



**платформа аутентификации и управления
доступом**

Руководство администратора

Листов 229

Содержание

Содержание	2
Перечень сокращений	12
Перечень терминов.....	13
Перечень электронных приложений	17
1. Общие сведения	18
1.1. Назначение и функции X-IDBox	18
1.2. Функциональные роли	19
1.3. Состав комплекта дистрибутивов ПО X-IDBox	20
2. Условия применения	24
2.1. Требования к серверной части	24
2.2. Требования к АРМ пользователя	24
2.3. Требования к необходимому уровню квалификации администратора и рекомендации по освоению системы.....	25
3. Указания по комплексной наладке	26
3.1. Перечень ресурсов, необходимых для проведения комплексной наладки.....	26
3.2. Условия, при соблюдении которых возможно проведение комплексной наладки.....	26
3.3. Перечень и последовательность работ по комплексной наладке	26
3.4. Требования к операционной системе «РЕД ОС»	26
3.5. Требования к операционной системе «Astra Linux Special Edition»	27
3.6. Установка и настройка СУБД	27
3.6.1. Установка и настройка СУБД Postgres Pro	27
3.6.2. Установка и настройка СУБД PostgreSQL из состава дистрибутива ОС «Astra Linux SE»	28
3.7. Создание схем БД	28
3.7.1. Создание схем БД x_idbox_database.....	28
3.7.2. Создание схем БД x_id_box_scheduler	28
3.7.3. Создание схем БД storage	29

3.7.4. Создание схем БД state_machine_queue	29
3.7.5. Создание схем БД sm	29
3.7.6. Создание схем БД x_idbox_maintenance	29
3.7.7. Создание схем БД archive_order	30
3.7.8. Создание схем БД x_idbox_internal_message.....	30
4. Подготовка конфигурационных файлов	31
4.1. Файл конфигурации и взаимодействия сервисов.....	31
4.2. Файл конфигурации ППО «Сервис кеширования данных».....	31
4.3. Файлы конфигурации веб-сервера.....	31
4.4. Файлы конфигурации Модуля фильтрации запросов к ИС	31
4.5. Файл конфигурации ведения журналов	32
4.6. Файлы конфигурации Kerberos	32
5. Установка системы.....	33
5.1. Установка и настройка ППО «Сервис аутентификации».....	33
5.1.1. Предусловия.....	33
5.1.2. Установка	33
5.1.3. Настройка	33
5.2. Установка и настройка Модуля фильтрации запросов к ИС	45
5.2.1. Предусловия.....	45
5.2.2. Установка	45
5.3. Установка и настройка ППО «Сервис авторизации»	45
5.3.1. Предусловия.....	45
5.3.2. Установка	46
5.3.3. Настройка	46
5.4. Установка и настройка ППО «Сервис обработки данных»	46
5.4.1. Предусловия.....	46
5.4.2. Установка	46
5.4.3. Настройка	47
5.5. Установка и настройка ППО «Модуль отправки уведомлений информационным системам с использованием Kafka»	47

5.5.1. Предусловия.....	47
5.5.2. Установка	47
5.5.3. Настройка	47
5.6. Установка и настройка ППО «Модуль отправки уведомлений информационным системам с использованием RabbitMQ»	48
5.6.1. Предусловия.....	48
5.6.2. Установка	48
5.6.3. Настройка	48
5.7. Установка и настройка ППО «Модуль отправки уведомлений информационным системам с использованием REST».....	48
5.7.1. Предусловия.....	48
5.7.2. Установка	49
5.7.3. Настройка	49
5.8. Установка и настройка ППО «Сервис работы с основными БД»	49
5.8.1. Предусловия.....	49
5.8.2. Установка	49
5.8.3. Настройка	50
5.9. Установка и настройка ППО «Сервис синхронизации данных каталогов».....	50
5.9.1. Предусловия.....	50
5.9.2. Установка	50
5.9.3. Настройка	50
5.10. Установка и настройка Модуля балансировки внутренних запросов	51
5.10.1.Предусловия.....	51
5.10.2.Установка	51
5.10.3.Настройка	51
5.11. Установка и настройка ППО «Сервис взаимодействия с пользовательским интерфейсом управления доступом».....	51
5.11.1.Предусловия.....	51
5.11.2.Установка	52

5.11.3. Настройка	52
5.12. Установка и настройка ППО «Пользовательский интерфейс управления доступом»	52
5.12.1. Предусловия.....	52
5.12.2. Установка	53
5.12.3. Настройка	53
5.13. Установка и настройка ППО «Сервис идентификации»	55
5.13.1. Предусловия.....	55
5.13.2. Установка	55
5.13.3. Настройка	56
5.14. Установка и настройка адаптера к ППО «Сервис интеграции с LDAP-каталогами»	56
5.14.1. Предусловия.....	56
5.14.2. Установка	56
5.14.3. Настройка	56
5.15. Установка и настройка ППО «Сервис обработки заявок»	60
5.15.1. Предусловия.....	60
5.15.2. Установка	60
5.15.3. Настройка	60
5.16. Установка и настройка ППО «Сервис организации выполнения заявок»	61
5.16.1. Предусловия.....	61
5.16.2. Установка	61
5.16.3. Настройка	61
5.17. Установка и настройка ППО «Сервис изменения заявок»	61
5.17.1. Предусловия.....	61
5.17.2. Установка	62
5.17.3. Настройка	62
5.18. Установка и настройка ППО «Сервис загрузки организаций»	62
5.18.1. Предусловия.....	62
5.18.2. Установка	62

5.18.3. Настройка	62
5.19. Установка и настройка ППО «Сервис загрузки ОШС».....	63
5.19.1. Предусловия.....	63
5.19.2. Установка	63
5.19.3. Настройка	63
5.20. Установка и настройка ППО «Сервис загрузки ролевых моделей»	63
5.20.1. Предусловия.....	63
5.20.2. Установка	64
5.20.3. Настройка	64
5.21. Установка и настройка ППО «Сервис автоматических операций»	64
5.21.1. Предусловия.....	64
5.21.2. Установка	64
5.21.3. Настройка	65
5.22. Установка и настройка ППО «Сервис обеспечения целостности данных».....	65
5.22.1. Предусловия.....	65
5.22.2. Установка	65
5.22.3. Настройка	65
5.23. Установка и настройка ППО «Пользовательский интерфейс аутентификации»	66
5.23.1. Предусловия.....	66
5.23.2. Установка	66
5.23.3. Настройка	66
5.24. Установка и настройка ППО «Сервис работы с данными заявок»	68
5.24.1. Предусловия.....	68
5.24.2. Установка	69
5.24.3. Настройка	69
5.25. Установка и настройка ППО «Сервис работы с очередью заявок»	69
5.25.1. Предусловия.....	69
5.25.2. Установка	69

5.25.3. Настройка	70
5.26. Установка и настройка ППО «Сервис работы с исходными данными заявок»	70
5.26.1. Предусловия.....	70
5.26.2. Установка	70
5.26.3. Настройка	70
5.27. Установка и настройка ППО «Сервис загрузки назначений»	71
5.27.1. Предусловия.....	71
5.27.2. Установка	71
5.27.3. Настройка	71
5.28. Установка и настройка ППО «Сервис регистрации и изменения данных пользователей»	71
5.28.1. Предусловия.....	71
5.28.2. Установка	72
5.28.3. Настройка	72
5.29. Установка и настройка ППО «Сервис валидации данных»	72
5.29.1. Предусловия.....	72
5.29.2. Установка	72
5.29.3. Настройка	72
5.30. Установка и настройка ППО «Сервис выполнения автоматических расчетов».....	73
5.30.1. Предусловия.....	73
5.30.2. Установка	73
5.30.3. Настройка	73
5.31. Установка и настройка ППО «Сервис работы с архивом заявок»	76
5.31.1. Предусловия.....	76
5.31.2. Установка	76
5.31.3. Настройка	76
5.32. Установка и настройка ППО «Сервис работы с БД внутренних уведомлений»	77

5.32.1. Предусловия.....	77
5.32.2. Установка	77
5.32.3. Настройка	77
5.33. Установка и настройка ППО «Сервис загрузки справочников»	77
5.33.1. Предусловия.....	77
5.33.2. Установка	78
5.33.3. Настройка	78
5.34. Установка и настройка ППО «Сервис кеширования данных»	78
5.34.1. Предусловия.....	78
5.34.2. Установка	78
5.34.3. Настройка	79
5.35. Установка и настройка веб-сервера	79
5.35.1. Предусловия.....	79
5.35.2. Установка веб-сервера	79
5.35.3. Настройка веб-сервера.....	80
5.36. Добавление ИС X-IDBox	80
6. Обновление системы	83
6.1. Подготовка к обновлению	83
6.1.1. Проверки перед началом работ.....	83
6.1.2. Резервное копирование.....	84
6.2. Полное обновление системы	85
6.3. Частичное обновление системы	85
6.4. Восстановление предыдущей версии в случае неуспешного обновления	86
6.5. Проверка после обновления и восстановления системы.....	87
7. Администрирование системы.....	90
7.1. Настройка параметров запуска.....	90
7.1.1. Настройка параметров JVM	90
7.2. Управление учётными записями пользователей и назначение пользователям прав доступа	90

7.3. Настройка событий безопасности, подлежащих регистрации, их состава и содержания	91
7.4. Настройка веб-серверов для работы с системой	92
7.5. Настройка рабочих станций пользователей для работы с системой.....	93
7.6. Настройки правил выборки подотчётных организаций	93
7.7. Добавление настраиваемых функций для условий применимости ролей и политик авторизации	94
7.8. Кастомизация атрибутов сессии	95
7.8.1. Добавление нового атрибута сессии	95
8. Подключение информационной системы	97
8.1. Настройка сетевого взаимодействия	97
8.2. Подключение ИС	97
8.3. Подключение ИС OAuth 2.0-клиента в X-IDBox	100
8.4. Загрузка ролей и защищаемых объектов ИС	105
8.5. Создание пользователя с ролью «Менеджер ИС»	106
8.6. Настройка отправки уведомлений	107
9. Обслуживание системы.....	111
9.1. Порядок обслуживания и проверка работоспособности системы.....	111
9.1.1. Управление СУБД.....	111
9.1.2. Управление веб-сервером.....	111
9.1.3. Управление сервисами ППО X-IDBox.....	112
9.2. Проверка и анализ ключевых параметров функционирования системы и электронных журналов событий	116
9.3. Резервное копирование и восстановление данных	117
9.3.1. Объекты резервного копирования	118
9.3.2. Применяемые методы и инструменты резервного копирования .	118
9.3.3. Конфигурационные требования к серверу СУБД.....	119
9.3.4. Периодичность выполнения резервного копирования.....	120
9.3.5. Восстановление данных.....	120
9.3.6. Политика хранения и ротации резервных копий	121

9.3.7. Хранение резервных копий	122
9.3.8. Контроль качества и аудит	123
9.4. Настройка мониторинга системы.....	124
9.4.1. Мониторинг инфраструктурных компонентов	125
9.4.2. Мониторинг ППО X-IDBox.....	126
9.4.3. Мониторинг Nginx	128
9.4.4. Мониторинг Apache2	129
9.4.5. Мониторинг СУБД Postgres Pro / PostgreSQL	131
9.4.6. Рекомендации по организации мониторинга резервного копирования	132
Приложение А Шаблон информационных потоков между ИС и X-IDBox	135
Приложение Б Описание настроек	136
Б.1 Индивидуальные настройки стенда	136
Б.2 Обязательные настройки.....	138
Б.3 Опциональные настройки	139
Б.4 Настройки сервиса xidbox-authentication.....	146
Б.5 Настройки сервиса xidbox-state-machine-queue	150
Б.6 Настройки сервиса xidbox-role-politics-upload.....	150
Б.7 Настройки сервиса xidbox-database	151
Б.8 Настройки сервиса xidbox-backend	151
Б.9 Настройки сервиса xidbox-frontbackend	153
Б.10 Настройки сервиса xidbox-scheduler	154
Б.11 Настройки сервиса xidbox-orchestrator	156
Б.12 Настройки сервиса xidbox-storage.....	161
Б.13 Настройки сервиса xidbox-order	161
Б.14 Настройки сервиса xidbox-state-machine-database	162
Б.15 Настройки сервиса xidbox-ldap	162
Б.16 Настройки сервиса xidbox-organizational-structure	165
Б.17 Настройки сервиса xidbox-signature.....	166
Б.18 Настройки сервиса xidbox-request-background-processing	166

Б.19 Настройки сервиса xidbox-callback-kafka.....	168
Б.20 Настройки сервиса xidbox-directory-synchronization.....	168
Б.21 Настройки сервиса xidbox-order-archive-database.....	169
Б.22 Настройки сервиса xidbox-internal-message-database.....	169
Б.23 Настройки сервиса xidbox-organization	169
Б.24 Настройки сервиса xidbox-user-upload	170
Б.25 Настройки сервиса xidbox-user-profile-upload	170
Б.26 Настройки для всех сервисов	170
Приложение В Дополнительные данные о событиях безопасности.....	173
Приложение Г Структура данных в источнике.....	218
Приложение Д Сопоставление типов заявок и шаблонов уведомлений	222
Лист регистрации изменений	227

Перечень сокращений

JVM	– Java Virtual Machine (виртуальная машина)
SpEL	– Spring Expression Language (язык выражений в Spring Framework)
TTL	– Time To Live (период актуальности кеша)
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
КСЗ	– комплекс средств защиты
ОЗУ	– оперативное запоминающее устройство
ОС	– операционная система
ОШС	– организационно-штатная структура
ПО	– программное обеспечение
ППО	– прикладное программное обеспечение
СНИЛС	– страховой номер индивидуального лицевого счёта
СУБД	– система управления базами данных
УЗ	– учётная запись
ЦПУ	– центральное процессорное устройство

Перечень терминов

LDAP-каталог	– каталог учётных записей пользователей, взаимодействие с которым осуществляется по протоколу LDAP (поддерживаются Active Directory, FreeIPA, ALD Pro)
PITR	– Point-in-Time Recovery. Восстановление на момент времени. Функциональность, позволяющая восстановить состояние БД на произвольную временную отметку, вплоть до секунды, в пределах срока хранения архивов WAL
WAL	– Write-Ahead Log. Журнал предзаписи. Последовательность бинарных записей всех изменений данных, используемая для обеспечения отказоустойчивости и непрерывного архивирования
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
Базовая резервная копия	– полная копия файлов каталога данных СУБД (data directory), создаваемая инструментами физического резервирования
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
Контейнер ИС	– структурная единица ИС, предназначенная для хранения отдельных частей ролевой модели ИС и работы с ними
Логический дамп	– текстовое или бинарное представление структуры и содержимого БД, создаваемое для переноса данных или выборочного восстановления
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
Подсистема ИС	– структурная единица ИС, предназначенная для обеспечения возможности управления доступом к частям ИС, при их наличии
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

Приложение ИС	– структурная единица ИС, обеспечивающая возможность единого управления доступом в ИС, имеющую несколько приложений с идентичным или отличающимся набором функций, а также настройки способов аутентификации
Профиль учётной записи пользователя	– набор значений атрибутов учётной записи X-IDBox, однозначно ассоциирующий субъект доступа с организацией, в интересах (от имени) которой субъектом доступа выполняются операции, реализованные в X-IDBox и ИС, интегрированных с X-IDBox
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
Уведомление	– электронное письмо, которое отправляется на адрес электронной почты пользователя и (или) в системе при наступлении определённого события
Управление доступом	– ограничение и контроль доступа субъектов доступа к объектам доступа в ИС в соответствии с установленными правилами разграничения доступа
Условия применимости политики авторизации	– условия, которые определяют возможность выполнения действия с ресурсом
Условия применимости роли	– условия, которые влияют на доступность роли для назначения конкретному пользователю

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
Шаблон уведомления	– шаблон электронного письма, который содержит параметры, заполняющиеся автоматически требуемой информацией, и отправляется на адрес электронной почты пользователя и (или) в системе при наступлении определённого события
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 электронных приложений

Название приложения	Имя файла
Шаблон требуемой информации для подключения ИС	Шаблон требуемой информации для подключения ИС.docx
Пример стандартного файла с текстами серверных ошибок	exceptionMessages.properties
Формат файла с преобразованием условий ролевой модели в SQL	condition-to-sql.json

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) Подтверждение выполнения операций в системе путем использования заявок, формируемых для каждого выполняемого действия в системе.

5) Просмотр списка организаций.

6) Управление настройками безопасности и парольными политиками.

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

1.2. Функциональные роли

В пользовательском интерфейсе управления доступом X-IDBox по умолчанию предусмотрены следующие функциональные роли:

- Пользователь;
- Системный администратор;
- Администратор ИБ;
- Менеджер информационной системы;
- Менеджер учётных записей;
- Главный 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 и Главному менеджеру учётных записей. Также Главному менеджеру учётных записей доступно управление УЗ пользователей и профилями УЗ пользователей, а Менеджеру учётных записей доступно управление УЗ пользователей и профилями УЗ пользователей своей организации и её обособленных подразделений.

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, и управление настройками безопасности.

Ролевая модель пользовательского интерфейса управления доступом X-IDBox может быть настроена с учетом необходимых ролей и правил доступа в рамках имеющихся функций.

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 RPM	Дистрибутив DEB
ППО «Сервис аутентификации»	xidbox-authentication-[version].[commit].x86_64.rpm	xidbox-authentication_[version].[commit].[revision]_amd64.deb
Модуль фильтрации запросов к ИС	xidbox-authn-gateway-[version].[commit].x86_64.rpm	xidbox-authn-gateway_[version].[commit].[revision]_amd64.deb
ППО «Сервис авторизации»	xidbox-authorization-[version].[commit].x86_64.rpm	xidbox-authorization_[version].[commit].[revision]_amd64.deb
ППО «Сервис обработки данных»	xidbox-backend-[version].[commit].x86_64.rpm	xidbox-backend_[version].[commit].[revision]_amd64.deb
ППО «Модуль отправки уведомлений информационным системам с использованием Kafka»	xidbox-callback-kafka-[version].[commit].x86_64.rpm	xidbox-callback-kafka_[version].[commit].[revision]_amd64.deb
ППО «Модуль отправки уведомлений информационным системам с использованием RabbitMQ»	xidbox-callback-rabbit-[version].[commit].x86_64.rpm	xidbox-callback-rabbit_[version].[commit].[revision]_amd64.deb
ППО «Модуль отправки уведомлений информационным системам с использованием REST»	xidbox-callback-rest-[version].[commit].x86_64.rpm	xidbox-callback-rest_[version].[commit].[revision]_amd64.deb
ППО «Сервис работы с основными БД»	xidbox-database-[version].[commit].x86_64.rpm	xidbox-database_[version].[commit].[revision]_amd64.deb
ППО «Сервис синхронизации данных каталогов»	xidbox-directory-synchronization-[version].[commit].x86_64.rpm	xidbox-directory-synchronization_[version].[commit].[revision]_amd64.deb
Модуль балансировки внутренних запросов	xidbox-eureka-[version].[commit].x86_64.rpm	xidbox-eureka_[version].[commit].[revision]_amd64.deb
ППО «Сервис взаимодействия с пользовательским интерфейсом управления доступом»	xidbox-frontbackend-[version].[commit].x86_64.rpm	xidbox-frontbackend_[version].[commit].[revision]_amd64.deb

ПО	Дистрибутив RPM	Дистрибутив DEB
ППО «Пользовательский интерфейс управления доступом»	xidbox-frontend-[version].[commit].x86_64.rpm	xidbox-frontend_[version].[commit].[revision]_amd64.deb
ППО «Сервис идентификации»	xidbox-identification-[version].[commit].x86_64.rpm	xidbox-identification_[version].[commit].[revision]_amd64.deb
ППО «Сервис интеграции с LDAP-каталогами»	xidbox-ldap-[version].[commit].x86_64.rpm	xidbox-ldap_[version].[commit].[revision]_amd64.deb
ППО «Сервис обработки заявок»	xidbox-orchestrator-[version].[commit].x86_64.rpm	xidbox-orchestrator_[version].[commit].[revision]_amd64.deb
ППО «Сервис организации выполнения заявок»	xidbox-orchestrator-helper-[version].[commit].x86_64.rpm	xidbox-orchestrator-helper_[version].[commit].[revision]_amd64.deb
ППО «Сервис изменения заявок»	xidbox-order-[version].[commit].x86_64.rpm	xidbox-order_[version].[commit].[revision]_amd64.deb
ППО «Сервис загрузки организаций»	xidbox-organization-[version].[commit].x86_64.rpm	xidbox-organization_[version].[commit].[revision]_amd64.deb
ППО «Сервис загрузки ОШС»	xidbox-organizational-structure-[version].[commit].x86_64.rpm	xidbox-organizational-structure_[version].[commit].[revision]_amd64.deb
ППО «Сервис загрузки ролевых моделей»	xidbox-role-politics-upload-[version].[commit].x86_64.rpm	xidbox-role-politics-upload_[version].[commit].[revision]_amd64.deb
ППО «Сервис автоматических операций»	xidbox-scheduler-[version].[commit].x86_64.rpm	xidbox-scheduler_[version].[commit].[revision]_amd64.deb
ППО «Сервис обеспечения целостности данных»	xidbox-signature-[version].[commit].x86_64.rpm	xidbox-signature_[version].[commit].[revision]_amd64.deb
ППО «Пользовательский интерфейс аутентификации»	xidbox-signin-[version].[commit].x86_64.rpm	xidbox-signin_[version].[commit].[revision]_amd64.deb
ППО «Сервис работы с данными заявок»	xidbox-state-machine-database-[version].[commit].x86_64.rpm	xidbox-state-machine-database_[version].[commit].[revision]_amd64.deb
ППО «Сервис работы с очередью заявок»	xidbox-state-machine-queue-[version].[commit].x86_64.rpm	xidbox-state-machine-queue_[version].[commit].[revision]_amd64.deb

ПО	Дистрибутив RPM	Дистрибутив DEB
ППО «Сервис работы с исходными данными заявок»	xidbox-storage-[version].[commit].x86_64.rpm	xidbox-storage_[version].[commit].[revision]_amd64.deb
ППО «Сервис загрузки назначений»	xidbox-user-profile-upload-[version].[commit].x86_64.rpm	xidbox-user-profile-upload_[version].[commit].[revision]_amd64.deb
ППО «Сервис регистрации и изменения данных пользователей»	xidbox-user-upload-[version].[commit].x86_64.rpm	xidbox-user-upload_[version].[commit].[revision]_amd64.deb
ППО «Сервис валидации данных»	xidbox-validation-[version].[commit].x86_64.rpm	xidbox-validation_[version].[commit].[revision]_amd64.deb
ППО «Сервис выполнения автоматических расчетов»	xidbox-request-background-processing-[version].[commit].x86_64.rpm	xidbox-request-background-processing_[version].[commit].[revision]_amd64.deb
ППО «Сервис работы с архивом заявок»	xidbox-order-archive-database-[version].[commit].x86_64.rpm	xidbox-order-archive-database_[version].[commit].[revision]_amd64.deb
ППО «Сервис работы с БД внутренних уведомлений»	xidbox-internal-message-database-[version].[commit].x86_64.rpm	xidbox-internal-message-database_[version].[commit].[revision]_amd64.deb
ППО «Сервис загрузки справочников»	xidbox-dictionary-upload-[version].[commit].x86_64.rpm	xidbox-dictionary-upload_[version].[commit].[revision]_amd64.deb
ППО «Сервис кеширования данных»	xidbox-cache-[version].[commit].x86_64.rpm	xidbox-cache_[version].[commit].[revision]_amd64.deb

2. Условия применения

Все компоненты X-IDBox поставляются в виде RPM и DEB 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 или физических серверов под управлением ОС Linux с пакетным менеджером RPM или DEB, входящей в реестр отечественного ПО, с характеристиками из расчета на один сервис не меньше:

- ЦПУ – 1 vCPU (1 физическое ядро);
- ОЗУ – 2 ГБ, за исключением сервиса xidbox-cache, для которого требуется не менее 8 ГБ;
- HDD – от 10 до 50 ГБ. Конкретный объем определяется, исходя из установленного уровня логирования, а также принятой политики хранения и ротации логов.

2.2. Требования к АРМ пользователя

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

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-браузером;
- знание протоколов SOAP, REST;
- навыки работы с БПО и ППО, используемым на стороне ИС;
- опыт администрирования ОС семейства Linux;
- опыт работы с Postgres Pro, веб-серверами (Nginx, Apache2 и Tomcat);
- опыт работы 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 ППО X-IDBox .
- 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 параметров сетевого интерфейса (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. Требования к операционной системе «Astra Linux Special Edition»

- версия не ниже 1.8;
- статические настройки параметров сетевого интерфейса (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.

3.6. Установка и настройка СУБД

3.6.1. Установка и настройка СУБД Postgres Pro

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

<https://postgrespro.ru/docs>

3.6.2. Установка и настройка СУБД PostgreSQL из состава дистрибутива ОС «Astra Linux SE»

Установите и настройте то количество кластеров СУБД PostgreSQL, которое определено в зависимости от схемы развертывания ППО X-IDBox, в соответствии с официальной документацией ОС «Astra Linux SE» «Руководство по КСЗ. Часть 3. Защищенная СУБД»:

<https://wiki.astralinux.ru>

3.7. Создание схем БД

Требования к серверу, на котором планируется создание схем БД:

- сервер с установленной ОС «РЕД ОС» версии не ниже 7.3.1 или ОС «Astra Linux SE» версии не ниже 1.8.1 подготовлен к установке сервисов (п. 3.4 или п. 3.5);
- установлена и настроена СУБД Postgres Pro версии не ниже 14 и находящейся в долгосрочной поддержке (LTS) (п. 3.6.1). В случае использования СУБД PostgreSQL из состава дистрибутива ОС «Astra Linux SE» выполняются настройки согласно п. 3.6.2.

3.7.1. Создание схем БД x_idbox_database

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

3.7.2. Создание схем БД x_id_box_scheduler

На любом сервере кластера СУБД, 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.

3.7.3. Создание схем БД storage

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

3.7.4. Создание схем БД state_machine_queue

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

3.7.5. Создание схем БД sm

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

3.7.6. Создание схем БД x_idbox_maintenance

БД x_idbox_maintenance должна размещаться на отдельном сервере кластера СУБД, отличном от кластера, на котором размещена основная БД x_idbox_database. Такое разделение необходимо для снижения нагрузки на основную БД x_idbox_database, обеспечивающую работу критически важных сервисов X-IDBox.

На любом сервере кластера СУБД, предназначенного для БД x_idbox_maintenance, создайте БД x_idbox_maintenance. Схемы и таблицы будут созданы автоматически при установке и запуске сервисов системы.

3.7.7. Создание схем БД archive_order

На любом сервере кластера СУБД, предназначенного для БД archive_order, создайте БД archive_order. Схемы и таблицы будут созданы автоматически при установке и запуске сервисов системы.

3.7.8. Создание схем БД x_idbox_internal_message

На любом сервере кластера СУБД, предназначенного для БД x_idbox_internal_message, создайте БД x_idbox_internal_message. Схемы и таблицы будут созданы автоматически при установке и запуске сервисов системы.

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 приведён в Приложении Б.

4.2. Файл конфигурации ППО «Сервис кеширования данных»

Создайте конфигурационный файл по образцу «application.properties» (из прилагаемых дистрибутивов), принимая во внимание комментарии по тексту файла образца.

4.3. Файлы конфигурации веб-сервера

Создайте конфигурационные файлы по образцу файлов из архива «nginx.zip» для ОС «РЕД ОС» или «apache.zip» для ОС «Astra Linux SE» (из прилагаемых дистрибутивов), принимая во внимание комментарии по тексту файлов образцов.

4.4. Файлы конфигурации Модуля фильтрации запросов к ИС

Создайте конфигурационные файлы по образцу файлов из архива «authng.zip» для ОС «РЕД ОС» или «apache_authng.zip» для ОС «Astra Linux SE» (из прилагаемых дистрибутивов), принимая во внимание комментарии по тексту файлов образцов.

4.5. Файл конфигурации ведения журналов

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

4.6. 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 СУБД, 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 описанными в п. 3.4 и п. 3.5.

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 5.1.3.5.

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).

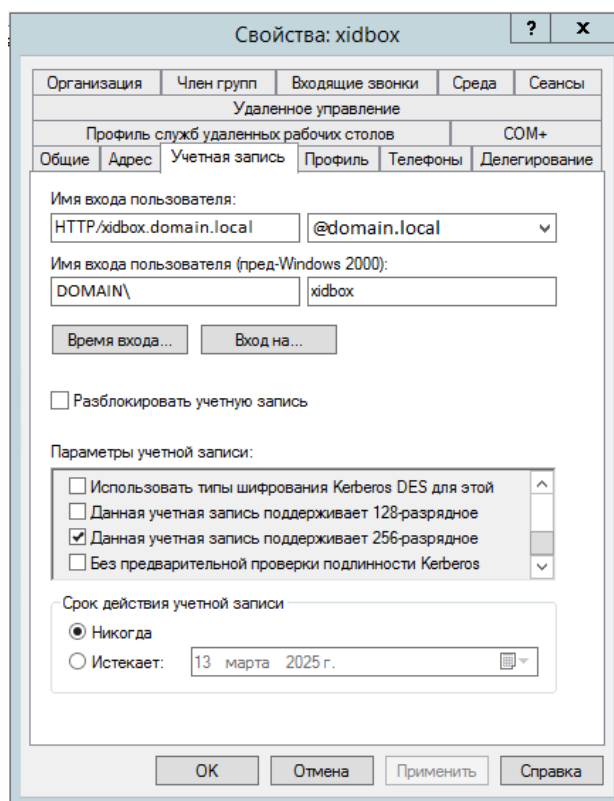


Рисунок 1 – Настройка учётной записи в Active Directory

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.

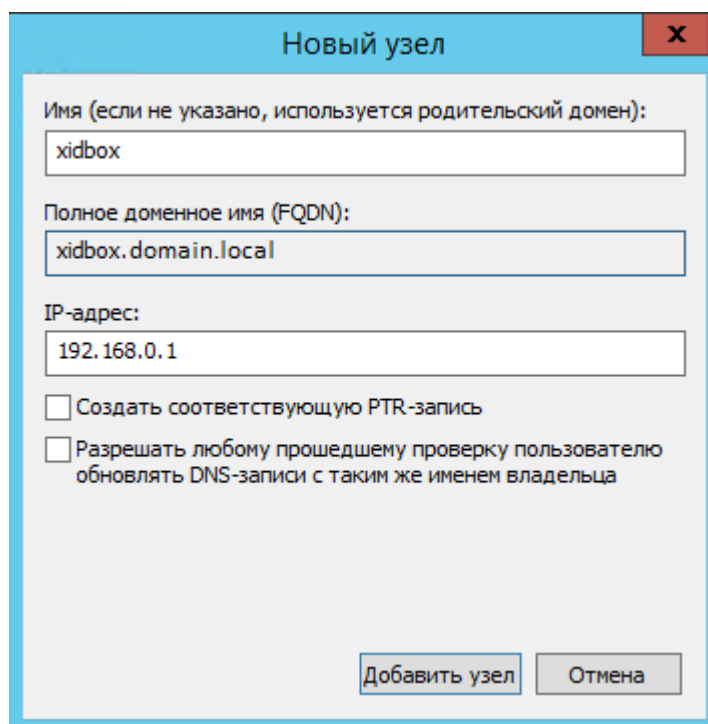


Рисунок 2 – Добавление записи хоста в DNS Active Directory

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).

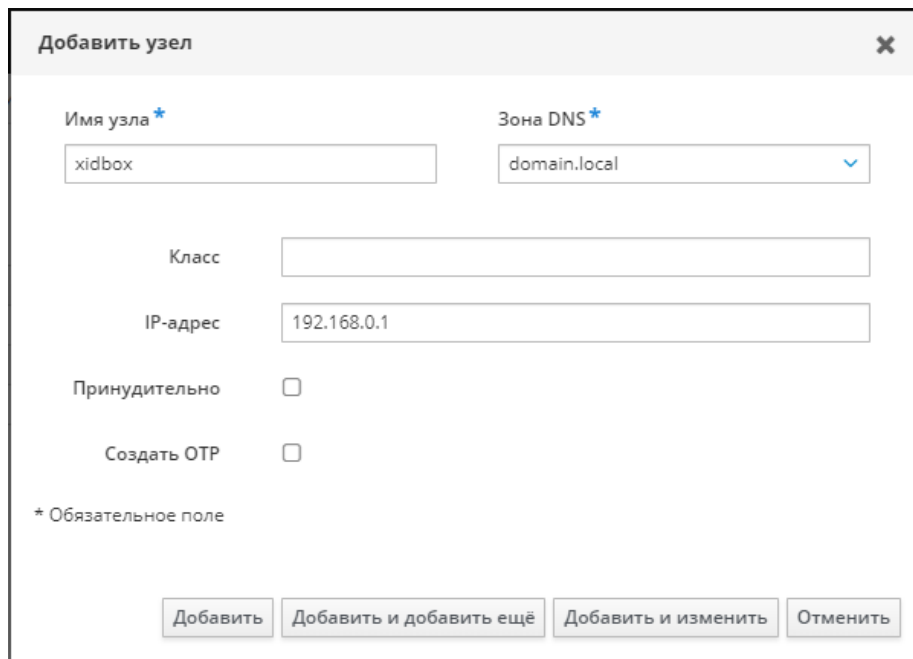


Рисунок 3 – Создание узла в FreeIPA

- 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).

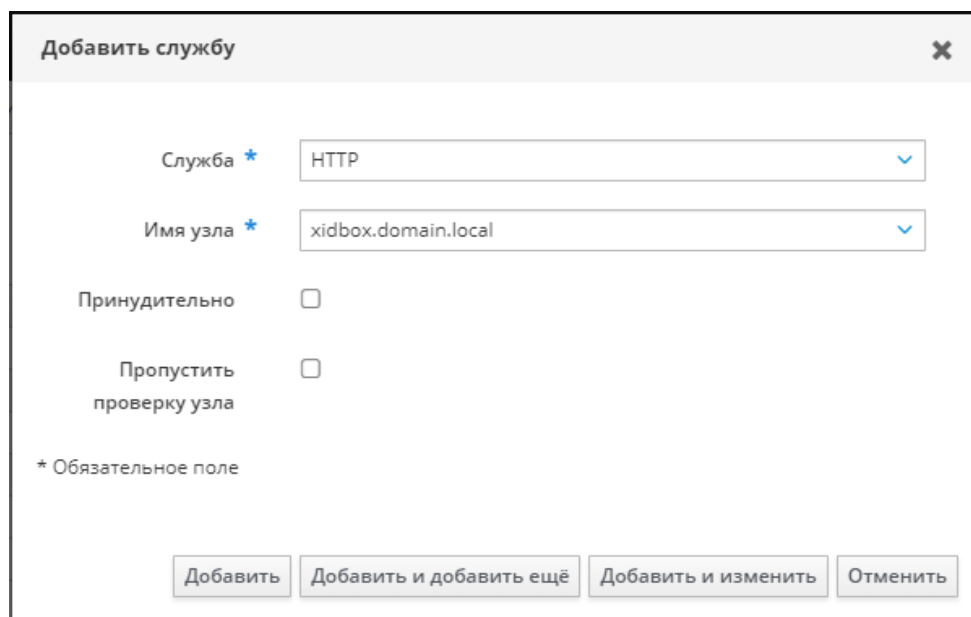


Рисунок 4 – Создание службы в FreeIPA

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 контроллера домена ALD Pro

Настройка доменной аутентификации на стороне контроллера домена ALD Pro выполняется аналогично настройке для FreeIPA, описанной в п. 5.1.3.3.

5.1.3.5. 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. 4.6, 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. 4.6, 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.

5.1.3.6. Изменение текстов серверных ошибок

В ППО «Сервис аутентификации» предусмотрена возможность изменения текстов серверных ошибок. Для применения изменённых текстов добавьте в директорию «/opt/xidbox/services/xidbox-authentication/» файл «exceptionMessages.properties» с изменёнными текстами ошибок.

Если в файле указаны не все используемые ошибки, то для них будут использованы стандартные тексты ошибок. Список ошибок и их стандартные формулировки приведены в файле «exceptionMessages.properties».

5.2. Установка и настройка Модуля фильтрации запросов к ИС

5.2.1. Предусловия

Сервер подготовлен для установки компонентов X-IDBox, включая веб-серверы, устанавливаемые совместно с Модулем фильтрации запросов к ИС. Тип веб-сервера определяется используемой операционной системой:

- при использовании ОС «РЕД ОС» применяется веб-сервер Nginx, поставляемый в составе дистрибутива ОС «РЕД ОС»;
- при использовании ОС «Astra Linux SE» применяется веб-сервер Apache2, поставляемый в составе дистрибутива ОС «Astra Linux SE».

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.
- 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 СУБД, 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 «Сервис работы с основными БД»

5.8.1. Предусловия

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

5.8.2. 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.

5.8.3. 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 синхронизации данных каталогов»

5.9.1. Предусловия

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

5.9.2. Установка

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

5.9.3. 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».

5.10. Установка и настройка Модуля балансировки внутренних запросов

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 Модуля балансировки внутренних запросов, установите Модуль балансировки внутренних запросов 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, с именем «xidbox.properties».

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

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

5.11.3. Настройка

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

5.11.3.1. Изменение текстов серверных ошибок

В ППО «Сервис взаимодействия с пользовательским интерфейсом управления доступом» предусмотрена возможность изменения текстов серверных ошибок. Для применения изменённых текстов добавьте в директорию «/opt/xidbox/services/xidbox-frontbackend/» файл «exceptionMessages.properties» с изменёнными текстами ошибок.

Если в файле указаны не все используемые ошибки, то для них будут использованы стандартные тексты ошибок. Список ошибок и их стандартные формулировки приведены в файле «exceptionMessages.properties».

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

5.12.1. Предусловия

Сервер подготовлен для установки компонентов X-IDBox, включая веб-серверы, устанавливаемые совместно с Пользовательским интерфейсом

управления доступом. Тип веб-сервера определяется используемой операционной системой:

- при использовании ОС «РЕД ОС» применяется веб-сервер Nginx, поставляемый в составе дистрибутива ОС «РЕД ОС»;
- при использовании ОС «Astra Linux SE» применяется веб-сервер Apache2, поставляемый в составе дистрибутива ОС «Astra Linux SE».

5.12.2. Установка

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

5.12.3. Настройка

5.12.3.1. Кастомизация пользовательского интерфейса управления доступом

ППО «Пользовательский интерфейс управления доступом» поддерживает возможность кастомизации без изменения стандартных файлов поставки.

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

Для кастомизации пользовательского интерфейса управления доступом:

- 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-frontend/custom/global.css».

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

- «/opt/xidbox/services/xidbox-frontend/custom/favicon.ico»;
- «/opt/xidbox/services/xidbox-frontend/custom/fonts/custom-font.woff2».

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

- для Nginx:

```
systemctl restart nginx
```

- для Apache2:

```
systemctl restart apache2.service
```

При обращении к ресурсам пользовательского интерфейса управления доступом веб-сервер в первую очередь использует ресурсы из каталога «custom». Если файл в данном каталоге отсутствует, используется стандартный файл из каталога поставки.

5.12.3.2. Кастомизация текстов в пользовательском интерфейсе управления доступом

ППО «Пользовательский интерфейс управления доступом» поддерживает возможность кастомизации текстов без изменения стандартных файлов поставки.

Для этого используются файлы локализации в формате .json, сгруппированные по функциональным модулям: users.json, user-profiles.json, dictionaries.json, information-systems.json, localization.json, orders.json, organizations.json, roles.json, security-settings.json, templates.json.

При установке ППО «Пользовательский интерфейс управления доступом» в директории создаётся каталог «xidbox-frontend», предназначенный для размещения файлов переопределенного оформления: «/opt/xidbox/services/xidbox-frontend/».

Для кастомизации текстов в пользовательском интерфейсе управления доступом:

1) В прилагаемых дистрибутивах найдите соответствующий файл в формате .json в каталоге «frontend/xidbox-frontend».

2) Внесите необходимые изменения в найденный файл.

3) Скопируйте изменённый файл в каталог «xidbox-frontend» (созданный в директории при установке ППО «Пользовательский интерфейс управления доступом»), например: «/opt/xidbox/services/xidbox-frontend/users.json».

После кастомизации текстов перезапуск веб-сервера не требуется – изменения применяются автоматически (при следующем обращении к интерфейсу или после обновления страницы).

Пользовательский интерфейс управления доступом при загрузке ППО сначала проверяет наличие кастомного файла в каталоге «xidbox-frontend»:

- Если файл существует и валиден – используется он.
- Если файл не существует или невалиден – загружается стандартный файл из каталога поставки.
- Если в кастомном файле изменена только часть текстов, то остальной текст будет взят в стандартном файле из каталога поставки.

5.13. Установка и настройка ППО «Сервис идентификации»

5.13.1. Предусловия

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

5.13.2. Установка

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

5.13.3. Настройка

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

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

5.14.1. 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.

5.14.2. 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.

5.14.3. Настройка

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

5.14.3.1. 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.

5.14.3.2. 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
```

5.14.3.3. Создание технической учётной записи в ALD Pro

Процедура создания технической учётной записи на контроллере домена ALD Pro аналогична процедуре для FreeIPA, описанной в п. 5.14.3.2.

5.14.3.4. 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.14.

5.15. Установка и настройка ППО «Сервис обработки заявок»

5.15.1. Предусловия

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

5.15.2. Установка

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

5.15.3. Настройка

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

5.16. Установка и настройка ППО «Сервис организации выполнения 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 сервиса организации выполнения заявок, установите ППО «Сервис организации выполнения 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 изменения 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 изменения заявок, установите ППО «Сервис изменения 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 загрузки организаций»

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 сервиса загрузки организаций, установите ППО «Сервис загрузки организаций» 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 ОШС»

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 ОШС, установите ППО «Сервис загрузки ОШС» 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 ролевых моделей»

5.20.1. Предусловия

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

5.20.2. Установка

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

5.20.3. 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 автоматических операций»

5.21.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры СУБД, 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 автоматических операций, установите ППО «Сервис автоматических операций» 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 обеспечения целостности данных»

5.22.1. Предусловия

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

5.22.2. Установка

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

5.22.3. 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 «Пользовательский интерфейс аутентификации»

5.23.1. Предусловия

Сервер подготовлен для установки компонентов X-IDBox, включая веб-серверы, устанавливаемые совместно с Пользовательским интерфейсом аутентификации. Тип веб-сервера определяется используемой операционной системой:

- при использовании ОС «РЕД ОС» применяется веб-сервер Nginx, поставляемый в составе дистрибутива ОС «РЕД ОС»;
- при использовании ОС «Astra Linux SE» применяется веб-сервер Apache2, поставляемый в составе дистрибутива ОС «Astra Linux SE».

5.23.2. Установка

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

5.23.3. Настройка

5.23.3.1. 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, чтобы изменения вступили в силу:

- для Nginx:

```
systemctl restart nginx
```

- для Apache2:

```
systemctl restart apache2.service
```

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

5.23.3.2. Кастомизация текстов в пользовательском интерфейсе аутентификации

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

Для этого используются файлы `localization.json`.

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

Для кастомизации текстов в пользовательском интерфейсе аутентификации:

- 1) В прилагаемых дистрибутивах найдите файл `localization.json` в каталоге «frontend/xidbox-signin».
- 2) Внесите необходимые изменения в найденный файл.
- 3) Скопируйте изменённый файл в каталог «xidbox-signin» (созданный в директории при установке ППО «Пользовательский интерфейс аутентификации»), например: «/opt/xidbox/services/xidbox-signin/localization.json».

После кастомизации текстов перезапуск веб-сервера не требуется – изменения применяются автоматически (при следующем обращении к интерфейсу или после обновления страницы).

Пользовательский интерфейс аутентификации при загрузке ППО сначала проверяет наличие кастомного файла в каталоге «xidbox-signin»:

- Если файл существует и валиден – используется он.
- Если файл не существует или невалиден – загружается стандартный файл из каталога поставки.
- Если в кастомном файле изменена только часть текстов, то остальной текст будет взят в стандартном файле из каталога поставки.

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

5.24.1. 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.

5.24.2. 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.

5.24.3. Настройка

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

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

5.25.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры СУБД, 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 очередью заявок, установите ППО «Сервис работы с очередью 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 исходными данными заявок»

5.26.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры СУБД, 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 исходными данными заявок, установите ППО «Сервис работы с исходными данными 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 загрузки назначений»

5.27.1. Предусловия

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

5.27.2. Установка

На серверах, предназначенных для установки сервиса загрузки назначений, установите ППО «Сервис загрузки назначений» 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 регистрации и изменения данных пользователей»

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 регистрации и изменения данных пользователей, установите ППО «Сервис регистрации и изменения данных пользователей» 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 валидации данных»

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 валидации данных, установите ППО «Сервис валидации данных» 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 выполнения автоматических расчетов»

Сервис выполнения автоматических расчетов использует данные из основной БД `x_idbox_database`, но с целью снижения нагрузки на основную БД `x_idbox_database` и обеспечения устойчивой работы сервиса, данные предоставляются через логическую реплику, размещенную в БД `x_idbox_maintenance`, которая расположена на отдельном сервере кластера СУБД.

5.30.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры СУБД, 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 выполнения автоматических расчетов, установите ППО «Сервис выполнения автоматических расчетов» 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»`.

ППО «Сервис выполнения автоматических расчетов» поддерживает различные режимы инициализации схемы с учётом типа логической репликации.

Для выбора режима используется параметр:

`xidbox.request-background-processing.service.spring liquibase.contexts`

Допустимые значения:

- default – создаёт основную структуру сервиса;
- partial_logic_replication – создаёт структуру и реплицируемые таблицы, применяется при репликации отдельных столбцов (PostgreSQL 15 и выше);
- full_logic_replication – создаёт структуру и реплицируемые таблицы для полной логической репликации.

Значение по умолчанию:

default,partial_logic_replication

Параметр default обязателен для создания основной структуры, необходимой для работы сервиса.

5.30.3.1. Настройка логической репликации

Перед выполнением операций по настройке логической репликации для ППО «Сервис выполнения автоматических расчетов» необходимо подготовить структуру БД, используемых сервисом выполнения автоматических расчётов. БД создаётся в соответствии с требованиями в п. 3.7, а схемы БД x_idbox_maintenance согласно п. 3.7.6. Формирование схем и таблиц выполняется автоматически сервисами после их запуска, поэтому настройка репликации проводится только после запуска серверов и инициализации сервисов. Эти действия являются обязательными предварительными шагами для корректной работы логической репликации.

Настройка СУБД для организации логической репликации выполняется в соответствии с официальной документацией (см. п. 3.6).

Для создания публикации на мастере выполните следующие действия:

- 1) Подключитесь к БД x_idbox_database.
- 2) Для создания полной репликации таблиц выполните SQL-команду:

```
CREATE PUBLICATION pub_xidbox FOR TABLE  
usr, user_profile, organization;
```

где pub_xidbox – имя публикации.

Для PostgreSQL версии 15 и выше возможно ограничение реплицируемых столбцов, если используется частичная логическая репликация.

3) Для создания частичной репликации (PostgreSQL версии 15 и выше) выполните SQL-команду:

```
CREATE PUBLICATION pub_xidbox FOR TABLE
usr (
    user_id, user_uuid, first_name, last_name,
    middle_name, snils, inn, birthday,
    login, email, password, password_changed,
    email_verified, count_error_auth_attempt,
    state, is_blocked, reg_date,
    privacy_policy_accepted, notify_password_expires,
    notify_password_expired,
    security_policy_accepted, salt
),
user_profile (
    id, uuid, user_id, organization_id,
    is_blocked, state, work_email, work_email_verified,
    department_name, position_name,
    registration_date
),
organization (
    id, uuid, full_name, short_name, type_id,
    inn, kpp, ogrn, state, is_blocked,
    address, registration_date, create_date
);
```

где pub_xidbox – имя публикации.

4) Для создания подписки на реплике подключитесь к БД x_idbox_maintenance и создайте подписку, выполнив SQL-команду:

```
CREATE SUBSCRIPTION sub_xidbox
CONNECTION 'host=<MASTER_HOST>
dbname=x_idbox_database user=<REPL_USER>
password=<PASSWORD>'
PUBLICATION pub_xidbox
WITH (create_slot = true, slot_name = sub_slot);
```

где:

– sub_xidbox – имя подписки;

- `pub_xidbox` – имя публикации;
- `sub_slot` – имя репликационного слота, который используется мастером для отслеживания изменений, необходимых для реплики;
- `MASTER_HOST` – адрес сервера мастера (хост, где размещена БД `x_idbox_database`);
- `REPL_USER` – имя пользователя для подключения к мастеру;
- `PASSWORD` – пароль пользователя `REPL_USER` для подключения к мастеру.

5.31. Установка и настройка ППО «Сервис работы с архивом заявок»

5.31.1. Предусловия

- Сервер соответствует требованиям, приведенным в п. 2.1.
- Установлены и настроены кластеры СУБД, 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 работы с архивом заявок, установите ППО «Сервис работы с архивом заявок» 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 ППО «Сервис работы с БД внутренних уведомлений»

5.32.1. Предусловия

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

5.32.2. Установка

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

5.32.3. Настройка

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

5.33. Установка и настройка ППО «Сервис загрузки справочников»

5.33.1. Предусловия

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

– Установлены и настроены кластеры СУБД, предназначенные для работы с сервисом.

5.33.2. Установка

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

5.33.3. Настройка

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

5.34. Установка и настройка ППО «Сервис кеширования данных»

5.34.1. Предусловия

– Сервер соответствует требованиям, приведенным в п. 2.1.

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

5.34.2. Установка

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

5.34.3. Настройка

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

5.35. Установка и настройка веб-сервера

5.35.1. Предусловия

Сервер соответствует требованиям, приведенным в п. 2.1.

5.35.2. Установка веб-сервера

На сервере, предназначенном для установки Модуля фильтрации запросов к ИС, установите и настройте веб-сервер, в зависимости от используемой операционной системы. В ОС «РЕД ОС» используется веб-сервер Nginx, а в ОС «Astra Linux SE» – веб-сервер Apache2. Оба веб-сервера устанавливаются из стандартных пакетов, входящих в состав соответствующих дистрибутивов.

На серверах под управлением ОС «РЕД ОС» для установки Nginx выполните команду:

```
sudo dnf update
sudo dnf install nginx
```

На серверах под управлением ОС «Astra Linux SE» установите Apache2:

```
sudo apt-get update
sudo apt-get install -y apache2
```

Для обеспечения корректной работы установите и активируйте дополнительные модули, входящие в состав дистрибутива ОС «Astra Linux SE»:

```
sudo a2enmod proxy
sudo a2enmod proxy_http
sudo a2enmod proxy_balancer
sudo a2enmod lbmethod_byrequests
sudo a2enmod rewrite
```

```
sudo a2enmod headers
```

После активации модулей выполните перезапуск веб-сервера.

5.35.3. Настройка веб-сервера

Настройка веб-сервера осуществляется на основе шаблонов конфигураций, поставляемых с дистрибутивом X-IDBox. Файлы конфигурации, подготовленные в ходе выполнения п. 4.3:

- для Nginx копируются в директорию «/etc/nginx/conf.d/»;
- для Apache2 копируются в директорию «/etc/apache2/sites-available/».

В случае Apache2 необходимо деактивировать файл конфигурации по умолчанию:

```
a2dissite 000-default.conf
```

и активировать файлы конфигураций командой:

```
a2ensite <имя_конфигурационного_файла>
```

5.36. 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 из файла «xidbox_full.txt» при использовании пользовательского интерфейса X-IDBox или из файла «xidbox_minimal.txt», если пользовательский интерфейс управления доступом X-IDBox не используется (из прилагаемых дистрибутивов). Для этого загрузите файл ролевой модели, 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. Обновление системы

Обновление ППО X-IDBox представляет собой регламентированную процедуру, выполняемую для установки новой версии системы, либо отдельных её компонентов.

Процесс обновления включает следующие сценарии:

- полное обновление версии (обновление всех сервисов X-IDBox);
- частичное обновление (обновление отдельных сервисов, включая hotfix-поставки);
- восстановление предыдущей версии в случае неуспешного обновления.

Обновление проводится с использованием штатного менеджера пакетов как при установке из доступного репозитория, так и при установке из локальных пакетов ППО X-IDBox, предварительно размещённых на целевых хостах.

Все операции обновления выполняются пользователем, обладающим административным доступом ко всем серверам, на которых развернуты сервисы системы.

6.1. Подготовка к обновлению

Подготовка к обновлению системы X-IDBox включает выполнение обязательных предварительных действий, направленных на обеспечение корректности процесса обновления и возможности восстановления работоспособности системы в случае возникновения ошибок.

6.1.1. Проверки перед началом работ

Перед началом выполнения работ по обновлению выполните следующие проверки:

- 1) Проверьте доступность источника обновлений:

- при использовании корпоративного репозитория, содержащего пакеты ППО X-IDBox, подтверждена доступность новых версий пакетов с каждого целевого хоста;

- при установке из локальных пакетов ППО X-IDBox подтверждено наличие полного набора обновляемых пакетов на каждом целевом хосте.

2) Проверьте наличие достаточного свободного места на всех серверах, содержащих сервисы X-IDBox, для загрузки и установки пакетов, хранения временных файлов и резервных копий БД.

3) Проверьте готовность конфигурационных файлов (при необходимости). Если поставка обновления содержит изменения или добавление новых конфигурационных параметров, требуется заранее подготовить необходимые конфигурации в соответствии с технической документацией или рекомендациями.

6.1.2. Резервное копирование

Резервное копирование является обязательным этапом подготовки и должно включать:

1) Базы данных:

- при полном обновлении – резервное копирование всех БД X-IDBox;
- при частичном обновлении – резервное копирование только тех БД, с которыми взаимодействуют обновляемые сервисы (при наличии информации об изменении структуры БД в описании версии).

2) Конфигурационные файлы:

- актуальные конфигурационные файлы сервисов X-IDBox;
- конфигурационные файлы веб-серверов и ППО «Модуля фильтрации запросов к ИС».

3) Кастомные ресурсы (при наличии):

- резервирование кастомных пользовательских оформлений;

– резервирование файла с изменёнными текстами серверных ошибок «exceptionMessages.properties».

Резервное копирование БД рекомендуется выполнять после остановки соответствующих сервисов X-IDBox, что обеспечивает консистентность данных и отсутствие активных транзакций. Порядок и требования к резервному копированию приведены в п. 9.3.

6.2. Полное обновление системы

Полное обновление предполагает обновление всех сервисов X-IDBox.

Для полного обновления системы выполните следующие действия:

1) Остановите все сервисы X-IDBox на всех хостах системы (см. п. 9.1.3.2).

2) Выполните резервное копирование всех БД (см. п. 6.1.2).

3) Обновите пакеты ППО X-IDBox с помощью менеджера пакетов, например:

```
yum update xidbox-*
```

4) При необходимости примените обновлённые версии конфигурационных файлов, подготовленные в соответствии с п. 6.1.1.

5) Выполните очистку кеша.

6) Запустите все сервисы X-IDBox (см. п. 9.1.3.1).

7) Проверьте работоспособность сервисов X-IDBox (см. п. 9.1.3.4).

8) Проверьте работоспособность системы (см. п. 6.5).

6.3. Частичное обновление системы

Частичное обновление применяется при необходимости обновления отдельных сервисов X-IDBox без остановки всей системы.

Для частичного обновления системы выполните следующие действия:

1) Определите перечень сервисов, подлежащих обновлению (в соответствии с составом дистрибутива).

2) Остановите только те сервисы, которые планируете обновлять (см. п. 9.1.3.2).

3) Для каждого обновляемого сервиса, взаимодействующего с БД (при наличии информации об изменении структуры БД в описании версии), выполните резервное копирование соответствующей БД (см. п. 6.1.2).

4) Обновите пакеты выбранных сервисов, например:

```
yum update xidbox-<service>
```

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

5) При необходимости примените обновлённые версии конфигурационных файлов, подготовленные в соответствии с п. 6.1.1.

6) Выполните очистку кеша. Очистка кеша выполняется при наличии соответствующей информации в описании версии.

7) Запустите обновлённые сервисы (см. п. 9.1.3.1).

8) Проверьте работоспособность обновлённых сервисов X-IDBox (см. п. 9.1.3.4).

9) Проверьте работоспособность системы (см. п. 6.5).

6.4. Восстановление предыдущей версии в случае неуспешного обновления

В случае неуспешного обновления необходимо выполнить возврат к предыдущей стабильной версии системы. Порядок восстановления зависит от типа выполненного обновления.

– После полного обновления:

1) Остановите все сервисы X-IDBox (см. п. 9.1.3.2).

2) Восстановите БД из резервной копии, созданной перед обновлением (см. п. 6.1.2).

3) Верните пакеты ППО X-IDBox к предыдущей версии через менеджер пакетов, например:

```
yum downgrade xidbox-*
```

4) Восстановите конфигурационные файлы из резервной копии.

5) Выполните очистку кеша.

6) Запустите все сервисы X-IDBox (см. п. 9.1.3.1).

7) Проверьте работоспособность системы (см. п. 6.5).

– После частичного обновления:

1) Остановите только те сервисы, которые были обновлены (см. п. 9.1.3.2).

2) Восстановите БД, связанные с обновлёнными сервисами, из резервной копии (см. п. 6.1.2) (при наличии).

3) Верните пакеты обновлённых сервисов к предыдущей версии, например:

```
yum downgrade xidbox-*
```

4) Восстановите конфигурационные файлы из резервной копии.

5) Выполните очистку кеша.

6) Запустите сервисы X-IDBox (см. п. 9.1.3.1).

7) Проверьте работоспособность системы (см. п. 6.5).

6.5. Проверка после обновления и восстановления системы

Проверка выполняется после успешного полного или частичного обновления системы X-IDBox, а также после восстановления предыдущей версии системы в случае неуспешного обновления.

В рамках проверки необходимо:

- убедиться, что все сервисы запущены и функционируют (см. п. 9.1.3.4);
- проверить журналы сервисов на наличие ошибок и критических предупреждений;

– выполнить проверку основных сценариев: аутентификации, идентификации и авторизации.

Для проверки основных сценариев: аутентификации, идентификации и авторизации выполните следующие действия:

1) Перейдите по адресу страницы входа подключённой ИС и убедитесь в её доступности, а также в возможности выполнить аутентификацию пользователя.

2) Выполните вход в подключённую ИС с использованием УЗ пользователя, имеющего доступ к данной ИС, и убедитесь в успешном выполнении аутентификации.

3) После успешного входа убедитесь, что система корректно определяет пользователя.

4) Убедитесь, что доступ пользователя к функциональности системы осуществляется в соответствии с назначенными правами.

5) Проверьте корректность получения данных УЗ пользователя с помощью API ППО «Сервис идентификации». Описание используемых методов API, форматов запросов и ответов приведено в документе «Руководство разработчика. Часть 2. Сервис идентификации». Для получения данных об УЗ пользователя по логину выполните запрос в ППО «Сервис идентификации» API «Получение данных об УЗ пользователя по логину», например:

```
curl --location  
http://{{host}}/identification/api/v2/user?login=<login>
```

6) Убедитесь, что в ответе на запрос возвращаются корректные данные УЗ пользователя, включая его идентификатор (uuid).

7) Проверьте корректность получения данных о профиле УЗ пользователя. Используя значение «uuid», полученное на предыдущем шаге, выполните запрос в ППО «Сервис идентификации» API «Получение информации о профиле УЗ пользователя по идентификатору», например:

```
curl --location  
"http://{{host}}/identification/api/v2/user-profile?uuid=<uuid>"
```

8) Убедитесь, что в ответе на запрос возвращается корректная и соответствующая ожидаемым данным информация о профиле УЗ пользователя.

Проверка авторизации осуществляется путём проверки получения списка ИС, в которых у указанного профиля УЗ пользователя есть доступ.

Описание используемых методов API приведено в документе «Руководство разработчика. Часть 5. Сервис авторизации».

9) Для осуществления проверки выполните запрос в ППО «Сервис авторизации» API «Получение списка ИС, в которых у указанного профиля УЗ пользователя есть доступ», например:

```
curl --location 'http://{{host}}/authz/api/v2/user-  
profiles/info-systems' \  
--header 'Content-Type: application/json' \  
--data '{  
  "userProfiles": [  
    {  
      "userProfileUuid": "<user_profile_uuid>"  
    }  
  ]  
}'
```

10) В параметре «userProfileUuid» укажите uuid профиля УЗ пользователя, полученный на предыдущих шагах проверки идентификации.

11) Убедитесь, что в ответе на запрос возвращается корректный перечень ИС, доступ к которым предоставлен данному профилю УЗ пользователя.

7. Администрирование системы

7.1. Настройка параметров запуска

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

7.1.1. Настройка параметров JVM

Для Java-сервисов X-IDBox предусмотрена возможность настройки параметров виртуальной машины Java (JVM), включая объём heap-памяти и размер стека потоков. Эти параметры задаются с использованием переменной `JAVA_OPTS`, определённой в unit-файлах `systemd`. При необходимости значения по умолчанию могут быть переопределены пользователем через файл `«/etc/default/<имя сервиса>»` для каждого сервиса отдельно (перечень сервисов приведён в таблице 3).

Пример содержимого файла:

```
JAVA_OPTS="-Xmx2048m -Xms512m -Xss10m"
```

Описание параметров JVM:

- `Xmx` – максимальный размер heap-памяти, доступной JVM;
- `Xms` – начальный размер heap-памяти;
- `Xss` – размер стека каждого потока.

Для применения изменённых параметров необходимо выполнить перезагрузку соответствующего сервиса согласно п. 9.1.3.3.

7.2. Управление учётными записями пользователей и назначение пользователям прав доступа

Управление данными УЗ пользователя и правами доступа пользователя осуществляется в веб-интерфейсе X-IDBox, а также с помощью API ППО «Сервис

регистрации и изменения данных пользователей» и ППО «Сервис загрузки назначений», в том числе путём загрузки файлов в специальных форматах, описанных в документе «Руководство разработчика. Часть 11. Форматы файлов для загрузки через пользовательский интерфейс» и «Руководство разработчика. Часть 4. Сервис регистрации и изменения данных пользователей».

Подробное описание загрузки файлов через веб-интерфейс приведено в Руководстве пользователя.

7.3. 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"
    ]
  }
]
```

7.4. Настройка веб-серверов для работы с системой

В составе X-IDBox используется веб-сервер, соответствующий установленной операционной системе: при работе под управлением ОС «РЕД ОС» применяется Nginx, а при использовании ОС «Astra Linux SE» используется Apache2. Настройка веб-серверов для работы системы выполняется в соответствии с описанием, приведённым в п. 5.35.3, с учётом шаблонов конфигурационных файлов, поставляемых в составе дистрибутива для каждой поддерживаемой операционной системы.

Подробные сведения о правилах настройки, конфигурирования и эксплуатации веб-сервера приведены в официальной документации соответствующего ПО. Для получения дополнительной информации следует обращаться к документации Nginx или документации Apache HTTP Server на официальных ресурсах разработчиков.

7.5. Настройка рабочих станций пользователей для работы с системой

Описание подготовки рабочих станций пользователей приведено в Руководстве пользователя.

7.6. Настройки 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 «е»;
- 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».

7.7. Добавление настраиваемых функций для условий применимости ролей и политик авторизации

При необходимости расширить список доступных функций для использования в условиях применимости ролей и политик авторизации необходимо зарегистрировать настраиваемые функции. Для этого требуется написать выражение в SpEL-нотации с учётом следующих требований:

- Наименование функции должно содержать латинские символы (в любом регистре) и `_`, не должно пересекаться с существующими наименованиями функций и зарезервированными словами: `this`, `super`.

- Тип данных выходного аргумента – логический.

Далее необходимо указать название функции и тело функции (выражение в SpEL-нотации) в соответствующей настройке:

- Для унарной функции – `xidbox.authz.spel.custom-method.unary.<наименование функции>=<тело функции>`. Например: `xidbox.authz.spel.custom-method.unary.IS_EMPTY=right.isEmpty()`, где `IS_EMPTY` – наименование функции, а `right.isEmpty()` – её тело.

- Для бинарной функции – `xidbox.authz.spel.custom-method.binary.<наименование функции>=<тело функции>`. Например: `xidbox.authz.spel.custom-method.binary.ANY_MATCH=left.stream().noneMatch(#predicate('entity.uuid.equals(right)', attributes))`, где `ANY_MATCH` – наименование функции, а `left.stream().noneMatch(#predicate('entity.uuid.equals(right)', attributes))` – её тело.

7.8. Кастомизация атрибутов сессии

Набор атрибутов сессии, сохраняемых в истории сессий, при необходимости, можно изменить. Список заголовков запроса, которые сохраняются в виде атрибутов сессии, задается в таблице «session_header» основной БД x_idbox_database.

Чтобы данные сохранялись корректно, заголовки должны передаваться в запросах к сервису xidbox-authn-gateway или проксироваться на уровне веб-сервера Apache2 / Nginx следующим образом:

- В конфигурации Apache2 необходимо настроить проксирование требуемых заголовков в файле «проxy-params.conf» из прилагаемых дистрибутивов.

- В конфигурации Nginx необходимо добавить требуемый заголовок в блок «rewrite_by_lua_block» всех location, где есть этот блок (файлы «xidbox.conf» и «проxy.locations» из прилагаемых дистрибутивов).

7.8.1. Добавление нового атрибута сессии

Для добавления нового атрибута сессии, содержащего IP-адрес сервиса xidbox-authn-gateway, который обрабатывал аутентификацию пользователя, выполните следующие действия:

- 1) Добавьте новый заголовок в таблицу «session_header» основной БД x_idbox_database:

```
INSERT INTO x_id_box.session_header (id, name,
label, order_number) VALUES (3, 'x-custom-header',
'IP адрес сервиса authn-gateway', 3)
```

- 2) В зависимости от используемого веб-сервера:

- При использовании Apache2 добавьте следующую строку в файл «проxy-params.conf»:

```
RequestHeader set X-Custom-Header
"expr=%{REMOTE_ADDR}"
```

– При использовании Nginx добавьте во все блоки «rewrite_by_lua_block» в файлах «xidbox.conf» и «proxy.locations» следующую строку:

```
ngx.req.set_header("X-Custom-Header",  
ngx.var.remote_addr)
```

Например, было:

```
location /api/v1/auth/user {  
    rewrite_by_lua_block {  
        ngx.req.set_header("X-Real-IP",  
ngx.req.get_headers()["X-Real-IP"] or  
ngx.var.remote_addr)  
    }  
    access_by_lua_file  
/etc/nginx/lualib/user_profile_selection.lua;  
    include /etc/nginx/conf.d/proxy.pass;  
}
```

Стало:

```
location /api/v1/auth/user {  
    rewrite_by_lua_block {  
        ngx.req.set_header("X-Real-IP",  
ngx.req.get_headers()["X-Real-IP"] or  
ngx.var.remote_addr)  
        ngx.req.set_header("X-Custom-Header",  
ngx.var.remote_addr)  
    }  
    access_by_lua_file  
/etc/nginx/lualib/user_profile_selection.lua;  
    include /etc/nginx/conf.d/proxy.pass;  
}
```

3) Перезапустите Apache2 / Nginx, в зависимости от используемого веб-сервера.

4) Перезапустите сервис xidbox-cache-service / очистите кеш.

8. Подключение информационной системы

8.1. 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.

8.2. 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) Добавьте файл в директорию «/etc/nginx/conf.d/» для Модуля фильтрации запросов к ИС. Данный файл обеспечивает отображение страницы аутентификации и проксирование запросов от аутентифицированных пользователей,

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;

```

}

Исключение составляют новые ИС, подключаемые только через OAuth 2.0-клиент – для них добавление настроек в модуль не требуется.

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).

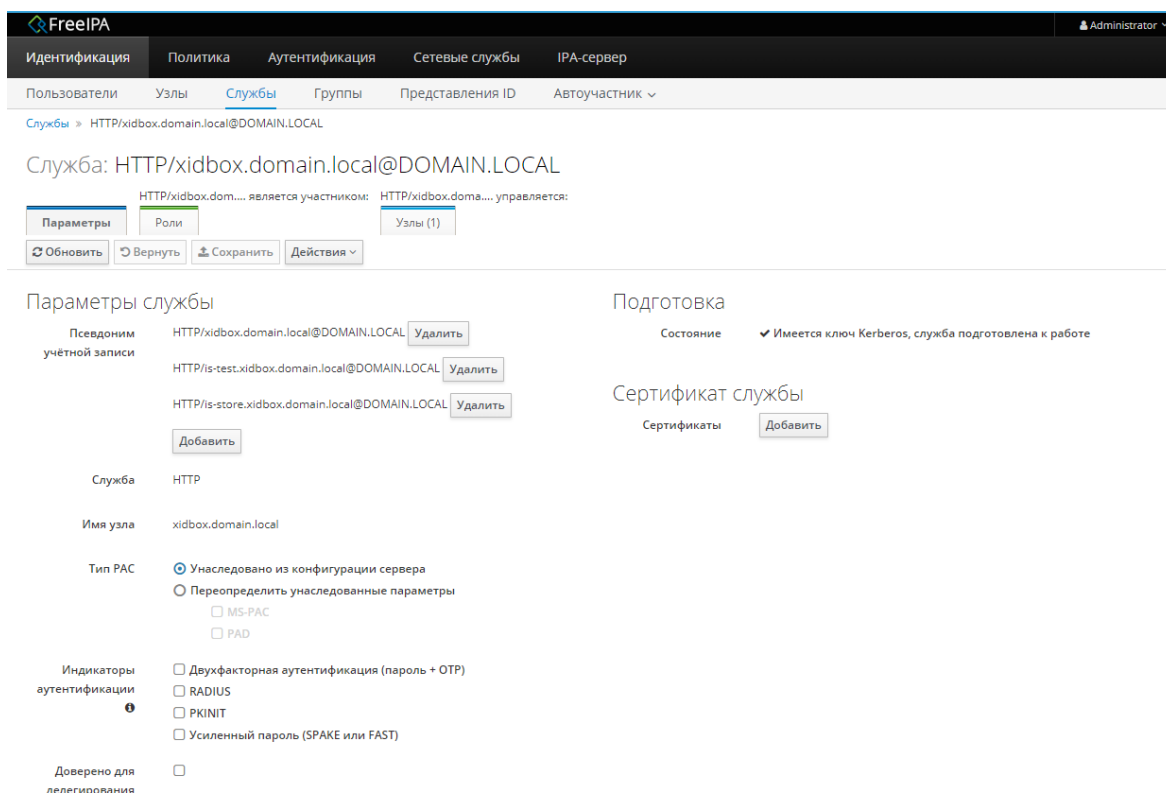


Рисунок 6 – Псевдоним для службы в FreeIPA с указанием внешнего адреса ИС

Порядок настройки для ALD Pro:

Процедура настройки на контроллере домена ALD Pro аналогична процедуре для FreeIPA, описанной выше.

8.3. 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.

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

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

Синтаксис написания шаблонов:

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

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

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

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

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

2) Продолжите в зависимости от результата выполненного запроса:

- Запрос не вернул данные – перейдите к шагу 3).
- 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 3).
- Запрос вернул данные и `oauth_client_id == "null"`, при этом `oauth_access == true` – перейдите к шагу 4).
- Запрос вернул данные и `oauth_client_id != "null"` – для данной ИС уже есть зарегистрированный OAuth 2.0-клиент. Дополнительных действий не требуется.

3) 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
    }
  ]
}
```

4) 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, ouath_client_mnemonic,
oauth_client_secret);

--связывание ИС и OAuth 2.0-клиента
update x_id_box.information_system
set ouath_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
(ouath_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(ouath_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),
ouath_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
$$;
```

- 5) Очистите кеш.
- 6) Передайте ИС сгенерированный секретный код (client_secret).

8.4. 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».

8.5. Создание пользователя с ролью «Менеджер ИС»

Для создания пользователя с ролью «Менеджер ИС» при использовании пользовательского интерфейса управления доступом X-IDBox:

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>"
    }
  ]
}
```

8.6. 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);
```

9. Обслуживание системы

9.1. Порядок обслуживания и проверка работоспособности системы

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

9.1.1. Управление СУБД

Запуск, остановка и перезагрузка кластеров СУБД выполняются в соответствии с официальной документацией.

Тип используемой СУБД и документации определяется выбранным вариантом установки и настройки, указанным в п. 3.6.1 и 3.6.2.

Если используется Postgres Pro версии не ниже 14 (LTS) – все операции управления кластером (запуск, остановка, перезагрузка, проверка статуса, управление репликами) выполняются в соответствии с официальной документацией Postgres Pro:

<https://postgrespro.ru/docs>

Если используется PostgreSQL из состава ОС «Astra Linux SE» – управление кластером выполняется в соответствии с официальной документацией ОС «Astra Linux SE» «Руководство по КСЗ. Часть 3. Защищенная СУБД», с учётом особенностей установленной версии PostgreSQL и параметров защищённого режима.

9.1.2. Управление веб-сервером

Все операции по запуску, остановке, перезапуску и проверке состояния веб-сервера выполняются в соответствии с официальной документацией соответствующего ПО:

- Nginx: <http://nginx.org/ru/docs>;
- Apache2: <https://httpd.apache.org/docs/2.4>.

9.1.3. 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
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 «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	Название управляемого сервиса
ППО «Сервис валидации данных»	xidbox-validation
ППО «Сервис выполнения автоматических расчетов»	xidbox-request-background-processing
ППО «Сервис работы с архивом заявок»	xidbox-order-archive-database
ППО «Сервис работы с БД внутренних уведомлений»	xidbox-internal-message-database
ППО «Сервис загрузки справочников»	xidbox-dictionary-upload
ППО «Сервис кеширования данных»	xidbox-cache

9.1.3.1. Запуск

На сервере с установленным сервисом выполните команду:

```
systemctl start <service>
```

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

9.1.3.2. Остановка

На сервере с установленным сервисом выполните команду:

```
systemctl stop <service>
```

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

9.1.3.3. Перезагрузка

На сервере с установленным сервисом выполните команду:

```
systemctl restart <service>
```

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

9.1.3.4. Мониторинг работоспособности

На сервере с установленным сервисом выполните команду:

```
systemctl status <service>
```

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

9.1.3.5. Мониторинг состояния

Для мониторинга состояния сервисов и их корректной работы используются актуаторы в соответствии с таблицей 4.

Таблица 4 – Перечень управляемых сервисов ППО X-IDBox и соответствующих им актуаторов

ППО	URL-адрес актуатора
ППО «Сервис аутентификации»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
Модуль фильтрации запросов к ИС	–
ППО «Сервис авторизации»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис обработки данных»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Модуль отправки уведомлений информационным системам с использованием Kafka»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Модуль отправки уведомлений информационным системам с использованием RabbitMQ»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Модуль отправки уведомлений информационным системам с использованием REST»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис работы с основными БД»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис синхронизации данных каталогов»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
Модуль балансировки внутренних запросов	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис взаимодействия с пользовательским интерфейсом управления доступом»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис идентификации»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис интеграции с LDAP-каталогами»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator

ППО	URL-адрес актуатора
ППО «Сервис обработки заявок»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис организации выполнения заявок»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис изменения заявок»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис загрузки организаций»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис загрузки ОШС»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис загрузки ролевых моделей»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис автоматических операций»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис обеспечения целостности данных»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис работы с данными заявок»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис работы с очередью заявок»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис работы с исходными данными заявок»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис загрузки назначений»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис регистрации и изменения данных пользователей»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис валидации данных»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис выполнения автоматических расчетов»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис работы с архивом заявок»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис работы с БД внутренних уведомлений»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис загрузки справочников»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator
ППО «Сервис кеширования данных»	http://<SERVICE-HOST>:<SERVICE-PORT>/actuator

9.2. 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 5.

Таблица 5 – 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 43	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 43	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 6.

Таблица 6 – Ключи для дополнительных данных о событиях безопасности

Наименование ключа	Значение ключа	Описание
cs1Label	objectUid	Идентификатор объекта, с которым было выполнено соответствующее действие
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	Способ 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.

9.3. Резервное копирование и восстановление данных

Требования, порядок и периодичность выполнения процедур резервного копирования и восстановления данных для СУБД PostgreSQL/PostgresPro, необходимых для работы системы X-IDBox, описаны ниже.

Основной целью выполнения резервного копирования является обеспечение сохранности и целостности данных, минимизация времени простоя сервисов в случае возникновения нештатных ситуаций (аппаратные сбои, ошибки персонала, повреждение файловой системы), а также обеспечение возможности восстановления данных на заданный момент времени (PITR).

9.3.1. Объекты резервного копирования

Процедуре резервного копирования подлежат:

1) Все БД ИС X-IDBox:

- x_id_box_scheduler, x_idbox_database (Оперативная БД);
- x_idbox_maintenance (БД автоматических расчетов);
- sm, state_machine_queue, storage (БД заявок);
- archive_order (БД архивных заявок);
- x_idbox_internal_message (БД внутренних уведомлений).

2) Системные БД (postgres, template0, template1) – для консистентности данных кластера БД.

3) Конфигурационные файлы PostgreSQL/PostgresPro:

- postgresql.conf – основные параметры кластера;
- pg_hba.conf – настройки аутентификации и сетевых подключений;
- pg_ident.conf – правила сопоставления пользователей;
- дополнительные параметры (например, standby.signal для физической репликации).

4) Файлы журналов WAL для обеспечения возможности восстановления до произвольной точки времени (PITR).

9.3.2. Применяемые методы и инструменты резервного копирования

Допускается использование исключительно следующего перечня утилит и методов, предоставляемых пакетом PostgreSQL, входящих в состав сертифицированного дистрибутива ОС, или сертифицированными средствами PostgresPro:

1) Логическое резервирование:

- pg_dump – утилита создания дампа отдельной БД;
- pg_dumpall – утилита создания дампа всего кластера БД, включая глобальные объекты (роли и табличные пространства).

2) Физическое резервирование:

– pg_basebackup – базовая утилита создания бинарной копии каталога данных СУБД;

– pg_probackup – утилита расширенного управления физическими резервными копиями, поддерживающая инкрементальное и дельта-копирование, верификацию и управление политиками хранения.

3) Непрерывное архивирование:

– WAL-архивирование – обязательная процедура сохранения файлов журнала предзаписи во внешнее хранилище для обеспечения возможности восстановления на момент времени (PITR).

9.3.3. Конфигурационные требования к серверу СУБД

Для обеспечения технической возможности выполнения непрерывного архивирования WAL и снятия корректных физических резервных копий администратор обязан установить следующие значения параметров конфигурационного файла postgresql.conf, приведенные в таблице 7.

Таблица 7 – Значения параметров конфигурационного файла

Параметр	Требуемое значение	Описание
wal_level	replica	Минимально достаточный уровень логирования для поддержки репликации и PITR
archive_mode	on	Активация механизма перехвата и архивирования сегментов WAL
archive_command	Определяется администратором	Указание системной команды для безопасного перемещения сегмента WAL в выделенное архивное хранилище

Каталог, используемый в качестве приемника для архива WAL, должен располагаться на отдельном физическом носителе или сетевом файловом ресурсе, отличном от хранилища основных файлов данных СУБД. Доступ к данному каталогу должен быть предоставлен системной учетной записи, от имени которой выполняется процесс СУБД.

9.3.4. Периодичность выполнения резервного копирования

Периодичность выполнения резервного копирования индивидуальна для каждого метода:

1) Логическое копирование:

- Периодичность – ежедневно, в период регламентного технологического окна с минимальной нагрузкой на дисковую подсистему.

- Формат хранения – рекомендуется использование сжатого пользовательского формата, обеспечивающего гибкость при выборочном восстановлении.

- Целевое назначение – формирование переносимой копии для целей аудита и оперативного восстановления отдельных объектов схемы данных.

2) Физическое копирование:

- Базовая копия (pg_basebackup/pg_probackup) – выполняется с периодичностью, установленной для конкретного класса ИС, но не реже одного раза в семь календарных дней.

- Инкрементальное копирование (функция pg_probackup) – рекомендуется к применению в продуктивных средах с высокой интенсивностью изменений данных для минимизации окна резервирования и объема передаваемых данных. Периодичность устанавливается не реже одного раза в календарные сутки.

3) Непрерывное архивирование WAL – осуществляется в автоматическом режиме. Администратор должен обеспечить мониторинг состояния каталога архива, не допуская его переполнения и своевременно применяя политику ротации устаревших сегментов.

9.3.5. Восстановление данных

Восстановление из логического дампа применяется в случаях, когда требуется перенос данных на иную версию платформы, выборочное восстановление утраченных записей или когда глубина архива WAL недостаточна

для физического восстановления. Процедура предполагает предварительное создание пустой БД-приемника и последующее восстановление объектов из файла дампа.

Восстановление на момент времени (PITR) на основе физической копии – метод является основным сценарием ликвидации последствий аварийных ситуаций. Процедура включает следующие шаги:

- 1) Остановка сервера СУБД.
- 2) Замещение текущего содержимого каталога данных содержимым последней валидной физической копии.
- 3) Конфигурирование директив восстановления: указание пути к архиву WAL и требуемой временной отметки остановки восстановления.
- 4) Размещение файла-триггера начала процедуры восстановления.
- 5) Запуск сервера СУБД в режиме восстановления до выхода в штатный режим работы.

9.3.6. Политика хранения и ротации резервных копий

Сроки хранения устанавливаются в зависимости от типов резервной копии, приведенных в таблице 8.

Таблица 8 – Рекомендуемые сроки хранения

Тип резервной копии	Рекомендуемый срок хранения
Логические дампы (pg_dump, pg_dumpall)	30 суток
Полные физические копии (pg_basebackup, pg_probackup)	14 суток
Инкрементальные копии (pg_probackup)	До момента удаления родительской полной копии
Архивные сегменты WAL	Срок, эквивалентный глубине хранения полной копии, плюс двое суток

По истечении установленного срока файлы резервных копий подлежат автоматическому удалению средствами планировщика задач или встроенными механизмами утилиты pg_probackup.

9.3.7. Хранение резервных копий

Хранение резервных копий и журналов предзаписи (WAL) должно быть организовано в выделенном хранилище, отличном от основного хоста, на котором функционирует экземпляр СУБД.

Хранилище резервных копий должно соответствовать критериям, приведенным в таблице 9.

Таблица 9 – Требования к организации хранилища резервных копий

Критерий	Требование
Отказоустойчивость	Хранилище должно быть размещено на отдельном физическом устройстве, сетевом ресурсе (NAS/SAN) или объектном хранилище (S3-совместимом), исключаящем единую точку отказа с основным сервером СУБД
Консистентность данных	Файловая система или протокол доступа к хранилищу должны гарантировать атомарность операций записи и целостность файлов резервных копий и сегментов WAL
Доступность	Хранилище должно обеспечивать бесперебойный доступ для операций чтения и записи со стороны сервера СУБД в режиме, приближенном к постоянному (24/7), для обеспечения корректной работы механизма непрерывного архивирования WAL

9.3.7.1. Состав данных, подлежащих обязательному хранению

Не зависимо от выбранного метода создания резервной копии (логического или физического), в хранилище должны быть размещены следующие компоненты, обеспечивающие полноценное восстановление работоспособности системы:

1) Конфигурационные файлы экземпляра СУБД – полный набор параметров, определяющих поведение сервера (postgresql.conf), правила аутентификации (pg_hba.conf) и правила сопоставления пользователей (pg_ident.conf).

2) Данные БД – содержимое пользовательских и системных БД, полученное в результате выполнения регламентных процедур резервного копирования средствами утилит `pg_dump`, `pg_dumpall`, `pg_basebackup` или `pg_probackup`.

3) Журналы предзаписи (WAL) – полный набор сегментов WAL, заархивированных в период между созданием последовательных полных или инкрементальных резервных копий, необходимый для выполнения восстановления на момент времени (PITR).

9.3.7.2. Обеспечение готовности к восстановлению

Резервные копии, размещенные в хранилище, должны находиться в состоянии, пригодном для немедленного использования в рамках процедур аварийного восстановления. Администратор СУБД должен обеспечить:

- наличие актуальной документации с указанием сетевого пути, протокола доступа и учетных данных для подключения к хранилищу в аварийной ситуации;
- соответствие сроков хранения данных в хранилище, установленное в п. 9.3.6;
- отсутствие повреждений и искажений в хранимых файлах, подтверждаемое результатами плановых проверок целостности.

9.3.8. Контроль качества и аудит

Плановая проверка возможности восстановления (Disaster Recovery Test) проводится не реже одного раза в год на технологическом стенде, изолированном от продуктивной среды.

Процедура проверки включает:

- полное восстановление кластера из последней базовой резервной копии `pg_probackup` / `pg_basebackup`;
- восстановление на произвольный момент времени с использованием архива WAL;

- верификацию целостности данных путем выполнения контрольных SQL-запросов (сравнение количества строк в ключевых таблицах или подсчет контрольных сумм).

В ходе плановой проверки подтверждаются следующие показатели:

- читаемость и целостность последней созданной физической копии;
- корректность применения последовательности WAL-файлов для достижения заданной точки восстановления;
- консистентность (логическая непротиворечивость) данных по завершении процедуры.

Все действия по изменению конфигурации архивирования, запуску внепланового копирования или восстановления данных подлежат обязательной регистрации в журнале учета работ с указанием точного времени и идентификатора системы.

9.4. Настройка мониторинга системы

Настройка мониторинга выполняется с целью обеспечения непрерывного контроля состояния инфраструктурных компонентов и сервисов системы, а также своевременного выявления возможных отказов, деградации производительности и аномального поведения компонентов.

Для организации централизованного сбора, хранения и визуализации метрик рекомендуется использование следующего набора специализированных программных средств:

- Zabbix. (Базовый мониторинг виртуальных машин, контроль доступности сервисов и сбор инфраструктурных метрик, настройка оповещений).
- Prometheus. (Сбор, хранение и обработка метрик приложений и сервисов в формате временных рядов).
- Grafana. (Визуализация данных, построение аналитических дашбордов и настройка оповещений).

Установка и настройка указанных программных средств выполняется в соответствии с официальной документацией производителей:

- Zabbix: <https://www.zabbix.com/documentation>
- Prometheus: <https://prometheus.io/docs>
- Grafana: <https://grafana.com/docs>

9.4.1. Мониторинг инфраструктурных компонентов

9.4.1.1. Выбор системы

Для мониторинга инфраструктурных компонентов (операционных систем, сетевых интерфейсов и дисковых подсистем) рекомендуется использовать следующие системы мониторинга: Zabbix (основной вариант) или Prometheus (альтернативный вариант).

9.4.1.2. Настройка node_exporter (при использовании Prometheus)

При использовании Prometheus для мониторинга инфраструктурных компонентов на контролируемые узлы необходимо установить экспортер системных метрик node_exporter.

Экспортер node_exporter предоставляет метрики операционной системы в формате, совместимом с системой мониторинга Prometheus, через конечную точку (по умолчанию порт 9100). Сбор метрик осуществляется путем периодического опроса данной конечной точки сервером Prometheus.

Установка и настройка node_exporter выполняется в соответствии с официальной документацией:

<https://prometheus.io/docs/guides/node-exporter/>

9.4.1.3. Минимально необходимые инфраструктурные метрики

С использованием Zabbix, Prometheus и Grafana рекомендуется осуществлять мониторинг следующего базового набора инфраструктурных метрик:

- загрузка центрального процессора (CPU Usage);
- использование оперативной памяти (Memory Usage);
- использование дискового пространства (Disk Space Usage);
- показатели дисковых операций ввода-вывода (Disk I/O);
- сетевые показатели (входящий и исходящий трафик);
- системная нагрузка (Load Average);
- количество открытых файловых дескрипторов (File Descriptors);
- доступность узла мониторинга (Host Availability).

9.4.2. Мониторинг ППО X-IDBox

Мониторинг ППО X-IDBox осуществляется через встроенный механизм Spring Boot Actuator, предоставляющий метрики в формате Prometheus по конечной точке /actuator/prometheus.

9.4.2.1. Включение конечной точки метрик

В файле конфигурации и взаимодействия сервисов «xidbox.properties», подготовленном в результате выполнения действий, описанных в п. 4.1, необходимо активировать соответствующие конечные точки Actuator.

Пример конфигурации:

```
xidbox.<SERVICE_NAME>.service.management.endpoints.  
web.exposure.include = health,prometheus,metrics
```

Расширенный перечень настроек сервисов приведен в Приложении Б.

Для применения измененных параметров необходимо выполнить перезагрузку соответствующего сервиса согласно п. 9.1.3.3.

9.4.2.2. Доступ к метрикам

После успешной настройки метрики микросервиса доступны по следующему URL-пути:

```
http://<SERVICE-HOST>:<SERVICE-PORT>/actuator/prometheus
```

9.4.2.3. Настройка задачи сбора в Prometheus

Для конфигурации сбора метрик с сервиса X-IDBox в файл конфигурации Prometheus (prometheus.yml) необходимо добавить задачу (job) в секцию «scrape_configs»:

```
scrape_configs:
  - job_name: "<JAVA-SERVICE>"
    metrics_path: '/actuator/prometheus'
    static_configs:
      - targets:
        - "<SERVICE-HOST>:<SERVICE-PORT>"
```

9.4.2.4. Отслеживаемые JVM-метрики

Осуществляется сбор следующих метрик, приведенных в таблице 10.

Таблица 10 – Отслеживаемые JVM-метрики

Метрика	Описание
process_uptime_seconds	Время действия процесса в секундах
jvm_memory_used_bytes	Объём используемой памяти (heap или non-heap) в байтах
http_server_requests_seconds_count	Общее количество HTTP-запросов, полученных приложением
http_server_requests_seconds_sum	Суммарное время обработки всех HTTP-запросов в секундах
http_server_requests_seconds_max	Максимальное время обработки одного HTTP-запроса
jvm_memory_used_bytes	Объём используемой памяти (heap или non-heap) в байтах
jvm_memory_committed_bytes	Объём выделенной (зарезервированной) JVM памяти в байтах

Метрика	Описание
jvm_memory_max_bytes	Максимально допустимый объём памяти, который может использовать JVM
process_cpu_usage	Использование CPU текущим процессом
system_load_average_1m	Средняя нагрузка на систему за последнюю 1 минуту
process_files_open_files	Текущее количество открытых файловых дескрипторов процессом
process_files_max_files	Максимально допустимое количество открытых файлов для процесса (ulimit)
jvm_threads_states_threads	Количество потоков по состояниям (RUNNABLE, WAITING, BLOCKED, и т.д.)
logback_events_total	Общее количество лог-сообщений, разбитое по уровням (INFO, WARN, ERROR, и т.д.)
jvm_threads_live_threads	Текущее количество активных потоков
jvm_threads_daemon_threads	Количество активных потоков-демонов
jvm_threads_peak_threads	Пиковое количество потоков с момента запуска
jvm_gc_pause_seconds_count	Количество пауз на сборку мусора
jvm_gc_pause_seconds_sum	Общее время, затраченное на GC паузы
jvm_gc_pause_seconds_max	Максимальная длительность одной GC паузы
jvm_gc_memory_allocated_bytes_total	Всего выделено памяти в heap между GC
jvm_gc_memory_promoted_bytes_total	Объём памяти, перемещённый из young generation в old generation
jvm_buffer_memory_used_bytes	Используемая память для java.nio.Buffer в байтах
jvm_buffer_total_capacity_bytes	Общая вместимость всех буферов (ByteBuffer, etc.) в байтах
jvm_buffer_count_buffers	Количество буферов в JVM

9.4.3. Мониторинг Nginx

9.4.3.1. Включение модуля stub_status

Мониторинг Nginx осуществляется через встроенный модуль «ngx_http_stub_status_module». Для его активации внесите изменения в конфигурационный файл «/etc/nginx/nginx.conf»:

- 1) Добавьте блок «location» следующего содержания:

```

nginx
location /nginx_status {
    stub_status;
    allow 127.0.0.1;
    deny all;
}

```

```
}
```

- 2) После внесения изменений выполните перезапуск сервиса Nginx.

9.4.3.2. Доступ к метрикам

После успешной активации модуля метрики доступны по адресу:

http://localhost/nginx_status

9.4.3.3. Отслеживаемые метрики

Осуществляется сбор следующих показателей, приведенных в таблице 11.

Таблица 11 – Отслеживаемые метрики Nginx

Метрика	Описание
Active connections	Общее количество открытых в текущий момент соединений
Accepts	Общее количество клиентских соединений, принятых сервером
Handled	Общее количество обработанных соединений
Requests	Общее количество обработанных HTTP-запросов
Reading	Количество соединений, в которых Nginx читает заголовок запроса
Writing	Количество соединений, в которых Nginx отправляет ответ клиенту
Waiting	Количество бездействующих (keep-alive) соединений в ожидании нового запроса

9.4.4. Мониторинг Apache2

9.4.4.1. Включение модуля mod_status

Мониторинг Apache2 осуществляется через встроенный модуль mod_status, который предоставляет страницу с текущим состоянием сервера в формате, пригодном для автоматического парсинга. Для его активации выполните следующие действия:

- 1) Активируйте модуль:

```
sudo a2enmod status
```

2) Отредактируйте файл конфигурации модуля «/etc/apache2/mods-enabled/status.conf», настроив доступ и включив расширенную статистику:

```
<Location "/server-status">
    SetHandler server-status
    # Ограничение доступа: разрешить только с
    локального хоста и серверов мониторинга
    Require local
    Require ip 127.0.0.1 ::1
    Require ip <IP-адрес_сервера_Prometheus>
</Location>

# Включение расширенной статистики (рекомендуется)
ExtendedStatus On
```

3) Примените изменения, перезапустив Apache2:

```
sudo systemctl restart apache2
```

9.4.4.2. Доступ к метрикам

После успешной активации модуля метрики будут доступны по двум адресам:

- для просмотра администратором: `http://<HOST>/server-status`
- для автоматического сбора (машинный формат): `http://<HOST>/server-status?auto`

9.4.4.3. Настройка сбора метрик в Prometheus

Prometheus не поддерживает разбор формата ответа Apache `mod_status`, поэтому необходимо использовать промежуточный экспортер – Apache exporter.

Установка и настройка экспортера Apache exporter выполняется в соответствии с официальной документацией:

<https://prometheus.io/docs/instrumenting/exporters/> (раздел «Apache exporter»).

9.4.4.4. Отслеживаемые метрики

Осуществляется сбор ключевых показателей, получаемых через Apache Exporter, приведенных в таблице 12.

Таблица 12 – Отслеживаемые метрики Apache Exporter

Метрика	Описание
apache_up	Доступность веб-сервера для мониторинга
apache_uptime_seconds_total	Время непрерывной работы сервера в секундах
apache_accesses_total	Общее количество обработанных запросов
apache_scoreboard	Состояние слотов (рабочих процессов/поток): waiting, starting, reading, sending, keepalive, closing, logging, finishing, idle_cleanup, open
apache_workers	Количество рабочих процессов/поток в разных состояниях: busy, idle
apache_sent_kilobytes_total	Общий объем переданных данных в килобайтах
apache_cpu_load	Текущая загрузка CPU процессом Apache (доступно при ExtendedStatus On)

9.4.5. Мониторинг СУБД Postgres Pro / PostgreSQL

9.4.5.1. Выбор системы мониторинга

Для мониторинга СУБД Postgres Pro / PostgreSQL рекомендуется использовать систему мониторинга Zabbix (основной вариант) с применением стандартных шаблонов мониторинга PostgreSQL, поставляемых вместе с дистрибутивом Zabbix.

В качестве альтернативного решения для мониторинга PostgreSQL может использоваться Prometheus со специализированным экспортером postgres_exporter.

9.4.5.2. Настройка postgres_exporter (при использовании Prometheus)

При использовании Prometheus для сбора метрик PostgreSQL необходимо установить и настроить экспортер метрик postgres_exporter, который обеспечивает предоставление метрик БД в формате, совместимом с Prometheus.

Установка и настройка экспортера `postgres_exporter` выполняется в соответствии с официальной документацией:

<https://prometheus.io/docs/instrumenting/exporters/> (раздел «PostgreSQL exporter»).

9.4.5.3. Основные метрики PostgreSQL

Мониторинг PostgreSQL должен обеспечивать сбор и анализ следующих основных метрик состояния БД, приведенных в таблице 13.

Таблица 13 – Отслеживаемые метрики PostgreSQL

Метрика		Описание
Доступность БД		Состояние экземпляра (доступен / недоступен)
Количество активных подключений		Текущее число подключений в сравнении с лимитом <code>max_connections</code>
Использование дискового пространства		Объём, занимаемый БД на диске, и динамика его роста
Состояние репликации	lag replication	Величина отставания реплики от мастера в байтах и секундах
	статус репликации	Streaming/paused/stopped
Роль сервера		Текущее состояние (master / replica / standby)

9.4.6. Рекомендации по организации мониторинга резервного копирования

Мониторинг процессов резервного копирования является неотъемлемой частью стратегии обеспечения отказоустойчивости данных. Отсутствие или некорректная настройка средств мониторинга создает риск возникновения ситуации, при которой факт неработоспособности системы резервирования обнаруживается только в момент попытки аварийного восстановления.

Целью организации мониторинга резервного копирования является:

- своевременное выявление отклонений в работе механизмов резервного копирования;
- оперативное оповещение ответственного персонала о возникновении нештатных ситуаций;

– обеспечение подтверждения факта успешного выполнения регламентных процедур.

Система мониторинга резервного копирования должна охватывать следующие ключевые аспекты:

- факт и статус завершения процедур создания резервных копий;
- непрерывность процесса архивирования WAL;
- доступность и достаточность свободного пространства в целевом хранилище;
- сроки актуальности (возраст) имеющихся резервных копий.

9.4.6.1. Критические параметры, подлежащие контролю

При организации мониторинга резервного копирования контролю подлежат следующие параметры:

- 1) Контроль выполнения процедур создания резервных копий.

Администратор должен обеспечить автоматизированную проверку следующих условий, приведенных в таблице 14.

Таблица 14 – Параметры, подлежащие контролю

Контролируемый параметр	Критерий штатного состояния
Код завершения утилит <code>pg_dump</code> , <code>pg_dumpall</code> , <code>pg_basebackup</code> , <code>pg_probackup</code>	Успешное завершение с нулевым кодом возврата
Факт создания файла резервной копии в целевом каталоге	Наличие файла с меткой времени, соответствующей текущей дате регламентного запуска
Ненулевой размер итогового файла резервной копии	Размер файла превышает минимальный пороговый уровень, исключающий запись пустого или поврежденного дампа
Статус выполнения команды <code>pg_probackup</code>	Отсутствие статусов <code>ERROR</code> , <code>CORRUPT</code> или <code>EXPIRED</code> в выводе утилиты для последней выполненной копии

- 2) Контроль состояния непрерывного архивирования WAL. Особое внимание должно уделяться мониторингу механизма `archive_command`, так как его длительная неработоспособность приводит к риску потери данных за период после создания последней полной копии.

Необходимо обеспечить контроль следующих параметров:

- Контроль наличия ошибок архивирования. В системном журнале СУБД PostgreSQL не должны присутствовать записи уровня ERROR или WARNING, содержащие текст «archive command failed».

- Контроль отставания архивирования. Администратору рекомендуется реализовать проверку разницы между временем модификации последнего заархивированного сегмента WAL в хранилище и текущим системным временем. Превышение порогового значения, равного удвоенному параметру `archive_timeout`, свидетельствует о потенциальной проблеме в канале передачи данных или переполнении хранилища.

3) Контроль дискового пространства хранилища резервных копий. Переполнение файловой системы, используемой для хранения архива WAL или файлов резервных копий, является одной из наиболее частых причин отказа системы резервирования.

Рекомендуется настроить мониторинг свободного пространства со следующими пороговыми значениями:

- Предупредительный порог – при занятости 80% объема хранилища.
- Критический порог – при занятости 90% объема хранилища.

4) Контроль актуальности резервных копий.

Для соблюдения требований политики хранения данных и обеспечения возможности восстановления данных за заданный период необходимо регулярно контролировать временную метку последней успешно созданной резервной копии каждого типа. Максимально допустимые сроки актуальности резервных копий приведены в таблице 15.

Таблица 15 – Максимально допустимые сроки актуальности резервных копий

Тип резервной копии	Максимально допустимый срок актуальности
Последняя полная физическая копия	Не более 24 часов с момента регламентного запуска
Последний заархивированный сегмент WAL	Не более значения, установленного параметром <code>archive_timeout</code> (рекомендуется контроль в пределах удвоенного таймаута)

Приложение А

Шаблон информационных потоков между ИС и X-IDBox

Таблица 16 – 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 а нагрузки перед веб-серверами Nginx>	80 TCP	Запросы к сервисам X-IDBox	Запросы к сервисам X-IDBox	нет	нет

Приложение Б
Описание настроек

Б.1 Индивидуальные настройки стенда

Таблица 17 – Индивидуальные настройки стенда

Сервис	Техническое наименование	Обязательность	Значение по умолчанию	Пример	Назначение
Все сервисы	xidbox.eureka.service.url	Да	http://localhost:8096	http://<EUREKA_SERVICE_NAME>:<EUREKA_SERVICE_port>:	URL на сервис xidbox-eureka
	xidbox.redis.spring.data.redis.host	Да	localhost	<CACHE_SERVICE_NAME>	Хост сервиса xidbox-cache. Сервис xidbox-cache используется для хранения кеша и сессий пользователей
xidbox-frontbackend xidbox-backend xidbox-orchestrator	xidbox.front.service.base.url	Да	http://localhost:8010	http://<X-IDBOX_URL>	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.order	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-authentication	xidbox.session.domain-name.domain	Да	localhost	<DOMAIN_NAME>	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 сервиса xidbox-cache
xidbox-state-machine-queue	xidbox.state-machine-queue.service.spring.datasource.url	Да	jdbc:postgresql://localhost/state_machine_queue	jdbc:postgresql://<DB_HOST>:<DB_PORT>/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
	xidbox.state-machine-queue.service.spring.datasource.password	Да	postgres	postgres	Пароль пользователя для подключения БД сервиса xidbox-state-machine-queue

Сервис	Техническое наименование	Обязательность	Значение по умолчанию	Пример	Назначение
xidbox-database	xidbox.database.service.spring.data source.url	Да	jdbc:postgresql://localhost/x_idbox_database	jdbc:postgresql://<DB_HOST>:<DB_PORT>/x_idbox_database	URL для подключения БД сервиса x-idbox-database-service
	xidbox.database.service.spring.data source.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-database
	xidbox.database.service.spring.data source.password	Да	postgres	postgres	Пароль пользователя для подключения БД сервиса xidbox-database
xidbox-scheduler	xidbox.scheduler.service.spring.data source.url	Да	jdbc:postgresql://localhost/x_id_box_scheduler	jdbc:postgresql://<DB_HOST>:<DB_PORT>/x_id_box_scheduler	URL для подключения БД сервиса xidbox-scheduler
	xidbox.scheduler.service.spring.data source.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-scheduler
	xidbox.scheduler.service.spring.data source.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://<DB_HOST>:<DB_PORT>/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://<DB_HOST>:<DB_PORT>/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://<DB_HOST>:<DB_PORT>/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://<DB_HOST>:<DB_PORT>/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
	xidbox.role-politics-upload.service.spring.datasource.password	Да	postgres	postgres	Пароль пользователя для подключения БД сервиса xidbox-role-politics-upload

Сервис	Техническое наименование	Обязательность	Значение по умолчанию	Пример	Назначение
xidbox-request-background-processing	xidbox.request-background-processing.service.spring.datasource.url	Да	jdbc:postgresql://localhost/x_idbox_maintenance	jdbc:postgresql://<DB_HOST>:<DB_PORT>/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
	xidbox.gateway.url	Да	localhost	http://<GATEWAY_HOST_URL>	URL для обращения к другим сервисам через Gateway
xidbox-order-archive-database	xidbox.order-archive-database.service.spring.datasource.url	Да	jdbc:postgresql://localhost/archive_order	jdbc:postgresql://<DB_HOST>:<DB_PORT>/archive_order	URL для подключения БД сервиса xidbox-order-archive-database
	xidbox.order-archive-database.service.spring.datasource.username	Да	postgres	postgres	Имя пользователя для подключения БД сервиса xidbox-order-archive-database
	xidbox.order-archive-database.service.spring.datasource.password	Да	postgres	postgres	Пароль для подключения БД сервиса xidbox-order-archive-database

Б.2 Обязательные настройки

Таблица 18 – Настройки, которые должны быть указаны в xidbox.properties

Техническое наименование	Рекомендуемое значение	Назначение
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-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
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 адрес электронной почты УЗ пользователя, мс
xidbox.universal-token.verify-user-profile-work-email	36000000	Срок действия токена, который позволяет верифицировать адрес электронной почты профиля УЗ пользователя, мс

Б.3 Опциональные настройки

Таблица 19 – 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	–	
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.constraint-for-role-policies-field.max-length	1024	Максимально допустимая длина значений технических полей в ролевой модели
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
xidbox.pagination.internal.role-max-limit	2001	Максимальное количество в результирующей выборке из таблицы ролей
xidbox.pagination.internal.information-system-max-limit	2001	Максимальное количество в результирующей выборке из таблицы ИС
xidbox.pagination.internal.information-system-container-max-limit	2001	Максимальное количество в результирующей выборке из таблицы контейнеров ИС
xidbox.pagination.internal.subsystem-max-limit	2001	Максимальное количество в результирующей выборке из таблицы подсистем ИС
xidbox.pagination.internal.application-max-limit	2001	Максимальное количество в результирующей выборке из таблицы приложений ИС
xidbox.pagination.internal.dictionary-max-limit	2001	Максимальное количество в результирующей выборке из таблицы справочников

Название	Значение по умолчанию	Назначение
xidbox.pagination.internal.dictionary-item-max-limit	2001	Максимальное количество в результирующей выборке из таблицы записей справочника
xidbox.pagination.internal.related-order-max-limit	2001	Максимальное количество в результирующей выборке для списка связанных заявок
xidbox.pagination.internal.archive-related-order-max-limit	2001	Максимальное количество в результирующей выборке для списка архивных связанных заявок
xidbox.directory-sync.allow-synchronization	false	Признак, отвечающий за запуск синхронизации с каталогом по LDAP. Значение «true» – если синхронизация запускается. Значение «false» – если синхронизация не запускается
xidbox.directory-sync.allow-sync-user-mac	false	Признак, отвечающий за запуск синхронизации уровней и категорий доступа УЗ пользователя с каталогом по LDAP. Значение «true» – если синхронизация запускается. Значение «false» – если синхронизация не запускается
xidbox.directory-sync.allow-sync-user-dynamic-field	false	Признак, отвечающий за запуск синхронизации настроек динамических полей УЗ пользователя с каталогом по LDAP. Значение «true» – если синхронизация запускается. Значение «false» – если синхронизация не запускается
xidbox.directory-sync.reg.user-profile.reg-user-profile-sync	NO	Режим регистрации профиля УЗ пользователя при регистрации УЗ пользователя (при синхронизации с LDAP-каталогом). Возможные значения: – «NO» – профиль УЗ пользователя не регистрируется. – «ONE_TO_ONE» – регистрируется один профиль для УЗ пользователя. – «ONE_TO_MANY» – регистрируются профили для УЗ пользователя согласно списку организаций в LDAP-каталоге. Идентификаторы организаций в LDAP-каталоге указываются через запятую. По умолчанию (если в каталоге не задана организация) профиль УЗ пользователя регистрируется в организации с идентификатором из настройки «xidbox.directory-sync.reg.user-profile.default-organization-uuid»
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.change-user-profile-state-with-user-state	false	Признак, включающий изменение состояния профилей УЗ пользователей с состоянием УЗ пользователей. Относится только к тем профилям УЗ пользователей, которые участвуют в синхронизации. Значение «true» – если состояние профилей УЗ пользователей меняется вместе со состоянием УЗ пользователей. Значение «false» – если состояние профилей УЗ пользователей не меняется
xidbox.directory-sync.revoke-roles-when-profile-is-permanently-blocked	false	Признак, отвечающий за снятие ролей у профиля УЗ пользователя при его постоянном блокировании. Значение «true» – если роли снимаются. Значение «false» – если роли не снимаются
xidbox.directory.mode	false	Признак, отображающий, включена ли работа с LDAP-каталогом. Значение «true» – если работа с LDAP-каталогом включена. Значение «false» – если работа с LDAP-каталогом отключена

Название	Значение по умолчанию	Назначение
xidbox.directory-sync.create-order-if-not-has-changes-by-scheduler	false	Признак, отвечающий за необходимость создания автоматической заявки на синхронизацию данных с LDAP-каталогом при отсутствии изменений. Значение «true» – если заявка на синхронизацию создается в начале синхронизации. Значение «false» – если заявка на синхронизацию создается только в момент обнаружения расхождений с данными из LDAP-каталога. Если изменения отсутствуют, то заявка на синхронизацию не создается
xidbox.directory.check-ldap-user-state-before-auto-unblock	false	Признак, отвечающий за проверку состояния УЗ пользователя перед автоматической разблокировкой УЗ пользователя с LDAP-каталогом. Значение «true» – если проверка осуществляется. Значение «false» – если проверка не осуществляется
xidbox.directory.check-ldap-user-state-before-authentication	false	Признак, отвечающий за проверку состояния УЗ пользователя перед аутентификацией с LDAP-каталогом. Значение «true» – если проверка осуществляется. Значение «false» – если проверка не осуществляется
xidbox.directory.check-ldap-user-state-before-authentication-strict	false	Признак, отвечающий за необходимость прерывания процесса аутентификации в случае невозможности проверки статуса УЗ пользователя в LDAP-каталоге. Значение «true» – если необходимо прерывать аутентификацию и выводить ошибку. Значение «false» – если необходимо продолжать аутентификацию
xidbox.directory-sync.source-info-system	xidbox	Наименование источника динамических полей. Влияет на то, будут ли при включенной настройке «xidbox.data.change.prohibition-of-change-user-or-user-profile» со значением «true» изменяться динамические поля с указанным источником
xidbox.data.change.prohibition-of-change-user-or-user-profile	false	Признак, отвечающий за возможность изменять основные данные УЗ пользователя и профиля УЗ пользователя через веб-интерфейс Значение «true» – если изменения запрещены. Значение «false» – если изменения разрешены
xidbox.data.change.prohibition-of-external-change-user-or-user-profile	false	Признак, отвечающий за возможность изменять основные данные УЗ пользователя и профиля УЗ пользователя через внешние сервисы. Значение «true» – если изменения запрещены. Значение «false» – если изменения разрешены
xidbox.user.profile.role.prohibition-of-change	false	Признак, отвечающий за возможность изменять роли профиля УЗ пользователя через веб-интерфейс. Значение «true» – если изменения запрещены. Значение «false» – если изменения разрешены
xidbox.user.profile.role.prohibition-of-external-change	false	Признак, отвечающий за возможность изменять роли профиля УЗ пользователя через внешние сервисы. Значение «true» – если изменения запрещены. Значение «false» – если изменения разрешены
xidbox.user.registration.prohibition-of-registration-anonymous	false	Признак, отвечающий за возможность самостоятельной регистрации пользователя. Значение «true» – если самостоятельная регистрация недоступна. Значение «false» – если самостоятельная регистрация доступна
xidbox.user.registration.prohibition-of-registration	false	Признак, отвечающий за возможность регистрации пользователя. Значение «true» – если регистрация недоступна. Значение «false» – если регистрация доступна

Название	Значение по умолчанию	Назначение
xidbox.user.registration.prohibition-of-batch-registration	false	Признак, отвечающий за возможность регистрации с помощью загрузки пользователей из файла. Значение «true» – если регистрация с помощью загрузки пользователей недоступна. Значение «false» – если регистрация с помощью загрузки пользователей доступна
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.approval.head-role	head_manager	Техническое наименование роли, которая отвечает за согласование заявок во всех организациях в случае отсутствия профилей УЗ пользователей с ролью, отвечающей за конкретную организацию. Если значение настройки не указано, то при отсутствии профилей УЗ пользователей с ролью, отвечающих за конкретную организацию, согласование не будет передано профилям с этой ролью
xidbox.approval.organization-role	manager	Техническое наименование роли, которая отвечает за согласование заявок (при наличии этой роли в шагах согласования), где объект связан с организацией или подотчетными организациями согласующего. Если значение настройки не указано, то при согласовании заявок проверка наличия у объекта заявки связи с организациями согласующего производиться не будет (то есть доступными будут считаться все профили УЗ пользователей с данной ролью, вне зависимости от организации)
xidbox.approval.information-system-role	information_system_manager	Техническое наименование роли, которая отвечает за согласование заявок (при наличии этой роли в шагах согласования), где объект управления связан с контролируемой ИС. Если значение настройки не указано, то при согласовании заявок проверка наличия у объекта заявки связи с ИС, подконтрольной профилям УЗ пользователей с данной ролью производиться не будет (то есть доступными будут считаться все профили УЗ пользователей с данной ролью, вне зависимости от ИС)
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-resource-type-response-ttl	300s	TTL кеша ответа для API «Получение списка доступных ресурсов по типу ресурса и действию 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 ресурсам
xidbox.authz.cache.authz-active-access-rules-by-user-profile-id-and-info-system-and-resource-type-ttl	300s	TTL кеша правил доступов профиля УЗ пользователя по ИС и типу ресурса

Название	Значение по умолчанию	Назначение
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	Признак необходимости проверять условия применимости ролей. Значение «true» – если необходимо проверять условия применимости ролей. Значение «false» – если не нужно проверять условия применимости ролей
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.applicability.role.ignore-block-user-profile-in-applicability-condition	true	Признак необходимости игнорировать временное или постоянное блокирование профиля УЗ пользователя при проверке условий применимости роли. Значение «true» – если необходимо игнорировать временное или постоянное блокирование профиля УЗ пользователя. Значение «false» – если не нужно игнорировать временное или постоянное блокирование профиля УЗ пользователя
xidbox.authz.applicability.role.ignore-block-user-in-applicability-condition	true	Признак необходимости игнорировать временное или постоянное блокирование УЗ пользователя при проверке условий применимости роли. Значение «true» – если необходимо игнорировать временное или постоянное блокирование УЗ пользователя. Значение «false» – если не нужно игнорировать временное или постоянное блокирование УЗ пользователя
xidbox.authz.spel.custom-method.unary.<наименование функции>	–	Описание унарных настраиваемых функций для использования в условиях применимости ролей и политик авторизации (см. п. 7.7)
xidbox.authz.spel.custom-method.binary.<наименование функции>	–	Описание бинарных настраиваемых функций для использования в условиях применимости ролей и политик авторизации (см. п. 7.7)
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

Название	Значение по умолчанию	Назначение
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
xidbox.organizational-structure.disabled	false	Признак отключения сервиса загрузки ОШС. Если сервис загрузки ОШС отключается, то этот признак необходимо установить в значении «true». Значение «true» – если данные ОШС не передаются. Значение «false» – если данные ОШС передаются
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.

Название	Значение по умолчанию	Назначение
		Например: – P1DT2H3M4S – 1 день, 2 часа, 3 минуты и 4 секунды. – P5D – 5 дней. – PT24H – 24 часа
xidbox.mac.view-in-user-card	false	Признак отображения уровней и категорий доступа в карточке УЗ пользователя. Значение «true» – если отображается. Значение «false» – если не отображается
xidbox.mac.view-in-identification-for-user	false	Признак отображения уровней и категорий доступа в ответе на запрос в ППО «Сервис идентификации» для УЗ пользователя. Значение «true» – если отображается. Значение «false» – если не отображается
xidbox.mac.mic-maximum-mask-for-convert	63	Максимальный уровень целостности, который разрешено преобразовывать в список уровней. Например, при использовании в динамических атрибутах в авторизации
xidbox.kerberos.krb5	–	Наименование файла конфигурации Kerberos, используемого для подключения сервисов к базе данных с использованием аутентификации с помощью доменной учётной записи
xidbox.kerberos.jaas	–	Наименование файла конфигурации JAAS, используемого для подключения сервисов к базе данных с использованием аутентификации с помощью доменной учётной записи
xidbox.<наименование сервиса>.service.condition.sql.config-location	classpath:/common/condition-to-sql.json	Путь до файла с преобразованием условий ролевой модели в SQL. Поддерживается для ППО «Сервис работы с основными БД» (xidbox-database) и ППО «Сервис изменения заявок» (xidbox-order). Формат преобразования условий ролевой модели в SQL приведён в файле «condition-to-sql.json»
xidbox.authn.custom.headers.enable	true	Признак необходимости передавать ИС дополнительную информацию о пользователе в настраиваемых HTTP-заголовках запроса. Значение «true» – если необходимо передавать ИС дополнительную информацию о пользователе. Значение «false» – если не нужно передавать ИС дополнительную информацию о пользователе
xidbox.authn.custom.headers.settings[*]	–	Настройка информации о пользователе, которая передаётся ИС в настраиваемых HTTP-заголовках запроса, где * – числовой индекс настройки, нумерация с 0: – xidbox.authn.custom.headers.settings[*].header-name – наименование HTTP-заголовка; – xidbox.authn.custom.headers.settings[*].attribute-source – источник поля/атрибута в X-IDBox, который необходимо передать ИС в качестве значения HTTP-заголовка запроса, могут принимать следующее значения: – current_user_main_attribute; – current_user_profile_organization_main_attribute; – current_user_profile_main_attribute; – current_user_dynamic_attribute; – current_user_profile_dynamic_attribute; – current_user_profile_organization_dynamic_attribute; – current_user_detail; – xidbox.authn.custom.headers.settings[*].pattern – SpEL-выражение для извлечения значения атрибутов из источника.

Название	Значение по умолчанию	Назначение
		Структура данных в источнике поля/атрибута в X-IDBox приведена в Приложении Г. Пример настройки приведён в Приложении Г

Б.4 Настройки сервиса xidbox-authentication

Таблица 20 – 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 сервисе xidbox-cache
xidbox.authentication.service.kerberos.krb5	/app/kerberos/krb5.conf	Наименование файла конфигурации Kerberos, используемого для аутентификации с помощью доменной учётной записи
xidbox.authentication.service.kerberos.jaas	/app/kerberos/jaas.conf	Наименование файла конфигурации JAAS, используемого для аутентификации с помощью доменной учётной записи
xidbox.authentication.service.kerberos.jaas-profile-name	KerberosAcceptorWithTicket	Наименование 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. 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.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
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 сервисе xidbox-cache, 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.esia-adapter.domain	http://localhost:3010	URL адаптера ЕСИА, например: http://localhost:3010
xidbox.authentication.service.esia-adapter.auth-code-endpoint-v2	/v1/createAuthReq/ac	URL адаптера для получения параметров запроса авторизационного кода для v2
xidbox.authentication.service.esia-adapter.auth-code-endpoint-v3	/v1/createAuthReq/v2/ac	URL адаптера для получения параметров запроса авторизационного кода для v3

Название	Значение по умолчанию	Назначение
xidbox.authentication.service.esia-adapter.access-token-endpoint-v2	/v1/createTokenReq/te	URL адаптера для получения параметров запроса токенов доступа для v2
xidbox.authentication.service.esia-adapter.access-token-endpoint-v3	/v1/createTokenReq/v3/te	URL адаптера для получения параметров запроса токенов доступа для v3
xidbox.authentication.service.esia-adapter.access-token-verification-endpoint	/v1/tokenResp	URL адаптера для проверки токена доступа
xidbox.authentication.service.esia-adapter.validate-access-token-enabled	true	Признак необходимости валидировать токен доступа перед парсингом. Значение «true» – если необходимо валидировать токен доступа перед парсингом. Значение «false» – если не требуется валидировать токен доступа перед парсингом
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
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

Название	Значение по умолчанию	Назначение
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
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

Название	Значение по умолчанию	Назначение
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
xidbox.authn.need-send-link-for-verify-user-profile-work-email	true	Признак необходимости отправлять ссылку на подтверждение адреса электронной почты профиля УЗ пользователя после успешной аутентификации. Значение «true» – если необходимо отправлять ссылку на подтверждение адреса электронной почты. Значение «false» – если не нужно отправлять ссылку на подтверждение адреса электронной почты
xidbox.authentication.service.job.session-cleanup.cron	0 * * * * *	Расписание внутреннего процесса для проверки сессий на завершенность. Если сессия завершена, то в БД записывается дата окончания сессии
xidbox.authentication.service.job.count-session-for-check	500	Ограничение максимального количества одновременно запрашиваемых сессий
xidbox.authentication.service.job.session-cleanup.max-random-delay-in-second	5	Задержка начала выполнения процесса проверки сессий на завершенность, в секундах
xidbox.authn.check-email-verified-for-authentication	true	Признак необходимости проверять верификацию адреса электронной почты УЗ пользователя при аутентификации. Значение «true» – если необходимо проверять верификацию адреса электронной почты УЗ пользователя. Значение «false» – если не требуется проверять верификацию адреса электронной почты УЗ пользователя

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

Таблица 21 – 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 22 – 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_CHECK_UPLOAD_FAILED	Название шага сценария загрузки ролевой модели, на котором необходимо начинать обработку файла
xidbox.role-politics-upload.service.file-processing.retry-count	10	Лимит количества перезапусков обработки файла, после которого сценарий будет считаться проваленным
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
xidbox.role-politics-upload.service.upload-message.retry-delay-sec	10	Минимальная задержка между запусками попыток выполнить загрузку, секунд

Б.7 Настройки сервиса xidbox-database

Таблица 23 – 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
xidbox.database.service.auth.session.level	none	Устанавливает уровень сессии. Возможные значения: none, l1, l2,...ln
xidbox.database.service.cache.ttl.organization-type	12h	Установка TTL для кеша типа организаций
xidbox.database.service.cache.ttl.sub-organization-rules	12h	Установка TTL для кеша правил выборки подотчетных организаций
xidbox.database.service.spring.jpa.properties.hibernate.max-batch-size-by-select-via-in	512	Максимальное количество параметров в запросе с оператором IN при пакетной выборке. Необходимо для оптимизации планов запросов с оператором IN, максимальное значение зависит от типа и версии БД. В качестве значения указывается только степень числа 2

Б.8 Настройки сервиса xidbox-backend

Таблица 24 – Настройки сервиса xidbox-backend

Название	Значение по умолчанию	Назначение
xidbox.backend.service.spring.mail.host	localhost	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.sender	noreply@noreply.noreply	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

Название	Значение по умолчанию	Назначение
xidbox.backend.service.mail.ignore-for-send-order-type.<техническое наименование типа заявки>	–	Отключение отправки определенных шаблонов уведомлений для заявок определенного типа. Формат указания настройки: – xidbox.backend.service.mail.ignore-for-send-order-type. <техническое наименование типа заявки>=<техническое наименование шаблона уведомления 1>,...,<техническое наименование шаблона уведомления n> – технические наименования шаблонов уведомлений указываются через запятую; – xidbox.backend.service.mail.ignore-for-send-order-type. <техническое наименование типа заявки>=* – отключение отправки всех шаблонов уведомлений для заявок определенного типа. Сопоставление типов заявок и шаблонов уведомлений приведено в Приложении Д
xidbox.backend.service.mail.send-only-by-email	email_confirmation, email_confirmation_for_order	Перечень технических наименований шаблонов уведомлений, которые отправляются только на электронную почту
xidbox.backend.service.upload-batch.user-dynamic-field-descriptions-count	100	Количество обновляемых настроек динамических полей УЗ пользователя в побочных заявках при загрузке обновления настроек динамических полей УЗ пользователя
xidbox.backend.service.upload-batch.user-profile-dynamic-field-descriptions-count	100	Количество обновляемых настроек динамических полей профиля УЗ пользователя в побочных заявках при загрузке обновления настроек динамических полей профиля УЗ пользователя
xidbox.backend.service.upload-batch.organization-dynamic-field-descriptions-count	100	Количество обновляемых настроек динамических полей организаций в побочных заявках при загрузке обновления настроек динамических полей организаций
xidbox.backend.service.path.tmp	\${java.io.tmpdir:tmp}	Путь, в котором будут создаваться временные папки и файлы при загрузке
xidbox.backend.service.path.report-dir	report	Наименование папки, в которой будут временно сохраняться промежуточные и финальные отчеты при загрузке
xidbox.backend.service.report.formatted-output	true	Признак, определяющий, что отчёты будут отформатированы с переводом строк и отступами. Значение «true» – если необходимо отформатировать отчёты. Значение «false» – если не нужно форматировать отчёты
xidbox.backend.service.report.page-size-for-get-children-upload-user	50	Максимальное количество дочерних заявок, которые будут использованы для формирования отчёта о загрузке пользователей
xidbox.backend.service.report.page-size-for-get-children-upload-organization	50	Максимальное количество дочерних заявок, которые будут использованы для формирования отчёта о загрузке организаций
xidbox.backend.service.organizations-black-or-white-list-for-send-order-type.org-uuids.<техническое наименование типа заявки>	–	Тип заявки и список идентификаторов организаций для фильтрации по чёрному или белому списку при отправке уведомлений. При пустом значении параметра фильтрация не осуществляется
xidbox.backend.service.organizations-black-or-white-list-for-send-order-type.white-list.<техническое наименование типа заявки>	false	Признак, определяющий, применяется ли белый список для указанного в настройке типа заявки. Значение «true» – для указанного типа заявки применяется белый список. Значение «false» – для указанного типа заявки применяется чёрный список

Б.9 Настройки сервиса xidbox-frontbackend

Таблица 25 – Настройки сервиса xidbox-frontbackend

Название	Значение по умолчанию	Назначение
xidbox.frontbackend.service.spring.mail.host	<MAIL_RELAY_URL>	Хост сервера для отправки сообщений
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

Название	Значение по умолчанию	Назначение
xidbox.frontbackend.service.core-fields.user-label-map.lastName	\u0424\u0430\u043c\u0438\u043b\u0438\u0446	Наименование основного атрибута УЗ пользователя «Фамилия». В кодировке Unicode должна быть указана кириллица. По умолчанию – «Фамилия»
xidbox.frontbackend.service.core-fields.user-label-map.firstName	\u0418\u043c\u044f	Наименование основного атрибута УЗ пользователя «Имя». В кодировке Unicode должна быть указана кириллица. По умолчанию – «Имя»
xidbox.frontbackend.service.core-fields.user-label-map.middleName	\u0418\u0442\u0447\u0435\u0441\u0442\u0432\u043e	Наименование основного атрибута УЗ пользователя «Отчество». В кодировке Unicode должна быть указана кириллица. По умолчанию – «Отчество»
xidbox.frontbackend.service.core-fields.user-label-map.birthday	\u0414\u0430\u0442\u0430\u0440\u043e\u0436\u0434\u0435\u043d\u0438\u044f	Наименование основного атрибута УЗ пользователя «Дата рождения». В кодировке Unicode должна быть указана кириллица. По умолчанию – «Дата рождения»
xidbox.frontbackend.service.core-fields.user-label-map.inn	\u0418\u041d\u041d	Наименование основного атрибута УЗ пользователя «ИНН». В кодировке Unicode должна быть указана кириллица. По умолчанию – «ИНН»
xidbox.frontbackend.service.core-fields.user-label-map.snils	\u0421\u041d\u0418\u041b\u0421	Наименование основного атрибута УЗ пользователя «СНИЛС». В кодировке Unicode должна быть указана кириллица. По умолчанию – «СНИЛС»
xidbox.frontbackend.service.core-fields.user-label-map.login	\u041b\u043e\u0433\u0438\u043d	Наименование основного атрибута УЗ пользователя «Логин». В кодировке Unicode должна быть указана кириллица. По умолчанию – «Логин»
xidbox.frontbackend.service.core-fields.user-label-map.email	Email	Наименование основного атрибута УЗ пользователя «Адрес электронной почты УЗ пользователя». По умолчанию – «Email»
xidbox.frontbackend.service.core-fields.user-profile-label-map.workEmail	Email	Наименование основного атрибута профиля УЗ пользователя «Адрес электронной почты профиля УЗ пользователя». По умолчанию – «Email»
xidbox.frontbackend.service.approval.order-tech-names-for-approval	usr_reg,change_user_profile_positions,change_account_data	Список технических наименований заявок, для которых необходимо добавление атрибутов согласования для авторизации
xidbox.frontbackend.service.approval.approval-state-tech-names	on_approval,on_last_approval	Список технических наименований состояний заявок, при которых необходимо добавление атрибутов согласования для авторизации
xidbox.frontbackend.service.approval.role-tech-name-for-organization	manager	Техническое наименование роли, отвечающей за согласование внутри подотчётных организаций
xidbox.frontbackend.service.approval.rule-for-sub-organizations	separate_divisions	Техническое наименование правила выборки подотчётных организаций

Б.10 Настройки сервиса xidbox-scheduler

Таблица 26 – 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

Название	Значение по умолчанию	Назначение
xidbox.scheduler.service.block-inactive-users.cron	0 0 2 * * ?	Сгон 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 * * * ?	Сгон 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 * * ?	Сгон 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 * * * ?	Сгон выполнения задачи на отправку уведомлений о скором истечении срока действия пароля
xidbox.scheduler.service.notify-about-coming-password-expiration.sleep-between-delete-next-pack	PT0S	Задержка между отправками уведомлений о скором истечении срока действия пароля следующему списку пользователей
xidbox.scheduler.service.notify-about-completed-password-expiration.limit	10	Максимальное количество пользователей, которым будут отправлены сообщения об истекшем сроке действия пароля за одно выполнение задачи
xidbox.scheduler.service.notify-about-completed-password-expiration.cron	0 0 * * * ?	Сгон выполнения задачи на отправку уведомлений об истекшем сроке действия пароля
xidbox.scheduler.service.notify-about-completed-password-expiration.sleep-between-delete-next-pack	PT0S	Задержка между отправками уведомлений об истекшем сроке действия пароля следующему списку пользователей
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 * * * ?	Сгон выполнения задачи на блокирование активных профилей УЗ пользователя в неактивных организациях
xidbox.scheduler.service.synchronize-users-from-directory.cron	0 0 1 ? * * *	Сгон выполнения задачи на создание заявки на синхронизацию УЗ пользователя из LDAP-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 * * ?	Сгон 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 * * * ?	Сгон 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 * * * ?	Сгон выполнения задачи на удаление записей в истории сессий профилей УЗ пользователя
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.archive-order-mark.limit	1000	Максимальное количество цепочек заявок, которое будет обрабатываться задачей, помечающей заявки для архивации
xidbox.scheduler.service.archive-order-mark.archive-after-days	30	Количество дней, через которое заявку можно архивировать
xidbox.scheduler.service.archive-order-mark.cron	0 0 0 * * ?	Сгон выполнения задачи, помечающей заявки для архивации
xidbox.scheduler.service.archive-orders.limit	25	Максимальное количество цепочек заявок, которые будут перенесены в архив
xidbox.scheduler.service.archive-orders.cron	0 0 2 * * ?	Сгон выполнения задачи, архивирующей заявки
xidbox.scheduler.service.remove-expired-oauth-tokens.limit	10	Максимальное количество просроченных OAuth2.0 токенов, которые будут удалены за одно выполнение задачи

Название	Значение по умолчанию	Назначение
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.notify-about-coming-user-block-inactive.cron	0 0 0 * * ?	Срон для отправки уведомлений о предстоящей блокировке УЗ пользователей по причине неактивности
xidbox.scheduler.service.notify-about-coming-user-block-inactive.limit	10	Максимальное количество пользователей, которым будет отправлено уведомление о предстоящей блокировке УЗ пользователей по причине неактивности
xidbox.scheduler.service.update-orders-approval-process.cron	0 */10 * * * ?	Срон для актуализации процесса согласования в заявках
xidbox.scheduler.service.update-orders-approval-process.limit	10	Максимальное количество заявок, для которых необходимо выполнить проверку процесса согласования
xidbox.scheduler.service.update-orders-approval-process.orderTypes	usr_reg,change_account_data,change_user_profile_positions,change_user_profile_roles	Перечень технических наименований типов заявок, для которых необходимо выполнять проверку процесса согласования
xidbox.scheduler.service.update-orders-approval-process.orderStates	on_approval,on_last_approval	Перечень технических наименований состояния заявок, для которых необходимо выполнять проверку процесса согласования
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-orchestrator

Таблица 27 – 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

Название	Значение по умолчанию	Назначение
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, 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.notification.order_cancel.block_account.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об отмене заявки для сценария постоянного блокирования УЗ пользователя. Значение «true» – если необходимо отправлять уведомления об отмене заявки. Значение «false» – если не нужно отправлять уведомления об отмене заявки
xidbox.notification.order_cancel.permanent_block_user_profile.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об отмене заявки для сценария постоянного блокирования профиля УЗ пользователя. Значение «true» – если необходимо отправлять уведомления об отмене заявки. Значение «false» – если не нужно отправлять уведомления об отмене заявки
xidbox.notification.order_cancel.temporarily_block_account.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об отмене заявки для сценария временного блокирования УЗ пользователя. Значение «true» – если необходимо отправлять уведомления об отмене заявки. Значение «false» – если не нужно отправлять уведомления об отмене заявки
xidbox.notification.order_cancel.temporarily_block_user_profile.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об отмене заявки для сценария временного блокирования профиля УЗ пользователя. Значение «true» – если необходимо отправлять уведомления об отмене заявки. Значение «false» – если не нужно отправлять уведомления об отмене заявки
xidbox.notification.order_cancel.unblock_account.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об отмене заявки для сценария разблокирования УЗ пользователя. Значение «true» – если необходимо отправлять уведомления об отмене заявки. Значение «false» – если не нужно отправлять уведомления об отмене заявки
xidbox.notification.order_cancel.unblock_user_profile.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об отмене заявки для сценария разблокирования профиля УЗ пользователя. Значение «true» – если необходимо отправлять уведомления об отмене заявки. Значение «false» – если не нужно отправлять уведомления об отмене заявки
xidbox.notification.order_cancel.role	system_administrator	Техническое наименование роли, которой отправляются уведомления об отмене заявки

Название	Значение по умолчанию	Назначение
xidbox.notification.order_cancel.information-system	xidbox	Техническое наименование ИС роли, которой отправляются уведомления об отмене заявки
xidbox.notification.change_user_success.change_account_data.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об успешном выполнении заявки для сценария изменения данных пользователя. Значение «true» – если необходимо отправлять уведомления об успешном выполнении заявки. Значение «false» – если не нужно отправлять уведомления об успешном выполнении заявки
xidbox.notification.change_user_success.usr_synchronization.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об успешном выполнении заявки для сценария синхронизации пользователей. Значение «true» – если необходимо отправлять уведомления об успешном выполнении заявки. Значение «false» – если не нужно отправлять уведомления об успешном выполнении заявки
xidbox.notification.change_user_success.head_role	head_manager	Техническое наименование роли, отвечающей за все организации, которой отправляются уведомления об изменении данных пользователя. Уведомление отправляется только при отсутствии профилей УЗ пользователей с ролью, отвечающей за конкретную организацию
xidbox.notification.change_user_success.organization_role	manager	Техническое наименование роли, отвечающей за конкретную организацию, которой отправляются уведомления об изменении данных пользователя
xidbox.notification.change_user_success.information-system	xidbox	Техническое наименование ИС роли, которой отправляются уведомления об изменении данных пользователя
xidbox.notification.change_user_profile_success.change_user_profile_data.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об успешном выполнении заявки для сценария изменения данных профиля УЗ пользователя. Значение «true» – если необходимо отправлять уведомления об успешном выполнении заявки. Значение «false» – если не нужно отправлять уведомления об успешном выполнении заявки
xidbox.notification.change_user_profile_success.change_user_profile_positions.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об успешном выполнении заявки для сценария изменения должностей профиля УЗ пользователя. Значение «true» – если необходимо отправлять уведомления об успешном выполнении заявки. Значение «false» – если не нужно отправлять уведомления об успешном выполнении заявки
xidbox.notification.change_user_profile_success.change_user_profile_roles.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об успешном выполнении заявки для сценария изменения ролей профиля УЗ пользователя. Значение «true» – если необходимо отправлять уведомления об успешном выполнении заявки. Значение «false» – если не нужно отправлять уведомления об успешном выполнении заявки

Название	Значение по умолчанию	Назначение
xidbox.notification.change_user_profile_success.permanent_block_user_profile.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об успешном выполнении заявки для сценария постоянного блокирования профиля УЗ пользователя. Значение «true» – если необходимо отправлять уведомления об успешном выполнении заявки. Значение «false» – если не нужно отправлять уведомления об успешном выполнении заявки
xidbox.notification.change_user_profile_success.head_role	head_manager	Техническое наименование роли, отвечающей за все организации, которой отправляются уведомления об изменении данных профиля УЗ пользователя. Уведомление отправляется только при отсутствии профилей УЗ пользователей с ролью, отвечающей за конкретную организацию
xidbox.notification.change_user_profile_success.organization_role	manager	Техническое наименование роли, отвечающей за конкретную организацию, которой отправляются уведомления об изменении данных профиля УЗ пользователя
xidbox.notification.change_user_profile_success.information-system	xidbox	Техническое наименование ИС роли, которой отправляются уведомления об изменении данных профиля УЗ пользователя
xidbox.notification.order_processing_error.role	security_administrator	Техническое наименование роли, которой отправляются уведомления об ошибке обработки заявки
xidbox.notification.order_processing_error.information-system	xidbox	Техническое наименование ИС роли, которой отправляются уведомления об ошибке обработки заявки
xidbox.notification.order_processing_error.enabled	true	Признак, отвечающий за необходимость отправки уведомлений об ошибке обработки заявки. Значение «true» – если необходимо отправлять уведомления об ошибке обработки заявки. Значение «false» – если не нужно отправлять уведомления об ошибке обработки заявки
xidbox.dynamic-field-descriptions.usr_synchronization.enabled	true	Признак, отвечающий за необходимость синхронизации настроек динамических полей при выполнении сценария синхронизации пользователей. Значение «true» – если необходимо синхронизировать настройки динамических полей. Значение «false» – если не нужно синхронизировать настройки динамических полей
xidbox.verification-of-rights.change_account_data.enabled	true	Признак, отвечающий за необходимость проверки прав доступа при выполнении заявки на изменение данных УЗ пользователя. Значение «true» – если необходима проверка прав доступа. Значение «false» – если не нужна проверка прав доступа
xidbox.verification-of-rights.change_user_profile_positions.enabled	true	Признак, отвечающий за необходимость проверки прав доступа при выполнении заявки на изменение должностей профиля УЗ пользователя. Значение «true» – если необходима проверка прав доступа. Значение «false» – если не нужна проверка прав доступа
xidbox.approval.types.usr_reg.enabled	true	Признак, отвечающий за необходимость согласования заявок на регистрацию пользователя. Значение «true» – если необходимо согласование заявок на регистрацию пользователя. Значение «false» – если согласование заявок на регистрацию пользователя не требуется
xidbox.approval.types.usr_reg.step.<номер шага>.head-role	head_manager	Список технических наименований ролей на заданном шаге, которые отвечают за согласование заявки на регистрацию пользователя во всех организациях. Номер шага начинается с 1
xidbox.approval.types.usr_reg.step.<номер шага>.organization-role	manager	Список технических наименований ролей на заданном шаге, которые отвечают за согласование заявки на регистрацию пользователя внутри организации. Номер шага начинается с 1

Название	Значение по умолчанию	Назначение
xidbox.approval.types.usr_reg.step.<номер шага>.approved-by-all	false	Признак, отвечающий за необходимость согласования заявки на регистрацию пользователя на заданном шаге всеми указанными ролями. Значение «true» – если необходимо согласование заявки на регистрацию пользователя. Значение «false» – если согласование заявки на регистрацию пользователя не требуется. Номер шага начинается с 1
xidbox.approval.types.usr_reg.information-system	xidbox	Техническое наименование ИС, которой принадлежит роль, отвечающая за согласование заявки на регистрацию пользователя
xidbox.approval.types.change_user_profile_positions.enabled	true	Признак, отвечающий за необходимость согласования заявок на изменение должностей профиля УЗ пользователя. Значение «true» – если необходимо согласование заявок на изменение должностей профиля УЗ пользователя. Значение «false» – если согласование заявок на изменение должностей профиля УЗ пользователя не требуется
xidbox.approval.types.change_user_profile_positions.step.<номер шага>.head-role	head_manager	Список технических наименований ролей на заданном шаге, которые отвечают за согласование заявки на изменение должностей профиля УЗ пользователя во всех организациях. Номер шага начинается с 1
xidbox.approval.types.change_user_profile_positions.step.<номер шага>.organization-role	manager	Список технических наименований ролей на заданном шаге, которые отвечают за согласование заявки на изменение должностей профиля УЗ пользователя внутри организации. Номер шага начинается с 1
xidbox.approval.types.change_user_profile_positions.step.<номер шага>.approved-by-all	false	Признак, отвечающий за необходимость согласования заявки на изменение должностей профиля УЗ пользователя на заданном шаге всеми указанными ролями. Значение «true» – если необходимо согласование заявки на изменение должностей профиля УЗ пользователя. Значение «false» – если согласование заявки на изменение должностей профиля УЗ пользователя не требуется. Номер шага начинается с 1
xidbox.approval.types.change_user_profile_positions.information-system	xidbox	Техническое наименование ИС, которой принадлежит роль, отвечающая за согласование заявки на изменение должностей профиля УЗ пользователя
xidbox.approval.types.change_account_data.enabled	true	Признак, отвечающий за необходимость согласования заявок на изменение данных УЗ пользователя. Значение «true» – если необходимо согласование заявок на изменение данных УЗ пользователя. Значение «false» – если согласование заявок на изменение данных УЗ пользователя не требуется
xidbox.approval.types.change_account_data.step.<номер шага>.head-role	head_manager	Список технических наименований ролей на заданном шаге, которые отвечают за согласование заявки на изменение данных УЗ пользователя во всех организациях. Номер шага начинается с 1
xidbox.approval.types.change_account_data.step.<номер шага>.organization-role	manager	Список технических наименований ролей на заданном шаге, которые отвечают за согласование заявки на изменение данных УЗ пользователя внутри организации. Номер шага начинается с 1

Название	Значение по умолчанию	Назначение
xidbox.approval.types.change_account_data.step.<номер шага>.approved-by-all	false	Признак, отвечающий за необходимость согласования заявки на изменение данных УЗ пользователя на заданном шаге всеми указанными ролями. Значение «true» – если необходимо согласование заявки на изменение данных УЗ пользователя. Значение «false» – если согласование заявки на изменение данных УЗ пользователя не требуется. Номер шага начинается с 1
xidbox.approval.types.change_account_data.information-system	xidbox	Техническое наименование ИС, которой принадлежит роль, отвечающая за согласование заявки на изменение данных УЗ пользователя

Б.12 Настройки сервиса xidbox-storage

Таблица 28 – 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.13 Настройки сервиса xidbox-order

Таблица 29 – 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
xidbox.order.service.archive.order.state-tech-names	success,error,rejected,cancel	Технические наименования статусов заявок, в которых заявки необходимо переносить в архив

Б.14 Настройки сервиса xidbox-state-machine-database

Таблица 30 – 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.15 Настройки сервиса xidbox-ldap

Настройки для ALD Pro и FreeIpa полностью совпадают.

Таблица 31 – Настройки сервиса xidbox-ldap

Название	Значение для AD	Значение для FreeIpa	Значение для ALD	Значение для OpenLdap	Назначение
xidbox.ldap.service.spring.ldap.urls	–	–	–	–	URL на службу LDAP-каталога
xidbox.ldap.service.spring.ldap.base	dc=xidbox,dc=example,dc=ru	dc=example,dc=ru	dc=example,dc=ru	dc=xidbox,dc=example,dc=ru	Базовый суффикс, от которого должны происходить все операции
xidbox.ldap.service.spring.ldap.username	cn=Admin,cn=Users,dc=xidbox,dc=example,dc=ru	uid=admin,cn=users,cn=accounts,dc=example,dc=ru	uid=admin,cn=users,cn=accounts,dc=example,dc=ru	cn=admin,dc=xidbox,dc=example,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	ALD	OpenLdap	Вариант протокола: AD, FreeIpa, ALD, OpenLdap
xidbox.ldap.service.directory.base	cn=Users	cn=users,cn=accounts	cn=users,cn=accounts	ou=Users	Суффикс для поиска УЗ пользователя
xidbox.ldap.service.directory.base-schema	cn=attributeTypes,CN=Aggregate,CN=Schema,CN=Configuration,DC=example,DC=ru	schema=attributeTypes,cn=schema	schema=attributeTypes,cn=schema	–	Суффикс для получения описания из схемы атрибутов элементов LDAP
xidbox.ldap.service.directory.description-attribute-name	NAME	DESC	DESC	–	Наименование атрибута, в котором содержится описание из схемы атрибутов элементов LDAP
xidbox.ldap.service.lockout-duration.policies-base	–	–	–	ou=policies	Путь до расположения политик в LDAP-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

Название	Значение для AD	Значение для FreeIpa	Значение для ALD	Значение для OpenLdap	Назначение
xidbox.ldap.service.lockout-duration.update-frequency	1800000	1800000	1800000	1800000	Частота обновления политики постоянного и продолжительности временного блокирования, мс
xidbox.ldap.service.openldap.filter	—	—	—	(objectclass=inetOrgPerson)	Дополнительный фильтр. Только для OpenLdap
xidbox.ldap.service.free-ipa.mac.free-ipa-mac-level-max	—	xaldusermacmax	—	—	Название атрибута для максимального уровня конфиденциальности УЗ пользователя
xidbox.ldap.service.free-ipa.mac.free-ipa-mac-level-min	—	xaldusermacmin	—	—	Название атрибута для минимального уровня конфиденциальности УЗ пользователя
xidbox.ldap.service.free-ipa.mac.free-ipa-mac-category	—	x-ald-user-mac	—	—	Название атрибута для максимальных и минимальных категорий конфиденциальности УЗ пользователя
xidbox.ldap.service.free-ipa.mac.free-ipa-mic	—	x-ald-user-mic-level	—	—	Название атрибута для категорий целостности УЗ пользователя
xidbox.ldap.service.free-ipa.mac.mac-level-base	—	cn=mac-levels,cn=mac-services,cn=parsec-configs,cn=etc	—	—	Суффикс для поиска словаря с описанием уровней конфиденциальности
xidbox.ldap.service.free-ipa.mac.mac-level-filter	—	x-ald-mac-level-object	—	—	Фильтр для поиска описания уровней конфиденциальности
xidbox.ldap.service.free-ipa.mac.mac-level-label	—	cn	—	—	Атрибут для определения наименования уровня конфиденциальности в словаре
xidbox.ldap.service.free-ipa.mac.mac-level-value	—	x-ald-mac-level	—	—	Атрибут для определения числового уровня конфиденциальности в словаре
xidbox.ldap.service.free-ipa.mac.mac-category-base	—	cn=mac-categories,cn=mac-services,cn=parsec-configs,cn=etc	—	—	Суффикс для поиска словаря с описанием категорий конфиденциальности
xidbox.ldap.service.free-ipa.mac.mac-category-filter	—	x-ald-mac-category-object	—	—	Фильтр для поиска описания категорий конфиденциальности
xidbox.ldap.service.free-ipa.mac.mac-category-label	—	cn	—	—	Атрибут для определения наименования категории конфиденциальности в словаре
xidbox.ldap.service.free-ipa.mac.mac-category-value	—	x-ald-mac-category	—	—	Атрибут для определения числовой категории конфиденциальности в словаре
xidbox.ldap.service.free-ipa.mac.mic-level-base	—	cn=mic-levels,cn=mic-services,cn=parsec-configs,cn=etc	—	—	Суффикс для поиска словаря с описанием уровней целостности
xidbox.ldap.service.free-ipa.mac.mic-level-filter	—	x-ald-user	—	—	Фильтр для поиска описания уровней целостности
xidbox.ldap.service.free-ipa.mac.mic-level-label	—	cn	—	—	Атрибут для определения наименования уровня целостности в словаре
xidbox.ldap.service.free-ipa.mac.mic-level-value	—	x-ald-user-mic-level	—	—	Атрибут для определения числового уровня целостности в словаре
xidbox.ldap.service.ald.mac.ald-mac-level-max	—	—	xaldusermacmax	—	Название атрибута для максимального уровня конфиденциальности УЗ пользователя
xidbox.ldap.service.ald.mac.ald-mac-level-min	—	—	xaldusermacmin	—	Название атрибута для минимального уровня конфиденциальности УЗ пользователя
xidbox.ldap.service.ald.mac.ald-mac-category	—	—	x-ald-user-mac	—	Название атрибута для максимальных и минимальных категорий конфиденциальности УЗ пользователя

Название	Значение для AD	Значение для FreeIpa	Значение для ALD	Значение для OpenLdap	Назначение
xidbox.ldap.service.ald.mac.ald-mic	—	—	x-ald-user-mic-level	—	Название атрибута для категорий целостности УЗ пользователя
xidbox.ldap.service.ald.mac.mac-level-base	—	—	cn=mac-levels,cn=mac-services,cn=parsec-configs,cn=etc	—	Суффикс для поиска словаря с описанием уровней конфиденциальности
xidbox.ldap.service.ald.mac.mac-level-filter	—	—	x-ald-mac-level-object	—	Фильтр для поиска описания уровней конфиденциальности
xidbox.ldap.service.ald.mac.mac-level-label	—	—	cn	—	Атрибут для определения наименования уровня конфиденциальности в словаре
xidbox.ldap.service.ald.mac.mac-level-value	—	—	x-ald-mac-level	—	Атрибут для определения числового уровня конфиденциальности в словаре
xidbox.ldap.service.ald.mac.mac-category-base	—	—	cn=mac-categories,cn=mac-services,cn=parsec-configs,cn=etc	—	Суффикс для поиска словаря с описанием категорий конфиденциальности
xidbox.ldap.service.ald.mac.mac-category-filter	—	—	x-ald-mac-category-object	—	Фильтр для поиска описания категорий конфиденциальности
xidbox.ldap.service.ald.mac.mac-category-label	—	—	cn	—	Атрибут для определения наименования категории конфиденциальности в словаре
xidbox.ldap.service.ald.mac.mac-category-value	—	—	x-ald-mac-category	—	Атрибут для определения числового уровня категории конфиденциальности в словаре
xidbox.ldap.service.ald.mac.mic-level-base	—	—	cn=mic-levels,cn=mic-services,cn=parsec-configs,cn=etc	—	Суффикс для поиска словаря с описанием уровней целостности
xidbox.ldap.service.ald.mac.mic-level-filter	—	—	x-ald-user	—	Фильтр для поиска описания уровней целостности
xidbox.ldap.service.ald.mac.mic-level-label	—	—	cn	—	Атрибут для определения наименования уровня целостности в словаре
xidbox.ldap.service.ald.mac.mic-level-value	—	—	x-ald-user-mic-level	—	Атрибут для определения числового уровня целостности в словаре
xidbox.ldap.service.ald.organization.attribute-name	—	—	user-custom-attr	—	Наименование атрибута, в котором хранятся кастомизированные поля пользователя ¹⁾
xidbox.ldap.service.ald.organization.field-name-of-uuid	—	—	<например, organization_uuid>	—	Наименование поля, в котором содержится идентификатор организации, зарегистрированной в X-IDBox ¹⁾ . Значение указанного поля в LDAP-каталоге может содержать несколько идентификаторов организаций через запятую. Поле ожидается в списке кастомизированных полей пользователя, наименование которого задается настройкой «xidbox.ldap.service.ald.organization.attribute-name»
xidbox.ldap.service.ald.organization.external-identifier[0].source-tech-name	—	—	<например, SVR>	—	Техническое наименование источника идентификатора ¹⁾
xidbox.ldap.service.ald.organization.external-identifier[0].field-tech-name	—	—	<например, orgCode>	—	Техническое наименование поля идентификатора ¹⁾

Название	Значение для AD	Значение для FreeIpa	Значение для ALD	Значение для OpenLdap	Назначение
xidbox.ldap.service.ald.organization.external-identifier[0].field-name-of-directory	–	–	organization_identifier	–	Наименование поля, в котором содержится значение идентификатора в LDAP-каталоге ¹⁾ . Значение указанного поля в LDAP-каталоге может содержать несколько идентификаторов организаций через запятую. Поле ожидается в списке кастомизированных полей пользователя, наименование которого задается настройкой «xidbox.ldap.service.ald.organization.attribute-name»
xidbox.ldap.service.organization.field-name-of-uuid	<например, organization_uuid>	<например, organization_uuid>	–	<например, organization_uuid>	Наименование поля, в котором содержится идентификатор организации, зарегистрированной в X-IDBox ²⁾ . Значение указанного поля в LDAP-каталоге может содержать несколько идентификаторов организаций через запятую
xidbox.ldap.service.organization.external-identifier[0].source-tech-name	<например, SVR>	<например, SVR>	<например, SVR>	<например, SVR>	Техническое наименование источника идентификатора ²⁾
xidbox.ldap.service.organization.external-identifier[0].field-tech-name	<например, orgCode>	<например, orgCode>	<например, orgCode>	<например, orgCode>	Техническое наименование поля идентификатора ²⁾
xidbox.ldap.service.organization.external-identifier[0].field-name-of-directory	organization_identifier	organization_identifier	organization_identifier	organization_identifier	Наименование поля, в котором содержится значение идентификатора в LDAP-каталоге ²⁾ . Значение указанного поля в LDAP-каталоге может содержать несколько идентификаторов организаций через запятую
xidbox.ldap.service.ald.attribute-name	–	–	user-custom-attr	–	Наименование атрибута пользователя, в котором хранятся «Дополнительные сведения». Допускается только для ALD Pro

¹⁾ Настройки позволяют считывать только те данные, которые указаны во вкладке «Дополнительные сведения» карточки УЗ пользователя в ALD Pro.
²⁾ Настройки позволяют считывать только те данные, которые указаны в атрибутах пользователя LDAP-каталога

Б.16 Настройки сервиса xidbox-organizational-structure

Таблица 32 – Настройки сервиса xidbox-organizational-structure

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

Б.17 Настройки сервиса xidbox-signature

Таблица 33 – Настройки сервиса xidbox-signature

Название	Значение по умолчанию	Назначение
xidbox.signature-counter-agent.service.use-counter-agent-service	false	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	–	Схема и наименование сервиса, реализацию которого необходимо использовать
xidbox.signature-counter-agent.service.path	–	Часть URL, по которому будет располагаться ожидаемая реализация

Б.18 Настройки сервиса xidbox-request-background-processing

Таблица 34 – 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

Название	Значение по умолчанию	Назначение
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
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); - structure,partial_logic_replication – создает SQL-структуру для реплицированных таблиц и создает только структуру таблиц; - data,partial_logic_replication – создает SQL-структуру для реплицированных таблиц и выполняет только миграцию данных (без структуры таблиц)
xidbox.request-background-processing.service.eureka.authz.client.enabled	false	Включает использование eureka для доступа к сервису авторизации. Иначе используется шлюз (gateway) по настройке xidbox.gateway.url
xidbox.request-background-processing.service.authz-request.processing.archive-stale-delay	1m	Задержка между задачами архивации простаивающих запросов. Запрос считается простаивающим, когда с последнего запроса результатов прошло значение минимального время действия запроса настройки «xidbox.request-background-processing.service.authz-request.processing.min-ttl»
xidbox.request-background-processing.service.authz-request.processing.min-ttl	1d	Минимальное время действия запроса

Название	Значение по умолчанию	Назначение
xidbox.request-background-processing.client.rest.connect-timeout	60s	Время, в течение которого должно быть установлено соединение с сервером
xidbox.request-background-processing.client.rest.read-timeout	60s	Время, в течение которого сервер должен дать ответ

Б.19 Настройки сервиса xidbox-callback-kafka

Таблица 35 – 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.20 Настройки сервиса xidbox-directory-synchronization

Таблица 36 – Настройки сервиса xidbox-directory-synchronization

Название	Значение по умолчанию	Назначение
xidbox.directory-synchronization.service.dynamic-field.source	–	Наименование источника динамических полей в X-IDBox
xidbox.directory-synchronization.service.dynamic-field.simple-map.<техническое наименование динамического поля в xidbox>=<наименование атрибута в LDAP-каталоге>	–	Сопоставление значений динамических полей X-IDBox с типом «SIMPLE» и атрибутов LDAP-каталога
xidbox.directory-synchronization.service.dynamic-field.simple-array-map.<техническое наименование динамического поля в xidbox>=<наименование атрибута в LDAP-каталоге>	–	Сопоставление значений динамических полей X-IDBox с типом «SIMPLE_ARRAY» и атрибутов LDAP-каталога
xidbox.directory-synchronization.service.core-field.ldap.middle-name	–	Наименование атрибута пользователя в LDAP-каталоге, в котором хранится отчество. Если наименование пустое, то отчество не синхронизируется
xidbox.directory-synchronization.service.core-field.ldap.middle-name-regex	"[a-zA-Za-яА-ЯЁё][a-zA-Za-яА-ЯЁё\\-]*[a-zA-Za-яА-ЯЁё]?"	Регулярное выражение для валидации отчества
xidbox.directory-synchronization.service.core-field.ldap.inn	–	Наименование атрибута пользователя в LDAP-каталоге, в котором хранится ИНН. Если наименование пустое, то ИНН не синхронизируется
xidbox.directory-synchronization.service.core-field.ldap.inn-regex	\\d{10} \\d{12}	Регулярное выражение для валидации ИНН
xidbox.directory-synchronization.service.core-field.ldap.snils	–	Наименование атрибута пользователя в LDAP-каталоге, в котором хранится СНИЛС. Если наименование пустое, то СНИЛС не синхронизируется
xidbox.directory-synchronization.service.core-field.ldap.snils-regex	\\d{3}-?\\d{3}-?\\d{3}[-]?\\d{2}	Регулярное выражение для валидации СНИЛС
xidbox.directory-synchronization.service.core-field.ldap.email	syncLdapToXidboxUserEmail	Наименование атрибута пользователя в LDAP-каталоге, в котором хранится адрес электронной почты. Если наименование пустое, то адрес электронной почты не синхронизируется. По умолчанию указано техническое наименование, значение которого генерируется системой в зависимости от типа LDAP-каталога
xidbox.directory-synchronization.service.core-field.ldap.email-regex	(?=^.{1,512}\$)[^А-Яа-яЁё@\\s]+@[^А-Яа-яЁё@\\s.][^А-Яа-яЁё@\\s]*\\. [^А-Яа-яЁё@\\s]+	Регулярное выражение для валидации адреса электронной почты пользователя

Б.21 Настройки сервиса xidbox-order-archive-database

Таблица 37 – Настройки сервиса xidbox-order-archive-database

Название	Значение по умолчанию	Назначение
xidbox.order-archive-database.service.spring.jpa.show-sql	false	Признак для вывода SQL-запросов, которые выполняются к БД xidbox-order-archive-database. Значение «true» – если SQL-запросы выводятся. Значение «false» – если SQL-запросы не выводятся
xidbox.order-archive-database.service.spring.jpa.properties.hibernate.default_schema	archive_order	Наименование схемы, к которой подключается сервис xidbox-order-archive-database
xidbox.order-archive-database.service.spring.liquibase.liquibase-schema	archive_changes	Схема создания и использования таблиц liquibase
xidbox.order-archive-database.search.count-exact-threshold	5000	Максимальный результат приблизительного вычисления количества заявок, при котором будет выполнен точный подсчет их количества
xidbox.order-archive-database.search.probe-value	0.01	Процент архивных заявок (значение от 0 до 1, где 1 = 100%), от которого будет рассчитываться приблизительное количество заявок в БД

Б.22 Настройки сервиса xidbox-internal-message-database

Таблица 38 – Настройки сервиса xidbox-internal-message-database

Название	Значение по умолчанию	Назначение
xidbox.internal-message-database.service.spring.liquibase.contexts	pg11GreaterOrEqual	Управляет процессом запуска скриптов миграции, доступны 3 режима: – только структура – structure,pg11GreaterOrEqual или structure,pg10; – только данные – data,pg11GreaterOrEqual или data,pg10; – структура и данные – default,pg11GreaterOrEqual или default,pg10 или structure,data,pg11GreaterOrEqual или structure,data,pg10. Режим работы сервиса с БД, принимает одно из значений: – pg11GreaterOrEqual – для работы с PostgreSQL версии 11 и выше; – pg10 – для работы с PostgreSQL версии 10
xidbox.internal-message-database.service.create-internal-message-partitions.cron	0 0 0 * * ?	Срон задачи для создания партиции системных уведомлений

Б.23 Настройки сервиса xidbox-organization

Таблица 39 – Настройки сервиса xidbox-organization

Название	Значение по умолчанию	Назначение
xidbox.organization.service.path.tmp	\${java.io.tmpdir:tmp}	Путь, в котором будут создаваться временные папки и файлы при загрузке
xidbox.organization.service.path.init-dir	init	Наименование папки, в которую будут временно сохраняться входные файлы при загрузке
xidbox.organization.service.path.report-dir	report	Наименование папки, в которой будут временно сохраняться промежуточные отчеты при загрузке

Б.24 Настройки сервиса xidbox-user-upload

Таблица 40 – Настройки сервиса xidbox-user-upload

Название	Значение по умолчанию	Назначение
xidbox.user-upload.service.path.tmp	\${java.io.tmpdir:tmp}	Путь, в котором будут создаваться временные папки и файлы при загрузке
xidbox.user-upload.service.path.init-dir	init	Наименование папки, в которую будут временно сохраняться входные файлы при загрузке
xidbox.user-upload.service.path.report-dir	report	Наименование папки, в которой будут временно сохраняться промежуточные отчеты при загрузке

Б.25 Настройки сервиса xidbox-user-profile-upload

Таблица 41 – Настройки сервиса xidbox-user-profile-upload

Название	Значение по умолчанию	Назначение
xidbox.user-profile-upload.service.path.tmp	\${java.io.tmpdir:tmp}	Путь, в котором будут создаваться временные папки и файлы при загрузке
xidbox.user-profile-upload.service.path.init-dir	init	Наименование папки, в которую будут временно сохраняться входные файлы при загрузке
xidbox.user-profile-upload.service.path.report-dir	report	Наименование папки, в которой будут временно сохраняться промежуточные отчеты при загрузке

Б.26 Настройки для всех сервисов

Для возможности разграничить настройки каждой группы сервисов в общем «xidbox.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 42.

Таблица 42 – 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
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

Название	Значение по умолчанию	Назначение
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.application-id-name	xidbox-request-application-id	Наименование заголовка запроса, в котором передается идентификатор приложения ИС, отправившего запрос
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
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/authorz-to-service?serviceTechName=	Путь, по которому происходит запрос для получения данных для проверки контрольной суммы запроса

Название	Значение по умолчанию	Назначение
authn-request-verification.application-info-protocol	http://	Протокол, по которому необходимо сделать запрос для получения информации о приложении ИС
authn-request-verification.application-info-uri	x-idbox-database-service/database/api/v1/information/system/application/info?techName=	Путь, по которому необходимо сделать запрос для получения информации о приложении ИС
authn-request-verification.content-cache-mode	–	Способ хранения тела запросов при расчете контрольной суммы: – RAM – оперативная память (или если свойство не указано); – мять (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 uthn-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.application-id-name	xidbox-request-application-id	Наименование заголовка ответа, в котором передается идентификатор приложения ИС, отправившего 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

Приложение В
Дополнительные данные о событиях безопасности

В таблице 43 приведены все данные, сохраняемые в расширении записей о событиях безопасности. Те ключи, которые не предопределены в формате CEF, перечислены также в таблице 6.

Таблица 43 – 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	Способ 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 ОИШ; – DEPARTMENT_LEVELS – загрузка изменений уровней подразделений; – DEPARTMENTS – загрузка изменений подразделений; – POSITIONS – загрузка изменений должностей; – INFO_SYSTEMS – загрузка ИС; – INFO_SYSTEM_STRUCTURE – загрузка структуры ИС – USER_DYNAMIC_FIELD_DESCRIPTIONS – загрузка обновления настроек динамических полей УЗ пользователя; – USER_PROFILE_DYNAMIC_FIELD_DESCRIPTIONS – загрузка обновления настроек динамических полей профиля УЗ пользователя; – DICTIONARY – загрузка справочника; – DICTIONARY_DATA – загрузка данных справочника; – USER_PROFILE_DYNAMIC_FIELD_SOURCE_CONFIGURATION – загрузка конфигурации источника динамических полей профиля УЗ пользователя	– 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 ОИШ;
		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 – objectUid	–	
		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 ОИШ; – DEPARTMENT_LEVELS – загрузка изменений уровней подразделений; – DEPARTMENTS – загрузка изменений подразделений; – POSITIONS – загрузка изменений должностей; – INFO_SYSTEM_STRUCTURE – загрузка структуры ИС – USER_DYNAMIC_FIELD_DESCRIPTIONS – загрузка обновления настроек динамических полей УЗ пользователя; – USER_PROFILE_DYNAMIC_FIELD_DESCRIPTIONS – загрузка обновления настроек динамических полей профиля УЗ пользователя; – DICTIONARY – загрузка справочника; – DICTIONARY_DATA – загрузка данных справочника; – USER_PROFILE_DYNAMIC_FIELD_SOURCE_CONFIGURATION – загрузка конфигурации источника динамических полей профиля УЗ пользователя	– 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
		cs2Label	Фиксированное значение – objectUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой произошло событие загрузки данных	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие загрузки информации	DATA_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 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;
		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 – objectUid	–	
		cs1	Загружаемые данные	Возможные значения: – USERS – загрузка пользователей; – PROFILES – загрузка профилей УЗ пользователей; – ROLES_ASSIGNMENT – загрузка назначений ролей	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
				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 ОИИС; – DEPARTMENT_LEVELS – загрузка изменений уровней подразделений; – DEPARTMENTS – загрузка изменений подразделений; – POSITIONS – загрузка изменений должностей; – INFO_SYSTEM_STRUCTURE – загрузка структуры ИС – USER_DYNAMIC_FIELD_DESCRIPTIONS – загрузка обновления настроек динамических полей УЗ пользователя; – USER_PROFILE_DYNAMIC_FIELD_DESCRIPTIONS – загрузка обновления настроек динамических полей профиля УЗ пользователя – DICTIONARY – загрузка справочника; – DICTIONARY_DATA – загрузка данных справочника; – USER_PROFILE_DYNAMIC_FIELD_SOURCE_CONFIGURATION – загрузка конфигурации источника динамических полей профиля УЗ пользователя	– загрузка ролевой модели; – загрузка ОИИС; – 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
		cs2Label	Фиксированное значение – objectUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой произошло событие загрузки данных	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие выгрузки информации	DATA_EXPORT	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксируется при попытке выгрузки информации. Фиксируются следующие параметры: – дата и время события безопасности; – идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации
		source	Фиксированное значение – XIDBOX	–	
		suid	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, который выгружает данные	
		cs4Label	Фиксированное значение – typeData	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		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	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор регистрируемой УЗ пользователя	
		cs2Label	Фиксированное значение – orderId	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		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	–	
		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
		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 – objectUid	–	
		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 – objectUid	–	
		cs1	Идентификатор УЗ пользователя	Идентификатор УЗ пользователя, данные которой будут изменены	
		cs2Label	Фиксированное значение – orderUid	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		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 описания динамических полей УЗ пользователя	DESCRIPTION_OF_USER_DYNAMIC_FIELDS_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 обновление описания динамических полей УЗ пользователя. 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 изменение описания динамических полей УЗ пользователя. Если идентификатор отсутствует (заявка на изменение описания динамических полей УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1	Идентификатор источника динамических полей	Идентификатор источника динамических полей, в рамках которого изменятся описание динамических полей	
		cs1Label	Фиксированное значение – objectId	–	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
				–	
Событие окончания создания заявки на изменение описания динамических полей УЗ пользователя	DESCRIPTION_OF_USER_DYNAMIC_FIELDS_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 обновление описания динамических полей УЗ пользователя. 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 изменение описания динамических полей УЗ пользователя. Если идентификатор отсутствует (заявка на изменение описания динамических полей УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1	Идентификатор источника динамических полей	Идентификатор источника динамических полей, в рамках которого изменятся описание динамических полей	
		cs1Label	Фиксированное значение – objectId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение описания динамических полей	
		cs2Label	Фиксированное значение – orderId	–	

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 начала создания заявки на изменение описания динамических полей профиля УЗ пользователя	DESCRIPTION_OF_USER_PROFILE_DYNAMIC_FIELDS_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 обновление описания динамических полей профиля УЗ пользователя. 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 изменение описания динамических полей профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение описания динамических полей профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1	Идентификатор источника динамических полей	Идентификатор источника динамических полей, в рамках которого изменятся описание динамических полей	
		cs1Label	Фиксированное значение – objectId	–	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие окончания создания заявки на изменение описания динамических полей профиля УЗ пользователя	DESCRIPTION_OF_USER_PROFILE_DYNAMIC_FIELDS_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 обновление описания динамических полей профиля УЗ пользователя. 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 изменение описания динамических полей профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение описания динамических полей профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	
		cs1	Идентификатор источника динамических полей	Идентификатор источника динамических полей, в рамках которого изменятся описание динамических полей	
		cs1Label	Фиксированное значение – objectId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение описания динамических полей	
		cs2Label	Фиксированное значение – orderId	–	
		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 изменение/сброс пароля	PASSWORD_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/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_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/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	
		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).

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 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	
		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	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
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 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 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	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		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_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 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_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/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	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается изменение сертификатов	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		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	
Событие начала создания заявки на синхронизацию УЗ пользователей с LDAP-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 LDAP-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
		source	Фиксированное значение – orderId	Источник события безопасности	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs2Label	Фиксированное значение – orderId	–	безопасности; – идентификационная информация источника события безопасности; – результат события безопасности
		cs2	Идентификатор заявки	Идентификатор заявки, по которой ожидается событие синхронизации УЗ пользователей	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Синхронизация УЗ пользователей с LDAP-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 (логируется в момент перехода заявки на синхронизацию УЗ пользователей из LDAP-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 синхронизации 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; – 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 – objectId	–	
		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;
		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	
		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	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на обновление источника динамических полей УЗ пользователя	UPDATE_USER_DYNAMIC_FIELD_SOURCE_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 обновление источника динамических полей 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	–	
		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 обновление источника динамических полей УЗ пользователя	UPDATE_USER_DYNAMIC_FIELD_SOURCE_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 обновление источника динамических полей 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	–	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие обновления источника динамических полей УЗ пользователя	UPDATE_USER_DYNAMIC_FIELD_SOURCE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует обновление источника динамических полей 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	–	
		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 УЗ пользователя	Идентификатор УЗ пользователя регистрируемого профиля УЗ пользователя	
		cs8Label	Фиксированное значение – objectId	–	
		cs8	Идентификатор организации	Идентификатор организации, в которой регистрируется профиль 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 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 УЗ пользователя	Идентификатор УЗ пользователя регистрируемого профиля УЗ пользователя	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, по которой ожидается событие регистрации профиля УЗ пользователя	
		cs8Label	Фиксированное значение – objectId	–	
		cs8	Идентификатор организации	Идентификатор организации, в которой регистрируется профиль УЗ пользователя	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
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 (логируется 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	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs8Label	Фиксированное значение – objectUid	–	
		cs8	Идентификатор организации	Идентификатор организации, в которой регистрируется профиль 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 логе пустой	
		cs1Label	Фиксированное значение – objectUid	–	
		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: – 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 изменяются	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой происходит изменение данных	

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 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 (логируется 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: – 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, должности которого изменяются	
		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 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: – 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 изменены	
		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	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
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 – objectId	–	
		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. 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 ожидается 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 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	
		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;
		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 роли профиля УЗ пользователя. Если идентификатор отсутствует (заявка на изменение ролей профиля УЗ пользователя была создана автоматически) – ключ «suid» в логе пустой	– 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, 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 – objectUid	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, у которого меняются роли	
		cs2Label	Фиксированное значение – orderUid	–	
		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
		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	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs1Label	Фиксированное значение – objectUid	–	источника события безопасности; – результат события безопасности; – субъект доступа
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, у которого меняются роли	
		cs2Label	Фиксированное значение – orderUid	–	
		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 – objectUid	–	
		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	
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 – objectUid	–	
		cs1	Идентификатор профиля УЗ пользователя	Идентификатор профиля УЗ пользователя, сессии которого были завершены	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается завершение сессий	
		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 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	
Событие начала создания заявки на обновление источника динамических полей профилей УЗ пользователя	UPDATE_USER_PROFILE_DYNAMIC_FIELD_SOURCE_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 обновление источника динамических полей профилей 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	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на обновление источника динамических полей профилей УЗ пользователя	UPDATE_USER_PROFILE_DYNAMIC_FIELD_SOURCE_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 обновление источника динамических полей профилей 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	
		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 обновления источника динамических полей профилей УЗ пользователя	UPDATE_USER_PROFILE_DYNAMIC_FIELD_SOURCE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует обновление источника динамических полей профилей 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	
		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: – 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 – objectId	–	
		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 – objectId	–	
		cs1	Идентификатор организации	Идентификатор регистрируемой организации	
		cs2Label	Фиксированное значение – orderId	–	
		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).

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
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Идентификатор организации	Идентификатор созданной организации. Пустое значение, если событие завершилось неуспешно	
		cs2Label	Фиксированное значение – orderId	–	
		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: – 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 – objectId	–	
		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 – objectId	–	
		cs1	Идентификатор организации	Идентификатор организации, данные которой меняются	
		cs2Label	Фиксированное значение – orderId	–	
		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 (логируется в момент перехода заявки на изменение данных организации в финальное

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник события безопасности	состояние). Фиксируются следующие параметры: – 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. 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: – 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 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	
		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	

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 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; – результат события безопасности; – субъект доступа
		source	Фиксированное значение – XIDBOX	Источник события безопасности	
		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 начала создания заявки на обновление источника динамических полей организации	UPDATE_ORGANIZATION_DYNAMIC_FIELD_SOURCE_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 обновление источника динамических полей 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	–	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на обновление источника динамических полей организации	UPDATE_ORGANIZATION_DYNAMIC_FIELD_SOURCE_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 обновление источника динамических полей 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	–	
		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 обновления источника динамических полей организации	UPDATE_ORGANIZATION_DYNAMIC_FIELD_SOURCE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует момент обновления источника динамических полей 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	–	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
События, связанные с ролевой моделью, ролями и ЗО					
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 ЗО. 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 ЗО	
		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 ЗО. 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 ЗО	
		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	

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 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;

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		source	Фиксированное значение – XIDBOX	Источник 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 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 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 (логируется в момент перехода заявки на изменение 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 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:

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 роли	
		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	

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 ИС					
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 – orderUid	–	
		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 (логировается в момент перехода заявки на регистрацию 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, который инициировал регистрацию 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, которую регистрируют	
		cs2Label	Фиксированное значение – orderUid	–	
		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	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
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; – 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 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	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 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, данные которой меняются	
		cs8Label	Фиксированное значение – objectId	–	
		cs8	Загружаемые данные	ORGANIZATIONAL_STRUCTURE – Загрузка ОШС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на создание ОШС	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 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, данные которой меняются	
		cs2Label	Фиксированное значение – orderUid	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается событие создания ОШС	
		cs8Label	Фиксированное значение – objectUid	Идентификатор организации	
		cs8	Загружаемые данные	ORGANIZATIONAL_STRUCTURE – Загрузка ОШС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания ОШС	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 создание ОШС у организации (логировается 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 – objectUid	–	
		cs1	Идентификатор организации	Идентификатор организации, для которой создавалась ОШС	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие создания ОШС	
		cs8Label	Фиксированное значение – objectUid	–	
		cs8	Загружаемые данные	ORGANIZATIONAL_STRUCTURE – Загрузка ОШС	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие начала создания заявки на изменение ОШС	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 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 – objectUid	–	
		cs1	Идентификатор организации	Идентификатор организации, данные которой меняются	
		cs8Label	Фиксированное значение – objectUid	–	
		cs8	Загружаемые данные	В зависимости от того, что загружается: – DEPARTMENT_LEVELS – Загрузка изменений уровней подразделений – DEPARTMENTS – Загрузка изменений подразделений – POSITIONS – Загрузка изменений должностей	

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 создания заявки на изменение ОИШС	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 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, данные которой меняются	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается событие изменения ОИШС	
		cs8Label	Фиксированное значение – objectId	–	
		cs8	Загружаемые данные	В зависимости от того, что загружается: – DEPARTMENT_LEVELS – Загрузка изменений уровней подразделений – DEPARTMENTS – Загрузка изменений подразделений – POSITIONS – Загрузка изменений должностей	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие изменения ОИШС	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 изменения подразделений/должностей/уровней подразделений у организации (логируется в момент перехода заявки на загрузку ОИШС 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 ОИШС	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие изменения ОИШС	
		cs8Label	Фиксированное значение – objectId	–	
		cs8	Загружаемые данные	ORGANIZATIONAL_STRUCTURE – Загрузка ОИШС	

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 со справочниками					
Событие начала создания заявки на деактивацию справочника	DICTIONARY_DEACTIVATE_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 деактивацию справочника. 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	Техническое наименование справочника	Техническое наименование справочника, который будет деактивирован	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие создания заявки на деактивацию справочника	DICTIONARY_DEACTIVATE_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 деактивацию справочника. 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	Техническое наименование справочника	Техническое наименование справочника, который деактивируется	
		cs2Label	Фиксированное значение – orderId	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается событие деактивации справочника	
		outcome	Результат события	Возможные значения: – success – событие завершилось успешно; – failure – событие завершилось неуспешно	
Событие деактивации справочника	DICTIONARY_DEACTIVATE	dtz	Фиксированное значение – Europe/Moscow	Часовой пояс, в котором было зафиксировано событие (UTC). Логирование событий безопасности производится в часовом поясе Москвы	Событие фиксирует деактивацию справочника (логировается в момент перехода заявки на деактивацию справочника 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	
		cs1Label	Фиксированное значение – objectId	–	
		cs1	Техническое наименование справочника	Техническое наименование справочника, который деактивируется	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs2Label	Фиксированное значение – orderUid	–	– результат события безопасности; – субъект доступа
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло событие деактивации справочника	
		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 – orderUid	–	
		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	
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 (логируется 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;
		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	–	

Название события	label	Ключ (KEY)	Значение (VALUE)	Описание ключей и их значений	Описание события
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой произошло изменение настроек безопасности	- результат события безопасности; - субъект доступа
		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	
		outcome	Результат события	Возможные значения: - success – событие завершилось успешно; - failure – событие завершилось неуспешно	
Событие начала создания заявки на обновление описания атрибутов уровней и категорий доступа	MANDATORY_ACCESS_CONTROL_ATTRIBUTE_DESCRIPTION_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 обновление описания атрибутов уровней и категорий доступа. 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 инициировал обновление описания атрибутов уровней и категорий доступа	
		source	Фиксированное значение – XIDBOX	Источник события 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 создания заявки на обновление описания атрибутов уровней и категорий доступа	MANDATORY_ACCESS_CONTROL_ATTRIBUTE_DESCRIPTION_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 обновление описания атрибутов уровней и категорий доступа. 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 обновление описания атрибутов уровней и категорий доступа	
		cs2Label	Фиксированное значение – orderUid	–	
		cs2	Идентификатор заявки	Идентификатор заявки, на основании которой ожидается событие обновления описания атрибутов уровней и категорий доступа	
		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 (логируется 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	

Приложение Г
Структура данных в источнике

В таблице 44 приведена структура данных в источнике поля/атрибута в X-IDBox.

Таблица 44 – Структура данных в источнике поля/атрибута в X-IDBox

Источник	Наименование параметра	Параметр (атрибут)	Тип данных	Обязательность	Описание
current_user_detail	Идентификатор УЗ пользователя	uuid	UUID	Да	Идентификатор УЗ пользователя
	Идентификатор профиля УЗ пользователя	userProfileUuid	UUID	Да	Идентификатор профиля УЗ пользователя
	Признак верификации адреса электронной почты профиля УЗ пользователя	userProfileWorkEmailVerified	Логический	Да	Значение «true» – если адрес электронной почты профиля УЗ пользователя верифицирован. Значение «false» – если адрес электронной почты профиля УЗ пользователя не верифицирован
	Адрес электронной почты профиля УЗ пользователя	userProfileWorkEmail	Строка	Да	Адрес электронной почты профиля УЗ пользователя
	Логин	login	Строка	Да	Логин УЗ пользователя
	Адрес электронной почты УЗ пользователя	email	Строка	Нет	Адрес электронной почты УЗ пользователя
	Дата и время верификации адреса электронной почты УЗ пользователя	emailVerified	Дата и время	Нет	Дата и время верификации адреса электронной почты УЗ пользователя
	Серийный номер сертификата	serialNumber	Целое число	Нет	Серийный номер сертификата
	Состояние УЗ пользователя	state	Строка	Да	Состояние УЗ пользователя
	Дата и время согласия на обработку персональных данных	privacyPolicyAccepted	Дата и время	Нет	Дата и время согласия на обработку персональных данных
	Дата и время уведомления о мерах защиты информации	securityPolicyAccepted	Дата и время	Нет	Дата и время уведомления о мерах защиты информации
	Дата и время предыдущего успешного входа	previousSuccessfulLoginTime	Дата и время	Нет	Дата и время предыдущего успешного входа
	Количество неуспешных попыток входа	numberOfUnsuccessfulAttemptsSincePreviousSuccessfulLogin	Целое число	Нет	Количество неуспешных попыток входа
	Дата и время предыдущей неуспешной попытки входа	previousFailedLoginTime	Дата и время	Нет	Дата и время предыдущей неуспешной попытки входа
	Пройденные способы аутентификации	authTypes	Массив	Нет	Список пройденных способов аутентификации. Возможные значения: – LOGIN – логин и пароль; – CERT – сертификат; – KERBEROS_TICKET – доменная учётная запись с использованием протокола Kerberos; – ESIA – Госуслуги (ЕСИА)
	Разрешённые хосты с учётом первого фактора аутентификации	availableHostsByFirstFactor	Объект	Нет	Список адресов разрешённых хостов информационных систем с учётом первого фактора аутентификации

Источник	Наименование параметра	Параметр (атрибут)	Тип данных	Обязательность	Описание
current_user_main_attribute	Идентификатор УЗ пользователя	uuid	UUID	Да	Идентификатор УЗ пользователя
	Имя	firstName	Строка	Да	Имя пользователя
	Фамилия	lastName	Строка	Да	Фамилия пользователя
	Отчество	middleName	Строка	Нет	Отчество пользователя
	ИНН	inn	Строка	Нет	ИНН пользователя
	СНИЛС	snils	Строка	Нет	СНИЛС пользователя
	Дата рождения	birthday	Дата	Нет	Дата рождения пользователя
	Логин	login	Строка	Да	Логин УЗ пользователя
	Адрес электронной почты УЗ пользователя	email	Строка	Нет	Адрес электронной почты УЗ пользователя
	Дата и время изменения пароля	passwordChanged	Дата и время	Нет	Дата и время изменения пароля
	Дата и время верификации адреса электронной почты	emailVerified	Дата и время	Нет	Дата и время верификации адреса электронной почты УЗ пользователя
	Количество неуспешных попыток входа	countErrorAuthAttempt	Целое число	Да	Количество неуспешных попыток входа
	Признак блокирования УЗ пользователя	isBlocked	Логический	Да	Значение «true» – если УЗ пользователя заблокирована. Значение «false» – если УЗ пользователя не заблокирована
	Дата регистрации УЗ пользователя	registrationDate	Дата	Да	Дата регистрации УЗ пользователя
	Дата и время согласия на обработку персональных данных	privacyPolicyAccepted	Дата и время	Нет	Дата и время согласия на обработку персональных данных
	Дата и время уведомления о мерах защиты информации	securityPolicyAccepted	Дата и время	Нет	Дата и время уведомления о мерах защиты информации
	Дата отправки пользователю уведомления о скором окончании срока действия пароля	notifyPasswordExpires	Дата	Нет	Дата отправки пользователю уведомления о скором окончании срока действия пароля
	Дата отправки пользователю уведомления об окончании срока действия пароля	notifyPasswordExpired	Дата	Нет	Дата отправки пользователю уведомления об окончании срока действия пароля
	Дата отправки пользователю уведомления о приближении срока блокирования УЗ пользователя по причине неактивности	notifyBlockInactive	Дата	Нет	Дата отправки пользователю уведомления о приближении срока блокирования УЗ пользователя по причине неактивности
	Информация об уровнях и категориях доступа	mac	Объект	Нет	Информация об уровнях и категориях доступа УЗ пользователя
	Максимальный уровень конфиденциальности	macLevelMax	Целое число	Да	Максимальный уровень конфиденциальности
	Минимальный уровень конфиденциальности	macLevelMin	Целое число	Да	Минимальный уровень конфиденциальности
	Маска максимально доступных категорий конфиденциальности	macMaskCategoriesMax	Целое число	Да	Маска максимально доступных категорий конфиденциальности
	Маска минимальных категорий конфиденциальности	macMaskCategoriesMin	Целое число	Да	Маска минимальных категорий конфиденциальности
	Маска неиерархического уровня целостности УЗ пользователя	micMaskLevels	Целое число	Да	Маска неиерархического уровня целостности УЗ пользователя
	Дата и время последнего успешного входа	lastSuccessAuthAt	Дата и время	Нет	Дата и время последнего успешного входа
	Дата и время обновления данных УЗ пользователя	updateDate	Дата и время	Нет	Дата и время обновления данных УЗ пользователя

Источник	Наименование параметра	Параметр (атрибут)	Тип данных	Обязательность	Описание
current_user_profile_main_attribute	Идентификатор профиля УЗ пользователя	uuid	UUID	Да	Идентификатор профиля УЗ пользователя
	Адрес электронной почты профиля УЗ пользователя	workEmail	Строка	Нет	Адрес электронной почты профиля УЗ пользователя
	Дата и время верификации адреса электронной почты профиля УЗ пользователя	workEmailVerified	Дата и время	Нет	Дата и время верификации адреса электронной почты профиля УЗ пользователя
	Дата регистрации профиля УЗ пользователя	registrationDate	Дата и время	Да	Дата регистрации профиля УЗ пользователя
	Дата изменения профиля УЗ пользователя	changed	Дата и время	Да	Дата изменения профиля УЗ пользователя
current_user_profile_organization_main_attribute	Идентификатор организации	uuid	UUID	Да	Идентификатор организации
	Полное наименование организации	fullName	Строка	Да	Полное наименование организации
	Краткое наименование организации	shortName	Строка	Да	Краткое наименование организации
	ИНН	inn	Строка	Нет	ИНН организации
	КПП	kpp	Строка	Нет	КПП организации
	ОГРН	ogrn	Строка	Нет	ОГРН организации
	Адрес	address	Строка	Нет	Адрес организации
	Дата регистрации	registrationDate	Дата	Нет	Дата регистрации организации
	Дата создания	createDate	Дата и время	Да	Дата создания организации в системе
	Внешние идентификаторы организации	externalIdentifiers	Массив	Нет	Список внешних идентификаторов организации
	Техническое наименование источника	fieldSourceTechName	Строка	Да	Техническое наименование источника
	Техническое наименование поля	fieldTechName	Строка	Да	Техническое наименование поля в источнике
	Значение идентификатора	value	Строка	Да	Значение внешнего идентификатора в источнике
current_user_dynamic_attribute		–	Объект	Нет	Список пар (Техническое наименование динамического атрибута, Динамический атрибут) для динамических атрибутов УЗ пользователя
current_user_profile_dynamic_attribute		–	Объект	Нет	Список пар (Техническое наименование динамического атрибута, Динамический атрибут) для динамических атрибутов профиля УЗ пользователя
current_user_profile_organization_dynamic_attribute		–	Объект	Нет	Список пар (Техническое наименование динамического атрибута, Динамический атрибут) для динамических атрибутов организации пользователя

Пример настройки информации о пользователе, которая передаётся ИС в настраиваемых HTTP-заголовках запроса (xidbox.authn.custom.headers.settings[*]):

```
xidbox.authn.custom.headers.settings[0].header-name=xidbox-user-profile-user-login
xidbox.authn.custom.headers.settings[0].attribute-source=current_user_main_attribute
xidbox.authn.custom.headers.settings[0].pattern=login
```

```
xidbox.authn.custom.headers.settings[1].header-name=xidbox-user-profile-organization-inn
xidbox.authn.custom.headers.settings[1].attribute-source=current_user_profile_organization_main_attribute
xidbox.authn.custom.headers.settings[1].pattern=inn

xidbox.authn.custom.headers.settings[2].header-name=xidbox-user-profile-workEmail
xidbox.authn.custom.headers.settings[2].attribute-source=current_user_profile_main_attribute
xidbox.authn.custom.headers.settings[2].pattern=workEmail

xidbox.authn.custom.headers.settings[3].header-name=xidbox-user-profile-user-dynamic-single-attribute-with-name-
simpleUserFieldName
xidbox.authn.custom.headers.settings[3].attribute-source=current_user_dynamic_attribute
xidbox.authn.custom.headers.settings[3].pattern=?[key.techName ==
'user_dynamic_field_source'].![value][0].simpleFields.?[dynamicFieldTechName == 'simpleUserFieldName'][0].content.value

xidbox.authn.custom.headers.settings[4].header-name=xidbox-user-profile-user-profile-dynamic-array-attribute-with-name-
simpleUserArrayFieldName
xidbox.authn.custom.headers.settings[4].attribute-source=current_user_profile_dynamic_attribute
xidbox.authn.custom.headers.settings[4].pattern=?[key.techName ==
'user_profile_dynamic_field_source'].![value][0].simpleArrayFields.?[dynamicFieldTechName ==
'simpleUserArrayFieldName'][0].content[1].value

xidbox.authn.custom.headers.settings[5].header-name=xidbox-user-profile-user-organization-object-attribute-with-name-
userArrayObjectFieldName
xidbox.authn.custom.headers.settings[5].attribute-source=current_user_profile_organization_dynamic_attribute
xidbox.authn.custom.headers.settings[5].pattern=?[key.techName ==
'organization_field_source'].![value][0].objectArrayFields.?[dynamicFieldTechName ==
'userArrayObjectFieldName'][0].content[0].?[key == 'obj'].![value][0].content.value

xidbox.authn.custom.headers.settings[6].header-name=xidbox-user-profile-user-current_user_detail-prev-failed-login-time
xidbox.authn.custom.headers.settings[6].attribute-source=current_user_detail
xidbox.authn.custom.headers.settings[6].pattern=previousFailedLoginTime
```

Приложение Д

Сопоставление типов заявок и шаблонов уведомлений

В таблице 45 приведено сопоставление типов заявок и шаблонов уведомлений X-IDBox.

Таблица 45 – Сопоставление типов заявок и шаблонов уведомлений

Техническое наименование типа заявки	Наименование типа заявки	Техническое наименование шаблона уведомления	Наименование шаблона уведомления/Тема письма
block_user	Блокирование учетной записи	account_is_permanent_blocked	Учетная запись заблокирована
		order_cancel	Заявка отменена
		order_processing_error	Ошибка обработки заявки
block_organization	Блокирование организации	order_processing_error	Ошибка обработки заявки
change_account_data	Изменение данных учетной записи	created_order_to_change_account_data	Создана заявка на изменение данных учетной записи
		user_data_change_rejected	Изменение данных учетной записи отклонено
		email_confirmation_for_order	Подтверждение адреса электронной почты
		change_user_success	Данные учетной записи изменены
		user_data_changed	Изменение данных учетной записи завершено
		user_data_change_canceled	Данные учетной записи не были обновлены
		pend_approval_change_account_data	Требуется согласование заявки
		pend_confirmation_change_account_data	Требуется утверждение заявки
		order_processing_error	Ошибка обработки заявки
change_info_system_application	Изменение приложения ИС	order_processing_error	Ошибка обработки заявки
change_info_system	Изменение ИС	change_info_system	Изменение ИС успешно завершено
		change_info_system_rejected	Изменение ИС не выполнено
		order_processing_error	Ошибка обработки заявки
change_mail_templates	Изменение шаблонов уведомлений	change_notification_templates	Заявка на изменение шаблонов уведомлений
		order_processing_error	Ошибка обработки заявки
change_organization_data	Изменение данных организации	order_processing_error	Ошибка обработки заявки
change_password	Изменение пароля	password_changed	Пароль был успешно изменен
		order_processing_error	Ошибка обработки заявки
change_role_data	Изменение данных роли	change_role_data	Заявка на изменение данных роли
		order_processing_error	Ошибка обработки заявки
change_security_settings	Изменение настроек безопасности	change_security_settings	Заявка на изменение настроек безопасности
		order_processing_error	Ошибка обработки заявки
change_user_certs	Изменение списка сертификатов учетной записи	change_user_profile_certificate_list	Заявка на изменение списка сертификатов учетной записи
		order_processing_error	Ошибка обработки заявки
change_user_profile_data	Изменение данных профиля учетной записи	email_confirmation_for_order	Подтверждение адреса электронной почты
		change_user_profile_success	Данные или роли профиля учетной записи изменены
		user_profile_data_change_success	Изменение данных профиля учетной записи успешно завершено
		order_processing_error	Ошибка обработки заявки
change_user_profile_notification_settings	Изменение настроек уведомлений	change_notification_settings	Настройки уведомлений успешно изменены

Техническое наименование типа заявки	Наименование типа заявки	Техническое наименование шаблона уведомления	Наименование шаблона уведомления/ Тема письма
change_user_profile_positions	Изменение должностей профиля учетной записи пользователя	order_processing_error	Ошибка обработки заявки
		order_cancel	Заявка отменена
		change_user_profile_success	Данные или роли профиля учетной записи изменены
		change_user_profile_positions	Заявка на изменение должностей профилей учетных записей
		pend_approval_change_user_profile_positions	Требуется согласование заявки
		pend_confirmation_change_user_profile_positions	Требуется утверждение заявки
		order_processing_error	Ошибка обработки заявки
change_user_profile_roles	Изменение ролей профиля учетной записи	change_roles_rejected	Заявка на изменение ролей профиля учетной записи отклонена
		change_roles	Заявка на изменение ролей профиля учетной записи создана
		change_user_profile_success	Данные или роли профиля учетной записи изменены
		change_roles_success	Заявка на изменение ролей профиля учетной записи выполнена
		pend_approval_change_user_profile_roles	Требуется согласование заявки
		pend_confirmation_change_user_profile_roles	Требуется утверждение заявки
		order_cancel	Заявка отменена
		order_processing_error	Ошибка обработки заявки
reg_info_system_application	Регистрация приложения ИС	order_processing_error	Ошибка обработки заявки
reg_info_system	Регистрация ИС	registration_info_system	Регистрация ИС успешно завершена
		registration_info_system_rejected	Регистрация ИС не выполнена
		order_processing_error	Ошибка обработки заявки
create_oauth_consent	Предоставление доступа внешней системе через OAuth 2.0	order_processing_error	Ошибка обработки заявки
create_organization	Регистрация организации	order_processing_error	Ошибка обработки заявки
deactivate_dictionary	Деактивация справочника	order_processing_error	Ошибка обработки заявки
delete_oauth_consent	Отзыв доступа внешней системы через OAuth 2.0	order_processing_error	Ошибка обработки заявки
end_sessions	Завершение сессий профиля учетной записи	end_sessions	Завершение сеансов пользователя
		order_canceled_end_sessions	Отмена заявки на завершение сеансов пользователя
		order_processing_error	Ошибка обработки заявки
permanent_block_user_profile	Блокирование профиля учетной записи	change_user_profile_success	Данные или роли профиля учетной записи изменены
		user_profile_is_permanent_blocked	Профиль учетной записи заблокирован
		order_cancel	Заявка отменена
		order_processing_error	Ошибка обработки заявки
reset_password	Сброс пароля	change_password	Восстановление пароля
		password_changed	Пароль был успешно изменен
		password_reset_rejected	Сбросить пароль не удалось
		order_processing_error	Ошибка обработки заявки
temporarily_block_user	Временное блокирование учетной записи	account_is_temporarily_blocked	Учетная запись временно заблокирована
		order_cancel	Заявка отменена
		order_processing_error	Ошибка обработки заявки
temporarily_block_user_profile	Временное блокирование профиля учетной записи	user_profile_is_temporarily_blocked	Профиль учетной записи временно заблокирован

Техническое наименование типа заявки	Наименование типа заявки	Техническое наименование шаблона уведомления	Наименование шаблона уведомления/ Тема письма
unlock_user	Разблокирование учетной записи	order_cancel	Заявка отменена
		order_processing_error	Ошибка обработки заявки
		account_unlock_process_started	Запущен процесс разблокирования учетной записи
		account_is_unlocked	Учетная запись разблокирована
		order_cancel	Заявка отменена
unlock_user_profile	Разблокирование профиля учетной записи пользователя	order_processing_error	Ошибка обработки заявки
		user_profile_is_unlocked	Профиль учетной записи разблокирован
		order_cancel	Заявка отменена
update_description_of_organization_dynamic_fields	Обновление настроек динамических полей организаций	order_processing_error	Ошибка обработки заявки
		order_processing_error	Ошибка обработки заявки
		order_processing_error	Ошибка обработки заявки
update_description_of_user_dynamic_fields	Обновление настроек динамических полей УЗ	order_processing_error	Ошибка обработки заявки
update_description_of_user_profile_dynamic_fields	Обновление настроек динамических полей профиля УЗ	order_processing_error	Ошибка обработки заявки
update_dictionary_data	Изменение данных справочника	order_processing_error	Ошибка обработки заявки
update_mandatory_access_control_attribute_description	Обновление описания атрибутов уровней и категорий доступа	order_processing_error	Ошибка обработки заявки
upload_change_account_data	Загрузка изменений данных учетных записей	uploaded_usr	Заявка на загрузку пользователей исполнена
		order_processing_error	Ошибка обработки заявки
upload_change_organizations_state	Загрузка изменений состояний организаций	order_processing_error	Ошибка обработки заявки
upload_change_user_profile_data	Загрузка изменений данных профилей УЗ	uploaded_user_profile	Заявка на загрузку профилей учетных записей исполнена
		order_processing_error	Ошибка обработки заявки
upload_change_user_profile_positions	Загрузка изменений должностей профилей учетных записей	order_processing_error	Ошибка обработки заявки
upload_description_of_organization_dynamic_fields	Загрузка обновления настроек динамических полей организаций	order_processing_error	Ошибка обработки заявки
upload_description_of_user_dynamic_fields	Загрузка обновления настроек динамических полей УЗ	order_processing_error	Ошибка обработки заявки
upload_description_of_user_profile_dynamic_fields	Загрузка обновления настроек динамических полей профиля УЗ	order_processing_error	Ошибка обработки заявки
upload_dictionary	Загрузка справочника	order_processing_error	Ошибка обработки заявки
upload_info_system_applications	Загрузка приложения ИС	order_processing_error	Ошибка обработки заявки
upload_info_system_structure	Загрузка структуры ИС	change_info_system_structure	Изменение структуры ИС успешно завершено
		change_info_system_structure_not_complete	Изменение структуры ИС не выполнено
		order_processing_error	Ошибка обработки заявки
upload_info_system_structure_change	Загрузка изменений структуры ИС	change_info_system_structure	Изменение структуры ИС успешно завершено
		change_info_system_structure_not_complete	Изменение структуры ИС не выполнено
		order_processing_error	Ошибка обработки заявки
upload_info_systems	Загрузка ИС	order_processing_error	Ошибка обработки заявки
upload_organization	Загрузка организаций	uploaded_organization	Заявка на загрузку организаций исполнена
		order_processing_error	Ошибка обработки заявки
upload_organization_change	Загрузка изменений данных организации	uploaded_organization	Заявка на загрузку организаций исполнена

Техническое наименование типа заявки	Наименование типа заявки	Техническое наименование шаблона уведомления	Наименование шаблона уведомления/ Тема письма
		order_processing_error	Ошибка обработки заявки
upload_organization_dynamic_field_source	Загрузка источника динамических полей организаций	order_processing_error	Ошибка обработки заявки
upload_organizational_structure	Загрузка организационно-штатной структуры	order_processing_error	Ошибка обработки заявки
upload_role	Загрузка ролей и ЗО	upload_roles	Загрузка ролей в систему завершена
		order_processing_error	Ошибка обработки заявки
upload_change_role	Загрузка изменений ролей и ЗО	upload_roles	Загрузка ролей в систему завершена
		order_processing_error	Ошибка обработки заявки
upload_user_dynamic_field_source	Загрузка источника динамических полей УЗ	order_processing_error	Ошибка обработки заявки
upload_user_profile_dynamic_field_source_configuration	Загрузка конфигурации источника динамических полей профиля УЗ	order_processing_error	Ошибка обработки заявки
upload_user_profile_dynamic_field_source	Загрузка источника динамических полей профилей УЗ	order_processing_error	Ошибка обработки заявки
upload_user_profile_roles	Загрузка изменений ролей профилей учетных записей	uploaded_usr_profile_roles	Заявка на загрузку изменений ролей профилей учетных записей исполнена
		order_processing_error	Ошибка обработки заявки
upload_user_profile	Загрузка профилей учетных записей	uploaded_user_profile	Заявка на загрузку профилей учетных записей исполнена
		order_processing_error	Ошибка обработки заявки
upload_usr	Загрузка пользователей	uploaded_usr	Заявка на загрузку пользователей исполнена
		order_processing_error	Ошибка обработки заявки
user_profile_reg	Регистрация профиля учетной записи	email_confirmation	Подтверждение адреса электронной почты
		user_profile_registered	Регистрация профиля учетной записи успешно завершена
		order_cancel	Заявка отменена
		order_processing_error	Ошибка обработки заявки
usr_delete	Удаление учетной записи пользователя	delete_user	Удаление учетной записи пользователя
		delete_user_success	Заявка на удаление учетной записи исполнена
		order_processing_error	Ошибка обработки заявки
usr_reg	Регистрация пользователя	email_confirmation	Подтверждение адреса электронной почты
		created_order_to_registration_user	Создана заявка на регистрацию пользователя
		user_registration_rejected	Регистрация пользователя не выполнена
		account_activation	Создание учетной записи
		user_registered	Регистрация пользователя успешно завершена
		pend_approval_reg_usr	Требуется согласование заявки
		pend_confirmation_reg_usr	Требуется утверждение заявки
		order_processing_error	Ошибка обработки заявки
usr_synchronization	Синхронизация данных с каталогом	change_user_success	Данные учетной записи изменены
		usr_synchronization	Синхронизация данных с каталогом успешно завершена
		order_processing_error	Ошибка обработки заявки
—	—	user_inactive_block_notification	Приближение срока блокировки учетной записи по причине неактивности

Техническое наименование типа заявки	Наименование типа заявки	Техническое наименование шаблона уведомления	Наименование шаблона уведомления/ Тема письма
—	—	password_expired	Срок действия пароля истек
—	—	password_expires	Истечение срока действия пароля
—	—	two_factor_code_send	Подтверждение входа в ИС

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 возможности кастомизации
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
1.1.0	Добавлено ППО «Сервис работы с архивом заявок»: xidbox-order-archive-database, описание его установки и настройки
	Добавлено ППО «Сервис работы с БД внутренних уведомлений»: xidbox-internal-message-database, описание его установки и настройки
	Добавлено ППО «Сервис загрузки справочников»: xidbox-dictionary-upload, описание его установки и настройки
	Добавлено ППО «Сервис кеширования данных»: xidbox-cache, описание его установки и настройки
	В описании настроек сервисов дополнены настройки сервисов: xidbox-authentication, xidbox-role-politics-upload, xidbox-database, xidbox-backend, xidbox-frontbackend, xidbox-scheduler, xidbox-orchestrator, xidbox-order, xidbox-ldap, xidbox-request-background-processing, xidbox-directory-synchronization, опциональные настройки и настройки для всех сервисов;

Версия	Изменения
	добавлены настройки сервисов: xidbox-directory-synchronization, xidbox-order-archive-database, xidbox-internal-message-database, xidbox-organization, xidbox-user-upload и xidbox-user-profile-upload
	Обновлены дополнительные данные о событиях безопасности
	В разделы настройки ППО «Сервис аутентификации» и ППО «Сервис взаимодействия с пользовательским интерфейсом управления доступом» добавлено описание возможности изменения текстов серверных ошибок
	В описании функциональных возможностей X-IDBox и описании функциональной роли Администратора ИБ удалена возможность управления списком разрешённых удостоверяющих центров
	В описании функциональных ролей X-IDBox добавлена роль Главного менеджера учётных записей и изменены функциональные возможности роли Менеджера учётных записей
	Добавлено описание создания схем БД x_idbox_maintenance, archive_order и x_idbox_internal_message
	В раздел настройки ППО «Сервис выполнения автоматических расчетов» добавлено описание настройки логической репликации
	Дополнено описание обновления системы
	В раздел администрирования системы добавлено описание настройки параметров JVM
	В раздел администрирования системы добавлено описание создания настраиваемых функций для условий применимости ролей и политик авторизации
	Добавлено приложение с сопоставлением типов заявок и шаблонов уведомлений
	Дополнено описание к параметру post_logout_redirect_uri в разделе подключения ИС OAuth 2.0-клиента в X-IDBox
	В раздел «Управление сервисами ППО X-IDBox» добавлено описание возможности мониторинга состояния ППО X-IDBox
	Удалёна информация о кеш-сервере Redis
	Добавлено приложение со структурой данных в источнике поля/атрибута в X-IDBox и примером настройки «xidbox.authn.custom.headers.settings[*]»
	В описание состава комплекта дистрибутивов ПО X-IDBox добавлен дистрибутив DEB
	Добавлено описание требований к операционной системе «Astra Linux Special Edition»
	Добавлено описание установки и настройки СУБД PostgreSQL из состава дистрибутива ОС Astra Linux SE

Версия	Изменения
	В описание установки и настройки ППО «Сервис аутентификации» добавлен пункт с настройкой доменной аутентификации на стороне контроллера домена ALD Pro
	В описание установки и настройки адаптера к ППО «Сервис интеграции с LDAP-каталогами» добавлен пункт с созданием технической учётной записи в ALD Pro
	В разделе «Установка и настройка веб-сервера» дополнено описание установки и настройки веб-сервера Nginx и добавлено описание установки и настройки веб-сервера Apache2
	Добавлено описание резервного копирования и восстановления данных
	Добавлено описание настройки мониторинга системы
	В раздел «Администрирование системы» добавлено описание кастомизации атрибутов сессии
	В раздел «Подготовка конфигурационных файлов» добавлено описание подготовки файла конфигурации ППО «Сервис кеширования данных»
	В раздел настройки ППО «Пользовательский интерфейс управления доступом» добавлено описание возможности кастомизации
	В раздел настройки ППО «Пользовательский интерфейс аутентификации» добавлено описание возможности кастомизации текстов