

***Хореев П. Б.***

*Методы и средства защиты информации в компьютерных системах: учеб. пособие для студ. высш. учеб. заведений / П.Б.Хорев. — 3-е изд., стер. — М.: Издательский центр «Академия», 2007. — 256 с.*

*Основное внимание в учебном пособии уделено программным и программно-аппаратным методам и средствам защиты информации. Рассмотрены, в частности, модели безопасности, используемые в защищенных версиях операционной системы Windows (в том числе использование функций криптографического интерфейса приложений CryptoAPI) и операционных системах «клона» Unix.*

*Для студентов высших учебных заведений. Может быть полезно специалистам в области информационной безопасности.*

# СОДЕРЖАНИЕ

Предисловие.....	3
<b>Глава 1. КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....</b>	<b>6</b>
1.1.Основные понятия защиты информации .....	6
1.2.Угрозы информационной безопасности и каналы утечки информации .....	9
1.3.Организационно-правовое обеспечение информационной безопасности .....	13
1.4.Инженерно-технические методы и средства защиты информации.....	16
1.5.Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.....	18
1.6. Требования к комплексным системам защиты информации .....	20
<b>Глава 2. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА .....</b>	<b>25</b>
2.1.Способы несанкционированного доступа к информации в компьютерных системах и защиты от него.....	25
2.2.Аутентификация пользователей на основе паролей и модели «рукопожатия» .....	30
2.3.Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью .....	35
2.4.Программно-аппаратная защита информации от локального несанкционированного доступа.....	41
2.5.Аутентификация пользователей при удаленном доступе. Защита информации от несанкционированного доступа в сетях.....	44
<b>Глава 3. ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ОПЕРАЦИОННЫХ СИСТЕМАХ .....</b>	<b>60</b>

3.1. Защита информации от несанкционированного доступа в открытых версиях операционной системы Windows.....	60
3.2. Дискреционное и мандатное управление доступом к объектам компьютерных систем.....	69
3.3. Подсистема безопасности защищенных версий операционной системы Windows.....	73
3.4. Аудит событий безопасности в защищенных версиях операционной системы Windows.....	102
3.5. Защита информации от несанкционированного доступа в операционных системах семейства Unix.....	109

#### **Глава 4. КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ**

#### **БЕЗОПАСНОСТИ .....123**

4.1. Элементы теории чисел.....	123
4.2. Основные понятия криптологии. Симметричные и асимметричные криптосистемы.....	125
4.3. Способы создания симметричных криптосистем. Абсолютно стойкий шифр .....	127
4.4. Криптографическая система DES и ее модификации.....	138
4.5. Криптографическая система ГОСТ 28147—89.....	143
4.6. Принципы построения асимметричных криптографических систем .....	146
4.7. Электронная цифровая подпись и ее применение.....	151
4.8. Использование симметричных и асимметричных криптографических систем .....	154
4.9. Компьютерная стеганография и ее применение.....	164

#### **Глава 5. КРИПТОГРАФИЧЕСКИЙ ИНТЕРФЕЙС ПРИЛОЖЕНИЙ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS**

#### **(CRYPTOAPI) .....171**

5.1. Принципы построения и использования CryptoAPI.....	171
5.2. Создание и передача криптографических ключей с помощью функций CryptoAPI.....	178
5.3. Использование функций CryptoAPI для шифрования и расшифрования данных .....	185
5.4. Использование функций CryptoAPI для получения и проверки электронной цифровой подписи.....	189
5.5. Защита документов Microsoft Office от несанкционированного доступа .....	192
5.6. Шифрующая файловая система в защищенных версиях операционной системы Windows .....	200
<b>Глава 6. ЗАЩИТА КОМПЬЮТЕРНЫХ СИСТЕМ ОТ ВРЕДОНОСНЫХ ПРОГРАММ .....</b>	<b>207</b>
6.1. Вредоносные программы и их классификация.....	207
6.2. Загрузочные и файловые вирусы.....	210
6.3. Методы обнаружения и удаления вирусов.....	218
6.4. Программные закладки и методы защиты от них.....	227
<b>Глава 7. ЗАЩИТА ПРОГРАММНЫХ СРЕДСТВ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ И КОПИРОВАНИЯ.....</b>	<b>234</b>
7.1. Принципы построения систем защиты от копирования.....	234
7.2. Методы защиты инсталляционных дисков от копирования .....	237
7.3. Методы настройки устанавливаемого программного обеспечения на характеристики компьютера.....	240
7.4. Методы противодействия исследованию алгоритма работы системы защиты.....	246
Список литературы.....	251