

М.З. Якубова, А.К. Мукашева, О.А. Мананкова

АҚПАРАТТЫҚ ҚАУІПСІЗДІК НЕГІЗДЕРІ

Оқу күралы

Алматы, 2021

ӘОЖ004.056.5(075.8)

КБЖ32.972.53я73

К65

Рецензенттер:

техника ғылымдарынын кандидаты, Қ.И. Сәтбаев атындағы ҚазҰТЗУ акпараттық қауіпсіздік кафедрасының профессоры,
Е.Ж. Айтхожаева.

техника ғылымдарының докторы, АЭжБУ автоматтандыру және басқару кафедрасының профессоры, **Е.Т. Утенбергенов.**

PhD, ЛЖКА қашыктықтан оқыту Орталығы, директор орынбасары,
Д.Т. Касымова.

К65 Якубова М.З., Мукашева А.К., Мананкова О.А.

Ақпараттық қауіпсіздік негіздері: *Оқу құралы* (барлық мамандықтар студенттері үшін)/ М.З. Якубова, А.К. Мукашева, О.А. Мананкова,. – Алматы: ЖПИС «Лантар Трейд», 2021. – 114 б.: З кесте, 78 ил. библиогр. - 38атау.

ISBN 978-601-7939-85-4

Оқу құралында жүйелердің акпараттық қауіпсіздігі, телекоммуникациялық технологиялардың, сондай-ак OpNetModeler, Wireshark және Cryptool2 заманауи виртуалды модельдеу орталарын колдана отырып, акпараттық ресурстарды коргаудың негізгі әдістері мен құралдары туралы негізгі ұғымдары бар.

Ұсынылған оқу құралында телекоммуникация қызметтерінің конвергенциясы туралы мәліметтер жинақталған, жүйеленген және ұсынылған.

Оқу құралы барлық мамандықтардың студенттеріне арналған.

ӘОЖ004.056.5(075.8)

КБЖ32.972.53я73

Алматы энергетика және байланыс университетінің Ғылыми кеңесі баспаға ұсынды (20.04.2021 ж. № 11 хаттама). АЭжБУ ведомстволық әдебиетті шыгарудың 2021 жылға арналған тақырыптық жоспары бойынша басып шыгарылады, позиция 9.

ISBN 978-601-7939-85-4

©Якубова М.З., Мукашева А.К.,

Мананкова О.А., 2021

© ЖПИС «Лантар Трейд», 2021

Мазмұны

Кіріспе	5
ТАРАУ1. АҚПАРАТТЫҚ ҮГІМДАРЫ.....	6
1.1 Ақпараттық қауіпсіздіктін даму кезендері.....	6
1.2 Ақпараттық қауіпсіздік жайлы түсінік.....	8
1.3 Ақпараттық қауіпсіздік тұжырымдамасы	9
1.4 Ақпараттық қауіпсіздікті камтамасыз ету деңгейлері	12
1.4.1 Заннамалық деңгейі	12
1.4.1 Өкімшілік деңгейі.....	17
1.4.2 Процедуралық деңгей	19
1.4.3 Бағдарламалық-техникалық деңгей.....	21
1.4.4 Қолданыстағы қауіпсіздік шараларының артықшылықтарымен кемшіліктері.....	24
Озін-өзі бақылау сұраптары:	25
ТАРАУ 2.АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖҮЙЕЛЕРІНІҢ КАУІПТЕРІН, ОСАЛДЫҚТАРЫ МЕН ШАБУЫЛДАРЫН ЖІКТЕУ.....	27
2.1 Ақпараттық жүйелер мен олардың осалдықтарының қауіпсіздігіне төнетін көтерлерді бағалау әдістемесі	35
2.2 Шабуылдарды анықтау және алдын алу жүйелері	43
2.3 Қауіпсіздік сканерлері	46
Озін-өзі бақылау сұраптары:	49
ТАРАУ 3.CRYPTOOL2 БАҒДАРЛАМАСЫН ҚОЛДАНУ АРҚЫЛЫ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІН ПРАКТИКАЛЫҚ АСПЕКТИЛЕРІ.....	50
3.1 Cryptool2 ортасында Цезарь алгоритмі бойынша шифрлау және дешифрлеу әдісін игеру	50
3.1.1 CrypTool2 ортасында Цезарь Шифрінің схемасын күру	51
3.1.2 Жиіліктік талдау	55
3.1.3 Цезарь шифрін Brute Force көмегімен бұзу	55
3.2 AES алгоритмінің шифрлау режимдерін енгізу	56
3.3 AES алгоритмінің шифрлау режимдерін енгізу	60
3.3.1 ECB режимі	60
3.3.2 AES-те CBC шифрлау режимін іске асыру	66
3.3.3 AES-те CFB шифрлау режимін іске асыру	72
3.3.4 AES-те OFB шифрлау режимін іске асыру	76
Озін-өзі бақылау сұраптары:	80
ТАРАУ 4.OPNET MODELER ЖӘНЕ WIRESHARK БАҒДАРЛАМАЛАРЫН ҚОЛДАНА ОТЫРЫП, АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІН ПРАКТИКАЛЫҚ АСПЕКТИЛЕРІ	81
4.1 Жергілікті сымсыз желіні жобалау және Wireshark көмегімен жасалған желіге шабуыл жасау мысалында Opnet Modeler v. 14 бағдарламалық ортасын орнату және зерттеу	81
4.1.1 Пайдаланушы косымшаларын және олардың профильдерін баптау	89

4.1.2 Серверді баптау	91
4.1.3 Сымсыз косылым маршрутизаторларын баптау	93
4.1.4 Коммутаторларды (Ширыштықтарды) баптау	94
4.1.5 Соңғы пайдаланушыларды баптау (жұмыс станциялары – жеке компьютерлер).....	95
4.1.6 Мобильді станциялардың қозғалысын баптау	96
4.1.7 Желі протоколын орнату.	97
4.1.8 Имитационды модельдеу.	97
4.1.9 Wireshark комегімен шабуыл жасау	99
4.1.10 Желлік трафикті түсіру.	101
4.1.11 Пакеттерді сұзу.	101
4.2 Opnet Modeler v.14.5 бағдарламалық ортасында ғаламдық сымсыз желіні жобалау және Wireshark комегімен жасалған желіге шабуылды жүзеге асыру.....	105
4.2.1 Opnet-те сымсыз желі архитектурасын құру	105
4.2.2 Желі жабдығын баптау, трафикті генерациялау.	107
4.2.3 Желіге шабуылды іске асыру	109
Өзін-өзі бакылау сұраптары:.....	111