KIBERXAVFSIZLIKNI TA’MINLASHDA TEXNOLOGIK, TASHKILIY VA HUQUQIY OMILLARNING INTEGRATSIYALASHGAN MODELI

Xazratov Fazliddin Xikmatovich,
Buxoro davlat universiteti
Amaliy matematika va dasturlash texnologiyalari
kafedrasi dotsenti

Annotatsiya. Ushbu maqolada raqamli transformatsiya sharoitida kiberxavfsizlikni ta’minlashning dolzarb masalalari tahlil qilingan. Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida yuzaga kelayotgan kiberxavf va tahdidlarning asosiy turlari o‘rganilgan. Tadqiqotda kiberhujumlarning iqtisodiy va ijtimoiy oqibatlari, ularning davlat, biznes va ta’lim tizimlariga ta’siri yoritilgan. Sun’iy intellekt, mashinaviy o‘qitish, kriptografik himoya vositalari hamda ko‘p bosqichli autentifikatsiya texnologiyalarining kiberxavfsizlikni ta’minlashdagi o‘rni tahlil qilingan. Shuningdek, inson omili, raqamli savodxonlik va foydalanuvchilar xatti-harakatlarining axborot xavfsizligiga ta’siri baholangan. Tadqiqot natijalari kiberxavfsizlikni ta’minlashda texnik, tashkiliy va huquqiy choralarni kompleks ravishda qo‘llash zarurligini ko‘rsatadi.

Kalit so‘zlar: kiberxavfsizlik, axborot xavfsizligi, kiberhujum, raqamli transformatsiya, sun’iy intellekt, mashinaviy o‘qitish, kriptografiya, autentifikatsiya, fishing, zararli dasturlar, risk management; AHP, FMEA, NIST Cybersecurity Framework, ISO/IEC 27001.

Kirish. So‘nggi yillarda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi, internet tarmog‘i qamrovining kengayishi va raqamli xizmatlarning ommalashuvi natijasida jamiyatning barcha sohalarida raqamli transformatsiya jarayonlari sezilarli darajada jadallashdi. Davlat boshqaruvi, bank-moliya tizimi, elektron tijorat, sanoat, sog‘liqni saqlash va ta’lim sohalarida raqamli texnologiyalarning keng joriy etilishi katta hajmdagi ma’lumotlarni qayta ishlash, saqlash va uzatish zaruratini yuzaga keltirmoqda [13].

Raqamli iqtisodiyotning rivojlanishi axborot resurslari va tarmoqlarining o‘zaro integratsiyalashuvini kuchaytirib, yangi imkoniyatlar bilan bir qatorda yangi xavf va tahdidlarni ham yuzaga keltirmoqda. Kiberjinoyatchilikning murakkablashuvi, zararli dasturlarning takomillashuvi, fishing hujumlari, ijtimoiy muhandislik usullari, xizmat ko‘rsatishni rad etish (DDoS) hujumlari hamda ilg‘or doimiy tahdidlar (Advanced Persistent Threats – APT) sonining ortib borishi axborot tizimlari xavfsizligini ta’minlash masalasini dolzarb ilmiy-amaliy muammoga aylantirdi [2].

Zamonaviy kiberhujumlar nafaqat texnik infratuzilmaga zarar yetkazadi, balki tashkilotlarning moliyaviy barqarorligi, ishchanlik obro‘si va foydalanuvchilarning shaxsiy ma’lumotlari daxlsizligiga ham jiddiy xavf tug‘diradi [1]. Ayniqsa, davlat axborot tizimlari, muhim infratuzilma obyektlari va moliyaviy tashkilotlarga qaratilgan kiberhujumlar milliy xavfsizlikka salbiy ta’sir ko‘rsatishi mumkin [7].

Xalqaro tajriba shuni ko‘rsatadiki, kiberxavfsizlikni ta’minlash faqat texnik himoya vositalarini joriy etish bilan cheklanmaydi. Mazkur jarayon kompleks yondashuvni, jumladan, huquqiy-me’yoriy bazani takomillashtirish, xavflarni boshqarish tizimini joriy etish, xalqaro standartlarga muvofiq axborot xavfsizligini tashkil etish hamda foydalanuvchilarning raqamli savodxonligini oshirishni talab etadi [6; 11].

So‘nggi yillarda sun’iy intellekt, mashinaviy o‘qitish, katta ma’lumotlar (Big Data) va bulutli texnologiyalarning rivojlanishi kiberxavfsizlikni ta’minlashning yangi imkoniyatlarini

yaratmoqda. Sun’iy intellekt asosidagi tizimlar kiberhujumlarni real vaqt rejimida aniqlash, xavflarni prognoz qilish va himoya choralarini avtomatlashtirish imkonini bermoqda [3; 4]. Shu bilan birga, ushbu texnologiyalardan kiberjinoyatchilar tomonidan foydalanish ehtimoli yangi tahdidlarni yuzaga keltirmoqda [5].

O‘zbekistondahamraqamliiqtisodiyotnirivojlantirish,elektronhukumattizimlarinikengaytirish va davlat xizmatlarini raqamlashtirish jarayonlari kiberxavfsizlikni ta’minlash masalasiga alohida e’tibor qaratishni taqozo etmoqda [15]. Mamlakatda milliy axborot infratuzilmasini himoya qilish, kiberxavfsizlik bo‘yicha malakali kadrlarni tayyorlash va zamonaviy himoya vositalarini joriy etish bo‘yicha qator islohotlar amalga oshirilmoqda [14; 16].

Mazkur tadqiqotning maqsadi raqamli transformatsiya sharoitida kiberxavfsizlikni ta’minlashning nazariy va amaliy jihatlarini tahlil qilish, zamonaviy kiberxavf va tahdidlarning xususiyatlarini o‘rganish hamda axborot resurslarini himoya qilishning samarali usullarini aniqlashdan iborat.

Tadqiqotning obyekti sifatida zamonaviy axborot tizimlari va ularning kiberxavfsizlik infratuzilmasi tanlandi.

Tadqiqotning predmeti kiberxavfsizlikni ta’minlashning texnologik, tashkiliy va huquqiy mexanizmlari hisoblanadi (1-rasm).

Tadqiqotning ilmiy yangiligi kiberxavfsizlikni ta’minlashda sun’iy intellekt va mashinaviy o‘qitish texnologiyalarining imkoniyatlarini kompleks tahlil qilish, xalqaro tajriba va milliy yondashuvlarni qiyosiy o‘rganish hamda axborot resurslarini himoya qilishning integratsiyalashgan modelini taklif etish bilan izohlanadi.

Tadqiqot natijalarining amaliy ahamiyati shundan iboratki, ishlab chiqilgan tavsiyalar davlat tashkilotlari, ta’lim muassasalari va xo‘jalik yurituvchi subyektlarda kiberxavfsizlikni ta’minlash tizimlarini takomillashtirishda foydalanilishi mumkin.

Tadqiqot metodologiyasi. Mazkur tadqiqotda kiberxavfsizlikni ta’minlashning zamonaviy yondashuvlarini kompleks o‘rganish maqsadida sifat va miqdoriy tahlil elementlarini o‘zida mujassamlashtirgan aralash metodologik yondashuvdan foydalanildi. Tadqiqotning metodologik asosini tizimli yondashuv, risklarga asoslangan yondashuv hamda qiyosiy tahlil usullari tashkil etdi.

Tadqiqotning nazariy bazasi sifatida kiberxavfsizlik, axborot xavfsizligi, sun’iy intellekt va raqamli transformatsiya sohalariga oid xorijiy, rus va mahalliy olimlarning ilmiy ishlari, xalqaro standartlar hamda me’yoriy-huquqiy hujjatlar tahlil qilindi [3; 6; 11]. Tadqiqot jarayonida Scopus bazasida indekslangan ilmiy maqolalar, monografiyalar, xalqaro tashkilotlarning tavsiyalari va amaliy hisobotlardan foydalanildi (2-rasm).

Tadqiqot quyidagi bosqichlarda amalga oshirildi:

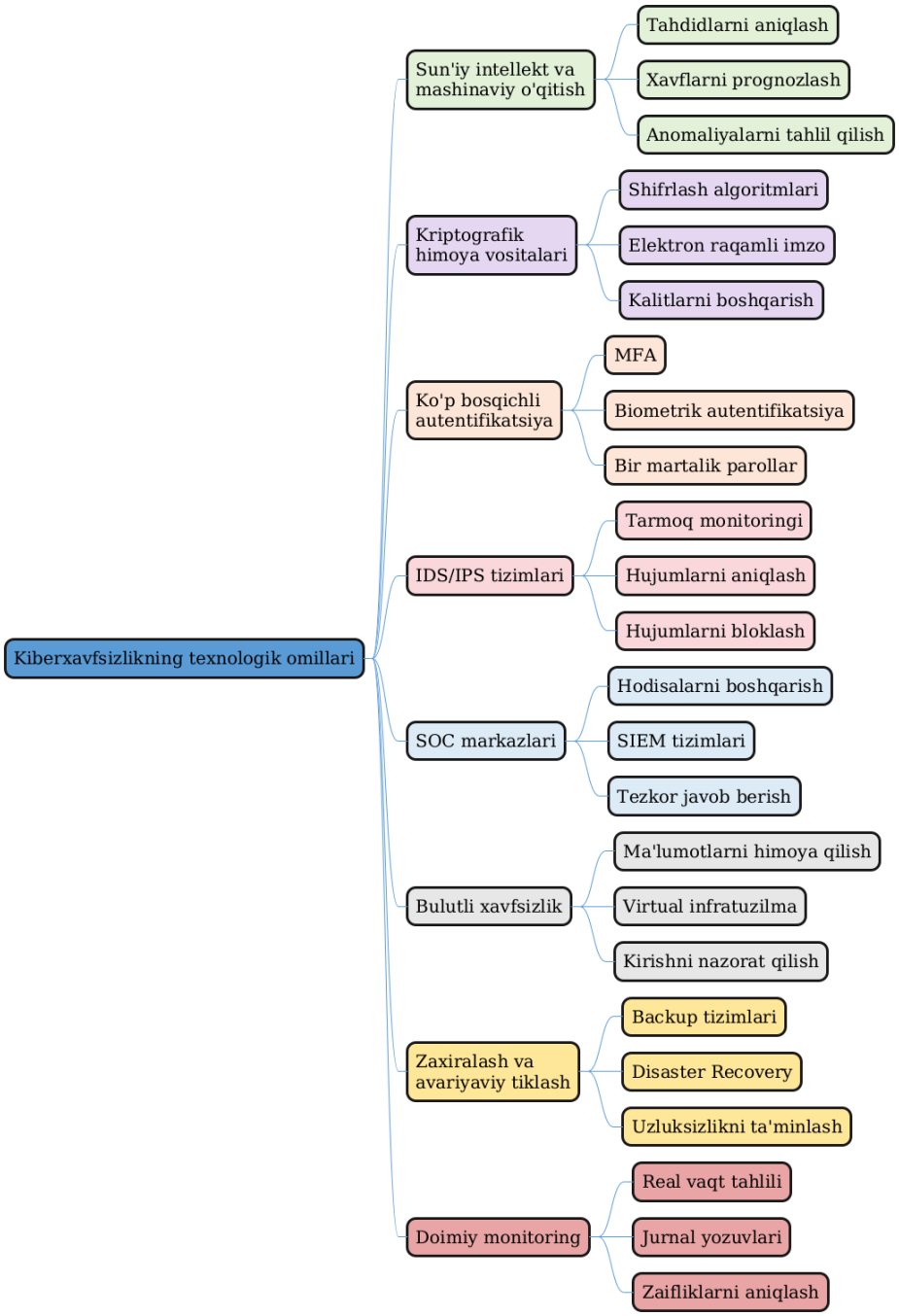
Birinchi bosqich – ilmiy adabiyotlarni tanlash va saralash. Mazkur bosqichda kiberxavfsizlik sohasiga oid ilmiy manbalar kontent-tahlil asosida o‘rganildi. Adabiyotlarni tanlashda ularning ilmiy yangiligi, dolzarbligi, nashr etilgan yili, indeksatsiya darajasi hamda tadqiqot mavzusiga mosligi asosiy mezon sifatida belgilandi. Xususan, 2019–2025-yillarda chop etilgan va Scopus bazasida indekslangan ilmiy maqolalarga ustuvorlik berildi [2; 4; 5].

Ikkinchi bosqich – nazariy va qiyosiy tahlil. Turli mamlakatlarda kiberxavfsizlikni ta’minlash bo‘yicha qo‘llanilayotgan yondashuvlar, texnologiyalar va strategiyalar o‘zaro taqqoslandi. Kiberhujumlarning turlari, ularning amalga oshirish mexanizmlari hamda oqibatlari tizimli ravishda tahlil qilindi [1; 7]. Shuningdek, sun’iy intellekt asosidagi himoya vositalarining samaradorligi an’anaviy kiberxavfsizlik tizimlari bilan qiyoslandi [3; 4].

Uchinchi bosqich – xalqaro standartlar va me’yoriy hujjatlarni tahlil qilish. Axborot xavfsizligini

boshqarish tizimlariga oid xalqaro standartlar, jumladan, ISO/IEC 27001, NIST Cybersecurity Framework va boshqa me’yoriy hujjatlar o‘rganildi. Mazkur standartlarning asosiy talablari va amaliy qo‘llash mexanizmlari tahlil qilinib, ularni milliy axborot tizimlariga integratsiya qilish imkoniyatlari baholandi [11; 12].

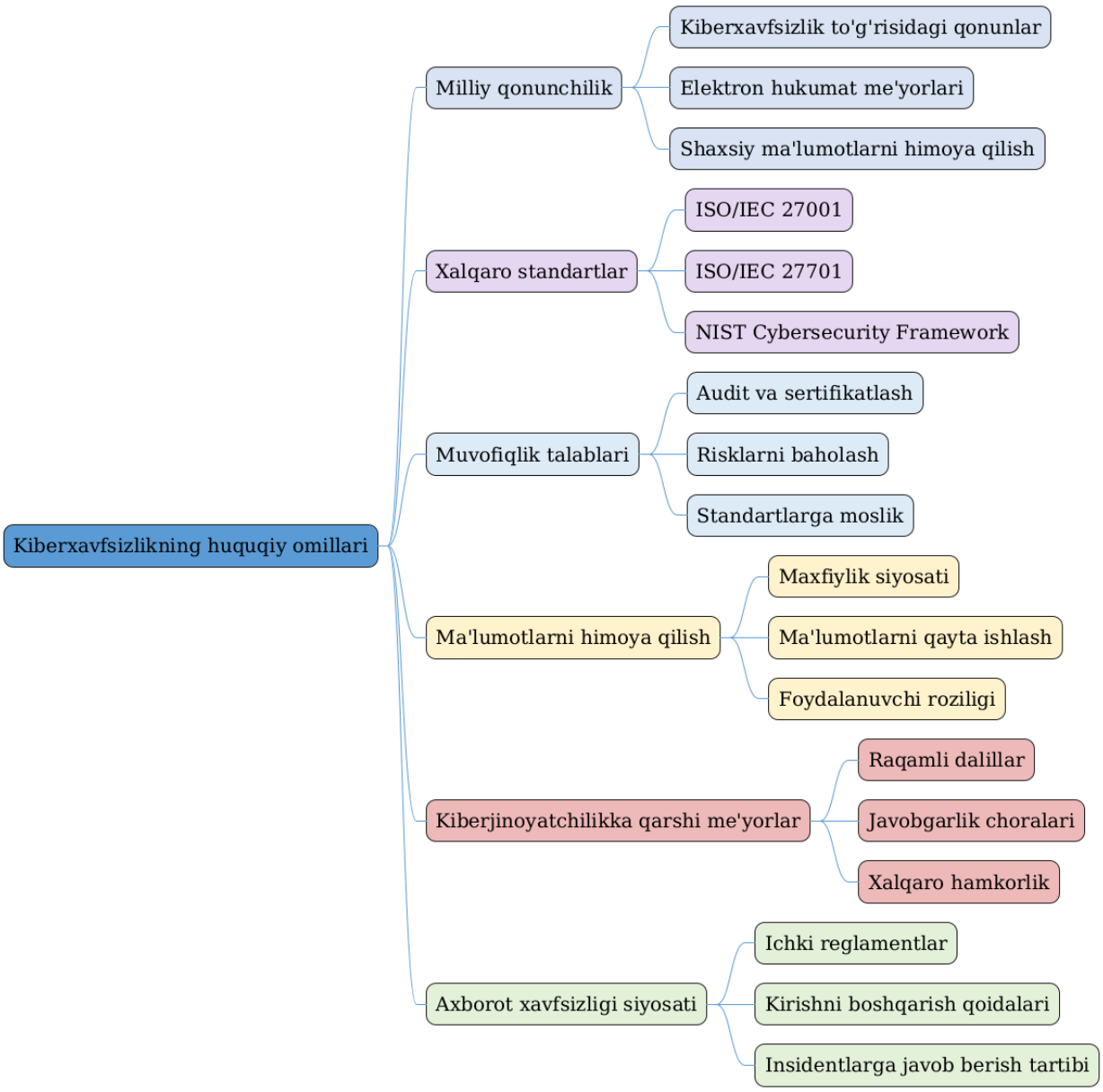
To‘rtinchi bosqich – xavflarni baholash va tasniflash. Tadqiqot davomida kiberxavflarni aniqlash va baholashning risklarga asoslangan yondashuvi qo‘llanildi. Kiberxavflar ehtimollik darajasi, ta’sir ko‘lami va yuzaga kelish chastotasiga ko‘ra guruhlarga ajratildi. Tahdidlarni baholashda maxfiylik, yaxlitlik va mavjudlik tamoyillariga asoslangan CIA modeli mezon sifatida qabul qilindi [9].



1-rasm. Kiberxavfsizlikning texnologik omillari modeli.

Beshinchi bosqich – natijalarni umumlashtirish va tavsiyalar ishlab chiqish. Olingan natijalar tizimlashtirildi hamda kiberxavfsizlikni takomillashtirishga qaratilgan amaliy tavsiyalar ishlab chiqildi. Tavsiyalarni ishlab chiqishda texnik, tashkiliy va ta’limiy omillarning o‘zaro bog‘liqligi inobatga olindi [14; 16].

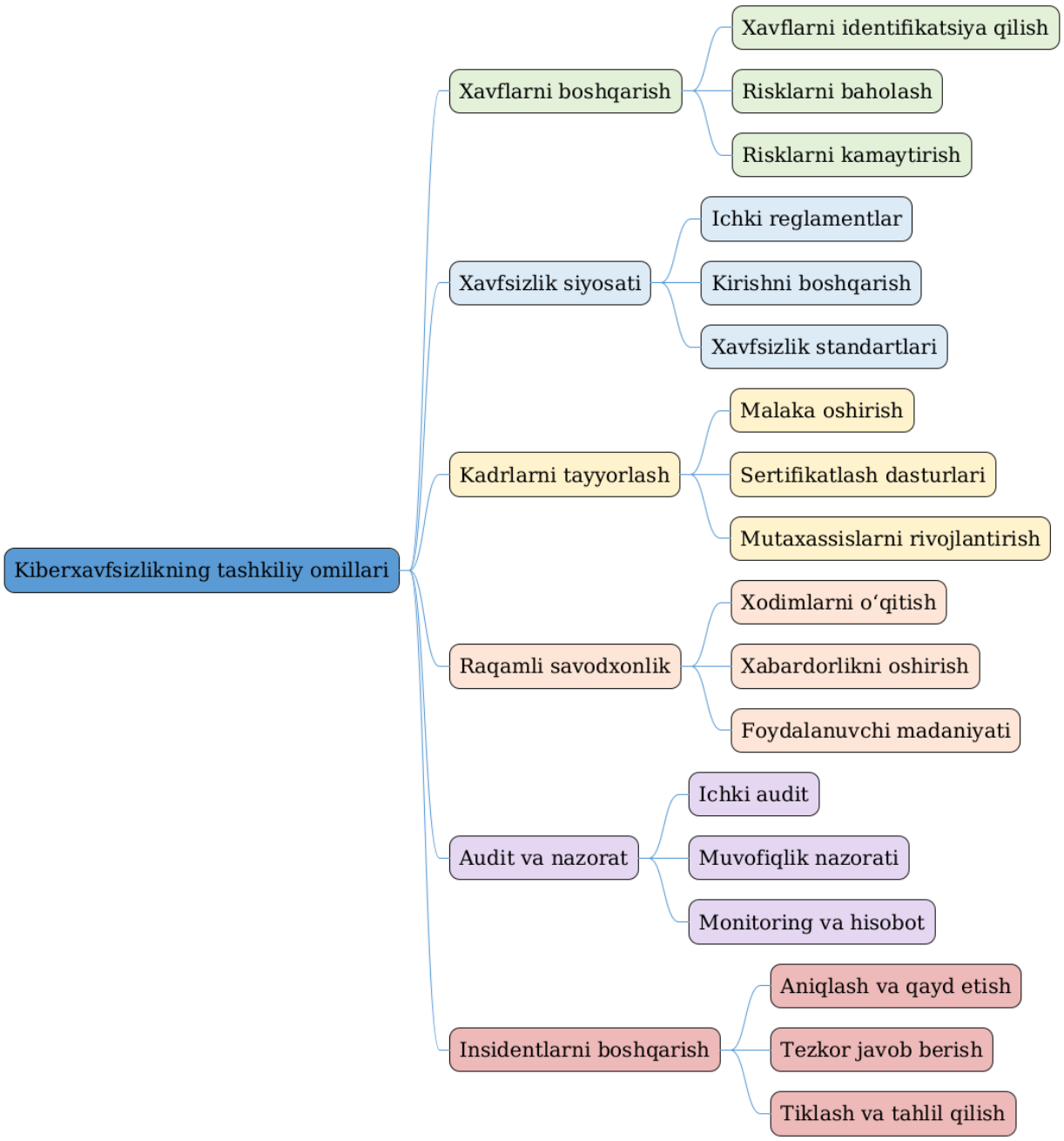
Tadqiqotning ilmiy ishonchliligini ta’minlash maqsadida ma’lumotlarni triangulyatsiya qilish usulidan foydalanildi. Bunda turli manbalardan olingan nazariy va amaliy ma’lumotlar o‘zaro solishtirildi hamda natijalarning izchilligi tekshirildi. Tadqiqotning metodologik cheklovlari sifatida kiberxavfsizlik sohasining yuqori dinamik xususiyatga egaligi, yangi tahdidlarning doimiy ravishda paydo bo‘lishi va ayrim kiberhodisalar bo‘yicha ochiq ma’lumotlarning cheklanganligini qayd etish mumkin. Shunga qaramay, tanlangan metodologik yondashuv kiberxavfsizlikni ta’minlashning zamonaviy tendensiyalarini chuqur tahlil qilish hamda amaliy tavsiyalar ishlab chiqish imkonini berdi.



2-rasm. Kiberxavfsizlikning huquqiy omillari modeli.

Adabiyotlar tahlili. Kiberxavfsizlik zamonaviy axborot jamiyatining barqaror rivojlanishini

ta’minlovchi strategik yo‘nalishlardan biri hisoblanadi. Raqamli transformatsiya jarayonlarining jadallashuvi, bulutli texnologiyalar, buyumlar interneti (Internet of Things – IoT), sun’iy intellekt va katta ma’lumotlar (Big Data) texnologiyalarining keng joriy etilishi axborot infratuzilmasiga bo‘lgan talabni oshirish bilan bir qatorda yangi turdagi kiberxavf va tahdidlarning yuzaga kelishiga sabab bo‘lmoqda [7]. So‘nggi yillarda kiberxavfsizlik bo‘yicha olib borilgan tadqiqotlar asosan kiberhujumlarni aniqlash, axborot tizimlarining zaifliklarini baholash, xavflarni boshqarish, sun’iy intellekt asosidagi himoya vositalarini ishlab chiqish va foydalanuvchilarning axborot xavfsizligi madaniyatini shakllantirish masalalariga qaratilgan [6].



3-rasm. Kiberxavfsizlikning tashkiliy omillari modeli.

Xorijiy tadqiqotchilar tomonidan kiberxavfsizlikning nazariy va amaliy jihatlari keng o‘rganilgan. Bada va Nurse [1] kiberhujumlarning ijtimoiy-psixologik oqibatlarini tahlil qilib,

inson omili aksariyat kiberhodisalarning asosiy sababi ekanligini ta’kidlaydilar. Mualliflarning fikriga ko‘ra, texnik himoya vositalarining rivojlanishiga qaramasdan, foydalanuvchilarning xabardorlik darajasi va xavfsizlik madaniyati yetarli darajada shakllanmaganligi kiberxavflarning muvaffaqiyatli amalga oshirilishiga zamin yaratmoqda [1].

Kiberhujumlarning murakkab va uzoq muddatli shakllaridan biri bo‘lgan ilg‘or doimiy tahdidlar (Advanced Persistent Threats – APT) Alshamrani, Myneni, Chowdhary va Huang [2] tomonidan tizimli ravishda o‘rganilgan. Mualliflar APT hujumlarining razvedka, kirib borish, ichki tarmoqda tarqalish va ma’lumotlarni noqonuniy olib chiqish bosqichlarini tavsiflaganlar. Tadqiqot natijalari an’anaviy himoya vositalari mazkur turdagi hujumlarni aniqlashda cheklangan imkoniyatlarga ega ekanligini ko‘rsatadi [2].

Kiberxavfsizlikni ta’minlashda sun’iy intellekt va mashinaviy o‘qitish texnologiyalarining qo‘llanilishi alohida ilmiy yo‘nalish sifatida shakllanmoqda. Sarker, Furhad va Nowrozy [3] sun’iy intellekt asosidagi kiberxavfsizlik tizimlarini tahlil qilib, ularning anomaliyalarni aniqlash, xavflarni prognoz qilish va avtomatlashtirilgan qarorlar qabul qilishdagi afzalliklarini asoslab berganlar. Biroq, mualliflar sun’iy intellekt modellarining ma’lumotlar sifati va hajmiga yuqori darajada bog‘liqligi hamda noto‘g‘ri ijobiy natijalar (false positives) muammosi mavjudligini qayd etadilar. Li va hammualliflar [4] chuqur o‘rganish algoritmlariga asoslangan hujumlarni aniqlash tizimlarini tahlil qilib, konvolyutsion neyron tarmoqlar (CNN), rekurrent neyron tarmoqlar (RNN) va uzoq qisqa muddatli xotira (LSTM) modellarining tarmoq trafigidagi g‘ayritabiiy faoliyatni aniqlashda yuqori samaradorlikka ega ekanligini aniqlaganlar. Shu bilan birga, mazkur modellarni real sharoitlarda qo‘llash uchun katta hajmdagi belgilangan ma’lumotlar to‘plamlariga ehtiyoj mavjudligi ta’kidlangan [4]. Le, Nguyen va Tran [5] korporativ muhitda kiberxavfsizlik analitikasining rivojlanish tendensiyalarini o‘rganib, tahdidlarni aniqlash va ularga javob qaytarishda katta ma’lumotlar, bulutli hisoblash texnologiyalari va xavfsizlik operatsion markazlari (Security Operations Center – SOC)ning muhim rolini asoslab berganlar. Tadqiqot natijalari kiberxavfsizlikni ta’minlashda ma’lumotlarga asoslangan yondashuvlarning samaradorligini ko‘rsatadi [5]. Katsikeas, Johnson, Ekstedt va Lagerström [6] kiberxavfsizlik sohasidagi ilmiy tadqiqotlarning evolyutsiyasini tahlil qilib, zamonaviy tadqiqotlarning asosiy yo‘nalishlari sifatida kriptografiya, tarmoq xavfsizligi, xavflarni boshqarish, sun’iy intellekt va raqamli forensikani ajratib ko‘rsatganlar. Mualliflar mazkur yo‘nalishlarning integratsiyasi kiberxavfsizlikning yangi paradigmasini shakllantirayotganini ta’kidlaydilar. Xu [7] tomonidan ishlab chiqilgan kiberxavfsizlik dinamikasi konsepsiyasi kiberxavfsizlikni doimiy ravishda o‘zgarib turuvchi murakkab tizim sifatida talqin etadi. Muallifning fikriga ko‘ra, kiberxavf va tahdidlarning evolyutsion tabiati himoya vositalarining adaptiv va proaktiv xususiyatga ega bo‘lishini talab qiladi [7].

Rus olimlari tomonidan axborot xavfsizligini ta’minlashning metodologik va amaliy jihatlari chuqur tadqiq etilgan. Kasperskiy [8] zararli dasturlar evolyutsiyasi va ularning tarqalish mexanizmlarini tahlil qilib, zamonaviy zararli dasturlar tobora murakkablashib borayotganini hamda ularni aniqlash uchun ko‘p qatlamli himoya tizimlarini joriy etish zarurligini ta’kidlaydi. A.A. Malyuk, S.V. Pazizin, N.S. Pogojin [9] avtomatlashtirilgan axborot tizimlarida axborotni himoya qilishning tashkiliy va texnik mexanizmlarini o‘rganib, xavflarni boshqarishning kompleks modelini taklif etganlar. Ushbu model tahdidlarni aniqlash, zaifliklarni baholash va himoya choralarini ishlab chiqish bosqichlarini qamrab oladi. Domarev [10] axborot xavfsizligini tizimli yondashuv asosida o‘rganib, texnik, tashkiliy va inson omillarining o‘zaro bog‘liqligini asoslab bergan. Muallifning fikricha, kiberxavfsizlikni ta’minlashda faqat texnik vositalardan foydalanish yetarli emas, balki xavfsizlik siyosatini shakllantirish va xodimlarni muntazam tayyorlash ham muhim ahamiyatga ega. Shangin [11] kompyuter tarmoqlari xavfsizligini ta’minlashning nazariy

asoslarini tahlil qilib, xavfsizlik siyosati, kirishni boshqarish va kriptografik himoya vositalarining samaradorligini asoslab bergan. Tsirlov [12] esa axborot xavfsizligining fundamental tamoyillari – maxfiylik, yaxlitlik va mavjudlik konsepsiyalarini keng yoritib, ularning zamonaviy axborot tizimlaridagi ahamiyatini ko‘rsatgan (3-rasm).

O‘zbekistonlik olimlarning ilmiy ishlarida milliy axborot infratuzilmasini himoya qilish, raqamli iqtisodiyot sharoitida kiberxavfsizlikni ta’minlash hamda soha uchun malakali kadrlar tayyorlash masalalari ustuvor yo‘nalish sifatida qaralmoqda.

Aripov va Maraximov [13] axborot xavfsizligining nazariy asoslari, kriptografik himoya usullari va zamonaviy axborot tizimlarini himoyalash texnologiyalarini tahlil qilganlar. Yuldashev va Raxmonov [14] milliy axborot tizimlarida yuzaga kelayotgan kiberxavflarni aniqlash va ularni bartaraf etish mexanizmlarini o‘rganganlar. Abduqodirov va Xaitov [15] raqamli iqtisodiyot sharoitida axborot xavfsizligini ta’minlashning tashkiliy-huquqiy jihatlarini tahlil qilib, milliy kiberxavfsizlik siyosatini takomillashtirish bo‘yicha tavsiyalar ishlab chiqqanlar. Maraximov va Tojiboyev [16] O‘zbekistonda kiberxavfsizlikni rivojlantirishning ustuvor yo‘nalishlarini belgilab, kiberxavfsizlik infratuzilmasini modernizatsiya qilish, malakali mutaxassislarni tayyorlash va xalqaro hamkorlikni kengaytirish zarurligini asoslab berganlar.

Tahlil qilingan ilmiy manbalar shuni ko‘rsatadiki, kiberxavfsizlik bo‘yicha mavjud tadqiqotlarning aksariyati alohida texnologik yechimlar, tahdidlarni aniqlash usullari yoki tashkiliy mexanizmlarni o‘rganishga qaratilgan. Biroq, raqamli transformatsiya sharoitida sun’iy intellekt asosidagi himoya vositalari, inson omili, xalqaro standartlar va milliy xavfsizlik talablarini yagona integratsiyalashgan tizim doirasida kompleks tahlil qilish masalalari yetarli darajada o‘rganilmagan.

Mazkur tadqiqotning o‘ziga xosligi shundaki, unda kiberxavfsizlikni ta’minlashning texnologik, tashkiliy va ijtimoiy omillari o‘zaro bog‘liqlikda tahlil qilinadi hamda xalqaro tajriba va milliy yondashuvlar asosida axborot resurslarini himoya qilishning kompleks modeli taklif etiladi.

Natija va muhokamalar. Kiberxavfsizlikni ta’minlashda texnologik, tashkiliy va huquqiy omillarning nisbiy ahamiyatini aniqlash maqsadida AHP, FMEA va risk-matritsa usullaridan kompleks foydalanildi. Kiberxavflar ehtimollik darajasi (P) va ta’sir ko‘lami (I) bo‘yicha 5 balli shkala asosida baholandi. Umumiy risk darajasi quyidagi formula yordamida aniqlandi:

$$R = P \times I \quad (1)$$

Risk darajalari quyidagicha tasniflandi:

- 1–5 ball – past risk;
- 6–10 ball – o‘rta risk;
- 11–15 ball – yuqori risk;
- 16–25 ball – kritik risk.

1-jadval

Kiberxavf omili	Ehtimollik (P)	Ta’sir (I)	Risk balli (R)	Ustuvorlik
Fishing hujumlari	5	4	20	Kritik
Inson omili	4	5	20	Kritik
Zararli dasturlar	4	4	16	Kritik
DDoS hujumlari	3	5	15	Yuqori
Ichki tahdidlar	3	5	15	Yuqori
APT hujumlari	2	5	10	O‘rta
Bulutli xizmatlar zaifligi	3	3	9	O‘rta
Huquqiy nomuvofiqlik	2	4	8	O‘rta

Risk-matritsa natijalari shuni ko‘rsatdiki, inson omili va fishing hujumlari eng yuqori ustuvorlikka ega bo‘lib, ularga qarshi profilaktik choralarni kuchaytirish zarur. Kiberxavf omillarining ustuvorligini aniqlash uchun FMEA usulidan foydalanildi. Bunda har bir xavf uchta mezon bo‘yicha baholandi:

- S (Severity) – oqibatning jiddiyligi;
- (Occurrence) – yuzaga kelish ehtimoli;
- D (Detection) – aniqlash qiyinligi.

Risk ustuvorlik soni (RPN) quyidagi formula orqali hisoblandi:

$$RPN = S \times O \times D \quad (2)$$

2-jadval

Kiberxavf omili	S	O	D	RPN	Ustuvorlik
Inson omili	9	8	7	504	1
Fishing hujumlari	8	9	6	432	2
Zararli dasturlar	8	7	6	336	3
DDoS hujumlari	9	5	6	270	4
Ichki tahdidlar	8	5	6	240	5
APT hujumlari	10	3	7	210	6
Huquqiy nomuvofiqlik	7	4	5	140	7

FMEA natijalari inson omili kiberxavfsizlikka eng katta tahdid ekanligini ko‘rsatdi. Mazkur omil bo‘yicha xodimlarni muntazam o‘qitish va raqamli savodxonlikni oshirish muhim ahamiyat kasb etadi. Kiberxavfsizlikni ta’minlashga ta’sir etuvchi asosiy omillar uchta guruhga ajratildi:

- texnologik omillar;
- tashkiliy omillar;
- huquqiy omillar.

Ekspert baholash asosida Saatining 1–9 shkalasi yordamida juft taqqoslash matritsasi shakllantirildi.

3-jadval

Omillar	Texnologik	Tashkiliy	Huquqiy
Texnologik	1	2	4
Tashkiliy	1/2	1	3
Huquqiy	1/4	1/3	1

Hisoblash natijasida quyidagi ustuvorlik koeffitsiyentlari olindi:

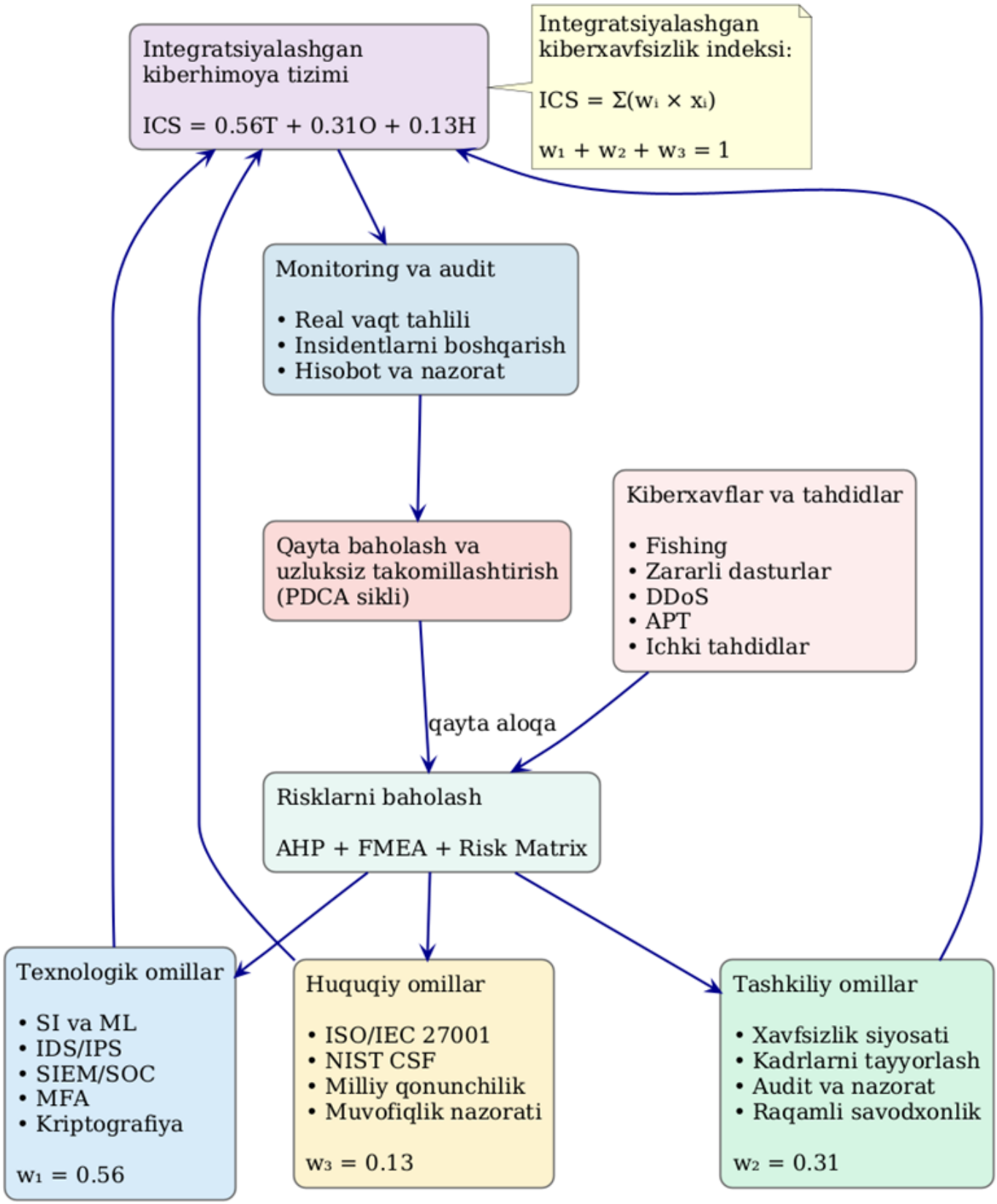
- texnologik omillar – 0,56;
- tashkiliy omillar – 0,31;
- huquqiy omillar – 0,13.

Konsistentlik koeffitsiyenti (CR) 0,1 dan kichik bo‘lib, ekspert baholarining mosligi tasdiqlandi. AHP natijalari kiberxavfsizlikni ta’minlashda texnologik omillar yetakchi ahamiyatga ega ekanligini ko‘rsatdi. Shu bilan birga, tashkiliy va huquqiy omillarni e’tibordan chetda qoldirish kiberhimoya tizimining umumiy samaradorligini pasaytirishi mumkin. Kompleks baholash natijalariga ko‘ra, kiberxavfsizlikni ta’minlashda texnologik yechimlarni joriy etish bilan bir qatorda xodimlarning raqamli savodxonligini oshirish, xavfsizlik siyosatini takomillashtirish va amaldagi me’yoriy-huquqiy bazani mustahkamlash ustuvor yo‘nalishlar sifatida belgilandi.

Kiberxavfsizlikni ta’minlashning integratsiyalashgan modeli texnologik, tashkiliy va huquqiy omillarning o‘zaro bog‘liqligiga asoslanadi. Modelda omillarning nisbiy ahamiyati Analitik ierarxiya jarayoni (AHP) usuli yordamida aniqlanib, mos ravishda 0,56; 0,31 va 0,13 koeffitsiyentlar olindi. Integratsiyalashgan kiberxavfsizlik indeksi (ICS) omillarning vaznli yig‘indisi sifatida hisoblandi:

$$ICS=0.56T+0.31O+0.13H \quad (3)$$

Mazkur model tashkilotlarda kiberxavfsizlik holatini kompleks baholash, ustuvor yo‘nalishlarni aniqlash hamda resurslarni samarali taqsimlash imkonini beradi (4-rasm).



4-rasm. Kiberxavfsizlikni ta’minlashning integratsiyalashgan modeli.

Xulosa. Raqamli transformatsiya jarayonlarining jadallashuvi axborot tizimlari va raqamli infratuzilmalarning kiberxavfsizligini ta’minlash masalasini strategik ahamiyatga ega yo‘nalishga aylantirmoqda. Tadqiqot natijalari shuni ko‘rsatdiki, zamonaviy kiberxavf va tahdidlar, jumladan, fishing hujumlari, zararli dasturlar, DDoS hujumlari hamda ilg‘or doimiy tahdidlar (APT) axborot

resurslarining maxfiyligi, yaxlitligi va mavjudligiga jiddiy xavf tug‘dirmoqda.

Tahlillar kiberxavfsizlikni samarali ta’minlash faqat texnik himoya vositalarini joriy etish bilan cheklanmasligini, balki tashkiliy, huquqiy va ta’limiy choralarni o‘zaro uyg‘un holda qo‘llash zarurligini tasdiqladi. Sun’iy intellekt va mashinaviy o‘qitish texnologiyalari kiberhujumlarni erta aniqlash, xavflarni prognoz qilish va himoya jarayonlarini avtomatlashtirishda yuqori samaradorlikka ega ekanligi aniqlandi. Shu bilan birga, ushbu texnologiyalarni amaliyotga joriy etishda ma’lumotlar sifati, algoritmlarning ishonchliligi hamda noto‘g‘ri ijobiy natijalar xavfi kabi omillarni hisobga olish lozim.

Tadqiqot davomida xalqaro standartlar, jumladan, ISO/IEC 27001 va NIST Cybersecurity Framework talablarini milliy axborot tizimlariga integratsiya qilish kiberxavfsizlikni mustahkamlashning muhim omili ekanligi asoslandi. Shuningdek, foydalanuvchilarning raqamli savodxonligini oshirish, xavfsizlik madaniyatini shakllantirish va malakali kadrlar tayyorlash kiberxavfsizlikni ta’minlashning ustuvor yo‘nalishlari sifatida belgilandi.

Taklif etilgan integratsiyalashgan yondashuv texnologik, tashkiliy va ijtimoiy omillarning o‘zaro bog‘liqligini hisobga olgan holda axborot resurslarini himoya qilish samaradorligini oshirish imkonini beradi. Mazkur tadqiqot natijalaridan davlat tashkilotlari, ta’lim muassasalari va xo‘jalik yurituvchi subyektlarda kiberxavfsizlik tizimlarini takomillashtirishda foydalanish mumkin. Kelgusidagi tadqiqotlarda sun’iy intellekt asosidagi kiberxavfsizlik tizimlarining samaradorligini real sharoitlarda baholash, yangi avlod kiberxavflarini prognozlash va adaptiv himoya mexanizmlarini ishlab chiqishga alohida e’tibor qaratish maqsadga muvofiqdir.

Foydalanilgan adabiyotlar.

1. Bada, M., Nurse, J.R.C. The social and psychological impact of cyber-attacks // Emerging Cyber Threats and Cognitive Vulnerabilities. – London : Academic Press, 2020. – P. 73–92. – DOI: 10.1016/B978-0-12-816203-3.00004-6.

2. Alshamrani, A., Myneni, S., Chowdhary, A., Huang, D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities // IEEE Communications Surveys & Tutorials. – 2019. – Vol. 21, No. 2. – P. 1851–1877. – DOI: 10.1109/COMST.2019.2891891.

3. Sarker, I.H., Furhad, M.H., Nowrozy, R. AI-driven cybersecurity: An overview, security intelligence modeling and research directions // SN Computer Science. – 2021. – Vol. 2, No. 3. – Art. 173. – DOI: 10.1007/s42979-021-00557-0.

4. Li, J., Liu, H., Luo, X., et al. Deep learning-based intrusion detection systems: A systematic review and future trends // Computer Networks. – 2022. – Vol. 213. – Art. 109134. – DOI: 10.1016/j.comnet.2022.109134.

5. Le, T.D., Nguyen, H.T., Tran, D.T. Cybersecurity analytics for the enterprise environment: A systematic literature review // Electronics. – 2025. – Vol. 14, No. 11. – Art. 2252. – DOI: 10.3390/electronics14112252.

6. Katsikeas, S., Johnson, P., Ekstedt, M., Lagerström, R. Research communities in cyber security: A comprehensive literature review // Computers & Security. – 2022. – Vol. 121. – Art. 102840. – DOI: 10.1016/j.cose.2022.102840.

7. Xu, S. Cybersecurity dynamics: A foundation for the science of cybersecurity // The Science of Cybersecurity. – Cham : Springer, 2021. – P. 1–31. – DOI: 10.1007/978-3-030-78506-6_1.

8. Касперский, Е.В. Компьютерное зловредство в вопросах и ответах. – Москва : Альпина Паблишер, 2021. – 312 с.

9. Малюк, А.А., Пазизин, С.В., Погожин, Н.С. Введение в защиту информации в автоматизированных системах. – Москва : Горячая линия – Телеком, 2020. – 376 с.

10. Домарев, В.В. Безопасность информационных технологий. Системный подход. – Киев : ДиаСофт, 2019. – 992 с.
11. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей. – Москва : ФОРУМ, 2022. – 416 с.
12. Цирлов, В.Л. Основы информационной безопасности автоматизированных систем. – Москва : Феникс, 2021. – 448 с.
13. Aripov, M.M., Maraximov, A.R. Axborot xavfsizligi asoslari. – Toshkent : Cho‘lpon, 2021. – 320 b.
14. Yuldashev, B.S., Raxmonov, A.A. Kiberxavfsizlik tahdidlarini aniqlash va ularni bartaraf etish usullari // Muhammad al-Xorazmiy avlodlari. – 2023. – № 2. – B. 85–92.
15. Abduqodirov, A.A., Xaitov, O.X. Raqamli iqtisodiyot sharoitida axborot xavfsizligini ta’minlashning dolzarb masalalari // Axborot-kommunikatsiya texnologiyalari va telekommunikatsiyalarning zamonaviy muammolari : ilmiy-amaliy konferensiya materiallari. – Toshkent, 2022. – B. 114–119.
16. Maraximov, A.R., Tojiboyev, J.A. O‘zbekistonda kiberxavfsizlikni rivojlantirishning ustuvor yo‘nalishlari // TATU xabarlari. – 2024. – № 1. – B. 56–64.