

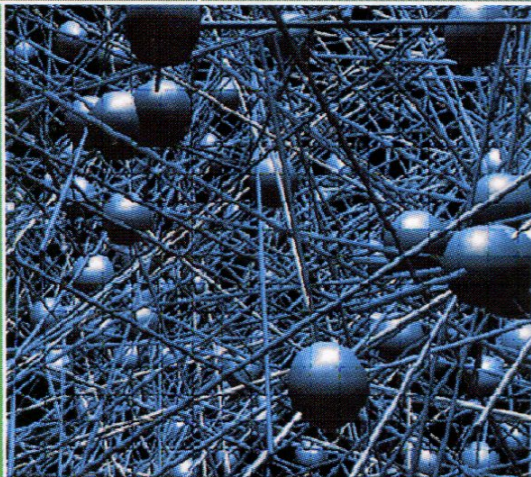
Высшее профессиональное образование

А. В. Черемушкин

# КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

## Основные свойства и уязвимости

Учебное пособие



Информационная  
безопасность

А. В. ЧЕРЕМУШКИН

# КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ ОСНОВНЫЕ СВОЙСТВА И УЯЗВИМОСТИ

*Допущено*

*Учебно-методическим объединением по образованию  
в области информационной безопасности  
в качестве учебного пособия для студентов высших учебных заведений,  
обучающихся по специальности «Компьютерная безопасность»*



Москва

Издательский центр «Академия»

2009

# ОГЛАВЛЕНИЕ

Предисловие . . . . .	3
Список обозначений . . . . .	6
<b>Глава 1. Понятие криптографического протокола . . . . .</b>	<b>8</b>
1.1. Основные определения . . . . .	8
1.2. Свойства, характеризующие безопасность протоколов . . . . .	13
1.3. Виды криптографических протоколов . . . . .	21
1.4. Основные атаки на безопасность протоколов . . . . .	28
1.5. Формальные методы анализа протоколов обеспечения безопасности . . . . .	35
<b>Глава 2. Криптографические хеш-функции . . . . .</b>	<b>45</b>
2.1. Функции хеширования и целостность данных . . . . .	45
2.2. Хеш-функции, задаваемые ключом . . . . .	49
2.3. Хеш-функции, не зависящие от ключа . . . . .	54
2.4. Хеш-функции на основе дискретного логарифмирования . . . . .	63
2.5. Возможные атаки на функции хеширования . . . . .	64
<b>Глава 3. Коды аутентификации . . . . .</b>	<b>68</b>
3.1. Определения и свойства . . . . .	68
3.2. Ортогональные массивы . . . . .	71
3.3. Характеристика оптимальных кодов аутентификации . . . . .	74
<b>Глава 4. Схемы цифровых подписей . . . . .</b>	<b>79</b>
4.1. Общие положения . . . . .	79
4.2. Цифровые подписи на основе систем шифрования с открытыми ключами . . . . .	85
4.3. Цифровые подписи на основе специально разработанных алгоритмов . . . . .	87
4.4. Цифровые подписи на основе симметричных систем шифрования . . . . .	93
4.5. Другие протоколы цифровой подписи . . . . .	94
<b>Глава 5. Протоколы идентификации . . . . .</b>	<b>98</b>
5.1. Виды протоколов идентификации . . . . .	98
5.2. Протоколы идентификации, использующие пароли (слабая аутентификация) . . . . .	100
5.3. Протоколы идентификации, использующие технику «запрос — ответ» (сильная аутентификация) . . . . .	106

5.4. Протоколы идентификации, использующие технику доказательства знания . . . . .	114
<b>Глава 6. Протоколы с нулевым разглашением . . . . .</b>	<b>128</b>
6.1. Протоколы решения математических задач . . . . .	128
6.2. Протокол привязки к биту . . . . .	129
6.3. Игровые протоколы . . . . .	131
6.4. Протокол подписания контракта . . . . .	135
6.5. Сертифицированная электронная почта . . . . .	139
6.6. Аргумент с нулевым разглашением . . . . .	141
6.7. Протокол (схема) электронного голосования . . . . .	143
<b>Глава 7. Протоколы передачи ключей . . . . .</b>	<b>147</b>
7.1. Передача ключей с использованием симметричного шифрования . . . . .	147
7.2. Передача ключей с использованием асимметричного шифрования . . . . .	161
<b>Глава 8. Открытое распределение ключей . . . . .</b>	<b>170</b>
8.1. Виды протоколов открытого распределения ключей и их свойства . . . . .	170
8.2. Протокол Диффи — Хеллмана и его усиления . . . . .	173
8.3. Аутентифицированные протоколы . . . . .	181
<b>Глава 9. Предварительное распределение ключей . . . . .</b>	<b>188</b>
9.1. Схемы предварительного распределения ключей в сети связи . . . . .	188
9.2. Групповые протоколы . . . . .	203
<b>Глава 10. Аппаратные средства для защиты ключей в компьютере . . . . .</b>	<b>211</b>
10.1. Проблема защиты главного ключа . . . . .	211
10.2. Архитектура криптографической подсистемы . . . . .	214
10.3. Примеры протоколов распределения ключей . . . . .	219
<b>Глава 11. Семейство протоколов IPsec . . . . .</b>	<b>225</b>
11.1. Структура протокола IPsec . . . . .	225
11.2. Управление ключами в протоколе IPsec . . . . .	230
11.3. Атаки на протокол IPsec . . . . .	249
<b>Глава 12. Управление ключами . . . . .</b>	<b>253</b>
12.1. Проблема управления ключами . . . . .	253
12.2. Жизненный цикл ключей . . . . .	255
12.3. Услуги, предоставляемые доверенной третьей стороной . . . . .	258
12.4. Особенности управления ключами в симметричных системах шифрования . . . . .	258
12.5. Особенности управления ключами в асимметричных системах шифрования . . . . .	261
Список литературы . . . . .	264