

Содержание:

СПИСОК РИСУНКОВ.....	16
СПИСОК ТАБЛИЦ	16
1 ВВЕДЕНИЕ.....	19
1.1 МАТЕРИАЛЫ, ИСПОЛЬЗОВАННЫЕ ПРИ НАПИСАНИИ МОНОГРАФИИ	21
1.1.1 Юридические правила.....	21
1.1.2 Международные стандарты.....	21
1.1.3 Публикации и монографии.....	21
1.1.4 Статьи семинаров и конференций.....	21
1.1.5 Методики фирм и исследовательские отчёты	22
1.2 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	27
2 ВЗАИМООТНОШЕНИЯ МЕЖДУ ЭЛЕМЕНТАМИ БЕЗОПАСНОСТИ	33
2.1 АКТИВЫ	35
2.1.1 Вычисление выведенных величин активов	36
2.2 УГРОЗЫ	37
2.2.1 Самые частые угрозы для информационной системы	42
2.2.2 Угроза конфиденциальности	43
2.2.3 Угрозы доступности	46
2.2.4 Угроза для целостности.....	54
2.2.5 Угрозы для компьютерной сети.....	60
2.3 УЯЗВИМОСТЬ	63
2.3.1 Примеры уязвимости избранных типов активов	63
2.4 ПОСЛЕДСТВИЯ	68
2.4.1 Примеры последствий	68
2.5 РИСК.....	71
2.5.1 Остаточный риск	71
2.6 МЕРЫ БЕЗОПАСНОСТИ	72
2.6.1 Обще применяемые меры безопасности.....	75
2.6.2 Примеры мер безопасности для компьютеров.....	76
2.6.3 Примеры мер безопасности для серверов.....	78
2.6.4 Примеры мер безопасности для активных элементов сети	80
2.6.5 Примеры мер безопасности для окружающей территории	83
2.6.6 Примеры мер безопасности для здания	85
2.6.7 Примеры мер безопасности для канцелярии	86
2.6.8 Примеры мер безопасности для защиты от инцидентов связанных с безопасностью	89
2.6.9 Примеры мер антивирусной защиты	90
2.6.10 Примеры мер безопасности для сохранения непрерывной деятельности	91
2.6.11 Тип воздействия и уровень мер безопасности	93
2.7 ОГРАНИЧЕНИЯ	97
3 АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	99
3.1 АНАЛИЗ РИСКОВ	99
3.1.1 Стратегия анализа рисков.....	99
3.1.2 Основной подход.....	101
3.1.3 Неформальный подход.....	102
3.1.4 Детальный анализ рисков.....	103
3.1.5 Комбинированный подход	104
3.2 УПРАВЛЕНИЕ РИСКАМИ	105
3.2.1 Защитные меры безопасности.....	108
3.2.6 Выявление остаточных рисков.....	108
4 МЕТОДИКА АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ	109
4.1 ПОНИМАНИЕ МЕТОДИКИ АНАЛИЗА И УПРАВЛЕНИЯ РИСКАМИ	109
4.2 МАТРИЦА С ЗАДААННЫМИ ВЕЛИЧИНАМИ	111
4.3 УПОРЯДОЧЕНИЕ УГРОЗ, СОГЛАСНО УРОВНЮ РИСКА.	115
4.4 ОПРЕДЕЛЕНИЕ ЧАСТОТЫ ВОЗНИКНОВЕНИЯ РИСКОВ И ВЕЛИЧИНЫ ВОЗМОЖНОГО УЩЕРБА	116
4.5 РАЗЛИЧИЕ МЕЖДУ ДОПУСТИМЫМИ И НЕДОПУСТИМЫМИ РИСКАМИ	118
4.6 РЕЗЮМЕ К ПРИВЕДЁННЫМ МЕТОДИКАМ.....	119

5	СТАНДАРТ ISO/IEC 27005	121
5.1	ОБЩИЕ ТРЕБОВАНИЯ	123
5.2	СТРУКТУРА ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	123
5.3	РАЗРАБОТКА ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	125
5.3.1	<i>Подход к управлению рисками</i>	125
5.3.2	<i>Организационные предпосылки управления рисками</i>	127
5.4	ОЦЕНКА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	127
5.4.1	<i>Методика оценки рисков</i>	127
5.4.1.1	Качественная оценка риска	128
5.4.1.2	Количественная оценка риска	128
5.5	ЗАЩИТА РИСКА ИНФОРМАЦИОННОЙ СИСТЕМЫ	129
5.6	ПРИНЯТИЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	130
5.7	ОПОВЕЩЕНИЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	130
5.8	МОНИТОРИНГ И ИЗУЧЕНИЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	131
5.9	РЕЦЕНЗИЯ ВКЛАДА НОВОЙ НОРМЫ	131
6	ИНСТРУМЕНТЫ, ПОМОГАЮЩИЕ В ПРОВЕДЕНИИ АНАЛИЗОВ РИСКОВ	133
6.1	ENISA – ПЕРЕЧЕНЬ ИНСТРУМЕНТОВ	133
6.2	CALLIO SECURA 17799	138
6.3	CRAMM	139
6.4	COBRA	140
6.5	RISKWATCH	142
7	ВЗАИМООТНОШЕНИЯ АНАЛИЗА РИСКОВ ИС И СУИБ	143
8	АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ СОГЛАСНО СТАНДАРТУ ISO/IEC 27001	145
8.1	ТРЕБОВАНИЯ К АНАЛИЗУ И УПРАВЛЕНИЮ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	145
8.2	ПОДВЕДЕНИЕ ИТОГОВ И ИНТЕРПРЕТАЦИЯ ТРЕБОВАНИЙ	150
8.3	ОПРЕДЕЛЕНИЕ КРИТЕРИЕВ ДЛЯ АКЦЕПТАЦИИ ОСТАТОЧНЫХ РИСКОВ	162
8.4	ИЗУЧЕНИЕ И ОЦЕНКА ОСТАТОЧНЫХ РИСКОВ	163
8.4.1	<i>Входные остаточные риски</i>	164
8.4.2	<i>Требуемые остаточные риски</i>	164
8.4.3	<i>Реальные остаточные риски после введения мер безопасности</i>	168
8.4.4	<i>Изучение остаточных рисков</i>	169
8.4.5	<i>Остаточные риски как составная часть операционных и стратегических рисков организации</i>	177
8.5	ПОВТОРНЫЙ АНАЛИЗ РИСКОВ С УЧЁТОМ ВЛИЯНИЯ МЕР БЕЗОПАСНОСТИ РЕАЛИЗОВАННЫХ НА ПРАКТИКЕ	179
8.6	ИЗМЕРЕНИЕ ЭФФЕКТИВНОСТИ И ДЕЙСТВИЯ МЕР	179
8.6.1	<i>Измерение эффективности и действия мер посредством достигаемых остаточных рисков</i>	179
8.6.2	<i>Измерение эффективности и функционирования мер безопасности на практике</i>	180
8.7	ИЗМЕРЕНИЕ ПРОЦЕССОВ СУИБ	180
8.8	ИЗМЕРЕНИЕ ЦЕЛЕЙ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ	181
9	АНАЛИЗ И УПРАВЛЕНИЕ РИСКАМИ СОГЛАСНО СТАНДАРТАМ БЕЗОПАСНОСТИ ДЛЯ ISVS	183
9.1	ИЗБРАННЫЕ ПРАВОВЫЕ НОРМЫ СР ДЛЯ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ	183
9.1.1	<i>Закон № 575/С.з. об организации деятельности правительства и организации центрального государственного управления</i>	184
9.1.2	<i>Закон № 275/2006 С.з. об информационных системах общественного управления</i>	185
9.1.3	<i>Указ МФ СР о стандартах для ISVS</i>	188
9.1.4	<i>Закон № 211/ 2000 С.з. о свободном доступе к информации и об изменении и дополнении некоторых законов</i>	192
9.1.5	<i>Закон № 300/2000 С.з. Уголовного права</i>	194
9.1.6	<i>Подведение итогов приведённых правовых норм</i>	198
9.2	ТРЕБОВАНИЯ К АНАЛИЗУ И УПРАВЛЕНИЮ РИСКАМИ КОМПЕТЕНТНЫХ ЛИЦ	200
9.3	ПОДВЕДЕНИЕ ИТОГОВ И ИНТЕРПРЕТАЦИЯ ТРЕБОВАНИЙ	200
9.4	СРАВНЕНИЕ ТРЕБОВАНИЙ К АНАЛИЗУ И УПРАВЛЕНИЮ РИСКАМИ СОГЛАСНО СТАНДАРТАМ БЕЗОПАСНОСТИ ДЛЯ ISVS И СТАНДАРТА ISO/IEC 27001	204

10	ГАРАНТИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	221
10.1	ТРЕБУЕМАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	221
10.2	ПОЛУЧЕНИЕ И ПРОВЕРКА ГАРАНТИЙ	224
11	ЗАКЛЮЧЕНИЕ	231
12	ЛИТЕРАТУРА.....	233
12.1	МОНОГРАФИИ И ПУБЛИКАЦИИ	233
12.2	СТАТЬИ.....	235
12.3	ФИРМЕННЫЕ МЕТОДИКИ	236
12.4	ЗАКОНЫ И ПОСТАНОВЛЕНИЯ	237
12.5	ISO НОРМЫ.....	238
12.6	ISO/IEC НОРМЫ	238
12.7	STN НОРМЫ.....	239
13	РЕЗЮМЕ.....	241