АТ КОНСАЛТИНГ
РОСАТОМ

Центр управления пользователями 2.0

Управление секретами и конфиденциальными данными в динамической среде

Проблема хранения секретов компании

АТ КОНСАЛТИНГ
РОСАТОМ

Секрет – это любая информация, которая необходима для аутентификации:
токены, SSH-ключи, сертификаты, логины и пароли

Секреты могут быть:

По мере роста компании ИТ-отделы и команды DevOps сталкиваются с проблемой **расползания инфраструктурных секретов**, когда секреты инфраструктуры «разбросаны» по нескольким местам. При этом становится невозможно контролировать их использование

Неправильное хранение инфраструктурных секретов приводит к компрометации и утечке информации

ЦУП 2.0 Модуль управления секретами

АТ КОНСАЛТИНГ
РОСАТОМ

Это менеджер инфраструктурных секретов – программный продукт, развертываемый на серверах компании

Возможности:

Данное решение позволит централизованно хранить и управлять всеми аутентификационными данными:

- логины и пароли учетных записей
- ключи для сервисов (например, Kubernetes)
- ключи непрерывной интеграции CI/CD
- ключи сертификатов: внутренний PKI, подписи мобильных приложений и т. п.
- общие конфиденциальные данные

Для кого:

Банковский сектор

Госучреждения, министерства и ведомства

Крупный бизнес

Телеком-операторы

Облачные провайдеры

Преимущества Модуля управления секретами ЦУП 2.0

АТ КОНСАЛТИНГ
РОСАТОМ

01 Исключение доступа к секретам сотрудников поддержки и эксплуатации.
Управление (создание, ротация, доставка) секретов выполняется автоматизировано и без участия человека

02 Инструмент для контроля доступа, аудита и надзора за секретами компании

03 Интегрируется со всем стеком технологий в ИТ-ландшафте современной компании, со всеми популярными системами CI/CD и языками программирования

04 Выполнение рекомендованных мер по защите информации согласно ГОСТ 57580.1-2017 (рекомендации регулятора финансового рынка – Банка России)

Решение основано на open source-компонентах с российскими разработками

ЦУП 2.0 – импортонезависимое корпоративное решение

АТ КОНСАЛТИНГ
РОСАТОМ

Модуль управления секретами замещает собой и превосходит зарубежные аналоги:

01

Vault (open source)

02

Conjur Secrets Management

03

HashiCorp Vault Enterprise

04

Akeyless Vault Platform

- Защищает ИТ-инфраструктуру – какой бы сложной она ни была
- Функционирует в высоконагруженном режиме
- Легкое масштабирование, вертикальное и горизонтальное
- Обеспечивает взаимодействие всех типов приложений, от классических до микросервисных, в контейнерах и оркестраторах
- Журналирование использования учетных данных

Варианты решений на рынке

АТ КОНСАЛТИНГ
РОСАТОМ

Функциональные возможности	ЦУП 2.0 Модуль управления секретами Enterprise	HashiCorp Vault Enterprise	Conjur Secrets Management Enterprise	Vault Open source
Отказоустойчивость (построение кластера, георазпределение)	✓			
Масштабируемость (поддержка шардирования)	✓			
Производительность (чтение секретов со всех узлов кластера)	✓	✓	✓	
Мультитенантность (построение изолированных областей хранения секретов)	✓	✓		
Управление комплексными операциями создания хранилищ	✓			
Fast unseal (быстрый переезд в случае выхода из строя кластера)	✓			
Расширяемые возможности интеграции с информационными системами	✓	✓		✓
Автоматическое переключение соединений СУБД Active/Standby	✓	✓		✓

Показатели производительности на продуктивной инфраструктуре крупного банка

АТ КОНСАЛТИНГ
РОСАТОМ

Показатели	Нагрузка
Доступность	**99,999%**
Класс системы	**mission critical +**
Количество тенантов (изолированных областей хранения секретов)	**2 000**
Количество секретов	**50 600**
Одновременные подключения	**500**
Скорость обработки запросов	**15 000 – 20 000 rps**

Лицензии и сертификаты

АТ КОНСАЛТИНГ
РОСАТОМ

- **Сертификата соответствия ФСТЭК России на 4 уровень доверия и ТУ № 4921 от 25.03.2025**
- **Продукт Центр управления пользователями 2.0 зарегистрирован в реестре российского ПО под № 5757 от 20.09.2019**
- **Компания имеет бессрочную лицензию ФСТЭК на деятельность по разработке и производству средств защиты конфиденциальной Информации**

Продукт соответствует требованиям информационной безопасности, допускается применение продукта в государственных и банковских информационных системах

Преимущества компании

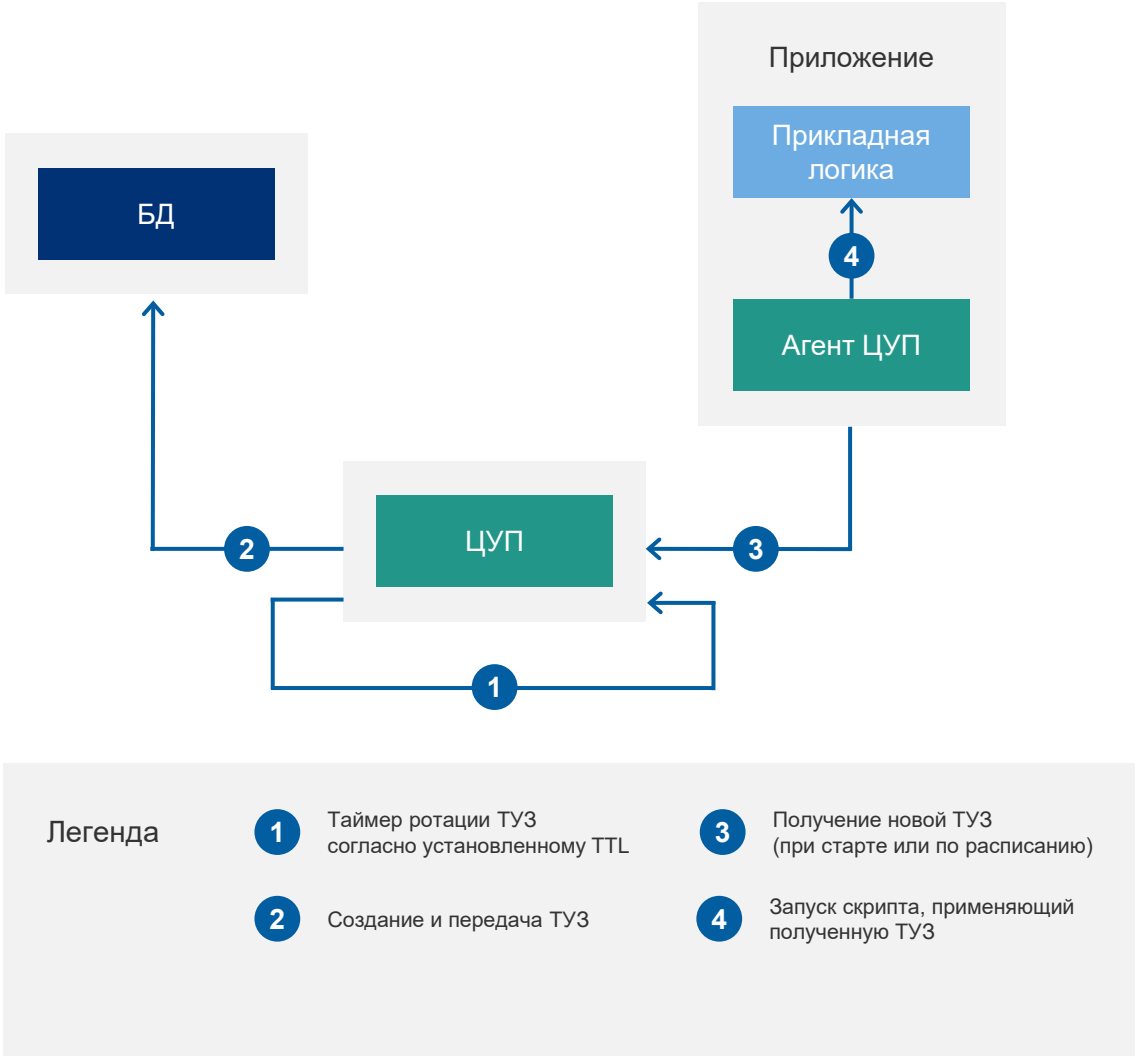
АТ КОНСАЛТИНГ
РОСАТОМ

- Российский разработчик программного обеспечения
- Доработка решений под задачи заказчика
- Русскоязычная техническая поддержка 24x7

- Бесплатное тестирование продукта
- Партнерская программа
- Организация референсов и презентаций

Варианты использования продукта

АТ КОНСАЛТИНГ
РОСАТОМ



Использование совместно с готовым ПО

Сценарий использования системы управления секретами на готовом ПО включает установку агента ЦУП, где доработка интеграции нецелесообразна

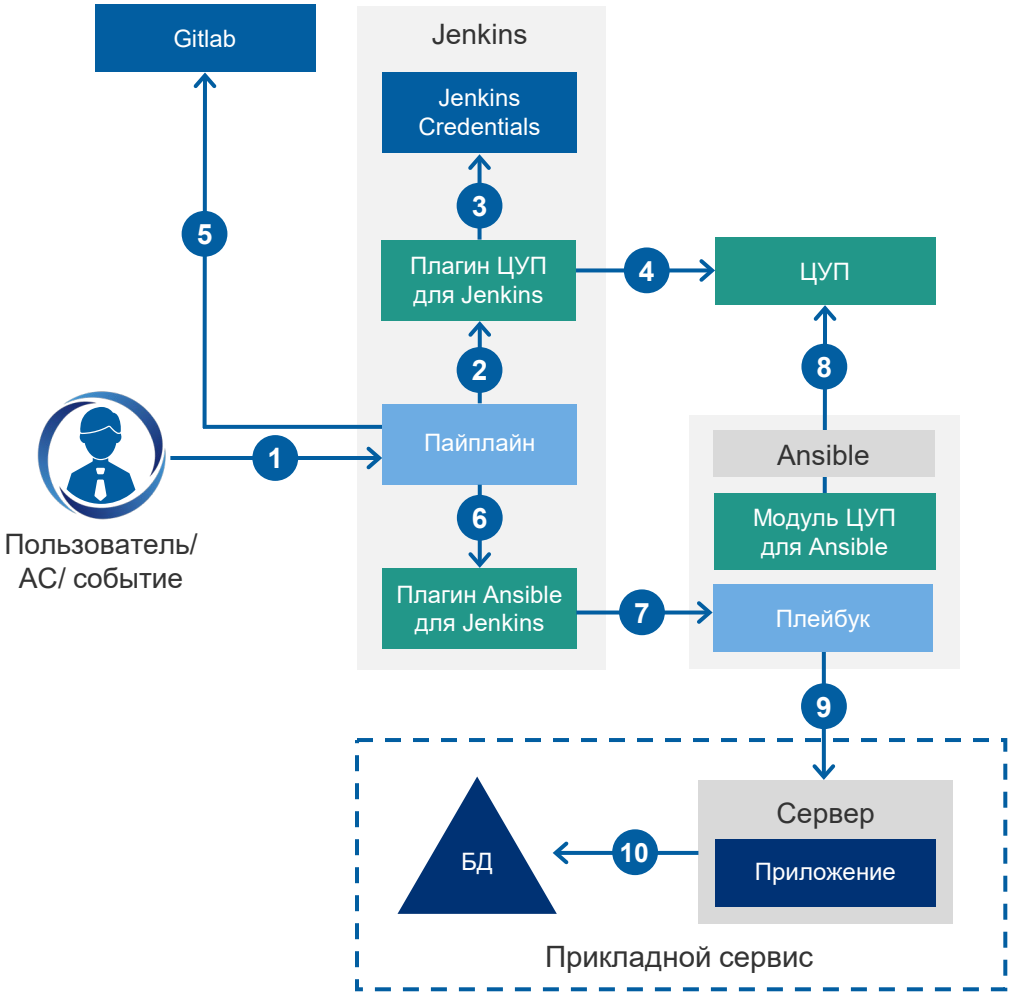
Агент позволяет получать секреты и запускать скрипты, применяющие полученные секреты

Агент ЦУП поддерживает шаблонирование, что позволяет генерировать конфигурационные файлы с внедренными секретами

В схеме описан автоматизированный сценарий ротации и доставки по адресу технической учетной записи (далее – ТУЗ)

Варианты использования продукта

АТ КОНСАЛТИНГ
РОСАТОМ



Использование в сценариях автоматизации CI/CD

Типовой сценарий использования системы управления секретами – это получение секретов для пайплайнов Jenkins и плейбуков Ansible

Интеграционные плагины из коробки:

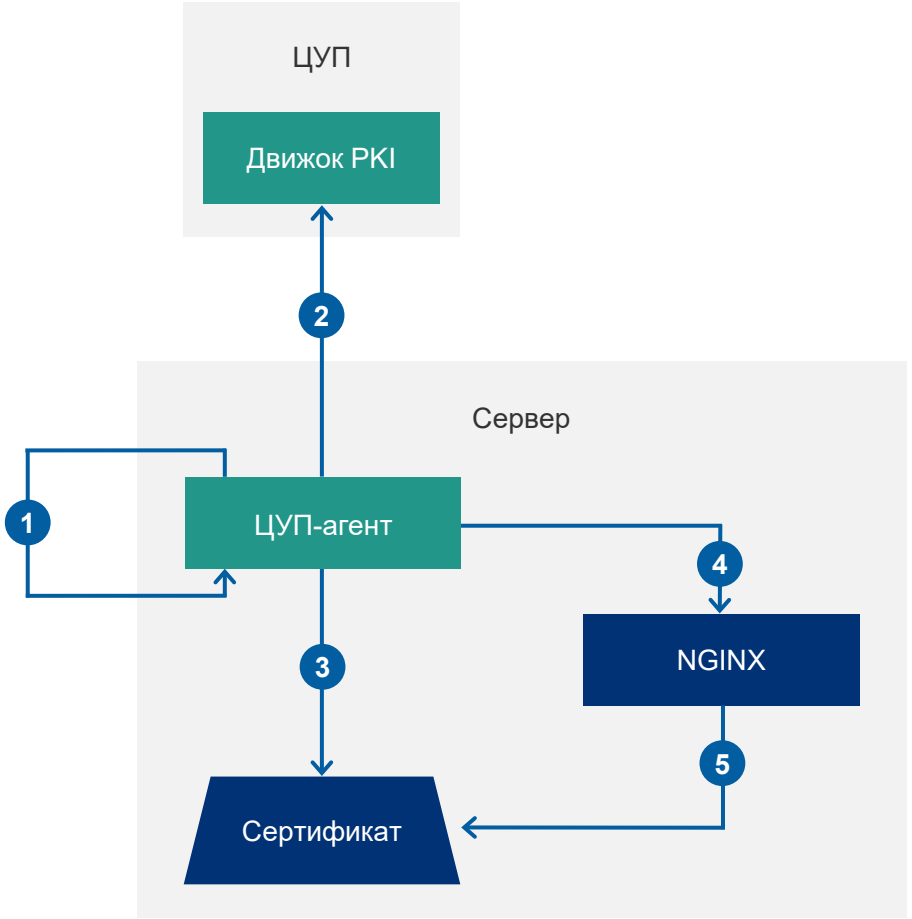
- Jenkins
- Ansible
- Kubernetes/OpenShift
- Nexus
- Dynatrace
- Prometheus
- ELK
- Rabbit MQ

Легенда:

1. Запуск
2. Запрос секретов у ЦУП
3. Получение creds для ЦУП
4. Запрос логина/пароля к Gitlab
5. Аутентификация и получение исходного код
6. Передача управления Плагину Ansible
7. Запуск Ansible
8. Получение секрета БД
9. Использование секрета в Ansible скрипте разворачивания
10. Аутентификация в БД

Варианты использования продукта

АТ КОНСАЛТИНГ
РОСАТОМ



Смена сертификатов на балансировщиках

ЦУП 2.0 имеет функциональную возможность управления сертификатами

В архитектуре ЦУП предусмотрен свой PKI-центр, но также не исключена возможность использовать PKI-центр заказчика

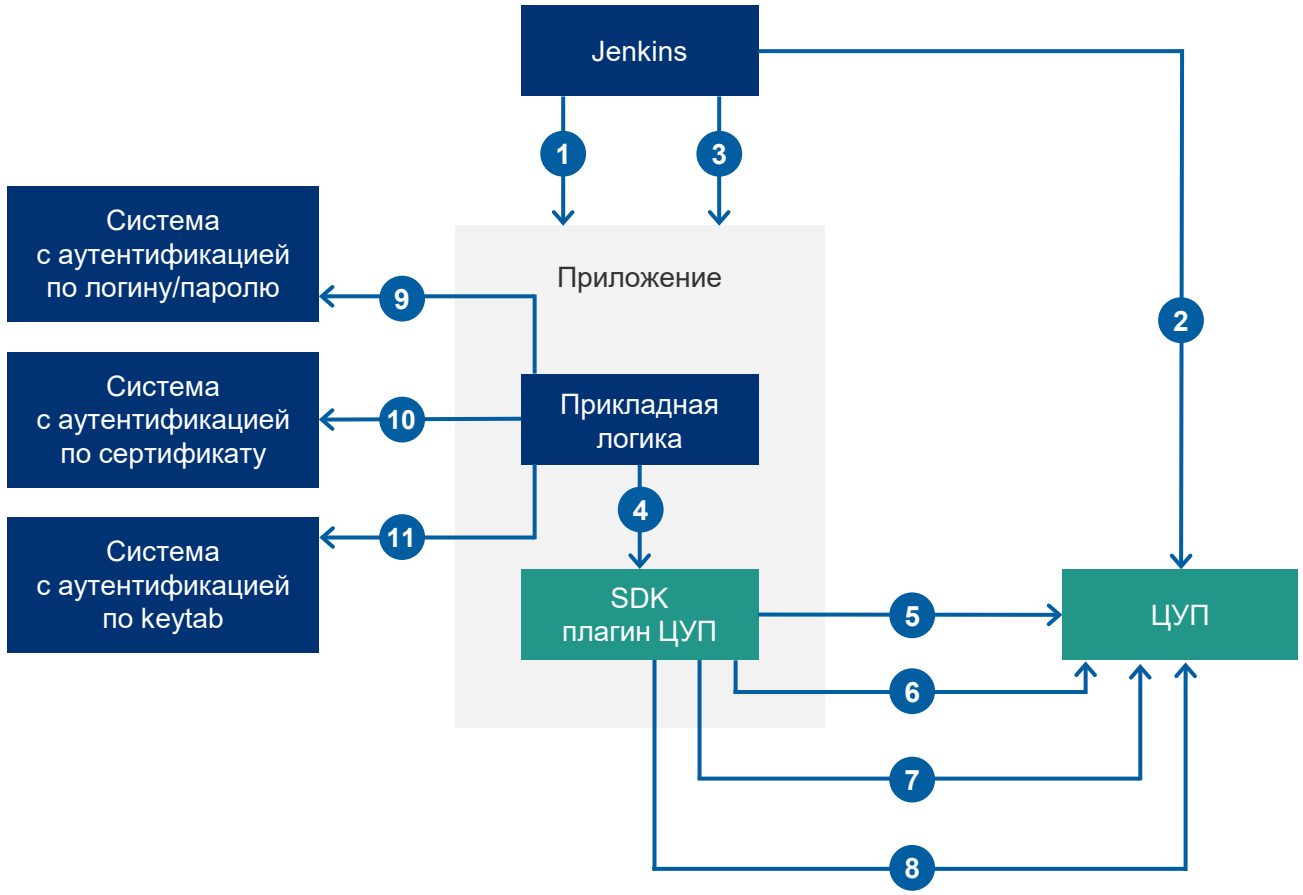
Как результат мы будем иметь безопасную автоматизацию, которая будет создавать сертификат согласно установочному периоду, доставлять его по адресу и проводить смену сертификата

Легенда

1 Таймер отслеживания валидности сертификата
2 Выпуск сертификата
3 Сохранение сертификата
4 Перезагрузка (reload)
5 Чтение нового сертификата

Варианты использования продукта

АТ КОНСАЛТИНГ
РОСАТОМ



Использование с разрабатываемым ПО

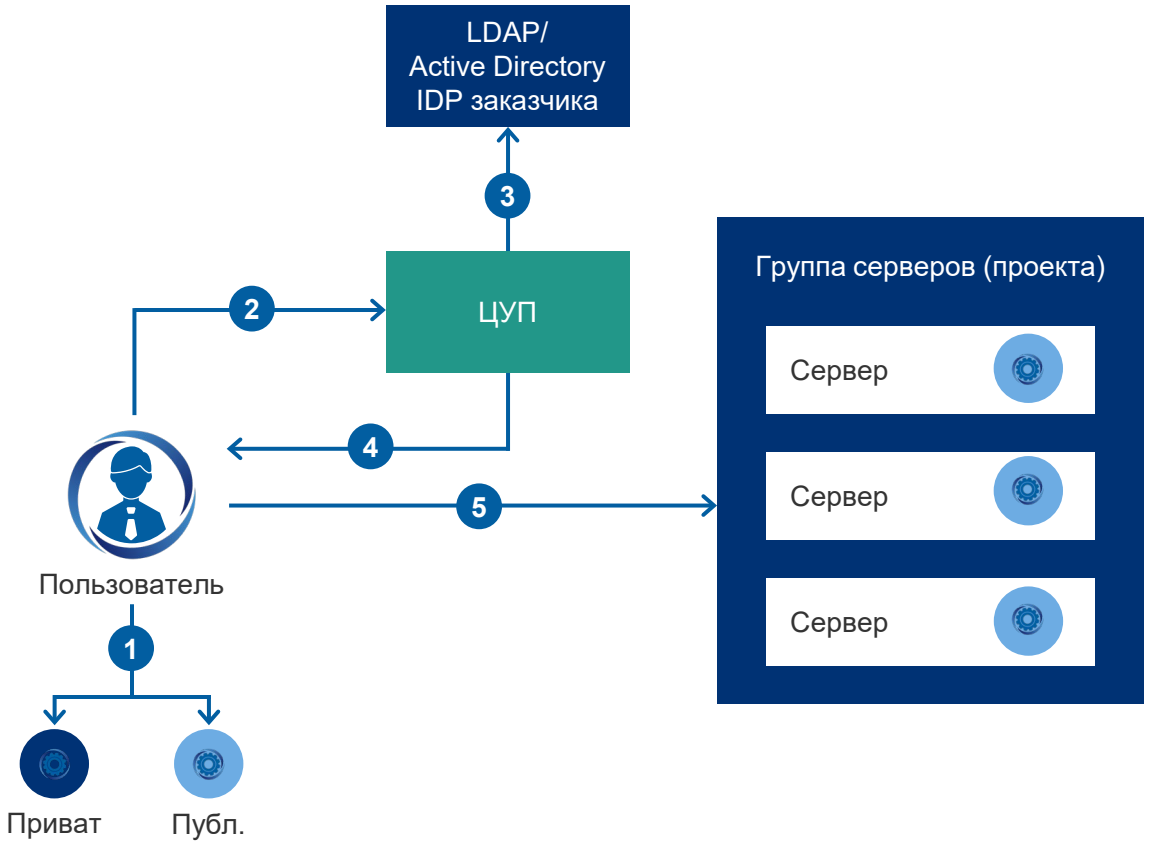
- Разрабатываемое или дорабатываемое ПО может использовать систему управления секретами непосредственно через API либо с использованием SDK, поставляемого с системой
- При этом желательно, чтобы секрет для доступа к ЦУП тоже хранился в ЦУП и передавался приложению на этапе развертывания

Легенда:

1 Развертывание
2 Запрос creds для SDK ЦУП
3 Передача creds для SDK ЦУП
4 Запрос секретов
5 Аутентификация в ЦУП
6 Запрос логина/пароля
7 Запрос сертификата
8 Запрос keytab
9 Вход по логину/паролю
10 Вход по сертификату
11 Вход по keytab

Варианты использования продукта

АТ КОНСАЛТИНГ
РОСАТОМ



Легенда:

1 Наличие пары SSH-ключей

2 Запрос сертификата

3 Аутентификация

4 Выдача пользовательского сертификата SSH

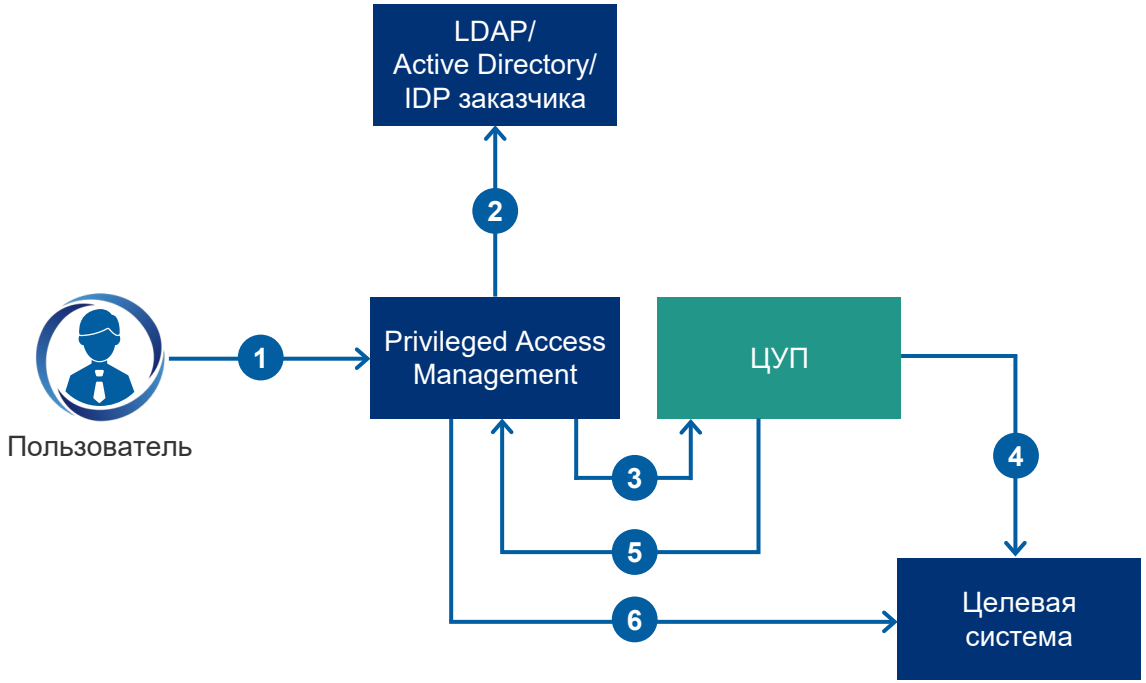
5 SSH-соединение по сертификату

Управление SSH-доступом

- ЦУП 2.0 Модуль управления секретами содержит движок SSH secrets engine, который позволяет выпускать подписанные SSH-сертификаты и ограничивать срок их действия
- На стороне ЦУП 2.0 настраивается разграничение доступа к группам серверов
- При увольнении сотрудника эксплуатации, имевшего доступ к инфраструктуре, достаточно заблокировать его УЗ в IDP компании
- Срок жизни выдаваемых сертификатов может быть ограничен несколькими минутами, что позволит исключить риск утечки

Варианты использования продукта

АТ КОНСАЛТИНГ
РОСАТОМ



Легенда:

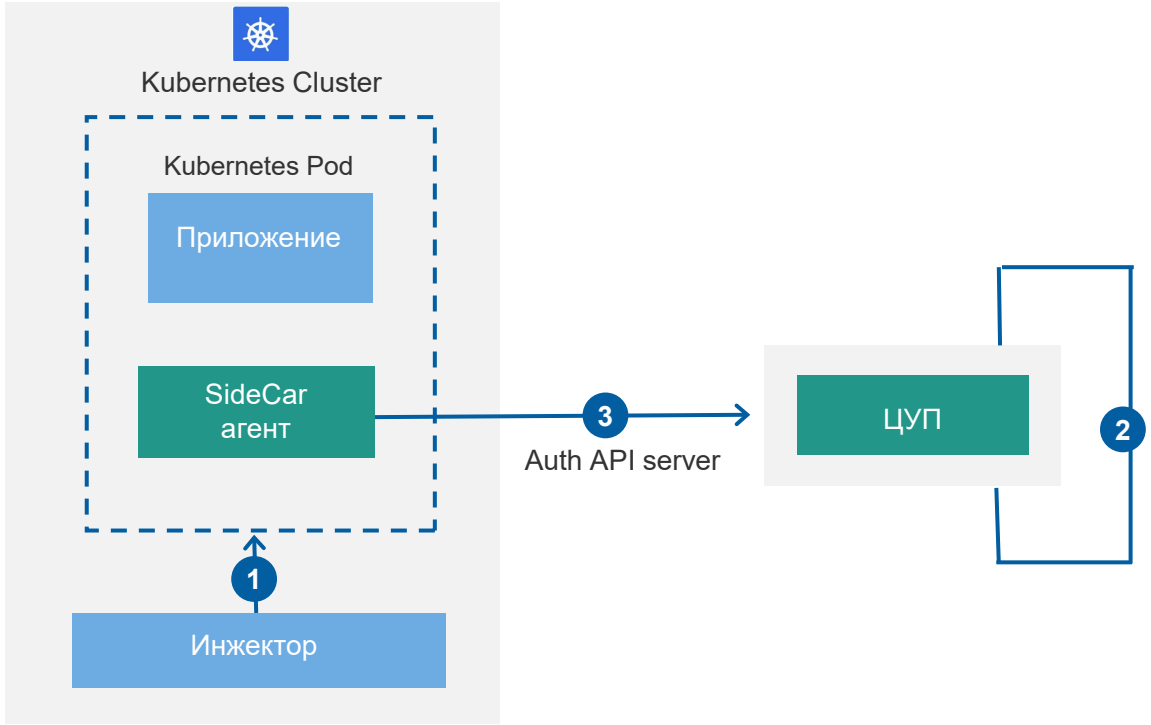
1. Вход в систему
2. Аутентификация и получение групп
3. Запрос учетных данных для авторизации в целевой системе
4. Создание УЗ
5. Передача УЗ
6. Предоставление доступа в целевую систему

Использование с PAM-системами

- PAM-система и ЦУП 2.0 Модуль управления секретами (Vault) интегрируются в части получения учетных данных для авторизации привилегированных пользователей в целевых системах
- Интеграция с ЦУП 2.0 позволяет обеспечить автоматизированную генерацию, ротацию и отзыв учетных данных, SSH-ключей, сертификатов Kubernetes и пр. в целевых системах
- Целевыми системами могут быть любые ресурсы, доступ на которые контролируется PAM, например, серверы, виртуальные машины, кластеры Kubernetes

Варианты использования продукта

АТ КОНСАЛТИНГ
РОСАТОМ



Использование в контейнеризированной среде Kubernetes

В схеме описан сценарий встраивания ЦУП 2.0 в контейнеризированную среду Kubernetes

Из «коробки» доступна интеграция, где система управления секретами обеспечивает автоматизированный процесс управления секретами, по заданным TTL секреты автоматически будут ротироваться и доставляться в поды с приложением.

Легенда

1. Запуск пода с SideCar агентом
2. Таймер ротации Секрета согласно установленному TTL
3. Аутентификация и получение секрета в ЦУП 2.0 с помощью Auth API Server Kubernetes

Интеграции из коробки

АТ КОНСАЛТИНГ
РОСАТОМ

CI/CD, инфраструктура и мониторинг:

- GitLab
- Jenkins
- Ansible
- Kubernetes/OpenShift
- Nexus
- Dynatrace
- Zabbix
- Ключ-АСТРОМ
- Prometheus
- ELK
- VolgaBlob Smart Monitor

Базы данных:

- Cassandra
- Couchbase
- Elasticsearch
- Opensearch
- InfluxDB
- MongoDB
- MongoDB Atlas
- MSSQL
- MySQL/MariaDB
- Oracle
- PostgreSQL
- SAP Hana
- IgniteDB

Системы аутентификации:

- OIDC-системы
- Microsoft Active Directory
- OpenLDAP
- RADIUS
- Kerberos
- LinOTP
- Rabbit MQ
- Linux/Unix OS
- RedHat IDM

Модуль управления секретами ЦУП 2.0 дополняет своей функциональностью такие решения, как IAM, PAM, IDM

Функциональная архитектура продукта

АТ КОНСАЛТИНГ
РОСАТОМ

ЦУП МОДУЛЬ УПРАВЛЕНИЯ СЕКРЕТАМИ

Решение «ЦУП. Модуль управления секретами» позволяет управлять секретами, показателями, частично конфигурационной информацией

Решение основано на open source-компонентах с российскими разработками

Запись в реестре российского ПО № 5757 от 20.09.2019

Собственная разработка

Частично собственная разработка

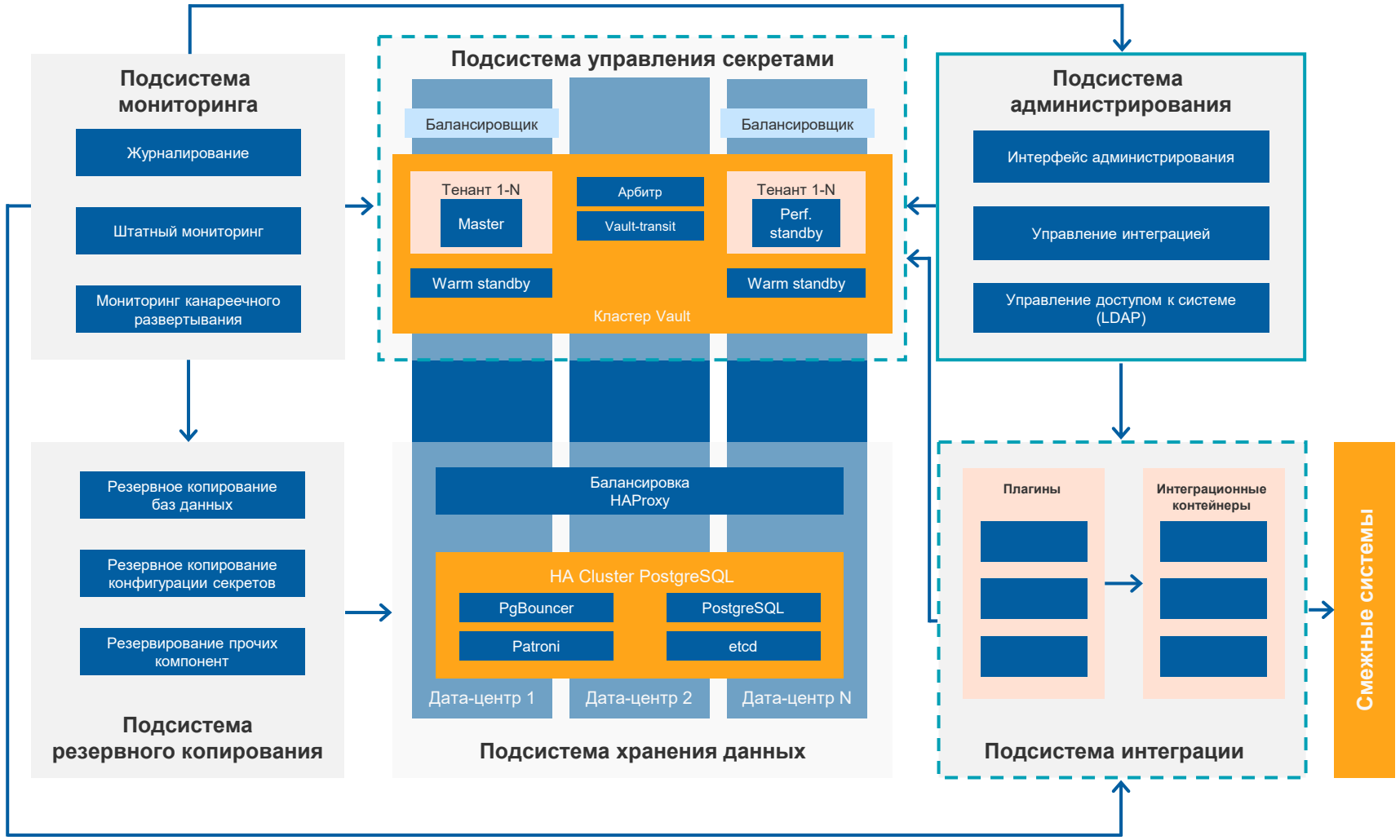


Схема лицензирования ЦУП2.0

1. Лицензия на право использования продукта, срочная

	Показатели объема	Показатели объема	Показатели объема
Количество инсталляций	1 / без ограничений	1 / без ограничений	1 / без ограничений
Производительность	до 1000rps	от 1000 до 5000rps	более 5000rps
Геораспределение	требуется/не требуется	требуется/не требуется	требуется/не требуется
Мультикластерность	требуется/не требуется	требуется/не требуется	требуется/не требуется

2. Сертификат технической поддержки, срок действия - 1год

	Описание технической поддержки
Стандарт	консультирование в режиме 8x5, без поставки обновлений (входит в базовую лицензию)
Расширенный	консультирование в режиме 8x5, поставка обновлений, решение инцидентов SLA (приобретается отдельно)
Премиум	консультирование в режиме 24x7, поставка обновлений, решение инцидентов с SLA (приобретается отдельно)

Дорожная карта

АТ КОНСАЛТИНГ
РОСАТОМ

ЦУП2.0 МОДУЛЬ УПРАВЛЕНИЯ СЕКРЕТАМИ

1Q 2025

- Сертификация ФСТЭК на 4 уровень доверия и ТУ

2Q 2025

- Внедрение отечественных СКЗИ
- Дополнительные методы аутентификации с использованием отечественных провайдеров

3Q 2025

- Биллинг хранения секретов
- Дополнительные плагины для управления секретами в отечественных СУБД

4Q 2025

- Развитие инструментов телеметрии и мониторинга
- Внедрение инструментов самодиагно-стики ЦУП 2.0

1Q 2026

- Подтверждение контроля встраивания СКЗИ ФСБ

О компании

АТ КОНСАЛТИНГ
РОСАТОМ

Сегодня АТ Консалтинг занимает лидирующие позиции на рынке ИТ-услуг в России и СНГ

В партнерстве с компаниями-лидерами телекоммуникационного, финансового, производственного, топливно-энергетического секторов, а также органами государственной власти и региональными ведомствами мы делаем проекты, которые меняют жизнь людей к лучшему

6 000+

экспертов по всей России и странам СНГ

22+

года опыта на рынке

1 000+

проектов ежегодно в государственном и коммерческом секторах

Отзывы наших клиентов

АТ КОНСАЛТИНГ
РОСАТОМ

СБЕР

Виктор Орловский

Член правления, старший вице-президент

Я с уверенностью могу сказать, что в последнее время Сбербанк является самой быстро меняющейся крупной компанией в России, а возможно и в мире. Наряду с внедрением «лучших практик» мы активно развиваем технологии будущего, не имеющие аналогов в современной банковской индустрии.
В любом случае начинать стоит только те проекты, которые в момент реализации все еще являются инновационными – современные решения требуют большого запаса прочности и функциональности.

Внедрение таких технологий – сложный процесс, требующий детальной проработки, поэтому мы активно привлекаем к сотрудничеству ведущих экспертов рынка. Среди наших партнеров – компания АТ Консалтинг.
Мне нравится работать с ней в первую очередь потому, что эксперты компании Нацелены на получение требуемого результата, не останавливаются перед трудностями, ищут новые решения и, как следствие, растут профессионально Ведь, как известно, серьезные проблемы нельзя решать на том же уровне мышления, на котором они возникли.

Alfa-Bank

Дмитрий Сережин

Финансовый директор, блок «Финансы» Альфа-Банка

Сотрудничество с консультантами АТ Консалтинг, учитывая их опыт и экспертизу, дает нам уверенность в качественном результате совместно реализуемых проектов.

Наши клиенты

АТ КОНСАЛТИНГ
РОСАТОМ

Государство

- ГК «Автодор»
- АНО «Дирекция Красноярск 2019»
- Комитет по информатизации и связи г. Санкт-Петербурга
- МВД России
- КГБУЗ «Медицинский центр – управляющая компания Алтайского медицинского кластера»
- Министерство обороны России
- Минэкономразвития России
- Мои документы
- РОСРЕЕСТР
- ФСИН России
- ГУП «Центр информационных технологий Республики Татарстан»

Телеком и медиа

- Коммерсант.ru
- МегаФон
- МТС
- Ростелеком
- ТРИКОЛОР
- IBS Platformix
- TELE2
- VEON
- YOTA

Финансы

- Альфа Банк
- Банк России
- ВТБ
- ГАЗПРОМБАНК
- ИНГОССТРАХ
- МОСКОВСКАЯ БИРЖА
- HALYK BANK
- НСПК
- ПОЧТА БАНК
- РОСГОССТРАХ
- РоссельхозБанк
- СБЕР БАНК
- Altyn Bank

ТЭК

- ГАЗПРОМ
- ИНТЕР РАО ЕЭС
- КазМунайГаз
- МРСК ЮГА
- РОСНЕФТЬ
- РОСАТОМ
- РОССЕТИ
- РОССЕТИ СИБИРЬ
- ТПК-1
- ТПК ЕВР

Производство

- EURO CEMENT
- НОРНИКЕЛЬ
- Центр Внедрения ПРОТЕК
- СИБУР
- УРАЛКАЛИЙ
- ФОСАГРО
- ОМК
- Миэль
- Pfizer
- S7 Airlines

Торговля и питание

- АЗБУКА ВКУСА
- Вимм-Билль-Данн
- ДИКСИ
- ЛЕНТА
- Новосибирская аптечная сеть
- ЧЕРКИЗОВО
- LEROY MERLIN
- M

Спасибо
за внимание