СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «АЛЬТЕРНАТИВНАЯ ГЕНЕРИРУЮЩАЯ КОМПАНИЯ-1»

ДЕКЛАРАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. СВЕДЕНИЯ О ДОКУМЕНТЕ

1.1 Настоящий документ определяет Декларацию информационной безопасности ООО «АГК-1».

1.2 Документ разработан Отделом информационной безопасности Общества.

1.3 Срок действия: до замены (отмены).

1.4 Оригинал документа хранится в Отделе информационной безопасности.

1.5 Подразделение Общества, ответственное за документ (разработка, пересмотр, оценка), – Отдел информационной безопасности.

1.6 Настоящий документ пересматривается 1 раз в 3 года или в случае существенных изменений. Целями пересмотра документа являются:

- обеспечение постоянной пригодности/применимости документа;
- обеспечение соответствия положений документа в ответ на изменения в деятельности Общества, применяемых информационных технологиях, законодательстве в области информационной безопасности;
- обеспечение результативности применения положений документа.

При пересмотре документа необходимо оценивать возможность улучшения его положений.

1.7 Требования настоящего документа обязательны для выполнения всеми работниками Общества.

2. ТЕРМИНЫ И СОКРАЩЕНИЯ

В настоящем документе применяются термины и сокращения, указанные в ISO/IEC 27000, а также следующие:

Наименование	Значение	Принятое сокращение
Общество, Организация	Общество с ограниченной ответственностью «Альтернативная генерирующая компания-1»	ООО «АГК-1»

3. НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ

ISO/IEC 27001:2013. Информационные технологии – Методы защиты - Системы менеджмента информационной безопасности – Требования.

4. ДЕКЛАРАЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1.1 Для обеспечения безопасности своей деятельности Общество считает важнейшей своей задачей обеспечение защиты активов и намерено обеспечить их надлежащую защиту, требует от всех работников четкого соблюдения норм и правил информационной безопасности.

4.1.2 В области информационной безопасности Общество руководствуется следующими принципами:

– вовлечение руководства в процессы управления информационной безопасностью;

– риск-ориентированный подход к управлению информационной безопасностью;

– законность принимаемых организационных и технических мер защиты;

– стремление к постоянному совершенствованию информационной безопасности Общества.

4.1.3 В качестве инструмента для эффективной реализации целей информационной безопасности в Обществе внедрена система управления информационной безопасностью (СУИБ), созданная в соответствии с требованиями международного стандарта ISO/IEC 27001:2013.

4.1.4 Признание необходимости системы менеджмента информационной безопасности является стратегическим решением Общества.

4.1.5 Руководство анализирует СУИБ, чтобы гарантировать ее постоянную пригодность, соответствие и результативность. Для проведения регулярного анализа и принятия решений по улучшению СУИБ в Обществе на постоянной основе действует коллегиальный орган – Комитет по информационной безопасности.

4.1.6 Руководство регулярно проводит совещания по вопросам обеспечения информационной безопасности с целью формирования четких указаний, осуществления контроля их выполнения, а также оказания административной поддержки в решении вопросов информационной безопасности.

4.1.7 Руководство и работники Общества понимают свои обязательства по защите активов и несут персональную ответственность за несоблюдение требований информационной безопасности. Указанные требования включаются в трудовые договоры и должностные инструкции работников, а также в договоры (соглашения) с контрагентами (внешними сторонами).

4.1.8 В Обществе регулярно проводятся мероприятия по оценке уровня информационной безопасности с привлечением независимых организаций, что позволяет поддерживать систему информационной безопасности Общества в

актуальном состоянии и обеспечивает независимое подтверждение высокого уровня информационной безопасности.

4.1.9 Основой эффективности информационной безопасности являются регулярно проводимые мероприятия по анализу и оценке рисков информационной безопасности.

4.1.10 Понимая, что наиболее критичным элементом безопасности Общества являются его работники, руководство поощряет заинтересованность и осведомленность работников в решении проблем и вопросов в области информационной безопасности.