

ПРОГРАММНЫЙ КОМПЛЕКС
«МЕНЕДЖЕР УПРАВЛЕНИЯ КОРПОРАТИВНЫМИ СЕКРЕТАМИ
НАSPBOX»

Жизненный цикл программного обеспечения

Листов 15

Оглавление

Введение	3
Термины и определения	4
Перечень сокращений.....	5
Общие сведения.....	5
Состав и функции компонентов Системы.....	6
Условия применения	8
Требования к техническим средствам	8
Требования и условия организационного характера	9
Требования и условия технического характера	9
Требования и условия технологического характера.....	9
Требования к квалификации персонала сопровождения	10
Загрузка и установка	10
Входные и выходные данные	10
Поддержание работоспособности ПО	10
Параметры работ по поддержанию жизненного цикла	10
Требования к производительности Системы.....	11
Обязанности системного администратора	12
Процедура резервного копирования	12
Процедура резервного восстановления	13
Тестирование Системы после перезапуска.....	13
Устранение неисправностей, выявленных в ходе эксплуатации	14
Сообщения об ошибках и исключительные ситуации	14
Совершенствование ПО	15
Техническая поддержка.....	15

Введение

Данный документ содержит описание процессов, обеспечивающих поддержание жизненного цикла программного обеспечения, в том числе устранение неисправностей, выявленных в ходе эксплуатации программного обеспечения, совершенствование программного обеспечения, а также информацию о персонале, необходимом для обеспечения такой поддержки.

Термины и определения

Термин	Определение
Заказчик	Заказчик Системы
Исполнитель	ООО «ХАСПБОКС»
Модуль ротации и управления секретами	Компонент, отвечающий за хранение секретов
Пользователь	Сотрудник Заказчика, обладающий правом доступа к Системе
Программное обеспечение (ПО)	Совокупность компьютерных программ и программных документов, необходимых для эксплуатации этих программ
Система	HASPBOX
Haspboxsvc	Компонент, отвечающий за аутентификацию, авторизацию и связь с базой данных
PostgreSQL	Реляционная система управления базами данных, в которых хранятся все данные для работы системы. Все критические данные (такие как сгенерированные пароли – шифруются с использованием компонента – Haspbox CSP)
HaspboxCSP	Компонент, отвечающий за взаимодействие с отечественной системой криптографической защиты «КриптоПРО CSP 5.0»
HaspboxRE	Компонент, отвечающий за взаимодействие с внешними системами, для управления и ротации паролей.

Перечень сокращений

Сокращение	Расшифровка
БД	База данных
ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
API	Application programming interface
CPU	Central processing unit

Общие сведения

Программный комплекс «Менеджер управления корпоративными секретами HASPBOX» (далее HASPBOX) — это инструмент для хранения и управления паролями и секретами на основе парольных политик. Рабочий процесс HASPBOX обеспечивает контроль безопасности и интеграцию на нескольких уровнях, отслеживая и управляя доступом пользователей посредством:

- жестких ограничений на основе уникальных идентификаторов пользователя;
- доступа к учетным данным для сеансов через модуль ротации и управления секретами;
- управления инфраструктурой внутри кода для автоматизации настройки разрешений пользователей;

HASPBOX позволяет пользователям, аутентифицированным локально в системе, получать авторизованный доступ к целевым системам на основе заданных политик доступа, которые определены в HASPBOX. Доступ к целевым системам осуществляется с помощью уникальных идентификаторов.

Основные особенности и преимущества HASPBOX:

- доступ на основе уникальных идентификаторов;
- мониторинг событий;
- использование сертифицированных средств криптографической защиты (КриптоПРО CSP не ниже версии 5.0);
- возможность работы на отечественной ОС Astra linux SE не ниже версии 1.7

Состав и функции компонентов Системы

Система представляет собой микросервисную инфраструктуру. Составные компоненты Системы:

- haspbox.core
Обеспечивает базовые функции системы по хранению и управлению инфраструктурой секретов, взаимодействием с пользователями по средствам пользовательского интерфейса
- haspbox.api
Обеспечивает функциональные возможности межпрограммного взаимодействия с внешними системами по средствам REST API
- haspbox.auth
Обеспечивает функциональные возможности по авторизации пользователей в системе
- haspbox.kv
Обеспечивает функциональные возможности управления секретами формата «ключ-значение»
- haspbox.crypto
Обеспечивает функциональные возможности по взаимодействию с внешним сервисом КриптоПРО CSP для генерации случайных чисел по алгоритму ГОСТ Р ИСО 28640-2012 и шифрования данных по алгоритму ГОСТ Р 34.12-2015;
- haspbox.rotate
Обеспечивает функциональные возможности по управлению секретами на конечных информационных системах, поддерживаемых ПК HASPBOX

Функциональная схема взаимодействия компонентов представлена на рисунке 1:

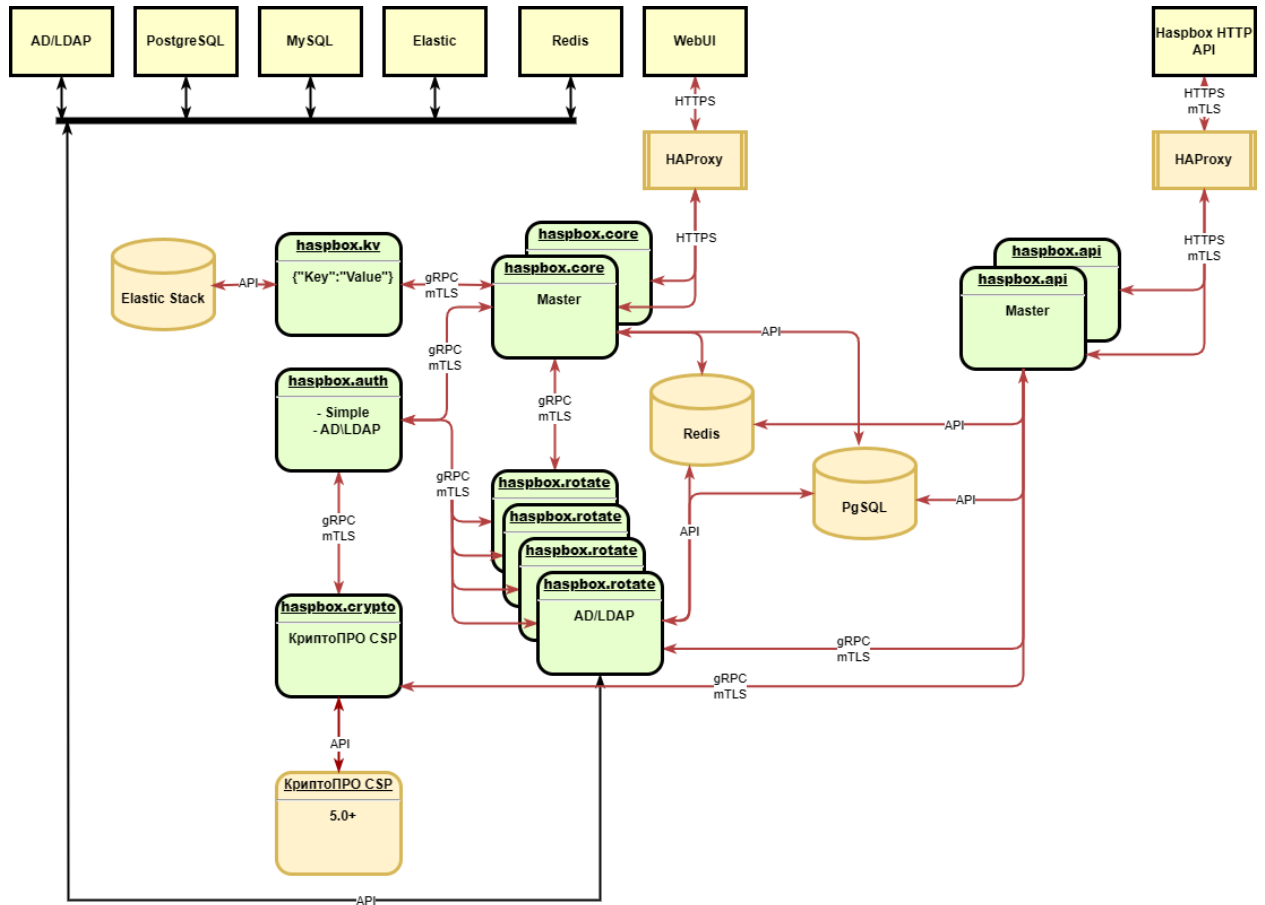


Рисунок 1. Функциональная схема

Условия применения

Требования к техническим средствам

Требования к техническим средствам для установки компонентов Haspbox представлены в табл. 1–2.

Табл. 1. Требования для установки компонентов системы на одном сервере

Платформа	Linux
Количество ядер центрального процессора	От 2
Оперативная память	От 4 ГБ
Дисковое пространство	От 100 ГБ

Табл. 2. Требования для установки haspbox.crypto

Платформа	Linux
Количество ядер центрального процессора	От 2
Оперативная память	От 4 ГБ
Установленное ПО «КриптоПРО CSP» не ниже версии 5.0	Да
Дисковое пространство	От 100 ГБ

Подключение к интерфейсу Системы осуществляется с помощью браузера пользователя следующих версий:

- Opera (версия 114 и выше);
- Firefox (версия 130 и выше);
- «Яндекс Браузер» (версия 24.10.1 и выше);
- Google Chrome (версия 130 и выше).

Требования и условия организационного характера

Система обслуживается персоналом Исполнителя.

Для обеспечения работоспособности Системы оперативный персонал службы, ответственной за эксплуатацию данного ПО, должен обеспечивать постоянный мониторинг всех компонентов Системы.

Требования и условия технического характера

Для работы Системы не требуется обеспечения особых требований и условий технического характера.

Требования и условия технологического характера

Для работы Системы не требуется обеспечения особых требований и условий технологического характера.

Требования к квалификации персонала сопровождения

Система сопровождается персоналом Исполнителя. Для обеспечения работоспособности Системы оперативный персонал службы, ответственной за эксплуатацию данного ПО, должен обеспечивать постоянное сопровождение Системы и своевременное обновление всех ее компонентов.

Загрузка и установка

Система запускается в следующем порядке:

1. Запуск PostgreSQL.
2. Запуск основных компонентов Haspbox.
3. Запуск Haspbox CSP.

Входные и выходные данные

Входными данными для Системы являются данные, идентифицирующие пользователя или сервиса в системе.

Выходными данными для Системы являются учетные данные для настроенных систем.

Поддержание работоспособности ПО

Параметры работ по поддержанию жизненного цикла

Порядок, состав и периодичность проведения профилактических работ представлены в табл. 3.

Табл. 3. Параметры работ по поддержанию жизненного цикла

Вид регламента	Длительность, часов	Операция	Исполнитель
Ежемесячный	4	Обслуживание компонентов Системы	Системный администратор
Ежемесячный	4	Установка обновлений ОС	Системный администратор
Ежемесячный	6	Установка обновлений Системы	Системный администратор
Ежедневный	1	Анализ корректности функционирования	Системный администратор

Требования к производительности Системы

№	Параметр мониторинга	Уровень критичности	Пороговые значения
1	Дисковое пространство	Critical	Значение $\geq 25\%$ — normal. Менее 25% — warning. Менее 5% — critical
2	Наличие памяти	Critical	Значение $\leq 25\%$ — normal. Менее 25% — warning. Менее 5% — critical

3	Загрузка процессора	Critical	Загрузка более 90% на всех CPU
4	Размер swap-памяти	Critical	Значение $\geq 10\%$ — normal. Менее 10% — warning. Менее 5% — critical

Обязанности системного администратора

Системный администратор отвечает за стабильность и корректность работы Системы.

Обязанности системного администратора:

- модернизация, настройка и мониторинг работоспособности Системы;
- анализ журналов ошибок Системы, уведомление разработчиков Системы об ошибках и нештатных ситуациях, возникающих при работе Системы;
- контроль за работоспособностью серверов приложений и серверов БД, их перезапуск в случае нештатных остановок, уведомление разработчиков Системы о нештатных ситуациях и ошибках, возникающих при работе серверов.

Процедура резервного копирования

Резервное копирование Системы рекомендуется осуществлять путем создания моментальной копии всех файловых систем (снапшота) серверов, на которых развернута Система. Определение частоты выполнения процедуры резервного копирования осуществляется на основании частоты изменений конфигураций Системы.

На первых этапах эксплуатации Системы рекомендуется выполнять процедуру резервного копирования с периодичностью раз в неделю.

Резервное копирование баз данных Системы выполняется средствами СУБД в режиме онлайн в резервные ресурсы СУБД, а также средствами платформы виртуализации.

Процедура резервного восстановления

Для резервного восстановления Системы необходимо:

- остановить компоненты Системы;
- удалить текущие базы данных;
- провести восстановление базы данных и других компонентов Системы с помощью скрипта восстановления или платформы виртуализации;
- запустить базы данных и другие компоненты Системы.

Тестирование Системы после перезапуска

Для тестирования Системы после перезапуска необходимо:

- убедиться, что в лог-файлах всех компонентов Системы отсутствуют критические ошибки;
- проверить корректность настроек всех компонентов Системы;
- авторизоваться в веб-интерфейсе Системы с полномочиями пользователя и убедиться, что пользователю доступны основные функции пользовательского интерфейса Системы.

Устранение неисправностей, выявленных в ходе эксплуатации

Сообщения об ошибках и исключительные ситуации

В случае сбоя в работе Системы или неправильного реагирования на команды пользователя следует:

- зафиксировать все действия пользователя, которые привели к указанной ситуации;
- зафиксировать текст сообщения (при наличии сообщения) о сбое в работе Системы;
- связаться с разработчиком и передать информацию о времени возникновения и характере проблемы.

Совершенствование ПО

Система постоянно развивается: в ней появляются новые дополнительные возможности, выходят новые версии, оптимизируется использование ресурсов серверов, обновляется веб-интерфейс, обновление ПО совершается в соответствии с «Руководством по установке».

Техническая поддержка

Условия технической поддержки содержатся в договоре с пользователем решения.