



**платформа аутентификации и управления
доступом**

Руководство администратора

Листов 152

Содержание

Содержание	2
Перечень сокращений	10
Перечень терминов.....	11
Перечень приложений.....	14
1. Общие сведения	15
1.1. Назначение и функции X-IDBox	15
1.2. Функциональные роли	16
1.3. Состав комплекта дистрибутивов ПО X-IDBox	17
2. Условия применения	20
2.1. Требования к серверной части	20
2.2. Требования к АРМ пользователя	20
2.3. Требования к необходимому уровню квалификации администратора и рекомендации по освоению системы.....	21
3. Указания по комплексной наладке	22
3.1. Перечень ресурсов, необходимых для проведения комплексной наладки.....	22
3.2. Условия, при соблюдении которых возможно проведение комплексной наладки.....	22
3.3. Перечень и последовательность работ по комплексной наладке	22
3.4. Требования к операционной системе «РЕД ОС»	22
3.5. Установка и настройка СУБД Postgres Pro Ent.....	23
3.6. Создание схем БД	23
3.6.1. Создание схем БД x_idbox_database.....	23
3.6.2. Создание схем БД x_id_box_scheduler	24
3.6.3. Создание схем БД storage	24
3.6.4. Создание схем БД state_machine_queue	24
3.6.5. Создание схем БД sm	24
3.7. Установка и настройка СУБД Redis	24
4. Подготовка конфигурационных файлов	25

4.1. Файл конфигурации и взаимодействия сервисов.....	25
4.2. Файлы конфигурации веб-сервера.....	25
4.3. Файлы конфигурации Модуля фильтрации запросов к ИС	25
4.4. Файл конфигурации ведения журналов	25
4.5. Файлы конфигурации Kerberos	25
5. Установка системы	27
5.1. Установка и настройка ППО «Сервис аутентификации».....	27
5.1.1. Предусловия.....	27
5.1.2. Установка	27
5.1.3. Настройка	27
5.2. Установка и настройка Модуля фильтрации запросов к ИС	38
5.2.1. Предусловия.....	38
5.2.2. Установка	38
5.3. Установка и настройка ППО «Сервис авторизации»	39
5.3.1. Предусловия.....	39
5.3.2. Установка	39
5.3.3. Настройка	39
5.4. Установка и настройка ППО «Сервис обработки данных»	39
5.4.1. Предусловия.....	39
5.4.2. Установка	40
5.4.3. Настройка	40
5.5. Установка и настройка ППО «Модуль отправки уведомлений информационным системам с использованием Kafka»	40
5.5.1. Предусловия.....	40
5.5.2. Установка	40
5.5.3. Настройка	41
5.6. Установка и настройка ППО «Модуль отправки уведомлений информационным системам с использованием RabbitMQ»	41
5.6.1. Предусловия.....	41
5.6.2. Установка	41

5.6.3. Настройка	41
5.7. Установка и настройка ППО «Модуль отправки уведомлений информационным системам с использованием REST»	42
5.7.1. Предусловия	42
5.7.2. Установка	42
5.7.3. Настройка	42
5.8. Установка и настройка ППО «Модуль подписания с использованием КриптоПро»	42
5.8.1. Предусловия	42
5.8.2. Установка	43
5.8.3. Настройка	43
5.9. Установка и настройка ППО «Сервис работы с основными БД»	43
5.9.1. Предусловия	43
5.9.2. Установка	43
5.9.3. Настройка	44
5.10. Установка и настройка ППО «Сервис синхронизации данных каталогов»	44
5.10.1. Предусловия	44
5.10.2. Установка	44
5.10.3. Настройка	44
5.11. Установка и настройка Модуля балансировки внутренних запросов	45
5.11.1. Предусловия	45
5.11.2. Установка	45
5.11.3. Настройка	45
5.12. Установка и настройка ППО «Сервис взаимодействия с пользовательским интерфейсом управления доступом»	45
5.12.1. Предусловия	45
5.12.2. Установка	46
5.12.3. Настройка	46

5.13. Установка и настройка ППО «Пользовательский интерфейс управления доступом»	46
5.13.1. Предусловия.....	46
5.13.2. Установка	46
5.14. Установка и настройка ППО «Сервис идентификации»	47
5.14.1. Предусловия.....	47
5.14.2. Установка	47
5.14.3. Настройка	47
5.15. Установка и настройка адаптера к ППО «Сервис интеграции с LDAP-каталогами»	47
5.15.1. Предусловия.....	47
5.15.2. Установка	48
5.15.3. Настройка	48
5.16. Установка и настройка ППО «Сервис обработки заявок»	51
5.16.1. Предусловия.....	51
5.16.2. Установка	51
5.16.3. Настройка	51
5.17. Установка и настройка ППО «Сервис организации выполнения заявок»	51
5.17.1. Предусловия.....	51
5.17.2. Установка	52
5.17.3. Настройка	52
5.18. Установка и настройка ППО «Сервис изменения заявок»	52
5.18.1. Предусловия.....	52
5.18.2. Установка	52
5.18.3. Настройка	52
5.19. Установка и настройка ППО «Сервис загрузки организаций»	53
5.19.1. Предусловия.....	53
5.19.2. Установка	53
5.19.3. Настройка	53
5.20. Установка и настройка ППО «Сервис загрузки ОШС».....	53

5.20.1. Предусловия.....	53
5.20.2. Установка	54
5.20.3. Настройка	54
5.21. Установка и настройка ППО «Сервис загрузки ролевых моделей»	54
5.21.1. Предусловия.....	54
5.21.2. Установка	54
5.21.3. Настройка	55
5.22. Установка и настройка ППО «Сервис автоматических операций»	55
5.22.1. Предусловия.....	55
5.22.2. Установка	55
5.22.3. Настройка	55
5.23. Установка и настройка ППО «Сервис обеспечения целостности данных».....	56
5.23.1. Предусловия.....	56
5.23.2. Установка	56
5.23.3. Настройка	56
5.24. Установка и настройка ППО «Пользовательский интерфейс аутентификации»	56
5.24.1. Предусловия.....	56
5.24.2. Установка	57
5.24.3. Настройка	57
5.25. Установка и настройка ППО «Сервис работы с данными заявок»	58
5.25.1. Предусловия.....	58
5.25.2. Установка	58
5.25.3. Настройка	58
5.26. Установка и настройка ППО «Сервис работы с очередью заявок»	59
5.26.1. Предусловия.....	59
5.26.2. Установка	59
5.26.3. Настройка	59

5.27. Установка и настройка ППО «Сервис работы с исходными данными заявок»	59
5.27.1. Предусловия.....	59
5.27.2. Установка	60
5.27.3. Настройка	60
5.28. Установка и настройка ППО «Сервис загрузки назначений»	60
5.28.1. Предусловия.....	60
5.28.2. Установка	60
5.28.3. Настройка	61
5.29. Установка и настройка ППО «Сервис регистрации и изменения данных пользователей»	61
5.29.1. Предусловия.....	61
5.29.2. Установка	61
5.29.3. Настройка	61
5.30. Установка и настройка ППО «Сервис валидации данных»	62
5.30.1. Предусловия.....	62
5.30.2. Установка	62
5.30.3. Настройка	62
5.31. Установка и настройка ППО «Сервис выполнения автоматических расчетов».....	62
5.31.1. Предусловия.....	62
5.31.2. Установка	63
5.31.3. Настройка	63
5.32. Установка и настройка веб-сервера Nginx.....	63
5.32.1. Предусловия.....	63
5.32.2. Установка Nginx	63
5.32.3. Настройка Nginx.....	64
5.33. Добавление ИС X-IDBox	64
6. Администрирование системы.....	67
6.1. Обновление системы	67

6.2. Настройка сетевого взаимодействия	67
6.3. Подключение информационной системы	67
6.3.1. Подключение ИС	67
6.3.2. Подключение ИС OAuth 2.0-клиента в X-IDBox	70
6.3.3. Загрузка ролей и защищаемых объектов ИС	75
6.3.4. Создание пользователя с ролью «Менеджер ИС»	75
6.3.5. Настройка отправки уведомлений	77
6.4. Настройка параметров запуска	80
6.5. Управление учётными записями пользователей и назначение пользователям прав доступа	80
6.6. Настройка событий безопасности, подлежащих регистрации, их состава и содержания	80
6.7. Настройка веб-серверов для работы с системой	82
6.8. Настройка рабочих станций пользователей для работы с системой	82
6.9. Настройка правил выборки подотчётных организаций	82
7. Обслуживание системы	84
7.1. Порядок обслуживания и проверка работоспособности системы	84
7.1.1. Управление СУБД Postgres Pro Ent.	84
7.1.2. Управление кеш-сервером Redis	84
7.1.3. Управление веб-сервером Nginx	84
7.1.4. Управление сервисами ППО X-IDBox	84
7.2. Проверка и анализ ключевых параметров функционирования системы и электронных журналов событий	86
7.3. Резервное копирование и восстановление данных	88
Приложение А Шаблон информационных потоков между ИС и X-IDBox	90
Приложение Б Описание настроек сервисов	91
Б.1 Индивидуальные настройки стенда	91
Б.2 Обязательные настройки	93
Б.3 Опциональные настройки	94
Б.4 Настройки сервиса xidbox-authentication	97

Б.5	Настройки сервиса xidbox-state-machine-queue	100
Б.6	Настройки сервиса xidbox-role-politics-upload.....	101
Б.7	Настройки сервиса xidbox-database	101
Б.8	Настройки сервиса xidbox-backend.....	102
Б.9	Настройки сервиса xidbox-frontbackend	102
Б.10	Настройки сервиса xidbox-scheduler	104
Б.11	Настройки сервиса xidbox-crypto	105
Б.12	Настройки сервиса xidbox-orchestrator	106
Б.13	Настройки сервиса xidbox-storage.....	107
Б.14	Настройки сервиса xidbox-order.....	107
Б.15	Настройки сервиса xidbox-state-machine-database	107
Б.16	Настройки сервиса xidbox-ldap	107
Б.17	Настройки сервиса xidbox-organizational-structure	108
Б.18	Настройки сервиса xidbox-signature.....	108
Б.19	Настройки сервиса xidbox-request-background-processing.....	109
Б.20	Настройки сервиса xidbox-callback-kafka.....	110
Б.21	Настройки, одинаковые для всех сервисов.....	110
Б.22	Настройки, одинаковые для всех клиентов сервисов	112
Приложение В Дополнительные данные о событиях безопасности.....		113
Лист регистрации изменений		152

Перечень сокращений

UTC	–	coordinated universal time (всемирное координированное время)
АРМ	–	автоматизированное рабочее место
БД	–	база данных
БПО	–	базисное программное обеспечение
ЕСИА	–	единая система идентификации и аутентификации
ЗО	–	защищаемый объект
ИБ	–	информационная безопасность
ИНН	–	идентификационный номер налогоплательщика
ИС	–	информационная система
ОЗУ	–	оперативное запоминающее устройство
ОС	–	операционная система
ОШС	–	организационно-штатная структура
ПО	–	программное обеспечение
ППО	–	прикладное программное обеспечение
СКЗИ	–	средство криптографической защиты информации
СУБД	–	система управления базами данных
УЗ	–	учётная запись
УЦ	–	удостоверяющий центр
ЦПУ	–	центральное процессорное устройство
ЭП	–	электронная подпись

Перечень терминов

Авторизация	– предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом
Атрибут	– признак или свойство субъекта доступа или объекта доступа
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 УЗ пользователя, профиля УЗ 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
Идентификация	– действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов
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
Парольная политика	– набор минимальных требований к характеристикам паролей, используемых пользователем для доступа к X-IDBox

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
Правила разграничения доступа	– правила, регламентирующие условия доступа субъектов доступа к объектам доступа в автоматизированной ИС
Профиль учётной записи пользователя	– набор значений атрибутов учётной записи X-IDBox, однозначно ассоциирующий субъект доступа с организацией, в интересах (от имени) которой субъектом доступа выполняются операции, реализованные в X-IDBox и ИС, интегрированных с X-IDBox
Ресурс	– защищаемый объект интегрированной ИС, который используется в политиках авторизации и относится к определенному типу ресурса
Роль	– предопределенная совокупность правил доступа к ресурсам (политик авторизации), устанавливающих допустимое взаимодействие между субъектами доступа и объектами доступа
Список разрешенных УЦ	– перечень УЦ, сертификаты, выданные которыми, могут быть использованы в X-IDBox
Субъект доступа	– пользователь и/или ИС, действия которого по доступу к объектам доступа регламентируются политиками авторизации
Удостоверяющий центр	– юридическое лицо, индивидуальный предприниматель или государственный орган, или орган местного самоуправления, осуществляющий функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ
Управление доступом	– ограничение и контроль доступа субъектов доступа к объектам доступа в ИС в соответствии с установленными правилами разграничения доступа

- 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
- Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

Перечень приложений

Название приложения	Имя файла
Шаблон требуемой информации для подключения ИС	Шаблон требуемой информации для подключения ИС.docx

1. Общие сведения

1.1. Назначение и функции X-IDBox

X-IDBox представляет собой систему идентификации, аутентификации и разграничения доступа, имеющую встроенный механизм управления доступом.

X-IDBox обеспечивает процедуру единого входа во все ИС, интегрированные с X-IDBox, что позволяет выполнять переход между ИС без повторной аутентификации. Для каждой ИС возможна настройка способов аутентификации.

X-IDBox предоставляет следующие функциональные возможности:

1) Управление УЗ пользователей (для всех ИС, интегрированных с X-IDBox, поддерживается единый каталог пользователей):

- регистрация пользователей, включая самостоятельную регистрацию пользователей;
- загрузка списка пользователей из файла;
- загрузка изменения ролей пользователей из файла;
- изменение личных данных пользователей;
- блокирование (в том числе и временное) и разблокирование УЗ пользователей;
- уведомление пользователей об операциях, связанных с действиями над учётными записями.

2) Управление профилями УЗ пользователей:

- добавление профилей к УЗ пользователей;
- загрузка профилей УЗ пользователей из файла;
- редактирование сведений о профилях УЗ пользователей;
- управление доступом к интегрированным ИС путем назначения и (или) снятия ролей;
- управление доступом к X-IDBox путем назначения и (или) снятия ролей;

- блокирование (в том числе и временное) и разблокирование профилей УЗ пользователей;

- уведомление пользователей об операциях, связанных с жизненным циклом заявок и управлением доступом.

3) Управление ролями:

- изменение параметров ролей, в том числе управление процессом согласования назначения роли;

- загрузка ролей доступа из файла;

- экспорт перечня ролей.

4) Обеспечение юридической значимости операций в системе путем подписания заявок, формируемых для каждого выполняемого действия в системе.

5) Просмотр списка организаций.

6) Управление списком разрешённых УЦ: добавление и удаление УЦ из списка.

7) Управление настройками безопасности и парольными политиками.

8) Управление шаблонами уведомлений: создание, изменение и удаление шаблонов.

1.2. Функциональные роли

В X-IDBox в соответствии с имеющимися зонами ответственности предусмотрены следующие функциональные роли:

- Пользователь;
- Системный администратор;
- Администратор ИБ;
- Менеджер информационной системы;
- Менеджер учётных записей.

Каждая УЗ пользователя наделена определёнными правами в соответствии со своей ролью, подробный перечень прав приведен в Руководстве пользователя.

Одному профилю УЗ пользователя может быть назначено несколько ролей в X-IDBox (обязательно включая роль Пользователя).

Роль Пользователя присваивается автоматически при регистрации профиля УЗ пользователя и не подлежит отзыву, а также изменению срока действия. Операции, доступные Пользователю, выполняются им только по отношению к своей собственной УЗ пользователя и профилям, связанным.

Назначать и отзывать роли в X-IDBox, а также изменять сроки их действия может только Системный администратор. Системный администратор может выполнять регистрацию пользователей, блокирование и разблокирование УЗ пользователей, управление профилями УЗ пользователей, шаблонами уведомлений.

Управление ролями в ИС, интегрированных с X-IDBox, доступно Менеджеру учётных записей. Также ему доступно управление УЗ пользователей и профилями УЗ пользователей.

Менеджер информационной системы может управлять только одной ИС. Все операции, доступные Менеджеру информационной системы, связаны именно с управляемой ИС.

Администратору ИБ доступно блокирование и разблокирование УЗ пользователей и профилей УЗ пользователей, управление списком разрешённых УЦ и настройками безопасности.

1.3. Состав комплекта дистрибутивов ПО X-IDBox

В таблице 1 приведен комплект дистрибутивов ПО X-IDBox.

Таблица 1 – Комплект дистрибутивов ПО X-IDBox

ПО	Дистрибутив
ППО «Сервис аутентификации»	xidbox-authentication-[version].[commit].x86_64.rpm
Модуль фильтрации запросов к ИС	xidbox-authn-gateway-[version].[commit].x86_64.rpm
ППО «Сервис авторизации»	xidbox-authorization-[version].[commit].x86_64.rpm
ППО «Сервис обработки данных»	xidbox-backend-[version].[commit].x86_64.rpm

ПО	Дистрибутив
ППО «Модуль отправки уведомлений информационным системам с использованием Kafka»	xidbox-callback-kafka-[version].[commit].x86_64.rpm
ППО «Модуль отправки уведомлений информационным системам с использованием RabbitMQ»	xidbox-callback-rabbit-[version].[commit].x86_64.rpm
ППО «Модуль отправки уведомлений информационным системам с использованием REST»	xidbox-callback-rest-[version].[commit].x86_64.rpm
ППО «Модуль подписания с использованием КриптоПро»	xidbox-crypto-[version].[commit].x86_64.rpm
ППО «Сервис работы с основными БД»	xidbox-database-[version].[commit].x86_64.rpm
ППО «Сервис синхронизации данных каталогов»	xidbox-directory-synchronization-[version].[commit].x86_64.rpm
Модуль балансировки внутренних запросов	xidbox-eureka-[version].[commit].x86_64.rpm
ППО «Сервис взаимодействия с пользовательским интерфейсом управления доступом»	xidbox-frontbackend-[version].[commit].x86_64.rpm
ППО «Пользовательский интерфейс управления доступом»	xidbox-frontend-[version].[commit].x86_64.rpm
ППО «Сервис идентификации»	xidbox-identification-[version].[commit].x86_64.rpm
ППО «Сервис интеграции с LDAP-каталогами»	xidbox-ldap-[version].[commit].x86_64.rpm
ППО «Сервис обработки заявок»	xidbox-orchestrator-[version].[commit].x86_64.rpm
ППО «Сервис организации выполнения заявок»	xidbox-orchestrator-helper-[version].[commit].x86_64.rpm
ППО «Сервис изменения заявок»	xidbox-order-[version].[commit].x86_64.rpm
ППО «Сервис загрузки организаций»	xidbox-organization-[version].[commit].x86_64.rpm
ППО «Сервис загрузки ОШС»	xidbox-organizational-structure-[version].[commit].x86_64.rpm
ППО «Сервис загрузки ролевых моделей»	xidbox-role-politics-upload-[version].[commit].x86_64.rpm
ППО «Сервис автоматических операций»	xidbox-scheduler-[version].[commit].x86_64.rpm

ПО	Дистрибутив
ППО «Сервис обеспечения целостности данных»	xidbox-signature-[version].[commit].x86_64.rpm
ППО «Пользовательский интерфейс аутентификации»	xidbox-signin-[version].[commit].x86_64.rpm
ППО «Сервис работы с данными заявок»	xidbox-state-machine-database-[version].[commit].x86_64.rpm
ППО «Сервис работы с очередью заявок»	xidbox-state-machine-queue-[version].[commit].x86_64.rpm
ППО «Сервис работы с исходными данными заявок»	xidbox-storage-[version].[commit].x86_64.rpm
ППО «Сервис загрузки назначений»	xidbox-user-profile-upload-[version].[commit].x86_64.rpm
ППО «Сервис регистрации и изменения данных пользователей»	xidbox-user-upload-[version].[commit].x86_64.rpm
ППО «Сервис валидации данных»	xidbox-validation-[version].[commit].x86_64.rpm
ППО «Сервис выполнения автоматических расчетов»	xidbox-request-background-processing-[version].[commit].x86_64.rpm

2. Условия применения

Все компоненты X-IDBox поставляются в виде rpm-пакетов и размещаются только на виртуальных машинах и серверах.

Специальные требования к настройке оборудования локальной вычислительной сети и сетей передачи данных не предъявляются.

2.1. Требования к серверной части

Для корректного функционирования сервисов X-IDBox необходим перечень виртуальных машин под управлением ОС Linux с пакетным менеджером rpm, входящей в реестр отечественного ПО, с характеристиками из расчета на один сервис не ниже:

- ЦПУ – Core 4;
- ОЗУ – 16 ГБ;
- HDD – 200 ГБ.

2.2. Требования к АРМ пользователя

Для корректной работы X-IDBox на АРМ пользователя необходима установка и настройка СКЗИ и веб-браузера.

X-IDBox поддерживает совместимость со следующими:

- Chromium-GOST версии 112.0.5615.165 или выше;
- Яндекс.Браузер версии 21.11.4.727 или выше.

Для работы с пользовательским интерфейсом управления доступом X-IDBox необходимо СКЗИ «КриптоПро CSP» версии 4.0 или выше, а вместе с ним – «КриптоПро ЭЦП Browser plug-in» версии 2.0.

Подробное описание подготовки АРМ пользователя к работе с X-IDBox приведено в Руководстве пользователя.

2.3. Требования к необходимому уровню квалификации администратора и рекомендации по освоению системы

Администратор должен обладать следующими знаниями и навыками:

- навыки работы с персональным компьютером;
- навыки работы с веб-обозревателем;
- знание протоколов SOAP, REST;
- навыки работы с БПО и ППО, используемым на стороне ИС;
- опыт администрирования ОС семейства Linux;
- опыт работы с Postgres Pro Ent., NoSQL СУБД (Redis), веб-серверами (Nginx, Tomcat);
- знакомство с системами мониторинга (Zabbix, Grafana, Prometheus).

3. Указания по комплексной наладке

3.1. Перечень ресурсов, необходимых для проведения комплексной наладки

Для проведения комплексной наладки необходимы подготовленные виртуальные машины для установки сервисов X-IDBox, минимальные требования к конфигурации которых приведены в п. 2.1.

3.2. Условия, при соблюдении которых возможно проведение комплексной наладки

Комплексная наладка проводится при наличии:

- документации X-IDBox;
- дистрибутивов X-IDBox (ППО).
- дистрибутивов БПО, СУБД.

3.3. Перечень и последовательность работ по комплексной наладке

Комплексная наладка проводится в следующей последовательности:

- 1) Подготовка сервера или виртуальных машин для установки компонентов X-IDBox.
- 2) Установка БПО и СУБД.
- 3) Подготовка конфигурационных файлов.
- 4) Установка сервисов X-IDBox.
- 5) Настройка сервисов X-IDBox.

3.4. Требования к операционной системе «РЕД ОС»

Обязательные требования к операционной системе «РЕД ОС»:

- версия не ниже 7.3.1;

- статические настройки протокола TCP/IP;
- регистрация сервера в DNS;
- наличие привилегированного пользователя для установки;
- настроенный или выключенный SELinux;
- настроенная служба синхронизации времени с контроллером домена;
- настроенный или выключенный межсетевой экран.

3.5. Установка и настройка СУБД Postgres Pro Ent.

Установите и настройте то количество кластеров Postgres Pro Ent., которое определено в зависимости от схемы развертывания ППО X-IDBox, в соответствии с официальной документацией:

<https://postgrespro.ru/docs/enterprise/15/tutorial-install>

3.6. Создание схем БД

Требования к серверу, на котором планируется создание схем БД:

- сервер с установленной ОС «РЕД ОС» версии не ниже 7.3.1 подготовлен к установке сервисов (п. 3.4);
- установлена и настроена СУБД Postgres Pro Ent. версии не ниже 14 и находящейся в долгосрочной поддержке (LTS) (п. 3.5).

3.6.1. Создание схем БД x_idbox_database

На любом сервере кластера Postgres Pro Ent., предназначенного для БД x_idbox_database, создайте БД x_idbox_database. Схемы и таблицы будут созданы автоматически при установке и запуске сервисов системы.

3.6.2. Создание схем БД x_id_box_scheduler

На любом сервере кластера Postgres Pro Ent., предназначенного для БД x_id_box_scheduler, создайте БД x_id_box_scheduler. Схемы и таблицы будут созданы автоматически при установке и запуске сервисов системы.

3.6.3. Создание схем БД storage

На любом сервере кластера Postgres Pro Ent., предназначенного для БД storage, создайте БД storage. Схемы и таблицы будут созданы автоматически при установке и запуске сервисов системы.

3.6.4. Создание схем БД state_machine_queue

На любом сервере кластера Postgres Pro Ent., предназначенного для БД state_machine_queue, создайте БД state_machine_queue. Схемы и таблицы будут созданы автоматически при установке и запуске сервисов системы.

3.6.5. Создание схем БД sm

На любом сервере кластера Postgres Pro Ent., предназначенного для БД sm, создайте БД sm. Схемы и таблицы будут созданы автоматически при установке и запуске сервисов системы.

3.7. Установка и настройка СУБД Redis

Установите и настройте то количество кластеров Redis, которое определено в зависимости от схемы развертывания ППО X-IDBox, в соответствии с официальной документацией:

<https://redis.readthedocs.io/>

4. Подготовка конфигурационных файлов

4.1. Файл конфигурации и взаимодействия сервисов

Создайте конфигурационный файл по образцу «xidbox.properties» (из прилагаемых дистрибутивов), принимая во внимание комментарии по тексту файла образца. Расширенный список настроек сервисов приведен в Приложении Б.

4.2. Файлы конфигурации веб-сервера

Создайте конфигурационные файлы по образцу файлов из архива «nginx.zip» (из прилагаемых дистрибутивов), принимая во внимание комментарии по тексту файлов образцов.

4.3. Файлы конфигурации Модуля фильтрации запросов к ИС

Создайте конфигурационные файлы по образцу файлов из архива «authng.zip» (из прилагаемых дистрибутивов), принимая во внимание комментарии по тексту файлов образцов.

4.4. Файл конфигурации ведения журналов

Создайте конфигурационный файл по образцу «logback-spring.xml» (из прилагаемых дистрибутивов), принимая во внимание комментарии по тексту файла образца.

4.5. Файлы конфигурации Kerberos

Если необходимо предоставить пользователям возможность входа с доменными учётными записями, создайте конфигурационные файлы «jaas.conf» и

«krb5.conf» по образцу файлов из архива «kerberos.zip» (из прилагаемых дистрибутивов), принимая во внимание комментарии по тексту файлов образцов.

5. Установка системы

5.1. Установка и настройка ППО «Сервис аутентификации»

5.1.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Postgres Pro Ent., предназначенные для работы с сервисом.
- Установлены и настроены кластеры Redis, предназначенные для работы с сервисом.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.
- Если необходимо предоставить пользователям возможность входа с использованием доменных учётных записей, потребуется настроить службу синхронизации времени с контроллером домена. Данная операция выполняется в соответствии с требованиями к операционной системе «РЕД ОС», описанными в п. 3.4.

5.1.2. Установка

На серверах, предназначенных для установки сервиса аутентификации, установите ППО «Сервис аутентификации» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.1.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

Для корректной работы перед первым запуском ППО «Сервис аутентификации» необходимо сгенерировать и настроить ключи для подписания сессионных данных пользователей. Для этого выполните действия, описанные в п. 5.1.3.1.

Если необходимо предоставить пользователям возможность входа с доменными учётными записями, потребуется настроить контроллер домена и ППО «Сервис аутентификации». В противном случае данная настройка не требуется.

В зависимости от используемого типа контроллера домена необходимо выполнить настройки в соответствии с п. 5.1.3.2, 5.1.3.3 и 5.1.3.4.

5.1.3.1. Генерация ключей для подписания сессионных данных

Для генерации и настройки использования ключей:

1) Сгенерируйте ключи для подписания сессионных данных пользователей, хранящихся в виде JWT в браузере пользователя. Для этого предлагается использовать утилиту `keytool`, исполняемый файл которой входит в набор инструментов Java (JDK).

Для генерации ключей выполните команду:

```
keytool -genkey -keyalg RSA -alias xidbox-auth-  
token -keystore xidbox-jwt.jks -keysize 2048 -  
storetype JCEKS
```

где:

- `genkey` – генерирует новую пару ключей (открытый/закрытый ключ);
- `keyalg` – выбирает алгоритм шифрования, в данном случае RSA;
- `alias` – устанавливает метку для этой пары ключей в хранилище.

Можно выбрать любое наименование;

- `keystore` – наименование файла хранилища ключей;
- `keysize` – определяет размер ключа (в битах). 2048 – это стандартный размер, обеспечивающий хорошую безопасность;

- storetype – тип хранилища ключей для создания экземпляра.

Затем введите пароль для хранилища и заполните информацию о владельце ключа (ФИО, организация и т.д.).

2) Настройте ППО «Сервис аутентификации» для использования сгенерированных ключей. Для этого измените параметры в файле конфигурации «xidbox.properties»:

- Идентификатор (алиас) сертификата для подписи JWT:

```
xidbox.authentication.service.jwt.jwt-certificate-alias
```

- Путь к хранилищу, где лежит ключ и сертификат для подписи JWT:

```
xidbox.authentication.service.jwt.keystore-file
```

- Пароль от хранилища и приватного ключа:

```
xidbox.authentication.service.jwt.keystore-password
```

- Частота обновления JWT, в секундах:

```
xidbox.authentication.service.jwt.refresh-ttl-second
```

Пример настройки:

```
xidbox.authentication.service.jwt.jwt-certificate-alias=xidbox-auth-token
xidbox.authentication.service.jwt.keystore-file=file:./jwt/xidbox-jwt.jks
xidbox.authentication.service.jwt.keystore-password=qwerty
xidbox.authentication.service.jwt.refresh-ttl-second=30
```

В примере приведен способ указания относительного пути от исполняемого файла ППО «Сервис аутентификации» к сгенерированному файлу с ключами.

Описание каждого параметра приведено в приложении Б.4.

5.1.3.2. Настройка доменной аутентификации на стороне контроллера домена Active Directory

Для настройки доменной аутентификации на стороне контроллера домена Active Directory необходимо:

- 1) Создать сервисную учётную запись.
- 2) Добавить псевдонимы для сервисной учётной записи (Service Principal Name).
- 3) Добавить хост в DNS Active Directory.
- 4) Сгенерировать keytab-файл.

Для создания сервисной учётной записи в Active Directory выполните следующие действия:

- 1) На контроллере домена перейдите в **Панель управления**.
- 2) В разделе **Администрирование** выберите пункт **Пользователи и компьютеры Active Directory**.
- 3) В нужной директории домена создайте нового пользователя с определенным именем. Например, xidbox.
- 4) Для созданной учётной записи рекомендуется задать постоянный пароль и отключить истечение его срока действия.
- 5) В свойствах созданной учётной записи на вкладке **Учётная запись** установите флаг **Данная учётная запись поддерживает 256-разрядное шифрование** (рис. 1).

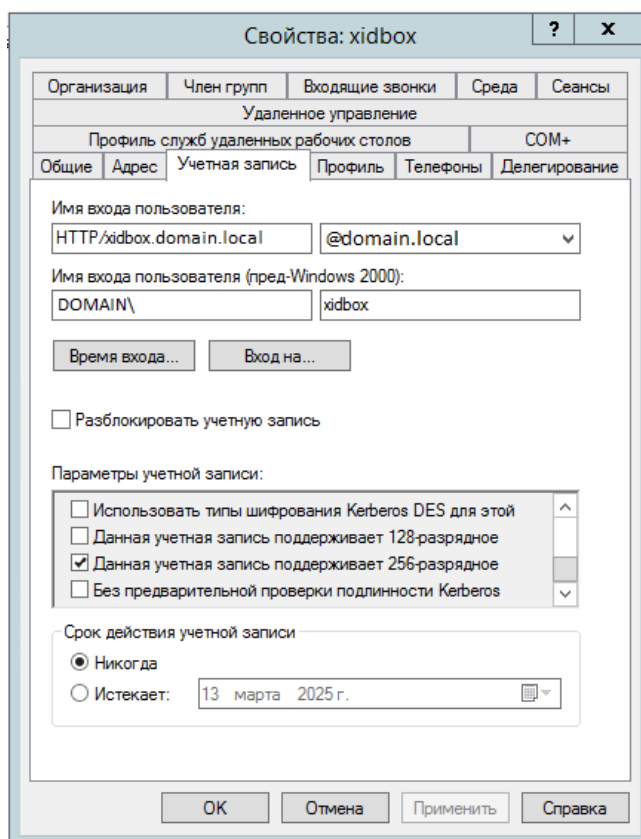


Рисунок 1 – Настройка учётной записи в Active Directory

Для добавления псевдонимов для сервисной учётной записи в Active Directory выполните следующие действия:

1) Откройте командную строку с правами администратора на контроллере домена.

2) Используйте следующую команду для добавления SPN:

```
>setspn -A HTTP/xidbox.domain.local domain\xidbox
```

где:

- HTTP/xidbox.domain.local – имя сервиса и домена;
- domain\xidbox – имя сервисной учётной записи в домене.

3) Для проверки зарегистрированных SPN используйте команду:

```
setspn -L domain\xidbox
```

Пример выполнения команды:

```
> setspn -L domain\xidbox
Registered ServicePrincipalNames for
CN=xidbox,CN=Users,DC=domain,DC=local:
HTTP/xidbox.domain.local
```

4) Убедитесь, что все необходимые SPN добавлены корректно.

Для добавления хоста в DNS Active Directory выполните следующие действия:

- 1) На контроллере домена перейдите в **Панель управления**.
- 2) В разделе **Администрирование** выберите пункт **Диспетчер DNS**.
- 3) Перейдите в **Зону прямого просмотра** и выберите нужную доменную зону.
- 4) **Создайте запись** (A или AAAA).
- 5) В поле **Имя** введите имя хоста. Например, xidbox.
- 6) В поле **IP-адрес** введите IP-адрес сервера.
- 7) Нажмите **Добавить узел** и подтвердите создание записи (рис. 2).
- 8) Убедитесь, что новая запись появилась в списке.

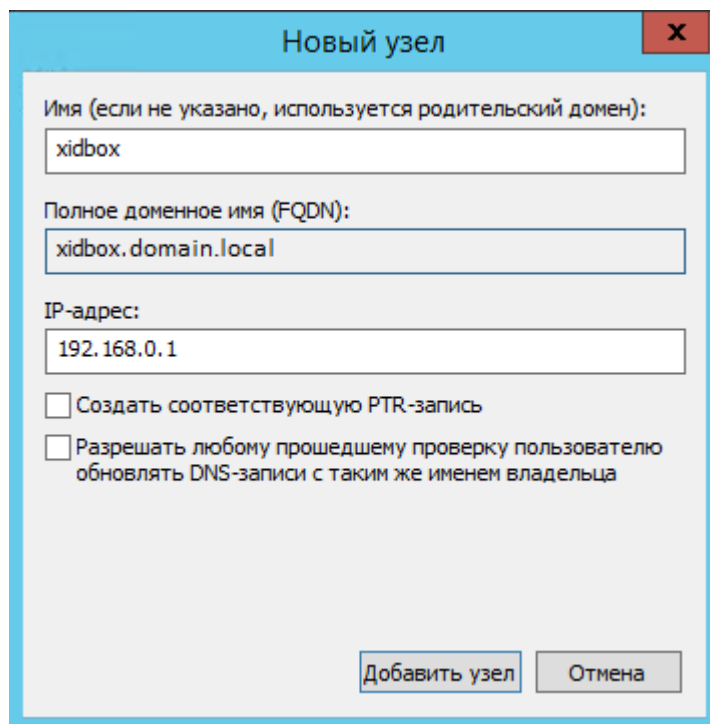


Рисунок 2 – Добавление записи хоста в DNS Active Directory

Для генерации keytab-файла в Active Directory выполните следующие действия:

- 1) Откройте командную строку с правами администратора.
- 2) Выполните следующую команду для создания keytab-файла (пример для сервиса HTTP/xidbox.domain.local):

```
ktpass -out xidbox.keytab -princ  
HTTP/xidbox.domain.local@DOMAIN.LOCAL -mapuser
```

```
domain\xidbox -crypto AES256-SHA1 -ptype  
KRB5_NT_PRINCIPAL -pass *
```

где:

- HTTP/xidbox.domain.local@DOMAIN.LOCAL – имя сервиса и домена в верхнем регистре;
- domain\xidbox – учётная запись;
- AES256-SHA1 – алгоритм шифрования.

Пример выполнения команды:

```
> ktpass -princ  
HTTP/xidbox.domain.local@DOMAIN.LOCAL -mapuser  
xidbox -pass <password_user> -crypto AES256-SHA1 -  
ptype KRB5_NT_PRINCIPAL -out xidbox.keytab  
Targeting domain controller: ad.domain.local  
Using legacy password setting method  
Successfully mapped HTTP/xidbox.domain.local to  
xidbox.  
Key created.  
Output keytab to xidbox.keytab:  
Keytab version: 0x502  
keysize 102 HTTP/xidbox.domain.local@DOMAIN.LOCAL  
ptype 1 (KRB5_NT_PRINCIPAL) vno 15 etype 0x12  
(AES256-SHA1) keylength 32  
(0xf987ed3839239dbd65433a40f710b0e3b128cf05cc62b309  
006ce7d75acf96f9)
```

- 3) Убедитесь, что файл «xidbox.keytab» успешно создан.

5.1.3.3. Настройка доменной аутентификации на стороне контроллера домена FreeIPA

Для настройки доменной аутентификации на стороне контроллера домена FreeIPA выполните следующие действия:

- 1) Подключитесь к веб-консоли управления FreeIPA с помощью браузера.
- 2) Создайте узел. Для этого в разделе **Идентификация** выберите пункт **Узлы** и нажмите кнопку **Добавить**.
- 3) В поле **Имя узла** введите имя узла. Например, xidbox.

- 4) Из выпадающего списка **Зона DNS** выберите соответствующую зону DNS.
- 5) В поле **IP-адрес** введите IP-адрес сервера. Например, 192.168.0.1.
- 6) Нажмите кнопку **Добавить** (рис. 3).

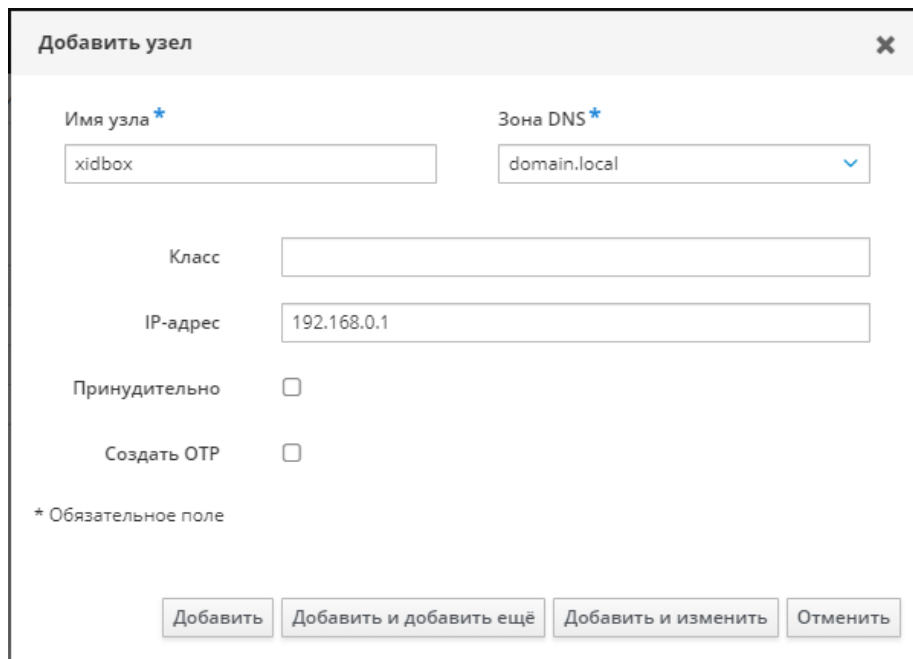


Рисунок 3 – Создание узла в FreeIPA

- 7) Создайте HTTP-сервис для ранее созданного узла. Для этого в разделе **Идентификация** выберите пункт **Службы** и нажмите кнопку **Добавить**.
- 8) Из выпадающего списка **Служба** выберите **HTTP**.
- 9) Из выпадающего списка **Имя узла** выберите соответствующее имя узла.
- 10) Нажмите кнопку **Добавить** (рис. 4).

Рисунок 4 – Создание службы в FreeIPA

Для генерации keytab-файла в FreeIPA выполните следующие действия:

1) Подключитесь к серверу FreeIPA с правами администратора.

2) Авторизуйтесь как администратор домена:

```
> kinit admin
```

3) Выполните следующую команду для генерации keytab-файла (пример для сервиса HTTP/xidbox.domain.local):

```
> ipa-getkeytab -s freeipa.domain.local -p
HTTP/xidbox.domain.local@DOMAIN.LOCAL -k
xidbox.keytab
```

где:

- freeipa.domain.local – адрес сервера FreeIPA;
- HTTP/xidbox.domain.local@DOMAIN.LOCAL – имя сервиса;
- xidbox.keytab – путь к keytab-файлу.

Пример выполнения команды:

```
> ipa-getkeytab -s freeipa.domain.local -p
HTTP/xidbox.domain.local@DOMAIN.LOCAL -k
xidbox.keytab
```

Таблица ключей успешно получена и сохранена в:
xidbox.keytab

4) Убедитесь, что файл «xidbox.keytab» успешно создан.

5.1.3.4. Настройка доменной аутентификации на стороне ППО

«Сервис аутентификации»

Необходимые данные перед началом настройки доменной аутентификации в ППО «Сервис аутентификации»:

- Имя домена. Например, DOMAIN.LOCAL.
- IP-адрес сервера и порт (Значение порта по умолчанию – 88), на котором функционирует служба Kerberos. Например, 127.0.0.1:88.
- Сгенерированный ранее keytab-файл для сервисной учётной записи X-IDBox.

Для подготовки файлов с настройками параметров аутентификации по протоколу Kerberos:

- 1) В директорию «/opt/xidbox/config/kerberos» скопируйте файл конфигурации «jaas.conf», подготовленный в ходе выполнения п. 4.5, с именем «jaas.conf».

Пример минимально достаточного содержимого:

```
KerberosAcceptorWithTicket { /* Произвольное
название профиля */
    /*
        Настройка jaas для обязательного прохождения
        Kerberos аутентификации с использованием модуля
        Krb5LoginModule.
        Используется для аутентификации приложения на
        kdc-сервере и возможности проверять билеты
        клиентов.
    */
    com.sun.security.auth.module.Krb5LoginModule
required
    storeKey=true
    doNotPrompt=true
    useKeyTab=true

principal="HTTP/xidbox.domain.local@DOMAIN.LOCAL"
    keyTab="file:/kerberos/xidbox.keytab";
};
```

2) В файле укажите произвольное наименование профиля. В примере, приведенном выше `KerberosAcceptorWithTicket` – это значение, которое в дальнейшем потребуется указать в параметре `xidbox.authentication.service.kerberos.jaas-profile-name`, а также установить значения:

- `principal` – указывается полное наименование принципала, содержащее SPN и Kerberos-область (`realm`), для которого был сгенерирован `keytab`-файл;

- `keytab` – указывается путь к сгенерированному `keytab`-файлу. В примере приведен способ указания относительного пути от исполняемого файла ППО «Сервис аутентификации» к сгенерированному `keytab`-файлу.

3) В директорию «`/opt/xidbox/kerberos`» скопируйте файл конфигурации «`krb5.conf`», подготовленный в ходе выполнения п. 4.5, с именем «`krb5.conf`».

Пример минимально достаточного содержимого:

```
[libdefaults]
    # Определение области Kerberos по умолчанию для
    клиента
    default_realm = DOMAIN.LOCAL # Указывается
    имя домена
    # Необходимо раскомментировать три строки ниже,
    если используется контроллер домена Active
    Directory (AD)
    #default_tgs_enctypes = aes256-cts-hmac-
    sha1-96
    #default_tkt_enctypes = aes256-cts-hmac-
    sha1-96
    #permitted_enctypes = aes256-cts-hmac-sha1-
    96
[realms]
    # Настройка области Kerberos
    DOMAIN.LOCAL = { # Указывается имя домена
        kdc = 127.0.0.1:88 # Указывается IP-адрес
        сервера и порт на котором функционирует служба
        Kerberos
    }
```

4) Настройте ППО «Сервис аутентификации» для использования подготовленных файлов «jaas.conf» и «krb5.conf». Для этого измените параметры в файле конфигурации «xidbox.properties»:

– Путь к ранее созданному файлу «krb5.conf»:

```
xidbox.authentication.service.kerberos.krb5
```

– Путь к ранее созданному файлу «jaas.conf»:

```
xidbox.authentication.service.kerberos.jaas
```

– Название профиля из файла «jaas.conf»:

```
xidbox.authentication.service.kerberos.jaas-  
profile-name
```

Пример настройки:

```
xidbox.authentication.service.kerberos.krb5=file:/k  
erberos/krb5.conf  
xidbox.authentication.service.kerberos.jaas=file:/k  
erberos/jaas.conf  
xidbox.authentication.service.kerberos.jaas-  
profile-name=KerberosAcceptorWithTicket
```

В примере приведен способ указания относительных путей от исполняемого файла ППО «Сервис аутентификации» к подготовленным файлам.

Описание каждого параметра приведено в приложении Б.4.

5.2. Установка и настройка Модуля фильтрации запросов к ИС

5.2.1. Предусловия

Сервер с установленным и настроенным веб-сервером Nginx в соответствии с п. 5.32.

5.2.2. Установка

На серверах, предназначенных для установки Модуля фильтрации запросов к ИС, установите Модуль фильтрации запросов к ИС из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.3. Установка и настройка ППО «Сервис авторизации»

5.3.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Redis, предназначенные для работы с сервисом.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.3.2. Установка

На серверах, предназначенных для установки сервиса авторизации, установите ППО «Сервис авторизации» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.3.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.4. Установка и настройка ППО «Сервис обработки данных»

5.4.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Postgres Pro Ent., предназначенные для работы с сервисом.
- Установлены и настроены кластеры Redis, предназначенные для работы с сервисом.

– Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.4.2. Установка

На серверах, предназначенных для установки сервиса обработки данных, установите ППО «Сервис обработки данных» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.4.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.5. Установка и настройка ППО «Модуль отправки уведомлений информационным системам с использованием Kafka»

5.5.1. Предусловия

– Сервер соответствует требованиям, приведенным в п. 2.1.

– Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.5.2. Установка

На серверах, предназначенных для установки Модуля отправки уведомлений ИС с использованием Kafka, установите ППО «Модуль отправки уведомлений информационным системам с использованием Kafka» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.5.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.6. Установка и настройка ППО «Модуль отправки уведомлений информационным системам с использованием RabbitMQ»

5.6.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.6.2. Установка

На серверах, предназначенных для установки Модуля отправки уведомлений ИС с использованием RabbitMQ, установите ППО «Модуль отправки уведомлений информационным системам с использованием RabbitMQ» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.6.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.7. Установка и настройка ППО «Модуль отправки уведомлений информационным системам с использованием REST»

5.7.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.7.2. Установка

На серверах, предназначенных для установки Модуля отправки уведомлений ИС с использованием REST, установите ППО «Модуль отправки уведомлений информационным системам с использованием REST» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.7.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем xidbox.properties.

5.8. Установка и настройка ППО «Модуль подписания с использованием КристоПро»

5.8.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.8.2. Установка

На серверах, предназначенных для установки криптографического сервиса, установите ППО «Модуль подписания с использованием КриптоПро» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.8.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем xidbox.properties.

5.9. Установка и настройка ППО «Сервис работы с основными БД»

5.9.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Postgres Pro Ent., предназначенные для работы с сервисом.
- Установлены и настроены кластеры Redis, предназначенные для работы с сервисом.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.9.2. Установка

На серверах, предназначенных для установки сервиса работы с основными БД, установите «ППО «Сервис работы с основными БД» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.9.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.10. Установка и настройка ППО «Сервис синхронизации данных каталогов»

5.10.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.10.2. Установка

На серверах, предназначенных для установки сервиса синхронизации данных каталогов, установите ППО «Сервис синхронизации данных каталогов» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.10.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1 настоящего документа, с именем «xidbox.properties».

5.11. Установка и настройка Модуля балансировки внутренних запросов

5.11.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.11.2. Установка

На серверах, предназначенных для установки Модуля балансировки внутренних запросов, установите Модуль балансировки внутренних запросов из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.11.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.12. Установка и настройка ППО «Сервис взаимодействия с пользовательским интерфейсом управления доступом»

5.12.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Redis, предназначенные для работы с сервисом.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.12.2. Установка

На серверах, предназначенных для установки сервиса взаимодействия с пользовательским интерфейсом управления доступом, установите ППО «Сервис взаимодействия с пользовательским интерфейсом управления доступом» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.12.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.13. Установка и настройка ППО «Пользовательский интерфейс управления доступом»

5.13.1. Предусловия

Сервер с установленным и настроенным веб-сервером Nginx в соответствии с п. 5.32.

5.13.2. Установка

На серверах, предназначенных для установки пользовательского интерфейса управления доступом, установите ППО «Пользовательский интерфейс управления доступом» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.14. Установка и настройка ППО «Сервис идентификации»

5.14.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Redis, предназначенные для работы с сервисом.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.14.2. Установка

На серверах, предназначенных для установки сервиса идентификации, установите ППО «Сервис идентификации» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.14.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.15. Установка и настройка адаптера к ППО «Сервис интеграции с LDAP-каталогами»

5.15.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены сервисы каталогов, предназначенные для работы с сервисом.

– Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.15.2. Установка

На серверах, предназначенных для установки сервиса интеграции с LDAP-каталогами, установите ППО «Сервис интеграции с LDAP-каталогами» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.15.3. Настройка

Для корректной работы сервиса необходимо создать техническую учётную запись на контроллере домена. В зависимости от типа используемого контроллера домена необходимо выполнить соответствующие действия.

5.15.3.1. Создание технической учётной записи в Active Directory

Для создания технической учётной записи в Active Directory необходимо выполнить действия аналогичные описанию в п. 5.1.3.2.

5.15.3.2. Создание технической учётной записи в FreeIPA

Для создания технической учётной записи через веб-консоль FreeIPA выполните следующие действия:

- 1) Войдите в систему, используя учётные данные администратора или пользователя с правами на создание учётных записей.
- 2) В главном меню веб-консоли FreeIPA перейдите в раздел **Идентификация**.
- 3) Выберите подраздел **Пользователи**.
- 4) Создайте новую учётную запись. Например, xidbox_service (рис. 5).

FreeIPA Administrator

Идентификация | Политика | Аутентификация | Сетевые службы | IPA-сервер

Пользователи | Узлы | Службы | Группы | Представления ID | Автоучастник

Активные пользователи » xidbox_service

✓ Пользователь: xidbox_service

Параметры

xidbox_service является участником:

Группы пользователей (1)	Сетевые группы	Роли	Правила HBAC	Правила Sudo	Привилегии Parsec
Минимальные категории конфиденциальности	Максимальные категории конфиденциальности		Маска аудита успеха		
Маска аудита отказа					

Обновить | Вернуть | Сохранить | Действия

Параметры идентификации

Должность

Имя * xidbox

Фамилия * xidbox

Полное имя * xidbox xidbox

Отображаемое имя xidbox xidbox

Инициалы xx

GECOS xidbox xidbox

Класс

Параметры учётной записи

Имя учётной записи пользователя xidbox_service

Пароль *****

Окончание действия пароля 2099-08-17 01:15:29Z

UID 964600010

ID группы 964600010

Псевдоним учётной записи xidbox_service@DOMAIN.LOCAL Удалить

Добавить

Окончание действия учётной записи YYYY-MM-DD hh : mn UTC Отменить

Рисунок 5 – Создание технической учётной записи в FreeIPA

5) Для созданной учётной записи задайте постоянный пароль и увеличьте срок его действия. Для этого выполните следующие действия в командной строке:

– Авторизуйтесь как администратор домена.

```
#kinit admin
```

– Выполните следующую команду для установки срока действия пароля.

```
#ipa user-mod xidbox_service --
setattr=krbPasswordExpiration=20990101010000Z
```

Пример выполнения команды:

```
-----
----
Изменён пользователь "xidbox_service"
```

```
-----  
-----  
Имя учётной записи пользователя: xidbox_service  
Имя: xidbox  
Фамилия: xidbox  
Домашний каталог: /home/xidbox_service  
Оболочка входа: /bin/bash  
Имя учётной записи: xidbox_service@DOMAIN.LOCAL  
Псевдоним учётной записи:  
xidbox_service@DOMAIN.LOCAL  
Окончание действия учётной записи Kerberos:  
20990101000000Z  
Окончание действия пароля пользователя:  
20990101010000Z  
Адрес электронной почты:  
xidbox_service@domain.local  
UID: 964600010  
ID группы: 964600010  
Учётная запись отключена: False  
Пароль: True  
Участник групп: ipausers  
Доступные ключи Kerberos: True
```

5.15.3.3. Настройка конфигурационного файла

Для настройки конфигурационного файла выполните следующие действия:

- 1) В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».
- 2) Настройте сервис, изменив следующие параметры в файле конфигурации «xidbox.properties»:

```
- xidbox.ldap.service.spring.ldap.urls;  
- xidbox.ldap.service.spring.ldap.base;  
- xidbox.ldap.service.spring.ldap.username;  
- xidbox.ldap.service.spring.ldap.password;  
- xidbox.ldap.service.directory.source;
```

- `xidbox.ldap.service.directory.base`.

Описание каждого параметра приведено в приложении Б.15.

5.16. Установка и настройка ППО «Сервис обработки заявок»

5.16.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет

Java Axiom JDK Certified версии 17.

5.16.2. Установка

На серверах, предназначенных для установки обработки заявок, установите ППО «Сервис обработки заявок» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.16.3. Настройка

В директорию «`/opt/xidbox/config`» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «`xidbox.properties`».

5.17. Установка и настройка ППО «Сервис организации выполнения заявок»

5.17.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет

Java Axiom JDK Certified версии 17.

5.17.2. Установка

На серверах, предназначенных для установки сервиса организации выполнения заявок, установите ППО «Сервис организации выполнения заявок» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.17.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.18. Установка и настройка ППО «Сервис изменения заявок»

5.18.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.18.2. Установка

На серверах, предназначенных для установки изменения заявок, установите ППО «Сервис изменения заявок» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.18.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.19. Установка и настройка ППО «Сервис загрузки организаций»

5.19.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.19.2. Установка

На серверах, предназначенных для установки сервиса загрузки организаций, установите ППО «Сервис загрузки организаций» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.19.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.20. Установка и настройка ППО «Сервис загрузки ОШС»

5.20.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.20.2. Установка

На серверах, предназначенных для установки сервиса загрузки ОШС, установите ППО «Сервис загрузки ОШС» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.20.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.21. Установка и настройка ППО «Сервис загрузки ролевых моделей»

5.21.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Postgres Pro Ent., предназначенные для работы с сервисом.
- Установлены и настроены кластеры Redis, предназначенные для работы с сервисом.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.21.2. Установка

На серверах, предназначенных для установки сервиса загрузки ролевых моделей, установите ППО «Сервис загрузки ролевых моделей» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.21.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.22. Установка и настройка ППО «Сервис автоматических операций»

5.22.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Postgres Pro Ent., предназначенные для работы с сервисом.
- Установлены и настроены кластеры Redis, предназначенные для работы с сервисом.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.22.2. Установка

На серверах, предназначенных для установки сервиса автоматических операций, установите ППО «Сервис автоматических операций» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.22.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.23. Установка и настройка ППО «Сервис обеспечения целостности данных»

5.23.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.23.2. Установка

На серверах, предназначенных для установки сервиса обеспечения целостности данных, установите ППО «Сервис обеспечения целостности данных» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.23.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.24. Установка и настройка ППО «Пользовательский интерфейс аутентификации»

5.24.1. Предусловия

Сервер с установленным и настроенным веб-сервером Nginx в соответствии с п. 5.32.

5.24.2. Установка

На серверах, предназначенных для установки пользовательского интерфейса аутентификации, установите ППО «Пользовательский интерфейс аутентификации» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.24.3. Настройка

5.24.3.1. Кастомизация пользовательского интерфейса аутентификации

ППО «Пользовательский интерфейс аутентификации» поддерживает возможность кастомизации страницы аутентификации без изменения стандартных файлов поставки.

При установке ППО «Пользовательский интерфейс аутентификации» в директории создаётся каталог «custom», предназначенный для размещения файлов переопределенного оформления: «`/opt/xidbox/services/xidbox-signin/custom`».

Для кастомизации страницы аутентификации:

1) Внесите необходимые изменения в файл `global.css` (например, фирменные цвета, шрифты, изображения и т. п.).

2) Скопируйте изменённый файл `global.css` в каталог «custom»: «`/opt/xidbox/services/xidbox-signin/custom/global.css`».

3) При необходимости добавьте в каталог «custom» дополнительные файлы (например, логотипы, шрифты):

- «`/opt/xidbox/services/xidbox-signin/custom/favicon.ico`»;

- «`/opt/xidbox/services/xidbox-signin/custom/fonts/custom/font.woff2`».

4) После размещения файлов кастомизации выполните перезапуск веб-сервера Nginx, чтобы изменения вступили в силу:

```
systemctl restart nginx
```

При обращении к ресурсам страницы аутентификации веб-сервер Nginx в первую очередь использует ресурсы из каталога «custom». Если файл в данном каталоге отсутствует, используется стандартный файл из каталога поставки.

5.25. Установка и настройка ППО «Сервис работы с данными заявок»

5.25.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Postgres Pro Ent., предназначенные для работы с сервисом.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.25.2. Установка

На серверах, предназначенных для установки сервиса работы с данными заявок, установите ППО «Сервис работы с данными заявок» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.25.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.26. Установка и настройка ППО «Сервис работы с очередью заявок»

5.26.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Postgres Pro Ent., предназначенные для работы с сервисом.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.26.2. Установка

На серверах, предназначенных для установки сервиса работы с очередью заявок, установите ППО «Сервис работы с очередью заявок» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.26.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.27. Установка и настройка ППО «Сервис работы с исходными данными заявок»

5.27.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Postgres Pro Ent., предназначенные для работы с сервисом.

– Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.27.2. Установка

На серверах, предназначенных для установки сервиса работы с исходными данными заявок, установите ППО «Сервис работы с исходными данными заявок» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.27.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.28. Установка и настройка ППО «Сервис загрузки назначений»

5.28.1. Предусловия

– Сервер соответствует требованиям, приведенным в п. 2.1.

– Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.28.2. Установка

На серверах, предназначенных для установки сервиса загрузки назначений, установите ППО «Сервис загрузки назначений» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.28.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.29. Установка и настройка ППО «Сервис регистрации и изменения данных пользователей»

5.29.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.29.2. Установка

На серверах, предназначенных для установки сервиса регистрации и изменения данных пользователей, установите ППО «Сервис регистрации и изменения данных пользователей» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.29.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.30. Установка и настройка ППО «Сервис валидации данных»

5.30.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Redis, предназначенные для работы с сервисом.
- Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.30.2. Установка

На серверах, предназначенных для установки сервиса валидации данных, установите ППО «Сервис валидации данных» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.30.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.31. Установка и настройка ППО «Сервис выполнения автоматических расчетов»

5.31.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры Redis, предназначенные для работы с сервисом.

– Предоставлен доступ к репозиторию, содержащему установочный пакет Java Axiom JDK Certified версии 17.

5.31.2. Установка

На серверах, предназначенных для установки сервиса выполнения автоматических расчетов, установите ППО «Сервис выполнения автоматических расчетов» из прилагаемых дистрибутивов в соответствии с таблицей 1.

5.31.3. Настройка

В директорию «/opt/xidbox/config» скопируйте файл конфигурации и взаимодействия сервисов, подготовленный в ходе выполнения п. 4.1, с именем «xidbox.properties».

5.32. Установка и настройка веб-сервера Nginx

5.32.1. Предусловия

Сервер соответствует требованиям, приведенным в п. 2.1.

5.32.2. Установка Nginx

На сервере, предназначенном для установки модуля фильтрации запросов к ИС, установите и настройте Nginx (версия 1.25.1) в соответствии с официальной документацией:

https://nginx.org/ru/linux_packages.html

5.32.3. Настройка Nginx

В директорию «/etc/nginx/conf.d/» скопируйте файлы конфигурации модуля фильтрации запросов к ИС, подготовленные в ходе выполнения п. 4.2.

5.33. Добавление ИС X-IDBox

Для добавления ИС X-IDBox:

1) Выполните запрос к ППО «Сервис загрузки ролевых моделей» API «Загрузка информационных систем» (см. «Руководство разработчика. Часть 3. Сервис загрузки ролевых моделей»).

2) Укажите доступные способы входа, а также ссылку на хост ИС X-IDBox. Пример тела запроса:

```
{
  "items": [
    {
      "name": "ИС XIDBox",
      "shortName": "XIDBox",
      "techName": "xidbox",
      "availableAuthenticationTypes": [
        {
          "type": "LOGIN",
          "factor": "FIRST",
          "host":
            "<your_server_address_with_frontend>"
        }
      ],
      "oauthAccess": false
    }
  ]
}
```

2) Загрузите ролевую модель X-IDBox. Для этого загрузите файл «xidbox.txt» (из прилагаемых дистрибутивов), используя ППО «Сервис загрузки ролевых моделей» API «Загрузка информационных систем» (см. «Руководство разработчика. Часть 3. Сервис загрузки ролевых моделей»).

3) Загрузите организацию, выполнив запрос в ППО «Сервис загрузки организаций» API «Загрузка организаций» (см. «Руководство разработчика. Часть 6. Сервис загрузки организаций»). В запросе укажите данные своей или необходимой организации.

4) Загрузите пользователя, выполнив запрос в ППО «Сервис регистрации и изменения данных пользователей» API «Регистрация пользователей» (см. «Руководство разработчика. Часть 4. Сервис регистрации и изменения данных пользователей»).

5) Получите идентификатор УЗ пользователя, выполнив запрос в ППО «Сервис идентификации» API «Получение данных об УЗ пользователя по логину» (см. «Руководство разработчика. Часть 2. Сервис идентификации»). В запросе в параметре «login» укажите значение логина УЗ пользователя, полученное на шаге 4).

6) Получите идентификатор профиля УЗ пользователя, выполнив запрос в ППО «Сервис идентификации» API «Получение списка профилей УЗ пользователя по её идентификатору» (см. «Руководство разработчика. Часть 2. Сервис идентификации»). В запросе в параметре «userId» укажите значение идентификатора УЗ пользователя, полученное на шаге 5).

7) Назначьте профилю УЗ пользователя роль «Системный администратор» в ИС X-IDBox, выполнив запрос в ППО «Сервис загрузки назначений» API «Загрузка назначений ролей» (см. «Руководство разработчика. Часть 9. Сервис загрузки назначений»). В запросе укажите следующие параметры:

– идентификатор профиля УЗ пользователя – идентификатор, полученный на шаге 6);

– техническое наименование роли – «system_administrator»;

– дата и время начала действия роли – текущие;

– дата и время окончания действия роли – не указывать. Пример тела запроса:

```
{
  "infoSystem": "xidbox",
  "userProfiles": [
```

```
{
  "uuid": "<your_user_profile_uuid>",
  "rolesToAdd": [
    {
      "roleTechName": "system_administrator",
      "startDate": "<current_time_and_date>"
    }
  ]
}
```

8) Войдите в систему через веб-интерфейс (http://<your_server_address>/signin) и подтвердите согласие на обработку персональных данных.

6. Администрирование системы

6.1. Обновление системы

Обновление версий ППО X-IDBox проводится через штатный менеджер пакетов, после размещения новых дистрибутивов сервисов X-IDBox (п. 1.3) в доступный репозиторий.

6.2. Настройка сетевого взаимодействия

При настройке сетевого взаимодействия ИС и X-IDBox необходимо обеспечить сетевое взаимодействие компонентов ИС и X-IDBox.

Шаблон сетевого взаимодействия приведен в Приложении А.

6.3. Подключение информационной системы

6.3.1. Подключение ИС

Для подключения новой ИС:

1) Запросите данные подключаемой ИС. Необходимые данные для подключения ИС представлены в Шаблоне требуемой информации для подключения ИС (приведен в файле Шаблон требуемой информации для подключения ИС.docx).

2) Выполните запрос к ППО «Сервис загрузки ролевых моделей» API «Загрузка информационных систем» (см. «Руководство разработчика. Часть 3. Сервис загрузки ролевых моделей»).

3) Укажите доступные способы входа, а также ссылку на хост ИС X-IDBox. Пример тела запроса:

```
{
  "items": [
    {
      "name": "ИС XIDBox",
```

```
"shortName": "XIDBox",
"techName": "xidbox",
"availableAuthenticationTypes": [
  {
    "type": "LOGIN",
    "factor": "FIRST",
    "host": "<Внешний_адрес_ИС>"
  }
],
"oauthAccess": false
}
]
```

4) При необходимости добавьте в файл «nginx.conf» блок конфигурации – необходим для отображения страницы аутентификации на хосте ИС и проксирования запросов аутентифицированных пользователей в ИС,

где:

- <Внешний_адрес_ИС> – внешний адрес ИС;
- <new_info_system_tech_name> – техническое наименование новой ИС;
- <Адрес_для_проксирования_запросов_в_ИС> – адрес для проксирования запросов в ИС;
- <Порт_ИС> – порт ИС.

Пример конфигурации:

```
server {
    listen      80;
    server_name <Внешний_адрес_ИС>;

    set $stand_scheme http;
    client_max_body_size 1g;

    error_page 500 502 503 504 /50x.html;

    location / {
        access_by_lua_file
        /etc/nginx/conf.d/auth.lua;
    }
}
```

```
        set $upstream_<new_info_system_tech_name>
        <Адрес_для_проксирования_запросов_в_ИС>:<Порт_ИС>;
        include /etc/nginx/conf.d/proxy.pass;
        proxy_pass
        http://$upstream__<new_info_system_tech_name>$request_uri;
    }

    include /etc/nginx/conf.d/proxy.locations;

}
```

В случае, если настроена аутентификация с помощью доменной учётной записи, в зависимости от используемого типа контроллера домена, выполните следующие действия:

Порядок настройки для Active Directory:

1) Добавьте dns-запись в контроллере домена для внешнего адреса ИС аналогично описанию в п. 5.1.3.2.

2) Добавьте псевдоним для сервисной учётной записи в Active Directory с указанием внешнего адреса ИС.

Для добавления псевдонима для сервисной учётной записи в Active Directory выполните следующие действия:

1) Откройте командную строку с правами администратора на контроллере домена.

2) Введите команду для добавления SPN:

```
setspn -A
HTTP/<ВНЕШНИЙ_АДРЕС_ИС>.xidbox.domain.local
domain\xidbox
```

где:

– HTTP/<ВНЕШНИЙ_АДРЕС_ИС>.xidbox.domain.local – имя сервиса и домена,

– domain\xidbox – имя сервисной учётной записи в домене.

3) Для проверки зарегистрированных SPN используйте команду:

```
setspn -L domain\xidbox
```

Пример выполнения команды:

```
> setspn -L domain\xidbox
Registered ServicePrincipalNames for
CN=xidbox,CN=Users,DC=domain,DC=local:
HTTP/xidbox.domain.local
HTTP/is-test.xidbox.domain.local
```

4) Убедитесь, что все необходимые SPN добавлены корректно.

Порядок настройки для FreeIPA:

1) Добавьте хост в FreeIPA для внешнего адреса ИС аналогично описанию в п. 5.1.3.3.

2) Добавьте псевдоним для службы в FreeIPA с указанием внешнего адреса ИС, созданного для X-IDBox аналогично описанию в п. 5.1.3.3 (рис. 6).

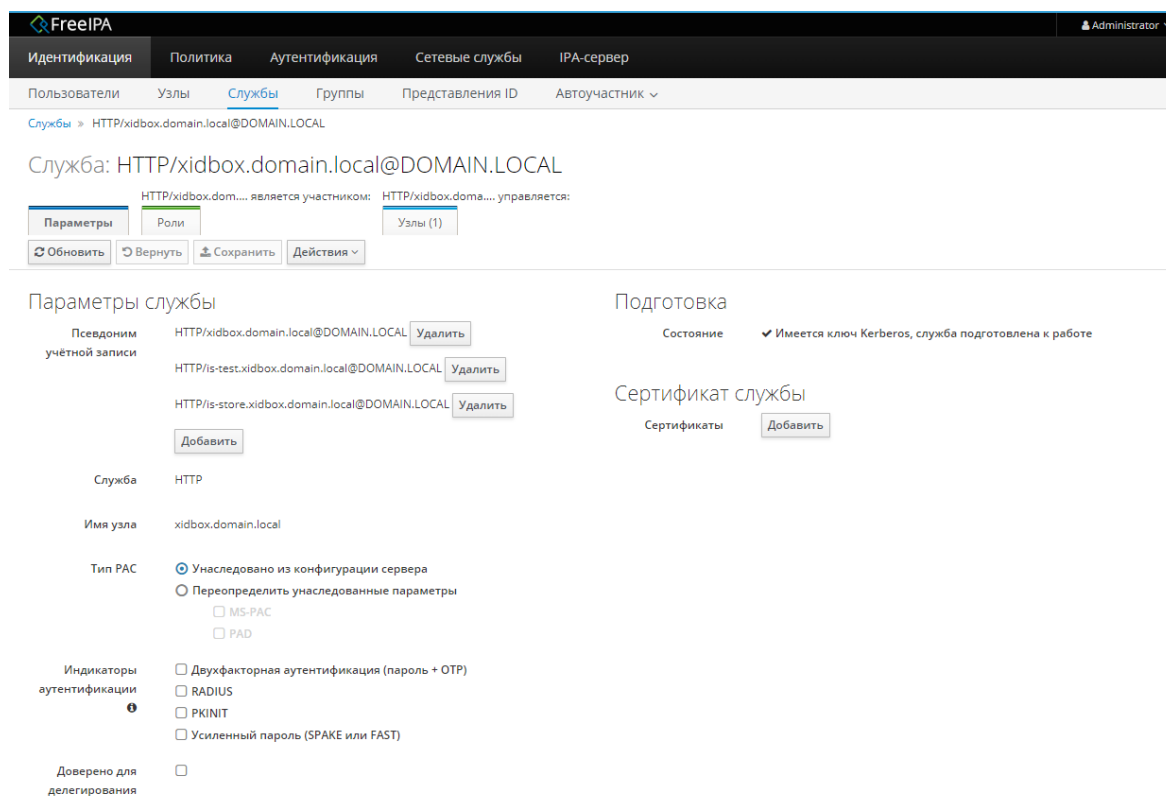


Рисунок 6 – Псевдоним для службы в FreeIPA с указанием внешнего адреса ИС

6.3.2. Подключение ИС OAuth 2.0-клиента в X-IDBox

Для подключения новой ИС OAuth 2.0-клиента:

- 1) Укажите следующие данные подключаемой ИС OAuth 2.0-клиента:
 - полное наименование;
 - сокращенное наименование;

- мнемонику ИС (техническое наименование ИС);
- мнемонику (client_id) OAuth 2.0-клиента;
- адрес, по которому будет перенаправляться пользователь после успешной аутентификации (redirect_url);
- адрес, по которому будет перенаправляться пользователь, аутентифицированный через OpenID Connect 1.0, после успешного выхода из системы (post_logout_redirect_url), необязательный параметр;
- области доступа (scope) – список разрешений, требуемый ИС OAuth 2.0-клиента, приведен в таблице 2.

Таблица 2 – Возможные значения области доступа (scope)

Значение	Наименование	Описание
user	Данные УЗ пользователя	Данные основных полей УЗ пользователя
user-profile	Данные профиля УЗ пользователя	Данные основных полей профиля УЗ пользователя
organization	Данные организации профиля УЗ пользователя	Данные организации профиля УЗ пользователя
user-dynamic-fields	Динамические поля УЗ пользователя	Динамические поля УЗ пользователя. Перечень доступных динамических полей указывается в процессе настройки доступа через OAuth 2.0
user-profile-dynamic-fields	Динамические поля профиля УЗ пользователя	Динамические поля профиля УЗ пользователя. Перечень доступных динамических полей указывается в процессе настройки доступа через OAuth 2.0
organization-dynamic-fields	Динамические поля организации профиля УЗ пользователя	Динамические поля организации профиля УЗ пользователя. Перечень доступных динамических полей указывается в процессе настройки доступа через OAuth 2.0
openid	Идентификатор УЗ пользователя	Получение токена OpenID Connect 1.0 с идентификационными данными пользователя
email	Адрес электронной почты пользователя	Получение адреса электронной почты и признака верификации адреса электронной почты пользователя

Значение	Наименование	Описание
profile	Логин, ФИО, дата рождения пользователя	Получение логина, ФИО, даты рождения пользователя

2) Проверьте, зарегистрирована ли ИС OAuth 2.0-клиента в X-IDBox. Для этого выполните следующий запрос к БД x_id_box:

```
select id, oauth_client_id, oauth_access
from x_id_box.information_system
where tech_name = '{мнемоника ИС (техническое
наименование ИС) из шага 1)}';
```

3) Продолжите в зависимости от результата выполненного запроса:

- Запрос не вернул данные – перейдите к шагу 4).
- Запрос вернул данные и `oauth_client_id == "null"`, при этом `oauth_access == false` – необходимо обновить данные ИС OAuth 2.0-клиента в X-IDBox, для этого перейдите к шагу 4).
- Запрос вернул данные и `oauth_client_id == "null"`, при этом `oauth_access == true` – перейдите к шагу 5).
- Запрос вернул данные и `oauth_client_id != "null"` – для данной ИС уже есть зарегистрированный OAuth 2.0-клиент. Дополнительных действий не требуется.

4) Зарегистрируйте или измените ИС OAuth 2.0-клиента в X-IDBox. Для этого выполните запрос к ППО «Сервис загрузки ролевых моделей» API «Загрузка информационных систем» (см. «Руководство разработчика. Часть 3. Сервис загрузки ролевых моделей»). В теле запроса укажите следующие параметры, предварительно заполнив данные:

```
{
  "items" : [
    {
      "name" : "{полное наименование из шага 1)}",
      "shortName" : "{сокращенное наименование из
шага 1)}",
      "techName" : "{мнемоника ИС (техническое
наименование ИС) из шага 1)}",
      "availableAuthenticationTypes" : [],
      "oauthAccess" : true
    }
  ]
}
```

```

    }
  ]
}

```

5) Заполните данные для OAuth 2.0-клиента в БД x_id_box. Для этого выполните следующий запрос, предварительно заполнив в нем требуемые в блоке «DECLARE» данные:

```

DO
$$
DECLARE
    oauth_client_mnemonic
constant text    := '{мнемоника (client_id) OAuth
2.0-клиента из шага 1)}';
    oauth_client_secret
constant text    := '{сгенерированный секретный код
(client_secret)}';
    oauth_client_information_system_tech_name
constant text    := '{мнемоника ИС (техническое
наименование ИС) из шага 1)}';
    -- параметр ниже заполняется, исходя из
    области доступа (scope) из шага 1) (в примере
    максимально возможные разрешения, приведенные в
    таблице 2)
    ouath_client_allowed_scopes
constant text[] := '{"openid","user", "user-
profile","organization","user-dynamic-
fields","user-profile-dynamic-
fields","organization-dynamic-fields"}'::text[];
    ouath_client_redirect_url
constant text    := '{адрес (redirect_url) из
шага 1)}';
    ouath_client_post_logout_redirect_url
constant text    := '{адрес
(post_logout_redirect_url) из шага 1)}';
BEGIN
    -- создание записи об ИС OAuth 2.0-клиента
    insert into x_id_box.oauth_client(id,
client_id, client_secret)

```

```
values (default, oauth_client_mnemonic,
oauth_client_secret);

--связывание ИС и OAuth 2.0-клиента
update x_id_box.information_system
set oauth_client_id = (select oc.id from
x_id_box.oauth_client oc where oc.client_id =
oauth_client_mnemonic)
where tech_name =
oauth_client_information_system_tech_name;

-- создание разрешения для OAuth 2.0-
клиента
INSERT INTO x_id_box.oauth_client_scope
(oauth_client_id, scope_id)
select oc.id, os.id
from x_id_box.oauth_client oc
inner join x_id_box.oauth_scope os
on 1 = 1
inner join (select
unnest(oauth_client_allowed_scopes) as tech_name) t
on (t.tech_name =
os.tech_name)
where oc.client_id = oauth_client_mnemonic;

INSERT INTO
x_id_box.oauth_client_redirect_uri
(oauth_client_id, redirect_uri)
VALUES ((select oc.id from
x_id_box.oauth_client oc where oc.client_id =
oauth_client_mnemonic),
oauth_client_redirect_url);

--только при наличии (post_logout_redirect_url) из
шага 1)
INSERT INTO
x_id_box.oauth_client_post_logout_redirect_uri
(oauth_client_id, post_logout_redirect_uri)
VALUES ((select oc.id from
x_id_box.oauth_client oc where oc.client_id =
```

```
oauth_client_mnemonic),  
ouath_client_post_logout_redirect_url);  
  
    END  
    $$;
```

6) Сбросьте кеш Redis.

7) Передайте ИС сгенерированный секретный код (client_secret).

6.3.3. Загрузка ролей и защищаемых объектов ИС

Загрузка защищаемых объектов ИС (типы ресурсов, ресурсы, действия, атрибуты) обеспечивает возможность последующего разграничения доступа пользователей к этим объектам через формирование ролей и политик авторизации, содержащих ограничения на действия с этими объектами:

1) Сформируйте ролевую модель подключаемой ИС.

2) Загрузите ролевую модель новой ИС. Для этого загрузите файл с разработанной ролевой моделью. Загрузка ролевой модели доступна через веб-интерфейс X-IDBox и через API. Порядок загрузки ролевой модели через веб-интерфейс X-IDBox приведен в Руководстве пользователя. Порядок загрузки ролевой модели через API и описание формата файла приведены в документе «Руководство разработчика. Часть 3. Сервис загрузки ролевых моделей».

6.3.4. Создание пользователя с ролью «Менеджер ИС»

Для создания пользователя с ролью «Менеджер ИС»:

1) Выполните запрос в ППО «Сервис регистрации и изменения данных пользователей» API «Регистрация пользователей» (см. «Руководство разработчика. Часть 4. Сервис регистрации и изменения данных пользователей»). При необходимости предварительно загрузите организацию, в которой необходимо зарегистрировать данного пользователя:

2) Получите идентификатор УЗ пользователя, выполнив запрос в ППО «Сервис идентификации» API «Получение данных об УЗ пользователя по логину» (см. «Руководство разработчика. Часть 2. Сервис идентификации»). В запросе в параметре «login» укажите значение логина УЗ пользователя, полученное на шаге 1).

3) Получите идентификатор профиля УЗ пользователя, выполнив запрос в ППО «Сервис идентификации» API «Получение списка профилей УЗ пользователя по её идентификатору» (см. «Руководство разработчика. Часть 2. Сервис идентификации»). В запросе в параметре «userId» укажите значение идентификатора УЗ пользователя, полученное на шаге 2).

4) Назначьте профилю УЗ пользователя роль «Менеджер ИС» в ИС X-IDBox, выполнив запрос в ППО «Сервис загрузки назначений» API «Загрузка назначений ролей» (см. «Руководство разработчика. Часть 9. Сервис загрузки назначений»). В запросе укажите следующие параметры:

- идентификатор профиля УЗ пользователя – идентификатор, полученный на шаге 3);
- техническое наименование роли – «information_system_manager»;
- дата и время начала действия роли – текущие;
- дата и время окончания действия роли – не указывать;
- техническое наименование подконтрольной ИС – техническое наименование новой ИС. Пример тела запроса:

```
{
  "infoSystem": "xidbox",
  "userProfiles": [
    {
      "uuid": "<UUID профиля пользователя>",
      "rolesToAdd": [
        {
          "roleTechName":
            "information_system_manager",
          "startDate": "<Текущая дата и время>"
        }
      ]
    }
  ],
}
```

```
"controlledInfoSystemTechName": "<Техническое  
наименования ИС>"  
}  
]  
}
```

6.3.5. Настройка отправки уведомлений

Настройка отправки уведомлений в X-IDBox осуществляется по переданной от ИС заявке на подключение уведомлений (см. «Руководство разработчика. Часть 7. Модуль отправки уведомлений информационным системам»).

Для корректной настройки вставьте соответствующие параметры в таблицу БД «x_id_box.information_system_callback_setting»:

- information_system_id – идентификатор ИС, которая подписывается на получение уведомления о событии;

- information_system_callback_type_id – тип уведомления на которое подписывается ИС;

- information_system_callback_type_version – версия данных для типа «information_system_callback_type_id»;

Доступные поддерживаемые версии для конкретного типа можно посмотреть с помощью запроса:

```
select versions from  
x_id_box.information_system_callback_type ct where  
tech_name='USER_UPDATE'
```

- value – настройка в формате .jsonb, в котором должны содержаться поля:

- type – должно принимать одно из значений: «KAFKA»/«RABBIT»/«REST_API»;

- settings – объект, содержащий поля в формате "ключ" : "значение", которые:

- для KAFKA могут быть заданы только из значений, указанных в документации по адресу: <https://docs.spring.io/spring-boot/reference/messaging/kafka.html>.
- для RABBIT могут быть заданы только из значений, указанных в документации по адресу: <https://spring.io/guides/gs/messaging-rabbitmq>.
- для REST_API могут быть заданы только в виде "url" : "{endpoint_url}", где {endpoint_url} – адрес конечной точки на стороне ИС.

Пример настройки отправки уведомления о событии «USER_CREATE» версии «1» для ИС «is_test» в Kafka:

```
insert into
x_id_box.information_system_callback_setting(inform
ation_system_id,
information_system_callback_type_id,
information_system_callback_type_version, value)
values (
    (select is.id from
x_id_box.information_system is where
is.tech_name='is_test'),
    (select ct.id from
x_id_box.information_system_callback_type ct where
ct.tech_name='USER_CREATE'),
    1,
    '{
        "type": "KAFKA",
        "settings": {
            "key.serializer":
"org.apache.kafka.common.serialization.StringSerial
izer",
            "value.serializer":
"org.springframework.kafka.support.serializer.JsonS
erializer",
            "bootstrap.servers":
"kafka.example.ru:29092"
        }
    }'::jsonb);
```

Пример настройки отправки уведомления о событии «USER_DELETE» версии «1» для ИС «is_test» в очередь «for_user_delete RabbitMQ»:

```
insert into
x_id_box.information_system_callback_setting(inform
ation_system_id,
information_system_callback_type_id,
information_system_callback_type_version, value)
values (
    (select is.id from
x_id_box.information_system is where
is.tech_name='is_test'),
    (select ct.id from
x_id_box.information_system_callback_type ct where
ct.tech_name='USER_DELETE'),
    1,
    '{
        "type": "RABBIT",
        "settings": {
            "spring.rabbit.host": "10.11.23.10",
            "spring.rabbit.port": "5672",
            "spring.rabbit.user": "user",
            "spring.rabbit.password": "guest",
            "spring.rabbit.queueName":
"for_user_delete"
        }
    }'::jsonb);
```

Пример настройки отправки уведомления о событии «USER_PROFILE_UPDATE» версии «1» для ИС «is_test» с использованием REST:

```
insert into
x_id_box.information_system_callback_setting(inform
ation_system_id,
information_system_callback_type_id,
information_system_callback_type_version, value)
values (
    (select is.id from
x_id_box.information_system is where
is.tech_name='is_test'),
```

```
(select ct.id from
x_id_box.information_system_callback_type ct where
ct.tech_name='USER_PROFILE_UPDATE'),
1,
'{
    "type": "REST_API",
    "settings": {
        "url": "http://callback-rest-api-
consumer-mock.example.ru:8080/consumer"
    }
}'::jsonb);
```

6.4. Настройка параметров запуска

Настройка параметров запуска X-IDBox осуществляется путём подготовки конфигурационных файлов. Подробное описание операций приведено в п. 4.1.

6.5. Управление учётными записями пользователей и назначение пользователям прав доступа

Управление данными УЗ пользователя и правами доступа пользователя осуществляется в веб-интерфейсе X-IDBox, в т.ч. путём загрузки файлов в специальных форматах, описанных в документе «Руководство разработчика. Часть 11. Форматы файлов для загрузки через пользовательский интерфейс».

Подробное описание загрузки файлов приведено в Руководстве пользователя.

6.6. Настройка событий безопасности, подлежащих регистрации, их состава и содержания

Параметры журналирования всех событий безопасности хранятся в виде единого основного файла «cef-log-event.json», в котором каждое событие описано в виде набора атрибутов:

- name – техническое наименование события;

- label – наименование события безопасности;
- eventClass – тип события;
- severity – важность события;
- enable – признак отключения журналирования события (по умолчанию включено);
- fields – список журналируемых ключей.

При необходимости можно задать параметры событий безопасности, подлежащих регистрации (в том числе событий, связанных с изменением ролей и полномочий пользователей), состава и содержания информации о них.

Параметры журналирования событий безопасности задаются в отдельном дополнительном файле, местоположение данного файла указывается в настройках X-IDBox в параметре «logback-spring.xml».

В дополнительном файле указываются только те события и только те атрибуты событий, которые необходимо изменить. При этом в настройках нельзя добавить события безопасности, значения ключей которых не предусмотрены основным списком ключей данного события, также нельзя исключать из лога события безопасности сразу все ключи.

При подключении дополнительного файла настроек безопасности будут изменены логи только тех событий, которые описаны в нем, все остальные события безопасности будут логироваться в соответствии с настройками по умолчанию, описанными в основном файле.

Пример дополнительного файла настроек параметров журналирования событий безопасности (отключение журналирования события «Действия привилегированных пользователей»; для события «Событие авторизации пользователя» указывается только часовой пояс, в котором было зафиксировано событие, и результат события):

```
[
  {
    "name": "ADMIN_ACTION",
    "enable": false
  },
  {
```

```
"name": "USER_AUTHORIZATION",  
"fields": [  
    "dtz",  
    "outcome"  
]  
}  
]
```

6.7. Настройка веб-серверов для работы с системой

Веб-серверы в X-IDBox функционируют на основе БПО Nginx. Описание установки и настройки веб-серверов приведено в п. 5.32.

6.8. Настройка рабочих станций пользователей для работы с системой

Подготовка рабочих станций пользователей включает в себя установку и настройку необходимого ПО, а также подготовку сертификатов. Все необходимые операции описаны в Руководстве пользователя.

6.9. Настройка правил выборки подотчётных организаций

В X-IDBox возможно использование динамических полей профиля УЗ пользователя со списком подотчётных организаций.

К настройке правил выборки подотчётных организаций применяются следующие требования:

- правило выборки пишется в виде SQL-запроса;
- в результате должны возвращаться все поля таблицы организаций;
- псевдоним (alias) основной таблицы должен быть «e»;
- в правиле допускается использование параметра «:uuid», куда будет подставляться uuid организации, для которой происходит выборка.

Примеры правил выборки:

- подотчётные организации, сгруппированные по совпадению ИНН:

```
select e.* from x_id_box.organization e join  
x_id_box.organization o2 on e.inn = o2.inn and  
e.uuid != o2.uuid where o2.uuid = :uuid
```

- подотчётные организации, сгруппированные по совпадению адреса:

```
select e.* from x_id_box.organization e inner join  
x_id_box.organization o2 on e.address = o2.address  
where e.uuid != o2.uuid and o2.uuid = :uuid
```

Использование подотчётных организаций в условиях политик авторизации приведено в документе «Руководство разработчика. Часть 3. Сервис загрузки ролевых моделей».

7. Обслуживание системы

7.1. Порядок обслуживания и проверка работоспособности системы

Проверка работоспособности выполняется отдельно для каждого сервиса в составе X-IDBox.

7.1.1. Управление СУБД Postgres Pro Ent.

Запуск, остановка и перезагрузка Postgres Pro Ent. проводится в соответствии с официальной документацией:

<https://postgrespro.ru/docs>

7.1.2. Управление кеш-сервером Redis

Запуск, остановка и перезагрузка Redis проводится в соответствии с официальной документацией:

<https://redis.io/documentation>

7.1.3. Управление веб-сервером Nginx

Запуск, остановка и перезагрузка Nginx проводится в соответствии с официальной документацией:

<http://nginx.org/ru/docs>

7.1.4. Управление сервисами ППО X-IDBox

В таблице 3 приведен перечень управляемых сервисов ППО X-IDBox.

Таблица 3 – Перечень управляемых сервисов ППО X-IDBox

ППО	Название управляемого сервиса
ППО «Сервис аутентификации»	xidbox-authentication

ППО	Название управляемого сервиса
Модуль фильтрации запросов к ИС	xidbox-authn-gateway
ППО «Сервис авторизации»	xidbox-authorization
ППО «Сервис обработки данных»	xidbox-backend
ППО «Модуль отправки уведомлений информационным системам с использованием Kafka»	xidbox-callback-kafka
ППО «Модуль отправки уведомлений информационным системам с использованием RabbitMQ»	xidbox-callback-rabbit
ППО «Модуль отправки уведомлений информационным системам с использованием REST»	xidbox-callback-rest
ППО «Модуль подписания с использованием КриптоПро»	xidbox-crypto
ППО «Сервис работы с основными БД»	xidbox-database
ППО «Сервис синхронизации данных каталогов»	xidbox-directory-synchronization
Модуль балансировки внутренних запросов	xidbox-eureka
ППО «Сервис взаимодействия с пользовательским интерфейсом управления доступом»	xidbox-frontbackend
ППО «Сервис идентификации»	xidbox-identification
ППО «Сервис интеграции с LDAP-каталогами»	xidbox-ldap
ППО «Сервис обработки заявок»	xidbox-orchestrator
ППО «Сервис организации выполнения заявок»	xidbox-orchestrator-helper
ППО «Сервис изменения заявок»	xidbox-order
ППО «Сервис загрузки организаций»	xidbox-organization
ППО «Сервис загрузки ОШС»	xidbox-organizational-structure
ППО «Сервис загрузки ролевых моделей»	xidbox-role-politics-upload
ППО «Сервис автоматических операций»	xidbox-scheduler
ППО «Сервис обеспечения целостности данных»	xidbox-signature
ППО «Сервис работы с данными заявок»	xidbox-state-machine-database
ППО «Сервис работы с очередью заявок»	xidbox-state-machine-queue
ППО «Сервис работы с исходными данными заявок»	xidbox-storage
ППО «Сервис загрузки назначений»	xidbox-user-profile-upload
ППО «Сервис регистрации и изменения данных пользователей»	xidbox-user-upload
ППО «Сервис валидации данных»	xidbox-validation
ППО «Сервис выполнения автоматических расчетов»	xidbox-request-background-processing

7.1.4.1. Запуск

На сервере с установленным сервисом выполните команду:

```
systemctl start <service>
```

где <service> – название управляемого сервиса в соответствии с таблицей 3.

7.1.4.2. Остановка

На сервере с установленным сервисом выполните команду:

```
systemctl stop <service>
```

где <service> – название управляемого сервиса в соответствии с таблицей 3.

7.1.4.3. Перезагрузка

На сервере с установленным сервисом выполните команду:

```
systemctl restart <service>
```

где <service> – название управляемого сервиса в соответствии с таблицей 3.

7.1.4.4. Мониторинг работоспособности

На сервере с установленным сервисом выполните команду:

```
systemctl status <service>
```

где <service> – название управляемого сервиса в соответствии с таблицей 3.

7.2. Проверка и анализ ключевых параметров функционирования системы и электронных журналов событий

Функции, обеспечивающие просмотр электронных журналов событий безопасности, не предусмотрены в X-IDBox.

Журнал событий безопасности записывается в формате CEF. Каждая запись имеет следующий вид:

<дата и время> <host> CEF:<version>|<eventClass>|<label>|<severity>|
[Extension]

Основные параметры записей, а также фиксированные значения некоторых из них описаны в таблице 4.

Таблица 4 – Основные параметры записей в журнале событий безопасности

Параметр	Значение	Описание
<дата и время>	–	Дата и время, когда было зарегистрировано событие, по стандарту UTC
<host>	–	Имя сервера, на котором было зарегистрировано событие
<version>	Значение по умолчанию – 1	Версия формата CEF
<eventClass>	Значение по умолчанию – security	Тип события
<label>	Указано в соответствующем столбце таблицы 29	Название события, влияющее на состав дополнительных данных о событии безопасности
severity	Значение по умолчанию – 3	Важность события
Extension	Ключи и значения указаны в соответствующих столбцах таблицы 29	Расширение для зарегистрированного события безопасности, содержит пары ключ-значение для различных событий

При регистрации событий безопасности используется поле расширения (Extension), содержащее набор пар ключ-значение (<KEY>=<VALUE>). Расширение может содержать любое количество таких пар в любом порядке, разделённых пробелами (« »). Для различных событий безопасности могут использоваться predetermined ключи, предусмотренные форматом CEF, а также специальные ключи для X-IDBox, описанные в таблице 5.

Таблица 5 – Ключи для дополнительных данных о событиях безопасности

Наименование ключа	Значение ключа	Описание
cs1Label	objectId	Идентификатор объекта, с которым было выполнено соответствующее действие

Наименование ключа	Значение ключа	Описание
cs2Label	orderId	Идентификатор заявки, на основании которой было выполнено соответствующее действие
cs3Label	infoSystemUid	Идентификатор ИС
cs4Label	typeData	Наименование экспортируемых данных
cs5Label	resource	Техническое наименование ресурса, к которому запрашивается разрешение на совершение действия
cs6Label	resourceType	Техническое наименование типа ресурса, к которому запрашивается разрешение на совершение действия
cs7Label	authenticationType	Тип аутентификации

Подробный состав данных в расширении для различных событий безопасности, в зависимости от названия события безопасности, описан в Приложении В.

Если не удалось зафиксировать значение ключа для события безопасности, то либо этот ключ отсутствует в записи о данном событии безопасности, либо записывается пустое значение.

7.3. Резервное копирование и восстановление данных

Для обеспечения целостности и сохранности данных системы в целом и её подсистем необходимо периодически проводить резервное копирование БД X-IDBox.

Резервное копирование и восстановление должно проводиться на сервере средствами ОС и стандартными инструментами СУБД Postgres Pro. Эти работы должны выполняться администратором сервера БД или лицами, состав которых определен администратором.

Основные процедуры, связанные с обеспечением сохранности информации, выполняются администратором сервера БД в соответствии с правилами, регламентирующими порядок сохранения и восстановления данных в организации и рекомендациями производителя СУБД Postgres Pro.

При проведении мероприятий по обеспечению сохранности информации в БД X-IDBox должны выполняться следующие рекомендации:

1) Ежедневное резервное копирование данных. Копирование должно выполняться не реже одного раза в сутки. Состав копируемой информации, используемые устройства хранения резервных копий, методы резервного копирования и программные средства для выполнения этих операций, а также ротация резервных копий должны соответствовать правилам и регламентам организации.

2) Организация кластера средствами Postgres Pro, состоящего как минимум из двух реплик.

При возникновении инцидента, требующего восстановления данных, выполняются работы по восстановлению БД. В зависимости от примененных мер по обеспечению сохранности информации в БД могут быть выполнены следующие действия:

1) Использование зеркальных копий данных.

2) Восстановление файлов базы данных с использованием последних резервных копий.

Приложение А
Шаблон информационных потоков между ИС и X-IDBox

Таблица 6 – Шаблон сетевого взаимодействия ИС и X-IDBox

Имя узла источника	IP-адрес сервера источника	Порт сервера источника	Имя сервера получателя	IP-адрес сервера получателя	Порт сервера получателя	Наименование сервиса	Функциональное назначение правил	Уровень конфиденциальности данных	Требования к целостности и авторству передаваемых данных
<Имя сервера с установленным модулем фильтрации запросов к ИС>	<IP-адрес сервера с установленным модулем фильтрации запросов к ИС>	1024-65535 TCP	<Имя сервера ИС>	<IP-адрес сервера ИС>	<Порт сервера ИС>	Маршрутизация аутентифицированного трафика до ИС	Маршрутизация аутентифицированного трафика до ИС	нет	нет
<Имя сервера ИС>	<IP-адрес сервера ИС>	1024-65535 TCP	<Имя сервера балансировщика нагрузки перед веб-серверами Nginx>	<IP-адрес сервера балансировщика нагрузки перед веб-серверами Nginx>	80 TCP	Запросы к сервисам X-IDBox	Запросы к сервисам X-IDBox	нет	нет

Приложение Б
Описание настроек сервисов

Б.1 Индивидуальные настройки стенда

Таблица 7 – Индивидуальные настройки стенда

Сервис	Техническое наименование	Обязательность	Значение по умолчанию	Пример	Назначение
Все сервисы	xidbox.eureka.service.url	Да	http://localhost:8096	http://xidboxeureka.dcs.infosec.ru:8096	URL на сервис xidbox-eureka
	xidbox.redis.spring.data.redis.host	Да	localhost	redis.xidbox.dcs.infosec.ru	Хост Redis. Redis используется для хранения кеша и сессий пользователей
xidbox-frontbackend xidbox-backend xidbox-orchestrator	xidbox.front.service.base.url	Да	http://localhost:8010	http://xidbox.dcs.infosec.ru	URL пользовательского интерфейса, который будет указываться в письмах, направляемых на адрес электронной почты УЗ пользователей и профилей УЗ пользователей
	xidbox.front.service.registration.url	Да	\${xidbox.front.service.base.url}/signin/create-password	\${xidbox.front.service.base.url}/signin/create-password	URL страницы для активации УЗ пользователя. Необходимо для уведомлений на активацию УЗ пользователя
	xidbox.front.service.set-password.url	Да	\${xidbox.front.service.base.url}/signin/create-password	\${xidbox.front.service.base.url}/signin/create-password	URL страницы для установки пароля УЗ пользователя. Необходимо для уведомлений на установку пароля УЗ пользователя
	xidbox.front.service.link.to.orders	Да	\${xidbox.front.service.base.url}/orders	\${xidbox.front.service.base.url}/orders	URL страницы карточки заявки. Необходимо для уведомлений с указанием ссылки на карточку заявки
	xidbox.front.service.link.to.email-confirmation	Да	\${xidbox.front.service.base.url}/signin/confirmed	\${xidbox.front.service.base.url}/signin/confirmed	URL для подтверждения адреса электронной почты УЗ пользователей и профилей УЗ пользователей
	xidbox.front.service.link.to.email-confirmation-2fa	Да	\${xidbox.front.service.base.url}/signin/confirmed/2fa	\${xidbox.front.service.base.url}/signin/confirmed/2fa	URL для подтверждения адрес электронной почты УЗ пользователей и профилей УЗ пользователей с последующей отправкой кода для двухфакторной аутентификации
xidbox-authentication	xidbox.session.domain-name.domain	Да	localhost	xidbox.dcs.infosec.ru	Домен для установки cookie, в т. ч. для установки сессии пользователя. Значение должно совпадать со значением переменной \$domain в xidbox.conf
	xidbox.redis.spring.data.redis.port	Да	6379	6379	Порт Redis. Redis используется для хранения кеша и сессий пользователей
xidbox-state-machine-queue	xidbox.state-machine-queue.service.spring.datasource.url	Да	jdbc:postgresql://localhost/state_machine_queue	jdbc:postgresql://xidboxdb.dcs.infosec.ru:5432/state_machine_queue	URL для подключения БД сервиса xidbox-state-machine-queue
	xidbox.state-machine-queue.service.spring.datasource.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-state-machine-queue

Сервис	Техническое наименование	Обязательность	Значение по умолчанию	Пример	Назначение
	xidbox.state-machine-queue.service.spring.datasource.password	Да	postgres	postgres	Пароль пользователя для подключения БД сервиса xidbox-state-machine-queue
xidbox-database	xidbox.database.service.spring.datasource.url	Да	jdbc:postgresql://localhost/x_idbox_database	jdbc:postgresql://xidboxdb.dcs.infosec.ru:5432/x_idbox_database	URL для подключения БД сервиса x-idbox-database-service
	xidbox.database.service.spring.datasource.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-database
	xidbox.database.service.spring.datasource.password	Да	postgres	postgres	Пароль пользователя для подключения БД сервиса xidbox-database
xidbox-scheduler	xidbox.scheduler.service.spring.datasource.url	Да	jdbc:postgresql://localhost/x_id_box_scheduler	jdbc:postgresql://xidboxdb.dcs.infosec.ru:5432/x_id_box_scheduler	URL для подключения БД сервиса xidbox-scheduler
	xidbox.scheduler.service.spring.datasource.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-scheduler
	xidbox.scheduler.service.spring.datasource.password	Да	postgres	postgres	Пароль пользователя для подключения БД сервиса x-idbox-scheduler-service
xidbox-state-machine-database	xidbox.state-machine-database.service.spring.datasource.url	Да	jdbc:postgresql://localhost/sm	jdbc:postgresql://xidboxdb.dcs.infosec.ru:5432/sm	URL для подключения БД сервиса xidbox-state-machine-database
	xidbox.state-machine-database.service.spring.datasource.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-state-machine-database
	xidbox.state-machine-database.service.spring.datasource.password	Да	postgres	postgres	Пароль пользователя для подключения БД сервиса xidbox-state-machine-database
xidbox-storage	xidbox.storage.service.spring.datasource.url	Да	jdbc:postgresql://localhost/storage	jdbc:postgresql://xidboxdb.dcs.infosec.ru:5432/storage	URL для подключения БД сервиса xidbox-storage
	xidbox.storage.service.spring.datasource.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-storage
	xidbox.storage.service.spring.datasource.password	Да	postgres	postgres	Пароль пользователя для подключения БД сервиса xidbox-storage
xidbox-order	xidbox.order.service.spring.datasource.url	Да	jdbc:postgresql://localhost/order	jdbc:postgresql://xidboxdb.dcs.infosec.ru:5432/order	URL для подключения БД сервиса xidbox-order
	xidbox.order.service.spring.datasource.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-order
	xidbox.order.service.spring.datasource.password	Да	postgres	postgres	Пароль пользователя для подключения БД сервиса xidbox-order
xidbox-role-politics-upload	xidbox.role-politics-upload.service.spring.datasource.url	Да	jdbc:postgresql://localhost/upload_role_queue	jdbc:postgresql://xidboxdb.dcs.infosec.ru:5432/upload_role_queue	URL для подключения БД сервиса xidbox-role-politics-upload
	xidbox.role-politics-upload.service.spring.datasource.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-role-politics-upload

Сервис	Техническое наименование	Обязательность	Значение по умолчанию	Пример	Назначение
	xidbox.role-politics-upload.service.spring.datasource.password	Да	postgres	postgres	Пароль пользователя для подключения БД сервиса xidbox-role-politics-upload
xidbox-request-background-processing	xidbox.request-background-processing.service.spring.datasource.url	Да	jdbc:postgresql://localhost/x_idbox_maintenance	jdbc:postgresql://xidboxdb.dcs.infosec.ru:5432/x_idbox_maintenance	URL для подключения БД сервиса xidbox-request-background-processing
	xidbox.request-background-processing.service.spring.datasource.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-request-background-processing
	xidbox.request-background-processing.service.spring.datasource.password	Да	postgres	postgres	Пароль для подключения БД сервиса xidbox-request-background-processing

Б.2 Обязательные настройки

Таблица 8 – Настройки, которые должны быть указаны в application.properties

Техническое наименование	Рекомендуемое значение	Назначение
xidbox.signature.required	false	Признак, отвечающий за требование пользователю подписывать с помощью ЭП пользовательские заявки. Значение «true» – если требуется ЭП и её валидация перед созданием пользовательских заявок. Значение «false» – если не требуется подпись, вместо ЭП система создает хеш-сумму. Алгоритм хеш-функции указывается в xidbox.signature.hash-sign-algorithm
xidbox.signature.allowed-algorithms	1.2.643.7.1.1.3.2, 1.2.643.7.1.1.3.3	Список OID алгоритмов создания ЭП. Если настройка не указана или значение не указано, то разрешается любой алгоритм, по которому должна быть создана ЭП при подписании пользовательских заявок, иначе допускается только тот алгоритм, OID которого указан в этой настройке
xidbox.signature.hash-sign-algorithm	SHA-512	Алгоритм хеширования. Допустимые значения: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512
xidbox.signature.use-hash-for-customer-signature	true	Признак регулирует необходимость рассчитывать хеш-сумму вместо обращения к сервису создания подписей (xidbox-signature) при создании пользовательских заявок, которые создаются анонимным пользователем. Пример заявок: сброс пароля
xidbox.signature.use-hash-for-technical-signature	true	Признак регулирует необходимость рассчитывать хеш-сумму вместо обращения к сервису создания подписей (xidbox-signature) при создании технических заявок, т. е. все заявки на загрузке сущностей, все побочные заявки
xidbox.user-certificate.max-count	2	Количество разрешённых сертификатов для входа по сертификату
xidbox.logger.mask-value-keys	password,oldPassword,newPassword	Список полей, значения которых необходимо маскировать при выводе в лог
xidbox.logger.mask-value-keys-in-response	password,oldPassword,newPassword,salt,clientSecret	Список полей, значения которых необходимо маскировать при выводе в лог
xidbox.logger.ignore-method-for-urls.<HTTP-метод>	–	Список методов, которые не будут логироваться, например: xidbox.logger.ignore-method-for-urls.GET[1]=/actuator/metrics/http.server.requests
xidbox.universal-token.set-password-by-user-reg	36000000	Срок действия токена, который позволяет установить пароль после регистрации УЗ пользователя, мс

Техническое наименование	Рекомендуемое значение	Назначение
xidbox.universal-token.set-password-by-reset-password	36000000	Срок действия токена, который позволяет установить пароля при его сбросе, мс
xidbox.universal-token.verify-user-email	36000000	Срок действия токена, который позволяет верифицировать почту УЗ пользователя, мс
xidbox.universal-token.verify-user-profile-work-email	36000000	Срок действия токена, который позволяет верифицировать почту профиля УЗ пользователя, мс

Б.3 Опциональные настройки

Таблица 9 – Опциональные настройки

Название	Значение по умолчанию	Назначение
xidbox.database.service.url	http://x-idbox-database-service	Схема и наименование группы экземпляров сервисов в xidbox-eureka, т. е. вместо конкретного хоста указывается наименование группы экземпляров сервисов
xidbox.crypto.service.url	http://x-idbox-crypto-service	
xidbox.orchestrator.service.url	http://x-idbox-orchestrator-service	
xidbox.storage.service.url	http://x-idbox-storage-service	
xidbox.order.service.url	http://x-idbox-order-service	
xidbox.authz.service.url	http://x-idbox-authorization-service	
xidbox.validation.service.url	http://x-idbox-validation-service	
xidbox.authentication.service.url	http://x-idbox-authentication-service	
xidbox.backend.service.url	http://x-idbox-backend-service	
xidbox.state-machine-database.service.url	http://x-idbox-state-machine-database-service	
xidbox.state-machine-queue.service.url	http://x-idbox-state-machine-queue-service	
xidbox.ldap.service.url	http://x-idbox-ldap-service	
xidbox.directory-synchronization.service.url	http://x-idbox-directory-synchronization-service	
xidbox.authentication.service.login-url-scheme.cert	https	Схема для URL с аутентификацией с помощью сертификата
xidbox.authentication.service.login-url-scheme.other	https	Схема для URL с аутентификацией различными способами (по логину и паролю, через Госуслуги (ЕСИА) и т. д.), кроме аутентификации с помощью сертификата
xidbox.session.spring.session.timeout	1800s	Срок жизни аутентифицированной сессии (поле sessionTTL из формата JWT)
xidbox.session.spring.session.for-authentication.timeout	300s	Срок жизни промежуточной сессии JSESSION (поле max-age)
xidbox.constraint-for-dto-fields.max-length	255	Ограничение максимальной длины полей. Настройка работает по умолчанию для тех полей, для которых явно не указаны иные ограничения
xidbox.info-system.tech-name	xidbox	Техническое наименование X-IDBox
xidbox.constraint-for-login.min-length	3	Минимально допустимая длина логина
xidbox.constraint-for-login.max-length	255	Максимально допустимая длина логина
xidbox.constraint-for-user-dynamic-field-value-max-length	255	Максимально допустимая длина значения динамического поля УЗ пользователя
xidbox.constraint-for-user-profile-dynamic-field-value-max-length	255	Максимально допустимая длина значения динамического поля профиля УЗ пользователя
xidbox.constraint-for-organization-dynamic-field-value-max-length	255	Максимально допустимая длина значения динамического поля организации
xidbox.constraint-for-role-attribute-value-max-length	255	Максимально допустимая длина значения роли атрибута
xidbox.constraint-for-host-max-length	255	Максимально допустимая длина значения хоста для входа
xidbox.pagination.internal.organization-max-limit	2001	Максимальное количество в результирующей выборке из таблицы организаций
xidbox.pagination.internal.user-max-limit	2001	Максимальное количество в результирующей выборке из таблицы УЗ пользователя
xidbox.pagination.internal.user-profile-max-limit	2001	Максимальное количество в результирующей выборке из таблицы профилей УЗ пользователя

Название	Значение по умолчанию	Назначение
xidbox.pagination.internal.role-max-limit	2001	Максимальное количество в результирующей выборке из таблицы ролей
xidbox.directory-sync.reg.user-profile.default-organization-uuid	–	Идентификатор организации, в которой необходимо регистрировать профиль УЗ пользователя при регистрации УЗ пользователя при синхронизации со службой каталогов
xidbox.directory-sync.check-ldap-user-state-before-auto-unblock	true	Признак, отвечающий за проверку с каталогом статуса УЗ пользователя перед автоматической разблокировкой УЗ пользователя. Значение «true» – если проверка осуществляется. Значение «false» – если проверка не осуществляется
xidbox.directory-sync.check-ldap-user-state-before-authentication	true	Признак, отвечающий за проверку с каталогом статуса УЗ пользователя перед аутентификацией. Значение «true» – если проверка осуществляется. Значение «false» – если проверка не осуществляется
xidbox.directory-sync.allow-user-state-change-from-permanent-to-temporarily-blocked	true	Признак, отвечающий за возможность разблокировать УЗ пользователя из постоянной блокировки во временную. Значение «true» – если проверка разрешена. Значение «false» – если проверка запрещена
xidbox.approval.roles	information_system_manager,account_manager,security_administrator,system_administrator	Список технических наименований допустимых ролей X-IDBox, которые могут участвовать в согласовании назначения ролей профилю УЗ пользователя
xidbox.authz.cache.disable-calculate-role-applicability	false	Признак отключения расчета применимости ролей. Значение «true» – если расчет применимости роли не производится. Значение «false» – если расчет применимости роли производится
xidbox.authz.cache.authz-multi-response-ttl	500s	TTL кеша ответа для API «Массовый авторизационный запрос»
xidbox.authz.cache.authz-attribute-response-ttl	500s	TTL кеша ответа для API «Получение списка ресурсных атрибутов, участвующих в авторизации»
xidbox.authz.cache.authz-resources-response-ttl	500s	TTL кеша ответа для API «Получение списка доступных ресурсов и действий для конкретного профиля УЗ пользователя»
xidbox.authz.cache.authz-available-info-systems-response-ttl	500s	TTL кеша ответа для API «Получение списка ИС, в которых у указанного профиля УЗ пользователя есть доступ»
xidbox.authz.cache.authz-conditions-response-ttl	500s	TTL кеша ответа для API «Получение списка условий для успешного прохождения авторизации»
xidbox.authz.cache.authz-reverse-user-profiles-response-ttl	500s	TTL кеша ответа для API «Получение списка профилей УЗ пользователя, для которых выполняется успешная авторизация для заданного ресурса и действия»
xidbox.authz.cache.authz-active-access-rules-by-user-profile-id-and-info-system-ttl	300s	TTL кеша правил доступов профиля УЗ пользователя по ИС, типам ресурсов и ресурсов
xidbox.authz.cache.cache-responses-for-all-info-systems	true	Признак регулирует, включен ли кеш ответов, или необходимо использовать xidbox.authz.cache.info-system-settings. Значение «true» – если кеш включен, настройки в xidbox.authz.cache.info-system-settings игнорируются. Значение «false» – если кеш регулируется только xidbox.authz.cache.info-system-settings
xidbox.authz.cache.info-system-settings.<техническое наименование ИС>	–	Указывается техническое наименование и включен ли кеш ответа. Если настройка для ИС не задана, то по умолчанию указано значение «false». Значение «true» – если кеш включен. Значение «false» – если кеш отключен
xidbox.authz.applicability.role.use-applicability-condition	true	Значение условия применимости по умолчанию

Название	Значение по умолчанию	Назначение
xidbox.authz.applicability.role.<техническое наименование типа ресурсов>	information_system_role_type	Техническое наименование типа ресурса и ресурс, которые используются для создания политик доступов применимости ролей
xidbox.authz.applicability.role.action	assignee	Техническое наименование действия, которое используется для создания политик доступов применимости ролей
xidbox.authz.applicability.role.info-system-and-role-delimiter	–	Разделитель, который используется для создания технического наименования условий применимости ролей
xidbox.authz.service.rate-limit.user-profiles-in-multiply-organizations.duration	1s	Длительность периода, в котором действует ограничение на количество запросов
xidbox.authz.service.rate-limit.user-profiles-in-multiply-organizations.limit	100	Ограничение на количество запросов (суммарно для всех экземпляров сервиса авторизации) для периода
xidbox.mail.view-order-link.method	LINK_AND_KEY	Настройка способа отображения номера и заявки в письмах. Значение подставляется в шаблон письма на место макроса %view_order_link_form_property%. Возможные значения настройки: – LINK – добавлять в письмо ссылку на заявку (см. настройку xidbox.mail.view-order-link.for-link); – LINK_AND_KEY – добавлять в письмо ссылку и номер заявки (см. настройку xidbox.mail.view-order-link.for-link-and-key); – KEY – добавлять в письмо номер заявки (см. настройку xidbox.mail.view-order-link.for-key); – NONE – не добавлять ссылку и номер заявки
xidbox.mail.view-order-link.for-link	Для просмотра заявки перейдите по ссылке.	Текст шаблона для отображения ссылки на заявку в письме
xidbox.mail.view-order-link.for-link-and-key	Номер заявки %ordr_key%. Для просмотра перейдите по ссылке.	Текст шаблона для отображения ссылки на заявку и её номер в письме
xidbox.mail.view-order-link.for-key	Номер заявки %ordr_key%.	Текст шаблона для отображения ссылки на заявку и ее номер в письме
xidbox.send-messages.check-email-verified	true	Признак необходимости верификации электронной почты перед отправкой сообщений. Значение «true» – если проверка требуется. Значение «false» – если проверка не требуется

Название	Значение по умолчанию	Назначение
xidbox.block-inactive-users.delay-before-block-updated-user	–	Длительность отложенного периода от даты последнего обновления перед блокировкой неактивных пользователей. Неактивный пользователь не будет блокироваться, пока с момента последнего изменения состояния УЗ не пройдет указанный период. Значение задается в виде строки, где: – Р – начало строкового представления длительности; – Т – разделяет временную часть (часы, минуты, секунды) от части с днями. Если присутствует только временная часть, Т все равно используется; – D – день; – H – час; – M – минута; – S – секунда. Например: – P1DT2H3M4S – 1 день, 2 часа, 3 минуты и 4 секунды. – P5D – 5 дней. – PT24H – 24 часа

Б.4 Настройки сервиса xidbox-authentication

Таблица 10 – Настройки сервиса xidbox-authentication

Название	Значение по умолчанию	Назначение
xidbox.authentication.service.async.threads	5	Количество потоков для обработки асинхронных запросов сервисом xidbox-authentication
xidbox.authentication.service.spring.session.redis.cleanup-cron	0 * * * * *	Выражение Cron для задания очистки истекшей сессии. Поддерживается только в том случае, если для типа репозитория установлено индексированное значение
xidbox.authentication.service.spring.session.redis.repository-type	indexed	Тип репозитория сессий в Redis
xidbox.authentication.service.kerberos.krb5	/app/kerberos/krb5.conf	Название файла конфигурации Kerberos
xidbox.authentication.service.kerberos.jaas	/app/kerberos/jaas.conf	Название файла конфигурации JAAS
xidbox.authentication.service.kerberos.jaas-profile-name	KerberosAcceptorWithTicket	Название используемого профиля из файла конфигурации JAAS
xidbox.authentication.service.esia.esia-version	v2	Используемая версия ЕСИА, например, v2 или v3
xidbox.authentication.service.esia.client-id	–	Идентификатор системы-клиента (X-IDBox) в ЕСИА
xidbox.authentication.service.esia.scope	openid snils inn email usr_org fullname	Область доступа, т. е. область доступа, т. е. запрашиваемые права
xidbox.authentication.service.esia.scope-org	openid	Область доступа, т. е. запрашиваемые права для юридических лиц
xidbox.authentication.service.esia.esia-domain	http://localhost:8090	Адрес сервера ЕСИА
xidbox.authentication.service.esia.client-certificate-hash	49F35F513FADF313C51C2BEDDADE68985857EDBFEA93E83DCFB2E67287CD2546	Отпечаток сертификата системы-клиента, которым подписывается client_secret
xidbox.authentication.service.esia.esia-certificate-alias	d9427172-de30-442b-98c1-13258007374a	Идентификатор сертификата (алиас хранилища) для подписи запросов в ЕСИА. Сертификат и хранилище должны быть доступны для сервиса, реализующего взаимодействие с СКЗИ
xidbox.authentication.service.esia.callback-uri-path	/signin/esia/callback	Путь адреса, по которому должен быть направлен пользователь, после того как даст разрешение на доступ к ресурсу
xidbox.authentication.service.esia.callback-uri-schema	http	Схема адреса, по которой должен быть направлен пользователь, после того как даст разрешение на доступ к ресурсу

Название	Значение по умолчанию	Назначение
xidbox.authentication.service.esia.person-filter	conf_acc	Необязательный параметр, позволяющий производить авторизацию только для определенных групп лиц, допустимые значения: conf_acc, acc_kid, acc_not_kid, conf_acc acc_kid
xidbox.authentication.service.esia.state-life-time-seconds	3600	Длительность жизни значений state в Redis, в секундах. State – набор случайных символов, имеющий вид 128-битного идентификатора запроса (необходимо для защиты от перехвата), генерируется по стандарту UUID
xidbox.authentication.service.esia.esia-access-type	offline	Тип доступа ЕСИА, возможные значения: Значение «offline» – если требуется иметь доступ, когда владелец не может быть вызван. Значение «online» – если доступ требуется только при наличии владельца
xidbox.authentication.service.esia.proxy-enable	false	Признак использования прокси при взаимодействии с ЕСИА. Возможные значения: Значение «true» – если прокси включено. Значение «false» – если прокси выключено
xidbox.authentication.service.esia.proxy-host	–	Прокси хост
xidbox.authentication.service.esia.proxy-port	0	Прокси порт
xidbox.authentication.service.jwt.jwt-certificate-alias	xidbox-auth-token	Идентификатор (алиас) сертификата для подписи JWT
xidbox.authentication.service.jwt.keystore-file	file:CI/jwt/xidbox-jwt.jks	Путь к хранилищу, где лежит ключ и сертификат для подписи JWT
xidbox.authentication.service.jwt.keystore-password	1qaz@WSX	Пароль от хранилища и приватного ключа
xidbox.authentication.service.jwt.refresh-ttl-second	30	Частота обновления токена, в секундах
xidbox.authentication.service.login-url-scheme.cert	https	Протокол URL-адреса входа для входа по сертификату
xidbox.authentication.service.login-url-scheme.other	https	Протокол URL-адреса входа для способов, отличных от входа по сертификату
xidbox.authentication.service.oauth2.login-entry-point	http://localhost/signin	URL страницы входа, необходим для перенаправления в случае необходимости аутентифицировать пользователя
xidbox.authentication.service.oauth2.consent-endpoint	http://localhost/signin/oauth2/consent	URL страницы подтверждения доступов
xidbox.authentication.service.oauth2.token-endpoint	/authentication/api/v1/oauth2/token	URL для получения токена авторизации и токена обновления по авторизационному коду
xidbox.authentication.service.oauth2.token-revocation-endpoint	/authentication/api/v1/oauth2/revoke	URL для отзыва токена авторизации и токена обновления
xidbox.authentication.service.oauth2.require-consent	true	Признак необходимости подтверждения пользователем доступов для внешней ИС. Значение «true» – если подтверждение необходимо. Значение «false» – если подтверждение не требуется
xidbox.authentication.service.oauth2.authorization-server-issuer	http://localhost:8085	URL, который используется в качестве идентификатора эмитента
xidbox.authentication.service.oauth2.authorization-endpoint	/authentication/api/v1/oauth2/authorize	URL для получения авторизационного кода
xidbox.authentication.service.oauth2.token-introspection-endpoint	/authentication/api/v1/oauth2/token-info	URL для проверки состояния токена
xidbox.authentication.service.oauth2.jwk-set-endpoint	/authentication/api/v1/oauth2/jwks	URL для получения набора публичных ключей OAuth2.0 сервера
xidbox.authentication.service.oauth2.oidc-user-info-endpoint	/authentication/api/v1/oauth2/userinfo	URL для получения данных пользователя, аутентифицированного через OpenId Connect 1.0
xidbox.authentication.service.oauth2.oidc-logout-endpoint	/authentication/api/v1/oauth2/logout	URL для выхода из OpenID Connect 1.0
xidbox.authentication.service.oauth2.authorization-grant-type[*]=	client_credentials	xidbox.authentication.service.oauth2.authorization-grant-type[0]=client_credentials xidbox.authentication.service.oauth2.authorization-grant-type[1]=authorization_code xidbox.authentication.service.oauth2.authorization-grant-type[2]=refresh_token
xidbox.authentication.service.oauth2.reuse-refresh-tokens	true	Признак разрешения переиспользования токенов обновления. Значение «true» – если переиспользование разрешено. Значение «false» – если переиспользование не разрешено
xidbox.authentication.service.oauth2.access-token-time-to-live-min	5	Длительность жизни токена доступа

Название	Значение по умолчанию	Назначение
xidbox.authentication.service.oauth2.refresh-token-time-to-live-min	60	Длительность жизни токена обновления
xidbox.authentication.service.oauth2.certificate-alias	xidbox-auth-token	Идентификатор (алиас) сертификата для подписи токенов доступа и обновления
xidbox.authentication.service.oauth2.keystore-file	file:CI/jwt/xidbox-jwt.jks	Путь к хранилищу, где лежит ключ и сертификат для подписи токенов доступа и обновления
xidbox.authentication.service.oauth2.keystore-password	1qaz@WSX	Пароль от хранилища и приватного ключа
xidbox.authentication.service.oauth2.require-reference-to-info-system	true	Признак, отвечающий за ограничение привязки клиентов к ИС
xidbox.authentication.service.oauth2.hosts.authorization-endpoint-host	–	Хост получения авторизационного кода, например: http://some-host Используется для генерации значения URL указанной конечной точки в API «Получение конфигурации OAuth 2.0 сервера» и «Получение конфигурации OpenId Connect 1.0». Если значение не указано, для генерации URL используется хост из xidbox.authentication.service.oauth2.authorization-server-issuer
xidbox.authentication.service.oauth2.hosts.token-endpoint-host	–	Хост получения токенов по коду, например: http://some-host Используется для генерации значения URL указанной конечной точки в API «Получение конфигурации OAuth 2.0 сервера» и «Получение конфигурации OpenId Connect 1.0». Если значение не указано, для генерации URL используется хост из xidbox.authentication.service.oauth2.authorization-server-issuer
xidbox.authentication.service.oauth2.hosts.token-revocation-endpoint-host	–	Хост для отзыва токена, например: http://some-host Используется для генерации значения URL указанной конечной точки в API «Получение конфигурации OAuth 2.0 сервера» и «Получение конфигурации OpenId Connect 1.0». Если значение не указано, для генерации URL используется хост из xidbox.authentication.service.oauth2.authorization-server-issuer
xidbox.authentication.service.oauth2.hosts.token-introspection-endpoint-host	–	Хост для проверки состояния токена, например: http://some-host Используется для генерации значения URL указанной конечной точки в API «Получение конфигурации OAuth 2.0 сервера» и «Получение конфигурации OpenId Connect 1.0». Если значение не указано, для генерации URL используется хост из xidbox.authentication.service.oauth2.authorization-server-issuer
xidbox.authentication.service.oauth2.hosts.jwk-set-endpoint-host	–	Хост для получения набора публичных ключей OAuth 2.0 сервера, например: http://some-host Используется для генерации значения URL указанной конечной точки в API «Получение конфигурации OAuth 2.0 сервера» и «Получение конфигурации OpenId Connect 1.0». Если значение не указано, для генерации URL используется хост из xidbox.authentication.service.oauth2.authorization-server-issuer
xidbox.authentication.service.oauth2.hosts.oidc-user-info-endpoint-host	–	Хост для получения данных пользователя аутентифицированного через OpenId Connect 1.0, например: http://some-host Используется для генерации значения URL указанной конечной точки в API «Получение конфигурации OAuth 2.0 сервера» и «Получение конфигурации OpenId Connect 1.0». Если значение не указано, для генерации URL используется хост из xidbox.authentication.service.oauth2.authorization-server-issuer

Название	Значение по умолчанию	Назначение
xidbox.authentication.service.oauth2.hosts.oidc-logout-endpoint-host	–	Хост для выхода из OpenID Connect 1.0, например: http://some-host Используется для генерации значения URL указанной конечной точки в API «Получение конфигурации OAuth 2.0 сервера» и «Получение конфигурации OpenId Connect 1.0». Если значение не указано, для генерации URL используется хост из xidbox.authentication.service.oauth2.authorization-server-issuer
xidbox.authentication.service.spring.security.oauth2.resourceserver.jwt.issuer-uri	http://localhost:8085	URI, который может быть конечной точкой обнаружения OpenID Connect или конечной точкой метаданных сервера авторизации OAuth 2.0, определенной в RFC 8414
xidbox.authentication.service.login.option.enable-someone-else-computer	false	Признак необходимости отображения на странице входа опцию «Чужой компьютер». Значение «true» – если необходимо отображать опцию. Значение «false» – если отображать не надо
xidbox.authentication.service.auth.types.external-request-header-name	–	Наименование заголовка запроса, наличие которого означает, что запрос на получение способов аутентификации ИС поступил из внешней сети. Используется для возможности разделения способов аутентификации для запросов из внешней и внутренней сети. Если значение не указано, то считается, что все запросы поступили из внутренней сети
xidbox.authentication.service.auth.types.excluded-auth-types-for-external-request.{info-system-tech-name}	–	Список способов аутентификации через запятую, которые нужно исключить для запросов из внешних сетей на получение способов аутентификации, где {info-system-tech-name} – техническое наименование ИС, для которой применяется настройка. Например, чтобы исключить способ входа по логину для запросов из внешних сетей для ИС X-IDBox: xidbox.authentication.service.auth.types.excluded-auth-types-for-external-request.xidbox=LOGIN
xidbox.authentication.service.auth.types.excluded-auth-types-for-internal-request.{info-system-tech-name}	–	Список способов аутентификации через запятую, которые нужно исключить для запросов из внутренней сети на получение способов аутентификации, где {info-system-tech-name} – техническое наименование ИС, для которой применяется настройка. Например, чтобы исключить способ входа по логину для запросов из внутренней сети для ИС X-IDBox: xidbox.authentication.service.auth.types.excluded-auth-types-for-internal-request.xidbox=LOGIN

Б.5 Настройки сервиса xidbox-state-machine-queue

Таблица 11 – Настройки сервиса xidbox-state-machine-queue

Название	Значение по умолчанию	Назначение
xidbox.state-machine-queue.service.spring.jpa.show-sql	true	Признак для вывода SQL-запросов, которые выполняются к БД x-idbox-state-machine-queue-service
xidbox.state-machine-queue.service.spring.jpa.properties.hibernate.default_schema	state_machine_queue	Наименование схемы, к которой подключается сервис x-idbox-state-machine-queue-service
xxidbox.state-machine-queue.service.spring.liquibase.liquibase-schema	changes	Схема создания и использования таблиц liquibase

Б.6 Настройки сервиса xidbox-role-politics-upload

Таблица 12 – Настройки сервиса xidbox-role-politics-upload

Название	Значение по умолчанию	Назначение
xidbox.role-politics-upload.service.file-processing.thread-count	1	Количество потоков, которые последовательно разбирают очередь файлов на загрузку ролевой модели или изменение ролевой модели. При указании значения 0 экземпляр сервиса не выполняет обработку файлов
xidbox.role-politics-upload.service.file-processing.update-queue-delay	500	Задержка между опросами количества свободных потоков и запроса новых файлов на загрузку, мс
xidbox.role-politics-upload.service.file-processing.restart-stuck-queue-enable	false	Признак необходимости перезапуска обработки зависших файлов. Значение «true» – если перезапуск включен. Значение «false» – если перезапуск отключен
xidbox.role-politics-upload.service.file-processing.restart-stuck-queue-delay	10000	Задержка между проверками зависших файлов для перезапуска, мс
xidbox.role-politics-upload.service.file-processing.allowed-file-processing-duration-before-restart-in-seconds	900	Допустимая длительность обработки файла до перезапуска, секунд
xidbox.role-politics-upload.service.file-processing.state-machine-processing-state-name	BEFORE_STOP	Название шага сценария загрузки ролевой модели, на котором необходимо начинать обработку файла
xidbox.role-politics-upload.service.folder.root	\${java.io.tmpdir}	Путь к папке, в которой хранятся временные файлы
xidbox.role-politics-upload.service.folder.roles	roles	Наименование папки с ролевой моделью, в которой хранятся временные файлы
xidbox.role-politics-upload.service.spring.jpa.show-sql	false	Признак для вывода SQL-запросов, которые выполняются к БД xidbox-state-machine-database. Значение «true» – если SQL-запросы выводятся. Значение «false» – если SQL-запросы не выводятся
xidbox.role-politics-upload.service.spring.jpa.properties.hibernate.default_schema	upload_role_queue	Наименование схемы, к которой подключается сервис x-idbox-database-service
xidbox.role-politics-upload.service.spring.liquibase.liquibase-schema	upload_role_queue_changes	Схема создания и использования таблиц liquibase

Б.7 Настройки сервиса xidbox-database

Таблица 13 – Настройки сервиса xidbox-database

Название	Значение по умолчанию	Назначение
xidbox.database.service.spring.jpa.show-sql	true	Признак для вывода SQL-запросов, которые выполняются к БД xidbox-database. Значение «true» – если SQL-запросы выводятся. Значение «false» – если SQL-запросы не выводятся
xidbox.database.service.spring.jpa.properties.hibernate.default_schema	x_id_box	Наименование схемы, к которой подключается сервис xidbox-database
xidbox.database.service.spring.liquibase.liquibase-schema	changes	Схема создания и использования таблиц liquibase

Б.8 Настройки сервиса xidbox-backend

Таблица 14 – Настройки сервиса xidbox-backend

Название	Значение по умолчанию	Назначение
xidbox.backend.service.spring.mail.host	xidboxmaildev.dcs.infosec.ru	Хост сервера для отправки сообщений
xidbox.backend.service.spring.mail.port	25	Порт сервера для отправки сообщений
xidbox.backend.service.spring.mail.default-encoding	UTF-8	Кодировка темы и тела сообщений
xidbox.backend.service.spring.mail.username	–	Логин для аутентификации в почтовом сервере
xidbox.backend.service.spring.mail.password	–	Пароль для аутентификации в почтовом сервере
xidbox.backend.service.mail.sende	noreply@infosec.ru	Адрес электронной почты, от имени которого будут отправляться сообщения
xidbox.backend.service.mail.threads	5	Количество потоков, которыми отправляются асинхронные сообщения в почтовый сервер
xidbox.backend.service.block.start-date.before-delay-sec	60	Допустимое расхождение между текущим временем и датой начала блокировки в секундах (в меньшую сторону)
xidbox.backend.service.block.start-date.after-delay-sec	15	Допустимое расхождение между текущим временем и датой начала блокировки в секундах (в большую сторону)
xidbox.backend.service.approval.allow-change-roles-to-blocked-profile	false	Признак, определяющий, разрешено ли назначать роли заблокированным профилям УЗ пользователей при загрузках назначения ролей. Значение «true» – если разрешено. Значение «false» – если запрещено
xidbox.backend.service.mail.ignore-for-send-order-type.<техническое наименование типа заявки>	–	Если в свойствах содержится тип заявки и техническое наименование шаблона, то сообщение по шаблону не отправляется. Вместо технического наименования шаблона допускается указать «*», тогда все сообщения для указанного типа заявки не будут отправляться
xidbox.backend.service.upload-batch.user-dynamic-field-descriptions-count	100	Количество обновляемых описаний динамических полей УЗ пользователя в побочных заявках при загрузке обновления описания динамических полей УЗ пользователя
xidbox.backend.service.upload-batch.user-profile-dynamic-field-descriptions-count	100	Количество обновляемых описаний динамических полей профиля УЗ пользователя в побочных заявках при загрузке обновления описания динамических полей профиля УЗ пользователя
xidbox.backend.service.upload-batch.organization-dynamic-field-descriptions-count	100	Количество обновляемых описаний динамических полей организаций в побочных заявках при загрузке обновления описания динамических полей организаций
xidbox.backend.service.mail.organizations-black-or-white-list	–	Список идентификаторов организаций для фильтрации по черному или белому списку при отправке уведомлений. При пустом значении параметра фильтрация не осуществляется
xidbox.backend.service.mail.use-organizations-white-list	false	Признак, определяющий, применяется ли белый список. Значение «true» – применяется белый список. Значение «false» – применяется черный список

Б.9 Настройки сервиса xidbox-frontbackend

Таблица 15 – Настройки сервиса xidbox-frontbackend

Название	Значение по умолчанию	Назначение
xidbox.frontbackend.service.spring.mail.host	xidboxmaildev.dcs.infosec.ru	Хост сервера для отправки сообщений

Название	Значение по умолчанию	Назначение
xidbox.frontbackend.service.spring.mail.port	25	Порт сервера для отправки сообщений
xidbox.frontbackend.service.spring.mail.default-encoding	UTF-8	Кодировка темы и тела сообщений
xidbox.frontbackend.service.spring.mail.username	–	Логин для аутентификации в почтовом сервере
xidbox.frontbackend.service.spring.mail.password	–	Пароль для аутентификации в почтовом сервере
xidbox.frontbackend.service.mail.template.allowable-macros.activation_href	\${xidbox.front.service.registration.url}?token=0052f40b-e12f-4fcb-ac23-988c2b4f539b	Значение макросов, которые подставляются при отправке тестовых сообщений
xidbox.frontbackend.service.mail.template.allowable-macros.user_name	Ivan Ivanovich	
xidbox.frontbackend.service.mail.template.allowable-macros.password_expiration_date	2021-01-20	
xidbox.frontbackend.service.mail.template.allowable-macros.order_href	\${xidbox.front.service.base.url}/orders/0052f40b-e12f-4fcb-ac23-988c2b4f539b	
xidbox.frontbackend.service.mail.template.allowable-macros.confirmation_href	\${xidbox.front.service.base.url}/confirmation/0052f40b-e12f-4fcb-ac23-988c2b4f539b	
xidbox.frontbackend.service.mail.template.allowable-macros.reject_reason	Some reason	
xidbox.frontbackend.service.mail.template.allowable-macros.ordr_type	Technical	
xidbox.frontbackend.service.mail.template.allowable-macros.ordr_key	RT 022341_20	
xidbox.frontbackend.service.mail.template.allowable-macros.two_factor_code	857413	
xidbox.frontbackend.service.mail.template.allowable-macros.reason	Scheduled vacation	
xidbox.frontbackend.service.mail.template.allowable-macros.blocking_until	21.01.2020 12:23:53	
xidbox.frontbackend.service.mail.template.allowable-macros.organization_short_name	Some organization	
xidbox.frontbackend.service.security.setting.dictionary-size-of-allowed-chars	30	Минимальный допустимый размер пароля
xidbox.frontbackend.service.security.setting.settings-names-for-anonymous	minLength,allowUniqueSymbolsSequence,minPasswordDifference	Список настроек безопасности, которые выводятся на пользовательский интерфейс для неаутентифицированного пользователя, при создании пароля
xidbox.frontbackend.service.block.start-date.before-delay-sec	60	Допустимое расхождение между текущим временем и датой начала блокировки в секундах (в меньшую сторону)
xidbox.frontbackend.service.block.start-date.after-delay-sec	15	Допустимое расхождение между текущим временем и датой начала блокировки в секундах (в большую сторону)
xidbox.frontbackend.service.to.file.pdf.font-size	12	Размер шрифта при выгрузке данных в формате .pdf
xidbox.frontbackend.service.to.file.pdf.font	fonts/times.ttf	Путь на ttf шрифта, который используется для выгрузки в формате .pdf
xidbox.frontbackend.service.export.max-user-count	2000	Максимальный размер выгрузки списка УЗ пользователей
xidbox.frontbackend.service.export.max-user-profile-count	2000	Максимальный размер выгрузки списка профилей УЗ пользователей
xidbox.frontbackend.service.export.max-organization-count	2000	Максимальный размер выгрузки списка организаций
xidbox.frontbackend.service.export.max-order-count	2000	Максимальный размер выгрузки списка заявок
xidbox.frontbackend.service.export.max-role-count	2000	Максимальный размер выгрузки списка ролей
xidbox.frontbackend.service.folder.root	\${java.io.tmpdir}	Полный путь к папке для хранения временных файлов
xidbox.frontbackend.service.folder.users	users	Название временной папки для файлов с данными пользователей для регистрации
xidbox.frontbackend.service.folder.roles	roles	Название временной папки для файлов с информацией о ролевой модели

Б.10 Настройки сервиса xidbox-scheduler

Таблица 16 – Настройки сервиса xidbox-scheduler

Название	Значение по умолчанию	Назначение
xidbox.scheduler.spring.jpa.show-sql	true	Признак для вывода SQL-запросов, которые выполняются к БД xidbox-scheduler. Значение «true» – если SQL-запросы выводятся. Значение «false» – если SQL-запросы не выводятся
xidbox.scheduler.service.spring.jpa.properties.hibernate.default_schema	x_id_box_scheduler	Наименование схемы, к которой подключается сервис xidbox-scheduler
xxidbox.scheduler.service.spring.liquibase.liquibase-schema	changes	Схема создания и использования таблиц liquibase
xidbox.scheduler.service.remove-expired-certificates.limit	5	Максимальное количество удаляемых из БД просроченных сертификатов за одно выполнение задачи
xidbox.scheduler.service.remove-expired-certificates.cron	0 5/15 * * * ? *	Срон выполнения задачи на удаление просроченных сертификатов
xidbox.scheduler.service.remove-expired-user-profile-roles.limit	5	Максимальное количество ролей, которые истекли, и необходимо снять их с профиля УЗ пользователя за одно выполнение задачи
xidbox.scheduler.service.remove-expired-user-profile-roles.cron	0 10/15 * * * ?	Срон выполнения задачи на снятие ролей с профиля УЗ пользователя, которые истекли
xidbox.scheduler.service.block-inactive-users.limit	5	Максимальное количество заблокированных неактивных УЗ пользователя за одно выполнение задачи
xidbox.scheduler.service.block-inactive-users.cron	0 0 2 * * ?	Срон выполнения задачи на блокировку неактивных УЗ пользователя
xidbox.scheduler.service.restart-state-machines.limit	5	Максимальное количество перезапусков КА, которые долгое время не меняли статус за одно выполнение задачи
xidbox.scheduler.service.restart-state-machines.cron	0 0 * * * ?	Срон выполнения задачи на перезапуск КА
xidbox.scheduler.service.restart-state-machines.max-work-duration	PT1H	Время в простое, при превышении которого КА требуется перезапуск
xidbox.scheduler.service.remove-expired-user-two-factor-codes.limit	10	Максимальное количество невостребованных кодов для двухфакторной аутентификации на удаление за одно выполнение задачи
xidbox.scheduler.service.remove-expired-user-two-factor-codes.cron	0 0 0 * * ?	Срон выполнения задачи на удаление невостребованных кодов для двухфакторной аутентификации
xidbox.scheduler.service.notify-about-coming-password-expiration.limit	10	Максимальное количество пользователей, которым будут отправлены сообщения о скором истечении срока действия пароля за одно выполнение задачи
xidbox.scheduler.service.notify-about-coming-password-expiration.cron	0 0 * * * ?	Срон выполнения задачи на отправку уведомлений о скором истечении срока действия пароля
xidbox.scheduler.service.block-user-profiles-in-inactive-organizations.limit	10	Максимальное количество заблокированных активных профилей УЗ пользователя в неактивных организациях за одно выполнение задачи
xidbox.scheduler.service.block-user-profiles-in-inactive-organizations.cron	0 */18 * * * ?	Срон выполнения задачи на блокирование активных профилей УЗ пользователя в неактивных организациях
xidbox.scheduler.service.synchronize-users-from-directory.cron	0 0 0 15 5 ?	Срон выполнения задачи на создание заявки на синхронизацию УЗ пользователя из каталога
xidbox.scheduler.service.remove-expired-tokens.limit	10	Максимальное количество просроченных токенов на удаление за одно выполнение задачи
xidbox.scheduler.service.remove-expired-tokens.cron	0 0 0 * * ?	Срон выполнения задачи на удаление просроченных токенов
xidbox.scheduler.service.remove-archived-user-profile-roles.limit	10	Максимальное количество архивных ролей на снятие с профиля УЗ пользователя за одно выполнение задачи
xidbox.scheduler.service.remove-archived-user-profile-roles.cron	0 15/15 * * * ?	Срон выполнения задачи на снятия архивных ролей с профиля УЗ пользователя
xidbox.scheduler.service.remove-user-profile-session-history.limit	10	Максимальное количество записей в истории сессий профилей УЗ пользователя на удаление за одно выполнение задачи
xidbox.scheduler.service.remove-user-profile-session-history.cron	0 0 * * * ?	Срон выполнения задачи на удаление записей в истории сессий профилей УЗ пользователя

Название	Значение по умолчанию	Назначение
xidbox.scheduler.service.remove-user-profile-session-history.outdated-period-in-days	730	Количество дней, по истечении которых запись в истории сессии считается к удалению
xidbox.scheduler.service.remove-expired-oauth-tokens.limit	10	Максимальное количество просроченных OAuth2.0 токенов, которые будут удалены за одно выполнение задачи
xidbox.scheduler.service.remove-expired-oauth-tokens.cron	0 0 0 * * ?	Срон выполнения задачи на удаление просроченных OAuth2.0 токенов
xidbox.scheduler.service.remove-expired-oauth-tokens.sleep-between-delete-next-pack	PT0S	Задержка между удалением следующего списка просроченных OAuth2.0 токенов
xidbox.scheduler.service.spring.quartz.properties.org.quartz.threadPool.threadCount	5	Количество потоков в пуле, должно быть равно количеству job + 3
xidbox.scheduler.service.spring.quartz.properties.org.quartz.jobStore.dataSource	x_id_box_scheduler	Схема, в которой хранятся таблицы для сервиса
xidbox.scheduler.service.spring.quartz.properties.org.quartz.jobStore.misfireThreshold	10000	Количество миллисекунд, в течение которых планировщик будет «ждать» триггер, чтобы пройти его в следующий раз, прежде чем он будет считаться «невыполненным»
xidbox.scheduler.service.spring.quartz.properties.org.quartz.jobStore.clusterCheckinInterval	5000	Частота (в миллисекундах), с которой этот экземпляр «регистрируется» с другими экземплярами кластера. Влияет на скорость обнаружения неудачных экземпляров
xidbox.scheduler.service.spring.quartz.properties.org.quartz.jobStore.isClustered	true	Признак, позволяющий включить кластеризацию Значение «true» – если кластеризация включена. Значение «false» – если кластеризация отключена
xidbox.scheduler.service.spring.quartz.properties.org.quartz.jobStore.dontSetAutoCommitFalse	false	Признак вызова setAutoCommit (false) для соединений, полученных из DataSource. Значение «true» – Quartz не будет вызывать setAutoCommit (false) для соединений, полученных из DataSource. Значение «false» – Quartz будет вызывать setAutoCommit (false) для соединений, полученных из DataSource
xidbox.scheduler.service.spring.datasource.hikari.maximum-pool-size	7	Максимальное количество потоков в пуле, должно быть на 5 больше, чем job

Б.11 Настройки сервиса xidbox-crypto

Таблица 17 – Настройки сервиса xidbox-crypto

Название	Значение по умолчанию	Назначение
xidbox.crypto.service.crl dp.ibm	true	Признак для включения настройки проверки точки распространения CRL (IBM). Значение «true» – если настройки проверки включены. Значение «false» – если настройки проверки отключены
xidbox.crypto.service.crl dp.ocsp	true	Признак для проверки ocsp (список отзыва сертификатов). Значение «true» – если проверка ocsp включена. Значение «false» – если проверка ocsp отключена
pxidbox.crypto.service.crl dp.path-to-dir-with-crls	/usr/local/share/ca-certificates/crls	Путь, где хранится актуальный список отозванных сертификатов
xidbox.crypto.service.crl dp.crl-urls	http://testca2012.cryptopro.ru/cdp/	URL для получения списка отозванных сертификатов
xidbox.signature-counter-agent.service.path	crypto/api/v1/cryptos	Часть пути
xidbox.crypto.service.sign.default-storage-alias	d9427172-de30-442b-98c1-13258007374a	Идентификатор (алиас) сертификата, которым будут подписываться данные по умолчанию. Пароль обязательно указывается через настройку xidbox.crypto.service.sign.storage-alias-password.<идентификатор сертификата>

Название	Значение по умолчанию	Назначение
xidbox.crypto.service.sign.storage-alias-password.<идентификатор сертификата>	<пароль>	Перечисление – идентификатор сертификата и пароль для доступа к закрытому ключу. Например: xidbox.crypto.service.sign.storage-alias-password.d9427172-de30-442b-98c1-13258007374a=1qaz@WSX

Б.12 Настройки сервиса xidbox-orchestrator

Таблица 18 – Настройки сервиса xidbox-orchestrator

Название	Значение по умолчанию	Назначение
xidbox.orchestrator.service.scenarios.fail-event-scenario-name	fail_event_scenario	Наименование сценария, который запускается в случае непредвиденной ситуации при выполнении КА
xidbox.orchestrator.service.scenarios.folder-path	scenario/json	Путь папки, в которой лежат сценарии, которые необходимо загрузить в БД
xidbox.orchestrator.service.scenarios.default-retry-delay-milliseconds	1000	Задержка между попытками повторить запрос по умолчанию. Для состояний, не реализующих вызов API
xidbox.orchestrator.service.instance.id	first orchestrator	Идентификатор конкретного экземпляра сервиса. Необходимо указывать уникальный для более ясного логирования в БД
xidbox.orchestrator.service.instance.primary-queue-thread-count	2	Количество потоков, обрабатывающих первичную очередь
xidbox.orchestrator.service.instance.primary-queue-delay	500	Задержка между опросами первичной очереди
xidbox.orchestrator.service.instance.secondary-queue-thread-count	2	Количество потоков, обрабатывающих вторичную очередь
xidbox.orchestrator.service.instance.secondary-queue-delay	500	Задержка между опросами вторичной очереди
xidbox.orchestrator.service.instance.pre-primary-queue-fill-factor	2	Коэффициент предварительного заполнения пула из первичной очереди (пул заполняется из расчета коэффициент, умноженный на количество потоков, для обработки первичной очереди)
xidbox.orchestrator.service.instance.pre-secondary-queue-fill-factor	2	Коэффициент предварительного заполнения пула из вторичной очереди (пул заполняется из расчета коэффициент, умноженный на количество потоков, для обработки вторичной очереди)
xidbox.orchestrator.service.instance.state-machine-check-event-count	10	Максимальное количество КА, для которых наступило событие, направленное во вторичную очередь
xidbox.orchestrator.service.instance.event-check-delay	500	Задержка между проверками наступления событий
xidbox.orchestrator.service.retry.api-millisec	1000,2000,30000,60000,120000,240000,480000,960000,1920000,3840000	Задержка между попытками повторить запрос по умолчанию. Для состояний, реализующих вызов API
xidbox.directory-sync.check-ldap-user-state-before-auto-unblock	true	Признак, отвечающих за проверку с каталогом статуса УЗ пользователя перед автоматической разблокировкой УЗ пользователя. Значение «true» – если проверка осуществляется. Значение «false» – если проверка не осуществляется

Б.13 Настройки сервиса xidbox-storage

Таблица 19 – Настройки сервиса xidbox-storage

Название	Значение по умолчанию	Назначение
xidbox.storage.service.spring.jpa.show-sql	true	Признак для вывода SQL-запросов, которые выполняются к БД xidbox-storage. Значение «true» – если SQL-запросы выводятся. Значение «false» – если SQL-запросы не выводятся
xidbox.storage.service.spring.jpa.properties.hibernate.default_schema	storage	Наименование схемы, к которой подключается сервис xidbox-storage
xidbox.storage.service.spring.liquibase.liquibase-schema	changes	Схема создания и использования таблиц liquibase

Б.14 Настройки сервиса xidbox-order

Таблица 20 – Настройки сервиса xidbox-order

Название	Значение по умолчанию	Назначение
xidbox.order.service.spring.jpa.show-sql	true	Признак для вывода SQL-запросов, которые выполняются к БД xidbox-order. Значение «true» – если SQL-запросы выводятся. Значение «false» – если SQL-запросы не выводятся
xidbox.order.service.spring.jpa.properties.hibernate.default_schema	ordr	Наименование схемы, к которой подключается сервис xidbox-order
xidbox.order.service.spring.liquibase.liquibase-schema	ordr_changes	Схема создания и использования таблиц liquibase

Б.15 Настройки сервиса xidbox-state-machine-database

Таблица 21 – Настройки сервиса xidbox-state-machine-database

Название	Значение по умолчанию	Назначение
xidbox.state-machine-database.service.spring.jpa.show-sql	true	Признак для вывода SQL-запросов, которые выполняются к БД xidbox-state-machine-database. Значение «true» – если SQL-запросы выводятся. Значение «false» – если SQL-запросы не выводятся
xidbox.state-machine-database.service.spring.jpa.properties.hibernate.default_schema	sm	Наименование схемы, к которой подключается сервис xidbox-state-machine-database
xidbox.state-machine-database.service.spring.liquibase.liquibase-schema	ordr_changes	Схема создания и использования таблиц liquibase

Б.16 Настройки сервиса xidbox-ldap

Таблица 22 – Настройки сервиса xidbox-ldap

Название	Значение для AD	Значение для FreeIpa	Значение для OpenLdap	Назначение
xidbox.ldap.service.spring.ldap.urls	–	–	–	URL на службу каталога
xidbox.ldap.service.spring.ldap.base	dc=xidbox,dc=dc,dc=infosec,dc=ru	dc=dc,dc=infosec,dc=ru	dc=xidbox,dc=dc,dc=infosec,dc=ru	Базовый суффикс, от которого должны происходить все операции

Название	Значение для AD	Значение для FreeIpa	Значение для OpenLdap	Назначение
xidbox.ldap.service.spring.ldap.username	cn=Admin,cn=Users,dc=xidbox,dc=dc,dc=infosec,dc=ru	uid=admin,cn=users,cn=accounts,dc=dc,dc=infosec,dc=ru	cn=admin,dc=xidbox,dc=dc,dc=infosec,dc=ru	Имя пользователя для подключения к службе
xidbox.ldap.service.spring.ldap.password=	–	–	–	Пароль для подключения к службе
xidbox.ldap.service.spring.ldap.base-environment.java.naming.ldap.attributes.binary=	objectGUID	–	–	Сопоставление типа атрибутов с его названием
xidbox.ldap.service.directory.source	AD	FreeIpa	OpenLdap	Вариант протокола: AD, FreeApi, OpenLdap
xidbox.ldap.service.directory.base	cn=Users	cn=users,cn=accounts	ou=Users	Суффикс для поиска УЗ пользователя
xidbox.ldap.service.lockout-duration.policies-base=	–	–	ou=policies	Путь до расположения политик в каталоге
xidbox.ldap.service.lockout-duration.password-policies-cn	objectClass=domain	–	cn=default	Название (CommonName) парольной политики
xidbox.ldap.service.lockout-duration.attribute-name	lockoutDuration	–	pwdLockoutDuration	Название атрибута, в котором хранится значение
xidbox.ldap.service.lockout-duration.update-frequency	1800000	1800000	1800000	Частота обновления политики продолжительности временного блокирования, мс
xidbox.ldap.service.openldap.filter	–	–	(objectclass=inetOrgPerson)	Дополнительный фильтр. Только для OpenLdap

Б.17 Настройки сервиса xidbox-organizational-structure

Таблица 23 – Настройки сервиса xidbox-organizational-structure

Название	Значение по умолчанию	Назначение
xidbox.organizational-structure.level-value-generation-step	10	Максимальная глубина сгенерированного уровня ОШС

Б.18 Настройки сервиса xidbox-signature

Таблица 24 – Настройки сервиса xidbox-signature

Название	Значение по умолчанию	Назначение
xidbox.signature-counter-agent.service.use-counter-agent-service=true	true	Признак, отвечающий за вызов внешней реализации методов данного сервиса. Значение «true» – если необходимо использовать реализацию внешнего сервиса. Значение «false» – если необходимо использовать собственную реализацию
xidbox.signature-counter-agent.service.url	http://x-idbox-crypto-service	Схема и наименование сервиса, реализацию которого необходимо использовать
xidbox.signature-counter-agent.service.path	crypto/api/v1/ryptos	Часть URL, по которому будет располагаться ожидаемая реализация

Б.19 Настройки сервиса xidbox-request-background-processing

Таблица 25 – Настройки сервиса xidbox-request-background-processing

Название	Значение по умолчанию	Назначение
xidbox.request-background-processing.service.spring.jpa.show-sql	true	Признак для вывода SQL-запросов, которые выполняются к БД xidbox-request-background-processing. Значение «true» – если SQL-запросы выводятся. Значение «false» – если SQL-запросы не выводятся
xidbox.request-background-processing.service.spring.jpa.properties.hibernate.default_schema	x_id_box	Наименование схемы, к которой подключается сервис xidbox-request-background-processing
xidbox.request-background-processing.service.spring.liquibase.liquibase-schema	changes	Схема создания и использования таблиц liquibase
xidbox.request-background-processing.service.authz-request.processing.thread-pool-size	1	Количество потоков на обработку групп авторизационных запросов (один на группу)
xidbox.request-background-processing.service.authz-request.processing.processing-thread-pool-size	25	Количество потоков для авторизационных запросов
xidbox.request-background-processing.service.authz-request.processing.group-key-delay	20s	Задержка при получении новой группы запросов на обработку
xidbox.request-background-processing.service.authz-request.processing.profile-batch-size	500	Размер списка профилей УЗ пользователей для последовательной обработки
xidbox.request-background-processing.service.authz-request.processing.repeat-on-failed	5	Количество повторений запроса, если сервис авторизации вернул ошибку
xidbox.request-background-processing.service.authz-request.processing.repeat-delay	5s	Задержка между попытками запроса к сервису авторизации в случае ошибки
xidbox.request-background-processing.service.authz-request.processing.max-request-count-to-authz-per-second	200	Максимально допустимое количество запросов к сервису авторизации в секунду. Рекомендуется выделять около 10% допустимой нагрузки сервиса авторизации на все экземпляры сервиса автоматических расчетов. Например: – Максимальная производительность сервиса авторизации – 2000 запросов в секунду. – Количество экземпляров сервиса автоматических расчетов – 2. – Рассчитанное значение свойств $2000 \cdot 10\% / 2 = 100$ запросов в секунду для каждого экземпляра
xidbox.request-background-processing.service.authz-request.processing.deleting-oldest-request-enabled	true	Признак необходимости удаления старых запросов и результатов расчетов. Значение «true» – если удаление включено Значение «false» – если удаление отключено
xidbox.request-background-processing.service.authz-request.processing.delete-oldest-request-delay	20s	Задержка между задачами удаления старых запросов
xidbox.request-background-processing.service.authz-request.processing.max-request-count-cache-size	20	Максимально допустимое количество запросов, для которых хранятся результаты
xidbox.request-background-processing.service.authz-request.processing.request-batch-size-for-delete	2	Размер списка запросов для удаления
xidbox.request-background-processing.service.authz-request.processing.result-batch-size-for-delete	1000	Размер списка результатов для удаления
xidbox.request-background-processing.service.authz-request.processing.result-batch-size-for-update	500	Размер списка результатов для обновления

Название	Значение по умолчанию	Назначение
xidbox.request-background-processing.service.authz-request.processing.restart-stuck-requests-group-enabled	true	Признак необходимости перезапуска зависших расчетов для групп запросов. Значение «true» – если перезапуск включен. Значение «false» – если перезапуск отключен
xidbox.request-background-processing.service.authz-request.processing.restart-stuck-requests-group-delay	20s	Задержка между задачами перезапуска зависших расчетов для групп запросов
xidbox.request-background-processing.service.authz-request.processing.allowed-requests-group-processing-stuck-duration-before-restart	5m	Допустимая длительность простоя в расчетах для групп запросов до перезапуска
xidbox.request-background-processing.service.spring.liquibase.contexts	default,partial_logic_replication	Контекст выполнения SQL-скриптов миграции, необходимых для работы сервиса. Допустимые варианты настроек: – default,partial_logic_replication – создает SQL-структуру для реплицированных таблиц, используется в случае, если можно настроить логическую репликацию Postgres по определенным столбцам; – default,full_logic_replication – создает SQL-структуру для реплицированных таблиц, используется в случае, если нельзя настроить логическую репликацию Postgres по определенным столбцам, а таблицы реплицируются целиком; – default – не создает SQL-структуру для реплицированных таблиц (не рекомендуется для использования, так как предполагается, что те таблицы, которые требуются для работы данного сервиса, будут созданы любыми другими внешними средствами или инструментами)

Б.20 Настройки сервиса xidbox-callback-kafka

Таблица 26 – Настройки сервиса xidbox-callback-kafka

Название	Значение по умолчанию	Назначение
xidbox.information-system-send-callback-kafka.service.setting.kafka-send-interrupt-timeout	1s	Время ожидания отправки запроса в топик Kafka

Б.21 Настройки, одинаковые для всех сервисов

Для возможности разграничить настройки каждой группы сервисов в общем «application.properties» файле используется префикс, который формируется по шаблону «xidbox<наименование сервиса>.service». Например, для настройки порта (название настройки «server.port») для сервиса «xidbox-database» необходимо использовать имя «xidbox.database.service.server.port», для сервиса «xidbox-backend» – «xidbox.backend.service.server.port=8093» и т. д. Данный префикс опущен в таблице 27.

Таблица 27 – Настройки, одинаковые для всех сервисов

Название	Значение по умолчанию	Назначение
server.port	В зависимости от сервиса	Номер порта, который прослушивает экземпляр сервиса
application.name	В зависимости от сервиса	Наименование сервиса
eureka.client.service-url.defaultZone	\${EUREKA_URI:\${xidbox.eureka.service.url}/eureka}	URI для взаимодействия с eureka

Название	Значение по умолчанию	Назначение
management.endpoints	Перечень значений приведен по адресу, указанному в столбце «Назначение»	Spring Boot Endpoint: https://docs.spring.io/spring-boot/reference/actuator/endpoints.html
server.max-http-request-header-size	1024	Максимальная длина значения header
syslog.host	Нет	Хост сервиса для сбора логов, например, graylog
syslog.port	Нет	Порт сервиса для сбора логов, например, graylog
logging.level.root	info	Уровень логирования по умолчанию
logging.level.*	Нет	Уровень логирования для конкретного пакета https://docs.spring.io/spring-boot/reference/features/logging.html
logging.rotation.max-file-size	Нет	Максимальный размер файла для ротации, например, 10MB
logging.rotation.max-archive-size-each-appender	Нет	Максимальный суммарный размер файлов в архиве, например, 1GB
logging.rotation.max-files-in-archive	Нет	Максимальное количество файлов в архиве, например, 100
logger.console.enabled	Нет	Признак для вывода логов в консоль. Значение «true» – если логи выводятся в консоль. Значение «false» – если логи не выводятся в консоль
spring.servlet.multipart.file-size-threshold	2KB	Порог, после которого файл записывается на диск
spring.servlet.multipart.max-request-size	2MB	Максимальный размер запроса
spring.servlet.multipart.max-file-size	2MB	Максимальный размер файла в запросе
logger.json-in-file	true	Выводит лог в формате .json, параметры: – timestamp – время лога; – message – сообщение лога; – logger_name – класс, который инициировал лог; – thread_name – название потока, в котором произошел лог; – level – уровень лога; – replicaName – наименование экземпляра сервиса; – appName – наименование сервиса; – appPort – порт, который слушает сервис. При значении «false» – вывод по шаблону «%d{yyyy-MM-dd HH:mm:ss.SSS} %highlight(\${LOG_LEVEL_PATTERN:-%5p}) %magenta(\${PID:- }) %green(---) [%15.15t] %cyan(%-40.40logger{39}) %green(:) %magenta(%X{Request-id}) %m %n»
authn-request-verification.request.header.trigger-name	xidbox-ext-request	Наименование заголовка – признака запроса из ИС для расчета контрольной суммы
authn-request-verification.request.header.timestamp-name	xidbox-request-timestamp	Наименование заголовка запроса, в котором передается дата и время запроса для расчета контрольной суммы
authn-request-verification.request.header.auth-id-name	xidbox-request-auth-id	Наименование заголовка запроса, в котором передается идентификатор отправившей запрос ИС для расчета контрольной суммы
authn-request-verification.request.header.checksum-name	xidbox-request-checksum	Наименование заголовка запроса, в котором передается контрольная сумма запроса
authn-request-verification.request.header.algorithm-name	xidbox-request-algorithm	Наименование заголовка запроса, в котором передается алгоритм расчета контрольной суммы
authn-request-verification.request.header.check-sign-off-name	xidbox-request-check-off	Наименование заголовка – признака отключения сверки контрольной суммы учитывается только при условии включенного режима разработчика (authn-request-verification.dev-mode = true)
authn-request-verification.timestamp-diff-sec	15	Максимально допустимая разница во времени запроса и сервера, в секундах. Используется для проверки заголовка timestamp для расчета контрольной суммы
authn-request-verification.disable-verification	false	Признак проверки контрольной суммы запроса. Значение «true» – если отключена проверка контрольной суммы запроса. Значение «false» – если включена проверка контрольной суммы запроса

Название	Значение по умолчанию	Назначение
authn-request-verification.authn-setting-protocol	http://	Протокол, по которому происходит запрос для получения данных для проверки контрольной суммы запроса
authn-request-verification.authn-setting-uri	x-idbox-database-service/database/api/v1/information/system/setting/authz-to-service?serviceTechName=	Путь, по которому происходит запрос для получения данных для проверки контрольной суммы запроса
authn-request-verification.content-cache-mode	–	Способ хранения тела запросов при расчете контрольной суммы: – RAM – оперативная память (или если свойство не указано); – HARD – жесткий диск; – HYBRID – смешанный, в зависимости от размера тела запроса и буфера (см. настройку authn-request-verification.content-cache-limit-m-b)
authn-request-verification.content-cache-limit-m-b	2	Размер буфера оперативной памяти для хранения контента (в МБ). Используется при authn-request-verification.content-cache-mode = HYBRID, если размер тела запроса меньше этого значения, то хранится в оперативной памяти, иначе на жестком диске
authn-request-verification.content-cache-tmp-path	temp	Путь к директории для хранения файлов с телом запроса. Обязательна для content-cache-mode = HARD или HYBRID
authn-request-verification.dev-mode	false	Признак включения/отключения режима разработчика при расчете контрольной суммы. Значение «true» – если режим включен, значение заголовка из настройки authn-request-verification.request.header.check-sign-off-name игнорируется, проверка хеш-суммы не производится. Значение «false» – если режим отключен
authn-request-verification.setting-update-interval-minute	30	TTL кеша настроек доступов ИС, указывается в минутах
authn-request-verification.response.header.timestamp-name	xidbox-response-timestamp	Наименование заголовка ответа, в котором передаются дата и время ответа при ответе на запрос
authn-request-verification.response.header.auth-id-name	xidbox-response-auth-id	Наименование заголовка ответа, в котором передается идентификатор ИС, отправившей запрос при ответе на запрос
authn-request-verification.response.header.checksum-name	xidbox-response-checksum	Наименование заголовка ответа, в котором передается контрольная сумма ответа
authn-request-verification.response.header.algorithm-name	xidbox-response-algorithm	Наименование заголовка ответа, в котором передается алгоритм расчета контрольной суммы

Б.22 Настройки, одинаковые для всех клиентов сервисов

Для возможности разграничить настройки каждой группы клиентской части сервисов в общем «application.properties» файле используется префикс, который формируется по шаблону «xidbox.<наименование сервиса>.client». Например, для настройки «connect-timeout» (название настройки «feign.connect-timeout») для сервиса «xidbox-database» необходимо использовать настройку «xidbox.database.client.feign.connect-timeout», для сервиса «xidbox-backend» – «xidbox.backend.client.feign.connect-timeout» и т. д. Данный префикс опущен в таблице 28.

Таблица 28 – Настройки, одинаковые для всех клиентов сервисов

Название	Значение по умолчанию	Назначение
feign.connect-timeout	60 сек	Время, в течение которого должно быть установлено соединение с сервером
feign.read-timeout	60 сек	Время, в течение которого сервер должен дать ответ

Приложение В
Дополнительные данные о событиях безопасности

В таблице 29 приведены все данные, сохраняемые в расширении записей о событиях безопасности. Те ключи, которые не предопределены в формате CEF, перечислены также в таблице 5.

Таблица 29 – Данные о событиях безопасности

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
Вход и выход из системы					
Событие аутентификации пользователя	USER_AUTHENTICATION	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует вход пользователя. Фиксируются следующие параметры: – идентификация типа события безопасности; – дата и время входа в систему; – результат попытки входа; – идентификатор, предъявленный при попытке доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор пользователя	Событие содержит атрибут, если возможно определить внутренний идентификатор УЗ пользователя. Атрибут содержит внутренний идентификатор пользователя, под которым была совершена попытка войти в систему	
		suser	Внешний идентификатор пользователя	Событие содержит атрибут, если невозможно определить внутренний идентификатор УЗ пользователя. Атрибут содержит внешний идентификатор, по которому пользователь пытался совершить вход. Фиксируемое значение: – при аутентификации по логину и паролю – Логин; – при аутентификации по сертификату – Токен; – при аутентификации с помощью доменной учётной записи с использованием протокола Kerberos – Ticket Kerberos	
		cs7Label	Фиксированное значение – authenticationType	–	
		cs7	Тип аутентификации	Возможные значения: – LOGIN_AUTHENTICATION – аутентификация по логину и паролю; – CERT_AUTHENTICATION – аутентификация по сертификату; – DOMAIN_AUTHENTICATION – аутентификация с помощью доменной учётной записи с использованием протокола Kerberos; – TWO_FA_AUTHENTICATION – двухфакторная аутентификация; – ESIA_AUTHENTICATION – аутентификация через Госуслуги (ЕСИА)	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
		reason	Причина	Если событие завершилось неуспешно – содержит сообщение об ошибке, переданное в ответе на запрос. Если событие завершилось успешно – содержит фиксированное значение «ОК»	
Событие авторизации пользователя	USER_AUTHORIZATION	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует каждый авторизационный запрос пользователя. Фиксируются следующие параметры: – идентификация типа события безопасности; – дата и время входа в систему; – результат попытки входа; – идентификатор, предъявленный при попытке доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который запрашивает разрешение на совершение действия с ресурсом	
		cs3Label	Фиксированное значение – infoSystemUid	–	
		cs3	Идентификатор ИС	ИС, к ресурсу которой запрашивается доступ	
		cs6Label	Фиксированное значение – resourceType	–	
		cs6	Техническое наименование типа ресурса	Техническое наименование типа ресурса, к которому запрашивается разрешение на совершение действия	
		cs5Label	Фиксированное значение – resource	–	
		cs5	Техническое наименование ресурса	Содержит техническое наименование ресурса, к которому запрашивается разрешение на совершение действия	
		act	Действие	Действие, выполнение которого запрашивает пользователь	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие выхода пользователя из системы	USER_LOGOUT	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует выход пользователя. Фиксируются следующие параметры: – идентификация типа события безопасности; – дата и время входа (выхода) в систему; – результат попытки входа (выхода); – идентификатор, предъявленный при попытке доступа
		suid	Идентификатор профиля УЗ пользователя	Внутренний идентификатор профиля УЗ пользователя, под которым пользователь осуществил попытку выхода	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Общие события в системе					
Действия привилегированных пользователей	ADMIN_ACTION	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует любые действия привилегированного пользователя. Привилегированными считаются пользователи с ролями:

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	– Системный администратор; – Администратор ИБ; – Менеджер информационной системы; – Менеджер учётных записей. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который внес изменения	
		suser	Фиксированное значение – System	Событие содержит атрибут, если невозможно определить внутренний идентификатор профиля УЗ пользователя	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор объекта, с которым было выполнено соответствующее действие	Возможные значения: – пусто – если возникла ошибка при попытке осуществления действия над объектом; – идентификатор УЗ пользователя; – идентификатор профиля УЗ пользователя; – идентификатор организации; – техническое наименование ИС; – идентификатор заявки; – идентификатор роли; – наименование настройки системы	
		act	Действие, которое совершил пользователь	Возможные значения: – VIEW – просмотр; – ADD – добавление новых данных; – UPDATE – изменение данных; – DELETE – удаление данных	
		request	Метод и URL, без тела запроса	–	
		outcome	Результат события	Возможные значения: – success – действие выполнилось успешно; – failure – при выполнении действия произошла ошибка	
Событие начала создания заявки на загрузку информации	DATA_LOADING_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на осуществление загрузки данных. Предусмотрена загрузка следующих видов данных: – загрузка пользователей; – загрузка профилей УЗ пользователей; – загрузка назначений ролей профилей УЗ пользователей; – загрузка изменений должностей профилей УЗ пользователей; – загрузка организаций; – загрузка изменений состояний организаций; – загрузка ролевой модели; – загрузка ОПС; – загрузка изменений уровней подразделений;
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициирует загрузку данных. Если загрузка данных была через API – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Загружаемые данные	Возможные значения: – USERS – загрузка пользователей; – PROFILES – загрузка профилей УЗ пользователей; – ROLES_ASSIGNMENT – загрузка назначений ролей профилей УЗ пользователей; – POSITIONS_ASSIGNMENT – загрузка изменений должностей профилей УЗ пользователей;	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
				– ORGANIZATIONS – загрузка организаций; – ORGANIZATIONS_STATUS – загрузка изменений состояний организаций; – ROLE_MODEL – загрузка ролевой модели; – ORGANIZATIONAL_STRUCTURE – загрузка ОИШС; – DEPARTMENT_LEVELS – загрузка изменений уровней подразделений; – DEPARTMENTS – загрузка изменений подразделений; – POSITIONS – загрузка изменений должностей; – INFO_SYSTEMS – загрузка ИС	– загрузка изменений подразделений; – загрузка изменений должностей. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на загрузку информации	DATA_LOADING_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на осуществление загрузки данных (событие логируется в момент создания соответствующей типу загрузки заявки). Предусмотрена загрузка следующих видов данных: – загрузка пользователей; – загрузка профилей УЗ пользователей; – загрузка назначений ролей профилей УЗ пользователей; – загрузка изменений должностей профилей УЗ пользователей; – загрузка организаций; – загрузка изменений состояний организаций; – загрузка ролевой модели; – загрузка ОИШС; – загрузка изменений уровней подразделений; – загрузка изменений подразделений; – загрузка изменений должностей. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициирует загрузку данных. Если загрузка данных была через API – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Загружаемые данные	Возможные значения: – USERS – загрузка пользователей; – PROFILES – загрузка профилей УЗ пользователей; – ROLES_ASSIGNMENT – загрузка назначений ролей профилей УЗ пользователей; – POSITIONS_ASSIGNMENT – загрузка изменений должностей профилей УЗ пользователей; – ORGANIZATIONS – загрузка организаций; – ORGANIZATIONS_STATUS – загрузка изменений состояний организаций; – ROLE_MODEL – загрузка ролевой модели; – ORGANIZATIONAL_STRUCTURE – загрузка ОИШС; – DEPARTMENT_LEVELS – загрузка изменений уровней подразделений; – DEPARTMENTS – загрузка изменений подразделений; – POSITIONS – загрузка изменений должностей	
		cs2Label	Фиксированное значение – objectId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой произошло событие	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
Событие загрузки информации	DATA_LOADING_FINISH			загрузки данных	Событие фиксирует осуществление загрузки данных (событие логируется в момент перехода соответствующей типу загрузки заявки в финальное состояние). Предусмотрена загрузка следующих видов данных: – загрузка пользователей; – загрузка профилей УЗ пользователей; – загрузка назначений ролей профилей УЗ пользователей; – загрузка изменений должностей профилей УЗ пользователей; – загрузка организаций; – загрузка изменений состояний организаций; – загрузка ролевой модели; – загрузка ОИШС; – загрузка изменений уровней подразделений; – загрузка изменений подразделений; – загрузка изменений должностей. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
		dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициирует загрузку данных. Если загрузка данных была через API – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Загружаемые данные	Возможные значения: – USERS – загрузка пользователей; – PROFILES – загрузка профилей УЗ пользователей; – ROLES_ASSIGNMENT – загрузка назначений ролей профилей УЗ пользователей; – POSITIONS_ASSIGNMENT – загрузка изменений должностей профилей УЗ пользователей; – ORGANIZATIONS – загрузка организаций; – ORGANIZATIONS_STATUS – загрузка изменений состояний организаций; – ROLE_MODEL – загрузка ролевой модели; – ORGANIZATIONAL_STRUCTURE – загрузка ОИШС; – DEPARTMENT_LEVELS – загрузка изменений уровней подразделений; – DEPARTMENTS – загрузка изменений подразделений; – POSITIONS – загрузка изменений должностей	
		cs2Label	Фиксированное значение – objectId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой произошло событие загрузки данных	
Событие выгрузки информации	DATA_EXPORT	outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	Событие фиксируется при попытке выгрузки информации. Фиксируются следующие параметры: – дата и время события безопасности; – идентификатор субъекта доступа,
		dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	
		source	Фиксированное значение – XIDBOX	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который выгружает данные	осуществляющего вывод информации на носитель информации
		cs4Label	Фиксированное значение – typeData	–	
		cs4	Наименование списка, который выгружается	Возможные значения: – users – список УЗ пользователей; – profiles – список профилей УЗ пользователей; – organizations – список организаций; – roles – список ролей; – orders – список заявок	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
События, связанные с УЗ пользователей					
Событие начала создания заявки на регистрацию УЗ пользователя	USER_REGISTRATION_OR DER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на регистрацию УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал создание заявки на регистрацию УЗ. Если идентификатор отсутствует (заявка на создание УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор регистрируемой УЗ пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на регистрацию УЗ пользователя	USER_REGISTRATION_OR DER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на регистрацию УЗ пользователя (событие логируется в момент создания заявки на регистрацию пользователя). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал создание заявки на регистрацию УЗ. Если идентификатор отсутствует (заявка на создание УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs1	Идентификатор УЗ пользователя	Идентификатор регистрируемой УЗ пользователя	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, созданной для регистрации пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие регистрации УЗ пользователя	USER_REGISTRATION	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует создание УЗ пользователя в системе (логировается в момент перехода заявки на регистрацию пользователя в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал создание заявки на регистрацию УЗ. Если идентификатор отсутствует (заявка на создание УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор созданной УЗ пользователя. Пустое значение, если событие завершилось неуспешно	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой произошло событие регистрации пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение данных УЗ пользователя	USER_DATA_CHANGE_OR DER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на изменение данных УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля пользователя, который инициировал создание заявки на изменение данных УЗ пользователя. Если идентификатор отсутствует (заявка на изменение данных УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs1	Идентификатор УЗ пользователя	Идентификатор УЗ пользователя, данные которой будут изменены	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение данных УЗ пользователя	USER_DATA_CHANGE_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на изменение данных УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал создание заявки на изменение данных УЗ пользователя. Если идентификатор отсутствует (заявка на изменение данных УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор УЗ пользователя, данные которой будут изменены	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, созданной для изменения данных УЗ пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения данных УЗ пользователя	USER_DATA_CHANGE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменение данных УЗ пользователя (логируется в момент перехода заявки на изменение данных УЗ пользователя в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал создание заявки на изменение данных УЗ пользователя. Если идентификатор отсутствует (заявка на изменение данных УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор УЗ пользователя, данные которой будут изменены	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение данных	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение/сброс пароля	PASSWORD_CHANGE_OR DER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на изменение/сброс пароля. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который изменяет/сбрасывает пароль. Если идентификатор отсутствует (заявка на изменение/сброс пароля была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор УЗ пользователя, у которой меняется/сбрасывается пароль	
		act	Действие над паролем	Возможные значения: – CHANGE – изменение пароля; – RESET – сброс пароля	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение/сброс пароля	PASSWORD_CHANGE_OR DER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на изменение/сброс пароля. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор УЗ пользователя, у которой меняется/сбрасывается пароль	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение/сброс пароля	
		act	Действие над паролем	Возможные значения: – CHANGE – изменение пароля; – RESET – сброс пароля	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения/сброса пароля	PASSWORD_CHANGE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменение/сброс пароля (логировается в момент перехода заявки на изменение/сброс пароля в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который изменяет/сбрасывает пароль. Если идентификатор отсутствует (заявка на изменение/сброс пароля была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор УЗ пользователя, у которой меняется/сбрасывается пароль	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение/сброс пароля	
		act	Действие над паролем	Возможные значения: – CHANGE – изменение пароля; – RESET – сброс пароля	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на блокирование/разблокирование УЗ пользователя	USER_BLOCKING_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на блокирование/временное блокирование/разблокирование УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который меняет состояние УЗ пользователя. Если идентификатор отсутствует (заявка на блокирование/разблокирование УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор блокируемой/разблокируемой УЗ пользователя	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		act	Действие с УЗ пользователя	Возможные значения: - PERMANENT_BLOCKED – постоянное блокирование; - TEMPORARILY_BLOCKED – временное блокирование; - ACTIVE – разблокирование	
		outcome	Результат события	Возможные значения: - success – событие завершилось успешно; - failure – событие завершилось неуспешно	
Событие создания заявки на блокирование/разблокирование УЗ пользователя	USER_BLOCKING_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на блокирование/временное блокирование/разблокирование УЗ пользователя. Фиксируются следующие параметры: - тип события безопасности; - дата и время события безопасности; - идентификационная информация источника события безопасности; - результат события безопасности; - субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который меняет состояние УЗ пользователя. Если идентификатор отсутствует (заявка на блокирование/разблокирование УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор блокируемой/разблокируемой УЗ пользователя	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается блокирование/разблокирование УЗ пользователя	
		act	Действие с УЗ пользователя	Возможные значения: - PERMANENT_BLOCKED – постоянное блокирование; - TEMPORARILY_BLOCKED – временное блокирование; - ACTIVE – разблокирование	
		outcome	Результат события	Возможные значения: - success – событие завершилось успешно; - failure – событие завершилось неуспешно	
Событие блокирования/разблокирования УЗ пользователя	USER_BLOCKING	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует блокирование/разблокирование УЗ пользователя (логируется в момент перехода заявки на блокирование/временное блокирование/разблокирование УЗ
		source	Фиксированное значение – XIDBOX	Источник события безопасности	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который меняет состояние УЗ пользователя. Если идентификатор отсутствует (заявка на блокирование/разблокирование УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	пользователя в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор блокируемой/разблокируемой УЗ пользователя	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит блокирование/разблокирование УЗ пользователя	
		act	Действие с УЗ пользователя	Возможные значения: – PERMANENT_BLOCKED – постоянное блокирование; – TEMPORARILY_BLOCKED – временное блокирование; – ACTIVE – разблокирование	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение списка сертификатов пользователя	USER_CERTIFICATES_OR DER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на добавление/удаление сертификата пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение сертификатов УЗ пользователя	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор УЗ пользователя, сертификаты которой будут изменены	
		act	Действие над сертификатами	Возможные значения: – ADD – добавление сертификатов; – REPLACE – изменение сертификатов; – DELETE – удаление сертификатов	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение списка сертификатов пользователя	USER_CERTIFICATES_OR DER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на добавление/удаление сертификата пользователя. Фиксируются следующие параметры:

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	– тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение сертификатов УЗ пользователя	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор УЗ пользователя, сертификаты которой будут изменены	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается изменение сертификатов	
		act	Действие над сертификатами	Возможные значения: – ADD – добавление сертификатов; – REPLACE – изменение сертификатов; – DELETE – удаление сертификатов	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения списка сертификатов пользователя	USER_CERTIFICATES	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует добавление/удаление сертификата пользователя (логируется в момент перехода заявки на изменение списка сертификатов УЗ пользователя в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение сертификатов УЗ пользователя	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор УЗ пользователя, сертификаты которой будут изменены	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение сертификатов	
		act	Действие над сертификатами	Возможные значения: – ADD – добавление сертификатов; – REPLACE – изменение сертификатов; – DELETE – удаление сертификатов	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
Событие начала создания заявки на синхронизацию УЗ пользователей с каталогом	USER_SYNCHRONIZATION_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на синхронизацию данных УЗ пользователей. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		source	Фиксированное значение – orderId	Источник события безопасности	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на синхронизацию УЗ пользователей с каталогом	USER_SYNCHRONIZATION_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на синхронизацию данных УЗ пользователей. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		source	Фиксированное значение – orderId	Источник события безопасности	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой ожидается событие сихронизации УЗ пользователей	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Синхронизация УЗ пользователей с каталогом	USER_SYNCHRONIZATION	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует синхронизацию данных УЗ пользователей (логировается в момент перехода заявки на синхронизацию УЗ пользователей из каталога в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой произошло событие сихронизации УЗ пользователей	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на логическое удаление УЗ пользователя/профиля УЗ пользователя	USER_LOGIC_DELETE_OR_DER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на логическое удаление УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности;
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал удаление УЗ пользователя/профиля УЗ пользователя	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs1Label	Фиксированное значение – objectUid	–	– результат события безопасности; – субъект доступа
		cs1	Идентификатор УЗ пользователя	Идентификатор удаляемой УЗ пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на логическое удаление УЗ пользователя/профиля УЗ пользователя	USER_LOGIC_DELETE_OR DER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на логическое удаление УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал удаление УЗ пользователя/профиля УЗ пользователя	
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор удаляемой УЗ пользователя	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой ожидается событие удаления УЗ пользователя/профиля УЗ пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие логического удаления УЗ пользователя/профиля УЗ пользователя	USER_LOGIC_DELETE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует логическое удаление УЗ пользователя (логируется в момент перехода заявки на логическое удаление УЗ пользователя в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал удаление УЗ пользователя/профиля УЗ пользователя	
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор удаленной УЗ пользователя	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой произошло событие удаления УЗ пользователя/профиля УЗ пользователя	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
События, связанные с профилями УЗ пользователей					
Событие начала создания заявки на регистрацию профиля УЗ пользователя	PROFILE_REGISTRATION_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на регистрацию профиля УЗ пользователя в системе. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	–	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал создание профиля УЗ пользователя. Если идентификатор отсутствует (заявка на создание профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор регистрируемого профиля УЗ пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на регистрацию профиля УЗ пользователя	PROFILE_REGISTRATION_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на регистрацию профиля УЗ пользователя в системе. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	–	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал создание профиля УЗ пользователя. Если идентификатор отсутствует (заявка на создание профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор регистрируемого профиля УЗ пользователя	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой ожидается событие регистрации профиля УЗ пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
Событие регистрации профиля УЗ пользователя	PROFILE_REGISTRATION	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует создание профиля УЗ пользователя в системе (логировается в момент перехода заявки на регистрацию профиля УЗ пользователя в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал создание профиля УЗ пользователя. Если идентификатор отсутствует (заявка на создание профиля УЗ пользователя была создана автоматически) – ключ «suid» в лог не записывается	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор созданного профиля УЗ пользователя. Пустое значение, если событие завершилось неуспешно	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой произошло событие регистрации профиля УЗ пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение данных профиля УЗ пользователя	PROFILE_DATA_CHANGE_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на изменение данных профиля УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение данных профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение данных профиля УЗ пользователя была создана автоматически) – ключ «suid» в лог пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, данные которого изменяются	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение данных профиля УЗ пользователя	PROFILE_DATA_CHANGE_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на изменение данных профиля УЗ пользователя. Фиксируются следующие параметры:

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	– тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение данных профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение данных профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, данные которого изменяются	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение данных	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения данных профиля УЗ пользователя	PROFILE_DATA_CHANGE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменения данных профиля УЗ пользователя (логировается в момент перехода заявки на изменение данных профиля УЗ пользователя в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение данных профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение данных профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, данные которого изменены	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение данных	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение должностей профиля УЗ пользователя	PROFILE_POSITIONS_CHANGE_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на изменение должностей профиля УЗ пользователя. Фиксируются следующие параметры:

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	– тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение данных профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение данных профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, должности которого изменяются	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение должностей профиля УЗ пользователя	PROFILE_POSITIONS_CHANGE_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на изменение должностей профиля УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение данных профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение данных профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, должности которого изменяются	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение должностей	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения должностей профиля УЗ пользователя	PROFILE_POSITIONS_CHANGE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменения должностей профиля УЗ пользователя (логируется в момент перехода заявки на изменение должностей профиля УЗ пользователя в финальное состояние). Фиксируются следующие параметры:
		source	Фиксированное значение – XIDBOX	Источник события безопасности	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение данных профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение данных профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	– тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, должности которого изменены	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение должностей	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на блокирование/разблокирование профиля УЗ пользователя	PROFILE_BLOCKING_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на блокирование/временное блокирование/разблокирование профиля УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который меняет состояние профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение состояния профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор блокируемого/разблокируемого профиля УЗ пользователя	
		act	Действие с профилем УЗ пользователя	Возможные значения: – PERMANENT_BLOCKED – постоянное блокирование; – TEMPORARILY_BLOCKED – временное блокирование; – ACTIVE – разблокирование	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на блокирование/разблокирование профиля УЗ пользователя	PROFILE_BLOCKING_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на блокирование/временное блокирование/разблокирование профиля УЗ пользователя.

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который меняет состояние профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение состояния профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор блокируемого/разблокируемого профиля УЗ пользователя	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается блокирование/разблокирование профиля УЗ пользователя	
		act	Действие с профилем УЗ пользователя	Возможные значения: – PERMANENT_BLOCKED – постоянное блокирование; – TEMPORARILY_BLOCKED – временное блокирование; – ACTIVE – разблокирование	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие блокирования/разблокирования профиля УЗ пользователя	PROFILE_BLOCKING	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует блокирование/разблокирование профиля УЗ пользователя (логируется в момент перехода заявки на блокирование/временное блокирование/разблокирование профиля УЗ пользователя в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который меняет состояние профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение состояния профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор блокируемого/разблокируемого профиля УЗ пользователя	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит блокирование/разблокирование профиля УЗ пользователя	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		act	Действие с профилем УЗ пользователя	Возможные значения: - PERMANENT_BLOCKED – постоянное блокирование; - TEMPORARILY_BLOCKED – временное блокирование; - ACTIVE – разблокирование	
		outcome	Результат события	Возможные значения: - success – событие завершилось успешно; - failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение ролей профиля УЗ пользователя	PROFILE_ROLE_CHANGE_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на назначение/изменение/снятие ролей профиля УЗ пользователя. Фиксируются следующие параметры: - тип события безопасности; - дата и время события безопасности; - идентификационная информация источника события безопасности; - результат события безопасности; - субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который меняет роли профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение ролей профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, у которого меняются роли	
		outcome	Результат события	Возможные значения: - success – событие завершилось успешно; - failure – событие завершилось неуспешно	
Событие создания заявки на изменение ролей профиля УЗ пользователя	PROFILE_ROLE_CHANGE_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на назначение/изменение/снятие ролей профиля УЗ пользователя. Фиксируются следующие параметры: - тип события безопасности; - дата и время события безопасности; - идентификационная информация источника события безопасности; - результат события безопасности; - субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который меняет роли профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение ролей профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, у которого меняются роли	
		cs2Label	Фиксированное значение – orderId	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение ролей профиля УЗ пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения ролей профиля УЗ пользователя	PROFILE_ROLE_CHANGE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует назначение/изменение/снятие ролей профиля УЗ пользователя (логируется в момент перехода заявки на изменение ролей профиля УЗ пользователя в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который меняет роли профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение ролей профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, у которого меняются роли	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение ролей профиля УЗ пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на завершение сессий профиля УЗ пользователя	PROFILE_SESSIONS_END_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на завершение сессий профиля УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который завершает сессии профиля УЗ пользователя	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, сессии которого будут завершены	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
Событие создания заявки на завершение сессий профиля УЗ пользователя	PROFILE_SESSIONS_END_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на завершение сессий профиля УЗ пользователя. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который завершает сессии профиля УЗ пользователя	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, сессии которого были завершены	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается завершение сессий	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие завершения сессий профиля УЗ пользователя	PROFILE_SESSIONS_END	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует завершение сессий профиля УЗ пользователя (если завершение сессий сопровождается созданием заявки, то событие логируется в момент перехода заявки на завершение сессий пользователя в финальное состояние; если завершение сессий происходит без создания заявки (пользователь завершает сессии собственного профиля УЗ пользователя), то событие логируется в момент завершения сессий). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который завершает сессии профиля УЗ пользователя	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, сессии которого были завершены	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит завершение сессий. Если заявка отсутствует (пользователь завершил свои сессии) – пустое значение	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
События, связанные с организациями					
Событие начала создания заявки на регистрацию организации	ORGANIZATION_REGISTRATION_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на регистрацию организации в системе. Фиксируются следующие параметры:

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	– тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор организации	Идентификатор регистрируемой организации	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на регистрацию организации	ORGANIZATION_REGISTRATION_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на регистрацию организации в системе. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор организации	Идентификатор регистрируемой организации	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой ожидается событие регистрации организации	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие регистрации организации	ORGANIZATION_REGISTRATION	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует создание организации в системе (логируется в момент перехода заявки на регистрацию организации в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор организации	Идентификатор созданной организации. Пустое значение, если событие завершилось неуспешно	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой произошло событие регистрации организации	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение организации	ORGANIZATION_CHANGE_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на изменение данных организации в системе. Фиксируются следующие параметры:

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	– тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор организации	Идентификатор организации, данные которой меняются	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение организации	ORGANIZATION_CHANGE_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на изменение данных организации в системе. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор организации	Идентификатор организации, данные которой меняются	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой ожидается событие изменения данных организации	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения организации	ORGANIZATION_CHANGE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменение данных организации в системе (логировается в момент перехода заявки на изменение данных организации в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs1Label	Фиксированное значение – objectUid	–	
		cs1	Идентификатор организации	Идентификатор организации, данные которой меняются. Пустое значение, если событие завершилось неуспешно	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие изменения данных организации	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на блокирование организации	ORGANIZATION_BLOCKING_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на блокирование организации в системе. Фиксируются следующие параметры:

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	– тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициирует создание заявки на блокирование организации	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор организации	Идентификатор организации, данные которой меняются. Пустое значение, если событие завершилось неуспешно	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие изменения данных организации	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на блокирование организации	ORGANIZATION_BLOCKING_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на блокирование организации в системе. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал создание заявки на блокирование организации	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор организации	Идентификатор организации, данные которой меняются. Пустое значение, если событие завершилось неуспешно	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие изменения данных организации	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие блокирования организации	ORGANIZATION_BLOCKING	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует блокирование организации в системе (логировается в момент перехода заявки на блокирование организации в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности;
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал блокирование организации	
		cs1Label	Фиксированное значение – objectId	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs1	Идентификатор организации	Идентификатор организации, данные которой меняются. Пустое значение, если событие завершилось неуспешно	– результат события безопасности
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие изменения данных организации	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
События, связанные с ролевой моделью, ролями и 3О					
Событие начала создания заявки на загрузку ролевой модели	ROLE_MODEL_LOADING_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на загрузку ролей и 3О. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал процесс работы с 3О	
		cs3Label	Фиксированное значение – infoSystemUid	–	
		cs3	Техническое наименование (мнемоника) ИС	ИС, которой загружается ролевая модель	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на загрузку ролевой модели	ROLE_MODEL_LOADING_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на загрузку ролей и 3О. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал процесс работы с 3О	
		cs3Label	Фиксированное значение – infoSystemUid	ИС, которой загружается ролевая модель	
		cs3	Техническое наименование (мнемоника) ИС	ИС, которой загружается ролевая модель	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой ожидается загрузка ролевой модели	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
Событие завершения процесса работы с 3О	ROLE_MODEL_LOADING_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на загрузку ролей и 3О (логируется в момент перехода заявки на загрузку ролей и 3О в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал процесс работы с 3О	
		cs3Label	Фиксированное значение – infoSystemUid	ИС, которой загружается ролевая модель	
		cs3	Техническое наименование (мнемоника) ИС	ИС, которой загружается ролевая модель	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается загрузка ролевой модели	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение ролевой модели	ROLE_MODEL_CHANGE_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на изменение ролевой модели. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициирует создание заявки, в рамках которой изменяется ролевая модель. Если загрузка данных была через API – ключ «suid» в логе пустой	
		cs3Label	Фиксированное значение – infoSystemUid	–	
		cs3	Техническое наименование (мнемоника) ИС	ИС, у которой меняется ролевая модель	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение ролевой модели	ROLE_MODEL_CHANGE_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на изменение ролевой модели. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности;
		source	Фиксированное значение – XIDBOX	Источник события безопасности	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициирует создание заявки, в рамках которой изменяется ролевая модель. Если загрузка данных была через API – ключ «suid» в логе пустой	– идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		cs3Label	Фиксированное значение – infoSystemUid	–	
		cs3	Техническое наименование (мнемоника) ИС	ИС, у которой меняется ролевая модель	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается изменение ролевой модели	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения ролевой модели	ROLE_MODEL_CHANGE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменение ролевой модели (логировается в момент перехода заявки на изменение ролей и ЗО в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициирует создание заявки, в рамках которой изменяется ролевая модель. Если загрузка данных была через API – ключ «suid» в логе пустой	
		cs3Label	Фиксированное значение – infoSystemUid	–	
		cs3	Техническое наименование (мнемоника) ИС	ИС, у которой меняется ролевая модель	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло изменение ролевой модели	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение роли	ROLE_CHANGE_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на изменение данных роли. Фиксируются следующие параметры: – тип события безопасности; – дата и время события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение роли	безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор роли	Идентификатор измененной роли	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение роли	ROLE_CHANGE_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на изменение данных роли. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение роли	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор роли	Идентификатор измененной роли	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается событие изменения данных роли	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения роли	ROLE_CHANGE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменение данных роли (логировается в момент перехода заявки на изменение данных роли в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение роли	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор роли	Идентификатор измененной роли	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие изменения данных роли	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
События, связанные с ИС					

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
Событие начала создания заявки на регистрацию ИС	IS_REGISTRATION_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на регистрацию ИС. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал создание заявки на регистрацию ИС	
		cs3Label	Фиксированное значение – infoSystemUid	–	
		cs3	Идентификатор ИС	ИС, которую регистрируют	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на регистрацию ИС	IS_REGISTRATION_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на регистрацию ИС. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал регистрацию ИС	
		cs3Label	Фиксированное значение – infoSystemUid	–	
		cs3	Идентификатор ИС	ИС, которую регистрируют	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается событие регистрации ИС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие регистрации ИС	IS_REGISTRATION	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует создание ИС (логируется в момент перехода заявки на регистрацию ИС в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	–	Идентификатор профиля УЗ пользователя, который инициировал регистрацию ИС	
		cs3Label	Фиксированное значение – infoSystemUid	–	
		cs3	Идентификатор ИС	ИС, которую регистрируют	
		cs2Label	Фиксированное значение – orderId	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие создания ИС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение ИС	IS_CHANGE_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на изменение данных ИС. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение данных ИС	
		cs3Label	Фиксированное значение – infoSystemUid	–	
		cs3	Идентификатор ИС	ИС, которая изменяется	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение ИС	IS_CHANGE_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на изменение данных ИС. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение данных ИС	
		cs3Label	Фиксированное значение – infoSystemUid	–	
		cs3	Идентификатор ИС	ИС, которая изменяется	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается изменение ИС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения ИС	IS_CHANGE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменение данных ИС (логировается в момент перехода заявки на изменение ИС в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности;
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение данных ИС	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs3Label	Фиксированное значение – infoSystemUid	–	– идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		cs3	Идентификатор ИС	ИС, которая изменяется	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло изменение ИС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
События, связанные с ОШС					
Событие начала создания заявки на создание ОШС	ORG_STRUCTURE_REGISTRATION_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на создание ОШС у организации. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор организации	Идентификатор организации, для которой создавалась ОШС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на создание ОШС	ORG_STRUCTURE_REGISTRATION_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на создание ОШС у организации. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор организации	Идентификатор организации, для которой создавалась ОШС	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается событие создания ОШС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания ОШС	ORG_STRUCTURE_REGISTRATION	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует создание ОШС у организации (логируется в момент перехода заявки на загрузку ОШС в финальное состояние).

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор организации	Идентификатор организации, для которой создавалась ОШС	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие создания ОШС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение ОШС	ORG_STRUCTURE_CHANGE_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на изменение подразделений/должностей/уровней подразделений у организации. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор организации	Идентификатор организации, для которой изменяется ОШС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение ОШС	ORG_STRUCTURE_CHANGE_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на изменение подразделений/должностей/уровней подразделений у организации. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор организации	Идентификатор организации, для которой изменяется ОШС	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается событие изменения ОШС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
Событие изменения ОШС	ORG_STRUCTURE_CHANGE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменения подразделений/должностей/уровней подразделений у организации (логируется в момент перехода заявки на загрузку ОШС в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор организации	Идентификатор организации, для которой изменяется ОШС	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие изменения ОШС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
События, связанные с настройками системы					
Событие начала создания заявки на изменение настроек безопасности	SECURITY_SETTINGS_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует начало создания заявки на изменение настроек безопасности. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение настроек безопасности	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение настроек безопасности	SECURITY_SETTINGS_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует создание заявки на изменение настроек безопасности. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение настроек безопасности	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается изменение настроек безопасности	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
Событие изменения настроек безопасности	SECURITY_SETTINGS	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменение настроек безопасности (логировается в момент перехода заявки на изменение настроек безопасности в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение настроек безопасности	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло изменение настроек безопасности	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение списка разрешенных УЦ	CERTIFICATES_SETTINGS_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент начала создания заявки на изменение списка разрешенных УЦ. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение списка УЦ	
		act	Действие с УЦ	Возможные значения: – ADD – добавление УЦ; – DELETE – удаление УЦ	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение списка разрешенных УЦ	CERTIFICATES_SETTINGS_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на изменение списка разрешенных УЦ. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение списка УЦ	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается событие изменения списка УЦ	
		act	Действие с УЦ	Возможные значения: – ADD – добавление УЦ; – DELETE – удаление УЦ	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения списка разрешенных УЦ	CERTIFICATES_SETTINGS	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует изменение списка разрешенных УЦ (логировается в момент перехода заявки на изменение списка разрешенных УЦ в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение списка УЦ	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие изменения списка УЦ	
		act	Действие с УЦ	Возможные значения: – ADD – добавление УЦ; – DELETE – удаление УЦ	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение шаблона уведомления	TEMPLATES_SETTINGS_ORDER_CREATE_START	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует начало создания заявки на добавление/изменение/удаление шаблона уведомления. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение шаблонов уведомлений	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на изменение шаблона уведомления	TEMPLATES_SETTINGS_ORDER_CREATE_FINISH	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент создания заявки на добавление/изменение/удаление шаблона уведомления. Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение шаблонов уведомлений	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается событие изменения шаблонов уведомлений	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения шаблона уведомления	TEMPLATES_SETTINGS	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует добавление/изменение/удаление шаблона уведомления (логировается в момент перехода заявки на изменение шаблонов уведомлений в финальное состояние). Фиксируются следующие параметры: – тип события безопасности; – дата и время события безопасности; – идентификационная информация источника события безопасности; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который инициировал изменение шаблонов уведомлений	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие изменения шаблонов уведомлений	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	

Лист регистрации изменений

Версия	Изменения
1.0.0	Начальная версия
1.0.1	В раздел администрирования системы добавлено описание подключения ИС OAuth 2.0-клиента в X-IDBox и описание настроек отправки уведомлений ИС
	В описании настроек сервисов дополнены настройки сервисов: xidbox-authentication, xidbox-backend, xidbox-callback-kafka и обязательная настройка
1.0.2	В описание подключения ИС OAuth 2.0-клиента в X-IDBox добавлен необязательный параметр post_logout_redirect_url
	В описании настроек сервисов дополнены настройки сервиса xidbox-authentication
1.0.3	В описании настроек сервисов дополнены настройки сервисов: xidbox-authentication, xidbox-backend и дополнительная настройка блокировки неактивных пользователей
1.0.4	Добавлено описание правил выборки подотчётных организаций
	В описании настроек сервисов дополнены настройки сервиса xidbox-scheduler
	В описание подключения ИС добавлена необходимость запроса данных о подключаемой ИС и файл-шаблон с перечнем требуемой информации
	В раздел настройки ППО «Пользовательский интерфейс аутентификации» добавлено описание возможностей кастомизации интерфейса
1.0.5	В описании подключения ИС OAuth 2.0-клиента в X-IDBox дополнены возможные значения области доступа (scope)
	В описании настроек сервисов дополнены настройки сервиса xidbox-request-background-processing