

Содержание

1 Область применения	1
2 Нормативные ссылки.....	1
3 Термины и определения	1
3.1 Термины, относящиеся к риску информационной безопасности	1
3.2 Термины, относящиеся к менеджменту рисков информационной безопасности	3
4 Структура настоящего стандарта.....	5
5 Менеджмент рисков информационной безопасности	5
5.1 Процесс менеджмента рисков информационной безопасности	5
5.2 Циклы менеджмента рисков информационной безопасности	7
6 Установление контекста.....	7
6.1 Аспекты, касающиеся организации	7
6.2 Идентификация основных требований заинтересованных сторон	8
6.3 Применение оценки рисков	8
6.4 Установление и поддержание критериев рисков информационной безопасности	8
6.5 Выбор соответствующего метода.....	12
7 Процесс оценки рисков информационной безопасности.....	13
7.1 Общие положения	13
7.2 Идентификация рисков информационной безопасности	13
7.3 Анализ рисков информационной безопасности	16
7.4 Оценивание рисков информационной безопасности.....	18
8 Процесс обработки рисков информационной безопасности.....	19
8.1 Общие положения	19
8.2 Выбор подходящих вариантов обработки рисков информационной безопасности	19
8.3 Определение всех средств управления, необходимых для внедрения вариантов обработки рисков информационной безопасности	20
8.4 Сравнение определенных средств управления со средствами управления, указанными в ISO/IEC 27001:2022 (приложение A).....	23
8.5 Подготовка положения о применимости	23
8.6 План обработки рисков информационной безопасности	24
9 Операционная деятельность	26
9.1 Выполнение процесса оценки рисков информационной безопасности	26
9.2 Выполнение процесса обработки рисков информационной безопасности	27
10 Эффективное использование соответствующих процессов СМИБ	27
10.1 Контекст организации	27
10.2 Лидерство и приверженность	28
10.3 Обмен информацией и консультирование по рискам информационной безопасности	28
10.4 Документированная информация	29
10.5 Мониторинг и анализ.....	31
10.6 Анализ со стороны руководства	32

СТБ ISO/IEC 27005-2024

10.7 Корректирующие действия32

10.8 Постоянное улучшение33

Приложение А (справочное) Примеры методов поддержки процесса оценки риска34

Библиография54

Приложение ДА (справочное) Сведения о соответствии ссылочного международного стандарта государственному стандарту55