F6

ПО «F6 Transaction Fraud Protection»

Руководство администратора

Оглавление

Термины и сокращения **3**

#1 Общие сведения **4**

1.1. Введение 4

1.2. Назначение ПО 4

1.3. Программно-аппаратные среды функционирования ПО 4

1.4. Технические требования к составу оборудования при размещении в инфраструктуре Заказчика 4

1.5. Требования к базам данных 5

#2 Общие принципы функционирования ПО **6**

#3 Обязанности и функции администратора Заказчика **7**

#4 Порядок встраивания **8**

4.1. Подготовка инфраструктуры 8

4.2. Предоставление доступа и развертывание 8

4.3. Конфигурация и проверка 8

4.4. Подготовка к эксплуатации 9

4.5. Создание тестовых учетных записей 9

#5 Поддержание функционирования ПО **10**

Термины и сокращения

Заказчик	Лицо, использующее программное обеспечение на основании заключенного договора и эксплуатирующее его в своей инфраструктуре
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО «БУДУЩЕЕ»; • Компанией-интегратором, по выбору Заказчика
Операция	Отдельное действие или событие в системе, связанное с выполнением бизнес-процесса или обработкой данных и подлежащее анализу и учету
ПО	Программное обеспечение «F6 Transaction Fraud Protection»
Пользователь	Лицо, взаимодействующее с цифровыми каналами обслуживания Заказчика, в отношении которого применяется антифрод-защита
Разработчик	АО «БУДУЩЕЕ»
СУБД	Система управления базами данных
Транзакция	Зафиксированное финансовое действие, приводящее к изменению денежных средств, финансовых активов или обязательств между субъектами и подлежащее учёту, контролю и подтверждению
API	(Application Programming Interface) Программный интерфейс, который позволяет разным системам обмениваться данными и взаимодействовать друг с другом по заранее определенным правилам
API Connector	Серверный модуль системы, предназначенный для интеграции backend-систем Заказчика с антифрод-платформой через API и обеспечения передачи транзакционных событий и получения результатов их обработки
On-premises	Модель развертывания программного обеспечения, при которой система устанавливается и эксплуатируется в собственной инфраструктуре Заказчика, без использования внешних облачных сервисов

#1 Общие сведения

1.1. Введение

Настоящий документ содержит описание реализации программного обеспечения «F6 Transaction Fraud Protection» (далее — ПО, Transaction Fraud Protection).

1.2. Назначение ПО

«F6 Transaction Fraud Protection» — система, предназначенная для защиты пользователей и транзакций в момент их совершения. Она анализирует операции, оценивает риски, выявляет аномалии и маркирует подозрительные действия. Платформа автоматизирует расследования и обеспечивает полный цикл защиты в соответствии с требованиями регуляторов.

1.3. Программно-аппаратные среды функционирования ПО

Для корректного функционирования ПО необходим веб-браузер.

ПО поддерживает работу на следующих версиях браузеров:

- Internet Explorer версии 8.0 и выше;
- Google Chrome версии 4.0 и выше;
- Mozilla Firefox версии 3.5 и выше;
- Apple Safari версии 4.0 и выше;
- Opera версии 10.5 и выше;
- iOS Safari версии 3.2 и выше;
- Opera Mobile версии 11.0 и выше;
- Google Chrome for Android версии 11.0 и выше;
- Mozilla Firefox for Android версии 26.0 и выше;
- Windows Internet Explorer Mobile версии 10.0 и выше;
- Яндекс Браузер версии 23.1.1 и выше.

В браузере устройства Заказчика должно быть разрешено исполнение скриптов JavaScript.

1.4. Технические требования к составу оборудования при размещении в инфраструктуре Заказчика

При размещении в инфраструктуре Заказчика требуется выделить следующие минимальные вычислительные мощности для установки системы в промышленную эксплуатацию:

- Серверы приложений (3 шт.):
  - CPU: 4 core, 2Mhz и выше;
  - RAM: 32 GB;
  - HDD: 200 GB;
  - ОС: Ubuntu, РЕД ОС.
- Серверы баз данных (3 шт.):

- CPU: 4 core, 2Mhz и выше;
- RAM: 32 GB;
- HDD: 1 TB;
- ОС: Ubuntu, РЕД ОС.

Требования для разворачивания предоставленной тестовой среды:

- Среда виртуализации: система управления контейнерами Kubernetes.

1.5. Требования к базам данных

ПО функционирует с использованием следующих СУБД:

- Apache Cassandra 4.0 и выше;
- Elasticsearch 7.0 и выше;
- ClickHouse 20.1 и выше.

#2 Общие принципы функционирования ПО

На рисунке 1 изображены общие принципы функционирования ПО.

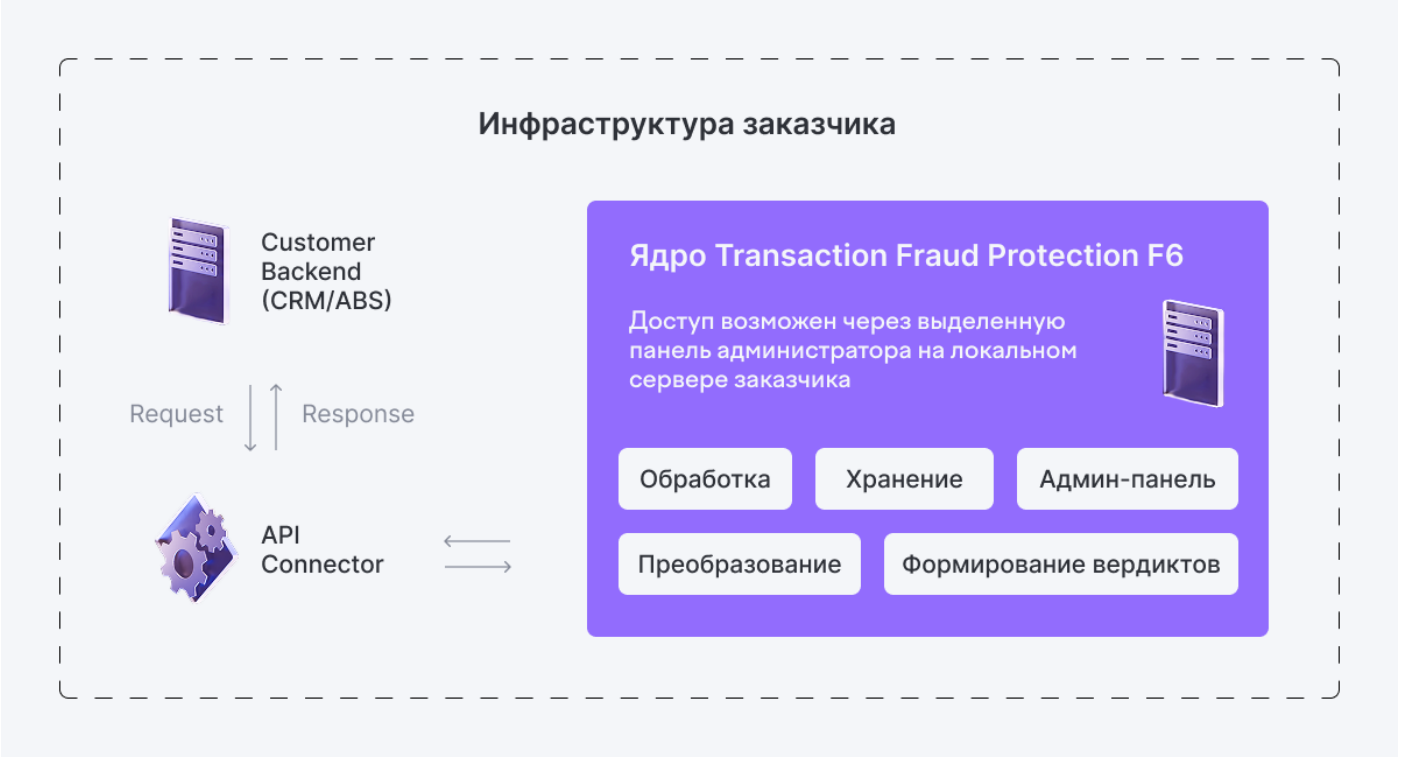

Рисунок 1. Общие принципы функционирования ПО «F6 Transaction Fraud Protection»

Платформа предоставляется в виде on-premises-решения для развертывания в инфраструктуре Заказчика. Взаимодействие с системой осуществляется через API-интерфейс, а результаты обработки операций возвращаются с использованием различных технологий, включая MQ-очереди и API-ответы.

API Connector — это серверный модуль Transaction Fraud Protection, предназначенный для прямого подключения backend-систем Заказчика. Модуль интегрируется с внутренней архитектурой защищаемого сервиса и обеспечивает защиту транзакций, инициированных из различных каналов, включая веб-каналы, мобильные приложения и API.

ПО осуществляет сбор и анализ данных об операциях, поступающих из защищаемых систем Заказчика, и направляет их на обработку в аналитическую платформу Разработчика. При выявлении признаков мошенничества в транзакции (аномалии в реквизитах, подозрительные паттерны) система незамедлительно направляет Заказчику уведомление, на основании которого Заказчик может предпринять действия по блокировке операции либо провести дополнительную проверку.

#3 Обязанности и функции администратора Заказчика

В обязанности администратора входит следующее:

- Обеспечение доступа сотрудникам Исполнителя для установки и первоначальной настройки необходимого ПО и компонентов системы в инфраструктуре Заказчика;
- Интеграция установленного ПО с требуемыми сервисами и платформами в соответствии с технической документацией;
- Выполнение штатных (стандартных) настроек площадки (проекта) для обеспечения ее работоспособности в рамках требований бизнес-процессов;
- Обеспечение стабильного и бесперебойного функционирования вычислительной инфраструктуры, предоставленной Исполнителем, в рабочем режиме;
- Мониторинг работы системы и выполнение регулярных регламентных операций при необходимости;
- Обработка типовых инцидентов, связанных с доступностью и базовой функциональностью системы, в рамках первой линии поддержки.

#4 Порядок встраивания

4.1. Подготовка инфраструктуры

Для обеспечения корректного развертывания и дальнейшей эксплуатации ПО необходимо выполнить следующие подготовительные действия:

- Исполнитель предоставляет Заказчику расчет необходимых мощностей и технические требования к инфраструктуре (серверы, хранилища, сеть, СУБД и т. д.) для развертывания ПО;
- Заказчик на основе полученных требований подготавливает и предоставляет необходимые ресурсы (выделенные серверы, виртуальные машины, кластеры, сети, учетные записи);
- Заказчик согласует доступ к репозиториям Разработчика и конфигурационным серверам Разработчика;
- Заказчик согласует перечень доменов, используемых системой для приема запросов на обработку, а также для интеграции с внутренними и внешними системами;
- Заказчик согласует IP-адреса, с которых будет осуществляться взаимодействие с ПО.

4.2. Предоставление доступа и развертывание

В рамках развертывания системы и подготовки ее к эксплуатации стороны выполняют следующие действия:

- Заказчик обеспечивает доступ сотрудникам Исполнителя к предоставленным ресурсам в объеме, необходимом для проведения работ;
- Исполнитель загружает необходимые дистрибутивы и пакеты для развертывания системы;
- Исполнитель настраивает оркестрируемое контейнерное окружение и сетевое взаимодействие k8s-кластера;
- Исполнитель назначает узлам кластера согласованные доменные имена, загружает клиентские сертификаты и/или выпускает сертификаты для работы HTTPS;
- Исполнитель настраивает службы приема и обработки трафика, инициализацию баз данных, брокеры сообщений и/или службы отправки данных для интеграции с системами Заказчика;
- Исполнитель регистрирует площадку на сервере конфигураций Разработчика для проведения управления конфигурациями и выполнения обновлений;
- Исполнитель развертывает стек приложений для мониторинга, системных оповещений и логирования работы всех критичным элементов системы. Настраивается централизованный сбор метрик и алертов с площадки;
- Исполнитель выполняет развертывание админ-панели с графическим интерфейсом для работы в системе;
- Выполняется загрузка актуальной конфигурации правил обработки трафика, политик и шаблонов;
- Осуществляется настройка почтовой службы и интеграция с системой аутентификации Заказчика.

4.3. Конфигурация и проверка

На данном этапе специалисты Исполнителя выполняют первоначальную настройку площадки и проверку ее работоспособности, включая:

- конфигурирование параметров системы;
- интеграцию с внешними сервисами;

- настройку бизнес-логики.

Проводится комплексная проверка корректности развертывания процессинга и работоспособности всей системы, включая тестовые запуски, верификацию ключевых процессов, проверку получаемых метрик и проведение функциональных испытаний.

4.4. Подготовка к эксплуатации

Специалисты Исполнителя выполняют финальные административные настройки, необходимые для начала эксплуатации системы, включая:

- настройку административной панели управления;
- создание и конфигурация проектов (окружений) в системе;
- создание учетных записей для специалистов Заказчика в соответствии с требуемыми ролями.

4.5. Создание тестовых учетных записей

Для проверки корректности настройки системы и настроенных алгоритмов Исполнителю необходим доступ к тестовой учетной записи. Данный доступ требуется для формирования тестовых запросов, получения и анализа ответных пакетов, а также для верификации срабатывания алгоритмов в условиях, приближенных к реальной эксплуатации.

Условия предоставления тестовых учетных записей определяются Заказчиком.

#5 Поддержание функционирования ПО

Поддержание функционирования ПО заключается в контроле настроек, проведенных в рамках установки ПО. Иных регламентных мероприятий со стороны Заказчика ПО не требует.