

«Утверждаю»

ДОКУМЕНТИРОВАННАЯ ПРОЦЕДУРА
ВНУТРЕННИЙ АУДИТ
СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Содержание

| | |
|---|----|
| 1 Назначение и область применения..... | 3 |
| 2 Нормативные ссылки..... | 3 |
| 3 Термины и определения | 3 |
| 4 Сокращения и обозначения..... | 3 |
| 5 Ответственность и полномочия..... | 4 |
| 6 Требования..... | 6 |
| 6.1 Общие положения..... | 6 |
| 6.2 Организация аудита..... | 7 |
| 6.3 Проведение аудита | 8 |
| 6.4 Документирование результатов аудита..... | 9 |
| 6.5 Анализ внутренних аудитов | 11 |
| 6.6 Методика оценивания компетентности внутренних аудиторов | 12 |
| 7 Записи..... | 15 |
| Лист регистрации изменений..... | 24 |
| Лист ознакомления | 25 |

1 Назначение и область применения

1.1 Настоящая документированная процедура устанавливает порядок проведения внутреннего аудита в системе менеджмента информационной безопасности (далее - СМИБ), построенной на основе стандарта ISO/IEC 27001:2022.

1.2 Настоящая документированная процедура является внутренним нормативным документом, ее требования распространяются на работников Компании, уполномоченных проводить внутренние аудиты СМИБ, а также руководителей структурных подразделений Компании.

2 Нормативные ссылки

2.1 В настоящей документированной процедуре Компании приведены ссылки на следующие нормативные документы:

| | |
|--|--|
| ISO 9000:2015 (СТ РК ISO 9000-2017) | Системы менеджмента качества. Основные положения и словарь; |
| ISO/IEC 27001:2015 (СТ РК ISO/IEC 27001-2016) | Системы менеджмента информационной безопасности. Требования; |
| ISO 19011:2018 (СТ РК ISO 19011:2019) | Руководящие указания по аудиту систем менеджмента |

3 Термины и определения

3.1 В настоящей документированной процедуре применяются термины и соответствующие им определения в соответствии со стандартом СМИБ Компании.

4 Сокращения и обозначения

4.1 В настоящей документированной процедуре организации применены следующие сокращения и обозначения в соответствии с таблицей 1:

Таблица 1 Сокращения и обозначения

| № п/п | Сокращения и обозначения | Полное название приведенных обозначений и сокращений |
|-------|--------------------------|---|
| 1 | ISO | International Organization for Standardization |
| 2 | СМИБ | Система менеджмента информационной безопасности |
| 3 | ЗСП | Заинтересованное структурное подразделение |
| 4 | Политика СМИБ | Политика в области информационной безопасности |
| 5 | Цели СМИБ | Цели в области информационной безопасности |
| 6 | ВНД | Внутренний нормативный документ |
| 7 | ДП | Документированная процедура |
| 8 | ДИ | Должностная инструкция |
| 9 | ПИ | Производственная инструкция |
| 10 | ИБОТ | Инструкция по охране труда |
| 11 | ЗД | Заместитель директора |
| 12 | РЗСП | Руководители заинтересованных структурных подразделений |
| 13 | СП | Структурное подразделение |
| 14 | ВА | Внутренний аудит |
| 15 | ДП | Документированная процедура |
| 16 | КД | Корректирующие действия |
| 17 | ГВА | Группа внутренних аудиторов |