Вручную Автоматиче	Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис Локальная сис	~	-	
< >>	\Расширенный / Стандартный /							1	

Рис. 151. Вікно «Службы»

Після цього необхідно знайти службу «Смарт-карта», натиснути на ній правою кнопкою миші, обрати «Свойства», Рис. 152

🔠 Управление компьютером							-		×
Файл Действие Вид Справ	ка								
🗢 🄿 🙇 🖬 🗐 🙆	2 📷 🕨 🗉 🕪								
🌆 Управление компьютером (л	🔍 Службы							Действия	
 Служебные программы Планировщик заданий 	Смарт-карта	Имя	Описание	Состояние	Тип запуска	Вход от имени	^	Службы	•
> 🚺 Просмотр событий	Запустить службу	Служба установки Microso Спокба установки устрой	oft St Обеспечи	Выполняется	Вручную Вручную (ак	Локальная сис Локальная сис		Допо	•••••
> 👔 Общие папки		Служба хранения данных	поль Обеспечи		Вручную (ак	Локальная сис		Смарт-ка.	🔺
Производительность	Описание:	🚇 Служба хранилища	Предостав	Выполняется	Автоматиче	Локальная сис		Допо	
🛔 Диспетчер устройств	Управляет доступом к устройствам	🤹 Служба шифрования диск	ков Bi BDESVC пр		Вручную (ак	Локальная сис			
🛚 🗸 📴 Запоминающие устройст	чтения смарт-карт. Если эта служба	🖏 Служба шлюза уровня пр	илож Обеспечи		Вручную	Локальная слу			
📰 Управление дисками	сможет считывать смарт-карты.	🎑 Службы криптографии	Предостав	Выполняется	Автоматиче	Сетевая служба			
🗸 🖕 Службы и приложения	Если эта служба отключена, любые	🧛 Службы удаленных рабоч	них ст Разрешает		Вручную	Сетевая служба			
Службы	служоы, которые явно зависят от нее не могут быть запушены.	😳 Смарт-карта	Запустить		Вручную (ак	Локальная слу			
правляющии элемен		😪 События получения н	Остановить		Вручную	Локальная сис			
		Сопоставитель конечн		олняется	Автоматиче	Сетевая служба			
		🤐 Сохранение игр на Хb	приостановить		Вручную (ак	Локальная сис			
		Средство построения	Продолжить	рлняется	Автоматиче	Локальная сис			
		Стандартная служба с Стандартная служба с	Перезапустить		вручную	Локальная сис			
		од телефония Од телефония	Все задачи	>	вручную	Сетевая служоа			
1		Пелефонная связь			бручную (ак	Локальная слу			
			Обновить	блияется	Renality and	Локальная сис			
			Свойства		Вручную	Локальная сис			
		О Удаденный вызов про		DOWDETCO	Автоматиче	Сетевая спохба			
6		Одаленный реестр — — — — — — — — — — — — — — — — — — —	Справка		Отключена	Локальная слу			
		Удостоверение приложен	ия Определя		Вручную (ак	Локальная слу			
		Узел системы диагностики	и Узел систе		Вручную	Локальная сис			
1		🕵 Узел службы диагностики	Узел служ	Выполняется	Вручную	Локальная слу	- 11		
		Узел универсальных PNP-	устр Позволяет		Вручную	Локальная слу			
4		🤹 Управление приложениям	ли Обработк		Вручную	Локальная сис			
		🖏 Управление уровнями хра	нили Оптимизи		Вручную	Локальная сис			
		🖏 Установщик ActiveX (AxIns	stSV) Обеспечи		Вручную	Локальная сис	~		
< >	Расширенный Стандартный /								
Открытие окна свойств выбранно	го объекта.								

Рис. 152. Меню служби «Смарт-карта»

У вікні «Свойства Смарт-карта» необхідно натиснути на кнопку «Запустить», Рис. 153, а також обрати Тип запуска - «Автоматически», Рис. 154.

Свойства: Смарт-карта (Локальный компьютер)									
Общие	Вход в си	стему	стему Восстановление Зависимости						
Имя сл	іужбы:	SCard S	òvr						
Отобра имя:	жаемое	Смарт-карта							
Описание:		Управляет доступом к устройствам чтения смарт-карт. Если эта служба остановлена, этот компьютер не сможет считывать смарт-карты.							
		Если з	та служба отключе	на, любые служ	(бы, 🍐	^			
Исполн	няемый фа	айл:							
C:\Win	dows\syste	em32\sv	chost.exe -k LocalSe	erviceAndNoImpe	ersonation				
<u>Т</u> ип за	пуска:	Вручн	ую		`	1			
						_			
Состоя	ние:	Остано	влена						
Запустить Остановить Приостановить Продолжить									
Вы можете указать параметры запуска, применяемые при запуске службы из этого диалогового окна.									
Параметры <u>з</u> апуска:									
			ОК	Отмена	При <u>м</u> ен	нить			

Рис. 153. Вікно «Свойства: Смарт-карта»

Свойства: Смарт-карта (Локальный компьютер)						×		
Общие	Вход в с	истему	Восстановление	ановление Зависимост				
Имясл	Имя службы:		SCardSvr					
Отобра имя:	ажаемое	Смарт-карта						
Описание:		Управляет доступом к устройствам чтения смарт-карт. Если эта служба остановлена, этот компьютер не сможет считывать смарт-карты. Если эта служба отключена, любые службы,						
Исполн	няемый ф	айл:						
C:\Win	dows\syste	em32∖sv	chost.exe -k LocalS	erviceAndNoIr	npersonation			
<u>Т</u> ип за	пуска:	Вручную 🗸						
			атически (отложен	ный запуск)				
Состоя	ние:	Вручную Отключена						
3a <u>n</u>	устить	О <u>с</u> та	Остановить Приостановить Прододжить					
Вы можете указать параметры запуска, применяемые при запуске службы из этого диалогового окна.								
Параметры <u>з</u> апуска:								
			ОК	Отмена	При <u>м</u> енит	њ		

Рис. 154. Налаштування типу запуску служби «Смарт-карта»

Після цього необхідно підтвердити збереження обраних параметрів натисканням «ОК».

No labels