

## Программный комплекс «Ankey RBI»

Описание применения

## Аннотация

Данный документ представляет собой описание применения программного комплекса «Ankey RBI» (далее – ПК «Ankey RBI», комплекс).

В разделе «Назначение» дан краткий обзор основных функций и возможностей комплекса.

В разделе «Условия применения» указаны условия, необходимые для использования комплекса, минимальный состав технических средств, который должны иметь серверы и автоматизированные рабочие места (АРМ) для установки комплекса.

В соответствующих разделах указаны задачи, которые решает комплекс, и функции, с помощью которых эти задачи решаются, а также описаны виды входных и выходных данных для основных функций комплекса.

# Содержание

1. Назначение .....	5
1.1. Назначение программы .....	5
1.2. Структура ПК и принцип работы .....	5
1.3. Роли и аутентификация пользователей .....	7
1.4. Функциональные возможности.....	7
2. Условия применения.....	9
2.1. Расчет минимального количества ядер центрального процессора .....	10
2.2. Расчет минимального количества оперативной памяти .....	10
2.3. Требования к сетевым взаимодействиям .....	11
3. Описание задачи .....	12
3.1. Защита от угроз при доступе в Интернет .....	12
3.2. Исключение ущерба при ошибке пользователя .....	12
4. Входные и выходные данные.....	13
4.1. Данные при работе клиента с контейнером .....	13
4.2. Входные данные.....	13
4.2.1. Настройка учетной записи локального администратора ПК «Ankey RBI» .....	14
4.2.2. Настройка подключения для интеграции со службами каталогов данных по протоколу LDAP .....	14
4.2.3. Настройка ролей для пользователей служб каталогов.....	15
4.2.4. Настройка HTTPS .....	15
4.2.5. Настройка взаимодействия по протоколу Kerberos .....	16
4.2.6. Настройка режима высокой доступности брокера.....	16
4.2.7. Настройка аудита.....	16
4.2.8. Настройка интеграции с антивирусным ПО.....	17
4.2.9. Настройка оповещения о критических состояниях .....	17
4.2.10. Параметр для настройки профиля по умолчанию .....	18
4.3. Выходные данные .....	18

Перечень терминов и определений.....	19
Перечень сокращений .....	20

# 1. Назначение

## 1.1. Назначение программы

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;
- обеспечение 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 экземпляров браузера в изолированном программном окружении (контейнере).

Ниже представлена функциональная схема ПК «Ankey RBI» (рис. 1.1).

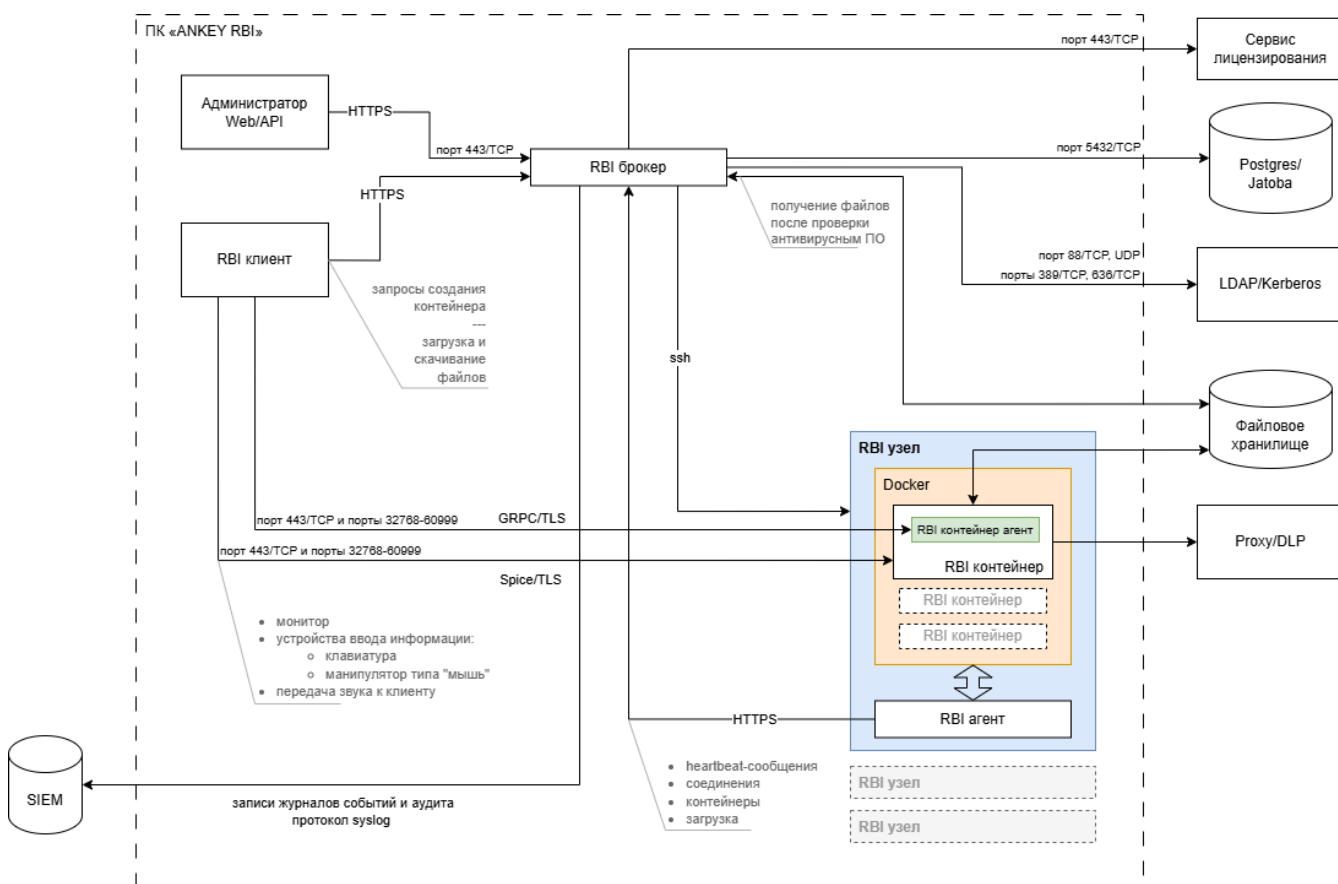


Рисунок 1.1– Функциональная схема ПК «Ankey RBI»

Для каждого пользователя на сервере ПК «Ankey RBI» запускается отдельный экземпляр браузера в 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 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. Роли и аутентификация пользователей

В ПК «Ankey RBI» реализована ролевая модель разграничения доступа. Группам пользователей назначаются права доступа в соответствии с ролевой моделью и принадлежностью пользователя группе безопасности. Для разграничения доступа авторизованных пользователей к функциональным возможностям в ПК «Ankey RBI» предусмотрены следующие роли:

- 1) Администратор – роль с полным доступом к функциям настройки и администрирования комплекса.
- 2) Аудитор – роль, имеющая ограниченный доступ к веб-интерфейсу, с возможностью просмотра журнала событий безопасности.
- 3) Пользователь – роль для доступа к изолированному приложению и с ограниченным доступом к веб-интерфейсу комплекса (только раздел «Мои файлы»).

Описание ролевой модели и сопоставление доступа к разделам веб-интерфейса ПК «Ankey RBI» в зависимости от выбранной роли представлено в подразделе 1.4 документа «Программный комплекс «Ankey RBI». Руководство администратора».

При аутентификации с использованием протокола Kerberos роль пользователя определяется по имени группы безопасности сервера каталогов (LDAP), в которой состоит учетная запись пользователя.

### 1.4. 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 буфера обмена как из изолированного приложения, так и с АРМ пользователя;
- интеграция с антивирусным ПО для проверки скачанных файлов;
- использование в изолированном приложении ключевых носителей, подключенных к АРМ пользователя.

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 службы каталога к профилям;
- контроль сессий пользователей;
- мониторинг вычислительных ресурсов, используемых комплексом;
- просмотр журнала системных событий и событий безопасности;
- экспорт журналов событий в формате CSV.



## 2. Условия применения

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

- количество ядер процессора: минимальное количество требуемых процессорных ядер рассчитывается на основе формул, приведенных в пункте 2.1 текущего документа;
- оперативная память: минимальное количество требуемой оперативной памяти рассчитывается на основе формул, приведенных в пункте 2.2 текущего документа;
- сетевой адаптер узла: подбирается из расчета 30 Мбит/с на каждого пользователя узла. Для того, чтобы рассчитать количество пользователей на один узел, необходимо планируемое количество пользователей ПК «Ankey RBI» разделить на количество узлов.

Установка брокера и агентов 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 клиента 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.);
- 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 с браузерами, которые работают на основе проекта с открытым кодом Chromium, начиная с версии 120 и выше, а также с браузером Mozilla Firefox, начиная с версии 121.0.1 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. Информация о настройке СУБД представлена в подразделе 2.1 документа «Программный комплекс «Ankey RBI». Руководство администратора».

## 2.1. Расчет минимального количества ядер центрального процессора

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

Алгоритм и формулы для расчета количества процессорных ядер представлен ниже.

Шаг первый – рассчитать количество потоков на один контейнер  $N_{1п}$  по формуле:

$$N_{1п} = N_{\text{exp}} \times K_{\text{и}}, (1)$$

где  $N_{\text{exp}}$  – количество потоков;

$K_{\text{и}}$  – коэффициент использования.

Рекомендуемые значения параметров для расчета количества потоков представлены в таблице 2.1.

Таблица 2.1– Значения параметров для расчета количества потоков

Параметр	Значение
$N_{\text{exp}}$	0,5
$K_{\text{и}}$	0,5

Шаг второй – рассчитать количество ядер на один контейнер  $N_{1я}$  по формуле:

$$N_{1я} = \frac{N_{1п}}{2}, (2)$$

Шаг третий – рассчитать общее количество ядер  $N_{\text{sum}}$  по формуле:

$$N_{\text{sum}} = N_{1я} \times X, (3)$$

где  $X$  – количество контейнеров.

В случае отклонения профиля нагрузки от среднестатистического коэффициент использования  $K_{\text{и}}$  может измениться.

## 2.2. Расчет минимального количества оперативной памяти

Для корректного функционирования ПК «Ankey RBI» необходимо рассчитать минимальное количество оперативной памяти узлов, требуемой для запуска контейнеров.

Алгоритм и формулы для расчета количества оперативной памяти представлен ниже.

Шаг первый – рассчитать объем требуемой памяти на один контейнер  $V_{1\text{mem}}$  по формуле:

$$V_{1\text{mem}} = V_{\text{exp}} \times K_{\text{tmp}} \times K_{\text{buf}} \times K_{\text{tab}}, (4)$$

где  $V_{\text{exp}}$  – количество памяти на один контейнер;

$K_{\text{tmp}}$  – коэффициент памяти под временные файлы;

$K_{\text{buf}}$  – коэффициент памяти под системные буферы;

$K_{tab}$  – коэффициент использования вкладок.

Рекомендуемые значения параметров для расчета количества памяти представлены в таблице 2.2.

Таблица 2.2– Значения параметров для расчета количества памяти

Параметр	Значение
$V_{exp}$	0,75 Гб
$K_{tmp}$	1,15
$K_{buf}$	1,2
$K_{tab}$	1,5

Шаг второй – рассчитать общий объем памяти  $V_{1sum}$  по формуле:

$$V_{1sum} = V_{1mem} \times X, (5)$$

где  $X$  – количество контейнеров.

В случае отклонения профиля нагрузки от среднестатистического коэффициенты могут измениться.

### 2.3. Требования к сетевым взаимодействиям

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

- 1) Исходящие взаимодействия из подсети, в которой установлен «Ankey RBI» 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.
- 2) Входящие взаимодействия в подсеть, в которой установлен ПК «Ankey RBI» 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 RBI» (см. рис. 1.1).

## 3. Описание задачи

ПК «Ankey RBI» решает следующие задачи:

- защита от угроз при доступе в Интернет;
- исключение ущерба при ошибке пользователя.

### 3.1. Защита от угроз при доступе в Интернет

ПК «Ankey RBI» обеспечивает запуск веб-браузера в изолированном окружении на удаленном сервере, а не на АРМ пользователя. Обработка веб-контента происходит на удаленном сервере, после чего сервер отправляет видеопоток на АРМ пользователя. Таким образом, ПК «Ankey RBI» переносит риски использования сети Интернет (запуск вредоносного кода, скрытый майнинг и т. д.) с АРМ пользователя в изолированное окружение на удаленном сервере.

### 3.2. Исключение ущерба при ошибке пользователя

ПК «Ankey RBI» позволяет предотвратить заражение вредоносными программами внутренних сетей предприятия, которые могут возникнуть при ошибке пользователя, например, при случайном скачивании вредоносного файла или при переходе по ссылкам, ведущим на фишинговые сайты.

## 4. Входные и выходные данные

### 4.1. Данные при работе клиента с контейнером

При работе клиента с контейнером, содержащим изолированное приложение, осуществляется следующее взаимодействие:

- 1) Взаимодействие клиента с выделенным контейнером с изолированным приложением по протоколам SPICE-TLS и GRPC-TLS.
- 2) Обмен файлами пользователей. Описание параметров и ограничений файлов, загружаемых в веб-интерфейс ПК «Ankey RBI», приведены в таблице 4.1. К файлам, скачанным из сети Интернет при работе с клиентом ПК «Ankey RBI», требования к названию, формату и размеру не предъявляются.

Таблица 4.1– Параметры и ограничения файлов

Параметр	Описание
Название	Название может содержать любые символы, цифры, буквы. Ограничения: – длина названия должна составлять не более 124 знаков при использовании кириллицы или символов и не более 255 при использовании букв латинского алфавита; – название не должно быть пустым (состоять из пробелов)
Формат	В комплексе не предусмотрено ограничений по допустимым форматам загружаемых файлов. Установка образов доступна только из файлов с расширением TAR и только пользователю с ролью администратора
Размер	Размер загружаемых файлов зависит только от объема свободной памяти на носителе информации (физическом или виртуальном) для хранения файлов пользователей
Количество одновременно загружаемых файлов	10

### 4.2. Входные данные

В веб-интерфейсе реализована возможность управлением следующими параметрами при наличии соответствующих полномочий (согласно ролевой модели, представленной в подразделе 1.3 настоящего руководства):

- данные аутентификации пользователей;

- настройки системы;
- профили;
- образы контейнеров;
- настройки узлов;
- настройки пользователей и групп;
- запросы пользователей на запуск контейнеров.

Указанные выше параметры являются входными данными для ПК «Ankey RBI».

Настройки системы представлены в виде девяти групп параметров (пункты 4.2.1 – 4.2.10), объединенных по назначению, а также одного отдельного параметра.

#### 4.2.1. Настройка учетной записи локального администратора ПК «Ankey RBI»

Описание параметров, используемых при работе с учетной записью локального администратора, приведено в таблице 4.2.

Примечание. Имя пользователя и пароль следует вводить с учетом регистра.

Таблица 4.2– Состав и описание параметров локального администратора ПК «Ankey RBI»

Параметр	Описание
Имя пользователя	Требования к имени пользователя: <ul style="list-style-type: none"><li>– длина имени должна составлять от 2 до 64 символов;</li><li>– имя может содержать цифры и заглавные/строчные буквы латинского алфавита</li></ul>
Пароль	Требования к паролю пользователя: <ul style="list-style-type: none"><li>– в пароле должно быть не менее 4 уникальных символов;</li><li>– длина пароля должна составлять от 2 до 64 символов;</li><li>– пароль может содержать цифры и заглавные/строчные буквы латинского алфавита;</li><li>– пароль может содержать следующие специальные символы: (пробел) ! " # \$ % &amp; ' ( ) * + , - . / : ; &lt; = &gt; ? @ [ ] ^ _ ` { } ~</li></ul>

#### 4.2.2. Настройка подключения для интеграции со службами каталогов данных по протоколу LDAP

Описание параметров, вводимых для настройки работы ПК «Ankey RBI» с внешними LDAP-каталогами, приведено в таблице 4.3.

Таблица 4.3– Параметры настройки работы ПК «Ankey RBI» с внешними каталогами данных

Параметр	Описание
----------	----------

Параметр	Описание
Вид службы каталогов	Параметр для выбора вида службы каталогов. Выпадающий список со следующими значениями: <ul style="list-style-type: none"><li>– «FreeIPA»;</li><li>– «Microsoft AD DS или Samba DC»</li></ul>
LDAP сервер	Текстовое поле для ввода адреса LDAP/LDAPS-сервера
LDAP admin DN	Текстовое поле для ввода идентификатора пользователя LDAP, имеющего права на просмотр информации о пользователях каталога и группах безопасности каталога
Пароль LDAP	Текстовое поле для ввода пароля пользователя, указанного в поле «LDAP admin DN»
LDAP base DN	Текстовое поле для ввода базового объекта каталога, с которого начинается поиск записей

#### 4.2.3. Настройка ролей для пользователей служб каталогов

Описание параметров, вводимых для настройки сопоставления групп службы каталогов с ролями ПК «Ankey RBI», приведено в таблице 4.4.

Таблица 4.4– Параметры настройки работы ПК «Ankey RBI» с внешними каталогами данных

Параметр	Описание
LDAP группа администраторов	Выпадающий список для выбора группы. Всем пользователям, входящим в эту группу, будет назначена роль администратора
LDAP группа аудиторов	Выпадающий список для выбора группы. Всем пользователям, входящим в эту группу, будет назначена роль аудитора
LDAP группа пользователей	Выпадающий список для выбора группы. Всем пользователям, входящим в эту группу, будет назначена роль пользователя СБДИ

#### 4.2.4. Настройка HTTPS

Описание параметров, вводимых для настройки HTTPS, приведено в таблице 4.5.

Таблица 4.5– Параметры настройки HTTPS

Параметр	Описание
Адрес RBI-сервера	Текстовое поле для ввода сетевого адреса сервера

Параметр	Описание
Корневые сертификаты	Поле для загрузки файла сертификата с расширением PEM или указания содержимого PEM-файла
Редактировать как текст	Переключатель, отвечающий за формат загрузки корневых сертификатов
Ключ HTTPS-сервера	Текстовое поле для указания ключа HTTPS сервера
Сертификат-HTTPS сервера	Текстовое поле для указания сертификата HTTPS сервера
Секретный ключ JWT	Текстовое поле для указания секретного ключа JWT
Время жизни JWT, сек	Поле для указания времени жизни токена доступа

#### 4.2.5. Настройка взаимодействия по протоколу Kerberos

Описание параметров, вводимых для настройки взаимодействия по протоколу Kerberos, приведено в таблице 4.6.

Таблица 4.6– Параметры настройки Kerberos

Параметр	Описание
Kerberos realm	Текстовое поле для ввода имени домена
Keytab-файл сервиса	Поле для загрузки файла в формате .keytab

#### 4.2.6. Настройка режима высокой доступности брокера

Описание параметров, необходимых при использовании режима высокой доступности, приведено в таблице 4.7.

Таблица 4.7– Параметры настройки высокой доступности

Параметр	Описание
Кластерный IP	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

#### 4.2.7. Настройка аудита

Описание параметров, вводимых для настройки аудита, приведено в таблице 4.8.



Таблица 4.8– Параметры настройки высокой доступности

Параметр	Описание
Удалять записи аудита через, дней	Поле для указания количества дней, через которое все записи в разделе «Аудит» будут удалены. Устанавливаемое значение должно быть равно 365 или больше. Значение меньше 365 установить нельзя. Если данные аудита требуется оставить без автоматического удаления, то данное поле необходимо оставить пустым
Адрес SIEM syslog-сервера	Поле для указания адреса дополнительного сервера, на который будут продублированы сообщения о событиях безопасности

#### 4.2.8. Настройка интеграции с антивирусным ПО

Описание параметров, вводимых для настройки интеграции с антивирусной программой, приведено в таблице в таблице 4.9.

Таблица 4.9– Параметры настройки высокой доступности

Параметр	Описание
Использовать антивирусную программу	Выпадающий список, в котором необходимо выбрать антивирусную систему или отказаться от ее использования. В поле доступны следующие значения: – «Нет» – антивирусная система не будет использоваться; – «Kaspersky Scan Engine» – будет использована антивирусная система Kaspersky Scan Engine. При скачивании файлов на АРМ пользователя из раздела веб-интерфейса «Мои файлы» будет проведена проверка на наличие вирусов и угроз
Адрес KSE	Адрес используемой антивирусной системы Kaspersky Scan Engine. Указывается только в случае, если выбрано использование антивирусной системы Kaspersky Scan Engine в параметре «Использовать антивирус»

#### 4.2.9. Настройка оповещения о критических состояниях

Описание параметров, вводимых для настройки оповещений о критических состояниях, приведено в таблице 4.10.

Таблица 4.10– Параметры настройки высокой доступности

Параметр	Значение
SMTP-сервер	Адрес сервера, который используется для отправки и получения

Параметр	Значение
	сообщений электронной почты через Интернет
Email источника оповещений	Email, с которого пользователям будут отправлены уведомления
Получатели оповещений	Email пользователей, которые будут получать уведомления. Указываются через запятую
Типы уведомлений	Для настройки типов уведомлений доступны четыре переключателя: <ul style="list-style-type: none"><li>– «Выключить все уведомления»;</li><li>– «Недоступность брокера»;</li><li>– «Использование ОЗУ узла больше чем на 80%»;</li><li>– «Использование ОЗУ брокера больше чем на 80%»;</li><li>– «Использование дискового пространства узла больше чем на 80%»;</li><li>– «Использование дискового пространства брокера больше чем на 80%»;</li><li>– «Загрузка процессора узла больше чем 90% в течение 5 минут»;</li><li>– «30 дней до истечения одного из сертификатов»</li></ul>

#### 4.2.10. Параметр для настройки профиля по умолчанию

Параметр представляет собой поле для выбора профиля по умолчанию. Выпадающий список с профилями становится доступен после создания хотя бы одного профиля.

### 4.3. Выходные данные

К выходным данным ПК «Ankey RBI» относятся:

- информация о запущенных контейнерах;
- журнал системных событий. Выгрузка журнала системных событий осуществляется по запросу администратора/аудитора в файлы формата CSV.

## 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.  |
| 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.  |
| РЕМ                            | – файл сертификата безопасности, который используется для установления безопасного канала связи между веб-сервером и браузером. Имеет кодировку Base64 и содержит закрытый ключ, сертификат сервера и/или комбинацию других сертификатов. |

## Перечень сокращений

В настоящем документе применены следующие сокращения:

AD DS	–	Active Directory Domain Services
CA	–	Certification Authority
DN	–	Distinguished Name
FreeIPA	–	Free Identity, Policy and Audit
LDAP	–	Lightweight Directory Access Protocol
LDAPS	–	LDAP over SSL/TLS
TCP	–	Transmission Control Protocol
TLS	–	Transport Layer Security
UDP	–	User Datagram Protocol
АРМ	–	автоматизированное рабочее место
БД	–	база данных
ОС	–	операционная система
ПК	–	программный комплекс
ПО	–	программное обеспечение
СБДИ	–	системы безопасного доступа в сеть Интернет
СУБД	–	система управления базами данных
ЭП	–	электронная подпись