F6

ПО «F6 Session Fraud Protection»

Описание функциональных характеристик

Оглавление

Термины и сокращения

АС	Автоматизированная система
Дроппер	Зарегистрированный в системе Заказчика Пользователь, передающий третьим лицам данные и реквизиты, необходимые для управления приложением или совершения операций, либо выполняющий указания третьих лиц за вознаграждение
Заказчик	Лицо, использующее программное обеспечение на основании заключённого 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 учёту
ПО	Программное обеспечение «F6 Session Fraud Protection»
Пользователь	Лицо, взаимодействующее с цифровыми каналами обслуживания Заказчика, в отношении которого применяется антифрод-защита
Разработчик	АО «БУДУЩЕЕ»
СУБД	Система управления базами данных
Файлы cookie	Небольшие текстовые данные, сохраняемые браузером на устройстве при взаимодействии с веб-ресурсом и используемые для хранения служебной информации о сессии, устройстве и параметрах взаимодействия
API	(«Application Programming Interface») Программный интерфейс, который позволяет разным системам обмениваться данными и взаимодействовать друг с другом по заранее определенным правилам
IP-адрес	(«Internet Protocol Address») Уникальный числовой идентификатор устройства в компьютерной сети, используемый для обмена данными в интернете или локальной сети
RSA	Криптографический алгоритм асимметричного шифрования, использующий пару ключей (публичный и приватный) для защиты данных и обеспечения безопасного обмена информацией

Mobile SDK	Модуль программного обеспечения «F6 Session Fraud Protection» для встраивания в мобильные приложения
On-premises	Модель развёртывания программного обеспечения, при которой система устанавливается и эксплуатируется в собственной инфраструктуре Заказчика, без использования внешних облачных сервисов
SaaS	(«Software as a Service») Модель предоставления программного обеспечения, при которой система размещается и эксплуатируется в облачной инфраструктуре поставщика, а доступ к ней осуществляется через сеть без установки в инфраструктуре Заказчика
SIM-карта	(«Subscriber Identity Module») Электронный идентификационный модуль для мобильной связи, содержащий уникальный номер абонента и обеспечивающий доступ к услугам оператора сотовой связи
SHA1	Криптографический алгоритм хеширования, преобразующий исходные данные (например, имя учётной записи) в фиксированную последовательность символов, не позволяющую восстановить первоначальное значение напрямую
Web Snippet	Модуль программного обеспечения «F6 Session Fraud Protection» для встраивания в веб-приложения

#1 Общие сведения

1.1. Введение

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

1.2. Назначение ПО

«F6 Session 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 Session Fraud Protection» позволяют:

1. Выявлять хищения с использованием социальной инженерии, включая подложные сайты, мошеннические рассылки и звонки, а также активность в социальных сетях;
2. Выявлять мошеннические действия с учётной записью пользователя: несанкционированный доступ, множественные регистрации, выполнение несанкционированных действий от имени пользователя;
3. Выявлять финансовые мошеннические операции, такие как хищения в системах дистанционного банковского обслуживания, карточное мошенничество и подмена платёжных реквизитов;
4. Выявлять мошеннические операции с использованием вредоносного программного обеспечения, включая веб-инъекции, мобильные трояны и несанкционированный удалённый доступ;
5. Выявлять отмывание денежных средств и финансирования терроризма, включая вывод средств через сеть связанных компаний либо с использованием так называемых «дропперов» (подставных получателей);
6. Выявлять кредитное мошенничество, включая подачу множественных заявок и использование похищенных персональных данных;
7. Выявлять вредоносную бот-активность, включая перебор учётных данных, имитацию действий пользователя и автоматизированный сбор информации из открытых источников;
8. Оценивать конечных пользователей на основе сведений о приложениях, установленных на используемых ими устройствах;
9. Выявлять факты использования браузеров в режиме «инкогнито» при выполнении операций.

#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

В случае использования облачной интеграции требования к оборудованию отсутствуют.

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 к развёртыванию 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 рисунке 1 изображены общие принципы функционирования ПО.

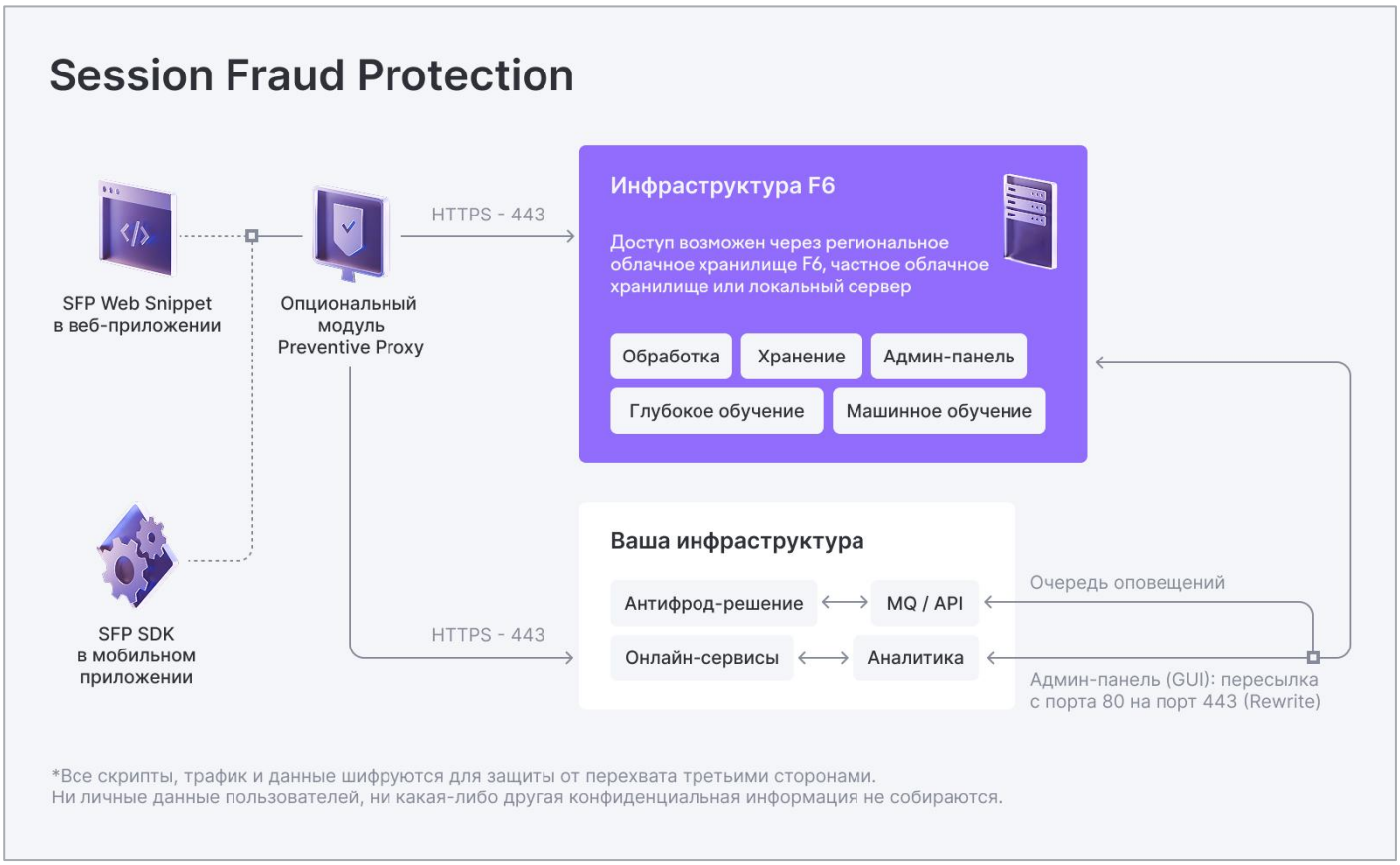

Рисунок 1. Общие принципы функционирования ПО "F6 Session Fraud Protection"

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

Web Snippet (далее — скрипт) — пользовательский модуль Session Fraud Protection для защиты веб-ресурсов, реализованный на языке JavaScript. Модуль загружается совместно со страницами защищаемого веб-ресурса.

Mobile SDK (далее — SDK) — пользовательский модуль Session Fraud Protection для защиты мобильных приложений, реализованный на языке Java (для устройств на операционной системе Android) и Swift (для устройств на операционной системе iOS). Модуль запускается совместно с мобильным приложением.

ПО осуществляет сбор контрольных данных со страниц защищаемых веб-ресурсов или мобильных приложений, а также с устройства Пользователя, и направляет их для дальнейшего анализа в автоматизированную систему (далее — АС) АО «БУДУЩЕЕ» (далее — Разработчик).

При выявлении признаков работы вредоносного ПО на устройстве Пользователя либо иных мошеннических атак АС Разработчика незамедлительно уведомляет Заказчика.

ПО может быть представлено Заказчику двумя способами:

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

Модули Web Snippet и SDK требуют встраивания в защищаемое приложение. ПО не требует установки на устройстве пользователя и функционирует без его участия.

Все данные передаются посредством протокола HTTPS с использованием порта 443.

#4 Реализация ПО

4.1. Структура ПО

Структура ПО представлена на рисунке 2.

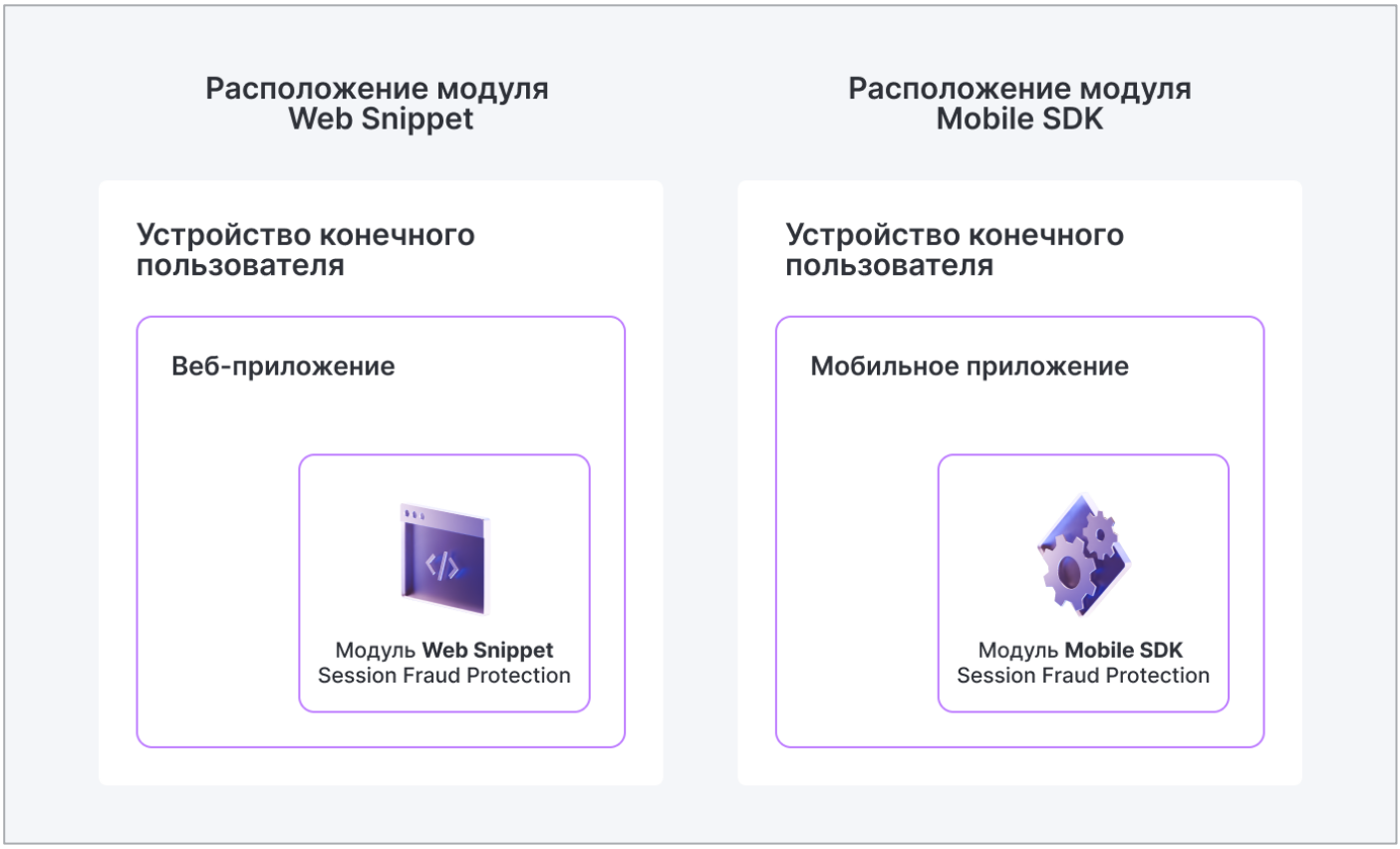

Рисунок 2. Структура ПО

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 включает пользовательские модули, реализованные на языках Java, Swift и JavaScript.

Для веб-приложений модуль загружается на устройство пользователя совместно со страницами защищаемого веб-ресурса (Web Snippet), а для мобильных приложений — запускается вместе с приложением (SDK).

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 развёртывания АС в инфраструктуре Заказчика данные от пользовательских модулей пересылаются в АС Заказчика.

Пользовательские модули ПО включают в себя:

- Подсистему получения данных с устройства Пользователя

  Подсистема предназначена для получения параметров работы пользователей в рамках сессии в защищаемом приложении Заказчика. Она собирает 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 предназначена для выполнения настроек и администрирования ПО;

- Подсистему аналитики

  Подсистема предназначена для работы аналитиков АС с выявленными событиями мошеннической активности, получения отчётов 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

Система сбора контрольных данных о структуре защищаемого приложения осуществляет:

- В модуле Web Snippet:
  - Сбор данных о JavaScript-коде;
  - Сбор данных об iframe;
  - Сбор данных о формах;
  - Сбор информации об использовании файлов cookie.
- В модуле Mobile SDK:
  - Сбор признаков работы вредоносных приложений на мобильном устройстве Пользователя (только в Android SDK);
  - Сбор идентификационных данных мобильного устройства Пользователя;
  - Сбор признаков работы на эмуляторе мобильного устройства Пользователя;
  - Сбор данных о поведении Пользователя.

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

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

- В модуле Mobile SDK:
    - Сбор параметров для идентификации устройства пользователя. Параметры, позволяющие однозначно идентифицировать мобильное устройство, передаются в серверную часть Session Fraud Protection в хешированном виде для сокрытия их исходных значений.

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:

- Отправка зашифрованных контрольных данных в АС;
- Периодическая отправка 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 рисунке 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 мобильного приложения;
- АС Разработчика;
- АС Заказчика.

АС Разработчика состоит из следующих компонентов:

- Серверная инфраструктура, которая принимает, обрабатывает и анализирует контрольные данные, полученные от пользовательского модуля;
- 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. Пользовательский модуль загружается на устройство Пользователя совместно с запуском мобильного приложения или загрузкой веб-ресурса;
2. Пользовательский модуль собирает контрольные данные со страницы веб-ресурса или мобильного приложения и отправляет 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 веб-интерфейс сервера управления АС Разработчика имеет возможность получать детальную информацию о выявленном подозрительном событии, включая идентификационные сведения о пользователе и его устройстве;
7. Заказчик через веб-интерфейс сервера управления АС Разработчика имеет возможность предоставлять обратную связь по выявленному событию, которая учитывается при последующей обработке данных, поступающих от пользовательского модуля;
8. Оповещение о событиях, получение их детальной информации и передача обратной связи также возможны с использованием API АС Разработчика.

5.4. Данные, передаваемые пользовательскими модулями

Пользовательские модули передают контрольные данные с устройства пользователя.

Модуль Web Snippet:

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 Пользователя;
    - Характеристики движения курсором.
2. Данные о странице защищаемого веб-ресурса:
    - JavaScript-код, загружаемый на страницы веб-ресурса;
    - Структуру и атрибуты веб-форм, размещённых 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 её версия;
        - Разрядность операционной системы;
        - Название и модель устройства Пользователя.
    - Accept-Encoding;
    - Accept-Language;
    - Разрешение экрана;
    - Глубина цвета;
    - Доступность ActiveX;
    - Часовой пояс;
    - Шрифты браузера;
    - Плагины браузера;
    - Поддерживаемые языки;
    - Canvas-отпечаток.

Модуль Mobile SDK:

1. Данные о пользователе:
    - Результат применения алгоритма SHA1 к имени учётной записи Пользователя;
    - Результат применения алгоритма RSA с публичным ключом Заказчика к имени учётной записи Пользователя;
    - Характеристики нажатий и движения по экрану.
2. Данные об устройстве:
    - Название сотового оператора;
    - 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 передаётся пользовательская информация, кроме обезличенного имени учетной записи Пользователя или иного обезличенного идентификатора. Имя учётной записи Пользователя передаётся в виде:

- Результата хеш-функции от имени учётной записи;
- Результата шифрования имени учётной 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 информацией 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.fp.f6.security;
- https://fp-back.fp.f6.security;
- https://ru.id.fp.f6.security.

Для защиты периметра Заказчика может быть применён любой тип фильтрации, ограничивающий обмен между АС Заказчика и указанными сайтами АС Разработчика. Любому из вышеуказанных доменных имён 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.