“JOURNAL OF SCIENCE-INNOVATIVE RESEARCH IN UZBEKISTAN” JURNALI
VOLUME 2, ISSUE 1, 2024. JANUARY
ResearchBib Impact Factor: 8.654/2023 ISSN 2992-8869

RIVOJLANGAN CHET EL MAMLAKATLARIDA AXBOROTNI MUHOFAZA QILISH TIZIMI HAMDA KRIPTOGRAFIK SHIFRLARNI KLASSIFIKATSIYALASH

Ilmiy rahbar: i.f.d., PhD **F.T.Jumayev**
Kompyuter tizimlari va ularning dasturiy ta’minoti
yo‘nalishi magistranti **Ikromov Husniddin Abduvoid o‘g‘li**

Annotatsiya: Ushbu maqolada Rivojlangan chet el mamlakatlaridagi axborotni muhokama qilish tizimi hamda kriptografik shifrlarni klassifikatsiyalash haqida bo‘li, maqolada bir nechta rivojlangan mamlakatlar axborot tizimi muhofazasi bayon qilingan

Kalit so‘zlar: tahdid, mohofaza, Xalqaro tarmoq, Milliy xavfsizlik agentligi, AQSh ning milliy xavfsizligini ta’minlash tizimi, Federal tekshirishlar byurosi, Buyuk Britaniyadagi axborotni himoyalash tizimi, Germaniyaning axborotni himoyalash tizimi, Fransiyada axborotni himoyalash tizimi, Rossiya Federatsiyasining axborotni himoyalash tizimi

Mamlakatning tahdidlarga mos aks ta’sir ko‘rsatish layoqatiga ega bo‘lgan axborot xavfsizlik tizimini yaratish uchun, rivojlangan chet el mamlakatlarida axborot urushining zamonaviy konsepsiyalari, o‘ziga xos xususiyatlari, axborot qurolining turlari va qo‘llash samaradorligi, shuningdek, chet el mamlakatlarida axborot xavfsizligini ta’minlash masalalari qay tarzda yechilishi haqida aniq bir tasavvurga ega bo‘lish kerak. Axborot quroli deb nomlanuvchi vositalar:

– axborot massivlarini yo‘q qilish, buzish yoki o‘g‘irlash;
– himoya tizimlarini yengish;
– qonuniy foydalanuvchilar huquqlarini cheklash;
– kompyuter tizimlarini, texnik vositalarni ishini izdan chiqarish;
– shular kabi boshqa amallarni bajaradi.

Hozirda hujumkor axborot quroliga quyidagilarni keltirish mumkin:

– ko‘payish, dasturlarga kirish, aloqa liniyalari, ma’lumot uzatish tarmog‘i orqali uzatish, boshqaruv tizimini ishdan chiqarish va shu kabi boshqa qobiliyatlarga ega bo‘lgan kompyuter viruslari;

– mantiqiy bomba – dasturiy o‘rnatma qurilmalari, signal bo‘yicha yoki aniq vaqtda harakatga keltirish uchun harbiy yoki fuqarolik infratuzilma axborot-boshqaruv markazlariga oldindan kirgiziladi;

– telekommunikatsiya tarmoqlarida axborot almashishini susaytiruvchi, davlat yoki harbiy boshqarish kanallarida axborotni soxtalashtiruvchi vositalar;

– tekshiruvchi dasturlarni neytrallash vositalari;

– obyektning dasturiy ta’minotiga raqib tomonidan ongli ravishda turli xatoliklarni kiritish. Axborot qurolini qo‘llash oqibatini kamaytirish yoki oldini olish uchun quyidagi chora-tadbirlarni ko‘rish kerak:

– axborot resurslarini fizik asosini tashkil etuvchi material-texnik obyektlarni himoyalash; – ma’lumotlar bazasi va bankini normal va uzluksiz ishlashini ta’minlash;

– ruxsat etilmagan kirishlardan, buzish yoki yo‘q qilishdan axborotlarni himoyalash;

– axborot sifatini (vaqtidaligini, aniqligini, to‘laligini va foydalana olishlikni) saqlab qolish.

Axborot qurolidan himoyalovchi dasturiy tasnifdagi amaliy tadbirlarga quyidagilar kiradi:

1. Xalqaro tarmoq orqali turli xil axborot almashinuvida iqtisodiy va boshqa tuzilmalarning ehtiyojini bashoratlash va monitoringini tashkil qilish. Buning uchun transchegara, shu qatorda Internet orqali ham, almashinuvni nazorat qilish uchun maxsus tuzilmalarni yaratish; ochiq tarmoqlarda axborot xavfsizligi tahdidlarini bartaraf etish bo‘yicha davlat va nodavlat idoralarning chora-tadbirlarini koordinatsiya qilish; xalqaro hamkorlikni tashkil etish mumkin.

2. Axborot resurslarining xavfsizligi talablariga rioya qilgan holda milliy va korporativ tarmoqlarni jahon ochiq tarmog‘lariga ulanishini ta’minlovchi axborot texnologiyalarni takomillashtiruvchi davlat dasturini ishlab chiqish.

3. Jahon axborot tarmoqlarida ishlash uchun ommaviy foydalanuvchilarni va axborot xavfsizligi bo‘yicha mutaxassislarni tayyorlash va malakasini oshirish kompleks tizimini tashkil qilish.

4. Ochiq jahon tarmoqlari foydalanuvchilarining mas’uliyatlari va majburiyatlari, reglament huquqi va axborot resurslari bilan foydalanish qoidalarining milliy qonunchilik qismini ishlab chiqish. Jahon ochiq tarmoqlari

ishlashining me’yoriy-huquqiy ta’minotini va xalqaro qonunchiligini ishlab chiqishda faol ishtirok etish.

AQSh ning milliy xavfsizligini ta’minlash tizimi. Milliy xavfsizlik agentligi (MXA-NBA) – radioelektron tutib qolish sohasida jahonda peshqadam hisoblanadi. Agentlikning maqsadi – texnik vositalar yordamida AQSh ning milliy xavfsizligini ta’minlash. AQSh ning tashqi xavfsizligini ta’minlashda Markaziy razvedka boshqarmasi (MRB-SRU)ga asosiy o‘rinlardan biri ajratilgan. U yerda boshqa davlatlar tomonidan milliy axborot infratuzilmaga qilinadigan tahdidlar haqidagi axborotlarni qidirish va qayta ishlash bo‘yicha razvedkaning imkoniyatlarini kengaytirishga yo‘naltirilgan reja ishlab chiqilgan va tatbiq qilingan. Agentura ishiga oid an’anaviy usullardan tashqari, MRB texnik yo‘l orqali yopiq ma’lumotlar bazasiga kirishni va ochiq manbalarning tahliliga katta e’tibor qaratadi. Keyingi vaqtlarda MRB axborot va kompyuter texnologiyalari bo‘yicha mutaxassislarni, jumladan xakerlar orasidan tanlashni amalga oshirmoqda. **Federal tekshirishlar byurosi** (FTB-FBR) ham, eng avvalo AQSh infratuzilmasini himoyalash nuqtai nazaridan axborot urushi doktrinasini tatbiq qilishda ishtirok etadi. AQSh da kompyuter jinoyatchiligiga qarshi kurashish maqsadida 1996-yili «Kompyuterlarni qo‘llash orqali firibgarlik va suiiste’mol qilishlar to‘g‘risida»gi federal qonun qabul qilingan va ushbu turdagi jinoyatchilik bilan kurashish bo‘yicha FTB tarkibida bo‘linma tashkil etish ko‘zda tutilgan. FTB telekommunikatsiya tarmog‘i orqali amalga oshiriladigan ayg‘oqchilik, maxfiy ma’lumotlarni oshkor qilish, davlat instansiyalarni aldash, terrorizm, xiyla ishlatish va firibgarlik kabi noxush holatlarni tekshirish bilan shug‘ullanadi. Uning tarkibiga kompyuter jinoyatchiligi bilan shug‘ullanuvchi yettita bo‘linma kiradi, ularning shtati 300 kishini tashkil qiladi. AQSh ning Mudofaa vazirligi (MV) xalqaro Internet tarmog‘ining ajdodi hisoblanib, birinchi bo‘lib mamlakatning xavfsizligiga yangi tahdidning va axborot qurolining kuchini anglab yetdi va hozirgi vaqtda harbiy sohada axborot urushi doktrinasini tatbiq qilishda yetakchi o‘rinni egallaydi. MV ilmiy kengashining ekspertlar komissiyasi axborot urushi hodisasiga qarshi harbiy telekommunikatsiya va kompyuter tarmoqlari xavfsizligini ta’minlovchi shoshilinch choralarni qabul qilish lozimligi haqida doklad tayyorladi. Pentagon harbiy avtomatlashtirilgan axborot tizimlarini «qizil buyruqlar» deb ataluvchi zaiflikka tekshirish uchun harbiy kompyuter tarmoqlarini himoyasini ta’minlash bilan shug‘ullanish maqsadida xakerlarni ishga qabul qiladi. Hozirgi kunda AQSh idoralari faoliyatidagi umumiy

tendensiya axborot urushi olib borishning asosiy tashkiliy va konseptual prinsiplarini ishlab chiqish, axborot texnologiyalarni qo‘llab yangi ish usullarini qidirish hisoblanadi.

Buyuk Britaniyadagi axborotni himoyalash tizimi. Buyuk Britaniyada axborot xavfsizligini ta’minlash davlat tizimini yaratishda axborot urushi dushmanning axborot tizimiga ta’sir etuvchi va bir vaqtda mamlakatning shaxsiy tizimlarini himoyalovchi harakatlar deb qaraladi. Buyuk Britaniyaning Razvedka va xavfsizlik bo‘yicha parlament komiteti Britaniya maxsus xizmatlari ustidan nazorat idorasi sifatida 1994- yilda tashkil etilgan. Bu komitet «Razvedka xizmatlari to‘g‘risida»gi qonunga muvofiq uchta maxsus xizmat: Maxfiy xizmat (MI5), SIS razvedkasi va Hukumat aloqa markazi tomonidan budjet mablag‘larining sarflanishini, bu xizmatlarning boshqarilishini va ularning olib borayotgan siyosatini nazorat qilish uchun tuzilgan. Secret Intelligence Service/MI6 – Buyuk Britaniyaning asosiy razvedka xizmati. SIS Tashqi ishlar vazirligi (TIV) tizimiga kiritilgan bo‘lib xorijda 87 ta qarorgohga va Londonda shtab-kvartiraga ega. SISni Bosh direktor boshqaradi va u bir vaqtning o‘zida Tashqi ishlar vazirining o‘rinbosari ham hisoblanadi. Shunday qilib, formal ravishda SIS Buyuk Britaniyaning TIV nazorati ostida hisoblanadi, biroq, shu bilan birga u to‘g‘ridan-to‘g‘ri premyer-ministrga chiqishi mumkin. Kontrrazvedka xizmati – Military Intelligence-5 (MI-5) 1909-yilda ichki xavfsizlikni ta’minlash bilan shug‘ullanuvchi maxfiy xizmatlar Byurosining ichki departamenti sifatida tuzilgan. Hukumat aloqa markazi Buyuk Britaniyaning maxsus xizmatlar tizimida radioayg‘oqchilik uchun javob beradi. Markaz TIV tarkibiga kiritilgan bo‘lib, xodimlarining soni va axborotni topish hajmi bo‘yicha mamlakatning yirik idoralaridan biri hisoblanadi.

Germaniyaning axborotni himoyalash tizimi. Axborot oqimlarining xavfsizligini ta’minlashga mas’ul koordinatsiyalovchi hukumat idorasi bo‘lib 1991-yilda tashkil etilgan Federal xavfsizlik xizmati (BSI) hisoblanadi. Bu xizmat axborot texnikasi sohasidagi xavfsizlikni ta’minlaydi. Hozirgi vaqtda BSI faoliyatining umumiy konsepsiyasi NATO va YES bilan yaqin hamkorlikda quyidagi funksiyalarni bajarilishini ko‘zda tutadi: – axborot texnologiyalarni joriy etishdagi ehtimoliy xavfni baholash; – milliy kommutatsiya tizimlarining himoyalash darajasini baholash uchun mezonlar, usullar va sinov vositalarini ishlab chiqish; – axborot tizimlarining himoyalanish darajasini tekshirish va muvofiqlik sertifikatlarini berish; – muhim davlat obyektlariga axborot tizimlarini joriy etish

uchun ruxsatnoma berish; – davlat idoralari, politsiya va boshqa idoralarda axborot almashinishda maxsus xavfsizlik choralarini amalga oshirish; – sanoat vakillariga maslahatlar berish. Xavfsizlikni ta’minlovchi boshqa davlat idoralari: – Germaniyaning federal razvedka xizmati (Bundesnachrichten-dienst /BND/). BND federal kansler boshqarmasiga bo‘ysunadigan bo‘linma hisoblanadi. BNDning shtat tarkibi 7000 kishidan ziyodni tashkil etadi, ulardan 2000ga yaqini bevosita xorijda razvedka ma’lumotlarini yig‘ish bilan band. Xodimlar orasida taxminan 70 ta turli soha vakillari: harbiy xizmatchilar, huquqshunoslar, tarixchilar, muhandislar va texnik mutaxassislar mavjud. – Konstitutsiyani himoyalash federal byurosi (Verfassungsschutz /BfV/). Ushbu byuro BND va BSI bilan bir qatorda mamlakatning uchta maxsus xizmatlaridan biri hisoblanadi va u Germaniyaning ichki ishlar vazirligiga bo‘ysunadi. Barcha federal yerlarda mahalliy ichki ishlar vazirligiga bo‘ysunadigan o‘zining mos xizmatlari mavjud. Har yili to‘plangan axborotlar asosida Konstitutsiyaga rioya etilganligi doirasidagi ish holati haqida hukumatga hisobot taqdim etiladi, unda xulosalar va tavsiyalar qilinadi. Hukumat, o‘z navbatida, aniq choralarni amalga oshirish kerakligi haqida qaror qabul qiladi. Axborotning yarmidan ko‘pini maxsus xizmat ochiq manbalardan: ommaviy axborot vositalarida chop etilgan nashrlar, Internet, majlis va mitinglarda ishtirok etish orqali yig‘adi. Axborotning bir qismi ayrim kishilardan va boshqa idoralardan kelib tushadi.

Fransiyada axborotni himoyalash tizimi. Fransiya kibermaydonda o‘zining fuqarolarini nazorat qilish bo‘yicha tuzilma tashkil etgan. Fransuzlar «Eshelon» nomli Amerika tizimiga o‘xshash o‘z tizimini yaratdilar. U deyarli barcha xususiy global kommunikatsiyalarni tutib qolishga yo‘naltirilgan. Milliy xavfsizlikni ta’minlash bo‘yicha siyosatning strategik yo‘nalishlarini ishlab chiqish bilan CLUSIF (Club de la securite informatique francaise) birlashmasi shug‘ullanadi. U o‘zining statusi bo‘yicha informatika sohasida ishlovchi yuridik va fizik shaxslarning ochiq assotsiatsiyasi hisoblanadi. CLUSIF davlat tomonidan to‘liq qo‘llab quvvatlanadi va maxsus xizmatlar bilan yaqin aloqaga ega. Fransiyaning maxsus xizmati strukturasi. Fransiya razvedka uyushmasining umumiy shtati, uchta har xil vazirlikka bo‘ysunuvchi xizmatlarda ishlaydigan 12779 ga yaqin xodimlardan iborat. Uchta xizmat Tashqi xavfsizlikning Bosh direksiyasi (DGSE); Harbiy razvedka boshqarmasi (DRM) va Harbiy kontrrazvedka boshqarmasi (DPSD) Mudofaa vazirligi himoyasida faoliyat olib boradi. Maxsus xizmatlarga

jandarmeriyani (Gendarmerie) ham kiritish mumkin. Uning vazifalaridan biri bo‘lib razvedka faoliyatini yuritish hisoblanadi – jandarmeriyaning har bir qismida razvedka bo‘limi mavjud. Ikkita maxsus xizmat: kontrrazvedka (DST) va Bosh razvedka xizmati (RG) Ichki ishlar vazirligiga bo‘ysungan.

Rossiya Federatsiyasi (RF)ning axborot xavfsizligini ta’minlovchi davlat idoralari strukturasi. Axborot xavfsizligining davlat siyosatini ishlab chiqish, qonunlar, normativ-me’yoriy hujjatlar tayyorlash, axborotni muhofaza qilishni ta’minlash bo‘yicha o‘rnatilgan me’yorlarni bajarilishi ustidan nazoratni davlat idoralari amalga oshiradilar. RF Prezidenti axborot xavfsizligini ta’minlovchi davlat idoralariga boshchilik qiladi. U Xavfsizlik kengashini boshqaradi va davlatda axborot xavfsizligini ta’minlashga doir farmonlarni tasdiqlaydi. Mamlakatning davlat xavfsizligiga oid boshqa masalalar bilan bir qatorda axborot xavfsizligi tizimining umumiy boshqaruvini RF Prezidenti va Hukumati amalga oshiradi. RF Prezidenti huzuridagi Xavfsizlik Kengashi davlat xavfsizligi masalalari bilan bevosita shug‘ullanuvchi hokimiyat idorasi hisoblanadi. Xavfsizlik Kengashi tarkibiga Axborot xavfsizligi bo‘yicha idoralararo komissiya kiradi. Komissiya davlatning axborot xavfsizligi sohasida Prezident farmonlarini tayyorlaydi, qonun chiqarish tashabbusi bilan chiqadi, vazirlik va idoralar rahbarlarining faoliyatini muvofiqlashtiradi. Axborot xavfsizligi bo‘yicha idoralararo komissiyaning ishchi idorasi bo‘lib RF Prezidenti huzuridagi Davlat texnik komissiyasi hisoblanadi. Bu komissiya qonun loyihalarini tayyorlashni amalga oshiradi, normativ me’yoriy hujjatlarni ishlab chiqadi, axborotni muhofaza qilish vositalarini (kriptografik vositalardan tashqari) sertifikatlashtirishni tashkil etadi, himoya vositalarini ishlab chiqish sohasidagi faoliyatni litsenziyalashtiradi va axborotni muhofaza qilish bo‘yicha mutaxassislarni o‘qitadi. Axborotni muhofaza qilish sohasida izlanishlar olib boruvchi davlat ilmiy-tadqiqot tashkilotlari faoliyatini muvofiqlashtiradi. Bu komissiya Davlat sirini himoyalash bo‘yicha idoralararo komissiya ishini ham ta’minlaydi. Davlat sirini himoyalash bo‘yicha idoralararo komissiyasiga davlat sirini tashkil etadigan ma’lumotlardan foydalanish, axborotni muhofaza qilish vositalarini yaratish hamda davlat sirini himoyalash bo‘yicha xizmat ko‘rsatish bilan bog‘liq korxona, muassasa va tashkilotlarni litsenziyalashni boshqarish vazifasi yuklatilgan. RF vazirlik va idoralarida axborot xavfsizligi siyosatining mos darajalarini boshqarishni ta’minlovchi iyerarxiyaga asoslangan tuzilmalar mavjud. Bu tuzilmalar, turli-xil nomlangani bilan o‘xshash funksiyalarni bajaradilar.

Foydalanilgan adabiyotlar ro‘yxati:

1. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: Учебное пособие. – Брянск, 2007.
2. Алферов А.П., Зубов А.Ю., Кузьмин А.С, Черемушкин А.В. Основы криптографии: Учебное пособие. – М., 2002.
3. Арипов М. , Пудовченко Ю. Е., Арипов М. Основы Интернет. – Т., 2003.
4. Безбогов А.А. Методы и средства защиты компьютерной информации. Учебное пособие. – Тамбов, 2006.
5. Давыдов А.С., Маслова Т.В. Информационные технологии в деятельности органов внутренних дел: Учебное пособие. – Челябинск, 2007.
6. Зайцев А.П., Голубятников И.В., Мещеряков Р.В. Программноаппаратные средства обеспечения информационной безопасности: Учебное пособие. – М., 2006.
7. Информационные технологии управления в органах внутренних дел: Учебник / Под ред. доцента Ю.А. Кравченко. – М., 1998.
8. Мельников В.П. и др. Информационная безопасность и защита информации: Учебое пособие. – М., 2008.
9. Казиев В.М. Введение в правовую информатику.
10. – http://www.intuit.ru.
11. Karimov I.M. va boshqalar. Axborot texnologiyalari: Darslik. – T., 2011.
12. Karimov I.M. va boshqalar. Informatika: Darslik. – T., 2012.
13. Левин М. Безопасность в сетях Internet и Intranet. – М., 2001.
14. Мельников В.П. Информационная безопасность. Учебое пособие. – М., 2005.
15. Миродова Ш. Проблемы обеспечения информационной безопасности Республике Узбекистан в условиях глоболизации. – Т., 2008.
16. Муҳаммадиев Ж.Ў. Ахборот хавфсизлиги: муаммо ва ечимлар: Монография. – Т., 2011.
17. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. – М., 2005.