**Технічні умови**

**подання фінансовими компаніями та кредитними спілками до Національного банку України звітності про активні операції та ведення Кредитного реєстру 2.0 Національного банку України** (версія 1.0)

Ці технічні умови (далі - ТУ) визначають вимоги щодо подання інформації згідно з Правилами подання звітності про активні операції (затверджені постановою Правління Національного банку України від 22 січня 2024 року № 9, Положенням про взаємодію фінансових компаній та кредитних спілок з Національним банком України щодо Кредитного реєстру Національного банку України (затверджене постановою Правління Національного банку України від 21 грудня 2023 року № 176) 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 фінансовими компаніями, кредитними спілками (далі – Респондент) і Національним банком України (далі – НБУ) з метою взаємодії з інформаційною системою НБУ, призначеною для накопичення інформації про активні операції Респондентів і ведення Кредитного реєстру НБУ 2.0 (далі – Система), здійснюється згідно з технологією REST API.
	2. Під час інформаційного обміну між Респондентом та Системою повинні виконуватись наступні вимоги: здійснення автентифікації сторін інформаційного обміну, забезпечення конфіденційності інформації, шо передається, та неможливість ознайомлення з нею третіх сторін; контроль цілісності та підтвердження походження (автентичності) інформації, що передається.
	3. Конфіденційність інформації, що передається між Респондентом та Системою, забезпечується за допомогою використання криптографічного протоколу TLS (Transport Layer Security) з односторонньою автентифікацією - Респондент перевіряє сертифікат сервера НБУ (далі – Сервер), вимоги до налаштування якого наведено нижче (див. п.2).
	4. Контроль цілісності та підтвердження автентичності інформації, що передається, забезпечується шляхом її підписання кваліфікованим електронним підписом (КЕП) або удосконаленим електронним підписом (УЕП), що базується на кваліфікованому сертифікаті електронного підпису уповноваженої особи Респондента. Вимоги до формату КЕП/УЕП наведені у пункті 4.
	5. Національний банк при перевірці КЕП/УЕП також здійснює автентифікацію Респондента і у разі, якщо підпис накладено представником неналежного Респондента, подальша обробка інформації не відбувається.
	6. Усі повідомлення інформаційного обміну мають формуватися з використанням формату JSON та відповідати формалізованому опису, визначеному у JSON – схемі.
	7. JSON - схеми повідомлень наведені у додатках. У всіх повідомленнях використовується кодування символів UTF-8.
2. Вимоги до використання криптографічного протоколу TLS
	1. Система використовує клієнт-серверну технологію. Респонденти виступають в якості клієнтів, 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 2.11.
	5. При встановленні з’єднання виконується одностороння автентифікація. При цьому клієнт здійснює автентифікацію Сервера. Сервер не здійснює автентифікацію клієнта.
	6. Сервер повинен використовувати виключно сертифікати, видані центром сертифікації Національного банку України. Усі сертифікати Сервера повинні бути сертифікатами X.509 версії 3.
	7. Клієнт повинен здійснювати автентифікацію Сервера і не встановлювати з’єднання, коли у Сервера немає належного сертифіката, виданого АЦСК Національного банку. Клієнт повинен здійснювати валідацію сертифіката Сервера по всьому ланцюжку довіри до кореневого сертифіката.
	8. Клієнт повинен переконатись, що сертифікат належить саме Серверу. Для цього потрібно перевірити в реквізиті «Постачальник» сертифіката значення полів:

|  |  |
| --- | --- |
| **Назва поля** | **Значення** |
| 2.5.4.97 | NTRUA-00032106 |
| CN | National Bank of Ukraine Certificate authority RSA |

Значення мають збігатись. Якщо значення не збігаються, клієнт не повинен встановлювати з’єднання з Сервером та надсилати інформацію.

* 1. Клієнт та пов’язані з ним апаратна та операційна платформа повинні підтримуватись у актуальному стані з точки зору оновлень безпеки.
	2. Клієнт не повинен застосовувати компресію даних на рівні протоколу TLS.
	3. 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. Порядок забезпечення ключовою системою
	1. Уповноважені представники Респондента самостійно визначають кваліфікованого надавача електронних довірчих послуг (далі - КНЕДП), послугами якого будуть користуватись для підписання інформації, що передається.
	2. Отримання електронних довірчих послуг (генерація ключів, формування кваліфікованих сертифікатів, створення підписів тощо) уповноваженими особами Респондента здійснюється у відповідності до регламенту роботи відповідного КНЕДП.
	3. Кваліфікований сертифікат електронного підпису уповноваженої особи Респондента повинен бути виданий як представнику юридичної особи (повинен містити код ЄДРПОУ) Респондента.

1. Вимоги до забезпечення цілісності інформації
	1. При підписанні даних, що надсилаються до Національного банку, застосовуються такі вимоги до формату кваліфікованого/удосконаленого електронного підпису:

|  |  |
| --- | --- |
| Параметр | Значення |
| Тип контейнеру | ASiC-E |
| Алгоритм підпису | ECDSA |
| Тип підпису, що використовується в контейнері ASiC | CAdES |
| Рівень підпису CAdES | CAdES-X long |

1. Опис роботи Системи
	1. Система використовує клієнт-серверну технологію. Респонденти відправляють та отримують інформацію за допомогою HTTP-запитів до відповідних вебсервісів.
	2. Для тестування і відпрацювання технології інформаційної взаємодії між системами автоматизації Респондентів з Системою розгорнуто тестові вебсервіси.
	3. Взаємодія з вебсервісами відбувається за адресами: cr2.bank.gov.ua – для продуктивного середовища і [cr2test.bank.gov.ua](https://cr2test.bank.gov.ua) – для тестового (далі по тексту замість зазначених конкретних адрес використовується змінна **cr\_server**).
2. Подання інформації до Системи
	1. На стороні Системи для прийому інформації від Респондента та надання інформації Респонденту налаштовано вебсервіси: 1) вебсервіс «Пакет» (загальний пакет), 2) вебсервіс «Перевірка статусу» (Перевірка статусу обробки загального пакету).
	2. Респондент формує повідомлення у форматі JSON (правила формування повідомлень наведено у розділі 10) та підписує це повідомлення КЕП/УЕП (використовуються параметри, що зазначені у пункті 4.1). В результаті підписання має бути сформовано ASiC-E контейнер, який подається Респондентом у запиті типу POST у закодованому за допомогою Base64 вигляді в тілі запиту (BODY) та надсилається на відповідний вебсервіс «Пакет» або «Перевірка статусу».
	3. Запит, що надходить до вебсервісу «Пакет», проходить два етапи обробки, на яких він може бути відхилений:
3. автентифікація, авторизація, перевірка цілісності інформації (верифікація кваліфікованого електронного підпису та перевірка, чи має право Респондент, представник якого підписав запит, взаємодіяти з Системою), перевірка поданої інформації в запиті на відповідність JSON-схемі;
4. перевірка поданої інформації в запиті на відповідність правилам контролю, викладеним у (посилання на контролі).
	1. Якщо запит до вебсервісу «Пакет» не пройде перевірки першого етапу, то Респондент одразу у відповіді на запит (тобто у поточному сеансі) отримає повідомлення про помилку і сеанс завершується. Усю інформацію у запиті буде відхиллено (див. приклад нижче).

**Приклад відповіді на запит (вебсервіс «Пакет») 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":" 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 до вебсервісу «Пакет» успішно пройде перевірки першого етапу, то Респондент одразу у відповіді на запит (тобто у поточному сеансі) отримає повідомлення з унікальним ідентифікатором пакету {package\_id} і сеанс завершується.
	2. Отримання Респондентом ідентифікатору пакету свідчить про успішність проходження першого етапу перевірки і початок другого етапу.
	3. Другий етап перевірки відбувається в асинхронному режимі. Про остаточний результат обробки пакету Респондент може дізнатись, надіславши запит (тип POST) на вебсервіс «Перевірка статусу», використовуючи отриманий ідентифікатор пакету {package\_id}. Формування тіла запиту відбувається за правилами, описаними в пункті 6.2.
	4. Запит, що надходить до вебсервісу «Перевірка статусу», проходить також перший етап обробки, описаний в абзаці 1) пункту 6.3.
	5. Від вебсервісу «Перевірка статусу» Респондент 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;
* **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).
1. Загальна структура повідомлень, що надходять від Респондента до Системи.

**Приклад запиту типу POST на вебсервіс «Пакет».**

**Подання інформації до вебсервісу /cr2\_comps/api/v1/main\_pkg (для фінансових компаній) або /cr2\_unions/api/v1/main\_pkg (для кредитних спілок)**

|  |
| --- |
| **POST** **https://cr\_server/cr2\_comps/api/v1/main\_pkg**Content-Type: application/json**{ASiC-E container}** |

Тут **{ASiC-E container}** є результатом накладанняКЕП/УЕП на повідомлення, що сформовані Респондентом.

**Приклад (скорочено) повідомлення, на який накладається КЕП/УЕП:**

|  |
| --- |
| { "data": { " reporting\_date": "2022-12-12", "person\_full": [ { "person\_id\_full": "77777", "f150\_event": "011", "event\_date": "2021-03-02", "in\_cr": true, "related\_person": [ { "f150\_event": "011", "event\_date": "2022-11-11", "person\_info": { "person\_id\_short": "22222" }, "k062\_connection\_type": [ "04", "08" ], "share\_direct\_participation": 10, "share\_indirect\_participation": 14 },. . . "initial\_agreem\_id": [ "1nkoy9iibd" ], "agreem\_no": "a1", "agreem\_start\_date": "2022-10-15", "agreem\_end\_date": { "value": "2022-11-10" } } ] }} |

**Приклад запиту типу POST на вебсервіс «Перевірка статусу».**

|  |
| --- |
| **POST** **cr\_server/cr2\_status/api/v1/request\_status**Content-Type: application/json**{ASiC-E container}** |

Тут **{ASiC-E container}** є результатом накладанняКЕП/УЕП на повідомлення (унікальний ідентифікатор пакету {package\_id}).

**Приклад повідомлення, на який накладається КЕП/УЕП:**

|  |
| --- |
| { "data": { "package\_id": "f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66" }} |

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. Загальний опис інформації та структура повідомлень, що отримує Респондент у відповідь на свій запит.
	1. Інформацію про відповіді від вебсервісу, що може отримати клієнт у разі не успішної обробки запиту наведено в Додатку 2.
	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 (вебсервіс «Пакет») | Створення нового запису | 201 | Відповідь містить код стану HTTP та квитанцію з результатом виконання операції; |
| POST (вебсервіс «Перевірка статусу») | Перевірка статусу | 200 | Відповідь містить код стану HTTP та квитанцію з результатом виконання операції; |

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

|  |
| --- |
| **HTTP/**1.1 200 OKSessionId: f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66Content-Type: application/json{"package\_id":"f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66","web\_service\_url":"https://172.22.3.17:8160/cr2\_comps/api/v1/main\_pkg","http\_method":"POST","client\_id":"ЕДРПОУ з сертифіката Респондента","general\_http\_status\_code":201,"kvi\_date":"2023-11-06T14:44:47.587Z"} |

* 1. Реквізити відповіді за результатами роботи вебсервісу «Пакет» (запит типу POST):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №з/п | Зміст реквізиту | Найменування реквізиту  | Тип (макс.дов-жина) | Обов’язковість заповнення | Примітки |
| 1 | Унікальний ідентифікатор пакету, що було надіслано Респондентом | 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 | ЕДРПОУ з сертифіката Респондента | client\_id | C(15) | + |  |
| 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 POST від вебсервісу «Перевірка статусу» в разі обробки повідомлення з помилками**

|  |
| --- |
| **HTTP/**1.1 424SessionId: f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66Content-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 POST від вебсервісу «Перевірка статусу» в разі, коли повідомлення за ідентифікатором пакету не знайдено**

|  |
| --- |
| **HTTP/**1.1 404SessionId: f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66Content-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 POST від вебсервісу «Перевірка статусу» в разі успішної обробки повідомлення (інформацію прийнято)**

|  |
| --- |
| **HTTP/**1.1 200SessionId: f21fb933e1845d028ec776958b67705d7fc5d696434834f6002743814cec1d66Content-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» (запит типу POST):

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №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****Passed****Failed** |
| 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 Респондентом.
	1. Усі вхідні повідомлення мають відповідати ієрархічній структурі, що зазначена у файлі Пакети для JSON.xlsx.
	2. Перед відправкою повідомлень, вони мають бути перевірені та валідовані Респондентом 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), ID03.Фінансове зобов'язання (liability), ID04.Активна операція (loan), ID05.Забезпечення (collateral),  ID06.Узагальнююча угода (contract)(тільки для фінансових компаній).
	6. Будь-яке повідомлення Packet має обов'язково містити набір даних ID01.Особа (розширені відомості) (person\_full) та хоча б один з наборів даних ID03.Фінансове зобов'язання (liability) або ID04.Активна операція (loan).
	7. Для однозначної ідентифікації екземпляру набору даних Респондентом формуються ідентифікатори, які не можуть бути змінені у часі. Респондентом 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 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 Респондента).
	9. Набор 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). Набор 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 повідомленні Packet 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. JSON-схеми JS\_Main\_Comps.json або JS\_Main\_Unions.json).
2. JSON схеми повідомлення в Системі
	1. Під час інформаційного обміну використовуються головна JSON схема (див. JSON-схеми JS\_Main\_Comps.json (для фінансових компаній) або JS\_Main\_Unions.json (для кредитних спілок) для загального пакету, а також додаткові JSON схеми для формування значень довідників, на які є посилання з головної схеми. Головну JSON-схему реалізовано відповідно до моделі даних, що міститься у файлі Пакети для JSON.xlsx.
	2. На стороні Системи виконується перевірка повідомлення за JSON-схемою. Якщо повідомлення не пройшло перевірку на відповідність до JSON схеми, Респондент отримує відповідь з кодом стану HTTP 422 та коротким описом помилки у форматі JSON.

Додаток 2

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 | Клієнта не автентифіковано | 403 | Відповідь містить код стану HTTP та короткий опис |
| Авторизація | Клієнт немає відповідних повноважень | 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 |
| 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 |