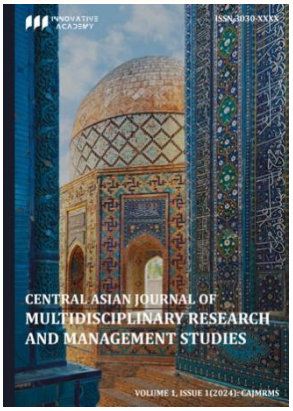


ELEKTRON HUKUMAT TIZIMIDA XODIMLARNING AXBOROT XAVFSIZLIGI VA KIBERXAVFSIZLIK BO'YICHA XABARDORLIGINI OSHIRISH HAMDA RAQAMLI KOMPETENSIYALARINI RIVOJLANTIRSH

Jaksilikova Guldana Muratbay qizi

Toshkent davlat yuridik universiteti

Ommaviy huquq fakulteti

Davlat va jamiyat boshqaruvi yo'nalishi 2- bosqich talabasi

e-mail: guldanajaksilikova22@gmail.com

https://doi.org/10.5281/zenodo.17614975

ARTICLE INFO

Received: 1st November 2025
Accepted: 2nd November 2025
Published: 15th November 2025

KEYWORDS

elektron hukumat, axborot xavfsizligi, kiberxavfsizlik, kiberjinoyatlar, gemifikatsiya, lavozimga moslashtirilgan o'quv dasturlari, raqamli kompetensiyalar, davlat xizmatchilari.

ABSTRACT

Mazkur maqolada elektron hukumat tizimining rivojlanishi natijasida axborotlarning raqamlashtirilishi, elektron davlat xizmatlarining kengayishi hamda barcha sohalarning raqamli transformatsiyasi jarayonida yuzaga kelayotgan kiberjinoyatlar global miqyosda va O'zbekiston misolida tahlil qilinadi. Davlat sektorida mavjud axborot tizimlari, resurslari va veb-saytlarga nisbatan kiberhujumlar sonining ortib borish sabablari hamda ularning asosiy turlari statistik ma'lumotlar asosida o'rganiladi. Shuningdek, O'zbekistonning kiberhimoya sohasidagi siyosati o'rganilib, ilg'or xorijiy tajriba asosida davlat xizmatchilarining raqamli kompetensiyalarini rivojlantirishning innovatsion yo'nalishlari, xususan lavozimga moslashtirilgan, sun'iy intellekt va gemifikatsiya elementlariga asoslangan maxsus kiberxavfsizlik o'quv dasturlarini joriy etish bo'yicha takliflar ishlab chiqilgan.

KIRISH

Birlashgan Millatlar Tashkiloti tomonidan belgilangan Barqaror rivojlanish maqsadlariga (SDG) erishishning eng samarali vositalaridan biri sifatida elektron hukumat tizimini rivojlantirish e'tirof etilgan. Bugungi kunda tashkilotga a'zo aksariyat davlatlar davlat xizmatlarini raqamlashtirish orqali boshqaruvning samaradorligini oshirish, shaffoflikni ta'minlash va fuqarolarga qulaylik yaratish yo'lida izchil choralar ko'rmoqda. Shu nuqtai nazardan, O'zbekiston Respublikasi ham mazkur yo'nalishda faol islohotlarni amalga oshirib kelmoqda. Jumladan, "Raqamli O'zbekiston–2030" strategiyasi doirasida mamlakat miqyosida sifatli, qulay va talabi yuqori bo'lgan elektron davlat xizmatlarini kengaytirish, ularni bosqichma-bosqich raqamli shaklga o'tkazish**,** hamda 2022 yilga qadar avtomatlashtirilgan xizmatlar ulushini 60 foizga yetkazish maqsad qilib qo'yilgan edi.[1] 2024 yil holatiga ko'ra, Yagona interaktiv davlat xizmatlari portali orqali 24 ta soha doirasida 320 dan ortiq davlat organlari, tashkilot va muassasalar tomonidan 770 dan ortiq elektron davlat xizmatlari

fuqarolarga taqdim etilmoqda. Elektron hukumat tizimi fuqarolarga davlat idoralari bilan to‘g‘ridan-to‘g‘ri va tezkor muloqot o‘rnatish**,** byurokratik to‘siqlarni kamaytirish**,** korrupsiya xavfini pasaytirish hamda davlat xizmatlaridan shaffof va samarali tarzda foydalanish imkonini bermoqda. Ammo elektron hukumat tizimida axborotlarning raqamlashtirilishi, elektron davlat xizmatlarining kengayishi va ijtimoiy, iqtisodiy, siyosiy va ma’naviy sohalarning raqamli transformatsiyasi natijasida, davlat idoralarida saqlanayotgan maxfiy axborotlarga, shuningdek, davlat organlarining veb-saytlariga nisbatan kiberhujumlar soni ortib bormoqda. Elektron hukumat tizimlarining texnik xavfsizligini ta’minlashga qaratilgan moliyaviy resurslar ajratilayotgan bo‘lishiga qaramay, axborot xavfsizligining buzilishi va kiberhujumlar sonining ortishi tendensiyasi kuzatilib, ularning aksariyati inson omili, ya’ni davlat xizmatchilarining raqamli kompetensiyalarining yetishmovchiligi asosida sodir etilmoqda**.** ENISA (European Union Agency for Cybersecurity) tomonidan 2023 yilda o‘tkazilgan tahlil natijalariga ko‘ra, davlat sektorida axborot xavfsizligining buzilishi holatlarining 77 foizi inson omiliga bevosita bog‘liq ekani aniqlangan. [2] IBM (International Business Machines Corporation) tomonidan 2023 yilda o‘tkazilgan tadqiqotlarga ko‘ra, global miqyosda kiberhujumlar oqibatida ko‘rilgan o‘rtacha zarar 5.56 million AQSh dollaridan oshgan.[3] O’zbekistonda Kiberxavfsizlik markazining 2023 yilgi hisobotida mamlakatdagi 86 ta axborot tizimi va resurslar xavfsizlik darajasini baholash natijasida 7 740 ta zaiflik aniqlangani ma’lum qilingan. Shuningdek, milliy internet segmentida joylashgan 677 ta veb-resursda jami 1 186 ta zaiflik qayd etilgan bo‘lib, ulardan 1 022 tasi davlat organlariga tegishliligi aniqlangan.[4] Global va milliy statistika ma’lumotlarini tahlili shuni ko’rsatdiki, elektron hukumat tizimlarining xavfsizligi va barqaror rivoji faqat texnik himoya choralari bilan emas, balki davlat xizmatchilarining raqamli kompetensiyalarini takomillashtirish bilan chambarchas bog‘liq.

TADQIQOT MAQSADI

Mazkur tadqiqotning maqsadi — elektron hukumat tizimida faoliyat yurituvchi davlat idoralari xodimlarining axborot xavfsizligi va kiberxavfsizlik bo‘yicha xabardorlik darajasini oshirish hamda ularning raqamli kompetensiyalarini rivojlantirish yo‘nalishida xorijiy davlatlar tajribasida qo‘llanilgan eng samarali yondashuvlarni aniqlash, shu orqali inson omili nuqtai nazaridan elektron hukumat tizimining xavfsizlik darajasini mustahkamlashdan iborat.

TADQIQOT VAZIFALARI

1. Global miqyosda va O‘zbekiston Respublikasida elektron hukumat tizimiga nisbatan sodir etilayotgan kiberhujumlarning turlari, ko‘lami va dinamikasini tahlil qilish;
2. O‘zbekiston Respublikasidagi elektron hukumat tizimlari va davlat veb-resurslarida kiberxujumlarning kelib chiqish omillari hamda ularni yuzaga keltiruvchi asosiy sabablarni tahlil qilish;
3. O‘zbekistonda axborot xavfsizligi va kiberhimoya sohasidagi mavjud normativ-huquqiy hujjatlar hamda davlat siyosatini tahlil qilish;
4. Xorijiy davlatlar tajribasidagi axborot xavfsizligi va kiberxavfsizlik bo‘yicha xodimlarni tayyorlash usullarini tahlil qilish va shunga asoslanib elektron hukumat tizimida innovatsion yondashuvlar ishlab chiqish.

MATERIALLAR VA USLUBLAR

“Enhancing Employees’ Information Security Awareness in Private and Public Organisations: A Systematic Literature Review” nomli moqaloda davlat va xususiy sektorlarda xodimlarning axborot xavfsizligi xabardorligi hamda raqamli kompetensiyalarining ahamiyati tahlil qilinadi. Tadqiqotda texnik choralar axborot xavfsizligini ta’minlash uchun yetarli emasligi aniqlangan.

Shu bois asosiy e'tibor inson omiliga, xususan xodimlarning raqamli kompetensiyalarini rivojlantirishga qaratilgan. Mualliflar barcha sohalar integratsiyalashganligi sababli, muammoning faqat bitta jihatini o'rganish orqali to'liq yechimga erishib bo'lmasligini asoslaydi. Tadqiqot jarayonida elektron hukumat tizimida xodimlarning axborot xavfsizligi va kiberxavfsizlik bo'yicha xabardorligini oshirish hamda raqamli kompetensiyalarini rivojlantirish masalalari yuzasidan mahalliy va xalqaro ilmiy jurnallar, tahliliy hisobotlar, normative-huquqiy hujjatlar hamda amaliy tajribalardan foydalanildi. Asosiy ma'lumot manbalari sifatida European Union Agency for Cybersecurity (ENISA) tomonidan chop etilgan *ENISA Threat Landscape 2023* hisobotlari, The HIPAA Journal, Asimily (ilg'or xavf boshqaruvi platformasi), shuningdek IBM tomonidan e'lon qilingan xalqaro ilmiy manbalar tanlab olindi. "6 Reasons Why the Public Sector is a Prime Target for Cyberattacks" nomli Asimily maqolasida davlat sektorlariga qaratilgan kiberhujumlarning asosiy sabablari va omillari yoritib berilgan. "Ransomware: Types, Examples & Removal Tactics" (Fortinet Cyberglossary, 2025) va "Phishing vs. Spear Phishing: Why One Attack Is Getting Harder to Catch" (Valimail Blog, 2025) maqolalarida davlat sektoriga nisbatan sodir etiladigan kiberhujumlarning xususiyatlari, usullari va oqibatlari batafsil tahlil qilingan. "What is Role-Based Security Awareness Training, and How Can It Be Customized and Adapted?" nomli Keepnet Labs Blog maqolasida davlat sektorida xodimlarning raqamli ko'nikmalarini rivojlantirishdagi eng samarali yechim sifatida lavozimga moslashtirilgan kiberxavfsizlik bo'yicha o'quv dasturlarini (Role-Based Security Training) joriy etish taklif etiladi.

NATIJALAR VA STATISTIKA

Global miqyosda quyidagi sabablarga ko'ra davlat sektoriga nisbatan kiberxujumlar amalga oshiriladi:

1. **Katta hajmdagi axborotning mavjudligi**

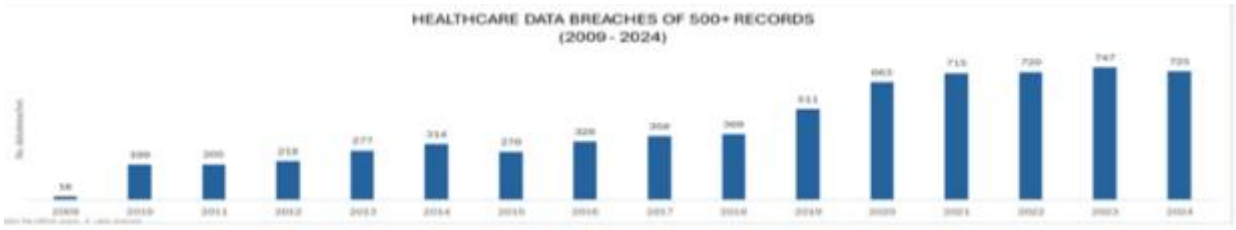
Davlat sektori o'zida katta hajmdagi maxfiy va kiberjinoyatchilar nuqtayi nazaridan yuqori qiymatga ega bo'lgan ijtimoiy, iqtisodiy hamda siyosiy axborotlarni, masalan masalan fuqarolarning shaxsiy ma'lumotlari, jismoniy va yuridik shaxslarning bank hisobvaraqalari, davlat sirlariga ega. Ushbu turdagi axborotlar uchun kiberjinoyatlar shaxsiy, moliyaviy manfaatga yo'naltirilishi bilan birga, boshqa davlatlar tomonidan moliyalashtiriladigan kiberjinoyatchilar guruhi tomonidan ham nishonga olinadi. Microsoft tadqiqotlariga ko'ra, AQSH davlat sektoriga qilingan kiberjinoyatlarning 40% boshqa davlatlar tomonidan moliyalashtirilgan kiberjinoiy guruhlar tomonidan amalga oshirilgan.**[5]** O'zbekistonda misolida tahlil qiladigan bo'lsak, Kiberxavfsizlik markazining 2023-yilgi hisobotiga muvofiq, 2023-yilda amalga oshirilgan kiberhujumlarning geografik taalluqliligi tahliliga ko'ra, eng ko'p kiberhujumlar quyidagi davlatlar hududidagi IP-manzillardan amalga oshirilgani kuzatilgan.

1-diagramma. Veb-resurslarga bo'lgan kiberhujumlar davlatlar kesimida aks etishi.

2. **Davlatning muhim axborot infratuzilmasi obyektlarining mavjudligi**

Davlat o'z faoliyatida boshqaruv, davlat xizmatlari ko'rsatish, mudofaa, milliy xavfsizlik, huquq-tartibot, yoqilg'i-energetika majmui, atom energetikasi, neft-kimyo tarmoqlari, bank-moliya tizimi, sog'liqni saqlash, suv resurslaridan foydalanish va suv ta'minoti kabi strategik ahamiyatga ega sohalarni qamrab oladi. Mazkur sohalarning har biri kiberjinoyatchilar uchun

nishon bo‘lishi mumkin. Masalan, sog‘liqni saqlash tizimiga qaratilgan kiberhujumlar bemorlarning shaxsiy ma’lumotlarini o‘zgartirish yoki yo‘q qilish, shuningdek, operatsiya jarayonlarida qo‘llaniladigan texnik apparatlarni masofadan boshqarish va bloklashga bo‘lgan harakatlarni o‘z ichiga oladi. Ba’zi holatlarda, apparatlarni qayta ishga tushirish yoki tibbiy tizimlarga kirish imkonini tiklash evaziga, kiberjinoyatchilar o‘z hisob raqamlariga kriptovalyuta shaklida to‘lov amalga oshirilishini talab qiladilar.



2-diagramma. *The HPPA Journal* ma’lumotlariga ko‘ra, AQShda sog‘liqni saqlash sohasiga nisbatan amalga oshirilgan axborot xavfsizligiga oid kiberhujumlar soni yildan-yilga ortib bormoqda. 2009-yilda qayd etilgan kiberhujumlar soni atigi **18 ta** bo‘lgan bo‘lsa, 2024-yilga kelib ushbu ko‘rsatkich **747 taga** yetgan.[6]

3. Kiberxavfsizlikni moliyalashtirishdagi moliyaviy resurslarning yetishmovchiligi

Davlat organlari, muassasalari va tashkilotlarining ko‘pligi sababli ularning barcha darajadagi axborot tizimlari va veb-resurslarinining kiberxavfsizligini davlat byudjetidan moliyalashtirishda taqchillik kuzatiladi. Asosiy davlat hokimiyati organlari — qonun chiqaruvchi, ijro va sud tizimlari — axborot xavfsizligi nuqtayi nazaridan yetarli darajada moliyalashtirilgan bo‘lishi mumkin. Biroq ularning quyi tarkibiy boshqarmalari va bo’linmalarida moliyaviy resurslarning yetishmasligi, natijada kiberxavfsizlik infratuzilmasining zaiflashishi holatlari kuzatiladi. Masalan, “2025-yil uchun O‘zbekiston Respublikasining Davlat byudjeti to‘g‘risida”gi Qonunga muvofiq, “Kiberxavfsizlik markazi” faoliyatini moliyalashtirish uchun 75 million so‘m ajratilgan. Bu ko‘rsatkich madaniyat sohasidagi (davlat buyurtmasi asosida milliy kino mahsulotlarini yaratish uchun — 110 million so‘m) hamda sport sohasidagi (olimpiya o‘yinlariga tayyorgarlik ko‘rish uchun — 190 million so‘m) xarajatlarga nisbatan qariyb ikki baravar kam.[7]

Davlat xizmatchilariga nisbatan sodir qilinadigan kiberhujumlarning turlari.

1. Fishing

Axborot xavfsizligi sohasida keng tarqalgan kiberjinoyatlardan biri bo’lib, ushbu turdagi kiberhujum ijtimoiy muhandislik (social engineering) usullari orqali inson psixologiyasiga ta’sir ko‘rsatish yo‘li bilan amalga oshiriladi. Hujum jarayonida kiberjinoyatchilar soxta elektron pochta xabarlari, telefon qo‘ng‘iroqlari yoki matnli xabarlar (SMS) orqali foydalanuvchini chalg‘itib, uni maxfiy ma’lumotlarni oshkor etishga undaydi. Odatda, hujumchi o‘zini qonuniy va ishonchli tashkilot yoki shaxs sifatida tanishtiradi hamda shaxsni identifikatsiyalashga imkon beruvchi ma’lumotlar**,** bank va kredit karta raqamlari, parollar kabi axborotlarni qo‘lga kiritishga harakat qiladi. O‘zbekiston Respublikasi hududida ham phishing hujumlari orqali foydalanuvchilarni aldash holatlari keng tarqalgan**.** Jumladan, O‘zbekiston Respublikasi Prezidentining rasmiy veb-sayti **(**www.prezident.uz**)**, banklar va boshqa moliyaviy institutlarning soxta nusxalarini yaratish orqali foydalanuvchilarning shaxsiy ma’lumotlari va moliyaviy resurslariga tajovuz qilingan. Fishing kiberjinoyatini yozma xabarlar, masalan e-mail yoki SMS orqali amalga oshirish bosqichlari. Kiberjinoyatchi tomonidan nishondagi shaxsga fishing xabarnoma yuboriladi. Nishondagi shaxsning shubhali

linkni bosishi bilan fishing veb-sahifaga yo'naltirib, shaxsning maxfiy ma'lumotlari o'zlashtiriladi.

2. Spear-fishing

Fishingning yanada takomillashgan varianti bo'lib, u bitta yoki cheklangan doiradagi shaxslarga yo'naltirilgan, aniq va maqsadli kiberhujum. Ushbu hujum turida nishondagi shaxs yoki guruh haqida muayyan vaqt davomida axborot yig'iladi va yig'ilgan ma'lumotlar jinoyatni muvaffaqiyatli amalga oshirishda qo'llaniladi. Spear-fishing hujumlari odatda ijtimoiy muhandislik usullari va soxtalashtirilgan elektron pochta xabarlari orqali amalga oshiriladi; hujumchi o'zini nishonning oilasi yoki yaqin tanishi sifatida tanishtirishi mumkin. Davlat organlarida bu uslub bilan, ayniqsa, muhim lavozimdagi xodimlar nishonga olinadi, chunki ularning ma'lumotlari orqali tizimlarga ruxsatsiz kirish yoki maxfiy hujjatlarga erishish osonlashadi.

3. Ransomware

Kompyuter, server yoki tarmoqdagi fayllarni yoki butun tizimni shifrlab, foydalanuvchini ularni ochish imkonidan mahrum qiluvchi zararli dastur (malware) turi. Mazkur kiberjinoyatda kiberjinoyatchi tomonidan nishondagi shaxs o'rganiladi va fishing orqali zararli dasturni kompyuterga o'rnatadi. Nishondagi shaxsning fayllari yoki butunlay kompyuteriga zararli dasturni o'rnatish uchun kuzatishni va o'rganishni amalga oshiradi. Tanlangan zararlantirish obyektini shifrlaydi va shifrlanganlik haqida nishondagi shaxsga xabarnoma jo'natib, kriptovalyuta shaklida pul mablag'ini talab qiladi.

O'zbekistondagi kiberjinoyatlar

O'zbekistonda Kiberxavfsizlik markazining 2023 yilgi hisobotida davlat sektoridagi axborot tizimlari va veb-resurslarga sodir etilgan kiberjinoyatlar tahlili keltirilgan. Axborot tizimlarining kiberxavfsizlik talablariga moslik ekspertizasiga muvofiq davlat tashkilotlarining shaxsiy tashabbuslar asosida 86 ta axborot tizimi va resurslarida axborot xavfsizligi ta'minlanganlik holati bo'yicha o'rganish va tahlil ishlari olib borilib, 740 ta zaiflik aniqlandi.

4-diagramma. Aniqlangan zaifliklar sonining sohalar kesimida aks etishi.

Mazkur zaifliklar kelib chiqishining asosiy sabablari:

- Ishonchli va tajribaga ega bo'lmagan tashkilotlarga ishlab chiqish uchun loyihalarni topshirish;
- AKT va kiberxavfsizlik sohasida malakali mutaxassislar yetishmovchiligi;
- Kiberxavfsizlik masalalarini hal etishda yetarli darajada moliyalashtirilmaslik;
- Tashkilotlarda malakali xodimlarning yetishmasligi;
- Tashkilotlarda moliyaviy barqarorlikning yo'qligi;
- Axborot tizimlari va resurslarini o'z vaqtida va muntazam kiberxavfsizlik; talablariga muvofiqligi bo'yicha ekspertizadan o'tkazishga e'tiborsizlik;

- Davlat organlari rahbariyati va mas'ul xodimlar tomonidan mavjud zaiflik va kamchiliklarni bartaraf etish bo'yicha muntazam nazorat o'rnatilmaganligi.[4]

Internet tarmog'ining milliy segmentidagi veb-resurslarni doimiy nazorat qilish jarayonida jami 158 ta kiberxavfsizlik hodisasi aniqlangan, bu esa 2022 yilga nisbatan 32% ga kam. Aniqlangan hodisalarning 38 tasi davlat organlari veb-resurslariga to'g'ri keladi. Quyida aniqlangan hodisalarning asosiy turlari keltirilgan.

5-diagramma. Aniqlangan kiberxavfsizlik hodisalarining turlari.

Davlat idoralari veb-resurslarida aniqlangan kiberxavfsizlik hodisalarini tahlil qilish natijasida ular quyidagi zaifliklar tufayli yuzaga kelgani aniqlangan:

- foydalanuvchi kontentini tekshirish va filtrdan o'tkazish mexanizmining mavjud emasligi va zaif parol himoyasi.

O'zbekistonda kiberxavfsizlikni ta'minlash siyosatining normativ-huquqiy asosi.

Kiberxavfsizlik sohasidagi munosabatlarni tartibga solish maqsadida O'zbekiston Respublikasining "Kiberxavfsizlik tog'risida" gi Qonuni 15 aprel 2022 yili qabul qilingan bo'lib, 17-iyul 2022 yili kuchga kirgan. Qonunga muvofiq Kiberxavfsizlik sohasidagi yagona davlat siyosatini O'zbekiston Respublikasi Prezidenti belgilaydi va Davlat xavfsizlik xizmati mazkur sohasidagi vakolatli davlat organi hisoblanadi. Shuningdek, "Kiberxavfsizlik markazi" davlat unitar korxonasi 2019-yil 14-sentabrdagi O'zbekiston Respublikasi Prezidentining "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish hamda ularni himoya qilish tizimini takomillashtirishga oid qo'shimcha chora-tadbirlar to'g'risida"gi qaroriga muvofiq o'z faoliyatini amalga oshirib kelmoqda. Mazkur Qonunning 14-moddasida davlat organlari va tashkilotlarining kiberxavfsizlifini ta'minlashga qaratilgan huquq va majburiyatlari keltirilgan bo'lib, unga muvofiq:

Davlat organlari va tashkilotlari quyidagi huquqlarga ega:

➢ kiberxavfsizlikni ta'minlash maqsadida vakolatli davlat organidan kibertahdidlar, dasturiy ta'minotdagi, uskunalar va texnologiyalardagi zaifliklar to'g'risidagi axborotni olish;

➢ vakolatli davlat organidan kiberhujumlardan himoya qilish vositalari va usullari, ularni aniqlash hamda bartaraf etish yo'llari to'g'risida axborot va maslahatlar olish;

➢ kiberxavfsizlikni ta'minlashga doir chora-tadbirlarni ishlab chiqish va amalga oshirish.

Davlat organlari va tashkilotlarga quyidagi majburiyatlar yuklatilgan:

➢ o'z tasarrufidagi axborot tizimlari va resurslarining kiberxavfsizligini, tarmoqlar ishining barqarorligini ta'minlashi, shuningdek kiberxavfsizlik bo'yicha o'z majburiyatlarini bajarishi, vakolatli davlat organini kiberhujumlar to'g'risida ogohlantirishi;

➢ o'z axborot tizimlari va resurslarida saqlanayotgan ma'lumotlarning o'g'irlanishi hamda qalbakilashtirilishi holatlarining oldini olish choralarini ko'rishi;

➢ o'z axborot tizimlari va resurslarini kiberhimoya qilish uchun sertifikatlashtirilgan apparat, apparat-dasturiy va dasturiy ta'minotdan foydalanishi.[8]

Mazkur Qonunning 18-moddasiga muvofiq davlat organlarining axborot resurslari, davlat organlarining axborot tizimlari, muhim axborot infratuzilmasi obyektlari toifasiga kiritilgan axborot tizimlari majburiy tartibda **kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan** o'tkaziladi. Ekspertizaning o'tkazilish tartib-taomili O'zbekiston Respublikasi Davlat xavfsizlik xizmati raisining buyrug'i bilan tasdiqlangan Kiberxavfsizlik talablariga muvofiqlik yuzasidan ekspertizadan o'tkazish tartibi to'g'risidagi nizom asosida o'tkaziladi. "Kiberxavfsizlik markazi" davlat unitar korxonasi va O'zbekiston Respublikasi Markaziy banki ekpertizadan o'tkazuvchi tashkilotlar hisoblanadi. Qonunning 19-moddasida Davlat organlari va tashkilotlari axborot tizimlari hamda resurslarining, shuningdek muhim axborot infratuzilmasi obyektlarining kiberxavfsizligini ta'minlash uchun qo'llaniladigan apparat, apparat-dasturiy va dasturiy vositalar majburiy tartibda **sertifikatlashtirilishi** lozimligi ta'kidlangan. Sertifikatlash uchun vakolatli tashkilot Kiberxavfsizlik markazi hisoblanadi. Kiberxavfsizlik markazining 2023 yilgi hisobotida Dasturiy ta'minotlarni sertifikatlashtirish xizmatlari ko'rsatish hajmi 2022 yilga nisbatan 13 foizga kamaygan bo'lsa-da, ushbu yo'nalish bo'yicha tuzilgan yangi shartnomalar ulushi 25,9 foizga oshgan. Jumladan, dasturiy ta'minotlarni sertifikatlashtirish bo'yicha jami 34 ta shartnoma imzolangan. Sertifikatlash tartib-taomili Axborot tizimlari va resurslarining kiberxavfsizligini ta'minlash uchun qo'llaniladigan apparat, apparat-dasturiy hamda dasturiy vositalarni sertifikatlashtirish tartibi to'g'risidagi nizom bilan belgilangan. Shuningdek, **axborotlashtirish obyektlari va muhim axborot infratuzilmasi obyektlarining Kiberxavfsizlikning ta'minlanganlik darajasini baholash** o'tkaziladi. Bu axborot tizimlari va resurslarining himoyalanganlik holatini, shuningdek ko'rilayotgan tashkiliy choralarning samaradorligini aniqlashga qaratilgan tashkiliy-texnik tadbirlar majmuidan iborat. Kiberxavfsizlik markazining 2023 yilgi hisobotida Davlat va xo'jalik boshqaruvi organlarining ixtisoslashtirilgan bo'linmalari hamda boshqa tashkilotlarga axborot va kiberxavfsizlikni ta'minlash, mavjud kamchiliklarni bartaraf etish masalalari bo'yicha jami 986 ta maslahat yordami ko'rsatildi. Axborot va kiberxavfsizlik masalalariga oid mavzularda 17 ta davlat tashkilotida seminarlar, treninglar va amaliy mashg'ulotlar o'tkazildi. Respublika va mahalliy ijro etuvchi hokimiyat organlarining axborot-kommunikatsiya texnologiyalarini rivojlantirish uchun mas'ul xodimlari malakasini oshirish va reyting baholashni tashkil etish chora-tadbirlari to'g'risidagi Hukumat qarori qabul qilingan. Mazkur qarorga muvofiq, 2023-yil 1-iyuldan boshlab davlat organlarining **axborot-kommunikatsiya texnologiyalari sohasiga** mas'ul xodimlari har 3 yilda bir marotaba malakasini oshirishi belgilangan. Shuningdek, 2023-yil 1-avgustdan **boshlab davlat organlarining birinchi rahbarlari** raqamli texnologiyalarni keng joriy etish va loyihalarni samarali amalga oshirish masalalari bo'yicha Davlat boshqaruvi akademiyasida qisqa muddatli o'quv kurslarida tahsil olishi belgilangan. [9] Ammo mazkur o'quv kursalari va xodimlarning raqamli kompetensiyalarini oshirishga qaratilgan malaka oshirishi cheklangan doiradagi shaxslar uchun. Natijada, boshqa davlat organlari, tashkilot va muassasa xodimlarining raqamli ko'nikmalari rivojlantirish masalasiga aniq yechim berilmagan va ularning raqamli kompetensiyalarining statistikasi ham mavjud emas.

MUHOKAMA

Davlat organlari, tashkilotlar va muassasalarda faoliyat yurituvchi xodimlarning har biri qonunchilikda belgilangan aniq majburiyat va funksional vazifalarga ega. Shu sababli, ularga nisbatan sodir etiladigan kiberjinoyatlarning turlari ham lavozim xususiyatiga qarab farqlanadi. Masalan, rahbarlik lavozimidagi shaxslar ko'pincha "whale attack" deb nomlanuvchi kiberhujumlarning nishoniga aylanadi. Bunday kiberhujumlar yuqori lavozimli mansabdor shaxslarga rasmiy ko'rinishdagi, yuqori darajada ishonarli soxta veb-sahifalar yoki email orqali amalga oshiriladi. Aksincha, soliq organlari xodimlariga nisbatan spear fishing orqali soliq to'lovchilardan kelgan murojaat yoki hujjat shaklida hujumlar amalga oshiriladi. Mazkur tahdidlarni inobatga olgan holda, Lavozimga moslashtirilgan maxsus

kiberxavfsizlik o‘quv dasturi (Role-Based Security Training) joriy etilishi maqsadga muvofiq, negaki bu orqali har bir davlat xizmatchisinig o‘z lavozimiga xos bo‘lgan kiberxavflardan himoyalanish ko‘nikmalarini shakllantirishga imkon beradi. An’anaviy o‘quv dasturlaridan farqli ravishda, RBST dasturi:

- xodimning lavozimi va faoliyat sohasi asosida real kiberhujumlarni o‘rganadi;
- amaliy mashg‘ulotlar va simulyatsiyalar orqali tahdidlarni aniqlash, tahlil qilish va ularga javob qaytarish ko‘nikmalarini shakllantiradi.

Tadqiqotlar shuni ko‘rsatadiki, lavozimga moslashtirilgan o‘quv dasturlari an’anaviy treninglarga nisbatan 30% ga samaraliroq bo‘lib, xodimlarning tahdidlarni aniqlash va ularga tezkor chora ko’rish va himoyalanish qobiliyatini oshiradi.

Geymifikatsion usullar orqali kiberhujumlar simulyatsiyasi asosida davlat xizmatchilari uchun o‘quv dasturi

Lavozimga moslashtirilgan kiberhujumlar simulyatsiyasi orqali
har bir davlat xizmatchisiga o‘z lavozimiga xos kiberxujum ssenariy ishlab chiqiladi va tekshiruvdan o’tkaziladi. Masalan, rahbarlar “whaling”, moliya bo‘limi xodimlari esa “phishing” holatlari bo‘yicha mashq qiladilar. Bu yondashuv xodimlarning kiberxujumlarga amaliy tayyorgarligini kuchaytiradi. Sun’iy intellekt texnologiyalariga asoslangan kiberhujumlar simulyatsiyasi davlat xizmatchilariga real kiberxavflarni aniqlash, tahlil qilish va ularga real kiberxujumlar sodir etilganda tezkor qaror qabul qilish ko‘nikmalarini shakllantirish imkonini beradi. Bunday o‘quv jarayonlari an’anaviy nazariy ta’limdan farqli ravishda, amaliy mashg‘ulotlar orqali ishtirokchilarning hayotiy kiberxujumlarga oldindan tayyorlaydi. Simulyatsiya platformalariga geymifikatsion elementlarni qo‘shish o‘quv jarayonining samaradorligini sezilarli darajada oshiradi. Masalan, tezkor fikr-mulohaza (instant feedback), reyting tizimlari, ball yig‘ish mexanizmlari, interaktiv viktorinalar bo’lishi mumkin. Ular o‘quv jarayonini qiziqarli va raqobatga asoslangan shaklga keltiradi, bu esa xodimlarning o‘rganilgan bilimlarni uzoq muddatli eslab qolishga yordam beradi.

XULOSA

Elektron hukumat tizimining keng joriy etilishi davlat boshqaruvi samaradorligini oshirayotgan bo‘lsa-da, bu jarayon bilan bir qatorda kiberxavfsizlikka doir yangi tahdidlarning yuzaga kelmoqda. ENISA (2023) hisobotiga muvofiq davlat sektorida kiberxavflarning katta qismi inson omiliga, ya’ni davlat xizmatchilarining axborot xavfsizligi bo‘yicha bilim va ko‘nikmalarining yetarli emasligiga tog’ri keladi. Shu bois, davlat organlari faoliyatida aniq lavozimga moslashtirilgan suniy intelekt va gemifikatsion elementlar asosida maxsus kiberxavfsizlik o‘quv kurslarini joriy etish tahlifi berildi Shuningdek, sun’iy intellekt asosida ishlab chiqilgan kiberxujumlar simulyatsiyasi yordamida xodimlar real kiberxujumlar orqali tayyorlash masalasi ta’kidlandi.

MANFAATLAR TO’QNASHUVI

Mazkur maqola faqat ilmiy maqsadlarda amalga oshirilgan bo‘lib, muallif ushbu tadqiqot jarayonida hech qanday shaxsiy, moliyaviy manfaatlar to‘qnashuvi mavjud emasligini ma’lum qiladi.

FOYDALANILGAN ADABIYOTLAR:

1. O‘zbekiston Respublikasi Prezidentining Farmoni “Raqamli O‘zbekiston — 2030” strategiyasini tasdiqlash va uni samarali amalga oshirish chora-tadbirlari to‘g‘risida. — PF- 6079, 05.10.2020. // Lex.uz. — URL: https://lex.uz/egovstrategy

2. ENISA Threat Landscape 2023. — European Union Agency for Cybersecurity, 2023. — URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
3. IBM. Cost of a data breach: The industrial sector. — IBM Think Insights, 2024. — URL: https://www.ibm.com/think/insights/data-breach
4. «O‘zbekiston Respublikasi Kiberxavfsizligi - 2023 yil hisoboti» [Elektron resurs]. — Toshkent: Kiberxavfsizlik markazi DUK, 2024. — URL: https://csec.uz/2023report
5. “6 Reasons Why the Public Sector is a Prime Target for Cyberattacks.” — Asimily Blog, 2024. — URL: https://asimily.com/ps-cyberattacks
6. “Healthcare Data Breach Statistics.” — The HIPAA Journal, 26 Oct 2025. — URL: https://www.hipaajournal.com/healthcare-data-breach-statistics/
7. O‘zbekiston Respublikasining Qonuni «Davlat byudjeti to‘g‘risida — 2025 yil». — O‘RQ- 1011, 24.12.2024. // Lex.uz. — URL: https://lex.uz/uz/docs/-7277618
8. O‘zbekiston Respublikasining Qonuni “Kiberxavfsizlik to‘g‘risida”. — 15.04.2022. // Lex.uz. — URL: https://lex.uz/cyberlaw
9. “Davlat organlari rahbarlari raqamli texnologiyalar bo‘yicha qisqa muddatli kurslarda o‘qitiladi.” — Digital.uz, 22 May 2023. — URL: https://digital.uz/news/view/1685
10. O‘zbekiston Respublikasining Qonuni “Elektron hukumat to‘g‘risida”. — 2015-yil 9-dekabr. // Lex.uz. — URL: https://lex.uz/egovlaw
11. O‘zbekiston Respublikasining Qonuni «Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida». — 12.12.2002, № 439- II. // Lex.uz. — URL: https://lex.uz/docs/-52268
12. “Davlat organlari rahbarlari raqamli texnologiyalar bo‘yicha qisqa muddatli kurslarda o‘qitiladi.” — Digital.uz, 22 May 2023. — URL: https://digital.uz/news/view/1685
13. “Ransomware: Types, Examples & Removal Tactics.” — Fortinet Cyberglossary, 2025. — URL: https://www.fortinet.com/resources/cyberglossary/ransomware
14. “Phishing vs. spear phishing: Why one attack is getting harder to catch (2025 update).” — Valimail Blog. — URL: https://www.valimail.com/ps- vs- spear- phishing
15. “What is Role- Based Security Awareness Training, and How Can It Be Customized and Adapted?” — Keepnet Labs Blog. — URL: https://keepnetlabs.com/blog/what-is-role-based-security-awareness-training-and-how-can-it-be-customized-and-adapted