СНГБ
БАНК НАШЕГО ГОРОДА

Наименование тендера	Техническое задание на комплексный анализ защищенности платежного приложения системы переводов в Viber АО БАНК "СНГБ" с предоставлением исходного кода.
Срок предоставления ТКП:	14.09.2020
Этапы проведения работ	**Этапы работ:** 1. Проведение комплексной проверки действующего функционала и последующей перепроверки устранения выявленных уязвимостей платежных приложений с учетом международных стандартов, рекомендаций и лучших практик: - Open Web Application Security Project Mobile Security Testing Guide (https://owasp.org) - Open Web Application Security Project Web Security Testing Guide (https://owasp.org) - Open Source Security Testing Methodology Manual (https://www.isecom.org) - Penetration Testing Execution Standard (http://www.pentest-standard.org) - Web Application Security Consortium (WASC) Threat Classification (http://www.webappsec.org); - NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (www.nist.gov); 2. Проведение анализа уязвимостей требованиям к оценочному уровню доверия не ниже ОУД 4 в соответствии с ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».
Дополнительные требования к участникам и оказания услуг	1. Исполнитель должен выполнять работы своими силами без привлечения третьей стороны. 2. Опыт оказания подобных работы организациям в финансово-кредитном секторе, не менее 3 лет, просим участников подтвердить рекомендательными письмами, желательно по направлению анализ защищенности приложений. 3. Все работы проводятся Исполнителем удаленно. (Командировок и выездов на площадки Заказчика, находящиеся не в г. Москва, не предусмотрено.) 4. Исполнитель должен подтвердить отсутствие в санкционном списке https://sanctionssearch.ofac.treas.gov/. 5. Оплата услуг осуществляется поэтапно, в течении 10 рабочих дней после подписания акта оказания услуг. 6. Обязательное указание в ТКП сроков и стоимости по каждому этапу работ. 7. Обмен документами осуществляется посредством СЭД "Диадок". 8. Участник тендера должен представить в ТКП методику проведения тестирования, а также стоимость и сроки работ по каждому этапу. 9. Заказчик в праве осуществлять передачу отчета по результатам работ, разработчику ПО (третьей стороне) для устранения выявленных уязвимостей, а также получать консультацию от Исполнителя посредством телефонной связи, с привлечением третьей стороны. 10. Наличие лицензии на осуществление деятельности по технической защите конфиденциальной информации на проведение работ и услуг, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации». 11. Срок исполнения обязательств по работам, указанным на этапе 1: 15 рабочих дней, с даты заключения договора.

	12. Срок исполнения обязательств по работам, указанным на этапе 2: не позднее 01.05.2021г.
Состав и цели работ	1. Получение объективной оценки защищенности платежного приложения Заказчика от внешних злоумышленников. 2. Выявление недостатков в применяемых Заказчиком мерах информационной безопасности и оценка возможности их использования нарушителем. 3. Практическая демонстрация возможности использования уязвимостей (на примере наиболее критических). 4. Предложение адекватного комплекса организационных, технических и управляющих мер, направленных на предотвращение угроз информационной безопасности, а также перечня неотложных технических мер для повышения защищенности платежного приложения Заказчика. 5. Повторная проверка устранения уязвимостей. 6. Проверка нового разработанного функционала с повторной проверкой устранения уязвимостей. 7. Проведение анализа уязвимостей требованиям к оценочному уровню доверия не ниже ОУД 4 в соответствии с ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».
Требования к методике и составу работ	Анализ защищенности платежного приложений проводится в соответствии с: - Open Web Application Security Project Mobile Security Testing Guide (https://owasp.org); - Open Web Application Security Project Web Security Testing Guide (https://owasp.org); - Open Source Security Testing Methodology Manual (https://www.isecom.org) - Penetration Testing Execution Standard (http://www.pentest-standard.org) - Web Application Security Consortium (WASC) Threat Classification (http://www.webappsec.org); - NIST SP 800-115, Technical Guide to Information Security Testing and Assessment (www.nist.gov); - ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности». Идентификация уязвимостей осуществляется на основе рекомендаций производителей по безопасной конфигурации ПО, материалов свободных исследовательских групп по поиску уязвимостей Open Web Application Security Project (OWASP), каталогов уязвимостей Common Vulnerabilities and Exposures (CVE). Для систематизации выявленных уязвимостей по степени критичности необходимо использовать международный стандарт оценки уязвимостей Common Vulnerability Scoring System (CVSS) версии 3. В процессе проведения работ допустимо использовать ручные и автоматические проверки.
	Модель нарушителя: Внешний злоумышленник без логического доступа к платежному приложению (Б1) Злоумышленник в канале связи без логического доступа к платежному приложению (Б2) Злоумышленник с физическим доступом к устройству с установленным платежным приложением (Б3) Злоумышленник с логическим доступом к платежному приложению (В1) Злоумышленник в канале связи с логическим доступом к платежному приложению (В2) Злоумышленник с физическим доступом к устройству с установленным платежным приложением и логическим доступом к платежному приложению (В3)

	Анализ защищенности клиентской части приложения «Client-side» методом черного ящика, то есть путем анализа функций и параметров настройки приложения со стороны нарушителя, не обладающего логическим доступом к платежному приложению; методом серого ящика, то есть путем анализа функций и параметров настройки приложения со стороны нарушителя, обладающего пользовательским или иным доступом к платежному приложению; методом белого ящика, то есть путем анализа исходного кода клиентской части приложения.
	Анализ защищенности серверной части приложения «Server-side» методом черного ящика, то есть со стороны нарушителя, не обладающего логическим доступом к платежному приложению; методом серого ящика, то есть со стороны нарушителя, обладающего пользовательским или иным доступом к платежному приложению; методом белого ящика, то есть путем анализа исходного кода серверной части приложения.
	Анализ защищенности канала передачи данных между серверной и клиентской частью приложения «Communications channel»
Результат оказания услуг	**По этапу 1:** Отчет о результатах проверки / перепроверки защищенности платежного приложения: -общие сведения о проведенном анализе защищенности платежного приложения, с указанием версий исследуемого продукта и версия протокола обмена; -результаты проведенных проверок; -выводы (как развернутые технические, так и более краткие для руководства); -оценка состояния защищенности платежного приложения Заказчика; -перечень и описание существующих угроз; -описание хода работ, выявленных уязвимостей, ранжирование их по степени потенциальной опасности, вероятности их использования, описание последствий реализации выявленных уязвимостей оценкой критичности уязвимостей по международному стандарту Common Vulnerability Scoring System (v.3); -рекомендации по устранению выявленных уязвимостей; -рекомендации по изменению конфигурации и настроек оборудования, используемых защитных механизмов и программных средств, принятию дополнительных мер и применению дополнительных средств защиты, по установке необходимых обновлений для используемого программного обеспечения и т.п.; -результаты эксплуатации нескольких критичных уязвимостей, включая информацию о полученном уровне привилегий в платежном приложении на различных этапах работы. **по этапу 2:** Технический отчет с результатами соответствия оценочному уровню доверия не ниже ОУД 4 в соответствии с ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».