**ОАО АФК "Система"**

|  |  |  |
| --- | --- | --- |
| **УТВЕРЖДАЮ** |  | **СОГЛАСОВАНО** |
| [Введите должность представителя предприятия-заказчика] |  | [Введите должность представителя предприятия-разработчика] |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[ФИО] |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ФИО] |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ г. |  | «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ г. |
| **СОЗДАНИЕ КОРПОРАТИВНОГО СТАНДАРТА, МЕТОДИКИ И РЕГЛАМЕНТА ПРОВЕДЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**  **ОАО АФК «Система»**  Техническое задание  AFKMAZ.ТЗ | | |
| **СОГЛАСОВАНО** |  | **СОГЛАСОВАНО** |
| [Введите должность представителя предприятия-заказчика] |  | [Введите должность представителя предприятия-разработчика] |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_[ФИО] |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [ФИО] |
| «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ г. |  | «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ г. |

**СОДЕРЖАНИЕ**

[1. Общие сведения 2](#_Toc411523144)

[1.1. Полное наименование работ и ее условное обозначение 2](#_Toc411523145)

[1.2. Шифр темы 2](#_Toc411523146)

[1.3. Перечень документов, на основании которых производится работа 2](#_Toc411523147)

[1.4. Плановые сроки начала и окончания работ 3](#_Toc411523148)

[1.5. Порядок оформления и предъявления результатов работ 3](#_Toc411523149)

[2. Цели и задачи проведения работ 4](#_Toc411523150)

[3. Описание объекта аудита 5](#_Toc411523151)

[3.1. Информационные системы 5](#_Toc411523152)

[3.2. Средства защиты информации 5](#_Toc411523153)

[4. Состав и содержание работ 6](#_Toc411523154)

[4.1. Перечень стадий работ 6](#_Toc411523155)

[4.2. Требования к стадиям работ 6](#_Toc411523156)

[4.2.1. Разработка Корпоративного Стандарта ИБ 6](#_Toc411523157)

[4.2.2. Разработка Корпоративной Методики проведения аудита ИБ 7](#_Toc411523158)

[4.2.3. Разработка Корпоративного регламента проведения аудита ИБ 8](#_Toc411523159)

[5. Требования к документированию 9](#_Toc411523160)

[5.1. Общие требования 9](#_Toc411523161)

[5.2. Перечень отчетных документов и требования к их содержанию 9](#_Toc411523162)

[6. Перечень обозначений и сокращений 11](#_Toc411523163)

[7. Термины и определения 11](#_Toc411523164)

# Общие сведения

## Полное наименование работ и ее условное обозначение

Проведение работ по созданию Корпоративного Стандарта ИБ, Методики и Регламента проведения аудита информационной безопасности в ОАО АФК «Система».

## Шифр темы

AFKMAZ

## Перечень документов, на основании которых производится работа

1. Корпоративный Кодекс «Безопасность» ОАО АФК «Система».
2. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014).
3. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 — 2014» (СТО БР ИББС-1.2-2014).
4. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности СТО БР ИББС-1.1-2007» (СТО БР ИББС-1.1-2007).
5. Международный стандарт ISO/IEC 27001:2013 «Information technology. Security techniques. Information security management systems. Requirements»;
6. Международный стандарт ISO/IEC 27002:2013 «Information technology. Security techniques. Code of practice for information security management».
7. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
9. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
10. Модель угроз безопасности информации, составляющей коммерческую тайну ОАО АФК «Система», при её обработке в Корпоративной информационной системе (разработана в рамках реализации проекта "Создание системы защиты информации, составляющей коммерческую тайну ОАО АФК "Система"). - Москва, 2010.
11. Частная модель нарушителя и угроз безопасности персональных данных (разработана в рамках реализации проекта "Создание системы защиты персональных данных ОАО АФК "Система"). - Москва, 2014.

## Плановые сроки начала и окончания работ

Дата начала работ: с момента подписания договора

Дата окончания работ: 29.05.2015

Календарные сроки выполнения этапов, а также порядок их документального оформления определяются договором.

## Порядок оформления и предъявления результатов работ

По окончании выполнения работ Исполнителем составляется и направляется Заказчику на рассмотрение Акт выполненных работ, в котором должен быть указан состав выполненных работ и их стоимость. А также отчетные документы, предусмотренные договором.

Заказчик в течение 10 дней с момента получения Акта подписывает акт или направляет Исполнителю мотивированный отказ с перечнем необходимых доработок, составленный в письменном виде. Ненаправление Заказчиком Исполнителю разногласий к Акту не является принятием работ со стороны Заказчика.

В случае мотивированного отказа от приемки выполненных работ стороны в течение 10 календарных дней оформляют Протокол согласования необходимых доработок, порядка и сроков их выполнения.

В случае изменения объемов и/или сроков выполняемых работ, указанные изменения оформляются путем подписания обеими сторонами дополнительных соглашений.

# Цели и задачи проведения работ

Целью работы является подготовка корпоративных документов, регламентирующих оценку текущего уровня информационной безопасности, уровня менеджмента информационной безопасности и уровня осознания информационной безопасности с учетом динамики их изменения на основании лучших практик, мировых и отечественных стандартов в области информационной безопасности.

В рамках работ должен быть разработан пакет корпоративных документов, включающий в себя Стандарт ИБ, Методику и Регламент проведения аудита ИБ. По инициативе исполнителя могут быть разработаны и иные документы, при этом указанное обстоятельство не должно повлиять на общий срок и/или стоимость выполняемых работ.

Для достижения данной цели необходимо выполнить следующий объем задач:

* анализ нормативной документации в области защиты информации, а также моделей нарушителей и угроз безопасности информации, утвержденных в ОАО АФК «Система»;
* анализ и выявление положений мировых и отечественных стандартов в области информационной безопасности актуальных для создания корпоративных документов;
* инвентаризация набора применяемых защитных мер (действующие организационные ограничения и средства защиты информации);
* систематизация требований по информационной безопасности и правил проверки корректности их выполнения на базе документов п.1.3;
* стандартизация подходов и способов оценки соответствия обеспечения ИБ Заказчика корпоративным и нормативным требованиям документов, указанных в п.1.3;
* разработка и введение понятных групповых и частных показателей, оценивающих степень соответствия обеспечения ИБ организации требованиям корпоративных документов, и способов оценки этих показателей;
* проведение работ по апробации Методики и Регламента проведения аудита, получение предварительных результатов оценки.

# Описание объекта аудита

Разрабатываемый комплект документов (Корпоративный Стандарт, Методика и Регламент) должны быть применимы к следующим активам Заказчика:

1. Информационные системы.
2. Средства защиты информации.
3. Информационные сервисы.
4. Каналы передачи данных.

Перечень и краткое описание информационных систем и средств защиты информации подлежащих аудиту информационной безопасности, могут быть представлены по запросу после подписания соглашения о конфиденциальности.

# Состав и содержание работ

## Перечень стадий работ

Работы должны быть проведены в один этап, включающий в себя следующие стадии:

1. Разработка Корпоративного Стандарта ИБ.
2. Разработка Корпоративной Методики проведения аудита ИБ.
3. Разработка Корпоративного Регламента проведения аудита ИБ.

## Требования к стадиям работ

### Разработка Корпоративного Стандарта ИБ

**Требования к работам и результату:**

* + - 1. Должен быть проведен анализ действующей у Заказчика нормативно-правовой, технической и организационно-распорядительной документации в области информационной безопасности.
      2. Должен быть проведен анализ лучших практик, мировых и отечественных стандартов в области информационной безопасности.
      3. Должны быть определены рамки применения разрабатываемых документов, устанавливающие границы аудита информационной безопасности.
      4. В границы аудита информационной безопасности должны входить, по крайней мере, следующие области:
         1. обеспечение ИБ при назначении и распределении ролей;
         2. обеспечение ИБ при управлении доступом и регистрацией;
         3. обеспечение ИБ при использовании ресурсов сети Интернет, включая защиту периметра и каналов передачи данных;
         4. обеспечение ИБ при администрировании ИТ-инфраструктуры;
         5. обеспечение ИБ при использовании действующих средств защиты;
         6. обеспечение ИБ при обработке персональных данных;
         7. обеспечение ИБ при защите коммерческой тайны.

**Работы по данной стадии должны включать:**

* + - 1. Разработку состава требований по информационной безопасности с учетом их соответствия нормативным требованиям по защите персональных данных и коммерческой тайны.
      2. Составление сводной таблицы применяемых в организации Заказчика технических и организационных контрмер по каждому из требований ИБ. В рамках данного пункта должна быть проведена комплексная работа по обследованию и инвентаризации всех применяемых у Заказчика защитных мер.
      3. Определение приемлемых и специфических для Заказчика методов проведения внутренних проверок выполнения требований ИБ. Данные способы организационных и технических проверок должны быть отражены в разрабатываемых методике и регламенте аудита.
      4. Анализ применимости показателей информационной безопасности, представленных в Стандарте Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 — 2014». Выбор актуальных для Заказчика показателей.
      5. Анализ применимости требований международного стандарта ISO/IEC 27001:2013 по обеспечению и управлению информационной безопасностью. Выбор актуальных для Заказчика показателей.
      6. Выработка ключевых для Заказчика показателей информационной безопасности. Данные показатели должны быть в дальнейшем учтены в методике проведения аудита.
      7. Оформление документа «Отчет о применяемых защитных мерах и требованиях ИБ».
      8. Разработка Корпоративного Стандарта со сводным перечнем требований по информационной безопасности на базе нормативных документов, указанных в п. 1.3.

### Разработка Корпоративной Методики проведения аудита ИБ

**Требования к работам и результату:**

* + - 1. Методика должна строиться с учетом формализованных в Корпоративном Стандарте ИБ требований информационной безопасности.
      2. В ходе разработки Методики должны быть сформулированы показатели ИБ и критерии их оценки.
      3. Показатели информационной безопасности должны быть сгруппированы (определены групповые показатели) для упрощения определения общего уровня информационной безопасности и систематизации частных показателей ИБ.
      4. В рамках разработки Методики должны быть сформированы опросные листы и формы оценки соответствия текущего уровня ИБ.
      5. В качестве приложений к Методике должны быть разработаны формы оценки уровня безопасности в формате Microsoft Excel с возможностью подсчета общего уровня ИБ.
      6. В рамках разработки методики должны быть определены количественные и качественные шкалы измерения показателей ИБ.
      7. Методика должна включать оценку следующих характеристик ИБ:
         1. текущий уровень информационной безопасности;
         2. менеджмент информационной безопасности;
         3. уровень осознания информационной безопасности.

**Работы по данной стадии должны включать:**

* + - 1. Разработку Корпоративной методики проведения аудита ИБ на базе Корпоративного Стандарта ИБ (разрабатывается на предыдущей стадии).

### Разработка Корпоративного регламента проведения аудита ИБ

**Требования к работам и результату:**

* + - 1. Разработанный Регламент должен быть применим к организационно-штатной структуре Заказчика и определять роли сотрудников, участвующих в проведении самооценки ИБ (внутреннего аудита) от заинтересованных подразделений Заказчика, а также роль внешней организации при проведении внешнего аудита ИБ.
      2. Регламент проведения аудита ИБ должен строиться на базе, разработанной в рамках выполнения данного ТЗ, Методики.
      3. Разрабатываемый Регламент должен определять последовательность действий, выполняемых в рамках аудита ИБ.
      4. Регламент должен определять распределение полномочий, ответственность и обязанности участников аудита, в том числе устанавливать необходимость привлечения специализированных сторонних организаций для проведения внешнего аудита и вовлеченность подразделений Заказчика для проведения внутреннего аудита (самооценки).
      5. Регламент должен устанавливать периодичность проведения аудитов.
      6. Регламент должен определять порядок и форму документальной фиксации результатов аудита.

**Работы по данной стадии должны включать:**

* + - 1. Разработку Корпоративного Регламента проведения аудита ИБ.
      2. Работы по проведению самооценки ИБ совместно с Исполнителем работ, а также апробации Методики и Регламента проведения аудита по результатам проведенной оценки.

# Требования к документированию

## Общие требования

Комплект проектных/отчетных материалов предоставляется Заказчику в электронном виде (в формате PDF и MS Word) и на твердой копии в трех экземплярах. Вся разрабатываемая документация должна быть выполнена на русском языке.

## Перечень отчетных документов и требования к их содержанию

Состав и требования к содержанию основных отчетных документов отражает следующая таблица.

Таблица 1. Перечень и состав отчетных документов

| **Описание работ** | **Отчетный документ** |
| --- | --- |
| Разработка Корпоративного Стандарта ИБ | Отчет о применяемых защитных мерах и требованиях ИБ   1. Описание области аудита ИБ. 2. Состав действующих требований по информационной безопасности 3. Состав применяемых мер защиты 4. Анализ реализации действующих требований ИБ 5. Обзор методов проведения аудита ИБ 6. Анализ применимости рекомендованных СТО БР показателей ИБ 7. Перечень согласованных корпоративных показателей ИБ 8. Выводы   Корпоративный Стандарт ИБ   1. Введение 2. Область применения 3. Нормативные ссылки 4. Термины и определения 5. Обозначения и сокращения 6. Корпоративные требования по информационной безопасности 7. Проверка и оценка информационной безопасности |
| Разработка Корпоративной Методики проведения аудита ИБ | Корпоративная Методика проведения аудита ИБ   1. Введение 2. Область применения 3. Нормативные ссылки 4. Термины и определения 5. Обозначения и сокращения 6. Роли участников аудита ИБ 7. Показатели информационной безопасности 8. Способы оценивания показателей 9. Методика проведения самооценки ИБ 10. Методика проведения аудита ИБ силам внешней организации |
| Разработка Корпоративного Регламента проведения аудита ИБ | Корпоративный Регламент проведения аудита информационной безопасности   1. Введение 2. Область применения 3. Нормативные ссылки 4. Термины и определения 5. Регламент действий при самооценке уровня ИБ 6. Регламент взаимодействия с внешними организациями-аудиторами 7. Требования к документальному оформлению результатов аудита   Приложение № 1. Опросные листы и формы оценки соответствия. |

# Перечень обозначений и сокращений

|  |  |
| --- | --- |
| **АИС** | Автоматизированные информационные системы |
| **ИБ** | Информационная безопасность |
| **КТ** | Коммерческая тайна |
| **СЗИ** | Средство защиты информации |
| **ТЗ** | Техническое задание |
| **ФЗ** | Федеральный закон |

# Термины и определения

|  |  |  |
| --- | --- | --- |
| **Актив Заказчика** |  | Все, что имеет ценность для Заказчика и находится в его распоряжении. |
| **Аудит ИБ, внешний аудит ИБ** |  | Независимая оценка соответствия ИБ, выполняемая работниками организации, являющейся внешней по отношению к Заказчику, допускающая возможность формирования профессионального аудиторского суждения о состоянии ИБ Заказчика [2]. |
| **Защитная мера, контрмера** |  | Сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения информационной безопасности [2]. |
| **Корпоративная Методика проведения аудита ИБ** |  | Документ, стандартизирующий подход и способ оценки соответствия обеспечения ИБ Заказчика требованиям Корпоративного Стандарта ИБ. |
| **Корпоративный Регламент проведения аудита ИБ** |  | Документ, описывающий последовательность действий и требования к результатам внутреннего аудита ИБ Заказчика в соответствии с Корпоративной Методикой проведения аудита ИБ. |
| **Корпоративный Стандарт ИБ** |  | Корпоративный документ Заказчика, в котором в целях добровольного многократного использования устанавливаются правила обеспечения информационной безопасности активов Заказчика. |
| **Критерий оценки (аудита) ИБ** |  | Совокупность требований к обеспечению ИБ, определенных Корпоративным Стандартом ИБ или его частью [2]. |
| **Область аудита информационной безопасности** |  | Содержание и граница аудита ИБ [2]. |
| **Роль** |  | Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом [2]. |
| **Самооценка ИБ, внутренний аудит ИБ** |  | Оценка соответствия информационной безопасности требованиям Корпоративного Стандарта ИБ, выполняемая работниками Заказчика [2]. |
| **Свидетельства оценки соответствия (аудита) ИБ установленным критериям** |  | Записи, изложение фактов и другая информация, которые имеют отношения к критериям оценки соответствия и могут быть проверены [2]. |
| **Стандарт** |  | Документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг [2]. |
| **Угроза** |  | Опасность, предполагающая возможность потерь [2]. |
| **Показатель информационной безопасности** |  | Мера или характеристика для оценки информационной безопасности [3]. |