**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**для проекта**

**«Приобретение комплексного решения для предотвращения онлайн-мошенничества и бот активности в каналах дистанционного обслуживания»**

**г. Ташкент - 2025 г.**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**«Приобретение комплексного решения для предотвращения онлайн-мошенничества и бот активности в каналах дистанционного обслуживания»**

1. **ОБЩИЕ СВЕДЕНИЯ**

## **1.1 Наименование.**

Техническое задание на приобретение комплексного решения для предотвращения онлайн-мошенничества и бот активности в каналах дистанционного обслуживания.

## **1.2 Термины и сокращения**

| **Термин** | **Понятие** |
| --- | --- |
| Организации (Клиент) | Банки и платёжные организации |
| ДБО ФЛ | Система дистанционного банковского обслуживания физических лиц (интернет-банкинг, мобильный банк) Организации |
| ДБО ЮЛ | Система дистанционного банковского обслуживания юридических лиц (интернет- банкинг, мобильный банк) Организации |
| P2P | Страница Организации для перевода денежных средств с карты на карту. |
| 3-D Secure | Страницы, банка-эмитента, для подтверждения операции при оплате товара в сети Интернет |
| ССА | Система сессионного антифрода |
| ПО | Программное обеспечение |
| Обфускация | Приведение исходного текста или исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции |
| Оператор | Пользователь ССА, выполняющий анализ и настройку правил ССА. |
| Пользователь | Пользователь системы ДБО ФЛ или ЮЛ, который авторизовывался в систему не менее 1 раза в течение 12 месяцев. |
| Прокси-сервер | Сервер (комплекс программ) в компьютерных сетях, позволяющий пользователям выполнять косвенные запросы к другим сетевым службам. |
| Правило | Набор из одного или нескольких критериев, объединённых логическими операциями для осуществления сравнения данных о текущем поведении пользователей Заказчика и его устройстве с ранее накопленными данными на наличие признаков несовпадения для выявления аномалий. |
| Веб-сенсор | Часть ССА, поставляемая в виде JavaScript-кода и устанавливаемая на веб-страницу цифрового канала обслуживания (Интернет-банкинг, P2P, 3-D Secure) для сбора информации, необходимой для выявления признаков мошенничества, либо автоматизированной активности. |
| Мобильный-сенсор | Часть ССА, поставляемая в виде SDK для ОС iOS/Android и устанавливаемая в мобильное приложение Организации для сбора информации, необходимой для выявления признаков мошенничества и подготовки аутентификации на основе рисков. |
| УЗ | Учетная запись. |
| API | Application Programming Interface – набор готовых классов, процедур, функций, структур и констант, предоставляемых программным продуктом для использования во внешних программных продуктах. |
| Фишинг | Вид интернет-мошенничества, направленный на завладения идентификационных данных пользователей путем использования поддельных страниц. |
| Вишиниг | Вид интернет-мошенничества, направленный на завладения идентификационных данных пользователей, либо данных необходимых для совершения несанкционированных финансовых операций, путем использования телефонной коммуникации. |
| Cookie | Сессионный токен — небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя. |
| Proxy | Промежуточный сервер в компьютерной сети между пользователем интернета и целевыми серверами. |
| TOR | Система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде. |
| Web-инъекции | Изменение (внедрение) содержимого веб-страницы на стороне клиента (в браузере) |

## **2. ОБЛАСТЬ ПРИМЕНЕНИЯ.**

ССА должна производить сбор и анализ сессионных и поведенческих данных в цифровых ресурсах Организации (ДБО ФЛ, ДБО ЮЛ, P2P, 3-D Secure) в целях выявления признаков осуществления мошеннической деятельности, направленной на пользователей Организации, автоматизированной активности, попыток легализации (отмывания) доходов, полученных преступным путем, осуществления незаконной предпринимательской деятельности, иных противоправных действий, в частности, связанных с обеспечением расчетов «теневого» игорного бизнеса (незаконных «онлайн-казино» и «онлайн-лотерей»), нелегальных участников финансового рынка (в том числе, лиц, незаконно предлагающих услуги форекс-дилеров, организаторов «финансовых пирамид»), а также в целях совершения операций в «криптовалютных обменниках».

В рамках использования ССА необходимо предоставлять сотрудникам Организации и сторонним системам Организации доступ к данным (в т.ч. посредством API) с информацией о сессиях пользователей, их устройствах и результатах срабатывания правил системы для возможности проведения дополнительного анализа.

ПО должно соответствовать заявленным производителем целям использования и функциональным возможностям, указанным в Спецификации. В ПО должно отсутствовать вредоносное программное обеспечение. Использование Организациям данного ПО не должно привести, в частности, к несанкционированному уничтожению, блокированию, модификации, копированию компьютерной информации Организации или нейтрализации средств защиты компьютерной информации Организации, а также к иному ущербу Организации.

## **3. ТРЕБОВАНИЯ К КЛИЕНТСКОЙ ЧАСТИ ССА.**

## **3.1 В веб сервисах**

Должны осуществляться:

* идентификация устройства пользователя на базе его параметров (device fingerprinting);
* глобальная идентификация устройства пользователя на кросс-клиентском уровне;
* выявление фактов несанкционированного использования учетных данных клиентов;
* выявление фактов инъекции стороннего кода в защищаемое веб-приложение;
* выявление мошеннических внедрений в веб-часть на стороне сервера (веб-инъекции);
  + решение должно обеспечивать выявление инъекций в клиентскую часть (html, js, и т.п.) веб-приложения заказчика на стороне конечного пользователя;
  + решение должно обеспечивать ручную и автоматизированную классификацию таких инъекций веб-приложения заказчика;
  + решение должно обеспечивать классификацию динамически меняющихся инъекций;
  + в результате выявления вредоносной инъекции на стороне конечного пользователя ССА должно генерировать событие.
* выявление фишинга;
  + решение должно собирать информацию о переходах на веб-приложение Организации;
  + решение должно выявлять копирование легитимного веб-приложения Организации и его использование для вредоносных целей;
  + собранные ссылки должны классифицироваться в автоматизированном режиме, в том числе с использованием алгоритмов машинного обучения, включая, но не ограничиваясь: проверку изображений на схожесть с логотипом, favicon, текстовое содержание страницы, SSL-сертификаты.
* определение работы клиента через TOR, proxy и «анонимайзеры»;
* выявление доступа со скомпрометированных выделенных серверов или устройств компаний, предоставляющих услуги хостинга и колокации;
* мониторинг используемых браузеров в каждом клиенте для формирования рисков;
* выявление использования антидетект браузера;
  + Должны выявляться антидетект-браузеры Dolphin, Incognition, CheBrowser, AdsPower и другие;
* выявление работы мошенника и легитимного пользователя на базе поведенческих данных: навигации, движения курсора, скорости и последовательности нажатия клавиш, паузы, взаимодействия с формами на веб ресурсе Организации;
* выявление и блокировка автоматизированных попыток взлома учетных записей (“brute force”) или использования скомпрометированных учетных записей со сторонних ресурсов (“credential stuffing”);
* предоставление дополнительных вердиктов в сторонние системы Организации, например, система транзакционного антифрода;
* отправка информации о действиях пользователя в приложении Организации при его использовании;
* получение информации из следующих типов браузеров, а также блокировка подключения при использовании пользователем версий ниже следующих:
* Chromium 26 и выше (включая Google Chrome, Yandex Browser, Opera)
* Internet Explorer 9 и выше
* Microsoft Edge 13 и выше
* Mozilla Firefox 4 и выше
* Safari 8 и выше

В браузере устройства пользователя должно быть включено исполнение скриптов JavaScript.

* выявление вредоносной активности пользователя и ПО на основе иных правил (мультиаккаунтинг, использование мошеннических подсетей и др), выбранных со стороны Организации;
  + выявленные
* работать как на многостраничных Интернет-ресурсах Организации, так и реализованных по технологии Single Page Application;
* не собирать и не предоставлять конфиденциальную информацию, в том числе персональные данные и сведения составляющие банковскую тайну (данные такого типа предоставляются только ССА).

## **3.2 В мобильных приложениях**

Должны осуществляться и передаваться CCA:

* идентификация мобильного устройства;
* глобальная идентификация устройства пользователя на кросс-клиентском уровне;
* выявление подделки мобильного приложения Организации (проверка подписи, контроль целостности);
* предоставление информация в ССА сведений о версии ОС и наличия root прав, выявление запуска приложения на эмуляторе мобильного устройства;
* выявление удаленных подключений к клиентскому устройству (выявление использования средств удаленного управления);
  + по появлению и наличию ПО для удаленного доступа и управления;
  + по наличию активных сессий удаленного управления;
  + выявление удаленного управления по поведенческим признакам.
* идентификация смены сим-карты клиентом и передача информации в ССА;
* при использовании приложения Организации должны собираться и передаваться в ССА сведения (характеристики) о касаниях и свайпах пользователя, взаимодействии с элементами пользовательского интерфейса приложения, скорости набора текста, данных сенсоров мобильного устройства;
* предоставление информации в ССА GPS данных и сведений о используемых каналах передачи данных (Wi-Fi, мобильная сеть, проводной интернет);
  + должны собираться долгота, широта, высота, направление, скорость нахождения/движения с GPS-датчика мобильного устройства;
  + должна собираться идентификационная информация вышки сотовой связи, к которой в текущей момент подключено мобильной устройство;
  + должны собираться идентификаторы точек доступа Wi-Fi к которой подключено устройство и других доступных для мобильного устройства
* предоставление информации об обнаружения дебаггера на устройстве пользователя в ССА;
  + выявление режима разработчика на мобильной устройстве
  + выявление активной сессии отладки мобильного приложения
* не оказывать существенного замедления работы приложений Заказчика на устройствах пользователя;
* сбор необходимой информации и предоставление в ССА не должен вызывать появление каких-либо диалогов или запросов подтверждений, требующих реакции со стороны пользователя, а также появление каких-либо уведомлений для пользователя;
* не оказывать существенного прироста сетевой активности между устройством пользователя и ССА Организации или её инфраструктурой;
* функционировать как в нативных мобильных приложениях, так и в гибридных   
  (с использованием WebView компонентов);
* отправлять информацию о действиях пользователя ~~только~~ в приложении Организации при его использовании;
* использовать стандартную функциональность браузеров и мобильных ОС Android и iOS;
* функционировать и уметь получать информацию ОС:
* Android v.5 (API 14) и выше;
* iOS v.10 и выше.
* не собирать и не предоставлять конфиденциальную информацию, в том числе персональные данные и сведения составляющие банковскую тайну (данные такого типа предоставляются только ССА.

# **4. ОБЩИЕ ТРЕБОВАНИЯ К ССА**

**4.1** **Перечень компонентов ССА**

**ССА должна включать следующие компоненты**

* подсистема сбора данных с устройства пользователя (веб- и мобильные сенсоры);
* подсистема выявления и блокировки бот-активности;
* подсистема обработки данных и управления правилами корреляции;
* подсистема аналитики данных;
* подсистема отчетности и визуализации;
* подсистема информационного обмена;
* подсистема информационного обмена c Централизованным антифродом РУЗ.

**4.2 Требования к подсистеме получения данных с устройства пользователя.**

Подсистема должна:

* не нарушать работоспособность систем Заказчика;
* учитывать возможные виды активного противодействия мошенника на работоспособность подсистемы:
  + иметь защиту от статического анализа;
  + клиентская часть ССА для веб-сервисов должна обеспечивать динамическую обфускацию кода;
  + обеспечивать защиту передаваемых данных из клиентского модуля ССА от ознакомления мошенником;
  + обеспечивает контроль целостности передаваемых данных из клиентского модуля ССА;
  + выявлять средства отладки и подмены runtime.
* выявлять индикаторы компрометации устройства пользователя Организации:
  + для веб-приложений ССА должно обеспечивать:
    - выявление инъекций в клиентскую часть (html, js, и т.п.) веб-приложения заказчика на стороне конечного пользователя;
    - ручную и автоматизированную классификацию таких инъекций веб-приложения заказчика;
    - классификацию динамически меняющихся инъекций;
    - выявление обращения к подозрительным или мошенническим ресурсам сети Интернет;
    - выявление несанкционированных обращений к заданным полям форм и другим элементам страницы.
  + для мобильных приложений заказчика:
    - обеспечивать сигнатурный анализ вредоносного программного обеспечения, установленного на конечном устройстве пользователя;
    - обеспечивать поведенческий анализ наличия и работы вредоносного программного обеспечения на конечном устройстве пользователя, включая, но не ограничиваясь:
      * предоставление административных прав приложению
      * источник установки
      * осуществление overlay активности
      * автоматические действия вредоносного программного обеспечения в мобильной ОС и сторонних приложениях
      * наличие опасных или типичных сочетаний прав (permissions) для вредоносного программного обеспечения
      * подмены системных настроек
* определять работу клиента через TOR, proxy и «анонимайзеры»;
  + использовать результаты профилирования всего адресного пространства IPv4 на наличие открытых портов сетевых сервисов для предоставления услуг proxy и VPN;
  + использовать результаты профилирования доменных имен и IP-адресов для выявления «анонимайзеров»;
  + выявлять несоответствие геопозиции, полученной с устройства и через IP-адрес;
* выявлять доступ со скомпрометированных выделенных серверов или устройств компаний~~,~~ предоставляющих услуги хостинга и колокации;
  + использовать сторонние источники профилирования сетевых устройств в сети Интернет;
  + использовать события выявления автоматизированной активности для разметки.
* идентифицировать разные мобильные устройства одного пользователя в рамках приложения при смене устройств и сим-карт;
  + выявлять случаи, когда легитимный пользователь меняет свое мобильное устройство на новую модель
  + выявлять случаи, когда пользователь меняет (e)SIM-карту на своем мобильной устройстве.
* выявлять работу мошенника и легитимного пользователя на базе поведенческих данных: характеристик касаний и свайпов пользователя, взаимодействия с элементами пользовательского интерфейса приложения, скорости набора текста, данных сенсоров мобильного устройства:
  + профилирование динамики нажатий клавиш пользователя и выявление аномалий;
  + профилирование динамики движения курсора пользователя и выявление аномалий;
  + профилирование поведенческих характеристик взаимодействия пользователя с экраном мобильного устройства с учетом сенсоров, и выявление аномалий;
  + профилирование типовых действий пользователя в интерфейсе веб и мобильного приложений и их поведенческих характеристик, и выявления аномалий;
  + выявление схожести действий пользователя с профилем мошенника.
* выявлять мошенничество с использованием данных GPS и сведений о типах каналах связи:
  + профилировать геопозиции с учетом высокорисковых событий на площадках ССА;
  + выявлять подмену геопозиции на устройстве конечного пользователя.
* блокировать вредоносную активность пользователя и ПО на основе иных правил (мультиаккаунтинг, использование мошеннических подсетей и др), выбранных со стороны Организации:
  + при выявлении высокорисковой активности на стороне пользователя ССА должна предоставлять механизмы блокировки/прерывания такой активности
* выявлять сессии клиентов с включенным дебаггером и учитывать при анализе действий клиента;
* защищать мобильное API от использования ботами или сторонними мобильными приложениями:
  + выявлять прямые обращения к API серверной части мобильного приложения;
  + выявлять обращения к API серверной части мобильного приложения из подложного или стороннего мобильного приложения;
  + защищать от хищения сессионного файла cookie для последующего обхода фазы авторизации пользователя на стороне мошенника.
* предоставлять дополнительные вердикты в сторонние системы Организации, например, в систему транзакционного антифрода;
* блокировать вредоносную активность на основе иных правил (мультиаккаунтинг, количество и характеристики устройств, мошеннических подсетей и др), выбранных или настроенных Организацией;
  + ССА должно обеспечивать блокировку/прерывание сессии или действия клиента в ДБО Организации, включая, но не ограничиваясь: вход в личный кабинет, совершение транзакции, изменение профиля.
* уметь принимать решения о легитимности на основании сведений о мобильной ОС и браузерах;
  + ССА должно выявлять антидетект-браузеры;
  + выявлять root-ованные/jailbreak мобильные устройства;
  + выявлять headless-браузеры, которые используются для автоматизации действий мошенника.
* использовать HTTPS-соединение (TLS и SSL) для передачи данных модулей ССА;
  + должна быть предоставлена возможность SSL pinning на стороне мобильного приложения.
* принимать данные о действиях пользователя в приложении Организации, при его использовании, и передавать их в подсистему обработки данных;
* собранные данные передавать в обфусцированном виде с контролем их целостности;
* поддерживать передачу собранных данных через каналы передачи данных между пользователем и Организацией;
* поддерживать динамическую обфускацию кода веб-сенсора с изменением параметров обфускации передаваемых данных с возможностью указания частоты обфускации;
* иметь монолитную поставку (архитектуру) веб-сенсора без модульности для целей обеспечения автономности, целостности и безопасности;

## **4.3 Требования к подсистеме обработки данных.**

Подсистема должна:

* выполнять прием и проверку данных на целостность от подсистемы сбора данных;
  + должна быть проверка целостности переданных данных из клиентского модуля ССА, что данные не были подменены мошенником на пути их следования до серверной части ССА
* выполнять составление профиля пользователя и его устройств на основании информации получаемых из подсистем сбора данных;
* выполнять кросс-канальную корреляцию данных по сессиям работы каждого пользователя Организации;
* выполнять корреляцию данных по сессиям работы одного устройства и пользователя в сервисах разных Организаций;
  + ССА должна обеспечивать единую и уникальную идентификацию устройства конечного пользователя для Организаций как в веб, так и мобильных каналах. Device fingerprinting не является таким идентификатором, так как такая идентификация не является уникальной для конкретного устройства;
  + Единый идентификатор устройства должен использоваться ССА для обмена и учета вердиктов других Организаций ССА;
  + ССА должна предоставлять механизм обмена и корреляции данных между Организациями для совместной классификации устройств, включая, но не ограничиваясь следующими данными: единый уникальный идентификатор устройства, IP-адреса и их классификация, сигнатуры вредоносного программного обеспечения, высокорисковые геолокации;
  + Обмен и корреляция должна предоставляться как для ССА установленной в периметре Организации, так и в «облачном» исполнении ССА;
  + Обмен сессионными данными должен быть реализован внутри Республики Узбекистан.
* поддерживать анализ действий каждого пользователей с использованием правил корреляции (в т.ч. используя машинное обучение);
* осуществлять быстрый поиск по идентификатору клиента Организации, отпечатки устройства, IP-адресу, идентификатору сессии и другим параметрам от системы сбора ССА;
* давать возможность (самостоятельно сотрудникам Организации) настраивать правила выявления и блокировки мошеннической активности и уровня риска для каждой сессии, в том числе:
* возможность активации/деактивации правил;
* возможность гибкого редактирования правил путем добавления определённых событий для сработки с условием «ИЛИ», «И» и «НЕ»;
* возможность самостоятельно гибко подстраивать каждое событие в правиле добавляя или удаляя;
* возможность изменения уровня сработки данного события с использованием различных условий, а именно – «>», «<» или «=», «содержит» и «не содержит»;
* предоставлять возможность создания тестовых событий в режиме онлайн на продуктивных данных для целей проверки новых гипотез выявления мошеннической активности;
* предоставлять возможность тестирования правил на исторических данных для оценки эффективности и проверки новых гипотез выявления мошеннической активности;
* иметь возможность настройки и использования совокупности событий в правилах корреляции для генерации инцидентов (групп событий);
* поддерживать возможность создания и использования в правилах специализированных списков по пользователям, IP адресам, идентификаторов устройств (Пример: списки для блокировки, для исключений, для сомнительных устройств и др.);
* обогащаться индикаторами из сторонних источников данных.

## **4.4 Требования к подсистеме анализа и обработки данных**

Подсистема должна:

* обеспечивать корреляцию данных с другими сессиями работы данного и других пользователей Организации;
* проводить идентификацию и корреляцию данных на кросс-канальном уровне и уровне других Заказчиков ССА;
* обогащать знания о мошеннической активности данного и других клиентов Организации с использованием знаний от других Заказчиков системы (при их согласии);
* обеспечивать возможность анализа графовых связей между клиентами, устройствами, геолокациями и другими сессионными данными клиентов Организации, а также данными других Заказчиков;
  + ССА должна обеспечивать обмен информацией о вердиктах и разметках по сессионным данным между Организациями
* реализовывать просмотр выявленных одиночных событий и сгруппированных по сессиям работы браузера на устройстве пользователя;
* глобальное выявление мошенничества на кросс-клиентском уровне;
* выявление входящего/исходящего активного звонка по сотовой сети во время сессии клиента в ДБО;
* выявление входящего/исходящего активного звонка c использованием сервисов обмена мгновенными сообщениями во время сессии клиента в ДБО;
* система должна имеет возможность интеграции с другими внешними антифрод системами от сторонних производителей;
* выявление фактов несанкционированного использования учетных данных клиентов (вход с нового устройства в ДБО, вход с мошеннического устройства в ДБО);
* реализовывать просмотр деталей по каждому выявленному событию, которые должны включать:
* время события;
* уровень критичности;
* тип выявленного события;
* детализация события в зависимости от типа
* реализовывать отдельный инструмент для просмотра профиля клиента с группировкой связей по основным сущностям (устройства, сессии, геолокации)
* реализовывать просмотр и категорирование инъекций, внесенных на страницы Заказчика;
* реализовывать просмотр и категорирование доменов (например, зловредный, сомнительный и легитимный), обращение к которым были зафиксированы в ходе сессий пользователи на ресурсах Организации;
* реализовывать вывод статистики по активности пользователей, количеству выявленных событий среди них;
* обеспечить возможность управления учетными записями, формирования новых ролей и разграничения прав по ролям и учетным записями системы владельцем ССА;
* обеспечивать возможность аналитики данных в выделенном интерфейсе.

## **4.5 Требования к надежности.**

Должны выполняться следующие требования:



* возможность функционировать в соответствии с отказоустойчивой схемой в рамках нескольких площадок (не менее двух) и иметь схему функционирования в катастрофоустойчивой конфигурации;
  + ССА должна обеспечивать disaster recovery (DR) план по переключению обработки сессионной информации на запасную площадку;
  + запасная площадка должна обновляться при изменении настроек на основной;
  + создаваемые профили устройств и пользователей должны обновляться на запасной площадке в автоматической режиме для корректной ее работы в случае недоступности основной площадки.
* поддерживать масштабирование существующей инсталляции без переустановки и существенного изменения архитектуры в случае необходимости увеличения производительности;
* пиковая нагрузка не должна приводить к деградации производительности программного интерфейса обмена сообщениями, используемого для доступа к вердиктам аутентификации на основе рисков;
* иметь собственные (не наложенные) механизмы резервирования и восстановления слоя данных;
* обеспечивать резервирование основных компонентов;
* соответствовать требованиям контроля отказоустойчивости:
* обеспечивать мониторинг и контроль состояния ее основных компонентов;
* обеспечивать механизмы контроля доступного места на диске, потребления ресурсов процессора и памяти, количества обрабатываемых сессий пользователей;
* уведомлять о критических значениях событиях и сбоях в работе по протоколам smtp.
* соответствовать следующим показателям надежности:
* штатный режим работы ССА – 7 дней в неделю 24 часа в сутки;
* общее допустимое времени простоя в неделю не должно превышать 1 час
* время восстановления после сбоя должно быть не более 3 часов.
* доступность серверной части frontend-, backend- и db-серверов должна составлять не менее 99,95% в год
* доступность web- консоли должна составлять не менее 99,90% в год
* обеспечивать целостность и корректность данных при разрыве соединения во время взаимодействия с системами Заказчика.

## **4.6** **Требования к Web-интерфейсу ССА.**

Должны выполняться следующие требования:

* Web-интерфейс ССА не должен требовать установки дополнительного программного обеспечения на устройство оператора (Java, ActiveX, дополнительные модули браузера).
* в Web-интерфейсе должно существовать разграничение прав доступа и дополнительное к парольной политике ограничение доступа с помощью одного из методов:
* ограничение доступа по диапазону IP-адресов;
* системы двухфакторной аутентификации.
* Web-интерфейс ССА должен предоставлять доступ к:
* статистике ССА (сводные данные за период по пользовательской активности, типам и статусам инцидентов);
* данным по полученным инцидентам;
* детализации по инцидентам;
* Web-интерфейс пользователя ССА должен предоставлять доступ к службе отчетов, которая позволяет генерировать отчеты по инцидентам.
* Web-интерфейс пользователя ССА и вся справочная документация должны быть полностью русифицированы за исключением системных команд.

**4.7. Требования к программному интерфейсу API ССА**

Должны выполняться следующие требования:

* взаимодействие с API осуществляется по защищенному HTTPS-протоколу с проверкой прав доступа к вызываемым функциям;
* программный интерфейс API предоставляет доступ к полученным данным по инцидентам в реальном времени внешним системам, используя формат JSON;
* в состав передаваемых данных программного интерфейса включены:
* уникальный идентификатор инцидента;
* классификация по типу инцидента;
* источник инцидента (канал, сессия, устройство, учетная запись пользователя);
* время инцидента;
* уникальный идентификатор сессии;
* имя пользователя;
* информация о браузере и устройстве пользователя;
* URI на котором произошел инцидент;
* User-Agent пользователя.
* при получении общего риска дополнительно получать идентификаторы сработавших правил и риск по каждому правилу;
* позволять получать выявление событий как в режиме реального времени, так и в диалоговом (запросном) режиме;
* обеспечивает возможность получения порции выявленных событий по сочетанию следующих параметров:
* периода времени;
* по идентификатору сессии Заказчика (когда это возможно);
* по заданному множеству типов событий.
* наличие поддержки технологии RBA (risk-based authentication) - аутентификации на основе рисков, в том числе предоставление автоматического вердикта аутентификации на основе рисков в системах Организации. Время формирования вердикта по аутентификации на основе рисков не должно превышать 1000 мс.
* предоставляет механизм обогащения транзакционного типа данными включая, но не ограничиваясь:
* обезличенный идентификатор карты отправителя и карты получателя;
* сумма;
* платежный терминал.
* формат данных о выявленном событие унифицирован, в то же время допускает указание дополнительных данных, специфических для события;
* предоставляет возможность давать обратную связь по выявленным событиям в целях обучения системы и повышения качества выявления мошеннической активности;
* использует типовые промышленные протоколы и методы экспорта/импорта данных;
* обеспечивает конфиденциальность передаваемых данных в выявленных событиях;
* обеспечивает pull, push и гибридный вариант передачи событий;
  1. **Требования к подсистеме в части анализа связей и их использования**
* выявление использования для работы в системе ДБО одного устройства несколькими пользователями;
* возможность выявления фактов входа в систему ДБО пользователей с использованием устройств, идентификаторы которых совпадают с идентификаторами устройств других пользователей системы ДБО, по запросу Организации;
* возможность поиска и выгрузки (через интерфейс пользователя, а также посредством запроса через API) идентификаторов пользователей системы ДБО, которые использовали для входа в систему ДБО те же устройства, что и заданный пользователь/пользователи;
* возможность поиска и выгрузки (через интерфейс пользователя, а также посредством запроса через API) идентификаторов (Логин или другой идентификатор) пользователей системы ДБО по таким параметрам, как номер инцидента, уникальный идентификатор устройства, IP адрес;
* возможность поиска и выгрузки (через интерфейс пользователя, а также посредством запроса через API) инцидентов по таким параметрам, как тип инцидента, номера инцидентов, IP адрес, уникальный идентификатор устройства, логин или другой идентификатор пользователя, дата и время инцидента;
* система должна обрабатывать запросы Организации в режиме онлайн для согласованного с Организацией пикового значения количества запросов в день.

# **4.9. Требования к подсистеме информационного обмена с Централизованным антифродом РУЗ**

ССА должна обеспечивать передачу сессионных данных по подозрительным и мошенническим событиям в Централизованный антифрод РУЗ.

# **5. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ ССА**

Должны выполняться следующие требования:

* поддерживать разграничение доступа на основе настраиваемой ролевой модели, построенной с учетом рабочих обязанностей Операторов;
* обеспечивать регистрацию действий Операторов в административной панели ССА;
* обеспечивать защищенное шифрованное соединение к web-интерфейсу управления;
* обеспечивать защиту от забытой сессии – поддерживать отключение неактивного соединения с web-интерфейсом по истечении промежутка времени или закрытии браузера;
* обеспечивать защищенное шифрованное соединение между всеми узлами ССА;
* обеспечивать механизмы защиты на уровне операционной системы (ограничение прав доступа, запрещение неиспользуемых сетевых сервисов и т.п.);
* обеспечивать ограничение доступа к базе данных ССА по сети.