KIBERXAVFSIZLIK VA JAMOAT XAVFSIZLIGINI TA'MINLASHNING USTUVOR YO'NALISHLARI SIFATIDA

O'ktamov Ilyosbek G'olibjon o'g'li
Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti.

https://doi.org/10.5281/zenodo.14251788

Annotatsiya. *Mazkur maqolada kiberxavfsizlik va jamoat xavfsizligini ta'minlashning ustuvor yo'nalishlari sifati haqida so'z yuritiladi. Shuningdek, Milliy kiberxavfsizlik nafaqat ushbu munosabatlar sohasini huquqiy tartibga solishni, balki internet resurslaridan foydalanish savodxonligini, raqamli madaniyatni rivojlantirishni ham nazarda tutadi, jismoniy va moddiy resurslar bilan bir xil himoya qilishni talab qiladigan fuqaroning shaxsiy raqamli ma'lumotlari haqida aniq tasavvurni shakllantirishuf qaratilgan.*

Kalit so'zlar: *milliy kiberxavfsizlik, axborot xavfsizligi, xavfsiz internet makoni, suveren kiberxavfsizlik, sun'iy intellekt, kibermakon.*

CYBER SECURITY AND PUBLIC SAFETY AS PRIORITIES

Abstract. *This article discusses the quality of cybersecurity and public safety priorities. Also, the National cyber security not only envisages the legal regulation of this sphere of relations, but also the development of literacy in the use of Internet resources, development of digital culture, aimed at forming a clear idea about the personal digital data of a citizen, which requires the same protection as physical and material resources.*

Key words: *national cyber security, information security, safe internet space, sovereign cyber security, artificial intelligence, cyber space.*

КИБЕРБЕЗОПАСНОСТЬ И ОБЩЕСТВЕННАЯ БЕЗОПАСНОСТЬ КАК ПРИОРИТЕТЫ

Аннотация. *В данной статье рассматриваются приоритеты качества кибербезопасности и общественной безопасности. Также Национальная кибербезопасность предусматривает не только правовое регулирование этой сферы отношений, но и развитие грамотности в использовании интернет-ресурсов, развитие цифровой культуры, направленной на формирование четкого представления о персональных цифровых данных гражданина. , который требует такой же защиты, как физические и материальные ресурсы.*

Ключевые слова: *национальная кибербезопасность, информационная безопасность, безопасное интернет-пространство, суверенная кибербезопасность, искусственный интеллект, киберпространство.*

Kirish.

Milliy kiberxavfsizlik siyosatini shakllantirish uzoq va murakkab jarayondir. Mustaqil, ammo davlat va fuqarolar uchun xavfsiz internet makonining mavjudligi nafaqat davlatning iqtisodiy va siyosiy institutlarining muvaffaqiyatli ishlashining kalitidir (bu davlatning asosiy funksiyalaridan biri hisoblanadi), balki butun jamiyat ham. Kiberxavfsizlik bo‘yicha davlat siyosatining meyoriy-huquqiy bazasining muammoli yo‘nalishlarini o‘rganish xavfsiz internet makonini yaratish uchun davlat va shaxsiy javobgarlikni aniqlashtirish va ajratish, ushbumakonni himoya qilishni chegaralash va davlat tomonidan muayyan maqsadlarda foydalanishuchun asos bo‘lishi kerak. Milliy kiberxavfsizlik nafaqat ushbu munosabatlar sohasini huquqiy tartibga solishni, balki internet resurslaridan foydalanish savodxonligini, raqamli madaniyatni rivojlantirishni ham nazarda tutadi; jismoniy va moddiy resurslar bilan bir xil himoya qilishni talab qiladigan fuqaroning shaxsiy raqamli ma’lumotlari haqida aniq tasavvurni shakllantirishdan iborat.

Asosiy qism.

Zamonaviy dunyoda kiberxavfsizlik jarayonlarini boshqarish axborot jamiyatining axloqiy va axloqiy asoslarini hisobga olmasdan mumkin emas. Demak, har qanday jamiyatda “shaxsning halokat, yovuzlik va adolatsizlik ayblovini o‘z zimmasiga olgan erkinlik o‘lchovini aniq anglashi davlat uchun muhimdir. Axborot texnologiyalari va kompyuter imkoniyatlari bu muammolarni yanada kuchaytiradi”. Shuning uchun davlat ruxsat etilgan chegaralarni belgilash uchun vosita sifatida huquqiy vositalardan foydalanishi kerak. Aynan shu nuqtai nazardan - axborot jamiyatining ilgari misli ko‘rilmagan imkoniyatlariga erishish va eng so‘nggi ma’lumotlardan foydalanish natijasida ochiladigan yangi imkoniyatlar yordamida «ruxsat etilgan chegaralarni» kesib o‘tishning oldini olish va kommunikatsiya texnologiyalari (AKT), jadal tartibga soluvchi qonun ijodkorligi faoliyati milliy va xalqaro miqyosda hamda mintaqaviy va global darajada amalga oshirilmoqda. Axir, aynan yangi chaqiriq va tahdidlarning mavjudligi kiberxavfsizlik sohasini xalqaro huquqiy tartibga solish uchun eng kuchli rag‘bat bo‘lib qolmoqda.

Shu munosabat bilan “Suveren kiberxavfsizlik: Global muammolar internetdagi OAV cheklovlariga qanday ta’sir qiladi tahliliy ma’ruzasi mualliflari ta’kidlaganidek, “uyushgan jinoiy guruhlar, yolg‘iz hujumchilar, rasmiylashtirilgan va rasmiylashtirilmagan buzg‘unchi siyosiy guruhlar, harbiylar tomonidan kibermakondan foydalanish imkoniyati mavjud va davlatlarning maxsus xizmatlari. Ularning maqsadi - jinoyatlar sodir etish, harbiy va fuqarolik infratuzilmasiga (shu jumladan tanqidiy) buzg‘unchi ta’sir ko‘rsatish uchun siyosiy sabablarga ko‘ra xakerlik hujumlarini amalga oshirish va maxfiy ma’lumotlarni to‘plash.

Davlat yoki kuchli korporatsiyalar manfaatlarini ko‘zlab to‘g‘ridan-to‘g‘ri josuslik dunyo hamjamiyati tomonidan kiberxavfsizlikni huquqiy tartibga solish muammosini e’tiborsiz qoldirib bo‘lmaydi”.

Dunyoning yetakchi davlatlari o‘zlarining kiberxavfsizliklarini ta’minlash muammolarini hal qilish siyosatida o‘zlarining axborot resurslarini rivojlantirish va himoya qilishga, shuningdek, boshqa mamlakatlarning axborot resurslariga ta’sir o‘tkazish imkoniyatiga tobora ko‘proq e’tibor qaratmoqda. Shu maqsadda, xususan, bugungi kunda dunyoning ko‘pgina nufuzli geosiyosiy subektlari (AQSH, Rossiya, Yevropa Ittifoqi, Xitoy, Hindiston va boshqalar) tarmoqdan ayrim mamlakatlar uchun foydalanish uchun ixtisoslashgan harbiy bo‘linmalarni yaratgan yoki yaratish jarayonida.

Jinoiy guruhlar, yolg‘iz hujumchilar, rasmiylashtirilgan va rasmiylashtirilmagan buzg‘unchi siyosiy guruhlar, harbiylar tomonidan kibermakondan foydalanish imkoniyati mavjud va davlatlarning maxsus xizmatlari. Ularning maqsadi - jinoyatlar sodir etish, harbiy va fuqarolik infratuzilmasiga (shu jumladan tanqidiy) buzg‘unchi ta’sir ko‘rsatish uchun siyosiy sabablargako‘ra xakerlik hujumlarini amalga oshirish va maxfiy ma’lumotlarni to‘plash. Davlat yoki kuchli korporatsiyalar manfaatlarini ko‘zlab to‘g‘ridan-to‘g‘ri josuslik dunyo hamjamiyati tomonidan kiberxavfsizlikni huquqiy tartibga solish muammosini e’tiborsiz qoldirib bo‘lmaydi”.

Dunyoning yetakchi davlatlari o‘zlarining kiberxavfsizliklarini ta’minlash muammolarini hal qilish siyosatida o‘zlarining axborot resurslarini rivojlantirish va himoya qilishga, shuningdek, boshqa mamlakatlarning axborot resurslariga ta’sir o‘tkazish imkoniyatiga tobora ko‘proq e’tibor qaratmoqda. Shu maqsadda, xususan, bugungi kunda dunyoning ko‘pgina nufuzli geosiyosiy subektlari (AQSH, Rossiya, Yevropa Ittifoqi, Xitoy, Hindiston va boshqalar) tarmoqdan ayrim mamlakatlar uchun foydalanish uchun ixtisoslashgan harbiy bo‘linmalarni yaratgan yoki yaratish jarayonida.

Kiberxavfsizlik muammolari sohasidagi mutaxassislar Xitoy va AQShning eng faol va kuchli kiber birliklari hozirda eng faol va qudratli hisoblanadi degan umumiy fikrga kelishdi.

Xitoy kiberqo‘shinlarining salohiyati, hajmi va vazifalari to‘g‘risida rasmiy ma’lumotlar yo‘qligiga qaramay, FQB uchun tayyorlangan va OAVga taqdim etilgan maxfiy hisobotdan qandaydir tasavvurga ega bo‘lish mumkin. Hisobot materiallarida Xitoy kiber-kuchlarining rivojlanish darajasi ta’kidlangan va bu rivojlanishning AQSH uchun tahdidlari ko‘rsatilgan.

Hisobotda XXR «kiberterrorizm nuqtai nazaridan Qo‘shma Shtatlar uchun eng yaxlit tahdid»[1] va hozirda «hayotiy infratuzilmani yo‘q qilish, bank, tijorat, harbiy va mudofaa ma’lumotlar bazalariga kirish» uchun yetarli salohiyatga ega bo‘lishi mumkin bo‘lgan kuch deb ataladi. FQB ma’lumotlariga ko‘ra, bugungi kunda XXR 180 000 xakerlik armiyasiga ega.

Ular har kuni AQSH kibermakoniga hujum qiladi va har yili AQSH Mudofaa vazirligi kompyuterlariga 90 000ga yaqin hujumlarni amalga oshiradi. 180 000 xakerning 30 000 tasi harbiylar, 150 000 tasi esa xususiy sektordagi kompyuter mutaxassislari (kiber fazoda harbiy yoki razvedkavazifalari bilan shug‘ullanuvchi xususiy kompaniyalar xodimlari). Ularning vazifasi AQSH harbiy va tijorat sirlariga kirish va hukumat va moliyaviy xizmatlarni buzishdir.

Mashhur nemis futurologi K. H. Shtaynmuller, «Kelajakning aniq tahdidi - Internetdagi kiber urush xavfi yoki uning o‘rnini bosadigan narsa - sovuq va issiq to‘qnashuv o‘rtasidagi chegaralarni yo‘q qiladi»»[2].

Randall Dipert o‘zining «Kiber urushning axloqiy muammolari» maqolasida Kiber urush bo‘yicha Jeneva konvensiyasining analogini yaratish zarurligi haqida o‘ylashni[3] taklif qiladi.

«Kiberdushmanlar ma’lumotlar bazalarini yo‘q qilishga, aloqa tizimlarini yopishga, bank hisoblarini tozalashga, butun shaharlarni zulmatga botirishga, ishlab chiqarishni yopib qo‘yishga, sog‘liqni saqlash tizimiga vayronagarchilikka olib kelishga va hokazolarga intilishadi. Ammo odatiy urushlardan farqli o‘laroq, kiberjanglar hatto uzoqdan Jeneva konvensiyasiga o‘xshab ketadigan hech narsa bilan tartibga solinmaydi. Kiber urush jinoyatchilarini cheklovchi xalqaro huquqning chegaralari yoki standartlari yo‘q”, - deya ogohlantiradi G. Dipert. Shu bilan birga, olimning fikricha, Jeneva konvensiyasi qoidalarini (sizbilganingizdek, uzoq vaqtdan beri oddiy urushlar o‘tkazish qoidalarini tartibga solib kelayotgan) oddiygina qabul qilib, raqamli harbiy amaliyotlarga o‘tkazib bo‘lmaydi.

Zamonaviy texnologiyalarning jadal rivojlanishi jarayoni taraqqiyot bilan birga qator muammolarni ham keltirib chiqardi va xalqaro hamjamiyatni tashvishga solmoqda. Insoniyat tomonidan kashf etilgan ba’zi yangi fan va texnika yutuqlari bugungi kunda sayyoramiz aholisi xavfsizligiga tahdid solmoqda. Aslida, kiberjinoyatchilik yangi hodisa bo‘lib, uning har bir davlatning milliy xavfsizligiga tahdidlari seziladi va Tojikiston ham bu tahdidlardan xoli yemas.

Kiber jinoyatlar tushunchasi ostida kompyuter texnologiyalari, internet va ijtimoiy tarmoqlar orqali sodir etiladigan jinoyatlar tushuniladi.

Kompyuter tizimlariga hujum qilish, shaxsiy ma’lumotlarni o‘zlashtirish, noqonuniy va yolg‘onma’lumotlarni tarqatish, kiberterrorizm va hokazolar kiberjinoyatlar deb tushunilib, turli iqtisodiy, ijtimoiy va siyosiy muammolarni keltirib chiqaradi. Hozirgi zamonda davlat, tashkilot va internet foydalanuvchilari kiberjinoyatlar tahdidi va xavfidan uzoq turolmaydi. Chunki kiber jinoyatlar butun dunyoga tarqaldi va undan faqat himoyalanish orqali himoyalanish mumkin.

Soha mutaxassislari har yili kiberjinoyatlar soni ortib borayotgani, tahlillarga ko‘ra, ayrim mamlakatlarda ijtimoiy tarmoqlar va internet foydalanuvchilari soni 4 dan 10 gacha kiber jinoyatlar qurboniga aylanayotganini ta’kidlamoqda.

Aytish joizki, kibertahdidlarning kuchayishi mamlakatlarni o‘z axborot xavfsizligiga alohida e’tibor qaratishga majbur qildi, chunki fan-texnika asri bo‘lgan XXI asrda har bir davlat va xalqning milliy xavfsizligi uning axborot xavfsizligiga bog‘liq. Bizningcha, kiberjinoyatlarning yangi tahdid va xatarlarini inobatga olgan holda rivojlangan davlatlar uning xavf-xatarlaridan himoyalanish uchun kiberxavfsizlik bo‘yicha maxsus strategiyani amalga oshiradi.

Bir qator ilg‘or davlatlarning sun’iy intellekt sohasidagi milliy strategiyalarini tahlil qilish mamlakatimiz uchun ustuvor yo‘nalish sifatida quyidagi beshta yo‘nalishni ajratib ko‘rsatish imkonini beradi:

- Sun’iy intellekt sohasida fundamental amaliy tadqiqotlar o‘tkazish - matematik usullardan foydalangan holda yangi sun’iy intellekt algoritmlarini yaratish;
- sun’iy intellekt injiniringini rivojlantirish - fundamental amaliy tadqiqotlar natijasida olingan algoritmlarni turli amaliy muammolarni hal qilishda qo‘llash, yangi dasturiy ta’minot va texnologik yechimlarni ishlab chiqish;
- Ma’lumotlar – ma’lumotlarni yig‘ish, saqlash, qayta ishlash va optimallashtirish (algoritmlarni o‘rgatish uchun);
- kadrlar tayyorlash – sun’iy intellekt sohasida yuqori malakali ilmiy kadrlar va mutaxassislarni tayyorlash, yangi ta’lim dasturlarini yaratish;
- Qonunchilik bazasi – sun’iy intellekt texnologiyalarini rivojlantirishni qo‘llab-quvvatlovchi qonunlar, standartlar va axloqiy qoidalarni ishlab chiqish va amalga oshirish[4].

Mamlakatimizda sun’iy intellekt muhandisligining ustuvor yo‘nalishlarini aniqlash uchun bir qator omillarga e’tibor qaratish lozim. Sun’iy intellekt texnologiyalari odamlarni monoton ishlardan ozod qilish, qarorlar qabul qilishni qo‘llab-quvvatlash, xavfli ish joylarini avtomatlashtirish, odamlar o‘rtasidagi muloqotni qo‘llab-quvvatlash, ijtimoiy ta’sir va ijtimoiy integratsiyani kuchaytirish, mamlakatning ichki va tashqi xavfsizligini ta’minlash uchun qo‘llaniladi. Sun’iy intellekt texnologiyalari iqtisodiy rivojlanish vositasiga aylanib bormoqda va harbiy sohada hal qiluvchi ustunlikka erishish imkoniyatini berishi mumkin. Sun’iy intellekt muhandisligi ushbu ko‘p tarmoqli sohalardagi zaif nuqtalarni yengib o‘tadigan va chegaralarni yengib o‘tadigan texnologik yechimlarga e’tibor qaratishi kerak. Shu munosabat bilan sun’iy intellekt yechimlarini turli sohalarda qo‘llashga ko‘maklashish muhim vazifalardan biri hisoblanadi.

Ma’lumotlar AI modellari uchun «yoqilg‘i» bo‘lib xizmat qiladi. Muayyan muammo bo‘yicha modelni o‘rgatish haqiqiy ma’lumotlarni talab qiladi va ma’lumotlar qanchalik ko‘p va

yaxshi bo‘lsa, modellarni o‘rgatish imkoniyati shunchalik yaxshi bo‘ladi. Shuning uchun ma’lumotlarni to‘plash, saqlash va mavjudligini ta’minlash katta ahamiyatga ega. Shumunosabat bilan mamlakatimizda hosil bo‘ladigan ma’lumotlarni to‘plash, raqamlashtirish va ulardan foydalanish imkoniyatini ta’minlash, muvofiqlashtirilgan yagona siyosatni amalga oshirish, bu jarayon uchun zarur infratuzilmani yaratish ustuvor vazifalardan biridir.

Xulosa qilib ayitganda, kibermakon va umuman kiberxavfsizlik bo‘yicha so‘nggi AKTlarni ishlab chiqish va ulardan foydalanish sohasida eng rivojlangan jahon kuchlari to‘g‘risida yagona nuqtai nazarning yo‘qligi, shuningdek, mualliflik huquqini ta’minlash bo‘yicha global munozaralarning kuchayishi qo‘shimcha asoratlarni keltirib chiqaradi. Shu bilan birga, to‘g‘ri ta’kidlash joizki, xalqaro miqyosda kiberxavfsizlik muammolarini hal etishda izchil taraqqiyot kuzatilmoqda, xususan, milliy va mintaqaviy darajada kiberjinoyatchilikka qarshi kurashish bo‘yicha davlatlararo konsensusga erishish mumkin edi. Kiberxavfsizlik sohasidagi boshqa muammolar zamonaviy kibertahdidlarga qarshi kurashish chora-tadbirlari tizimini yaratish maqsadida keyingi tadqiqotlarni talab qiladi.

REFERENCES

1. Американская концепция угроз информационной безопасности и ее международно-политическая составляюшая Батуэва Елена Владимировна Диссертатсии 2014 стр 207.
2. Управление процессами обеспечения кибербезопасности как фактор международной стабилности. Текст научной стати по спетсиалности «Политологические науки» 2017, №4 (2).
3. https://www.delfi.lv/tech/tehnologii/ekspert-nuzhna-zhenevskaya-konven ciyadlyakibervojn. d?id =34688001.
4. O‘zbekiston Respublikasi Prezidentining qarori, 17.02.2021 yildagi PQ-4996-son.