

Программный комплекс «Ankey RBI»

Руководство администратора

Аннотация

Данный документ представляет собой руководство администратора для работы с программным комплексом (ПК) «Ankey RBI» (далее – ПК «Ankey RBI», комплекс). Руководство содержит сведения, необходимые администраторам для установки, настройки и эксплуатации ПК «Ankey RBI».

Руководство администратора содержит следующие разделы:

- 1) Раздел 1, в котором приведены назначение и функции ПК «Ankey RBI» и сведения о технических и программных средствах, обеспечивающих его выполнение.
- 2) Раздел 2, в котором приведено описание действий, которые необходимо предварительно выполнить перед установкой ПК «Ankey RBI».
- 3) Раздел 3, в котором приведено описание действий по установке ПК «Ankey RBI».
- 4) Раздел 4, в котором приведено описание действий по настройке параметров ПК «Ankey RBI».
- 5) Раздел 5, в котором приведено описание действий, которые необходимо выполнить для запуска ПК «Ankey RBI».
- 6) Раздел 6, в котором представлена информация о лицензировании ПК «Ankey RBI».
- 7) Раздел 7, в котором представлено описание веб-интерфейса ПК «Ankey RBI».
- 8) Раздел 8, в котором приведено описание обновления ПК «Ankey RBI».
- 9) Раздел 9, в котором приведены описание процесса удаления ПК «Ankey RBI».
- 10) Раздел 10, в котором приведена информация о резервном копировании и восстановлении данных ПК «Ankey RBI».
- 11) Раздел 11, в котором указаны тексты сообщений, выдаваемых в ходе выполнения настройки, проверки ПК «Ankey RBI», описание их содержания и действий, которые необходимо предпринять по этим сообщениям.

Содержание

1	Общие сведения о ПК «Ankey RBI»	6
1.1	Назначение ПК «Ankey RBI»	6
1.2	Структура ПК и принцип работы	6
1.3	Запуск изолированного приложения.....	8
1.3.1	Возможности пользователя при работе с изолированным приложением	8
1.4	Роли и аутентификация пользователей	8
1.4.1	Описание ролевой модели.....	8
1.4.2	Аутентификация пользователей.....	9
1.5	Функциональные возможности.....	10
1.6	Сведения о технических и программных средствах, необходимых для функционирования ПК «Ankey RBI»	11
1.6.1	Расчет минимального количества физических ядер центрального процессора.....	12
1.6.2	Расчет минимального количества оперативной памяти.....	13
1.6.3	Рекомендации по разбиению дисков для установки ПК «Ankey RBI»	14
1.7	Требования к сетевым взаимодействиям	15
1.8	Требования к пропускной способности сети	16
1.9	Требования к персоналу, обслуживающему ПК «Ankey RBI».....	16
1.10	Ограничения при функционировании ПК «Ankey RBI».....	16
2	Подготовка к установке ПК	17
2.1	Подготовка базы данных	17
2.1.1	Пример подготовки базы данных.....	18
2.2	Требования к файловому хранилищу.....	19
2.3	Подготовка службы каталогов FreeIPA или ALD Pro	19
2.3.1	Базовая настройка	19
2.3.2	Настройка службы KDC для поддержки аутентификации по протоколу Kerberos на прокси-сервере.....	19
2.4	Подготовка службы каталогов Microsoft AD DS	20
2.4.1	Базовая настройка для Microsoft AD DS	20
2.4.2	Настройка службы KDC для поддержки аутентификации по протоколу Kerberos на прокси-сервере для Microsoft AD DS	22
2.4.3	Настройка доверия в Microsoft AD DS	22
2.5	Подготовка службы каталогов Samba DC	24
2.5.1	Базовая настройка для Samba DC	25
2.5.2	Настройка службы KDC для поддержки аутентификации по протоколу Kerberos на прокси-сервере для Samba DC	25
2.6	Подготовка TLS-сертификатов.....	26
2.7	Подготовка сертификатов брокеров и узлов.....	26
3	Установка ПК.....	28
3.1	Установка брокера	28
3.2	Установка в режиме высокой доступности.....	29
3.2.1	Настройка высокой доступности.....	30
3.3	Установка клиента на АРМ пользователя	31
3.3.1	Установка клиента на АРМ пользователя под управлением РЕД ОС, Astra Linux или ALT Linux.....	32
3.3.2	Установка клиента на АРМ пользователя под управлением ОС Windows	34
3.3.3	Настройка возможности аутентификации в клиенте ПК «Ankey RBI» по	

	сертификатам, располагающимся на ключевом носителе.....	37
	3.3.4 Настройка возможности авторизации на порталах с поддержкой двухсторонней аутентификации.....	38
4	Настройка параметров комплекса.....	39
4.1	Группа настроек «Настройка HTTPS»	40
4.2	Группа настроек «Интеграция с LDAP»	41
4.3	Группа настроек «Сопоставление LDAP групп ролям RBl»	42
4.4	Группа настроек «Интеграция с Kerberos»	42
4.5	Группа настроек «Учетная запись локального администратора»	43
4.6	Настройки профиля по умолчанию.....	43
4.7	Группа настроек «Режим высокой доступности брокера»	43
4.8	Группа настроек «Аудит».....	43
4.9	Группа настроек «Интеграция с антивирусной программой»	44
4.10	Группа настроек «Оповещения о критических состояниях»	45
4.11	Группа настроек «Пользовательские файлы»	45
5	Настройка комплекса для запуска изолированных приложений	47
5.1	Добавление узла	47
5.2	Загрузка и установка файла с образом изолированного приложения	47
5.3	Настройка профиля контейнера по умолчанию.....	48
5.4	Назначение профиля контейнера УЗ пользователей и групп пользователей служб каталогов.....	48
5.5	Завершение работы с веб-интерфейсом	49
6	Лицензирование и активация ПК «Ankey RBl»	50
6.1	Активация лицензии комплекса	51
6.1.1	Особенности активации лицензии при использовании режима высокой доступности.....	51
6.1.2	Порядок действий при активации лицензии	51
6.2	Активация лицензии комплекса при подключении к сети Интернет через прокси-сервер	54
7	Функциональные возможности комплекса.....	55
7.1	Общее описание веб-интерфейса ПК «Ankey RBl».....	55
7.2	Управление узлами.....	58
7.2.1	Добавление узлов.....	60
7.2.2	Подготовка узла к использованию.....	61
7.2.3	Возможность запуска новых контейнеров на узле	62
7.2.4	Установка лицензию на право использования СКЗИ «КриптоПро CSP» на узел	62
7.3	Работа с файлами.....	63
7.3.1	Загрузка файлов	64
7.3.2	Установка образа изолированного приложения	65
7.4	Работа с образами	65
7.4.1	Автоматическое обновление образов с последующей автоматической установкой.....	67
7.4.2	Обновление образов при подключении к сети Интернет через прокси- сервер	67
7.5	Настройка профилей.....	67
7.5.1	Создание профиля.....	68
7.6	Управление привязкой УЗ пользователей или групп пользователей служб каталогов для привязки к профилям	72
7.6.1	Создание новой настройки.....	74
7.6.2	Редактирование и удаление настроек	75

7.6.3	Назначение нескольких профилей пользователю или группе	75
7.6.4	Назначение квот пользователю или группе	78
7.7	Управление сессиями пользователей	78
7.7.1	Отправка сообщения пользователю	80
7.7.2	Теневое подключение к сессиям пользователей	81
7.7.3	Завершение сессии пользователя	81
7.8	Просмотр журнала системных событий	82
7.9	Просмотр информации о брокерах	83
7.10	Использование плагинов для работы с криптографическими ключами и электронной подписью	84
7.10.1	Настройка ПК «Ankey RBI» для работы с плагинами	85
8	Обновление программы	86
8.1	Обновление брокера и узлов	86
8.2	Обновление клиента	86
8.2.1	Обновление клиента на РЕД ОС, Astra Linux или ALT Linux	86
8.2.2	Обновление клиента на Windows 10/11	87
9	Удаление программы	88
9.1	Удаление ПК «Ankey RBI» с сервера	88
9.2	Удаление ПК «Ankey RBI» с узлов	88
9.3	Удаление ПК «Ankey RBI» с АРМ пользователя	88
10	Резервное копирование и восстановление данных	89
10.1	Резервное копирование данных	89
10.2	Восстановление данных из резервной копии	89
11	Обслуживание и решение проблем	90
11.1	Ошибки при попытке получения доступа к веб-интерфейсу	90
11.2	При попытке доступа к веб-интерфейсу не появляется возможность доменной аутентификации	90
11.3	В веб-интерфейсе отображается некорректный список разделов меню	91
11.4	Узел находится в режиме Офлайн	91
11.5	Не добавляется узел	92
11.6	При настройке групп LDAP не отображаются списки доступных групп	92
11.7	При попытке запуска изолированного приложения появляется ошибка сертификата	92
11.8	При попытке запуска изолированного приложения появляется ошибка запуска сессии	92
11.9	При попытке ввода валидного значения ключа лицензии появляется нелокализованная ошибка	93
11.10	Не работают «Настройки пользователя» после смены имени УЗ пользователя на контроллере домена	93
11.11	Ошибка использования алгоритмов шифрования KDC	94
11.12	Ошибка выполнения аутентификации кеша протокола Kerberos	94
11.13	Ошибка при загрузке образа	95
11.14	Как настроить инспектирование SSL	95
11.15	Ошибка подключения RBI-брокера к LDAPS	95
11.16	Работа с продуктовыми метриками	96
11.16.1	Продуктовые метрики	96
11.16.2	Настройка ZABBIX для отображения метрик	98
11.16.3	Настройка сервисов Prometheus и Grafana для отображения метрик	101
	Перечень сокращений	104
	Перечень терминов и определений	105
	Приложение 1	106

1 Общие сведения о ПК «Ankey RBI»

1.1 Назначение ПК «Ankey RBI»

ПК «Ankey RBI» является специализированным программным комплексом (ПК), который с помощью защищенной изолированной среды обеспечивает безопасный доступ к сети Интернет для пользователей.

ПК «Ankey RBI» предназначен для:

- реализации безопасного доступа пользователей в сеть Интернет;
- обеспечения защиты информационных ресурсов предприятия;
- обеспечения централизованного управления доступом к ресурсам в сети Интернет.

1.2 Структура ПК и принцип работы

ПК «Ankey RBI» представляет собой сервер для создания изолированной среды для каждого отдельного пользователя, а также специальный веб-интерфейс с возможностью конфигурирования параметров отдельных контейнеров.

Ниже представлена функциональная схема ПК «Ankey RBI» (рис. 1).

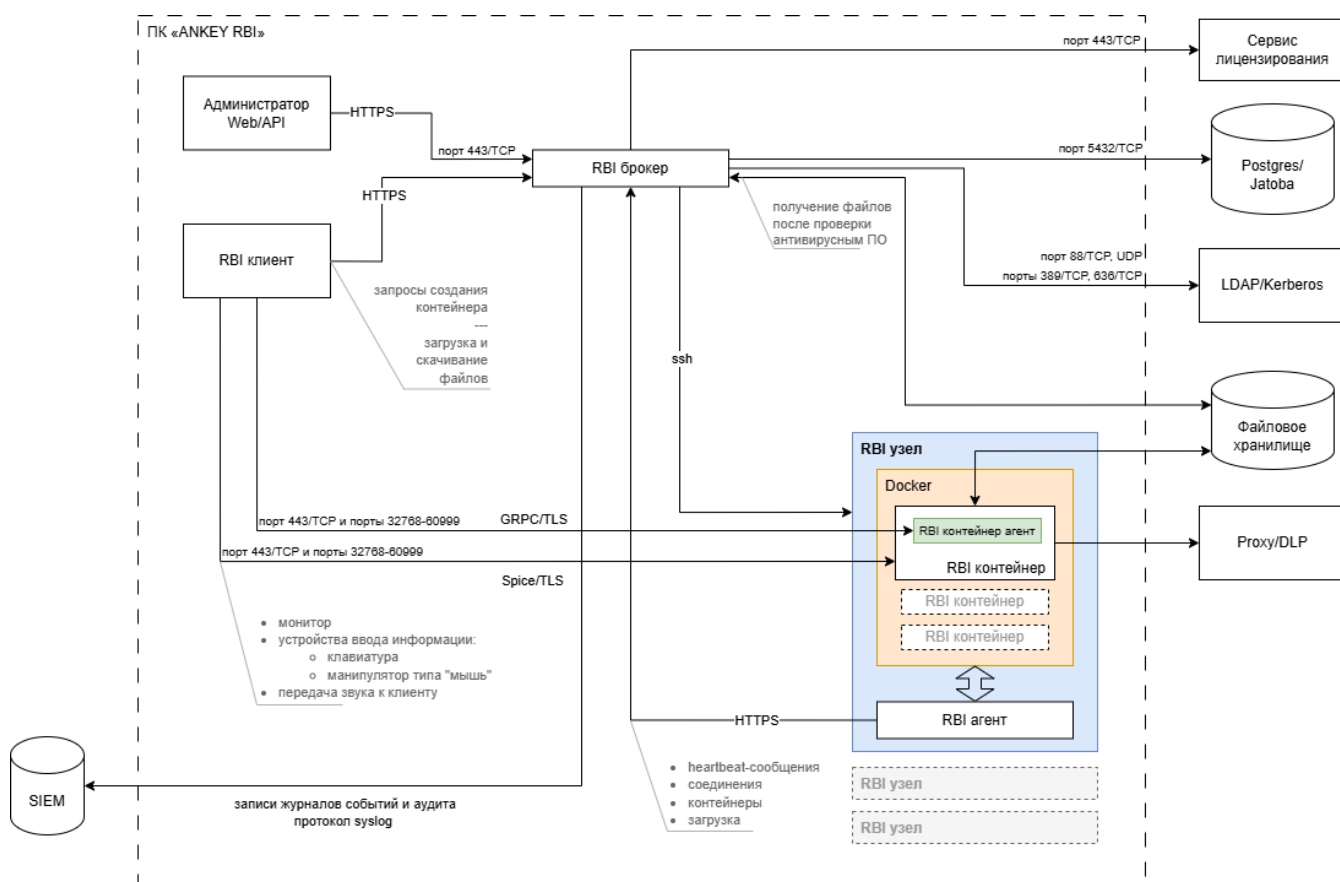


Рисунок 1 – Функциональная схема ПК «Ankey RBI»

Для каждого пользователя на сервере ПК «Ankey RBI» запускается отдельный экземпляр браузера в изолированном программном окружении (контейнере).

ПК «Ankey RBI» состоит из следующих частей:

- брокер – сервис для управления Docker-контейнерами и подключениями клиентских приложений к контейнерам. На брокере реализован веб-интерфейс программного комплекса;
- агент – сервис, который управляет запущенными контейнерами на узле и отправляет на брокер необходимую информацию об узле и контейнерах;
- узел – сервер (или виртуальная машина) под управлением операционной системы (ОС) РЕД ОС, на котором фактически работают контейнеры с изолированными приложениями (браузерами). На узле установлены и работают Docker и агент;
- образ – Docker-образ, содержащий в себе всю необходимую программную среду для создания и запуска изолированного приложения, а также необходимый для работы клиентского приложения;
- агент контейнера – компонент, необходимый для работы клиентского приложения, который работает в каждом из контейнеров с запущенным изолированным приложением;
- контейнер – экземпляр образа;
- клиентское приложение (далее – клиент) – программа, установленная на автоматизированном рабочем месте (АРМ) пользователя, которая обеспечивает взаимодействие пользователя с изолированным приложением.

Компоненты, необходимые для работы ПК «Ankey RBI»:

- Jatoba/PostgreSQL – СУБД, в которой брокер сохраняет необходимые для работы данные (кроме файлов и образов): информация об узлах, информация о брокерах, состояние запущенных сессий и системные настройки;
- место хранения данных – свободное пространство на носителе информации (локальном или сетевом) для хранения файлов пользователей и образов контейнеров. Поддерживается работа с носителем данным, подключенным с использованием протоколов Fibre Channel (FC), Internet Small Computer System Interface (iSCSI) или Serial ATA (SATA). Файлы пользователей, скачанные при работе с клиентом ПК «Ankey RBI», размещаются в хранилище файлов, после чего пользователь может скачать файл на свое АРМ с использованием веб-интерфейса ПК «Ankey RBI». Аналогично происходит загрузка файлов;
- служба каталогов, доступная по протоколу LDAP – для работы ПК «Ankey RBI» необходимо наличие одной из следующих служб каталогов: FreeIPA, Microsoft Active Directory Domain Services (Microsoft AD DS), Samba DC;
- служба Key Distribution Center, доступная по протоколу Kerberos;
- прокси-сервер с поддержкой аутентификации с использованием протокола Kerberos (опционально).

1.3 Запуск изолированного приложения

Порядок взаимодействия между клиентом ПК «Ankey RBI» и серверной частью (брокер, агент, узел) ПК «Ankey RBI» при запуске изолированного приложения приведен ниже:

- 1) Пользователь запускает клиент ПК «Ankey RBI».
- 2) Брокер производит процедуру аутентификации УЗ пользователя АРМ на брокере с использованием прокола Kerberos.
- 3) Клиент отправляет HTTPS-запрос брокеру для запуска контейнера.
- 4) Брокер производит авторизацию пользователя в соответствии с ролевой моделью.
- 5) Брокер с помощью протокола SSH создает контейнер на узле с наименьшей загрузкой.
- 6) Клиент запускает утилиту Remote Viewer, работающую по протоколу SPICE-TLS, которая осуществляет подключение к контейнеру на узле с приложением по набору уникальных реквизитов: адрес узла, порт, пароль. В результате на АРМ пользователя отображается изолированное приложение (веб-браузер), с которым пользователь может взаимодействовать, как при работе с обычным веб-браузером.

1.3.1 Возможности пользователя при работе с изолированным приложением

Для каждого пользователя обеспечена возможность сохранения в отдельном хранилище и последующее восстановление ограниченного набора настроек браузера:

- история посещения веб-ресурсов;
- закладки;
- настройки браузера;
- сохраненные пароли.

Между контейнером и АРМ пользователя происходит двусторонний обмен информацией, при этом:

- отображается окно изолированного приложения (браузера);
- обеспечивается обмен данными через буфер обмена;
- обеспечивается синхронизация с раскладкой клавиатуры на АРМ пользователя;
- воспроизводится аудио- и видеoinформация в браузере (от контейнера к клиенту);
- передаются действия пользователя с манипулятором типа «мышь» и клавиатурой при работе с изолированным приложением.

1.4 Роли и аутентификация пользователей

1.4.1 Описание ролевой модели

В ПК «Ankey RBI» реализована ролевая модель разграничения доступа. Группам пользователей назначаются права доступа в соответствии с их группой безопасности в службе каталога. Для разграничения доступа авторизованных пользователей к функциональным возможностям в ПК «Ankey RBI» предусмотрены следующие роли:

- 1) Администратор – роль с полным доступом, имеет доступ к функциям настройки и администрирования комплекса.
- 2) Аудитор – роль, имеющая ограниченный доступ к веб-интерфейсу и журналу событий безопасности.
- 3) Пользователь – роль для доступа к изолированному приложению.

В таблице 1 представлено сопоставление ролей ПК «Ankey RBI» их функциональным возможностям, доступным в веб-интерфейсе.

Таблица 1 – Сопоставление ролей ПК «Ankey RBI» их функциональным возможностям веб-интерфейса

Название раздела веб-интерфейса	Администратор	Аудитор	Пользователь
Лицензия и техподдержка	Полный доступ к разделу	Нет доступа	Нет доступа
Мои файлы	Полный доступ к разделу	Ограниченный доступ к разделу: загрузка и скачивание файлов	Ограниченный доступ к разделу: загрузка и скачивание файлов
Сессии пользователей	Полный доступ к разделу	Ограниченный доступ к разделу: просмотр списка своих активных сессий и возможность их закрытия	Ограниченный доступ к разделу: просмотр списка своих активных сессий и возможность их закрытия
Настройки пользователей	Полный доступ к разделу	Нет доступа	Нет доступа
Настройки групп	Полный доступ к разделу	Нет доступа	Нет доступа
Профили	Полный доступ к разделу	Нет доступа	Нет доступа
Образы	Полный доступ к разделу	Нет доступа	Нет доступа
Узлы	Полный доступ к разделу	Нет доступа	Нет доступа
Брокеры	Полный доступ к разделу	Нет доступа	Нет доступа
Аудит	Полный доступ к разделу	Полный доступ к разделу	Нет доступа
Настройки системы	Полный доступ к разделу	Нет доступа	Нет доступа

1.4.2 Аутентификация пользователей

Предусматривается два способа аутентификации пользователей с ролью «Администратор»:

- с помощью встроенной локальной учетной записи (УЗ) администратора комплекса;
- с использованием протокола Kerberos.

Примечание. Встроенная локальная УЗ администратора используется для первоначальной настройки комплекса или при работе в аварийных ситуациях.

После аутентификации пользователя по протоколу Kerberos брокер определяет роль пользователя по его принадлежности к группам безопасности в службе каталога, определенных в настройках системы.

1.5 Функциональные возможности

В ПК «Ankey RBI» реализованы следующие функциональные возможности:

- централизованное управление изолированными приложениями (браузерами);
- подключение клиента к индивидуальным экземплярам изолированного приложения;
- аутентификация УЗ пользователей по протоколу Kerberos (в службах каталогов FreeIPA, Microsoft AD DS и Samba DC) для доступа к изолированным браузерам;
- доменная и локальная аутентификация для доступа к веб-интерфейсу ПК «Ankey RBI»;
- поддержка установки корневых сертификатов в изолированном приложении;
- аутентификация по протоколу Kerberos на прокси-сервере;
- передача звука и видео из изолированного приложения на АРМ пользователя;
- передача звука с микрофона, подключенного к АРМ пользователя, в изолированное приложение;
- синхронизация с раскладкой клавиатуры на АРМ пользователя;
- передача буфера обмена как из изолированного приложения, так и с АРМ пользователя;
- интеграция с антивирусным ПО для проверки скачанных файлов;
- аутентификация в клиенте ПК «Ankey RBI» по сертификатам, располагающимся на ключевом носителе (смарт-карте);
- поддержка плагинов для работы с носителями криптографических ключей и электронной подписью в изолированном приложении.

Единый пользовательский веб-интерфейс ПК «Ankey RBI» предоставляет доступ пользователям к следующим функциональным возможностям:

- управление общими настройками ПК «Ankey RBI»;
- работа с файлами;
- работа с образами;
- управление узлами;
- управление профилями (настройками изолированного приложения);
- привязка пользователей службы каталогов к профилям;
- привязка групп служб каталога к профилям;
- управление сессиями пользователей;

- мониторинг вычислительных ресурсов, используемых комплексом;
- просмотр журнала системных событий и событий безопасности;
- экспорт журналов событий в формате CSV.

1.6 Сведения о технических и программных средствах, необходимых для функционирования ПК «Ankey RBI»

Минимальные технические параметры, которые должен иметь сервер для установки ПК «Ankey RBI» без поддержки конфигураций высокой доступности:

- количество физических ядер процессора: минимальное количество требуемых процессорных ядер рассчитывается на основе формул, приведенных в пункте 1.6.1 данного руководства;
- оперативная память: минимальное количество требуемой оперативной памяти рассчитывается на основе формул, приведенных в пункте 1.6.2 данного руководства;
- дисковое пространство: рекомендации по разбиению дисков для установки ПК «Ankey RBI» приведены в пункте 1.6.3 данного руководства;
- сетевой адаптер узла: подбирается из расчета количество пользователей. Для этого требуется количество пользователей ПК «Ankey RBI» умножить на необходимую скорость на необходимую скорость на одного пользователя, исходя из планируемого режима работы. Требования к пропускной способности сети в соответствии с режимами работы пользователя представлены в подразделе 1.9 данного руководства.

Установка серверной части ПК «Ankey RBI» должна осуществляться на серверы, функционирующие под управлением операционной системы РЕД ОС версии 7.3 (64 бит), сертификат соответствия № 4060 (выдан ФСТЭК России 12 января 2019 г.) или РЕД ОС версии 8 (64 бит).

Установка клиентской части ПК «Ankey RBI» должна осуществляться на АРМ, функционирующие под управлением одной из следующих операционных систем:

- Astra Linux Special Edition версии 1.7 (64 бит), сертификат соответствия № 2557 (выдан ФСТЭК России 27 января 2012 г.);
- ОС «Альт Рабочая станция» версии 10.2 или 10.4 (далее – ALT Linux);
- РЕД ОС версии 7.3 (64 бит), сертификат соответствия № 4060 (выдан ФСТЭК России 12 января 2019 г.);
- РЕД ОС версии 8 (64 бит);
- Microsoft Windows 10 (32 бит/64 бит);
- Microsoft Windows 11 (32 бит/64 бит).

Веб-интерфейс программного комплекса поддерживает работу со следующими браузерами:

- «Google Chrome» версии 132.0.6834.110/111 и выше;
- «Chromium» версии 132.0.6834.110/111 и выше;
- «Яндекс Браузер» версии 24.10.4.753 и выше.

Для эксплуатации и эффективного применения ПК «Ankey RBI» необходимо использовать лицензионное системное программное обеспечение.

Данные ПК «Ankey RBI» должны храниться во внешней СУБД. В качестве внешней СУБД поддерживаются:

- PostgreSQL 14 и выше;
- «Защищенная система управления базами данных (БД) «Jatoba», сертификат соответствия № 4327 (выдан ФСТЭК России 19 ноября 2020 г.).

СУБД может быть установлена локально на сервере комплекса или на удаленном сервере, таким образом, чтобы порт сервера БД был доступен брокеру. Для обеспечения высокой доступности СУБД должна быть:

- установлена на нескольких серверах;
- настроена в кластерном режиме active/passive или active/active.

Внимание! При установке СУБД без кластерного режима работы, высокая доступность ПК «Ankey RBI» не гарантирована.

Требования к файловому хранилищу представлены в подразделе 2.2 данного руководства.

1.6.1 Расчет минимального количества физических ядер центрального процессора

Для корректного функционирования ПК «Ankey RBI» необходимо рассчитать минимальное количество требуемых физических ядер центрального процессора (с учетом Hyper-Threading).

При проведении расчетов необходимо учитывать реализованную в системе «Ankey RBI» возможность назначения пользователю или группе пользователей нескольких профилей, предназначенных для запуска изолированных приложений с индивидуальными настройками.

Каждый экземпляр приложения, запускаемый в контексте отдельного профиля пользователя или группы, требует выделения дополнительных ресурсов и должен быть учтен при расчете минимального количества физических ядер центрального процессора.

Ниже представлена формула для расчета количества физических ядер центрального процессора:

$$N_{sum} = \frac{N_{exp} \times K_{и} \times (N_{cscu} + N_{дс})}{K_H} \quad (1)$$

где:

- N_{sum} – расчетное количество физических ядер центрального процессора, шт.;
- N_{exp} – количество потоков. Рекомендуемое значение параметра: 0,5;
- $K_{и}$ – коэффициент использования. Рекомендуется использовать значение параметра в диапазоне от 0,1 до 1;

- K_n – коэффициент нелинейности. Рекомендуемое значение параметра: 1,5;
- N_{ccu} – количество конкурентных пользователей (Concurrent user – CCU);
- N_{dc} – количество дополнительных сессий изолированного приложения. Параметр является необязательным и зависит от использования дополнительных профилей.

При получении дробного результата значение должно быть округлено до ближайшего целого в большую сторону.

Примечание. Значение коэффициента использования K_n может изменяться в случае отклонения профиля нагрузки от среднестатистического.

Пример расчета необходимого количества физических ядер центрального процессора для 150 пользователей (для расчета используется K_n со значением 1 и без дополнительных сессий):

$$N_{sum} = \frac{0,5 \times 1 \times 150}{1,5} = 50 \text{ шт.}$$

Пример расчета необходимого количества физических ядер центрального процессора для 150 пользователей с одним профилем и 5 пользователей, имеющих по 2 профиля, каждый из которых позволяет запустить дополнительный экземпляр изолированного приложения (всего 10 дополнительных сессий) (для расчета используется K_n со значением 1):

$$N_{sum} = \frac{0,5 \times 1 \times 150 + 10}{1,5} = 53,3. \text{ Округляем до 54 шт.}$$

1.6.2 Расчет минимального количества оперативной памяти

Для корректного функционирования ПК «Ankey RBI» необходимо рассчитать минимальное количество требуемой оперативной памяти.

При проведении расчетов необходимо учитывать реализованную в системе «Ankey RBI» возможность назначения пользователю или группе пользователей нескольких профилей, предназначенных для запуска изолированных приложений с индивидуальными настройками.

Для каждого экземпляра приложения, запускаемого в контексте отдельного профиля пользователя или группы, должен быть выделен дополнительный объем оперативной памяти.

Ниже представлена формула для расчета количества оперативной памяти:

$$V_{sum} = V_{exp} \times K_{tmp} \times K_{buf} \times K_{tab} \times (N_{ccu} + N_{dc}), \quad (2)$$

где:

- V_{sum} – расчетный объем оперативной памяти, Гб;
- V_{exp} – объем требуемой памяти для одного контейнера, Гб. Рекомендуемое значение параметра: 0,75;
- K_{tmp} – коэффициент памяти под временные файлы. Рекомендуемое значение параметра: 1,2;

- K_{buf} – коэффициент памяти под системные буферы. Рекомендуемое значение параметра: 1,2;
- K_{tab} – коэффициент использования вкладок. Рекомендуемое значение параметра: 1,5.
- N_{ccu} – количество конкурентных пользователей;
- N_{dc} – количество дополнительных сессий изолированного приложения. Параметр является необязательным и зависит от использования дополнительных профилей.

Примечание. В случае отклонения профиля нагрузки от среднестатистического, коэффициенты могут измениться.

Пример расчета необходимого объема оперативной памяти для 150 пользователей (без дополнительных сессий):

$$V_{sum} = 0,75 \times 1,2 \times 1,2 \times 1,5 \times 150 = 243 \text{ Гб}$$

Пример расчета необходимого объема оперативной памяти для 150 пользователей с одним профилем и 5 пользователей, имеющих по 2 профиля, каждый из которых позволяет запустить дополнительный экземпляр изолированного приложения (всего 10 дополнительных экземпляров):

$$V_{sum} = 0,75 \times 1,2 \times 1,2 \times 1,5 \times (150 + 10) = 259,2 \text{ Гб}$$

1.6.3 Рекомендации по разбиению дисков для установки ПК «Ankey RBI»

В таблице 2 представлены рекомендации по разбиению дисков в операционной системе РЕД ОС для установки ПК «Ankey RBI», а в таблице 3 – рекомендации по разбиению дисков для установки выделенных узлов.

Таблица 2 – Рекомендации по разбиению дисков для установки ПК «Ankey RBI»

Точка монтирования	Рекомендация по объему	Примечание
/root (корневой раздел)	от 50 Гб	–
/mnt/rbi	60% от имеющегося свободного дискового пространства	Место для хранения файлов
/var/lib/pgsql или /var/lib/jatoba	от 100 Гб	Данный раздел необходим только в случае, если на сервере, на котором будет установлен ПК «Ankey RBI», также будет установлен сервер СУБД
/var	от 50 Гб	Журналы событий и другие изменяемые данные
/var/lib/docker	30% от имеющегося свободного дискового пространства	Рабочий каталог Docker

Примечание. Контейнер с одной пользовательской сессией занимает на дисковом пространстве около 250 Мбайт. Очистка дискового пространства от данных контейнеров, завершивших свою работу, происходит раз в сутки.

Таблица 3 – Рекомендации по разбиению дисков для установки выделенных узлов ПК «Ankey RBl»

Точка монтирования	Рекомендация по объему	Примечание
/root (корневой раздел)	от 50 Гб	–
/var	от 50 Гб	Журналы событий и другие изменяемые данные
/var/lib/docker	30% от имеющегося свободного дискового пространства	Рабочий каталог Docker

1.7 Требования к сетевым взаимодействиям

Для корректной работы ПК «Ankey RBl» необходимо выполнить настройку сетевых взаимодействий на межсетевых экранах:

- Исходящие взаимодействия из подсети, в которой установлен «Ankey RBl» до:
 - службы KDC контролера домена – порт 88/TCP, UDP;
 - сервера каталогов, работающего по протоколу LDAP/LDAPS – порты 389/TCP, 636/TCP;
 - сервера СУБД Jatoba/PostgreSQL – порт 5432/TCP;
 - сервиса лицензирования – порт 443/TCP на хост license.gaz-is.ru
 - сервисов обновлений – порт 443/TCP на хосты <https://license-token.gaz-is.ru> и <https://update.gaz-is.ru>.
- Входящие взаимодействия в подсеть, в которой установлен ПК «Ankey RBl» из:
 - сетей, где расположены APM, имеющие доступ к веб-интерфейсу – порт 443/TCP;
 - сетей, где расположены APM, на которых установлены клиенты - порт 443/TCP и порты 32768-60999 для подключения к выделенному контейнеру по протоколу SPICE-TLS+GRPC-TLS.

Сетевые взаимодействия отображены на функциональной схеме ПК «Ankey RBl» (см. рис. 1).

Если требуется изменить диапазон портов SPICE-TLS+GRPC-TLS по умолчанию, то следует изменить настройку «net.ipv4.ip_local_port_range» на всех узлах ПК. Для этого необходимо выполнить следующую команду:

```
sudo sysctl -w net.ipv4.ip_local_port_range = "1024 65535"
```

Для просмотра значения настройки «net.ipv4.ip_local_port_range» необходимо ввести команду в консоли каждого узла:

```
sysctl net.ipv4.ip_local_port_range
```

1.8 Требования к пропускной способности сети

Для корректной работы ПК «Ankey RBI» необходимо обеспечить следующую пропускную способность локальной вычислительной сети в соответствии представленными ниже режимами работы:

- офисный режим: работа в браузере с текстовой информацией, не предусматривающая просмотр/прослушивание видео и аудио контента – 5 Мбит/с;
- офисный режим с элементами мультимедиа: работа в данном режиме подразумевает использование веб-страниц с различными медиаформатами (текст, аудио, видео, графика и анимация) – 30 Мбит/с;
- просмотр видео в формате до 1/2 экрана – 60 Мбит/с.

1.9 Требования к персоналу, обслуживающему ПК «Ankey RBI»

Администратор, обслуживающий ПК «Ankey RBI», должен иметь:

- базовые знания операционных систем Unix/Linux, Windows;
- опыт администрирования баз данных PostgreSQL, Jatoba;
- базовые знания скриптовых языков (Powershell/Bash);
- базовые знания высокодоступных и сетевых файловых систем (OCFS2, NFS);
- базовые знания работы со службами каталогов.

1.10 Ограничения при функционировании ПК «Ankey RBI»

При работе с ПК «Ankey RBI» необходимо учитывать следующие ограничения разрешения монитора на АРМ пользователя:

- не менее 800х600;
- не более 2560х1600.

Важно: для корректной работы браузера в полноэкранном режиме изолированного приложения необходимо использовать разрешения экрана в пределах установленного диапазона. Использование разрешений за пределами этого диапазона может привести к неработоспособности функции масштабирования окна браузера внутри клиентского приложения.

2 Подготовка к установке ПК

ПК «Ankey RBI» поставляется заказчику на компакт-диске согласно комплектности, указанной в документе «Программный комплекс «Ankey RBI». Формуляр» или путем предоставления ссылки для скачивания дистрибутива.

Для обеспечения защиты ПК «Ankey RBI» от угроз безопасности информации, связанных с нарушением целостности в процессе передачи его пользователю, необходимо обеспечить контроль соответствия экземпляра ПК «Ankey RBI», переданного разработчиком, и экземпляра ПК «Ankey RBI», полученного пользователем.

Контроль соответствия на месте эксплуатации ПК «Ankey RBI» осуществляется путем сверки контрольных сумм дистрибутива со значениями, указанными в документе «Программный комплекс «Ankey RBI». Формуляр».

Установка ПК должна осуществляться под руководством специально подготовленного персонала. Требования к персоналу, обслуживающему ПК «Ankey RBI» указаны в подразделе 1.9 настоящего руководства.

Перед установкой ПК требуется обеспечить выделение в необходимом количестве IP-адресов для брокеров, узлов, а также кластерного IP-адреса в соответствии с требованиями предприятия, для которой предоставляется ПК «Ankey RBI».

В случае возникновения проблем технического характера необходимо обратиться в службу технической поддержки. Контакты технической поддержки указаны в документе «Программный комплекс «Ankey RBI». Формуляр».

2.1 Подготовка базы данных

Требования к внешней СУБД представлены в подразделе 1.10 данного руководства. В данном руководстве описано использование PostgreSQL в качестве внешней СУБД. Допускается использование других СУБД, поддерживаемых ПК «Ankey RBI».

Важно! Для подготовки базы данных рекомендуется ознакомиться с официальной документацией по установке СУБД от вендора. Информация о СУБД Jatoba представлена на официальном сайте – URL: <https://jatoba.ru/> (дата обращения: 15.11.2024).

Для подготовки СУБД требуется выполнить следующие действия:

- 1) Убедиться, что сетевые настройки позволяют серверам, на которых планируется установить брокеры, получать доступ к СУБД.
- 2) Создать БД для ПК «Ankey RBI», выполнив команду в консоли сервера:

```
sudo -u postgres createdb <имя базы данных>
```

- 3) Создать УЗ пользователя для БД ПК «Ankey RBI», выполнив команду в консоли сервера:

```
sudo -u postgres createuser <имя пользователя>
```

- 4) Задать пароль УЗ пользователя, выполнив команду в консоли сервера:

```
sudo -u postgres alter user <имя пользователя> with encrypted password '<пароль>'
```

- 5) Выдать все привилегии для пользователя БД на БД ПК «Ankey RBI» (за исключением привилегии GRANT), выполнив команду в консоли сервера:

```
sudo -u postgres grant all privileges on database <имя базы данных> to <имя пользователя>
```

- 6) Добавить разрешение на доступ к БД для пользователя ПК «Ankey RBI» со всех IP-адресов брокеров в конфигурационном файле «pg_hba.conf». Расположение файла зависит от используемой версии SQL-сервера. Если используется PostgreSQL, то файл будет иметь следующее расположение: /var/lib/pgsql/<версия>/data.

Например: /var/lib/pgsql/15/data/pg_hba.conf. Пример установки разрешений представлен в пункте 2.1.1 данного руководства.

- 7) Настроить СУБД для обслуживания сетевых запросов на всех доступных сетевых интерфейсах (см. подраздел 1.7 данного руководства).

2.1.1 Пример подготовки базы данных

Ниже представлен пример последовательности команд для подготовки БД ПК «Ankey RBI» – создание БД, создание пользователя и назначение привилегий.

Все команды выполняются в консоли РЕД ОС от имени пользователя PostgreSQL:

```
sudo su - postgres
psql
CREATE DATABASE DARBI LC_COLLATE \'ru_RU.utf8\' LC_CTYPE \'ru_RU.utf8\'
TEMPLATE template0;
CREATE USER darbi WITH PASSWORD \'Password\*123\';
GRANT ALL PRIVILEGES ON DATABASE DARBI TO darbi;
```

Примечание. В представленном примере пользователю предоставляется полный набор разрешений на доступ к БД. Для предоставления только необходимых разрешений рекомендуется ознакомиться с документацией к используемой СУБД. Список поддерживаемых СУБД представлен в подразделе 1.7 данного руководства.

С целью предоставления IP-адресам брокера возможности доступа к БД необходимо открыть конфигурационный файл «pg_hba.conf», выполнив команду:

```
nano /var/lib/pgsql/15/data/pg_hba.conf
```

Внести следующие изменения в открывшемся конфигурационном файле:

```
host all all 0.0.0.0/0 md5
```

Далее необходимо открыть конфигурационный файл «postgresql.conf», выполнив команду:

```
nano /var/lib/pgsql/15/data/postgresql.conf
```

Внести следующие изменения в открывшемся конфигурационном файле:

```
listen_addresses = '*'
```

2.2 Требования к файловому хранилищу

Брокеры и узлы должны иметь совместный доступ к файловому хранилищу для хранения данных пользователей и образов изолированных приложений. Файловое хранилище должно быть смонтировано в каталог /mnt/rbi на всех серверах, которые планируется использовать в качестве узлов и на которых планируется устанавливать брокеры.

Доступ к совместному файловому хранилищу осуществляется с использованием сетевой файловой системы Network File System (NFS).

Физическое хранение файлов на файловом хранилище рекомендуется организовать в высокодоступном режиме с использованием систем хранения данных (СХД), NAS или файловых систем OCFS2 over DRBD, GlusterFS.

2.3 Подготовка службы каталогов FreeIPA или ALD Pro

ПК «Ankey RBI» не имеет собственной базы пользователей и групп. ПК «Ankey RBI» производит аутентификацию/авторизацию пользователей с помощью сервисов, которые предоставляет домен.

Описание параметров, используемых в пунктах 2.3.1 и 2.3.2, представлено в Приложении 1.

2.3.1 Базовая настройка

Для настройки интеграции с FreeIPA или ALD Pro необходимо выполнить следующие действия в консоли контроллера домена:

- 1) Создать DNS запись для брокера:

```
ipa dnsrecord-add <доменное имя> <имя брокера> --a-rec=<кластерный IP-адрес>
```

- 2) Создать запись типа ipaservice для брокера:

```
ipa host-add <имя брокера>.<доменное имя>
```

- 3) Создать записи типа ipahosts для каждого брокера:

```
ipa service-add <SPN для брокера>
```

- 4) Создать DNS записи для каждого из узлов:

```
ipa dnsrecord-add <доменное имя> <имя первого узла> --a-rec=<IP-адрес первого брокера>
ipa dnsrecord-add <доменное имя> <имя второго узла> --a-rec=<IP-адрес первого брокера>
```

- 5) Сформировать keytab-файл для УЗ ipaservice брокера:

```
ipa-getkeytab -p <SPN для брокера> -k
<имя брокера>.<доменное имя>.keytab
```

- 6) Сохранить полученный keytab-файл на APM администратора.

2.3.2 Настройка службы KDC для поддержки аутентификации по протоколу Kerberos на прокси-сервере

Сервис «Ankey RBI» позволяет получить Kerberos билет для доступа к сервису (Ticket-Granting Service (TGS)) от имени УЗ пользователя для прокси-сервера с Kerberos

аутентификацией. Для настройки этой возможности необходимо выполнить следующие действия в консоли контроллера домена FreeIPA:

- 1) Создать объект `servicedelegationrule`:

```
ipa servicedelegationrule-add <имя правила>
```

- 2) Создать объект `servicedelegationtarget`:

```
ipa servicedelegationtarget-add <имя правила для делегирования>
```

- 3) Добавить DNS запись для брокера, созданную на первом шаге пункта 2.3.1 в `servicedelegationrule`, созданный на первом шаге пункта 2.3.2:

```
ipa servicedelegationrule-add-member --principals <имя домена> <имя правила>
```

- 4) Добавить запись `ipaservice`, созданную на втором шаге пункта 2.3.1 в `servicedelegationtarget`, созданный на втором шаге пункта 2.3.2:

```
ipa servicedelegationtarget-add-member --principals=<SPN для прокси сервера> <имя правила для делегирования>
```

- 5) Добавить `ipaservice` прокси-сервера в `servicedelegationtarget`, созданный на втором шаге пункта 2.3.2:

```
ipa servicedelegationrule-add-target --servicedelegationtargets=<имя правила для делегирования> <имя правила>
```

Примечание. Предполагается, что прокси-сервер уже существует и запись `ipaservice` для сервера создана.

2.4 Подготовка службы каталогов Microsoft AD DS

ПК «Ankey RBI» не имеет собственной базы пользователей и групп. ПК «Ankey RBI» производит аутентификацию/авторизацию пользователей с помощью сервисов, которые предоставляет домен. Для настройки интеграции необходимо выполнить действия, приведенные ниже.

Примечания. Все перечисленные ниже команды выполняются на контроллере домена с правами доменного администратора в PowerShell.

Описание параметров, используемых в пунктах 2.4.1 и 2.4.2, представлено в Приложении 1.

2.4.1 Базовая настройка для Microsoft AD DS

Необходимо создать DNS запись типа «А» для брокера с помощью команды:

```
Add-DnsServerResourceRecordA -Name <имя брокера> -IPv4Address <кластерный IP-адрес> -ZoneName <имя домена> -CreatePtr
```

Пример выполнения команды:

```
Add-DnsServerResourceRecordA -Name rbi-server -IPv4Address 10.116.174.25 -ZoneName example.ru -CreatePtr
```

Примечание. При установке единственного экземпляра брокера без поддержки высокой доступности указывается IP-адрес данного брокера. Если брокер устанавливается в режиме высокой доступности, то в параметре «Кластерный IP» указывается кластерный IP-адрес (пункт 3.2.1 данного руководства).

Затем создать учетную запись пользователя для брокера, выполнив следующую команду:

```
New-ADUser -Name "<имя сервисной УЗ для брокера>" -GivenName "<имя сервисной УЗ для брокера>"
-SamAccountName "<имя сервисной УЗ для брокера>" -UserPrincipalName
"<имя сервисной УЗ для брокера>@<имя домена>" -Path "CN=Users,DC=example,DC=ru"
-AccountPassword (ConvertTo-SecureString "пароль" -AsPlainText -force)
-Enabled $true
```

Пример выполнения команды:

```
New-ADUser -Name "rbi-server-svc" -GivenName "rbi-server-svc" -SamAccountName "rbi-
server-svc" -UserPrincipalName "rbi-server-svc@example.ru" -Path "CN=rbi-server-
svc,DC=example,DC=ru" -AccountPassword (ConvertTo-SecureString "PrimerPass" -
AsPlainText -force) -Enabled $true
```

Выполнить команду для получения информации о пользователе:

```
Get-ADUser <имя сервисной УЗ для брокера> | Set-ADUser -PasswordNeverExpires:$True
-CannotChangePassword:$True
```

Пример выполнения команды:

```
Get-ADUser rbi-server-svc | Set-ADUser -PasswordNeverExpires:$True -
CannotChangePassword:$True
```

Присвоить учетную запись Service Principal Name (SPN), выполнив команду:

```
setspn -A <SPN для брокера>@<доменная область> <имя сервисной УЗ для брокера>
```

Пример выполнения команды:

```
setspn -A HTTP/rbi-server.example.ru@EXAMPLE.RU rbi-server-svc
```

Проверить корректность назначения SPN:

```
setspn -L <имя сервисной УЗ для брокера>
```

Пример выполнения команды:

```
setspn -L rbi-server-svc
```

Далее создать DNS-записи для каждого из узлов:

```
Add-DnsServerResourceRecordA -Name <имя первого узла> -IPv4Address
<IP-адрес первого узла> -ZoneName <имя домена> -CreatePtr
Add-DnsServerResourceRecordA -Name <имя второго узла> -IPv4Address
<IP-адрес второго узла> -ZoneName <имя домена> -CreatePtr
```

Пример выполнения команды:

```
Add-DnsServerResourceRecordA -Name rbi-node_1 -IPv4Address
10.116.174.11 -ZoneName example.ru -CreatePtr
Add-DnsServerResourceRecordA -Name rbi-node_2 -IPv4Address
10.116.174.12 -ZoneName example.ru -CreatePtr
```

Сформировать keytab-файл для УЗ MS AD брокера:

```
ktpass -princ <SPN для брокера>@<доменная область> -mapuser  
<имя сервисной УЗ для брокера> -crypto All -ptype KRB5_NT_PRINCIPAL -pass <пароль> -  
target  
<адрес контроллера домена> -out c:\ps\<имя брокера>.keytab
```

Пример выполнения команды:

```
ktpass -princ HTTP/rbi-server.example.ru@EXAMPLE.RU -mapuser rbi-server-svc -crypto  
All -ptype KRB5_NT_PRINCIPAL -pass PrimerPass -target dc1-build.example.ru -out  
c:\pac-build-win_1.keytab
```

Сохранить полученный keytab-файл на APM администратора.

2.4.2 Настройка службы KDC для поддержки аутентификации по протоколу Kerberos на прокси-сервере для Microsoft AD DS

Сервис «Ankey RBI» позволяет настроить Ticket-Granting Service (TGS) от УЗ сервисного пользователя для прокси-сервера с Kerberos аутентификацией. Для настройки данной возможности необходимо выполнить следующие действия:

- 1) Открыть консоль управления объектами в домене Microsoft AD DS.
- 2) Выбрать пользователя «rbi-server».
- 3) В открывшемся окне перейти на вкладку «Delegation».
- 4) Выбрать пункт «Trust this computer for delegation to specified services → Use Kerberos only».
- 5) Нажать кнопку «Add».
- 6) Выбрать учетную запись существующего сервисного пользователя, от имени которой работает прокси-сервер, и нажать кнопку «ОК».
- 7) Нажать кнопку «ОК».

2.4.3 Настройка доверия в Microsoft AD DS

Сервис «Ankey RBI» позволяет подключать пользователей из любого домена, входящего в тот же лес, что и домен, в котором развернут комплекс.

Для обеспечения доступа пользователей из другого домена (далее домен Б) к функциональным возможностям «Ankey RBI», необходимо установить доверие между доменом (далее домен А), в котором развернут «Ankey RBI», и доменом Б.

Примечание. Перед установкой доверия необходимо чтобы:

- оба домена имели функциональный уровень Windows Server 2003 или выше и были правильно настроены с точки зрения DNS и сетевой связности;
- порты для AD (например, 53, 88, 135, 389, 445, 636 и др.) были открыты;
- системное время синхронизировано (разница во времени между контроллерами доменов не должна превышать 5 минут).

При настройке достаточно на стороне, устанавливающей доверие (домен А) выбрать установку одностороннего исходящего доверия. Для этого:

- 1) На контроллере домена А откройте оснастку Active Directory Domains and Trusts (Домены и доверительные отношения Active Directory) (можно использовать консоль, запустив domain.msc).
- 2) Выберите в списке записей имя домена А, щёлкните по нему правой кнопкой манипулятора типа «мышь» и в выпадающем меню выберите пункт «Свойства» (Properties) (рис. 2).

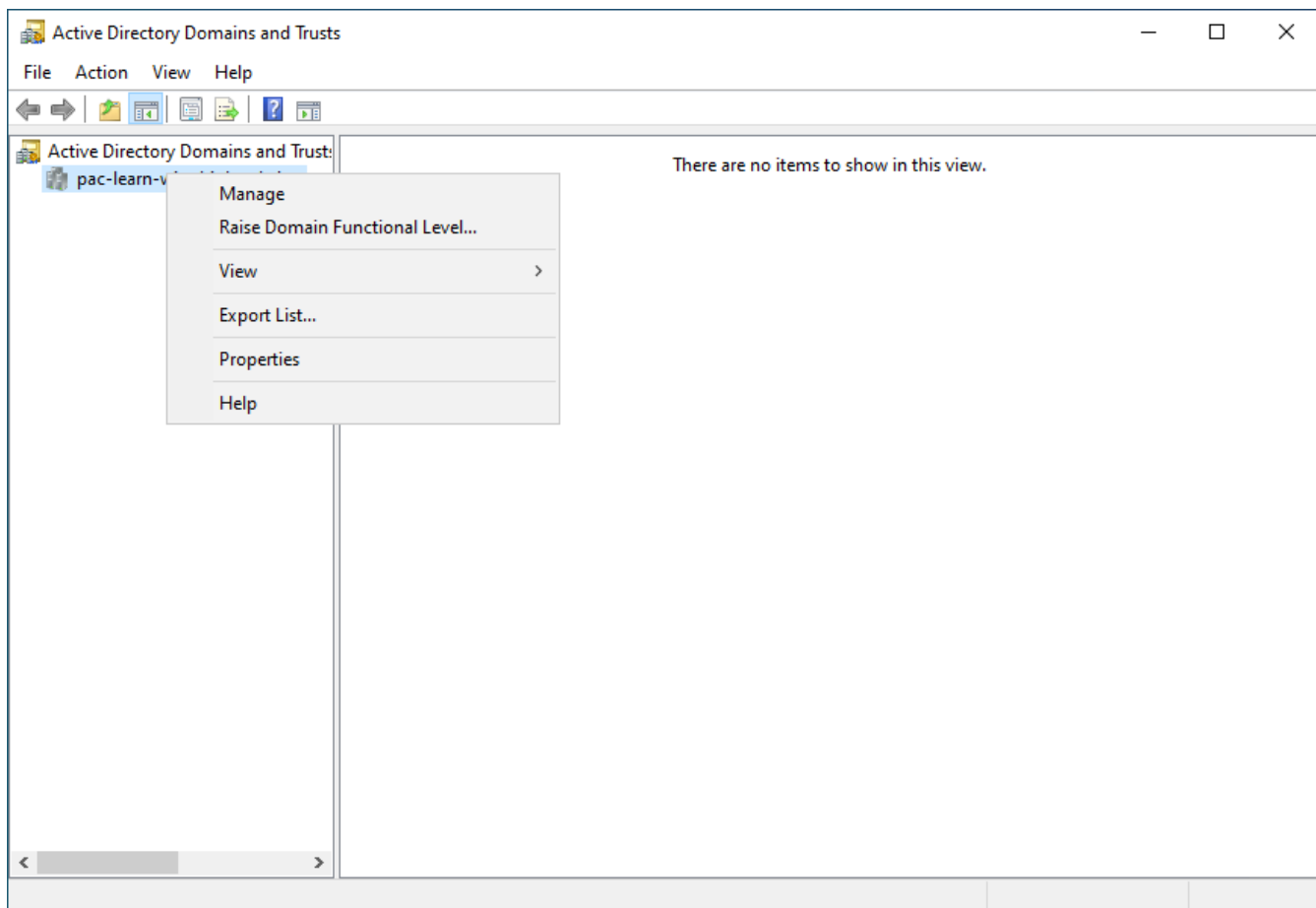


Рисунок 2 – Окно «Домены и доверительные отношения» с выпадающим меню

- 3) В открывшемся окне перейдите на вкладку «Доверительные отношения» (Trusts) (рис. 3) и нажмите кнопку создания доверительного отношения (New Trust). Запустится мастер установки доверительного отношения.

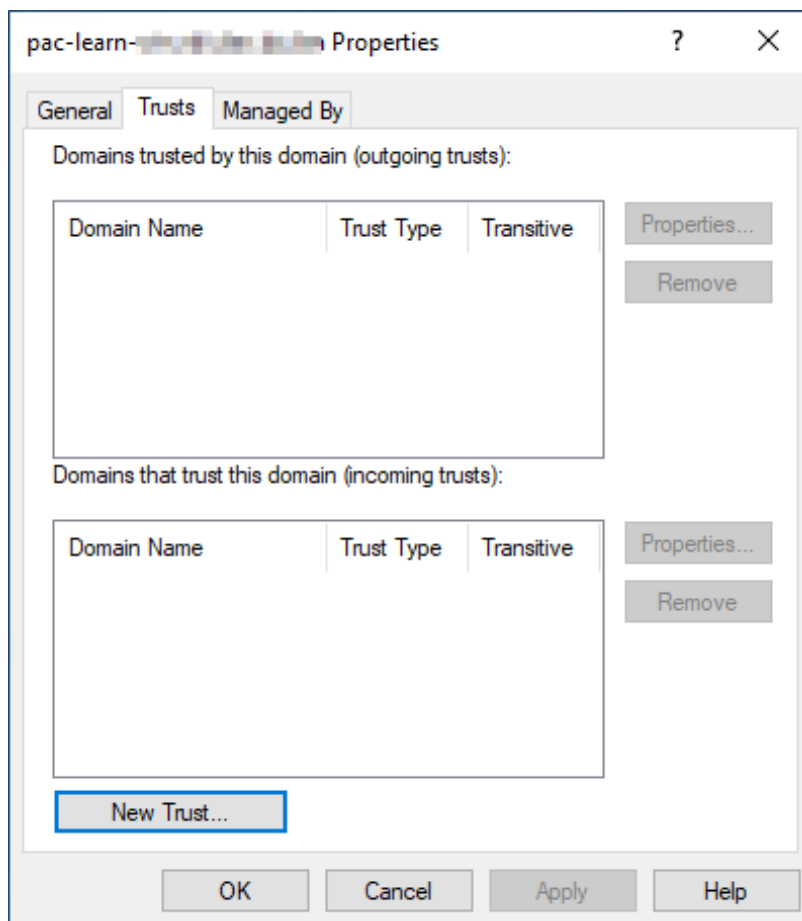


Рисунок 3 – Вкладка «Доверительные отношения»

- 4) Далее в мастере установки необходимо указать:
- FQDN корневого домена Б (например, «forestB.local»);
 - тип доверия «Forest trust»;
 - доверие одностороннее исходящее «Outgoing»;
 - сторона доверительного отношения «Both this domain and the specified domain» (если известны данные учетной записи администратора домена Б) или «This domain only» (если неизвестны). В втором случае администратору домена Б необходимо установить одностороннее входящее доверие с доменом А;
 - область действия «Forest-wide»;
 - аутентификация «Forest-wide authentication».

Далее необходимо в Microsoft AD Users and Computers домена А создать группу пользователей для сопоставления LDAP групп ролям пользователей RBI (см. подраздел 4.3 данного руководства), установив область действия группы «Domain local». Затем в эту группу включить пользователей из домена Б.

2.5 Подготовка службы каталогов Samba DC

ПК «Ankey RBI» не имеет собственной базы пользователей и групп. ПК «Ankey RBI» производит аутентификацию/авторизацию пользователей с помощью сервисов, которые

предоставляет домен. Для настройки интеграции необходимо выполнить действия, приведенные ниже.

Примечания. Все перечисленные ниже команды выполняются в командной оболочке Bash.

Описание параметров, используемых в пунктах 2.5.1 и 2.5.2, представлено в Приложении 1.

2.5.1 Базовая настройка для Samba DC

Необходимо получить все DNS-записи с помощью команды:

```
samba-tool dns query <адрес контроллера домена> @ ALL -U Administrator
```

Далее необходимо добавить DNS-записи для всех узлов и брокера, выполнив последовательно следующие команды:

```
samba-tool dns add <адрес контроллера домена> <имя первого узла> A <IP-адрес первого узла> -U Administrator  
samba-tool dns add <адрес контроллера домена> <имя второго узла> A <IP-адрес второго узла> -U Administrator  
samba-tool dns add <адрес контроллера домена> <имя брокера> A 10.116.179.25 -U Administrator
```

Затем необходимо создать учетную запись пользователя для брокера, выполнив последовательно следующие команды:

```
samba-tool user create --random-password <имя сервисной УЗ для брокера>  
samba-tool user setexpiry <имя сервисной УЗ для брокера> --noexpiry  
samba-tool spn add <SPN для брокера>@EXAMPLE.RU <имя сервисной УЗ для брокера>
```

Далее требуется сформировать keytab-файл для УЗ ipaservice брокера, выполнив последовательно следующие команды

```
samba-tool domain exportkeytab /tmp/<имя брокера>.keytab --principal=<SPN для брокера>  
klist -ke /tmp/<имя брокера>.keytab  
KRB5_TRACE=/dev/stdout kinit -5 -V -k -t /tmp/<имя брокера>.keytab <SPN для брокера>
```

Сохранить полученный keytab-файл на APM администратора.

2.5.2 Настройка службы KDC для поддержки аутентификации по протоколу Kerberos на прокси-сервере для Samba DC

Сервис «Ankey RBI» позволяет настроить Ticket-Granting Service (TGS) от УЗ сервисного пользователя для прокси-сервера с Kerberos аутентификацией.

Для настройки данной возможности необходимо выполнить следующие действия проверить текущие настройки делегирования для пользователя «», выполнив следующую команду:

```
samba-tool delegation show <имя сервисной УЗ для брокера>
```

Далее необходимо доверить пользователю делегирование spn проху, выполнив следующую команду:

```
samba-tool delegation add-service <имя сервисной УЗ для брокера> <SPN для прокси сервера> -U administrator
```

2.6 Подготовка TLS-сертификатов

Корневые сертификаты добавляются в ПК «Ankey RBI» путем импорта из файлов формата X.509 PEM или PKCS#12 PFX.

Примечание. Способ подготовки сертификатов может отличаться и зависит от используемых в организации центров сертификации.

TLS-сертификат, импортируемый в ПК «Ankey RBI», должен удовлетворять следующим требованиям:

- сертификат должен быть выпущен с использованием шаблона Web Server;
- сертификат должен быть помечен как экспортируемый;
- в сертификате должны быть указаны все используемые DNS имена;
- сертификат должен быть выпущен в формате PKCS#12 (Public-Key Cryptography Standards), содержащий цепочку сертификатов и закрытый ключ. Или ключ сервера, сертификат должны быть в формате PEM.

Полученные сертификаты необходимо использовать при настройке параметров ПК «Ankey RBI».

2.7 Подготовка сертификатов брокеров и узлов

Для работы брокеров и узлов ПК «Ankey RBI» требуется выпуск ключа и сертификата RSA.

Примечание. Способ подготовки сертификатов может отличаться и зависит от используемых в организации центров сертификации.

Общие требования к сертификатам:

- тип: RSA;
- обязательное указание FQDN в полях «CN» и «subjectAltName»;
- в поле «extendedKeyUsage» необходимо разрешить проверку подлинности сервера.

Ниже представлен пример создания CSR (Certificate Signing Request) – запроса на выдачу сертификата с помощью OpenSSL:

```
openssl req -new -out $FQDN.csr -newkey rsa:2048 -nodes -sha256 -keyout $FQDN.key -  
config <имя_конфигурационного_файла>.conf
```

После выполнения запроса, в текущем каталоге будут созданы файлы запроса сертификата \$FQDN.csr, файл ключа \$FQDN.key и файл .conf, в котором необходимо заполнить поля: «CN», «subjectAltName», «extendedKeyUsage», «C» (код региона), «ST» (регион), «L» (город), «O» (название компании) и «OU» (подразделение).

Ниже представлена структура конфигурационного файла и пример заполнения:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
prompt = no
[req_distinguished_name]
C = RU
ST = SPb
L = Saint-Petersburg
O = Company
OU = IT
CN = {FQDN}
[v3_req]
keyUsage = keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
basicConstraints = CA:false
[alt_names]
DNS.1 = {FQDN}
```

Полученный CSR необходимо отправить администраторам компании, чтобы они на его основании выпустили сертификат, который далее будет использован для брокеров, узлов и ПК «Ankey RBI».

3 Установка ПК

3.1 Установка брокера

Внимание! Перед установкой брокера необходимо:

- ознакомиться с рекомендациями по разбиению дисков для установки ПК «Ankey RBI», представленными в пункте 1.6.1 данного руководства;
- при установке брокера на сервер, который не планируется использовать в качестве узла, необходимо установить на него корневые сертификаты предприятия.

Для установки брокера требуется загрузить архив с дистрибутивом программного обеспечения (ПО) по ссылке на скачивание, которая будет отправлена в письме производителем, или скопировать с предоставленного компакт-диска.

Перед установкой брокера необходимо установить библиотеку поддержки сервиса лицензирования, выполнив в каталоге с дистрибутивами в консоли РЕД ОС команду:

```
sudo dnf install gis-activator14-1.4.1-2.x86_64.rpm
```

Для установки брокера требуется перейти в каталог с дистрибутивами и в консоли РЕД ОС выполнить последовательность действий и команд, приведенных ниже:

Примечание. Все команды вводятся от имени суперпользователя root, либо используя программу sudo.

- 1) Установить брокер, выполнив команду:

```
sudo dnf install rbi-server-X.X.X.XX.x86_64.rpm
```

- 2) Дождаться окончания установки. Отсутствие каких-либо ошибок в консоли будет свидетельствовать об успешной установке брокера.
- 3) Разрешить запись в каталог /mnt/rbi/ (файловое хранилище) пользователю rbi-server (создается автоматически при установке брокера) с помощью следующей команды:

```
chown rbi-server:rbi-server /mnt/rbi
```

- 4) Разрешить автозапуск и запустить службу брокера, выполнив следующие команды:

```
systemctl enable rbi-server.service  
systemctl start rbi-server.service
```

- 5) Активировать службу лицензирования брокера, выполнив следующие команды:

```
systemctl enable rbi-license  
systemctl start rbi-license
```

- 6) Открыть браузер и ввести IP-адрес брокера. При возникновении предупреждения о ненадежности сертификата безопасности необходимо продолжить открытие веб-сайта, после чего отобразится веб-интерфейс ПК «Ankey RBI», в котором требуется заполнить следующие поля:

- «DB connection string» – строка подключения к БД. Подробнее о подготовке БД см. подраздел 2.1 данного руководства. Данные указываются в следующем формате:
postgres://<username>:<password>@host:<host>/<dbname>
где: <username> и <password> – данные служебной УЗ пользователя БД; <host> – адрес сервера БД; <dbname> – наименование БД.
 - «Имя пользователя для администратора» – в данном поле устанавливается имя пользователя, который будет локальным администратором ПК «Ankey RBl». Требования к имени локального администратора представлены в подразделе 4.5 данного руководства;
 - «Пароль администратора» – в данном поле устанавливается пароль для локального администратора. Требования к паролю локального администратора представлены в подразделе 4.5 данного руководства. Примечание. Вышеуказанные данные учетных записей используются только для первичной настройки ПК «Ankey RBl» или в случае аварийных ситуаций. После настройки служб каталогов LDAP/LDAPS необходимо использовать для авторизации в комплексе УЗ службы каталога.
- 7) Нажать кнопку «Проверить возможность установки». На этом этапе брокер проверяет доступность БД. После успешной проверки появится сообщение о готовности установки.
 - 8) Нажать кнопку «Установить сервер». На этом этапе брокер инициализирует БД. Администратор будет перенаправлен на стартовую страницу веб-интерфейса для авторизации.

После выполненных действий брокер считается установленным. Необходимо перейти к настройкам параметров комплекса.

3.2 Установка в режиме высокой доступности

Важно! Для настройки высокой доступности должен быть предварительно установлен один брокер.

Брокер поддерживает работу в режиме высокой доступности (high availability) по схеме active/standby. В случае недоступности активного брокера по любой причине (например, выход из строя оборудования, недоступность сетевого подключения и т. д.), резервный брокер берет на себя обслуживание запросов.

Примечания:

- 1) Режим высокой доступности обеспечивается автоматическим переключением IP-адреса между брокерами с помощью сервиса keepalived, который работает по протоколу VRRP (Virtual Router Redundancy Protocol). Сервер с активным брокером получает «кластерный IP-адрес» на локальный сетевой интерфейс. Для корректной работы протокола VRRP все брокеры должны находиться в одной подсети.

- 2) Убедиться, что настройка файлового хранилища выполнена на всех серверах для размещения брокера.

3.2.1 Настройка высокой доступности

Примечание. Все команды вводятся от имени суперпользователя root, либо используя программу sudo.

Для настройки режима высокой доступности необходимо выполнить действия, приведенные ниже.

Изменить на всех серверах, которые будут использованы для размещения брокеров, файл «/etc/keepalived/keepalived.conf». Содержание файла необходимо заменить на представленную ниже информацию:

```
! Configuration File for keepalived
global_defs {
enable_script_security
vrrp_skip_check_adv_addr
}
include /etc/keepalived/conf.d/*.conf
```

В случае, если на сервере включена система «SELinux», то необходимо разрешить вносить изменения в сервис keepalived. Для определения состояния системы «SELinux» необходимо выполнить следующую команду:

```
sestatus
```

Если в результате выполнения команды был получен ответ «SELinux status: enabled», то необходимо выполнить следующую команду:

```
semanage permissive -a keepalived_t
```

Далее установить дополнительный экземпляр брокера. Для этого необходимо:

- 1) Выполнить шаги 1 – 5 из подраздела 3.1.
- 2) Открыть браузер и ввести IP-адрес брокера, полученный на этапе подготовки к установке, после чего отобразится веб-интерфейс ПК «Ankey RBI», в котором требуется заполнить следующие поля:
 - «DB connection string» — строка подключения к базе данных. Подробнее о подготовке БД см. подраздел 2.1 данного руководства. Данные указываются в следующем формате:
postgres://<username>:<password>@host:<host>/<dbname>
где: <username> и <password> – данные служебной УЗ пользователя БД; <host> – адрес сервера БД; <dbname> – наименование БД.
 - «Имя пользователя для администратора» — в данном поле указывается имя УЗ локального администратора, которое было указано при настройке первого экземпляра брокера.

- «Пароль администратора» — в данном поле указывается пароль УЗ локального администратора, который был указан при настройке первого экземпляра брокера.
- 3) Нажать кнопку «Проверить возможность установки». Будет проведена проверка доступности БД и наличие в ней данных о существующем экземпляре брокера. После успешной проверки появится сообщение о готовности к установке дополнительного экземпляра брокера.
- 4) Нажать кнопку «Установить дополнительный сервер». Будет проведено добавление дополнительного экземпляра брокера в существующую БД. После успешного добавления пользователь будет перенаправлен на стартовую страницу веб-интерфейса для авторизации.

Затем необходимо настроить кластерный IP-адрес. Для этого следует открыть браузер, ввести IP-адрес первого из установленных брокеров, авторизоваться и перейти в раздел «Настройки системы». Если в разделе «Настройки системы» появилось уведомление о необходимости перезапуска сервера, то требуется выполнить перезагрузку, нажав кнопку «Перезапустить».

После этого в разделе «Настройки системы» необходимо перейти в настройки «Высокая доступность» и заполнить следующие поля:

- «Кластерный IP-адрес» – свободный IP-адрес из подсети, в которой находятся IP-адреса всех установленных брокеров;
- «Пароль VRRP» – назначается автоматически при установке первого экземпляра брокера. Изменение параметра требуется только в случае инцидента безопасности.

Перезапустить все зарегистрированные брокеры, выполнив команду (на каждом из брокеров):

```
sudo systemctl restart rbi-server
```

Включить автозапуск и перезапустить сервис keeplived на всех брокерах, выполнив последовательно следующие команды:

```
sudo systemctl enable keeplived  
sudo systemctl restart keeplived
```

Открыть страницу веб-интерфейса ПК «Ankey RBI» по FQDN-адресу кластерного IP-адреса, перейти в пункт меню «Брокеры» и убедиться, что отображаются оба брокера. Экземпляр брокера, который был установлен первым, должен отображаться со статусом «Активный». Дополнительный экземпляр брокера отображается со статусом «Запасной».

3.3 Установка клиента на АРМ пользователя

Внимание! Перед установкой клиента необходимо убедиться, что корневые сертификаты, которыми подписаны TLS-сертификаты брокеров и узлов, установлены на АРМ пользователя.

3.3.1 Установка клиента на АРМ пользователя под управлением РЕД ОС, Astra Linux или ALT Linux

Для установки клиента требуется загрузить архив с дистрибутивом ПО по ссылке на скачивание, которая будет отправлена в письме производителем, или скопировать с предоставленного компакт-диска.

Далее следует перейти в каталог с дистрибутивами и в консоли РЕД ОС, Astra Linux или ALT Linux выполнить следующую команду:

```
sudo dnf install rbi-client-X.X.X.XX.x86_64.rpm
```

3.3.1.1 Добавление ярлыка для ПК «Ankey RBI» на рабочий стол пользователя

Для добавления ярлыка для ПК «Ankey RBI» на рабочий стол пользователя необходимо выполнить указанные ниже команды в консоли РЕД ОС, Astra Linux или ALT Linux.

Примечание. Команду необходимо вводить от имени УЗ пользователя, на рабочий стол которого требуется добавить ярлыки.

Команда добавления ярлыка для запуска клиента:

```
rbi_shortcut -s <https://FQDN rbi-сервера> -n <Имя ярлыка для запуска клиента>
```

Команда добавления ярлыка для запуска веб-интерфейса:

```
rbi_shortcut -s <https://FQDN rbi-сервера> -w -n <Имя ярлыка для запуска веб-интерфейса>
```

где:

- флаг **-s** – используется для указания адреса брокера, к которому будет произведено подключение при нажатии на ярлык на рабочем столе. Адрес указывается в следующем формате: `https://<FQDN rbi-сервера>`;
- флаг **-w** (необязательный) – используется для создания ярлыка для запуска веб-интерфейса. Имя ярлыка по умолчанию – «RBI Web UI». В качестве браузера, в котором будет запускаться веб-интерфейс, используется браузер на АРМ пользователя, который установлен по умолчанию;
- флаг **-n** (необязательный) – используется для указания имени ярлыка на рабочем столе. Если флаг не указан, то по умолчанию ярлыку присваивается следующее имя: ПК RBI;
- флаг **-m** (необязательный) – используется, если клиенту необходимо предоставить доступ к устройствам на АРМ пользователя (микрофон). После флага необходимо указать команду:

```
--use-mic
```

Внимание! После создании ярлыка для запуска веб-интерфейса администраторам, обслуживающим ПК «Ankey RBI», необходимо разрешить веб-браузеру производить

аутентификацию по протоколу Kerberos с помощью политики браузера «AuthServerAllowlist».

После выполнения всех действий на рабочем столе АРМ пользователя появятся следующие ярлыки:

- ярлык «ПК RBI»  – используется для запуска изолированного приложения;
- ярлык «RBI Web UI»  – используется для запуска веб-интерфейса.

3.3.1.2 **Добавление ярлыка для ПК «Ankey RBI» на рабочий стол всех пользователей**

Администратору ПК «Ankey RBI» доступна возможность добавления на все АРМ пользователей ярлыки для запуска веб-интерфейса и клиента. Для этого администратору необходимо на своем АРМ в консоли РЕД ОС выполнить указанные ниже команды.

Внимание! Централизованное создание ярлыков доступно только для всех новых пользователей, которые еще не авторизовывались в домене. Ярлык будет доступен на АРМ новых пользователей после первой авторизации в домене. Для создания ярлыка на АРМ уже существующих пользователей необходимо выполнить действия, представленные в пункте 3.3.1 данного руководства.

Команда добавления ярлыка для запуска клиента:

```
/usr/local/bin/rbi_shortcut -s <https://FQDN rbi-сервера> -a -n <Имя ярлыка для запуска клиента>
```

Команда добавления ярлыка для запуска веб-интерфейса:

```
rbi_shortcut -s <https://FQDN rbi-сервера> -a -w -n <Имя ярлыка для запуска веб-интерфейса>
```

где:

- флаг -s – описание флага представлено в пункте 3.3.1;
- флаг -a – используется для централизованного создания ярлыка на АРМ всех новых пользователей;
- флаг -w (необязательный) – описание флага представлено в пункте 3.3.1;
- флаг -n (необязательный) – описание флага представлено в пункте 3.3.1.

3.3.1.3 **Настройка возможности запуска клиента ПК «Ankey RBI» в качестве браузера по умолчанию**

Для настройки возможности запуска клиента ПК «Ankey RBI» в качестве браузера по умолчанию на РЕД ОС, Astra Linux или ALT Linux необходимо на АРМ пользователя:

- 1) Открыть файл конфигурации «.desktop» ПК «Ankey RBI» и добавить в него следующую строку:

```
Categories=Network;WebBrowser;  
MimeType=text/html;x-scheme-handler/x-scheme-handler/https;
```

- 2) В этом же файле в строке «Exec» требуется убрать «%f» и добавить «-o %U». Ниже представлен пример результата:

```
Exec=/usr/local/bin/rbi-client -c https://rbi.example.server -o $U
```

- 3) Обновить базу данных ярлыков в меню приложений, выполнив следующую команду:

```
sudo update-desktop-database
```

- 4) С помощью xdg выбрать ПК «Ankey RBI» в качестве браузера по умолчанию. Для этого требуется выполнить следующую команду:

```
xdg-settings set default-web-browser rbi-client.desktop
```

3.3.2 Установка клиента на АРМ пользователя под управлением ОС Windows 10/11

Примечание. Перед установкой клиента необходимо установить утилиту Remote Viewer (virt-viewer).

Для установки ПК «Ankey RBI» на АРМ пользователя под управлением Windows 10/11 требуется загрузить архив с дистрибутивом ПО по ссылке на скачивание, которая будет отправлена в письме производителем, или скопировать с предоставленного компакт-диска.

- 1) Запустить от имени администратора файл для установки клиента: «rbiclient.msi».
- 2) В появившемся приветственном окне нажать кнопку «Далее» (рис. 4).

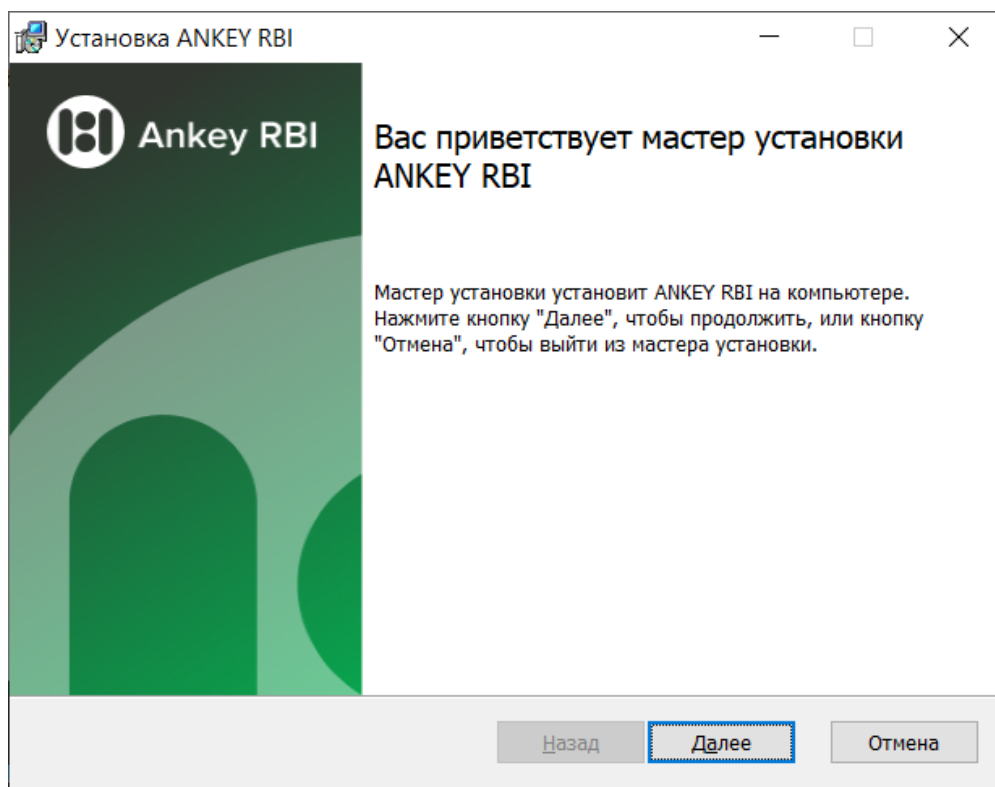


Рисунок 4 – Приветственное окно

- 3) Затем снова нажать кнопку «Далее» (рис. 5), чтобы выполнить установку клиента в папке по умолчанию, или кнопку «Изменить», чтобы выбрать другую папку.

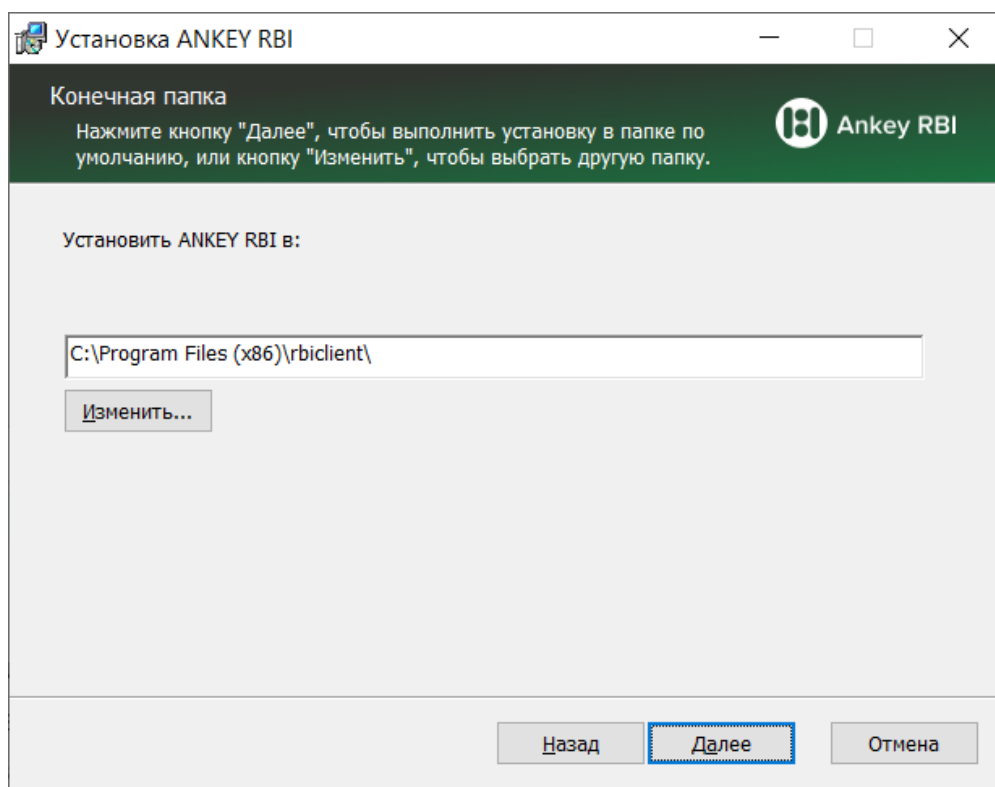


Рисунок 5 – Выбор пути установки

- 4) Указать адрес RBI-сервера и нажать кнопку «Далее» (рис. 6).

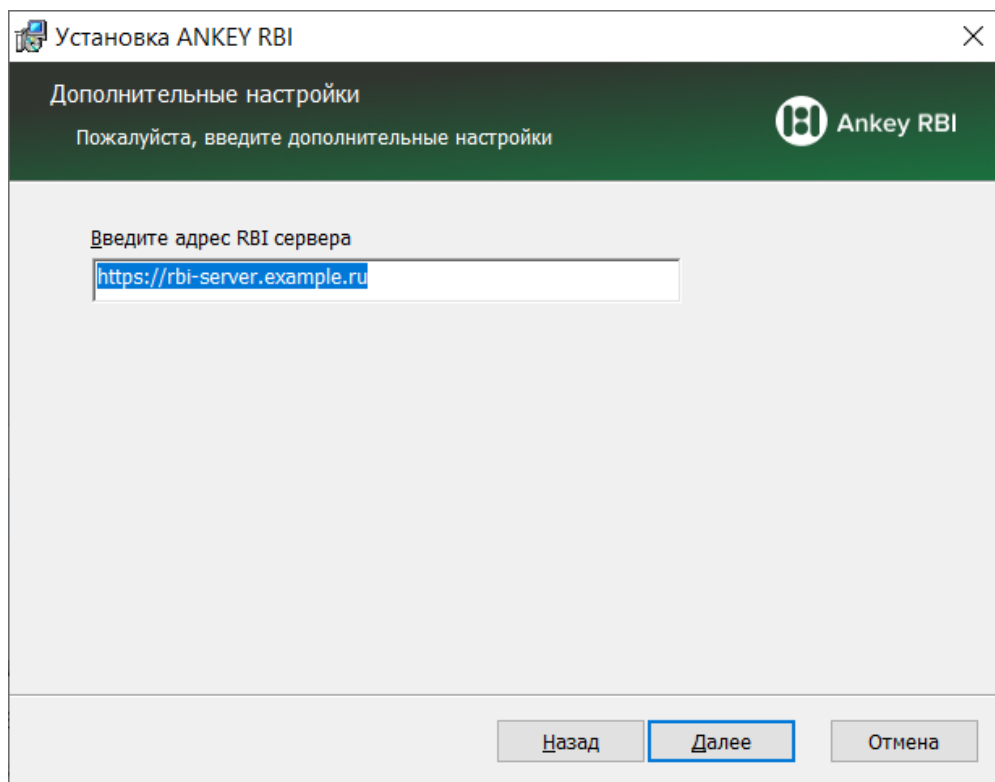


Рисунок 6 – Указание RBI-сервера

- 5) Нажать кнопку «Установить» (рис. 7) и дождаться завершения установки.

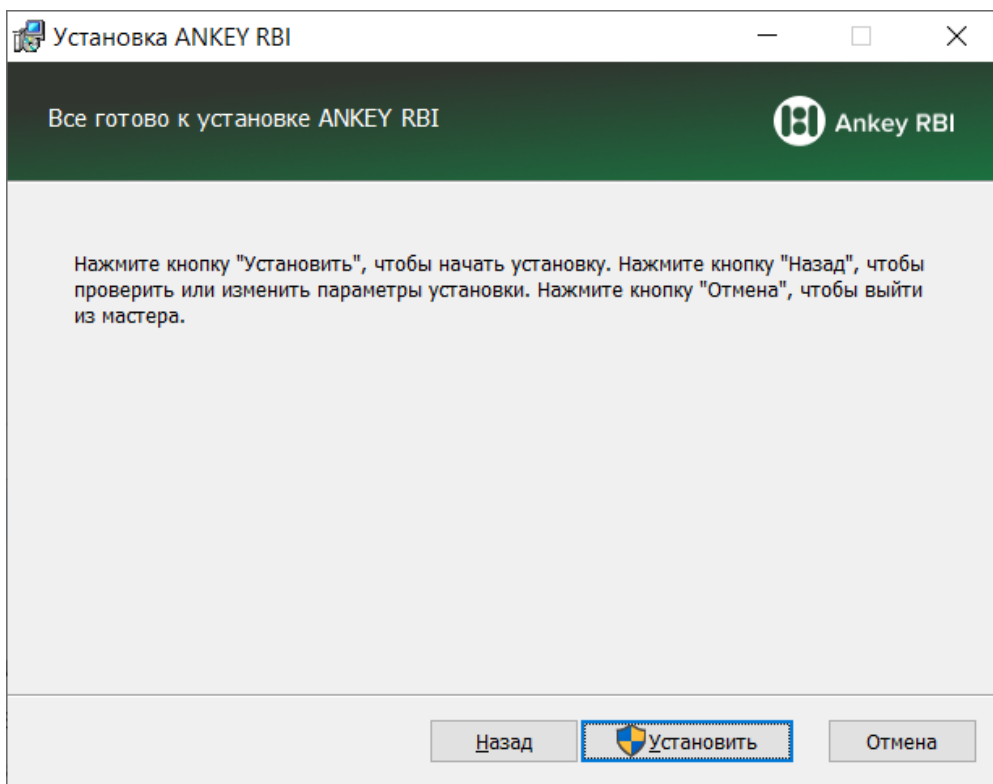


Рисунок 7 – Подтверждение установки

- 6) Нажать кнопку «Готово» (рис. 8).

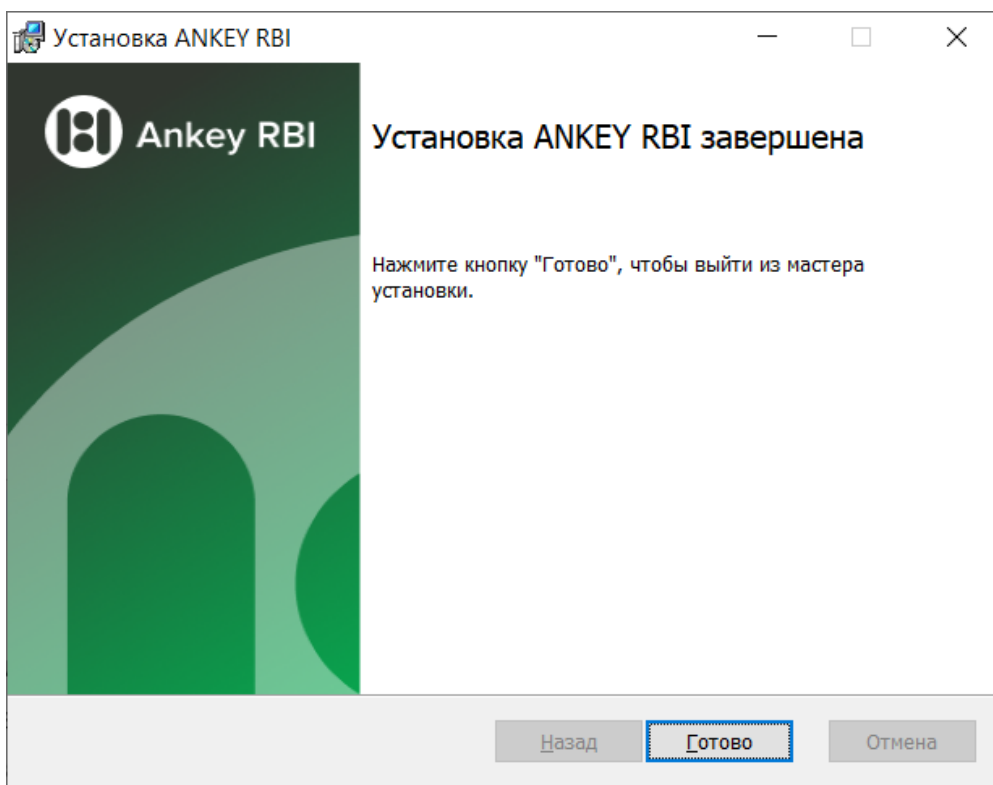


Рисунок 8 – Завершение установки

После выполнения всех действий на рабочем столе АРМ пользователя появятся следующие ярлыки:

- ярлык ПК «Ankey RBI»  – используется для запуска изолированного приложения;
- ярлык «Ankey RBI» Web UI  – используется для запуска веб-интерфейса.

3.3.2.1 **Настройка возможности запуска клиента ПК «Ankey RBI» в качестве браузера по умолчанию**

Для настройки возможности запуска клиента ПК «Ankey RBI» в качестве браузера по умолчанию на ОС Windows 10/11 необходимо на АРМ пользователя открыть меню «Пуск», перейти в «Параметры» → «Приложения» → «Приложения по умолчанию» и далее в пункте «Веб-браузер» выбрать из списка клиент ПК «Ankey RBI».

3.3.3 **Настройка возможности аутентификации в клиенте ПК «Ankey RBI» по сертификатам, располагающимся на ключевом носителе**

Для настройки возможности аутентификации в клиенте ПК «Ankey RBI» по сертификатам, располагающимся на ключевом носителе (смарт-карте), требуется установить на АРМ пользователя драйверы или другое специальное ПО, в зависимости от используемых ключевых носителей.

Установка драйверов или специального ПО для ключевых носителей производится согласно официальной документации от вендора.

Примечание. Ключевые носители должны поддерживать работу с криптографическим стандартом PKCS#11.

Для настройки аутентификации в клиентском приложении ПК «Ankey RBI» с помощью сертификатов, располагающихся на ключевых носителях, необходимо нажать правой кнопкой манипулятора типа «мышь» на ярлык  и выбрать «Свойства»:

- 1) Для операционных систем Astra Linux Special Edition, ALT Linux и РЕД ОС – перейти на вкладку «Простой» и в поле «Команда» указать запись с ключом для аутентификации по ключевым носителям. Например:

```
--pkcs11 /<путь к библиотеке>/<название библиотеки>.so --smartcard-login
```

или с короткой формой ключа:

```
--pkcs11 /<путь к библиотеке>/<название библиотеки>.so -s
```

- 2) Для операционных систем Windows – перейти на вкладку «Ярлык» и в поле «Объект» добавить запись с ключом для аутентификации по ключевым носителям. Например:

```
--pkcs11 /<путь к библиотеке>/<название библиотеки>.dll --smartcard-login
```

или с короткой формой ключа:

```
--pkcs11 /<путь к библиотеке>/<название библиотеки>.dll -s
```

Далее сохранить изменения и закрыть окно «Свойства».

3.3.4 Настройка возможности авторизации на порталах с поддержкой двухсторонней аутентификации

ПК «Ankey RBI» позволяет авторизоваться на государственных порталах, использующих двухстороннюю аутентификацию по TLS на основе ГОСТ (mutual TLS, mTLS).

Для реализации данной возможности требуется:

- установить на каждый узел лицензию на право использования СКЗИ «КриптоПро CSP» версии 5.0 на сервере (подробнее в подразделе 7.2 данного руководства);
- установить на АРМ пользователя драйверы или другое специальное ПО, в зависимости от используемых ключевых носителей.

Установка сертификатов, драйверов или специального ПО для ключевых носителей производится согласно официальной документации от вендора.

Далее необходимо нажать правой кнопкой манипулятора типа «мышь» на ярлык  и выбрать «Свойства»:

- 1) Для операционных систем Astra Linux Special Edition, ALT Linux и РЕД ОС – перейти на вкладку «Простой» и в поле «Команда» указать запись с ключом для аутентификации по ключевым носителям:

```
--pcsc-forwarding
```

Внимание! Для обеспечения корректной работы в ОС пользователя должен быть запущен демон «pcscd».

Для проверки работы необходимо выполнить следующую команду:

```
systemctl status pcscd
```

- 2) Для операционных систем Windows – перейти на вкладку «Ярлык» и в поле «Объект» добавить запись с ключом для аутентификации по ключевым носителям:

```
--pcsc-forwarding
```

Далее сохранить изменения и закрыть окно «Свойства».

Внимание! При работе на АРМ под управлением ОС Windows возможно возникновение ошибки mTLS-авторизации при прерывании пользователем работы с изолированным приложением. Если произошла такая ошибка, то для продолжения работы с ресурсом, использующем mTLS-авторизацию, необходимо:

- принудительно завершить сессию, если она не была завершена автоматически;
- повторно запустить изолированное приложение.

4 Настройка параметров комплекса

Для использования функциональных возможностей ПК после установки должна быть выполнена настройка параметров ПК.

Настройка параметров комплекса осуществляется в веб-интерфейсе, для запуска которого необходимо:

- 1) Запустить браузер на АРМ администратора ПК.
- 2) Ввести в адресной строке IP-адрес установленного брокера (см. подраздел 3.1 данного руководства).
- 3) Заполнить поля «Имя пользователя» и «Пароль» (рис. 9). При авторизации необходимо использовать имя пользователя и пароль, указанные в ходе процесса установки экземпляра ПО для локального администратора ПК «Ankey RBI» (см. подраздел 3.1 данного руководства).

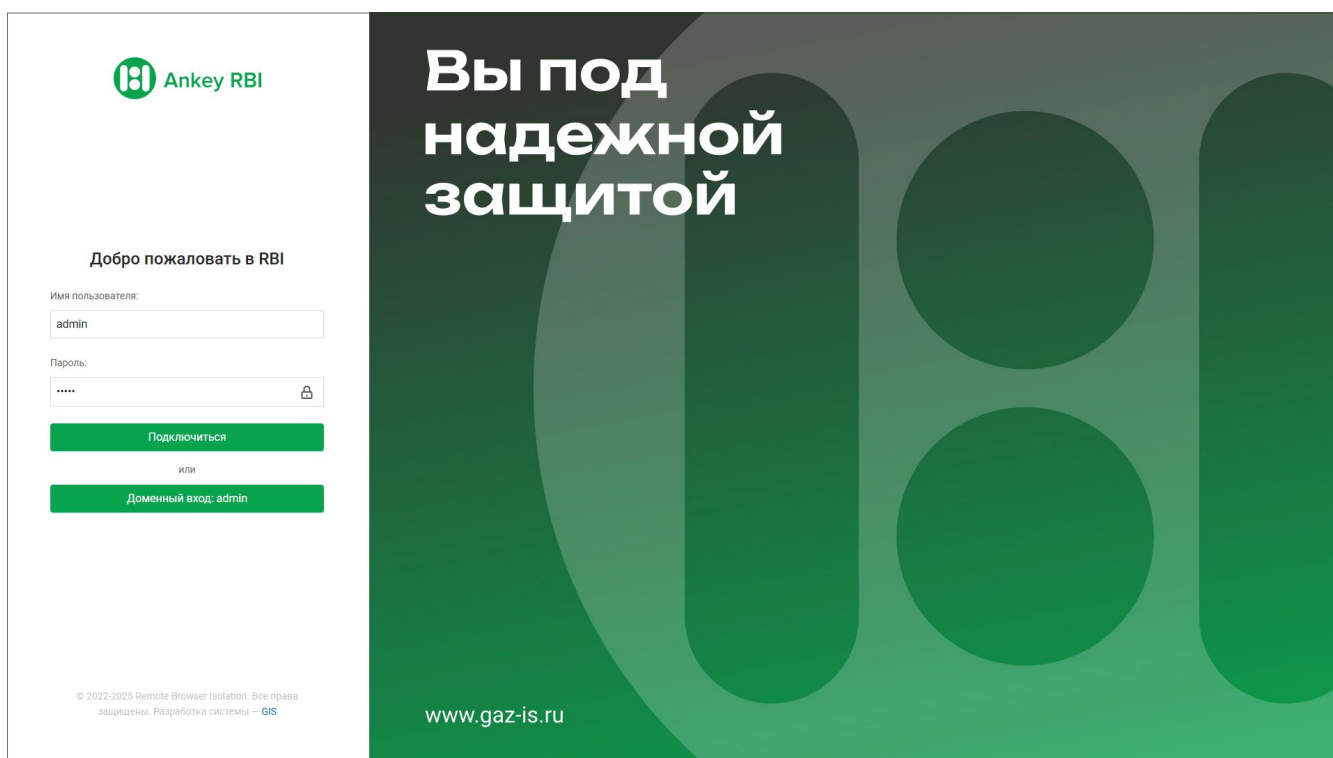


Рисунок 9 – Стартовая страница веб-интерфейса ПК «Ankey RBI»

Примечание. Если в течение 15 минут было 4 неудачных попытки локальной авторизации, то появится сообщение о блокировке аутентификации. Следующая попытка авторизации будет возможна по истечении 15 минут после последней неудачной попытки.

- 4) Нажать кнопку «Подключиться». Будет осуществлен вход в комплекс.

Далее необходимо перейти в раздел «Настройка системы» (рис. 10) и заполнить значения параметров комплекса, согласно представленному ниже описанию.

Настройки системы

Необходимо перезапустить RBI-сервер Перезапустить

- > Настройки HTTPS
- > Интеграция с LDAP
- > Сопоставление LDAP групп ролям RBI
- > Интеграция с Kerberos
- > Пользовательские файлы
- > Режим высокой доступности
- > Аудит
- > Оповещение о критических состояниях
- > Интеграция с антивирусной программой
- > Учетная запись локального администратора

Профиль по умолчанию: По умолчанию

Сохранить

Рисунок 10 – Раздел «Настройки системы» веб-интерфейса ПК «Ankey RBI»

Обратите внимание, что при изменении следующих настроек в системе появится уведомление о необходимости перезапуска сервера, который требуется выполнить, нажав кнопку «Перезапустить»:

- «Корневые сертификаты»;
- «Сертификат HTTPS-сервера»;
- «Ключ HTTPS-сервера»;
- «Секретный ключ JWT»;
- «Keytab-файл сервиса»;
- «Адрес SIEM syslog сервера».

4.1 Группа настроек «Настройка HTTPS»

Для корректной работы сервера ПК «Ankey RBI» необходимо настроить следующие параметры:

- «Адрес RBI-брокера» – сетевой адрес брокера, указываемый в виде FQDN. В адресе должна быть использована схема: `https://<FQDN rbi-брокера>`;
- «Корневые сертификаты» – корневой сертификат TLS. Загружается в виде файла с расширением PEM или указывается содержимое PEM-файла в текстовом поле. В данном поле допускается указать один или несколько сертификатов. Для загрузки сертификатов необходимо нажать кнопку «Загрузить файл» и выбрать файлы для загрузки;
- «Редактировать корневые сертификаты в виде текста» – переключатель, отвечающий за формат загрузки корневых сертификатов. Если переключатель активен, то сертификат указывается в текстовом поле, если неактивен – в виде загружаемого файла;

- «Ключ HTTPS-сервера» – текстовое поле для указания ключа HTTPS сервера. Указывается в виде текста, который начинается с «-----BEGIN PRIVATE KEY-----» или «-----BEGIN RSA PRIVATE KEY-----». После сохранения параметра его значение в целях безопасности отображается в интерфейсе в виде ***;
- «Сертификат HTTPS-сервера» – текстовое поле для указания сертификата HTTPS сервера. Указывается в виде текста, который начинается с -----BEGIN CERTIFICATE-----. После сохранения параметра его значение в целях безопасности отображается в интерфейсе в виде ***;
- «Секретный ключ JWT» – при настройке ПК рекомендуется пропустить заполнение данного поля. Значение данного параметра заполняется автоматически во время установки комплекса. Параметр используется для подписи JWT-токенов, выданных при аутентификации пользователей на сервере. Изменение параметра требуется только в случае инцидента безопасности. В случае изменения параметра потребуется повторная авторизация пользователей;
- «Срок действия токена авторизации, мин» – время существования токена доступа в минутах, по истечении которого потребуется повторная аутентификация в веб-интерфейсе ПК «Ankey RBI». Минимальное значение для данного параметра – 5 минут, максимальное – 1440 минут;
- «Максимальный срок жизни сессии пользователя в веб-интерфейсе, мин» – максимальное время жизни сессии пользователя в минутах, по истечении которого потребуется повторная аутентификация в веб-интерфейсе ПК «Ankey RBI». Значение параметра «Максимальный срок жизни сессии пользователя в веб-интерфейсе, мин» не может быть меньше, чем значение параметра «Срок действия токена авторизации, мин». Максимальное значение для данного параметра – 43200 минут.

Внимание! Допускается загрузка сертификатов в виде PFX-файла. Для этого необходимо нажать кнопку «Загрузить PFX» и выбрать файлы для загрузки. При загрузке файлов параметры «Ключ HTTPS-сервера» и «Сертификат HTTPS-сервера» будут заполнены автоматически. Если PFX-файл содержит корневые сертификаты, кроме ключа и сертификата HTTPS-сервера, то параметр «Корневые сертификаты» также будет автоматически заполнен.

4.2 Группа настроек «Интеграция с LDAP»

Для получения сервером информации об УЗ пользователей служб каталогов, необходимо установить следующие параметры:

- 1) «Вид службы каталогов» – в выпадающем списке выбрать один из двух видов: «FreeIPA или ALD Pro» или «Microsoft AD DS или Samba DC».
- 2) «LDAP сервер» – адрес LDAP/LDAPS-сервера. Указывается в формате: ldap:<адрес LDAP-сервера> или ldaps:<адрес LDAPS-сервера>. Например ldap://ipa.pac-dev-ipa.rbi.local или ldaps://ipa.pac-dev-ipa.rbi.local.

- 3) «LDAP admin DN» – идентификатор пользователя LDAP, имеющего права на просмотр информации о пользователях каталога и группах безопасности каталога:
 - для «FreeIPA» указывается в формате LDAP DN. Например, uid=admin,cn=users,cn=accounts,dc=pac-dev-ipa,dc=rbi,dc=local;
 - для «Microsoft AD DS или Samba DC» указывается в формате: Administrator@pac-dev-win.rbi.local.
- 4) «Пароль LDAP» – пароль пользователя, указанного в поле «LDAP admin DN»;
- 5) «LDAP base DN» – базовый объект каталога, с которого начинается поиск записей.

После изменения настроек LDAP необходимо нажать кнопку «Сохранить».

4.3 Группа настроек «Сопоставление LDAP групп ролям RBI»

Для сопоставления LDAP групп ролям пользователей RBI необходимо установить следующие параметры:

- «LDAP группа администраторов» – выбрать группу из выпадающего списка. Всем пользователям, входящим в эту группу, будет назначена роль администратора;
- «LDAP группа аудиторов» – выбрать группу из выпадающего списка. Всем пользователям, входящим в эту группу, будет назначена роль аудитора;
- «LDAP группа пользователей» – выбрать группу из выпадающего списка. Всем пользователям, входящим в эту группу, будет назначена роль пользователя.

Примечания:

- 1) Для настройки данных параметров должна быть настроена интеграция с LDAP.
- 2) Не рекомендуется использовать встроенные группы безопасности доменов Windows и SambaDC (например, «Users» и «Administrators») для определения ролей пользователей. Необходимо создавать новые отдельные группы.
- 3) Если пользователи RBI имеют учетные записи в разных доменах, то при создании групп необходимо установить область действия «Domain local». При этом, если учетные записи пользователей сгруппированы по принадлежности их к доменам, отличным от домена, в котором развернут «Ankey RBI», то эти группы также должны иметь область действия «Domain local».

4.4 Группа настроек «Интеграция с Kerberos»

Для настройки интеграции Kerberos необходимо установить следующие параметры:

- «Kerberos realm» – имя домена заглавными буквами;
- «Keytab-файл сервиса» – в данном поле необходимо выбрать и загрузить keytab-файл, подготовленный на этапе установки комплекса (см. подраздел 2.3 данного руководства).

4.5 Группа настроек «Учетная запись локального администратора»

Учетные данные локального администратора указывается в процессе установки комплекса (см. подраздел 3.1 данного руководства) и не требуют настройки.

Изменение учетных данных локального администратора требуется только в случае инцидента безопасности.

В таблице 4 представлены требования к имени и паролю локального администратора ПК «Ankey RBI».

Таблица 4 – Требования к имени и паролю УЗ локального администратора ПК «Ankey RBI»

Параметр	Описание
Имя	Требования к имени: – длина имени должна составлять от 2 до 64 символов; – имя может содержать цифры и заглавные/строчные буквы латинского алфавита
Пароль	Требования к паролю: – в пароле должно быть не менее 4 уникальных символов из следующих наборов: цифры, заглавные/строчные буквы латинского алфавита и специальные символы: (пробел) !"#\$%&'()*+,-./:;<=>?@[]^_`{ }~; – длина пароля должна составлять от 8 до 64 символов

Примечание. В ПК «Ankey RBI» предусмотрено ограничение ввода неправильного пароля. Максимальное количество неуспешных попыток аутентификации до блокировки – 4 в течение 15 минут. Следующая попытка авторизации будет возможна по истечении 15 минут после последней неудачной попытки.

4.6 Настройки профиля по умолчанию

Профиль по умолчанию необходим для запуска изолированного приложения и должен быть настроен после создания первого профиля контейнера (см. подраздел 5.3 данного руководства).

Профиль по умолчанию будет использоваться для всех сессий пользователей, за исключением сессий пользователей, для которых напрямую или через группу назначены другие профили (см. подраздел 5.4).

4.7 Группа настроек «Режим высокой доступности брокера»

Параметры для настройки высокой доступности брокера устанавливаются только в случае использования режима высокой доступности (см. подраздел 3.2 данного руководства).

4.8 Группа настроек «Аудит»

Ниже представлено описание параметров, вводимых для настройки аудита:

- «Удалять записи аудита через, дней» – оставить пустым или установить количество дней, через которое все записи в разделе «Аудит» будут удалены. Устанавливаемое значение должно быть равно 365 или больше. Значение меньше 365 установить нельзя;
- «Адрес SIEM syslog сервера» – адрес дополнительного сервера по протоколу UDP (например, udp://10.116.174.53), на который будут продублированы сообщения о событиях из раздела «Аудит». Сообщения формируются в соответствии со стандартом RFC 5424, при этом поле данных сообщения (MSG) содержит информацию в формате JSON. Параметры сообщений не настраиваются.

4.9 Группа настроек «Интеграция с антивирусной программой»

Для настройки интеграции с антивирусной программой необходимо установить значения следующих параметров:

- 1) «Использовать антивирусную программу» – выпадающий список, в котором необходимо выбрать антивирусную программу или отказаться от ее использования:
 - «Нет» – антивирусная программа не будет использоваться;
 - «Kaspersky Scan Engine» – будет использована антивирусная программа Kaspersky Scan Engine;
 - «VR Protect» – будет использована антивирусная программа VR Protect;
 - «Dr. Web» – будет использована антивирусная программа Dr. Web.

Если выбрана любая антивирусная программа, то при скачивании файлов на АРМ пользователя из раздела веб-интерфейса «Мои файлы» будет проведена проверка на наличие вирусов и угроз.

- 2) «Адрес KSE» – адрес используемой антивирусной программы Kaspersky Scan Engine.
- 3) «Точка монтирования файлового ресурса к серверу с антивирусом» – каталог на сервере с антивирусной программой, к которому подключен файловый ресурс. Значение данного параметра необходимо указать, если антивирусная программа и ПК «Ankey RBI» находятся на разных серверах. Если ПК «Ankey RBI» и антивирусная программа находятся на одном сервере, то значение параметра не требуется указывать и в таком случае будет использована точка монтирования по умолчанию.

Примечание. Параметры «Адрес KSE» и «Точка монтирования файлового ресурса к серверу с антивирусом» указываются только в случае, если выбрано использование антивирусной программы Kaspersky Scan Engine в параметре «Использовать антивирус».

- 4) «Максимальное время проверки файла антивирусной программой, сек» – максимальное время антивирусной проверки файла в секундах. Если проверка файла не будет выполнена в течение указанного времени, то проверка файла

будет прервана и будет заблокирована возможность скачивания этого файла.
Допустимый диапазон значений: от 5 до 3600 секунд.

4.10 Группа настроек «Оповещения о критических состояниях»

Для настройки оповещений о критических состояниях системы необходимо установить значения следующих параметров:

- «SMTP-сервер» – адрес сервера, который используется для отправки сообщений электронной почты;
- «Адрес электронной почты, от имени которой будут отправляться уведомления» – адрес электронной почты, от имени которого пользователям будут отправлены уведомления;
- «Получатели оповещений (указываются через запятую)» – адреса электронной почты, на которые будут отправлены уведомления;
- «Выключить все оповещения» – переключатель для включения/выключения всех типов оповещений;
- «Недоступность узла» – переключатель для включения/выключения оповещений о недоступности узла;
- «Недоступность брокера» – переключатель для включения/выключения оповещений о недоступности брокера;
- «Использование ОЗУ узла больше чем на 80%» – переключатель для включения/выключения оповещений о повышенной загрузке ОЗУ узла;
- «Использование ОЗУ брокера больше чем на 80%» – переключатель для включения/выключения оповещений о повышенной загрузке ОЗУ брокера;
- «Использование дискового пространства узла больше чем на 80%» – переключатель для включения/выключения оповещений о переполненности памяти узла;
- «Использование дискового пространства брокера больше чем на 80%» – переключатель для включения/выключения оповещений о переполненности памяти брокера;
- «Загрузка процессора узла больше чем 90% в течение 5 минут» – переключатель для включения/выключения оповещений о загрузке процессора узла;
- «30 дней до истечения одного из сертификатов» – переключатель для включения/выключения оповещений об истечении срока действия одного из сертификатов.

При нажатии на кнопку «Отправить тестовое письмо» будет отправлено тестовое сообщение на адрес электронной почты, указанный в поле «Получатели оповещений».

4.11 Группа настроек «Пользовательские файлы»

В ПК «Ankey RBI» предусмотрены возможности:

- автоматической очистки папок пользователей при неактивности. Для этого необходимо установить количество дней в поле «Удалять пользовательские

- файлы при неактивности пользователя более, дней» или оставить это поле пустым, если очистка не требуется;
- автоматического удаления файлов пользователя по истечении срока хранения. Для этого установить количество дней необходимо в поле «Период хранения пользовательских файлов, дней» или оставить это поле пустым, если автоматическое удаление файлов не требуется.

5 Настройка комплекса для запуска изолированных приложений

После настройки параметров комплекса необходимо перейти к настройке возможности запуска пользователями изолированного приложения. Для этого администратор ПК «Ankey RBI» должен выполнить следующую последовательность действий:

- 1) Добавить узел.
- 2) Загрузить и установить файл с образом изолированного приложения.
- 3) Создать и настроить профиль.
- 4) Назначить профиль по умолчанию.
- 5) Назначить созданный профиль конкретным пользователям или группам пользователей (опционально).

5.1 Добавление узла

Для добавления узла необходимо перейти в раздел веб-интерфейса «Узлы».

Далее необходимо добавить новый узел, согласно представленному ниже алгоритму:

- 1) Нажать кнопку «Добавить узел» в правом верхнем углу веб-интерфейса.
- 2) В диалоговом окне появится список действий и команд, которые необходимо выполнить на сервере, который планируется добавить в качестве узла (подробное описание команд представлено в пункте 7.2.1 данного руководства).
- 3) Заполнить все обязательные поля и нажать кнопку «Ок» (подробное описание полей представлено в пункте 7.2.1 данного руководства).
- 4) В списке узлов появится новый узел в статусе «Требуется подготовка».
- 5) В выпадающем меню напротив ранее созданного узла выбрать кнопку «Подготовить».
- 6) Подтвердить запуск подготовки узла.
- 7) После завершения процесса автоматизированной настройки узла необходимо убедиться, что напротив созданного узла установлен статус «Онлайн».
- 8) Убедиться, что разрешены соединения с узлом. В случае, если соединения запрещены, то необходимо их разрешить, нажав в выпадающем меню кнопку «Разрешить соединения».

5.2 Загрузка и установка файла с образом изолированного приложения

Для загрузки и установки файла необходимо перейти в раздел веб-интерфейса «Мои файлы».

Далее необходимо загрузить файл, согласно представленному ниже алгоритму:

- 1) Нажать на область для загрузки файлов, выбрать необходимый файл с расширением TAR/BZ2 и нажать кнопку «Открыть» или переместить необходимый файл в область для загрузки и нажать кнопку «Загрузить файл».

Примечание. Обратите внимание, что в ПК «Ankey RBI» нельзя установить образ из файла с расширением BZ2, если ранее был установлен такой же образ из файла с расширением TAR.

- 2) Дождаться загрузки файла.
- 3) Нажать напротив загруженного файла в выпадающем меню кнопку «Установить образ».
- 4) Подтвердить установку файла в качестве образа.
- 5) Дождаться успешной установки файла.
- 6) Перейти в раздел «Образы».
- 7) Убедиться, что установленный образ отображается в списке.

5.3 Настройка профиля контейнера по умолчанию

Для настройки профиля контейнера необходимо перейти в раздел веб-интерфейса «Профили».

Далее необходимо добавить новый профиль, выполнив следующие действия:

- 1) Нажать кнопку «Создать профиль».
- 2) Заполнить все обязательные поля:
 - указать имя профиля;
 - в поле «Образы» в выпадающем списке выбрать образ, загруженный на предыдущем этапе.
- 3) Нажать кнопку «Сохранить».
- 4) Перейти в раздел веб-интерфейса «Настройки системы».
- 5) В параметре «Профиль по умолчанию» выбрать ранее созданный профиль.
- 6) Нажать кнопку «Сохранить».

Примечание. При настройке профиля обязательными для заполнения полями являются только имя профиля и «Образы». Все остальные поля являются опциональными. Например, при необходимости возможно запретить пользователям скачивать/загружать файлы или воспроизводить звук из изолированного приложения.

После выполнения всех вышеперечисленных пунктов первоначальная настройка ПК «Ankey RBI» считается завершенной. Пользователи могут запускать изолированные приложения с настройками профиля по умолчанию. При необходимости возможно назначить созданный профиль конкретным пользователям или группам пользователей.

Примечание. Использование профиля по умолчанию для пользователей и групп является опциональным. При необходимости возможно использовать другие профили, отличные от профиля по умолчанию.

5.4 Назначение профиля контейнера УЗ пользователей и групп пользователей служб каталогов

Для назначения профиля контейнера УЗ пользователей или групп пользователей служб каталогов необходимо перейти в раздел веб-интерфейса «Настройки пользователей»

или «Настройки групп». Для проверки работоспособности ПК «Ankey RBI» достаточно назначить профиль одному конкретному пользователю.

Для создания настройки пользователя/группы необходимо выполнить действия, описанные в пункте 7.6.1 данного руководства.

После этого новая настройка пользователя/группы появится в общем списке.

5.5 Завершение работы с веб-интерфейсом

Для завершения работы с веб-интерфейсом администратору необходимо:

- 1) Нажать кнопку «Выход из системы».
- 2) Закрыть веб-браузер или соответствующую вкладку.

ПК «Ankey RBI» предусматривает ограничение на максимальное время существования сессии (по умолчанию – 24 часа), после чего сессия в веб-интерфейсе будет закрыта.

6 Лицензирование и активация ПК «Ankey RBI»

Для использования функциональных возможностей ПК «Ankey RBI» после установки комплекса должна быть активирована лицензия на право использования продукта. ПК «Ankey RBI» поддерживает ограниченный режим использования без лицензии. Для получения информации о предусмотренных типах лицензий необходимо обратиться в отдел поддержки компании-вендора.

В таблице 5 представлена информация о функциональных возможностях и ограничениях, которые предусмотрены в режиме использования комплекса без лицензии.

Таблица 5 – Параметры лицензии

Параметр	Без лицензии
Аутентификация в ПК «Ankey RBI» по смарт-картам	Да
Интеграции со службами каталогов по протоколу Kerberos	Да
Интеграция с антивирусным ПО	Нет
Количество одновременно запущенных сессий	3
Срок действия базовой поддержки	–
Срок действия гарантийной поддержки	–
Срок действия расширенной поддержки	–
Срок действия лицензии	–
Функция авторизации браузера в контейнер на Proxy с помощью Kerberos	Да
Функция использования смарт-карт в контейнерах	Да

Возможны три варианта действий с лицензиями комплекса:

- 1) Активация новой лицензии – легальный переход ПО из состояния ограничения функциональных возможностей в состояние использования полнофункциональной версии комплекса в течение срока действия лицензии. Активация лицензии производится один раз на каждый брокер.
- 2) Реактивация лицензии – повторная активация ПО, которая может потребоваться, например, при переустановке брокера на новый сервер. При реактивации происходит процесс отзыва лицензии с сервера, на которой ранее была сделана активация этой лицензии. На месте, где лицензия была отозвана, ПО перестает быть активированным, а функциональные возможности будут ограничены. На новом сервере ключ лицензии при этом будет заменен на новый.
- 3) Обновление лицензии – изменение параметров лицензии, например, добавление в текущую лицензию новых функциональных возможностей (расширенная техническая поддержка и т. д.). Ключ лицензии не изменяется. Обновление происходит автоматически, а внесение изменений в условия лицензии осуществляют администраторы сервера лицензирования.

В веб-интерфейсе ПК «Ankey RBI» предусмотрена кнопка  для перехода в раздел с данными о лицензии и техподдержке, а также цветовой индикатор для оценки состояния лицензии:

- зеленый цвет индикатора – лицензия активирована и до окончания срока действия лицензии осталось более 30 дней;
- желтый цвет индикатора – до окончания срока действия лицензии или технической поддержки осталось менее 30 дней;
- красный цвет индикатора – лицензия отсутствует, срок действия лицензии истек или лицензия активирована, но еще не начала действовать.

Лицензирование комплекса осуществляется в режиме онлайн после установки и первоначальной настройки.

6.1 Активация лицензии комплекса

Активация лицензии комплекса осуществляется при наличии подключения к сети Интернет и возможности подключения к серверу лицензирования.

6.1.1 Особенности активации лицензии при использовании режима высокой доступности

В случае, если ПК установлен в режиме высокой доступности (см. подраздел 5.2 данного руководства), то активировать лицензию необходимо на каждом брокере отдельно.

Для каждого из брокеров будут предоставлены отдельные лицензионные ключи:

- основной – для активации основного брокера;
- дополнительный – для активации дополнительного брокера (в режиме высокой доступности). Данный ключ, в отличие от основного, содержит параметр «is_additional_ha_license».

Активация основного брокера осуществляется только основным ключом. При попытке активировать дополнительным ключом основной брокер будет получена ошибка и заблокирована кнопка «Получить ключ активации».

6.1.2 Порядок действий при активации лицензии

Для активации лицензии комплекса необходимо:

- 1) Перейти на страницу «Брокеры».
- 2) Напротив выбранного брокера выбрать в выпадающем меню кнопку «Ввести лицензию».
- 3) В открывшемся окне ввести ключ лицензии и нажать кнопку «Проверить» (рис. 11).

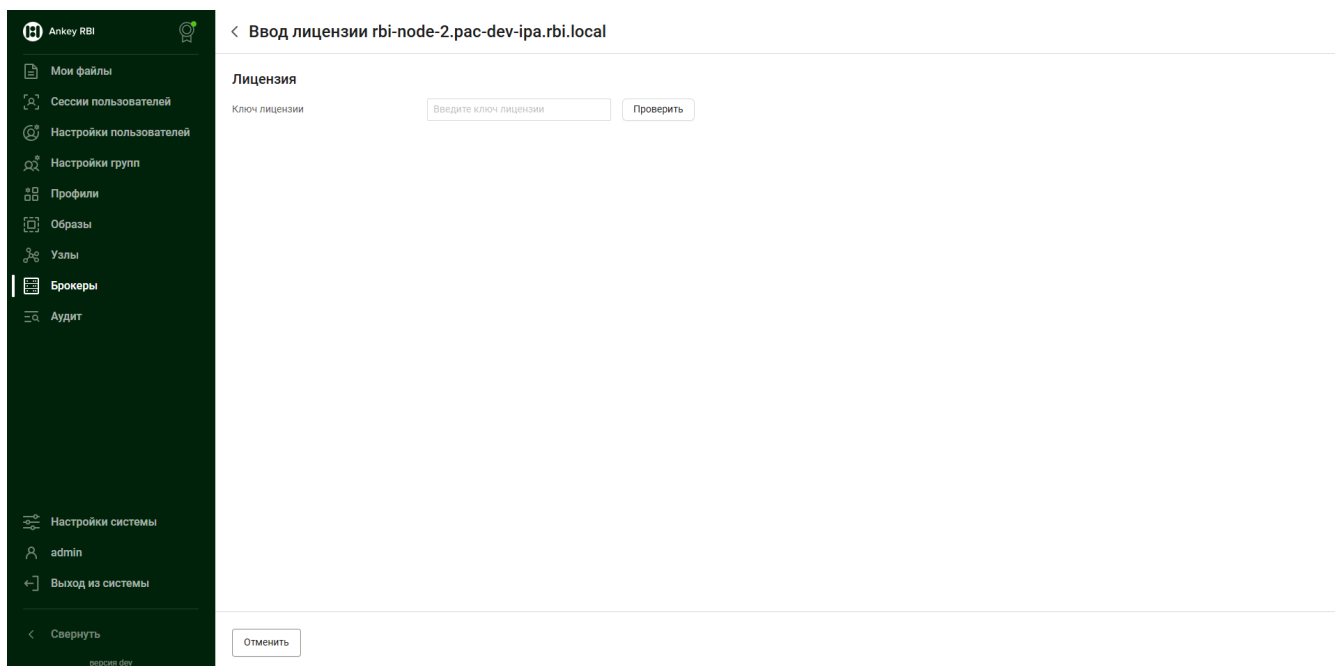


Рисунок 11 – Окно веб-интерфейса для ввода ключа лицензии

- 4) После успешной проверки на странице будут отображены параметры, которые доступны для данной лицензии.
- 5) В поле «Email» необходимо ввести адрес электронной почты для отправки ключа активации.
- 6) Нажать кнопку «Получить ключ активации». Далее, в зависимости от типа лицензии, ключ активации будет отправлен на указанный адрес электронной почты или автоматически заполнен в поле для ввода ключа активации на странице «Лицензирование».

Если ключ был отправлен на адрес электронной почты, то необходимо скопировать из полученного сообщения ключ активации и на странице «Лицензирование» установить значение ключа в соответствующее поле.

- 7) Нажать кнопку «Активировать лицензию».
- 8) Дождаться сообщения об успешной активации лицензии (рис. 12).

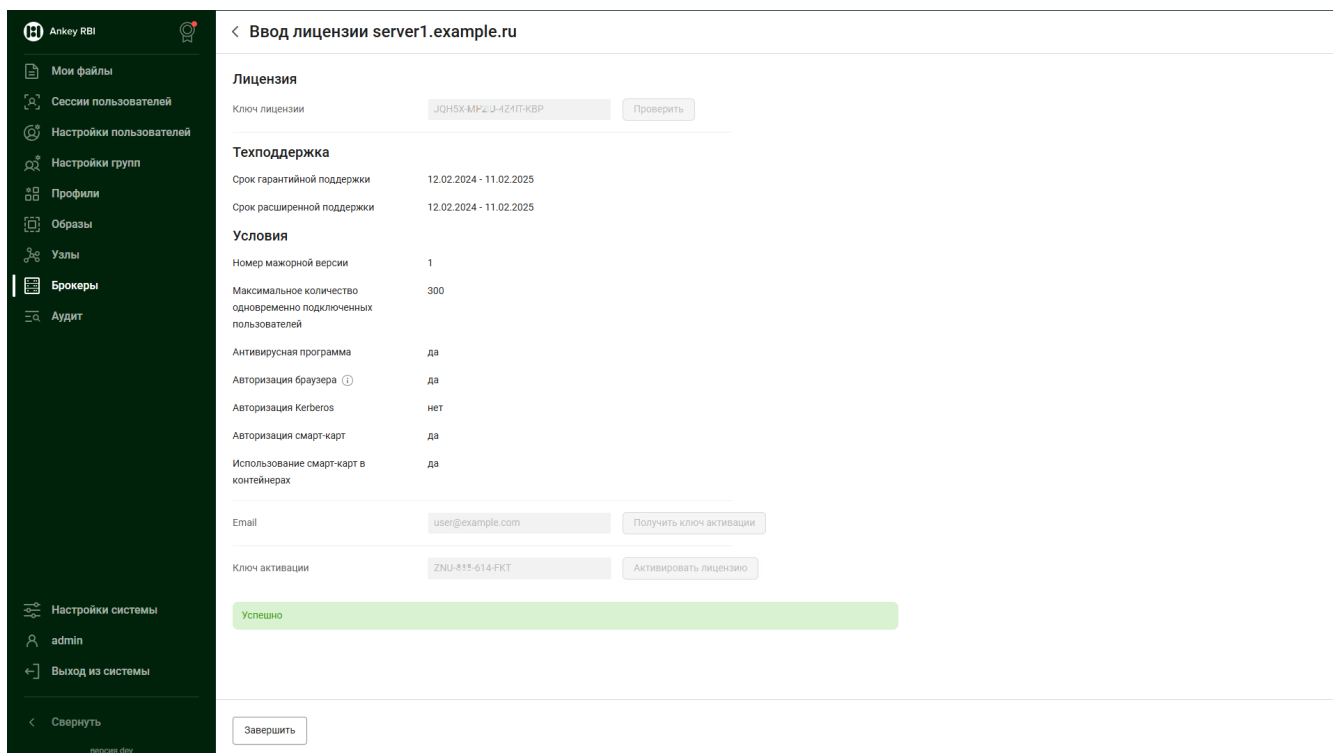


Рисунок 12 – Окно веб-интерфейса с сообщением об успешной активации лицензии

9) Нажать кнопку «Завершить».

После успешной активации лицензии на странице появится надпись «Лицензия в порядке» и будут отображаться параметры лицензии (см. рис. 12):

- «Серийный номер» – серийный номер лицензии;
- «Срок действия лицензии»;
- «Срок гарантийной поддержки»;
- «Срок расширенной поддержки»;
- «Номер мажорной версии» – ограничение лицензии для определенной версии ПК;
- «Максимальное количество одновременно подключенных пользователей» – максимальное количество пользователей, которые могут одновременно подключиться к изолированному приложению;
- «Антивирусная программа» – наличие возможности интеграции с антивирусной программой;
- «Авторизация браузера» – наличие возможности авторизации браузера в контейнере на прокси с использованием протокола Kerberos;
- «Авторизация Kerberos» – наличие возможности авторизации с использованием протокола Kerberos в контейнере;
- «Авторизация смарт-карт» – наличие возможности авторизации с помощью смарт-карт;
- «Использование смарт-карт в контейнерах» – наличие возможности использования смарт-карт в контейнере.

6.2 Активация лицензии комплекса при подключении к сети Интернет через прокси-сервер

Если активация лицензии комплекса выполняется при подключении к сети Интернет через прокси-сервер, то необходимо выполнить следующие действия:

- 1) Выполнить команду на активном брокере:

```
systemctl edit rbi-license
```

- 2) В открывшейся форме редактирования добавить и сохранить следующие данные в секцию «Service» (если ее нет, то добавить):

Внимание! Данные необходимо добавить до строки «Lines below this comment will be discarded».

```
Environment="RBI_LICENSE_PROXY=http://<user>:<password>@<FQDN прокси-сервера>:<port>"
```

Примечание. Параметры «user» и «password» являются опциональными.

- 3) Перезагрузить сервис лицензирования, выполнив следующую команду:

```
sudo systemctl restart rbi-license
```

7 Функциональные возможности комплекса

7.1 Общее описание веб-интерфейса ПК «Ankey RBl»

Управление ПК «Ankey RBl» происходит с помощью веб-интерфейса комплекса.

Подключение к веб-интерфейсу осуществляется с помощью любого поддерживаемого веб-браузера.

По умолчанию в браузере доступна только авторизация локального администратора. Чтобы использовать в браузере Kerberos-аутентификацию необходимо добавить параметры запуска.

Ниже представлен пример настройки параметров запуска браузера для РЕД ОС:

- 1) Навести курсор на ярлык браузера на панели задач или на рабочем столе и нажать правую клавишу мыши.
- 2) В контекстном меню выбрать «Параметры», если ярлык находится на панели задач, «Свойства», если ярлык на рабочем столе.
- 3) В поле «Команда» после указания пути к запускаемому файлу дописать следующую команду:

```
--auth-server-allowlist=\\*.<доменное имя>
```

Пример полной записи команды:

```
/usr/bin/chromium-browser  
--auth-server-allowlist=\\*.<доменное имя> %U
```

Для доступа к веб-интерфейсу необходимо ввести в адресную строку веб-браузера IP-адрес установленного брокера. После этого откроется страница авторизации (рис. 13), на которой требуется авторизоваться одним из двух способов:

- ввести имя пользователя и пароль локального администратора и нажать кнопку «Подключиться». Данный способ авторизации рекомендуется использовать только во время первоначальной настройки комплекса или в случаях, связанных с инцидентами безопасности или когда другой способ авторизации по какой-либо причине недоступен;
- доменный вход. Рекомендуемый способ авторизации, при котором пользователю после авторизации будут доступны только разделы, соответствующие его роли в системе.



Добро пожаловать в RBI

Имя пользователя:

Пароль:



Подключиться

или

Доменный вход: admin

© 2022-2025 Remote Browser Isolation. Все права
защищены. Разработка системы — GIS

Рисунок 13 – Авторизация в ПК «Ankey RBI»

Все доступные разделы, в зависимости от роли авторизованного пользователя (см. подраздел 1.4 данного руководства), отображаются в левой боковой панели меню. При нажатии на кнопку «Свернуть» панель меню сворачивается и отображаются только иконки разделов. Чтобы развернуть меню необходимо нажать на кнопку .

Выход из сессии в веб-интерфейсе осуществляется при нажатии на кнопку «Выход из системы».

В правой части веб-интерфейса отображается основное рабочее поле.

Справа от логотипа ПК «Ankey RBI» отображается кнопка  для перехода в раздел с данными о лицензии и техподдержке. В данном разделе отображается только информация о состоянии лицензии, доступности техподдержки для каждого брокера (рис. 14). Управление лицензиями осуществляется в разделе «Брокеры».

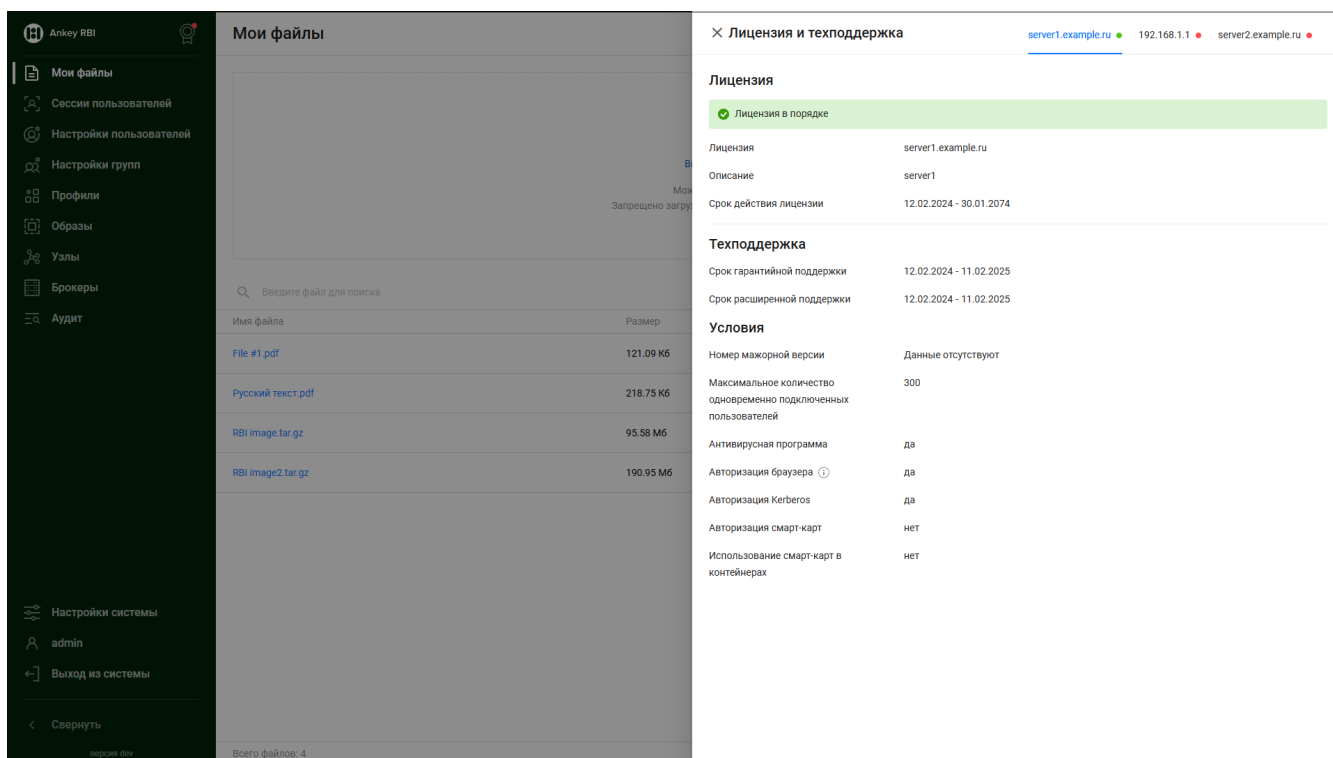


Рисунок 14 – Состояние лицензии

Список всех разделов веб-интерфейса и их описание представлен в таблице 6.

Таблица 6 – Описание разделов веб-интерфейса

Название раздела	Описание
Мои файлы	Раздел для управления файлами пользователей и загружаемыми образами. Данный раздел доступен для пользователей с любой ролью
Сессии пользователей	Раздел для управления сессиями пользователей. Пользователи с ролями «Аудитор» и «Пользователь» могут видеть только свои текущие сессии. Пользователи с ролью «Администратор» видят сессии всех пользователей

Название раздела	Описание
	(активные и архивные), а также могут просматривать и управлять сессиями в режиме «Теневая сессия»
Настройки пользователей	Раздел для привязки профиля к одному конкретному пользователю из службы каталогов. Данный раздел доступен только пользователям с ролью «Администратор»
Настройки групп	Раздел для привязки профиля к группе пользователей из службы каталогов. Данный раздел доступен только пользователям с ролью «Администратор»
Профили	Раздел для создания и управления профилями. Данный раздел доступен только пользователям с ролью «Администратор»
Образы	В данном разделе отображается список образов, готовых к использованию. Данный раздел доступен только пользователям с ролью «Администратор»
Узлы	Раздел для управления узлами. Данный раздел доступен только пользователям с ролью «Администратор»
Брокеры	В данном разделе отображается список брокеров. Данный раздел доступен только пользователям с ролью «Администратор»
Аудит	В данном разделе отображается информация о событиях системы. Данный раздел доступен пользователям с ролью «Администратор» и «Аудитор»
Настройки системы	Раздел для управления настройками ПК «Ankey RBI». Данный раздел доступен только пользователям с ролью «Администратор»

7.2 Управление узлами

В разделе «Узлы» отображается список всех узлов, на которых запускаются контейнеры.

По умолчанию страница с узлами содержит пустой список, в котором будут отображаться все узлы, добавленные администратором. Для созданных узлов отображается следующая информация:

- 1) «Адрес» – FQDN сервера, на котором запущен узел. Под адресом отображается текстовая информация об узле, которую администратор вносит вручную.
- 2) «Новые соединения» – признак, определяющий разрешение на создание контейнеров на узле. Устанавливается администратором системы:
 - «Принимает» – узел доступен для создания новых контейнеров;
 - «Отклоняет» – узел недоступен для создания новых контейнеров.
- 3) «Статус» – текущее состояние узла. Предусмотрены следующие статусы:
 - «Онлайн» – узел активен и присылает отчеты об активности, может быть использован брокером для запуска контейнеров;
 - «Офлайн» – узел не присылает отчеты об активности, не может быть использован брокером для запуска контейнеров;
 - «Требуется подготовка» – узел создан, но требует запуска процесса автоматизированной настройки для начала работы.

- 4) «ЦП» – отображение текущего процента загрузки центрального процессора.
- 5) «Оперативная память» – отображение текущего процента загрузки оперативной памяти.
- 6) «Сетевой адаптер» – отображение текущего процента загрузки сетевого интерфейса узла.
- 7) «Файловое хранилище» – отображение текущего процента заполнения файлового хранилища.
- 8) «Контейнеры»:
 - «Загруженные» – общее количество запущенных контейнеров на данном узле;
 - «Подключенные» – количество контейнеров, к которым в данный момент подключены пользователи.

Информация о загрузке центрального процессора, оперативной памяти, сетевого адаптера, файлового хранилища и контейнерах может быть отображена в виде шкал (рис. 15) или графиков (рис. 16). Для выбора необходимого типа отображения следует выбрать соответствующую вкладку.

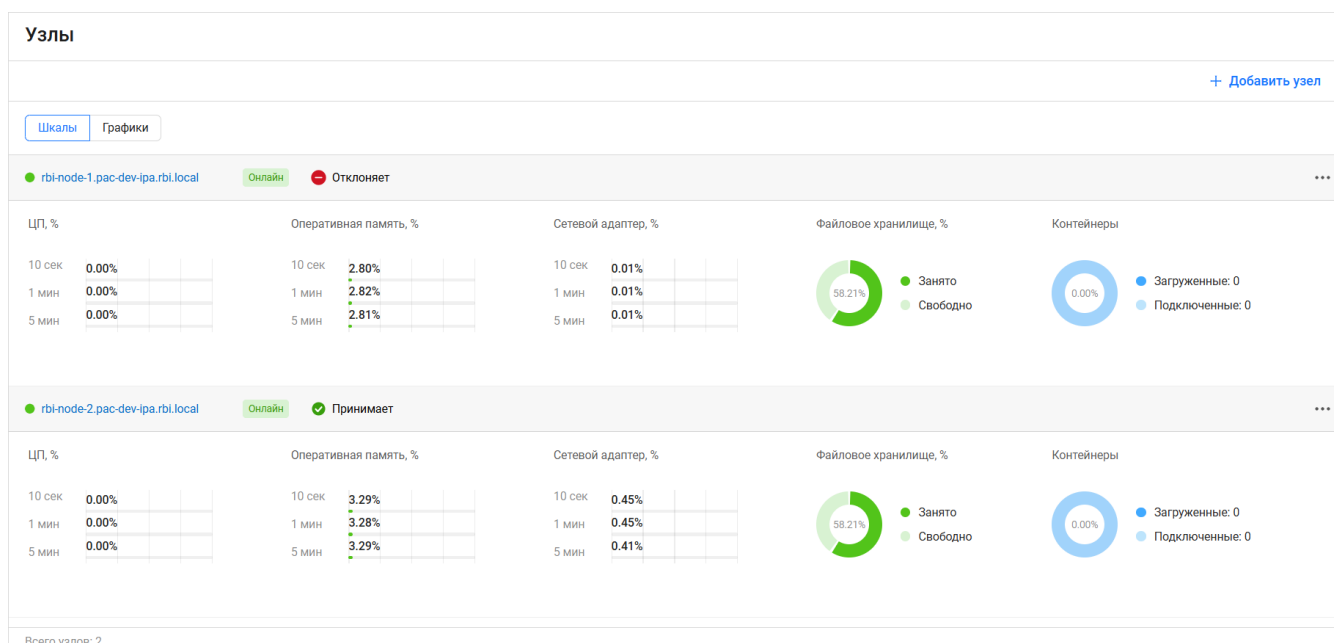


Рисунок 15 – Раздел «Узлы» веб-интерфейса ПК «Ankey RBI» с отображением шкал

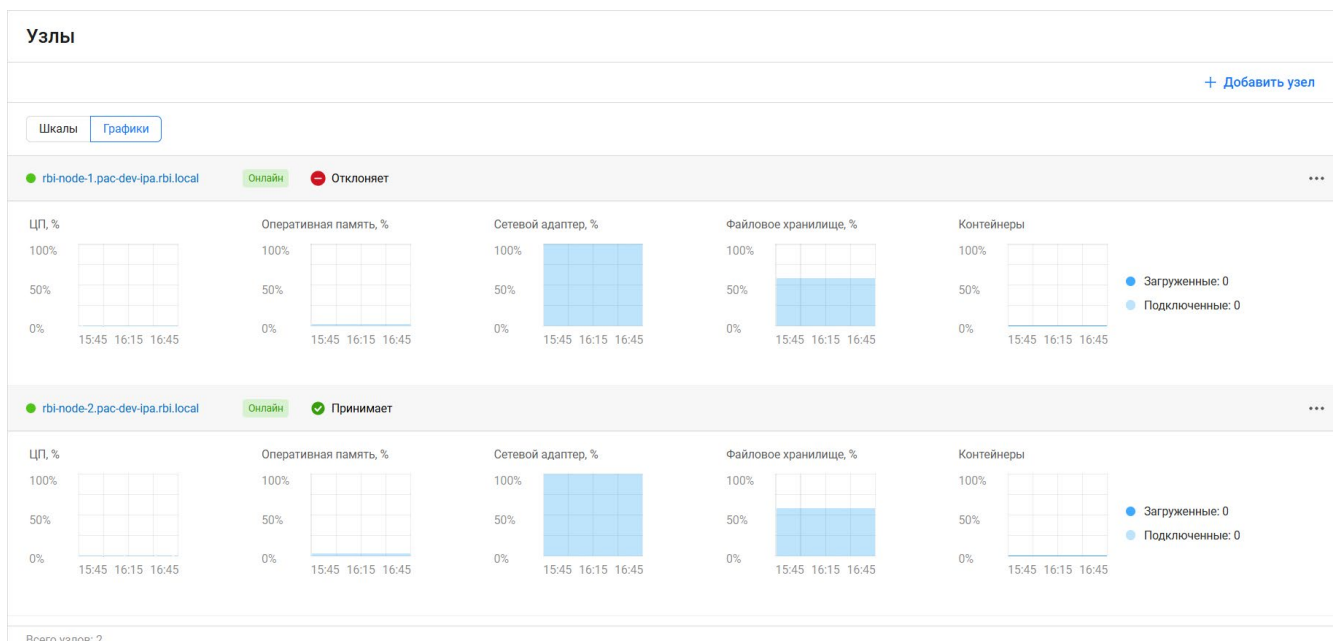


Рисунок 16 – Раздел «Узлы» веб-интерфейса ПК «Ankey RBI» с отображением графиков

7.2.1 Добавление узлов

Для добавления нового узла, необходимо нажать кнопку «Добавить узел». После этого откроется окно добавления узла (рис. 17).

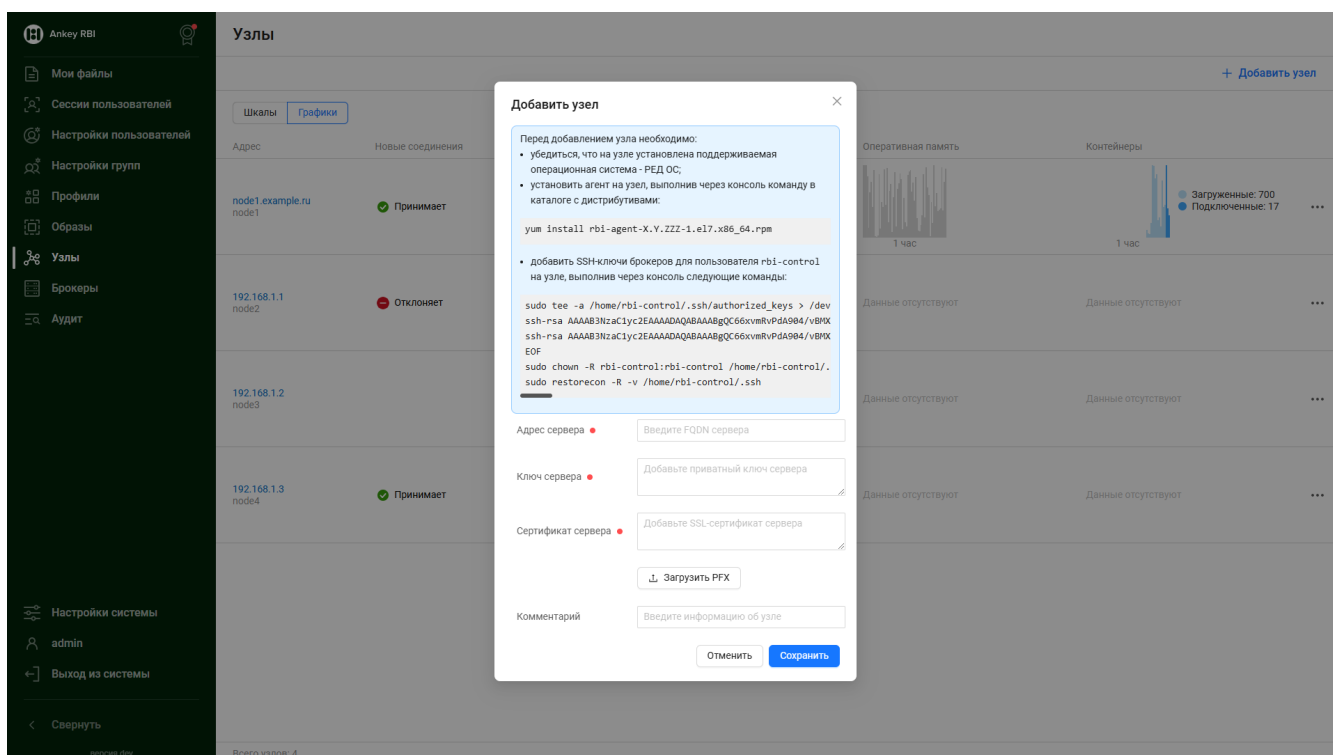


Рисунок 17 – Окно добавление узла

Перед добавлением нового узла необходимо выполнить предварительные настройки:

- убедиться, что на узле установлена поддерживаемая операционная система – РЕД ОС;

- установить агент на узел, выполнив через консоль команду в каталоге с дистрибутивами:

```
dnf install rbi-agent-X.Y.ZZZ-1.el7.x86_64.rpm
```

- добавить SSH-ключи брокеров для пользователя rbi-control на узле, выполнив через консоль следующие команды:

```
sudo tee -a /home/rbi-control/.ssh/authorized_keys \> /dev/null << EOF
ssh-rsa <значение ключа>= rbi-server@ rbi-server-02 EOF
sudo chown -R rbi-control: rbi-control /home/ rbi-control/.ssh
sudo restorecon -R -v /home/rbi-control/.ssh
```

В окне создания узла необходимо заполнить следующие поля:

- «Адрес сервера» (обязательное поле) – FQDN сервера, на котором будет запущен узел;
- «Ключ сервера» (обязательное поле) – приватный SSL-ключ сервера, на котором будет запущен узел;
- «Сертификат сервера» (обязательное поле) – приватный SSL-сертификат сервера, на котором будет запущен узел;
- «Комментарий» – текстовая информация об узле, которая будет отображаться в поле «Описание».

После заполнения обязательных полей необходимо нажать кнопку «Ок», после чего узел отобразится в списке.

Примечание. Обратите внимание, что если не выполнены предварительные настройки, то создание узла невозможно будет завершить.

С созданными узлами возможно проводить следующие действия:

- редактирование. Для этого необходимо напротив выбранного узла нажать кнопку «Изменить». Для изменения доступны все поля, которые были доступны при создании;
- удаление. Для этого необходимо напротив выбранного узла в выпадающем меню выбрать кнопку «Удалить».

Далее необходимо подготовить узел к использованию.

7.2.2 Подготовка узла к использованию

После создания узел находится в статусе «Требуется подготовка». Необходимо настроить узел перед запуском, выполнив следующие действия:

- 1) Напротив выбранного узла со статусом «Требуется подготовка», в выпадающем меню нажать кнопку «Подготовить».
- 2) В появившемся окне появится сообщение для подтверждения подготовки узла к использованию. Необходимо нажать кнопку «Да», чтобы продолжить настройку.

После этого появится иконка загрузки. Установка занимает около минуты. После успешной настройки статус узла изменится с «Требуется подготовка» на «Онлайн».

Внимание! Необходимо запустить повторную настройку узла, если:

- был изменен адрес, ключ или сертификат сервера;
- было обновление компонентов ПК «Ankey RBI»;
- были изменения системных настроек брокера: «Адрес RBI-сервера» или/и «Корневые сертификаты».

7.2.3 Возможность запуска новых контейнеров на узле

В веб-интерфейсе администратор имеет возможность запретить создание новых контейнеров на узле, например, чтобы провести обслуживание (перезагрузка, обновление ПО и др.) на сервере.

Чтобы изменить возможность запуска новых контейнеров на узле необходимо:

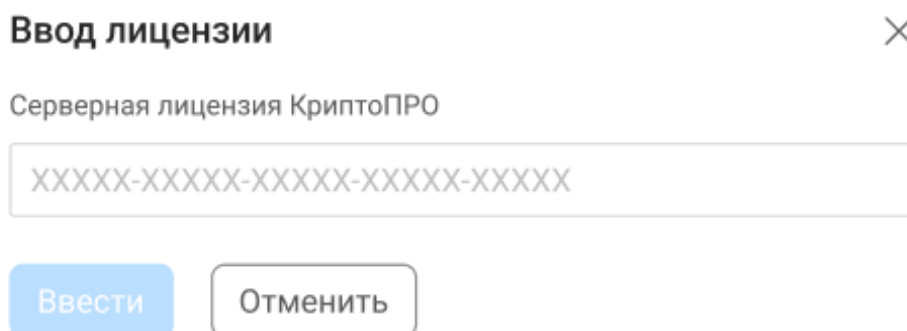
- 1) Напротив выбранного узла (со статусом «Онлайн» или «Офлайн») в выпадающем меню выбрать кнопку «Разрешить/Запретить соединения».
- 2) Во всплывающем окне появится сообщение для подтверждения действия. Необходимо нажать кнопку «Да», чтобы продолжить.

7.2.4 Установка лицензию на право использования СКЗИ «КриптоПро CSP» на узел

Для реализации возможности авторизоваться на государственных порталах, использующих двухстороннюю аутентификацию по TLS на основе ГОСТ (mutual TLS, mTLS) на каждом узле должна быть установлена лицензия на право использования СКЗИ «КриптоПро CSP» версии 5.0 на сервере.

Чтобы установить лицензию на узел необходимо:

- 1) Напротив выбранного узла (со статусом «Онлайн» или «Офлайн») в выпадающем меню выбрать кнопку «Ввести лицензию CSP».
- 2) Во всплывающем окне в поле «Серверная лицензия КриптоПро» ввести актуальный и валидный номер лицензии на право использования СКЗИ «КриптоПро CSP» версии 5.0 на сервере (рис. 18).



Ввод лицензии ×

Серверная лицензия КриптоПРО

XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX

Ввести **Отменить**

Рисунок 18 – Окно добавления серверная лицензии

- 3) Далее подтвердить действие, нажав кнопку «Ввести».

7.3 Работа с файлами

Раздел «Мои файлы» (рис. 19) служит для управления пользовательскими файлами, в том числе файлами с образами, из которых в дальнейшем устанавливаются образы контейнеров. В разделе «Мои файлы» веб-интерфейса ПК «Ankey RBI» отображается для каждого пользователя комплекса собственная область с файлами без возможности просмотра файлов других пользователей, а также обмена этими файлами.

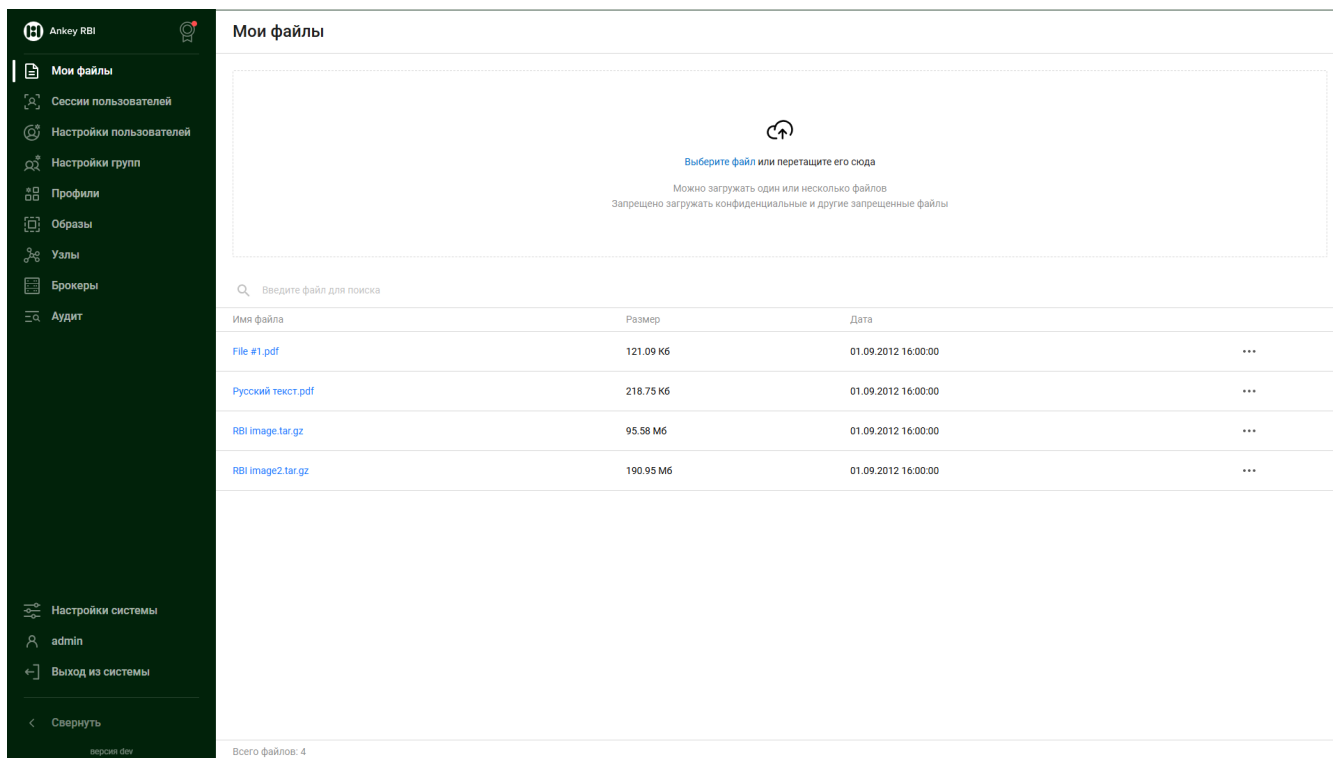


Рисунок 19 – Раздел «Мои файлы» веб-интерфейса ПК «Ankey RBI»

По умолчанию страница с файлами содержит пустой список, в котором будут отображаться все файлы, которые пользователь загрузил. О загруженных файлах отображается следующая информация:

- «Имя файла» – название и расширение загружаемого файла, которое совпадает с названием файла на АРМ пользователя;
- «Размер» – исходный размер загруженного файла. Отображается в байт/Гбайт;
- «Дата» – время и дата загрузки файла. Отображается в формате ДД-ММ-ГГГГ, чч:мм:сс.

С файлами возможно выполнить следующие действия:

- загрузка (подробное описание загрузки файлов представлено в пункте 7.3.1 данного руководства);
- скачивание – загруженные ранее файлы возможно скачать, нажав кнопку «Скачать» напротив необходимого файла;
- установка образа из файла (подробное описание установки образов из файлов представлено в пункте 7.3.2 данного руководства). Доступно только для файлов

- с расширением TAR, TAR.GZ, TAR.BZ2 и только пользователям с ролью администратора;
- удаление – загруженные ранее файлы можно удалить с сервера. Для этого необходимо напротив удаляемого файла в выпадающем меню нажать кнопку «Удалить», а в случае удаления нескольких – установить флаг напротив наименований удаляемых файлов и в отобразившейся строке с кнопками выбора операций выбрать пункт «Удалить»;
 - сортировка – загруженные файлы можно сортировать. По умолчанию список файлов отсортирован в порядке убывания даты и времени загрузки. Чтобы задать другой тип сортировки необходимо выбрать заголовок требуемого столбца таблицы (например, «Имя файла» или «Размер»). В заголовке отобразится знак , сортировка будет выполнена по убыванию значений выбранного столбца. Для изменения направления сортировки необходимо повторно выбрать заголовок столбца. В заголовке отобразится знак .

7.3.1 Загрузка файлов

В комплекс допускается загружать файлы с любым расширением, если они соответствуют следующим требованиям:

- в названии файла допустимо использование специальных символов, пробелов, цифр, букв кириллицы и латинского алфавита;
- название файла не может начинаться с символа точки «.» или с пробела;
- рекомендованная длина названия должна составлять не более 123 символов;
- название и расширение файла должно быть уникальным. При загрузке файла с названием и расширением, уже существующим в системе, ранее загруженный файл будет перезаписан на новый;
- одновременно возможно загружать не более 10 файлов;
- размер загружаемых файлов зависит только от объема свободной памяти на носителе информации (физическом или виртуальном) для хранения файлов пользователей.

Файл возможно загрузить, нажав на область для загрузки файлов или перенести файл в область для загрузки, после чего нажать кнопку «Загрузить файл». После загрузки файла отображается индикатор процесса загрузки файла с указанием его имени и расширения.

Успешно загруженный файл отобразится в списке файлов. Пользователи могут скачивать, удалять и устанавливать загруженные файлы (установка файлов разрешена только пользователям с ролью «Администратор»).

Если при загрузке произошла ошибка, то на экране появится соответствующий текст ошибки.

7.3.2 Установка образа изолированного приложения

Для установки образа изолированного приложения необходимо выполнить следующие действия:

- 1) Загрузить в раздел «Мои файлы» файл формата TAR/BZ2, который содержит образ изолированного приложения.

Примечание. Обратите внимание, что в ПК «Ankey RBI» нельзя установить образ из файла с расширением BZ2, если ранее был установлен образ из файла с расширением TAR.

- 2) Нажать напротив загруженного файла в выпадающем списке кнопку «Установить образ».
- 3) В появившемся диалоговом окне принять предложение по установке файла в качестве образа контейнера.

Далее появится индикатор загрузки. После успешной установки будет появиться сообщение «Файл {название_файла} успешно загружен как образ», а сам образ добавится в списке образов в разделе «Работа с образами».

Из одного файла возможно создать только один образ.

В ПК «Ankey RBI» предусмотрено автоматическое обновление образов с последующей автоматической установкой. Данная функциональная возможность включается при настройке профилей (см. пункт 7.5.1 данного руководства). Описание процесса автоматического обновления образа представлено пункте 7.4.1 данного руководства.

7.4 Работа с образами

В разделе «Образы» (рис. 20) отображается список всех установленных образов, которые допускается использовать для запуска изолированных приложений. Образы устанавливаются через раздел «Мои файлы».

Ankey RBI Мои файлы Сессии пользователей Настройки пользователей Настройки групп Профили Образы Узлы Брокеры Аудит Настройки системы admin Выход из системы Свернуть	Образы				
	ID образа	Описание	Из файла	Размер	Дата
	9c968c6e	Yandex browser 23.7.0	RBI image.tar.gz	30.64 M6	01.09.2012 16:00:00
	9c968c6e	Yandex browser 23.7.1	RBI (2) image.tar.gz	117.42 M6	05.09.2012 16:00:00
	Всего образов: 2				

Рисунок 20 – Раздел «Образы» веб-интерфейса ПК «Ankey RBI»

По умолчанию страница с образами содержит пустой список, в котором будут отображаться все установленные образы. О каждом образе отображается следующая информация:

- «ID образа» – идентификатор (тип string) образа, который генерируется автоматически при установке. Идентификатор состоит из набора букв, символов и цифр, который представляют собой захешированные атрибуты файла;
- «Описание» – текстовая информация об образе, которую администратор вносит вручную. В описании образа рекомендуется указывать название ПО и его версию;
- «Из файла» – название файла, из которого был установлен образ;
- «Размер» – размер исходного файла, на основе которого был установлен образ;
- «Дата» – время и дата создания образа. Отображается в формате ДД-ММ-ГГГГ, чч:мм:сс.

С установленными образами возможно проводить следующие действия:

- изменение описания. Для этого необходимо нажать кнопку «Изменить»;
- удаление. Установленные образы возможно удалить с сервера, нажав напротив необходимого образа в выпадающем списке кнопку «Удалить».

Примечание. Обратите внимание, что нельзя удалять образ, если он уже используется хотя бы в одном профиле.

Привязка профиля к пользователю осуществляется через раздел «Профили».

7.4.1 Автоматическое обновление образов с последующей автоматической установкой

Брокер каждый час проверяет наличие новых образов в выбранных линейках обновлений всех профилей. При наличии новой версии образа на сервере обновления производителя, он будет автоматически загружен и установлен, а также использован во всех профилях, в которых включено автоматическое обновление и выбрана соответствующая линейка обновлений.

7.4.2 Обновление образов при подключении к сети Интернет через прокси-сервер

Если необходимо настроить обновление образов при подключении к сети Интернет через прокси-сервер, то требуется выполнить следующие действия:

- 1) Выполнить команду на активном брокере:

```
systemctl edit rbi-server
```

- 2) В открывшейся форме редактирования добавить и сохранить следующие данные в секцию «Service» (если ее нет, то добавить):

Внимание! Данные необходимо добавить до строки «Lines below this comment will be discarded».

```
Environment="HTTPS_PROXY=https://<user>:<password>@<FQDN прокси-сервер>:<port>"
```

Примечание. Параметры «user» и «password» являются опциональными.

- 3) Перезагрузить брокер, выполнив следующую команду:

```
sudo systemctl restart rbi-server
```

- 4) Включить автоматическое обновление образов (см. пункт 7.4.1 настоящего руководства).

7.5 Настройка профилей

Раздел «Профили» (рис. 21) предназначен для создания и управления профилями. Профиль содержит настройки и ограничения для контейнеров, а также образ, из которого контейнер должен запускаться. Профиль может быть назначен группе или конкретному пользователю через разделы «Настройка групп» и «Настройка пользователей». В разделе «Настройки системы» необходимо выбрать профиль, который станет профилем пользователя по умолчанию, и будет использован в случае, если у пользователя нет профиля, определенного через разделы «Настройки групп» и «Настройки пользователей».

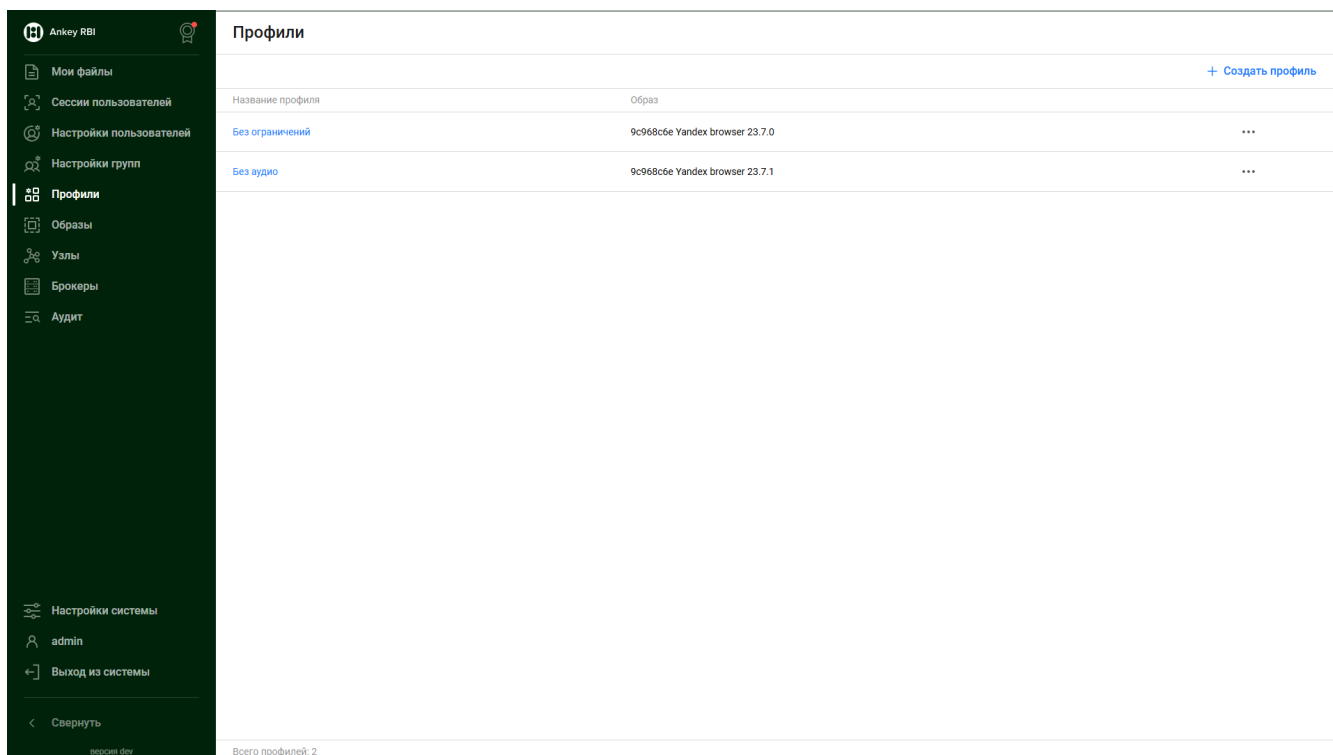


Рисунок 21 – Раздел «Профили» веб-интерфейса ПК «Ankey RBI»

По умолчанию страница содержит пустой список, в котором будут отображаться все профили, которые добавит администратор. О созданных профилях отображается следующая информация:

- «Название контейнера»;
- «Образ» – идентификатор (ID образа) и описание образа (если было заполнено), на основе которого была создан профиль.

7.5.1 Создание профиля

Для создания нового профиля, необходимо нажать кнопку «Создать профиль» в правом верхнем углу. После этого откроется окно создания профиля (рис. 22), в котором надо заполнить следующие поля:

- 1) «Идентификатор профиля» – уникальный идентификатор, который генерируется автоматически при создании профиля. Данный параметр нельзя указать вручную и нельзя изменить. При нажатии кнопки  идентификатор будет скопирован в буфер обмена.
- 2) «Название профиля» (обязательное поле).
- 3) «Образ» (обязательное поле) – в выпадающем списке необходимо выбрать образ, из которого будет запущено изолированное приложение при использовании данного профиля.
- 4) «Автоматически обновлять образ» – переключатель, отвечающий за включение/отключение возможности автоматического обновления образов до последней актуальной (по дате) версии с сервера обновлений GIS.

- 5) «Линейка обновлений» – поле, в котором выбирается идентификатор варианта сборки образа изолированного приложения с сервера обновлений GIS. Данное поле активно только при включенной возможности автоматического обновления образов.

Примечание. При включенном автоматическом обновлении образа поле «Образ» становится неактивным и отображает имя текущего образа, который используется в профиле.

- 6) «Время бездействия пользователя до запуска скринсейвера, мин» – время бездействия пользователя (в минутах), по истечении которого активируется специальная программа по сохранению состояния экрана (скринсейвер). Диапазон допустимых значений: от 1 мин до 1440 мин. Значение параметра должно быть меньше или равно значению, указанному в параметре «Время бездействия пользователя до отключения сессии, мин».
- 7) «Время бездействия пользователя до отключения сессии, мин» – время бездействия пользователя (в минутах), по истечении которого сессия отключается. В веб-интерфейсе в разделе «Сессии пользователей» сессия будет отображаться со статусом «Не подключена», а пользователь получит сообщение «Сессия была отключена». Диапазон допустимых значений: от 1 мин до 1440 мин. Значение параметра должно быть больше или равно значению, указанному в параметре «Время бездействия пользователя до запуска скринсейвера, мин».
- 8) «Время до закрытия сессии после ее отключения, мин» — время в минутах после отключения клиента, по истечении которого контейнер удаляется. Например, установлено значение 2 минуты. Пользователь закрыл клиент, после чего начинается отсчет времени:
- если пользователь в течение 2 минут снова подключится к изолированному приложению, то увидит его в том же состоянии, которое было перед отключением;
 - если пользователь в течение 2 минут не подключится к изолированному приложению, то контейнер удаляется. При следующем запуске браузера будет создан новый контейнер.

Внимание! Рекомендуется всегда устанавливать значения параметров «Время бездействия пользователя до запуска скринсейвера, мин», «Время бездействия пользователя до отключения сессии, мин» и «Время до закрытия сессии после ее отключения, мин». Если значения параметров не будут установлены, то в таком случае ресурсы сервера или сети могут быть использованы неэффективно.

Также обратите внимание, что скринсейвер не будет запущен, если в изолированном приложении открыт и воспроизводится видео или аудио файл.

- 9) «Максимально доступная память, Мб» – максимально доступная оперативная память для контейнера. Рекомендуется устанавливать значение в зависимости

от планируемых задач. Для большинства сценариев использования достаточно 3072 Мбайт.

- 10) «Максимальная полоса пропускания от контейнера, Мбит/с» – максимальная скорость передачи информации из контейнера к клиенту. Рекомендуется устанавливать значение в зависимости от планируемых задач. Например: - для просмотра видео в высоком разрешении (1080p и выше) необходима полоса пропускания от 50 мегабит/с и более; - для сценариев работы, не связанных с высокой нагрузкой и передачей данных, достаточно полосы пропускания от 3 мегабит/с.
- 11) «Использовать прокси-сервер» – при использовании прокси-сервера для изолированного приложения указывается его адрес в формате: `http(https)://<адрес прокси сервера>:<порт>`. Например: `http://proxy.company.ru:3128`;
- 12) «Kerberos SPN для прокси-сервера» – имя субъекта-службы.
- 13) «Исключение для прокси-сервера» – список IP-адресов или FQDN доменов (через запятую), для которых соединение устанавливается напрямую, минуя настроенный прокси-сервер. Используется для обеспечения прямого доступа к локальным, внутренним или доверенным ресурсам.
- 14) «Выключить звук» – при включенной настройке у пользователя не будет воспроизводиться звук в браузере.
- 15) «Запретить скачивать файлы из Интернета» – при включенной настройке пользователь не сможет скачивать файлы через браузер.
- 16) «Запретить загружать файлы в Интернет» – при включенной настройке пользователь не сможет загружать файлы через браузер в Интернет. Внимание! При активации настройки «Запретить загружать файлы в Интернет» в браузере будут действовать ограничения в виде невозможности скачивания изображений и веб-страниц.
- 17) «Использовать полный профиль браузера» – при включенной настройке будет использоваться механизм полных пользовательских профилей с возможностью сохранения и переноса данных пользовательской сессии (например, истории) между перезапусками контейнеров.
- 18) «Политики браузера» – политики безопасности браузера.

Рисунок 22 – Окно создания профиля контейнера

Чтобы подключение к ПК «Ankey RBI» заработало с созданным профилем, необходимо, чтобы на всех брокерах был валидный файл /etc/krb5.conf, в котором в параметре

«dns_canonicalize_hostname» должно быть установлено значение «true» (значение по умолчанию «fallback» приводит к ошибке).

Также необходимо убедиться, что в файле `/etc/krb5.conf` присутствуют настройки, позволяющие Kerberos найти KDC. Ниже представлены настройки и их значения, которые должны быть установлены в файле:

```
[libdefaults]
    dns_lookup_realm = true
    dns_lookup_kdc = true
    forwardable = true
[realms]
    PAC-REL-WIN.RBI.DEV.DA.LAN = {
        kdc = dc1-rel.pac-rel-win.rbi.dev.da.lan
    }
```

Примечание. Настройки могут отличаться и зависят от настроек домена.

С созданными профилями допускается проводить следующие действия:

- редактирование. Для этого необходимо нажать на выбранный профиль. Для изменения доступны все поля, которые были доступны при создании;
- удаление. Для этого необходимо напротив выбранного профиля в выпадающем меню выбрать кнопку «Удалить».

7.6 Управление привязкой УЗ пользователей или групп пользователей служб каталогов для привязки к профилям

В ПК «Ankey RBI» реализована возможность использования УЗ пользователей или групп пользователей служб каталогов для привязки к профилям.

Привязка УЗ пользователей/групп выполняется в веб-интерфейсе ПК «Ankey RBI»:

- в разделе «Настройки пользователей» – привязка к одному конкретному пользователю из службы каталогов (рис. 23);
- в разделе «Настройки групп» – привязка к группе пользователей службы каталогов (рис. 24).

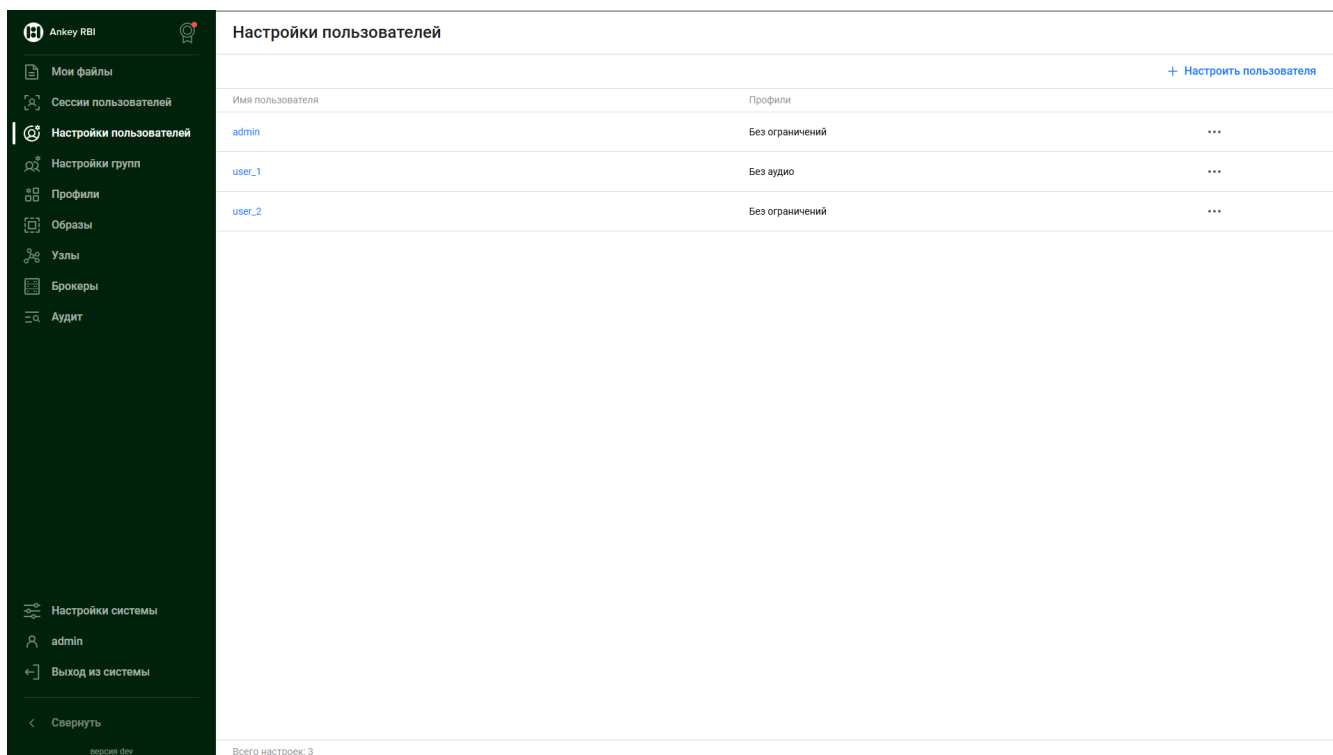


Рисунок 23 – «Настройки пользователей» веб-интерфейса ПК «Ankey RBI»

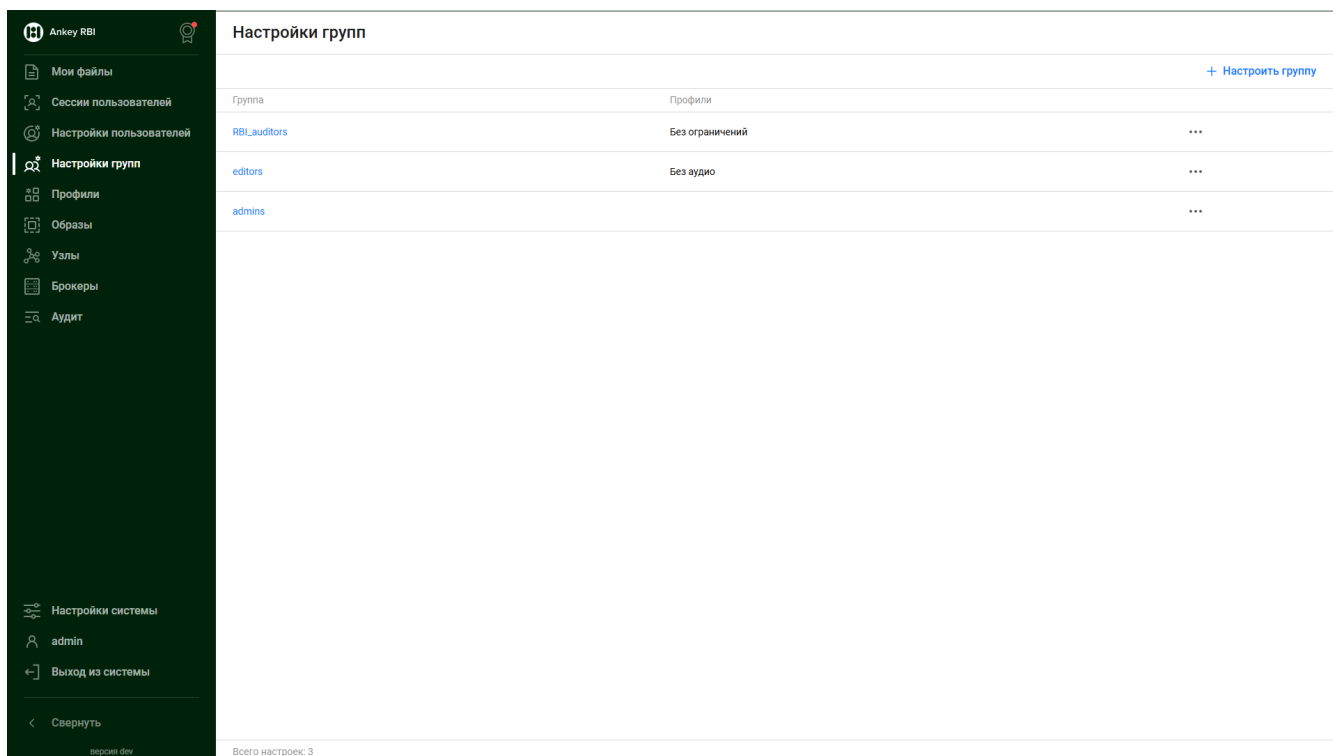


Рисунок 24 – Раздел «Настройки групп» веб-интерфейса ПК «Ankey RBI»

По умолчанию страница с настройками пользователей/групп содержит пустой список, в котором будут отображаться все созданные связи между пользователями/группами и профилями. О созданных настройках пользователей/групп отображается следующая информация:

- имя пользователя/группы;
- профиль, связанный с пользователем/группой.

7.6.1 Создание новой настройки

Для создания настройки пользователя необходимо:

- 1) Перейти в раздел веб-интерфейса ПК «Ankey RBI» «Настройки пользователей».
- 2) Нажать кнопку «Настроить пользователя».
- 3) В открывшемся окне заполнить следующие обязательные поля:
 - «Пользователь» – выбрать из выпадающего списка пользователя, для которого необходимо настроить профиль;
 - «Профиль» – выбрать из выпадающего списка профиль, который будет использоваться для пользователя (рис. 25).

Настройка пользователя [X]

Пользователь ●

Выберите пользователя [v]

Профиль

⋮ [Выберите профиль] [v] [trash icon]

+ Добавить

Квота на файловый ресурс, Мб

Введите значение

[Отменить] [Сохранить]

Рисунок 25 – Настройки пользователей

- 4) Нажать кнопку «Сохранить».

После этого новая настройка пользователя появится в общем списке.

Внимание! Для пользователей из другого домена (см. пункт 2.4.3 данного руководства) персональная настройка недоступна.

Для создания настройки группы необходимо:

- 1) Перейти в раздел веб-интерфейса ПК «Ankey RBI» «Настройки группы».
- 2) Нажать кнопку «Настроить группу».

- 3) В открывшемся окне заполнить следующие обязательные поля:
- «Группа» – выбрать из выпадающего списка группу, для которой необходимо настроить профиль;
 - «Профиль» – выбрать из выпадающего списка профиль, который будет использоваться для группы (рис. 26).

Настройка группы

Группа ●

Выберите группу

Профиль

⋮ Выберите профиль

+ Добавить

Квота на файловый ресурс, Мб

Введите значение

Отменить Сохранить

Рисунок 26 – Настройки группы

- 4) Нажать кнопку «Сохранить».

После этого новая настройка группы появится в общем списке.

7.6.2 Редактирование и удаление настроек

Настройки пользователей/групп возможно изменить, нажав на имя УЗ соответствующего пользователя.

Удалить настройку пользователей/групп возможно, нажав в выпадающем меню напротив соответствующей записи кнопку «Удалить».

7.6.3 Назначение нескольких профилей пользователю или группе

В ПК «Ankey RBI» предусмотрена возможность привязки к пользователю/группе нескольких профилей – возможность запускать несколько различных изолированных приложений с уникальными настройками.

Для привязки нескольких профилей к настройкам пользователя/группы в ПК «Ankey RBI» должно быть заведено два или более профиля (см. пункт 7.5.1 данного руководства).

Для добавления нескольких профилей необходимо при создании/редактировании настроек пользователя/группы нажать кнопку «Добавить», после чего появится поле для добавления дополнительного профиля (рис. 27 и 28).

Настройка пользователя [X]

Пользователь ●

new (new) [v]

Профиль

:: Яндекс [v] [trash]

:: Plugins [v] [trash]

+ Добавить

Квота на файловый ресурс, Мб

Введите значение

Отменить Сохранить

Рисунок 27 – Пример настройки пользователя с несколькими профилями

Настройка группы

Группа ●

Administrators

Профиль

:: Google Chrome

:: проху1

+ Добавить

Квота на файловый ресурс, Мб

Введите значение

Отменить Сохранить

Рисунок 28 – Пример настройки группы с несколькими профилями

Количество добавляемых дополнительных профилей ограничено количеством существующих в ПК «Ankey RBI» профилей.

Для удаления дополнительного профиля необходимо нажать кнопку  напротив профиля, который требуется удалить.

После добавления нескольких профилей для пользователя или группы, администратору, который обсуживает ПК «Ankey RBI», требуется создать ярлыки для запуска клиента (см. подраздел 3.3 данного руководства) с необходимым профилем на рабочем столе АРМ пользователя одним из следующих способов:

- запустить утилиту RBI-shortcut (см. подраздел 3.3 данного руководства) с параметром «–profile UUID»;
- добавить в существующий ярлык запуска клиента параметр «–profile UUID», где UUID – идентификатор профиля.

Если флаг не указан, то будет запускаться профиль, который отображается первым в списке настроек. Порядок профилей можно изменять при создании/редактировании настроек, нажав кнопку  и перетаскив профиль выше/ниже.

7.6.4 Назначение квот пользователю или группе

В ПК «Ankey RBI» предусмотрена возможность назначения квоты пользователю или группе на объем загружаемых файлов.

Для этого необходимо при создании/редактировании настроек пользователя/группы в поле «Квота на файловый ресурс, Мб» указать значение в диапазоне от 1 до 1 000 000 (рис. 29).

Настройка группы

Группа ●

Administrators

Профиль

:: Google Chrome

:: проху1

+ Добавить

Квота на файловый ресурс, Мб

100

Отменить Сохранить

Рисунок 29 – Пример настройки группы с указанием квоты

При этом следует учитывать, что:

- при запуске клиента с профилем «По умолчанию» применение квот отключено;
- если квота задана как для пользователя, так и для одной или нескольких групп, в которых он состоит, используется квота пользователя (имеет более высокий приоритет).

При превышении квоты пользователь получит сообщение «Ошибка загрузки файла, пользователем использовано X Мб из квоты в Y Мб», где X – это количество Мбайт, на которое превышена квота, равная Y Мбайт.

7.7 Управление сессиями пользователей

Раздел «Сессии пользователей» (рис. 30) предназначен для мониторинга и управления текущими сессиями пользователей и просмотра истории завершенных сессий.

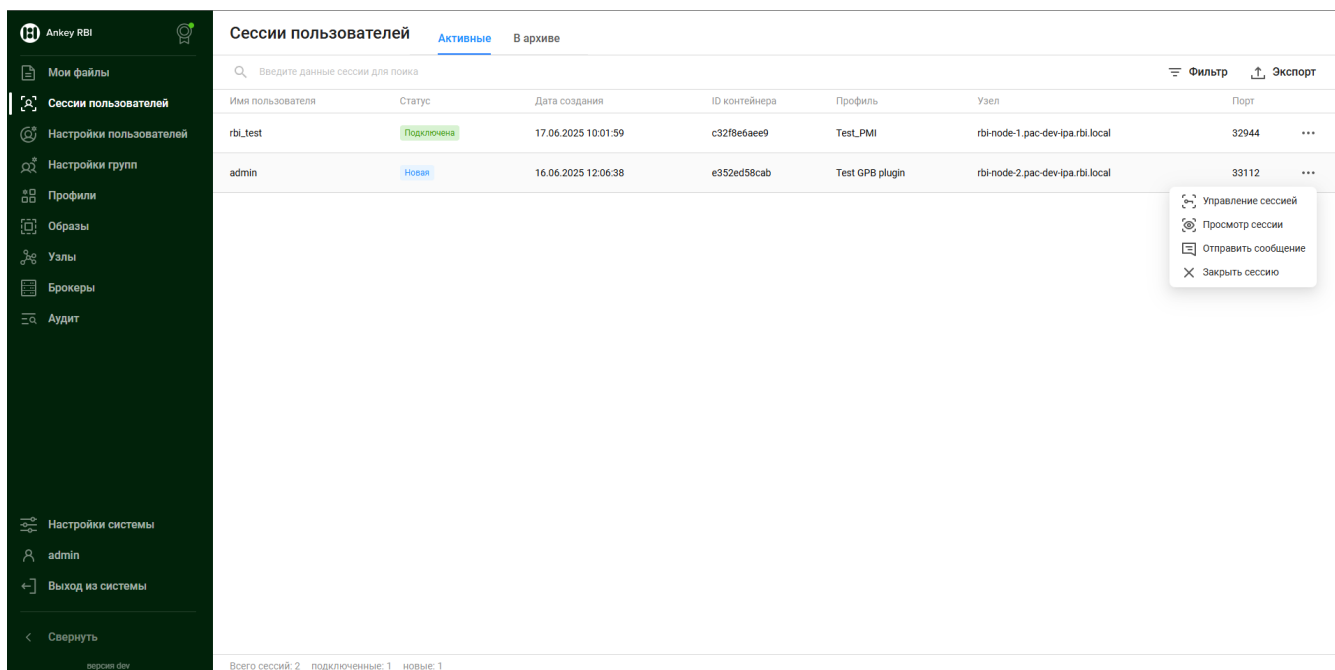


Рисунок 30 – Раздел «Сессии пользователей» веб-интерфейса ПК «Ankey RBI»

На странице раздела возможно фильтровать отображаемые данные по статусу контейнера. Для этого необходимо нажать на кнопку «Фильтр» и выбрать необходимый статус. По умолчанию отображаются все сессии пользователей.

На странице мониторинга отображаются все пользовательские сессии. Доступны две вкладки:

- «Активные» – сессии пользователей с действующими контейнерами. На данной вкладке отображаются контейнеры со статусами: «Новая», «Подключена», «Не подключена» (см. ниже описание статусов);
- «В архиве» – завершенные сессии пользователей. На данной вкладке отображаются контейнеры только со статусом «Завершена» (см. ниже описание статусов).

Для каждой пользовательской сессии доступна следующая информация:

- 1) «Имя пользователя» – УЗ пользователя, который работает в сессии.
- 2) «Статус» – текущее состояние контейнера. Предусмотрены следующие статусы:
 - «Новая» – контейнер только что создан;
 - «Подключена» – пользователь в настоящий момент подключен к изолированному приложению;
 - «Не подключена» – пользователь отключен от контейнера, изолированное приложение продолжает работать. Если до закрытия контейнера пользователь успеет снова открыть браузер, то статус сессии снова будет изменен на «Подключена»;
 - «Завершена» – статус, который отображается после завершения работы контейнера. Если после завершения работы контейнера пользователь еще

раз подключится к клиенту, то будет создан новый контейнер. Контейнеры с этим статусом отображаются только на вкладке «В архиве».

- 3) «Дата создания» – время и дата создания контейнера. Отображается в формате ДД-ММ-ГГГГ, чч:мм:сс;
- 4) «ID контейнера» – уникальный идентификатор контейнера;
- 5) «Профиль» – название профиля контейнера;
- 6) «Узел» – адрес узла, на котором запущен контейнер;
- 7) «Порт» – номер порта.

По умолчанию список сессий (как на вкладке «Активные», так и на вкладке «В архиве») отсортирован в порядке убывания даты и времени. Чтобы задать другой тип сортировки необходимо выбрать заголовок требуемого столбца таблицы. В заголовке отобразится знак , сортировка всех строк таблицы будет выполнена по убыванию значений выбранного столбца. Для изменения направления сортировки необходимо повторно выбрать заголовок столбца. В заголовке отобразится знак . Сортировка доступна для всех колонок, кроме колонки «Статус» на вкладке «В архиве».

Чтобы посмотреть информацию о конкретных сессиях, необходимо задать фильтры для поиска сессий. Для этого требуется нажать на кнопку «Фильтр» в правом верхнем углу веб-интерфейса. Для активных сессий доступна фильтрация по статусу. Для архивных сессий доступны следующие фильтры:

- 1) «Отобразить сессии с» и «Отобразить сессии по» – поля для указания временного периода, в котором была запущена сессия.
- 2) «Источник» – выпадающий список с адресами брокеров.

Для просмотра информации о конкретных сессиях также возможно использовать строку для поиска. Для активных сессий поиск доступен по всей информации (имя пользователя, статус, дата создания, ID контейнера, профиль, узел, порт), для архивных – только по ID контейнера.

Данные о сессиях возможно получить в виде отчета, экспортированного в текстовый файл с разделителями формата CSV. Для этого необходимо в правом верхнем углу веб-интерфейса нажать кнопку «Экспорт». По умолчанию, если не применены фильтры, то в отчет будут экспортированы все сессии. Если требуется сохранить отчет только с конкретными событиями, то перед скачиванием файла необходимо применить фильтры.

7.7.1 Отправка сообщения пользователю

Администратор может отправить пользователям ПК «Ankey RBI» текстовое сообщение, например, предупреждение о скором закрытии сессии в связи с техническими работами на сервере. Для отправки сообщений необходимо:

- 1) Установить флаг напротив имени пользователя или нескольких пользователей с активными сессиями, которым необходимо отправить сообщения.
- 2) В отобразившейся строке с кнопками выбора операций выбрать пункт «Отправить сообщение».

- 3) Далее в открывшемся окне ввести текст сообщения.
- 4) Нажать кнопку «Отправить».

Для отправки сообщения только одному пользователю необходимо:

- 1) Выбрать пользователя с активной сессией.
- 2) Напротив выбранного пользователя в выпадающем меню выбрать кнопку «Отправить сообщение».
- 3) Далее в открывшемся окне ввести текст сообщения.
- 4) Нажать кнопку «Отправить».

7.7.2 Теневое подключение к сессиям пользователей

Теневое подключение к сессиям пользователей позволяет администраторам подключиться к сессии любого пользователя для просмотра сессии изолированного приложения пользователя, а также управления сессией.

Сами пользователи при этом не будут получать уведомления о том, что к их сессии было осуществлено подключение.

Примечание. Просматривать и управлять можно сессиями со статусами «Подключена» и «Не подключена». Просмотр сессии со статусом «Не подключена» возможен только до истечения времени существования контейнера (см. пункт 7.5.1 данного руководства).

Для просмотра сессии без возможности управления необходимо:

- 1) Выбрать пользователя с активной сессией, которую необходимо посмотреть.
- 2) Напротив выбранного пользователя в выпадающем меню выбрать кнопку «Просмотр сессии».

Для просмотра сессии с возможностью управления необходимо:

- 1) Выбрать пользователя с активной сессией, которую необходимо посмотреть.
- 2) Напротив выбранного пользователя в выпадающем меню выбрать кнопку «Управление сессией».

В результате в соседней вкладке браузера откроется вкладка с содержимым активной сессии пользователя.

Для завершения просмотра/управления активной сессии необходимо просто закрыть вкладку браузера.

7.7.3 Завершение сессии пользователя

Администратор может принудительно завершить активные сессии пользователей, например, при проведении технических работ на сервере.

Аудитор и пользователь могут принудительно завершить только свои активные сессии.

Для завершения сессий необходимо:

- 1) Установить флаг напротив имени пользователя или нескольких пользователей с активными сессиями, которые необходимо завершить.

- 2) В отобразившейся строке с кнопками выбора операций выбрать пункт «Завершить сессию».
- 3) Подтвердить завершение сессий.

Если необходимо завершить сессию только одного пользователя, то можно:

- 1) Выбрать пользователя с активной сессией, которую необходимо завершить.
- 2) Напротив выбранного пользователя в выпадающем меню выбрать кнопку «Завершить сессию».

7.8 Просмотр журнала системных событий

Информация о событиях системы представлена в разделе веб-интерфейса «Аудит» (рис. 31). На странице раздела отображается информация о действиях пользователей системы.

Время	IP-адрес	Источник	Пользователь	Тип	Детали
08.07.2024 16:21:45	192.168.244.119	e0d7dcda-455b-45b9-9c13-07f5e0c55c4e	admin	Изменение настроек системы	Оповещения отк. Недоступн ОЗУ узла
08.07.2024 16:21:46	192.168.244.119	e0d7dcda-455b-45b9-9c13-07f5e0c55c4e	admin	Изменение настроек системы	Оповещения отк. Недоступн на 80% → больше ч 90% в теч
04.06.2024 16:26:24	192.168.244.152	e0d7dcda-455b-45b9-9c13-07f5e0c55c4e	admin	Изменение настроек системы	Кластерный IP Пароль VRRP 10.116.17 *** → ***
28.05.2024 14:50:42	192.168.244.152	e0d7dcda-455b-45b9-9c13-07f5e0c55c4e	admin	Загрузка файла в DARBI	Путь: /mnt/rbi/2 Результат: Отказано
21.05.2024 09:48:46	192.168.244.152	8e70f31d-4adc-4fed-95aa-89f788247de2	admin	Изменение настроек профиля	Профиль: fea5af01-test_profil Имя
20.05.2024 14:26:37	192.168.244.152	8e70f31d-4adc-4fed-95aa-89f788247de2	admin	Изменение настроек профиля	Профиль: aef10394-Максимальная 5 → Пуст
21.05.2024 10:03:16	192.168.244.152	8e70f31d-4adc-4fed-95aa-89f788247de2	admin	Изменение настроек профиля	ID образа d2a9a457
01.09.2012 16:00:00	192.168.51.1	192.168.1.1	admin@RBI.LOCAL	Авторизация пользователя	Администратор: Да Результат: Успешно
01.09.2012 16:00:00	192.168.51.1	192.168.1.1	admin@RBI.LOCAL	Авторизация пользователя	Администратор: Да Результат: Успешно
01.09.2012 19:00:00	192.168.51.1	192.168.1.1	user1@RBI.LOCAL	Начало пользовательской сессии	ID сессии: 7c88a34a-0d9f-46ed-b44b-dfda7105cc30 ID контейнера: a0541222ed9
01.09.2012 19:00:00	192.168.51.1	192.168.1.1	user1@RBI.LOCAL	Окончание пользовательской сессии	ID сессии: 7c88a34a-0d9f-46ed-b44b-dfda7105cc30 ID контейнера: a0541222ed8

Рисунок 31 – Раздел «Аудит» веб-интерфейса ПК «Ankey RBI»

По умолчанию на странице раздела отображается список со всеми зарегистрированными в системе событиями. Общее количество событий, сохраненных в журнале, отображается в левой нижней части веб-интерфейса.

Чтобы посмотреть информацию о конкретных событиях, необходимо задать фильтры для поиска событий. Для этого требуется нажать на кнопку «Фильтр» в правом верхнем углу веб-интерфейса. После этого откроется список фильтров, в котором доступны следующие поля:

- 1) «Отобразить события безопасности с» и «Отобразить события безопасности по» – поля для указания временного периода, в котором произошло событие в комплексе.alt text

- 2) «Тип» – список совершенных пользователями действий, которые возможно отобразить. Доступны следующие события для поиска:
- «Авторизация пользователя»;
 - «Начало пользовательской сессии»;
 - «Окончание пользовательской сессии»;
 - «Скачивание файла из «Ankey RBl»;
 - «Загрузка файла в «Ankey RBl»;
 - «Удаление пользовательского файла»;
 - «Удаление профиля»;
 - «Изменение настроек профиля»;
 - «Установка образа»;
 - «Удаление образа»;
 - «Удаление настроек пользователя»;
 - «Изменение настроек пользователя»;
 - «Удаление настроек групп»;
 - «Изменение настроек группы»;
 - «Изменение настроек узла»;
 - «Разрешение доступа на узел»;
 - «Запрет доступа на узел»;
 - «Изменение настроек системы»;
 - «Сессия завершена администратором»;
 - «Теневая сессия».
- 3) «Источник» – выпадающий список с адресами брокеров.
- 4) «Пользователь» – поле, в котором указывается имя пользователя, с которым связано событие.
- 5) «IP-адрес» – поле, в котором указывается IP-адрес АРМ пользователя, с которым связано системное событие.

После заполнения полей необходимо нажать кнопку «Применить». Информация о найденных событиях отобразится в виде списка. Чтобы отменить указанные в фильтрах данные, необходимо нажать кнопку «Сбросить».

Данные о событиях возможно получить в виде отчета, экспортированного в текстовый файл с разделителями формата CSV. Для этого необходимо в правом верхнем углу веб-интерфейса нажать кнопку «Экспорт». По умолчанию, если не применены фильтры, то в отчет будут экспортированы все события, которые сохранены в журнале. Если требуется сохранить отчет только с конкретными событиями, то перед скачиванием файла необходимо применить фильтры.

7.9 Просмотр информации о брокерах

Раздел «Брокеры» (рис. 32) служит для просмотра списка брокеров.

Адрес	Активность	Статус	Лицензирование	Дата создания	Описание
server1.example.ru	Активный	Онлайн	В порядке	01.07.2023 15:00:00	server1 ...
192.168.1.1	Запасной	Онлайн	Нет лицензии	01.07.2023 15:00:00	server2 ...
server2.example.ru	Активный	Онлайн	Истекла	01.07.2023 15:00:00	server2 ...

Всего брокеров: 3

Рисунок 32 – Раздел «Брокеры» веб-интерфейса ПК «Ankey RBI»

О каждом брокере отображается следующая информация:

- 1) «Адрес» – адрес брокера.
- 2) «Активность» – признак, указывающий текущую активность брокера в зависимости от того, является брокер основным или резервным:
 - «Активный» – брокер является активным и основным на текущий момент;
 - «Запасной» – брокер является резервным.
- 3) «Статус»:
 - «Онлайн» – брокер доступен для работы;
 - «Офлайн» – брокер недоступен для работы.
- 4) «Лицензирование» – состояние лицензии на данном брокере:
 - «В порядке» – лицензия активирована;
 - «Нет лицензии» – лицензия отсутствует.
- 5) «Дата создания» – время и дата создания брокера. Отображается в формате ДД-ММ-ГГГГ, чч:мм:сс.
- 6) «Описание» – текстовая информация о брокере.

7.10 Использование плагинов для работы с криптографическими ключами и электронной подписью

В ПК «Ankey RBI» предусмотрена возможность использовать в изолированном приложении плагины для работы с криптографическими ключами и электронной подписью (ЭП), установленные на АРМ пользователя.

Организация связи между ПК «Ankey RBI» и плагинами для поддержки работы с носителями криптографических ключей, установленными на АРМ пользователя, реализована с помощью следующих технологий:

- 1) Переадресация протокола Chrome Native Messaging, позволяющая расширениям веб-браузера в изолированном приложении обмениваться сообщениями с установленными на АРМ плагинами.
- 2) Переадресация локального TCP порта.

Поддерживаются следующие плагины:

- 1) Контур.Плагин.
- 2) Плагин Госуслуг (ЕПГУ).
- 3) Крипто-модуль Газпромбанка.
- 4) Blitz Smart Card Plugin.
- 5) КриптоПро ЭЦП.

Расширения, необходимые для работы веб-браузерами с плагинами, предварительно установлены в образ изолированного приложения (см. подраздел 7.4 данного руководства).

Внимание! При установке плагина «Крипто-модуль Газпромбанка» на АРМ пользователя в файл «hosts» операционной системы автоматически добавляется запись следующего вида:

```
127.0.0.1 cm.sftcomp.ru
```

Указанный выше адрес (cm.sftcomp.ru) должен быть обязательно внесен в список исключений для прокси-сервера.

7.10.1 Настройка ПК «Ankey RBI» для работы с плагинами

Для настройки работы ПК «Ankey RBI» с плагинами администратору, который обслуживает комплекс, необходимо убедиться в том, что все плагины, необходимые для работы пользователя и поддерживаемые изолированным приложением (список поддерживаемых плагинов представлен в подразделе 7.10 данного руководства) установлены и настроены на АРМ пользователя в соответствии с требованиями и рекомендациями разработчиков плагина.

8 Обновление программы

Обновление ПК «Ankey RBI» осуществляется из предоставленного разработчиком комплекта ПО путем установки новой версии поверх уже установленной. Порядок обновления компонентов ПК «Ankey RBI» представлен ниже.

8.1 Обновление брокера и узлов

Обновление брокера осуществляется путем установки новой версии брокера поверх предыдущей.

Для обновления брокера требуется загрузить архив с дистрибутивом ПО по ссылке на скачивание, которая будет отправлена в письме производителем, или скопировать с предоставленного компакт-диска.

Далее требуется перейти в каталог с дистрибутивами и в консоли РЕД ОС выполнить последовательность действий и команд, приведенных ниже:

Примечание. Все команды вводятся от имени суперпользователя root, либо используя программу sudo.

- 1) Выполнить обновление брокера с помощью следующих команд:

```
sudo dnf install gis-activator14-X.X.X.XX.x86_64.rpm
sudo dnf install rbi-server-X.X.X.XX.x86_64.rpm
sudo systemctl daemon-reload
sudo systemctl restart rbi-server
```

- 2) Дождаться окончания обновления. Отсутствие каких-либо ошибок в консоли будет свидетельствовать об успешном обновлении брокера.

- 3) На всех узлах выполнить команды установки нового агента:

```
sudo dnf install rbi-agent-X.X.X.XX.x86_64.rpm
sudo systemctl daemon-reload
sudo systemctl restart rbi-agent
```

- 4) Произвести переподготовку всех узлов через веб-интерфейс ПК «Ankey RBI» (подробнее в пункте 7.2.2 данного руководства).

Внимание! Переподготовку узлов нужно выполнить даже в том случае, когда обновлялся только брокер.

8.2 Обновление клиента

8.2.1 Обновление клиента на РЕД ОС, Astra Linux или ALT Linux

Обновление клиента на РЕД ОС, Astra Linux или ALT Linux выполняется путем установки новой версии клиента поверх предыдущей. Процесс установки клиента описан в пункте 3.3.1 данного руководства.

8.2.2 Обновление клиента на Windows 10/11

Обновление клиента на Windows 10/11 выполняется путем установки новой версии клиента поверх предыдущей. Процесс установки клиента описан в пункте 3.3.2 данного руководства.

9 Удаление программы

При удалении комплекса данные из БД и каталога с файлами пользователей не удаляются. При необходимости эти данные удалить вручную.

После удаления комплекса на узлах сохраняются загруженные Docker-образы и образы запущенных контейнеров, которые также требуется удалить вручную.

9.1 Удаление ПК «Ankey RBI» с сервера

Примечание. Все команды вводятся от имени суперпользователя root, либо используя программу sudo.

Для удаления ПК «Ankey RBI» на сервере необходимо в консоли РЕД ОС выполнить команду:

```
sudo dnf remove rbi-server
```

9.2 Удаление ПК «Ankey RBI» с узлов

Примечание. Все команды необходимо вводить от имени суперпользователя root, либо используя программу sudo.

Для удаления ПК «Ankey RBI» с узлов необходимо в консоли РЕД ОС выполнить команду:

```
sudo dnf remove rbi-agent
```

9.3 Удаление ПК «Ankey RBI» с АРМ пользователя

Примечание. Все команды необходимо вводить от имени суперпользователя root, либо используя программу sudo.

Для удаления ПК «Ankey RBI» с АРМ пользователя необходимо в консоли РЕД ОС, Astra Linux или ALT Linux выполнить команду:

```
sudo dnf remove rbi-client
```

Для удаления ПК «Ankey RBI» с АРМ пользователя под управлением Windows 10/11 необходимо:

- 1) Перейти в «Панель управления» ОС.
- 2) Перейти в раздел «Программы» и выбрать пункт «Программы и компоненты».
- 3) В списке установленных программ найти «Ankey RBI» и нажать на название левой кнопкой манипулятора «мышь».
- 4) Нажать кнопку «Удалить».

10 Резервное копирование и восстановление данных

10.1 Резервное копирование данных

Для резервного копирования данных ПК «Ankey RBI» необходимо выполнить следующие действия:

- 1) Создать резервную файловую хранилища (по умолчанию /mnt/rbi). Информация о файловой хранилище представлена в подразделе 2.2 данного руководства.
- 2) Создать резервную копию БД, выполнив следующую команду:

```
pg_dump postgres://username:password@host:<host>/dbname > backup.sql
```

Параметры команды описаны в подразделе 3.1 данного руководства.

- 3) Создать резервную копию конфигурационного файла, который имеет следующее расположение: /opt/rbi/etc/config.yaml. Необходимо создать резервные копии конфигурационных файлов на всех установленных брокерах.

10.2 Восстановление данных из резервной копии

Для восстановления данных ПК «Ankey RBI» из резервной копии необходимо выполнить следующие действия:

- 1) Выполнить установку пакетов. Информация об установке ПК «Ankey RBI» представлена в подразделе 3.1 данного руководства.
- 2) Восстановить содержимое файловой хранилища (по умолчанию /mnt/rbi).
- 3) Создать БД (см. подраздел 2.1 данного руководства) и восстановить содержимое БД из резервной копии.
- 4) Восстановить резервные копии конфигурационных файлов.
- 5) Разрешить автозапуск и запустить службу брокера (см. подраздел 3.1 данного руководства).
- 6) Выполнить повторную подготовку всех узлов. Информация о подготовке узлов представлена в пункте 7.2.2 данного руководства.

11 Обслуживание и решение проблем

В данном разделе представлены часто задаваемые вопросы и ответы, которые могут возникнуть при эксплуатации комплекса.

Если в процессе эксплуатации ПК «Ankey RBI» возникли вопросы и проблемы, которые не представлены в данном разделе, рекомендуется обратиться в техническую поддержку. Контакты технической поддержки указаны в документе «Программный комплекс «Ankey RBI». Формуляр».

11.1 Ошибки при попытке получения доступа к веб-интерфейсу

В таблице 7 представлено описание и решение проблем, которые могут возникнуть при попытке получения доступа к веб-интерфейсу.

Таблица 7 – Решение проблем при попытке получения доступа к веб-интерфейсу

Описание проблемы	Решение
Предупреждение о безопасности сертификата	Данная ошибка возникает в следующих случаях: 1) Не настроены сертификаты безопасности. Для решения данной проблемы необходимо настроить параметры системы, связанные с сертификатами (см. раздел «Основные настройки»). 2) Истек срок действия сертификата безопасности. Для решения данной проблемы рекомендуется заменить сертификат с истекшим сроком действия на новый. Если сертификат настроен правильно (введены СА сертификат, сертификат сервера и ключ сервера), но возникает ошибка, то необходимо: 3) Проверить, что адрес, по которому осуществляется доступ к серверу, совпадает с адресом, который указан в сертификате сервера. 4) Убедиться, что на АРМ, с которого осуществляется доступ, установлен сертификат удостоверяющего центра (СА сертификат), который выдал сертификат для rbi-сервера
Ошибка подключения к серверу	Необходимо убедиться, что сервер запущен
Ошибка аутентификации	Убедиться, что корректно введены логин и пароль

11.2 При попытке доступа к веб-интерфейсу не появляется возможность доменной аутентификации

Необходимо выполнить следующие действия:

- 1) Убедиться, что был выполнен вход на АРМ под доменной УЗ.
- 2) Убедиться, что в веб-браузере настроен параметр auth-server-allowlist, который настраивается через параметры командой строки веб-браузера (РЕД ОС, Astra

Linux или ALT Linux) или настройки групповой политики (Windows 10/11).
Например:

```
--auth-server-allowlist=*.<доменное имя>
```

- 3) Убедиться, что в настройках системы загружен корректный keytab-файл.

11.3 В веб-интерфейсе отображается некорректный список разделов меню

Для решение данной проблемы необходимо:

- 1) Авторизоваться в комплексе, используя данные УЗ локального администратора.
- 2) Перейти в раздел «Настройки системы».
- 3) Убедиться, что выбрана требуемая группа LDAP:
 - «LDAP группа администраторов»;
 - «LDAP группа пользователей»;
 - «LDAP группа аудиторов».

Разделы меню веб-интерфейса отличаются для пользователей с разными ролями. В таблице 8 представлен список ролей и соответствующий данным ролям разделы меню.

Таблица 8 – Роли ПК «Ankey RBI»

Роль	Разделы меню
Администратор	– Мои файлы; – Сессии пользователей; – Настройка пользователей; – Настройка групп пользователей; – Профили; – Образы; – Узлы; – Брокеры; – Аудит; – Настройки системы
Пользователь	– Мои файлы; – Сессии пользователей
Аудитор	– Мои файлы; – Сессии пользователей; – Аудит

Если у пользователя отображается список разделов, не соответствующий его роли, то необходимо убедиться, что пользователь включен в соответствующие группы безопасности.

11.4 Узел находится в режиме Офлайн

Выполнить следующие действия:

- 1) Убедиться, что узел правильно настроен.

- 2) Убедиться, что с узла есть возможность доступа к серверу, например, командой, введенной на узле:

```
curl https://rbi-server.example.ru
```

- 3) Убедиться, что на узле запущен агент:

```
systemctl status rbi-agent
```

11.5 Не добавляется узел

Убедиться, что правильно выполнены инструкции, изложенные в окне добавления узла.

11.6 При настройке групп LDAP не отображаются списки доступных групп

Если при настройке групп LDAP появилась информационная ошибка, то необходимо проверить корректность введенных значений параметров.

В случае, если значения были введены корректно, появится сообщение об успешном сохранении настроек.

11.7 При попытке запуска изолированного приложения появляется ошибка сертификата

Если при попытке запуска изолированного приложения возникла ошибка сертификата (рис. 33), то необходимо убедиться, что корневой сертификат удостоверяющего центра, выпустившего сертификат rbi-сервера, установлен как доверенный на APM пользователя.

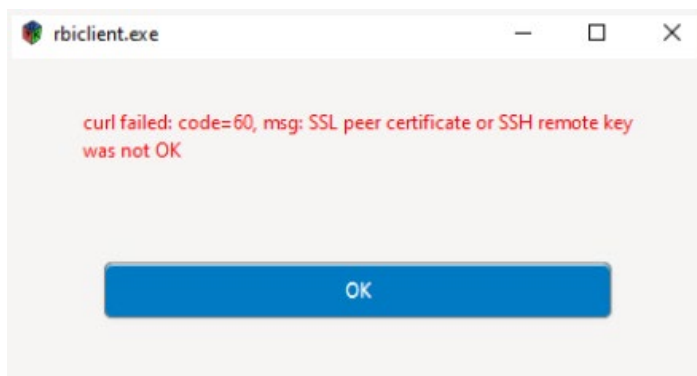


Рисунок 33 – Ошибка сертификата на ОС Windows 10/11

11.8 При попытке запуска изолированного приложения появляется ошибка запуска сессии

Если при попытке запуска изолированного приложения возникла ошибка запуска сессии (рис. 34), то необходимо убедиться, что в файле /etc/krb5.conf в параметре «dns_canonicalize_hostname» установлено значение «true». Подробная информация представлена в пункте 7.5.1 настоящего руководства.

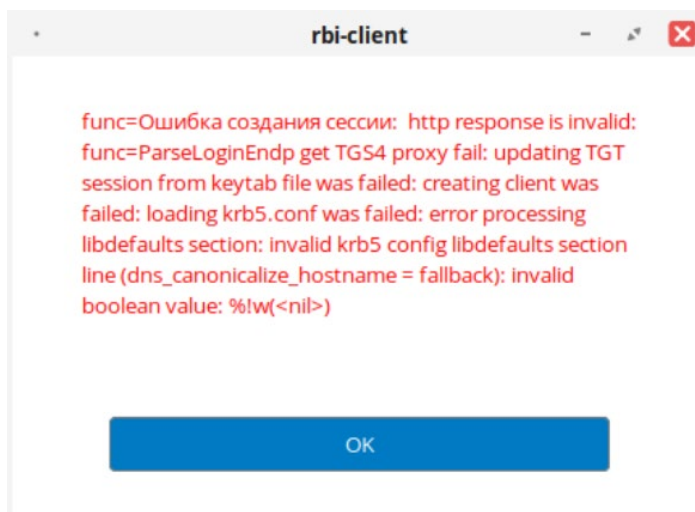


Рисунок 34 – Ошибка запуска сессии

11.9 При попытке ввода валидного значения ключа лицензии появляется нелокализованная ошибка

Если при вводе валидного значения ключа лицензии для брокера, не подключенного к серверу лицензирования, появляется ошибка (рис. 35) со следующим текстом:

```
Post "http://localhost:8000/api/v1/license/check-key": dial tcp [::1]:8000: connect: connection refused
```

то необходимо выполнить в консоли сервера:

```
systemctl enable rbi-license
systemctl start rbi-license
```



Рисунок 35 – Нелокализованная ошибка при вводе значения ключа лицензии

После выполнения команд требуется открыть веб-интерфейс ПК «Ankey RBI», перейти в раздел лицензирования и повторно проверить значение ключа лицензии, нажав кнопку «Проверить».

11.10 Не работают «Настройки пользователя» после смены имени УЗ пользователя на контроллере домена

После смены имени УЗ пользователя на контроллере домена (смена логина) у пользователя в ПК «Ankey RBI» перестают применяться «Настройки пользователя», связанные с его прежним логином. Необходимо удалить старую настройку и создать новую.

Внимание! После смены логина пропадут данные из профиля браузера и сохраненные файлы.

11.11 Ошибка использования алгоритмов шифрования KDC

В конфигурации протокола Kerberos (конфигурационный файл «krb5.conf») на АРМ пользователя могут быть запрещены к использованию алгоритмы шифрования, которые используются на KDC (рис. 36). Необходимо проверить следующие настройки: «default_tgs_enctypes», «default_tkt_enctypes», «preferred_enctypes».

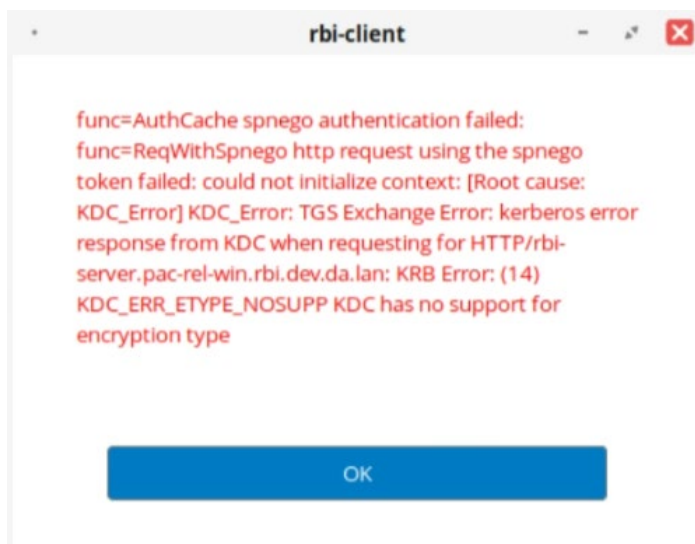


Рисунок 36 – Ошибка использования алгоритмов шифрования KDC

11.12 Ошибка выполнения аутентификации кеша протокола Kerberos

Если KDC не может найти имя на запрошенный SPN (рис. 37), то необходимо проверить, корректно ли назначен SPN для сервисной учетной записи брокера.

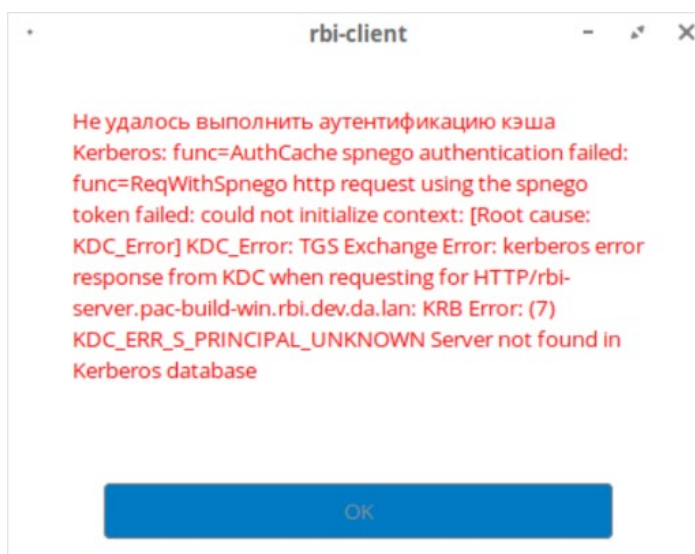


Рисунок 37 – Ошибка выполнения аутентификации кеша протокола Kerberos

11.13 Ошибка при загрузке образа

Если при загрузке образа возникла ошибка, показанная на рис. 38, то необходимо проверить, что файловое хранилище соответствует требованиям, указанным в подразделе 2.2 настоящего руководства.

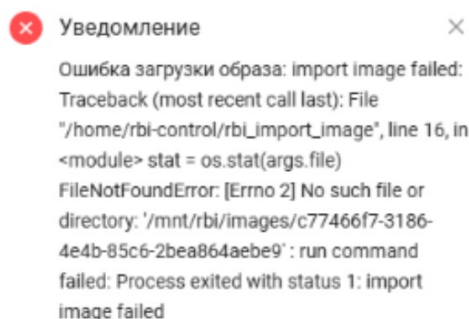


Рисунок 38 – Ошибка при загрузке образа

11.14 Как настроить инспектирование SSL

Обратите внимание, что ПК «Ankey RBI» не занимается инспекцией трафика. Учет трафика может быть настроен только с помощью прокси-сервера (см. пункты 2.3.2, 2.4.2 и 2.5.2 данного руководства). Если на прокси-сервере включено инспектирование SSL, то администратору, обслуживающему ПК «Ankey RBI», необходимо выполнить следующие действия для настройки инспекции данных:

- 1) В веб-интерфейсе ПК «Ankey RBI» перейти в раздел «Настройки системы» и раскрыть группу настроек «Настройки HTTPS».
- 2) В поле настройки «Корневые сертификаты» добавить соответствующий корневой сертификат.
- 3) Нажать кнопку «Сохранить».
- 4) Перейти в раздел «Узлы».
- 5) Для всех узлов выполнить переподготовку (см. пункт 7.2.2 данного руководства).

11.15 Ошибка подключения RBI-брокера к LDAPS

При возникновении ошибки подключения RBI-брокера к LDAPS необходимо проверить наличие корневых сертификатов на компьютерах, на которых установлены брокеры. При отсутствии сертификатов следует установить их, а при наличии – обновить до актуальной версии.

При использовании LDAPS-сервера с устаревшими алгоритмами шифрования (MD5, SHA) решение проблемы на стороне RBI-сервера невозможно. Для решения проблемы необходимо на RBI-брокере установить и настроить прокси-сервис Stunnel, который позволяет устанавливать безопасное соединение с сервисами, которые используют устаревшие и небезопасные алгоритмы шифрования. Пример схемы подключения приведен на рис. 39.

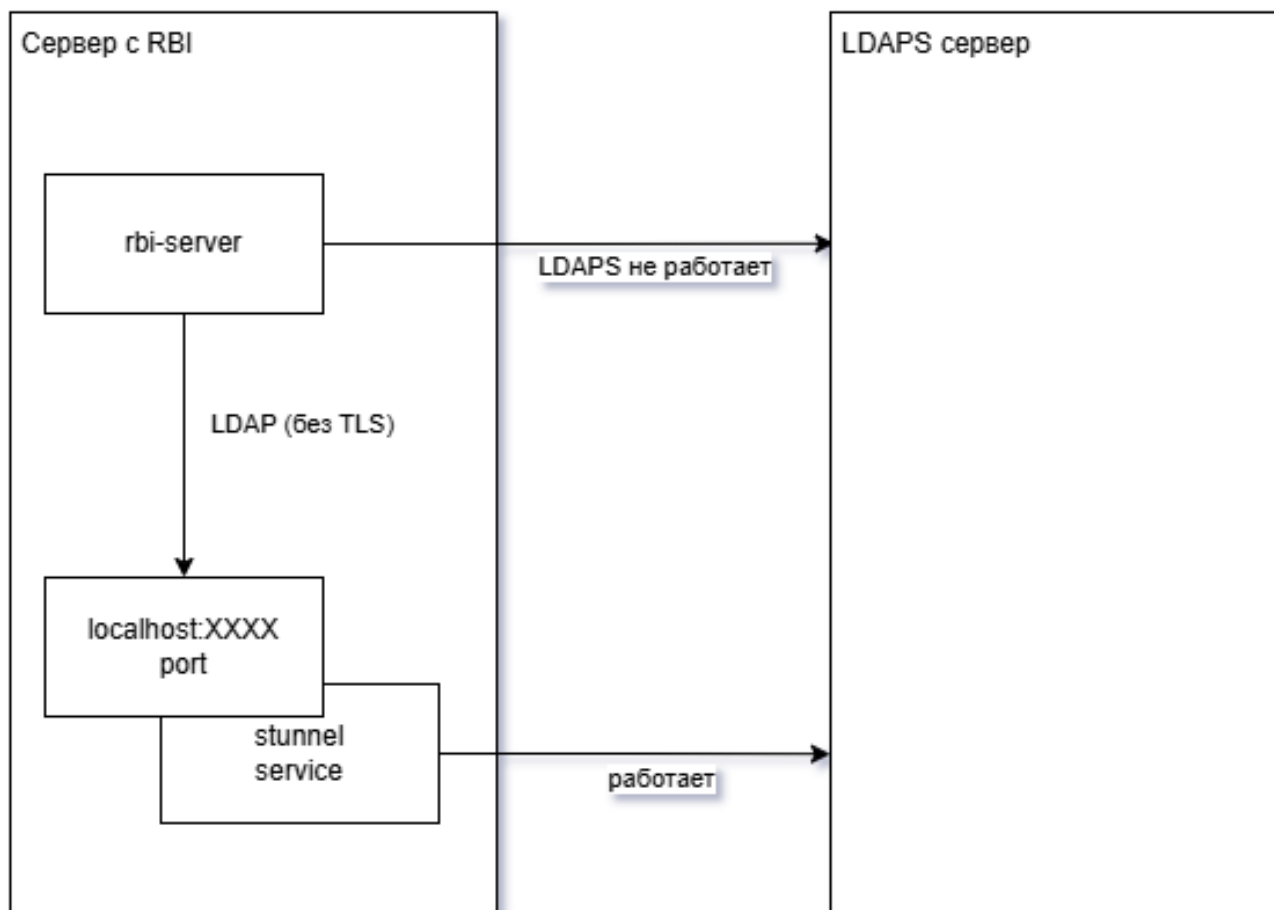


Рисунок 39 – Пример схемы подключения Stunnel

Внимание! В случае работы в режиме высокой доступности установить и настроить прокси-сервис Stunnel необходимо на каждом брокере.

11.16 Работа с продуктовыми метриками

11.16.1 Продуктовые метрики

Для мониторинга состояния и производительности ПК «Ankey RBI» используются продуктовые метрики, которые активный сервер автоматически публикует через HTTP-эндпоинты, предназначенные для интеграции с системами мониторинга: /api/v1/metrics для системы Prometheus и /api/v1/zabbix для ZABBIX.

Метрики представляют из себя счетчики (counter) или значения (gauge), которые накапливаются в памяти с момента старта сервиса. Тип данных float/int.

Список метрик и их описание представлены в таблице 9.

Таблица 9 – Продуктовые метрики

Наименование	Тип	Опции	Описание
rbi_running_containers	значение, int	{uuid=«node-uuid»}	Количество загруженных

Наименование	Тип	Опции	Описание
			контейнеров на узле
rbi_connected_containers	значение, int	{uuid=«node-uuid»}	Количество подключенные контейнеров на узле
rbi_node_last_heartbeat	значение, int	{uuid=«node-uuid»}	UNIX timestamp последнего webhook с этого узла
rbi_assignment_seconds_sum	счетчик, float	{uuid=«node-uuid»}	Количество секунд затраченных на выполнение скрипта rbi_start_container
rbi_assignment_seconds_count	счетчик, int	{uuid=«node-uuid»}	Количество запусков скрипта rbi_start_container
rbi_auth_requests	счетчик, int	{type=«local/domain»}	Количество попыток аутентификации
rbi_auth_errors	счетчик, int	{type=«local/domain»}	Количество ошибок аутентификации
rbi_api_errors	счетчик, int		Количество ошибок, которое вернул API (не учитывая webhook и авторизацию)
rbi_api_requests	счетчик, int		Количество запросов к API (не учитывая webhook и авторизацию)
rbi_files_upload_count	счетчик, int		Количество попыток загрузки файлов на сервер
rbi_files_upload_bytes	счетчик, int		Количество байт загруженных файлов на сервер
rbi_files_download_count	счетчик, int		Количество попыток скачивания файлов с сервера
rbi_files_download_bytes	счетчик, int		Количество байт скачанных файлов с сервера
rbi_uptime	счетчик, int		Время с момента запуска брокера
rbi_auth_requests_ldap	счетчик, int		Количество попыток LDAP аутентификации

11.16.2 Настройка ZABBIX для отображения метрик

Перед началом настройки ZABBIX для сбора метрик необходимо скачать шаблон по адресу: https://<FQDN rbi-server>/template_6_4.xml, где «FQDN rbi-server» сетевой адрес брокера ПК «Ankey RBI».

Далее необходимо зайти в панель управления ZABBIX, перейти в раздел «Сбор данных» → «Шаблоны» и загрузить ранее сохраненный шаблон. Для этого в правом верхнем углу нажать кнопку «Импорт» (рис. 40) и в открывшемся окне выбрать файл шаблона.

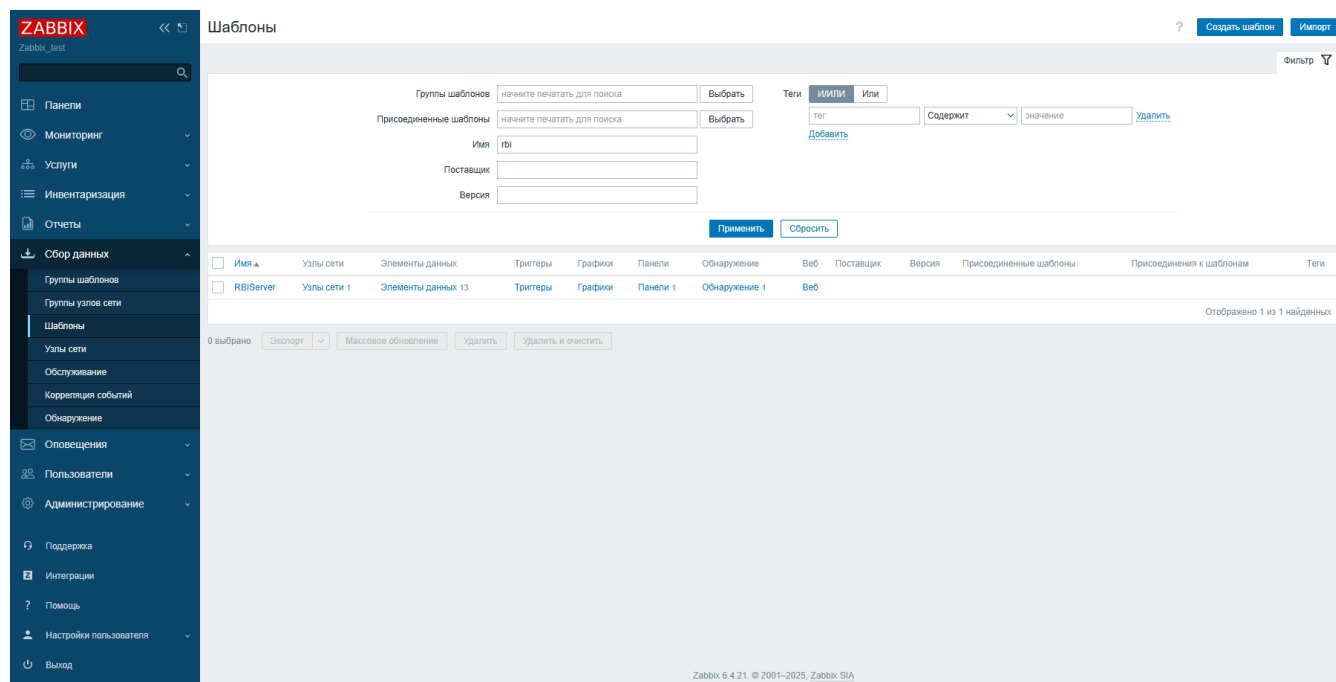


Рисунок 40 – Окно «Шаблоны»

После загрузки шаблона необходимо перейти к настройке узлов сети. Для этого необходимо перейти в раздел «Сбор данных» → «Группы узлов сети» (рис. 41) и в правом верхнем углу нажать кнопку «Создать группу узлов сети». В открывшемся окне в поле «Имя группы» ввести имя создаваемой группы узлов сети и нажать кнопку «Добавить». После этого группа узлов сети отобразится в списке.

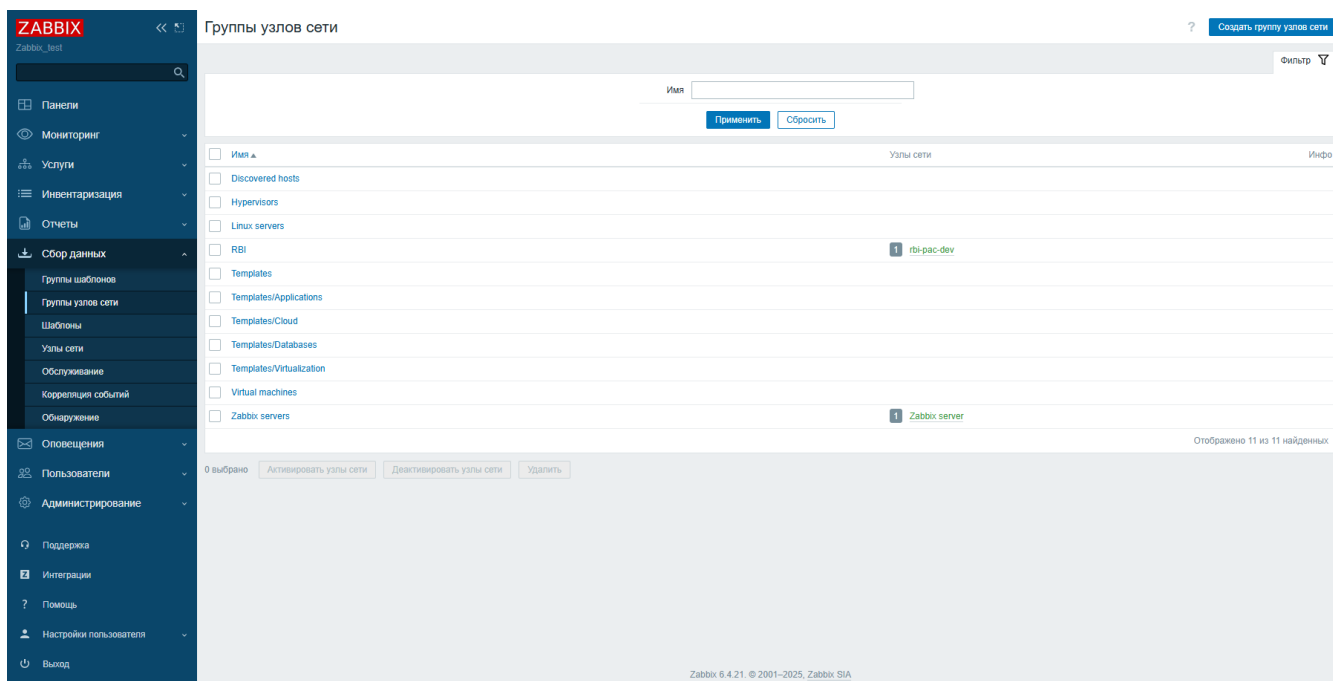


Рисунок 41 – Окно «Группы узлов сети»

Далее перейти в раздел «Сбор данных» → «Узлы сети» и в правом верхнем углу нажать кнопку «Создать узел сети» (рис. 42).

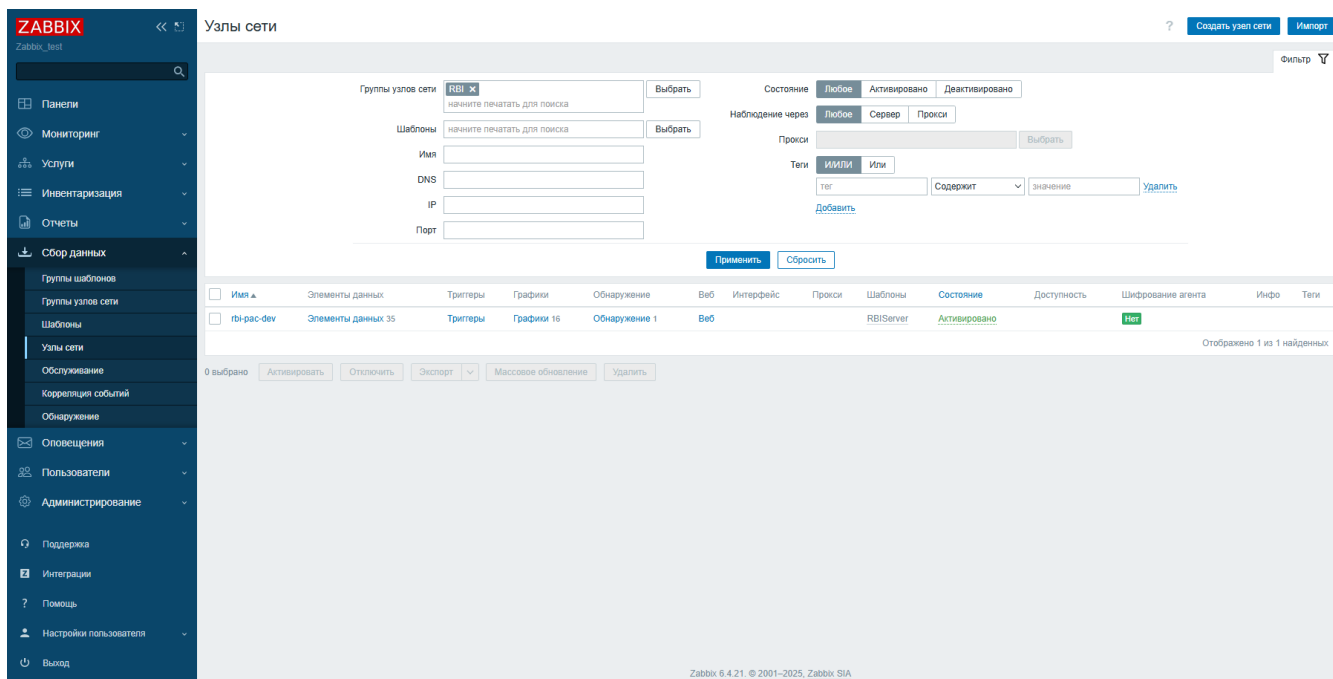


Рисунок 42 – Окно «Узлы сети»

В открывшемся окне (рис. 43) на вкладке «Узел сети»:

- в поле «Имя узла сети» указать имя узла;
- в поле «Шаблоны» выбрать загруженный шаблон;
- в поле «Группы узлов сети» выбрать созданную ранее группу узлов сети.

Новый узел сети

Узел сети IPMI Теги Макросы Инвентаризация Шифрование Преобразование значений

* Имя узла сети

Видимое имя

Шаблоны начните печатать для поиска

* Группы узлов сети RBI

Интерфейсы Интерфейсы не заданы.

[Добавить](#)

Описание

Наблюдение через прокси (без прокси)

Активировано ☒

Рисунок 43 – Окно «Новый узел сети»

Далее перейти на вкладку «Макросы» → «Макросы узла сети» и заполнить следующие поля:

- в поле «Макрос» указать `{RBI_URL}` (наименование макроса);
- в поле «Значение» указать FQDN или IP-адрес брокера ПК «Ankey RBI» или, при использовании режима высокой доступности, кластерный IP-адрес или FQDN кластерного IP. Например, 10.16.111.25 или rbi.example.server;
- в поле «Описание» указать описание макроса (необязательно).

После заполнения полей необходимо нажать кнопку «Добавить» и созданный узел сети появится в списке.

Для просмотра метрик необходимо перейти в раздел «Мониторинг» → «Узлы сети», найти строку созданного узла и в колонке «Панели» нажать кнопку «Панели». После этого откроется окно с продуктовыми метриками ПК «Ankey RBI» (рис. 44).



Рисунок 44 – Окно с отображением метрик

Примечание. Автоматическое создание элементов данных, триггеров, графиков и других сущностей на основе обнаруженных объектов происходит с задержкой по времени, так как ZABBIX выполняет обнаружение с определенной периодичностью.

11.16.3 Настройка сервисов Prometheus и Grafana для отображения метрик

Внимание! Требуется наличие рабочих сервисов Prometheus и Grafana.

Сначала необходимо настроить сервис Prometheus. Для этого:

- 1) Необходимо открыть файл «prometheus.yml», выполнив команду:

```
sudo nano /etc/prometheus/prometheus.yml
```

- 2) В файл добавить следующие строки, где в полях «targets» и «server_name» указать FQDN брокера ПК «Ankey RBI» или, при использовании режима высокой доступности, FQDN кластерного IP:

```
- job_name: "rbi-servers"
  scheme: https
  tls_config:
    ca_file: /<путь к сертификату>/<название корневого сертификата>.pem (или crt)
    server_name: "rbi-server.example.local"
  metrics_path: /api/v1/metrics
  static_configs:
    - targets:
      - "rbi-server.example.local:443"
      labels:
        env: rbi
```

- 3) Перезапустить сервис Prometheus, выполнив команду:

```
sudo systemctl restart prometheus.service
```

Далее необходимо перейти в панель управления Grafana и выполнить следующие действия:

- 1) Перейти в раздел «Connections» → «Data sources», нажать кнопку «Add data source» (или «Add new data source» если в системе уже есть источники данных) и далее выбрать в качестве источника данных Prometheus (рис. 45).

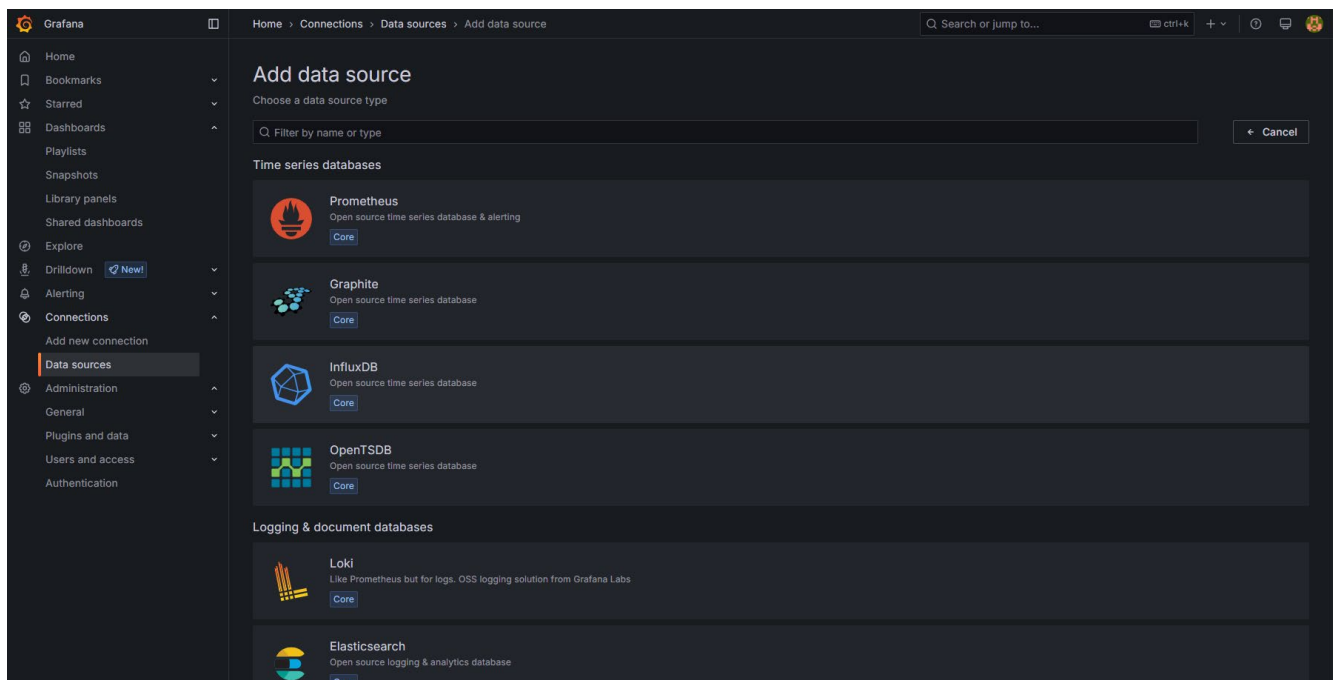


Рисунок 45 – Выбор источника данных

- 2) В открывшемся окне в поле «Prometheus server URL» ввести IP-адрес сервиса Prometheus в формате `http://localhost:9090/` и нажать кнопку «Save&test». Для индивидуализации источника можно изменить название в поле «Name».
- 3) Далее необходимо перейти в раздел «Dashboards» (рис. 46), нажать кнопку «Create dashboard» (или «New») и далее выбрать пункт «Import dashboard» или «Import», если использовалась кнопка «New».

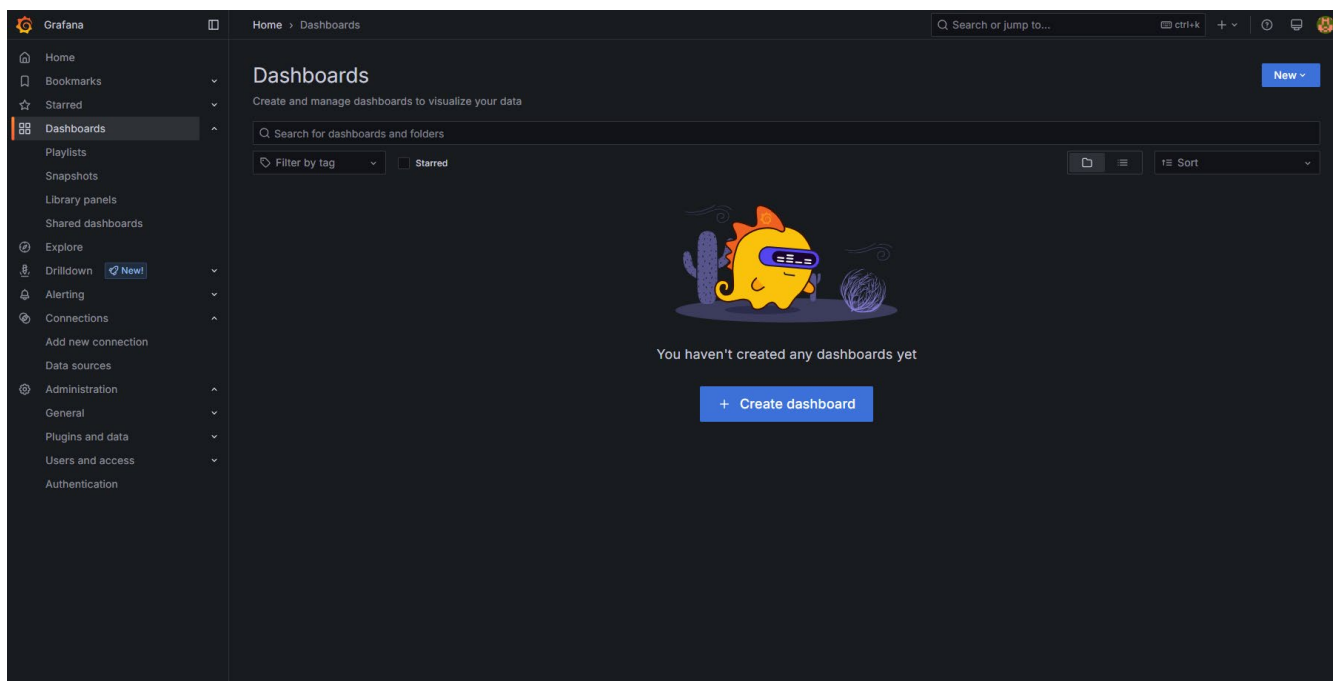


Рисунок 46 – Раздел «Dashboards»

- 4) Загружаем файл «rbi_grafana_dashboard.json». Файл находится по адресу: https://<FQDN rbi-server>/rbi_grafana_dashboard.json, где «FQDN rbi-server» сетевой адрес брокера ПК «Ankey RBI». После загрузки файла запись «RBI Product Metrics» появится в разделе «Dashboards».
- 5) Для просмотра метрик необходимо перейти в раздел «Dashboards», найти строку «RBI Product Metrics» и нажать на нее. После этого откроется окно с продуктовыми метриками ПК «Ankey RBI» (рис. 47).

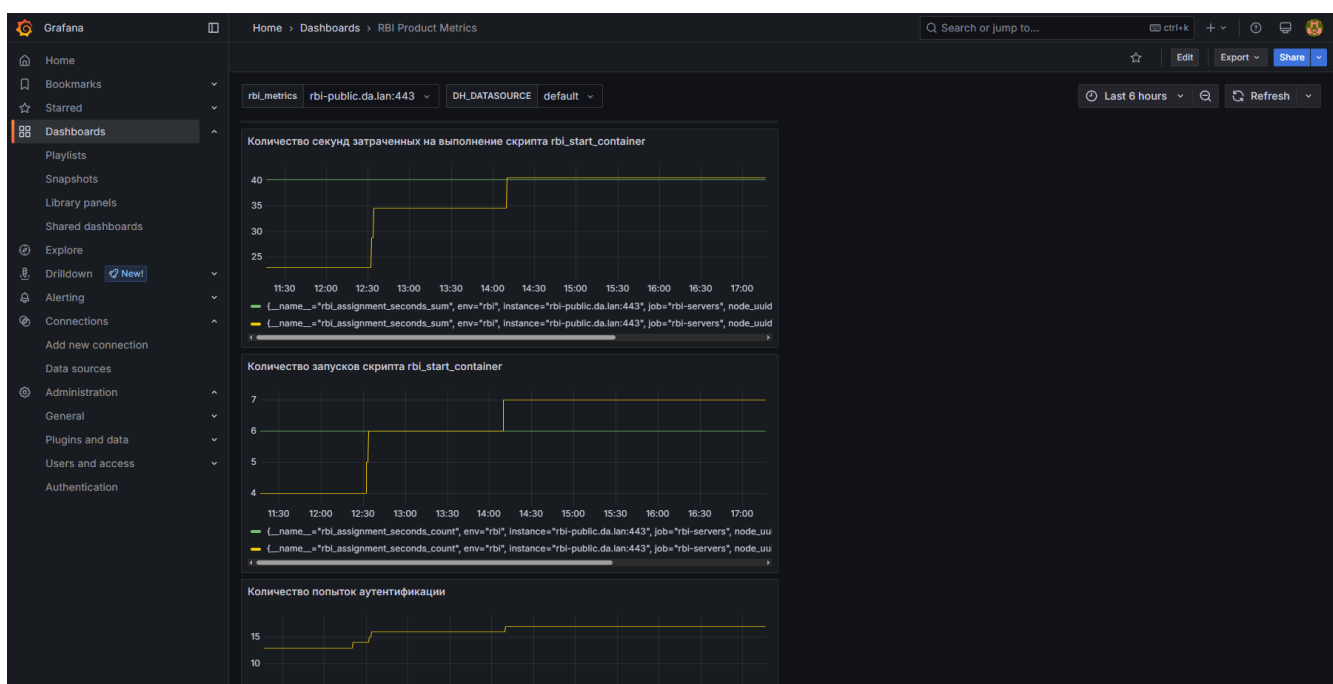


Рисунок 47 – Окно с отображением метрик

Перечень сокращений

В настоящем документе применены следующие сокращения:

CA	–	Certification Authority
CSR	–	Certificate Signing Request
DN	–	Distinguished Name
DNS	–	Domain Name System
DRBD	–	Distributed Replicated Block Device
FQDN	–	Fully Qualified Domain Name
KDC	–	Key Distribution Center
LDAP	–	Lightweight Directory Access Protocol
LDAPS	–	LDAP over SSL/TLS
NAS	–	Network Attached Storage
NFS	–	Network File System
OCFS2	–	Oracle Cluster File System
SMBFS	–	SAMBA File System
SPN	–	Service Principal Name
TGS	–	Ticket Granting Service
TLS	–	Transport Layer Security
АРМ	–	автоматизированное рабочее место
БД	–	база данных
ОС	–	операционная система
ПК	–	программный комплекс
ПО	–	программное обеспечение
СУБД	–	система управления базами данных
УЗ	–	учетная запись
ЭП	–	электронная подпись

Перечень терминов и определений

В настоящем документе применены следующие термины с соответствующими определениями:

Агент	– сервис, который управляет запущенными контейнерами на узле и отправляет на брокер необходимую информацию об узле и контейнерах.
Агент контейнера	– компонент, необходимый для работы клиентского приложения, который работает в каждом из контейнеров с запущенным изолированным приложением.
Брокер	– сервис для управления Docker-контейнерами и подключениями клиентских приложений к контейнерам. На брокере реализован веб-интерфейс программного комплекса.
Клиентское приложение (клиент)	– программа, установленная на АРМ пользователя, которая обеспечивает взаимодействие пользователя с изолированным приложением.
Контейнер	– экземпляр образа.
Образ	– Docker-образ, содержащий в себе всю необходимую программную среду для создания и запуска изолированного приложения, а также необходимый для работы клиентского приложения.
Скринсейвер	– специальная программа по сохранению состояния экрана, которая запускается через определенный промежуток времени, если пользователь оставил сессию в неактивном состоянии.
Узел	– сервер (или виртуальная машина) под управлением операционной системы РЕД ОС, на котором фактически работают контейнеры с изолированными приложениями (браузерами). На узле установлены и работают Docker и агент.
Docker	– программное обеспечение для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации, контейнеризатор приложений.
GlusterFS	– распределенная отказоустойчивая файловая система.
X.509 (PEM)	– файл (с расширением PEM) сертификата безопасности, который используется для установления безопасного канала связи между веб-сервером и браузером. Содержит закрытый ключ, сертификат сервера и/или комбинацию других сертификатов.
PKCS#12 (PFX)	– файл (с расширением PFX), содержащий сертификат и соответствующий секретный ключ.

Приложение 1

В настоящем приложении представлено описание параметров, которые используются в командах для подготовки службы каталогов.

Примечание. При вводе параметров необходимо соблюдать регистр букв.

Параметр	Описание	Пример
<имя правила>	Имя правила, которое разрешает ограниченное Kerberos делегирование rbi-серверу	rbi-rule
<имя правила для делегирования>	Имя правила разрешающего производить ограниченное Kerberos делегирование для прокси сервера	target-rbi-rule
<имя брокера>	DNS имя для брокера	rbi-server
<имя первого узла>	DNS имя для первого узла	rbi-node-01
<имя второго узла>	DNS имя для второго узла	rbi-node-02
<доменное имя>	Доменное имя с указанием доменной зоны	example.ru
<SPN для брокера>	SPN для брокера. Указывается в следующем формате: {тип службы}/{FQDN имя узла службы}	HTTP/rbi-server.example.ru
<SPN для прокси сервера>	SPN для прокси сервера. Указывается в следующем формате: {тип службы}/{FQDN имя прокси сервера}	HTTP/proxy.example.ru
<имя сервисной УЗ для брокера>	Имя сервисной УЗ для брокера	rbi-server-svc
<пароль УЗ брокера>	Пароль УЗ брокера	
<адрес контроллера домена>	Адрес контроллера домена	dc1.example.ru