



АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК «ПРИМОРЬЕ» (ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО)

## ТЕХНИЧЕСКОЕ ЗАДАНИЕ

**на проведение оценки соответствия ПАО АКБ «Приморье» требованиям  
Положения Банка России от 09.06.2012 № 382-П**

адрес: 690091, Россия, г.Владивосток, ул. Светланская, 47  
приемная: телефон (423) 2406200 2221255  
общий отдел: телефон (423) 2261902, факс (423) 2226875  
e-mail: [mail@primbank.ru](mailto:mail@primbank.ru)  
<http://www.primbank.ru>

## Оглавление

1. Введение .....	3
2. Цели и задачи работ .....	3
3. Состав работ .....	3
4. Требования к составу и содержанию работ .....	4
4.1. Этап 1. Проведение аудита соответствия требованиям Положения №382-П. ..	4
4.2. Этап 2. Выполнение Заказчиком рекомендаций по достижению соответствия требованиям Положения № 382-П.....	4
4.3. Этап 3. Выполнение Заказчиком рекомендаций по достижению соответствия требованиям Положения № 382-П.....	5
5. Сроки выполнения работ .....	5
6. Ограничения.....	5
7. Квалификационные требования .....	6

## 1. Введение

1.1. Банк, являясь участником НПС в ролях оператора по переводу денежных средств и оператора электронных денежных средств в соответствии с пунктом 2.15 Положения Банка России от 09.06.2012г. №382-п «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» обеспечивает проведение оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее – оценка соответствия) не реже одного раза в два года.

## 2. Цели и задачи работ

2.1. Целью выполнения работ является предоставление Заказчику результатов оценки выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением Банка России от 09.06.2012 №382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (далее – Положение № 382-П).

2.2. Для достижения поставленной цели должны быть решены следующие задачи:

2.2.1. анализ и оценка внутренней документации по обеспечению информационной безопасности Заказчика;

2.2.2. формирование области оценки и плана оценки соответствия;

2.2.3. проведение оценки соответствия Заказчика требованиям Положения № 382-П;

2.2.4. формирование перечня выявленных несоответствий состояния обеспечения информационной безопасности требованиям Положения № 382-П, разработка Плана приведения в соответствие Заказчика указанным требованиям;

2.2.5. консультирование Заказчика по вопросам соответствия требованиям Положения № 382- П;

2.2.6. формирование отчетных материалов по результатам оценки соответствия.

## 3. Состав работ

3.1. Этапы работ

3.1.1. Работы выполняются в 3 этапа:

- Проведение аудита соответствия требованиям Положения № 382-П.
- Выполнение Заказчиком рекомендаций по достижению соответствия требованиям Положения № 382-П.
- Формирование отчетных материалов по результатам оценки соответствия.

#### **4. Требования к составу и содержанию работ**

##### **4.1. Этап 1. Проведение аудита соответствия требованиям Положения №382-П.**

4.1.1. Установление способа взаимодействия и способа передачи конфиденциальной информации.

4.1.2. Выбор подлежащих оценке соответствия объектов:

- информационные системы;
- средства защиты информации;
- процессы обеспечения информационной безопасности;
- площадки;
- структурные подразделения.

4.1.3. Анализ и оценка предоставленных внутренних нормативных документов по обеспечению ИБ.

4.1.4. Анализ аналогичного отчета по результатам аудита 2019г.

4.1.5. Сбор свидетельств аудита для оценки выполнения требований Положения № 382-П.

4.1.6. Проведение анализа предоставленных свидетельств аудита, а также запрос дополнительных свидетельств аудита в случае необходимости.

4.1.7. Оценка применимых показателей Положения № 382-П.

4.1.8. Анализ результатов оценки соответствия.

4.1.9. Подготовка оптимального перечня мероприятий по повышению показателей информационной безопасности, необходимых для достижения уровня соответствия, рекомендуемого Банком России.

4.1.10. Формирование сводного файла оценки в соответствии с Приложением 2 к Положению 382-П с указанием текущей оценки и свидетельств выполнения (или не выполнения) требований в формате \*.xlsx, либо в другом формате по согласованию с Заказчиком.

4.1.11. По итогам выполнения работ должны быть разработаны следующие документы:

- сводный файл оценки в формате в соответствии с п 4.1.10;
- рекомендации по достижению соответствия требованиям Положения

№ 382-П.

4.1.12. Рекомендации по достижению соответствия требованиям Положения № 382-П должны содержать:

- несоответствия, выявленные в ходе проведения оценки соответствия;
- рекомендации по приведению в соответствие требованиям. Сортировка рекомендаций проводится по принципу максимального влияния на итоговую оценку

выполнения Требований.

##### **4.2. Этап 2. Выполнение Заказчиком рекомендаций по достижению соответствия требованиям Положения № 382-П**

4.2.1. Заказчик выполняет рекомендации по достижению соответствия требованиям Положения № 382-П.

4.2.2. Длительность этапа определяется план-графиком проведения работ.

4.2.3. По результату выполнения рекомендаций Заказчик присылает Исполнителю свидетельства выполнения рекомендаций. Исполнитель подтверждает корректность выполнения рекомендаций.

#### **4.3. Этап 3. Выполнение Заказчиком рекомендаций по достижению соответствия требованиям Положения № 382-П**

4.3.1. Исполнитель формирует отчетные материалы по результатам оценки соответствия, которые включают в себя:

- скорректированный сводный файл оценки в соответствии с Приложением 2 к Положению 382-П с указанием текущей оценки и свидетельств выполнения (или не выполнения) требований в формате \*.xlsx, либо в другом формате по согласованию с Заказчиком;

- итоговые документы в соответствии с требованиями Приложения 1 к Положению 382-П.

4.3.2. Требования к документированию:

- документы должны представляться в двух экземплярах на бумажном и электронном носителях;

- электронное представление документов должно соответствовать формату редакторов Microsoft Word, Microsoft Visio, Microsoft PowerPoint (\*.docx, \*.xlsx, \*.vsd, \*.ppt).

### **5. Сроки выполнения работ**

5.1. Работы выполняются после заключения договора в соответствии с утвержденным план графиком работ.

5.2. Ориентировочный срок начала работ после подписания договора.

5.3. Длительность работ в рамках этапа 1 определяется Исполнителем исходя из трудозатрат, при этом не может быть более 1 календарного месяца. Длительность работ этапа 3 определена сроком сдачи отчетной документации в п.5.4 и трудозатратами Исполнителя. Длительность этапа 2 определяется разницей между этапами 1 и 3.

5.4. Все отчетные документы должны быть подготовлены и согласованы до 15.12.2021. Дата окончания проведения оценки в отчетных документах 20.12.2021.

### **6. Ограничения**

6.1. Исполнитель гарантирует соблюдение условий конфиденциальности исходных данных и/или сведений, относящихся к деятельности Заказчика, ставших известными специалистам Исполнителя в ходе выполнения работ по аудиту.

6.2. В случае необходимости проведения проверки некоторого количества однотипных объектов (прикладных систем, серверов, сервисов, межсетевых экранов и т.п.), оценка выполняется на репрезентативной выборке из этих объектов. Объем и способ выборки определяется сотрудниками Исполнителя исходя из следующих принципов:

6.2.1. проведение проверок на данной выборке должно обеспечивать получение значимых для Заказчика результатов;

6.2.2. выборка должна быть достаточной для принятия обоснованного решения о выполнении данного требования на всем множестве объектов. Выборка, использовавшаяся при проведении оценки, указывается в отчете об обследовании/оценке.

6.2.3. Работы проводятся удаленно без необходимости присутствия на площадках Заказчика. При необходимости проводится интервьюирование сотрудников Заказчика в разумных пределах, либо путем заполнения опросных листов.

6.2.4. В рамках выполнения работ тестирование на проникновение не проводится.

## 7. Квалификационные требования

7.1. Исполнитель должен иметь лицензию на деятельность по технической защите конфиденциальной информации ФСТЭК России.

7.2. Исполнитель должен иметь опыт проведения не менее 2х аналогичных аудитов для компаний – участников Банковской системы России.

РАЗРАБОТАНО

Руководитель СИБ

\_\_\_\_\_

(дата)

\_\_\_\_\_

(подпись)

Шумко И.Г.

(Ф.И.О.)

СОГЛАСОВАНО

Директор ДЭБ

\_\_\_\_\_

(дата)

\_\_\_\_\_

(подпись)

Герасименко В.А.

(Ф.И.О.)

УТВЕРЖДЕНО

Зам. директора ДИБТ

\_\_\_\_\_

(дата)

\_\_\_\_\_

(подпись)

Домбинский В.А.

(Ф.И.О.)