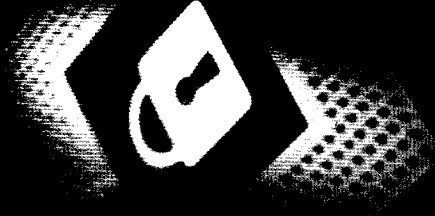


32
7-19

S.K. GANIYEV,
M.M. KARIMOV, K.A. TASHEV



AXBOROT XAVFSIZLIGI

TOSHKENT

32

7-13

O'ZBEKISTON RESPUBLIKASI OLIY VA O'RTA MAXSUS
TA'LIM VAZIRLIGI

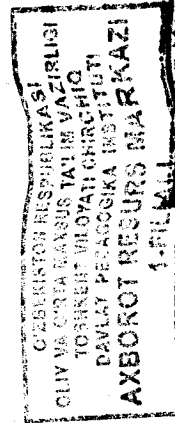
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

S.K. GANIYEV, M.M. KARIMOV, K.A. TASHEV

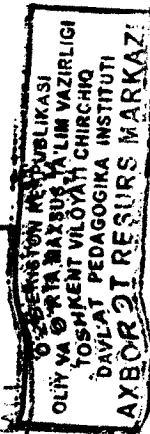
AXBOROT XAVFSIZLIGI

O'zbekiston Respublikasi Oliy va o'rta maxsus ta'lim vazirligi tomonidan oliy
o'quv yurtlarining "5330500 – Kompyuter injiniringi", "5330600 – Dasturiy
injiniringi", "5330100 – Telekommunikatsiya texnologiyalari", "5350200 –
Televizion texnologiyalar", "5350300 – Axborot kommunikatsiya texnologiyalari
sohasida iqtisodiyot va menejment", "5350400 – Axborot texnologiyalari
sohasida kasb ta'lim", "5350500 – Pochta aloqasi texnologiyasi",
"5350600 – Axborotlashirish va kutubxonahunoslik" ta'lim yo'nalishlari
talabalari uchun darslik sifatida tavsiya etilgan

Professor S.K. Ganiyev tahriri ostida



8670



TOSHKENT – 2017

UO'K: 004.056 (075.8)
KBK 32.973-018.2
G-19

G-19 S.K. Ganiyev, M.M. Karimov, K.A. Tashev. Axborot xavfsizligi. – I.: «Fan va texnologiya», 2017, 372 bet.

ISBN 978-9943-11-366-4

"Axborot xavfsizligi" fani bo'yicha darslik tayanch oliy o'quv yurti Toshkent axborot texnologiyalari universitetining "Axborot xavfsizligi" kafedrasini professor-o'qituvchilari tomonidan tayyorlangan bo'lib, unda axborot xavfsizligi tushunchasi va uning vazifalari, axborot xavfsizligiga bo'ladigan tahdidlar, hujumlar va zaifliklar, axborot xavfsizligi sohasiga oid xalqaro va milliy me'yoriy-huquqiy baza, xavfsizlik modellari, axborotni kriptografik himoyalash, identifikatsiya va autentifikatsiya, kompyuter viruslari va zararkunanda dasturlar bilan kurashish mexanizmlari, axborotni himoyalashda tammoqlararo ekranning o'zini, operatsion tizim himoyasi, axborotni sirqib chiqish kanallari va ularni aniqlash hamda obyektlarni inijener himoyalash va texnik qo'riqlash masalalari keltirilgan.

Darslik oliy o'quv yurti talabalari uchun mo'ljallangan bo'lib, undan axborot texnologiyalari, kompyuter tizimlari xavfsizligi sohasida faoliyat ko'rsatuvchilar ham foydalanishlari mumkin.

Учебник по дисциплине "Информационная безопасность" подготовлен профессорско-преподавательским составом кафедры "Информационная безопасность" Ташкентского университета информационных технологий, являющимся базовым учебным заведением по данному направлению. В учебнике раскрыто понятие информационной безопасности, рассмотрены задачи обеспечения безопасности, виды угроз, атак и присущие средства защиты недостатки. Рассмотрены также международные и национальные нормативно-правовые документы по безопасности, модели безопасности, криптографическая защита информации, вопросы идентификации и аутентификации, методы и механизмы борьбы с компьютерными вирусами и вредоносными программами, роль межсетевых экранов, методы защиты операционных систем, каналы утечки информации и способы их выявления, методы инженерной защиты объектов и их технической охраны.

Учебник предназначен для студентов высших учебных заведений, также будет полезен для всех специалистов, профессиональная деятельность которых связана с обеспечением информационной безопасности в компьютерных системах и сетях.

Textbook based on subject "Information security" for higher educational institution of the Tashkent University of Information Technologies which is prepared by the department "Information security", there was given concept of information security and its objectives, threats, attacks and vulnerabilities in information security, international and national normative-judicial base which related to information security sphere, security models, cryptographic protection of information, identification and authentication, mechanisms to combat with computer viruses and harmful programs, the role firewalls to protect information, protection of operation system, information leakage channels and determine them also engineer protection and technical defending of objects.

Students and people who works in information technologies, security of computer systems sphere.

UO'K: 004.056 (075.8)
KBK 32.973-018.2

Taqrizchilar:

Igamberdiyev X.Z. – Toshkent davlat texnika universiteti "Boshqarishda axborot texnologiyalari" kafedrasini professori, texnika fanlari doktori;
Ahmedova O.P. – "Unicon.UZ" DUK, Kriptografiya ilmiy-tadqiqot bo'limi boshlig'i, t.f.n.

ISBN 978-9943-11-366-4

© «Fan va texnologiya» nashriyoti, 2017.

MUQADDIMA

Kompyuter texnikasi va axborot tizimlarining iqtisodida, boshqarishda, aloqada, ilmiy tadqiqotlarda, ta'limda, xizmat ko'rsatish sohasida, tijorat, moliya va inson faoliyatining boshqa sohalarida qo'llanilishining rivoji axborotlashirish va, umuman, jamiyat rivojini belgilovchi yo'nalish hisoblanadi. Kompyuter texnikasining qo'llanishi evaziga erishiluvchi samara axborot ishlashni ko'laminig oshishi bilan ortib boradi. Ushbu texnikaning qo'llanish sohalarini va ko'lami uning ishlashining ishonchligi va barqarorligi muammolari bilan bir qatorda unda aylanuvchi axborot xavfsizligini ta'minlash muammosini tug'diradi.

Axborot xavfsizligi – axborotning nomaqbul (axborot mu-nosabatlarning tegishli subyektlari uchun) oshkor qilinishidan (konfidensialligining buzilishidan), buzilishidan (yaxlitligining buzilishidan), sirqib chiqishidan, yo'qotilishidan, modifikatsiyala-nishidan yoki foydalanuvchanlik darajasining pasayishidan hamda noqonuniy tirajlanishidan himoyalanganligi. Ushbu hodisalarning sababchisi tasodifiy ta'sirlar yoki buz'unchining (niyati buzuqning) atayin ruxsatsiz foydalanishi natijasidagi ta'sirlar bo'lishi mumkin.

Jamiyatning jadal sur'atlarda axborotlashirishi sababli axborot xavfsizligi muammosi nihoyatda dolzarb va doimo shunday bo'lib qoladi.

Kitobning birinchi bobida axborot xavfsizligi tushunchasi va uning vazifalari bayon etilgan. Milliy xavfsizlik tushunchasiga ta'rif berilib, uning tashkil etuvchilari batafsil yoritilgan. Axborot xavfsizligini ta'minlashning asosiy vazifalari keltirilib, shaxsning, jamiyatning va davlatning axborot muhitidagi manfaatlari bayon etilgan. Xavfsizlik siyosati, axborot xavfsizligi arxitekturasini va strategiyasi va ular orasidagi bog'liqlik masalalari ham ushbu bobdan o'rin olgan.

Kitobning ikkinchi bobi axborot xavfsizligiga bo'ladigan tahdidlar, hujumlar va zaifliklarga bag'ishlangan. Axborot xavfsiz-ligiga tahdidlar va zaifliklari tahlil etilib, ularning aktivlarga zarar

yetkaza olishlari uchun birlashishlari lozimligi misollar yordamida ko'rsatilgan. Axborotning maxfiyligini, yaxlitligini va foydalanuvchanligini buzish usullariga alohida e'tibor berilgan.

Kitobning uchinchi bobi axborot kommunikatsiya tizimlarida axborot xavfsizligini ta'minlash, boshqarish sohasiga oid xalqaro va milliy me'yoriy-huquqiy bazaga bag'ishlangan. Davlat va xususiy korxona hamda tashkilotlarda mavjud axborot kommunikatsiya tizimlarida axborot xavfsizligini ta'minlashda qo'llaniladigan me'yoriy huquqiy hujjatlar ko'rib chiqilgan.

Kitobning to'rtinchi bobi xavfsizlik modellari – diskretion, mandatlil va rolli modellarga bag'ishlangan. Diskretion modellarda foydalanishni boshqarish foydalanuvchilarga ma'lum obyektlar ustida ma'lum amallarni bajarish vakolatini berish yo'li bilan amalga oshirilishi, mandatlil modellarning foydalanishni xufiya holda – tizimning barcha subyektlar va obyektlariga xavfsizlik sathlarini belgilash orqali boshqarishi, rolli modelning xavfsizlikning tatbiqiy siyosatini akslantirishi batafsil bayon etilgan.

Kitobning beshinchi bobi axborotni kriptografik himoyalash usullari va vositalariga bag'ishlangan bo'lib, uzatiladigan ma'lumotlarni himoyalashda qo'llaniladigan simmetrik shifrlash tizimlarining strukturasi, algoritmlari va ular uchun foydalaniladigan kalitlarni taqsimlash sxemalari keltirilgan. Asimmetrik shifrlash tizimlariga oid kriptografik o'zgartirish sxemalari va shifrlash algoritmlarining matematik asoslari haqida so'z yuritilib, asimmetrik algoritmlar misol tariqasida keltirilgan. Elektron raqamli imzolarni shakllantirish va haqiqiyligini tasdiqlash jarayonlarini tashkil etuvchi algoritmlar tavsiflangan, rivojlangan davlatlarning elektron raqamli imzolari haqidagi standartlari keltirib o'tilgan. Undan tashqari ushbu bobda kriptografiyaning steganografik usullari, ularning turlari va texnologiyalari haqida qisqacha to'xtalib o'tilgan. Ushbu bobdan kriptografik algoritmlarni tahlillash usullari va vositalari ham o'rin olgan.

Kitobning oltinchi bobida tizimning foydalanuvchilar bilan o'zaro aloqasidagi asosiy jarayonlar – foydalanuvchi harakatini autentifikatsiyalash, avtorizatsiyalash va ma'murlash, bir va ko'p martali parollar hamda raqamli sertifikatlar asosidagi autentifikatsiyalash xususiyatlarining tahlili o'rin olgan. Foydalanuvchini

identifikatsiyalash va autentifikatsiyalashning namunaviy sxemalari keltirilgan. Simmetrik va asimmetrik kriptialgoritmlarga asoslangan qat'iy autentifikatsiyalashga alohida e'tibor berilib, jumladan, Kerberos protokoli muhokama etilgan. Ushbu bobdan biometrik identifikatsiyalash va autentifikatsiyalash vositalarining tavsifi ham o'rin olgan.

Kitobning yettinchi bobi kompyuter viruslari va zararkunanda dasturlar bilan kurashish mexanizmlariga bag'ishlangan. Kompyuter viruslarining tasnifi keltirilib, virus hayot sikli bosqichlari tahlilangan, viruslar va boshqa zarar keltiruvchi dasturlarning asosiy tarqalish kanallari ko'rilgan. Virusga qarshi dasturlarning asosiy muhokama etilib, himoyaning profilaktik choralari yoritilgan. Virusga qarshi himoya tizimini qurishdagi asosiy bosqichlar batafsil bayon etilgan.

Kitobning sakkizinchi bobi axborotni himoyalashda tarmoqlararo ekranlarning o'rni bag'ishlangan. Tarmoqlararo ekranlarning funksiyalari tahlili, ularning OSI modelining sathlarida ishlashi bo'yicha, xususiyatlari muhokama etilgan. Tarmoqlararo ekranlar asosidagi tarmoq himoyasining sxemalari keltirilgan.

Kitobning to'qqizinchi bobi operatsion tizim xavfsizligini ta'minlash muammolariga bag'ishlangan bo'lib, himoyalangan operatsion tizim tushunchasi, himoyalangan operatsion tizimni yaratishdagi yondashishlar va himoyalashning ma'muriy choralari bayon etilgan. Operatsion tizimni himoyalash qismitizimining asosiy funksiyalari hamda axborotni himoyalashda dasturiy ilovalarning qo'llanilishi masalalariga alohida e'tibor berilgan.

Kitobning o'ninchi bobi axborot sirqib chiqish kanallariga bag'ishlangan bo'lib, axborot sirqib chiqadigan texnik kanallar va ularning tasnifi keltirilgan. Axborot sirqib chiqadigan radioelektron, akustik, optik, moddiy kanallarning axborot eltuvchilari, informativligi, davriyligi va strukturalari yoritilgan. Axborot sirqib chiqadigan texnik kanallarni aniqlash usullari va vositalari bayon etilgan. Ushbu bobdan obyektlarni injener himoyalash va texnik qo'riqlash masalalari ham o'rin olgan.

Ilovalarda axborotni himoyalashning dasturiy vositalarini yaratish namunalari va atamalarining o'zbek, rus, ingliz tillaridagi izohli lug'ati keltirilgan.

I BOB. AXBOROT XAVFSIZLIGI TUSHUNCHASI VA UNING VAZIFALARI

1.1. Milliy xavfsizlik tushunchasi

Hozirda 29-avgust 1997-yili qabul qilingan "O'zbekiston Respublikasining milliy xavfsizligi konsepsiyasini tasdiqlash to'g'risida" qonuni amalda. Ushbu qonunga asoslanib, milliy xavfsizlik tushunchasiga quyidagicha ta'rif berish mumkin.

O'zbekiston Respublikasining milliy xavfsizligi deganda O'zbekiston Respublikasining suverenitetini ifodalovchi va hokimiyatning yagona manbai hisoblanuvchi ko'p millatli xalqning xavfsizligi tushuniladi.

Milliy xavfsizlikning, shartli ravishda, quyidagi tashkil etuvchilarini ko'rsatish mumkin:

- iqtisodiy xavfsizlik;
- ichki siyosiy xavfsizlik;
- ijtimoiy xavfsizlik;
- ma'naviy xavfsizlik;
- xalqaro xavfsizlik;
- axborot xavfsizligi;
- harbiy xavfsizlik;
- chegaraviy xavfsizlik;
- ekologik xavfsizlik.

Iqtisodiy xavfsizlik – shaxs, jamiyat va davlatning iqtisodiy sohadagi hayotiy muhim manfaatlarining ichki va tashqi tahdidlardan himoyalanganligi. Iqtisodiy xavfsizlikka binoan xalq o'zining iqtisodiy rivojlanish yo'llari va shakllarini tashqaridan aralashishsiz va bosimsiz mustaqil ravishda aniqlay oladi.

Ichki siyosiy xavfsizlik – hokimiyat institutlarining barqarorligi va samaradorligi, hokimiyat tuzilmalarining siyosiy jarayonlarni nazoratlash qobiliyati, aksariyat fuqarolar tomonidan madadlashga erishish, jamiyatda siyosiy barqarorlikni ta'minlovchi, samarali faoliyat yurituvchi nodavlat siyosiy institutlarning mavjudligi bilan

xarakterlanadi. Ichki siyosiy xavfsizlikka binoan siyosiy munosabatlar sohasida qarama-qarshilik, siyosiy ekstremizmning ommaviy tus olishi, hokimiyat bilan xalq orasida qarama-qarshilik bo'lmaydi. Fuqarolarning siyosiy ongi holati va jamiyatning siyosiy madaniyati jamiyatning xavfsiz siyosiy rivojiga jiddiy ta'sir ko'rsatadi.

Ijtimoiy xavfsizlik – shaxs, oila va jamiyatning hayotiy muhim manfaatlarining ichki va tashqi tahdidlardan himoyalanganligi. Ijtimoiy xavfsizlikning obyekti - milliy va ijtimoiy siyosat tomonidan tartibga solinuvchi xalq turmushi sifati va darajasini ta'minlovchi ijtimoiy tizimning barcha asosiy elementlari. Ijtimoiy rivojlanish strategiyasi, ularning uzoqligiga, kambag'allik darajasiga, turmush darajasidagi mintaqaviy mutanosibligiga, ta'lim va sog'liqni saqlash sifati, jamiyatdagi ma'naviyat va madaniyatning umumiy darajasiga va nihoyat, demografik muammolariga ta'siri ma'lum.

Ma'naviy xavfsizlik – bugungi kunda inson ma'naviyatiga qarshi yo'naltirilgan, bir qarashda arzimaz bo'lib tuyuladigan kichkina xabar ham axborot olamidagi globalashuv shiddatidan kuch olib, ko'zga ko'rinmaydigan, lekin zararini hech narsa bilan qoplab bo'lmaydigan ulkan ziyon yetkazishi mumkin. Ayniqsa, ommaviy madaniyat degan niqob ostida ahloqiy buzulqilik va zo'ravonlik, individualizm, egotsentrizm g'oyalarini tarqatish, kerak bo'lsa, shuning hisobidan boylik o'ttirish, boshqa xalqlarning necha ming yillik an'ana va qadriyatlarini, turmush tarzining ma'naviy negizlariga bepisandlik, ularni qo'porishga qaratilgan xatarli tahdidlar odamni tashvishga solmay qo'ymaydi. Hozirgi vaqtda axloqsizlikni mensimasdan, eskilik sarqiti deb qarash bilan bog'liq qadriyatlarini mensimasdan, inson hayoti, oila muqaddasligi va holatlar bugungi taraqqiyotga, inson hayoti, oila muqaddasligi va yoshlar tarbiyasiga katta xavf solmoqda va ko'pchilik butun jahonda bamioli balo-qazodek tarqalib borayotgan bunday xurujlarga qarshi kurashish naqadar muhim ekanini anglab olmoqda.

Xalqaro xavfsizlik – xalqaro munosabatlar nazariyasida xalqaro xavfsizlik deganda dunyo hamjamiyatining barqarorligini ta'minlovchi xalqaro munosabatlar holati tushuniladi. Boshqacha aytganda, xalqaro xavfsizlik – xalqaro munosabatlar subyektlariga