The Light of Islam

Volume 2020 | Issue 4 Article 19

2020

ON ENSURING INFORMATION SECURITY FOR INSTITUTIONS OF HIGHER EDUCATION

Xikmatilla Nigmatov
INTERNATIONAL ISLAMIC ACADEMY OF UZBEKISTAN, Professor, «Department of Modern Information and Communication Technologies», x.nigmatov@iiau.uz

Alisher Muhammadiyev
INTERNATIONAL ISLAMIC ACADEMY OF UZBEKISTAN, Teacher, a.muhammadiev@iiau.uz

DOI: 10.47980/TLOI/2020/4/13

OLIY O'QUV MUASSASALARIDA AXBOROT XAVFSIZLIGINI TA'MINLASH TO'G'RISIDA

ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЯХ

ON ENSURING INFORMATION SECURITY FOR INSTITUTIONS OF HIGHER EDUCATION

Xikmatilla NIGMATOV,
INTERNATIONAL ISLAMIC ACADEMY OF UZBEKISTAN, Professor, «Department of Modern Information and Communication Technologies» x.nigmatov@iiau.uz
11, A.Kadiri, Tashkent, 100011, Uzbekistan

Alisher MUHAMMADIYEV,
Teacher, a.muhammadiev@iiau.uz

Annotatsiya: Ushbu maqola bugungi kunda eng dolzarb, ahamiyatli va zarur hisoblangan mavzulardan hisoblangan axborotlar havfsizligini ta'minlashga bag'shlangan. Bunga sabablardan biri pandemiya sababli butun dunyo aholisi kompyuter tarmoqlari orqali raqamli boshqaruv tizimiga o'tkanligi hisoblanadi. Jumladan, Oliy o'quv uyrtlarimiz, xalq ta'lim muassasalari ham masofaviy tizimida videodarslar olib bormoqdalar.

Shuning uchun ushbu maqolada oliy o'quv muassasalarining kompyuter tizim va tarmoqlarida ma'lumotlarni xavfsizligini ta'minlash uchun qanday himoyalash me'zonidan va vositalaridan foydalanish kerak degan savollarga bajarilayotgan ilmiy tadqiqotlar asosida javob berishga parakat qilingan.

Hozirgi kunda barcha o'quv uyrtlari o'zining kompyuter tizimi va tarmoqlariga ega bo'lib, barcha qag'ozli, xisobkitob va tashkiliy ishlarini, hamda dars berish jarayonini kompyuterlarda bajarmoqdalar. Ana shu kompyuterlarda saqlanayotgan, ma'lumotlarni kommutatsion tarmoqlari orqali uzatish yoki qabul qilish jarayonlarida ularning havfsizligini ta'minlash masalalariga qaratilgan. Maqolada axborot xavfsizligi nuqtai nazaridan axborotni turkumlanishi, axborotni himoyalash tizimimi va ma'lumotlarni optimal boshqarishga suyanib, axborot tizimlarining lokal tarmoqlarida axborot himoyasining masalalari tahlil qilingan.

Kompyuter tarmoqlarining aloqa kanallari orqali uzatilayotgan ma'lumotlar xato bo'lib va kechikib borishligi tahlil qilinib asosiy me'zon (kriteriya) sifatida qanday parameter va xarakteristikalardan foydalanish kerakligi yoritilib berilgan. Har bir o'quv muassasasining axborat almashinish strukturasiga nimalar kirishligi ham belgilab berilgan. Oliy o'quv yurtlarida va ilmiy tadqiqot institutlarida ishlatilayotgan kompyuter tizimlari va tarmoqlarida axborotlarni himoyalashga katta e'tibor berish kerakligi, havf-xatarlarni va xujumlarni bartaraf etish uchun tashkiliy texnikaviy, tashkiliy huquqiy, kriptografik vositalardan keng foydalanish lozim ekanligi isbotlab berilgan. Axborotlarni himoyalashda texnik va iqtisodiy parametrlarini hisobga oladigan asosiy me'zon sifatida har bir axborotning maxfiyligi, zarurligi, uning qiymati hisobga olish kerakligi taklif etilgan.

Ushbu maqola kompyuter tizimi va tarmoqlarida axborotlarni havfsizligini boshqarish yonalishi bo'yicha ilmiy tadqiqotlar olib borayotganlar uchun mo'ljallangan.

Калит сўзлар: *telekommunikatsion tizim, havfsizlikni ta'minlash, himoya vositalari, axborot turlari, o'quv muassasalari, kompyuter tarmoqlari.*

Аннотация: Эта статья посвящена одной из самых актуальных и востребованных тем – обеспечению информационной безопасности. Одной из причин этого является то, что из-за вспыхнувшей пандемии население всего мира перешло на цифровую систему управления через компьютерные сети. В результате основная часть системы высшего, среднего и специального образования перешла на формы дистанционного обучения.

В этой статье мы попытались ответить, основываясь на научных исследованиях, на вопросы, связанные с тем, какие стандарты и средства защиты должны использоваться для обеспечения безопасности данных в компьютерных системах и сетях высших учебных заведений. В настоящее время все учебные заведения имеют свои компьютерные системы и сети, выполняют все необходимые расчетные и организационные работы, а также осуществляют учебный процесс на базе компьютеров. Мы сфокусировались на вопросах обеспечения их безопасности в процессах передачи или приема данных через коммутационные сети, имеющиеся на этих компьютерах.

В статье проанализированы вопросы защиты информации в локальных сетях информационных систем на основе систематизации информации с точки зрения информационной безопасности, системы защиты информации и оптимального управления данными.

Анализируя, как данные, передаваемые по каналам связи компьютерных сетей, доставляются с ошибками и задержками, мы получаем представление о том, какие параметры и характеристики следует использовать в качестве основного критерия. Что входит в структуру информационного обмена каждого учебного заведения. Доказано, что в компьютерных системах и сетях, используемых в высших учебных заведениях и научно-исследовательских институтах, необходимо уделять большое внимание защите информации, широко использовать организационно-технические, организационно-правовые, криптографические инструменты для устранения рисков и атак. В качестве основного критерия, учитывающего технические и экономические параметры защиты информации, предлагается учитывать конфиденциальность, необходимость каждой информации, ее ценность.

Эта статья предназначена для тех, кто проводит научные исследования по направлению Управления информационной безопасностью в компьютерных системах и сетях.

Ключевые слова: *телекоммуникационная система, обеспечение безопасности, средства защиты, виды информации, учебные заведения, компьютерные сети.*

Abstract: This article is devoted to one of the most relevant and demanded topics - information security. One of the reasons for this is that because of the pandemic, the world's population has switched to a digital management system through computer networks. As a result, the main part of the system of higher, secondary, and special education switched to the forms of distance learning.

In this article, we tried to answer, based on scientific research, the questions related to what standards and safeguards should be used to ensure the security of data in computer systems and networks of higher education institutions. At present, all educational institutions have their computer systems and networks, perform all the necessary calculations and organizational work, and also carry out the educational process based on computers. We focused on the issues of ensuring their security in the process of transmitting or receiving data through the switching networks available on these computers.

The article analyzes the issues of information security in local networks of information systems, based on the systematization of information from the point of view of information security, information security system, and optimal data management.

By analyzing how data transmitted over communication channels of computer networks are delivered with errors and delays, we get an idea of what parameters and characteristics should be used as the main criterion. It has been proved that in computer systems and networks used in higher educational institutions and research institutes, it is necessary to pay great attention to the protection of information, to widely use organizational, technical, legal, cryptographic tools to eliminate risks and attacks. As the main criterion, taking into account the technical and economic parameters of information protection, it is proposed to take into account confidentiality, the need for each information, and its value.

This article is intended for those who research the field of information security management in computer systems and networks.

Keywords: *telecommunications system, security, security tools, types of information, educational institutions, computer networks.*

КИРИШ

Ushbu maqolani yozishdan maqsad hozirgi kunda pandemiya sababli har bir o'quv muassasalarida videodarslar tashkil qilinib, darslarni axborot kommunikatsiya tarmoqlari orqali olib borilmoqda. Ushbu uzatish va qabul qilish jarayonida axborotlarni havfsizligini ta'minlash masalasi juda katta axamiyatga ega bo'lib qolganligi barchaga ma'lum. Har bir ma'lumot, xabar yoki axborot o'z qiymatiga ega bo'la boshladi. Ya'ni o'z vaqtida yetkazib berilmagan yoki xato va soxtalashib qabul qilingan har qanday ma'lumot qabul qiluvchini jumladan, o'quvchi yoki talabani, umuman barcha boshqaruv tizimini no'to'g'ri qaror chiqarishiga olib keladi. Bularni to'g'rilash esa katta ma'naviy va moliyaviy harajatlarga olib kelishi mumkin. Keng kompyuterlashtirilgan va axborotlashtirilgan zamonaviy jamiyatda real qadriyatlarga ega bo'lish, ularni boshqarish, qadriyatlarni uzatish va ularga murojaat qilish ko'pincha nomoddiy axborotlarga, ya'ni mavjud bo'lishi fizik tashuvchidagi birorta yozuv bilan bog'lanishi majburiy bo'lmagan axborotlarga asoslangandir. Shunga o'xshash, ba'zida yuqori axamiyatga ega bo'lgan maxfiy axborotni ishlatishga, o'zgartirishga, nusxalashga jismoniy va xuquqiy shaxslarning vakolatlari aniqlanadi. Shuning uchun axborotni maxfiyligi va butunligini ta'minlash bilan bog'liq bo'lgan barcha kerakli funktsiyalarni amalga oshirish uchun samarali vositalarni yaratish va ishlatish juda muhimdir.

O'rganilganlik darajasi. Shu bugungi kunga qadar olimlar ushbu yo'nalish bo'yicha olib borilgan ilmiy tadqiqotlarida axborotlarni o'z qiymatiga ega ekanligini hisobga olishmagan. Faqat Rossiya olimlaridan Vadim Nikolaevich Roginskiy, V.G.Kulakov, A.V.Sokolov, V.I.Zagorodniy, D.P.Zegjda, A.A.Malyuk va boshqalar axborot havfsizligi bilan shug'ullangan olimlar asosan texnikaviy vositalarga e'tibor berib axborotlarning turiga va ularning qiymatga ega ekanliklarini hisobga olmaganlar.

ASOSIY QISM

Insoniyatning XXI asrga kirib kelishi jamiyat hayotining xamma soxalarida axborot texnologiyalarini jadal rivojlanishi bilan chambarchas bog'liqligi kengayeb bormoqda. Axborot tobora ko'p jihatdan davlatning strategik resursi, ishlab chiqaruvchi kuchi va qimmatbaho maxsuloti bo'lib bormoqda. Bu davlatlarni, tashkilotlarni va alohida olingan fuqarolarni opponentlarga tegishli bo'lmagan axborotga ega bo'lish hisobiga, hamda raqobatchining yoki g'arazchining axborot resurslariga zarar yetkazish va o'zining axborot resurslarini himoya qilish hisobiga ustunlikka erishishga intilishini keltirib chiqaradi.

Hozigi kunda, ayniqsa bozor iqtisodiyatiga o'tish sababli har qanday axborot o'z qiymatiga ega bo'la boshladi. Ya'ni o'z vaqtida yetkazib berilmagan yoki xato va soxtalashib qabul qilingan har qanday ma'lumot qabul qiluvchini yoki boshqaruv tizimini no'to'g'ri qaror chiqarishiga olib keladi.

Axborot xavfsizligi nuqtai nazaridan axborotni quyidagicha turkumlash mumkin:

• maxfiylik — aniq bir axborotga faqat tegishli shaxslar doirasigina kirishi mumkinligi, ya'ni foydalanilishi qonuniy xujjatlarga muvofiq saqlab

qo‘yilib, hujjatlashtirilganligi kafolati. Bu bandning buzilishi o‘g‘irlik yoki axborotni oshkor qilish deyiladi;

• konfidentsiallik - ishonchliligi, tarqatilishi mumkin emasligi, mahfiyligi kafolati;

• yaxlitlik — axborot boshlang‘ich ko‘rinishda ekanligi, ya’ni uni saqlash va uzatishda ruhsat etilmagan o‘zgarishlar qilinmaganligi kafolati; bu bandning buzilishi axborotni soxtalashtirish deyiladi;

• autentifikatsiya — axborot zahirasi egasi deb e’lon qilingan shaxc haqiqatan ham axborotning egasi ekanligiga beriladigan kafolat; bu bandning buzilishi xabar muallifini soxtalashtirish deyiladi;

• apellyatsiya qilishlik — yetarlicha murakkab kategoriya, lekin elektron biznesda keng qo‘llaniladi. Kerak bo‘lganda xabarning muallifi kimligini isbotlash mumkinligi kafolati.

Yuqoridagidek, axborot tizimiga nisbatan quyidagicha tasnifni keltirish mumkin:

• ishonchlilik -- tizim me’yoriy va g‘ayri tabiiy hollarda rejalashtirilganidek o‘zini tutishlik kafolati;

• aniqlilik — hamma buyruqlarni aniq va to‘liq bajarish kafolati;

• tizimga kirishni nazorat qilish - turli shaxc guruxlari axborot manbalariga har xil kirishga egaligi va bunday kirishga cheklashlar doim bajarilishlik kafolati;

• nazorat qilinishi — istalgan paytda dastur majmuasining hoxlagan qismini to‘liq tekshirish mumkinligi kafolati;

• identifikatsiyalashni nazorat qilish — hozir tizimga ulangan mijoz aniq o‘zini kim deb atagan bo‘lsa, aniq o‘sha ekanligining kafolati;

• qasddan buzilishlarga to‘sqinlik qilish — oldindan kelishilgan me’yorlar chegarasida qasddan xato kiritilgan ma’lumotlarga nisbatan tizimning oldindan kelishilgan holda o‘zini tutishi.

Axborotni himoyalashning maqsadlari quyidagilardan iborat bo;ladi:

• axborotning kelishuvsiz chiqib ketishi, o’girlanishi, yo‘qotilishi, o‘zgartirilishi, soxtalashtirilishlarning oldini olish;

• shaxc, jamiyat, davlat xavfsizliligiga bo‘lgan havf-xatarning oldini olish;

• axborotni yo‘q qilish, o‘zgartirish, soxtalashtirish, nusxa ko‘chirish, to‘siqlash bo‘yicha ruxsat etilmagan harakatlarning oldini olish;

• hujjatlashtirilgan axborotning miqdori sifatida huquqiy tartibini ta’minlovchi, axborot zahirasi va axborot tizimiga har qanday noqonuniy aralashuvlarning ko‘rinishlarining oldini olish;

• axborot tizimida mavjud bo‘lgan shahsiy ma’lumotlarning shahsiy maxfiyligini va konfidentsialligini saqlovchi fuqarolarning konstitutsion huquqlarini himoyalash;

• davlat sirini, qonunchilikka mos hujjatlashtirilgan axborotning konfidentsialligini saqlash;

• axborot tizimlari, texnologiyalari va ularni ta’minlovchi vositalarni yaratish, ishlab chiqish va qo‘llashda sub’ektlarning huquqlarini ta’minlash hisoblanadi.

Axborot-kommunikatsiyalar texnologiyalarining ommaviy ravishda qog‘ozsiz avtomatlashtirilgan asosida boshqarilishi sababli axborot xavfsizligini ta’minlash murakkablashib va muhimlashib bormoqda. Shuning uchun ham avtomatlashtirilgan axborot tizimlarida axborotni ximoyalashning yangi zamonaviy texnologiyasini yaratishga to’g’ri kelmoqda.

Zamonaviy kompyuter tizimlari va tarmoqlari, Internet yomon niyatli odamlarga muhim maxfiy axborotni o‘g‘irlash, buzish yoki xalaqitlarga uchratish maqsadida korxonalar va tashkilotlarning ichki tarmoqlariga bostirib kirish uchun ko‘plab imkoniyatlar beradilar. Shu sababli hozirda insonlarni va jamiyatni axborot xavfsizligini va axborotni himoya qilishni ta’minlash muammosini kompleks yechishni dolzarb ravishda kerakligi paydo bo‘lmoqda.

Shu bilan birga ta’kidlash kerakki, o‘tkazilayotgan aktiv faol tadqiqotlarga qaramasdan, axborot xavfsizligini yaxlit tizimini yaratishni umumlashgan nazariyasi va amaliy kontseptsiyasi (yo‘nalishi) hanuzgacha yaratilmagan. Shuning uchun har bir axborot o’zining qandaydir qiymatiga ega bo’lganligi uchun shu axborot bilan ishlagan shaxslarga axborot xavfsizligini ta’minlash masalalarini barcha jabhalarida, ularning kompleksli va o‘zaro kelishilgan harakterini tushungan holda, yetarlicha tayyorgarlikka va mutaxassis sifatida mo‘ljal ola bilishga ega bo‘lishlari kerak.

Bugungi kunda kompyuter tizimi va tarmoqlarida axborotlar almashinuvi darajasi oshib borayotganligi, ma’lumotlarni hilma hilligi, ularni telekommunikatsiya tarmoqlari orqali uzatilayotgan tezligi juda yuqori ekanligi, qabul qilayotgan foydalanuvchilarga o‘z vaqtida, aniq va to‘liq yetkazib berish jarayonida axborotlarni himoyalash vazifasi asosiy masalalardan biri bo‘lib qolmoqda. Turli operatsion tizimlar bilan ishlaydigan kompyuterlarning axborot havfsizligini ta’minlash maqsadida ko‘pgina vositalar va usullar ishlab chiqilgan. Ushbu vositalar yordamida axborot xavfsizligini ta’minlash hozirgi kunda bizning akademiymizga kiritilgan yangi fan asosiga kiradi.

Zamonaviy kompyuter tizimlarini yaratilishi va global axborot tarmoqlarini paydo bo’lishi axborotni himoya qilish muammosini, xarakterini va diapazonini keskin o’zgartirdi. Keng kompyuterlashtirilgan va axborotlashtirilgan zamonaviy jamiyatda real qadriyatlarga ega bo’lish, ularni boshqarish, qadriyatlarni uzatish va ularga murojaat qilish ko’pincha nomoddiy axborotlarga, ya’ni mavjud bo’lishi fizik tashuvchidagi birorta yozuv bilan bog’lanishi majburiy bo’lmagan axborotlarga asoslangandir. Shunga o’xshash, ba’zida yuqori axamiyatga ega bo’lgan maxfiy axborotni

ishlatishga, o'zgartirishga, nusxalashga jismoniy va xuquqiy shaxslarning vakolatlari aniqlanadi. Shuning uchun axborotni maxfiyligi va butunligini ta'minlash bilan bog'liq bo'lgan barcha kerakli funksiyalarni amalga oshirish uchun samarali vositalarni yaratish va ishlatish juda muhimdir.

Axborot juda qadriyatli yoki o'ta muhim bo'lganligi sababli bunday axborotni saqlaydigan, qayta ishlaydigan yoki uzatadigan kompyuter tizimlariga nisbatan turli-tuman yomon niyatli harakatlar mumkindir. Masalan, buzg'unchi o'zini boshqa foydalanuvchi kabi ko'rsatishga intilishi, aloqa kanalini bildirmasdan eshitib olishi yoki tizim foydalanuvchilari almashayotgan axborotni ushlab olishi va o'zgartirishi mumkin. Zamonaviy kompyuter tizimlari va tarmoqlari, Internet yomon niyatli odamlarga muhim maxfiy axborotni o'g'irlash, buzish yoki xalaqitlarga uchratish maqsadida korxonalar va tashkilotlarning ichki tarmoqlariga bostirib kirish uchun ko'plab imkoniyatlar beradilar. Shu sababli hozirda insonlarni va jamiyatni axborot xavfsizligini va axborotni himoya qilishni ta'minlash muammosini kompleks yechishni dolzarb ravishda kerakligi paydo bo'lmoqda.

O'zbekiston Respulikasida jadal rivojlanayotgan informatsion-kommunikatsiya tehnologiyalari axborot himoyasi bo'yicha kompyuter tarmoq va tizimlarga alohida talab qo'yadi. Kompyuter tarmoqlari orqali aniq qiymatga ega, katta hajmdagi turli axborotlar almashinadi. Hozirgi vaqtda, bozor munosabatlariga o'tish davrida har qanday axborot undan foydalanuvchilar uchun maxsulot (tovar) hisoblanadi va har biri alohida-alohida turli qiymatga egadir (Усмонов А, Одилова З, Ниғматов Ҳ, 1984) Ma'lumki, axborot xavsizligi deganda axborotni himoyalash, ma'lumot egasi va foydalanuvchi subyektlar ma'lumot almashinuviga noma'qul ziyonlar yetkazadigan tabiiy va sun'iy hususiyatga ega qasddan yoki tasodifiy kirishlarga qarshi tuzilmani qo'llab quvvatlash, to'la qamrovli chora-tadbirni o'z ichiga oluvchi axborot himoyasi tuzilmasini saqlash, axborot xavfsizligi ta'minotini boshqarish tushiniladi. Axborot tizimiga qo'yiladigan asosiy talab tuzilmani saqlash va axborot manbasi konfedensialligi va yaxlitligi tashkil qiladi.

Himoya qilishning ishonchli tizimini qurish uchun yana yirik moddiy va moliyaviy harajatlar talab etiladi. Bu esa o'zini oqlaydi, negaki axborot ishonchligi va butunligining buzulishining oqibatlari eng og'ir oqibatlarga olib kelishi mumkin.

Axborot tarmoqlari orqali har xil tartiblarda kompyuter ma'lumotlari, tasvirli axborotlar, tovushli xabarlar kabi multimediya uzatishlari amalga oshirilmoqda. Eng e'tiborlisi, hozirgi vaqtda telealoqa mijoz tarmog'i va transporti sifatida foydalaniladigan xalqaro tarmoq Internetga ulanish jadal rivojlanmoqda, ayniqsa elektron videodarslar, telealoqa va axborot xavfsizligini ta'minlash uchun quyidagi himoya vositalari qo'llaniladi: Apparatli (uskunaviy-texnik); Dasturiy; Tashkiliy (tashkiliy-huquqiy va tashkiliy-texnikaviy); Jismoniy; Kriptografik; Huquqiy; Aloqa kanallari orqali ma'lumotlarni himoyalsh uchun maxsus vositalar va boshqalar.

Yuqorida berilgan axborot himoyasi vositalari tashkiliy-texnikaviy va tashkiliy-huquqiy, dasturiy-texnikaviy yoki texnikaviy-dasturiy kabi birga qo'shilgan holda ishlatilishi mumkin.

Axborot xavfsizligi (AX) ta'rifiga ko'ra, u nafaqat kompyuterga bog'liq, balki aloqa vositalari, salqinlatgichlar, suv, elektor, issiqlik bilan taminlash va albatta shaxsiy xizmat ishiga ko'maklashadigan tuzilmalarga ham bog'liq bo'ladi.

Axborot himoyasi axborot yuqolishining har qanday turi (o'g'irlanishi, yuqolishi, xato chiqishi, soxtalashtirilishi)ning ko'rinishida zararlarni oldini olishni ta'minlashi lozim. Axborot himoyasining o'lchov tashkiloti axborot xavfsizligi bo'yicha meyyoriy hujjatlar va amaldagi qonunlarga, axborot foydalanuvchisining qiziqishiga to'liq javobgarlikni amalga oshirishi kerak. Chunki, axborot himoya kafolati yuqori darajasi, murakkab fan-texnika masalasi uning himoyasini takomillashtirihs va ishlov berishni doim hal qilishi lozim.

Tarmoq va axborot tizimida axborot xavfsizligini ta'minlash muammosining javobi keng qamrovli va murakkab masala hisoblanadi.

Har qanday oliy o'quv yurtlari yoki ilmiy muasasalar kompyuter xonasi, buxgalteriya, turli xil global tarmoq, internetga chiqish imkoniyati bilan kompyuter tarmog'iga ulangan shaxsiy kompyuterlari bor strukturaviy bo'linmaga ega. O'rnatilgan kompyuterlar turli binolarda va bir-biridan turli masofalarda joylashgan bo'lishi mumkin.

Axborotni himoyalash tizimimi va ma'lumotlarni optimal boshqarishga suyanib, axborot tizimlarining lokal tarmoqlarida axborot himoyasining quyidagi masalalarini echishdan iborat:

– Tarmoq axborot xavfsizligi tizimini resursi, shaxsi va foydalanuvchilarni identifikatsiya qilish.

– Ro'yhatga kiritilgan ma'lumotlar bo'yicha foydalanuvchi shaxsini o'rnatish va tanish (bu printsipda ko'pgina axborot xavfsizligi modellari ishlaydi).

– Foydalanuvchilarning resursga murojatini qaydlashtirish, ruhsatsiz kirish resurslarni himoya qiladigan va foydalanuvchining noto'g'ri muomalasidan axborot xavfsizligini ta'minlash.

– Iqtisodiy bo'limlarning axborot xavfsizligini ta'minlash va xakazo.

Har bir muasasaning axborat almashinish strukturasiga quyidagilar kiradi:

1. Rektoratda yoki director xonasida joylashgan telefon tarmoqlari, kompyuter tarmoqlari orqali bog'lanishlar.

2. Dekanatlardagi, kafedralardagi, laboratoriyalardagi telefon va kompyuterlarni tarmoqga ulanishlar sxemasi.

3. Kompyuter sinflaridagi yoki laboratoriyalardagi barcha kompyuterlarining local (mahalliy) tarmog'i orqali Internetga chiqishlari.

4. Buhgalteriya, hisob-kitob bo'limlaridagi kompyuterlarning tashqi qurilmalar bilan bog'langanligi.

5. Barcha ikkilamchi bo'linmalardagi kompyuterlarning lokal yoki global kompyuter tarmog'iga ulanganligi va boshqalar kiradi.

Kompyuter tarmoqlari va tizimlarida hujumlarni aniqlovchi tizim Real Secure, Internet Scanner (AQSHda ishlab chiqarilgan) va boshqa dasturlardan foydalaniladi. Shuningdek, ruxsatsiz kirishdan himoyalash uchun Rossiyada "Informzashita" ilmiy-muhandislik korxonasi tomonidan ishlab chiqilgan Secret NETdan ham foydalaniladi.

Korporativ tarmoqlarning doimiy monitoringi (kunda 24 soat, yilda 365 kun) uchun "faol" himoya tizimi-hujumlarni aniqlovchi tizim mo'ljallangan. Bu tizim korporativ tarmoq uzellaridagi hujumlarga ta'sir ko'rsatadi va ularni bartaraf etib xavfsizlik administratoriga xabar beradi. Tarmoq xavfsizligini boshqarish aspektlarining muhim yechimlaridan biri hujumlarni aniqlash uchun mo'ljallangan. Hujum aniqlansa, boshqarish konsoli orqali administratorga yoki elektron pochtaga xabar keladi. Bundan tashqari, hujum ma'lumotlar ba'zasiga qayd qilinishi mumkin, shuningdek hujum amalga oshayotgan paytdagi hamma operatsiyalar tahlil uchun yozib qoldirilishi mumkin.

Har qanday zamonaviy axborot tizimini qurishda birqancha himoya mexanizmlarini ishlab chiqmasdan va amalga oshirmasdan turib, amaliy munosabatda bo'lish mumkin emas. Bu shunchaki oddiy (masalan, paketlar filtratsiyasi) va yetarlicha qiyin (masalan, tarmoqlararo ekranda Stateful Inspection texnologiyasini qo'llanilishi) mexanizmlar bo'lishi mumkin.

Bunday hollarning hammasida axborot himoyasi bo'limi va avtomatlashtirilgan boshqarmasi oldida bir qancha amalga oshiriladigan yoki foydalaniladigan axborot himoya mexanizmlari tashkilotda xavfsizlik siyosati qabul qilingan holatga muvoviq kelishini tekshirish masalasi paydo bo'ladi. Va bunday masala axborot tizimlarining komponentalarini yangilashni, operatsion tizimlarning komponentalarini o'zgartirishda takroriy ravishda paydo bo'ladi.

Korporativ tarmoqning hamma tugunlari uchun bu turdagi tekshiruvlarni o'tkazishga tarmoq administratorlarida yetarlicha vaqt yo'q. Axborotlarni himoyalash bo'limi va avtomatizatsiya boshqarmasi mutaxasislari axborot xavfsizligini ta'minlash mexanizmlaridan foydalangan holda himoyalanganlikni tahlillashni osonlashtiruvchi vositalarga muhtojdirlar. Avtomatlashtirish - bu jarayon skanerlaydigan dasturiy ta'minot (scanning software) yoki xavfsizlik skaneri (security scanner) deb ataluvchi himoyalanganlikni tahlillovchi vositalarga yordam beradi. Bu vositalardan foydalanish korporativ tarmoq tugunlarida zaifliklarni aniqlashga va ulardan yomon niyyatda foydalanishni bartaraf etishga yordam beradi.

Bu lokal yoki global tarmoq (internet)qa ulangan kompyuterdek, TSP/IP protokolini qo'llab-quvvatlovchi avtonom kompyuterlar ham bo'lishi mumkin. Tarmoqda ma'lum zaifliklarni yo'q bo'lishiga doimiy ishonchga tarmoq qurilmalarini skanerlash va dasturiy ta'minotdan foydalanish yo'li bilan erishish mumkin. Bu profilaktik chora tadbirlar potentsial zaiflikni o'z vaqtida topish va ularni o'sha zahoti bartaraf etishga yordam beradi.

Aloqa kanali bo'ylab axborot uzatilishi tezligini oshirish va aloqa tugunlarida kutish vaqtini kamaytirish bilan axborot kechikishini kamaytirishga erishish mumkin. Aloqa kanallaridagi xatolar sonini kamaytirishga erishish uchun esa, ma'lumotlar uzatish tizimlari halaqitga chidamliligini oshirish kerak bo'ladi, buning uchun axborot yoki taomil ortiqchaliklarini joriy etish (ular uzatish tezligi pasayishiga olib keladi), quvvatlar oshirilishi va ma'lumotlar uzatish texnik vositalarini murakkablashtirish zarur. Halaqitga chidamlilikni oshirish uchun quvvatliroq va murakkabroq texnik vositalarni qo'llash qo'shimcha moddiy xarajatlarga olib keladi, ular qiymat baholanishi orqali aniqlanadi.

Agar ideal ishonchli, himoyalangan, yuqori tezlikdagi telekommunikatsiya tarmog'ini qurish mumkin bo'lganda, axborot adresatga bir lahzada va xatosiz yetib borgan bo'lardi. Ammo bunday tizimni yaratish xarajatlari anchayin katta bo'lur edi.

Biroq, amalda telekommunikatsiya tarmog'i faoliyatida axborot bir lahzada yetib bormaydi, signallarning trakt bo'ylab o'tishi jarayonida esa, halaqitlar yoki boshqa omillar tufayli chetlanib bo'lmas xatolar yuzaga kelishi mumkin. Bundan tashqari, axborot adresatga ayrim chetlanishlar bilan yetkazilishi ham istisno qilinmaydi. Telekommunikatsiya tugunlarida axborot oqimlariga bir lahzada xizmat ko'rsatilishiga qator sabablar to'sqinlik qiladi, ular sirasida: tarmoq tugunlariga tushayotgan yuklamaning katta intensivligi barobarida berilgan yo'nalishlar bo'yicha kanallar sonining cheklanganligi; yoki mavjud aloqa tarmoqlari ishonchliligining yuqori emasligi; axborot uzatish tezligining cheklanganligi va boshqa, jumladan axborot yo'qotilishiga olib keluvchi ko'zda tutilmagan (g'ayriixtiyoriy) yoki qasddan qilingan (ko'zda tutilgan) tahdidlar kiradi.

Internet global tarmog'i bo'ylab raqamli ma'lumotlar uzatilishida ko'plab omillar, jumladan aloqa kanalaridagi halaqitlar ta'siri tufayli, IP paketlarda xatolar yuzaga keladi va bu paket takroriy yuborish uchun qaytib keladi, mana shu yetkazib berish tezligi

pasayishiga olib keladi. Ko‘pgina aniq holatlarda, agar yetkazish davomida yetkazilayotgan axborotda shifrlangan parametrning asl qiymati tasvirlanayotgan ob’ekt dinamikasi o‘zgarishi oqibatida o‘zgarsa, kechga qolish xatolardan biri bo‘lishi mumkin. Qabul qilinadigan axborot u foydalaniladigan tizimlarda kechga qolishi mavjud bo‘lganda muayyan jarayonlar nooptimal shaklda kechadi.

Aloqa kanallarida signallar o’tish jarayonida muqarrar hatolar paydo bo’lisa, kompyuter tarmoqlarida (lokal, shahar, korporativ, global) axborot sekin yetkaziladi. Bundan tashqari, axborotning manzilga ba’zi kamchiliklar bilan yetkazilishi mustasno emas. Telekommunikatsion tugunda axborotlar oqimining tez fursatda xizmat ko’rsatishiga to’sqinlik qiluvchi sabablar quyidagicha:

– tarmoq tugunlariga kiruvchi axborotlarning katta intensivligida kerakli yo’nalish bo’yicha kanallar soninig cheklanganligi;

– mavjud aloqa tarmog’ining ishonchliligini pastligi;

– axborot uzatish tezligining pastligi;

– kutilmagan (ataylab qilinmagan) yoki atayin qilingan (g’arazli) tahdid, yoki maxfiy axborot manbaiga ruxsatsiz kirish va boshqalar.

Ko’pgina aniq hollarda kechikish hatolardan biri bo’lishi mumkin parametrning haqiqiy mazmuni tavsiflangan ob’ektning dinamikasini o’zgarishi oqibatida kodlangan axborot uzatilish vaqtida o’zgaradi.

Zararning o’rtacha qiymati $\mathbf{C_{kech}}$ axborotni ushlanib qolish vaqtiga bog’liq:

$$\mathbf{C_{kech}= F(t_{kech}),}$$

– $\mathbf{t_{kech}}$ kechikish vaqti o’sishi bilan, zararning o’rtacha qiymati $\mathbf{C_{kech}}$ kattalashadi. Axborotni ushlanib qolish vaqtidan yo’qotilish qiymatini bog’liqligi $\mathbf{C_{kech}=f(t_{kech})}$ turli xarakterli bo’lishligi mumkin.

Qiymatli zarar, axborotni shartli kechikishi boshqarilayotgan ob’ekt-axborot iste’molchisi tomonidan axborotning ahamiyati aniqlanadi.

Yo’qotishning grafik qiymati $\mathbf{t_{kech}=0}$ va $\mathbf{t_{kech}=max}$ da har bir portsiya oqim uchun eng yuqori qiymatga yetadigan bo’lganda, lahzalik uzatishdagi kechikishdan hosil bo’lgan zararning va axborotni qabul qilinmasligida moliyaviy zarar kattaligining yo’qligiga muvofiq xarakterlanadi. Axborotni ushlanib qolish vaqtini egri o’sishi $\mathbf{C_{kech}=f(t_{por})}$ turli xarakterga ega bo’lishi mumkin: tekis (ravon), to’g’ri chiziqli va keskin o’sishi mumkin. Bundan tashqari, axborotning ba’zi portsiyalari chegaraviy vaqtga $\mathbf{(t_{por})}$ kechikib borishi mumkin. Axborotni tutilib turish vaqti $\mathbf{(t_{por})}$dan ko’p bo’lsa, moliyaviy zararning qiymati tezda oshadi (Нигматов Х. , 2003)

Ma’lumki, axborot iste’molchiga berilgan vaqtda qabul qilinuvchi va uzatiluvchi signalga mos ravishda, talab etiladigan darajada aniqliligi (ishonchliligi) ta’minlangan holda yetkazilishi kerak.

Foydalanilayotgan tizimda axborotni qabul qilishdagi xatolik kechikishdagi kabi yo’qotilishdek, qiymatni yo’qotish bilan xarakterlanishi mumkin bo’lgan aniqlangan jarayonni nooptimal boshqarishga olib kelishi mumkin. Tarmoq trakti bo’ylab signallarni o’tish jarayonida xatoliklar yuzaga kelishi mumkin. Har bir oqimning alohida ko’rinishi uchun xatolarning zararlik xarakteri axborot qiymati bilan bog’liq. Moliyaviy zararning maksimal qiymati boshqarilayotgan ob’ektning iqtisodiy ko’rsatkichlariga, shuningdek tugundan (tugunga) uzatish amalga oshirilayotgan kanalning turi va ko’rinishiga bog’liq bo’ladi.

Axborot himoyasi vazifasini ta’minlashdan foydalanib, axborot tizimini optimal qurish uchun axborot kechikishi va xatolardan umumiy yo’qotishlarni minimallashtirish zarur:

$$\mathbf{min[C]=min[\Sigma(C_{kech}+C_{xat})].}$$

Tarmoqlarda ushbu me’zon (minimum) yo’qotishlarni qo’llash boshqarilayotgan ob’ekt-axborot iste’molchisini texnik-iqtisodiy ko’rsatkichlarini hisobga olish imkonini beradi.

Ko’pgina aniq hollarda kerakli axborotni o’z vaqtida qabul qilmaslik yoki buzilgan yoki o’zgartirilgan axborotni qabul qilish xatolardan biri bo’lishi mumkin. Kodlangan, uzatilayotgan axborot uzatilish vaqtida yozilgan ob’ektning dinamikasini o’zgarishi sababli parametrning haqiqiy qiymati o’zgaradi. Tizim yoki ob’ektda axborotni qabul qilishda xatolikni bo’lishi aniqlangan jarayonni nooptimal ko’rinishga olib keladi. Qandaydir xatolik $\mathbf{C_{xat}}$ - qiymat bahosini aniqlaydi. Axborotni ushlanib yoki tutilib qolishidan qiymatli yo’qotilish - $\mathbf{C_{ush}}$ va $\mathbf{C_{xat}}$ - xatolik axborotni ahamiyatini aniqlaydi.

Axborot qiymati qo’yilgan maqsadga yetish uchun ob’ekt - qabul qiluvchini umumiy mehnat sarf-harajatlari tejashdan moddiy effekt sifatida aniqlanishi kerak. Umumiy hollarda maqsadga yetish:

$\mathbf{P=P_0-(C_{is}+C_p);}$ ifodasi bilan yoziladi.

Bu erda: $\mathbf{C_{is}}$, $\mathbf{C_p}$- axborot tizimi va yo’qotish qiymatlariga mos keladi.

P - bog’langan tizim ishini xarakterlaydigan ko’rsatkich;

$\mathbf{P_0}$ - absolyut aniqlik va axborot tizimini ishonchli ishlashda maksimal qiymat qabul qiluvchi ko’rsatkichi.

Oliy o’quv yurtlarida va ilmiy tadqiqot institutlarida axborot himoya vositalari va tizimlarini qurishda optimizatsiya mezoni sifatida ularni qurishga ketadigan umumiy sarf-harajatlar va kerakli axborotni olmaslik yoki noto’g’ri axborotni qabul qilish, shunungdek kerakli axborotni o’z vaqtida qabul qilib olmaslik kabi yo’qitishlarning umumiy qiymatini hisobga olish lozim bo’ladi.

Shuning uchun Internet foydalanuvchisi ushbu xavflarni oldini olish uchun quyidagi texnik yechim va tashkiliy ishlarni amalga oshirishi zarur:

1. Shaxsiy kompyuterga va mahalliy kompyuter tarmog‘iga hamda unda mavjud bo‘lgan informatsion resurslarga tashqaridan Internet orqali kirishni cheklovchi va ushbu jarayonni nazorat qilish imkonini beruvchi texnik va dasturviy usullardan foydalanish.

2. Tarmoqdagi informatsion muloqat ishtirokchilari va ular kuzatayotgan ma’lumotlarni asl nusxasiga mosligini tekshirish.

3. Ma’lumotlarni uzatish va qabul qilishda kiriptografiya usullaridan foydalanish.

4. Viruslarga qarshi nazoratchi va davolovchi dasturlardan foydalanish.

5. Shaxsiy kompyuter va mahalliy kompyuter tarmog‘iga begona shaxslarni qo‘ymaslik va ularda mavjud bo‘lgan ma’lumotlardan nusxa olish imkoniyatlarini cheklovchi tashkiliy ishlarni amalga oshirish zarur.

Bundan tashqari informatsion xavfsizlikni ta’minlash borasida Internet foydalanuvchilari orasida o‘rnatilmagan tartib qoidalari quyidagilardan iboratligi barchaga ma’lum bo’lishi kerak:

- Hech qachon hech kimga Internetdagi nomingiz va parolingizni aytmaslik.
- Hech qachon hech kimga o‘zingiz va oila a’zolaringiz haqidagi shaxsiy hamda ishxonangizga oid ma’lumotlarni Internet orqali yubormaslik.
- Internet orqali dasturlar almashmaslik.
- Internetda tarqatilayotgan duch kelgan dasturlardan foydalanmaslik. Dasturlarni faqat ishonchli egasi ma’lum bo‘lgan serverlardan ko‘chirish.
- Telegramm va Elektron pochta orqali yuborilgan «aktiv ob’ektlar» va dasturlarni ishlatmaslik, yoki qo‘shimchali o‘z-o‘zidan ochiluvchi noma’lum arxiv holidagi ma’lumotlarni ochmaslik.
- Elektron pochta xizmatidan foydalanayotgan paytda ma’lumotlarni shifrlash.
- Egasi noma’lum bo‘lgan xatlarni ochmaslik.
- Egasi ma’lum bo‘lgan va uning sifatiga kafolat beruvchi antivirus dasturlardan foydalanish va ularni muntazam yangilab borish.
- Internetda mavjud bo‘lgan informatsion resurslar va dasturlardan ularning mualliflari ruxsatisiz foydalanmaslik.
- Tarmoqdagi begona kompyuter va serverlarning IP manzillarini aniqlash va shu orqali ruxsat etilmagan serverlar va informatsion resurslarga kirish nusxa ko‘chirish, viruslar tarqatish kabi noqonuniy dasturlashtirish ishlari bilan shug‘ullanmaslik talab etiladi.

XULOSA

Keyingi yillarda olib borilgan ilmiy izlanishlar asosida quyidagi qisqa natig’alarga erishildi:

1. Axborot xavfsizligini ta’minlashning samaradorlik mezoni (kriteriyasi) tanlanib aniq masalalarni echish belgilandi.

2. Tanlab olingan tadqiqot ob’ektinining kompyuter tarmoq tuzilish strukturalari har xil variantlari tahlil etildi.

3. Kompyuter tizimi va tarmoqlarida axborotlarni himoyalashning asosiy vositalardan hisoblangan kriptografik himoyalash usullarining simmetrik va asimmetrik shifrlash (deshifrlash) usullari isbotlanib berildi.

4. Oliy o’quv yurtlarida va ilmiy tadqiqot institutlarida faoliyat etayotgan kompyuter tizimlari va tarmoqlarida axborotlarni himoyalashga katta e’tibor berish kerakligi, havf-xatarlarni va xujumlarni bartaraf etish uchun tashkiliy texnikaviy, tashkiliy huquqiy, kriptografik vositalardan keng foydalanish lozimligiga urg’u berildi.

5. Axborotlarni himoyalashda texnik va iqtisodiy parametrlarini hisobga oladigan asosiy me’zon sifatida har bir axborotning maxfiyligi, zarurligi, uning qiymati hisobga olish kerakligi taklif etildi.

ADABIYOTLAR:

1. Nigmatov H, Tursunov N. . (2018). Axborot xavfsizligi. Toshkent: Toshkent islom universiteti nashriyot-matbaa birlashmasi.
2. Nigmatov X, Umarov A. (2020). Monografiya. . Zamonaviy axborot-kommunikatsiya texnologiyalarining aloqa kanallarida axborotlarni himoyalash. Toshkent: inovatsiyon rivojlanish nashriyo-matbaa uyi.
3. Nigmatov, H. (1993). Opredelenie osnovnih kachestvennih pokazateley kompyuternih setey s raznotipnimi kanalami svyazi i izmenyaushiysya strukturoy. Toshkent.
4. Nigmatov, H. (1996). Modeli i algoritmi upravleniya setyu peredachi dannix s raznotipnimi kanalami svyazi i izmenyaushiysya strukturoy. Toshkent.
5. Nigmatov, H. (2004). Yangi axborot tehnologiyalari fanidan ta’lim berishni takomillashtirish to’g’risida. Toshkent.
6. Брагг, Р. (2001). Система безопасности Windows 2000. Москва: Вильямс.
7. Гайкович В., Першин А. (1993). Безопасность электронных банковских систем. Москва.
8. Герасименко В.А., Малюк А.А. (1997). Основы защиты информации. Москва.
9. Герасименко, В. (1994). Защита информации в автоматизированных системах обработки данных. Москва.
10. Гриняев, С. (1999). Интеллектуальное противодействие информационному оружию. Серия Информатизация России на пороге XXI века. Москва: СИНТЕГ.

11. Долотов, В. Д. Время технологий xDSL / В .Д. Долотов // Технологии и средства связи. – 2003. – № 1. – С. 36–38. . (200).
12. Завгородний, В. (2001). Комплексная защита информации в компьютерных системах: Учебное пособие для вузов. М. Логос.
13. Зегжда Д.П., Ивашко А.М. . (б.д.). Как построить защищенную информационную систему . Мир и семья.
14. Зима В.М., Молдовян А.А., Молдовян Н.А. (2001). Безопасность глобальных сетевых технологий. Петербург.
15. Каплан А., Нильсен М.Ш. (2000). Windows 2000 изнутри. Москва.
16. Кулаков, В. (2005). Информационная безопасность телекоммуникационных систем. Москва.
17. Леонова, А. (2000). Компьютерная преступность и информационная безопасность. АРИЛ.
18. Невдяев, Л. (2000). Мобилная связь 3-го поколения. Серия изданий Связь и бизнес. Москва.
19. Нигматов, Х. (2003). Введение в информационную безопасность. Ташкент: ТАДИ.
20. Нигматов, Х. (2013). Информационная безопасность. Защита информации в сетях телекоммуникации. Чимкент .
21. Нигматов, Х. (2013). Компьютерные сети и системы в IP телефонии. Чимкент : ЖЕБЕ.
22. Нигматов, Х. (2013). Системы и устройства спутниковой и мобилной радиосвязи. Чимкент : ЖЕБЕ.
23. Петренко С.А., Петренко А.А. . (2002). Аудит безопасности Intranet. Москва.
24. Ратынский, М. (2000). Основы сотовой связи. /Под редакцией Зимина Д.Б., - 2-е издание., перераб. и дополнен. Радио и связь. Москва.
25. Соколов А. В., Шенгин В.Ф. . (2002). Защита информации в распределённых корпоративных сетях и системах. Москва : ДМК – ПРЕСС.
26. Таненбаум, Э. (2003). Компьютерные сети . Питер.
27. Усмонов А, Одилова З, Ниғматов Ҳ. (1984). Upravleniye informasionnimi potokami ASU v setyax peredachi dannix. Toshkent: FAN nashr.
28. Щербаков, А. (2001). Введение в теорию и практику компьютерной безопасности. Москва: Мол-гачева.

REFERENCES

1. Nigmatov H, Tursunov N. . (2018). Axborot xavfsizligi. Toshkent: Toshkent islom universiteti nashriyot-matbaa birlashmasi.
2. Nigmatov X, Umarov A. (2020). Monografiya. . Zamonaviy axborot-kommunikatsiya texnologiyalarining aloqa kanallarida axborotlarni himoyalash. Toshkent: inovatsiyon rivojlanish nashriyo-matbaa uyi.
3. Nigmatov, H. (1993). Opredelenie osnovnih kachestvennih pokazateley kompyuternih setey s raznotipnimi kanalami svyazi i izmenyaushiysya strukturoy. Toshkent.
4. Nigmatov, H. (1996). Modeli i algoritmi upravleniya setyu peredachi dannix s raznotipnimi kanalami svyazi i izmenyaushiysya strukturoy. Toshkent.
5. Nigmatov, H. (2004). Yangi axborot tehnologiyalari fanidan ta'lim berishni takomillashtirish to'g'risida. Toshkent.
6. Bragg, R. (2001). Sistema bezopasnosti Windows 2000. Moskva: Vilyams.
7. Gaykovich V., Lershin A. (1993). Bezopasnost elektronnix bankovskix sistem. Moskva.
8. Gerasimenko V.A., Malyuk A.A. (1997). Osnovi zashiti informatsii. Moskva.
9. Gerasimenko, V. (1994). Zashita informatsii v avtomatizirovannix sistemax obrabotki dannix. Moskva.
10. Grinyayev, S. (1999). Intellektualnoye protivodeystviye informatsionnomu orujiyu. Seriya Informatizatsiya Rossii na poroge XXI veka. Moskva: SINTEG.
11. Dolotov, V. D. Vremya texnologiy xDSL / V .D. Dolotov // Texnologii i sredstva svyazi. – 2003. – № 1. – S. 36–38. . (200).
12. Zavgorodniy, V. (2001). Kompleksnaya zashita informatsii v kompyuternix sistemax: Uchebnoye posobiye dlya vuzov. M. Logos.
13. Zegjda D.P., Ivashko A.M. . (b.d.). Kak postroit zashishennuyu informatsionnuyu sistemu . Mir i semya.
14. Zima V.M., Moldovyan A.A., Moldovyan N.A. (2001). Bezopasnost globalnix setevix texnologiy. Peterburg.
15. Kaplan A., Nilsen M.Sh. (2000). Windows 2000 iznutri. Moskva.
16. Kulakov, B. (2005). Informatsionnaya bezopasnost telekommunikatsionnix sistem. Moskva.
17. Leonova, A. (2000). Kompyuternaya prestupnost i informatsionnaya bezopasnost. ARIL.
18. Nevdyayev, L. (2000). Mobilnaya svyaz 3-go pokoleniya. Seriya izdaniy Svyaz i biznes. Moskva.
19. Nigmatov, X. (2003). Vvedeniye v informatsionnuyu bezopasnost. Tashkent: TADI.
20. Nigmatov, X. (2013). Informatsionnaya bezopasnost. Zashita informatsii v setyax telekommunikatsii. Shimkent.
21. Nigmatov, X. (2013). Kompyuternie seti i sistemi v IP telefonii. Shimkent : JEBE.
22. Nigmatov, X. (2013). Sistemi i ustroystva sputnikovoy i mobilnoy radiosvyazi. Shimkent : JEBE.
23. Petrenko S.A., Petrenko A.A. . (2002). Audit bezopasnosti Intranet. Moskva.
24. Ratinskiy, M. (2000). Osnovi sotovoy svyazi. /Pod redaksiyey Zimina D.B., - 2-ye izdaniye., pererab. i dopolnen. Radio i svyaz. Moskva.
25. Sokolov A. V., Shengin V.F. . (2002). Zashita informatsii v raspredelyonnix korporativnix setyax i sistemax. Moskva : DMK – PRESS.
26. Tanenbaum, E. (2003). Kompyuternie seti . Piter.
27. Usmonov A, Odilova Z, Nig'matov H. (1984). Upravleniye informasionnimi potokami ASU v setyax peredachi dannix. Toshkent: FAN nashr.
28. Sherbakov, A. (2001). Vvedeniye v teoriyu i praktiku kompyuternoy bezopasnosti. Moskva: Mol-gacheva.