F6

ПО «F6 Transaction Fraud Protection»

Описание функциональных характеристик

Оглавление

Термины и сокращения

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
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 описывает функциональные характеристики 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. Функциональные возможности ПО

Функциональные возможности «F6 Transaction Fraud Protection» позволяют:

1. Выявлять хищения с использованием социальной инженерии, включая подложные сайты, мошеннические рассылки и звонки, а также активность в социальных сетях, за счет проверки транзакций;
2. Выявлять финансовые мошеннические операции, такие как хищения в системах дистанционного банковского обслуживания, карточное мошенничество, подмена платежных реквизитов и т. п.;
3. Выявлять мошенничество, связанное с использованием реквизитов, включенных в списки ФинЦЕРТ;
4. Выявлять кредитное мошенничество, включая подачу множественных заявок и использование похищенных персональных данных;
5. Проводить аналитику по сформированным инцидентам, выявляя взаимосвязи и типичные сценарии;
6. Маркировать транзакции по результатам проведенной аналитики с определением используемой схемы мошенничества.

#2 Требования к системе

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.

2.1. 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.

2.2. 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.

#3 Общие принципы функционирования ПО

На рисунке 1 изображены общие принципы функционирования ПО.

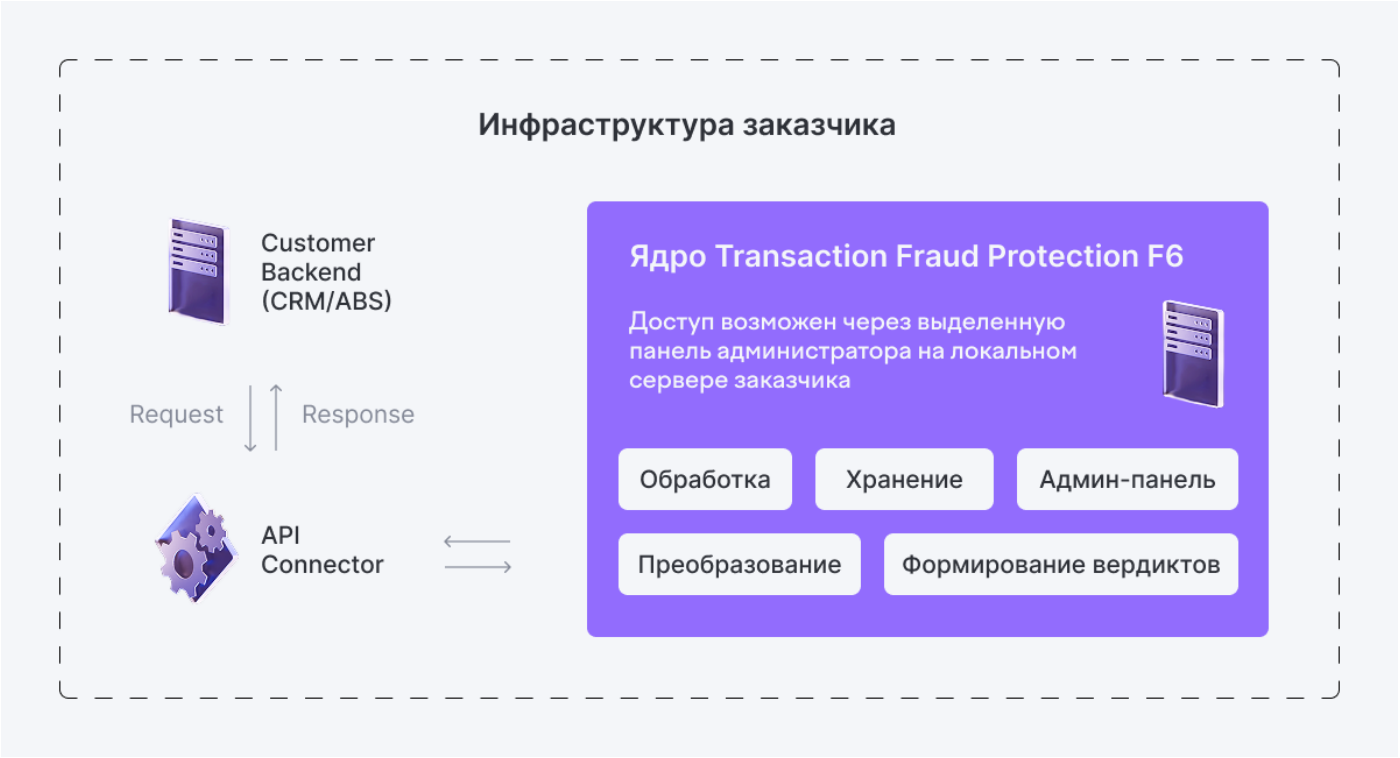

Рисунок 1. Общие принципы функционирования ПО "F6 Transaction Fraud Protection"

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.

#4 Реализация ПО

4.1. Структура ПО

Платформа предоставляется в виде On-premises-решения для обработки правил выявления мошеннических операций через API. Решение развертывается в инфраструктуре Заказчика и поддерживает пользовательские форматы данных, обеспечивая интеграцию с существующими платежными системами, процессингом и внутренними сервисами.

Взаимодействие с платформой осуществляется через API-интерфейс, а результаты обработки передаются в различных форматах — через API-ответы или MQ-очереди — в соответствии с архитектурой Заказчика.

4.2. Состав ПО

Архитектура ПО представляет собой сервис-ориентированную архитектуру, основанную на использовании распределенных, слабо связанных, заменяемых компонентов, оснащенных стандартизированными интерфейсами для взаимодействия по стандартизированным протоколам. Унификация программных интерфейсов осуществляется как минимум на следующих уровнях, но не ограничиваясь ими:

- Браузера пользователя;
- API Connector;
- АС Заказчика.

В состав ПО входят компоненты прикладного уровня, обеспечивающие сбор и анализ информации из транзакционных пакетов данных Заказчика с целью выявления аномалий и признаков мошенничества. При обнаружении подозрительной активности компоненты немедленно передают структурированный ответ непосредственно в автоматизированные системы Заказчика для блокировки или дополнительной верификации операции.

Компоненты ПО включают в себя:

- Подсистему получения данных из АС Заказчика

  Подсистема предназначена для получения детализированных параметров операций пользователей из защищаемых систем Заказчика. Она собирает признаки мошеннической активности, полные контекстные данные о транзакциях и поведенческие атрибуты для комплексного анализа рисков;

- Подсистему обработки данных

  Подсистема предназначена для обработки данных, полученных от подсистемы получения данных из АС Заказчика — проверки данных на валидность и целостность;

- Подсистему управления

  Подсистема предназначена для выполнения настроек и администрирования ПО;

- Подсистему аналитики

  Подсистема предназначена для работы аналитиков АС с выявленными событиями мошеннической активности, получения отчетов и статистики, настройки правил выявления мошеннической активности;

- Подсистему информационного обмена

  Подсистема предназначена для экспорта и импорта данных между АС Заказчика и ПО как в режиме реального времени, так и в диалоговом (запросном) режиме, а также для передачи в АС Заказчика вердиктов и скорингов по выявленным фактам мошеннической активности;

- Подсистему защиты информации

  Подсистема представляет собой программно-технический комплекс, предназначенный для защиты технических средств, программного обеспечения и данных АС от несанкционированного доступа. Подсистема выполняет функции

идентификации и аутентификации сторон, осуществляющих обмен информацией, а также функции разграничения прав доступа к информационным ресурсам АС.

4.3. Функции частей ПО

API Connector выполняет следующие ключевые функции для интеграции и защиты транзакций:

1. Прием и обработка транзакционных данных:
    - Прием структурированных транзакций в форматах JSON, XML или бинарных протоколах (ISO 8583, УФЭБС);
    - Валидация и обогащение данных в реальном времени, дополнение операций внутренними и внешними индикаторами риска;
    - Передача запросов в подсистемы для выполнения проверок по заданным правилам и сценариям.
2. Интеграция и взаимодействие:
    - Поддержка гибких протоколов взаимодействия (REST API, gRPC, MQ-очереди, Kafka);
    - Маршрутизация запросов к различным аналитическим компонентам в зависимости от типа операции или канала;
    - Обеспечение соответствия форматам заказчика и преобразование данных при необходимости.
3. Управление ответами и реакциями:
    - Возврат гибких ответов (решение, оценка риска, код причины, рекомендуемое действие);
    - Передача результатов и метаданных в АС Заказчика для исполнения решений (блокировка, пропуск).

#5 Взаимодействие ПО с автоматизированными системами

5.1. Принципиальная схема взаимодействия ПО

Принципиальная схема взаимодействия ПО с АС Заказчика и Разработчика представлена на рисунке 1.

5.2. Структура взаимодействия

Во взаимодействии участвуют следующие компоненты:

- АС Разработчика;
- АС Заказчика.

АС Разработчика состоит из следующих компонентов:

- Серверная инфраструктура, которая принимает, обрабатывает и анализирует контрольные данные, полученные от АС Заказчика;
- Сервер управления, предназначенный для взаимодействия Заказчика с АС Разработчика;
- АРМ администратора, обеспечивающее настройку и сопровождение АС.

АС Заказчика состоит из следующих компонентов:

- Совокупность веб-серверов и серверов приложений веб-ресурса;
- Модуль автоматизации, использующий API АС Разработчика для автоматизации реагирования на выявленные подозрительные события. Необходимость разработки данного модуля и правила реагирования определяются Заказчиком;
- АРМ администратора, предназначенное для ознакомления с подозрительными событиями и управления настройками их выявления.

5.3. Порядок взаимодействия

1. Инициация события. АС Заказчика формирует запрос с данными по операции и направляет его по защищенному каналу в систему Разработчика.
2. Обработка правил. Система Исполнителя анализирует транзакцию в соответствии с настроенными транзакционными правилами, профилями и внешними источниками данных (ФинЦЕРТ, списки), оценивая риск мошенничества.
3. Формирование решения. По результатам анализа система формирует и возвращает в АС Заказчика структурированный ответ (решение: разрешить, блокировать или запросить дополнительную проверку; оценка риска; код причины).
4. Отображение в веб-интерфейсе. После формирования решения детализированная информация о событии (атрибуты транзакции, сработавшие правила, оценка риска) становится доступной для просмотра в веб-интерфейсе.
5. Аналитика и обратная связь. Аналитик Заказчика через веб-интерфейс изучает событие, проводит расследование и при необходимости вносит корректировки.
6. Передача обратной связи. Заказчик через веб-интерфейс сервера управления АС Разработчика передает обратную связь по выявленному событию, которая учитывается при последующей обработке данных, поступающих от АС Заказчика.

5.4. Данные, передаваемые из АС Заказчика

Характер и состав данных, передаваемых из АС Заказчика на платформу Исполнителя, определяются Заказчиком индивидуально на этапе интеграции.

В рамках настройки взаимодействия согласовываются:

- Форматы передаваемых данных (например, структурированные пакеты по стандарту УФЭБС, ISO 8583, JSON, XML или иные внутренние форматы Заказчика);
- Типы обрабатываемых операций (платежи, переводы, верификация, логины и другие события, требующие анализа рисков);
- Контракты взаимодействия (описание полей, их семантика, обязательные и опциональные атрибуты);
- Форматы ответов и решений от системы Исполнителя (разрешение или блокировка, оценка риска, коды причин, рекомендации по дополнительной проверке).

Например, в качестве типового примера пакета данных может выступать транзакция в формате УФЭБС ED101, включающая всю необходимую для анализа информацию: реквизиты операции, данные об устройстве, контекст сессии и признаки, актуальные для выявления мошенничества.

Пример пакета данных:

```
<?xml version="1.0" encoding="Windows-1251"?>
<!--Центральный Банк Российской Федерации.
Унифицированные форматы электронных банковских сообщений.

ППС

Схемы с описанием прикладных частей электронных сообщений, используемых в расчетной сети Банка России.

-->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:ed="urn:cbr-ru:ed:v2.0" xmlns:lt="urn:cbr-
ru:ed:leaftypes:v2.0" targetNamespace="urn:cbr-ru:ed:v2.0" elementFormDefault="qualified"
attributeFormDefault="unqualified" version="2025.09.1">
	<xs:include schemaLocation="cbr_ed_objects_v2025.09.1.xsd"/>
	<xs:import namespace="urn:cbr-ru:ed:leaftypes:v2.0" schemaLocation="cbr_ed_leaftypes_v2025.09.1.xsd"/>
	<xs:annotation>
		<xs:documentation>Прикладные части ЭС</xs:documentation>
	</xs:annotation>
	<xs:element name="ED101" type="ed:ED101"/>
	<xs:complexType name="ED101">
		<xs:annotation>
			<xs:documentation>Платежное поручение</xs:documentation>
			<xs:documentation>Customer Credit Transfer</xs:documentation>
		</xs:annotation>
		<xs:complexContent>
			<xs:extension base="ed:EPDComplete">
				<xs:sequence>
					<xs:element name="IndirectParticipantInfo"
type="ed:IndirectParticipantInfoType" minOccurs="0" maxOccurs="1">
						<xs:annotation>
							<xs:documentation>Информация о косвенном
участнике.</xs:documentation>
							<xs:documentation>Information about Indirect
Participant.</xs:documentation>
						</xs:annotation>
```

```
                                        </xs:element>
                                        <xs:element name="ParticipantBusinessScenario"
type="lt:ParticipantBusinessScenarioType" minOccurs="0">
                                                <xs:annotation>
                                                        <xs:documentation>Идентификатор бизнес-сценария,
определяемый участником.</xs:documentation>
                                                        <xs:documentation>Participant-defined Business
Scenario.</xs:documentation>
                                                </xs:annotation>
                                        </xs:element>
                                        <xs:element name="SettlementCondition" type="ed:SettlementCondition"
minOccurs="0">
                                                <xs:annotation>
                                                        <xs:documentation>Реквизиты условия исполнения
распоряжения.</xs:documentation>
                                                        <xs:documentation>Payment Settlement Condition
Attributes.</xs:documentation>
                                                </xs:annotation>
                                        </xs:element>
                                        <xs:element name="Purpose" type="lt:Max210TextType">
                                                <xs:annotation>
                                                        <xs:documentation>Назначение платежа (поле
24).</xs:documentation>
                                                        <xs:documentation>Payment Purpose (Field
24).</xs:documentation>
                                                </xs:annotation>
                                        </xs:element>
                                        <xs:element name="DepartmentalInfo" type="ed:DepartmentalInfo"
minOccurs="0">
                                                <xs:annotation>
                                                        <xs:documentation>Ведомственная информация (поля 101, 104-
110).</xs:documentation>
                                                        <xs:documentation>Authorities Information (fields 101, 104-
110).</xs:documentation>
                                                </xs:annotation>
                                        </xs:element>
                                        <xs:element name="InitialED" type="ed:EDRefID" minOccurs="0">
                                                <xs:annotation>
                                                        <xs:documentation>Идентификаторы исходного ЭПС (поля 203-
205).</xs:documentation>
                                                        <xs:documentation>Initial FTI Identifiers (fields 203-
205).</xs:documentation>
                                                </xs:annotation>
                                        </xs:element>
                                        <xs:element name="ProcessingDetails" type="ed:ProcessingDetails"
minOccurs="0">
                                                <xs:annotation>
                                                        <xs:documentation>Идентификатор бизнес-сценария,
определяемый системой.</xs:documentation>
                                                        <xs:documentation>System-defined Business Scenario
Identifier.</xs:documentation>
                                                </xs:annotation>
                                        </xs:element>
                                        <xs:element name="Me2MeDetails" type="ed:Me2MeDetailsType" minOccurs="0">
```

```
                                        <xs:annotation>
                                                <xs:documentation>Информация о переводе денежных средств
физическим лицом между своими счетами.</xs:documentation>
                                        </xs:annotation>
                                </xs:element>
                        </xs:sequence>
                        <xs:attribute name="TransKind" type="lt:TwoDigitCodeType" use="required"
fixed="01">
                                <xs:annotation>
                                        <xs:documentation>Вид операции (поле 18).</xs:documentation>
                                        <xs:documentation>FTI Type (Field 18).</xs:documentation>
                                </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="Priority" type="lt:PaytPriorityCodeType" use="required">
                                <xs:annotation>
                                        <xs:documentation>Очередность платежа (поле 21).</xs:documentation>
                                        <xs:documentation>FTI Sequence (Field 21).</xs:documentation>
                                </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="ReceiptDate" type="lt:DateType">
                                <xs:annotation>
                                        <xs:documentation>Поступило в банк плательщика (поле
62).</xs:documentation>
                                        <xs:documentation>FTI's Acceptance Date to Payer's Bank (Field
62).</xs:documentation>
                                </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="FileDate" type="lt:DateType">
                                <xs:annotation>
                                        <xs:documentation>Дата помещения в картотеку (поле
63).</xs:documentation>
                                        <xs:documentation>FTI's Queueing Date into the queue of FTI's not
settled in time (Field 63).</xs:documentation>
                                </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="ChargeOffDate" type="lt:DateType">
                                <xs:annotation>
                                        <xs:documentation>Списано со счета плательщика (поле 71). Дата
списания денежных средств со счета плательщика.</xs:documentation>
                                        <xs:documentation>Payer's Account Debit Date (Field
71).</xs:documentation>
                                </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="SystemCode" type="lt:SystemCodeType" use="required">
                                <xs:annotation>
                                        <xs:documentation>Признак системы обработки.</xs:documentation>
                                        <xs:documentation>Fund transfer service (urgent/non-
urgent).</xs:documentation>
                                </xs:annotation>
                        </xs:attribute>
                        <xs:attribute name="PaymentID" type="lt:PaymentIDType">
                                <xs:annotation>
                                        <xs:documentation>Уникальный идентификатор платежа, присвоенный
получателем средств (поле 22)</xs:documentation>
```

```
                                        <xs:documentation>Unique Payment Identifier assigned by the
(ultimate) creditor (Field 22) OR Unique credit ID</xs:documentation>
                                    </xs:annotation>
                            </xs:attribute>
                            <xs:attribute name="ResField" type="lt:Max35TextType">
                                    <xs:annotation>
                                            <xs:documentation>Резервное поле (поле 23).</xs:documentation>
                                            <xs:documentation>Reserval Field (Field 23).</xs:documentation>
                                    </xs:annotation>
                            </xs:attribute>
                            <xs:attribute name="OperationID" type="lt:OperationIDType">
                                    <xs:annotation>
                                            <xs:documentation>Уникальный присваиваемый номер
операции.</xs:documentation>
                                            <xs:documentation>Unique Number assigned to
Operation.</xs:documentation>
                                    </xs:annotation>
                            </xs:attribute>
                            <xs:attribute name="BROperationID" type="lt:OperationIDType">
                                    <xs:annotation>
                                            <xs:documentation>Уникальный присваиваемый номер операции Банка
России.</xs:documentation>
                                            <xs:documentation>Unique Number assigned to Bank of Russia
Operation.</xs:documentation>
                                    </xs:annotation>
                            </xs:attribute>
                            <xs:attribute name="CBDCOperationID" type="lt:UUIDType">
                                    <xs:annotation>
                                            <xs:documentation>Идентификатор связанной операции на
ПлЦР.</xs:documentation>
                                            <xs:documentation>Unique Number of CBDC
Operation.</xs:documentation>
                                    </xs:annotation>
                            </xs:attribute>
                            <xs:attribute name="ForGKU" type="lt:GKUType">
                                    <xs:annotation>
                                            <xs:documentation>Признак платежа за ЖКУ, совершаемого
льготником.</xs:documentation>
                                            <xs:documentation>Payment for GKU.</xs:documentation>
                                    </xs:annotation>
                            </xs:attribute>
                    </xs:extension>
            </xs:complexContent>
    </xs:complexType>
</xs:schema>
```

#6 Обеспечение информационной безопасности

6.1. Защита передаваемых данных

Весь обмен информации между АС Разработчика и АС Заказчика производится по протоколу HTTPS.

Передаваемые данные дополнительно кодируются в целях защиты от вредоносного программного обеспечения, функционирующего на устройстве пользователя.

6.2. Безопасность периметра АС Заказчика

Обмен данными между АС Заказчика и АС Разработчика всегда инициируется только со стороны Заказчика на заранее оговоренные интерфейсы API.

6.3. Обеспечение доступности

В случае, если архитектура взаимодействия не предполагает размещения АС Разработчика в разрыв между системами Заказчика, ее недоступность не влияет на работоспособность и доступность защищаемых сервисов Заказчика. Функционирование бизнес-процессов и обработка операций продолжаются в штатном режиме, обеспечивая непрерывность обслуживания пользователей.

При этом АС Разработчика реализует механизмы отказоустойчивости собственной инфраструктуры.