ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «F6 Fraud Protection»

Описание функциональных характеристик

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	**Описание**
АС	Автоматизированная система АО «БУДУЩЕЕ»
Дроппер	Зарегистрированный пользователь в системе заказчика передавший третьим лицам все необходимы данные и реквизиты для управления приложением или выполняющий указания третьих лиц за вознаграждение
Заказчик	Лицо, которое использует на законных основаниях ПО на основании заключенного договора
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО «БУДУЩЕЕ»; • Компанией-интегратором, по выбору Заказчика
ПО	Программное обеспечение «F6 Fraud Protection»
Разработчик	АО «БУДУЩЕЕ»
Скриншот	Изображение, «снимок» экрана ПК или мобильного устройства, на котором запечатлено содержимое экрана устройства
СУБД	Система управления базами данных
ТС	Система взаимодействия Заказчика, позволяющая обмениваться сообщениями и создавать цепочки обращений, которая представляет из себя отдельный раздел «Службу Поддержки» в панели управления «F6 Fraud Protection». В случае недоступности указанных систем формат взаимодействия осуществляется через

	электронный почтовый ящик
Файл cookie	Файл с небольшим набором данных, которые веб-ресурс отправляет на компьютер пользователя для идентификации устройства
API	(Application Programming Interface) описание способов взаимодействия одной компьютерной программы с другими
Mobile SDK (далее – SDK)	Модуль программного обеспечения «F6 Fraud Protection» для встраивания в мобильные приложения
RSA	Криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших полупростых чисел
On-premise	Модель обслуживания, при которой данные и приложения размещаются и хранятся в инфраструктуре Пользователя
Saas (Software as a Service)	Модель обслуживания, при которой программное обеспечение размещено в облачной инфраструктуре
SHA1	(Secure Hash Algorithm 1) — алгоритм криптографического хеширования
Web Snippet (далее – скрипт)	Модуль программного обеспечения «F6 Fraud Protection» для встраивания в веб-приложения

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ описывает функциональные характеристики программного обеспечения «F6 Fraud Protection» (далее — ПО, F6 Fraud Protection, Fraud Protection).

1.2 Назначение ПО

«F6 Fraud Protection» — система для противодействия мошенничеству и защиты цифровой личности пользователя в цифровых каналах обслуживания, а также защиты цифровых ресурсов от ботов и предотвращения мошенничества. ПО позволяет выявлять и предотвращать мошенническую активность, а также улучшать пользовательский опыт в автоматизированных системах Заказчика.

1.3 Функциональные возможности ПО

Функциональные возможности «F6 Fraud Protection» позволяют:

- выявлять хищения с использованием социальной инженерии (подложные сайты, мошеннические рассылки и звонки, социальные сети);
- выявлять мошеннические действия с учетной записью пользователя (несанкционированный доступ, множественные регистрации, несанкционированные действия от имени пользователя);
- выявлять финансовое мошеннические операции (хищения из систем дистанционного банковского обслуживания, карточное мошенничество, подмена реквизитов);
- выявлять мошеннические действия с использованием вредоносного программного обеспечения (веб-инъекции, мобильные трояны, несанкционированный удаленный доступ);
- выявлять отмывание денежных средств и финансирование терроризма (вывод средств через сеть связанных компаний или через "дропперов");
- выявлять кредитное мошенничество (подача множественных заявок, использование ворованных персональных данных);
- выявлять вредоносную бот-активность (перебор паролей, симуляция активности пользователя, автоматизированный сбор информации из открытых источников);
- оценивать конечных пользователей по приложениям, установленным на их устройствах;
- выявлять активность в браузерах в режиме “инкогнито”.

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 пользователя должно быть разрешено исполнение скриптов JavaScript.

2.1 Технические требования к составу оборудования при размещении в инфраструктуре Заказчика

В случае использования **облачной интеграции** требования к оборудованию отсутствуют.

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

Три сервера приложений:

- CPU: 4 core 2Mhz+;
- RAM: 32 Gb;
- HDD: 200Gb;
- ОС: Ubuntu, Ред ОС.

Три сервера для размещения Баз данных:

- CPU: 4 core 2Mhz+;
- RAM: 32 Gb;
- HDD: 1Tb;

– ОС: Ubuntu, Ред ОС.

Требования для разворачивания предоставленной тестовой среды:

Среда виртуализации:

- Система контейнеризации Docker;
- 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 **Рисунок 1** изображены общие принципы функционирования ПО.

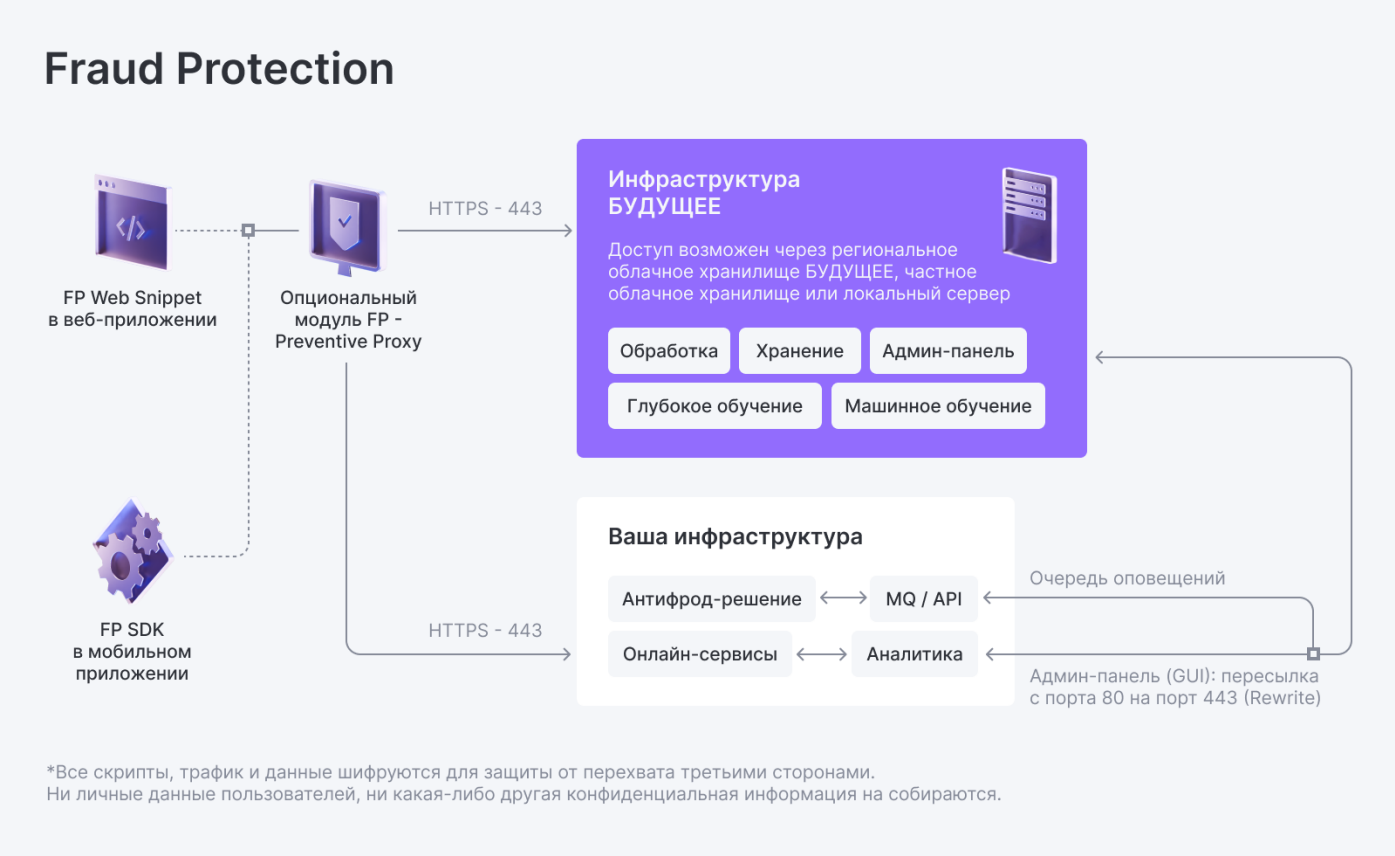

Рисунок 1. Общие принципы функционирования ПО.

ПО состоит из пользовательских модулей, реализованных на языках программирования Java/Swift и JavaScript.

WebSnippet (далее – скрипт) — клиентский модуль Fraud Protection для защиты веб-ресурсов, реализован на языке JavaScript. Модуль загружается совместно со страницами защищаемого веб-ресурса.

Mobile SDK (далее – SDK) — клиентский модуль Fraud Protection для защиты мобильных приложений, реализован на языке Java, для устройств на операционной системе Android, и Swift, для устройств на операционной системе IOS. Модуль запускается совместно с мобильным приложением.

ПО производит сбор контрольных данных со страницы защищаемого веб- или мобильного приложения и устройства клиента, и отсылает их для дальнейшего анализа в автоматизированную систему (далее – АС) АО «БУДУЩЕЕ» (далее – Разработчик). В случае выявления работы вредоносного ПО на устройстве пользователя или проведения иных мошеннических атак, АС Разработчика незамедлительно извещает об этом Заказчика.

ПО может быть представлена Заказчику двумя способами:

1. ПО как услуга (SaaS) – облачный интернет-сервис;
2. Размещение ПО в инфраструктуре Заказчика (On-premise).

Модули WebSnippet и SDK требуют встраивания в защищаемое приложение. ПО не требует инсталляции на устройстве пользователя и работает совершенно прозрачно для него.

Все данные передаются посредством протокола HTTPS с использованием порта 443.

4 РЕАЛИЗАЦИЯ ПО

4.1 Структура ПО

Структура ПО представлена на **Рисунок 2**.

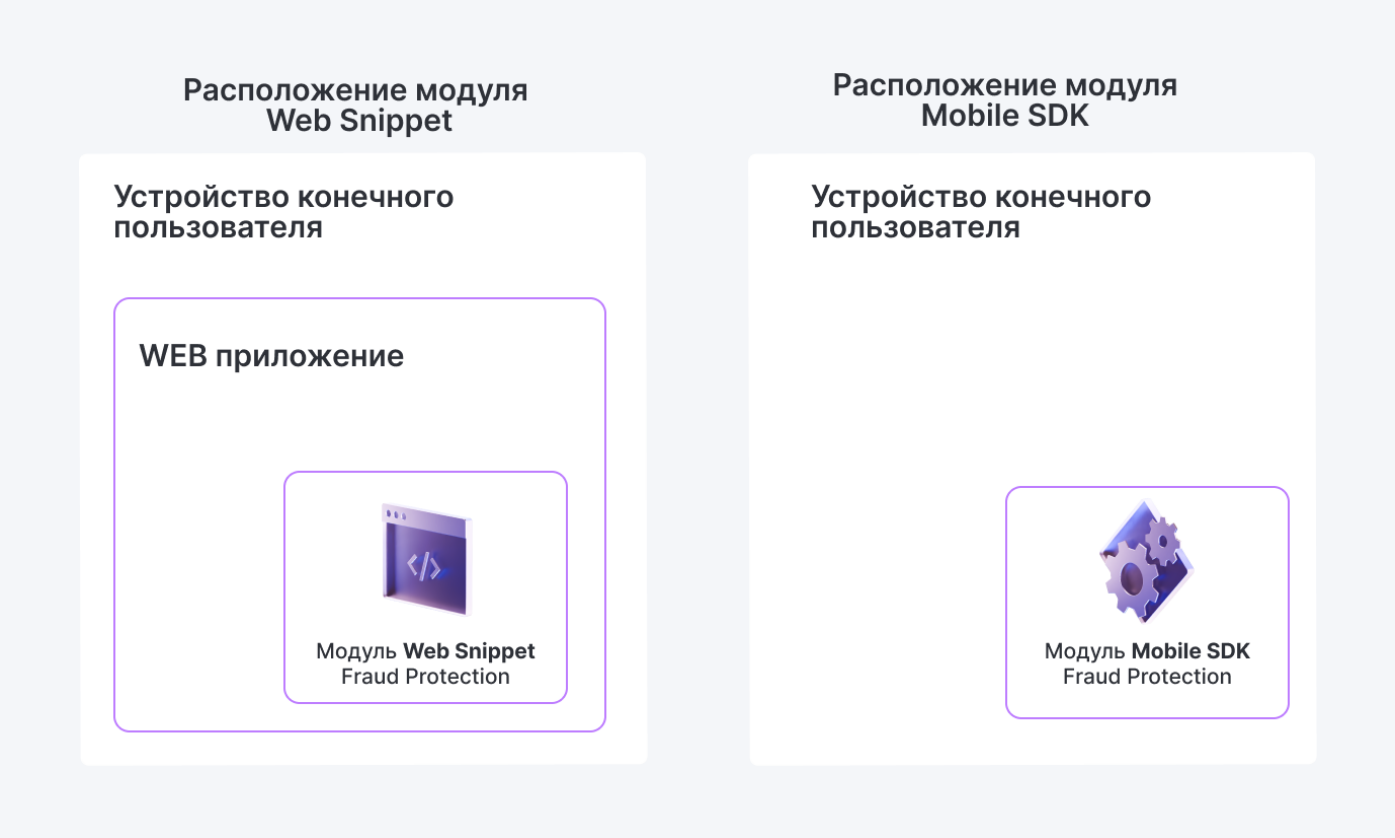

Рисунок 2. Структура ПО

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 на уровне, как минимум, но не ограничиваясь:

- браузера пользователя;
- мобильных приложений Заказчика;
- АС Заказчика;
- ПО.

ПО состоит в том числе из пользовательских модулей, реализованных на языке Java, Swift и JavaScript. Для веб-приложения модуль загружается на устройство пользователя совместно с защищаемым веб-ресурсом, для SDK при запуске мобильного приложения.

Пользовательские модули предназначены для сбора контрольных данных, непосредственно в контексте защищаемых приложений на устройстве пользователя, и их пересылки через сеть Интернет в АС Разработчика для последующей обработки и выявления признаков работы вредоносного программного обеспечения на устройстве пользователя. В случае развертывания АС в инфраструктуре Заказчика данные от пользовательских модулей пересылаются в АС Заказчика.

Модули ПО включают в себя:

- *Подсистему получения данных с устройства пользователя*. Подсистема предназначена для получения параметров работы пользователей в рамках их сессии в защищаемом приложении Заказчика, содержащих первичные данные о мошеннической активности на стороне пользователей, дополнительные идентификационные данные пользовательских устройств и другие параметры;
- *Подсистему обработки данных*. Подсистема предназначена для обработки данных, полученных от подсистемы получения данных с устройств пользователей защищаемого приложения Заказчика – проверки данных на валидность и целостность;
- *Подсистему управления*. Подсистема, предназначенная 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/импорта данных между АС Заказчика и ПО как в режиме реального времени, так и в диалоговом (запросном) режиме и передачи в АС Заказчика вердиктов и скоринга выявленных фактов мошеннической активности;
- *Подсистему защиты информации.* Подсистема представляет собой программно-технический комплекс, предназначенный для защиты технических средств, программного обеспечения и данных от несанкционированного доступа к данным АС. Выполняет функции по идентификации и аутентификации сторон, производящих обмен информацией, функции по разграничению прав доступа к информационным ресурсам АС.

4.3 Функции частей ПО

Система сбора контрольных данных о структуре защищаемого приложения осуществляет:

WebSnippet:

- Сбор данных о JavaScript-коде.
- Сбор данных об iframe.
- Сбор данных о формах.
- Сбор информации о том, как и почему вы или третьи лица используете файлы cookie.

Mobile SDK:

- Сбор признаков работы вредоносных приложений на мобильном устройстве пользователя (только в Android SDK).
- Сбор идентификационных данных мобильного устройства.
- Сбор признаков работы на эмуляторе мобильного устройства.
- Сбор данных о поведении пользователя.

Система сбора идентификационных данных пользователя в защищаемом приложении имеет следующие функции:

WebSnippet:

- Получение имени учетной записи пользователя на защищаемом веб-ресурсе из форм для ее ввода в целях идентификации пользователя на стороне АС Заказчика.

Mobile SDK:

- Модуль собирает параметры, для идентификации устройства пользователя. Параметры, которые однозначно идентифицируют мобильное устройство, передаются в серверную часть Fraud Protection в хэшированном виде, чтобы скрыть их исходные значения.

Система защиты обмена данными с АС имеет следующие функции:

- Шифрование идентификационных данных пользователя на публичном RSA-ключе Заказчика;
- Шифрование контрольных данных.

Система обмена данными с АС имеет следующие функции:

- Посылка зашифрованных контрольных данных в АС;

– Периодическая посылка сигнальных данных о работе пользовательского модуля в АС.

5 ВЗАИМОДЕЙСТВИЕ ПО С АВТОМАТИЗИРОВАННЫМИ СИСТЕМАМИ

5.1 Принципиальная схема взаимодействия ПО

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

5.2 Структура взаимодействия

Во взаимодействии участвуют следующие компоненты:

- Браузер или мобильное приложение на устройстве пользователя с загруженным пользовательским модулем в составе страницы защищаемого веб-ресурса или в составе мобильного приложения;
- АС Разработчика;
- АС Заказчика.

АС Разработчика состоит из следующих компонент:

- Серверная инфраструктура. Принимает, обрабатывает и анализирует контрольные данные, полученные от пользовательского модуля;
- Сервер управления. Служит для взаимодействия Заказчика с АС Разработчика;
- АРМ администратора. Обеспечивает настройку и сопровождение АС.

АС Заказчика состоит из следующих компонентов:

- Совокупность веб-серверов и серверов приложений веб-ресурса;
- Модуль автоматизации. Использует API к АС Разработчика для автоматизации реагирования на выявленные подозрительные события. Необходимость разработки этого модуля и правила реагирования определяются Заказчиком;
- АРМ оператора. Служит для ознакомления с подозрительными событиями и управления настройками выявления таких событий.

5.3 Порядок взаимодействия

1. Пользовательский модуль загружается на устройство клиента совместно с запуском мобильного приложения или загрузкой веб-ресурса;

2. Пользовательский модуль собирает контрольные данные со страницы веб-ресурса или мобильного приложения и посылает их для дальнейшего анализа в АС Разработчика;

3. Веб-серверы Заказчика отсылают заголовки запросов от пользователя в АС Разработчика для выявления случаев блокировки работы пользовательского модуля вредоносным программным обеспечением;

4. Серверная инфраструктура АС Разработчика анализирует полученные данные от пользовательского модуля и АС Заказчика на предмет наличия признаков вредоносных действий на устройстве пользователя;

5. При выявлении таких признаков АС Разработчика незамедлительно оповещает Заказчика по электронной форме;

6. Заказчик через сайт сервера управления АС Разработчика имеет возможность получить детальную информацию о выявленном подозрительном событии с идентификационной информацией о пользователе и его устройстве;

7. Заказчик через сайт сервера управления АС Разработчика имеет возможность дать обратную связь по выявленному событию, которая будет учтена в последующей обработке получаемых данных от пользовательского модуля;

8. Оповещение о событиях, их детальная информация и обратная связь по ним так же возможна с использованием API к АС Разработчика.

5.4 Данные, передаваемые пользовательскими модулями

Пользовательские модули передают следующие контрольные данные с устройства пользователя:

WebSnippet:

1. Данные о пользователе:
   - результат применения алгоритма SHA1 к имени учетной записи пользователя;
   - результат применения алгоритма RSA с публичным ключом Заказчика к имени учетной записи клиента;
   - характеристики движения курсором.
2. Данные о странице защищаемого веб-ресурса:
   - javascript-код, загружаемый на страницы веб-ресурса;
   - структуру и атрибуты веб-форм, размещенных на страницах веб-ресурса;
   - атрибуты следующих HTML-элементов: iframe, object, embed, applet.
3. Данные о браузере, через который производится доступ на веб-ресурс:
   - User-Agent, куда входят:
     - Браузер и его версия;
     - Операционная система и ее версия;
     - Разрядность операционной системы;
     - Название и модель устройства клиента.

- Accept-Encoding;
- Accept-Language;
- разрешение экрана;
- глубина цвета;
- доступность ActiveX;
- часовой пояс;
- шрифты браузера;
- плагины браузера;
- поддерживаемые языки;
- canvas-отпечаток.

Mobile SDK:

1. Данные о пользователе:
   - результат применения алгоритма SHA1 к имени учетной записи пользователя;
   - результат применения алгоритма RSA с публичным ключом Заказчика к имени учетной записи клиента;
   - характеристики нажатий и движения по экрану.
2. Данные об устройстве:
   - Название сотового оператора.
   - Серийный номер сим-карты.
   - Версия ПО.
   - Аппаратный идентификатор устройства.
   - Бренд мобильного устройства.
3. Данные сети, в которой находится устройство:
   - IP адрес устройства.
   - Идентификаторы точек доступа.
   - Сетевые сертификаты устройства.

По согласованию с Заказчиком, перечень собираемых данных может различаться в зависимости от конфигурации пользовательских модулей и особенностей защищаемых приложений.

6 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1 Обеспечение конфиденциальности пользовательских данных

В АС Разработчика не передается пользовательская информация кроме обезличенного имени учетной записи пользователя или иного обезличенного идентификатора. Имя учетной записи пользователя передается в виде:

- результата хеш-функции от имени учетной записи;
- и результата шифрования имени учетной записи с использованием публичного RSA-ключа Заказчика.

Обе операции производятся непосредственно на устройстве пользователя.

Получаемая Заказчиком информация о подозрительном событии содержит зашифрованное имя учетной записи. Используя соответствующий приватный RSA-ключ, только Заказчик может получить исходное имя пользователя.

Таким образом, имя пользователя недоступно третьим лицам, в том числе Разработчику.

6.2 Защита передаваемых данных

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

Передаваемые данные из пользовательского модуля в АС Разработчика дополнительно кодируются в целях защиты от вредоносного программного обеспечения, функционирующего на устройстве пользователя.

6.3 Безопасность периметра АС Заказчика

Обмен между АС Заказчика и АС Разработчика всегда инициируется только со стороны Заказчика на следующие домены:

- https://fp-api.facct.ru;
- https://fp-back.facct.ru;
- https://ru.id.facct.ru.

Для защиты периметра Заказчика может быть применен любой тип фильтрации, ограничивающий обмен между АС Заказчика и указанными сайтами АС Разработчика. Необходимо отметить, что любому из вышеуказанных доменных имен соответствует несколько IP-адресов, которые используются для обеспечения отказоустойчивости и распределения нагрузки.

6.4 Обеспечение доступности

Недоступность АС Разработчика никак не отражается на доступности и работоспособности защищаемого приложения как на стороне пользователя, так и на стороне Заказчика.

Тем не менее, АС Разработчика обеспечивает отказоустойчивость своей инфраструктуры.