**№ 2532**
**2025 yil «3» «noyabr»**

# ТЕХНИЧЕСКОЕ ЗАДАНИЕ
## Внедрение антивирусной защиты в мобильное приложение

**Ташкент 2025 г.**

# 1. ТЕРМИНЫ И СОКРАЩЕНИЯ

| Термин\Сокращение | Пояснение |
|---|---|
| SDK (Software Development Kit) | Набор инструментов для разработки программного обеспечения, включающий библиотеки, примеры кода и документацию. |
| Mobile Security SDK | Программный модуль, обеспечивающий функции антивирусной защиты и мониторинга безопасности мобильного приложения. |
| Threat Intelligence | Система сбора, анализа и обмена данными об актуальных киберугрозах |
| On-Demand / On-Access сканирование | Проверка файлов по требованию пользователя / в режиме реального времени |
| Root / Jailbreak | Получение несанкционированного доступа к системным привилегиям мобильного устройства (Android / iOS). |
| DNS (Domain Name System) | Система доменных имён, обеспечивающая сопоставление доменных имён и IP-адресов |
| API (Application Programming Interface) | Интерфейс взаимодействия между программными компонентами. |
| Киберугроза | Потенциальное действие или событие, способное нарушить конфиденциальность, целостность или доступность информации |
| Облачная инфраструктура | Совокупность распределённых вычислительных ресурсов, обеспечивающих обработку и хранение данных в реальном времени. |
| Интеграция | Процесс внедрения и настройки программного компонента в существующее приложение или инфраструктуру |
| Сигнатура угрозы | Уникальная последовательность признаков, по которой определяется вредоносный объект или активность |
| Самозащита приложения | Механизм, предотвращающий модификацию или вмешательство в код и логику работы мобильного приложения. |
| Антивирусный контроль | Это часть общей проверки безопасности мобильного устройства, направленная именно на обнаружение вредоносных объектов и подозрительной активности. |

**СОДЕРЖАНИЕ**

Термины и сокращения ..... 2
1. Общие сведения ..... 4
1.1 Полное наименование ПО и его условное обозначение ..... 4
1.2 Наименование организаций заказчика и разработчика ПО ..... 4
1.3 Перечень документов, на основании которых внедряется защита ..... 4
1.4 Плановые сроки начала и окончания ..... 4
1.5 Требования к Исполнителю ..... 5
2. Назначение и цели ..... 5
2.1 Назначение ..... 5
2.2 Цели создания ..... 5
3. Область применения ..... 5
3.1 Целевая аудитория продукта ..... 5
3.2 Сценарии использования ..... 5
4. Функциональные требования ..... 5
4.1 Многоступенчатая система защиты (пятиступенчатый подход): ..... 5
5. Нефункциональные требования ..... 7
6. Требования к реализации и внедрению ..... 7
7. Порядок приемки ..... 7
8. Прочие условия ..... 8
9. Заключение ..... 8

## 2. ОБЩИЕ СВЕДЕНИЯ

Данное техническое задание определяет требования к внедрению и интеграции Mobile Security SDK в мобильные приложения Банка. Предполагается, что интегрированное решение обеспечит многоуровневую защиту мобильных платформ (Android и iOS), повысит уровень безопасности финансовых операций и защиту конфиденциальных данных.

### 2.1 Полное наименование ПО и его условное обозначение

Полное наименование: Внедрение антивирусной защиты в мобильное приложение.

### 2.2 Наименование организаций заказчика и разработчика ПО

Заказчик – АКБ “Узпромстройбанк” (далее - “Заказчик” или “Банк”)

Адрес «Заказчика»: Узбекистан г.Ташкент. 100000, улица Шахрисабз, 3 дом

МФО: 00440

ИНН: 200833707

Наименование банка: ОПЕРУ при АКБ “Узпромстройбанк”

Адрес электронной почты: info@sqb.uz

Исполнитель разработки ПО (далее - “Разработчик” или “Исполнитель”) будет определен по результатам отбора наилучшего предложения.

### 2.3 Перечень документов, на основании которых внедряется защита

- Закон Республики Узбекистан «О телекоммуникациях» № ЗРУ–1015 от 27 декабря 2024 г.
- Закон Республики Узбекистан «Об электронной коммерции» № ЗРУ–385 от 29 апреля 2015 г.
- Закон Республики Узбекистан «Об электронной цифровой подписи» № ЗРУ–562 от 15 декабря 2018 г.
- Постановление Президента Республики Узбекистан № ПП–153 от 30 апреля 2025 г. *«О мерах, направленных на дальнейшее развитие деятельности по борьбе с преступлениями, совершаемыми с помощью информационных технологий»*.
- O‘z DSt 2875:2014 — *Датацентрлар учун талаблар* (Требования к центрам обработки данных).
- ISO/IEC 27001:2022 — *Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования.*
- ISO/IEC 27034-1:2011 — *Информационные технологии. Безопасность приложений. Общие принципы.*
- ISO/IEC 19790:2012 — *Криптографические модули. Требования к безопасности.*
- ГОСТ 34.602–89 — *Техническое задание на создание автоматизированной системы.*
- ГОСТ 19.201–78 — *Техническое задание. Требования к содержанию и оформлению.*
- Внутренние нормативные документы Банка в области информационной безопасности, защиты персональных данных и эксплуатации мобильных приложений.

### 2.4 Плановые сроки начала и окончания

Плановый срок начала – после заключения контракта

Плановый срок окончания – согласно условиям договора, но не более 6 месяцев.

### 2.5 Требования к Исполнителю

Иметь действующую авторизацию партнера/дистрибьютора поставщика решения, обеспечивающий право на использование решения и получение технической поддержки на территории Республики Узбекистан.

## 3. НАЗНАЧЕНИЕ И ЦЕЛИ

### 3.1 Назначение

Интегрировать SDK в мобильные приложения, обеспечивающие доступ к финансовым ресурсам и другим конфиденциальным данным Банка.

Повысить уровень безопасности мобильных транзакций и операций.

Обеспечить своевременное оповещение о выявленных угрозах и своевременное реагирование на атаки.

### 3.2 Цели создания

Реализовать проверку безопасности мобильного устройства (антивирусный контроль, анализ настроек, проверка root-статуса и наличие подозрительных приложений).

Интегрировать механизмы защиты соединения с интернетом (проверка DNS, валидация сертификатов, анализатор безопасности Wi-Fi, веб-фильтрация).

Реализовать механизмы самозащиты приложения (проверка цифровой подписи, контроль целостности и обнаружение попыток подмены функционала).

Организовать интеграцию с глобальной облачной инфраструктурой для получения актуальной информации об угрозах и оперативного реагирования.

## 4. ОБЛАСТЬ ПРИМЕНЕНИЯ

### 4.1 Целевая аудитория продукта

Мобильные приложения, используемые Банком, в том числе для организации внутренней работы, обслуживания клиентов и проведения финансовых операций.

Приложения, работающие с финансовыми, личными и коммерческими данными.

Количество лицензий:

- 950 000 (девятьсот пятьдесят тысяч) лицензий — для мобильного приложения физических лиц;
- 50 000 (пятьдесят тысяч) лицензий — для мобильного приложения юридических лиц.

### 4.2 Сценарии использования

Защита мобильных устройств сотрудников банка при работе с критическими данными.

Контроль безопасности приложений, распространяемых через официальный мобильный магазин банка.

Обеспечение оперативного реагирования на угрозы за счёт интеграции с глобальной облачной инфраструктурой.

## 5. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

### 5.1 Многоступенчатая система защиты (пятиступенчатый подход):

**Анализ устройства:**

- Сканирование на наличие небезопасных настроек.
- Проверка установленных приложений на предмет опасного содержимого (Android).
- Оценка репутации приложений на основе глобальных баз данных (Android).
- Проверка целостности устройства с возможностью обнаружения root-прав (Android) или jailbreak-состояния (iOS);

**Защита устройства:**

- Реализация классических антивирусных функций (On-Demand и On-Access сканеры) для профилактики заражения вредоносными программами (Android).
- Реализация контроля устанавливаемых / обновляемых приложений (Android)
- Периодическое сканирование устройства по расписанию (Android)
- Опционально – наличие фонового сервиса для обеспечения постоянной защиты устройства. (Android)

**Защита соединений:**

- Проверка безопасности сетевых соединений (анализ безопасности Wi-Fi сетей, проверка DNS, валидация сертификатов). (iOS, Android)
- Встроенные средства веб-фильтрации для блокировки доступа к вредоносным ресурсам. (iOS, Android)

**Защита приложения:**

- Решение должно обладать встроенными механизмами самозащиты, включая проверку цифровой подписи и контроль целостности на этапе выполнения. (Android)
- Система должна обеспечивать выявление и предотвращение любых попыток несанкционированного вмешательства в функциональность или логику работы приложения.(Android)
- Дополнительные функции защиты должны включать:
- Постоянное обновление базы знаний об актуальных угрозах (Threat Intelligence) в режиме реального времени; (iOS, Android)
- Гибкие механизмы настройки под особенности защищаемого приложения, позволяющие реализовать адаптивную и своевременно обновляемую систему защиты. (iOS, Android)
- Сбор сигнатур и аналитических данных о киберугрозах должен осуществляться на территории Республики Узбекистан, а также в сопредельных государствах (Российская Федерация, Республика Казахстан, Кыргызская Республика, Республика Таджикистан, Китайская Народная Республика) с целью обеспечения точности, актуальности и региональной релевантности системы обнаружения угроз. (iOS, Android)

### 4.2. Интеграция с глобальной облачной инфраструктурой:

Опциональная маршрутизация и передача данных об угрозах в облачную платформу.

- Получение обновляемой информации об угрозах в реальном времени.
- Минимизация ложных срабатываний за счёт корреляции данных с глобальными базами.

### 4.3. Поддержка платформ:

Полная совместимость с актуальными версиями Android и iOS. Поддержка новых выпускаемых версий. Поддержка Android (7+), iOS (14+)

### 4.4. Параметры безопасности:

- Минимальное время реакции на обнаружение угроз.
- Высокая степень защиты данных и конфиденциальности.
- Сертификация на соответствие международным стандартам безопасности (перечень сертификатов и результаты тестирований могут быть приведены в приложении).

## 6. НЕФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ

### 5.1. Производительность:

- Минимальное влияние на скорость работы мобильного приложения.
- Оптимизация потребления ресурсов устройства (память, процессор).

### 5.2. Надёжность:

- Гарантированное обнаружение более 410 000 новых угроз ежедневно, обновление актуальной информации о новых угрозах в режиме реального времени.
- Высокая степень доступности (более 99.9%) к облачной инфраструктуре для оперативного обновления информации об угрозах при наличии интернет-соединения на устройстве.

### 5.3. Масштабируемость:

- Возможность интеграции в различные мобильные приложения с различной архитектурой.

### 5.4. Удобство использования:

- Минимальное вмешательство в пользовательский интерфейс приложения.
- Прозрачное информирование пользователя о состоянии защиты.

## 7. ТРЕБОВАНИЯ К РЕАЛИЗАЦИИ И ВНЕДРЕНИЮ

### 6.1. Этапы внедрения:

- Подготовительный этап: анализ текущей инфраструктуры, сбор требований.
- Интеграция SDK в тестовую версию мобильного приложения.
- Проведение внутренних тестирований и обеспечения соответствия требованиям.
- Пилотное внедрение и апробация на группе пользователей.
- Внедрение в полном масштабе и переход в продуктивную эксплуатацию.

### 6.2. Техническая документация и инструкции:

- Полный комплект документации по интеграции и эксплуатации SDK.
- Руководство для разработчиков и методические рекомендации по настройке мер безопасности.

### 6.3. Поддержка и обновления:

- Гарантия технической поддержки от поставщика на период эксплуатации.
- Регулярное обновление компонентов безопасности и алгоритмов обнаружения угроз.
- Наличие локальных инженеров в Центральной Азии по SDK
- Поддержка русского языка в SDK

## 8. ПОРЯДОК ПРИЕМКИ

### 7.1. Критерии приемки

- Соответствие функциональных возможностей заявленным требованиям.
- Успешное прохождение тестов по безопасности и нагрузочному тестированию. - Подтверждение интеграции с глобальной облачной инфраструктурой.
- Отсутствие критических ошибок и стабильная работа на целевых платформах.

### 7.2. Процедура приемки:

- Проведение демонстрационного тестирования в присутствии представителей Банка.
- Согласование результатов тестирования, оформление акта приемки работы.
- Заключение договора о техподдержке и гарантийном обслуживании.

## 9. ПРОЧИЕ УСЛОВИЯ

**Лицензирование**: Продукт поставляется по модельным схемам лицензирования.

**Конфиденциальность**: Все данные, передаваемые между компонентами решения, не покидают инфраструктуру заказчика (в случаях, когда это технически возможно) и защищены современными средствами шифрования.

**Юридические аспекты**: Все условия интеграции и использования продукта соответствуют требованиям законодательства Республики Узбекистан в сфере информационной безопасности.

## 10. ЗАКЛЮЧЕНИЕ

Настоящее техническое задание является основой для внедрения антивирусного SDK в мобильные приложения АКБ «Узпромстройбанк». Решение, ориентированное на многоуровневую защиту мобильных устройств, позволит обеспечить высокий уровень безопасности, предотвращая современные кибератаки и минимизируя риски утечки конфиденциальных данных.

**Boshqaruv Raisi o'rinbosari:** **D.Umarov**

kelishuvchilar: T.Rapiyev, V.Krasnov, A.Kenjayev, A.Ergashev, S.Ikramov

*https://hujjat.sqb.uz/?pin=rU87cU71&id=75e1a74a-d0c2-4569-9c7b-278e37b1eec3*