

ПРОГРАММНЫЙ КОМПЛЕКС
«МЕНЕДЖЕР УПРАВЛЕНИЯ КОРПОРАТИВНЫМИ СЕКРЕТАМИ
НАSPBOX»

Описание функциональных характеристик программного обеспечения

Листов 7

Оглавление

Оглавление	2
Термины и определения	3
Перечень сокращений.....	4
Функциональные характеристики.....	5
Цели и назначение	5
Ключевые функции	5
Функциональные разделы и компоненты системы	6
Журнал событий	7

Термины и определения

Термин	Определение
Исполнитель	ООО «HASPBOX»
Пользователь	Сотрудник Заказчика, обладающий правом доступа к HASPBOX
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)
Haspbox CSP	Компонент, отвечающий за взаимодействие с отечественной системой криптографической защиты «КриптоПРО CSP 5.0»
Haspbox RE	Компонент, отвечающий за взаимодействие с внешними системами, для управления и ротации паролей.

Перечень сокращений

Сокращение	Расшифровка
БД	База данных
API	Application programming interface
IP	Internet Protocol
ОС	Операционная система

Функциональные характеристики

Цели и назначение

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;

Ключевые функции

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 функциональные возможности HASPBOX:

- Единое централизованное хранилище секретов (пароли, ключи, сертификаты и другая конфиденциальная информация)
- Создание и автоматическое изменение инфраструктурных паролей
- Интеграция с системами автоматизации для получения и изменения секретов инфраструктуры по встроенному REST API
- Автоматическая проверка и генерация паролей на основании настраиваемой парольной политики
- Гибкая ролевая модель пользователей системы
- Защита паролей средствами дополнительного ГОСТ-шифрования на базе КриптоПро
- Поддержка автоматического взаимодействия с наиболее популярными БД и сервисам, включая PostgreSQL, MySQL, redis, Elasticsearch и другие

- Поддержка управления учетными записями через SSH
- Аудит паролей защищаемых паролей на предмет неконтролируемой смены в обход системы
- Журналирование и аудит процессов управления паролями
- Резервирование системы на случай нештатных ситуаций

Функциональные разделы и компоненты системы

Основными функциональными разделами системы являются:

- Мои хранилища;
- Управление доступом;
- Настройки;
- Профили подключения;
- Журнал событий

Мои хранилища

Раздел содержит список пользовательских секретов в виде Описание, ключ и значение. Элементы данного раздела предназначены для личного использования списков доступа пользователей к информационным системам.

Управление доступом

Раздел содержит информацию об управляемых базах данных и учетных записях в них, а также внешних сервисах, которые используют внутреннее хранилище Haspbox для получения хранимых секретов.

Базы данных

Раздел содержит список баз данных и пользователей, для которых система управляет секретами.

Внешние сервисы

Раздел содержит список внешних сервисов, которым разрешены подключения с целью получения управляемыми секретами по протоколу REST API.

Настройки

Управление пользователями системы

Данный раздел содержит информацию о существующих пользователях системы и предоставляет возможность добавления новых пользователей.

Парольные политики

Раздел содержит списки парольных политик, которые используются для генерации секретов при смене паролей на целевых контролируемых учетных записях.

Политики создаются единые для всей системы и могут быть использованы при ротации секретов.

Журнал событий

Данный раздел содержит информацию о событиях системы, включающую в себя информацию о работе планировщика управления внешними секретами в рамках контролируемых систем.