



**платформа аутентификации и управления
доступом**

Руководство разработчика

Часть 5

Сервис авторизации

Листов 47

Содержание

Перечень сокращений	4
Перечень терминов.....	5
1. Кеширование ответов сервиса авторизации	7
2. Массовый авторизационный запрос	8
2.1. Данные в запросе	8
2.2. Данные в ответе на запрос	10
2.3. Возможные ошибки.....	11
2.4. Пример выполнения запроса	12
3. Получение списка ИС, в которых у указанного профиля УЗ пользователя есть доступ.....	15
3.1. Данные в запросе	15
3.2. Данные в ответе на запрос	16
3.3. Возможные ошибки.....	16
3.4. Пример выполнения запроса	17
4. Получение списка доступных ресурсов и действий для конкретного профиля УЗ пользователя	20
4.1. Данные в запросе	20
4.2. Данные в ответе на запрос	22
4.3. Возможные ошибки.....	22
4.4. Пример выполнения запроса	23
5. Получение списка профилей УЗ пользователя, для которых выполняется успешная авторизация для заданного ресурса и действия	25
5.1. Данные в запросе	25
5.2. Данные в ответе на запрос	26
5.3. Возможные ошибки.....	27
5.4. Пример выполнения запроса	28
6. Получение списка ресурсных атрибутов, участвующих в авторизации	31
6.1. Данные в запросе	31
6.2. Данные в ответе на запрос	32

6.3. Возможные ошибки	32
6.4. Пример выполнения запроса	32
7. Получение списка условий для успешного прохождения авторизации	35
7.1. Данные в запросе	35
7.2. Данные в ответе на запрос	36
7.3. Возможные ошибки	37
7.4. Пример выполнения запроса	37
8. Получение списка профилей УЗ пользователей разных организаций, для которых выполнена успешная авторизация для заданного ресурса и действия	40
8.1. Данные в запросе	40
8.2. Данные в ответе на запрос	42
8.3. Возможные ошибки	43
8.4. Пример выполнения запроса	43
Лист регистрации изменений	47

Перечень сокращений

ИНН	–	идентификационный номер налогоплательщика
ИС	–	информационная система
СНИЛС	–	страховой номер индивидуального лицевого счёта
УЗ	–	учётная запись

Перечень терминов

Идентификатор	– признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ними идентификационную информацию
Идентификация	– действия по присвоению субъектам и объектам доступа идентификаторов и (или) по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов
Информационная система	– совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Объект доступа	– единица ИС (документ, поле, атрибут и т. п.), доступ к которой разграничивается политиками авторизации
Политика авторизации	– правило доступа, определяющее возможность выполнения действия или нескольких действий с ресурсом или несколькими ресурсами одного типа, при наличии у пользователя соответствующих назначенных ролей и выполнении заданного условия применимости политики авторизации
Профиль учётной записи пользователя	– набор значений атрибутов учётной записи X-IDBox, однозначно ассоциирующий субъект доступа с организацией, в интересах (от имени) которой субъектом доступа выполняются операции, реализованные в X-IDBox и ИС, интегрированных с X-IDBox
Ресурс	– защищаемый объект интегрированной ИС, который используется в политиках авторизации и относится к определенному типу ресурса
Роль	– предопределенная совокупность правил доступа к ресурсам (политик авторизации), устанавливающих допустимое взаимодействие между субъектами доступа и объектами доступа
Субъект доступа	– пользователь и/или ИС, действия которого по доступу к объектам доступа регламентируются политиками авторизации

Учётная запись пользователя – логический объект (совокупность данных пользователя), существующий в пределах X-IDBox и представляющий субъекта доступа в X-IDBox и ИС, интегрированных с X-IDBox

1. Кеширование ответов сервиса авторизации

По умолчанию кешируются все ответы из сервиса авторизации.

Срок жизни кеша по каждому ответу регулируется настройками. Кеш инвалидируется:

- по истечении срока жизни и не зависит от частоты обращений;
- при обновлении ролевой модели (по техническому наименованию ИС), обновлении роли, обновлении данных или состояния профиля УЗ пользователя и изменении адреса электронной почты УЗ пользователя.

При этом для определенных ИС кеш ответа можно отключить, если соответствующая ИС настройка «xidbox.authz.cache.info-system-settings» имеет значение «false». Однако эта настройка игнорируется, если настройка «xidbox.authz.cache.cache-responses-for-all-info-systems» имеет значение «true». При этом несмотря на вышеописанные настройки, если в запросе передан заголовок «Cache-Control» со значением «no cache», то расчет ответа происходит без учёта кеша ответа, но с учётом иных кешей (кеш УЗ пользователя, профиля УЗ пользователя, организации и т.д. не отключается через указанные выше настройки или заголовок).

Для отключения кеша расчёта применимости ролей необходимо установить значение «false» в настройке «xidbox.authz.cache.disable-calculate-role-applicability», но при этом HTTP-запросы, которые будут выполняться в сервисе авторизации для расчета применимости роли, регулируются настройками, описанными выше.

Подробное описание настроек сервисов приведено в Руководстве администратора.

2. Массовый авторизационный запрос

Имя ресурса: /authz/api/v1/authz/multi

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Accept: application/json

2.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 1.

Описание данных в запросе приведено в таблице 2.

Таблица 1 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак отключения кеша ответа	Cache-Control	Строка	Нет	При передаче значения «no cache» ответ будет рассчитываться без учёта кеша ответа, иначе будут применяться настройки в сервисе (см. п. 1)

Таблица 2 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя, для которого необходимо получить результат проверки наличия прав у пользователя на совершение действия с ресурсом

Параметр	Название параметра	Тип данных	Обязательность	Описание
Техническое наименование ИС	infoSystemTechName	Строка	Да	Техническое наименование ИС, в которой у профиля УЗ пользователя настроен доступ для совершения действия с ресурсом
Настройка результатов	mode	Строка	Нет	Информация о данных, которые необходимо передавать в ответе. Возможные значения: – HAS_ACCESS – передавать только те пары ресурсов и действий, к которым у профиля УЗ пользователя настроены необходимые права; – ALL (значение по умолчанию) – передавать результаты по всем парам действия и ресурса
Данные для авторизации	authRequests	Массив	Да	Список пар, для которых необходимо проверить наличие доступа у профиля УЗ пользователя
Ресурс	resource	Строка	Да	Техническое наименование ресурса, для которого проверяется возможность совершения действия конкретным профилем УЗ пользователя
Тип ресурса	resourceType	Строка	Да	Техническое наименование типа ресурса, для которого проверяется возможность совершения действия конкретным профилем УЗ пользователя

Параметр	Название параметра	Тип данных	Обязательность	Описание
Действие	action	Строка	Да	Техническое наименование действия, для которого проверяется наличие прав у конкретного профиля УЗ пользователя на его совершение с ресурсом
Атрибуты	attributeMap	Объект	Нет	Список значений ресурсных атрибутов
Атрибуты роли	roleAttributeMap	Объект	Нет	Список атрибутов ролей и их значений, используемых для фильтрации ролей
Признак необходимости учета применимости роли	useRolesApplicabilityCondition	Логический	Нет	Информация о необходимости учета применимости роли. Значение «true» – если применимость роли учитывается при авторизации, значение «false» – если применимость роли не учитывается при авторизации. Значение по умолчанию – «true»

2.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 3.

Таблица 3 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Идентификатор профиля УЗ пользователя, для которого осуществлялась проверка

Параметр	Название параметра	Тип данных	Описание
Техническое наименование ИС	infoSystemTechName	Строка	Техническое наименование ИС, в которой проверялось наличие прав для совершения действия с ресурсом у профиля УЗ пользователя
Результаты авторизации	authResponses	Массив	Результаты выполнения проверки наличия прав профиля УЗ пользователя на совершение запрашиваемых действий с ресурсом
Ресурс	resource	Строка	Техническое наименование ресурса из запроса
Тип ресурса	resourceType	Строка	Техническое наименование типа ресурса из запроса
Действие	action	Строка	Техническое наименование действия из запроса
Результат проверки	allowed	Логический	Результат выполнения проверки наличия прав. Возможные значения: – true – у пользователя есть право выполнять действие с ресурсом; – false – у пользователя отсутствует право выполнять действие с ресурсом или ресурс или действие отсутствует в политиках доступа

2.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 4.

Таблица 4 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Описание
Тип ошибки	type	Строка	Ошибка с сообщением или ошибка валидации
Информация об ошибке	payload	Строка/ Объект	Подробная информация об ошибке
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка

2.4. Пример выполнения запроса

Запрос:

Content-Type: application/json

Accept: application/json

```
{
  "userProfileUuid": "0152f40b-e12f-4fcb-ac23-
988c2b4f539b",
  "infoSystemTechName": "xidbox",
  "mode": "ALL",
  "authRequests": [
    {
      "action": "read",
      "resource": "ordr_cards",
      "resourceType": "ordr_cards_type"
    },
    {
      "action": "create",
      "resource": "decision",
      "resourceType": "decision_type",
      "attributeMap": {
        "ORDR_TYPE": "usr_reg"
      }
    }
  ],
  "roleAttributeMap": {
    "tech_name_2": "value_2",
    "tech_name_3": "value_3"
  },
  "useRolesApplicabilityCondition": true
}
```

Ответ на запрос

Content-Type: application/json

```
{
```

```
"userProfileUuid": "0152f40b-e12f-4fcb-ac23-
988c2b4f539b",
"infoSystemTechName": "xidbox",
"authResponses": [
  {
    "action": "read",
    "resource": "ordr_cards",
    "resourceType": "ordr_cards_type",
    "allowed": false
  },
  {
    "action": "create",
    "resource": "decision",
    "resourceType": "decision_type",
    "allowed": false
  }
]
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Информационная система не найдена.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка валидации:

Content-Type: application/json

```
{
  "type": "VALIDATION",
  "payload": {
    "fields": [
      {
        "fieldName": "authRequests[0].resourceType",
        "errors": "Данное поле должно содержать хотя
бы один не пробельный символ"
```

```
        }  
      ]  
    },  
    "timestamp": "2022-04-14T09:00:38.996714Z"  
  }  
}
```

3. Получение списка ИС, в которых у указанного профиля УЗ пользователя есть доступ

Имя ресурса: /authz/api/v1/user-profiles/info-systems

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Accept: application/json

3.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 5.

Описание данных в запросе приведено в таблице 6.

Таблица 5 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак отключения кеша ответа	Cache-Control	Строка	Нет	При передаче значения «no cache» ответ будет рассчитываться без учёта кеша ответа, иначе будут применяться настройки в сервисе (см. п. 1)

Таблица 6 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Список профилей УЗ пользователя	userProfiles	Массив	Да	Список профилей УЗ пользователя
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя

3.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 7.

Таблица 7 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Описание
Список профилей УЗ пользователя	userProfiles	Массив	Список профилей УЗ пользователя
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Идентификатор профиля УЗ пользователя
Список ИС	infoSystems	Массив	Информация об ИС, в которой у профиля УЗ пользователя есть хотя бы одна роль
Идентификатор ИС	infoSystemUuid	UUID	Идентификатор ИС
Техническое наименование ИС	techName	Строка	Техническое наименование ИС
Наименование ИС	name	Строка	Наименование ИС
Короткое наименование ИС	shortName	Строка	Короткое наименование ИС

3.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 8.

Таблица 8 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Описание
Тип ошибки	type	Строка	Ошибка с сообщением или ошибка валидации
Информация об ошибке	payload	Строка/ Объект	Подробная информация об ошибке
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка

3.4. Пример выполнения запроса

Запрос:

POST http://{host}}/authz/api/v1/user-profiles/info-systems

Content-Type: application/json

Accept: application/json

```
{
  "userProfiles": [
    {
      "userProfileUuid": "0152f40b-e12f-4fcb-ac23-988c2b4f539b"
    },
    {
      "userProfileUuid": "5e6ea47d-056d-4629-a925-925e0254d39b"
    }
  ]
}
```

Ответ:

Content-Type: application/json

```
{
  "userProfiles": [
    {
      "userProfileUuid": "0152f40b-e12f-4fcb-ac23-988c2b4f539b",
      "infoSystems": [
        {
          "infoSystemUuid": "ca35bccb-093e-4017-9078-cf592cb6872c",
          "techName": "xidbox",
          "name": "ИС X-IDBOX",
          "shortName": "X-IDBOX"
        }
      ]
    }
  ]
}
```

```
{
  "infoSystemUuid": "354fade7-05e0-
4b64-b1b7-be6f6d4f23a8",
  "techName": "test_system",
  "name": "ИС для тестов",
  "shortName": "Тестовая ИС"
}
],
{
  "userProfileUuid": "5e6ea47d-056d-4629-
a925-925e0254d39b",
  "infoSystems": []
}
]
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Профиль учетной записи не найден.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка валидации:

Content-Type: application/json

```
{
  "type": "VALIDATION",
  "payload": {
    "fields": [
      {
        "fieldName": "userProfiles",
        "errors": "Поле не должно быть пустым"
      }
    ]
  },
}
```

```
"timestamp": "2022-04-14T09:00:38.996714Z"  
}
```

4. Получение списка доступных ресурсов и действий для конкретного профиля УЗ пользователя

Имя ресурса: /authz/api/v1/user-profiles/resources

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Accept: application/json

4.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 9.

Описание данных в запросе приведено в таблице 10.

Таблица 9 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак отключения кеша ответа	Cache-Control	Строка	Нет	При передаче значения «no cache» ответ будет рассчитываться без учёта кеша ответа, иначе будут применяться настройки в сервисе (см. п. 1)

Таблица 10 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя, для которого необходимо получить перечень доступных ресурсов и действий

Параметр	Название параметра	Тип данных	Обязательность	Описание
Техническое наименование ИС	infoSystemTechName	Строка	Да	Техническое наименование ИС, в которой у профиля УЗ пользователя настроен доступ к ресурсам и действиям
Ресурсы	resources	Массив	Да	Массив с парами «ресурс – тип ресурса». Список ресурсов указанных типов, к которым у профиля УЗ пользователя есть доступ
Ресурс	resource	Строка	Да	Техническое наименование ресурса
Тип ресурса	resourceType	Строка	Да	Техническое наименование типа ресурса
Атрибуты	attributeMap	Объект	Нет	Список атрибутов запроса
Действие	action	Строка	Нет	Действие с ресурсом
Атрибуты роли	roleAttributeMap	Объект	Нет	Список атрибутов ролей и их значения, используемые для фильтрации ролей
Признак необходимости учета применимости роли	useRolesApplicabilityCondition	Логический	Нет	Информация о необходимости учета применимости роли. Значение «true» – если применимость роли учитывается при авторизации, значение «false» – если применимость роли не учитывается при авторизации. Значение по умолчанию – «true»

4.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 11.

Таблица 11 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Описание
Право доступа	–	Объект	Техническое наименование ресурса и действия, которые профиль УЗ пользователя может с ним выполнять
Тип ресурса	resourceType	Строка	Техническое наименование типа ресурса, который был указан в запросе
Ресурс	resource	Строка	Техническое наименование ресурса, который был указан в запросе
Действие с ресурсом	actions	Массив	Перечень действий, которые профиль УЗ пользователя может выполнять с ресурсом, указанным в параметре «Ресурс» соответствующего типа, указанного в параметре «Тип ресурса», и в соответствии с назначенными на текущий момент ролями профиля УЗ пользователя

4.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 12.

Таблица 12 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Описание
Тип ошибки	type	Строка	Ошибка с сообщением или ошибка валидации
Информация об ошибке	payload	Строка/ Объект	Подробная информация об ошибке
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка

4.4. Пример выполнения запроса

Запрос:

```
POST http://{{host}}/authz/api/v1/user-  
profiles/resources
```

```
Content-Type: application/json
```

```
Accept: application/json
```

```
{  
  "userProfileUuid": "966cfa0e-cc90-4e97-aea3-  
df5aa1759099",  
  "infoSystemTechName": "xidbox",  
  "resources": [  
    {  
      "resource": "certification_authority",  
      "resourceType": "certification_authorities_type"  
    },  
    {  
      "resource": "certification_authorities",  
      "resourceType": "certification_authorities_type"  
    }  
  ],  
  "attributeMap": {  
    "CURRENT_USER_ID": "0052f40b-e12f-4fcb-ac23-  
988c2b4f539b"  
  },  
  "roleAttributeMap": {  
    "tech_name_2": "value_2",  
    "tech_name_3": "value_3"  
  },  
  "useRolesApplicabilityCondition": true  
}
```

Ответ:

```
Content-Type: application/json
```

```
[
```

```
{
  "resource": "certification_authority",
  "resourceType": "certification_authorities_type",
  "actions": []
},
{
  "resource": "certification_authorities",
  "resourceType": "certification_authorities_type",
  "actions": []
}
]
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Пользователь не найден.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка валидации:

Content-Type: application/json

```
{
  "type": "VALIDATION",
  "payload": {
    "fields": [
      {
        "fieldName": "infoSystemTechName",
        "errors": "Данное поле должно содержать хотя  
бы один не пробельный символ"
      }
    ]
  },
  "timestamp": "2022-04-14T14:03:29.080453Z"
}
```

5. Получение списка профилей УЗ пользователя, для которых выполняется успешная авторизация для заданного ресурса и действия

Имя ресурса: /authz/api/v1/user-profiles

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Accept: application/json

5.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 13.

Описание данных в запросе приведено в таблице 14.

Таблица 13 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак отключения кеша ответа	Cache-Control	Строка	Нет	При передаче значения «no cache» ответ будет рассчитываться без учёта кеша ответа, иначе будут применяться настройки в сервисе (см. п. 1)

Таблица 14 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Техническое наименование ИС	infoSystemTech Name	Строка	Да	Техническое наименование ИС
Тип ресурса	resourceType	Строка	Да	Техническое наименование типа ресурса
Ресурс	resource	Строка	Да	Техническое наименование ресурса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Действие	action	Строка	Да	Техническое наименование действия над ресурсом
Организация	organizationUuid	UUID	Да	Идентификатор организации, которой должен принадлежать профиль УЗ пользователя
Атрибуты	attributeMap	Объект	Нет	Список ресурсных атрибутов и их значения, используемые для авторизации
Атрибуты роли	roleAttributeMap	Объект	Нет	Список атрибутов ролей и их значения, используемые для фильтрации ролей
Признак необходимости учета применимости роли	useRolesApplicabilityCondition	Логический	Нет	Информация о необходимости учета применимости роли. Значение «true» – если применимость роли учитывается при авторизации, значение «false» – если применимость роли не учитывается при авторизации. Значение по умолчанию – «true»

5.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 15.

Таблица 15 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Описание
Техническое наименование ИС	infoSystemTechName	Строка	Техническое наименование ИС

Параметр	Название параметра	Тип данных	Описание
Тип ресурса	resourceType	Строка	Техническое наименование типа ресурса
Ресурс	resource	Строка	Техническое наименование ресурса
Действие	action	Строка	Техническое наименование действия над ресурсом
Идентификатор организации	organizationinUuid	UUID	Идентификатор организации
Полное наименование организации	organizationFullName	Строка	Полное наименование организации
Профили УЗ пользователя	userProfiles	Массив	Список профилей УЗ пользователя, которые могут совершить действия над ресурсом
Пользователь	user	Объект	Информация о пользователе
Идентификатор пользователя	userProfileUuid	UUID	Идентификатор пользователя
Имя	firstName	Строка	Имя пользователя
Фамилия	lastName	Строка	Фамилия пользователя
Отчество	middleName	Строка	Отчество пользователя
ИНН	inn	Строка	ИНН пользователя
СНИЛС	snils	Строка	СНИЛС пользователя
Почта УЗ пользователя	email	Строка	Адрес электронной почты УЗ пользователя
Профиль УЗ пользователя	userProfile	Объект	Информация о профиле УЗ пользователя
Идентификатор профиля УЗ пользователя	uuid	UUID	Идентификатор профиля УЗ пользователя
Почта профиля УЗ пользователя	workEmail	Строка	Адрес электронной почты профиля УЗ пользователя

5.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 16.

Таблица 16 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Описание
Тип ошибки	type	Строка	Ошибка с сообщением или ошибка валидации

Параметр	Название параметра	Тип данных	Описание
Информация об ошибке	payload	Строка/ Объект	Подробная информация об ошибке
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка

5.4. Пример выполнения запроса

Запрос:

```
POST http://{{host}}/authz/api/v1/user-profiles
Content-Type: application/json
Accept: application/json
```

```
{
  "infoSystemTechName": "xidbox",
  "resourceType": "decision_type",
  "resource": "decision",
  "action": "create",
  "organizationUuid": "c25ebd5e-6d16-44a5-9267-
4d3a172cb0ba",
  "attributeMap": {
    "ORDR_TYPE": "usr_reg"
  },
  "roleAttributeMap": {
    "tech_name_2": "value_2",
    "tech_name_3": "value_3"
  },
  "useRolesApplicabilityCondition": true
}
```

Ответ:

```
Content-Type: application/json
```

```
{
  "infoSystemTechName": "xidbox",
  "resourceType": "decision_type",
  "resource": "decision",
  "action": "create",
```

```
"organizationUuid": "c25ebd5e-6d16-44a5-9267-4d3a172cb0ba",
"organizationFullName": "ИП Цепеш В.",
"userProfiles": [
  {
    "user": {
      "uuid": "0052f40b-e12f-4fcb-ac23-988c2b4f539b",
      "firstName": "Иван",
      "lastName": "Всемогущий",
      "middleName": null,
      "inn": null,
      "snils": null,
      "email": "max@infosec.ru"
    },
    "userProfile": {
      "uuid": "0152f40b-e12f-4fcb-ac23-988c2b4f539b",
      "workEmail": "max@infosec.ru"
    }
  },
  {
    "user": {
      "uuid": "2543a4ab-907a-4ead-9370-bd16017bf3ae",
      "firstName": "Илья",
      "lastName": "ФОМИН",
      "middleName": "Никитич",
      "inn": null,
      "snils": null,
      "email": "jija@localhost.ru"
    },
    "userProfile": {
      "uuid": "29a99f6b-2ce5-449a-8596-c9517f425416",
      "workEmail": "jija@localhost.ru"
    }
  }
]
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Информационная система не найдена.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка валидации:

Content-Type: application/json

```
{
  "type": "VALIDATION",
  "payload": {
    "fields": [
      {
        "fieldName": "resource",
        "errors": "Данное поле должно содержать хотя
бы один не пробельный символ"
      }
    ]
  },
  "timestamp": "2022-04-14T09:00:38.996714Z"
}
```

6. Получение списка ресурсных атрибутов, участвующих в авторизации

Имя ресурса: /authz/api/v1/authz/attributes

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Accept: application/json

6.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 17.
Описание данных в запросе приведено в таблице 18.

Таблица 17 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак отключения кеша ответа	Cache-Control	Строка	Нет	При передаче значения «no cache» ответ будет рассчитываться без учёта кеша ответа, иначе будут применяться настройки в сервисе (см. п. 1)

Таблица 18 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Техническое наименование ИС	infoSystemTech Name	Строка	Да	Техническое наименование ИС
Список ресурсов	resources	Массив	Да	Список ресурсов, по которым запрашивается информация
Ресурс	resource	Строка	Да	Техническое наименование ресурса
Тип ресурса	resourceType	Строка	Да	Техническое наименование типа ресурса

6.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 19.

Таблица 19 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Описание
Техническое наименование ИС	infoSystemTechName	Строка	Техническое наименование ИС
Список ресурсов	resources	Массив	Список ресурсов, по которым запрашивается информация
Ресурс	resource	Строка	Техническое наименование ресурса
Тип ресурса	resourceType	Строка	Техническое наименование типа ресурса
Список ресурсных атрибутов	resourceAttributes	Массив	Список ресурсных атрибутов, которые используются в авторизации запросов для указанного ресурса

6.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 20.

Таблица 20 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Описание
Тип ошибки	type	Строка	Ошибка с сообщением или ошибка валидации
Информация об ошибке	payload	Строка/ Объект	Подробная информация об ошибке
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка

6.4. Пример выполнения запроса

Запрос:

```
POST http://{{host}}/authz/api/v1/authz/attributes
Content-Type: application/json
Accept: application/json
```

```
{
  "infoSystemTechName": "xidbox",
  "resources": [
    {
      "resource": "user_card",
      "resourceType": "user_card_type"
    },
    {
      "resource": "ordr_card",
      "resourceType": "ordr_card_type"
    }
  ]
}
```

Ответ:

```
Content-Type: application/json
```

```
{
  "infoSystemTechName": "xidbox",
  "resources": [
    {
      "resource": "user_card",
      "resourceType": "user_card_type",
      "resourceAttributes": [
        "USER_SYSTEMS",
        "USER_CARD_UUID"
      ]
    },
    {
      "resource": "ordr_card",
      "resourceType": "ordr_card_type",
      "resourceAttributes": [
        "USER_PROFILE_ROLE_TECH_NAMES",
        "ORDR_APPROVAL_STEP",
        "ORDR_TYPE",

```

```
        "AUTHOR_UUID",
        "CONTROL_OBJECT_UUID",
        "CONTROL_OBJECT_SYSTEMS"
    ]
}
]
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Информационная система не найдена.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка валидации:

Content-Type: application/json

```
{
  "type": "VALIDATION",
  "payload": {
    "fields": [
      {
        "fieldName": "infoSystemTechName",
        "errors": "Данное поле должно содержать хотя бы один не пробельный символ"
      }
    ]
  },
  "timestamp": "2022-04-14T09:00:38.996714Z"
}
```

7. Получение списка условий для успешного прохождения авторизации

Имя ресурса: /authz/api/v1/user-profiles/conditions

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Accept: application/json

7.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 21.

Описание данных в запросе приведено в таблице 22.

Таблица 21 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак отключения кеша ответа	Cache-Control	Строка	Нет	При передаче значения «по cache» ответ будет рассчитываться без учёта кеша ответа, иначе будут применяться настройки в сервисе (см. п. 1)

Таблица 22 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя
Техническое наименование ИС	infoSystemTech Name	Строка	Да	Техническое наименование ИС
Тип ресурса	resourceType	Строка	Да	Техническое наименование типа ресурса
Ресурс	resource	Строка	Да	Техническое наименование ресурса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Действие	action	Строка	Да	Техническое наименование действия
Признак подстановки значений динамических атрибутов	insertDynamicAttributes	Логический	Нет	Информация о необходимости подстановки динамических атрибутов. Значение «true» – если подставляются динамические атрибуты, значение «false» – если не подставляются. Значение по умолчанию – «false»
Атрибуты роли	roleAttributeMap	Объект	Нет	Список атрибутов ролей и их значения, используемые для фильтрации ролей
Признак необходимости учета применимости роли	useRolesApplicabilityCondition	Логический	Нет	Информация о необходимости учета применимости роли. Значение «true» – если применимость роли учитывается при авторизации, значение «false» – если применимость роли не учитывается при авторизации. Значение по умолчанию – «true»

7.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 23.

Таблица 23 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Идентификатор профиля УЗ пользователя из запроса
Техническое наименование ИС	infoSystemTechName	Строка	Техническое наименование ИС из запроса
Тип ресурса	resourceType	Строка	Техническое наименование типа ресурса
Ресурс	resource	Строка	Техническое наименование ресурса из запроса
Действие	action	Строка	Техническое наименование действия из запроса
Условия	conditions	Массив	Список условий с подставленными значениями из ресурсных атрибутов

7.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 24.

Таблица 24 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Описание
Тип ошибки	type	Строка	Ошибка с сообщением или ошибка валидации
Информация об ошибке	payload	Строка/ Объект	Подробная информация об ошибке
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка

7.4. Пример выполнения запроса

Запрос:

```
POST http://{{host}}/authz/api/v1/user-  
profiles/conditions  
Content-Type: application/json  
Accept: application/json
```

```
{
  "userProfileUuid": "0152f40b-e12f-4fcb-ac23-
988c2b4f539b",
  "infoSystemTechName": "xidbox",
  "resourceType": "ordr_card_type",
  "resource": "ordr_card",
  "action": "read",
  "insertDynamicAttributes": false,
  "roleAttributeMap": {
    "ORDR_TYPE": "usr_reg"
  },
  "useRolesApplicabilityCondition": true
}
```

Ответ:

Content-Type: application/json

```
{
  "userProfileUuid": "0152f40b-e12f-4fcb-ac23-
988c2b4f539b",
  "infoSystemTechName": "xidbox",
  "resourceType": "ordr_card_type",
  "resource": "ordr_card",
  "action": "read",
  "conditions": [
    "true",
    "true",
    "true",

    "current_user.uuid.equals(CONTROL_OBJECT_UUID) ||
current_user_profile.uuid.equals(CONTROL_OBJECT_UUID)
",

    "current_user_profile.uuid.equals(AUTHOR_UUID)",

    "CONTROL_OBJECT_SYSTEMS.contains(controlled_system)",

    "ORDR_TYPE.equals('change_user_profile_roles') &&
```

```
ORDR_APPROVAL_STEP.equals(1) &&  
USER_PROFILE_ROLE_TECH_NAMES.contains('system_adminis  
trator') && true"  
    ]  
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Информационная система не найдена.",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

Ошибка валидации:

Content-Type: application/json

```
{  
  "type": "VALIDATION",  
  "payload": {  
    "fields": [  
      {  
        "fieldName": "resource",  
        "errors": "Данное поле должно содержать хотя  
бы один не пробельный символ"  
      }  
    ]  
  },  
  "timestamp": "2022-04-14T09:00:38.996714Z"  
}
```

8. Получение списка профилей УЗ пользователей разных организаций, для которых выполнена успешная авторизация для заданного ресурса и действия

Имя ресурса: /authz/api/v1/user-profiles-in-multiply-organizations

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Accept: application/json

8.1. Данные в запросе

Описание данных в запросе приведено в таблице 25.

Таблица 25 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Техническое наименование ИС	infoSystemTech Name	Строка	Да	Техническое наименование ИС
Тип ресурса	resourceType	Строка	Да	Техническое наименование типа ресурса
Ресурс	resource	Строка	Да	Техническое наименование ресурса
Действие	action	Строка	Да	Техническое наименование действия над ресурсом
Организации	organizationUuids	Массив	Нет	Список идентификаторов организаций, которым должен принадлежать профиль УЗ пользователя
Атрибуты	attributeMap	Объект	Нет	Список ресурсных атрибутов и их значения, используемые для авторизации

Параметр	Название параметра	Тип данных	Обязательность	Описание
Атрибуты роли	roleAttributeMap	Объект	Нет	Список атрибутов ролей и их значения, используемые для фильтрации ролей
Признак необходимости учета применимости роли	useRolesApplicabilityCondition	Логический	Нет	Информация о необходимости учета применимости роли. Значение «true» – если применимость роли учитывается при авторизации, значение «false» – если применимость роли не учитывается при авторизации. Значение по умолчанию – «true»
Максимальное количество профилей УЗ пользователя в ответе	limit	Целое число	Да	Максимальное количество профилей УЗ пользователя в ответе. Максимальное значение – 500
Идентификатор профиля УЗ пользователя, на котором остановились в предыдущем запросе	afterProfileUuid	UUID	Нет	Идентификатор профиля УЗ пользователя, на котором остановились в предыдущем запросе, при превышении в ответе количества профилей УЗ пользователей, указанного в параметре «limit». В ответе будут содержаться профили УЗ пользователей, следующие после профиля УЗ пользователя с указанным UUID

8.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 26.

Таблица 26 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Описание
Техническое наименование ИС	infoSystemTechName	Строка	Техническое наименование ИС
Тип ресурса	resourceType	Строка	Техническое наименование типа ресурса
Ресурс	resource	Строка	Техническое наименование ресурса
Действие	action	Строка	Техническое наименование действия над ресурсом
Количество профилей УЗ пользователей в ответе	count	Целое число	Количество профилей УЗ пользователей в ответе
Профили УЗ пользователя	userProfiles	Массив	Список профилей УЗ пользователя, которые могут совершить действия над ресурсом
Пользователь	user	Объект	Информация о УЗ пользователя
Идентификатор УЗ пользователя	uuid	UUID	Идентификатор УЗ пользователя
Имя	firstName	Строка	Имя пользователя
Фамилия	lastName	Строка	Фамилия пользователя
Отчество	middleName	Строка	Отчество пользователя
ИНН	inn	Строка	ИНН пользователя
СНИЛС	snils	Строка	СНИЛС пользователя
Почта УЗ пользователя	email	Строка	Адрес электронной почты УЗ пользователя
Профиль УЗ пользователя	userProfile	Объект	Информация о профиле УЗ пользователя
Идентификатор профиля УЗ пользователя	uuid	UUID	Идентификатор профиля УЗ пользователя
Почта профиля УЗ пользователя	workEmail	Строка	Адрес электронной почты профиля УЗ пользователя
Идентификатор организации	organizationUuid	UUID	Идентификатор организации

Параметр		Название параметра	Тип данных	Описание
	Полное наименование организации	organizationFullName	Строка	Полное наименование организации

8.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 27.

Таблица 27 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Описание
Тип ошибки	type	Строка	Ошибка с сообщением или ошибка валидации
Информация об ошибке	payload	Строка/ Объект	Подробная информация об ошибке
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка

8.4. Пример выполнения запроса

Запрос (без организаций):

```
POST http://{host}}/authz/api/v1/user-profiles-in-multiply-organizations
```

```
Content-Type: application/json
```

```
Accept: application/json
```

```
{
  "infoSystemTechName" : "xidbox",
  "resourceType" : "decision_type",
  "resource" : "decision",
  "action" : "create",
  "attributeMap" : {
    "ORDR_TYPE" : "usr_reg"
  },
  "useRolesApplicabilityCondition" : true,
  "limit" : 100,
```

```
"afterProfileUuid" : null
}
```

Запрос (с организациями):

```
POST http://{{host}}/authz/api/v1/user-profiles-in-
multiply-organizations
Content-Type: application/json
Accept: application/json
```

```
{
  "infoSystemTechName" : "xidbox",
  "resourceType" : "decision_type",
  "resource" : "decision",
  "action" : "create",
  "organizationUids" : [
    "c25ebd5e-6d16-44a5-9267-4d3a172cb0ba",
    "99986ef0-2e6a-4c3f-aa66-758d87ec07e0"
  ],
  "attributeMap" : {
    "ORDR_TYPE" : "usr_reg"
  },
  "useRolesApplicabilityCondition" : true,
  "limit" : 100,
  "afterProfileUuid" : "5b8588c2-0f9a-48aa-bfcb-
f6b0cfebe077"
}
```

Ответ:

```
Content-Type: application/json
```

```
{
  "infoSystemTechName" : "xidbox",
  "resourceType" : "decision_type",
  "resource" : "decision",
  "action" : "create",
  "count" : 2,
  "userProfiles" : [
    {
```

```
    "user" : {
      "uuid" : "6ae8dc72-d317-4466-b9af-
35aa81fbb3d4",
      "firstName" : "Для внешнего",
      "lastName" : "Для внешнего",
      "middleName" : null,
      "inn" : null,
      "snils" : null,
      "email" : "is_test@test.ru"
    },
    "userProfile" : {
      "uuid" : "b2e203d7-79bc-4bad-b6eb-
0a48b2deb09d",
      "workEmail" : "is_test@test.ru",
      "organizationUuid" : "c25ebd5e-6d16-44a5-
9267-4d3a172cb0ba",
      "organizationFullName" : "ИП Цепеш В."
    }
  },
  {
    "user" : {
      "uuid" : "2543a4ab-907a-4ead-9370-
bd16017bf3ae",
      "firstName" : "Илья",
      "lastName" : "ФОМИН",
      "middleName" : "НИКИТИЧ",
      "inn" : null,
      "snils" : null,
      "email" : "jija@localhost.ru"
    },
    "userProfile" : {
      "uuid" : "29a99f6b-2ce5-449a-8596-
c9517f425416",
      "workEmail" : "jija@localhost.ru",
      "organizationUuid" : "c25ebd5e-6d16-44a5-
9267-4d3a172cb0ba",
      "organizationFullName" : "ИП Цепеш В."
    }
  }
}
```

```
}
```

Ответ, когда кеш результата не найден:

HTTP/1.1 202

<Response body is empty>

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Информационная система не найдена.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка валидации:

Content-Type: application/json

```
{
  "type": "VALIDATION",
  "payload": {
    "fields": [
      {
        "fieldName": "resource",
        "errors": "Данное поле должно содержать хотя
бы один не пробельный символ"
      }
    ]
  },
  "timestamp": "2022-04-14T09:00:38.996714Z"
}
```

Лист регистрации изменений

Версия	Изменения
1.0.0	Начальная версия
1.0.1	—
1.0.2	—
1.0.3	—
1.0.4	—
1.0.5	—