

Содержание

1 Область применения	1
2 Нормативные ссылки.....	1
3 Термины и определения	1
3.1 Термины и определения.....	1
3.2 Сокращения	4
4 Структура стандарта	5
4.1 Разделы	5
4.2 Темы и атрибуты	6
4.3 Описание средств управления	7
5 Организационные средства управления	7
5.1 Политики в области информационной безопасности.....	7
5.2 Роли и обязанности в области информационной безопасности	9
5.3 Разделение обязательств	9
5.4 Обязанности руководства/менеджмента	10
5.5 Взаимодействие с органами власти.....	11
5.6 Контакт с группами, имеющими особые интересы	11
5.7 Аналитические исследования угроз	12
5.8 Информационная безопасность в менеджменте проектов.....	13
5.9 Инвентаризация информации и других связанных с ней активов.....	15
5.10 Приемлемое использование информации и других связанных с ней активов	16
5.11 Возврат активов	17
5.12 Классификация информации	18
5.13 Маркировка (разметка) информации	19
5.14 Передача информации.....	20
5.15 Управление доступом	22
5.16 Менеджмент идентификации	23
5.17 Информация для аутентификации	24
5.18 Права доступа	26
5.19 Информационная безопасность в отношениях с поставщиками	27
5.20 Обеспечение информационной безопасности в рамках соглашений с поставщиками	29
5.21 Менеджмент информационной безопасности в цепи поставок информационно-коммуникационных технологий (ICT).....	30
5.22 Мониторинг, анализ и менеджмент изменений услуг поставщиков	32
5.23 Информационная безопасность при использовании облачных услуг	33
5.24 Планирование и подготовка к менеджменту инцидента информационной безопасности.....	35
5.25 Оценка событий в области информационной безопасности и принятие решений	37
5.26 Реагирование на инциденты информационной безопасности	37
5.27 Извлечение уроков из инцидентов информационной безопасности	38
5.28 Сбор свидетельств.....	38
5.29 Информационная безопасность во время сбоев	39

СТБ ISO/IEC 27002-2024

5.30	Готовность ICT к обеспечению непрерывности бизнеса	40
5.31	Правовые, законодательные, нормативные и договорные требования.....	41
5.32	Права интеллектуальной собственности.....	42
5.33	Защита записей.....	43
5.34	Безопасность частной жизни и защита персональных данных (персональной идентифицирующей информации (PII))	44
5.35	Независимый анализ информационной безопасности	45
5.36	Соблюдение политик, правил и стандартов в области информационной безопасности	46
5.37	Документированные процедуры операционной деятельности	47
6	Средства управления, связанные с людьми.....	48
6.1	Отбор.....	48
6.2	Сроки и условия найма.....	49
6.3	Осведомленность, обучение и подготовка в области информационной безопасности	49
6.4	Дисциплинарный процесс	51
6.5	Обязанности после увольнения или смены места работы	52
6.6	Соглашения о конфиденциальности или неразглашении	52
6.7	Удаленная работа.....	53
6.8	Отчетность о событиях информационной безопасности.....	55
7	Физические средства управления.....	55
7.1	Периметры физической безопасности.....	55
7.2	Физический доступ	56
7.3	Безопасность офисов, помещений и устройств	58
7.4	Мониторинг физической безопасности.....	58
7.5	Защита от физических и экологических угроз	59
7.6	Работа в охраняемых зонах.....	60
7.7	Чистый стол и чистый экран	60
7.8	Размещение и защита оборудования	61
7.9	Безопасность активов вне территориальных пределов.....	62
7.10	Носители информации	63
7.11	Службы обеспечения.....	64
7.12	Безопасность кабельных сетей	65
7.13	Техническое обслуживание оборудования	65
7.14	Безопасная утилизация или повторное использование оборудования.....	66
8	Технологические средства управления.....	67
8.1	Устройства конечного пользователя.....	67
8.2	Права привилегированного доступа	69
8.3	Ограничение доступа к информации	70
8.4	Доступ к исходному коду	72
8.5	Безопасная аутентификация	73
8.6	Менеджмент мощности	74
8.7	Защита от вредоносных программ	75
8.8	Менеджмент технических уязвимостей	76

8.9 Менеджмент конфигурации.....	79
8.10 Удаление информации.....	81
8.11 Маскирование данных.....	82
8.12 Предупреждение утечки данных.....	83
8.13 Резервное копирование информации.....	84
8.14 Избыточность средств обработки информации.....	85
8.15 Логирование (ведение журналов).....	86
8.16 Мониторинг деятельности.....	88
8.17 Синхронизация часов.....	90
8.18 Использование привилегированных программных утилит.....	91
8.19 Установка программного обеспечения в операционные системы.....	92
8.20 Безопасность сетей.....	93
8.21 Безопасность сетевых услуг.....	94
8.22 Разделение в сетях.....	95
8.23 Веб-фильтрация.....	95
8.24 Использование криптографии.....	96
8.25 Безопасный жизненный цикл разработки.....	98
8.26 Требования к безопасности приложений.....	99
8.27 Архитектура и принципы проектирования безопасных систем.....	100
8.28 Безопасное кодирование.....	102
8.29 Тестирование безопасности при разработке и приемке.....	104
8.30 Аутсорсинговая разработка.....	105
8.31 Разделение сред разработки, тестирования и производственного функционирования (продакшена).....	106
8.32 Менеджмент изменений.....	107
8.33 Тестовая информация.....	108
8.34 Защита информационных систем при аудиторском тестировании.....	109
Приложение А (справочное) Использование атрибутов.....	110
Приложение В (справочное) Соответствие между ISO/IEC 27002:2022 (настоящего стандарта) и ISO/IEC 27002:2013.....	122
Библиография.....	129