

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ГОТОВОЕ РЕШЕНИЕ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ ЛЮБЫХ ПРИКЛАДНЫХ СИСТЕМ

Digital Q.Security





ФУНКЦИОНАЛЬНОСТЬ И СФЕРЫ ПРИМЕНЕНИЯ

СОСТАВ И ФУНКЦИОНАЛЬНОСТЬ РЕШЕНИЯ

Digital Q.Security обеспечивает реализацию задач аутентификации, управления ролями и политиками доступа пользователей, ведения каталога пользователей, протоколирования событий информационной безопасности, взаимодействия с криптопровайдерами.



АУТЕНТИФИКАЦИЯ

Единый вход (SSO).
Поддержка протоколов OAuth2, OIDC, LDAPS.
Поддержка двухфакторной аутентификации.
Возможность поставки собственного форка Keycloak с дополнительными плагинами.
Контроль времени жизни и конкурентности пользовательской сессии



УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ

Создание и администрирование учетных записей и групп пользователей.
Синхронизация данных с внешними системами.



АУДИТ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ В СИСТЕМЕ

Фиксация и централизованное хранения информации о действиях пользователей при выполнении операций в прикладных решениях.



УПРАВЛЕНИЕ ПОЛИТИКАМИ ДОСТУПА

Создание и настройка ролевой модели (RBAC).
Разграничение прав доступа пользователей в соответствии с назначениями прав и привилегиями.
Поддержка атрибутной модели прав доступа (ABAC).



ЭЛЕКТРОННАЯ ПОДПИСЬ

Создание и проверка электронной подписи сообщений, файлов, электронных документов с помощью криптопровайдера КриптоПро (JCP, CSP).
Поддержка управления сертификатами электронной подписи пользователей и обновление списков отозванных сертификатов.

СФЕРЫ ПРИМЕНЕНИЯ

ПОСТРОЕНИЕ ЦЕНТРАЛИЗОВАННОГО ЯДРА БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ ПРОМЫШЛЕННЫХ СИСТЕМАХ (СОЗДАВАЕМЫХ С ПОМОЩЬЮ ДИАСОФТ, СОБСТВЕННЫМИ СИЛАМИ ИЛИ ДРУГИМИ ВЕНДОРАМИ)

- Единый вход (SSO) для сотрудников
- Безопасная аутентификация клиентов и сотрудников, в том числе с использованием многофакторных способов.
- Контроль доступа к конфиденциальным документам
- Централизованный сбор событий аудита для служб ИТ-безопасности
- Подпись документов с помощью ЭП
- Соответствие отраслевым стандартам и регуляциям
- Контроль разделения ответственности (SoD)

ИНТЕГРАЦИЯ С СУЩЕСТВУЮЩИМИ СИСТЕМАМИ ИБ В КОМПОНЕНТНОЙ (НАПРИМЕР, МИКРОСЕРВИСНОЙ) АРХИТЕКТУРЕ ДЛЯ ИСПОЛЬЗОВАНИЯ ВСЕХ ИЛИ ОТДЕЛЬНЫХ СЕРВИСОВ

- Возможность интеграции с IDM решениями, например с 1IDM или Avanpost
- Возможность интеграции SIEM-системами
- Возможность интеграции с российскими криптопровайдерами, например с КриптоПро и Валидата
- Возможность использования отдельных сервисов напрямую через API

ВСТРАИВАНИЕ МЕТОДОВ И ФУНКЦИЙ ПЛАТФОРМЫ, КАК БИБЛИОТЕК, В СОСТАВ ЛЮБЫХ ИНТЕРНЕТ-РЕШЕНИЙ, КЛИЕНТСКИХ ПОРТАЛОВ, БИЗНЕС-ПРОЦЕССОВ, БЭКЕНД-СЕРВИСОВ

- Аутентификация пользователей (OAuth2, OpenID Connect, SAML)
- Безопасный обмен токенами между сервисами
- Детальный аудит операций в личных кабинетах
- Возможность прозрачного для потребителя взаимодействия с централизованной системой



ЗАДАЧИ И ВЫЗОВЫ РЫНКА

ВОЗМОЖНО, ПЕРЕД ВАМИ СТОЯТ ПОХОЖИЕ ЗАДАЧИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

01 **ВНЕДРЕНИЕ ЕДИНОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ ДЛЯ 10+ ВНУТРЕННИХ СИСТЕМ**

Использование единого сервера аутентификации и технологии SSO, приводит к сокращению ИТ-расходов на управление доступами на 30%, а так же приводит к росту удовлетворенности пользователей за счет единого входа [SSO]

02 **ФИКСАЦИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ ПРИ ЗАПУСКЕ ОПЕРАЦИЙ В БИЗНЕС ПРИЛОЖЕНИЯХ**

Установка централизованной системы аудита повышает прозрачность системы на всех уровнях и значительно снижает риски при эксплуатации

03 **НЕОБХОДИМО ЦЕНТРАЛИЗОВАННО РАЗГРАНИЧИТЬ ДОСТУП К БИЗНЕС-ОБЪЕКТАМ ВАШИХ РЕШЕНИЙ**

Использование централизованной системы разграничения доступов на различных системных уровнях, начиная от шлюза вызовов, заканчивая контроллерами API повышает гибкость системы, ее безопасность и значительно снижает расходы на сопровождение

04 **ЗАКОНОДАТЕЛЬСТВО ТРЕБУЕТ НАЛИЧИЕ СЕРТИФИКАТА ФСТЭК ДЛЯ ВАШИХ ПРИЛОЖЕНИЙ**

Использование сертифицированной платформы значительно снизит расходы на сопровождение и развитие системы

ПОЧЕМУ РЫНОК ТРЕБУЕТ ГОТОВОЕ ЦЕНТРАЛИЗОВАННОЕ РЕШЕНИЕ ПО БЕЗОПАСНОСТИ

1

СЛОЖНОСТЬ УПРАВЛЕНИЯ РАЗРОЗНЕННЫМИ СИСТЕМАМИ И НЕПРОЗРАЧНОСТЬ ИХ ПРИМЕНЕНИЯ

Разрозненные системы аутентификации и авторизации усложняют поддержку и увеличивают риски. Отсутствие единой точки аудита и контроля мешает быстрому реагированию на инциденты, а нехватка прозрачности действий пользователей приводит к уязвимостям

3

ВЫСОКАЯ СТОИМОСТЬ СОБСТВЕННОЙ РАЗРАБОТКИ ПОДОБНЫХ СИСТЕМ

Создание системных механизмов «с нуля» для безопасной работы прикладных решений, а тем более эффективная поддержка нескольких таких систем — это дорого и долго

2

ТРУДОЕМКОСТЬ ИЛИ НЕВОЗМОЖНОСТЬ ПОДДЕРЖКИ ИНТЕГРАЦИИ МЕЖДУ МНОГОЧИСЛЕННЫМИ СИСТЕМАМИ

Большое количество автономных систем информационной безопасности требует разработки и поддержки многочисленных интеграционных адаптеров и наличия подходящих API у этих систем

4

ИМПОРТОНЕЗАВИСИМОСТЬ И СВОЕВРЕМЕННОЕ ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ РЕГУЛЯТОРА

Часто меняющиеся требования регулятора в части информационной безопасности, а также требования к импортозамещению усложняют сопровождение всего решения.

DIGITAL Q.SECURITY РЕШАЕТ ЭТИ ПРОБЛЕМЫ

01

Предоставляет централизованные модули аудита, политик доступа, аутентификации, а также возможности интеграции через стандартные для индустрии протоколы (REST, gRPC, Kafka Protocol) с подробно описанными контрактами взаимодействия и документацией.

02

Решение полностью импортонезависимо, входит в Единый реестр российских программ для ЭВМ и БД и сертифицировано ФСТЭК



ПРЕИМУЩЕСТВА И ВОЗМОЖНОСТИ

ПРЕИМУЩЕСТВА РЕШЕНИЯ

01

ЦЕНТРАЛИЗАЦИЯ ЯДРА БЕЗОПАСНОСТИ ДЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Digital Q.Security включает в себя все базовые компоненты и механизмы для обеспечения информационной безопасности прикладных систем

02

ВЫСОКАЯ ОТКАЗОУСТОЙЧИВОСТЬ И ПРОИЗВОДИТЕЛЬНОСТЬ

Благодаря децентрализованной архитектуре и распределенному хранению данных, решение DIGITAL Q.SECURITY способна обрабатывать большие объемы входящих запросов

03

ГИБКАЯ ИНТЕГРАЦИЯ

Поддержка интеграции с популярными системами и протоколами

04

УДОБСТВО ВНЕДРЕНИЯ

Быстрое развертывание и настройка с помощью user-friendly инсталлятора, а так же использованию современных пользовательских интерфейсов для настройки и администрирования, подробной пользовательской и администраторской документации.

05

ИМПОРТОНЕЗАВИСИМОЕ РЕШЕНИЕ

Digital Q.Security включена в Реестр российского программного обеспечения

06

СЕРТИФИКАТ СООТВЕТСТВИЯ ФСТЭК

Компоненты Digital Q.Security имеют заключение сертификационной лаборатории ФСТЭК и на данный момент проходят финальные испытания.

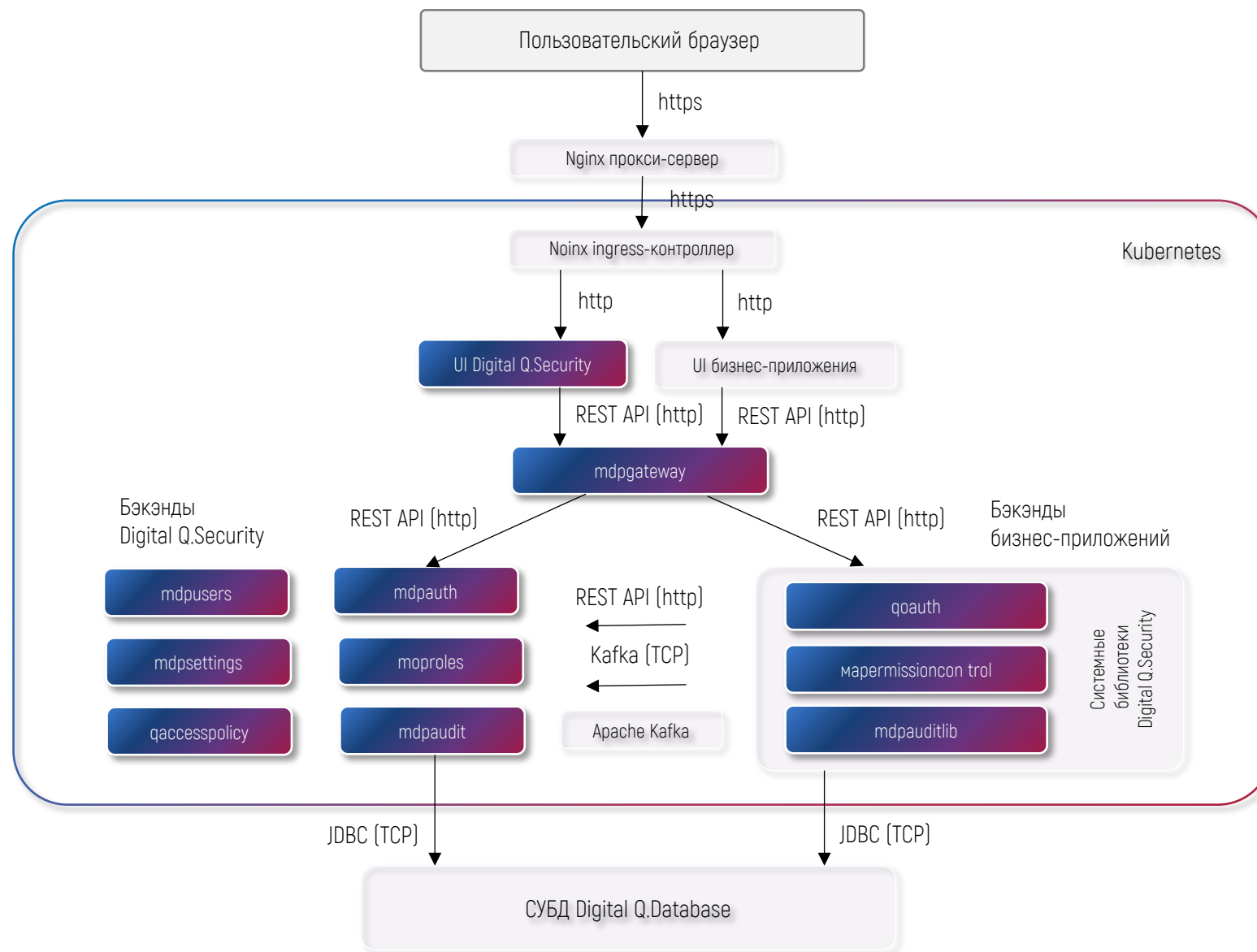


АРХИТЕКТУРА РЕШЕНИЯ

АРХИТЕКТУРА РЕШЕНИЯ

Компоненты решения представляют из себя набор микросервисов и подключаемых библиотек взаимодействующих между собой с помощью API и событийной модели

Компоненты поставляются в виде Docker или LXD образа и разворачиваются в k8s, Docker compose или в LXD-контейнер на импортозамещенных версиях ОС Linux



**БЕЗОПАСНОСТЬ,
КАК У БАНКА
В ВАШИХ ПРОДУКТАХ
С DIGITAL Q.SECURITY**

СПАСИБО

Россия, 127018, Москва
ул. Полковая, д. 3, стр. 14
Т: +7 (495) 780 7575; 789 9339
info@diasoft.ru
www.diasoft.ru