Приложение 1. Взаимосвязь между стандартами ISO/IEC 27001:2005, BS 7799-3:2006 и ISO/IEC 27005:2008

написано Александр Астахов | 11 июня, 2023

В таблице выделены курсивом те разделы стандартов, которые являются уникальными и взаимодополняющими.

Разделы из ISO/IEC 27001:2005	**Разделы из BS 7799-3:2006**	**Разделы из ISO/IEC 27005:2008**
	0. Введение0.1. Общие положения0.2. Процессный подход	Введение5. Исходные положения6. Обзор процесса управления рисками
1. Область действия	1. Область действия	1. Содержание
2. Нормативные ссылки	2. Нормативные ссылки	2. Нормативные ссылки
3. Термины и определения	3. Термины и определения	3. Термины и определения
	–	*4. Структура настоящего Международного стандарта*
4. Система управления информационной безопасностью	–	–
4.1. Общие требования	–	–

4.2. Создание и управление СУИБ	–	–
	4. Риски информационной безопасности в контексте организации	7. Определение контекста
	4.1. Область действия и политика системы управления информационной безопасностью	7.1. Общие соображения
	4.1.1. Деловая аргументация	–
	–	*7.2. Основные критерии*
	4.1.2. Область действия СУИБ	7.3. Область и границы
	4.1.3. Политика СУИБ	7.4. Организационная структура управления рисками информационной безопасности
	4.2. Подход/философия риска	–
4.2.1 Создание СУИБ	5. Оценка рисков	8. Оценка рисков информационной безопасности
	5.1. Процесс оценки рисков	8.1. Общее описание оценки рисков информационной безопасности

	5.2. Идентификация ресурсов5.3. Идентификация требований законодательства и бизнеса5.4. Определение ценности активов5.5. Идентификация и оценка угроз и уязвимостей5.6. Оценка угроз и уязвимостей5.7. Вычисление и оценивание рисков	8.2. Анализ рисков8.2.1. Идентификация рисков8.2.2. Расчет рисков
	5.7 Вычисление и оценивание рисков	8.3. Оценивание рисков
	5.8. Эксперт по оценке рисков	–
	6. Принятие решений по обработке и управлению рисками	9. Обработка рисков информационной безопасности
	6.1. Общие положения6.2. Принятие решения	9.1. Общее описание обработки рисков
	6.3. Уменьшение риска	9.2. Уменьшение риска
	6.4. Осознанное и объективное принятие риска	9.3. Сохранение риска
	6.5. Передача риска	9.4. Избежание риска
	6.6. Избежание риска	9.5. Передача риска

	6.4. Осознанное и объективное принятие риска	10. Принятие рисков информационной безопасности
	6.7. Остаточный риск	10. Принятие рисков информационной безопасности
	6.8. План обработки рисков	10. Принятие рисков информационной безопасности
4.2.2. Внедрение и эксплуатация СУИБ	6. Принятие решений по обработке и управлению рисками	
4.2.3. Мониторинг и анализ СУИБ	7. Непрерывная деятельность по управлению рисками	12. Мониторинг и пересмотр рисков информационной безопасности
	7.1. Непрерывное управление рисками безопасности	–
	7.2. Сопровождение и мониторинг	–
	7.4. Пересмотр и переоценка риска	12.1. Мониторинг и пересмотр факторов риска
4.2.4. Сопровождение и совершенствование СУИБ	7. Непрерывная деятельность по управлению рисками	12.2. Мониторинг, пересмотр и совершенствование управления рисками
4.3. Требования к документации	–	–
4.3.1. Общие положения	–	–

4.3.2. Управление документами	*7.6. Механизмы контроля документации*	–
4.3.3. Управление записями	–	–
5. Ответственность руководства	–	–
5.1. Приверженность руководства	–	–
5.2. Управление ресурсами	–	–
5.2.1. Предоставление ресурсов	–	–
5.2.2. Обучение, осведомленность и компетенция	–	–
6. Внутренние аудиты СУИБ	*7.5. Аудиты*	–
7. Анализ СУИБ руководством	*7.3. Анализ со стороны руководства*	–
7.1. Общие положения	–	–
7.2. Входные данные для анализа	–	–
7.3. Выходные данные анализа	–	–
8. Совершенствование СУИБ	7. Непрерывная деятельность по управлению рисками	12.1. Мониторинг и пересмотр факторов риска

8.1. Непрерывное совершенствование	–	–
8.2. Корректирующие меры	*7.7. Корректирующие и превентивные меры*	–
8.3. Превентивные меры	*7.7. Корректирующие и превентивные меры*	–
	7.8. Отчеты и коммуникации7.8.1. План коммуникаций7.8.2. Обратная связь и вовлеченность	11. Коммуникация рисков информационной безопасности
	7.9. Менеджер рисков безопасности	–
	–	*Приложение А. Определение областидействия и границ процесса управления рисками информационной безопасности*
	Приложение А. Примеры соответствия требованиям законодательства и нормативной базы	–
	Приложение В. Риски информационной безопасности и риски организации	–

	Приложение C. Примеры ресурсов, угроз, уязвимостей и методов оценки рисков	Приложение B. Идентификация и оценка активов и оценка воздействияПриложение C. Примеры типичных угрозПриложение D. Уязвимости и методы их оценки
	Приложение D. Инструменты управления рисками	
		Приложение E. Подходы к оценке рисков информационной безопасности
		Приложение F. Ограничения, оказывающие влияние на уменьшение рисков