



**платформа аутентификации и управления
доступом**

Руководство разработчика

Часть 10

Сервис аутентификации

Листов 262

Содержание

Перечень сокращений	12
Перечень терминов.....	13
Перечень электронных приложений	15
1. Заголовки, передаваемые в ИС	16
2. Получение информации из сессии пользователя	18
2.1. Получение данных аутентифицированного пользователя из сессии.....	18
2.1.1. Данные в запросе.....	18
2.1.2. Данные в ответе на запрос.....	18
2.1.3. Возможные ошибки	21
2.1.4. Пример выполнения запроса.....	21
2.2. Получение информации о пользователе по токenu сессии пользователя	23
2.2.1. Данные в запросе.....	23
2.2.2. Данные в ответе на запрос.....	24
2.2.3. Возможные ошибки	26
2.2.4. Пример выполнения запроса.....	27
2.3. Получение списка доступных для выбора профилей УЗ пользователя по сессии пользователя	29
2.3.1. Данные в запросе.....	29
2.3.2. Данные в ответе на запрос.....	30
2.3.3. Возможные ошибки	31
2.3.4. Пример выполнения запроса.....	31
2.4. Получение количества активных сессий профиля УЗ пользователя по сессии пользователя	33
2.4.1. Данные в запросе.....	33
2.4.2. Данные в ответе на запрос.....	34
2.4.3. Возможные ошибки	35
2.4.4. Пример выполнения запроса.....	35
2.5. Получение количества активных сессий профиля УЗ пользователя по идентификатору профиля УЗ пользователя.....	37

2.5.1. Данные в запросе.....	37
2.5.2. Данные в ответе на запрос.....	37
2.5.3. Возможные ошибки	38
2.5.4. Пример выполнения запроса.....	38
2.6. Получение списка активных сессий по идентификатору профиля УЗ пользователя.....	39
2.6.1. Данные в запросе.....	39
2.6.2. Данные в ответе на запрос.....	40
2.6.3. Возможные ошибки	40
2.6.4. Пример выполнения запроса.....	41
2.7. Получение списка активных сессий профиля УЗ пользователя по сессии пользователя.....	42
2.7.1. Данные в запросе.....	42
2.7.2. Данные в ответе на запрос.....	43
2.7.3. Возможные ошибки	44
2.7.4. Пример выполнения запроса.....	44
2.8. Обновление сессии аутентифицированного пользователя	46
2.8.1. Данные в запросе.....	47
2.8.2. Данные в ответе на запрос.....	47
2.8.3. Возможные ошибки	48
2.8.4. Пример выполнения запроса.....	48
2.9. Получение открытого ключа для проверки JWT	50
2.9.1. Данные в ответе на запрос.....	50
2.9.2. Возможные ошибки	50
2.9.3. Пример выполнения запроса.....	51
2.10. Получение информации о предыдущем входе пользователя	52
2.10.1. Данные в запросе.....	52
2.10.2. Данные в ответе на запрос.....	52
2.10.3. Возможные ошибки	53
2.10.4. Пример выполнения запроса.....	53

3. Получение настроек	55
3.1. Получение данных для отображения формы согласия на обработку персональных данных	55
3.1.1. Данные в ответе на запрос.....	55
3.1.2. Возможные ошибки	56
3.1.3. Пример выполнения запроса.....	56
3.2. Получение данных для отображения формы уведомления о мерах защиты информации.....	57
3.2.1. Данные в ответе на запрос.....	57
3.2.2. Возможные ошибки	58
3.2.3. Пример выполнения запроса.....	58
3.3. Получение списка доступных способов аутентификации для первого фактора по имени хоста	59
3.3.1. Данные в ответе на запрос.....	60
3.3.2. Возможные ошибки	61
3.3.3. Пример выполнения запроса.....	61
3.4. Получение настроек для страницы входа в ИС	62
3.4.1. Данные в ответе на запрос.....	62
3.4.2. Пример выполнения запроса.....	63
4. Аутентификация	64
4.1. Аутентификация с помощью логина и пароля	64
4.1.1. Данные в запросе.....	64
4.1.2. Данные в ответе на запрос.....	65
4.1.3. Возможные ошибки	66
4.1.4. Пример выполнения запроса.....	66
4.2. Аутентификация с помощью доменной учётной записи (по протоколу Kerberos).....	69
4.2.1. Данные в запросе.....	69
4.2.2. Данные в ответе на запрос.....	70
4.2.3. Возможные ошибки	70

4.2.4. Пример выполнения запроса.....	71
4.3. Двухфакторная аутентификация.....	72
4.3.1. Данные в запросе.....	73
4.3.2. Данные в ответе на запрос.....	74
4.3.3. Возможные ошибки	74
4.3.4. Пример выполнения запроса.....	75
4.4. Аутентификация с помощью сертификата	79
4.4.1. Данные в запросе.....	79
4.4.2. Данные в ответе на запрос.....	80
4.4.3. Возможные ошибки	81
4.4.4. Пример выполнения запроса.....	81
4.5. Аутентификация через Госуслуги (ЕСИА).....	85
4.5.1. Данные в запросе.....	85
4.5.2. Данные в ответе на запрос.....	86
4.5.3. Возможные ошибки	86
4.5.4. Пример выполнения запроса.....	87
4.5.5. Схема взаимодействия с адаптером ЕСИА	88
4.6. Получение уникального URL перенаправления пользователя для аутентификации через ЕСИА	89
4.6.1. Данные в ответе на запрос.....	89
4.6.2. Возможные ошибки	90
4.6.3. Пример выполнения запроса.....	90
4.7. Запрос кода для двухфакторной аутентификации	92
4.7.1. Данные в запросе.....	92
4.7.2. Данные в ответе на запрос.....	93
4.7.3. Возможные ошибки	94
4.7.4. Пример выполнения запроса.....	95
4.8. Получение доступных хостов для указанных способов аутентификации	96
4.8.1. Данные в запросе.....	97
4.8.2. Данные в ответе на запрос.....	97

4.8.3. Возможные ошибки	98
4.8.4. Пример выполнения запроса.....	98
5. Выход из системы.....	100
5.1. Выход из системы.....	100
5.1.1. Данные в запросе.....	100
5.1.2. Данные в ответе на запрос.....	100
5.1.3. Возможные ошибки	101
5.1.4. Пример выполнения запроса.....	101
5.2. Завершение всех сессий пользователя	103
5.2.1. Данные в запросе.....	103
5.2.2. Возможные ошибки	103
5.2.3. Пример выполнения запроса.....	104
5.3. Завершение активных сессий профиля УЗ пользователя, кроме текущей	104
5.3.1. Данные в запросе.....	104
5.3.2. Возможные ошибки	105
5.3.3. Пример выполнения запроса.....	105
5.4. Завершение всех активных сессий профиля УЗ пользователя	106
5.4.1. Данные в запросе.....	107
5.4.2. Данные в ответе на запрос.....	107
5.4.3. Возможные ошибки	107
5.4.4. Пример выполнения запроса.....	108
5.5. Завершение сессий заблокированных профилей УЗ пользователя	109
5.5.1. Данные в запросе.....	109
5.5.2. Возможные ошибки	109
5.5.3. Пример выполнения запроса.....	110
6. Аутентификация и получение данных о пользователе по OAuth 2.0	111
6.1. Возможные значения области доступа.....	117
6.2. Содержимое ID Token OpenId Connect 1.0.....	118
6.3. Получение авторизационного кода OAuth 2.0.....	123

6.3.1. Данные в запросе.....	123
6.3.2. Данные в ответе на запрос.....	124
6.3.3. Возможные ошибки	125
6.3.4. Пример выполнения запроса.....	125
6.4. Принятие решения о предоставлении доступа OAuth 2.0-клиенту к данным пользователя	127
6.4.1. Данные в запросе.....	127
6.4.2. Данные в ответе на запрос.....	129
6.4.3. Пример выполнения запроса.....	129
6.5. Получение OAuth 2.0 токенов доступа.....	131
6.5.1. Данные в запросе.....	131
6.5.2. Данные в ответе на запрос.....	133
6.5.3. Возможные ошибки	134
6.5.4. Пример выполнения запроса.....	134
6.6. Получение информации о токене OAuth 2.0.....	137
6.6.1. Данные в запросе.....	137
6.6.2. Данные в ответе на запрос.....	138
6.6.3. Возможные ошибки	140
6.6.4. Пример выполнения запроса.....	140
6.7. Обновление OAuth 2.0 токенов	142
6.7.1. Данные в запросе.....	142
6.7.2. Данные в ответе на запрос.....	143
6.7.3. Возможные ошибки	144
6.7.4. Пример выполнения запроса.....	144
6.8. Инвалидация OAuth 2.0 токена доступа.....	147
6.8.1. Данные в запросе.....	147
6.8.2. Возможные ошибки	148
6.8.3. Пример выполнения запроса.....	149
6.9. Получение данных УЗ пользователя с динамическими полями по токenu OAuth 2.0.....	150

6.9.1. Данные в запросе.....	150
6.9.2. Данные в ответе на запрос.....	151
6.9.3. Возможные ошибки	156
6.9.4. Пример выполнения запроса.....	156
6.10. Получение данных профиля УЗ пользователя с динамическими полями профиля УЗ пользователя и организации по токену OAuth 2.0.....	161
6.10.1. Данные в запросе.....	161
6.10.2. Данные в ответе на запрос.....	163
6.10.3. Возможные ошибки	172
6.10.4. Пример выполнения запроса.....	172
6.11. Получение всех описаний областей доступа (scope)	177
6.11.1. Данные в ответе на запрос.....	177
6.11.2. Возможные ошибки	178
6.11.3. Пример выполнения запроса.....	178
6.12. Получение наименования OAuth 2.0-клиента для отображения	180
6.12.1. Данные в запросе.....	180
6.12.2. Данные в ответе на запрос.....	181
6.12.3. Возможные ошибки	181
6.12.4. Пример выполнения запроса.....	181
6.13. Получение набора публичных ключей OAuth 2.0 сервера.....	182
6.13.1. Данные в ответе на запрос.....	182
6.13.2. Пример выполнения запроса.....	184
6.14. Получение конфигурации OAuth 2.0 сервера.....	185
6.14.1. Данные в ответе на запрос.....	185
6.14.2. Пример выполнения запроса.....	187
6.15. Получение конфигурации OpenId Connect 1.0	189
6.15.1. Данные в ответе на запрос.....	189
6.15.2. Пример выполнения запроса.....	194
6.16. Получение данных УЗ аутентифицированного пользователя через OpenId Connect 1.0	196

6.16.1. Данные в запросе.....	196
6.16.2. Данные в ответе на запрос.....	197
6.16.3. Возможные ошибки	199
6.16.4. Пример выполнения запроса.....	199
6.17. Выход из системы OpenID Connect 1.0	201
6.17.1. Данные в запросе.....	201
6.17.2. Возможные ошибки	202
6.17.3. Пример выполнения запроса.....	203
6.17.4. Сценарии выхода пользователя из системы.....	203
7. Обновление пароля.....	206
7.1. Обновление пароля.....	206
7.1.1. Данные в запросе.....	206
7.1.2. Возможные ошибки	206
7.1.3. Пример выполнения запроса.....	207
7.2. Обновление пароля по токену	207
7.2.1. Данные в запросе.....	207
7.2.2. Возможные ошибки	208
7.2.3. Пример выполнения запроса.....	208
7.3. Сброс пароля неаутентифицированным пользователем	209
7.3.1. Данные в запросе.....	209
7.3.2. Возможные ошибки	209
7.3.3. Пример выполнения запроса.....	210
7.4. Установка нового пароля пользователю	210
7.4.1. Данные в запросе.....	211
7.4.2. Возможные ошибки	211
7.4.3. Пример выполнения запроса.....	211
8. Обновление сессии пользователя	213
8.1. Установка профиля УЗ пользователя для текущей сессии	213
8.1.1. Данные в запросе.....	213
8.1.2. Данные в ответе на запрос.....	214

8.1.3. Возможные ошибки	217
8.1.4. Пример выполнения запроса.....	218
8.2. Обновление данных пользователя в текущей сессии	220
8.2.1. Данные в запросе.....	221
8.2.2. Данные в ответе на запрос.....	221
8.2.3. Возможные ошибки	225
8.2.4. Пример выполнения запроса.....	225
8.3. Установка признака отображения уведомления о мерах защиты информации для текущего пользователя	228
8.3.1. Данные в запросе.....	228
8.3.2. Данные в ответе на запрос.....	229
8.3.3. Возможные ошибки	232
8.3.4. Пример выполнения запроса.....	233
8.4. Установка признака согласия на обработку персональных данных для текущего пользователя.....	235
8.4.1. Данные в запросе.....	235
8.4.2. Данные в ответе на запрос.....	236
8.4.3. Возможные ошибки	238
8.4.4. Пример выполнения запроса.....	239
9. Подтверждение адреса электронной почты.....	242
9.1. Отправка ссылки с токеном для подтверждения адреса электронной почты УЗ пользователя	242
9.1.1. Данные в запросе.....	242
9.1.2. Пример выполнения запроса.....	242
9.2. Подтверждение адреса электронной почты УЗ пользователя по токenu	243
9.2.1. Данные в запросе.....	243
9.2.2. Пример выполнения запроса.....	243
9.3. Отправка ссылки с токеном для подтверждения адреса электронной почты профиля УЗ пользователя.....	244
9.3.1. Данные в запросе.....	244

9.3.2. Пример выполнения запроса.....	244
9.4. Проверка актуальности токена.....	245
9.4.1. Данные в запросе.....	245
9.4.1. Возможные ошибки	246
9.4.2. Пример выполнения запроса.....	246
10. Сценарий аутентификации из приложения ИС	247
10.1. Создание пароля для новой УЗ пользователя	247
10.2. Сброс пароля до аутентификации.....	248
10.3. Аутентификация	249
10.4. Получение информации из сессии пользователя	252
10.5. Обновление сессии пользователя.....	253
10.6. Обновление пароля после аутентификации.....	255
10.7. Выход из системы.....	255
Приложение А Пример системы-клиента для аутентификации через X-IDBox ..	257
Лист регистрации изменений	260

Перечень сокращений

ЕСИА	–	единая система идентификации и аутентификации
ИНН	–	идентификационный номер налогоплательщика
ИС	–	информационная система
КПП	–	код причины постановки на учёт
ОГРН	–	основной государственный регистрационный номер
ПДн	–	персональные данные
ПО	–	программное обеспечение
УЗ	–	учётная запись
JWT	–	JSON Web Token
OIDC	–	OpenID Connect
SDK	–	Software Development Kit

Перечень терминов

Авторизация	– предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом
Адаптер ЕСИА	– ПО «Адаптер-Инфраструктура» (Программное обеспечение программных библиотек (SDK) системы-клиента), которое обеспечивает взаимодействие ИС с ЕСИА
Аутентификация	– действия по проверке подлинности субъекта доступа и (или) объекта доступа, а также по проверке принадлежности субъекту доступа и (или) объекту доступа предъявленного идентификатора доступа и аутентификационной информации
Двухфакторная аутентификация	– метод проверки подлинности субъекта доступа при помощи запроса аутентификационных данных двух разных типов
Динамическое поле	– признак или свойство учётной записи пользователя, профиля учётной записи пользователя или организации, добавляемый из внешних источников, в т. ч. может задаваться ИС путем взаимодействия с сервисом X-IDBox
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
Интегрированная ИС	– ИС, подключенная к X-IDBox для использования ее сервисов
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
Приложение ИС	– структурная единица ИС, обеспечивающая возможность единого управления доступом в ИС, имеющую несколько приложений с идентичным или отличающимся набором функций, а также настройки способов аутентификации
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
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

Перечень электронных приложений

Название приложения		Имя файла
1	Пример системы-клиента для аутентификации через X-IDBox по OAuth2.0/ OpenID Connect 1.0	Руководство_разработчика_часть_10_spring-boot-oauth2-client.zip
2	Описание настроек системы-клиента для аутентификации через X-IDBox по OAuth2.0/ OpenID Connect 1.0	Руководство_разработчика_часть_10_настройки_spring-boot-oauth2-client.txt

1. Заголовки, передаваемые в ИС

Перечень заголовков, которые по умолчанию проставляются на основе сессии при проксировании запросов, приведён в таблице 1.

Таблица 1 – Заголовки запроса

Наименование заголовка	Тип данных	Описание
user-profile-uuid	UUID	Наименование заголовка, в котором передается идентификатор профиля УЗ пользователя
x-idbox-user-profile-uuid	UUID	Наименование заголовка, в котором передается идентификатор профиля УЗ пользователя
x-idbox-previous-successful-login-time	Дата и время	Наименование заголовка, в котором передается время предыдущего успешного входа
x-idbox-previous-failed-login-time	Дата и время	Наименование заголовка, в котором передается время предыдущей неудачной попытки входа
x-idbox-number-of-unsuccessful-attempts	Целое число	Наименование заголовка, в котором передается количество неудачных попыток входа

По запросу ИС предусмотрена возможность через службу технической поддержки настроить дополнительные заголовки, которые нужны ИС. Для этого ИС должны передать информацию о том, какие данные с какими наименованиями должны передаваться в заголовках. Наименование заголовка должно удовлетворять требованиям стандарта RFC-822, а данные должны выбираться из следующего перечня полей:

- основные поля УЗ пользователя:
 - uuid – идентификатор УЗ пользователя;
 - firstName – имя пользователя;
 - lastName – фамилия пользователя;
 - middleName – отчество пользователя;
 - inn – ИНН пользователя;
 - snils – СНИЛС пользователя;
 - birthday – дата рождения пользователя;
 - login – логин УЗ пользователя;
 - email – адрес электронной почты УЗ пользователя;
 - passwordChanged – дата и время установки текущего пароля;

- emailVerified – дата и время последней верификации адреса электронной почты УЗ пользователя;
- isBlocked – признак блокировки УЗ пользователя;
- state – состояние УЗ пользователя;
- privacy_policy_accepted – дата и время принятия согласия на обработку ПДн;
- security_policy_accepted – дата и время отключения уведомления о мерах защиты информации;
- основные поля профиля УЗ пользователя:
 - uuid – идентификатор профиля УЗ пользователя;
 - isBlocked – признак блокировки профиля УЗ пользователя;
 - state – состояние профиля УЗ пользователя;
 - workEmail – адрес электронной почты профиля УЗ пользователя;
 - workEmailVerified – дата и время последней верификации адреса электронной почты профиля УЗ пользователя;
- основные поля организации профиля УЗ пользователя:
 - uuid – идентификатор организации;
 - fullName – полное наименование организации;
 - shortName – сокращенное наименование организации;
 - inn – ИНН организации;
 - kpp – КПП организации;
 - ogrn – ОГРН организации;
 - isBlocked – признак блокировки организации;
 - state – состояние организации;
 - address – юридический адрес организации;
 - registrationDate – дата регистрации юридического лица;
- динамические поля УЗ пользователя;
- динамические поля профиля УЗ пользователя;
- динамические поля организации профиля УЗ пользователя.

2. Получение информации из сессии пользователя

2.1. Получение данных аутентифицированного пользователя из сессии

Имя ресурса: /authentication/api/v1/auth/user/uuid/by/session

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>

2.1.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 2.

Таблица 2 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Да	Сессия аутентифицированного пользователя

2.1.2. 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	Обязательность	Описание
Идентификатор	uuid	UUID	Да	Идентификатор пользователя
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя

Параметр	Название параметра	Тип данных	Обязательность	Описание
Адрес электронной почты профиля УЗ пользователя	userProfileWorkEmail	Строка	Нет	Адрес электронной почты профиля УЗ пользователя
Адрес электронной почты пользователя	email	Строка	Нет	Адрес электронной почты пользователя
Признак верификации адреса электронной почты пользователя	isEmailVerified	Логический	Да	Значение «true» – если адрес электронной почты пользователя верифицирован, значение «false» – если адрес электронной почты пользователя не верифицирован
Признак принятия пользователем согласия на обработку ПДн	needToAcceptPrivacyPolicy	Логический	Да	Значение «true» – если политика конфиденциальности не принята, значение «false» – если политика конфиденциальности принята
Признак отображения уведомления о мерах защиты	needToShowSecurityPolicy	Логический	Да	Значение «true» – если уведомление о мерах защиты включено, значение «false» – если уведомление о мерах защиты отключено
Признак отображения уведомления об отправке ссылки на подтверждение адреса электронной почты профиля УЗ пользователя	needToShowSendProfileEmailValidation	Логический	Да	Значение «true» – если отображение уведомления включено (если профиль УЗ пользователя не подтвержден, и настройки системы подразумевают отображение данного уведомления), значение «false» – если отображение уведомления отключено

Параметр	Название параметра	Тип данных	Обязательность	Описание
Пройденные способы аутентификации	authTypes	Массив	Да	Список пройденных способов аутентификации. Возможные значения: – LOGIN – логин и пароль; – CERT – сертификат; – KERBEROS_TICKET – доменная учётная запись с использованием протокола Kerberos; – CODE_FROM_EMAIL – подтверждение входа по коду, полученному на адрес электронной почты УЗ пользователя; – ESIA – Госуслуги (ЕСИА)
Разрешённые хосты с учётом первого фактора аутентификации	availableHostsBy FirstFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом первого фактора аутентификации
Разрешённые хосты с учётом второго фактора аутентификации	availableHostsBy SecondFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом второго фактора аутентификации
Список именованных атрибутов УЗ/профиля УЗ/организации пользователя	customUserProfileAttributes	Объект	Да	Список пар ключ/значение именованных атрибутов УЗ/профиля УЗ/организации пользователя. Используется для обогащения информации об аутентифицированном профиле УЗ пользователя
Время предыдущего успешного входа	previousSuccessfulLoginTime	Дата и время	Нет	Дата и время предыдущего успешного входа

Параметр	Название параметра	Тип данных	Обязательность	Описание
Количество неудачных попыток входа	numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin	Целое число	Нет	Количество неудачных попыток входа после предыдущего успешного входа
Время предыдущей неудачной попытки входа	previousFailedLoginTime	Дата и время	Нет	Дата и время предыдущей неудачной попытки входа

2.1.3. 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

2.1.4. Пример выполнения запроса

Запрос:

GET

http://{{host}}/authentication/api/v1/auth/user/uuid/by/session

Content-Type: application/json

Cookie: XIDBOXSession=

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZlRlc3NoVFRMI

jowLCJwcmV2aW91c1N1Y2Nlc3NmWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudW1iZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2a

W91c1N1Y2N1c3NmdWxMb2dpbiI6MCwic2Vzc2lvbklkIjoiMjYwOD
 U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
 vU2hvd1N1Y3VyaXR5UG9saWN5IjpmY
 WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn
 V1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU
 4ZmEiLCJpc0VtYWlsVmVyaWZpZWQiO
 nRydWUsInN1c3Npb25UVEwiOjAsImhhdCI6MTcyNTU0NjAzNH0.wX
 Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-
 lNOUaiO-JwicDi_labpTSacURDtfvFWZ
 QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
 KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
 1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
 yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IggNt_9FP1G_
 f4VPFw2fSJ6rtIR6PtKfjCqu7eU0AjRRNZ5gxxsLP2vNnh_NVQr7
 U45EIGOd9j-W8A

Ответ:

Content-Type: application/json

```
{
  "uuid": "0c54fdc5-4b00-4d3e-a521-2560d6d463d6",
  "userProfileUuid": "97149d84-90d1-49ff-ad63-f558cfef704d",
  "userProfileWorkEmail": "work_email@example.com",
  "email": "user_email@example.com",
  "isEmailVerified": true,
  "needToAcceptPrivacyPolicy": false,
  "needToShowSecurityPolicy": false,
  "needToShowSendProfileEmailValidation": false,
  "authTypes": [
    "ESIA"
  ],
  "availableHostsByFirstFactor": {
    "minitrue1984test": true,
    "xidbox.dcs.infosec.ru": true
  },
  "availableHostsBySecondFactor": {
    "xidbox.dcs.infosec.ru": true,
    "testhostlogin.ru": true
  }
}
```

```
    },  
    "customUserProfileAttributes": {  
      "customParam": "value"  
    },  
    "previousSuccessfulLoginTime": "2024-10-  
03T12:21:16.221556Z",  
    "numberOfUnsuccessfulAttemptsSincePrevious  
SuccessfulLogin": 0,  
    "previousFailedLoginTime": null  
  }  
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Сессия истекла.",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

2.2. Получение информации о пользователе по токenu сессии пользователя

Имя ресурса: /authentication/api/v1/auth/user/uuid/by/token

Метод: GET

HTTP-заголовки:

– Content-Type: application/json

2.2.1. Данные в запросе

Описание данных в запросе приведено в таблице 5.

Таблица 5 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Токен сессии пользователя	token	Строка	Да	Должно передаваться одно из значений «Cookie: XIDBOXSession» или «Cookie: JSESSION»

2.2.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 6.

Таблица 6 – Данные в ответе на запрос

Параметр	Наименование параметра	Тип данных	Обязательность	Описание
Идентификатор	uuid	UUID	Да	Идентификатор пользователя
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя
Адрес электронной почты профиля УЗ пользователя	userProfileWork Email	Строка	Нет	Адрес электронной почты профиля УЗ пользователя
Адрес электронной почты пользователя	email	Строка	Нет	Адрес электронной почты пользователя
Признак верификации адреса электронной почты пользователя	isEmailVerified	Логический	Да	Значение «true» – если адрес электронной почты пользователя верифицирован, значение «false» – если адрес электронной почты пользователя не верифицирован

Параметр	Наименование параметра	Тип данных	Обязательность	Описание
Признак принятия пользователем согласия на обработку ПДн	needToAcceptPrivacyPolicy	Логический	Да	Значение «true» – если политика конфиденциальности не принята, значение «false» – если политика конфиденциальности принята
Признак отображения уведомления о мерах защиты	needToShowSecurityPolicy	Логический	Да	Значение «true» – если уведомление о мерах защиты включено, значение «false» – если уведомление о мерах защиты отключено
Признак отображения уведомления об отправке ссылки на подтверждение адреса электронной почты профиля УЗ пользователя	needToShowSendProfileEmailValidation	Логический	Да	Значение «true» – если отображение уведомления включено (если профиль УЗ пользователя не подтвержден, и настройки системы подразумевают отображение данного уведомления), значение «false» – если отображение уведомления отключено
Пройденные способы аутентификации	authTypes	Массив	Да	Список пройденных способов аутентификации. Возможные значения: – LOGIN – логин и пароль; – CERT – сертификат; – KERBEROS_TICKET – доменная учётная запись с использованием протокола Kerberos; – CODE_FROM_EMAIL – подтверждение входа по коду, полученному на адрес электронной почты УЗ пользователя; – ESIA – Госуслуги (ЕСИА)

Параметр	Наименование параметра	Тип данных	Обязательность	Описание
Разрешённые хосты с учётом первого фактора аутентификации	availableHostsByFirstFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом первого фактора аутентификации
Разрешённые хосты с учётом второго фактора аутентификации	availableHostsBySecondFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом второго фактора аутентификации
Список именованных атрибутов УЗ/профиля УЗ/организации пользователя	customUserProfileAttributes	Объект	Да	Список пар ключ/значение именованных атрибутов УЗ/профиля УЗ/организации пользователя. Используется для обогащения информации об аутентифицированном профиле УЗ пользователя
Время предыдущего успешного входа	previousSuccessfulLoginTime	Дата и время	Нет	Дата и время предыдущего успешного входа
Количество неудачных попыток входа	numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin	Целое число	Нет	Количество неудачных попыток входа
Время предыдущей неудачной попытки входа	previousFailedLoginTime	Дата и время	Нет	Дата и время предыдущей неудачной попытки входа

2.2.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 7.

Таблица 7 – 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

2.2.4. Пример выполнения запроса

Запрос:

```
GET
http://{host}/authentication/api/v1/auth/user/uuid/
by/token?token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4
NTU5OC04NjI
1LTQxMmYtODkxZS1jNTMzZWZmM2M3YmYiLCJyZWZyZXNoVFRMIjow
LCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpc1RpbWUiOiIyMDI0LTA5L
TA1VDE0OjE1OjAyLjY4MDgxM1oiLCJ
udW1iZXJPZ1Vuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2aW91
c1N1Y2Nlc3NmdWxMb2dpc1I6MCwic2Vzc2lwbklkIjoimjYwODU1O
TgtODYyNS00MTJmLTg5MWUtYzUzM2V
hMzNjN2JmIiwibmVlZFRvU2hvd1N1Y3VyaXR5UG9saWN5IjpmYWxz
ZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1a
WQiOiJlMGJhYmE2My04NzMzLTQ4Y2Ut
ODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQiOnRyd
WUsInNlc3Npb25UVEwiOjAsIm1hdCI6MTcyNTU0NjAzNH0.wXZu6h
vvhXpNDaXUp70NZ7rqjaWzGQo8ze0hO
OJHK8S5Pczg0aXn-1NOUaiO-
JwicDi_labpTSacURDtFvFWZQqkxgP9UZnZ2g6v0rFwjPDumSflIH
x1zMeL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nym
CErA-1Rd
Tr9HdX6Vu4hwLBjE-
jjB7HynsZ3eQkNZM5n4hkrsjFG7mmyOL_PSFpKVT8G12VM64WQYD7
AfBh_z7SFLuF2KBk6IggqNt_9FP1G_f4VPFw2fSJ6rtIR6PtkfjCqu
7eU0AjRRNZ5gx
xsLP2vNnh_NVQr7U45EIGOd9j-W8A
Content-Type: application/json
```

Ответ:

Content-Type: application/json

```
{
  "uuid": "0c54fdc5-4b00-4d3e-a521-2560d6d463d6",
  "userProfileUuid": "97149d84-90d1-49ff-ad63-f558cfef704d",
  "userProfileWorkEmail": "work_email@example.com",
  "email": "user_email@example.com",
  "isEmailVerified": true,
  "needToAcceptPrivacyPolicy": false,
  "needToShowSecurityPolicy": false,
  "needToShowSendProfileEmailValidation": false,
  "authTypes": [
    "ESIA"
  ],
  "availableHostsByFirstFactor": {
    "minitrue1984test": true,
    "xidbox.dcs.infosec.ru": true
  },
  "availableHostsBySecondFactor": {
    "xidbox.dcs.infosec.ru": true,
    "testhostlogin.ru": true
  },
  "customUserProfileAttributes": {
    "customParam": "value"
  },
  "previousSuccessfulLoginTime": "2024-10-03T12:21:16.221556Z",
  "numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin": 0,
  "previousFailedLoginTime": null
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
```

```

    "type": "MESSAGE",
    "payload": "Сессия истекла.",
    "timestamp": "2022-04-14T08:31:58.423559Z"
  }

```

2.3. Получение списка доступных для выбора профилей УЗ

пользователя по сессии пользователя

Имя ресурса: /authentication/api/v1/auth/user-profiles/by/session

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>
- Cookie: JSESSION=<Сессия пользователя, находящегося в процессе аутентификации>

2.3.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 8.

Таблица 8 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет, если передаётся Cookie: JSESSION	Сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Cookie: JSESSION	Строка	Нет, если передаётся Cookie: XIDBOXSession	Сессия пользователя, находящегося в процессе аутентификации

Должно передаваться одно из значений «Cookie: XIDBOXSession» или «Cookie: JSESSION».

2.3.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 9.

Таблица 9 – Данные в ответе на запрос

Параметр	Наименование параметра	Тип данных	Обязательность	Описание
Список профилей УЗ пользователя	items	Массив	Да	Список профилей УЗ пользователя
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя
Идентификатор организации	organizationUuid	UUID	Да	Идентификатор организации, к которой привязан профиль УЗ пользователя
Краткое наименование организации	organizationShortName	Строка	Да	Краткое наименование организации, к которой привязан профиль УЗ пользователя
ИНН организации	organizationInn	Строка	Да	ИНН организации, к которой привязан профиль УЗ пользователя
КПП организации	organizationKpp	Строка	Нет	КПП организации, к которой привязан профиль УЗ пользователя
ОГРН организации	organizationOgrn	Строка	Нет	ОГРН организации, к которой привязан профиль

Параметр	Наименование параметра	Тип данных	Обязательность	Описание
Внешние идентификаторы организации	organizationExternalIdentifiers	Массив	Да	Список внешних идентификаторов организации, если отсутствуют, возвращается пустой список
Техническое наименование источника	fieldSourceTechName	Строка	Да	Техническое наименование источника
Техническое наименование поля	fieldTechName	Строка	Да	Техническое наименование поля
Значение идентификатора	value	Строка	Да	Значение идентификатора

2.3.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 10.

Таблица 10 – 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

2.3.4. Пример выполнения запроса

Запрос:

```
GET http://{host}/authentication/api/v1/auth/user-
profiles/by/session
Content-Type: application/json
Cookie: XIDBOXSession=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4
```

NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZ
XNoVFRMI
jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpcblRpbWUiOiIyMDI0LT
A5LTA1VDE0OjE1OjAyLjY4MDgxMloiLCJudWliZXJPZlVuc3VjY2V
zc2Z1bEF0dGVtcHRzU2luY2VQcmV2a
W91c1N1Y2Nlc3NmdWxMb2dpciI6MCwic2Vzc2lrbklkIjoimjYwOD
U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
vU2hvd1N1Y3VyaXR5UG9saWN5IjpmY
WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn
V1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU
4ZmEiLCJpc0VtYWlsVmVyaWZpZWQio
nRydWUsInNlc3Npb25UVEwiOjAsImIhdCI6MTcyNTU0NjAzNH0.wX
Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-
lNOUaiO-JwicDi_labpTSacURDtFvFWZ
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7
U45EIGOd9j-W8A

Ответ:

Content-Type: application/json

```
{
  "items": [
    {
      "userProfileUuid": "0152f40b-e12f-4fcb-ac23-988c2b4f539b",
      "organizationUuid": "c25ebd5e-6d16-44a5-9267-4d3a172cb0ba",
      "organizationShortName": "Стулья и сиденья",
      "organizationInn": "653718585092",
      "organizationKpp": null,
      "organizationOgrn": null,
      "organizationExternalIdentifiers": [
        {
          "fieldSourceTechName": "SVR",
          "fieldTechName": "orgCode",
          "value": "1232536"
```

```
    }  
  ]  
}  
]  
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Сессия истекла.",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

2.4. Получение количества активных сессий профиля УЗ

пользователя по сессии пользователя

Имя ресурса: /authentication/api/v1/auth/user-profile/sessions/for-current-session

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>
- Cookie: JSESSION=<Сессия пользователя, находящегося в процессе аутентификации>

2.4.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 11.
Описание данных в запросе приведено в таблице 12.

Таблица 11 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет, если передаётся Cookie: JSESSION	Сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Cookie: JSESSION	Строка	Нет, если передаётся Cookie: XIDBOXSession	Сессия пользователя, находящегося в процессе аутентификации

Должно передаваться одно из значений «Cookie: XIDBOXSession» или «Cookie: JSESSION».

Таблица 12 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя, для которого проверяется количество сессий. Идентификатор должен принадлежать аутентифицированному пользователю

2.4.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 13.

Таблица 13 – Данные в ответе на запрос

Параметр	Наименование параметра	Тип данных	Обязательность	Описание
Количество активных сессий	activeSessionAmount	Целое число	Да	Количество активных сессий

Параметр	Наименование параметра	Тип данных	Обязательность	Описание
Признак превышения максимального количества сессий	maxActiveSessionExceeded	Логический	Да	Значение «true» – если максимальное количество сессий превышено, значение «false» – если максимальное количество сессий не превышено

2.4.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 14.

Таблица 14 – 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

2.4.4. Пример выполнения запроса

Запрос:

```
GET http://{host}/authentication/api/v1/auth/user-
profile/sessions/for-current-
session?userProfileUuid=0152f40b-e12f-4fcb-ac23-
988c2b4f539b
Content-Type: application/json
Cookie: XIDBOXSession=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4
NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWZzM2M3YmYiLCJyZWZyZ
XNoVFRMI
```

```
jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LT
A5LTA1VDE0OjE1OjAyLjY4MDgxMloiLCJudWliZXJPZlVuc3VjY2V
zc2Z1bEF0dGVtcHRzU2luY2VQcmV2a
W91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lrbklkIjoimjYwOD
U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
vU2hvd1N1Y3VyaXR5UG9saWN5IjpmY
WxzZSwibmVlZFRvQWNjZXB0UHJpdmlFjeVBvbGljeSI6ZmFsc2UsIn
VlaWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU
4ZmEiLCJpc0VtYWlsVmVyaWZpZWQio
nRydWUsInNlc3Npb25UVEwiOjAsImhhdCI6MTcyNTU0NjAzNH0.wX
Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-
lNOUaiO-JwicDi_labpTSacURDtFvFWZ
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCERa-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8Gl2VM64WQYD7AfBh_z7SFLuF2KBk6IggNt_9FP1G_
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZ5gxxsLP2vNnh_NVQr7
U45EIGOd9j-W8A
```

Ответ:

Content-Type: application/json

```
{
  "activeSessionAmount": 0,
  "maxActiveSessionExceeded": false
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Сессия истекла.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Профиль принадлежит другому
пользователю, повторите вход.",
  "timestamp": "2024-10-03T13:08:51.673082362Z"
}
```

2.5. Получение количества активных сессий профиля УЗ пользователя по идентификатору профиля УЗ пользователя

Имя ресурса: /authentication/api/v1/auth/user-profile/sessions

Метод: GET

HTTP-заголовки:

– Content-Type: application/json

2.5.1. Данные в запросе

Описание данных в запросе приведено в таблице 15.

Таблица 15 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя, для которого проверяется количество сессий

2.5.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 16.

Таблица 16 – Данные в ответе на запрос

Параметр	Наименование параметра	Тип данных	Обязательность	Описание
Количество активных сессий	activeSessionAmount	Целое число	Да	Количество активных сессий
Признак превышения максимального количества сессий	maxActiveSessionExceeded	Логический	Да	Значение «true» – если максимальное количество сессий превышено, значение «false» – если максимальное количество сессий не превышено

2.5.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 17.

Таблица 17 – 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

2.5.4. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/authentication/api/v1/auth/user-profile/sessions?userProfileUuid=48d34c1b-3f7e-48fd-a8e4-53285a476f6e
Content-Type: application/json
```

Ответ:

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

```
{
  "activeSessionAmount": 0,
  "maxActiveSessionExceeded": false
}
```

Ошибка выполнения запроса:
Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "UserProfile not found by uuid:
1152f40b-e12f-4fcb-ac23-988c2b4f539b",
  "timestamp": "2024-08-26T14:57:22.317587366Z"
}
```

**2.6. Получение списка активных сессий по идентификатору профиля
УЗ пользователя**

Имя ресурса: /authentication/api/v1/auth/user-profile/sessions/all
Метод: GET
HTTP-заголовки:
– Content-Type: application/json

2.6.1. Данные в запросе

Описание данных в запросе приведено в таблице 18.

Таблица 18 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя, для которого проверяется список сессий

2.6.2. 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	Обязательность	Описание
Список активных сессий	items	Массив	Да	Список активных сессий
Идентификатор сессии	sessionId	Строка	Да	Идентификатор сессии
Дата и время создания сессии	sessionCreateDate	Дата и время	Да	Дата и время создания сессии
Атрибуты сессии	sessionAttributes	Массив	Да	Атрибуты сессии. При отсутствии атрибутов возвращается пустой массив
Наименование атрибута	label	Строка	Нет	Наименование атрибута
Значение атрибута	value	Строка	Нет	Значение атрибута

2.6.3. 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

2.6.4. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/authentication/api/v1/auth/user-  
profile/sessions/all?userProfileUuid=0152f40b-e12f-  
4fcb-ac23-988c2b4f539b  
Content-Type: application/json
```

Ответ:

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

```
{  
  "items": [  
    {  
      "sessionId": "3845d30b32bdb07ec5aa803183b374581  
e3cc1c95b578b1c785b459f50c0341b",  
      "sessionCreateDate": "2024-07-  
23T08:37:16.164Z",  
      "sessionAttributes": [  
        {  
          "label": "IP-адрес",  
          "value": "ip"  
        },  
        {  
          "label": "Браузер клиента",  
          "value": "browser"  
        }  
      ]  
    },  
    {  
      "sessionId": "59387db4fa1b291d143f32461513685a7  
8ede634f886c0308ac8f17d89f135ea",  
      "sessionCreateDate": "2024-07-  
23T09:07:22.740Z",  
      "sessionAttributes": []  
    }  
  ]  
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "UserProfile not found by uuid:
0252f40b-e12f-4fcb-ac23-988c2b4f539b",
  "timestamp": "2024-08-26T15:01:30.440962174Z"
}
```

2.7. Получение списка активных сессий профиля УЗ пользователя по сессии пользователя

Имя ресурса: /authentication/api/v1/auth/user-profile/sessions/all/for-current-session

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>
- Cookie: JSESSION=<Сессия пользователя, находящегося в процессе аутентификации>

2.7.1. 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
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет, если передаётся Cookie: JSESSION	Сессия аутентифицированного пользователя

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия пользователя, находящегося в процессе аутентификации	Cookie: JSESSION	Строка	Нет, если передаётся Cookie: XIDBOXSession	Сессия пользователя, находящегося в процессе аутентификации

Должно передаваться одно из значений «Cookie: XIDBOXSession» или «Cookie: JSESSION».

Таблица 22 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя, для которого проверяется список сессий. Идентификатор должен принадлежать аутентифицированному пользователю

2.7.2. 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	Обязательность	Описание
Список активных сессий	items	Массив	Да	Список активных сессий
Идентификатор сессии	sessionId	Строка	Да	Идентификатор сессии
Дата и время создания сессии	sessionCreateDate	Дата и время	Да	Дата и время создания сессии
Атрибуты сессии	sessionAttributes	Массив	Да	Атрибуты сессии. При отсутствии атрибутов возвращается пустой массив

Параметр	Название параметра	Тип данных	Обязательность	Описание
Наименование атрибута	label	Строка	Нет	Наименование атрибута
Значение атрибута	value	Строка	Нет	Значение атрибута

2.7.3. 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

2.7.4. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/authentication/api/v1/auth/user-
profile/sessions/all/for-current-
session?userProfileUuid=0152f40b-e12f-4fcb-ac23-
988c2b4f539b
Content-Type: application/json
Cookie: XIDBOXSession=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4
NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWZzM2M3YmYiLCJyZWZyZ
XNoVFRMI
jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LT
A5LTA1VDE0OjE0jAyljY4MDgxM1oiLCJudW1iZXJPZlVuc3VjY2V
zc2Z1bEF0dGVtcHRzU2luY2VQcmV2a
W91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lwbklkIjoimjYwOD
U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
vU2hvd1N1Y3VyaXR5UG9saWN5IjpmY
```

WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn
V1aWQiOiJlMGJhYmE2My04NzZLTQ4Y2UtODE2OC03MGY0OGYwNzU
4ZmEiLCJpc0VtYWlsVmVyaWZpZWQiO
nRydWUsInNlc3Npb25UVEwiOjAsImhhdCI6MTcyNTU0NjAzNH0.wX
Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0h0OJHK8S5Pczg0aXn-
lNOUaiO-JwicDi_labpTSacURDtfvFWZ
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxslP2vNnh_NVQr7
U45EIGOd9j-W8A

Ответ:

Content-Type: application/json

```
{
  "items": [
    {
      "sessionId": "3845d30b32bdb07ec5aa803183b374581e3cc1c95b578b1c785b459f50c0341b",
      "sessionCreateDate": "2024-07-23T08:37:16.164Z",
      "sessionAttributes": [
        {
          "label": "IP-адрес",
          "value": "127.0.0.1"
        },
        {
          "label": "Браузер клиента",
          "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/148.0.0.0 Safari/537.36"
        }
      ]
    },
    {
      "sessionId": "59387db4fa1b291d143f32461513685a78ede634f886c0308ac8f17d89f135ea",
```

```
    "sessionCreateDate": "2024-07-
23T09:07:22.740Z",
    "sessionAttributes": []
  }
]
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Сессия истекла.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Профиль принадлежит другому
пользователю, повторите вход.",
  "timestamp": "2024-10-03T13:08:51.673082362Z"
}
```

2.8. Обновление сессии аутентифицированного пользователя

Имя ресурса: /authentication/api/v1/jwt/refresh

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>

2.8.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 25.

Таблица 25 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Да	Сессия аутентифицированного пользователя

2.8.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 26. В ответе на запрос возвращается HTTP-заголовок.

Таблица 26 – Данные в HTTP-заголовке ответа на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Обновленная сессия аутентифицированного пользователя	Set-cookie: XIDBOXSession	Строка	Да	Новая сессия аутентифицированного пользователя
Информация о сроке действия сессии	Set-cookie: XIDBOXSessionTTL	Строка	Да	Информация о сроке действия сессии. Значение в формате .json, закодированное в base64 с полями: – jwtIssuedAt – значение обновления JWT в формате timestamp; – sessionTTL – срок действия JWT в секундах. Например, значение: XIDBOXSessionTTL= eyJqd3RJc3N1ZWRBd CI6MTc2OTYwNDMwMC wic2Vzc2lvb1RUTCI

Параметр	Название параметра	Тип данных	Обязательность	Описание
				6MTgwMH0=; содержимое: { "jwtIssuedAt"=1769604300, "sessionTTL"=1800 } Параметр доступен для клиентских скриптов (HttpOnly: false) и может использоваться в реализации фронтенд-логики приложений

2.8.3. 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

2.8.4. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/authentication/api/v1/jwt/refresh
Content-Type: application/json
Cookie: XIDBOXSession=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4
NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWZzM2M3YmYiLCJyZWZyZ
XNoVFRMI
```

```
jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LT  
A5LTA1VDE0OjE1OjAyLjY4MDgxMloiLCJudWliZXJPZlVuc3VjY2V  
zc2Z1bEF0dGVtcHRzU2luY2VQcmV2a  
W91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lwbklkIjoiMjYwOD  
U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRv  
U2hvd1N1Y3VyaXR5UG9saWN5IjpmY  
WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn  
V1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtoDE2OC03MGY0OGYwNzU  
4ZmEiLCJpc0VtYWlsVmVyaWZpZWQio  
nRydWUsInNlc3Npb25UVEwiOjAsImIhdCI6MTcyNTU0NjAzNH0.wX  
Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-  
lNOUaiO-JwicDi_labpTSacURDtfvFWZ  
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna  
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-  
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm  
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_  
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7  
U45EIGOd9j-W8A
```

Ответ:

Content-Type: application/json

Set-cookie:

```
XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJ  
JzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtoDkxZS1jNTMzZWEzM2M  
3YmYiLCJyZWZyZXNoVFRMIjowLCJwcmV2aW91c1N1Y2Nlc3NmdWxM  
b2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxMloiLC  
JudWliZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2aW  
91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lwbklkIjoiMjYwODU  
1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRv  
U2hvd1N1Y3VyaXR5UG9saWN5IjpmYWxzZSwibmVlZFRvQWNjZXB0U  
HJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04Nz  
MzMzLTQ4Y2UtoDE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZ  
pZWQioOnRydWUsInNlc3Npb25UVEwiOjAsImIhdCI6MTcyNTU0NjAz  
NH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0  
aXn-lNOUaiO-  
JwicDi_labpTSacURDtfvFWZQqkxgP9UZnZ2g6v0rFwjPDumSflIH  
x1zMeL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nym  
CErA-1RdTr9HdX6Vu4hwLBjE-  
jjB7HynsZ3eQkNZM5n4hkrsjFG7mmyOL_PSFpKVT8G12VM64WQYD7
```

```
AfBh_z7SFLuF2KBk6IgqNt_9FP1G_f4VPFw2fSJ6rtIR6PtkfjCqu
7eU0AjRRNZe5gxslP2vNnh_NVQr7U45EIGOd9j-W8A
Set-Cookie:
XIDBOXSessionTTL=eyJqd3RJc3N1ZWRBdCI6MTc2OTYwNDMwMCwi
c2Vzc2lvb1RUTCI6MTgwMH0=; Domain=localhost; Path=/
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Сессия истекла.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

2.9. Получение открытого ключа для проверки JWT

Имя ресурса: /authentication/api/v1/jwt/publickey

Метод: GET

2.9.1. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 28.

Таблица 28 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Открытый ключ	publicKey	Строка	Да	Открытый ключ для проверки JWT

2.9.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 29.

Таблица 29 – 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

2.9.3. Пример выполнения запроса

Запрос:

GET

`http://{host}/authentication/api/v1/jwt/publickey`

Ответ:

Content-Type: application/json

```
{
  "publicKey": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxkesnaI
chsJ6tVdL8ZrUtnB9wW8va8o3yIC51aBzooQ7pqtMhaLnycmQEQA
qtFM4HD1FkMb3n9mn3CJbE9kdb4TTCVwxK+TnCXk50mq2iUV99ETT
oC6d+8pkxp7IoBt808Y7jjNdArIL/W1VeGpraTqOLXHg5AJC4cdfW
dD6EM5HrHVu0m8TnkVDUZV+XAVjuV3iEl9cqsKXtrAeWVuisRR2eh
Xf26DRTI+usjy0e/7HADOGfC0RPKz1LZX0+G0VCYQYBe0vpXym1UO
gFhQMUB6fqGAiKE9/OMFmFOCHGNwF5OST1OXG9KB9g0igSoy46E6P
3Xzqg3WFxE1I9n/rQIDAQAB\n-----END PUBLIC KEY-----"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Ошибка получения ключей для проверки
токена.",
  "timestamp": "2024-09-16T10:48:11.880809375Z"
}
```

2.10. Получение информации о предыдущем входе пользователя

Имя ресурса: /authentication/api/v1/auth/user/previous-authn-info

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>

2.10.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 30.

Таблица 30 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Да	Сессия аутентифицированного пользователя

2.10.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 31.

Таблица 31 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Время предыдущего успешного входа	previousSuccessfulLoginTime	Дата и время	Да	Дата и время предыдущего успешного входа
Количество неудачных попыток входа	numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin	Целое число	Да	Количество неудачных попыток входа после предыдущего успешного входа

2.10.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 32.

Таблица 32 – 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

2.10.4. Пример выполнения запроса

Запрос:

GET

`http://{host}}/authentication/api/v1/auth/user/previous-authn-info`

Content-Type: application/json

Cookie:

XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZXNoVFRMI

jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudW1iZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2a

W91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lvbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1N1Y3VyaXR5UG9saWN5IjpmY

WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04NzZmLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQiO

nRydWUsInNlc3Npb25UVEwiOjAsIm1hdCI6MTcyNTU0NjAzNH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-lNOUaiO-JwicDi_labpTSacURDtfvFWZ

```
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7
U45EIGOd9j-W8A
```

Ответ:

Content-Type: application/json

```
{
  "previousSuccessfulLoginTime": "2025-02-
02T22:33:44.550Z",

  "numberOfUnsuccessfulAttemptsSincePreviousSuccessfulL
  ogin": 1
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Сессия истекла.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

3. Получение настроек

3.1. Получение данных для отображения формы согласия на обработку персональных данных

Имя ресурса: /authentication/api/v1/security-settings/privacy-policy

Метод: GET

3.1.1. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 33.

Таблица 33 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак отображения формы согласия на обработку ПДн	ask	Логический	Да	Значение «true» – если отображение формы согласия на обработку ПДн включено, параметры «Заголовок» и «Текст» заполняются, «false» – если отображение формы согласия на обработку ПДн отключено, параметры «Заголовок» и «Текст» не заполняются
Заголовок	header	Строка	Нет, если параметр ask = false	Текст заголовка
Текст	text	Строка	Нет, если параметр ask = false	Текст

3.1.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 34.

Таблица 34 – 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

3.1.3. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/authentication/api/v1/security-
settings/privacy-policy
```

Ответ:

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

```
{
  "ask": true,
  "header": "Политика конфиденциальности",
  "text": "Информируем Вас о реализации в системе мер
защиты информации и обработки персональных данных в
соответствии с 152-ФЗ «О персональных данных» и
правилами работы в системе!"
}
```

Ответ:

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

```
{
```

```
"ask": false,  
"header": null,  
"text": null  
}
```

Ошибка выполнения запроса:
Content-Type: application/json

```
{  
  "type": "UNKNOWN_ERROR",  
  "payload": "Произошла непредвиденная ошибка",  
  "timestamp": "2024-10-07T16:52:20.692408900Z"  
}
```

3.2. Получение данных для отображения формы уведомления о мерах защиты информации

Имя ресурса: /authentication/api/v1/security-settings/security-policy
Метод: GET

3.2.1. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 35.

Таблица 35 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак отображения уведомления о мерах защиты информации	ask	Логический	Да	Значение «true» – если отображение уведомления включено, параметры «Заголовок» и «Текст» заполняются, «false» – если отображение уведомления

Параметр	Название параметра	Тип данных	Обязательность	Описание
				отключено, параметры «Заголовок» и «Текст» не заполняются
Заголовок	header	Строка	Нет, если параметр ask = false	Текст заголовка
Текст	text	Строка	Нет, если параметр ask = false	Текст

3.2.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 36.

Таблица 36 – 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

3.2.3. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/authentication/api/v1/security-
settings/security-policy
```

Ответ:

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

```
{
  "ask": false,
```

```
"header": "Уведомление о реализованных в системе  
мерах защиты информации",  
"text": "Информируем Вас о реализации в системе мер  
защиты информации!"  
}
```

Ответ:

Content-Type: application/json

```
{  
  "ask": false,  
  "header": null,  
  "text": null  
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "UNKNOWN_ERROR",  
  "payload": "Произошла непредвиденная ошибка",  
  "timestamp": "2024-10-07T16:52:20.692408900Z"  
}
```

3.3. Получение списка доступных способов аутентификации для первого фактора по имени хоста

Имя ресурса: /authentication/api/v1/info-system/available-authentication-types-for-first-factor

Метод: GET

HTTP-заголовки:

– Content-Type: application/json

3.3.1. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 37.

Таблица 37 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Наименование хоста	host	Строка	Да	Наименование хоста, для которого получены способы аутентификации, берется из заголовка HOST-запроса
Способы аутентификации	types	Объект	Да	Список доступных способов аутентификации для хоста
Наименование способа аутентификации	%auth_type_name%	Массив	Нет	Список пар ключ/значение для разных способов аутентификации, где: – ключ – способ аутентификации; – значение – список хостов. Возможные значения способов аутентификации: – LOGIN – логин и пароль; – CERT – сертификат; – KERBEROS_TICKET – доменная учётная запись с использованием протокола Kerberos; – ESIA – Госуслуги (ЕСИА)
Признак необходимости отображать на странице входа опцию «Чужой компьютер»	enableOptionSomeoneElseComputer	Логический	Да	Значение «true» – если нужно отображать опцию, значение «false» – если не нужно отображать опцию

Параметр	Название параметра	Тип данных	Обязательность	Описание
Альтернативный хост ИС	alternativeHost	Строка	Нет	Альтернативный адрес текущей ИС, для которого у пользователя имеется хотя бы один доступный способ входа (если есть). Указывается, если для текущего хоста ИС у пользователя нет доступных способов входа

3.3.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 38.

Таблица 38 – 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

3.3.3. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/authentication/api/v1/info-
system/available-authentication-types-for-first-
factor
Content-Type: application/json
```

Ответ:

```
Content-Type: application/json
{
  "host": "xidbox.dcs.infosec.ru",
  "types": {
```

```
"ESIA": [  
  "xidbox.dcs.infosec.ru"  
],  
"KERBEROS_TICKET": [  
  "freeipa.xidbox.dcs.infosec.ru"  
],  
"LOGIN": [  
  "xidbox.dcs.infosec.ru"  
],  
"CERT": [  
  "tls.cert.xidbox.dcs.infosec.ru"  
]  
},  
"enableOptionSomeoneElseComputer": false,  
"alternativeHost": null  
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Отсутствует обязательный заголовок.",  
  "timestamp": "2024-09-16T10:48:11.880809375Z"  
}
```

3.4. Получение настроек для страницы входа в ИС

Имя ресурса: /authentication/api/v1/auth/properties

Метод: GET

HTTP-заголовки:

– Content-Type: application/json

3.4.1. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 39.

Таблица 39 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак необходимости отображать на странице входа опцию «Чужой компьютер»	enableOptionSomeoneElseComputer	Логический	Да	Значение «true» – если нужно отображать опцию, значение «false» – если не нужно отображать опцию
Признак необходимости отображать на странице входа кнопку «Зарегистрироваться»	registrationAnonymousAvailable	Логический	Да	Значение «true» – если нужно отображать кнопку, значение «false» – если не нужно отображать кнопку

3.4.2. Пример выполнения запроса

Запрос:

GET

`http://{{host}}/authentication/api/v1/auth/properties`

Content-Type: application/json

Ответ:

Content-Type: application/json

```
{
  "enableOptionSomeoneElseComputer": true,
  "registrationAnonymousAvailable": true
}
```

4. Аутентификация

В процессе аутентификации пользователя в cookie устанавливается сессия с наименованием JSESSION, которая обменивается на cookie с наименованием XIDBOXSession, после успешного выбора пользователем профиля УЗ пользователя. Если аутентифицированный пользователь проходит повторную аутентификацию, и в cookie присутствует действующая сессия с наименованием XIDBOXSession, то сессия с наименованием JSESSION не выдается. Если пользователь произвел смену профиля УЗ пользователя, то существующая сессия с наименованием XIDBOXSession обменивается на новую с тем же наименованием.

4.1. Аутентификация с помощью логина и пароля

Имя ресурса: /authentication/api/v1/auth/login

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession <Сессия аутентифицированного пользователя>

4.1.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 40.
Описание данных в запросе приведено в таблице 41.

Таблица 40 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Страница перенаправления после успешной аутентификации	Cookie: Auth-redirect	Строка	Нет	Страница перенаправления после успешной аутентификации. Необходим для указания страницы перенаправления после успешной аутентификации
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет	Сессия аутентифицированного пользователя

Таблица 41 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Логин	login	Строка	Да	Логин пользователя
Пароль	password	Строка	Да	Пароль пользователя

4.1.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 42. В ответе на запрос возвращаются HTTP-заголовки, приведенные в таблице 43.

Таблица 42 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Страница перенаправления после успешной аутентификации	location	Строка	Да	Страница перенаправления после успешной аутентификации

Таблица 43 – Данные в HTTP-заголовке ответа на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Set-cookie: XIDBOXSession	Строка	Нет	Обновленная сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Set-cookie: JSESSION	Строка	Нет	Новая сессия пользователя, находящегося в процессе аутентификации

Если пользователь не передал Cookie: XIDBOXSession, то выдается JSESSION (промежуточная сессия пользователя). Если пользователь передал XIDBOXSession, то возвращается обновленная XIDBOXSession.

4.1.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 44.

Таблица 44 – 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

4.1.4. Пример выполнения запроса

Запрос:

```
POST http://{{host}}/authentication/api/v1/auth/login
Content-Type: application/json
```

```
{
  "login": "login",
```

```
"password": "p@ssw0rd"
}
```

Ответ:

Content-Type: application/json

Set-cookie:

XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZXNoVFRMIjowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudW1iZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2aW91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lvbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1N1Y3VyaXR5UG9saWN5IjpmYWxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQ1OnRydWUsInNlc3Npb25UVEwiOiJAsIm1hdCI6MTcyNTU0NjAzNH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-lNOUaio-JwicDi_labpTSacURDtFvFWZQqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mmyOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IggNt_9FP1G_f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZ5gxxsLP2vNnh_NVQr7U45EIGOd9j-W8A

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Некорректный логин или пароль.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Content-Type: application/json

```
{
  "type": "MESSAGE",
```

```
"payload": "Учетная запись была временно  
заблокирована. Повторите попытку входа позднее.",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Учетная запись заблокирована.  
Обратитесь к Системному администратору или Менеджеру  
учетных записей.",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Некорректный логин или пароль. Осталось  
попыток: 5",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Невозможно войти в систему под данной  
учетной записью, т.к. уже выполнен вход под другим  
пользователем.",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Невозможно войти в систему.",  
  "timestamp": "2022-04-14T08:31:58.423559Z"
```

}

4.2. Аутентификация с помощью доменной учётной записи (по протоколу Kerberos)

Имя ресурса: /authentication/api/v1/auth/kerberos

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Authorization: Negotiate <Информация о билете Kerberos>
- Cookie: XIDBOXSession <Сессия аутентифицированного пользователя>

4.2.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 45.

Таблица 45 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Билет Kerberos	Authorization	Строка	Да	Билет Kerberos передается в заголовке «Authorization: Negotiate» HTTP-запроса
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет	Сессия аутентифицированного пользователя
Страница перенаправления после успешной аутентификации	Cookie: Auth-redirect	Строка	Нет	Страница перенаправления после успешной аутентификации. Необходим для указания страницы перенаправления после успешной аутентификации

4.2.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 46. В ответе на запрос возвращаются HTTP-заголовки, приведенные в таблице 47.

Таблица 46 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Страница перенаправления после успешной аутентификации	location	Строка	Да	Страница перенаправления после успешной аутентификации

Таблица 47 – Данные в HTTP-заголовке ответа на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Set-cookie: XIDBOXSession	Строка	Нет	Обновленная сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Set-cookie: JSESSION	Строка	Нет	Новая сессия пользователя, находящегося в процессе аутентификации

Если пользователь не передал Cookie: XIDBOXSession, то выдается JSESSION (промежуточная сессия пользователя). Если пользователь передал XIDBOXSession, то возвращается обновленная XIDBOXSession.

4.2.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 48.

Таблица 48 – 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

4.2.4. Пример выполнения запроса

Запрос:

POST

http://{host}/authentication/api/v1/auth/kerberos

Content-Type: application/json

Authorization: Negotiate

YIICzgYgKwYBBQUCoIIICwjCCAr6gDTALBgkqhkiG9xIBAgKiggKrB
IIICp2CCAqMGCSqGSIB3EgECAgEAboICKjCCAO6gAwIBBaEDAgEOog
cDBQAAAAAAo4IBk2GCAY8wgGGLoAMCAQWhHxsdRVhBTvBMRS5YSUR
CT1guRENTLklORk9TRUMuUlWiODA2oAMCAQOhLzAtGwRIVFRQGyVj
ZW50b3M3LmV4YW1wbGUueGlkYm94LmRjcy5pbmZvc2VjLnJlO4IBJ
zCCASOGAwIBEqEDAgEBooIBFQSCARHPYtIM1Zf4TD/R8MNNGb40R
NAMALhFDUt9PNXAEucjOWIOkc6I3++ndIA69uU1cjhX3wxZB6vYy9
Offhr9ISLwe1+AdJhuLgASPLHUMnZhrGxlpVtM0yAe406lsvRQ9l/
Io+o2WeFrk+I94SoBTGJQOWDF7CZ1hZsdPEklieFJ1ZF50RARyN+G
pmXhTt5Ofc9AxomG32d4WRtXqqQHR0/8RGXTe0WsyrM8igFALDBmp
ggkxSIre7wProBbZm6amWmZ8ktXuckz9NT7RsquyhbzBEI2fWc4gWa
V0mDVgo9hd9Cw1xUys/SAq/nVUfRZA634fg4K0BPmdgk4V8UnrjCs
oVXVxkyiZ17emgMP3ACgm8OkgeEwgd6gAwIBEqKB1gSB0yqav0lR5
a+s4p0tGP3XW4YkucZq0ncvEY18rXs3D1v7sNQDsoSKh5h6HcGGbI
Rgg6Nl3TS4MH+DwRPw87IlaT1821Asi+/hIktJXcyugnavzuH8FUF
Skyp1DtmzXSU71rUz5E/I1xB9uATOXXPcHCrtKVzrOsGsXJIm+Q3Y
t7qdo9/EYjn7euZtzGD2WkXG3A9UtbR8ztXjCjd4g0DKnTQAaRgJL
EwdVO+CRfwgnCnBxRZqc4om/qxlaklK+j3QAabr1H1FVIG+K2tsL5
gpPj0VH/w=

Ответ:

Content-Type: application/json

Set-cookie:

```
XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWUiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZXNoVFRMIjowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJjudW1iZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2aW91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lwbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1N1Y3VyaXR5UG9saWN5IjpmYWxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtoDE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQ1OnRydWUsInNlc3Npb25UVEwiOiJAsIm1hdCI6MTcyNTU0NjAzNH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-lNOUaiO-JwicDi_labpTSacURDtfvFWZQqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mmyOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxslP2vNnh_NVQr7U45EIGOd9j-W8A
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Невозможно войти под доменным пользователем.",
  "timestamp": "2023-04-06T06:38:05.602100900Z"
}
```

4.3. Двухфакторная аутентификация

Имя ресурса: /authentication/api/v1/auth/second-factor

Метод: POST

HTTP-заголовки:

– Content-Type: application/json

- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>
- Cookie: JSESSION=<Сессия пользователя, находящегося в процессе аутентификации>

4.3.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 49.

Описание данных в запросе приведено в таблице 50.

Таблица 49 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет, если передаётся Cookie: JSESSION	Сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Cookie: JSESSION	Строка	Нет, если передаётся Cookie: XIDBOXSession	Сессия пользователя, находящегося в процессе аутентификации

Таблица 50 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Код	code	Строка	Да	Код второго фактора аутентификации
Страница перенаправления после успешной аутентификации	Cookie: Auth-redirect	Строка	Нет	Страница перенаправления после успешной аутентификации. Необходим для указания страницы перенаправления после успешной аутентификации

4.3.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 51. В ответе на запрос возвращаются HTTP-заголовки, приведенные в таблице 52.

Таблица 51 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Страница перенаправления после успешной аутентификации	location	Строка	Да	Страница перенаправления после успешной аутентификации

Таблица 52 – Данные в HTTP-заголовке ответа на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Set-cookie: XIDBOXSession	Строка	Нет	Обновленная сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Set-cookie: JSESSION	Строка	Нет	Новая сессия пользователя, находящегося в процессе аутентификации

Если пользователь не передал Cookie: XIDBOXSession, то выдается JSESSION (промежуточная сессия пользователя). Если пользователь передал XIDBOXSession, то возвращается обновленная XIDBOXSession.

4.3.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 53.

Таблица 53 – 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

4.3.4. Пример выполнения запроса

Запрос:

POST

http://{host}/authentication/api/v1/auth/second-factor

Content-Type: application/json

Cookie:

XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmY

```
{
  "code": "1290"
}
```

Ответ:

Content-Type: application/json

Set-cookie:

XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZXNoVFRMIjowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudW1iZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2aW91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lvbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1N1Y3VyaXR5UG9saWN5IjpmYWxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQiOiOnRydWUsInNlc3Npb25UVEwiOiJAsImldhdCI6MTcyNTU0NjAz

NH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0
aXn-lNOUaiO-
JwicDi_labpTSacURDtFvFWZQqkxgP9UZnZ2g6v0rFwjPDumSflIH
x1zMeL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nym
CErA-1RdTr9HdX6Vu4hwLBjE-
jjB7HynsZ3eQkNZM5n4hkrsjFG7mmyOL_PSFpKVT8G12VM64WQYD7
AfBh_z7SFLuF2KBk6IgqNt_9FP1G_f4VPFw2fSJ6rtIR6PtkfjCqu
7eU0AjRRNZe5gxxsLP2vNnh_NVQr7U45EIGOd9j-W8A

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "ERROR_2FA",
  "payload": {
    "errorType": "AUTH_ERROR",
    "message": "Невозможно войти по коду.",
    "remainingAttemptCount": null,
    "validUntil": null
  },
  "timestamp": "2022-05-25T16:08:51.060989Z"
}
```

Ошибка выполнения запроса, если передан пустой параметр «code»:

Content-Type: application/json

```
{
  "type": "ERROR_2FA",
  "payload": {
    "errorType": "CODE_NOT_MATCH",
    "message": "Невозможно войти по коду.",
    "remainingAttemptCount": null,
    "validUntil": "2022-05-25T16:13:51.060989Z"
  },
  "timestamp": "2022-05-25T16:08:51.060989Z"
}
```

Ошибка выполнения запроса, если время сессии истекло или сессия неизвестна:

Content-Type: application/json

```
{
  "type": "ERROR_2FA",
  "payload": {
    "errorType": "AUTH_ERROR",
    "message": "Невозможно войти в систему. Повторите вход еще раз.",
    "remainingAttemptCount": null,
    "validUntil": null
  },
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка выполнения запроса, если попытка входа по коду второго фактора была unsuccessful:

Content-Type: application/json

```
{
  "type": "ERROR_2FA",
  "payload": {
    "errorType": "CODE_NOT_MATCH",
    "message": "Некорректный код. Осталось попыток ввода кода: 1",
    "remainingAttemptCount": 1,
    "validUntil": "2022-04-14T08:35:58.423559Z"
  },
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка выполнения запроса, если осталось «n» попыток входа (первый фактор):

Content-Type: application/json

```
{
  "type": "ERROR_2FA",
```

```
"payload": {
  "errorType": "AUTH_ERROR",
  "message": "Некорректный код. Повторите вход еще
раз. Осталось попыток: 1",
  "remainingAttemptCount": null,
  "validUntil": null
},
"timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка выполнения запроса, если закончились попытки входа:

Content-Type: application/json

```
{
  "type": "ERROR_2FA",
  "payload": {
    "errorType": "AUTH_ERROR",
    "message": "Учетная запись была временно
заблокирована. Повторите попытку входа позднее.",
    "remainingAttemptCount": null,
    "validUntil": null
  },
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка выполнения запроса, если код устарел и нужно запросить новый:

Content-Type: application/json

```
{
  "type": "ERROR_2FA",
  "payload": {
    "errorType": "CODE_EXPIRED",
    "message": "Код устарел. Запросите новый код.",
    "remainingAttemptCount": null,
    "validUntil": null
  },
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Ошибка выполнения запроса, если закончились попытки второго и первого фактора, и включена настройка бессрочного блокирования:

Content-Type: application/json

```
{
  "type": "ERROR_2FA",
  "payload": {
    "errorType": "AUTH_ERROR",
    "message": "Учетная запись заблокирована.",
    "remainingAttemptCount": null,
    "validUntil": null
  },
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

4.4. Аутентификация с помощью сертификата

Имя ресурса: /authentication/api/v1/auth/cert-tls

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- User-cert-tls: <Информация о сертификате, закодированном в base64>
- Cookie: XIDBOXSession <Сессия аутентифицированного пользователя>

4.4.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 54.

Таблица 54 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сертификат	user-cert-tls	Строка	Да	Информация о сертификате, закодированном в base64

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет	Сессия аутентифицированного пользователя
Страница перенаправления после успешной аутентификации	Cookie: Auth-redirect	Строка	Нет	Страница перенаправления после успешной аутентификации. Необходим для указания страницы перенаправления после успешной аутентификации

4.4.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 55. В ответе на запрос возвращаются HTTP-заголовки, приведенные в таблице 56.

Таблица 55 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Страница перенаправления после успешной аутентификации	location	Строка	Да	Страница перенаправления после успешной аутентификации

Таблица 56 – Данные в HTTP-заголовке ответа на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Set-cookie: XIDBOXSession	Строка	Нет	Обновленная сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Set-cookie: JSESSION	Строка	Нет	Новая сессия пользователя, находящегося в процессе аутентификации

Если пользователь не передал Cookie: XIDBOXSession, то выдается JSESSION (промежуточная сессия пользователя). Если пользователь передал XIDBOXSession, то возвращается обновленная XIDBOXSession.

4.4.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 57.

Таблица 57 – 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

4.4.4. Пример выполнения запроса

Запрос:

```
POST http://{host}}/authentication/api/v1/auth/cert-tls
```

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

```
user-cert-tls:
```

```
MIIIINgYJKoZIhvcNAQcCoIIIIJzCCCCMCAQExDjAMBggqhQMHAQECAgUAMAsGCSqGSIB3DQEHAaCCBXswggJzMIICIqADAgECAhA3QYiC9TmlkkrUTj3gAuo8MAgGBiqFAwICAzB/MSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGNyeXB0b3Byby5ydTElMAkGA1UEBhMCU1UxDzANBgNVBActBk1vc2NvdzEXMBUGA1UEChMOQ1JZUFRPLVBSTyBMTEMxITAfBgNVBAMTGENSESWVBUTy1QUk8gVGVzdCBDZW50ZXIgmJAeFw0xOTA1MjcwNzI0MjZaFw0yNDAlMjYwNzMDMDVaMH8xIzAhBgkqhkiG9w0BCQEWfHN1cHBvcnRAY3J5cHRvcHJvLnJlMQswCQYDVQQGEwJSVTEPMA0GA1UEBxMGTW9zY293MRcwFQYDVQQKEw5DU1lQVE8tUFJPIExMQzEhMB8GA1UEAxMYQ1JZUFRPLVBSTyBUZXN0IENlbmRlciAyMGMwHAYGKoUDAgITMBIGByqFAwICiWEGBYqFAwICHgEDQwAEQBSfFgSoq3ZRO59iO5HEvLzJrGAsZ3rDRQXu5qjKLtXre8L0iYEzUrMrx8rgbcoE1iuz
```

1xH+w8PUjwbG/N7w5KjeDB2MAsGA1UdDwQEAwIBhjAPBgNVHRMBA
f8EBTADAQH/MB0GA1UdDgQWBBROgz4Uae/sXXqVK18R/jcyFklVKz
ASBgkrBgEEAYI3FQEEBQIDAQABMCMGCSsGAQQBgjcVAQQWBBQEYlU
pCw6xzdf5fZq4yB9pnjaH8zAIBgYqhQMCAgMDQQDExbLVsTt/oSgq
g+5zc/Jq0PZojh1fEXVae3URTWOOfuXuPiVYIVKcPu38TgZD8fVBX
ikZZwIkuyPd5K5YSlpIMIIDADCCAq+gAwIBAgITEgBHxeIauKb+FR
zLZwABAEff4jAIBgYqhQMCAgMwfzEjMCEGCSqGSIB3DQEJARYUc3V
wcG9ydEBjcnlwdG9wcm8ucnUxCzAJBgNVBAYTA1JVMQ8wDQYDVQQH
EwZNB3Njb3cxZzAVBgNVBAoTDkNSWVBUTy1QUk8gTExDMSEwHwYDV
QQDExbDU1lQVE8tUFJPIFRlc3QgQ2VudGVyIDIwHhcnMTAwNzMTI
I0MDI5WhcnMTAwNzMTI1MDI5WjAbMRkwFwYDVQQDDDBBUZXR0IEN
lcnRpb3Njb3cxZzAVBgNVBAoTDkNSWVBUTy1QUk8gTExDMSEwHwYDV
BwEBAgIDQWAEQFuIOl6dMyr6TBTpwOmZbsBOz4v1+D3jbsTYKT0oB
s1R9ZoYGl7kgizlR66nP+zKxo0jZQa9MO1O2ks3dnZFrFqjggFhMI
IBXTAObgNVHQ8BAf8EBAMCBPAwHQYDVR0OBBYEFHTuD9gfREpt5T6
jWZrAvmWd2LWsmB8GA1UdIwQYMBaAFE6DPhRp7+xdepUrXxH+NzIW
SVUrMFwGA1UdHwRVMFMwUaBPoE2GS2h0dHA6Ly90ZXN0Y2EuY3J5c
HRvcHJvLnJlL0NlcnRFbnJvbGwvQ1JZUFRPLVBSTyUyMFRlc3Q1Mj
BDZW50ZXIlMjAyKDEpLmNybDCBrAYIKwYBBQUHAQEegZ8wgZwwZAY
IKwYBBQUHMAKGWgh0dHA6Ly90ZXN0Y2EuY3J5cHRvcHJvLnJlL0Nl
cnRFbnJvbGwvQ1JZUFRPLVBSTyUyMFRlc3Q1MjBUZXR0IENlbnRlc
iAyAhMSAEff4hq4pv4VHMtnAAEAR8XiMAwGC CqFAwCBAQICBQCgggF+MBgGCSqGSIB3DQEJAzelBgkqhkiG9w0BBw
EwHAYJKoZIhvcNAQkFMQ8XDTIwMDczMDE0MTU0NlowKgYKKwYBBAG
CN1gCATEcBBpEAG8AYwB1AG0AZQBuAHQAIABOAGEAbQBlADAvBgkq
hkiG9w0BCQQxIgQgIGoNYDHPzlg7c8vztB5nRULJ5qViaQzo8MnFB
FaP+GkwgeYGCyqGSIB3DQEJEAIVMYHWMiHTMIHQMIHNMAoGCCqFAw
cBAQICBCCBy2gCb208JGb9VpMji4DSWVERTzt3mibXUel9ke7R65zC
BnDCBhKSBgTB/MSMwIQYJKoZIhvcNAQkBFhRzdXBwb3J0QGNyeXB0
b3Byby5ydTELMakGA1UEBhMCU1UxZzANBgNVBAcTBk1vc2NvdzEXM
BUGA1UEChMOQ1JZUFRPLVBSTyBMTEMxITAfBgNVBAMTGNSWVBUTy
1QUk8gVGZvdCBDZW50ZXIgmGITEgBHxeIauKb+FRzLZwABAEff4jA

MBggqhQMHAQEBAQUABEAe7hvI39KrefmfMdt1Fd0+YhLvDbiOh87g
bBuGCSmiScavJjkwfE+Rj5yNv6L2Wr2yUWEpA7Io+iU8DHbUZ2Hm

Ответ:

Content-Type: application/json

Set-cookie:

XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzZWIiOiIyYnA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWZzM2M3YmYiLCJyZWZyZXNoVFRMIjowLCJwcmV2aW91c1NlY2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxMl0iLCJjudWl1ZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2aW91c1NlY2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lvbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1NlY3VyaXR5UG9saWN5IjpmYWxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQ1OnRydWUsInNlc3Npb25UVEwiOiJAsIm1hdCI6MTcyNTU0NjAzNH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-1NOUaiO-

JwicDi_labpTSacURDtfvFWZQqkxgP9UZnZ2g6v0rFwjPDumSflIH
x1zMeL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nym
CErA-1RdTr9HdX6Vu4hwLBjE-

jjB7HynsZ3eQkNZM5n4hkrsjFG7mmyOL_PSFpKVT8Gl2VM64WQYD7
AfBh_z7SFLuF2KBk6IgqNt_9FP1G_f4VPFw2fSj6rtIR6PtkfjCqu
7eU0AjrRNZe5qxxsLP2vNnh NVQr7U45EIGOd9j-W8A

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Невозможно войти в систему по сертификату.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

Content-Type: application/json

 $\{$

```
"type": "MESSAGE",  
"payload": "Учетная запись была временно  
заблокирована. Повторите попытку входа позднее.",  
"timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Учетная запись заблокирована.  
Обратитесь к Системному администратору или Менеджеру  
учетных записей.",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Невозможно войти в систему под данной  
учетной записью, т.к. уже выполнен вход под другим  
пользователем.",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Невозможно войти в систему по  
предоставленному сертификату.",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Невозможно войти в систему.",  
}
```

```
"timestamp": "2022-04-14T08:31:58.423559Z"
}
```

4.5. Аутентификация через Госуслуги (ЕСИА)

Имя ресурса: /authentication/api/v1/auth/esia

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Esia-state: <Уникальный идентификатор запроса>
- Esia-code: <Авторизационный код, полученный через ЕСИА>
- Cookie: XIDBOXSession <Сессия аутентифицированного пользователя>

4.5.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 58.

Таблица 58 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет	Сессия аутентифицированного пользователя
Идентификатор запроса	esia-state	UUID	Да	Уникальный идентификатор запроса
Авторизационный код из ЕСИА	esia-code	UUID	Да	Авторизационный код, полученный через ЕСИА
Страница перенаправления после успешной аутентификации	Cookie: Auth-redirect	Строка	Нет	Страница перенаправления после успешной аутентификации. Необходим для указания страницы перенаправления после успешной аутентификации

4.5.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 59. В ответе на запрос возвращаются HTTP-заголовки, приведенные в таблице 60.

Таблица 59 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Страница перенаправления после успешной аутентификации	location	Строка	Да	Страница перенаправления после успешной аутентификации

Таблица 60 – Данные в HTTP-заголовке ответа на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Set-cookie: XIDBOXSession	Строка	Нет	Обновленная сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Set-cookie: JSESSION	Строка	Нет	Новая сессия пользователя, находящегося в процессе аутентификации

Если пользователь не передал Cookie: XIDBOXSession, то выдается JSESSION (промежуточная сессия пользователя). Если пользователь передал XIDBOXSession, то возвращается обновленная XIDBOXSession.

4.5.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 61.

Таблица 61 – 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

4.5.4. Пример выполнения запроса

Запрос:

```
POST http://{host}/authentication/api/v1/auth/esia
Content-Type: application/json
Esia-state: bdd6b8e9-08fc-43c8-a7ef-9ea1ad0a278b
Esia-code: 86f25749-2930-4e03-ad3a-71e24f848e6c
```

Ответ:

Content-Type: application/json
Set-cookie:
XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZXNoVFRMIjowLCJwcmV2aW91c1NlY2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudW1iZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2aW91c1NlY2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lwbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1NlY3VyaXR5UG9saWN5IjpmYWxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQiOiOnRydWUsInNlc3Npb25UVEwiOiJAsImldhdCI6MTcyNTU0NjAzNH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-lNOUaiO-
JwicDi_labpTSacURDtfvFWZQqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMEL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-1RdTr9HdX6Vu4hwLBjE-
jjB7HynsZ3eQkNZM5n4hkrsjFG7mmyOL PSFpKVT8G12VM64WQYD7

AfBh_z7SFLuF2KBk6IgqNt_9FP1G_f4VPFw2fSJ6rtIR6PtkfjCqu
7eU0AjRRNZe5gxslP2vNnh_NVQr7U45EIGOd9j-W8A

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Невозможно войти через ЕСИА.",  
  "timestamp": "2024-08-15T06:38:05.602100900Z"  
}
```

4.5.5. Схема взаимодействия с адаптером ЕСИА

Для аутентификации пользователей в X-IDBox через Госуслуги (ЕСИА) используется ПО «Адаптер ЕСИА», которое обеспечивает упрощенное подключение операторов ИС к ЕСИА.

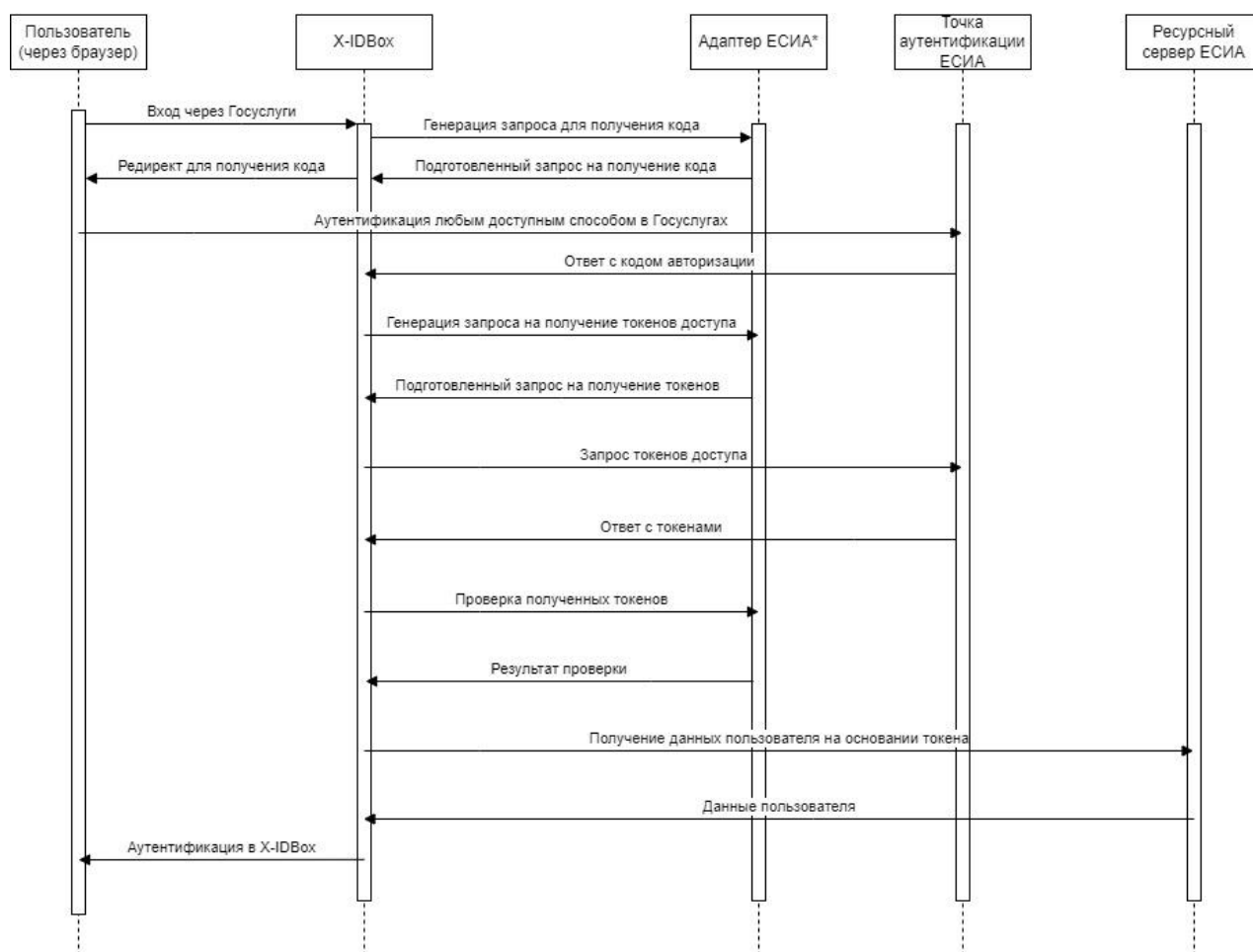
Подробная информация об адаптере ЕСИА представлена на официальном сайте:

<https://digitalcryptography.ru/projects/nashi-proekty/adapter/>

Для корректного функционирования в конфигурации адаптера ЕСИА должны быть:

- настроена мнемоника ИС;
- настроен криптоконтейнер с ключами для подписания запросов;
- установлены актуальные корневые сертификаты и выполнены сопутствующие настройки.

Схема взаимодействия X-IDBox с адаптером ЕСИА представлена на рис. 1.



* Под адаптером ЕСИА подразумевается типовое решение в виде программного обеспечения «Адаптер-Инфраструктура»

Рисунок 1 – Схема взаимодействия X-IDBox с адаптером ЕСИА

4.6. Получение уникального URL перенаправления пользователя для аутентификации через ЕСИА

Имя ресурса: /authentication/api/v1/auth/esia/person/redirect

Метод: GET

HTTP-заголовки:

– Content-Type: application/json

4.6.1. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 62.

Таблица 62 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Адрес для перенаправления	redirectUrl	Строка	Да	Сгенерированный адрес для перенаправления пользователя в ЕСИА

4.6.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 63.

Таблица 63 – 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

4.6.3. Пример выполнения запроса

Запрос:

GET

http://{{host}}/authentication/api/v1/auth/esia/person/redirect

Content-Type: application/json

Ответ:

Content-Type: application/json

```
{
  "redirectUrl": "http://esia-
mock.xidbox.dcs.infosec.ru:8090/aas/oauth2/ac?response_type=code&client_id=RKZN31&redirect_uri=http%3A%2F%
2Flocalhost%3A8090%2Fesia%2Fcallback&scope=openid%20s
```

nils%20inn%20email%20usr_org%20fullname&state=3a6f5ef
3-1667-473c-81f5-
f01b981510f8×tamp=2024.08.14%2016%3A27%3A20%20%2
B0300&client_secret=MIAGCSqGSib3DQEHAqCAMIACAQExDjAMB
ggqhQMHAQECAGUAMIAGCSqGSib3DQEHAaCAJIAEam9w%0D%0AZW5p
ZCBzblscYBpbm4gZW1haWwgdXNyX29yZyBmdWxsbmFtZTIwMjQuM
DguMTQgMTY6Mjc6MjAg%0D%0AKzAzMDBSS1pOMzEzYTZmNWVmMy0x
NjY3LTQ3M2MtODFmNS1mMDFiOTgxNTEwZjgAAAAAACggDCC%0D%0
AA0wwggL5oAMCAQICEyIAAGSwynqRhse1kZkAAAAAZLAWCgYIKoUD
BwEBAwIwETEPMA0GA1UEAxMG%0D%0AQ0EtRENTMB4XDTI0MDQyNzE
xMjI1OVVoXDTI1MDcyNzExMzI1OVowgdMxFDASBgNVBAMTC3Rlc3Qg
%0D%0AY2VydCAzMRRwGgYJKoZIhvcNAQkBFglpc2ZrQGVtYWlsLnJ
1MQ0wCwYDVQQJEwR0ZXN0MQ0wCwYD%0D%0AVQQKEwR0ZXN0MQ0wCw
YDVQQLEwR0ZXN0MRUwEwYDVQQQHHgwEHAQ%2BBEEE0gQyBDAXGzAZB
gNVBAge%0D%0AEgA3ADcAIAQcBD4EQQQ6BDIEMDELMAkGA1UEBhMC
UlUxFTATBgUqhQNkBBIKNzcXMDU2ODc2MDEY%0D%0AMBYGBSgFA2Q
BEg0xMDQ3Nzk3MDE5ODMwMGYwHwYIKoUDBwEBAQEwEwYHkoUDAgIk
AAAYIKoUDBwEB%0D%0AAgIDQwAEQLGGM%2BzMP%2BuDSOCOJ8dpVm4
6BsmMUYhSDM4OppaQ0Gi%2FBECOauDAKoIkUHsZkJiu27s9%0D%0A
rncOifcicn7m47sWk5ajggFeMIIBWjATBgNVHSUEDDAKBggrBgEFB
QcDAzALBgNVHQ8EBAMCBPAw%0D%0AHQYDVR0OBByEFezMCPhHW1Xa
UcTidq6DAoy0%2BNkPMB8GA1UdIwQYMBaAFAXTyBUuKTN4L1YXJs3
d%0D%0Asd%2FkYIz8MGwGA1UdHwRlMGMyaBfoF2GLmh0dHA6Ly9j
YS5kY3MuaW5mb3NlYy5ydS9DZXJ0RW5y%0D%0Ab2xsL0NBLURDUy5
jcmYgK2h0dHA6Ly9jYWRjcy5pdHNvYy5ydS9DZXJ0RW5yb2xsL0NB
LURDUy5j%0D%0AcwwgYcGCCsGAQUFBwEBBHsweTBMBggrBgEFBQc
wAoZAaHR0cDovL2NhLmRjcy5pbmZvc2VjLnJl%0D%0AL0NlcnRFbn
JvbGwvY2EuZGNzLmluZm9zZWmucnVfQ0EtRENTLmNydDAPBggrBgE
FBQcwAYYdaHR0%0D%0AcDovL2NhLmRjcy5pbmZvc2VjLnJlL29jc3
AwCgYIKoUDBwEBAwIDQQBC5xIiOFaNuYQEUojkKbAW%0D%0AL6DzD
yJt56lw7DY7J6yUT%2BzreOqI2qKgo7nN29QAZFCPH55lm69%2Bbt
ACTqsEzubiAAAxggF5MIIB%0D%0AdQIBATAoMBExDzANBgNVBAMTB
kNBLURDUwITIGAAZLDKegGGx7WRmQAAAABksDAMBggqhQMHAQEC%0
D%0AAgUAoIHpMBgGCSqGSib3DQEJAzelBgkqhkiG9w0BBwEwKQYJK
oZIhvcNAQk0MRwwGjAMBggqhQMh%0D%0AAQECAgUAoQoGCCqFAwcB
AQEBMC8GCSqGSib3DQEJBDEiBCAOwTHVpjzs8YLZfolqfVK8HKQPv
cmg%0D%0AUkufo2KRlCL95DBxBgsqhkiG9w0BCRACLzFiMGAWXjBc
MAoGCCqFAwcBAQICBCBJ819RP63zE8Uc%0D%0AK%2B3a3miYWFftv
%2BqT6D3PsuZyh80lRjAsMBWkEzARMQ8wDQYDVQQDEwZDQS1EQ1MC
EyIAAGSwynqR%0D%0Ahse1kZkAAAAAZLAWCgYIKoUDBwEBAQEEEQEc

```
nzp6TYNC%2Bk%2FfXDPGWewET3tPLymwn1wozk1EsYmYF%0D%0Avx  
txTWqLD3wtNpcklQubBtL66Oq9qLN1QsZpe8%2Bsx7kAAAAAAAAA%3  
D&access_type=offline"  
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "UNKNOWN_ERROR",  
  "payload": "Произошла непредвиденная ошибка",  
  "timestamp": "2024-08-15T12:29:37.643746300Z"  
}
```

4.7. Запрос кода для двухфакторной аутентификации

Имя ресурса: /authentication/api/v1/auth/second-factor/send-code

Метод: POST

HTTP-заголовки:

– Cookie: XIDBOXSession <Сессия аутентифицированного пользователя>

– Cookie: JSESSION <Сессия пользователя, находящегося в процессе аутентификации>

4.7.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 64.

Таблица 64 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет, если передаётся Cookie: JSESSION	Сессия аутентифицированного пользователя

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия пользователя, находящегося в процессе аутентификации	Cookie: JSESSION	Строка	Нет, если передаётся Cookie: XIDBOXSession	Сессия пользователя, находящегося в процессе аутентификации

Если пользователь не передал Cookie: XIDBOXSession, то выдается JSESSION (промежуточная сессия пользователя). Если пользователь передал XIDBOXSession, то возвращается обновленная XIDBOXSession.

4.7.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 65.

Таблица 65 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак необходимости ввода кода двухфакторной аутентификации	need_to_input_two_factor_code	Логический	Нет	Значение «true» – если нужно ввести код двухфакторной аутентификации, значение «false» – если не нужно вводить код двухфакторной аутентификации
Количество времени до окончания действия кода двухфакторной аутентификации в секундах	counter	Целое число	Нет	Количество времени до окончания действия кода двухфакторной аутентификации в секундах
Количество оставшихся попыток ввода кода двухфакторной аутентификации	remainingAttemptCount	Целое число	Нет	Количество оставшихся попыток ввода кода двухфакторной аутентификации пользователем

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак необходимости подтверждения адреса электронной почты	need_to_verify_email	Логический	Нет	Значение «true» – если пользователю нужно подтвердить адрес электронной почты, значение «false» – если пользователю не нужно подтверждать адрес электронной почты
Признак необходимости принятия согласия на обработку ПДн	need_to_accept_privacy_policy	Логический	Нет	Значение «true» – если пользователю нужно принять политику конфиденциальности, значение «false» – если пользователю не нужно принять политику конфиденциальности
Маскированный адрес электронной почты пользователя	userMaskedEmail	Строка	Нет	Маскированный адрес электронной почты пользователя

4.7.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 66.

Таблица 66 – 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

4.7.4. Пример выполнения запроса

Запрос:

POST

`http://{{host}}/authentication/api/v1/auth/second-factor/send-code`

Cookie:

`XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZXNoVFRMIjowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudWliZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2aW91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lvbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1NlY3VyaXR5UG9saWN5IjpmYXxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQioInRydWUsInNlc3Npb25UVEwiOiJAsImIhdCI6MTcyNTU0NjAzNH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-lNOUaiO-JwicDi_labpTSacURDtfvFWZQqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mmYOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IggNt_9FP1G_f4VPFw2fSJ6rtIR6PtKfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7U45EIGOd9j-W8A`

Ответ:

Content-Type: application/json

```
{
  "remainingAttemptCount": 10,
  "need_to_input_two_factor_code": true,
  "counter": 60,
  "userMaskedEmail": "R***m@infosec.ru"
}
```

Ответ:

Content-Type: application/json

```
{
  "need_to_verify_email": true
  "userMaskedEmail": "R***m@infosec.ru"
}
```

Ответ:

Content-Type: application/json

```
{
  "need_to_accept_privacy_policy": true
  "userMaskedEmail": "R***m@infosec.ru"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Сессия истекла.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

4.8. Получение доступных хостов для указанных способов аутентификации

Имя ресурса: /authentication/api/v1/info-system/available-hosts-by-auth-types

Метод: GET

HTTP-заголовки:

– Content-Type: application/json

4.8.1. Данные в запросе

Описание данных в запросе приведено в таблице 67.

Таблица 67 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Способы аутентификации	authTypes	Строка	Да	Способы аутентификации, для которых необходимо получить доступные хосты. Возможные значения: – LOGIN – логин и пароль; – CERT – сертификат; – KERBEROS_TICKET – доменная учётная запись с использованием протокола Kerberos; – CODE_FROM_EMAIL – подтверждение входа по коду, полученному на адрес электронной почты УЗ пользователя; – ESIA – Госуслуги (ЕСИА)

4.8.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 68.

Таблица 68 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Хосты, разрешающие аутентификацию первому фактору запрашиваемого способа	firstFactor	Массив	Да	Хосты, разрешающие аутентификацию первому фактору запрашиваемого способа

Параметр	Название параметра	Тип данных	Обязательность	Описание
Хосты, разрешающие аутентификацию второму фактору запрашиваемого способа	secondFactor	Массив	Да	Хосты, разрешающие аутентификацию второму фактору запрашиваемого способа

4.8.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 69.

Таблица 69 – 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

4.8.4. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/authentication/api/v1/info-
system/available-hosts-by-auth-
types?authTypes=LOGIN,ESIA
Content-Type: application/json
```

Ответ:

```
Content-Type: application/json
{
  "firstFactor": [
    "testhostlogintest_9655",
    "testhostlogin",
    "testhostloginautotest_system_hoyrvjkbpw",
  ],
```

```
    "secondFactor": []  
  }
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Отсутствует обязательный параметр  
authTypes",  
  "timestamp": "2024-09-12T13:36:19.765491700Z"  
}
```

5. Выход из системы

5.1. Выход из системы

Имя ресурса: /authentication/api/v1/auth/logout

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>

5.1.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 70.

Таблица 70 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Да	Сессия аутентифицированного пользователя

5.1.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 71.

Таблица 71 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Способы аутентификации	authTypes	Массив	Да	Список способов аутентификации входа, которые были выполнены для данной сессии. Возможные значения: – LOGIN – логин и пароль;

Параметр	Название параметра	Тип данных	Обязательность	Описание
				– CERT – сертификат; – KERBEROS_TICKET – доменная учётная запись; – CODE_FROM_EMAIL – подтверждение входа по коду, полученному на адрес электронной почты УЗ пользователя; – ESIA – Госуслуги
URL, по которому перенаправляется пользователь после выхода из системы (для ЕСИА)	esiaLogoutUrl	Строка	Нет	URL, по которому перенаправляется пользователь после выхода из системы (для ЕСИА). Не указан, если вход был выполнен не по ЕСИА

5.1.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 72.

Таблица 72 – 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

5.1.4. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/authentication/api/v1/auth/logout
Content-Type: application/json
```

Cookie:

```
XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZXNoVFRMIjowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudW1iZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2aW91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lwbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1N1Y3VyaXR5UG9saWN5IjpmYXxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQioInRydWUsInNlc3Npb25UVEwiOjAsImIhdCI6MTcyNTU0NjAzNH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-lNOUaiO-JwicDi_labpTSacURDtfvFWZQqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mmyOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7U45EIGOd9j-W8A
```

Ответ:

Content-Type: application/json

```
{
  "authTypes": [
    "ESIA",
    "LOGIN"
  ],
  "esiaLogoutUrl": "http://esia-
mock.xidbox.dcs.infosec.ru:8090/idp/ext/Logout?client
_id=XIDBOX&redirect_url=xidbox.dcs.infosec.ru%2fsigni
n"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Метод не разрешен.",  
  "timestamp": "2024-10-03T14:28:15.952771016Z"  
}
```

5.2. Завершение всех сессий пользователя

Имя ресурса: /authentication/api/v1/auth/session/invalidate

Метод: POST

HTTP-заголовки:

– Content-Type: application/json

5.2.1. Данные в запросе

Описание данных в запросе приведено в таблице 73.

Таблица 73 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор	userId	UUID	Да	Идентификатор пользователя

5.2.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 74.

Таблица 74 – 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

Параметр	Название параметра	Тип данных	Описание
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка

5.2.3. Пример выполнения запроса

Запрос:

POST

`http://{{host}}/authentication/api/v1/auth/session/invalidate?userUuid=0052f40b-e12f-4fcb-ac23-`

`988c2b4f539b`

`Content-Type: application/json`

Ошибка выполнения запроса:

`Content-Type: application/json`

```
{
  "type": "MESSAGE",
  "payload": "Not found by uuid: 1234b264-0a54-4690-9c89-c9b60bd559ba",
  "timestamp": "2024-10-03T14:28:15.952771016Z"
}
```

5.3. Завершение активных сессий профиля УЗ пользователя, кроме текущей

Имя ресурса: `/authentication/api/v1/auth/session/invalidate/for-current-session`

Метод: POST

HTTP-заголовки:

– `Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>`

5.3.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 75.

Описание данных в запросе приведено в таблице 76.

Таблица 75 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Да	Сессия аутентифицированного пользователя

Таблица 76 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя

5.3.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 77.

Таблица 77 – 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

5.3.3. Пример выполнения запроса

Запрос:

POST

`http://{{host}}/authentication/api/v1/auth/session/invalidate/for-current-`

`session?userProfileUuid=d61aacbf-2c32-4744-a4a9-17979a5ae45a`

Cookie: XIDBOXSession=

`eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4`

NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZ
XNoVFRMI
jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LT
A5LTA1VDE0OjE1OjAyLjY4MDgxMloiLCJudWliZXJPZlVuc3VjY2V
zc2Z1bEF0dGVtcHRzU2luY2VQcmV2a
W91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lrbklkIjoimjYwOD
U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
vU2hvd1N1Y3VyaXR5UG9saWN5IjpmY
WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn
V1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU
4ZmEiLCJpc0VtYWlsVmVyaWZpZWQio
nRydWUsInNlc3Npb25UVEwiOjAsImhhdCI6MTcyNTU0NjAzNH0.wX
Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-
lNOUaiO-JwicDi_labpTSacURDtFvFWZ
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7
U45EIGOd9j-W8A

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "UserProfile not found by uuid:
123aacbf-2c32-4744-a4a9-17979a5ae45a",
  "timestamp": "2024-10-03T14:30:30.972075118Z"
}
```

5.4. Завершение всех активных сессий профиля УЗ пользователя

Имя ресурса: /authentication/api/v1/auth/session/invalidate

Метод: POST

5.4.1. Данные в запросе

Описание данных в запросе приведено в таблице 78.

Таблица 78 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя

5.4.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 79.

Таблица 79 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Результат завершения сессий	result	Строка	Да	Если завершена хотя бы одна сессия: «Были завершены активные сессии профиля УЗ». Если не было завершено ни одной сессии: «Отсутствуют завершенные активные сессии профиля УЗ»

5.4.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 80.

Таблица 80 – 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

5.4.4. Пример выполнения запроса

Запрос:

```
POST
http://{{host}}/authentication/api/v1/auth/session/invalidate?userProfileUuid=48d34c1b-3f7e-48fd-a8e4-53285a476f6e
```

Ответ:

Content-Type: application/json

```
{
  "result": "Отсутствуют завершенные активные сессии профиля УЗ"
}
```

Ответ:

Content-Type: application/json

```
{
  "result": "Были завершены активные сессии профиля уЗ"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
```

```
"type": "MESSAGE",  
"payload": "UserProfile not found by uuid:  
123aacbf-2c32-4744-a4a9-17979a5ae45a",  
"timestamp": "2024-10-03T14:30:30.972075118Z"  
}
```

5.5. Завершение сессий заблокированных профилей УЗ

пользователя

Имя ресурса: /authentication/api/v1/auth/session/invalidate/user-profiles

Метод: POST

HTTP-заголовки:

– Content-Type: application/json

5.5.1. Данные в запросе

Описание данных в запросе приведено в таблице 81.

Таблица 81 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор УЗ пользователя	userUuid	UUID	Да	Идентификатор УЗ пользователя для сброса заблокированных профилей УЗ пользователя из сессий

5.5.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 82.

Таблица 82 – 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

5.5.3. Пример выполнения запроса

Запрос:

POST

`http://{{host}}/authentication/api/v1/auth/session/invalidate/user-profiles?userUuid=fa64b264-0a54-4690-9c89-c9b60bd559ba`

`Content-Type: application/json`

Ошибка выполнения запроса:

`Content-Type: application/json`

```
{
  "type": "MESSAGE",
  "payload": "Not found by uuid: fa64b264-0a54-4690-9c89-c9b60bd559ba",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

6. Аутентификация и получение данных о пользователе по OAuth 2.0

Разработчики внешней ИС могут предоставить своим пользователям возможность входить в систему, используя УЗ X-IDBox. Это избавляет разработчиков от необходимости делать собственное хранилище УЗ пользователей, обеспечивать безопасность хранения паролей, разрабатывать механизмы регистрации и аутентификации пользователей, поддерживать их в рабочем состоянии.

С целью обеспечения указанной функциональности в X-IDBox реализован механизм, основанный на спецификациях протокола авторизации OAuth 2.0 и расширении OpenID Connect 1.0.

Протокол определяет взаимодействие следующих сторон:

- владелец ресурса (resource owner) – сущность, которая может предоставить доступ к защищаемому ресурсу (например, пользователь предоставляет доступ к своим персональным данным);
- система-клиент (client) – приложение, которое запрашивает доступ к защищаемому ресурсу от имени его владельца;
- сервис авторизации (authorization server) – сервис, который выпускает для системы-клиента токены идентификации с разрешениями от владельца ресурса, а также токены доступа, позволяющие получать доступ к данным;
- поставщик ресурса (resource server) – сервис, обеспечивающий доступ к защищаемому ресурсу на основе проверки токенов идентификации и токенов доступа (например, к идентификационным данным пользователя).

Расширение OpenID Connect 1.0 предполагает использование токена идентификации (ID Token) в целях проведения идентификации и аутентификации пользователя. Токен идентификации содержит идентификационные данные пользователя, а также ряд служебных параметров (дата выдачи, время окончания срока действия и пр.).

Для иллюстрации использования OpenID Connect 1.0 в X-IDBox принята следующая терминология:

- владелец ресурса – это пользователь;
- система-клиент – это внешняя ИС, интегрированная с X-IDBox с целью идентификации и аутентификации, например, региональный портал услуг;
- сервис авторизации и поставщик ресурса – это X-IDBox.

Общая схема подключения системы к X-IDBox для проведения аутентификации представлена на рис. 2.

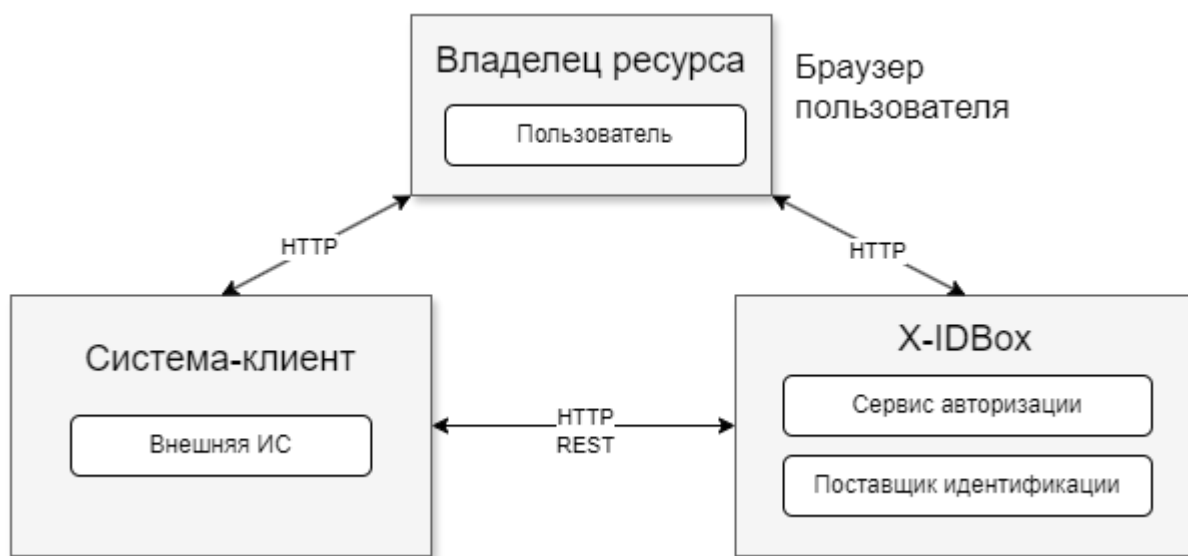


Рисунок 2 – Схема подключения внешней системы к X-IDBox

Для предоставления пользователям внешней системы возможности входа через X-IDBox, используя OAuth 2.0 или OpenID Connect 1.0, со стороны подключающейся системы необходимо обеспечить:

- Регистрацию и настройку ИС в X-IDBox, а также получение необходимых идентификаторов для доступа внешней ИС по протоколу OAuth 2.0, такие как мнемоника ИС, секретная фраза и другие.

Для выполнения данного пункта необходимо обратиться в службу технической поддержки.

- Реализацию необходимых интерфейсов системы-клиента для взаимодействия с REST-сервисами X-IDBox. Рекомендуемые сценарии аутентификации приведены ниже.

Рекомендуемый сценарий аутентификации при использовании OAuth 2.0 включает следующие шаги (рис. 3):

1) Пользователь нажимает на веб-странице (или в мобильном приложении) системы-клиента кнопку авторизации через X-IDBox.

2) Система-клиент формирует и отправляет в X-IDBox запрос на получение авторизационного кода (см. п. 6.3) с указанием требуемых областей доступа (см. п. 6.1) и средствами браузера перенаправляет пользователя на специальную страницу предоставления доступа.

3) X-IDBox осуществляет аутентификацию пользователя одним из доступных способов. Если пользователь еще не зарегистрирован в X-IDBox, то он может перейти к процессу регистрации.

4) Когда пользователь аутентифицирован, X-IDBox сообщает пользователю, что система-клиент запрашивает данные о нем в целях проведения идентификации и аутентификации, предоставляя перечень запрашиваемых системой-клиентом сведений.

5) Если пользователь дает разрешение на предоставление системе-клиенту указанных данных, то X-IDBox выдает системе-клиенту специальный авторизационный код.

6) Система-клиент формирует в адрес X-IDBox запрос на получение токенов доступа (см. п. 6.5), включая в запрос полученный ранее авторизационный код.

7) X-IDBox проверяет корректность запроса (например, что система-клиент зарегистрирована в X-IDBox, запрошены разрешенные пользователем области доступа (scope) и др.) и авторизационного кода, и передает системе-клиенту токены доступа и обновления.

8) После получения токена доступа система-клиент использует REST-сервисы X-IDBox для получения дополнительных данных о пользователе, необходимых для аутентификации во внешней системе (например, получение данных УЗ пользователя по токену OAuth 2.0 (см. п. 6.9), полный перечень доступных запросов на получение данных описан в настоящем руководстве).

Рекомендуемый сценарий аутентификации при использовании OpenID Connect 1.0 включает следующие шаги (рис. 3):

1) Пользователь нажимает на веб-странице (или в мобильном приложении) системы-клиента кнопку авторизации через X-IDBox.

2) Система-клиент формирует и отправляет в X-IDBox запрос на получение авторизационного кода (см. п. 6.3) с указанием требуемых областей доступа (см. п. 6.1), а также области доступа «openid», для получения токена идентификации (ID Token) и перенаправляет браузер пользователя на специальную страницу предоставления доступа.

3) X-IDBox осуществляет аутентификацию пользователя одним из доступных способов. Если пользователь еще не зарегистрирован в X-IDBox, то он может перейти к процессу регистрации.

4) Когда пользователь аутентифицирован, X-IDBox сообщает пользователю, что система-клиент запрашивает данные о нем в целях проведения идентификации и аутентификации, предоставляя перечень запрашиваемых системой-клиентом сведений.

5) Если пользователь дает разрешение на проведение аутентификации системой-клиентом, то X-IDBox выдает системе-клиенту специальный авторизационный код.

6) Система-клиент формирует в адрес X-IDBox запрос на получение токенов доступа (см. п. 6.5), включая в запрос полученный ранее авторизационный код.

7) X-IDBox проверяет корректность запроса (например, что система-клиент зарегистрирована в X-IDBox, запрошены разрешенные пользователем области доступа (scope) и др.) и авторизационного кода, и передает системе-клиенту токены доступа, идентификации и обновления.

8) Система-клиент извлекает идентификатор пользователя из токена идентификации (ID Token). Если идентификатор получен, а токен проверен, то система-клиент считает пользователя аутентифицированным.

9) После получения токена доступа система-клиент использует REST-сервисы X-IDBox для получения дополнительных данных о пользователе (например, получение данных УЗ пользователя по токену OAuth 2.0 (см. п. 6.9), полный перечень доступных запросов на получение данных описан в настоящем руководстве).

Пример системы-клиента для аутентификации через X-IDBox по OAuth2.0/OpenID Connect 1.0 приведен в Приложении А.

Сценарий аутентификации из приложения ИС приведен в п. 10.

Из возможных потоков выдачи токенов в X-IDBox поддерживается только поток авторизационного кода (Authorization code flow).

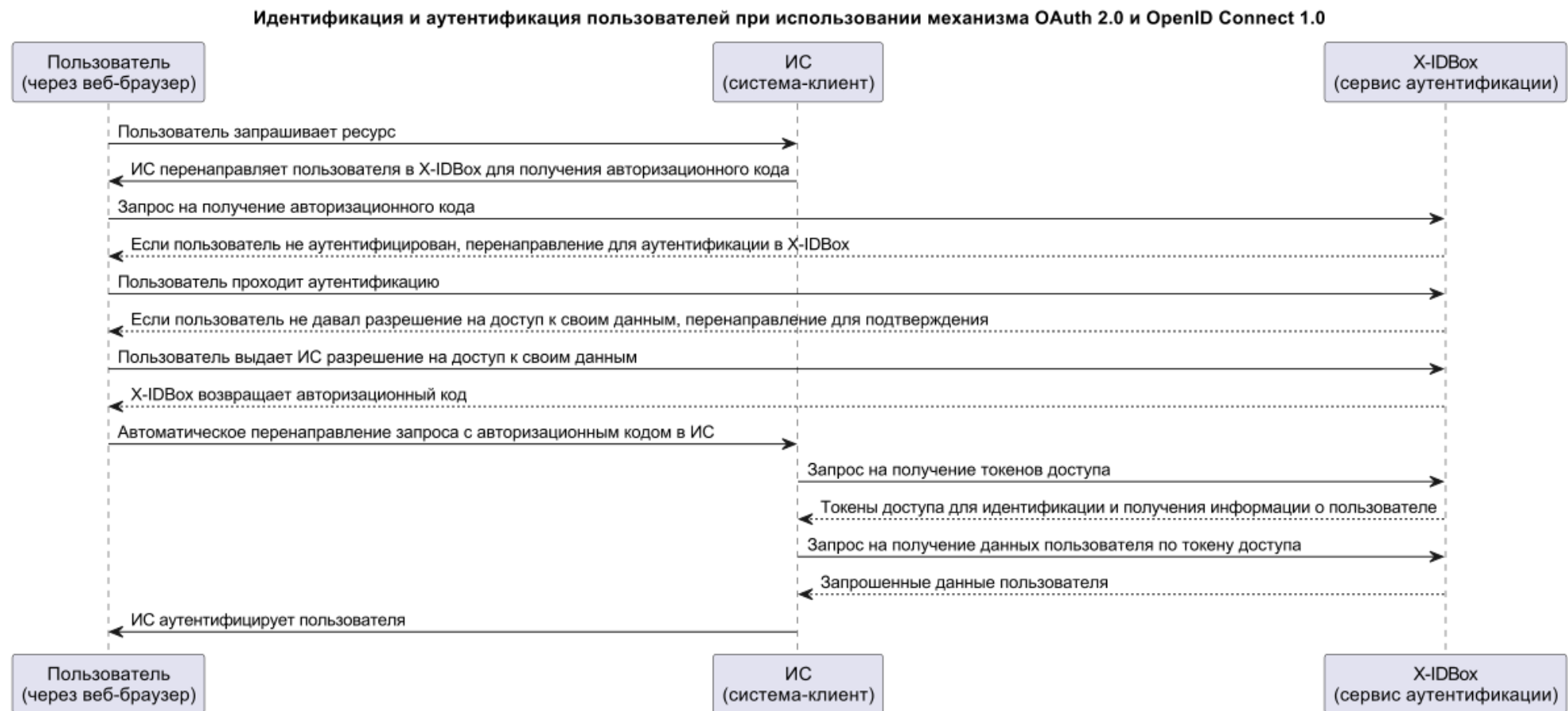


Рисунок 3 – Идентификация и аутентификация пользователей при использовании механизма OAuth 2.0 и OpenID Connect 1.0

6.1. Возможные значения области доступа

Описание возможных значений области доступа (параметра «scope») приведено в таблице 83.

Таблица 83 – Возможные значения области доступа

Значение	Наименование	Тип данных	Описание	Методы, в которых требуются указанные области доступа (scope)
user	Данные УЗ пользователя	Строка	Данные основных полей УЗ пользователя	Получение данных УЗ пользователя с динамическими полями по токену OAuth 2.0
user-profile	Данные профиля УЗ пользователя	Строка	Данные основных полей профиля УЗ пользователя	Получение данных профиля УЗ пользователя с динамическими полями профиля УЗ пользователя и организации по токену OAuth 2.0
organization	Данные организации профиля УЗ пользователя	Строка	Данные организации профиля УЗ пользователя	
user-dynamic-fields	Динамические поля УЗ пользователя	Строка	Динамические поля УЗ пользователя. Перечень доступных динамических полей указывается в процессе настройки доступа через OAuth 2.0	Получение данных УЗ пользователя с динамическими полями по токену OAuth 2.0
user-profile-dynamic-fields	Динамические поля профиля УЗ пользователя	Строка	Динамические поля профиля УЗ пользователя. Перечень доступных динамических полей указывается в процессе настройки доступа через OAuth 2.0	Получение данных профиля УЗ пользователя с динамическими полями профиля УЗ пользователя и организации по токену OAuth 2.0

Значение	Наименование	Тип данных	Описание	Методы, в которых требуются указанные области доступа (scope)
organization-dynamic-fields	Динамические поля организации профиля УЗ пользователя	Строка	Динамические поля организации профиля УЗ пользователя. Перечень доступных динамических полей указывается в процессе настройки доступа через OAuth 2.0	Получение данных профиля УЗ пользователя с динамическими полями профиля УЗ пользователя и организации по токenu OAuth 2.0
openid	Идентификатор УЗ пользователя	Строка	Получение токена OpenID Connect 1.0 с идентификационными данными пользователя	Получение данных УЗ аутентифицированного пользователя через OpenId Connect 1.0
email	Адрес электронной почты пользователя	Строка	Получение адреса электронной почты и признака верификации адреса электронной почты пользователя	Получение данных УЗ аутентифицированного пользователя через OpenId Connect 1.0
profile	Логин, ФИО, дата рождения пользователя	Строка	Получение логина, ФИО, даты рождения пользователя	Получение данных УЗ аутентифицированного пользователя через OpenId Connect 1.0

6.2. Содержимое ID Token OpenId Connect 1.0

ID-токен в OpenID Connect 1.0 представляет собой подписанный JSON Web Token (JWT), который содержит набор утверждений (claims) об аутентифицированном пользователе.

В зависимости от запрошенных областей доступа (scopes), ID-токен может содержать дополнительные утверждения, предоставляющие информацию о пользователе. Описание содержимого ID-токена приведено в таблице 84.

Таблица 84 – Содержимое ID-токена

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Идентификатор УЗ пользователя	sub	UUID	Да	Идентификатор УЗ пользователя	openid
URL-адрес сервера	iss	Строка	Да	URL-адрес сервера авторизации, выдавшего токен	openid
Мнемоника OAuth 2.0-клиента, для которого предназначен токен	aud	Строка	Да	Мнемоника OAuth 2.0-клиента, для которого предназначен токен	openid
Мнемоника OAuth 2.0-клиента, которому был выдан токен	azp	Строка	Да	Мнемоника OAuth 2.0-клиента, которому был выдан токен	openid
Время прохождения аутентификации	auth_time	Целое число	Да	Время прохождения аутентификации пользователем в формате timestamp	openid
Время выдачи токена	iat	Целое число	Да	Время выдачи токена в формате timestamp	openid
Время истечения срока действия токена	exp	Целое число	Да	Время истечения срока действия токена в формате timestamp	openid
Уникальный идентификатор токена	jti	UUID	Да	Уникальный идентификатор токена для предотвращения повторного использования	openid
Идентификатор сессии	sid	Строка	Да	Идентификатор сессии	openid
Идентификатор УЗ пользователя	userUuid	UUID	Да	Идентификатор УЗ пользователя	openid
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя	openid

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Адрес электронной почты УЗ пользователя	email	Строка	Да	Адрес электронной почты УЗ пользователя	openid, email
Признак верификации адреса электронной почты пользователя	email_verified	Логический	Да	Значение «true» – если адрес электронной почты пользователя верифицирован, значение «false» – если адрес электронной почты пользователя не верифицирован	openid, email
Логин	preferred_username	Строка	Да	Логин пользователя	openid, profile
Псевдоним	nickname	Строка	Да	Псевдоним пользователя	openid, profile
Фамилия пользователя	family_name	Строка	Да	Фамилия пользователя	openid, profile
Имя пользователя	given_name	Строка	Да	Имя пользователя	openid, profile
Отчество пользователя	middle_name	Строка	Нет	Отчество пользователя	openid, profile
Дата рождения	birthdate	Строка	Нет	Дата рождения пользователя	openid, profile
Время последнего изменения данных пользователя	updated_at	Целое число	Нет	Время последнего изменения данных аутентифицированного пользователя в формате timestamp	openid, profile

Пример значения ID-токена:

```
eyJraWQiOiIxZjA0MzQ2My1lZTBhLTM0OWItOWJjYi1hYmMxYzU3ODg5ODkiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIwMDUyZjQwYi1lMTJmLTRmY2ItYWMyMy05ODhjMmI0ZjUzOWIiLCJlbWFpbF92ZXJpZm11ZCI6dHJlZSwiaXNzIjoiaHR0cDovL2xvY2F
```

```

saG9zdDo4MDg1IiwicHJlZmVycmVkX3VzZXJuYW1lIjoibWF4Iiwiz2l2ZW5fbmFtZSI6ItCY0LJh0L0iLC
JtaWRkbGVfbmFtZSI6ItCc0LDQutCw0YDQuNC10LLQuNGHIiwic2lkIjoiaUgtd3BxWGhPUjhYazk0VVlNO
C1IdFU4Z0FkOVQ1LVhqTlhYOGhIVGt
2VSI6ImF1ZCI6InRlc3QtY2xpZW50IiwidXBkYXRlZGF9hdCI6MTc2NDY2Mzc4MSwiVEVTVCI6MTc2NDY2Mz
c4MSwiYXpwIjoiaGVzdC1jbGllbnQiLCJhdXRoX3RpbWUiOjE3NjQ2NjU2NzcsInVzZXJvdWlkIjoiaMDA1M
mY0MGItZTEyZi00ZmNiLWFjMjMtOTg
4YzJiNGY1MzliIiwibmlja25hbWUiOiJtYXgiLCJleHAiOjE3NjQ2Njc0OTMsIm1hdCI6MTc2NDY2NTY5My
wiZmFtaWx5X25hbWUiOiLQktGB0LXQvNC-
0LPRg9GJ0LjQuSIsImp0aSI6ImUzNmVhZGRmLTNmYUUtNDZjMy04YzNmLTA5YTQ4NDMyNTg0NCIsImV
tYWlsIjoiaUgtd3BxWGhPUjhYazk0VVlNO
mSVVlGK2hjM7_qYdZolgOl0L3KRw8Ye9aXn8dv6gNFvCf575NHpExurEModOIoz5wL4fUtHgyVZoKD0S4fw
Geww0Cxoyywe3SZ1BEms0XxmT1f8htZZ8-h92eJtXJkvYd6ZB2fmNfik3s_Gg4
0AbGNtVt2qs7g_KGxVPoujFPqfZFYgaLq5IDaqoZs-NRn7kbncYTCy6ICvCmwwweZN5l1N-
zPw_kBV4FvydOnRFDlEaQVhTiqT05oHWlv575dwwjPNPNd2O42Vp3aELBUmnyAp-
fBpWxzhdKpM4ksZ9BOXPZtgLU7wOHPxQi5wCVArG2FvWCw

```

Пример содержимого ID-токена:

```

{"kid": "1f043463-ee0a-349b-9bcb-abc1c5788989", "alg": "RS256"}
{
  "sub": "0052f40b-e12f-4fcb-ac23-988c2b4f539b",
  "email_verified": true,
  "iss": "http://localhost:8085",
  "preferred_username": "max",
  "given_name": "Иван",
  "middle_name": "Макариевич",
  "sid": "iH-wpqXhOR8Xk94UYM8-HtU8gAd9T5-XjNXX8hHTkvU",

```

```
"aud": "test-client",
"updated_at": 1764663781,
"TEST": 1764663781,
"azp": "test-client",
"auth_time": 1764665677,
"userUuid": "0052f40b-e12f-4fcb-ac23-988c2b4f539b",
"nickname": "max",
"exp": 1764667493,
"iat": 1764665693,
"family_name": "Всемогущий",
"jti": "e36eaddf-1fae-46c3-8c3f-09a484325844",
"email": "Max@localhost.ru"
}
signature
```

6.3. Получение авторизационного кода OAuth 2.0

Имя ресурса: /authentication/api/v1/oauth2/authorize

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>

6.3.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 85.

Описание данных в запросе приведено в таблице 86.

Таблица 85 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет	Сессия аутентифицированного пользователя. При отсутствии данных сессии в запросе произойдет перенаправление пользователя для прохождения аутентификации

Таблица 86 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Тип ответа, который ожидается от X-IDBox	response_type	Строка	Да	Тип ответа, который ожидается от X-IDBox. Для получения авторизационного кода указывается фиксированное значение: response_type=code

Параметр	Название параметра	Тип данных	Обязательность	Описание
Мнемоника OAuth 2.0-клиента	client_id	Строка	Да	Мнемоника OAuth 2.0-клиента. Присваивается системе-клиенту в процессе настройки доступа через OAuth 2.0
Адрес для перенаправления пользователя после получения кода	redirect_uri	Строка	Да	Адрес для перенаправления пользователя после получения кода. Присваивается системе-клиенту в процессе настройки доступа через OAuth 2.0, требуемое значение определяется системой-клиентом
Область доступа	scope	Строка	Да	Требуемые области доступа. Указываются через пробел. Возможные значения приведены в таблице 83

6.3.2. Данные в ответе на запрос

При выполнении запроса проверяется подтверждение пользователем всех запрошенных областей доступа.

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 87.

Таблица 87 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Авторизационный код	code	Строка	Нет, при наличии параметра error	Сгенерированный авторизационный код

Параметр	Название параметра	Тип данных	Обязательность	Описание
Тип ошибки	error	Строка	Нет, при наличии параметра code	Тип ошибки
Описание ошибки	error_description	Строка	Нет, при наличии параметра code	Описание ошибки
Ссылка на описание ошибки	error_uri	Строка	Нет, при наличии параметра code	Ссылка на документацию протокола OAuth 2.0 Authorization Framework

Если пользователь ещё не предоставлял разрешения на доступ OAuth 2.0-клиента к данным УЗ пользователя, то происходит перенаправление на страницу подтверждения доступов.

В случае ошибки в данных запроса или отказе пользователя предоставить данные для просмотра, происходит перенаправление на указанный в запросе `redirect_uri` с указанием информации об ошибке.

6.3.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 88.

Таблица 88 – Данные ошибки выполнения запроса в случае неизвестного или некорректного «client_id»

Параметр	Название параметра	Тип данных	Описание
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка
Код ответа	status	Целое число	Код ответа
Информация об ошибке	error	Строка	Информация об ошибке
Путь URL	path	Строка	Путь URL

6.3.4. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/
authentication/api/v1/oauth2/authorize?response_type=
code&client_id=test-
client&redirect_uri=http://localhost:3000/code&scope=
user openid
Content-Type: application/json
Cookie: XIDBOXSession=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4
NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZ
XNoVFRMI
jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LT
A5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudW1iZXJPZlVuc3VjY2V
zc2Z1bEF0dGVtcHRzU2luY2VQcmV2a
W91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lwbklkIjoimjYwOD
U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
vU2hvd1N1Y3VyaXR5UG9saWN5IjpmY
WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn
VlaWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU
4ZmEiLCJpc0VtYWlsVmVyaWZpZWQio
nRydWUsInNlc3Npb25UVEwiOiJAsImldhdCI6MTcyNTU0NjAzNH0.wX
Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-
lNOUaiO-JwicDi_labpTSacURDtfvFWZ
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZ5gxxsLP2vNnh_NVQr7
U45EIGOd9j-W8A
```

Ответ:

```
302
http://localhost:3000/code?code=S1yb10_vQp8yu93rUQWCZ
xOiMXE-mqaNcvT-9LS2GeipGd-
Pgdk9ctLAP1UK4k7gCNXBYC_iSVpuaM4hU3eTmidSrqMD7-
oETt4fLYlYlnXzjPx_IHU-_KL5W3oOyYtk
```

Ответ в случае отказа предоставить доступ:

```
302
http://localhost:3000/code?error=access_denied&error_
```

```
description=OAuth%202.0%20Parameter%3A%20client_id&error_uri=https%3A%2F%2Fdatatracker.ietf.org%2Fdoc%2Fhtml%2Frfc6749%23section-4.1.2.1
```

Ответ в случае некорректных областей доступа:

302

```
http://localhost:3000/code?error=invalid_scope&error_description=OAuth%202.0%20Parameter%3A%20scope&error_uri=https%3A%2F%2Fdatatracker.ietf.org%2Fdoc%2Fhtml%2Frfc6749%23section-4.1.2.1
```

Ошибка выполнения запроса в случае неизвестного или некорректного client_id:

HTTP/1.1 400

Content-Type: application/json

```
{
  "timestamp": "2025-06-02T07:32:30.580+00:00",
  "status": 400,
  "error": "Bad Request",
  "path": "/authentication/api/v1/oauth2/authorize"
}
```

6.4. Принятие решения о предоставлении доступа OAuth 2.0-клиенту к данным пользователя

Имя ресурса: /authentication/api/v1/oauth2/authorize

Метод: POST

HTTP-заголовки:

– Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>

6.4.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 89.
Описание данных в запросе приведено в таблице 90.

Таблица 89 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Да	Сессия аутентифицированного пользователя

Таблица 90 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Область доступа	scope	Строка	Да	Области доступа, которые подтвердил пользователь. Отображаются в карточке УЗ пользователя. Для указания нескольких областей необходимо указать параметр требуемое количество раз. Возможные значения приведены в таблице 83
Мнемоника OAuth 2.0-клиента	client_id	Строка	Да	Мнемоника OAuth 2.0-клиента. Присваивается системе-клиенту в процессе настройки доступа через OAuth 2.0
Идентификатор запроса	state	Строка	Да	Уникальное значение для обеспечения безопасности, полученное при перенаправлении пользователя на страницу подтверждения доступов

6.4.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 91.

Таблица 91 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Авторизационный код	code	Строка	Нет, при наличии параметра error	Сгенерированный авторизационный код
Тип ошибки	error	Строка	Нет, при наличии параметра code	Тип ошибки
Описание ошибки	error_description	Строка	Нет, при наличии параметра code	Описание ошибки
Ссылка на описание ошибки	error_uri	Строка	Нет, при наличии параметра code	Ссылка на документацию протокола OAuth 2.0 Authorization Framework

В случае ошибки в данных запроса или отказе пользователя предоставить данные для просмотра, происходит перенаправление на указанный в запросе `redirect_uri` с указанием информации об ошибке.

6.4.3. Пример выполнения запроса

Запрос на подтверждение доступов:

POST

```
http://{{host}}/authentication/api/v1/oauth2/authorize?scope=openid&scope=user&client_id=test-client&state=uxIUQ3bfkoDRTpCcqfJNTrGEdn4-OGz6axs1lRiX_4g=
```

Cookie:

```
XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWZzM2M3YmYiLCJyZWZyZXNoVFRMI
```

```
jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LT
A5LTA1VDE0OjE1OjAyLjY4MDgxMloiLCJudWliZXJPZlVuc3VjY2V
zc2Z1bEF0dGVtcHRzU2luY2VQcmV2a
W91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lrbklkIjoimjYwOD
U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
vU2hvd1NlY3VyaXR5UG9saWN5IjpmY
WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn
V1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtoDE2OC03MGY0OGYwNzU
4ZmEiLCJpc0VtYWlsVmVyaWZpZWQio
nRydWUsInNlc3Npb25UVEwiOjAsImIhdCI6MTcyNTU0NjAzNH0.wX
Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-
lNOUaiO-JwicDi_labpTSacURDtFvFWZ
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IggNt_9FP1G_
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7
U45EIGOd9j-W8A
```

Запрос на отклонение доступов:

POST

```
http://{host}/authentication/api/v1/oauth2/authorize?client_id=test-
client&state=jyuzbOdgxDYLPxQRkec8mN6xvdntr8juej4l2SLU
m68=
```

Cookie:

```
XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJz
dWUiOiIyNjA4NTU5OC04NjI1LTQxMmYtoDkxZS1jNTMzZWEzM2M
3YmYiLCJyZWZyZXNoVFRMI
jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LT
A5LTA1VDE0OjE1OjAyLjY4MDgxMloiLCJudWliZXJPZlVuc3VjY2V
zc2Z1bEF0dGVtcHRzU2luY2VQcmV2a
W91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lrbklkIjoimjYwOD
U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
vU2hvd1NlY3VyaXR5UG9saWN5IjpmY
WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn
V1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtoDE2OC03MGY0OGYwNzU
4ZmEiLCJpc0VtYWlsVmVyaWZpZWQio
```

```
nRydWUsInNlc3Npb25UVEwiOjAsImlhdCI6MTcyNTU0NjAzNH0.wX
Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-
lNOUaiO-JwicDi_labpTSacURDtFvFWZ
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_
f4VPFw2fSJ6rtIR6PtKfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7
U45EIGOd9j-W8A
```

Ответ:

302

```
http://localhost:3000/code?code=S1yb10_vQp8yu93rUQWCZ
xOiMXE-mqaNcvT-9LS2GeipGd-
Pgdk9ctLAP1UK4k7gCNXBYC_iSVpuaM4hU3eTmidSrqMD7-
oETt4fLYlYlnXzjPx_IHU-_KL5W3oOyYtk
```

Ответ в случае отказа предоставить доступ:

302

```
http://localhost:3000/code?error=access_denied&error_
description=OAuth%202.0%20Parameter%3A%20client_id&er
ror_uri=https%3A%2F%2Fdatatracker.ietf.org%2Fdoc%2Fht
ml%2Frfc6749%23section-4.1.2.1
```

6.5. Получение OAuth 2.0 токенов доступа

Имя ресурса: /authentication/api/v1/oauth2/token

Метод: POST

HTTP-заголовки:

- Content-Type: application/x-www-form-urlencoded
- Authorization: Basic <Информация об авторизации>

6.5.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 92.

Описание данных в запросе приведено в таблице 93.

Таблица 92 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Заголовок HTTP-авторизации	Authorization	Строка	Да	Значение Basic авторизации в виде строки, состоящей из мнемоники ИС и секретной фразы. Значения мнемоники и секретной фразы присваивается системе-клиенту в процессе настройки доступа через OAuth 2.0. Например: dGVzdC1jbGllbnQ6dGVzdC1jbGllbnQ= //test-client:test-client в base64

Таблица 93 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Тип ответа, который ожидается от X-IDBox	grant_type	Строка	Да	Тип ответа, который ожидается от X-IDBox. Для получения авторизационного кода указывается фиксированное значение: grant_type=authorization_code
Мнемоника OAuth 2.0-клиента	client_id	Строка	Да	Мнемоника OAuth 2.0-клиента. Присваивается системе-клиенту в процессе настройки доступа через OAuth 2.0

Параметр	Название параметра	Тип данных	Обязательность	Описание
Адрес для перенаправления пользователя после получения кода	redirect_uri	Строка	Да	Адрес для перенаправления пользователя после получения кода. Присваивается системе-клиенту в процессе настройки доступа через OAuth 2.0, требуемое значение определяется системой-клиентом
Авторизационный код	code	Строка	Да	Авторизационный код, полученный после успешной аутентификации пользователя и подтверждения доступов

6.5.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 94.

Таблица 94 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Токен доступа	access_token	Строка	Да	Токен доступа
Токен обновления	refresh_token	Строка	Да	Токен обновления
Область доступа токена	scope	Строка	Да	Области доступа токена, разделенные пробелом. Возможные значения приведены в таблице 83

Параметр	Название параметра	Тип данных	Обязательность	Описание
Токен идентификации OpenID Connect 1.0	id_token	Строка	Нет	Токен идентификации OpenId Connent 1.0. Генерируется, если при получении авторизационного кода был запрошен scope openid
Тип токена	token_type	Строка	Да	Тип токена
Срок действия	expires_in	Строка	Да	Срок действия в секундах, через который истечёт токен доступа

6.5.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 95.

Таблица 95 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Тип ошибки	error	Строка	Да	Тип ошибки
Описание ошибки	error_description	Строка	Нет	Описание ошибки
Ссылка на описание ошибки	error_uri	Строка	Нет	Ссылка на документацию протокола OAuth 2.0 Authorization Framework

6.5.4. Пример выполнения запроса

Запрос:

```
POST
http://{{host}}/authentication/api/v1/oauth2/token?client_id=test-client&grant_type=authorization_code&code=KSzcmdmCJV_urTIIBaoQYCoMd_dTvk5lD9lU-GWYEECrQyw63q6uZ-GX6R0ZvhlFq8CSTzuDkMwf4uV-cBNr-DVF5yFAd0nYuf2S7EhEU_QoiQRP-
```

```
186tDw4goV5kMEd&redirect_uri=http://localhost:3000/co
de
Content-Type: application/x-www-form-urlencoded
Authorization: Basic dGVzdC1jbGllbnQ6dGVzdC1jbGllbnQ=
```

Ответ:

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

```
{
  "access_token":
"eyJraWQiOiI5YzVjMzYyMS00NTY1LTQxNWItYTM0NS0zZjA5MTc2
Y2JhYjAiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJlMGJhYmE2My04
NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJhdWQiOiJ0ZXN0L
WNsaWVudCIsIm5iZiI6MTcyODU2Njk4OSwic2NvcGUiOiIsib3Blbm
lkiIiwidXNlciJdLCJpc3MiOiJodHRwOi8vbG9jYWxob3N0OjgwODU
iLCJ1c2VyVXVpZCI6ImUwYmFiYTYzLTg3MzMtNDhjZS04MTY4LTcw
ZjQ4ZjA3NThtYSIsImV4cCI6MTcyODU2NzI4OSwiaWF0IjoxNzI4N
TY2OTg5LCJ1c2VyUHJvZmlsZVVlaWQiOiI0YmIyY2UxOC1hZjgzLT
Q4YjQtYjBjNS0yNDY3NTY3NzM1YzMiZmFQ.wxDbBCr90LvJnwFf6eGT
0SNnY5hV7jimI2JKZOpN-kcsf1bOIal50il-
W4DBoU78jYoJlc2MK-h4wa9_kQ0P-
Z2Y6ct70ruAPAARKE1aV9j8A8jYhY1qW6XbfjOVYb4m-
xzDqzpCKRD6sVFWx71WuYM5gvmys1G81PmuMdmvLup-
ts3AT6ef5w1IbPTawPQi7wqvQfKAyloUC4ejuid3cgtGkfMwClDo7
BF5xkHRX1qo32WdGelFnTx52ODf2q1wqMYUEyE1Y24GFEwaqatnUw
6RRaPT26a9slk6IuLKNcKOJ9uy6oqDy3VdQSbIznjj4jtbCKvxzIg
goJC9xhlc3Q",
  "refresh_token":
"Su1lxql7wWiD4EHigr7TJCXgTtcJUuXVZQNX_2CokZVj0UiBAosj
OKo_4DY74j3k8klYVDtaqbDW0ClHP7SS39yXK3WakAfSCxQXBwue4
XsAz54G2OdpQE6OLB7k2tIo",
  "scope": "openid user",
  "id_token":
"eyJraWQiOiI5YzVjMzYyMS00NTY1LTQxNWItYTM0NS0zZjA5MTc2
Y2JhYjAiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJlMGJhYmE2My04
NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJhdWQiOiJ0ZXN0L
WNsaWVudCIsImF6cCI6InRlc3QtY2xpZW50IiwiaXV0aF90aW1lIj
oxNzI4NzY2OTY4LCJpc3MiOiJodHRwOi8vbG9jYWxob3N0OjgwODU
iLCJleHAiOiE3Mjg1Njg3OTAsIm1hdCI6MTcyODU2Njk5MwCwic2lk
```

```
IjoiSmw3bXF1WWlzbzZ1aHIySkJXZG9mS19YRjJ6aFBfQmNGMlE0R
0NsOEh3cyJ9.aMV45aaM2DjPG_X7v5sh7ZYNvAgVEzmdw0ew15t4g
2kK5-bKRyiTJPz1PsaJy0IN-
elBXlwr18r4xnerAY42fusGtc_jL2wt2aAPdeyofgmYpw4ynYatLj
zmjf2a-
w21Lt9JQVPHN8bIODM5gsaaphs2wW_wT2XIiC0TtVqB4b3F_1x00E
QXv4R8YFOaUcXCbYN6V83PjjYZpQWBbIG2qisiyHUfUqogRzER6aS
HFz5RP_mXwj_o1Bd5CXOTn1B_crAI_XCBYzS8ZLGpmADcjYXxA1AO
rFyjOkLZM9ONa-84QQopgIpcv4ZP0YNou3nD81g91Tm-aNCZIy-
Ep_88aA",
  "token_type": "Bearer",
  "expires_in": 300
}
```

Ошибка в случае некорректных данных:

Content-Type: application/json

```
{
  "error": "invalid_grant"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "error_description": "OAuth 2.0 Parameter: code",
  "error": "invalid_request",
  "error_uri":
  "https://datatracker.ietf.org/doc/html/rfc6749#section-5.2"
}
```

Ошибка в случае отсутствия прав на получение токенов доступа:

Content-Type: application/json

```
{
```

```
"error_description": "OAuth 2.0 Parameter:
grant_type",
"error": "unsupported_grant_type",
"error_uri":
"https://datatracker.ietf.org/doc/html/rfc6749#section-5.2"
}
```

6.6. Получение информации о токене OAuth 2.0

Имя ресурса: /authentication/api/v1/oauth2/token-info

Метод: POST или GET (поддерживаются оба метода)

HTTP-заголовки:

- Content-Type: application/x-www-form-urlencoded
- Authorization: Basic <Информация об авторизации>

6.6.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 96.

Описание данных в запросе приведено в таблице 97.

Таблица 96 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Заголовок HTTP-авторизации	Authorization	Строка	Да	Значение Basic авторизации в виде строки, состоящей из мнемоники ИС и секретной фразы. Значения мнемоники и секретной фразы присваивается системе-клиенту в процессе настройки доступа через OAuth 2.0. Например: dGVzdC1jbGllbnQ6dGVzdC1jbGllbnQ= //test-client:test-client в base64

Таблица 97 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Токен	token	Строка	Да	Токен, информацию о котором требуется получить

6.6.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 98.

Таблица 98 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак состояния токена	active	Логический	Да	Значение «true» – если токен валидный, значение «false» – если токен невалидный

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор аутентифицированного пользователя	sub	Строка	Да при active = true	Идентификатор аутентифицированного пользователя
Получатели токена	aud	Массив	Да при active = true	Список получателей токена, мнемоники внешней ИС, запросившей токен
Время до начала действия токена	nbf	Целое число	Да при active = true	Время в timestamp, с которого токен станет валидным
Область доступа токена	scope	Строка	Да при active = true	Области доступа токена, разделенные пробелом. Возможные значения приведены в таблице 83
Идентификатор генерирующей стороны	iss	Строка	Да при active = true	Идентификатор генерирующей стороны
Идентификатор УЗ пользователя	userUuid	UUID	Да при active = true	Идентификатор УЗ пользователя, данные которой доступны по токenu
Время истечения токена	exp	Целое число	Да при active = true	Время в timestamp, когда токен станет невалидным
Время создания токена	iat	Целое число	Да при active = true	Время в timestamp, когда токен был создан
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да при active = true	Идентификатор профиля УЗ пользователя, данные которого доступны по токenu
Мнемоника внешней ИС	client_id	Строка	Да при active = true	Мнемоника внешней ИС
Тип токена	token_type	Строка	Да при active = true	Тип токена. Определяет, для какого типа авторизации должен использоваться токен

6.6.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 99.

Таблица 99 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Тип ошибки	error	Строка	Да	Тип ошибки
Описание ошибки	error_description	Строка	Нет	Описание ошибки
Ссылка на описание ошибки	error_uri	Строка	Нет	Ссылка на документацию протокола OAuth 2.0 Authorization Framework

6.6.4. Пример выполнения запроса

Запрос:

POST

```
http://{host}/authentication/api/v1/oauth2/token-  
info?token=1yJraWQiOiIyOGE2ZmEyOS0wMDBiLTQzZTktOTBjMy  
02MDEzNDRmOGMxZDIiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJlMG  
JhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJhdWQ  
iOiJ0ZXN0LWNsaWVudCIsIm5iZiI6MTcyODAzMTAzNiwic2NvcGUi  
Olsib3Blbm1kIiwidXNlciJdLCJpc3MiOiJodHRwOi8vbG9jYXRob  
3N0OjgwODUiLCJlc2VyVXVpZCI6ImUwYmFiYTZLTg3MzMtNDhjZS  
04MTY4LTcwZjQ4ZjA3NThmYSIsImV4cCI6MTcyODAzMTMzNiwiawF  
0IjoxNzI4MDMxMDM2fQ.cpbXY1vvxfSeWH1JTeoBR4jgvMDP-  
Z1UuIF4ooF28-eqnzfGFC7VKNWC-rWfaPhzeDR-vmTEd4q4ML0ZeA-  
TGUvzcAdo-654uW3FSpz7HUU8CSxf2od-5zMpXn-  
zdg0KOc0WEitlKWDrMG4_0AtfRgBvpukUYwM8G9RE0TrU_RjMei6t  
CCEfD4L-  
un5qdbIfoTfk9xHK6W4AaPPCE6Dt5t4A_wmfyDbCmQo5vy4lhdmF9  
Rve4p8S38uEkca8aJwVWAzihhE5ZA2Kndn104z5GAfN0GS75VGfQY  
scC_4AFvRMF-ylKqj6_FYZbj8a5bMhAudSFhbaTb6l-MeryLtIhVg  
Content-Type: application/x-www-form-urlencoded  
Authorization: Basic dGVzdC1jbGllbnQ6dGVzdC1jbGllbnQ=
```

Ответ, если токен валиден:

Content-Type: application/json

```
{
  "active": true,
  "sub": "e0baba63-8733-48ce-8168-70f48f0758fa",
  "aud": [
    "test-client"
  ],
  "nbf": 1728031036,
  "scope": "openid user",
  "iss": "http://localhost:8085",
  "userUuid": "e0baba63-8733-48ce-8168-70f48f0758fa",
  "exp": 1728031336,
  "iat": 1728031036,
  "userProfileUuid": "4bb2ce18-af83-48b4-b0c5-
2467567735c3",
  "client_id": "test-client",
  "token_type": "Bearer"
}
```

Ответ, если токен невалиден:

Content-Type: application/json

```
{
  "active": false
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "error_description": "OAuth 2.0 Parameter: code",
  "error": "invalid_request",
  "error_uri":
"https://datatracker.ietf.org/doc/html/rfc6749#section-5.2"
```

```
}
```

Ошибка в случае отсутствия прав на получение токенов доступа:

Content-Type: application/json

```
{
  "error_description": "OAuth 2.0 Token Introspection
Parameter: token",
  "error": "invalid_request",
  "error_uri":
"https://datatracker.ietf.org/doc/html/rfc7662#section-2.1"
}
```

6.7. Обновление OAuth 2.0 токенов

Имя ресурса: /authentication/api/v1/oauth2/token

Метод: POST

HTTP-заголовки:

- Content-Type: application/x-www-form-urlencoded
- Authorization: Basic <Информация об авторизации>

6.7.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 100.

Описание данных в запросе приведено в таблице 101.

Таблица 100 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Заголовок HTTP-авторизации	Authorization	Строка	Да	Значение Basic авторизации в виде строки, состоящей из мнемоники ИС и секретной фразы. Значения мнемоники и секретной фразы присваивается системе-клиенту в процессе настройки доступа через OAuth 2.0. Например: dGVzdC1jbGllbnQ6dGVzdC1jbGllbnQ= //test-client:test-client в base64

Таблица 101 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Тип ответа, который ожидается от X-IDBox	grant_type	Строка	Да	Тип ответа, который ожидается от X-IDBox. Для получения авторизационного кода указывается фиксированное значение: grant_type=refresh_token
Токен обновления	refresh_token	Строка	Да	Токен обновления

6.7.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 102.

Таблица 102 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Токен доступа	access_token	Строка	Да	Токен доступа
Токен обновления	refresh_token	Строка	Да	Токен обновления
Область доступа токена	scope	Строка	Да	Области доступа токена, разделенные пробелом. Возможные значения приведены в таблице 83
Токен идентификации OpenID Connect 1.0	id_token	Строка	Да	Токен идентификации OpenId Connent 1.0
Тип токена	token_type	Строка	Да	Тип токена
Срок действия	expires_in	Строка	Да	Срок действия в секундах, через который истечёт токен доступа

6.7.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 103.

Таблица 103 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Тип ошибки	error	Строка	Да	Тип ошибки
Описание ошибки	error_description	Строка	Нет	Описание ошибки
Ссылка на описание ошибки	error_uri	Строка	Нет	Ссылка на документацию протокола OAuth 2.0 Authorization Framework

6.7.4. Пример выполнения запроса

Запрос:

POST

`http://{{host}}/authentication/api/v1/oauth2/token?gr`

```
ant_type=refresh_token&refresh_token=UGS83a-
bgnkuY7xwBVt1BGYGvMlX_v2_VYgOWlCro9Ax1o-g72B-
N1TnqnfxCglHtg1Yu8dhWwC8Ysf0vB4vK0J0yOI8kXr1darpAAZXE
hm81yrfs-Nznu1_u12048Tk
Content-Type: application/x-www-form-urlencoded
Authorization: Basic dGVzdC1jbGllbnQ6dGVzdC1jbGllbnQ=
```

Ответ:

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

```
{
  "access_token":
"eyJraWQiOiI5YzVjMzYyMS00NTY1LTQxNWItYTM0NS0zZjA5MTc2
Y2JhYjAiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJlMGJhYmE2My04
NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJhdWQiOiJ0ZXN0L
WNSaWVudCIsIm5iZiI6MTcyODU2Njk4OSwic2NvcGUiOlsib3Blbm
lkiIiwidXNlciJdLCJpc3MiOiJodHRwOi8vbG9jYWxob3N0OjgwODU
iLCJ1c2VyVXVpZCI6ImUwYmFiYTYzLTg3MzMtNDhjZS04MTY4LTcw
ZjQ4ZjA3NThtYSIsImV4cCI6MTcyODU2NzI4OSwiaWF0IjoxNzI4N
TY2OTg5LCJ1c2VyUHJvZmlsZVVlaWQiOiI0YmIyY2UxOC1hZjgzLT
Q4YjQtYjBjNS0yNDY3NTY3NzM1YzMiZmFQ.wxDbBCr90LvJnwFf6eGT
0SNnY5hV7jimI2JKZOpN-kcsf1bOIal50il-
W4DBoU78jYoJlc2MK-h4wa9_kQ0P-
Z2Y6ct70ruAPAARKE1aV9j8A8jYhY1qW6XbfjOVYb4m-
xzDqzpCKRD6sVFWx71WuYM5gvmys1G81PmuMdmvLup-
ts3AT6ef5w1IbPTawPQi7wqvQfKAyloUC4ejuid3cgtGkfMwClDo7
BF5xkHRX1qo32WdGelFnTx52ODf2q1wqMYUEyE1Y24GFEwaqatnUw
6RRaPT26a9slk6IuLKNcKOJ9uy6oqDy3VdQSbIznjj4jtbCKvxzIg
goJC9xhlc3Q",
  "refresh_token":
"Su1lxql7wWiD4EHiq7TJCXgTtcJUuXVZQNX_2CokZVj0UiBAosj
OKo_4DY74j3k8klYVDtaqbDW0ClHP7SS39yXK3WakAfSCxQXBwue4
XsAz54G2OdpQE6OLB7k2tIo",
  "scope": "openid user",
  "id_token":
"eyJraWQiOiI5YzVjMzYyMS00NTY1LTQxNWItYTM0NS0zZjA5MTc2
Y2JhYjAiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJlMGJhYmE2My04
NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJhdWQiOiJ0ZXN0L
WNSaWVudCIsImF6cCI6InRlc3QtY2xpZW50IiwiaXV0aF90aW1lIj
```

```
oxNzI4NTY2OTY4LCJpc3MiOiJodHRwOi8vbG9jYWxob3N0OjgwODU
iLCJleHAiOiE3Mjg1Njg3OTAsIm1hdCI6MTcyODU2Njk5MCwic2lk
IjoisSmw3bXF1WWlzbzZlaHIySkJXZG9mS19YRjJ6aFBfQmNGMlE0R
0NsOEh3cyJ9.aMV45aaM2DjPG_X7v5sh7ZYNvAgVEzmdw0ew15t4g
2kK5-bKRyiTJPz1PsaJy0IN-
elBXlwr18r4xnerAY42fusGtc_jL2wt2aAPdeyofgmYpw4ynYatLj
zmjf2a-
w21Lt9JQVPHN8bIODM5gsaaphs2wW_wT2XIiC0TtVqB4b3F_lx00E
QXv4R8YFOaUcXCbYN6V83PjjYZpQWBbIG2qisiyHUfUqogRzER6aS
HFz5RP_mXwj_o1Bd5CXOTn1B_crAI_XCBYzS8ZLGpmADcjYXxA1AO
rFyjOkLZM9ONa-84QQopgIpcv4ZP0YNou3nD81g91Tm-aNCZIy-
Ep_88aA",
  "token_type": "Bearer",
  "expires_in": 300
}
```

Ошибка в случае некорректных данных:

Content-Type: application/json

```
{
  "error": "invalid_grant"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "error_description": "OAuth 2.0 Parameter: code",
  "error": "invalid_request",
  "error_uri":
  "https://datatracker.ietf.org/doc/html/rfc6749#section-5.2"
}
```

Ошибка в случае отсутствия прав на получение токенов доступа:

Content-Type: application/json

```
{
  "error_description": "OAuth 2.0 Parameter:
grant_type",
  "error": "unsupported_grant_type",
  "error_uri":
"https://datatracker.ietf.org/doc/html/rfc6749#section-5.2"
}
```

6.8. Инвалидация OAuth 2.0 токена доступа

Имя ресурса: /authentication/api/v1/oauth2/revoke

Метод: POST

HTTP-заголовки:

- Content-Type: application/x-www-form-urlencoded
- Authorization: Basic <Информация об авторизации>

6.8.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 104.

Описание данных в запросе приведено в таблице 105.

Таблица 104 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Заголовок HTTP-авторизации	Authorization	Строка	Да	Значение Basic авторизации в виде строки, состоящей из мнемоники ИС и секретной фразы. Значения мнемоники и секретной фразы присваивается системе-клиенту в процессе настройки доступа через OAuth 2.0. Например: dGVzdC1jbGllbnQ6dGVzdC1jbGllbnQ= //test-client:test-client в base64

Таблица 105 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Токен	token	Строка	Да	Токен для инвалидации

6.8.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 106.

Таблица 106 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Тип ошибки	error	Строка	Да	Тип ошибки
Описание ошибки	error_description	Строка	Нет	Описание ошибки
Ссылка на описание ошибки	error_uri	Строка	Нет	Ссылка на документацию протокола OAuth 2.0 Authorization Framework

6.8.3. Пример выполнения запроса

Запрос:

POST

[illegible]

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "error_description": "OAuth 2.0 Parameter: code",
  "error": "invalid_request",
  "error_uri":
"https://datatracker.ietf.org/doc/html/rfc6749#section-5.2"
}
```

6.9. Получение данных УЗ пользователя с динамическими полями по токenu OAuth 2.0

Имя ресурса: /authentication/api/v1/oauth2/user

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Authorization: Bearer <Токен доступа>

6.9.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 107.

Описание данных в запросе приведено в таблице 108.

Таблица 107 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Заголовок HTTP-авторизации	Authorization	Строка	Да	Тип авторизации Bearer со значением токена доступа access_token

Для доступа к методу токен должен иметь область доступа (scope): user.

Таблица 108 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Техническое наименование источника динамических полей УЗ пользователя	dynamicFieldSourceTechName	Строка	Нет	Техническое наименование источника динамических полей УЗ пользователя. Обязателен для передачи при необходимости получения информации о динамических полях пользователя при наличии областей доступа (scope) в токене доступа: user, user-dynamic-fields

6.9.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 109.

Таблица 109 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Идентификатор	uuid	UUID	Да	Идентификатор пользователя	user
Имя пользователя	firstName	Строка	Да	Имя пользователя	user, profile
Фамилия пользователя	lastName	Строка	Да	Фамилия пользователя	user, profile
Отчество пользователя	middleName	Строка	Нет	Отчество пользователя	user, profile
ИНН	inn	Строка	Нет	ИНН пользователя	user
СНИЛС	snils	Строка	Нет	СНИЛС пользователя	user
Дата рождения	birthday	Дата	Нет	Дата рождения пользователя	user, profile
Логин	login	Строка	Нет	Логин пользователя	user, profile
Адрес электронной почты	email	Строка	Нет	Адрес электронной почты пользователя	user, email
Дата изменения пароля	passwordChanged	Дата и время	Нет	Дата и время изменения пароля. Если указано значение null, то пароль еще ни разу не устанавливался	user

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Дата верификации адреса электронной почты	emailVerified	Дата и время	Нет	Дата и время верификации адреса электронной почты пользователя	user, email
Признак блокирования УЗ пользователя	isBlocked	Логический	Да	Значение «true» – если УЗ пользователя заблокирована, значение «false» – если УЗ пользователя не заблокирована	user
Состояние УЗ пользователя	state	Строка	Да	Состояние УЗ пользователя	user
Дата согласия на обработку ПДн	privacyPolicyAccepted	Дата и время	Нет	Дата и время принятия политики конфиденциальности	user
Динамические поля пользователя	dynamicFields	Объект	Нет	Динамические поля пользователя	user, user-dynamic-fields
Идентификатор источника динамических полей	sourceUuid	UUID	Да	Идентификатор источника динамических полей УЗ пользователя	user, user-dynamic-fields
Техническое наименование источника динамических полей	sourceTechName	Строка	Да	Техническое наименование источника динамических полей УЗ пользователя	user, user-dynamic-fields
Наименование источника динамических полей	sourceLabel	Строка	Да	Наименование источника динамических полей УЗ пользователя	user, user-dynamic-fields

Параметр		Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
	Динамические поля	dynamicFields	Массив	Да	Список динамических полей	user, user-dynamic-fields
	Идентификатор динамического поля	uuid	UUID	Нет	Идентификатор динамического поля	user, user-dynamic-fields
	Наименование динамического поля	label	Строка	Нет	Наименование динамического поля	user, user-dynamic-fields
	Техническое наименование динамического поля	techName	Строка	Нет	Техническое наименование динамического поля	user, user-dynamic-fields
	Содержимое динамического поля	content	Объект/ Массив	Нет	Содержимое динамического поля. Тип данных зависит от содержимого динамического поля: – Объект – если динамическое поле простое. – Массив – если динамическое поле содержит объект или массив значений	user, user-dynamic-fields
	Значение динамического поля	value	Строка	Нет	Значение динамического поля. Только для простых динамических полей или динамических полей, содержащих массив значений	user, user-dynamic-fields

Параметр				Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
			Признак удаления значения динамического поля	isDeleted	Логический	Нет	Значение «true» – если значение динамического поля удалено, значение «false» – если значение динамического поля не удалено. Только для простых динамических полей или динамических полей, содержащих массив значений	user, user-dynamic-fields
			Идентификатор динамического поля объекта	uuid	UUID	Нет	Идентификатор динамического поля объекта. Только для динамических полей, содержащих объект	user, user-dynamic-fields
			Наименование динамического поля объекта	label	Строка	Нет	Наименование динамического поля объекта. Только для динамических полей, содержащих объект	user, user-dynamic-fields
			Техническое наименование динамического поля объекта	techName	Строка	Нет	Техническое наименование динамического поля объекта. Только для динамических полей, содержащих объект	user, user-dynamic-fields
			Содержимое динамического поля	content	Массив	Нет	Содержимое динамического поля. Только для динамических полей, содержащих объект	user, user-dynamic-fields
			Значение динамического поля объекта	value	Строка	Нет	Значение динамического поля объекта. Только для динамических полей, содержащих объект	user, user-dynamic-fields

Параметр					Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
				Признак удаления значения динамического поля	isDeleted	Логический	Нет	Значение «true» – если значение динамического поля удалено, значение «false» – если значение динамического поля не удалено. Только для динамических полей, содержащих объект	user, user-dynamic-fields

6.9.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 110. В случае возникновения ошибки при истекшем или несуществующем токене возвращается ответ, структура которого приведена в таблице 111. В ответе на запрос возвращается HTTP-заголовок.

Таблица 110 – 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

Таблица 111 – Данные в HTTP-заголовке ответа на запрос при истекшем или несуществующем токене

Параметр	Название параметра	Тип данных	Описание
Результат аутентификации	WWW-Authenticate	Строка	Ошибка с сообщением

6.9.4. Пример выполнения запроса

Запрос:

GET

http://{host}}/authentication/api/v1/oauth2/user?dynamicFieldSourceTechName=FREE_IPA

Content-Type: application/json

Authorization: Bearer

eyJraWQ4Y2U0ODE2OC03ZmM2FmMGFmYjQyMWIiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJlMGJhYme2My04NzZmLTQ4Y2U0ODE2OC03

```
MGY0OGYwNzU4ZmEiLCJhdWQiOiJ0ZXN0LWNsaWVudCIsIm5iZiI6M
TcyODU2MDk0OCwic2NvcGUiOlsib3BlbmlkIiwidXNlciJdLCJpc3
MiOiJodHRwOi8vbG9jYWxob3N0OjgwODUiLCJ1c2V
yVXVpZCI6ImUwYmFiYTYzLTg3MzMtNDhjZS04MTY4LTcwZjQ4ZjA3
NTNmYSIsImV4cCI6MTcyODU2MTI0OCwiaWF0IjoxNzI4NTYwOTQ4L
CJ1c2VyUHJvZmlsZVV1aWQiOiI0YmIyY2UxOC1hZj
gzLTQ4YjQtYjBjNS0yNDY3NTY3NzM1YzMiYmIyY2UxOC1hZj
B_ZBmk2nslaJdmR-
BU1xCM_TttCikRGVZ2pvsz8PTYK_tUk4gMYb9888n0EBFMlT_LzbH
g_cKSUJWEZ-ZV-p3st6QRGqSt
lm98FMHjw2qERQPlvema8oPkxPCuqlxNpKtiP0yzDLLznUAqCSmXD
p8Qu1P6SP91I5AN8CrBTBBRXC44oBE2bWHemUYmIo7lUgV0Bnovq0
zLndFl7yLqRF65O0O2IxYjp2ui2gbhUXB5VjmHOV1
5f5V8CyKf3p80D0fU_gE0_RM5O3a7sDiSW9fK_UFdUZzSzjMa6MsZ
u27nh4yrozMPIwjyOLRjusWH6QR3NkoA
```

Ответ:

Content-Type: application/json

```
{
  "uuid": "65bf51ce-7502-4f08-b5ec-39b6c446a465",
  "firstName": "Раиса", //Возвращается в ответе, если
  токен доступа «access_token» имеет область доступа
  (scope): profile
  "lastName": "Авдеева", //Возвращается в ответе,
  если токен доступа «access_token» имеет область
  доступа (scope): profile
  "middleName": "Петровна", //Возвращается в ответе,
  если токен доступа «access_token» имеет область
  доступа (scope): profile
  "inn": "658773838427",
  "snils": "79330927129",
  "birthday": "1985-02-03", //Возвращается в ответе,
  если токен доступа «access_token» имеет область
  доступа (scope): profile
  "login": "avdeeva", //Возвращается в ответе, если
  токен доступа «access_token» имеет область доступа
  (scope): profile
```

```
"email": "avdeeva@local.ru", //Возвращается в
ответе, если токен доступа «access_token» имеет
область доступа (scope): email
"passwordChanged": "2024-01-18T21:20:12.592912Z",
"emailVerified": "2024-02-08T09:35:53.260505Z",
//Возвращается в ответе, если токен доступа
«access_token» имеет область доступа (scope): email
"isBlocked": false,
"state": "ACTIVE",
"privacyPolicyAccepted": "2024-01-
18T21:20:12.592912Z",
"dynamicFields": { //Возвращается в ответе, если
токен доступа «access_token» имеет область доступа
(scope): user-dynamic-fields и передан параметр
«dynamicFieldSourceTechName»
  "sourceUuid": "5c84b6a9-6a28-483f-a40f-
ea8b6159fcf3",
  "sourceTechName": "FREE_IPA",
  "sourceLabel": "FREE_IPA",
  "dynamicFields": [
    {
      "uuid": "b7e5c345-6981-4a7e-aed0-
194360d7b661",
      "label": "Страна",
      "techName": "city",
      "content": {
        "value": "Россия",
        "isDeleted": false
      }
    },
    {
      "uuid": "ead47367-9a18-41be-9711-
60e48de70a64",
      "label": "Уникальный идентификатор профиля
LDAP",
      "techName": "ipaUniqueProfileID",
      "content": {
        "value": "415a46ed-06bf-49ad-933f-
c771fa22c389",
        "isDeleted": false
      }
    }
  ]
}
```

```
    }  
  },  
  {  
    "uuid": "ebfe666a-4e71-49b2-89e3-  
37827bc9109f",  
    "label": "Город",  
    "techName": "l",  
    "content": {  
      "value": "Калининград",  
      "isDeleted": false  
    }  
  },  
  {  
    "uuid": "9ffcfaf38-96e0-4c20-8c7d-  
35eb328f59ff",  
    "label": "Номер телефона",  
    "techName": "mobile",  
    "content": {  
      "value": null,  
      "isDeleted": false  
    }  
  }  
]  
}  
}
```

Ошибка выполнения запроса при непереданном заголовке Authorization или отсутствии у токена scope:

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Access Denied",  
  "timestamp": "2024-10-10T11:49:36.276139100Z"  
}
```

Ошибка выполнения запроса:

Content-Type: application/json

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

Ошибка выполнения запроса:

Content-Type: application/json

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

Ошибка при несуществующем токене:

HTTP/1.1 401
WWW-Authenticate: Bearer error="invalid_token",
error_description="An error occurred while attempting
to decode the Jwt: Signed JWT rejected: Invalid
signature",
error_uri="https://tools.ietf.org/html/rfc6750#section-3.1"

Ошибка при истекшем токене:

HTTP/1.1 401
WWW-Authenticate: Bearer error="invalid_token",
error_description="An error occurred while attempting
to decode the Jwt: Jwt expired at 2024-10-
28T07:01:34Z",
error_uri="https://tools.ietf.org/html/rfc6750#section-3.1"

6.10. Получение данных профиля УЗ пользователя с динамическими полями профиля УЗ пользователя и организации по токenu OAuth 2.0

Имя ресурса: /authentication/api/v1/oauth2/user-profile

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Authorization: Bearer <Токен доступа>

6.10.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 112.

Описание данных в запросе приведено в таблице 113.

Таблица 112 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Заголовок HTTP-авторизации	Authorization	Строка	Да	Тип авторизации Bearer со значением токена доступа access_token

Для доступа к методу токен должен иметь области доступа (scope): user-profile и organization.

Таблица 113 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Техническое наименование источника динамических полей профиля УЗ пользователя	dynamicFieldSource TechName	Строка	Нет	Техническое наименование источника динамических полей профиля УЗ пользователя. Обязателен для передачи при необходимости получения информации о

Параметр	Название параметра	Тип данных	Обязательность	Описание
				динамических полях профиля УЗ пользователя при наличии областей доступа (scope) в токене доступа: user-profile, organization, user-profile-dynamic-fields
Техническое наименование источника динамических полей организации	organizationDynamicFieldSourceTechName	Строка	Нет	Техническое наименование источника динамических полей организации. Обязателен для передачи при необходимости получения информации о динамических полях организации при наличии областей доступа (scope) в токене доступа: user-profile, organization, organization-dynamic-fields

6.10.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 114.

Таблица 114 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Идентификатор профиля УЗ пользователя	uuid	UUID	Да	Идентификатор профиля УЗ пользователя	user-profile, organization
Признак блокирования профиля УЗ пользователя	isBlocked	Логический	Да	Значение «true» – если профиль УЗ пользователя заблокирован, значение «false» – если профиль УЗ пользователя не заблокирован	user-profile, organization
Состояние профиля УЗ пользователя	state	Строка	Да	Состояние профиля УЗ пользователя	user-profile, organization
Адрес электронной почты профиля УЗ пользователя	workEmail	Строка	Нет	Адрес электронной почты профиля УЗ пользователя	user-profile, organization
Дата верификации адреса электронной почты профиля УЗ пользователя	workEmailVerified	Дата и время	Нет	Дата и время верификации адреса электронной почты профиля УЗ пользователя	user-profile, organization
Дата регистрации	registrationDate	Дата и время	Да	Дата и время регистрации профиля УЗ пользователя	user-profile, organization

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Данные об организации	organization	Объект	Да	Данные об организации, которой принадлежит профиль УЗ пользователя	user-profile, organization
Идентификатор	uuid	UUID	Да	Идентификатор организации	user-profile, organization
Полное наименование	fullName	Строка	Да	Полное наименование организации	user-profile, organization
Краткое наименование	shortName	Строка	Да	Краткое наименование организации	user-profile, organization
Техническое наименование типа	typeTechName	Строка	Да	Техническое наименование типа организации	user-profile, organization
Наименование типа	typeLabel	Строка	Да	Наименование типа организации	user-profile, organization
ИНН	inn	Строка	Да	ИНН организации	user-profile, organization
КПП	kpp	Строка	Нет	КПП организации	user-profile, organization
ОГРН	ogrn	Строка	Нет	ОГРН организации	user-profile, organization
Признак блокирования организации	isBlocked	Логический	Да	Значение «true» – если организация заблокирована, значение «false» – если организация не заблокирована	user-profile, organization
Состояние	state	Строка	Да	Состояние организации	user-profile, organization
Адрес	address	Строка	Да	Адрес организации	user-profile, organization

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Дата регистрации	registrationDate	Дата и время	Нет	Дата регистрации организации	user-profile, organization
Дата создания	createDate	Дата и время	Да	Дата создания организации в системе	user-profile, organization
Динамические поля профиля УЗ пользователя	dynamicFields	Объект	Нет	Динамические поля профиля УЗ пользователя	user-profile, organization, user-profile-dynamic-fields
Идентификатор источника динамических полей	sourceUuid	UUID	Да	Идентификатор источника динамических полей	user-profile, organization, user-profile-dynamic-fields
Техническое наименование источника динамических полей	sourceTechName	Строка	Да	Техническое наименование источника динамических полей	user-profile, organization, user-profile-dynamic-fields
Наименование источника динамических полей	sourceLabel	Строка	Да	Наименование источника динамических полей	user-profile, organization, user-profile-dynamic-fields
Динамические поля УЗ пользователя	dynamicFields	Массив	Да	Динамические поля УЗ пользователя	user-profile, organization, user-profile-dynamic-fields
Идентификатор динамического поля	uuid	UUID	Нет	Идентификатор динамического поля	user-profile, organization, user-profile-dynamic-fields

Параметр		Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
	Наименование динамического поля	label	Строка	Нет	Наименование динамического поля	user-profile, organization, user-profile-dynamic-fields
	Техническое наименование динамического поля	techName	Строка	Нет	Техническое наименование динамического поля	user-profile, organization, user-profile-dynamic-fields
	Содержимое динамического поля	content	Объект/ Массив	Нет	Содержимое динамического поля. Тип данных зависит от содержимого динамического поля: – объект – если динамическое поле простое; – массив – если динамическое поле содержит объект или массив значений	user-profile, organization, user-profile-dynamic-fields
	Значение динамического поля	value	Строка	Нет	Значение динамического поля. Только для простых динамических полей или динамических полей, содержащих массив значений	user-profile, organization, user-profile-dynamic-fields
	Признак удаления значения динамического поля	isDeleted	Логический	Нет	Значение «true» – если значение динамического поля удалено, значение «false» – если значение динамического поля не удалено. Только для простых динамических полей или динамических полей, содержащих массив значений	user-profile, organization, user-profile-dynamic-fields

Параметр				Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
			Идентификатор динамического поля объекта	uuid	UUID	Нет	Идентификатор динамического поля объекта. Только для динамических полей, содержащих объект	user-profile, organization, user-profile-dynamic-fields
			Наименование динамического поля объекта	label	Строка	Нет	Наименование динамического поля объекта. Только для динамических полей, содержащих объект	user-profile, organization, user-profile-dynamic-fields
			Техническое наименование динамического поля объекта	techName	Строка	Нет	Техническое наименование динамического поля объекта. Только для динамических полей, содержащих объект	user-profile, organization, user-profile-dynamic-fields
			Содержимое динамического поля	content	Массив	Нет	Содержимое динамического поля. Только для динамических полей, содержащих объект	user-profile, organization, user-profile-dynamic-fields
			Значение динамического поля объекта	value	Строка	Нет	Значение динамического поля объекта. Только для динамических полей, содержащих объект	user-profile, organization, user-profile-dynamic-fields
			Признак удаления значения динамического поля	isDeleted	Логический	Нет	Значение «true» – если значение динамического поля удалено, значение «false» – если значение динамического поля не удалено. Только для динамических полей, содержащих объект	user-profile, organization, user-profile-dynamic-fields

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Динамические поля организации	organizationDynamicFields	Объект	Нет	Динамические поля организации	user-profile, organization, organization-dynamic-fields
Идентификатор источника динамических полей	sourceUuid	UUID	Да	Идентификатор источника динамических полей	user-profile, organization, organization-dynamic-fields
Техническое наименование источника динамических полей	sourceTechName	Строка	Да	Техническое наименование источника динамических полей	user-profile, organization, organization-dynamic-fields
Наименование источника динамических полей	sourceLabel	Строка	Да	Наименование источника динамических полей	user-profile, organization, organization-dynamic-fields
Динамические поля УЗ пользователя	dynamicFields	Массив	Да	Динамические поля УЗ пользователя	user-profile, organization, organization-dynamic-fields
Идентификатор динамического поля	uuid	UUID	Нет	Идентификатор динамического поля	user-profile, organization, organization-dynamic-fields
Наименование динамического поля	label	Строка	Нет	Наименование динамического поля	user-profile, organization, organization-dynamic-fields

Параметр			Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
		Техническое наименование динамического поля	techName	Строка	Нет	Техническое наименование динамического поля	user-profile, organization, organization-dynamic-fields
		Содержимое динамического поля	content	Объект/ Массив	Нет	Содержимое динамического поля. Тип данных зависит от содержимого динамического поля: – Объект – если динамическое поле простое. – Массив – если динамическое поле содержит объект или массив значений	user-profile, organization, organization-dynamic-fields
		Значение динамического поля	value	Строка	Не	Значение динамического поля. Только для простых динамических полей или динамических полей, содержащих массив значений	user-profile, organization, organization-dynamic-fields
		Признак удаления значения динамического поля	isDeleted	Логический	Нет	Значение «true» – если значение динамического поля удалено, значение «false» – если значение динамического поля не удалено. Только для простых динамических полей или динамических полей, содержащих массив значений	user-profile, organization, organization-dynamic-fields
		Идентификатор динамического поля объекта	uuid	UUID	Нет	Идентификатор динамического поля объекта. Только для динамических полей, содержащих объект	user-profile, organization, organization-dynamic-fields

Параметр				Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
			Наименование динамического поля объекта	label	Строка	Нет	Наименование динамического поля объекта. Только для динамических полей, содержащих объект	user-profile, organization, organization-dynamic-fields
			Техническое наименование динамического поля объекта	techName	Строка	Нет	Техническое наименование динамического поля объекта. Только для динамических полей, содержащих объект	user-profile, organization, organization-dynamic-fields
			Содержимое динамического поля	content	Массив	Нет	Содержимое динамического поля. Только для динамических полей, содержащих объект	user-profile, organization, organization-dynamic-fields
			Значение динамического поля объекта	value	Строка	Нет	Значение динамического поля объекта. Только для динамических полей, содержащих объект	user-profile, organization, organization-dynamic-fields
			Признак удаления значения динамического поля	isDeleted	Логический	Нет	Значение «true» – если значение динамического поля удалено, значение «false» – если значение динамического поля не удалено. Только для динамических полей, содержащих объект	user-profile, organization, organization-dynamic-fields
Подразделения и должности профиля УЗ пользователя				positions	Массив	Нет	Подразделения и должности профиля УЗ пользователя	user-profile, organization
			Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя	user-profile, organization

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Идентификатор подразделения	departmentUuid	UUID	Да	Идентификатор подразделения	user-profile, organization
Наименование подразделения	departmentName	Строка	Да	Наименование подразделения	user-profile, organization
Техническое наименование подразделения	departmentTechName	Строка	Да	Техническое наименование подразделения	user-profile, organization
Идентификатор должности	positionUuid	UUID	Да	Идентификатор должности	user-profile, organization
Наименование должности	positionName	Строка	Да	Наименование должности	user-profile, organization
Техническое наименование должности	positionTechName	Строка	Да	Техническое наименование должности	user-profile, organization
Признак главы департамента	isDepartmentHead	Логический	Да	Значение «true» – если пользователь является главой департамента, значение «false» – если пользователь не является главой департамента	user-profile, organization
Дата и время назначения должности	appointmentDate	Дата и время	Да	Дата и время назначения должности	user-profile, organization

6.10.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 115. В случае возникновения ошибки при истекшем или несуществующем токене возвращается ответ, структура которого приведена в таблице 116. В ответе на запрос возвращается HTTP-заголовок.

Таблица 115 – 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

Таблица 116 – Данные в HTTP-заголовке ответа на запрос при истекшем или несуществующем токене

Параметр	Название параметра	Тип данных	Описание
Результат аутентификации	WWW-Authenticate	Строка	Ошибка с сообщением

6.10.4. Пример выполнения запроса

Запрос:

GET

http://{host}}/authentication/api/v1/oauth2/user-profile?dynamicFieldSourceTechName=FREE_IPA&organizationDynamicFieldSourceTechName=FREE_IPA

Content-Type: application/json

Authorization: Bearer

eyJraWQiaOiIyYTQ4N2Q0OS0zMzA0LTRkNDYtYTA5My0wM2FmMGFmYjQyMWIiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJlMGJhYme2My04NzMzLTQ4Y2UtODE2OC03

```
MGY00GYwNzU4ZmEiLCJhdWQiOiJ0ZXN0LWNsaWVudCIsIm5iZiI6M
TcyODU2MDk0OCwic2NvcGUiOlsib3BlbmlkIiwidXNlciJdLCJpc3
MiOiJodHRwOi8vbG9jYWxob3N0OjgwODUiLCJ1c2V
yVXVpZCI6ImUwYmFiYTYzLTg3MzMtNDhjZS04MTY4LTcwZjQ4ZjA3
NTNmYSIsImV4cCI6MTcyODU2MTI0OCwiaWF0IjoxNzI4NTYwOTQ4L
CJ1c2VyUHJvZmlsZVV1aWQiOiI0YmIyY2UxOC1hZj
gzLTQ4YjQtYjBjNS0yNDY3NTY3NzM1YzMifQ.R4kvVSxbpjirPRBm
B_ZBmk2nslaJdmR-
BU1xCM_TttCikRGVZ2pvsz8PTYK_tUk4gMYb9888n0EBFmLT_LzbH
g_cKSUJWEZ-ZV-p3st6QRGqSt
lm98FMHjw2qERQPlvema8oPkxPCuqlxNpKtiP0yzDLLznUAqCSmXD
p8Qu1P6SP91I5AN8CrBTBBRXC44oBE2bWHemUYmIo7lUgV0Bnovq0
zLndFl7yLqRF65O0O2IxYjp2ui2gbhUXB5VjmHOV1
5f5V8CyKf3p80D0fU_gE0_RM5O3a7sDISW9fK_UFdUZzSszjMa6MsZ
u27nh4yrozMPIwjyOLRjusWH6QR3NkoA
```

Ответ:

Content-Type: application/json

```
{
  "uuid": "abe4abec-5f38-49a3-bfdd-a990e11e9435",
  "isBlocked": false,
  "state": "ACTIVE",
  "workEmail": "liza@localhost.ru",
  "workEmailVerified": "2024-01-23T06:51:09.870305Z",
  "registrationDate": "2024-01-23T06:50:35.456343Z",
  "organization": {
    "uuid": "087a7cae-8cd3-44d5-896b-e86102164bba",
    "fullName": "АО Авоир дремучий",
    "shortName": "АО Авоир дремучий",
    "typeTechName": "juristic",
    "typeLabel": "Юридическое лицо",
    "inn": "2252455070",
    "kpp": "037271508",
    "ogrn": "1463527365443",
    "isBlocked": false,
    "state": "ACTIVE",
    "address": "Московская обл., г. Москва, ул.
Московская д.4, оф.2",
    "registrationDate": null,

```

```
"createDate": "2023-01-28T09:20:36.355757Z"
},
"dynamicFields": { //Возвращается в ответе, если
токен доступа «access_token» имеет область доступа
(scope): user-profile-dynamic-fields и передан
параметр «dynamicFieldSourceTechName»
  "sourceUuid": "5c84b6a9-6a28-483f-a40f-
ea8b6159fcf3",
  "sourceTechName": "FREE_IPA",
  "sourceLabel": "FREE_IPA",
  "dynamicFields": [
    {
      "uuid": "b7e5c345-6981-4a7e-aed0-
194360d7b661",
      "label": "Страна",
      "techName": "city",
      "content": {
        "value": "Россия",
        "isDeleted": false
      }
    },
    {
      "uuid": "ead47367-9a18-41be-9711-
60e48de70a64",
      "label": "Уникальный идентификатор профиля
LDAP",
      "techName": "ipaUniqueProfileID",
      "content": {
        "value": "415a46ed-06bf-49ad-933f-
c771fa22c389",
        "isDeleted": false
      }
    },
    {
      "uuid": "ebfe666a-4e71-49b2-89e3-
37827bc9109f",
      "label": "Город",
      "techName": "l",
      "content": {
        "value": "Калининград",
```

```
        "isDeleted": false
      }
    },
    {
      "uuid": "9ffcf3a38-96e0-4c20-8c7d-
35eb328f59ff",
      "label": "Номер телефона",
      "techName": "mobile",
      "content": {
        "value": null,
        "isDeleted": false
      }
    }
  ]
},
"organizationDynamicFields": { //Возвращается в
ответе, если токен доступа «access_token» имеет
область доступа (scope): organization-dynamic-fields
и передан параметр
«organizationDynamicFieldSourceTechName»
  "sourceUuid": "3557063c-3836-4f5a-8697-
9ed9574e5782",
  "sourceTechName": "FREE_IPA",
  "sourceLabel": "FREE_IPA",
  "dynamicFields": [
    {
      "uuid": "cb4c2043-fc45-4205-8d17-
83e696d4cbbd",
      "label": "Уникальный идентификатор LDAP",
      "techName": "entryUUID",
      "content": {
        "value": "CN=Авоир Дремучий
АД, CN=Organizations, DC=xidbox, DC=dcs, DC=infosec, DC=ru
",
        "isDeleted": false
      }
    }
  ]
},
"positions": [
```

```
{
  "userProfileUuid": "9d25606a-b69c-4c38-bdb9-330abd8cd5f7",
  "departmentUuid": "84d04f0e-479f-4ac6-9a03-6f41ae759674",
  "departmentName": "newDepartmentTechName1",
  "departmentTechName": "departmentTechName1",
  "positionUuid": "cb06dc2e-89a7-4f6f-a7fd-81b67223a622",
  "positionName": "position",
  "positionTechName": "positionTechName",
  "isDepartmentHead": true,
  "appointmentDate": "2024-02-19T17:16:21.601551Z"
}
```

Ошибка выполнения запроса при непереданном заголовке Authorization или отсутствии у токена scope:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Access Denied",
  "timestamp": "2024-10-10T11:49:36.276139100Z"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

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

Ошибка выполнения запроса:

Content-Type: application/json

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

Ошибка при несуществующем токене:

HTTP/1.1 401

WWW-Authenticate: Bearer error="invalid_token",
error_description="An error occurred while attempting
to decode the Jwt: Signed JWT rejected: Invalid
signature",
error_uri="https://tools.ietf.org/html/rfc6750#section-3.1"

Ошибка при истекшем токене:

HTTP/1.1 401

WWW-Authenticate: Bearer error="invalid_token",
error_description="An error occurred while attempting
to decode the Jwt: Jwt expired at 2024-10-
28T07:01:34Z",
error_uri="https://tools.ietf.org/html/rfc6750#section-3.1"

6.11. Получение всех описаний областей доступа (scope)

Имя ресурса: /authentication/api/v1/oauth2/scopes/all

Метод: GET

HTTP-заголовки:

– Content-Type: application/json

6.11.1. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 117.

Таблица 117 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Список областей доступа	items	Массив	Да	Список областей доступа
Техническое наименование	techName	Строка	Да	Техническое наименование
Наименование	name	Строка	Да	Наименование для отображения в интерфейсе
Признак отображения в интерфейсе	isDisplayOnInterface	Логический	Да	Значение «true» – если отображение в интерфейсе включено, значение «false» – если отображение в интерфейсе отключено

6.11.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 118.

Таблица 118 – 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

6.11.3. Пример выполнения запроса

Запрос:

GET

http://{{host}}/authentication/api/v1/oauth2/scopes/all

Content-Type: application/json

Ответ:

Content-Type: application/json

```
{
  "items": [
    {
      "techName": "openid",
      "name": "Идентификатор учетной записи",
      "isDisplayOnInterface": true
    },
    {
      "techName": "user-dynamic-fields",
      "name": "Динамические поля пользователя",
      "isDisplayOnInterface": true
    },
    {
      "techName": "user-profile-dynamic-fields",
      "name": "Динамические поля профиля УЗ",
      "isDisplayOnInterface": true
    },
    {
      "techName": "organization-dynamic-fields",
      "name": "Динамические поля организации
профиля",
      "isDisplayOnInterface": true
    },
    {
      "techName": "user-profile",
      "name": "Данные профиля УЗ",
      "isDisplayOnInterface": true
    },
    {
      "techName": "organization",
      "name": "Данные организации профиля",
      "isDisplayOnInterface": true
    },
    {
      "techName": "user",
      "name": "Данные учетной записи",
      "isDisplayOnInterface": true
    }
  ]
}
```

```

    },
    {
      "techName": "email",
      "name": "Адрес электронной почты учетной
записи",
      "isDisplayOnInterface": true
    },
    {
      "techName": "profile",
      "name": "Логин, ФИО, дата рождения",
      "isDisplayOnInterface": true
    }
  ]
}

```

Ошибка выполнения запроса:

Content-Type: application/json

```

{
  "type": "MESSAGE",
  "payload": "Метод не разрешен.",
  "timestamp": "2021-09-28T12:51:06.118102500Z"
}

```

6.12. Получение наименования OAuth 2.0-клиента для отображения

Имя ресурса: /authentication/api/v1/oauth2/client/readable-name

Метод: GET

HTTP-заголовки:

– Content-Type: application/json

6.12.1. Данные в запросе

Описание данных в запросе приведено в таблице 119.

Таблица 119 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Мнемоника OAuth 2.0-клиента	clientId	Строка	Да	Мнемоника OAuth 2.0-клиента

6.12.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 120.

Таблица 120 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Мнемоника OAuth 2.0-клиента	clientId	Строка	Да	Мнемоника OAuth 2.0-клиента
Наименование OAuth 2.0-клиента	readableName	Строка	Да	Наименование OAuth 2.0-клиента для отображения в интерфейсе

6.12.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 121.

Таблица 121 – 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

6.12.4. Пример выполнения запроса

Запрос:

GET

```
http://{{host}}/authentication/api/v1/oauth2/client/readable-name?clientId=test-client  
Content-Type: application/json
```

Ответ:

Content-Type: application/json

```
{  
  "clientId": "test-client",  
  "readableName": "ИС Ромашка"  
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Not found by clientId: test-client",  
  "timestamp": "2024-10-30T15:44:35.624637800Z"  
}
```

6.13. Получение набора публичных ключей OAuth 2.0 сервера

Имя ресурса: /authentication/api/v1/oauth2/jwks

Метод: GET

6.13.1. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 122.

Таблица 122 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Набор публичных ключей	keys	Массив	Да	Список публичных ключей
Тип ключа	key_type	Строка	Да	Вид криптографических алгоритмов, используемых для подписи ключа. Например, «RSA» или «EC» для ключей эллиптической кривой
Идентификатор ключа	key_id	Строка	Нет	Уникальный идентификатор ключа
Алгоритм подписи	alg	Строка	Нет	Алгоритм, который использовался для подписи ключа. Например, RS256, ES256, PS256
Операции с ключом	key_ops	Массив	Нет	Список строк, указывающих, для каких криптографических операций предназначен ключ
Использование ключа	use	Строка	Нет	Предполагаемое использование или цель ключа. Например, подписание («sig») или шифрование («enc»)
Значение открытого ключа типа «RSA»	n	Строка	Нет	Модуль открытого ключа
Значение экспоненты	e	Строка	Нет	Экспонента
Тип кривой ключа типа «EC»	crv	Строка	Нет	Тип кривой
Координата x	x	Строка	Нет	Координата x
Координата y	y	Строка	Нет	Координата y
Цепочка сертификатов X.509	x5c	Строка	Нет	Цепочка сертификатов PKI, используемых для подписи JWT

Параметр	Название параметра	Тип данных	Обязательность	Описание
Отпечаток сертификата X.509	x5t	Строка	Нет	Отпечаток SHA-1 сертификата X.509, используемого для подписи токена
URI получения открытого ключа X.509	x5u	Строка	Нет	URI, который ссылается на ресурс для сертификата открытого ключа X.509 или цепочки сертификатов

6.13.2. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/authentication/api/v1/oauth2/jwks
```

Ответ:

Content-Type: application/json

```
{
  "keys": [
    {
      "kty": "RSA",
      "e": "AQAB",
      "kid": "7be85f87-1965-4666-87c5-6c6b965ccfc0",
      "n":
"xkesnaIchsJ6tVdL8ZrUtnB9wW8va8o3yIC51aBzooQ7pqtMhaLn
ycmQEQAqtFM4HD1FkMb3n9mn3CJbE9kdb4TTCVwxK-
TnCXk50mq2iUV99ETToC6d-
8pkxp7IoBt808Y7jjNdArIL_W1VeGpratqOLXHg5AJC4cdfWdD6EM
5HrHVu0m8TnkVDUZV-
XAVjuV3iEl9cqsKXtrAeWVuisRR2ehXf26DRTI-
usjy0e_7HADOGfC0RPKz1LZX0-
G0VCYQYBe0vpXym1UOgFhQMUB6fqGAiKE9_OMFmFOCHGNwF5OST1O
XG9KB9g0igSoy46E6P3Xzqg3WfxElI9n_rQ"
    }
  ]
}
```

6.14. Получение конфигурации OAuth 2.0 сервера

Имя ресурса: /.well-known/oauth-authorization-server

Метод: GET

6.14.1. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 123.

В ответе перечислены конечные точки, поддерживаемые гранты OAuth 2.0, методы аутентификации и криптографические алгоритмы.

Таблица 123 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
URL-адрес сервера	issuer	Строка	Да	URL-адрес эмитента (идентификатор сервера)
URL-адрес авторизации	authorization_endpoint	Строка	Да	URL-адрес для запроса авторизационного кода
URL-адрес получения токенов	token_endpoint	Строка	Да	URL-адрес для получения токенов доступа, обновления и т.д.
Поддерживаемые методы аутентификации	token_endpoint_auth_methods_supported	Массив	Нет	Список поддерживаемых методов аутентификации клиента для получения токенов
Поддерживаемые алгоритмы	token_endpoint_auth_signing_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов подписи для получения токенов
Поддерживаемые типы ответа	response_types_supported	Массив	Да	Список поддерживаемых типов ответа
URL-адрес получения наборов ключей	jwks_uri	Строка	Нет	URL-адрес получения набора публичных ключей сервера

Параметр	Название параметра	Тип данных	Обязательность	Описание
URL-адрес получения информации о токене	introspection_endpoint	Строка	Нет	URL-адрес получения информации о токене
Поддерживаемые методы аутентификации	introspection_endpoint_auth_methods_supported	Массив	Нет	Список поддерживаемых методов аутентификации клиента для получения данных токена
Поддерживаемые алгоритмы	introspection_endpoint_auth_signing_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов подписи для получения информации о токене
URL-адрес для отзыва токена	revocation_endpoint	Строка	Нет	URL-адрес для отзыва токена
Поддерживаемые методы аутентификации	revocation_endpoint_auth_methods_supported	Массив	Нет	Список поддерживаемых методов аутентификации клиента для отзыва токена
Поддерживаемые алгоритмы	revocation_endpoint_auth_signing_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов подписи для отзыва токена
Поддерживаемые типы грантов	grant_types_supported	Массив	Нет	Список поддерживаемых типов грантов
Поддерживаемые режимы ответа	response_modes_supported	Массив	Нет	Поддерживаемые режимы ответа
URL-адрес регистрации клиента	registration_endpoint	Строка	Нет	URL-адрес регистрации клиента
Поддерживаемые значения области доступа	scopes_supported	Массив	Нет	Список поддерживаемых значений области доступа
URL-адрес авторизации устройства	device_authorization_endpoint	Строка	Нет	URL-адрес авторизации устройства
URL-адрес документации по сервису	service_documentation	Строка	Нет	URL-адрес документации по сервису

Параметр	Название параметра	Тип данных	Обязательность	Описание
Поддерживаемые локали пользовательского интерфейса	ui_locales_supported	Массив	Нет	Список поддерживаемых локалей пользовательского интерфейса
URL-адрес документа политики конфиденциальности	op_policy_uri	Строка	Нет	URL-адрес документа политики конфиденциальности
URL-адрес документа с условиями обслуживания	op_tos_uri	Строка	Нет	URL-адрес документа с условиями обслуживания
Поддерживаемые методы преобразования кода авторизации верификатором	code_challenge_methods_supported	Массив	Нет	Список поддерживаемых методов преобразования кода авторизации верификатором

6.14.2. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/.well-known/oauth-authorization-server
```

Ответ:

Content-Type: application/json

```
{
  "issuer": "http://localhost:8085",
  "authorization_endpoint":
"http://localhost:8085/authentication/api/v1/oauth2/authorize",
  "device_authorization_endpoint":
"http://localhost:8085/oauth2/device_authorization",
  "token_endpoint":
"http://localhost:8085/authentication/api/v1/oauth2/token",
  "token_endpoint_auth_methods_supported": [
    "client_secret_basic",
```

```
        "client_secret_post",
        "client_secret_jwt",
        "private_key_jwt"
    ],
    "jwks_uri":
"http://localhost:8085/authentication/api/v1/oauth2/jwks",
    "response_types_supported": [
        "code"
    ],
    "grant_types_supported": [
        "authorization_code",
        "client_credentials",
        "refresh_token",
        "urn:iETF:params:oauth:grant-type:device_code"
    ],
    "revocation_endpoint":
"http://localhost:8085/authentication/api/v1/oauth2/revoke",
    "revocation_endpoint_auth_methods_supported": [
        "client_secret_basic",
        "client_secret_post",
        "client_secret_jwt",
        "private_key_jwt"
    ],
    "introspection_endpoint":
"http://localhost:8085/authentication/api/v1/oauth2/token-info",
    "introspection_endpoint_auth_methods_supported": [
        "client_secret_basic",
        "client_secret_post",
        "client_secret_jwt",
        "private_key_jwt"
    ],
    "code_challenge_methods_supported": [
        "S256"
    ]
}
```

6.15. Получение конфигурации OpenId Connect 1.0

Имя ресурса: /.well-known/openid-configuration

Метод: GET

6.15.1. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 124.

В ответе перечислены конечные точки, поддерживаемые гранты, методы аутентификации и криптографические алгоритмы OpenId Connect 1.0 сервера.

Таблица 124 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
URL-адрес сервера	issuer	Строка	Да	URL-адрес эмитента (идентификатор сервера)
URL-адрес авторизации	authorization_endpoint	Строка	Да	URL-адрес для запроса авторизационного кода
URL-адрес получения токенов	token_endpoint	Строка	Да	URL-адрес для получения токенов доступа, обновления и т.д.
Поддерживаемые методы аутентификации	token_endpoint_auth_methods_supported	Массив	Нет	Список поддерживаемых методов аутентификации клиента для получения токенов
Поддерживаемые алгоритмы	token_endpoint_auth_signing_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов подписи для получения токенов
Поддерживаемые типы ответа	response_types_supported	Массив	Да	Список поддерживаемых типов ответа
URL-адрес получения наборов ключей	jwks_uri	Строка	Нет	URL-адрес получения набора публичных ключей сервера

Параметр	Название параметра	Тип данных	Обязательность	Описание
URL-адрес OpenID Connect получения данных пользователя	userinfo_endpoint	Строка	Да	URL-адрес OpenID Connect получения данных пользователя
URL-адрес для выхода	end_session_endpoint	Строка	Нет	URL-адрес для выхода из OpenID Connect
Поддерживаемые ссылки на классы	acr_values_supported	Массив	Нет	Список поддерживаемых ссылок на классы контекста аутентификации
Поддерживаемые типы идентификаторов	subject_types_supported	Массив	Нет	Список поддерживаемых типов идентификаторов субъекта (конечного пользователя)
Поддерживаемые алгоритмы JWS	id_token_signing_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов JWS для защиты выпущенных идентификационных токенов
Поддерживаемые алгоритмы JWE	id_token_encryption_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов JWE для защиты выданных идентификационных токенов
Поддерживаемые методы шифрования	id_token_encryption_enc_values_supported	Массив	Нет	Список поддерживаемых методов шифрования JWE для защиты выданных идентификационных токенов
Поддерживаемые алгоритмы JWS	userinfo_signing_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов JWS для защиты утверждений, возвращаемых при получении данных пользователя

Параметр	Название параметра	Тип данных	Обязательность	Описание
Поддерживаемые алгоритмы JWE	userinfo_encryption_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов шифрования JWE для защиты утверждений, возвращаемых при получении данных пользователя
Поддерживаемые методы шифрования	userinfo_encryption_enc_values_supported	Массив	Нет	Список поддерживаемых методов шифрования JWE для защиты утверждений, возвращаемых при получении данных пользователя
Поддерживаемые алгоритмы JWS	request_object_signing_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов JWS для запросов авторизации
Поддерживаемые алгоритмы JWE	request_object_encryption_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов шифрования JWE для запросов авторизации
Поддерживаемые методы шифрования	request_object_encryption_enc_values_supported	Массив	Нет	Список поддерживаемых методов шифрования JWE для запросов авторизации
Параметры отображения	display_values_supported	Массив	Нет	Список поддерживаемых параметров отображения
Типы утверждений	claim_types_supported	Массив	Нет	Список поддерживаемых типов утверждений OpenID Connect
Утверждения	claims_supported	Массив	Нет	Список поддерживаемых утверждений OpenID Connect

Параметр	Название параметра	Тип данных	Обязательность	Описание
Поддерживаемые локали утверждений	claims_locales_supported	Массив	Нет	Список поддерживаемых локалей утверждений OpenID Connect
Признак поддержки параметра запроса аутентификации	claims_parameter_supported	Логический	Нет	Значение «true» – если есть поддержка параметра запроса аутентификации OpenID для утверждений, значение «false» – если нет поддержки параметра запроса аутентификации OpenID для утверждений
Признак поддержки параметра запроса авторизации	request_parameter_supported	Логический	Нет	Значение «true» – если есть поддержка параметра запроса авторизации, значение «false» – если нет поддержки параметра запроса авторизации
Признак поддержки параметра запроса авторизации request_uri	request_uri_parameter_supported	Логический	Нет	Значение «true» – если есть поддержка параметра запроса авторизации request_uri, значение «false» – если нет поддержки параметра запроса авторизации request_uri
Признак необходимости регистрации request_uri для клиента	require_request_uri_registration	Логический	Нет	Значение «true» – если должны быть зарегистрированы request_uri для клиента, значение «false» – если не должны быть зарегистрированы request_uri для клиента. По умолчанию принимает значение «false»

Параметр	Название параметра	Тип данных	Обязательность	Описание
URL-адрес получения информации о токене	introspection_endpoint	Строка	Нет	URL-адрес получения информации о токене
Поддерживаемые методы аутентификации	introspection_endpoint_auth_methods_supported	Массив	Нет	Список поддерживаемых методов аутентификации клиента для получения данных токена
Поддерживаемые алгоритмы	introspection_endpoint_auth_signing_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов подписи для получения информации о токене
URL-адрес для отзыва токена	revocation_endpoint	Строка	Нет	URL-адрес для отзыва токена
Поддерживаемые методы аутентификации	revocation_endpoint_auth_methods_supported	Массив	Нет	Список поддерживаемых методов аутентификации клиента для отзыва токена
Поддерживаемые алгоритмы	revocation_endpoint_auth_signing_alg_values_supported	Массив	Нет	Список поддерживаемых алгоритмов подписи для отзыва токена
Поддерживаемые типы грантов	grant_types_supported	Массив	Нет	Список поддерживаемых типов грантов
Поддерживаемые режимы ответа	response_modes_supported	Массив	Нет	Поддерживаемые режимы ответа
URL-адрес регистрации клиента	registration_endpoint	Строка	Нет	URL-адрес регистрации клиента
Поддерживаемые значения области доступа	scopes_supported	Массив	Нет	Список поддерживаемых значений области доступа
URL-адрес авторизации устройства	device_authorization_endpoint	Строка	Нет	URL-адрес авторизации устройства
URL-адрес документации по сервису	service_documentation	Строка	Нет	URL-адрес документации по сервису

Параметр	Название параметра	Тип данных	Обязательность	Описание
Поддерживаемые локали пользовательского интерфейса	ui_locales_supported	Массив	Нет	Список поддерживаемых локалей пользовательского интерфейса
URL-адрес документа политики конфиденциальности	op_policy_uri	Строка	Нет	URL-адрес документа политики конфиденциальности
URL-адрес документа с условиями обслуживания	op_tos_uri	Строка	Нет	URL-адрес документа с условиями обслуживания
Поддерживаемые методы преобразования кода авторизации верификатором	code_challenge_methods_supported	Массив	Нет	Список поддерживаемых методов преобразования кода авторизации верификатором

6.15.2. Пример выполнения запроса

Запрос:

```
GET http://{{host}}/.well-known/openid-configuration
```

Ответ:

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

```
{
  "issuer": "http://localhost:8085",
  "authorization_endpoint":
"http://localhost:8085/authentication/api/v1/oauth2/autho
rize",
  "device_authorization_endpoint":
"http://localhost:8085/oauth2/device_authorization",
  "token_endpoint":
"http://localhost:8085/authentication/api/v1/oauth2/t
oken",
  "token_endpoint_auth_methods_supported": [
    "client_secret_basic",
    "client_secret_post",
```

```
    "client_secret_jwt",
    "private_key_jwt"
  ],
  "jwks_uri":
"http://localhost:8085/authentication/api/v1/oauth2/jwks",
  "userinfo_endpoint":
"http://localhost:8085/userinfo",
  "end_session_endpoint":
"http://localhost:8085/authentication/api/v1/oauth2/logout",
  "response_types_supported": [
    "code"
  ],
  "grant_types_supported": [
    "authorization_code",
    "client_credentials",
    "refresh_token",
    "urn:ietf:params:oauth:grant-type:device_code"
  ],
  "revocation_endpoint":
"http://localhost:8085/authentication/api/v1/oauth2/revoke",
  "revocation_endpoint_auth_methods_supported": [
    "client_secret_basic",
    "client_secret_post",
    "client_secret_jwt",
    "private_key_jwt"
  ],
  "introspection_endpoint":
"http://localhost:8085/authentication/api/v1/oauth2/token-info",
  "introspection_endpoint_auth_methods_supported": [
    "client_secret_basic",
    "client_secret_post",
    "client_secret_jwt",
    "private_key_jwt"
  ],
  "subject_types_supported": [
    "public"
```

```
[,
  "id_token_signing_alg_values_supported": [
    "RS256"
  ],
  "scopes_supported": [
    "openid",
    "email",
    "profile"
  ]
}
```

6.16. Получение данных УЗ аутентифицированного пользователя через OpenId Connect 1.0

Имя ресурса: /authentication/api/v1/oauth2/userinfo

Метод: GET

HTTP-заголовки:

- Content-Type: application/json
- Authorization: Bearer <Токен доступа>

6.16.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 125.

Таблица 125 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Заголовок HTTP-авторизации	Authorization	Строка	Да	Тип авторизации Bearer со значением токена доступа access_token

Для доступа к методу токен должен иметь область доступа (scope): openid.

6.16.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 126.

Таблица 126 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Идентификатор УЗ пользователя	sub	UUID	Да	Идентификатор УЗ пользователя	openid
Идентификатор УЗ пользователя	userId	UUID	Да	Идентификатор УЗ пользователя	openid
Идентификатор профиля УЗ пользователя	userId	UUID	Нет	Идентификатор профиля УЗ пользователя	openid
Адрес электронной почты	email	Строка	Да	Адрес электронной почты пользователя	openid, email
Признак верификации адреса электронной почты пользователя	email_verified	Логический	Да	Значение «true» – если адрес электронной почты пользователя верифицирован, значение «false» – если адрес электронной почты пользователя не верифицирован	openid, email
Псевдоним	nickname	Строка	Да	Псевдоним пользователя	openid, profile
Логин	preferred_username	Строка	Да	Логин пользователя	openid, profile

Параметр	Название параметра	Тип данных	Обязательность	Описание	Необходимые области доступа (scope) в токене доступа
Фамилия пользователя	family_name	Строка	Да	Фамилия пользователя	openid, profile
Имя пользователя	given_name	Строка	Да	Имя пользователя	openid, profile
Отчество пользователя	middle_name	Строка	Нет	Отчество пользователя	openid, profile
Дата рождения	birthdate	Строка	Нет	Дата рождения пользователя	openid, profile
Время последнего изменения данных пользователя	updated_at	Целое число	Нет	Время последнего изменения данных аутентифицированного пользователя в формате timestamp	openid, profile

6.16.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 127.

Таблица 127 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Тип ошибки	error	Строка	Да	Тип ошибки
Описание ошибки	error_description	Строка	Нет	Описание ошибки
Ссылка на описание ошибки	error_uri	Строка	Нет	Ссылка на документацию протокола OpenID Connect 1.0

6.16.4. Пример выполнения запроса

Запрос:

GET

```
http://{{host}}/authentication/api/v1/oauth2/userinfo
```

Content-Type: application/json

Authorization: Bearer

eyJraWQiOiIyYTQ4N2Q0OS0zMzA0LTRkNDYtYTA5My0wM2FmMGFmYjQyMWIiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJlMGJhYmE2My04NzMzLT04Y2UtODE2OC03

MGY0OGYwNzU4ZmEiLCJhdWQiOiJ0ZXN0LWNsaWVudCIsIm5iZiI6M
TcyODU2MDk0OCwic2NvcGUiOlsib3BlbmlkIiwidXNlciJdLCJpc3
MiOiJodHRwOi8vbG9jYWxob3N0OjgwODUuLCJ1c2V

yVXVpZCI6ImUwYmFiYTYzLTg3MzMtNDhjZS04MTY4LTcwZjQ4ZjA3
NThmYSIsImV4cCI6MTcyODU2MTI0OCwiaWF0IjoxNzI4NTYwOTQ4L
CJlc2VyUHJvZmlsZVV1aWQiOiI0YmIyY2UxOC1hZj

gzLTQ4YjQtYjBjNS0yNDY3NTY3NzM1YzMifQ.R4kvVSxbpjirPRBm
B ZBmk2nslaJdmR-

BU1xCM_TttCikRGVZ2pvsz8PTYK_tUk4gMYb9888n0EBFMlT_LzbH
q cKSUJWEZ-ZV-p3st6QRGqSt

lm98FMHjw2qERQPlvema8oPkxPCuqlxNpKtiP0yzDLLznUAqCSmXD
p8Qu1P6SP91I5AN8CrBTBBRXC44oBE2bWHemUYmIo7lUgV0Bnovq0
zLndFl7yLqRF65O0O2IxYjp2ui2qbhUXB5VjmHOV1

5f5V8CyKf3p80D0fU_gE0_RM5O3a7sDIsW9fK_UFdUZzSzjMa6MsZ
u27nh4yrozMPIwjyOLRjusWH6QR3NkoA

Ответ:

Content-Type: application/json

```
{
  "sub": "0052f40b-e12f-4fcb-ac23-988c2b4f539b",
  "userId": "0052f40b-e12f-4fcb-ac23-988c2b4f539b",
  "userProfileId": "1232f40b-e12f-4fcb-ac23-988c2b4f5321",
  "email": "user@domain.ru", //Для получения данных
  //токен должен иметь область доступа (scope): email
  "email_verified": true, //Для получения данных
  //токен должен иметь область доступа (scope): email
  "nickname": "user", //Для получения данных
  //токен должен иметь область доступа (scope): profile
  "preferred_username": "user", //Для получения
  //данных
  //токен должен иметь область доступа (scope): profile
  "family_name": "Иванов", //Для получения данных
  //токен должен иметь область доступа (scope): profile
  "given_name": "Иван", //Для получения данных
  //токен должен иметь область доступа (scope): profile
  "middle_name": "Иванович", //Для получения данных
  //токен должен иметь область доступа (scope): profile
  "birthdate": "2002-01-27" //Для получения данных
  //токен должен иметь область доступа (scope): profile
  "updated_at": "1764659107" //Для получения данных
  //токен должен иметь область доступа (scope): profile
}
```

Ошибка при истекшем токене:

HTTP/1.1 401

Content-Type: application/json

```
{
  "error": "invalid_token"
}
```

Ошибка при невалидном токене в части подписи:

HTTP/1.1 400

Content-Type: application/json

```
{
  "error_description": "OpenID Connect 1.0 UserInfo
Error: Last unit does not have enough valid bits",
  "error": "invalid_request",
  "error_uri": "https://openid.net/specs/openid-
connect-core-1_0.html#UserInfoError"
}
```

Ошибка при некорректных данных в токене:

HTTP/1.1 400

Content-Type: application/json

```
{
  "error_description": "OpenID Connect 1.0 UserInfo
Error: Can't parse access token:
eyJraWQiOiIxZjA0MzQ2My1lZTBhLTM0OW",
  "error": "invalid_request",
  "error_uri": "https://openid.net/specs/openid-
connect-core-1_0.html#UserInfoError"
}
```

6.17. Выход из системы OpenID Connect 1.0

Имя ресурса: /authentication/api/v1/oauth2/logout

Метод: GET или POST (поддерживаются оба метода)

6.17.1. Данные в запросе

Описание данных в запросе приведено в таблице 128.

Таблица 128 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Значение «IdToken»	id_token_hint	Строка	Да	Значение «IdToken»
Адрес для перенаправления пользователя	post_logout_redirect_uri	Строка	Нет	Адрес для перенаправления пользователя после успешного выхода из системы. Значение «post_logout_redirect_uri» должно быть зарегистрировано для OAuth 2.0-клиента

В случае использования OAuth 2.0-клиентом динамических значений `post_logout_redirect_uri` допускается применение шаблонов разрешённых адресов для перенаправления пользователя после выхода из системы с использованием «*» в регистрируемых для OAuth 2.0-клиента допустимых значениях `post_logout_redirect_uri`. При этом шаблон должен соответствовать формату URI, не допускается использовать шаблон в части схемы, например:

- `http://*test.test/*` – верное применение шаблона;
- `http*://test.test` – неверное применение шаблона.

Синтаксис написания шаблонов:

- `?` – соответствует одному любому символу;
- `*` – соответствует любому количеству символов (0 и более) в пределах одного сегмента (до разделителя `/`);
- `**` – соответствует любому количеству директорий/сегментов пути.

6.17.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 129.

Таблица 129 – Данные ошибки выполнения запроса

Параметр	Название параметра	Тип данных	Описание
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка
Код ответа	status	Целое число	Код ответа
Информация об ошибке	error	Строка	Информация об ошибке
Путь URL	path	Строка	Путь URL

6.17.3. Пример выполнения запроса

Запрос:

GET

http://{{host}}/authentication/api/v1/oauth2/logout?post_logout_redirect_uri=http://localhost/logout&id_token_hint=eyJraWQiOiIxZjA0MzQ2My1lZTBhLTU0OWItOWJjYi1hYmMxYzU3ODg5ODkiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIw

Ответ:

302 http://localhost/logout

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "timestamp": "2025-05-27T13:22:16.592+00:00",
  "status": 400,
  "error": "Bad Request",
  "path": "/authentication/api/v1/oauth2/logout"
}
```

6.17.4. Сценарии выхода пользователя из системы

Сценарии выхода пользователя из системы:

- 1) Выход из системы на стороне клиента.

Клиентское приложение может удалить сохраненные токены (id-токен, access-токен и refresh-токен) из браузера или памяти. Это действие аннулирует статус аутентификации пользователя на стороне клиента. Для веб-приложений, управляющих собственными сессиями входа пользователей, могут потребоваться дополнительные шаги очистки cookie и любых других данных сессии, чтобы гарантировать, что пользователь полностью вышел из системы. В данном сценарии выхода взаимодействие с OIDC-сервером не предусматривается.

Пример реализации локального выхода на стороне клиентского приложения:

```
function localLogout() {  
    // Удаление токенов из локального хранилища  
    localStorage.removeItem('access_token');  
    localStorage.removeItem('refresh_token');  
  
    // Перенаправление на страницу входа  
    window.location.href = '/login';  
}
```

Для запуска функции выхода добавьте кнопку или ссылку на страницу, чтобы вызвать функцию «localLogout»:

```
<button onclick="localLogout()">Выйти</button>
```

2) Выход из системы на стороне клиента или на стороне OIDC-сервера, инициированный клиентским приложением.

Для реализации такого сценария выхода клиентское приложение должно перенаправить пользователя на конечную точку завершения сессии OIDC-сервера для завершения сессии входа и очистки cookie сессии. В ссылке для перехода необходимо указать следующие параметры:

- id_token_hint – параметр, в значение которого необходимо подставить id-токен, выданный для текущей сессии входа (см. п. 6.5.2);
- post_logout_redirect_uri – ссылка на ресурс клиентского приложения, в который OIDC-серверу необходимо сделать перенаправление после успешного выхода.

Пример реализации:

```
function rpLogout() {
    const endSessionEndpoint = 'https://your-xidbox-
server.ru/signin/oauth-logout';

    // Запрос на выход с указанием токена
    const idToken = localStorage.getItem('id_token');

    if (idToken) {
        window.location.href =
`${endSessionEndpoint}?id_token_hint=${idToken}&post_
logout_redirect_uri=${encodeURIComponent('https://you
r-app.ru/login')}`;
    } else {
        // Если токен не найден, выполняем локальный
выход
        localLogout();
    }
}
```

Для запуска функции выхода добавьте кнопку или ссылку на страницу, чтобы вызвать функцию «rpLogout»:

```
<button onclick="rpLogout()">Выйти из системы
(RP)</button>
```

7. Обновление пароля

7.1. Обновление пароля

Имя ресурса: /authentication/api/v1/password/by/uuid

Метод: PUT

HTTP-заголовки:

– Content-Type: application/json

7.1.1. Данные в запросе

Описание данных в запросе приведено в таблице 130.

Таблица 130 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор пользователя	userId	UUID	Да	Идентификатор пользователя
Новый пароль	newPassword	Строка	Да	Новый пароль
Старый пароль	oldPassword	Строка	Да	Старый пароль

7.1.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 131.

Таблица 131 – 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

7.1.3. Пример выполнения запроса

Запрос:

PUT

`http://{{host}}/authentication/api/v1/password/by/uid`

`Content-Type: application/json`

```
{
  "userUuid": "0052f40b-e12f-4fcb-ac23-988c2b4f539b",
  "newPassword": "new_password",
  "oldPassword": "old_password"
}
```

Ошибка выполнения запроса:

`Content-Type: application/json`

```
{
  "type": "MESSAGE",
  "payload": "Пароль слишком простой, не соответствует требованиям сложности пароля",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

7.2. Обновление пароля по токenu

Имя ресурса: `/authentication/api/v1/auth/password/by/token`

Метод: PUT

HTTP-заголовки:

– `Content-Type: application/json`

7.2.1. Данные в запросе

Описание данных в запросе приведено в таблице 132.

Таблица 132 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Токен для сброса пароля	token	UUID	Да	Токен для сброса пароля
Пароль	password	Строка	Да	Пароль

7.2.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 133.

Таблица 133 – 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

7.2.3. Пример выполнения запроса

Запрос:

PUT

`http://{{host}}/authentication/api/v1/auth/password/by/token`

Content-Type: application/json

```
{
  "token": "b7305534-1211-48b0-b614-a685cacd438c",
  "password": "1qaz@WSX"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Срок действия ссылки истек или ссылка
некорректна. Попробуйте снова.",
  "timestamp": "2022-04-14T08:31:58.423559Z"
}
```

7.3. Сброс пароля неаутентифицированным пользователем

Имя ресурса: /authentication/api/v1/auth/password/reset/via/order/anonymous

Метод: POST

HTTP-заголовки:

– Content-Type: application/json

7.3.1. Данные в запросе

Описание данных в запросе приведено в таблице 134.

Таблица 134 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Логин	login	Строка	Да	Логин пользователя

7.3.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 135.

Таблица 135 – 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

7.3.3. Пример выполнения запроса

Запрос:

POST

```
http://{{host}}/authentication/api/v1/auth/password/reset/via/order/anonymous
Content-Type: application/json
{
  "login": "max@infoxec.ru"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "VALIDATION",
  "payload": {
    "fields": [
      {
        "fieldName": "login",
        "errors": "Некорректный логин. Допустимы только латинские буквы, цифры, точка, «_», «-» и «@»"
      }
    ]
  },
  "timestamp": "2024-10-02T16:23:12.585210158Z"
}
```

7.4. Установка нового пароля пользователю

Имя ресурса: /authentication/api/v1/password/by/uuid

Метод: POST

HTTP-заголовки:

– Content-Type: application/json

7.4.1. Данные в запросе

Описание данных в запросе приведено в таблице 136.

Таблица 136 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор пользователя	userId	UUID	Да	Идентификатор пользователя
Пароль	password	Строка	Да	Пароль

7.4.2. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 137.

Таблица 137 – 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

7.4.3. Пример выполнения запроса

Запрос:

```
POST
http://{{host}}/authentication/api/v1/password/by/uid
Content-Type: application/json
{
  "userId": "0052f40b-e12f-4fcb-ac23-988c2b4f539b",
  "password": "new_password"
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{  
  "type": "MESSAGE",  
  "payload": "Пароль слишком простой, не  
соответствует требованиям сложности пароля",  
  "timestamp": "2022-04-14T08:31:58.423559Z"  
}
```

8. Обновление сессии пользователя

8.1. Установка профиля УЗ пользователя для текущей сессии

Имя ресурса: /authentication/api/v1/auth/user

Метод: PUT

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>
- Cookie: JSESSION=<Сессия пользователя, находящегося в процессе аутентификации>

8.1.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 138.

Описание данных в запросе приведено в таблице 139.

Таблица 138 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет, если передаётся Cookie: JSESSION	Сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Cookie: JSESSION	Строка	Нет, если передаётся Cookie: XIDBOXSession	Сессия пользователя, находящегося в процессе аутентификации

Должно передаваться одно из значений «Cookie: XIDBOXSession» или «Cookie: JSESSION».

Таблица 139 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя, под которым продолжит работать пользователь

8.1.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 140. В ответе на запрос возвращаются HTTP-заголовки, приведенные в таблице 141.

Таблица 140 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор	uuid	UUID	Да	Идентификатор пользователя
Признак верификации адреса электронной почты пользователя	isEmailVerified	Логический	Да	Значение «true» – если адрес электронной почты пользователя верифицирован, значение «false» – если адрес электронной почты пользователя не верифицирован
Адрес электронной почты профиля УЗ пользователя	userProfileWorkEmail	Строка	Нет	Адрес электронной почты профиля УЗ пользователя
Адрес электронной почты пользователя	email	Строка	Нет	Адрес электронной почты пользователя

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак принятия пользователем согласия на обработку ПДн	needToAcceptPrivacyPolicy	Логический	Да	Значение «true» – если политика конфиденциальности не принята, значение «false» – если политика конфиденциальности принята
Признак отображения уведомления о мерах защиты	needToShowSecurityPolicy	Логический	Да	Значение «true» – если уведомление о мерах защиты включено, значение «false» – если уведомление о мерах защиты отключено
Признак отображения уведомления об отправке ссылки на подтверждение адреса электронной почты профиля УЗ пользователя	needToShowSendProfileEmailValidation	Логический	Да	Значение «true» – если отображение уведомления включено (если профиль УЗ пользователя не подтвержден, и настройки системы подразумевают отображение данного уведомления), значение «false» – если отображение уведомления отключено
Пройденные способы аутентификации	authTypes	Массив	Да	Список пройденных способов аутентификации. Возможные значения: – LOGIN – логин и пароль; – CERT – сертификат; – KERBEROS_TICKET – доменная учётная запись с использованием протокола Kerberos; – CODE_FROM_EMAIL – подтверждение входа по коду, полученному на адрес электронной почты УЗ пользователя; – ESIA – Госуслуги (ЕСИА)

Параметр	Название параметра	Тип данных	Обязательность	Описание
Разрешённые хосты с учётом первого фактора аутентификации	availableHostsByFirstFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом первого фактора аутентификации
Разрешённые хосты с учётом второго фактора аутентификации	availableHostsBySecondFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом второго фактора аутентификации
Список именованных атрибутов УЗ/профиля УЗ/организации пользователя	customUserProfileAttributes	Объект	Да	Список пар ключ/значение именованных атрибутов УЗ/профиля УЗ/организации пользователя. Используется для обогащения информации об аутентифицированном профиле УЗ пользователя
Время предыдущего успешного входа	previousSuccessfulLoginTime	Дата и время	Нет	Дата и время предыдущего успешного входа
Количество неудачных попыток входа	numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin	Целое число	Нет	Количество неудачных попыток входа
Время предыдущей неудачной попытки входа	previousFailedLoginTime	Дата и время	Нет	Дата и время предыдущей неудачной попытки входа

Таблица 141 – Данные в HTTP-заголовке ответа на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Обновленная сессия аутентифицированного пользователя	Set-cookie: XIDBOXSession	Строка	Да	Новая сессия аутентифицированного пользователя

Параметр	Название параметра	Тип данных	Обязательность	Описание
Информация о сроке действия сессии	Set-cookie: XIDBOXSessionTTL	Строка	Да	Информация о сроке действия сессии. Значение в формате json, закодированное в base64 с полями: – jwtIssuedAt – значение обновления JWT в формате timestamp; – sessionTTL – срок действия JWT в секундах. Например, значение: XIDBOXSessionTTL=eyJqd3RJc3N1ZWRBdCI6MTc2OTYwNDMwMCwic2Vzc2lvb1RUTCI6MTgwMH0=; содержимое: <pre>{ "jwtIssuedAt":1769604300, "sessionTTL":1800 }</pre> Параметр доступен для клиентских скриптов (HttpOnly: false) и может использоваться в реализации фронтенд-логики приложений

8.1.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 142.

Таблица 142 – 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

8.1.4. Пример выполнения запроса

Запрос:

PUT

http://{host}}/authentication/api/v1/auth/user?userProfileUuid=0152f40b-e12f-4fcb-ac23-988c2b4f539b

Content-Type: application/json

Cookie: XIDBOXSession=

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWZzM2M3YmYiLCJyZWZyZXNoVFRMI

jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LT

A5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudWl1ZXJPZlVuc3VjY2V

zc2Z1bEF0dGVtcHRzU2luY2VQcmV2aW91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc21vbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1N1Y3VyaXR5UG9saWN5IjpmY

WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQio

nRydWUsInNlc3Npb25UVEwiOjAsImhhdCI6MTcyNTU0NjAzNH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-lNOUaiO-JwicDi_labpTSacURDtfvFWZ

QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMEL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm

yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_f4VPFw2fSJ6rtIR6PtKfjCqu7eU0AjRRNZ5gxxsLP2vNnh_NVQr7U45EIGOd9j-W8A

Ответ:

Set-Cookie:

XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9;

Domain=localhost; Path=/; HttpOnly

Set-Cookie:

XIDBOXSessionTTL=eyJqd3RJc3NlZW50dCI6MTc2OTYwNDMwMCwi
c2Vzc2lvdmlRUTCI6MTgwMH0=; Domain=localhost; Path=/

Content-Type: application/json

```
{
  "uuid": "0c54fdc5-4b00-4d3e-a521-2560d6d463d6",
  "userProfileUuid": "97149d84-90d1-49ff-ad63-  
f558cfef704d",
  "userProfileWorkEmail": "work_email@example.com",
  "email": "user_email@example.com",
  "isEmailVerified": true,
  "needToAcceptPrivacyPolicy": false,
  "needToShowSecurityPolicy": false,
  "needToShowSendProfileEmailValidation": false,
  "authTypes": [
    "ESIA"
  ],
  "availableHostsByFirstFactor": {
    "minitrue1984test": true,
    "xidbox.dcs.infosec.ru": true
  },
  "availableHostsBySecondFactor": {
    "xidbox.dcs.infosec.ru": true,
    "testhostlogin.ru": true
  },
  "customUserProfileAttributes": {
    "customParam": "value"
  },
  "previousSuccessfulLoginTime": "2024-10-  
03T12:21:16.221556Z",
  "numberOfUnsuccessfulAttemptsSincePrevious  
SuccessfulLogin": 0,
  "previousFailedLoginTime": null }
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type" : "MESSAGE",
  "payload" : "Профиль принадлежит другому
пользователю, повторите вход.",
  "timestamp" : "2022-08-25T13:03:59.653407Z"
}
```

Content-Type: application/json

```
{
  "type" : "MESSAGE",
  "payload" : "Профиль неактивный. Выберите другой
профиль.",
  "timestamp" : "2022-08-25T13:03:59.653407Z"
}
```

Content-Type: application/json

```
{
  "type" : "MESSAGE",
  "payload" : "Организация неактивна. Выберите другой
профиль.",
  "timestamp" : "2022-08-25T13:03:59.653407Z"
}
```

8.2. Обновление данных пользователя в текущей сессии

Имя ресурса: /authentication/api/v1/auth/user

Метод: PUT

HTTP-заголовки:

– Content-Type: application/json

– Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>

– Cookie: JSESSION=<Сессия пользователя, находящегося в процессе аутентификации>

8.2.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 143.

Таблица 143 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет, если передаётся Cookie: JSESSION	Сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Cookie: JSESSION	Строка	Нет, если передаётся Cookie: XIDBOXSession	Сессия пользователя, находящегося в процессе аутентификации

Должно передаваться одно из значений «Cookie: XIDBOXSession» или «Cookie: JSESSION».

8.2.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 144. В ответе на запрос возвращаются HTTP-заголовки, приведенные в таблице 145.

Таблица 144 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор	uuid	UUID	Да	Идентификатор пользователя
Идентификатор выбранного профиля УЗ пользователя	userProfileUuid	UUID	Нет	Идентификатор выбранного профиля УЗ пользователя, под которым идёт авторизация
Адрес электронной почты профиля УЗ пользователя	userProfileWorkEmail	Строка	Нет	Адрес электронной почты профиля УЗ пользователя

Параметр	Название параметра	Тип данных	Обязательность	Описание
Адрес электронной почты пользователя	email	Строка	Нет	Адрес электронной почты пользователя
Признак верификации адреса электронной почты пользователя	isEmailVerified	Логический	Да	Значение «true» – если адрес электронной почты пользователя верифицирован, значение «false» – если адрес электронной почты пользователя не верифицирован
Признак принятия пользователем согласия на обработку ПДн	needToAcceptPrivacyPolicy	Логический	Да	Значение «true» – если политика конфиденциальности не принята, значение «false» – если политика конфиденциальности принята
Признак отображения уведомления о мерах защиты	needToShowSecurityPolicy	Логический	Да	Значение «true» – если уведомление о мерах защиты включено, значение «false» – если уведомление о мерах защиты отключено
Признак отображения уведомления об отправке ссылки на подтверждение адреса электронной почты профиля УЗ пользователя	needToShowSendProfileEmailValidation	Логический	Да	Значение «true» – если отображение уведомления включено (если профиль УЗ пользователя не подтвержден, и настройки системы подразумевают отображение данного уведомления), значение «false» – если отображение уведомления отключено
Пройденные способы аутентификации	authTypes	Массив	Да	Список пройденных способов аутентификации. Возможные значения: – LOGIN – логин и пароль;

Параметр	Название параметра	Тип данных	Обязательность	Описание
				– CERT – сертификат; – KERBEROS_TICKET – доменная учётная запись с использованием протокола Kerberos; – CODE_FROM_EMAIL – подтверждение входа по коду, полученному на адрес электронной почты УЗ пользователя; – ESIA – Госуслуги (ЕСИА)
Разрешённые хосты с учётом первого фактора аутентификации	availableHostsByFirstFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом первого фактора аутентификации
Разрешённые хосты с учётом второго фактора аутентификации	availableHostsBySecondFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом второго фактора аутентификации
Список именованных атрибутов УЗ/профиля УЗ/организации пользователя	customUserProfileAttributes	Объект	Да	Список пар ключ/значение именованных атрибутов УЗ/профиля УЗ/организации пользователя. Используется для обогащения информации об аутентифицированном профиле УЗ пользователя
Время предыдущего успешного входа	previousSuccessfulLoginTime	Дата и время	Нет	Дата и время предыдущего успешного входа
Количество неудачных попыток входа	numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin	Целое число	Нет	Количество неудачных попыток входа

Параметр	Название параметра	Тип данных	Обязательность	Описание
Время предыдущей неудачной попытки входа	previousFailedLoginTime	Дата и время	Нет	Дата и время предыдущей неудачной попытки входа

Таблица 145 – Данные в HTTP-заголовке ответа на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Обновленная сессия аутентифицированного пользователя	Set-cookie: XIDBOXSession	Строка	Да	Новая сессия аутентифицированного пользователя
Информация о сроке действия сессии	Set-cookie: XIDBOXSession TTL	Строка	Да	Информация о сроке действия сессии. Значение в формате .json, закодированное в base64 с полями: – jwtIssuedAt – значение обновления JWT в формате timestamp; – sessionTTL – срок действия JWT в секундах. Например, значение: XIDBOXSessionTTL=eYJqd3RJc3N1ZWRBdCI6MTc2OTYwNDMwMCwic2Vzc2lvd1RUTCi6MTgwMH0=; содержимое: <pre>{ "jwtIssuedAt":1769604300, "sessionTTL":1800 }</pre> Параметр доступен для клиентских скриптов (HttpOnly: false) и может использоваться в реализации фронтенд-логики приложений

8.2.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 146 или 147.

Таблица 146 – 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

Таблица 147 – Данные ошибки выполнения запроса, если сессия не передана в заголовке, не найдена или истекла

Параметр	Название параметра	Тип данных	Описание
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка
Код ответа	status	Целое число	Код ответа
Информация об ошибке	error	Строка	Информация об ошибке
Путь URL	path	Строка	Путь URL

8.2.4. Пример выполнения запроса

Запрос:

PUT http://{host}/authentication/api/v1/auth/user

Content-Type: application/json

Cookie:

XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZXNoVFRMIjowLCJwcmV2aW91c1N1Y2Nlc3NmWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudW1iZXJPZ1Vuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2a

W91c1N1Y2N1c3NmdWxMb2dpbiI6MCwic2Vzc2lvbklkIjoiMjYwOD
U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
vU2hvd1N1Y3VyaXR5UG9saWN5IjpmY
WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn
V1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU
4ZmEiLCJpc0VtYWlsVmVyaWZpZWQiO
nRydWUsInN1c3Npb25UVEwiOjAsImhhdCI6MTcyNTU0NjAzNH0.wX
Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-
lNOUaiO-JwicDi_labpTSacURDtfvFWZ
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7
U45EIGOd9j-W8A

Ответ:

Set-cookie: XIDBOXSession=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4
NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWZmM2M3YmYiLCJyZWZyZ
XNoVFRMI
jowLCJwcmV2aW91c1N1Y2N1c3NmdWxMb2dpblRpbWUiOiIyMDI0LT
A5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudWliZXJPZlVuc3VjY2V
zc2Z1bEF0dGVtcHRzU2luY2VQcmV2a
W91c1N1Y2N1c3NmdWxMb2dpbiI6MCwic2Vzc2lvbklkIjoiMjYwOD
U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
vU2hvd1N1Y3VyaXR5UG9saWN5IjpmY
WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn
V1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU
4ZmEiLCJpc0VtYWlsVmVyaWZpZWQiO
nRydWUsInN1c3Npb25UVEwiOjAsImhhdCI6MTcyNTU0NjAzNH0.wX
Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-
lNOUaiO-JwicDi_labpTSacURDtfvFWZ
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7
U45EIGOd9j-W8A

Set-Cookie:

```
XIDBOXSessionTTL=eyJqd3RJc3NlZWRBdCI6MTc2OTYwNDMwMCwi  
c2Vzc2lvb1RUTCi6MTgwMH0=; Domain=localhost; Path=/  
Content-Type: application/json
```

```
{  
  "uuid": "0c54fdc5-4b00-4d3e-a521-2560d6d463d6",  
  "userProfileUuid": "97149d84-90d1-49ff-ad63-  
f558cfef704d",  
  "userProfileWorkEmail": "work_email@example.com",  
  "email": "user_email@example.com",  
  "isEmailVerified": true,  
  "needToAcceptPrivacyPolicy": false,  
  "needToShowSecurityPolicy": false,  
  "needToShowSendProfileEmailValidation": false,  
  "authTypes": [  
    "ESIA"  
  ],  
  "availableHostsByFirstFactor": {  
    "minitrue1984test": true,  
    "xidbox.dcs.infosec.ru": true  
  },  
  "availableHostsBySecondFactor": {  
    "xidbox.dcs.infosec.ru": true,  
    "testhostlogin.ru": true  
  },  
  "customUserProfileAttributes": {  
    "customParam": "value"  
  },  
  "previousSuccessfulLoginTime": "2024-10-  
03T12:21:16.221556Z",  
  "numberOfUnsuccessfulAttemptsSincePrevious  
SuccessfulLogin": 0,  
  "previousFailedLoginTime": null  
}
```

Ошибка выполнения запроса:

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

```
{
  "type": "MESSAGE",
  "payload": "Пользователь не найден.",
  "timestamp": "2025-01-14T08:01:31.567836200Z"
}
```

Ошибка выполнения запроса, если сессия не передана в заголовке, не найдена или истекла:

Content-Type: application/json

```
{
  "timestamp": "2023-08-28T06:06:57.791+00:00"
  "status": 401,
  "error": "Unauthorized",
  "path": "/authentication/api/v1/auth/user"
}
```

8.3. Установка признака отображения уведомления о мерах защиты информации для текущего пользователя

Имя ресурса: /authentication/api/v1/auth/user/security-policy-accepted

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>
- Cookie: JSESSION=<Сессия пользователя, находящегося в процессе аутентификации>

8.3.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 148.

Таблица 148 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет, если передаётся Cookie: JSESSION	Сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Cookie: JSESSION	Строка	Нет, если передаётся Cookie: XIDBOXSession	Сессия пользователя, находящегося в процессе аутентификации

Должно передаваться одно из значений «Cookie: XIDBOXSession» или «Cookie: JSESSION».

8.3.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 149.

Таблица 149 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор	uuid	UUID	Да	Идентификатор пользователя
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя
Адрес электронной почты профиля УЗ пользователя	userProfileWorkEmail	Строка	Нет	Адрес электронной почты профиля УЗ пользователя
Адрес электронной почты пользователя	email	Строка	Нет	Адрес электронной почты пользователя

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак верификации адреса электронной почты пользователя	isEmailVerified	Логический	Да	Значение «true» – если адрес электронной почты пользователя верифицирован, значение «false» – если адрес электронной почты пользователя не верифицирован
Признак принятия пользователем согласия на обработку ПДн	needToAcceptPrivacyPolicy	Логический	Да	Значение «true» – если политика конфиденциальности не принята, значение «false» – если политика конфиденциальности принята
Признак отображения уведомления о мерах защиты информации	needToShowSecurityPolicy	Логический	Да	Значение «true» – если уведомление о мерах защиты включено, значение «false» – если уведомление о мерах защиты отключено
Признак отображения уведомления об отправке ссылки на подтверждение адреса электронной почты профиля УЗ пользователя	needToShowSendProfileEmailValidation	Логический	Да	Значение «true» – если отображение уведомления включено (если профиль УЗ пользователя не подтвержден, и настройки системы подразумевают отображение данного уведомления), значение «false» – если отображение уведомления отключено

Параметр	Название параметра	Тип данных	Обязательность	Описание
Пройденные способы аутентификации	authTypes	Массив	Да	Список пройденных способов аутентификации. Возможные значения: – LOGIN – логин и пароль; – CERT – сертификат; – KERBEROS_TICKET – доменная учётная запись с использованием протокола Kerberos; – CODE_FROM_EMAIL – подтверждение входа по коду, полученному на адрес электронной почты УЗ пользователя; – ESIA – Госуслуги (ЕСИА)
Разрешённые хосты с учётом первого фактора аутентификации	availableHostsBy FirstFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом первого фактора аутентификации
Разрешённые хосты с учётом второго фактора аутентификации	availableHostsBy SecondFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом второго фактора аутентификации
Список именованных атрибутов УЗ/профиля УЗ/организации пользователя	customUserProfileAttributes	Объект	Да	Список пар ключ/значение именованных атрибутов УЗ/профиля УЗ/организации пользователя. Используется для обогащения информации об аутентифицированном профиле УЗ пользователя
Время предыдущего успешного входа	previousSuccessfulLoginTime	Дата и время	Нет	Дата и время предыдущего успешного входа

Параметр	Название параметра	Тип данных	Обязательность	Описание
Количество неудачных попыток входа	numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin	Целое число	Нет	Количество неудачных попыток входа
Время предыдущей неудачной попытки входа	previousFailedLoginTime	Дата и время	Нет	Дата и время предыдущей неудачной попытки входа

8.3.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 150 или 151.

Таблица 150 – 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

Таблица 151 – Данные ошибки выполнения запроса, если сессия не передана в заголовке, не найдена или истекла

Параметр	Название параметра	Тип данных	Описание
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка
Код ответа	status	Целое число	Код ответа
Информация об ошибке	error	Строка	Информация об ошибке
Путь URL	path	Строка	Путь URL

8.3.4. Пример выполнения запроса

Запрос:

POST

`http://{{host}}/authentication/api/v1/auth/user/security-policy-accepted`

`Content-Type: application/json`

`Cookie: XIDBOXSession=`

`eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZlNoVFRMI`

`jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudW1lZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2a`

`W91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lwbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1N1Y3VyaXR5UG9saWN5IjpmY`

`WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInVlaWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQio`

`nRydWUsInNlc3Npb25UVEwiOjAsImIhdCI6MTcyNTU0NjAzNH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-lNOUaiO-JwicDi_labpTSacURDtfvFWZ`

`QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAnaKxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-`

`1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm`

`yOL_PSFpKVT8Gl2VM64WQYD7AfBh_z7SFLuF2KBk6IggqNt_9FP1G_f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZ5gxxsLP2vNnh_NVQr7U45EIGOd9j-W8A`

Ответ:

`Content-Type: application/json`

```
{
  "uuid": "0c54fdc5-4b00-4d3e-a521-2560d6d463d6",
  "userProfileUuid": "97149d84-90d1-49ff-ad63-f558cfef704d",
  "userProfileWorkEmail": "work_email@example.com",
  "email": "user_email@example.com",
```

```
"isEmailVerified": true,
"needToAcceptPrivacyPolicy": true,
"needToShowSecurityPolicy": false,
"needToShowSendProfileEmailValidation": false,
"authTypes": [
  "ESIA"
],
"availableHostsByFirstFactor": {
  "minitrue1984test": true,
  "xidbox.dcs.infosec.ru": true
},
"availableHostsBySecondFactor": {
  "xidbox.dcs.infosec.ru": true,
  "testhostlogin.ru": true
},
"customUserProfileAttributes": {
  "customParam": "value"
},
"previousSuccessfulLoginTime": "2024-10-03T12:21:16.221556Z",
"numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin": 0,
"previousFailedLoginTime": null
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Пользователь не найден.",
  "timestamp": "2025-01-14T08:01:31.567836200Z"
}
```

Ошибка выполнения запроса, если сессия не передана в заголовке, не найдена или истекла:

Content-Type: application/json

```
{
  "timestamp": "2023-08-28T06:06:57.791+00:00"
  "status": 401,
  "error": "Unauthorized",
  "path": "/authentication/api/v1/auth/user/security-policy-accepted"
}
```

8.4. Установка признака согласия на обработку персональных данных для текущего пользователя

Имя ресурса: /authentication/api/v1/auth/user/privacy-policy-accepted

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>
- Cookie: JSESSION=<Сессия пользователя, находящегося в процессе аутентификации>

8.4.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 152.

Таблица 152 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Нет, если передаётся Cookie: JSESSION	Сессия аутентифицированного пользователя
Сессия пользователя, находящегося в процессе аутентификации	Cookie: JSESSION	Строка	Нет, если передаётся Cookie: XIDBOXSession	Сессия пользователя, находящегося в процессе аутентификации

Должно передаваться одно из значений «Cookie: XIDBOXSession» или «Cookie: JSESSION».

8.4.2. Данные в ответе на запрос

В случае успешного выполнения запроса возвращается ответ, структура которого приведена в таблице 153.

Таблица 153 – Данные в ответе на запрос

Параметр	Название параметра	Тип данных	Обязательность	Описание
Идентификатор	uuid	UUID	Да	Идентификатор пользователя
Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя
Адрес электронной почты профиля УЗ пользователя	userProfileWorkEmail	Строка	Нет	Адрес электронной почты профиля УЗ пользователя
Адрес электронной почты пользователя	email	Строка	Нет	Адрес электронной почты пользователя
Признак верификации адреса электронной почты пользователя	isEmailVerified	Логический	Да	Значение «true» – если адрес электронной почты пользователя верифицирован, значение «false» – если адрес электронной почты пользователя не верифицирован
Признак принятия пользователем согласия на обработку ПДн	needToAcceptPrivacyPolicy	Логический	Да	Значение «true» – если политика конфиденциальности не принята, значение «false» – если политика конфиденциальности принята

Параметр	Название параметра	Тип данных	Обязательность	Описание
Признак отображения уведомления о мерах защиты	needToShowSecurityPolicy	Логический	Да	Значение «true» – если уведомление о мерах защиты включено, значение «false» – если уведомление о мерах защиты отключено
Признак отображения уведомления об отправке ссылки на подтверждение адреса электронной почты профиля УЗ пользователя	needToShowSendProfileEmailValidation	Логический	Да	Значение «true» – если отображение уведомления включено (если профиль УЗ пользователя не подтвержден, и настройки системы подразумевают отображение данного уведомления), значение «false» – если отображение уведомления отключено
Пройденные способы аутентификации	authTypes	Массив	Да	Список пройденных способов аутентификации. Возможные значения: – LOGIN – логин и пароль; – CERT – сертификат; – KERBEROS_TICKET – доменная учётная запись с использованием протокола Kerberos; – CODE_FROM_EMAIL – подтверждение входа по коду, полученному на адрес электронной почты УЗ пользователя; – ESIA – Госуслуги (ЕСИА)
Разрешённые хосты с учётом первого фактора аутентификации	availableHostsByFirstFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом первого фактора аутентификации

Параметр	Название параметра	Тип данных	Обязательность	Описание
Разрешённые хосты с учётом второго фактора аутентификации	availableHostsBySecondFactor	Объект	Да	Список адресов разрешённых хостов информационных систем с учётом второго фактора аутентификации
Список именованных атрибутов УЗ/профиля УЗ/организации пользователя	customUserProfileAttributes	Объект	Да	Список пар ключ/значение именованных атрибутов УЗ/профиля УЗ/организации пользователя. Используется для обогащения информации об аутентифицированном профиле УЗ пользователя
Время предыдущего успешного входа	previousSuccessfulLoginTime	Дата и время	Нет	Дата и время предыдущего успешного входа
Количество неудачных попыток входа	numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin	Целое число	Нет	Количество неудачных попыток входа
Время предыдущей неудачной попытки входа	previousFailedLoginTime	Дата и время	Нет	Дата и время предыдущей неудачной попытки входа

8.4.3. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 154 или 155.

Таблица 154 – 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

Параметр	Название параметра	Тип данных	Описание
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка

Таблица 155 – Данные ошибки выполнения запроса, если сессия не передана в заголовке, не найдена или истекла

Параметр	Название параметра	Тип данных	Описание
Время ошибки	timestamp	Строка	Время, в которое была получена ошибка
Код ответа	status	Целое число	Код ответа
Информация об ошибке	error	Строка	Информация об ошибке
Путь URL	path	Строка	Путь URL

8.4.4. Пример выполнения запроса

Запрос:

POST

http://{host}}/authentication/api/v1/auth/user/privacy-policy-accepted

Content-Type: application/json

Cookie: XIDBOXSession=

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWZzM2M3YmYiLCJyZWZyZXNoVFRMI

jowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudWl1ZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2a

W91c1N1Y2Nlc3NmdWxMb2dpbiI6MCwic2Vzc2lvbklkIjoimjYwODU1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFRvU2hvd1N1Y3VyaXR5UG9saWN5IjpmY

WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsInV1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU4ZmEiLCJpc0VtYWlsVmVyaWZpZWQio

nRydWUsInNlc3Npb25UVEwiOjAsIm1hdCI6MTcyNTU0NjAzNH0.wXZu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-lNOUaiO-JwicDi_labpTSacURDtFvFWZ

```
QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IgqNt_9FP1G_
f4VPFw2fSJ6rtIR6PtkfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7
U45EIGOd9j-W8A
```

Ответ:

Content-Type: application/json

```
{
  "uuid": "0c54fdc5-4b00-4d3e-a521-2560d6d463d6",
  "userProfileUuid": "97149d84-90d1-49ff-ad63-
f558cfef704d",
  "userProfileWorkEmail": "work_email@example.com",
  "email": "user_email@example.com",
  "isEmailVerified": true,
  "needToAcceptPrivacyPolicy": false,
  "needToShowSecurityPolicy": false,
  "needToShowSendProfileEmailValidation": false,
  "authTypes": [
    "ESIA"
  ],
  "availableHostsByFirstFactor": {
    "minitrue1984test": true,
    "xidbox.dcs.infosec.ru": true
  },
  "availableHostsBySecondFactor": {
    "xidbox.dcs.infosec.ru": true,
    "testhostlogin.ru": true
  },
  "customUserProfileAttributes": {
    "customParam": "value"
  },
  "previousSuccessfulLoginTime": "2024-10-
03T12:21:16.221556Z",
  "numberOfUnsuccessfulAttemptsSincePrevious
SuccessfulLogin": 0,
  "previousFailedLoginTime": null
}
```

Ошибка выполнения запроса:

Content-Type: application/json

```
{
  "type": "MESSAGE",
  "payload": "Пользователь не найден.",
  "timestamp": "2025-01-14T08:01:31.567836200Z"
}
```

Ошибка выполнения запроса, если сессия не передана в заголовке, не найдена или истекла:

Content-Type: application/json

```
{
  "timestamp": "2023-08-28T06:06:57.791+00:00"
  "status": 401,
  "error": "Unauthorized",
  "path": "/authentication/api/v1/auth/user/privacy-policy-accepted"
}
```

9. Подтверждение адреса электронной почты

9.1. Отправка ссылки с токеном для подтверждения адреса электронной почты УЗ пользователя

Имя ресурса: /authentication/api/v1/tokens/verify-email/send-token-anonymous

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Cookie: JSESSION=<Сессия пользователя, находящегося в процессе аутентификации>

9.1.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 156.

Таблица 156 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия пользователя, находящегося в процессе аутентификации	Cookie: JSESSION	Строка	Да	Сессия пользователя, находящегося в процессе аутентификации

9.1.2. Пример выполнения запроса

Запрос:

POST

http://{host}/authentication/api/v1/tokens/verify-email/send-token-anonymous

Content-Type: application/json

Cookie: JSESSION=7cb88e28-f5cb-416f-8506-89c4dc2d5604

9.2. Подтверждение адреса электронной почты УЗ пользователя по токену

Имя ресурса: /authentication/api/v1/tokens/verify-email-anonymous

Метод: POST

HTTP-заголовки:

– Content-Type: application/json

9.2.1. Данные в запросе

Описание данных в запросе приведено в таблице 157.

Таблица 157 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Токен для подтверждения адреса электронной почты	token	UUID	Да	Токен для подтверждения адреса электронной почты УЗ пользователя

9.2.2. Пример выполнения запроса

Запрос:

POST

http://{{host}}/authentication/api/v1/tokens/verify-email-anonymous

Content-Type: application/json

```
{  
  
  "token" : "bdee807e-6a24-4842-b7dc-d30914661a79"  
  
}
```

9.3. Отправка ссылки с токеном для подтверждения адреса электронной почты профиля УЗ пользователя

Имя ресурса:	/authentication/api/v1/tokens/verify-user-profile-work-email/send-token
--------------	---

Метод: POST

HTTP-заголовки:

- Content-Type: application/json
- Cookie: XIDBOXSession=<Сессия аутентифицированного пользователя>

9.3.1. Данные в запросе

Описание данных в HTTP-заголовке запроса приведено в таблице 158.

Таблица 158 – Данные в HTTP-заголовке запроса

Параметр	Название параметра	Тип данных	Обязательность	Описание
Сессия аутентифицированного пользователя	Cookie: XIDBOXSession	Строка	Да	Сессия аутентифицированного пользователя

9.3.2. Пример выполнения запроса

Запрос:

POST

```
http://{{host}}/authentication/api/v1/tokens/verify-  
user-profile-work-email/send-token
```

Content-Type: application/json

Cookie:

XIDBOXSession=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyNjA4NTU5OC04NjI1LTQxMmYtODkxZS1jNTMzZWEzM2M3YmYiLCJyZWZyZXNoVFRMIjowLCJwcmV2aW91c1N1Y2Nlc3NmdWxMb2dpblRpbWUiOiIyMDI0LTA5LTA1VDE0OjE1OjAyLjY4MDgxM1oiLCJudW1iZXJPZlVuc3VjY2Vzc2Z1bEF0dGVtcHRzU2luY2VQcmV2a

W91c1N1Y2N1c3NmdWxMb2dpbiI6MCwic2Vzc2lrbklkIjoimjYwOD
 U1OTgtODYyNS00MTJmLTg5MWUtYzUzM2VhMzNjN2JmIiwibmVlZFR
 vU2hvd1N1Y3VyaXR5UG9saWN5IjpmY
 WxzZSwibmVlZFRvQWNjZXB0UHJpdmFjeVBvbGljeSI6ZmFsc2UsIn
 V1aWQiOiJlMGJhYmE2My04NzMzLTQ4Y2UtODE2OC03MGY0OGYwNzU
 4ZmEiLCJpc0VtYWlsVmVyaWZpZWQiO
 nRydWUsInN1c3Npb25UVEwiOjAsImhhdCI6MTcyNTU0NjAzNH0.wX
 Zu6hvvhXpNDaXUp70NZ7rqjaWzGQo8ze0hOOJHK8S5Pczg0aXn-
 lNOUaiO-JwicDi_labpTSacURDtfvFWZ
 QqkxgP9UZnZ2g6v0rFwjPDumSflIHx1zMeL5hTorrVMPzk4CPbAna
 KxdfvkSxmtM_8Ay3aKZQT3Lgt0nymCErA-
 1RdTr9HdX6Vu4hwLBjE-jjB7HynsZ3eQkNZM5n4hkrsjFG7mm
 yOL_PSFpKVT8G12VM64WQYD7AfBh_z7SFLuF2KBk6IggNt_9FP1G_
 f4VPFw2fSJ6rtIR6PtKfjCqu7eU0AjRRNZe5gxxsLP2vNnh_NVQr7
 U45EIGOd9j-W8A

9.4. Проверка актуальности токена

Имя ресурса: /authentication/api/v1/tokens/<Токен>/validate-anonymous

Метод: GET

HTTP-заголовки:

– Content-Type: application/json

9.4.1. Данные в запросе

Описание данных в запросе приведено в таблице 159.

Таблица 159 – Данные в запросе

Параметр	Название параметра	Тип данных	Обязательность	Описание
Токен	token	UUID	Да	Токен для проверки актуальности срока действия

9.4.1. Возможные ошибки

В случае возникновения ошибки при выполнении запроса возвращается ответ, структура которого приведена в таблице 160.

Таблица 160 – 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

9.4.2. Пример выполнения запроса

Запрос:

GET

`http://{{host}}/authentication/api/v1/tokens/bdee807e-6a24-4842-b7dc-d30914661a79/validate-anonymous`

`Content-Type: application/json`

Ошибка выполнения запроса:

`Content-Type: application/json`

```
{
  "type": "MESSAGE",
  "payload": "Срок действия ссылки истек или ссылка некорректна. Попробуйте снова.",
  "timestamp": "2026-03-12T06:34:44.952055922Z"
}
```

10. Сценарий аутентификации из приложения ИС

10.1. Создание пароля для новой УЗ пользователя

Создание пароля требуется только в случае невозможности аутентификации по сертификату или через Госуслуги (ЕСИА).

После регистрации пользователя на указанный при регистрации адрес электронной почты отправится письмо со ссылкой для подтверждения адреса электронной почты УЗ пользователя. Ссылка действительна в течение ограниченного времени.

Для того, чтобы создать пароль, отправьте запрос, указав в теле запроса токен из полученной ссылки и желаемый пароль (см. п. 7.2), и добавьте заголовки запроса, описанные ниже.

Пример выполнения запроса:

```
PUT
http://{{host}}/authentication/api/v1/auth/password/b
y/token
Content-Type: application/json
xidbox-ext-request: true
xidbox-request-timestamp: <Текущее время в формате
timestamp>
xidbox-request-algorithm: SHA256
xidbox-request-auth-id: xidbox
xidbox-request-signature: <Цифровая подпись,
созданная с помощью алгоритма SHA-256>

{
  "token": "<Токен для сброса пароля, полученный на
адрес электронной почты>",
  "password": "<Пароль>"
}
```

Пример ответа:

Пустое тело ответа – статус 200

10.2. Сброс пароля до аутентификации

При необходимости обновления пароля выполните следующие действия:

1) Выполните запрос на сброс пароля неаутентифицированным пользователем, указав в теле запроса логин УЗ пользователя (см. п. 7.3) и добавьте заголовки запроса, описанные ниже.

Пример выполнения запроса:

```
POST
http://{{host}}/authentication/api/v1/auth/password/reset/via/order/anonymous
Content-Type: application/json
xidbox-ext-request: true
xidbox-request-timestamp: <Текущее время в формате timestamp>
xidbox-request-algorithm: SHA256
xidbox-request-auth-id: xidbox
xidbox-request-signature: <Цифровая подпись, созданная с помощью алгоритма SHA-256>

{
  "login": "<Логин пользователя>"
}
```

Пример ответа:

Пустое тело ответа – статус 200

На указанный при регистрации пользователя адрес электронной почты отправится письмо со ссылкой для сброса пароля.

2) Для того, чтобы задать пароль, выполните запрос на создание нового пароля, указав в теле запроса токен из полученной ссылки и желаемый пароль (см. п. 7.2), а также добавьте заголовки запроса, описанные ниже.

Пример выполнения запроса:

```
PUT
http://{{host}}/authentication/api/v1/auth/password/b
y/token
Content-Type: application/json
xidbox-ext-request: true
xidbox-request-timestamp: <Текущее время в формате
timestamp>
xidbox-request-algorithm: SHA256
xidbox-request-auth-id: xidbox
xidbox-request-signature: <Цифровая подпись,
созданная с помощью алгоритма SHA-256>

{
  "token": "<Токен для сброса пароля>",
  "password": "<Пароль>"
}
```

Пример ответа:

Пустое тело ответа – статус 200

10.3. Аутентификация

После создания пароля для входа в систему выполните следующие действия:

1) Отправьте запрос на аутентификацию с помощью логина и пароля (см. п. 4.1) и добавьте заголовки запроса, описанные ниже.

Пример выполнения запроса:

```
POST
http://{{host}}/authentication/api/v1/auth/login
Content-Type: application/json
Origin: <Хост страницы аутентификации>
Cookie: Auth-Redirect=/
xidbox-ext-request: true
xidbox-request-timestamp: <Текущее время в формате
timestamp>
xidbox-request-algorithm: SHA256
```

```
xidbox-request-auth-id: xidbox
xidbox-request-signature: <Цифровая подпись,
созданная с помощью алгоритма SHA-256>
```

```
{
  "login": "<Логин пользователя>",
  "password": "<Пароль>"
}
```

Пример ответа:

```
Content-Type: application/json
Set-Cookie: JSESSION=<Сессия пользователя,
находящегося в процессе аутентификации>; Domain=<Хост
аутентификации, для которого устанавливаются Cookie>;
Path=/; HttpOnly=true; SameSite=Lax
```

```
{
  "location": "/"
}
```

Если в настройках аутентификации ИС предусмотрена двухфакторная аутентификация, выполните п. 2) и 3). Если двухфакторная аутентификация не предусмотрена, пропустите их.

2) Отправьте запрос получения кода для двухфакторной аутентификации с указанием Cookie: JSESSION, полученной в результате предыдущего запроса (см. п. 4.7) и добавьте заголовки запроса, описанные ниже.

Пример выполнения запроса:

```
POST
http://{{host}}/authentication/api/v1/auth/second-
factor/send-code
Content-Type: application/json
Cookie: JSESSION=<Сессия пользователя, находящегося в
процессе аутентификации>
xidbox-ext-request: true
xidbox-request-timestamp: <Текущее время в формате
timestamp>
```

```
xidbox-request-algorithm:SHA256
xidbox-request-auth-id: xidbox
xidbox-request-signature: <Цифровая подпись,
созданная с помощью алгоритма SHA-256>
```

Пример ответа:

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

```
{
  "remainingAttemptCount": 3,
  "need_to_input_two_factor_code": true,
  "counter": 60,
  "userMaskedEmail": "max@test.ru"
}
```

На указанный при регистрации пользователя адрес электронной почты отправится письмо с кодом для двухфакторной аутентификации.

3) Отправьте запрос на прохождение двухфакторной аутентификации, указав в HTTP-заголовке запроса Cookie: JSESSION, а в теле запроса код, полученный на адрес электронной почты (см. п. 4.3) и добавьте заголовки запроса, описанные ниже.

Пример выполнения запроса:

```
POST
http://{{host}}/authentication/api/v1/auth/second-
factor
Content-Type: application/json
Cookie: JSESSION=<Сессия пользователя, находящегося в
процессе аутентификации>; Auth-Redirect=<Страница
перенаправления после успешной аутентификации>
Origin: <Хост двухфакторной аутентификации>
xidbox-ext-request: true
xidbox-request-timestamp: <Текущее время в формате
timestamp>
xidbox-request-algorithm: SHA256
xidbox-request-auth-id: xidbox
```

```
xidbox-request-signature: <Цифровая подпись,  
созданная с помощью алгоритма SHA-256>
```

```
{  
  "code": "<Код для двухфакторной аутентификации>"  
}
```

Пример ответа:

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

```
{  
  "location": "<Страница перенаправления после успешной  
аутентификации>"  
}
```

10.4. Получение информации из сессии пользователя

Для того, чтобы получить список доступных для выбора профилей УЗ пользователя по сессии пользователя, отправьте соответствующий запрос (см. п. 2.3) и добавьте заголовки запроса, описанные ниже.

Пример выполнения запроса:

```
GET  
http://{{host}}/authentication/api/v1/auth/user-  
profiles/by/session  
Content-Type: application/json  
Cookie: JSESSION=<Сессия пользователя, находящегося в  
процессе аутентификации>  
xidbox-ext-request: true  
xidbox-request-timestamp: <Текущее время в формате  
timestamp>  
xidbox-request-algorithm: SHA256  
xidbox-request-auth-id: xidbox  
xidbox-request-signature: <Цифровая подпись,  
созданная с помощью алгоритма SHA-256>
```

Пример ответа:

Content-Type: application/json

```
{
  "items": [
    {
      "userProfileUuid": "4bb2ce18-af83-48b4-b0c5-
2467567735c3",
      "organizationUuid": "24cc75bf-59dd-4933-9ed1-
e4131816f489",
      "organizationShortName": "Первая Компания",
      "organizationInn": "111111111111",
      "organizationKpp": null,
      "organizationOgrn": "8082846544113",
      "organizationExternalIdentifiers": []
    }
  ]
}
```

10.5. Обновление сессии пользователя

Для того, чтобы установить профиль УЗ пользователя для текущей сессии, отправьте соответствующий запрос (см. п. 8.1) и добавьте заголовки запроса, описанные ниже.

Пример выполнения запроса:

```
PUT
http://{host}/authentication/api/v1/auth/user?userP
rofileUuid=<Идентификатор профиля УЗ пользователя>
Content-Type: application/json
Cookie: JSESSION=<Сессия пользователя, находящегося в
процессе аутентификации>
xidbox-ext-request: true
xidbox-request-timestamp: <Текущее время в формате
timestamp>
xidbox-request-algorithm: SHA256
xidbox-request-auth-id: xidbox
xidbox-request-signature: <Цифровая подпись,
созданная с помощью алгоритма SHA-256>
```

В HTTP-заголовке ответа XIDBOXSession возвращается JWT-токен. В качестве uuid профиля УЗ пользователя передаётся один из идентификаторов, возвращённый в ответе на запрос получения списка доступных для выбора профилей УЗ пользователя (см. п. 10.4).

Пример ответа:

Set-cookie: XIDBOXSession=<JWT-токен>

Content-Type: application/json

```
{
  "uuid": "0c54fdc5-4b00-4d3e-a521-2560d6d463d6",
  "userProfileUuid": "4bb2ce18-af83-48b4-b0c5-2467567735c3",
  "userProfileWorkEmail": "work-email@box.ru",
  "email": "email@box.ru",
  "isEmailVerified": true,
  "needToAcceptPrivacyPolicy": false,
  "needToShowSecurityPolicy": false,
  "authTypes": [
    "ESIA"
  ],
  "availableHostsByFirstFactor": {
    "minitrue1984test": true,
    "xidbox.dcs.infosec.ru": true
  },
  "availableHostsBySecondFactor": {
    "xidbox.dcs.infosec.ru": true,
    "testhostlogin.ru": true
  },
  "customUserProfileAttributes": {
    "customParam": "value"
  },
  "previousSuccessfulLoginTime": "2024-10-03T12:21:16.221556Z",
  "numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin": 0,
```

```
"previousFailedLoginTime": null
}
```

10.6. Обновление пароля после аутентификации

Для того, чтобы изменить пароль, отправьте запрос на обновление пароля, указав в теле запроса идентификатор пользователя, старый и новый пароль (см. п. 7.1) и добавьте заголовки запроса, описанные ниже.

Пример выполнения запроса:

```
PUT
http://{{host}}/authentication/api/v1/password/by/uid
Content-Type: application/json
xidbox-ext-request: true
xidbox-request-timestamp: <Текущее время в формате
timestamp>
xidbox-request-algorithm: SHA256
xidbox-request-auth-id: xidbox
xidbox-request-signature: <Цифровая подпись,
созданная с помощью алгоритма SHA-256>

{
  "userUuid": "<Идентификатор пользователя>",
  "newPassword": "<Новый пароль>",
  "oldPassword": "<Старый пароль>"
}
```

Пример ответа:

Пустое тело ответа – статус 200

10.7. Выход из системы

Для того, чтобы выйти из системы, отправьте соответствующий запрос (см. п. 5.1) и добавьте заголовки запроса, описанные ниже.

Пример выполнения запроса:

```
GET http://{{host}}/authentication/api/v1/auth/logout
Content-Type: application/json
Cookie: XIDBOXSession=<JWT-токен>
xidbox-ext-request: true
xidbox-request-timestamp: <Текущее время в формате
timestamp>
xidbox-request-algorithm: SHA256
xidbox-request-auth-id: xidbox
xidbox-request-signature: <Цифровая подпись,
созданная с помощью алгоритма SHA-256>
```

Пример ответа:

```
Content-Type: application/json

{
  "authTypes": [
    "ESIA",
    "LOGIN"
  ],
  "esiaLogoutUrl": <URL-адрес, по которому
перенаправляется пользователь после выхода из
системы>
}
```

Приложение А

Пример системы-клиента для аутентификации через X-IDBox

Пример системы-клиента (внешней информационной системы) для аутентификации через X-IDBox по OAuth2.0/ OpenID Connect 1.0 приведен в архиве Руководство_разработчика_часть_10_spring-boot-oauth2-client.zip.

А.1 Настройка

Описание настроек системы-клиента для аутентификации через X-IDBox по OAuth2.0/ OpenID Connect 1.0 приведено в файле Руководство_разработчика_часть_10_настройки_spring-boot-oauth2-client.txt.

А.2 Аутентификация

После запуска сервиса становится доступен интерфейс для аутентификации (по умолчанию порт – 80) с возможностью OAuth 2.0 входа:

4) Для входа выберите «xidbox» в списке способов входа через OAuth 2.0 (рис. 4).

Please sign in

Username

Password

Sign in

Login with OAuth 2.0

https://oauth-poib.mf.csd.infosec.ru	- клиент, использующий автоконфигурацию
xidbox	- клиент, настроенный "вручную" через проперти

Рисунок 4 – Вход через OAuth 2.0

Вход по логину и паролю не работает, так как добавлен для имитации возможности выбора способа аутентификации.

После выбора способа входа через OAuth 2.0 произойдет перенаправление на страницу аутентификации в X-IDBox.

5) Аутентифицируйтесь в X-IDBox любым доступным способом.

После успешной аутентификации в X-IDBox произойдет перенаправление обратно в систему-клиента.

Главная страница системы-клиента содержит основную информацию аутентифицированного пользователя (рис. 5).

[Главная](#)
[Данные текущего пользователя](#)
[Данные текущего профиля](#)
[Проверка перехода между страницами](#)
[Выйти](#)

Вы успешно аутентифицированы

PrincipalName: 0152f40b-e12f-4fcb-ac23-988c2b4f539b

ClientId: spring-client

[illegible]

Access token expires at: 2025-05-16T07:30:28.920231900Z

Refresh token: IvObxGf8GKNtW-UPLXHhVgmkzgJIEYotkUbc9PkvAM5dWu0YA8h0RSa3ThjxC4we1NXQGKqUgE2M wT75WO0vD0uEhPcUegpd9LNi2HGTslm2t0zyVUc5XV5nx8oHKt

Granted Authorities: [OAUTH2 USER, SCOPE organization, SCOPE organization-dynamic-fields, SCOPE user, SCOPE user-dynamic-fields, SCOPE user-profile, SCOPE user-profile-dynamic-fields]

Principal attributes: {uuid=0152f40b-e12f-4cb2-298b-264b59f5, isBlocked=false, state=ACTIVE, workEmail=testovichko@localhost.rurumio.6736130314251874, workEmailVerified=2024-07-12T08:15:59.536065Z, registrationDate=2022-05-30T11:33:22.051Z, organization=02c25eb5d5-6d16-44a5-9267-4d3a172c2b0a, fullName=ИП Цепен В., shortName=Сружия и сядена, typePosition=individual_entrepreneur, typeLabel=Индивидуален предприемател, inn=63718385092, kpp=nnl, ogrn=317402700060160, isBlocked=false, state=ACTIVE, address=street, registrationDate=2022-05-30, createDate=2022-07-25T11:03:46.690719Z}, techName={}

Рисунок 5 – Главная страница системы-клиента

Доступные страницы ИС:

- «Главная» – содержит основную информацию аутентифицированного пользователя.

– «Данные текущего пользователя» – при переходе на страницу выполняется запрос в X-IDBox с использованием ранее полученного токена доступа (Access token) для получения данных аутентифицированного пользователя.

- «Данные текущего профиля» – при переходе на страницу выполняется запрос в X-IDBox с использованием ранее полученного токена доступа (Access token) для получения данных аутентифицированного профиля УЗ пользователя.

- «Проверка перехода между страницами» – имитация перехода между страницами системы-клиента.

- «Выйти» – перенаправление пользователя для выхода из системы-клиента.

Если в процессе аутентификации в X-IDBox был запрошен `score openid` (указывается в настройках), то при выходе из ИС будет произведен выход и из X-IDBox.

Лист регистрации изменений

Версия	Изменения
1.0.0	Начальная версия
1.0.1	Добавлен параметр «needToShowSendProfileEmailValidation» в ответ на запрос методов обновления сессии пользователя
	Добавлен метод «Отправка ссылки с токеном для подтверждения адреса электронной почты профиля УЗ пользователя»
	Добавлено описание сценариев выхода из системы OpenID Connect 1.0
1.0.2	Добавлены методы «Получение набора публичных ключей OAuth 2.0 сервера», «Получение конфигурации OAuth 2.0 сервера», «Получение конфигурации OpenId Connect 1.0», «Получение данных УЗ аутентифицированного пользователя через OpenId Connect 1.0» и «Выход из системы OpenID Connect 1.0»
	Добавлена обязательная передача заголовка «Content-Type: application/x-www-form-urlencoded» в запросе методов получения, обновления и инвалидации OAuth 2.0 токенов доступа и метода получения информации о токене OAuth 2.0
	Добавлен пример возможной ошибки выполнения запроса в случае неизвестного или некорректного «client_id» для метода получения авторизационного кода OAuth 2.0
	Добавлено описание и пример системы-клиента для аутентификации через X-IDBox по OAuth2.0/ OpenID Connect 1.0
1.0.3	–
1.0.4	Уточнены возможные значения способов аутентификации для методов «Получение данных аутентифицированного пользователя из сессии», «Получение информации о пользователе по токену сессии пользователя», «Получение списка доступных способов аутентификации для первого фактора по имени хоста», «Установка профиля УЗ пользователя для текущей сессии», «Обновление данных пользователя в текущей сессии», «Установка признака отображения уведомления о мерах защиты информации для текущего пользователя», «Установка признака согласия на обработку персональных данных для текущего пользователя»
1.0.5	Параметр «email» стал не обязательным в описании методов «Получение данных УЗ пользователя с динамическими полями по токену OAuth 2.0» и «Получение данных УЗ аутентифицированного пользователя через OpenId Connect 1.0»
	Параметр «workEmail» стал не обязательным в описании метода «Получение данных профиля УЗ пользователя с динамическими полями профиля УЗ пользователя и организации по токену OAuth 2.0»
	Дополнены возможные значения области доступа (параметра «scope»)

Версия	Изменения
	Добавлено описание дополнительных областей доступа (параметра «score») для методов «Получение данных УЗ пользователя с динамическими полями по токену OAuth 2.0» и «Получение данных УЗ аутентифицированного пользователя через OpenId Connect 1.0»
	Изменена форма описания (объединено описание методов): – получения данных УЗ пользователя/УЗ пользователя с динамическими полями по токену OAuth 2.0 для метода «Получение данных УЗ пользователя с динамическими полями по токену OAuth 2.0»; – получения данных профиля УЗ пользователя/профиля УЗ пользователя с динамическими полями/профиля УЗ пользователя с динамическими полями организации/профиля УЗ пользователя с динамическими полями профиля УЗ пользователя и организации по токену OAuth 2.0 для метода «Получение данных профиля УЗ пользователя с динамическими полями профиля УЗ пользователя и организации по токену OAuth 2.0»
	В описание аутентификации и получения данных о пользователе по OAuth 2.0 добавлено примечание о поддерживаемом потоке выдачи токенов
1.1.0	Добавлены параметры «authTypes» и «esiaLogoutUrl» в ответ на запрос для метода «Выход из системы»
	Изменён параметр «validUntil» на параметр «counter» и добавлен параметр «userMaskedEmail» в ответе на запрос для метода «Запрос кода для двухфакторной аутентификации»
	Добавлено описание сценария аутентификации из приложения ИС
	Добавлены методы «Получение информации о предыдущем входе пользователя», «Получение настроек для страницы входа в ИС» и «Проверка актуальности токена»
	Добавлены параметры «userUuid», «userProfileUuid» и «updated_at» в ответ на запрос для метода «Получение данных УЗ аутентифицированного пользователя через OpenId Connect 1.0»
	Добавлено описание содержимого ID Token OpenId Connect 1.0
	Добавлено примечание к параметру «post_logout_redirect_uri» для метода «Выход из системы OpenID Connect 1.0»
	Добавлен HTTP-заголовок «Set-cookie: XIDBOXSessionTTL» в ответы на запрос для методов «Обновление сессии аутентифицированного пользователя», «Установка профиля УЗ пользователя для текущей сессии» и «Обновление данных пользователя в текущей сессии»
	Добавлены параметры «email» и «userProfileWorkEmail» в ответ на запрос для методов «Получение данных аутентифицированного пользователя из сессии», «Получение информации о пользователе по токену сессии пользователя», «Установка профиля УЗ пользователя для текущей сессии», «Обновление данных пользователя в текущей сессии», «Установка признака отображения уведомления о мерах защиты информации для текущего пользователя», и «Установка признака согласия на обработку персональных данных для текущего пользователя»

Версия	Изменения
	Добавлена возможная ошибка выполнения запроса, если закончились попытки второго и первого фактора, и включена настройка бессрочного блокирования для метода «Двухфакторная аутентификация»
	В описание аутентификации через Госуслуги (ЕСИА) добавлена схема взаимодействия с адаптером ЕСИА
	Добавлен параметр «alternativeHost» в ответ на запрос для метода «Получение списка доступных способов аутентификации для первого фактора по имени хоста»
	Добавлен параметр «sessionAttributes» в ответ на запрос для методов «Получение списка активных сессий профиля УЗ пользователя по сессии пользователя» и «Получение списка активных сессий по идентификатору профиля УЗ пользователя»