

### АХМЕТОВ БЕРІК БАХЫТЖАНОВИЧ



техника ғылымдарының кандидаты, профессор, «Ш.Есенов атындағы Каспий технологиялар және инженеринг университеті» қарымдылық емес акционерлік қоғамының президенті (Алғаш, Қазақстан). 100-ден астам ғылыми және оқу-әдістемелік еңбектердің, соның ішінде оқулықтардың, оқу құралдарының, монографиялардың, өнертабысқа патенттердің авторы. Ақпаратты қорғау және қауіпсіздік, зияткерлік ақпараттық технологиялар саласындағы ғылым.

### БАБАК ВИТАЛИЙ ПАВЛОВИЧ



Украина Ұлттық Ғылым академиясының корреспондент-мүшесі, техника ғылымдарының докторы, Ұлттық Явация университетінің профессоры (Киев, Украина). Украинаның Ғылым мен техниканы өсіруге сіңірген қайраткері, Украинаның ғылым мен техника саласындағы мемлекеттік сыйлығының иегері. 100-ден астам ғылыми және оқу-әдістемелік еңбектердің, соның ішінде оқулықтардың, монографиялардың, сөздіктердің, өнертабысқа патенттердің авторы. Техникалық диагностика және ақпараттық технологиялар саласындағы ғылым.

### АЛИМСЕНТОВА ЖУЛДЫЗ КЕНЕСХАНОВНА



PhD, Г. Даукеев атындағы Алматы энергетика және байланыс университетінің IT-инженеринг кафедрасының доценті (Алматы, Қазақстан). 90-нан астам ғылыми және оқу-әдістемелік еңбектердің, соның ішінде оқулықтардың, оқу құралдарының, монографиялардың, авторлық құрастырмалардың авторы. Ақпаратты қорғау және қауіпсіздік, ақпараттық технологиялар саласындағы ғылым.

АҚПАРАТТЫ ҚОРҒАУДЫҢ ТЕОРИЯЛЫҚ НЕГІЗДЕРІ

АХМЕТОВ Б.Б., БАБАК В.П., АЛИМСЕНТОВА Ж.К.

Ахметов Берик Бахытжанович,  
Бабак Виталий Павлович,  
Алиментова Жулдыз Кенесхановна

# АҚПАРАТТЫ ҚОРҒАУДЫҢ ТЕОРИЯЛЫҚ НЕГІЗДЕРІ



**Ахметов Б.Б., Бабак В.П., Алимсеитова Ж.К.**

# **АҚПАРАТТЫ ҚОРҒАУДЫҢ ТЕОРИЯЛЫҚ НЕГІЗДЕРІ**

**О Қ У Л Ы Қ**

Қазақстан Республикасының білім және ғылым министрлігімен бекітілген

Ақтау - 2022

**УДК 004.056.5(075.8)**  
**ББК 32.973.202-018.2 я73**  
**А94**

**Пікір берушілер:**

Тукеев У.А. - техника ғылымдарының докторы, профессор, Әл-Фараби атындағы ҚазҰУ

Корченко А.Г. - техника ғылымдарының докторы, профессор Украинаның Ұлттық авиациялық университеті

Джурунтаев Д.З. - техника ғылымдарының докторы, профессор, Сәтбаев университеті

**А94 Ахметов Б.Б., Бабак В.П., Алимсеитова Ж.К. Ақпаратты қорғаудың теориялық негіздері.** Оқулық. – Ақтау. ЕУ, 2022 – 685 б. Сүрет. 422. Кесте. 43. Библиогр. – 46 атау.

ISBN 978-601-08-1831-6

Оқулықта ақпараттық сигналдарды түрлендірудің және зерттеудің математикалық аппаратына, ақпаратты, сигналдар мен деректерді өлшеу, жіберу және өңдеу технологияларына, кедергілерге төзімді кодтауға, ақпаратты жіберудің заманауи ақпараттық-коммуникациялық арналарын пайдалануға, шифрлау және керішифрлау алгоритмдеріне, стегано- және криптографияға, цифрлық қолтаңбаға және т. б. негізделген ақпаратты қорғаудың негізгі ұғымдары мен әдістері баяндалған. Алгоритмдік және техникалық әдістермен қатар конфиденциалды және коммерциялық ақпаратты қорғау, рұқсатсыз қол жеткізуден қорғау, зияткерлік меншікті қорғау, ақпаратты қорғауды заңнамалық қамтамасыз ету, сондай-ақ ақпаратты қорғау саласындағы халықаралық стандарттар қарастырылған.

Оқулық «Информатика», «Информатика мұғалімдерін даярлау» білім беру бағытына, сонымен қатар «Ақпараттық және коммуникациялық технологиялар» бағытында оқитын студенттері мен магистранттарына арналған.

**УДК 004.056.5(075.8)**  
**ББК 32.973.202-018.2 я73**

**ISBN 978-601-08-1831-6**

© Ахметов Б.Б., Бабак В.П., Алимсеитова Ж.К.  
© ЕУ, 2022

## М А З М Ұ Н Ы

<b>Алғысөз</b>	6
<b>1 тарау. Ақпаратты қорғаудың негізгі ұғымдары</b>	8
1.1. Терминдер және анықтамалар	9
1.2. Ақпарат қауіпсіздігіне төнетін қатерлерді жіктеу және оның осалдығын бағалау әдістері	17
1.3. Ақпараттың ағу арналары	27
1.4. Ақпаратты кешенді қорғау жүйелерін құру принциптері	35
1.5. Ақпараттық жүйелердің кедергілерге төзімділігін бағалау критерийлері	49
Негізгі тұжырымдар	55
Өзін-өзі бақылау сұрақтары	58
<b>2 тарау. Ақпаратты сандық бағалау</b>	61
2.1. Ақпарат, оның функциялары мен қасиеттері	62
2.2. Ақпараттың сандық сипаттамалары	65
2.3. Ақпарат өлшемдері	68
2.4. Энтропия және оның қасиеттері	72
2.5. Ақпарат көзінің өнімділігі мен артықтығы	76
2.6. Ақпараттың сигнал параметрлерімен байланысы	97
Негізгі тұжырымдар	100
Өзін-өзі бақылау сұрақтары	102
<b>3 тарау. Ақпараттық сигналдар және олардың математикалық модельдері</b>	103
3.1. Ақпараттық сигналдардың түрлері және олардың математикалық модельдері	104
3.2. Кездейсоқ сигналдар мен кедергілер	126
3.3. Сигналдар мен кедергілердің сандық сипаттамалары	133
3.4. Шектеулі спектрлі сигналдардың математикалық модельдері	138
3.5. Дискретті сигналдар	152
Негізгі тұжырымдар	176
Өзін-өзі бақылау сұрақтары	179
<b>4 тарау. Ақпаратты өңдеу</b>	181
4.1. Ақпаратты аналогтық өңдеу	182
4.2. Сигналдарды кванттау және дискреттеу	246
4.3. Ақпаратты цифрлық өңдеу	257
Негізгі тұжырымдар	298
Өзін-өзі бақылау сұрақтары	300
<b>5 тарау. Ақпаратты жіберу</b>	302
5.1. Деректерді жіберудің ақпараттық жүйелері	303

5.2. Ақпараттық арналардың түрлері, олардың математикалық модельдері мен сипаттамалары	308
5.3. Байланыс арналарында ақпаратты жіберу жылдамдығы	323
5.4. Ақпараттық жүйелер элементтерін синтездеу. Оңтайлы қабылдағыш	336
5.5. Көп арналы деректер жіберу желілері. Ақпараттық арналарды бөлу	349
5.6. Ақпаратты жіберу жүйелерінің шуға төзімділігі	357
Негізгі тұжырымдар	362
Өзін-өзі бақылау сұрақтары	364
<b>6 тарау. Ақпарат жіберу желілері</b>	<b>365</b>
6.1. Ақпараттық-коммуникациялық желілер	366
6.2. Ақпараттық желілерді жобалау	380
6.3. Ақпарат жіберудің сымсыз жүйелері және ақпараттық ресурстарды қорғау	390
6.4. Спутниктік арналар	405
6.5. Ақпараттық ресурстарға көптік қол жетімділік	413
Негізгі тұжырымдар	430
Өзін-өзі бақылау сұрақтары	432
<b>7 тарау. Ақпаратты кодтау</b>	<b>434</b>
7.1. Хабарлама көзін кодтау және деректерді қысу	435
7.2. Кедергіге төзімді кодтау	466
7.3. Блокты кедергіге төзімді кодтау	474
7.4. Үйіркілі кедергіге төзімді кодтау	497
Негізгі тұжырымдар	514
Өзін-өзі бақылау сұрақтары	515
<b>8 тарау. Ақпаратты шифрлау және керішифрлау</b>	<b>517</b>
8.1. Шифрлау модельдері мен жүйелері	518
8.2. Байланыс арналарында шифрлау	523
8.3. Симметриялық және асимметриялық шифрлау алгоритмдері мен жүйелері (ақпаратты криптографиялық қорғау)	526
8.4. Электрондық цифрлық қолтаңба	541
8.5. Ақпаратты қорғаудың стеганографиялық әдістері	558
8.6. Криптоталдау әдістері	569
Негізгі тұжырымдар	573
Өзін-өзі бақылау сұрақтары	574
<b>9 тарау. Ақпаратты рұқсатсыз қол жеткізуден қорғау</b>	<b>576</b>
9.1. Ақпараттық жүйелер ресурстарына рұқсатсыз қол жеткізу әдістері	577
9.2. Рұқсатсыз қол жеткізуден қорғау құралдары	596
9.3. Ақпаратты қорғау жүйелері мен процестерін модельдеу	602

9.4. Желілік рұқсатсыз қол жеткізуге қарсы тұру	617
Негізгі тұжырымдар	632
Өзін-өзі бақылау сұрақтары	635
<b>10 тарау. Ақпаратты қорғауды заңнамалық қамтамасыз ету</b>	<b>637</b>
10.1. Ақпаратты қорғаудың құқықтық негіздері	638
10.2. Ақпаратты қорғаудың ұйымдастырушылық шаралары	655
10.3. Ақпаратты қорғауды ғылыми-әдістемелік қамтамасыз ету	661
10.4. Ақпараттық қауіпсіздіктің халықаралық стандарттары	668
Негізгі тұжырымдар	673
Өзін-өзі бақылау сұрақтары	675
Пәндік көрсеткіш	677
Әдебиеттер тізімі	683

**Ахметов Берик Бахытжанович,  
Бабак Виталий Павлович,  
Алимсеитова Жулдыз Кенесхановна**

**АҚПАРАТТЫ ҚОРҒАУДЫҢ  
ТЕОРИЯЛЫҚ НЕГІЗДЕРІ**

**Оқулық**

Басуға қол қойылды 01.03.2022 ж.  
Таралымы 500 дана. Пішімі 60x84 1/16 Алматы қаласы,  
«Бірлік» баспасы, №1 баспаханалық қағаз.  
Е.-б.т. 43. Ш.б.л. 42,9. Тапсырыс №69.  
Бағасы келісімді.

**ISBN 978-601-08-1831-6**

