DOI: https://doi.org/10.5281/zenodo.14264291

KIBERXAVFSIZLIKNING GLOBAL XAVFSIZLIK MUAMMOLARI BILAN BOG'LIQLIGI

Norova Fazilat Fayzulloyevna
Buxoro davlat universiteti Axborot tizimlari va raqamli texnologiyalar kafedrasi o'qituvchisi

ANNOTASIYA:

Axborotni ishlash, uzatish va to'plashning zamonaviy usullarining rivojlanishi foydalanuvchilar axborotini yo'qolishi, buzilishi va oshkor etilishi bilan bog'liq tahdidlarning ortishiga olib kelmoqda. Shu sababli, kompyuter tizimlari va tarmoqlarida axborot xavfsizligini ta'minlash axborot texnologiyalari rivojining yetakchi yo'nalishlaridan biri hisoblanadi. Kiberxavfsizlik tarixi kompyuter va axborot texnologiyalarining paydo bo'lishi bilan boshlangan. Internetning rivojlanishi va tarqalishi ham kiberxavfsizlik tahdidlarining paydo bo'lishiga olib keldi. Maqolada kiberxavfsizlikning global xavfsizlik muammolari bilan bog'liqligi haqida ma'lumot berilgan.

Kalit so'zlar: *Axborot, kiberxavfsizlik, axborot xavfsizligi, tahdid, kiberhujum, kibertahdid, axborot resurslari, tarmoq, axborot tarmog'i, axborot quroli.*

АННОТАЦИЯ

Развитие современных методов обработки, передачи и сбора информации приводит к увеличению угроз, связанных с потерей, нарушением и раскрытием информации пользователей. Поэтому обеспечение информационной безопасности в компьютерных системах и сетях является одним из ведущих направлений развития информационных технологий. История кибербезопасности началась с появлением компьютерных и информационных технологий. Развитие и распространение Интернета также привело к появлению угроз кибербезопасности. В статье представлена информация о связи кибербезопасности с проблемами глобальной безопасности.

Ключевые слова: *Информация, кибербезопасность, информационная безопасность, угроза, кибератака, киберугроза, информационные ресурсы, сеть, информационная сеть, информационное оружие.*

ABSTRACT

The development of modern methods of processing, transmitting and collecting information leads to an increase in threats associated with the loss, violation and disclosure of user information. Therefore, ensuring information security in computer systems and networks is one of the leading areas of information technology development. The history of cybersecurity began with the advent of computer and information technology. The development and spread of the Internet has also led to the emergence of cybersecurity threats. The article provides information on the relationship between cybersecurity and global security issues.

Keywords: *Information, cybersecurity, information security, threat, cyberattack, cyber threat, information resources, network, information network, information weapon.*

Kiberxavfsiz dunyoni yaratish uchun biz jinoyatchilar kabi tez va global integratsiyalashgan bo‘lishimiz kerak. Mahalliy resurslar bilan global tahdidga duch kelishning o‘zi etarli bo‘lmaydi. Mamlakatlar o‘z sa'y-harakatlarini muvofiqlashtirish uchun ichki va xalqaro miqyosda ko‘proq harakat qilishlari kerak. Sanoat ko‘plab sohalarda yetakchi o‘rinni egallaganligi - texnik va risklarni boshqarish standartlarini ishlab chiqish, ma'lumot almashish forumlarini chaqirish va katta resurslarni sarflash uchun tahsinga loyiqdir. Xalqaro tuzilmalar, jumladan, 7 ta kiberekspertlar guruhi va Bazel qo‘mitasi moliyaviy sektor nazoratchilari uchun xabardorlikni oshirmoqda va sog‘lom amaliyotlarni aniqlamoqda. Ammo, ayniqsa, global nuqtai nazardan qarasak, ko‘p ish qilish kerak. Xalqaro hamjamiyat birlashishi va milliy darajada amalga oshirilayotgan ishlarni kuchaytirishi mumkin bo‘lgan to‘rtta yo‘nalish mavjud:

Birinchidan, biz xavf-xatarlarni ko‘proq tushunishimiz kerak: tahdidlarning manbai va tabiati va ular moliyaviy barqarorlikka qanday ta'sir qilishi mumkin. Xatarlarni yaxshiroq tushunish uchun bizga tahdidlar va muvaffaqiyatli hujumlarning ta'siri haqida ko‘proq ma’lumotlar kerak.

Ikkinchidan, biz tahdidlar haqida razvedka, hodisalar haqida xabar berish va chidamlilik va javob berish bo‘yicha eng yaxshi amaliyotlar bo‘yicha hamkorlikni yaxshilashimiz kerak. Xususiy va davlat sektori o‘rtasida axborot almashishni axshilash kerak, masalan, banklarning moliyaviy nazorat va huquqni muhofaza qilish organlariga muammolar haqida hisobot berishidagi to‘siqlarni kamaytirish orqali. Mamlakatdagi turli davlat idoralari uzluksiz muloqot qilishlari kerak. Va eng qiyin, mamlakatlar o‘rtasida ma'lumot almashishni yaxshilash kerak.

Uchinchidan, tartibga solish yondashuvlari yanada izchillikka erishishi kerak. Bugungi kunda mamlakatlarda turli standartlar, qoidalar va atamalar mavjud. Ushbu nomuvofiqlikni kamaytirish ko‘proq muloqotni osonlashtiradi. Nihoyat, hujumlar

kelishini bilib, davlatlar ularga tayyor bo‘lishlari kerak. Inqirozga tayyorgarlik ko‘rish va ularga javob berish protokollari milliy va transchegaraviy darajada ishlab chiqilishi kerak, bu esa operatsiyalarga imkon qadar tezroq javob berish va tiklash imkoniyatiga ega bo‘lishi kerak. Inqiroz mashqlari jarayonlar va qarorlarni qabul qilishdagi kamchiliklar va zaif tomonlarni ochib berish orqali chidamlilik va javob berish qobiliyatini shakllantirishda hal qiluvchi ahamiyatga ega bo‘ldi.

Kiberhujum dunyoning istalgan nuqtasidan yoki bir vaqtning o‘zida ko‘p joydan kelishi mumkinligi sababli, inqirozga javob berish protokollari mintaqalar va global miqyosda ifodalanishi kerak. Ya'ni, tegishli idoralar inqiroz paytida, yaqin atrofdagi va, ideal holda, uzoq mamlakatlarda ham “kimga qo‘ng'iroq qilishni” bilishi kerak. Kichik yoki rivojlanayotgan mamlakatlar uchun bu xalqaro e'tiborni talab qiladigan muammo.

Ko‘pchilik moliyaviy aloqalar uchun global banklar tomonidan taqdim etilgan moliyaviy xizmatlar yoki vakillik liniyalariga tayanadi. Transchegaraviy javob protokollarini ishlab chiqish mamlakatlarga inqirozdagi o‘z rollarini tushunishga yordam beradi va inqiroz yuzaga kelganda muvofiqlashtirilgan javobni ta'minlaydi.

Muvaffaqiyatli kiberhujumlar, ayniqsa shaxsiy va moliyaviy ma'lumotlar buzilgan taqdirda, ishonchsizlikni keltirib chiqarish orqali moliyaviy rivojlanishga to‘sqinlik qilishi mumkin.

Agar biz bozorlarni rivojlantiradigan va moliyaviy inklyuzivlikni kengaytiradigan yangi texnologiyalardan foyda olishni istasak, ishonchni saqlashimiz, axborot-kommunikatsiya texnologiyalari xavfsizligini ta'minlashimiz kerak. Kiberxavfsizlik bilan har doim ko‘proq narsa qilish kerak, chunki o‘zgarishlar tezligi hayratlanarli darajada tezdir.

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.

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.

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.

Xulosa sifatida shuni aytish lozimki, kibertahdid landshafti rivojlanishda davom etar ekan, mamlakatlar o‘z sa'y-harakatlarini muvofiqlashtirish uchun ichki va xalqaro miqyosda ko‘proq harakat qilishlari kerak. Har bir mamalakat kuchli kiberxavfsizlik pozitsiyasiga ega bo‘lishi juda muhimdir.

FOYDALANILGAN ADABIYOTLAR

1. Cybe r security policy guidebook. Jennifer L. Bayuk. Jason Healey. Paul Rohmeyer, et.c. Willey publisher.2018-y. 288 p. ISBN 978-1-118-02780-6.
2. Imomova Shafoat Mahmudovna, Norova Fazilat Fayzulloyevna. Ta’lim jarayonlarini raqamli texnologiyalar asosida takomillashtirish// Miasto Przyszłości, Vol. 32 (2023), C.47-49.
3. Имомова Ш.М., Норова Ф.Ф. Учебные методы организации спортивно оздоровительных мероприятий в образовательных учреждениях // ВЕСТНИК НАУКИ И ОБРАЗОВАНИЯ 2021. № 9 (112). Часть 2. С.38-41.
4. Имомова Ш.М., Норова Ф.Ф. РОЛЬ КЕЙС-МЕТОДА НА УРОКАХ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ // Вестник науки и образования, 2022. № 4 (129). Часть 2. С.76.
5. Имомова Ш.М., Норова Ф.Ф. РОЛЬ СОЦИАЛЬНЫХ СЕТЕЙ В ОБРАЗОВАНИИ//UNIVERSUM: ТЕХНИЧЕСКИЕ НАУКИ. №10(103), 2022. С. 30-32.
6. Norova F.F. Ta’limni dasturiy vositalar yordamida rivojlantirish// Miasto Przyszłości, Vol. 40 (2023), C.636-638.
7. Norova F.F. TA’LIMIY RAQAMLI RESURSLARNI YARATISH TEXNOLOGIYALARI// Educational Research in Universal Sciences. VOLUME 3 | ISSUE 6 | 2024, C.4-13.
8. Imamova Sh.M. Methodology of Development of Programming Skills in Mathematical Systems in Students Based on Computer Simulation Trainers// NATURALISTA CAMPANO Volume 28 Issue 1, 2024, -pp. 551-557.