Приложение № 1

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На проведение комплексного аудита информационной безопасности систем Дистанционного банковского обслуживания (Физических лиц и Юридических лиц) методом White Box и Black Box

Глава 1. Цель проекта

Объективная оценка уровня защищенности систем дистанционного банковского обслуживания (ДБО) для физических (B2C) и юридических лиц (B2B) путем детального анализа исходного кода, архитектуры и логики работы приложений. Выявление критических уязвимостей, оценка соответствия требованиям НБКР и выработка рекомендаций по устранению дефектов безопасности на уровне кода и инфраструктуры.

Глава 2. Область оценки (Scope)

Аудиту подлежат следующие компоненты (включая исходный код, конфигурации и тестовые среды):

1) ДБО Физических лиц: Мобильные приложения (iOS, Android), веб-банкинг.
2) ДБО Юридических лиц: Веб-клиент, интеграционные шлюзы (API / Host-to-Host).
3) Бэкенд и API: Серверная часть систем ДБО, микросервисы, внешние и внутренние API-интерфейсы.
4) Смежная инфраструктура: Серверы приложений, СУБД, веб-серверы, конфигурации средств защиты (WAF, NGFW).

Глава 3. Состав и этапы работ

Этап 1. Анализ архитектуры и конфигураций

1) Анализ архитектуры сети, схем информационных потоков и зон сегментации (DMZ, внутренний контур, процессинг).
2) Аудит конфигураций системного ПО, веб-серверов, СУБД и средств защиты информации.
3) Проверка политик разграничения доступа, механизмов аутентификации и авторизации (в т.ч. работы с ЭЦП, МФА, токенами).

Этап 2. Анализ защищенности методом White Box и Black box

Работы проводятся с полным предоставлением Исполнителю исходного кода, архитектурной документации (API Swagger/OpenAPI, схемы БД) и доступом к тестовым учетным записям.

Статический и динамический анализ кода (SAST / DAST / MAST):

1) Автоматизированный и экспертный (ручной) анализ исходного кода фронтенда и бэкенда.
2) Поиск уязвимостей, связанных с некорректной валидацией входных данных (OWASP Top 10, OWASP API Security Top 10).
3) Выявление зашитых в коде учетных данных, ключей шифрования и паролей (hardcoded secrets).

4) Анализ используемых сторонних библиотек и компонентов на наличие известных уязвимостей (SCA — Software Composition Analysis).

Аудит бизнес-логики и механизмов авторизации на уровне кода:

1) Анализ кода реализации критических операций: проведение платежей, переводы, изменение лимитов, регистрация устройств, выпуск/привязка карт и токенов.
2) Проверка разграничения прав доступа в коде (горизонтальный и вертикальный обход полномочий — BOLA/IDOR).
3) Анализ механизмов криптографической защиты: генерация сессионных ключей, алгоритмы подписи транзаций (ЭЦП), валидация SSL-сертификатов (включая SSL Pinning в мобильных приложениях).

Этап 3. Аудит механизмов противодействия фроду (Anti-fraud)

1) Оценка устойчивости ДБО к автоматизированным атакам (брутфорс, спреинг паролей, СМС-перехват) на уровне логики приложения.
2) Проверка корректности сбора и передачи обогащенных данных (Device ID, фингерпринт, геолокация) из клиентских приложений в антифрод-систему.
3) Тестирование сценариев реагирования ДБО на блокировки и подозрительные транзакции.

Этап 4. Соответствие регуляторным требованиям

1) Проверка соответствия систем ДБО требованиям Положений и нормативно-правовых актов Национального банка (НБКР) в части информационной безопасности и управления операционными/киберрисками.

Глава 4. Требования к Исполнителю

1 Наличие действующих лицензий на проведение работ в области ИБ (согласно законодательству КР).
2 Подтвержденный опыт проведения аудитов исходного кода (White Box) и систем ДБО в финансовом секторе (референс-лист).
3 Наличие у специалистов проектной команды профильных международных сертификаций по анализу кода и тестированию (OSCP, OSWE, CASE, CISSP, CISA или эквиваленты).

Глава 5. Формат отчетности и результаты

По окончании работ Исполнитель предоставляет:

1. Отчет для руководства:

   Краткое описание уровня защищенности, ключевых рисков и бизнес-последствий на языке топ-менеджмента.

2. Технический отчет:

   1) Детальное описание каждой найденной уязвимости с классификацией по шкале CVSS v3/v4.
   2) Ссылки на конкретные файлы и строки исходного кода, содержащие дефекты.
   3) Конкретные технические рекомендации по устранению (примеры безопасного кода, патчи, изменение конфигураций).

3. План устранения недостатков:

   Приоритезированный чек-лист для ИТ- и ИБ-команд банка.

Глава 6. Условия проведения работ

1) Предоставление доступов: Заказчик обязуется предоставить Исполнителю выгрузку исходного кода актуальных версий систем ДБО (или доступ в изолированный Git-репозиторий), документацию к API, а также развернуть тестовую среду (Staging), идентичную продуктивной, с тестовыми учетными записями для всех ролей пользователей (ФЛ, ЮЛ, Бухгалтер, Администратор, Операционист и др.).
2) Конфиденциальность: Передача исходного кода и документации осуществляется строго после подписания Соглашения о конфиденциальности (NDA) по защищенным каналам связи.
3) Безопасность тестирования: Деструктивные сценарии (DoS/DDoS) из рамок данного ТЗ исключены.
4) Срок выполнения работ: с 15 августа 2026 года – 15.11.2026 года.