

Содержание

| | |
|--|----|
| ВВЕДЕНИЕ..... | 3 |
| Используемые сокращения..... | 7 |
| Глава 1. ПОНЯТИЕ БЕЗОПАСНОСТИ..... | 8 |
| 1.1. Общие положения..... | 8 |
| 1.2. Безопасность в документах федерального уровня..... | 9 |
| 1.3. Понятие объекта безопасности (защищаемого объекта)..... | 10 |
| 1.4. Общее определение безопасности защищаемого объекта..... | 12 |
| 1.5. О понятии «кибербезопасность»..... | 17 |
| Глава 2. ПРОБЛЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОГО ОБЪЕКТА..... | 20 |
| 2.1. Основные составляющие проблемы..... | 20 |
| 2.2. Нормативно-правовая составляющая проблемы..... | 20 |
| 2.3. Организационная составляющая проблемы..... | 23 |
| 2.4. Экономическая составляющая проблемы..... | 27 |
| 2.5. Научно-методическая и научно-техническая составляющие проблемы..... | 29 |
| Глава 3. НАУЧНО-МЕТОДИЧЕСКИЙ АППАРАТ ИССЛЕДОВАНИЙ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОГО ОБЪЕКТА..... | 32 |
| 3.1. Понятие моделей, их классификация и требования к ним..... | 33 |
| 3.2. Символическое описание процессов негативных воздействий на объект безопасности..... | 37 |
| 3.3. Понятие имитационной моделирующей системы процессов негативных воздействий на объект безопасности..... | 38 |
| 3.4. Основные принципы построения имитационной моделирующей системы..... | 40 |
| 3.5. Структурная схема имитационной моделирующей системы..... | 41 |
| 3.6. Вопросы реализации имитационной моделирующей системы... | 42 |
| 3.7. Варианты реализации имитационной моделирующей системы. | 44 |
| 3.8. Понятие методики количественной оценки характеристик системы обеспечения безопасности..... | 46 |
| 3.9. Структурная схема методики..... | 47 |
| 3.10. Вопросы реализации методики..... | 48 |
| 3.11. Экспертные системы исследования и управления обеспечением безопасности защищаемого объекта..... | 55 |
| Глава 4. НЕГАТИВНЫЕ ВОЗДЕЙСТВИЯ НА ОБЪЕКТ БЕЗОПАСНОСТИ..... | 57 |
| 4.1. Понятие негативного воздействия..... | 57 |

| | |
|---|-----|
| 4.2. Общая схема процесса негативных воздействий на объект безопасности..... | 57 |
| 4.3. Основные особенности процесса реализации негативных воздействий на объект безопасности | 59 |
| 4.4. Природа и содержание негативных воздействий на объект безопасности..... | 61 |
| Глава 5. УЩЕРБ ОБЪЕКТАМ БЕЗОПАСНОСТИ | 71 |
| 5.1. Понятие ущерба..... | 71 |
| 5.2. Виды ущерба | 71 |
| 5.3. Масштабы ущерба..... | 74 |
| 5.4. Ранжирование масштабов ущерба | 77 |
| Глава 6. УГРОЗА ОБЪЕКТУ БЕЗОПАСНОСТИ И ЕЕ КОЛИЧЕСТВЕННАЯ ОЦЕНКА | 79 |
| 6.1. Понятие угрозы | 79 |
| 6.2. Количественный показатель угрозы..... | 81 |
| 6.3. Формальное определение количественного показателя угрозы .. | 85 |
| 6.4. Оценка веса факторов угрозы | 89 |
| 6.5. Методика количественной оценки угрозы..... | 90 |
| 6.6. Прикладное использование количественного показателя угрозы..... | 96 |
| Глава 7. УЯЗВИМОСТЬ ОБЪЕКТА БЕЗОПАСНОСТИ И ЕЕ КОЛИЧЕСТВЕННАЯ ОЦЕНКА | 98 |
| 7.1. Понятие уязвимости..... | 98 |
| 7.2. Количественный показатель уязвимости | 102 |
| 7.3. Методика количественной оценки уязвимости | 105 |
| Глава 8. РИСК ПОЛУЧЕНИЯ УЩЕРБА ОБЪЕКТОМ БЕЗОПАСНОСТИ И ЕГО КОЛИЧЕСТВЕННАЯ ОЦЕНКА .. | 116 |
| 8.1. Понятие риска..... | 116 |
| 8.2. О содержании словосочетания «управление рисками» | 117 |
| 8.3. Количественный показатель риска | 119 |
| 8.4. Методика количественной оценки риска..... | 120 |
| Глава 9. СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОГО ОБЪЕКТА..... | 124 |
| 9.1. Понятие обеспечения безопасности защищаемго объекта..... | 124 |
| 9.2. Понятие комплексной системы обеспечения безопасности..... | 125 |
| 9.3. Необходимые условия функционирования комплексной системы обеспечения безопасности | 129 |
| 9.4. Основные принципы построения комплексной системы обеспечения безопасности..... | 130 |

| | |
|--|-----|
| 9.5. Общие требования к комплексной системе обеспечения безопасности | 131 |
| Глава 10. ЭФФЕКТИВНОСТЬ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОГО ОБЪЕКТА И ЕЕ КОЛИЧЕСТВЕННАЯ ОЦЕНКА | 132 |
| 10.1. Понятия качества и эффективности системы обеспечения безопасности защищаемого объекта | 132 |
| 10.2. Содержание показателей эффективности системы обеспечения безопасности защищаемого объекта | 135 |
| 10.3. Количественный показатель эффективности нейтрализации угроз безопасности защищаемого объекта | 136 |
| 10.4. Количественный показатель эффективности недопущения реализации негативных воздействий на объект безопасности | 138 |
| 10.5. Количественный показатель эффективности защиты объекта безопасности от получения недопустимого ущерба..... | 138 |
| 10.6. Методика количественной оценки эффективности системы обеспечения безопасности защищаемого объекта..... | 139 |
| 10.7. Необходимые условия повышения эффективности систем обеспечения безопасности защищаемого объекта | 145 |
| Глава 11. РАЦИОНАЛЬНОСТЬ СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОГО ОБЪЕКТА | 147 |
| 11.1. Понятие рациональной системы обеспечения безопасности защищаемого объекта | 147 |
| 11.2. Содержание задачи выбора рациональной системы обеспечения безопасности защищаемого объекта | 147 |
| 11.3. Формальная постановка задачи выбора рациональной системы обеспечения безопасности защищаемого объекта..... | 149 |
| Глава 12. КАТЕГОРИРОВАНИЕ ОБЪЕКТОВ БЕЗОПАСНОСТИ | 151 |
| 12.1. Понятия «категория» и «категорирование» объекта безопасности..... | 151 |
| 12.2. Цель категорирования объектов безопасности | 154 |
| 12.3. Отрицательные последствия ущерба для объекта безопасности..... | 154 |
| 12.4. Количественное содержание категории объекта безопасности..... | 155 |
| 12.5. Определение категории объекта безопасности | 157 |
| Глава 13. УПРАВЛЕНИЕ ОБЕСПЕЧЕНИЕМ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОГО ОБЪЕКТА..... | 163 |
| 13.1. Понятие управления обеспечением безопасности защищаемого объекта | 163 |

| | |
|---|-----|
| 13.2. Информационно-телекоммуникационная система как важнейший элемент автоматизированной системы управления обеспечением безопасности защищаемого объекта..... | 165 |
| 13.3. Вопросы обоснования рационального варианта информационно-телекоммуникационной системы защищаемого объекта..... | 169 |
| Глава 14. ЭФФЕКТИВНОСТЬ УПРАВЛЕНИЯ ОБЕСПЕЧЕНИЕМ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОГО ОБЪЕКТА | 172 |
| 14.1. Общий подход к определению эффективности управления обеспечением безопасности защищаемого объекта..... | 172 |
| 14.2. Определение показателя эффективности АСУ обеспечением безопасности защищаемого объекта..... | 172 |
| 14.3. Формальное описание показателя эффективности АСУ обеспечением безопасности защищаемого объекта..... | 174 |
| 14.4. Практическое исследование эффективности АСУ обеспечением безопасности защищаемого объекта..... | 175 |
| 14.5. Оптимизация характеристик АСУ обеспечением безопасности защищаемого объекта | 177 |
| Глава 15. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЗАЩИЩАЕМОГО ОБЪЕКТА..... | 179 |
| 15.1. Общие положения | 179 |
| 15.2. Проблемные вопросы обеспечения информационной безопасности защищаемого объекта | 182 |
| 15.3. Угрозы информационной безопасности..... | 190 |
| 15.4. Уровни информационной безопасности | 195 |
| 15.5. Несанкционированный доступ к информационным ресурсам объекта безопасности | 200 |
| Глава 16. ОБНАРУЖЕНИЕ НЕГАТИВНЫХ ИНФОРМАЦИОННЫХ ВОЗДЕЙСТВИЙ НА ОБЪЕКТ БЕЗОПАСНОСТИ..... | 204 |
| 16.1. Общие положения | 204 |
| 16.2. Информационно-технологические атаки на информационные системы объекта безопасности | 206 |
| 16.3. Назначение и функции систем обнаружения атак на информационные системы объекта безопасности | 212 |
| 16.4. Методы обнаружения атак на информационные системы объекта безопасности..... | 215 |
| 16.5. Многоагентная технология защиты информации | 217 |
| Глава 17. ПРОТИВОДЕЙСТВИЕ НЕГАТИВНЫМ ИНФОРМАЦИОННЫМ ВОЗДЕЙСТВИЯМ НА ОБЪЕКТ БЕЗОПАСНОСТИ | 225 |
| 17.1. Общие положения | 225 |

| | |
|---|------------|
| 17.2. Противодействие негативным информационным воздействиям традиционными способами | 226 |
| 17.3. Активное противодействие негативным информационным воздействиям | 227 |
| 17.4. Ложные информационные системы | 229 |
| 17.5. Активное противодействие нарушителю посредством специальным образом подготовленной информации | 233 |
| 17.6. «Приманки» как средство анализа информационного нарушителя | 236 |
| Глава 18. КОЛИЧЕСТВЕННАЯ ОЦЕНКА СОСТОЯНИЯ И ЭФФЕКТИВНОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ЗАЩИЩАЕМОГО ОБЪЕКТА | 239 |
| 18.1. Понятие состояния и эффективности обеспечения безопасности информации защищаемого объекта | 239 |
| 18.2. Количественные показатели уязвимости и риска применительно к задаче обеспечения безопасности информации защищаемого объекта | 240 |
| 18.3. Количественные показатели состояния безопасности информации | 241 |
| 18.4. Количественные показатели эффективности обеспечения безопасности информации | 242 |
| 18.5. Методическая схема проведения количественных оценок показателей состояния и эффективности обеспечения безопасности информации | 243 |
| Глава 19. ПОДГОТОВКА ПЕРСОНАЛА СИСТЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОГО ОБЪЕКТА | 251 |
| 19.1. Человеческий фактор в обеспечении безопасности защищаемого объекта | 251 |
| 19.2. Нормативные основы подготовки персонала систем обеспечения безопасности защищаемого объекта | 252 |
| 19.3. Практические вопросы подготовки персонала систем обеспечения безопасности защищаемого объекта | 254 |
| Глава 20. ТЕХНИЧЕСКИЕ СРЕДСТВА, СИСТЕМЫ И ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗАЩИЩАЕМОГО ОБЪЕКТА | 262 |
| 20.1. Общие положения | 262 |
| 20.2. Системы контроля и управления доступом | 263 |
| 20.3. Технические средства досмотра и поиска | 269 |
| 20.4. Системы охранной и охранно-пожарной сигнализации | 273 |
| 20.5. Системы телевизионного наблюдения | 275 |

| | |
|---|-----|
| 20.6. Системы связи и оповещения | 278 |
| 20.7. Инженерно-технические средства защиты объекта безопасности..... | 281 |
| 20.8. Профайлинг как технология выявления лиц, имеющих противоправные намерения | 282 |
| 20.9. Технология дистанционного выявления потенциально опасных лиц с использованием виброизображения..... | 288 |
| 20.10. Эффективность технических средств, систем и технологий обеспечения безопасности защищаемого объекта и ее количественная оценка | 290 |
| Глава 21. ТЕРРОРИЗМ И БОРЬБА С НИМ | 292 |
| 21.1. Понятие терроризма..... | 292 |
| 21.2. Некоторые характеристики и особенности террористической деятельности | 294 |
| 21.3. Террористические акты с использованием террористов-смертников..... | 296 |
| 21.4. Общие рекомендации по поведению персонала систем обеспечения безопасности при обнаружении террориста-смертника..... | 301 |
| 21.5. Средства, используемые в диверсионно-террористических целях | 302 |
| 21.6. Выявление диверсионно-террористических средств | 305 |
| 21.7. Формирование и развитие у персонала СОБ практических навыков по выявлению потенциально опасных лиц..... | 307 |
| ЗАКЛЮЧЕНИЕ | 310 |
| Литература | 311 |