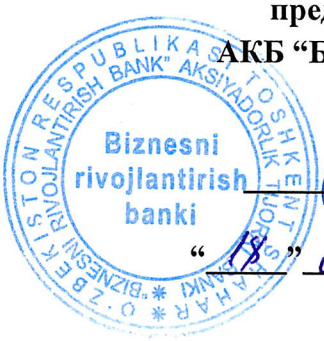
“УТВЕРЖДАЮ”

Первый заместитель
председателя правления
АКБ “Банк развития бизнеса”



_____ Ш. Юсупов

“ 18 ” августа 2025 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на приобретение сессионного антифрода

г. Ташкент - 2025 г.

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.

Термин	Понятие
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)

1 Общие сведения

В рамках закупки товаров и услуг для нужд АКБ «Банк развития бизнеса», поставщиком должна быть осуществлена поставка системы сессионной аналитики, производящая мониторинг, выявление аномалий, профилирование и анализ поведения пользователей, а также выявление бот-активности, производящие нелегитимные и мошеннические операции соответствующее нижеследующим техническим требованиям.

Полное наименование системы: Полное наименование — «Система сессионной аналитики, производящая мониторинг, выявление аномалий, профилирование и анализ поведения пользователей, а также выявление бот-активности, производящие нелегитимные и мошеннические операции в мобильных приложениях.». Далее – Система.

Сокращенное наименование системы в рамках настоящего документа: — ССА.

Исполнитель: Наименование организации исполнителя – (далее – Исполнитель) определяется по результатам открытого конкурса.

Заказчик: Наименование организации заказчика – АКБ «Банк развития бизнеса» (г. Ташкент, ул. Навои, 18А).

Срок начала работ: Работы по внедрению ССА начинаются с даты подписания договора на выполнение работ с Исполнителем

Срок окончания работ: В течение 15 дней после подписания договора с Исполнителем (но не позднее 01.09.2025 года).

Область применения

ССА должна производить сбор и анализ сессионных и поведенческих данных в мобилных приложениях.

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.

2 Перечень документов, на основании которых внедряется система

Решение №8 Комиссии по инновациям и проектам Банка от 15 июля 2024 года.

Письма Центрального банка №45-17/222 от 29.04.2024 года и №45-17/1752 от 14.07.2025 года.

Постановление Президента Республики Узбекистан №ПП-153 от 30.04.2025 года «О мерах, направленных на дальнейшее усиление деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий».

Постановление Правления центрального банка республики Узбекистан об утверждении положения о мерах по обеспечению информационной безопасности и кибербезопасности платежных систем операторов платежных систем и поставщиков платежных услуг и профилактики правонарушений, совершаемых посредством цифровых технологий (зарегистрировано министерством юстиции республики Узбекистан от 21.05.2024 г. Регистрационный № 3513)

Закон Республики Узбекистан о Кибербезопасности, от 15.04.2022 г. № ЗРУ-764;

Постановление Президента республики Узбекистан о дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры республики Узбекистан, от 31.05.2023 г. № ПП-167;

Постановление Президента от 15 июня 2020 года № ПП-4751 «О дополнительных мерах по дальнейшему совершенствованию системы обеспечения кибербезопасности в Республике Узбекистан»;

Постановление Президента республики Узбекистан «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры» республики Узбекистан, от 31.05.2023 г. № ПП-167;

3 Целью внедрения системы является

Система предназначена для автоматизированного выявления случаев нелегитимного использования мобильного приложения, обнаружения признаков мошеннической деятельности, а также предоставления интерфейса, обеспечивающего доступ аналитикам и внешним системам к данным о пользовательских сессиях, их устройствах и результатах срабатывания правил системы.

В части защиты веб-канала:

- идентификация отпечатка устройства пользователя (device fingerprinting);
- выявление фактов несанкционированного использования учетных данных клиентов;
- выявление фактов инъекции стороннего кода в защищаемое веб-приложение;
- выявление мошеннических внедрений в веб-часть на стороне клиента (веб-инъекции);
- обеспечение защиты от фишинг;
- выявление несанкционированных удаленных подключений к клиентскому устройству;
- определение работы клиента через TOR, proxy и «анонимайзеры»;
- выявление мошенничества с использованием средств удаленного управления (TeamViewer, AnyDesk, RDP, AmmyAdmin и т.д.);
- выявление доступа со скомпрометированных выделенных серверов или устройств компаний, предоставляющих услуги хостинга и колокации;
- выявление использования браузеров для подмены оригинальных параметров устройства (“antidetect browser”);

- выявление работы мошенника и легитимного пользователя на базе поведенческих данных: навигации, движения курсора, скорость и последовательность нажатия клавиш, паузы, взаимодействие с формами;

- выявление и блокировка вредоносной активности ботов: инициирующих прямые сетевые запросы к серверам Банка, использующих средства класса headless browser (Selenium, PhantomJS, и др.), повторно использующих легитимные cookie (cookie stuffing), имитирующих поведение человека и иные техники;

- выявление и блокировка автоматизированных попыток взлома учетных записей (“brute force”) или использования скомпрометированных учетных записей со сторонних ресурсов (“credential stuffing”);

- выявление средств подмены параметров устройства (Sphere, Multilogin, etc.);

- 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.

- 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).

- глобальный идентификатор устройства и корреляция между различными заказчиками в веб-канале.

В мобильных приложениях:

Должны осуществляться и передаваться ССА:

- идентификация мобильного устройства;

- выявление мобильных зловредных приложений с использованием сигнатурного анализа и поведенческого анализа;

- выявление запуска приложения на эмуляторе мобильного устройства или на неофициальной версии мобильной платформы (устройство с root-доступом);

- выявление несанкционированных удаленных подключений к клиентскому устройству (выявление использования средств удаленного управления);

- выявление фактов несанкционированного использования учетных данных клиентов (вход с нового устройства, вход с мошеннического устройства);

- выявление эмуляторов/симуляторов мобильных устройств с помощью пассивной биометрии в мобильном канале;

- определение работы клиента через TOR, proxy и «анонимайзеры»;

- выявление доступа со скомпрометированных выделенных серверов или устройств компаний, предоставляющих услуги хостинга и колокации;

- идентификация мобильных устройств одного пользователя в рамках приложения;

- отслеживание пользователя при смене мобильного устройства;

- анализ звонков, совершенных до запуска Android-приложения;

- глобальный идентификатор устройства и корреляция между различными заказчиками в мобильном канале;

- снижение уровня мошенничества;

-

- выявление признаков мошенничества при помощи социальной инженерии;

- ;

- выявление бот активности;

- повышение эффективности расследования инцидентов информационной безопасности;

- выявление подделки мобильного приложения Организации (проверка подписи, контроль целостности;

- идентификация смены сим-карты клиентом и передача информации в ССА;

- выявление средств для реализации deepfake атак;

- предоставление информации об обнаружения дебаггера на устройстве пользователя в ССА;

- 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).

- возможность использовать ССА в качестве второго фактора при аутентификации.

Требования к поставляемому программному обеспечению:

- Доставка программного обеспечения должна осуществляться путем передачи на электронном носители информации или отправкой лицензионных ключей на электронную почту банка;

- Вычислительные мощности для развёртывания программного обеспечения, предоставляются Заказчиком.

- Приобретаемое программное обеспечение должно иметь актуальную версию на момент поставки и в течение всего срока действия договора.

- ПО должна иметь разграничение и управление ролями пользователей.

3.1 Требования к гарантийному обслуживанию

- Исполнитель обязан предоставлять гарантийное обслуживание на поставляемое ПО.

-- Программное обеспечение должно иметь гарантийную и техническую поддержку сроком не менее одного года.

- Программное обеспечение должно быть полностью очищено от всех таможенных пошлин и прочих расходов, связанных с поставкой;

3.2 Требования к технической поддержке

- В рамках предоставляемой технической поддержки Заказчик должен иметь возможность сообщать о сбоях и запросах о технической помощи без ограничения количества запросов.

- Доступ к порталу технической поддержки не должен ограничиваться количеством учетным записям.

- Обработка тикетов должна, как минимум, включать решение технических проблем и настройку системы.

- Время ответа на новый открытый тикет не может превышать одного рабочего дня (8 часов).

- Служба технической поддержки должна гарантировать доступ к текущим версиям системы и обновлениям, а также к технической документации – как минимум, к руководствам пользователя и администратора системы.

- Техническая поддержка должна предоставляться в режиме 24/7.

- Поддержка исполнителя предоставляется на узбекском, английском и русском языках.

- Открытие технической проблемы должно быть возможно по крайней мере с помощью двух каналов связи: через портал технической поддержки, доступный через веб-браузер, позволяющий удаленно сообщать и отслеживать статус открытой заявки.

3.3 Требование к обучению персонала.

- Исполнитель обязуется произвести обучение персонала для достижения навыков, необходимых для использования и сопровождения программного обеспечения в соответствии с их назначением и функциональностью.

- Исполнитель должен проводить обучение для сотрудников заказчика по вопросам эксплуатации и администрирования ПО.

3.4 Требование к технической документация

- Исполнитель должен предоставлять полную документацию по установке, настройке и эксплуатации ПО.

- Все предоставляемые технические средства должны сопровождаться полной и актуальной технической документацией.

3.5 Требования к безопасности

Исполнитель должен обеспечивать контроль целостности ПО на всех этапах внедрение.

Персонал, осуществляющий установку ПО, должен иметь соответствующую квалификацию и опыт.

Исполнитель должен предоставлять регулярные обновления и патчи для ПО, включая обновления безопасности.

4 Требования к Участнику

- наличие статуса авторизованного партнера, подтвержденного производителем;
- наличие сертифицированного специалиста (уровня Advanced или эквивалентного) у поставщика решения или представителя вендора, который может проводить работы по установке и настройке решения русском, английском и на узбекском языке;
- исполнитель обязуется по согласованию с заказчиком произвести пуско-наладку «под ключ» всего программного обеспечение не позднее чем через 40 (сорок) дней с момента подписания актов приёма-передачи программного обеспечение, с обязательным привлечением к работам специалиста/инженера, имеющего соответствующую квалификацию для работы с поставляемым программном обеспечением;
- требуемым расчетам вычислительных ресурсов серверного оборудования (сайзинг) для поставляемого решения без привязанности к определенному производителю;
- порядку и условиям лицензирования, при их наличии (порядок взимания платы, вид предоставляемых лицензий (срочные/бессрочные, по количеству пользователей) и др.);
- сервисам (подписка и техническая поддержка);
- перечню осуществляемых работ (услуг) с конкретизацией объема и привлекаемых специалистов (*обоснование формирование стоимости оказываемых услуг в разрезе чел./час и длительность выполнение работ*);

в рамках выделенного бюджета:

- должен предоставить полностью укомплектованное и работоспособное решение, необходимое для обеспечения полноты использование запрашиваемой конфигурации;
- может предложить свое аналогичное решение (в том числе с превосходящими функциональными характеристиками и альтернативным подходом реализации подсистем/модулей), которое соответствует всем целям и задачам настоящего технического задания (с учетом целевого назначения);
- должен предпринять все необходимые меры по предотвращению утечки информации и обеспечению техники безопасности для своего персонала при внедрении системы на объектах Заказчика;
- не должен манипулировать длительностью внедрения программных решений в целях увеличения стоимости проекта;

5 Технико-технологические требования к системе

5.1 Требования к клиентской части ССА

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, 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).

5.2 В мобильных приложениях

Должны осуществляться и передаваться ССА:

- 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.

5.3 Технические требования

- Необходимо использовать СУБД ORACLE или PostgreSQL
- СУБД должна работать в режиме Master-Slave
- СУБД должна реплицироваться
- Все сервера входящих в ПО необходимо строить на основе на Oracle Linux 8/9.9 или Alma Linux
- Все сервера должны быть обновлены до последних стабильных версий, а обновления безопасности настроены на автоматическое применение
- Также учесть, чтоб система имела возможность работать на микро сервисное архитектуре
- Система должна поддерживать развёртывание в кластере на KUBERNETES
- Все пароли системы должны хранится в зашифрованном хранилище Vault Hashicorp и не должны хранится в конфиг файлах или в коде программы
- После окончания технического обслуживания и сопровождения, если передаются или покупаются права на ССА, то просим передать нам исходный код в силу того, когда закончится срок технической поддержки и обслуживания, чтоб разработчики банка могли сами изменять и дорабатывать систему
- Весь процесс доставки кода должен начинаться с банковской системы хранения версия GITLAB gitlab.brb.uz

6 Общие требования к ССА

6.1 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 с Централизованным антифродом РУЗ.

6.2 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 номер телефона;

- выявлять случаи, когда легитимный пользователь меняет свое мобильное устройство на новую модель

- выявлять случаи, когда пользователь меняет (e)SIM-карту на своем мобильном 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;

- 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;

6.3 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.

6.4 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 с 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.

6.5 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 автоматическом 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.

6.6 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.

6.7 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;

- 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.

6.8 Требования к подсистеме информационного обмена с Централизованным антифродом РУЗ

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

7. 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.

Директор департамента комплаенс-контроля **Ж.Юсупов**

Руководитель центра информационной безопасности **Б.Шамсиев**

Директор департамента информационных технологий **З.Орифхожаев**