задание: Изучить гос.стандарты менеджмента ИБ, проанализировать, что должна содержать политика безопасности.

ГОСТ Р ИСО/МЭК 27001

Политика безопасности, в контексте стандарта ГОСТ Р ИСО/МЭК 27001, является ключевым документом, определяющим общие принципы и цели информационной безопасности в организации. При изучении стандарта и анализе требований к политике безопасности, следует учитывать следующие основные элементы, которые должна содержать политика безопасности:

**Область действия:** политика безопасности должна четко определять область ее применения, включая информационные активы, процессы и системы, которые подлежат защите. Стандарт требует, чтобы политика безопасности соответствовала целям деятельности организации. Область действия политики безопасности должна охватывать все аспекты информационной безопасности в организации, включая:

* Информационные активы (данные, системы, сети)
* Физические активы (оборудование, носители информации)
* Нематериальные активы (репутация, интеллектуальная собственность)
* Персонал и его деятельность
* Процессы обработки, передачи и хранения информации
* Взаимодействие с внешними организациями и поставщиками
* Политика безопасности должна быть применима ко всем подразделениям и сотрудникам организации, а также к внешним сторонам, имеющим доступ к информационным активам

**Цели и задачи:** Политика безопасности должна содержать ясно сформулированные цели и задачи в области информационной безопасности, которые должны быть достигнуты.

**Ответственность:** Документ должен определить ответственность за соблюдение политики безопасности на всех уровнях организации, включая руководство и сотрудников.

**Конфиденциальность, целостность и доступность:** Стандарт определяет, что система менеджмента информационной безопасности должна сохранять конфиденциальность, целостность и доступность информации путем применения соответствующих процессов управления. Эти три аспекта информационной безопасности - конфиденциальность (сохранение конфиденциальности информации), целостность (сохранение целостности информации от несанкционированных изменений) и доступность (обеспечение доступности информации для авторизованных пользователей) - играют важную роль в обеспечении защиты информационных активов организации.

**Управление рисками**: Согласно ГОСТ Р ИСО/МЭК 27001, управление рисками информационной безопасности должно включать:

* Определение контекста организации, внутренних и внешних факторов, влияющих на ее способность достигать целей в области ИБ.
* Оценку рисков информационной безопасности, включая идентификацию, анализ и оценку рисков.
* Обработку рисков путем выбора соответствующих мер контроля или других действий для воздействия на риски.
* Оценку эффективности предпринятых мер по обработке рисков.
* Поддержание и сохранение информации задокументированной информации в качестве свидетельства результатов оценки рисков и обработки рисков.

Обучение и осведомленность: Политика безопасности должна включать требования по обучению сотрудников в области информационной безопасности и повышению их осведомленности.

Мониторинг и улучшение: Документ должен предусматривать механизмы мониторинга выполнения политики безопасности и процессы постоянного улучшения системы управления информационной безопасностью.

Анализируя ГОСТ Р ИСО/МЭК 27001, можно выделить эти ключевые аспекты, которые должна включать политика безопасности для обеспечения эффективной защиты информационных активов и соответствия стандарту.