

НАУЧНАЯ МЫСЛЬ



А.В. Бабаш, Е.К. Баранова

АКТУАЛЬНЫЕ ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ


ИНФРА-М

РИОР

НАУКА

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	3
ГЛАВА 1. ВОПРОСЫ УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	6
1.1. Методики анализа и оценки рисков информационной безопасности	6
1.2. Процедура применения методологии анализа рисков OCTAVE в соответствии с ГОСТом Р ИСО/МЭК 27005-2010.....	16
1.3. Особенности подхода к анализу рисков информационной безопасности для малого и среднего бизнеса	21
1.4. Анализ безопасности информационных систем методом тестирования на проникновение	29
Литература к главе 1.....	37
ГЛАВА 2. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ОСОБЕННОСТИ ОЦЕНКИ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ	39
2.1. Особенности управления инцидентами информационной безопасности	39
2.2. Современные ddos-атаки как угроза для бизнеса в интернете	51
2.3. Особенности оценки экономической эффективности системы защиты информации	60
Литература к главе 2.....	74
ГЛАВА 3. ИЗБРАННЫЕ АСПЕКТЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ	75
3.1. Обобщенная модель шифра.....	75
3.2. Расстояния единственности шифра	81
3.3. О периоде функционирования генератора псевдослучайных чисел IA (Indirection Addition)	92
3.4. Определение входного слова векторного перестановочного автомата по множеству пар начальных и заключительных состояний с помощью вероятностной модели Мицуру Мацуи (Mitsuru Matsui).....	101
3.5. Атака Монте-Карло с использованием слабых ключей на шифр одноразового блокнота	115
3.6. Атаки на шифр случайного гаммирования	124
3.6.1. Обоснование недешифруемости ШСГ	124
3.6.2. Обоснование дешифруемости ШСГ	127
3.6.3. Что же понимать под дешифруемостью и недешифруемостью ШСГ	135
3.6.4. Обсуждение результатов.....	138
Список источников к разделу 3.6	138
3.7. Периоды выходных последовательностей автоматов	141
3.7.1. Автоматы с L-потерей информации о выходе	141
3.7.2. Критерий внешней периодичности автомата.....	143
3.7.3. Автоматы с L-потерей информации	146
3.7.4. Периодически внешне наследственные автоматы	148
3.7.5. Критерий внешне наследственности автомата	157
3.7.6. Краткий обзор результатов по данной теме. Обозначения, основные понятия, вспомогательные результаты.....	159
3.7.7. Периоды выходных последовательностей автомата без внешне автономных состояний при входной периодической последовательности заданной полноты	162

3.7.8. Периоды выходных последовательностей линейного векторного автомата при заданной входной периодической последовательности	168
3.7.9. Период внешнего функционирования автономного последовательного соединения автоматов	173
3.7.10. Периоды выходных последовательностей перестановочного автомата без потери информации при заданных периодических входных последовательностях	175
3.7.11. Периоды выходных последовательностей последовательного соединения автономного автомата с перестановочным автоматом без потери информации	181
3.7.12. Необходимость построения автоматов с гарантированными периодами выходных последовательностей	184
3.7.13. Кодировущее устройство с конечной памятью	184
3.7.14. Полноцикловый автомат	187
3.7.15. Обратимый автомат	194
3.7.16. Обобщенный узел выборки	195
3.7.17. Основные обозначения и понятие подпериода последовательности	198
3.7.18. Автомат Медведева	199
3.7.19. Кодировущее устройство с конечной памятью (проходная линия задержки с функцией усложнения)	203
3.7.20. Обратимые автоматы	206
Список источников к разделу 3.7	207
Литература к главе 3	208
ЗАКЛЮЧЕНИЕ	209
СПИСОК ЛИТЕРАТУРЫ	210