БАНК ПРИМОРЬЕ

АКЦИОНЕРНЫЙ КОММЕРЧЕСКИЙ БАНК "ПРИМОРЬЕ" (ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО)

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на проведение оценки соответствия ПАО АКБ «Приморье» требованиям Стандарта ГОСТ Р 57580.1-2017

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
http: www.primbank.ru

Оглавление

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
http: www.primbank.ru

1. Введение

1.1. Банк, являясь участником платежной системы Банка России, в соответствии с требованиями Положения Банка России от 09.01.2019 № 672-П «О требованиях к защите информации в платежной системе Банка России» обеспечивает соответствие стандартному уровню (уровень 2) защиты информации, определенному Стандартом.

1.2. Банк, в целях противодействия осуществлению переводов денежных средств, в соответствии с требованиями Положения Банка России от 17.04.2019 № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» обеспечивает соответствие стандартному уровню защиты информации, определенному Стандартом.

1.3. Банк, обрабатывая биометрические персональные данные в целях идентификации граждан Российской Федерации, в соответствии с Приказом Минкомсвязи России от 25.06.2018 г. № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» обеспечивает соответствие стандартному уровню защиты информации, определенному Стандартом.

1.4. В целях подтверждения соответствия стандартному уровню защиты, Банк обеспечивает проведение оценки соответствия с привлечением сторонней организации, имеющей лицензию ФСТЭК на деятельность по технической защите конфиденциальной информации и обладающей необходимым уровнем компетенций.

2. Цели и задачи работ

2.1. Целью выполнения работ является предоставление Заказчику результатов оценки соответствия уровню защиты информации, определенному Стандартом.

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

2.2.1. Обследование объектов Заказчика, включающее анализ и оценку внутренней документации по обеспечению информационной безопасности и организационных и технических мер обеспечения безопасности.

2.2.2. Формирование области оценки (включая сегменты 683-П, 672-П, ЕБС).

2.2.3. Проведение предварительной оценки соответствия Заказчика.

2.2.4. Формирование предварительной оценки по результатам предварительного аудита (GAP-анализ) и рекомендаций по совершенствованию защиты информации и устранению выявленных недостатков.

2.2.5. Консультирование Заказчика по вопросам соответствия требованиям Стандарта.

2.2.6. Составление итогового отчета, включающего оценку соответствия текущего состояния защиты информации у Заказчика уровню защиты информации, определенному в Стандарте.

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
http: www.primbank.ru

3. Состав работ

3.1. Работы выполняются в 3 этапа:

3.1.1. Предварительная оценка соответствия Заказчика требованиям Стандарта.

3.1.2. Выполнение Заказчиком рекомендаций по достижению соответствия требованиям Стандарта.

3.1.3. Итоговая оценка соответствия Заказчика требованиям Стандарта.

4. Требования к составу и содержанию работ

Этап 1. Предварительная оценка соответствия Заказчика требованиям Стандарта

Подэтап 1.1. Сбор свидетельств очно на объектах Заказчика для дальнейшей оценки соответствия требованиям Стандарта.

Цель подэтапа. Получение свидетельств реализации мер защиты информации на объектах Заказчика.

Состав работ подэтапа. На данном подэтапе оказываются Услуги:

1. Установление способа взаимодействия и способа передачи конфиденциальной информации.
2. Подготовка и согласование плана проведения оценки соответствия с указанием интервьюируемых и сопровождающих лиц, а также дат проведения встреч интервью.
3. Анализ документарной информации по системе защиты информации, предоставленной Заказчиком.
4. Проведение экспресс-обследования на объектах Заказчика, подлежащих оценке, включая сбор свидетельств реализации мер защиты информации с использованием основных источников и методов.
5. Анализ исправления недостатков предыдущих аудитов и тестов на проникновение по направлению информационной безопасности.
6. Анализ параметров конфигураций и настроек средств защиты информации, тестов на проникновение.
7. Документирование результатов наблюдения и результатов сбора свидетельств.

Подэтап 1.2. Предварительная оценка выбора Заказчиком мер защиты информации.

Цель подэтапа. Определить степень соответствия существующих мер защиты информации требованиям Стандарта.

Состав работ подэтапа. На данном подэтапе оказываются следующие Услуги:

1. Формирование перечня неоцениваемых областей предварительной оценки (процессов, подпроцессов, направлений, мер) с обоснованием их исключения из области оценки.
2. Оценка выбора Заказчиком мер защиты информации отдельно для следующих процессов и подпроцессов защиты информации:

2.1. Процесс «Обеспечение защиты информации при управлении доступом»:

– подпроцесс «управление учетными записями и правами субъектов логического доступа»;

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
http: www.primbank.ru

– подпроцесс «идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»;

– подпроцесс «защита информации при осуществлении физического доступа»;

– подпроцесс «идентификация, классификация и учет ресурсов и объектов доступа».

2.2. Процесс «Обеспечение защиты вычислительных сетей»:

– подпроцесс «сегментация и межсетевое экранирование вычислительных сетей»;

– подпроцесс «выявление вторжений и сетевых атак»;

– подпроцесс «защита информации, передаваемой по вычислительным сетям»;

– подпроцесс «защита беспроводных сетей».

2.3. Процесс «Контроль целостности и защищенности информационной инфраструктуры».

2.4. Процесс «Защита от вредоносного кода».

2.5. Процесс «Предотвращение утечек информации».

2.6. Процесс «Управление инцидентами защиты информации»:

– подпроцесс «мониторинг и анализ событий защиты информации»;

– подпроцесс «обнаружение инцидентов и реагирование на них».

2.7. Процесс «Защита среды виртуализации».

2.8. Процесс «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств».

3. Оценка обоснований принятых компенсирующих мер защиты информации.

Подэтап 1.3. Предварительная оценка полноты реализации у Заказчика мер защиты информации.

Цель подэтапа. Определить полноту реализации выбранных Заказчиком мер защиты информации.

Состав работ подэтапа. На данном подэтапе оказываются следующие Услуги:

1. Предварительная оценка полноты реализации у Заказчика мер защиты информации отдельно для каждого из процессов по направлениям:

1.1. Планирование процесса системы защиты информации.

1.2. Реализация процесса системы защиты информации.

1.3. Контроль процесса системы защиты информации.

1.4. Совершенствование процесса системы защиты информации.

2. Предварительная оценка защиты информации на этапах жизненного цикла АС Заказчика.

3. Формирование перечня выявленных нарушений.

Подэтап 1.4. Подготовка Отчета о проведенной предварительной оценки

Цель подэтапа. Подготовить документальную оценку по результатам предварительного аудита (GAP-анализа) Заказчика требованиям Стандарта.

Состав работ подэтапа. На данном подэтапе оказываются следующие Услуги:

1. Изложение процесса проведения предварительной оценки.

2. Проведение расчетов итоговой оценки и оценки степени соответствия текущего состояния защиты информации у Заказчика требуемому уровню защиты информации.

3. Проводится учет мер по неиспользуемым технологиям, неактуальным угрозам и экономической нецелесообразности закрытия рисков предлагаемыми СЗИ.

4. Подготовка рекомендаций по совершенствованию защиты информации и устранению выявленных нарушений.

5. Формирование Отчета и приложений к нему.

5.1. Отчет предоставляется Исполнителем Заказчику в бумажной и электронной формах.

5.2. В Отчет дополнительно включается перечень предлагаемых технических средств защиты информации, отсутствующих у Заказчика, с указанием общего изменения оценки при их приобретении и оценочную стоимость.

Этап 2. Выполнение Заказчиком рекомендаций по достижению соответствия требованиям Стандарта

2.1. Заказчик выполняет рекомендации по достижению соответствия требованиям Стандарта.

2.2. Длительность этапа определяется план-графиком проведения работ, согласуемым отдельно.

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

Этап 3. Итоговая оценка соответствия Заказчика требованиям Стандарта

Подэтап 3.1. Итоговая оценка выбора Заказчиком мер защиты информации.

Цель подэтапа. Определить степень соответствия существующих мер защиты информации требованиям Стандарта.

Состав работ подэтапа. На данном подэтапе оказываются следующие Услуги:

1. Формирование перечня неоцениваемых областей оценки (процессов, подпроцессов, направлений, мер) с обоснованием их исключения из области оценки;

2. Оценка выбора Заказчиком мер защиты информации отдельно для следующих процессов и подпроцессов защиты информации:

2.1. Процесс «Обеспечение защиты информации при управлении доступом»:

– подпроцесс «управление учетными записями и правами субъектов логического доступа»;

– подпроцесс «идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа»;

– подпроцесс «защита информации при осуществлении физического доступа»;

– подпроцесс «идентификация, классификация и учет ресурсов и объектов доступа.

2.2. Процесс «Обеспечение защиты вычислительных сетей»:

– подпроцесс «сегментация и межсетевое экранирование вычислительных сетей»;

– подпроцесс «выявление вторжений и сетевых атак»;

– подпроцесс «защита информации, передаваемой по вычислительным сетям»;

– подпроцесс «защита беспроводных сетей».

2.3. Процесс «Контроль целостности и защищенности информационной инфраструктуры».

2.4. Процесс «Защита от вредоносного кода».

2.5. Процесс «Предотвращение утечек информации».

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
http: www.primbank.ru

2.6. Процесс «Управление инцидентами защиты информации»:

– подпроцесс «мониторинг и анализ событий защиты информации»;

– подпроцесс «обнаружение инцидентов и реагирование на них».

2.7. Процесс «Защита среды виртуализации».

2.8. Процесс «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств».

3. Оценка обоснований принятых компенсирующих мер защиты информации.

Подэтап 3.2. Итоговая оценка полноты реализации у Заказчика мер защиты информации.

Цель подэтапа. Определить полноту реализации выбранных Заказчиком мер защиты информации.

Состав работ подэтапа. На данном подэтапе оказываются следующие услуги:

1. Итоговая оценка полноты реализации у Заказчика мер защиты информации отдельно для каждого из процессов по направлениям:

1.1. Планирование процесса системы защиты информации.

1.2. Реализация процесса системы защиты информации.

1.3. Контроль процесса системы защиты информации.

1.4. Совершенствование процесса системы защиты информации.

2. Итоговая оценка защиты информации на этапах жизненного цикла АС Заказчика.

3. Проводится учет мер по неиспользуемым технологиям, неактуальным угрозам и экономической нецелесообразности закрытия рисков предлагаемыми СЗИ.

4. Проведение расчетов итоговой оценки и оценки степени соответствия текущего состояния защиты информации у Заказчика трем уровням защиты информации.

5. Результаты выполнения работ

5.1. Результатом оказания Услуг является подготовка отчета, включающего:

– сведения об Исполнителе;

– сведения о руководителе и членах проверяющей группы;

– сведения о Заказчике;

– цель оценки;

– сроки проведения оценки;

– область оценки;

– резюме для руководства;

– перечень неоцениваемых областей оценки (процессов, подпроцессов, направлений, мер) с обоснованием их исключения из области оценки;

– обоснование применения компенсирующих мер защиты информации при невозможности реализации отдельных выбранных мер;

– краткое изложение процесса оценки соответствия;

– числовое значение итоговой оценки соответствия защиты информации по трем уровням защиты информации;

– неразрешенные разногласия между исполнителем и заказчиком;

– перечень представителей со стороны Банка, которые сопровождали исполнителя;

– опись документов (копий документов) на бумажных носителях, прилагаемых к отчету с указанием общего количества томов приложений, количества и наименований документов, а также количества листов в каждом из них;

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
http: www.primbank.ru

– опись машинных носителей информации, прилагаемых к отчету (если есть).

5.2. К отчету прилагаются и являются неотъемлемой частью:

– заполненные листы для сбора свидетельств оценки процессов (подпроцессов);

– перечень выявленных нарушений защиты информации;

– рекомендации по совершенствованию защиты информации и устранению выявленных нарушений, в т.ч. по доработке локальных актов Заказчика;

– таблицы, содержащие числовые значения оценок процессов (подпроцессов) и направлений системы защиты информации;

– копии документов на бумажных носителях, являющихся свидетельствами выполнения требований защиты информации;

– машинные носители информации с электронными документами и файлами данных, являющихся свидетельствами выполнения требований защиты информации (если есть).

5.3. Допускается формирование единого отчета по всем сегментам оцениваемой деятельности (сегмент 672-П, сегмент 683-П, сегмент ЕБС) с отдельным расчетом значений мер, либо формирование разных отчетов по каждому сегменту отдельно.

5.4. Отчет предоставляется Исполнителем Заказчику в бумажной и электронной форме.

6. Сроки выполнения работ

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

6.2. Ориентировочный срок начала работ – октябрь 2020 г.

6.3. Длительность работ в рамках этапов 1 и 3 определяется Исполнителем, исходя из трудозатрат, при этом не может быть более 3-х календарных месяцев. Длительность этапа 2 определяется Заказчиком с учетом достижения определенных целевых значений.

7. Ограничения

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

7.2. Сроки и стоимость проведения работ должны быть рассчитаны с учетом проведения работ как на территории Исполнителя, так и на 2-х площадках Заказчика, расположенных в г. Владивосток и должны включать все необходимые командировочные расходы.

7.3. Предварительное обследование проводится очно на площадке Заказчика.

7.4. 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:

7.4.1. Проведение проверок на данной выборке должно обеспечивать получение значимых для Заказчика результатов.

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

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
http: www.primbank.ru

8. Квалификационные требования

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

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

8.3. Исполнитель должен иметь хотя бы одного сотрудника в составе рабочей группы по проекту, имеющего подтверждение наличия квалификаций по проведению аудита ГОСТ 57580.1 (свидетельство о повышении квалификации, сертификаты о прохождении обучений, семинаров, пр. свидетельства наличия квалификаций).

РАЗРАБОТАНО			
Руководитель СИБ	_____	_____	Шумко И.Г.
	дата	подпись	Ф.И.О.
СОГЛАСОВАНО			
Директор ДЭБ	_____	_____	Герасименко В.А.
	дата	подпись	Ф.И.О.
УТВЕРЖДЕНО			
Директор ДИБТ	_____	_____	Акулов С.С.
	дата	подпись	Ф.И.О.

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
http: www.primbank.ru