UDK 004.492

KIBER XAVFSIZLIKNI TA’MINLASHDA SUG‘URTALASH TIZIMINI JORIY ETISH

Mavlonov O.N.[1], *Meliko‘ziyev R.Sh.*[1], *Radjabova M.Sh.*[1]
[1] Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, Toshkent, O‘zbekiston
mavlonov8686@gmail.com, melikuziyevmurodbek7@gmail.com, abdujabbor.madina.1989@gmail.com

Annotatsiya. *Mazkur maqolada kiberxavfsizlikni ta’minlashda amaliy va samarali natija beruvchi sug‘urtalash tizimi to‘g‘risida tadqiqotlar olib borilgan. Kiber xavfsizlikni ta’minlashda sug‘urtalash tizimi axborot obyektlarini attestatsiyalashni amalga oshirishning asosiy yo‘nalishi bo‘lib, sug‘urtalash axborot xavfsizlikning garovi hisoblanadi. Shuningdek mazkur maqolada kiber tahdidlarning ba’zilari yani kiberterrorizm, kiber urush, kiber josuslik va kiber jinoyatchilar to‘g‘risida hamda kiber hujumlar qilingan mamlakatlar statistikasi haqida ma’lumotlar beriladi. Kiber hujumlarni oldini olish choralari ko‘rsatib o‘tiladi hamda ushbu maqolada kiber xavfsizlikni oldini olishning huquqiy asoslari ko‘rsatib o‘tilgan.*

Kalit so‘zlar: *Kiber xavfsizlik, axborot obyekti, sug‘urtalash, hujum, tahdid kiberxavfsizlik, kiberterrorizm, kiber urush, kiber josuslik, kiber jinoyatchilik.*

I. KIRISH

Internet ko‘p jihatdan dunyoni rivojlantirdi, lekin bizga ilgari hech qachon ma’lum bo‘lmagan turli ko‘rinish-dagi va juda murakkab ta’sirlarga yo‘l ochib berdi. Xavfsizlik istiqboli o‘sishi bilan birga xakerlik sohasi ham tez rivojlandi. Kiberxavfsizlikni ta’minlash masalasi va yechimi har bir mamlakatning asosiy e’tiboriga aylanmoqda va bu sohada keskin chora-tadbirlarni amalga oshirmoqda [1]. Ulardan biri, yuqori hisoblash va shifrlash texnologiya ta’min-langan kompaniyalarni tashkil etish va faoliyatini joriy rivojlantirishdir.

Kiberxavfsizlik bu internetga ulangan tizimlar, jumladan apparat-dasturiy, dasturiy ta’minot vositalar va ma’lumot-larni kiber hujumlardan himoyalash hisoblanadi. Uning tarkibi kiberxavfsizlik va fizik xavfsizlikdan tashkil topadi, hamda tashkilotlarning ma’lumotlar bazasiga va boshqa kompyuterlashtirilgan tizimlarga ruxsatsiz kirishdan himoya qilish uchun qo‘llaniladi va unda asosiy talablar yani ma’lumotlarning maxfiyligi, ishonchliligi va barqarorligini ta’minlashi lozim [1].

II. KIBERTAHDID OQIBATLARI

Kiberxavfsizlik ta’minlashning asosiy yo‘nalishlaridan biri axborot va tizimlarni kibertahdidlardan himoya qilish hisob-lanadi. Bu tahdidlar turli shakl va ko‘rinishlarda bo‘lishi mumkin [2]. Kibertahdidlar asosan innovatsion ko‘rinishlarda mamlakat yoki muhim shaxslarning maxfiy, siyosiy va harbiy manbalarini nishonga oladi. Bu esa kiberxavfsizlik siyosati, strategiyasi va operatsiyalariga rioya qilishda turli muammolarni keltirib chiqaradi.

Kiber tahdidlardan ba’zilari quyidagilar [3]:

- Kiberterrorizm - bu terroristik guruhlarning siyosiy maqsadlariga erishish uchun axborot texnologiyalaridan innovatsion foydalanish [4]. U tarmoqlar, kompyuter tizimlari va telekommunikatsiya infratuzilmalariga hujumlar natijasida shakllantiriladi. Misol uchun 5-6 yilda dahshatli oqibatlar keltirgan ISHID terrorchilik tashkiloti faoliyatida yaqqol ko‘rindi. Ular o‘z tizimida g‘oya va maqsadlarni targ‘ib qilish bilan shug‘ullanuvchi mutaxassislarni birlashtirgan alohida tuzilma tashkil etishdi. Bugungi kunda internetda tarqatilayotgan bu kabi ma’lumotlarning 80 foizi Yaqin Sharq hududlarida faoliyat yuritayotgan terrorchi tashkilotlarga tegishlidir. OAV ma’lumotlari tahlili hamda jabrlanuvchilarning iqrorlariga ko‘ra, radikal g‘oyalarning tarqatilishi va tashkilotlarga yollash harakatlarining aksariyati “Facebook”, “Odnoklassniki”, “Twitter”, “Vkontakte”, "Youtube" kabi ijtimoiy tarmoqlarda amalga oshirilmoqda [6];

- Kiber urush - bu davlatlarning axborot texnologiyalaridan foydalanib, har qanday davlatning tarmog‘idan o‘tish orqali ma’lum bir davlatning milliy manfaatlariga talofat yetkazish maqsadidagi harakatlaridir. Ko‘plab rivojlangan davlatlar tomonidan kiber urush qurolli urishlar tarkibiga kiritilgan. Kiber urush hujumlari davlatning milliy manfaatlarini ko‘zlab, davlat nazorati asosida yaxshi tayyorlangan xakerlar tomonidan kompyuter tarmoqlariga amalga oshiriladi. Kiber urush hujumi qimmatli ma’lumotlarni o‘z ichiga olgan aloqa, transport, savdo va tibbiy xizmatlar kabi infratuzilmalarni nishonga olib, asosiy maqsad esa tarmoq kalitini olish va ma’lumotlar bazasiga kiridir [4];

- Kiber josuslik - bu axborot texnologiyalaridagi maxfiy ma’lumotlarni egalari orqali yoki egalarining ruxsatisiz olish va foydalanishdan iborat. U ko‘pincha josuslik texnikalari va dasturlaridan foydalangan holda strategik, iqtisodiy, harbiy ustunlikni oshirish uchun qo‘llaniladi [4].

Kiber jinoyatchilar shaxsning biografik ma’lumotlari asosida kredit kartalari bilan firibgarlik; kiber ta’qib; internetda boshqalarga tuhmat qilish; kompyuter tizimiga ruxsatsiz kirishni qo‘lga kiritish; dasturiy ta’minotni litsenziyalash va savdo belgisining mualliflik huquqini noqonuniy o‘zlashtirish, noqonuniy nusxalarni yaratish uchun bostiruvchi shifrlash; qaroqchi dasturiy ta’minotni va jinoyat sodir etish uchun birovning shaxsini o‘g‘irlash kabi ishlarni amalga oshiruvchilar hisoblanadi. AQSH Federal qidiruv byurosi ma’lumotlariga ko‘ra, global pandemiya davrida AQSHda kiber jinoyatlar soni **400 foiz**ga oshgan [3].

Axborot tahdidlari va kiber hodisalar soni yildan-yilga ortib bormoqda. koronavirus avj olishi 2020-yilda onlayn faoliyatga o‘tgan kompaniyalar sonining sezilarli o‘sishiga sabab bo‘ldi, biroq buzg‘unchilik, hujum va tahdidlar shunga mutanosib ravishda oshdi. Ayniqsa hozirda xakerlik sohasi tez suratda rivojlanmoqda [5].

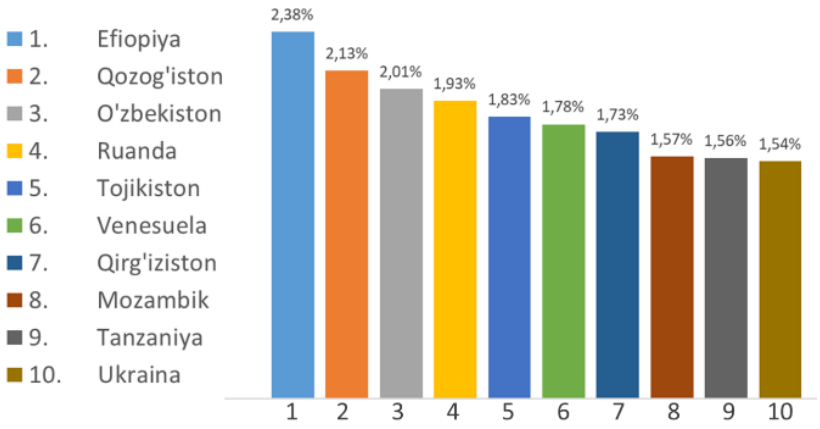
2022-yilning uchinchi choragida Kasperskiy laboratoriyasi **99 989 nafar** foydalanuvchining kompyuterlaridagi bank hisoblaridan pul o‘g‘irlash uchun mo‘ljallangan turli shakldagi zararli dasturlarni ishga tushishining oldini olgan [5]. Moliyaviy zararli keltiruvchi kiber hujumlar uyushtirilgan davlatlarning ulushi 1-jadvalda keltirilgan.

1-jadval. Kiber hujum qilingan mamlakat va hududlar statistikasi.

№	Mamlakat yoki hudud	Foiz ko‘rsatkichi
1.	Turkmaniston	4.7%
2.	Afg'oniston	4.6%
3.	Paragvay	2.8%
4.	Tojikiston	2.8%
5.	Yaman	2.3%
6.	Sudan	2.3%
7.	Xitoy	2.0%
8.	Shveytsariya	2.0%
9.	Misr	1.9%
10.	Venesuela	1.8%

Kasperskiy laboratoriyasi tomindan olib borilgan tadqiqotlar natijasiga ko‘ra 2021-yilda kiberhujumlarning global zarari **6 trillion dollar**dan oshdi [5].

2022-yilning uchinchi choragining o‘zida maynerlarning **153 773 ta** yangi modifikatsiyasini aniqlangan. Ulardan **140 000 dan** ortig‘i iyul va avgust oylariga to‘g‘ri keladi. Bundan ko‘rinadiki maynerlar ijodkorlarining faolligi yozda yuqori darajada. Maynerlar tomonidan hujumga uchragan davlat va hududlarning statistikasi 1-rasmdagi diogrammada ko‘rsatilgan [10].



1-rasm. Maynerlar hujumiga uchragan davlat va hududlarning statistikasi.

III. KIBER JINOYATCHILIK

Kiber jinoyatchilar amalga oshirgan harakatlaridan kelib chiqib, uch guruhga bo‘lish mumkin:

1-toifa kiberjinoyatchilar – kiber jinoyatlarni amalga oshirishga chan-qoqlar:

- Xobbi xakerlari;
- IT mutaxassislari (Ijtimoiy muhandislik eng katta tahdid-lardan biri);
- Siyosiy maqsadni ko‘zlovchi xakerlar;
- Terror tashkiloti.

2-toifa kiberjinoyatchilar – o‘zlarini kiber jinoyatchilar sifatida tan olmay-diganlar:

- Psixologik ta’sir ko‘rsatuvchi xakerlar;
- Moliyaviy maqsadni ko‘zlovchi xakerlar (korporativ josuslik);
- Davlat - homiylikdagi xakerlik (milliy josuslik, sabotaj);
- Uyushgan jinoyatchilar.

3-toifa kiberjinoyatchilar - insayderlar:

- Qasos olmoqchi bo‘lgan sobiq xodimlar;
- Talofat yetkazish yoki o‘g‘irlik yo‘li bilan iqtisodiy ustunlikka erishish uchun xodimlardan foydalangan holda kompaniya raqobati.

Tarixdan tashkilotlar va hukumatlar tahdidlarga qarshi kurashda aniq yondashuvni qo‘llaganlar, o‘zlarining tarmoqlarini va ulardagi qimmatli ma’lumotlarni himoya qilish uchun birgalikda individual xavfsizlik texnologiyalarini ishlab chiqarishgan. Bu usul nafaqat qimmat va murakkab, lekin zararli kiber buzilishlar haqidagi xabarlarni hozir ham eshitmoqdamiz va bu esa mazkur usullarni samarasiz ekanligini anglatmoqda. Darhaqiqat, ma’lumotlarning buzilishi bo‘yicha bir guruh ekspertlar tarmoqni kiberxavfsizlik sohasida ustuvorliklar masala sifatida belgiladi. Tashkilotlar kiber himoyani ta’minlash uchun maxsus ishlab chiqilgan mahalliy integratsiyalangan, avtomatlashtirilgan yangi avlod xavfsizlik platformalarini ishlab chiqish va uni ma’lumotlar bazasi hamda tarmoqlarda qo‘llash chora tadbirlar amalga oshirilmoqda.

Kiberxavfsizlikdan foydalanish kiberhujumlar, ma’lumotlar buzilishi va identifikator o‘g‘irlanishining oldini olishga va xavflarni boshqarishda yordam beradi. Tashkilot tarmoq xavfsizligi haqida aniq tushunchaga ega bo‘lsa va tahdidlarga qarshi samarali choralar ko‘rish rejasiga ega bo‘lsa, bu hujumlarga yo‘l qo‘ymaslik yaxshiroq ekanligini anglab yetamiz. Misol uchun, barcha foydalanuvchilarning kompyuterlarni zararli kodlarini doimiy skaner qilish va himoyasini ta’minlash umumiy axborotlashtirish obyektida ma’lumotlarni himoyani ta’minlash mumkin [7].

Yangi texnologiyalarida xakerlar xavfsizlik tendentsiyalari va qiyin vazifalarni bajaruvchi sun’iy intelekt tahdidlari foydalanmoqda. Bundan ma’lum bo‘ladiki axborot va boshqa aktivlarni turli shakldagi kiber tahdidlardan himoya qilish uchun amalga oshirilishi lozim bo‘lgan keskin choralar ko‘rilishi kerak.

Ransomware - bu jabrlanuvchining kompyuter tizimidagi fayllarini tajovuzkor tomonidan shifrlash orqali qulflab, undan parolni ochish hamda qulfdan chiqarish uchun to‘lov talab qilishni o‘z ichiga olgan zararli dastur turi. Ular quyidagilar:

- Zararli dasturiy ta’minot - bu foydalanuvchi kompyuteriga zarar yetkazish uchun ishlatiladigan har qanday fayl yoki dastur, masalan, qurtlar, kompyuter viruslari, troyan otlari va josuslik dasturlari [4].

Ijtimoiy muhandislik - bu himoyalangan maxfiy ma’lumotlarni yaxshilash deb aldash bilan ta’sir etib, foydalanuvchilarni xavfsizlik tartib-qoidalarini buzishga yo‘naltirishga tayanadigan hujum.

Fishing firibgarlikning bir ko‘rinishi bo‘lib, nufuzli manbalardan kelgan elektron pochta xabarlariga o‘xshash soxta elektron pochta xabarlari yuboriladi; biroq ushbu elektron pochta xabarlarining maqsadi kredit karta yoki login ma’lumotlari kabi muhim ma’lumotlarni o‘g‘irlashdir.

Kompaniya tizimlari va tarmoqlarini himoya qilish maqsadida axborot

xavfsizligi bo‘yicha tahlilchilar xavfsizlik choralarini rejalashtiradi va amalga oshiradi. Ular muhim ma’lumotlarning o‘g‘irlanishi, shikastlanishi yoki buzib kirishining oldini olish uchun ilg‘or yechimlarni yaratadi [2]. Ularning asosiy vazifasi kompaniya yoki tashkilot, mijozlar, xodimlar va boshqa har qanday ma’lumotlarni har qanday kiber hujum yoki xakerlikdan xavfsiz tarzda ma’lumotlarni saqlashdir.

IV. KIBERHUJUMLARNING ASORATI

Kiberhujumlar hatto eng nufuzli tashkilotga ham ko‘proq moliyaviy va obro‘ga putur yetkazadi. Kiberhujumga uchragan tashkilot resurslari va obro‘sini yo‘qotadi, savdo potentsiali pasaydi. Shunining uchun tashkilotda kiberxavfsizlik tartibga soluvchi jarimalar va sud tizimi bo‘yicha mavjud. Shuningdek yetkazilgan harajatlarni qoplash bo‘yicha sug‘urtalash amalga oshiriladi. 2017-yilda Buyuk Britaniya hukumatining kiberxavfsizlik bo‘yicha so‘rovi shuni ko‘rsatdiki, yirik biznes uchun o‘rtacha xarajat **19,600** kichik va o‘rta biznes uchun esa **1,570 funt sterling** sug‘urta to‘lashni amalga oshirgan [6].

Hujum bo‘yicha turli xil vositalari va hujum rejimlari mavjud. Kompleks vositalari uchun zararli dasturlardan foydalanilmoqda. Masalan, viruslar va qurtlar. O‘zlarining funktsional nusxalarini aks ettiruvchi va noqulaylikni keltirib chiqaruvchi, ma’lumotlarning maxfiyligi yoki yaxlitligini buzishgacha bo‘lgan effektlar bilan takrorlaydigan kompyuter dasturlari va troyan otlari, shuningdek xavfsiz ilovalar sifatida namoyon bo‘ladigan, ammo xaker keyinchalik qaytib kirishi uchun sharoit yaratadigan halokatli dasturlar [5]. Asosan tizimga kirish ko‘plab murakkab hujumlarning asosiy maqsadi hisoblanadi. Agar tajovuzkor tizimni to‘liq nazorat qilish yoki ildiz kirish huquqiga ega bo‘lsa, ular tizimning ichki ishlariga cheksiz kirish huquqiga ega. Raqamli ma’lumotlarning xususiyatlariga ko‘ra, jinoiy niyatga ega bo‘lgan shaxs ma’lumotni ushlab turadi, buzadi, foydalanadi, yo‘q qiladi, o‘g‘irlaydi va o‘zgartiradi. Axborotning qiymati yoki dasturning ahamiyati qanday ma’lumot bilan ishlashiga bog‘liq va unga hujum harakatlari turli darajada amalga oshiladi [4].

Kiber tahdidlarning kundan kunga rivojlanishiga sabablar bor? Birinchidan, kiber tahdidlarga qarshi kurash juda siyosiylashgan masalaga aylanganligi sababli, rasmiy tahdid qiluvchilar resurslari va ta’sirini oshirish maqsadida bir-biri bilan raqobatlashadigan konstruksiyalarini ishlab chiqmoqda. Bu esa tahdidlarning o‘sishiga olib kelmoqda. Natijada shoshilinch chora-tadbirlar zarurligini namoyon bo‘lmoqda. Ikkinchidan, psixologik tadqiqotlar shuni ko‘rsatdiki, xavfni idrok etish sezgi va his-tuyg‘ularga, shuningdek mutaxassislarning idrokiga juda bog‘liq. Kiberxavflar ekstremal shaklda, “dahshatli xavflar” deb atala boshlandi [6]. U noma’lum va halokatli bo‘lib, uni boshqarib bo‘lmaydi. Talofatning pastligi va xavf ehtimolining yo‘q degani emas. Faqat yetarli darajada buzg‘unchi yoki buzuvchi tizimli hujumlar bo‘lganda yoki tashkilotga zarar yetkazilganda kiber xafsizlik bo‘yicha choralar ko‘rilmoqda.

V. KIBER XAVFSIZLIKNI TA’MINLASHGA DOIR CHORA-TADBIRLAR TAHLILI

Mamlakatlar o‘rtasida kiberxavfsizlikni ta’minlash bo‘yicha ko‘pgina konsepsiyalar qabul qilingan va munozaralar o‘tkazilib, zaruriy choralar ishlab chiqilmoqda. Asosiy e’tibor va yo‘nalish obyektlardagi kompyuter va

tarmoqlarni himoya qilish uchun javobgarlikni o‘z zimmasiga oluvchi tashkilotlarni amaliyotga joriy etish [3]. Ma’lumki xususiy sektorda jamiyat faoliyati uchun muhim bo‘lgan ayrim obyektlar mavjud va uni himoyasini ta’minlash uchun qo‘shimcha choralar ko‘rish esa hukumat himoya darajasida amalga oshirilishi kerak. Bu harakatlar odatda kritik nufuzga ega bo‘lishi lozim. Axborot xavfsizligini ta’minlash - bu infratuzilmani himoya qilish va xavflarni boshqarish bo‘yicha asosiy usullardan biri bo‘lib, axborot xavfsizligini ta’minlanmasligi esa shaxs va jamiyat hayotining himoyalanmagan ekanligidan dalolat beradi. Bu esa jamiyatda katta ehtimol bilan talofatli kiber hodisalarni muqarrar ravishda ro‘y berishini anglatadi. Buning natijasidagi oqibatlarni tiklash qiyin bo‘lishi mumkin. Balki umuman tiklab ham bo‘lmas [3].

5.1 Kiber tahdidlar sabab yuzaga keluvchi talofatlarni oldini olish

Kiber tahdidlar va uning natijasida yuzaga keluvchi talofatlarni oldini olishning samarali yechimlaridan biri bu axborotlashtirish obyektlarini attestatsiyalashdan iboratdir.

“Milliy axborot resurslarini muhofaza qilishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi PQ-1572-son qarori va Vazirlar Mahkamasining 2011-yil 7-noyabrdagi 296-son qarori bilan tasdiqlangan tartibga ko‘ra O‘zbekiston Respublikasi Davlat xavfsizlik xizmati (oldingi nomi Milliy xavfsizlik xizmati) tomonidan axborotlashtirish obyektlarini attestatsiyadan o‘tkazishga doir ishlarning muyyan turlarini amalga oshirish uchun turli mulkchilik shaklidagi tashkilotlarga ruxsatnomalar beradi. Albatta faqat ma’lum talablarga muvofiq bo‘lganda [7-8]. Hozirda mamlakatimizda axborotlashtirish obyektlarining maxfiy ma’lumotlar xavfsizligi ta’minlash talab-lariga muvofiqligini attesatsiyalash O‘zbekiston Respublikasi Milliy xavfsizlik xizmati Raisining 2014-yil 1-maydagi 47-sonli buyrug‘i bilan tasdiqlangan axborotlashtirish obyektlarini attesatsiyadan o‘tkazish tartibi to‘g‘risidagi na’munaviy nizomga asosan amalga oshiriladi [9].

Axborot xavfsizligi talablariga muvofiqligi bo‘yicha attestatsiyalash sinovlarini o‘tkazish va attestatsiyalash xizmatini ko‘rsatilishi mumkin bo‘lgan axborotlashtirish obyektlarining turlari va ro‘yxati Davlat xaxfsizlik xizmati tomonidan belgilangan.

Axborotlashtirish obyektlariga quyidagilar kiradi:

- turli darajadagi va maqsadlardagi avtomatlashtirilgan tizimlar (axborot tizimlari) (axborotlashtirish vositalari va tizimlari);
- aloqa tizimlari, ma’lumotlarni qabul qilish, qayta ishlash va uzatish (axborotlashtirish vositalari va tizimlari);
- xizmat ko‘rsatish va ko‘paytirish tizimlari (axborotlashtirish vositalari va tizimlari bilan jihozlangan binolar);
- maxfiy muzokaralar o‘tkazish uchun mo‘ljallangan binolar va inshootlar (himoya qilinadigan binolar).
- obyektni attestatsiyalash jarayonida quyidagi ishlar amalga oshiriladi:
- axborot oqib chiqishining potensial kanallarini aniqlash uchun muhandislik tahlili;
- axborotni muhofaza qilish bo‘yicha tashkiliy-ma’muriy hujjatlarning yetarliligi va to‘liqligini tekshirish;
- axborotlashtirish obyektini maxsus nazorat-o‘lchov vositalaridan foydalangan holda instrumental tekshirish va axborotlashtirish obyektida qayta ishlangan himoyalangan axborotning texnik kanallar orqali chiqishi bo‘yicha xavfsizligini baholash;

- axborotlashtirish obyektining axborotga ruxsatsiz kirishdan himoya qilish bo‘yicha xavfsizlik talablariga muvofiqligini baholash.

VII. XULOSA

Mamlatimizda kiber xavfsizlik sohasini rivojlantirish bo‘yicha chora-tadbirlar amalga oshirilmoqda. Lekin ayrim tashkilotlarning axborot resurslarida kiber xavfsizlik ta’min-lanmagan. Shuning uchun kiber hujumlar uchrab turibdi. Bu sohaga e’tiborsizlik qilish oqibatlari qimmatga tushishi mumkin. Kiber xavfsizlikni manzilli ta’minlashning asosiy yo‘nalishlaridan biri axborotlashtirish obyektlarini attestatsiyadan o‘tkazish va axborot resurslarini sug‘urtalash tizimini joriy etishdir. Bu esa mamlakatimizda sodir etilayotgan kiber jinoyatlar sonini kamaytirishi mumkin.

Axborot xavfsizligini ta’minlashning asosiy choralaridan biri axborotlashtirish obyektini attestatsiyadan o‘tkazish va attestatsiyadan o‘tgandan so‘ng faoliyatiga ruxsat berishdir. Raqamli texnologiyalar rivojlanishi jadallash-moqda, bu esa attestatsiyalangan obyektlar xakerlar hujumiga har doim ham bardosh bera olmaydi. Bunga attestatsiyadan o‘tkazgan tashkilot ham o‘z javobgarligini olmaydi ham. Bunday vaziyatlarda sug‘urtalash va axborot resurslarini doimiy axborot xavsizligi nuqtai nazaridan testlab borish samarali hisoblanadi. Yuqorini nufuzga ega kompaniyalar o‘z axborot tizmini doimiy teslab boradi va hujumlarga qarshi ataka usulini amalga oshiradi. Shu orqali kutilishi mumkin bo‘lgan talofatlarning oldini oladi. Yetkazilgan zarar esa sug‘urtalangan bo‘ladi.

ADABIYOTLAR

[1] O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari va kommu-nikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi 2018-yil 19-fevraldagi PF-5349-son Farmoni.

[2] *Scannell, Kara* (24 February 2016). «CEO email scam costs companies $2bn». Financial Times (25 Feb 2016). Archived from the original on 23 June 2016. Retrieved 7 May 2016.

[3] *Marcel, Sébastien; Nixon, Mark; Li, Stan, eds.* (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks (PDF). London: Retrieved 8 October 2017.

[4] *Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr* A Dictionary of Computer Science. Oxford Reference. Retrieved 8 October 2017.

[5] *Федотов Н.Н. ДосАтаки в сети.* Документальная электросвязь. 2015, №13.

[6] *Nurmatov B.* Kiberterrorizm shiddat bilan o‘sib borayotganiga sabab nima. 17.03.2019. https://qashqadaryo.uz/oz/nview/kiberterrorizm-shiddat-bilan-%D0%BE-sib-borayotganiga-sabab-nima-17-03.

[7] “Milliy axborot resurslarini muhofaza qilishga doir qo‘shimcha chora-tadbirlar to‘g-‘risida” O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi PQ-1572-son qarori.

[8] O‘zbekiston Respublikasi Vazirlar mahkamasining 296-sonli qarori. 07.11.2011 y.

[9] “Axborotlashtirish obyektlarini attesatsiyadan o’tkazish tartibi to’g’risidagi na’munaviy nizom” O‘zbekiston Respublikasi Milliy xavfsizlik xizmati Raisining 2014 yil 1 maydagi 47-sonli buyrug'i bilan tasdiqlangan.

[10] *Афтер Амир.* Развитие информационных угроз в третьем квартале 2022 года. Статистика по ПК. 18 ноя 2022.

https://securelist.ru/it-threat-evolution-in-q3-2022-non-mobile-statistics/106077/

Поступила в редакцию 15.01.2023

Citation: *Mavlonov O.N., Meliko‘ziyev R.Sh., Radjabova M.Sh.* (2023). Kiber xavfsizlikni ta’minlashda sug‘urtalash tizimini joriy etish. Raqamli texnologiyalarning nazariy va amaliy masalalari xalqaro jurnali. 1(3). – B. 127-134.

IMPLEMENTING A CYBER SECURITY INSURANCE SYSTEM

Mavlonov O.N.[1], Melikuziev R.Sh.[1], Radjabova M.Sh.[1]

[1] Tashkent University of information technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan
mavlonov8686@gmail.com, melikuziyevmurodbek7@gmail.com

Abstract. *This article is about a practical and effective cybersecurity insurance system. In ensuring cybersecurity, the insurance system was considered the main obstacle to the certification of information objects. Insurance is also a guarantee of information security. This article also provides information about some of the cyber threats, namely cyber terrorism, cyber warfare, cyber espionage, and cyber criminals. Information is provided on the statistics of countries where cyber attacks were carried out. Measures to prevent cyber attacks will be shown. This article provides the legal framework for cybersecurity prevention.*

Keywords: *Cyber security, information object, insurance, attack, cyber security threat, cyber terrorism, cyber war, cyber espionage, cyber crime.*

ВНЕДРЕНИЕ СИСТЕМЫ СТРАХОВАНИЯ КИБЕРБЕЗОПАСНОСТИ

Мавлонов О.Н.[1], Меликузиев Р.Ш.[1], Раджабова М.Ш. [1]

[1]Ташкентский университет информационных технологий имени Мухаммада ал-Хорезми, Ташкент, Узбекистан
mavlonov8686@gmail.com, melikuziyevmurodbek7@gmail.com

Аннотация. *Данная статья посвящена практичной и эффективной системе страхования кибербезопасности. В обеспечении кибербезопасности основным препятствием для осуществления аттестации объектов информации считалась система страхования. Также страхование является гарантией информационной безопасности. В этой статье также представлена информация о некоторых киберугрозах, а именно о кибертерроризме, кибервойне, кибершпионаже и киберпреступниках и приведена информация о статистике стран, где были осуществлены кибератаки. Расссмотрены меры по предотвращению кибератак. Приведены правовые основы предотвращения кибербезопасности в Республике Узбекистан.*

Ключевые слова: *Кибербезопасность, информационный объект, страхование, атака, угроза кибербезопасности, кибертерроризм, кибервойна, кибершпионаж, киберпреступность.*