

# ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на услуги по разработке нормативных документации по информационной безопасности  
АКИБ «Ипотека-банк»

## 1. Термины и сокращения

Термин/сокращение	Определение
ИБ	Информационная безопасности
Инцидент ИБ	Событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий ИБ, имеющих значительную вероятность компрометации бизнес-операции и создания угрозы ИБ
СрЗИ	Средства защиты информации
Тестирование на проникновение (пентест)	Метод оценки безопасности информационных систем или сетей средствами моделирования атаки злоумышленника

## 2. Цель оказания Услуг

Целями оказания Услуг в рамках настоящего Технического задания являются:

- сбор информации о текущем состоянии процессов аутентификации и управлению инцидентами ИБ;
- анализ текущей нормативной документации Заказчика в области ИБ;
- разработка нормативных документов;

## 3. Сроки оказания Услуг

Порядок оказания Услуг по настоящему Техническому заданию Исполнитель согласовывает с Заказчиком в течении 5 (пяти) рабочих дней с даты подписания Договора.

Услуги оказываются согласно следующим срокам:

- Этапы 1-2 – не более 20 рабочих дней с даты подписания Договора. Срок выполнения работ по этапам 1-2 не включает в себя время, которое будет затрачено АКИБ «Ипотека-банк» на представление Исполнителю исходных данных в полном объеме, ознакомление с разработанными Исполнителем документами и их согласование.
- Этап 3 – не более 20 рабочих дней с даты подписания Договора и момента предоставления АКИБ «Ипотека-банк» вычислительных мощностей и удаленного доступа для настройки макета.
- Этап 4 – не более 10 рабочих дней с даты окончания Этапов 1-3.

## 4. Место оказания Услуг

Работы по обследованию (Этап 1) проводятся заочно на основании данных, запрошенных Исполнителем и предоставленных Ипотека-банк.

Работы макетированию технических средств управления и мониторинга инцидентами ИБ (Этап 3) проводятся Исполнителем удаленно на территории и на вычислительных мощностях АКИБ «Ипотека-банк».

## 5. Этапы оказания Услуг

Этап	Наименование этапа	Результаты этапа
1	Сбор исходных данных	1) Правила процедуры аутентификации; 2) Правила по мониторингу событий информационной безопасности и управлению инцидентами информационной безопасности;
2	Разработка нормативных документов	
3	Разработка рекомендаций по управлению инцидентами ИБ	1) Оценка стоимости модернизации подсистемы анализа и корреляции событий ИБ; 2) Отчет о результатах макетирования SIEM.
4	Проверка правил мониторинга и управления инцидентами ИБ, макета SIEM методом тестирования на проникновения (пентест)	3) Отчет

## 6. Описание требуемых Услуг

### 6.1. Этап 1 - Сбор исходных данных

Целью данного этапа является сбор исходных данных о текущем состоянии процессов аутентификации, управления и мониторинга инцидентами ИБ.

В рамках данного этапа необходимо провести следующие работы:

- анкетирование сотрудников АКИБ «Ипотека-банк», связанных с обработкой информации, занимающихся вопросами обеспечения безопасности информации;
- анализ имеющихся нормативных документов в области ИБ.

Работы по обследованию должны проводиться заочно на основании данных, запрошенных Исполнителем и предоставленных АКИБ «Ипотека-банк».

Сбор информации должен включать в себя:

- сбор нормативной документации по информационной безопасности;
- сбор информации по текущим процессам аутентификации;
- сбор информации по текущим процессам управления аутентификации;
- сбор информации о существующих СрЗИ и средствах мониторинга событий ИБ.

Сбор исходных данных должен осуществляться заочно в головном офисе АКИБ «Ипотека-банк», на основании данных, запрошенных Исполнителем и предоставленных АКИБ «Ипотека-банк».

### 6.2. Этап 2 – Разработка нормативной документации

На данном этапе необходимо разработать следующую нормативную документацию по защите информации:

- Правила процедуры аутентификации;
- Правила по мониторингу событий информационной безопасности и управлению инцидентами информационной безопасности.

Разработанную нормативную документацию Исполнитель должен согласовать с АКИБ «Ипотека-банк».

### **6.3. Этап 3 - Разработка рекомендаций по управлению инцидентов**

Целью данного этапа является формирование рекомендаций по техническим средствам управления инцидентами ИБ. На данном этапе необходимо провести выбор и макетирование решения по анализу и корреляций событий информационной безопасности (SIEM) с учетом индивидуальных особенностей процесса управления ИБ Заказчика.

Макетирование должно производиться на вычислительных мощностях АКИБ «Ипотека-банк». АКИБ «Ипотека-банк» предоставляет Исполнителю удаленный доступ для настройки макета SIEM.

Результатом данной стадии является:

- Оценка стоимости модернизации подсистемы анализа и корреляции событий ИБ;
- Отчет о результатах макетирования SIEM.

### **6.4. Этап 4 - Проверка правил мониторинга и управления инцидентами ИБ, макета SIEM методом тестирования на проникновения**

На данном этапе Исполнитель должен провести тестирование разработанных правил по управлению и мониторингу событий ИБ, макета SIEM. Данная проверка проводится методом тестирования на проникновения (пен-тест). Для этого Исполнитель осуществляет внешнее тестирование на проникновение согласованных узлов ИТ инфраструктуры АКИБ «Ипотека-банк». Ответственные сотрудники АКИБ «Ипотека-банк» проверяют разработанные Исполнителем правила и работу макета SIEM в разрезе отработки инцидентов, сгенерированных тестированием на проникновения.

Выявленные недочеты в нормативной документации, разработанной Исполнителем, корректируются. Результаты данного этапа отображаются в отчете.

## **7. Требования к отчетным документам**

Комплект отчетных документов должен включать:

- Правила процедуры аутентификации;
- Правила по мониторингу событий информационной безопасности и управлению инцидентами информационной безопасности;
- Оценка стоимости модернизации подсистемы анализа и корреляции событий ИБ;
- Отчет о результатах макетирования SIEM;
- Отчет о проверке правил мониторинга и управления событиями ИБ.

Отчетные документы передаются Заказчику в электронном виде в формате файлов WORD и PDF.

## **8. Требования к Исполнителю:**

- не менее 3х лет деятельности в указанной отрасли
- не менее 5 успешных аналогичных проекта
- наличие кадрового потенциала с указанием опыта работы по аналогичным проектам