**Технічні умови**

**подання Фондом гарантування вкладів фізичних осіб інформації**

**для ведення Кредитного реєстру Національного банку України (**КР2**)**

Ці технічні умови (далі – ТУ) визначають вимоги щодо подання Фондом гарантування вкладів фізичних осіб (далі – ФГВФО) даних про активні операції банків, щодо яких Національним банком України (далі – НБУ) прийнято рішення про віднесення їх до категорії неплатоспроможних або про відкликання банківської ліцензії та ліквідацію (далі - банк) згідно з Правилами надання Фондом гарантування вкладів фізичних осіб інформації до Кредитного реєстру Національного банку України №8 від 22.01.24 та Положенням про Кредитний реєстр Національного банку України (затверджене постановою Правління Національного банку України від 04 травня 2018 року № 50 зі змінами).

1. Загальні положення
	1. Інформаційний обмін між ФГВФО і інформаційною системою Національного банку України (далі – Система) накопичення звітності про активні операції банків та ведення Кредитного реєстру здійснюється згідно технології REST API.
	2. Передавання інформації між ФГВФО та НБУ повинно здійснюватися із використанням механізмів захисту інформації – автентифікації, конфіденційності та контролю цілісності.
	3. Для підтвердження автентичності та цілісності інформації використовується електронний підпис (далі – ЕП), вимоги до якого наведено у розділі 2.
	4. Система проводить автентифікацію та авторизацію ФГВФО використовуючи криптографічний протокол TLS (Transport Layer Security), вимоги до налаштування якого наведено нижче.
	5. Усі повідомлення інформаційного обміну мають формуватися з використанням формату JSON та відповідати формалізованому опису, визначеному у JSON – схемі.
	6. Порядок отримання JSON – схем наведено у розділі 12. У всіх повідомленнях використовується кодування символів UTF-8.
2. Вимоги до забезпечення цілісності інформації
	1. Для виконання операцій накладання та перевірки ЕП, ФГВФО може використовувати бібліотеки СКЗІ НБУ, а саме криптопровайдер NbuCSP, (наданий НБУ, з відповідною документацією), або інші бібліотеки, погоджені до використання з управлінням безпеки інформації Департаменту безпеки НБУ.
	2. ЕП накладається відповідно до вимог описаних в стандарті RFC 7515 – JSON Web Signature (JWS), використовується тип серіалізації Flattened JWS JSON Serialization.

Отриманий JWS JSON об’єкт, має містити такі вкладені об’єкти, що подаються у закодованому за допомогою Base64Url кодування (стандарт RFC 4648) вигляді:

* “payload” – об’єкт в якому передаються дані;
* “protected” – об’єкт, що містить захищений заголовок повідомлення;
* “signature” – значення ЕП.

**Приклад JWS, що використовує Flattened JWS JSON Serialization серіалізацію:**

|  |
| --- |
| {“payload” : ”EFycmF5T2ZURVNUVEFCIHhtbG5zOmk9Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvWE1MU2NoZW1hLWluc3RhbmNlIiB4bWxucz0iaHR0cDovL3NjaGVtYXMuZGF0YWNvbnRyYWN0Lm9yZy8yMDA0LzA3L0NyZWRSZWVzdHJfREJNb2RlbCI-PFRFU1RUQUIgaTp0eXBlPSJURVNUVEFC”,“protected” : ”NDwvVEFCX0lEPjxUQUJfVEVYVD7QnNCG0JrQntCb0JDQh9CE0pA8L1RBQl9URVhUPjwvVEVTVFRBQj48VEVTVFRBQiBpOnR5cGU9IlRFU1RUQUIiPjxUQUJ”,“signature” : “NCG0JrQntCb0JDQh9CE0pA8L1RBQl9URVhUPjwvVEVT”} |

Опис реквізитів об’єкта “protected” (в якому передається захищений заголовок повідомлень), що використовуються в Системі (усі реквізити є обов’язковими).

|  |  |  |
| --- | --- | --- |
| Найменування реквізиту | Зміст | Значення |
| alg | Криптографічний алгоритм який використано при створенні JWS об'єкту | RS512 |
| typ | Тип серіалізації JWS | JOSE+JSON |
| cty | Тип контенту JWS об'єкту | application/json |
| x5c | Масив строк, що містить один елемент, а саме: закодоване за допомогою Base64 кодування DER значення сертифіката, яке містить відкритий ключ, відповідний використаному для підпису закритому ключу. | Приклад:[“MIIHBDCCBOygAwIBAgIUBr3………IWD6NEdQyzpoxTCAdVXag56zqjLn”] |
| kid | Ідентифікатор ключа користувача, що використаний для підпису | XRxxPCRnnn |
| dateOper | Дата створення повідомлення | Дата у форматі D(19)[[1]](#footnote-1) |
| appId | Ідентифікатор інформаційної системи | PCR |

1. Вимоги до використання криптографічного протоколу TLS та відповідних сертифікатів відкритих ключів
	1. Система використовує клієнт-серверну технологію. ФГВФО виступає в якості клієнта, НБУ в якості серверу.
	2. Клієнт та Сервер (далі – Сторони) для встановлення захищеного з’єднання повинні використовувати криптографічний протокол TLS версії 1.2 або вище. Підтримка протоколу SSL будь якої версії або протоколу TLS версій 1.0 або 1.1 повинна бути відключена.
	3. Пріоритет у виборі криптографічних наборів при встановленні з’єднання визначається Сервером, незалежно від пріоритетів, визначених клієнтом.
	4. Клієнт повинен підтримувати один або кілька криптографічних наборів, визначених у пункті 3.9.
	5. Для шифрування інформації повинні використовуватись симетричні криптографічні алгоритми з довжиною ключа не менше 128 біт.
	6. Довжина відкритого ключа RSA повинна бути не меншою 2048 біт.
	7. Заборонено використовувати криптографічні набори які використовують попередньо узгоджений загальний секретний ключ (PSK).
	8. Для узгодження сеансових ключів використовуються протоколи DHE та ECDHE. Довжина відкритого ключа для протоколу DH повинна бути не меншою 2048 біт. Довжина відкритого ключа для протоколу ECDHE повинна бути не меншою 256 біт.
	9. Сторони можуть використовувати виключно наступні криптографічні набори:

|  |  |
| --- | --- |
| **TLS 1.3** |  |
| 1 | TLS\_AES\_256\_GCM\_SHA384 |
| 2 | TLS\_AES\_128\_СCM\_SHA256 |
| 3 | TLS\_AES\_128\_GCM\_SHA256 |
| **TLS 1.2** |  |
| 1 | ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 |
| 2 | ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 |
| 3 | DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 |
| 4 | ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 |
| 5 | ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 |
| 6 | DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 |

1. Номенклатура ключів, що використовуються

При взаємодії ФГВФО та Системою, ФГВФО має використовувати два ключі (які мають різні ідентифікатори), перший для накладання ЕП на повідомлення, що формуються, другий для шифрування SSL-з’єднання між ФГВФО та Системою, наприклад, для учасника з 3-символьним ідентифікатором Rxx ідентифікатори користувача СКЗІ НБУ матимуть вигляд XRxxPCR000 та XRxxPCR001.

Ідентифікатори ключів формуються за маскою:

X**RxxP**CR**nnn**

де:

X – константа, ознака зовнішнього користувача інформаційної мережі НБУ;

***Rxx*** – унікальний ідентифікатор Учасника в СКЗІ НБУ;

PCR – константа, тип інформаційної задачі;

***nnn*** – порядковий номер робочого місця, що взаємодії з Системою.

Якщо ФГВФО використовує більш ніж одне робоче місце, кожне з них використовує власні ідентифікатори ключів, які відрізняється номером робочого місця.

Ідентифікатор ключа, сформований за даними правилами, вміщується в реквізит "Common Name" поля сертифіката Subject та в розширення сертифікату "Subject Alternative Names” з OID 1.3.6.1.4.1.311.20.2.3 (User Principal Name (UPN)).

У разі генерації нового сертифікату відкритого ключа попередній сертифікат з тим самим ідентифікатором скасовується, і таким чином новий сертифікат "заміщує" старий.

1. Порядок забезпечення ключовою системою

Генерація таємного ключа для робочого місця здійснюється засобами модуля генерації ключів (МГК), згідно до п.3 Інструкції з використання програмно-апаратного модулю генерації криптографічних ключів СЕП та інформаційних задач для отримання «SSL-сертифікатів».

Для забезпечення процесу генерації/сертифікації ключів засобами МГК для тестового середовища використовується сервер тестового АЦСК НБУ, для продуктивного – сервер АЦСК НБУ.

Кореневі сертифікати АЦСК НБУ (тестового АЦСК НБУ) розсилаються централізовано або їх можна скачати з відповідних сайтів АЦСК (тестового АЦСК) НБУ.

1. Опис роботи Системи
	1. Система використовує клієнт-серверну технологію. ФГВФО відправляє та отримує інформацію за допомогою HTTP-запитів (POST, GET) до відповідних вебсервісів.
	2. Для тестування і відпрацювання технології інформаційної взаємодії між системами автоматизації ФГВФО з Системою розгорнуто тестові вебсервіси.
	3. Взаємодія з вебсервісами відбувається за адресами: **i0pcr1.**extern.bank.gov.ua– для продуктивного середовища і **https://i0pcrt1**.extern.bank.gov.ua – для тестового середовища. (Далі по тексту замість зазначених конкретних адрес використовується змінна **cr\_server**).Для коректної роботи з вебсервісами банкам необхідно виконати відповідні мережеві налаштування згідно з інструкцією, наданою у Додатку 2.

1. Подання інформації до Системи
	1. На стороні НБУ для прийому інформації від ФГВФО та надання інформації ФГВФО налаштовано вебсервіс: 1) вебсервіс «Пакет» (загальний пакет), 2) вебсервіс «Перевірка статусу» (Перевірка статусу обробки вхідного повідомлення)**.**
	2. ФГВФО надає інформацію до НБУ у розрізі банків. (При наданні інформації вказується МФО).
	3. ФГВФО формує повідомлення та надсилає його у запиті типу POST на відповідний вебсервіс.
	4. Запит, що надходить до вебсервісу, проходить декілька етапів обробки, на яких він може бути відхилений:

1) автентифікація, авторизація, перевірка цілісності інформації (верифікація електронного підпису), перевірка поданої інформації в запиті на відповідність JSON-схемі;

2) перевірка поданої інформації в запиті на відповідність правилам контролю, викладеним у (посилання на контролі).

* 1. Якщо запит не пройде перевірки першого етапу, то ФГВФО одразу у відповіді на запит отримає повідомлення про помилку і сеанс завершується. Усю інформацію у запиті буде відхиллено (див. приклад нижче).

**Приклад відповіді на запит типу POST у разі неуспішної обробки на першому етапі (містить код стану HTTP та короткий опис)**

|  |
| --- |
| **HTTP/**1.1 422 JSON Schema Validation ErrorContent-Type: application/jsonTransactionId: 452304SessionId: 332eb9e3b9f64b7af1570651f8aac8d27f354470612e03d25bba38d48dd678feX-Backside-Transport: FAIL FAILConnection: close{"errMessage":"[JSV0013] Invalid value: the value is not among the permitted enumerated values."} |

Короткий текстовий опис у відповіді може відрізнятись від наведеного в прикладі.

* 1. Якщо запит успішно пройде перевірки першого етапу, то ФГВФО одразу у відповіді на запит (тобто у поточному сеансі) отримає повідомлення з унікальним ідентифікатором пакету {package\_id} і сеанс завершується.
	2. Отримання ФГВФО ідентифікатору пакету свідчить про початок другого етапу перевірки.
	3. Другий етап перевірки відбувається в асинхронному режимі. Подальший результат обробки пакету на другому етапі перевірки ФГВФО може дізнатись, надіславши запит (тип GET) на вебсервіс «Перевірка статусу», використовуючи ідентифікатор пакету (див. приклад нижче п.).
	4. Від вебсервісу «Перевірка статусу» ФГВФО може отримати такі варіанти відповіді (де змінна {package\_id} є значенням Ідентифікатору пакету):
* **NotFound** – це говорить про те, що повідомлення за ідентифікатором {package\_id} не знайдено або вказаний ідентифікатор є невірним;
* **InProgress** – це говорить про те, що повідомлення за ідентифікатором {package\_id} знаходиться в обробці.
* **Passed** – це говорить про те, що повідомлення за ідентифікатором {package\_id} оброблено успішно, інформацію прийнято.
* **Failed** – це говорить про те, що повідомлення за ідентифікатором {package\_id} оброблено з помилками, інформацію не прийнято; (відповідь також буде включати перелік перших 10 помилок).
* **Unprocessable** – це говорить про те, що на стороні Системи сталася непередбачувана помилка обробки повідомлення за ідентифікатором {package\_id}. Необхідно відправити лист з інформацією про отримання даного статусу на скриньку pcr@bank.gov.ua та очікувати на подальші інструкції.
1. Загальна структура повідомлень, що надходять від ФГВФО до НБУ.

**Повідомлення (запит) типу POST.**

**Подання інформації до вебсервісу /cr2\_fond/api/v1/main\_pkg**

|  |
| --- |
| **POST** **https://cr\_server/cr2\_fond/api/v1/main\_pkg**Content-Type: application/json{“payload” : ”EFycmF5T2ZURVNUVEFCIHhtbG5zOmk9Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvWE1MU2NoZW1hLWluc3RhbmNlIiB4bWxucz0iaHR0cDovL3NjaGVtYXMuZGF0YWNvbnRyYWN0Lm9yZy8yMDA0LzA3L0NyZWRSZWVzdHJfREJNb2RlbCI-PFRFU1RUQUIgaTp0eXBlPSJURVNUVEFC”,“protected” : ”NDwvVEFCX0lEPjxUQUJfVEVYVD7QnNCG0JrQntCb0JDQh9CE0pA8L1RBQl9URVhUPjwvVEVTVFRBQj48VEVTVFRBQiBpOnR5cGU9IlRFU1RUQUIiPjxUQUJ”,“header” : null,“signature” : “NCG0JrQntCb0JDQh9CE0pA8L1RBQl9URVhUPjwvVEVT”} |

**Повідомлення (запит) типу GET.**

**Перевірка статусу обробки повідомлення (де змінна {package\_id} є значенням ідентифікатору запиту, що надається у відповідь в разі успішного проходження перевірок першого етапу).**

|  |
| --- |
| **GET** **cr\_server/cr2\_status/api/v1/request\_status/{package\_id}** Content-Type: application/json |

1. Опис форматів даних, що використовуються у повідомленнях.

|  |  |  |  |
| --- | --- | --- | --- |
| **Тип даних** | **Формат даних** | **Опис вимог до подання типу даних** | **Можливі допустимі значення** |
| Символьний **String** | C(10), або С(3:25) | Набуває значення набір (рядок) символів у вигляді а) C(Y) де Y-максимальна кількість символів, або C(X:Y) де X-мінімальна кількість символів,Y-максимальна кількість символів | “asdf” “ddf%#\_ “ “         “ “23456” “1900-02-15” “0” null. |
| Числовий **Number** | N(2) або N(7,4) | Набуває значення «число» у вигляді N(2), де 2-ціле число де кількість цифр у числі не більше 2 або N(7,4) де 7- ціле число де кількість цифр у числі не більше 7 та кількість цифр у числі після крапки не більше 4. | 1 2 324 -526 125.25 0.0000578, додатково може бути розширене значенням null. |
| Логічний **Boolean** | B | Набуває одного з визначеного переліку значень true або false | true, false, додатково може бути розширене значенням null. |
| Дата, ISO 8601 **Date** | D(10) | Набуває значення у форматі “YYYY-MM-DD”, де: YYYY – рік (чотири цифри), MM –місяць (дві цифри), DD – день (дві цифри). Наприклад: 2015-05-19 означає 19 травня 2015 року | “1900-02-15” “2000-08-24”, додатково може бути розширене значенням null. |
|
| Комбіновані дата й час, ISO 8601 **Date** | D(19) | Набуває значення у форматі “yyyy-MM-ddTHH:mm:ss ”, де: yyyy – рік (чотири цифри), MM – місяць (дві цифри), dd – день (дві цифри), HH –годин,mm – хвилин, ss – секунд Наприклад: 2015-05-19 означає 19 травня 2015 року 2015-05-19T15:22:37 | “2015-05-19T15:22:37”, в деяких випадках може містити долі секунд [sssss], додатково може бути розширене значенням null. |

1. Загальна структура повідомлення, що отримує ФГВФО у відповідь на свій запит у разі його успішної обробки.
	1. Інформацію про відповіді від вебсервісу, що може отримати клієнт у разі не успішної обробки запиту в залежності від етапу наведено в Додатку 1.
	2. Інформація про відповіді від вебсервісу у разі успішної обробки запиту в залежності від типу запиту:

|  |  |  |  |
| --- | --- | --- | --- |
| **Тип запиту** | **Опис запиту** | **Код стану HTTP** | **Інформація про відповідь** |
| POST | Створення нового запису | 201 | Відповідь містить код стану HTTP та квитанцію з результатом виконання операції; квитанція надається у вигляді підписаного JWS об’єкта. |

**Приклад відповіді на запит типу POST від вебсервісу «Пакет» в разі успішної обробки на першому етапі**

|  |
| --- |
| **HTTP/**1.1 201 OKX-Backside-Transport: OK OKConnection: Keep-AliveTransfer-Encoding: chunkedTransactionId: 297312SessionId: f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66X-Global-Transaction-ID: 055a38136548fbdf00048960Content-Type: application/json{"package\_id":"f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66","web\_service\_url":"https://172.22.3.17:8160/cr2\_banks/api/v1/main\_pkg","http\_method":"POST","client\_ip":"10.81.17.60","client\_ssl\_cert\_id":"XY12PCR001","client\_sign\_cert\_id":"XY12PCR002","general\_http\_status\_code":201,"kvi\_date":"2023-11-06T14:44:47.587Z"} |

* 1. Реквізити відповіді за результатами роботи відповідного сервісу (запит типу POST):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №з/п | Зміст реквізиту | Найменування реквізиту  | Тип (макс.дов-жина) | Обов’язковість заповнення | Примітки |
| 1 | Унікальний ідентифікатор пакету, що було надіслано Банком | package\_id | С(64) | + |  |
| 2 | Адреса вебсервіса, яким було оброблено інформацію | web\_service\_url | C(100) | + |  |
| 3 | Http метод запиту | http\_method | C(15) | + |  |
| 4 | IP адреса з якої було здійснено запит | client\_ip | C(15) | + |  |
| 5 | Ідентифікатор сертифіката, який був використаний для встановлення захищеного з’єднання | client\_ssl\_cert\_id | C(10) | + |  |
| 6 | Ідентифікатор ключа користувача, що був використаний для підпису | client\_sign\_cert\_id | C(10) | + |  |
| 7 | Код стану HTTP | general\_http\_status\_code | N(3) | + | Частина першого рядка відповіді сервера при запитах по протоколу HTTP (HttpStatusCode). |
| 9 | Дата та час формування квитанції | kvi\_date | D(19) | + | Дата та час у форматі YYYY-MM-DDThh:mm:ss[.sssss] |

**Приклад відповіді на запит типу GET від вебсервісу «Перевірка статусу» в разі обробки повідомлення з помилками**

|  |
| --- |
| **HTTP/**1.1 424X-Backside-Transport: OK OKConnection: Keep-AliveTransfer-Encoding: chunkedTransactionId: 297222SessionId: f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66X-Global-Transaction-ID: 055a38136548fbdf00048960Content-Type: application/json{  "status": "Failed",  "package\_id": "3ebf12de-9803-418d-88a8-54882d2a9e1c", "response\_timestamp": "2023-11-10T10:00:20.7276661Z",  "control\_errors": [    {      "error\_number": 1,      "error\_id": "00008:01.03",      "error\_code": "00008",      "error\_nesting": [        {          "data\_set\_name": "person\_full",          "data\_set\_index": 1,          "data\_set\_id": "111"        },        {          "data\_set\_name": "address",          "data\_set\_index": 0,          "data\_set\_id": null        }      ]    },    {      "error\_number": 2,      "error\_id": "05112:01.04",      "error\_code": "05112",      "error\_nesting": [        {          "data\_set\_name": "person\_full",          "data\_set\_index": 1,          "data\_set\_id": "111"        },        {          "data\_set\_name": "rating",          "data\_set\_index": 5,          "data\_set\_id": null        }      ]    }  ]} |

**Приклад відповіді на запит типу GET від вебсервісу «Перевірка статусу» в разі, коли повідомлення за ідентифікатором пакету не знайдено**

|  |
| --- |
| **HTTP/**1.1 404X-Backside-Transport: OK OKConnection: Keep-AliveTransfer-Encoding: chunkedTransactionId: 297222SessionId: f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66X-Global-Transaction-ID: 055a38136548fbdf00048960Content-Type: application/json{  "status": "NotFound",  "package\_id": "3ebf12de-9803-418d-88a8-54882d2a9e1c", "response\_timestamp": "2023-11-10T10:00:20.7276661Z"} |

**Приклад відповіді на запит типу GET від вебсервісу «Перевірка статусу» в разі успішної обробки повідомлення (інформацію прийнято)**

|  |
| --- |
| **HTTP/**1.1 200X-Backside-Transport: OK OKConnection: Keep-AliveTransfer-Encoding: chunkedTransactionId: 297222SessionId: f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66X-Global-Transaction-ID: 055a38136548fbdf00048960Content-Type: application/json{  "status": "Passed",  "package\_id": "3ebf12de-9803-418d-88a8-54882d2a9e1c", "response\_timestamp": "2023-11-10T10:00:20.7276661Z"} |

* 1. Реквізити відповіді за результатами роботи вебсервісу «Перевірка статусу»:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №з/п | Зміст реквізиту | Найменування реквізиту  | Тип (макс.дов-жина) | Обов’язковість заповнення | Примітки |
| 1 | Статус обробки пакету | status | С(8) | + | Набуває одне із значень:**NotFound****InProgress****Passed****Failed****Unprocessable** |
| 2 | Унікальний ідентифікатор пакету, що було надіслано Респондентом | package\_id | С(64) | + |  |
| 3 | Дата та час формування відповіді | response\_timestamp | D(19) | + | Дата та час у форматі YYYY-MM-DDThh:mm:ss[.sssss] |
| 4. Перелік помилок. Структура (масив) **control\_errors**. Якщо помилок кілька, то поля з 4.1. по 4.3. повторюються та є обов’язковими. Якщо помилок немає, структура (масив) **control\_errors** не зазначається. |
| 4.1 | Порядковий номер помилки | error\_number | N(2) | + |  |
| 4.2 | Узагальнений ідентифікатор помили відповідно до опису Контролів (посилання на Контролі) | error\_id | С(64) | + |  |
| 4.3 | Код помилки, відповідно до опису Контролів (посилання на Контролі) | error\_code | С(64) | + |  |
| 4.4 Реквізити, в яких допущенні помилки. Структура (масив) **error\_nesting**. Якщо реквізитів, в яких допущенні помилки кілька, то поля з 4.4.1. по 4.4.3 повторюються та є обов’язковими. Якщо помилкові реквізити відсутні, структура (масив) **error\_nesting** не зазначається. |
| 4.4.1 | Назва реквізиту | data\_set\_name | С(64) | + |  |
| 4.4.2 | Порядковий номер елементу в масиві, якщо реквізит, в якому допущено помилку є масивом  | data\_set\_index | N(2) | + | Якщо реквізит, в якому допущено помилку не є масивом, то значення data\_set\_index дорівнює 1. |
| 4.4.3 | Ідентифікатор в наборі даних, що включає реквізит, в якому допущено помилку | data\_set\_id | С(64) | + | Якщо набір даних немає ідентифікатора, то значення data\_set\_id дорівнює null. |

1. Правила формування повідомлень, що надсилаються ФГВФО.
	1. Усі вхідні повідомлення мають відповідати ієрархічній структурі, що зазначена у файлі [Пакети для JSON.xlsx](https://surveys.bank.gov.ua/about-NBUReestr/files/Pakety_dlia_JSON_FGVFO.xlsx).
	2. Перед відправкою повідомлень, вони мають бути перевірені та валідовані ФГВФО за JSON-схемою для запобігання надання некоректних даних.
	3. В кожному повідомлені обов’язково присутній реквізит «Звітна дата» (reporting\_date, ID - 0015);
	4. «Звітна дата» – дата, на яку складається звітність. Звітність складається щомісячно станом на 00 годин 00 хвилин першого числа місяця, наступного за звітним;
	5. Повідомлення Packet може складатися із наборів даних верхнього рівня ID01.Особа (розширені відомості) (person\_full), ID02.Особа (скорочені відомості) (person\_short), ID04.Активна операція (loan), ID05.Забезпечення (collateral).
	6. Будь-яке повідомлення Packet має обов'язково містити набір даних ID01.Особа (розширені відомості) (person\_full) та ID04.Активна операція (loan).
	7. Для однозначної ідентифікації екземпляру набору даних ФГВФО формуються ідентифікатори, які не можуть бути змінені у часі. ФГВФО має бути забезпечена унікальність ідентифікаторів в межах його облікової системи. Ідентифікатор може набувати символьне значення від 5 символів до 50-ти з можливістю використання цифр, великих та маленьких латинських літер і дефісу (без пробілів і спеціальних символів). Дублювання ідентифікаторів в рамках одного набору даних вхідного повідомлення не дозволяється.
	8. Набори даних верхнього рівня мають бути пов’язані між собою через ідентифікатори та можуть містити притаманні їм вкладені набори даних. При цьому має виконуватися наступна умова: всі пов'язані ідентифікаторами набори даних мають обов'язково міститися в одному вхідному повідомленні (крім випадків використання у вхідному повідомленні ідентифікаторів іншого банку).
	9. Набір даних верхнього рівня ID01.Особа (розширені відомості) (person\_full) має обов'язково містити один з вкладених наборів даних: ID34.Фізична особа, резидент (ind\_person), ID35.Юридична особа, резидент (entity), ID36.Фізична особа, нерезидент (non\_res\_ind\_person), ID37.Юридична особа, нерезидент (non\_res\_entity). Набір даних верхнього рівня ID02.Особа (скорочені відомості) (person\_short) має обов'язково містити один з вкладених наборів даних ID30.Фізична особа (скорочені відомості) (ind\_person\_short) або ID31.Юридична особа (скорочені відомості) (entity\_short). Набор даних верхнього рівня ID05.Забезпечення (collateral) має містити один або більше з наборів даних ID40.Об’єкт рухомого майна (movable), ID41.Об’єкт нерухомого майна (immovable), ID42.Фінансове забезпечення (deposit).
	10. В повідомленнях існують реквізити, значення яких може бути різним за типом даних. Для реалізації можливості вибору варіанту типу значень для таких реквізитів використовуються перемикачі-об’єднувачі. Наприклад, для усіх реквізитів, в яких крім реального значення може бути зазначений код з довідника причин неподання (довідник F170) використовуються перемикачі-об’єднувачі (див. JS\_Main\_Fond.json).
2. JSON схеми повідомлень в Системі
	1. У Системі повідомлення формуються в JSON форматі відповідно до JSON схем.
	2. В Системі використовується головна JSON схема, а також додаткові JSON схеми для формування значень довідників, на які є посилання з головної схеми.
	3. Перевірка повідомлень, що використовуються в Системі, виконується на стороні Системи. У разі отримання від ФГВФО повідомлення, що не пройшло перевірку на відповідність до JSON схеми, ФГВФО отримує відповідь з кодом стану HTTP 422 та коротким описом помилки у форматі JSON.
	4. Для отримання переліку JSON схем, що використовуються Системою, ФГВФО має здійснити HTTP запит типу GET за URL, що вказаний в п.12.7. Перелік JSON схем передається від Системи в тілі відповіді (Response body) у вигляді масиву JSON об’єктів.
	5. Реквізити, які містить окремий JSON об’єкт переліку JSON схем (елемент масиву):

|  |  |  |  |
| --- | --- | --- | --- |
| №з/п | Зміст реквізиту | Найменування реквізиту | Тип (максимальна довжина) |
| 1 | Ім’я файлу JSON схеми | name | C(25) |
| 2 | Розмір файлу JSON схеми в байтах | size | N |
| 3 | Дата та час модифікації файлу JSON схеми | modified | D(19) |
| 4 | Посилання, що може бути використане для отримання файлу JSON схеми | url | C(50) |

* 1. Для отримання конкретної схеми ФГВФО має здійснити HTTP запит типу GET за URL, який міститься в раніше отриманому переліку схем в значенні реквізиту «url» елемента, що містить інформацію про необхідний файл.
	2. Перелік URL, що використовуються в Системі (де **cr\_server** приймає значення відповідно до п.6.3):

|  |  |  |
| --- | --- | --- |
| Параметр | Опис | Значення |
| URL передачі даних (Packet) до Системи | п.7.3  | **cr\_server**:8167/cr2\_fond/api/v1/main\_pkg |
| URL для здійснення запиту про статус обробки повідомлення | п.7.8  | **cr\_server**:8168/cr2\_status/api/v1/request\_status/{package\_id} – де змінна {package\_id} є значенням Ідентифікатору пакету. |
| URL для отримання переліку JSON схем |  |  [**cr\_server:**8162/cr2\_fond/jsonschema](https://172.22.12.34:8034/jsonschema) |

1. Історія змін документа

|  |  |  |
| --- | --- | --- |
| **№ версії** | **Дата** | **Опис змін** |
| 1 | 30.01.2024 | Початкова версія |
| 1.1 | 12.08.2024 | Додано статуси обробки повідомлення Unprocessable та InProgress. |

Додаток 1

Інформація про відповіді від веб-сервісу, що може отримати клієнт у разі не успішної обробки запиту в залежності від етапу

|  |  |  |  |
| --- | --- | --- | --- |
| **Етап проходження запиту** | **Опис помилки** | **Код стану HTTP** | **Інформація про відповідь** |
| Автентифікація | Відсутній сертифікат користувача | 403 | Відповідь містить код стану HTTP та короткий опис |
| Автентифікація | Сертифікат виданий невідомим центром сертифікації | 403 | Відповідь містить код стану HTTP та короткий опис |
| Автентифікація | Термін дії сертифікату закінчився  | 403 | Відповідь містить код стану HTTP та короткий опис |
| Автентифікація | Сертифікат відкликано, або неможливо це перевірити | 403 | Відповідь містить код стану HTTP та короткий опис |
| Авторизація | Сертифікат валідний, але призначений для іншої інформаційної системи | 401 | Відповідь містить код стану HTTP та короткий опис |
| Авторизація | Сертифікат валідний, але має не вірний тип | 401 | Відповідь містить код стану HTTP та короткий опис |
| Технологічна перевірка | Не вірна адреса на яку здійснюється запит | 404 | Відповідь містить код стану HTTP та короткий опис |
| Технологічна перевірка | Вхідні дані не є валідним JSON об’єктом | 415 | Відповідь містить код стану HTTP та короткий опис |
| Технологічна перевірка | Вхідний JSON об’єкт не відповідає вимогам, що наведені в JSON схемі | 422 | Відповідь містить код стану HTTP та короткий опис |
| Технологічна перевірка | Підпис або дані пошкоджено, підпис не є дійсним | 412 | Відповідь містить код стану HTTP та короткий опис |
| Помилка під час обробки запиту | Під час обробки запиту виникла помилка | 500 | Короткий опис помилки |
| Сервіс недоступний | Проводяться технічні роботи по оновленню, або обслуговуванню сервісів. | 503 | Короткий опис помилки |

# Додаток 2

# Інструкція з налаштувань доступу до зовнішнього DNS-серверу

***(до уваги мережевих адміністраторів, IT-фахівців, фахівців з IT-безпеки)***

1. **Відкрити мережевий доступ** до DNS-серверу НБУ:

 172.22.2.2

1. **Перевірити доступність DNS-серверу** НБУ без будь-яких налаштувань у командному рядку в CMD за допомогою команди nslookup:

nslookup extern.bank.gov.ua 172.22.2.2

Очікуваний результат у разі наявності доступу:



У разі відсутності доступу:



1. **Налаштувати** в своїй мережі DNS таким чином, щоб **переадресовувати** запит на домен **\*.extern.bank.gov.ua** на вказаний DNS-сервер НБУ: 172.22.2.2.
2. Для робочих комп’ютерів:
3. **перевірити доступ** до вебсервісів з IP-адресами 172.22.12.48 172.22.12.47 (тест) по портах та 8167, 8162, 8168 командою telnet:

telnet 172.22.12.48 8167

telnet 172.22.12.48 8162

telnet 172.22.12.48 8168

telnet 172.22.12.47 8167

telnet 172.22.12.47 8162

telnet 172.22.12.47 8168

1. **додати** DNS-ім’я [i0pcr1.extern.bank.gov.ua](https://i0pcrt1.extern.bank.gov.ua), [i0pcrt1.extern.bank.gov.ua](https://i0pcrt1.extern.bank.gov.ua) або \*.extern.bank.gov.ua у виключення проксі-серверу.
2. Після виконання пунктів 1-4 **перевірити з робочого місця у банку** доступність вебсервісів, а саме:

nslookup [i0pcr1.extern.bank.gov.ua](https://i0pcrt1.extern.bank.gov.ua)

nslookup [i0pcrt1.extern.bank.gov.ua](https://i0pcrt1.extern.bank.gov.ua) (тест)

Очікуваний результат у разі наявності доступу:



1. Комбіновані дата й час, ISO 8601 Date [↑](#footnote-ref-1)