

УЧЕБНОЕ ПОСОБИЕ

ДЛЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

СПЕЦИАЛЬНОСТЬ



МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ



Е. И. ДУХАН
А. С. КОЛЕРОВ
Н. И. СИНАДСКИЙ

Оглавление

Введение	3
1. Методы и средства криптографической защиты информации	7
1.1. Основные термины криптографической защиты информации и их определения	7
1.2. Общая характеристика программно-аппаратных средств криптографической защиты информации....	16
1.3. Криптосредства	18
1.4. Электронная цифровая подпись	19
1.5. Контроль целостности	22
1.6. Уничтожение остаточной информации	23
1.7. Организация виртуальных частных сетей	25
2. Нормативно-правовое регулирование в сфере применения средств криптографической защиты информации	36
2.1. Нормативные документы в области применения средств криптографической защиты информации....	36
2.1.1. Требования Положения ПКЗ-2005	36
2.1.2. Требования к средствам электронной подписи	38
2.2. Лицензирование и сертификация в области проектирования средств криптографической защиты информации	42
2.2.1. Лицензирование деятельности в отношении шифровальных (криптографических) средств	42
2.2.2. Сертификация средств защиты информации	43
2.3. Использование криптографических средств для обеспечения безопасности персональных данных	46
2.3.1. Требования по организации и обеспечению функционирования шифровальных (криптографических) средств ..	46
2.3.2. Рекомендации по применению криптосредств при обработке персональных данных	59
3. Применение СКЗИ	72

3.1. Система защиты конфиденциальной информации StrongDisk	72
3.1.1. Основные характеристики системы StrongDisk	72
3.1.2. Терминология СКЗИ StrongDisk	73
3.1.3. Инициализация системы StrongDisk	74
3.1.4. Создание защищенных логических дисков	76
3.1.5. Настройка параметров системы StrongDisk	84
3.1.6. Сервисные операции	90
3.1.7. Гарантированное удаление данных	93
3.2. Система защиты корпоративной информации Secret Disk	94
3.2.1. Основные характеристики системы Secret Disk	94
3.2.2. Подготовка системы к установке Secret Disk	95
3.2.3. Инициализация системы Secret Disk	95
3.2.4. Создание защищенных логических дисков	96
3.2.5. Работа с защищенными дисками	97
3.2.6. Настройка СКЗИ Secret Disk	100
3.2.7. Журнал событий	101
3.2.8. Надежное удаление и перемещение файлов и папок	103
3.3. Система криптографической защиты информации «Верба-OW»	104
3.3.1. Основные характеристики СКЗИ «Верба-OW»	104
3.3.2. Ключевая система СКЗИ «Верба-OW»	107
3.4. Организация VPN средствами СКЗИ VipNet	112
3.4.1. Постановка задачи	112
3.4.2. Настройка сетевых соединений виртуальных машин	113
3.4.3. Установка СКЗИ VipNet	115
3.4.4. Настройка СКЗИ VipNet	118
3.5. Организация VPN средствами СКЗИ StrongNet	124
3.5.1. Описание системы	124
3.5.2. Постановка задачи	125
3.5.3. Генерация и распространение ключевой информации	125
3.5.4. Настройка СКЗИ StrongNet	126
3.5.5. Установка защищенного соединения	128
3.6. Организация VPN сетевого уровня средствами программного комплекса «Игла-П»	129
3.6.1. Описание системы	129
3.6.2. Структура виртуальной сети и настройка «Игла-П»	130
3.7. Организация VPN прикладного уровня средствами протокола S/MIME и СКЗИ «КриптоПро CSP»	133

3.7.1. Организация почтового обмена	134
3.7.2. Активизация IIS	135
3.7.3. Установка СКЗИ «КриптоПро CSP»	135
3.7.4. Установка Центра сертификации в ОС Windows Server	136
3.7.5. Получение сертификатов открытых ключей	136
3.7.6. Организация защищенного обмена электронной почтой	137
4. Проектирование средств криптографической защиты информации 12	139
4.1. Применение библиотек CryptoAPI для работы с СКЗИ «КриптоПро CSP» в среде программирования Borland Delphi	139
4.1.1. Постановка задачи	139
4.1.2. Подготовительные операции	142
4.1.3. Необходимые модули, функции и переменные	143
4.1.4. Создание, загрузка и удаление криптографического контейнера	148
4.1.5. Генерация, проверка наличия и экспорт открытых ключей	149
4.1.6. Формирование и проверка электронной подписи файлов	152
4.1.7. Зашифрование и расшифрование данных файла	155
4.1.8. Гарантированное уничтожение файла	157
4.1.9. Дополнительные задания	158
4.2. Применение библиотек CryptoPro.Sharpei для работы с СКЗИ «КриптоПро CSP» на базе платформы программирования Microsoft .Net Framework	159
4.2.1. Постановка задачи	159
4.2.2. Алгоритм работы и интерфейс программы	160
4.2.3. Обработка исключений	163
4.2.4. Необходимые модули, функции и переменные	164
4.2.5. Загрузка сертификата и экспорт открытого ключа ..	166
4.2.6. Формирование и проверка электронной подписи файла	168
4.2.7. Зашифрование и расшифрование данных файла	171
4.2.8. Гарантированное удаление файла	177
4.2.9. Проверка работоспособности программы	178
4.3. Проектирование средств криптографической защиты информации на базе библиотек СКЗИ «Верба-OW» ..	180
4.3.1. Создание программы, использующей криптографические функции из библиотеки «Верба-OW»	180

4.3.2. Работа со справочниками открытых ключей	184
4.4. Применение библиотек CryptoAPI для создания VPN-системы на основе СКЗИ «КриптоПро CSP» с применением ключей eToken	186
4.4.1. Особенности вызова функций из криптографической библиотеки	186
4.4.2. Постановка задачи	187
4.4.3. Создание интерфейса программы	188
4.4.4. Создание контейнера и генерация ключевой информации	190
4.4.5. Процесс обмена ключами	194
4.4.6. Процесс обмена сообщениями	201
4.4.7. Работа с электронными ключами eToken	204
Заключение	209
Литература	210
Приложение А. Рекомендации по проведению практических занятий	214
Приложение Б. Электронные идентификаторы	216
Приложение В. Основные термины криптографической защиты информации и их определения	220
Приложение Г. Типовые формы учетных документов по эксплуатации криптосредств	227
Приложение Д. Фонд оценочных средств	229