



По-настоящему безопасной можно считать лишь систему, которая выключена, замурована в бетонный корпус, заперта в помещении со свинцовыми стенами и охраняется вооруженным караулом, однако и в этом случае сомнения не оставят меня.

Ю. Спаффорд

ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

М. А. Борисов, И. В. Заводцев, И. В. Чижов

ОСНОВЫ ПРОГРАММНО- АППАРАТНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

**ИЗДАНИЕ ПЯТОЕ,
ПЕРЕРАБОТАННОЕ
И СУЩЕСТВЕННО ДОПОЛНЕННОЕ**



URSS

Оглавление

ВВЕДЕНИЕ	8
ГЛАВА 1. НЕОБХОДИМОСТЬ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ.....	13
1.1. Актуальность проблемы защиты информации	13
1.1.1. Роль человеческого фактора в обеспечении защиты информации в автоматизированных системах	13
1.1.2. Понятие информационной войны	19
1.1.3. Основные понятия и термины	26
1.1.4. Особенности современных автоматизированных (информационных) систем	30
1.1.5. Особенности информационных отношений между субъектами	36
1.1.6. Классификация методов и средств защиты информации от несанкционированного доступа	38
1.1.7. Механизмы защиты информации от несанкционированного доступа	41
1.2. Требования к системам и средствам защиты информации от несанкционированного доступа	43
1.2.1. Государственные требования к построению систем защиты информации	44
1.2.2. Особые требования к криптографическим средствам систем защиты информации от несанкционированного доступа	48
1.2.3. Классификация автоматизированных систем и требования по защите информации	52
1.2.4. Показатели защищённости средств вычислительной техники по защите информации от несанкционированного доступа	55
1.2.5. Соответствие классов защищённости АС различным уровням конфиденциальности	57
1.2.6. Требования к защищённости государственных информационных систем, обрабатывающих информацию, не составляющую государственную тайну	58
1.2.7. Классификация информационных систем персональных данных	59
1.2.8. Новое поколение нормативно-технических документов по безопасности информации	61

4 1.3. Разработка модели разграничения доступа к информации	69
1.3.1. Политика безопасности.....	71
1.3.2. Состав и содержание документов политики безопасности.....	73
1.3.3. Определение перечня защищаемых ресурсов и их критичности	78
1.3.4. Определение категорий персонала и программно-аппаратных средств, на которые распространяется разработанная политика безопасности	83
1.3.5. Определение угроз безопасности информации.....	84
1.3.6. Принципы построения системы защиты информации	94
1.3.7. Формирование требований к построению системы защиты информации и порядок подбора соответствующих программно-аппаратных средств	100
1.3.8. Определение угроз безопасности для автоматизированной системы и выбор средств защиты информации.....	104
ГЛАВА 2. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ	112
2.1. Системная классификация средств защиты информации.....	112
2.2. Аппаратные средства защиты информации	121
2.3. Основные принципы функционирования аппаратных средств защиты информации.....	123
2.4. Программные средства защиты информации	125
2.5. Основные принципы функционирования программных средств защиты	127
2.6. Угрозы перевода программной системы защиты в пассивное состояние	130
2.7. Кибергигиена — основа личной безопасности человека в информационном пространстве	132
ГЛАВА 3. УПРАВЛЕНИЕ ДОСТУПОМ В КОМПЬЮТЕРНЫХ СИСТЕМАХ....	136
3.1. Идентификация и аутентификация субъектов доступа и объектов доступа в компьютерных системах	136
3.1.1. Процедуры идентификации и аутентификации в компьютерных системах	136
3.1.2. Методы аутентификации в компьютерных системах	140
3.1.3. Классификация задач по назначению защищаемого объекта	147
3.1.4. Идентифицирующая информация. Протоколы аутентификации.....	149
3.1.5. Подходы к реализации средств идентификации и аутентификации. Физические средства аутентификации пользователей	153
3.2. Основные подходы к защите данных от несанкционированного доступа.....	159
3.2.1. Управление информационными потоками. Достоверная*вычислительная база.....	159
3.2.2. Иерархический доступ к файлу.....	161

3.2.3. Доступ к данным со стороны процесса. Понятие скрытого доступа	167
3.3. Модели управления доступом	168
3.3.1. Абстрактные модели доступа	169
3.3.2. Многоуровневые (мандатные) модели	174
3.3.3. Выбор модели	177
3.3.4. Корректность и полнота реализации разграничительной политики доступа	180
3.4. Реализация управления доступом средствами операционных систем	183
3.4.1. Защита информации в операционных системах UNIX	183
3.4.2. SELinux — система повышенной безопасности	190
3.4.3. Альтернативные системы безопасности	193
3.4.4. Особенности защиты информации в сетевой операционной системе Microsoft Windows	195
3.4.5. Сравнительный анализ реализации встроенных моделей защиты информации в операционных системах	202
3.4.6. Недостатки механизмов управления доступом в ОС семейств Unix и Microsoft Windows	204
ГЛАВА 4. ЗАДАЧИ КОНТРОЛЯ В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ИНФОРМАЦИИ	209
4.1. Методы контроля доступа к ресурсам компьютерной системы. Способы фиксации факта доступа к файлам	209
4.2. Структура и функции подсистемы контроля доступа программ и пользователей	214
4.3. Средства ведения и анализа системных журналов операционных систем	221
4.4. Средства комплексного мониторинга системы защиты информационной системы	227
4.5. Средства контроля за процессами. Свойства процессов и управление ими	231
4.6. Средства поиска остаточной информации на машинных носителях информации	238
4.7. Средства удаления остаточной информации на машинных носителях информации	243
ГЛАВА 5. РАЗРУШАЮЩИЕ ПРОГРАММНЫЕ ВОЗДЕЙСТВИЯ И ЗАЩИТА ОТ НИХ	260
5.1. Сущность разрушающих программных воздействий	260
5.2. Модели взаимодействия прикладных программ и программы-злоумышленника	262

Оглавление	6 5.3. Классификация разрушающих программных средств и их воздействий	266
	5.4. Закладки в программно-аппаратной среде	271
	5.5. Методы внедрения разрушающих программных средств.....	277
	5.6. Компьютерные вирусы как особый класс разрушающего программного воздействия	280
	5.6.1. Классификация компьютерных вирусов	281
	5.6.2. Особенности распространения и жизненный цикл вирусов	288
	5.7. Принципы и методы защиты от разрушающих программных воздействий	296
	5.7.1. Методы выявления программ-вирусов	296
	5.7.2. Необходимые и достаточные условия недопущения разрушающего воздействия	304
	5.7.3. Организационные средства защиты от компьютерных вирусов	310
	5.8. Построение и принципы работы типовых антивирусных средств.....	312
	Глава 6. ОБЕСПЕЧЕНИЕ И КОНТРОЛЬ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ	321
	6.1. Проблема обеспечения целостности информации	321
	6.2. Способы и средства обеспечения целостности информации	324
	6.3. Защита файлов от изменений	331
	6.4. Криптографические средства контроля целостности информации	335
	6.4.1. Способы выявления изменений	335
	6.4.2. Криптографические хэш-функции	339
	6.5. Электронная подпись.....	342
	6.5.1. Виды электронных подписей.....	346
	6.5.2. Угрозы электронной подписи.....	348
	6.5.3. Системы электронной подписи	349
	Глава 7. ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ШИФРОВАНИЯ	358
	7.1. Основные принципы криптографической защиты информации в автоматизированных системах	358
	7.1.1. Задачи, решаемые криптографическими средствами в автоматизированных системах	358
	7.1.2. Стойкость криптографических алгоритмов	360
	7.1.3. Алгоритмы криптографических преобразований и их характеристики	362

7.1.4. Симметричные криптоалгоритмы	364
7.1.5. Асимметричные (с открытым ключом) криптоалгоритмы	377
7.2. Уязвимости и защита алгоритма шифрования	382
7.2.1. Невозможность применения стойких криптоалгоритмов	384
7.2.2. Неправильная реализация криптоалгоритмов	385
7.2.3. Неправильное применение криптоалгоритмов	388
7.2.4. Человеческий фактор	390
7.3. Программно-аппаратные средства шифрования	390
7.3.1. Принцип чувствительной области и принцип главного ключа	392
7.3.2. Необходимые и достаточные функции аппаратного средства криптозащиты	395
7.3.3. Аппаратная реализация	397
7.3.4. Программная реализация	399
7.3.5. Программно-аппаратная реализация	400
7.3.6. Построение аппаратных компонентов криптозащиты данных	401
7.4. Защищённые носители данных	403
 ГЛАВА 8. МЕТОДЫ РАСПРЕДЕЛЕНИЯ И ХРАНЕНИЯ КЛЮЧЕВОЙ И ПАРОЛЬНОЙ ИНФОРМАЦИИ	 408
8.1. Построение ключевых систем	408
8.1.1. Генерация ключей	409
8.1.2. Проблемы распределения ключей в информационных системах	417
8.1.3. Пароли и ключи	419
8.2. Организация распределения ключевой и парольной информации	426
8.2.1. Прямой обмен ключами	429
8.2.2. Обмен ключами через посредника	430
8.2.3. Централизованное распределение ключевой информации	434
8.3. Методы распределения ключей и паролей в распределённых системах	439
8.3.1. Квалифицированные сертификаты ключей проверки электронной подписи	442
8.3.2. Механизмы контроля использования ключей	445
8.3.3. Организация хранения ключей и паролей	448
8.3.4. Хранение ключей и паролей на дисках	453
8.3.6. Управление открытыми ключами. Удостоверяющий центр	456
 ЛИТЕРАТУРА	 460