

Общее описание

программного продукта

«LAV. Цифровая платформа защиты бизнеса НЭКСУС»

Оглавление

1 Назначение и область применения.....	2
2 Пользовательские свойства и функциональные возможности	3
4 Архитектура.....	6
5 Системные требования	7
6 Сценарии эксплуатации	8
7 Сопровождение и администрирование	10

1 Назначение и область применения

В данном документе приведено общее описание программного продукта «LAV. Цифровая платформа защиты бизнеса НЭКСУС», более подробные сведения представлены в комплектах технической и пользовательской документации.

Программный продукт «LAV. Цифровая платформа защиты бизнеса НЭКСУС» представляет собой модульный программный продукт (компьютерную программу), для последующей реализации услуг по ее использованию потенциальным клиентам (юридическим лицам). В качестве потенциальных клиентов выступают службы безопасности, рисков, аудита, форензик в финансово-промышленных холдингах. Этот программный продукт предназначен для централизации и повышения эффективности процессов, связанных с обеспечением комплексной безопасности на отдельно взятом предприятии или в холдинговой группе. Модульный принцип построения позволяет гибко адаптировать возможности платформы под требования пользователей и планомерно наращивать её функциональное наполнение.

Применение данного программного комплекса значительно повышает исполнительскую дисциплину, снижает технологические риски и трудоемкость оказания услуг в области обеспечения безопасности. Наибольший эффект может быть получен при количестве одновременно обрабатываемых запросов от 100 в день и обрабатываемых событий от 500 в день.

2 Пользовательские свойства и функциональные возможности

Программный комплекс обладает следующими пользовательскими свойствами:

- Обеспечивает единые принципы разработки, развертывания, функционирования, взаимодействия модулей платформы между собой, формируя тем самым единую экосистему (пространство) для работы сотрудников служб безопасности разного профиля.
- Решает задачи централизации процессов описания, публикации, исполнения, оценки эффективности оказываемых услуг в области обеспечения безопасности.
- Гарантирует точное следование методикам, настроенным на этапах внедрения.
- Позволяет эволюционно развивать и расширять применяемые правила и маршруты оказания услуг, методики обогащения данных и правила оценки эффективности.
- Позволяет без программирования настраивать новые или модифицировать ранее существующие типы запросов на оказание услуг в области обеспечения безопасности.
- Позволяет без программирования настраивать новые или модифицировать ранее существующие правила централизованного сбора информации о событиях и мероприятиях различной экономической направленности, с последующей агрегацией по ним суммовых и количественных показателей, и гибко настраиваемым оперативным представлением сводных данных на виджетах дэшбордов для линейных исполнителей и руководителей различного уровня.
- Позволяет организовать работу операторов не только через web-интерфейс личных кабинетов, но и в режиме интеграции по API с ранее развернутыми на предприятиях программными комплексами.

В состав продукта «LAV. Цифровая платформа защиты бизнеса НЭКСУС» входит большое число модулей, базовыми из которых являются:

- Модуль «Авторизация»
- Модуль «Маркетплейс»
- Модуль «BPM. Управление процессами»
- Модуль «Каналы информирования»
- Модуль «Бизнес Аналитика»

Модуль «Авторизация».

Обеспечивает первичную аутентификацию и авторизацию операторов, реализует поддержку режима [Web SSO](#), генерирует и передает другим модулям программного комплекса JWT-токены ([JSON Web Token](#)). Позволяет вести единый реестр учетных записей операторов и их распределение по ролевой модели модулей программного комплекса.

Модуль «Маркетплейс».

Обеспечивает в режиме «единого окна» регистрацию и отслеживание хода исполнения запросов в подразделения безопасности. Позволяет настраивать типы запросов и наполнение витрины услуг в области обеспечения безопасности (маркетплейс).

Модуль «BPM. Управление процессами».

Позволяет разрабатывать, публиковать и исполнять схемы процессов исполнения запросов и проведения мероприятий в подразделениях безопасности. Обеспечивает стыковку с модулями информирования и свода аналитических показателей для передачи сообщений по ходу и результатам исполнения этапов обработки запросов и проведения мероприятий.

Модуль «Каналы информирования».

Обеспечивает ведение справочников каналов коммуникаций и шаблонов уведомлений. Обеспечивает стыковку с интеграционным контуром для рассылки уведомляющих сообщений.

Модуль «Бизнес Аналитика».

Позволяет настраивать без программирования правила агрегации показателей по входящим потокам сообщений. Обеспечивает ведение справочников аналитических регистров, панелей аналитики, виджетов, дэшбордов. Позволяет проектировать в режиме конструктора новые виджеты. Обеспечивает расчет агрегаций и оперативную визуализацию инфографики в процессе работы операторов с аналитическими дэшбордами.

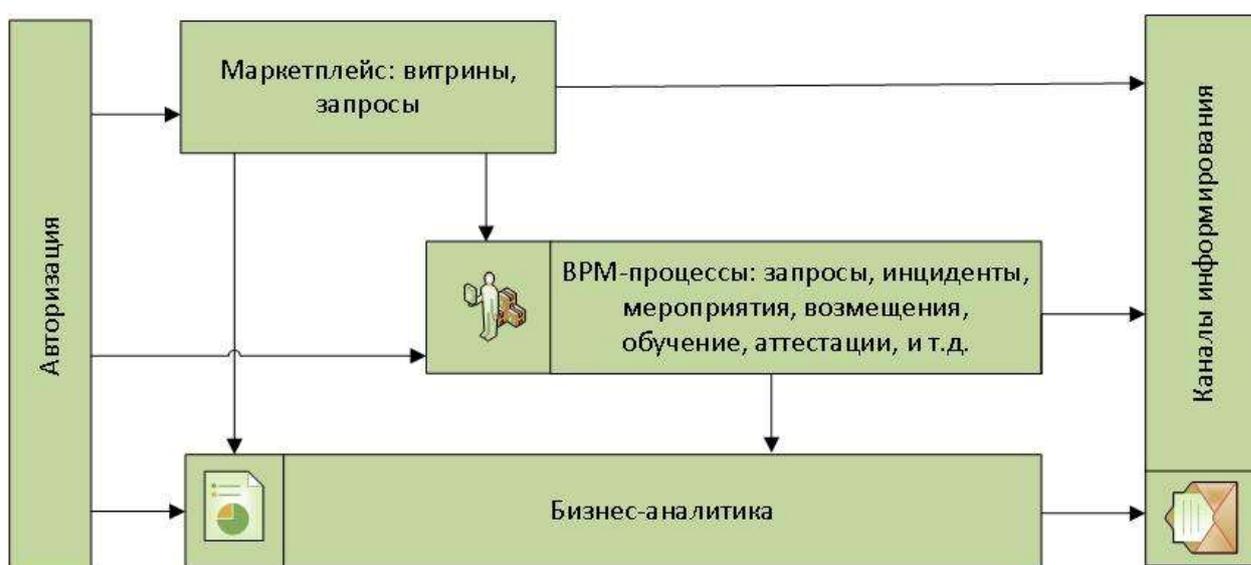
В качестве поставщиков внешних данных программный комплекс «LAB. Цифровая платформа защиты бизнеса НЭКСУС» может использовать методы сервиса «Контур-Фокус API», сервиса «DaData API», а также набор собственных коммуникационных адаптеров для получения данных из внутренних сервисов конкретного предприятия или группы компаний.

4 Архитектура

Программный комплекс реализован на языке JAVA с использованием фреймворка с открытым исходным кодом российской разработки - "Jmix" (<https://www.jmix.ru/>).

Взаимодействие программного комплекса с поставщиками информации осуществляется по защищенным транспортным каналам HTTPS/SSL посредством REST API вызовов и шин данных.

Архитектура связей между модулями программного комплекса представлена на рисунке:



Выделение коммуникационных компонентов на отдельный сервер и/или кластер серверов (в т.ч. построенный на базе контейнерных технологий) значительно упрощает логику сопровождения и позволяет динамически наращивать функциональность и производительность программного комплекса в целом.

В базовой поставке присутствуют адаптеры к методам сервиса «Контур-Фокус API» (<https://kontur.ru/focus-api>), и сервиса «DaData API» (<https://dadata.ru/>) которые на демонстрационном стенде могут быть перекрыты программными эмуляторами.

5 Системные требования

В качестве операционной системы серверов рекомендуется использовать российскую сборку ОС Astra Linux Special Edition 64-bit версии не ниже 1.7 в редакции «Смоленск» или иной дистрибутив ОС, совместимой на уровне linux-ядра.

В качестве среды исполнения Java-кода рекомендуется использовать российскую сборку Axiom/Liberica JDK 64-bit не ниже 17 версии. При этом допустимо использовать также сборку свободно-распространяемой Open JDK 17/21 64-bit.

В качестве системы управления базами данных рекомендуется использовать российскую сборку СУБД Postgres Pro не ниже 14 версии. При этом допустимо использовать также сборку свободно-распространяемой СУБД PostgreSQL 14.

Параметры серверного оборудования для непосредственного исполнения приложения необходимо подбирать, исходя из рекомендаций обеспечить не менее 4 ядер CPU 2GHz и не менее 16 Gb RAM на одно кластерное ядро.

Общая последовательность действий для запуска приложения:

- Подготовить сервера СУБД, загрузить на вновь созданные базы данных дампы начального состояния и/или выполнить набор sql-скриптов по начальному заполнению таблиц.
- Подготовить исполнительные сервера, настроить на них среду исполнения java-кода, разместить исполняемые файлы приложения и конфигурационные файлы.
- Подготовить коммуникационные сервера, настроить параметры коннекторов для получения внешних данных.
- Подготовить сетевую инфраструктуру, обеспечить требуемые уровни изоляции и защиты трафика.
- Подготовить средства балансировки трафика, обеспечения отказоустойчивости, средства резервного копирования.
- Обеспечить запуск и согласованное выполнение компонентов приложения.

Для демонстрационно-ознакомительных целей запуск элементов программного продукта «LAV. Цифровая платформа защиты бизнеса НЭКСУС» допустим в среде контейнеров Docker. Более подробное описание системных требований и последовательности развёртывания для этого случая приведено в соответствующем разделе технической документации.

6 Сценарии эксплуатации

Стандартным вариантом использования платформы НЭКСУС является ее развертывание в ЦОД в качестве «облачного» SaaS-сервиса с последующей настройкой коннекторов ко внешним источникам данных и регистрацией в системе учетных записей аналитиков для проведения настроек и учетных записей для конечных потребителей услуг. Сотрудники предприятий-заказчиков получают возможность как непосредственной работы с web-интерфейсами Личного кабинета, так и встраивания функциональных возможностей платформы НЭКСУС в контур автоматизации своего предприятия, посредством API-вызовов.

Общая последовательность действий для начала работы:

- Сменить начальный пароль администратора, завести учетные записи операторов, назначить функциональные роли. Завести технологические учетные записи для доступа по API.
- Настроить справочники, подключить шаблоны отчетных форм и/или дэшбордов информационных панелей.
- Обеспечить начальное обучение операторов и сотрудников сопровождения, определить порядок работы по инцидентам.
- Активировать учетные записи операторов, сообщить операторам реквизиты для доступа к функционалу личного кабинета.
- Активировать технологические учетные записи, сообщить группе интеграции реквизиты для доступа по API.
- В режиме личного кабинета и/или запросами по API начать формирование запросов на оказание услуг и сбор событий для расчета аналитических показателей.
- Обеспечить надлежащий мониторинг элементов программного комплекса и регламентную работу служб сопровождения.

Таким образом, сценарий эксплуатации программного продукта является типичным для многопользовательских информационных систем, предназначенных для решения специфических отраслевых задач.

На уровне рядового оператора сценарий работы выглядит следующим образом:

- Авторизация в приложении (ввод логина и пароля).
- Просмотр витрины услуг, выбор нужного типа услуги, оформление запроса на предоставление этой услуги, получение результатов по запросу.
- Просмотр истории запросов на оказание услуг.
- Просмотр и исполнение назначенных заданий.
- Просмотр дэшбордов с визуализацией аналитических показателей.

На уровне оператора с ролью, соответствующей аналитику-технологу, дополнительно будут доступны функциональные блоки:

- Проектирование в режиме конструктора новых типов.
- Проектирование в режиме конструктора новых правил сбора и агрегации данных.
- Проектирование в режиме конструктора новых правил расчета аналитических показателей.
- Проектирование в режиме конструктора наборов виджетов и их группировку в дэшборды.
- Проектирование в режиме конструктора схем исполнения запросов и проведения мероприятий в нотации BPMN 2.0.

На уровне администраторов и сотрудников сопровождения могут быть доступны функциональные блоки, связанные с ведением учетных записей, настройкой ролевой модели доступа, протоколы и статистические выборки по динамике работы программного комплекса.

При этом параметры web-сессий и действия операторов протоколируются вне зависимости от уровня доступа и ролевых ограничений.

7 Сопровождение и администрирование

Программный продукт «LAV. Цифровая платформа защиты бизнеса НЭКСУС» является многокомпонентным, поэтому его сопровождение и администрирование требует достаточно высокой квалификации и опыта.

Помимо программных компонентов, непосредственно являющихся составными частями комплекса, в реальной промышленной конфигурации могут оказаться востребованы следующие программно-аппаратные решения:

- Интеллектуальные маршрутизаторы сетевого трафика.
- Балансировщики сессионной нагрузки.
- Среды виртуализации.
- Среды исполнения контейнеризованных образов (микросервисы).
- Системы репликации БД и резервного копирования.
- Системы управления серверными конфигурациями.

Перечисленные решения не являются обязательными, но могут значительно повысить отказоустойчивость и масштабируемость сервисов ЦОД, предоставляемых на базе программного продукта «LAV. Цифровая платформа защиты бизнеса НЭКСУС», а также снизить затраты на их текущее сопровождение.