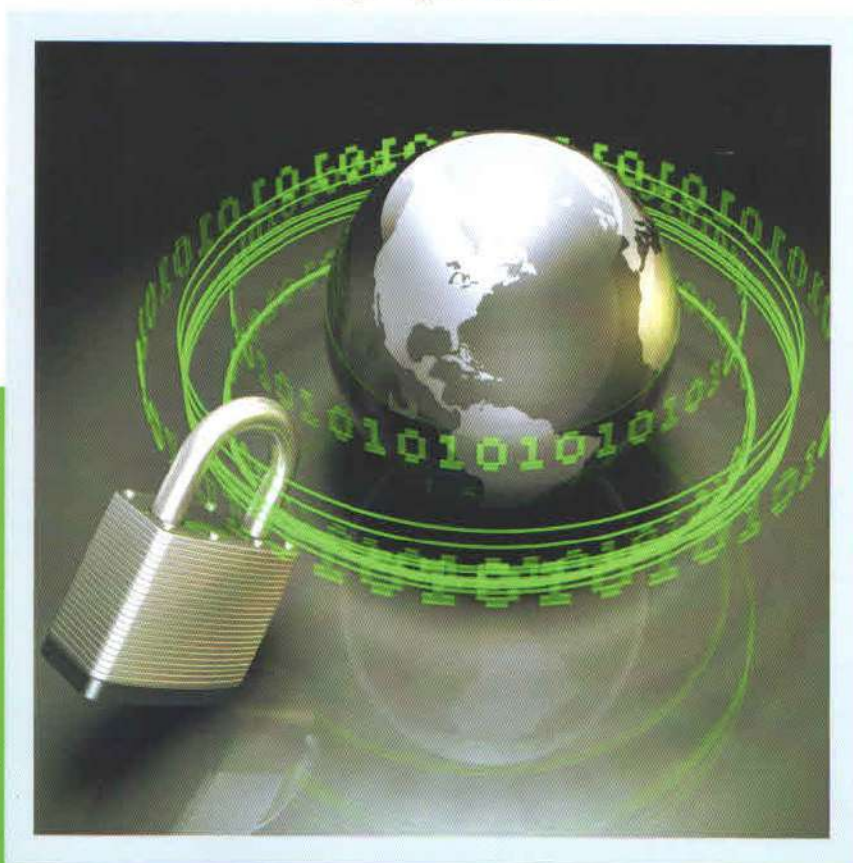


К.С. ДҮЙСЕБЕКОВА

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ АҚПАРАТТАРДЫ ҚОРҒАУ

ОҚУ ҚҰРАЛЫ



Алматы 2013

К.С. Дүйсебекова

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ АҚПАРАТТАРДЫ ҚОРҒАУ

Оқу құралы ¹

Алматы
«Қазак университеті»
2013

ӘОЖ 004.056
КБЖ 32.81
Д 87

*Баспаға Әл-Фараби атындағы Қазақ ұлттық университеті
механика-математика факультетінің Ғылыми кеңесі және
Редакциялық-баспа кеңесі шешімімен ұсынылған.*

Пікір жазғандар:

техника ғылымдарының докторы, профессор *Р.К. Өскенбаева*
техника ғылымдарының докторы, профессор *Ш.А. Жомартова*

Дүйсебекова К.С.

Д 87 Ақпараттық қауіпсіздік және ақпараттарды қорғау: оқу құралы.
– Алматы: Қазақ университеті, 2013. – 156 б.

ISBN 978-601-247-811-2

Оқу құралында компьютерлік жүйелердегі ақпараттарды қорғау әдістері, объектілері, ақпараттық қауіпсіздіктің математикалық негіздері, желі қауіпсіздігінің проблемалары қарастырылған. Әсіресе, ақпараттық қауіпсіздікті қамтамасыз ететін әдістердің алгоритмдерін зерттеп, программалауға, ол үшін есептеу жүйелерінің архитектурасын тиімді пайдалануға көңіл бөлінген.

Оқу құралы жоғары оқу орнында «Информатика», «Ақпараттық жүйелер», «Математикалық және компьютерлік модельдеу» мамандықтары бойынша даярланып жатқан студенттерге, магистранттарға, PhD докторанттарға көмек құралы ретінде ұсынылған.

ӘОЖ 004.056
КБЖ 32.81

МАЗМҰНЫ

Кіріспе.....	3
1. Дәстүрлі криптографиялық әдістер. Орын ауыстыру арқылы шифрлеу	11
1.1 Сиқырлы квадраттар.....	11
1.2 Вижинер әдісі. Вижинер кестесі.....	12
1.3. Уитстонның «қос квадрат» шифрі	14
2. Сандар теориясының элементтері. Криптографияның математикалық негіздері	15
2.1. Модулярлық арифметика	15
2.2. ЕҮОБ табуға арналған Евклид алгоритмі.....	17
2.3. Кері мәндерді есептеу	18
2.4. Кері мәндерді табудың негізгі тәсілдері	19
2.5. Жай сандардың көбейтіндісі үшін қалдықтардың келтірілген жиыны	20
2 (жалғасы). Хэш-функциялар. Бірбағытты хэш-функциялар	21
2.6. Бірбағытты Хэш-функциялар	22
2.7. Бір бағытты хэш-функцияның ұзындықтары.....	23
2.8. Бір бағытты хэш-функцияларға шолу.....	23
2.9. Қауіпсіз хэштеу алгоритмі(SHA)	23
3. Ашық кілтті жүйелер	27
3.1. RSA алгоритмі.....	28
3.2. RSA алгоритмінің қадамдары.....	29
4. RSA криптожүйесінің қауіпсіздігі мен тездігі.....	37
4.1. RSA криптожүйесінің қауіпсіздігі мен тездігі	37
4.2. Полиг-Хеллманның шифрлеу үрдісі.....	38
4.3. Эль-Гамальдің шифрлеу үрдісі.....	39
5. Блокты шифрлер туралы жалпы мағлұматтар.....	41
5.1. Блокты шифрлер туралы мағлұматтар.....	41
5.2. Файстель тораптары (желілері)	41
5 (жалғасы). Блокты ГОСТ 28147-89 шифрі.....	44
5.3. Блокты ГОСТ 28147-89 шифрі	44
5.4. Криптотүрлендірудің негізгі қадамы	45
5.5. Қарапайым ауыстыру режімі	48
5.6. Ашық деректерді қарапайым ауыстыру режімінде шифрлеу.....	48
5.7. Қарапайым ауыстыру режімінде кері шифрлеу	51
6. Гаммалау әдісі бойынша шифрлеу	53
6.1. Гаммалау әдісі бойынша шифрлеу.....	53
6.2. Жалған кездейсоқ сандар тізбегін генерациялау әдістері	54
7. Қазіргі заманғы жиі қолданылатын симметриялық криптожүйелер.....	57
7.1. Деректерді шифрлеудің американдық DES стандарты	58
8. F (Ri-1, Ki) шифрлеу функциясын есептеудің сұлбасы	63

9. Ақпаратты қысу	69
9.1. Тізбектей қысу	70
9.2. Энтропийлі түрде қысу	71
9.3. Графикалық ақпаратты өңдеу	74
10. Кескіндерді кодтау	79
10.1. RGB	80
10.2. CMY	80
10.3. CIE	82
10.4. YIQ	86
10.5. HLS және HSB	87
10.6. Түстік моделдерге кейбір ескертулер	88
10.7. Суреттерді форматтау және индексациялау	90
10.8. Суретті сүзгіден өткізу (филтрлеу)	84
11. Кілттерді құру, тарату, басқару, тіркеу	95
11.1. Кілттер генерациясы	95
11.2. Кілттерді сақтау	96
11.3. Кілттерді тарату	97
11.4. Кілттерді ашық тарату	97
11.5. Субъектіні идентификациялау және аутентификациялау	98
11.6. Қолданушының аутентификациясы	90
12. Ақпаратты қорғаудың аппараттық жабдықтары	99
12.1. Шифраторлар	100
12.2. Шифрлеу құралдары	101
12.3. Рұқсатсыз қол жеткізулерден қорғау құралдары	101
12.4. Ақпараттық ресурстарға қол жеткізуге шек қоятын жүйелер	102
12.5. Желілік шифраторлар	103
13. Қауіпсіздікті қамтамасыз етудің SSL хаттамасы	111
13.1. SSL сипаттамасы	111
13.2. Аутентификация және кілтті алмасу	113
13.3. Баспа хаттамасы (Record Layer)	114
13.4. Қол алысу хаттамасы (handshake)	114
13.5. Шифрді өзгерту хаттамасы (The Change Cipher Spec Protocol)	115
13.6. Дабыл хаттамасы (Alert Protocol)	115
13.7. SSL хаттамасында қолданылатын алгоритмдер	116
14. Windows XP, Unix, Linux операциялық жүйелерінің қауіпсіздігі	119
14.1. Windows XP операциялық жүйесінің (ОЖ) қауіпсіздігі	119
14.2. UNIX қауіпсіздік концепциясы	125
14.3. Linux-тің желілік және локальдық қауіпсіздігі	130
15. Электронды төлем жүйелері	133
15.1. Электронды төлем жүйелерінде ақпаратты қорғау әдісі	133
15.2. ЭТЖ қорғау жүйесінің құрылымының ортақ алгоритмі	134
Пайдаланылған әдебиеттер	144
Тест сұрақтары	145

Оқу басылымы

Дүйсебекова Күланда Сейтбекқызы

**АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ
АҚПАРАТТАРДЫ ҚОРҒАУ**

↓

Оқу құралы

Редакторы *Самат Қалуов*
Компьютерде беттеген *Сәуле Сарпекова*
Мұқабасын көркемдеген *Ринат Сқақов*

ИБ №6254

Басуға 01.02.2013 жылы қол қойылды. Пішімі 70x100¹/₁₆. Көлемі 9,75 б.т.

Офсетті қағаз. Сандық басылымы. Тапсырыс №231.

Таралымы 250 дана. Бағасы келісімді.

Әл-Фараби атындағы Қазақ ұлттық университетінің
«Қазақ университеті» баспасы.

050040, Алматы қаласы, әл-Фараби, 71.

«Қазақ университеті» баспаханасында басылды.