O‘ZBEKISTON RESPUBLIKASI
JAMOAT XAVFSIZLIGI
UNIVERSITETI

ZAMONAVIY TELEKAMUNIKATSIYA MUAMMOLARI VA INNOVATSION YECHIMLAR: XALQARO TAJRIBA, NAZARIYA VA AMALIYOT

xalqaro ilmiy-amaliy anjuman
MATERIALLARI TO’PLAMI
2026-yil 29-aprel

I QISM



O‘ZBEKISTON RESPUBLIKASI
JAMOAT XAVFSIZLIGI UNIVERSITETI

ZAMONAVIY TELEKOMMUNIKATSIYA MUAMMOLARI VA INNOVATSION YECHIMLARI: XALQARO TAJRIBA, NAZARIYA VA AMALIYOT

xalqaro ilmiy-amaliy anjumani
MATERIALLAR TO‘PLAMI

2026-yil 29-aprel

I QISM

TOSHKENT – 2026

KBK - 16
Z - 26

“Zamonaviy telekommunikatsiya muammolari va innovatsion yechimlari: xalqaro tajriba, nazariya va amaliyot” mavzusida xalqaro ilmiy-amaliy anjumani materiallari. Toshkent, O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti, 2026.- 439 bet.

Mazkur to‘plamda xorijiy oliy ta’lim muassasasi, Respublikamiz yetakchi oliy-harbiy ta’lim muassasalari professor-o‘qituvchilari, O‘zbekiston Respublikasi Milliy gvardiyasi sohaviy xizmatlari hamda sohaviy mutaxassislar bilan hamkorlikda “Zamonaviy telekommunikatsiya muammolari va innovatsion yechimlari: xalqaro tajriba, nazariya va amaliyot” mavzusida o‘tkazilgan xalqaro ilmiy-amaliy anjumanida Telekommunikatsiya sohasida va obyektlarni qo‘riqlanishini ta’minlashda yuzaga kelayotgan ayrim muammolarni aniqlab, ularning innovatsion yechimlarini topish, ushbu axborot kommunikatsiya texnologiyalari sohadagi ma’lumotlar bilan tanishish hamda yetakchi tashkilot va muassasalar mutaxassislari bilan o‘zaro tajriba almashish maqsadida tayyorlangan ma’ruzalari keltirilgan.

Ushbu to‘plam xorijiy hamda Respublikamiz oliy harbiy ta’lim muassasalari hamda soha bo‘yicha oliy ta’lim muassasalari professor-o‘qituvchilari, kursant va tinglovchilari, shuningdek Qurolli Kuchlar harbiy xizmatchilari uchun mo‘ljallangan.

Mualliflarning nuqtayi nazarlariga putur yetkazmaslik maqsadida to‘plamga kiritilgan materiallar faqatgina texnik jihatdan tahrir qilingan, shuning uchun tahrir hay’ati matnlarda uchraydigan ba’zi bir noaniqliklar uchun javobgarlik mualliflarga yuklanadi. Mualliflar o‘z maqola va tezislarida berilgan ma’lumotlar uchun shaxsan javobgar ekanliklari haqida ogohlantiradi.

Tahrir hay’ati a’zolari:

Tashmanov Ye.B.	texnik fanlar doktori, professor, podpolkovnik
Saidbayev B.Dj.	texnik fanlar bo‘yicha falsafa doktori (PhD), podpolkovnik
Yusupov U.A.	kafedra katta o‘qituvchisi, kapitan
Nigmatov Z.Z.	O‘z.Res HXvaMUning Quruqlikdagi qo‘shinlar institutining, Istiqbolli harbiy texnologiyalar kafedrasi dotsenti., t.f.f.d. (PhD), dotsent.
Xurramov A.I.	O‘z.Resi HXvaMUning Quruqlikdagi qo‘shinlar instituti Ilmiy ishlar va innovatsion faoliyatni tashkil etish bo‘limi katta ilmiy xodimi, t.f.d. (DSc), dotsent, kapitan

© O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti, 2026

mexanizmlari, shuningdek, unga qarshi kurashishda ilmiy yondashuvlar bo‘yicha aniq chora-tadbirlar belgilangan.

Shuningdek, qarorda Kiberjinoyatlarning oldini olish yo‘nalishidagi targ‘ibot-tashviqot tadbirlarida respublika miqyosida har yilning noyabr oyini «Kibermadaniyatni yuksaltirish oyligi» deb e’lon qilish belgilandi.

Xulosa qilib, bu jinoyat va tahdidlarni bartaraf etish uchun qonunlar bilan emas, balki profilaktika, ta’lim, madaniyat va fuqarolarning raqamli savodxonligini oshirish, xavfsizlik standartlarini yaratish, xalqaro hamkorlikni kuchaytirish talab etiladi.

Foydalanilgan adabiyotlar:

1. O‘zbekiston Respublikasi Konstitutsiyasi;
2. O‘zbekiston Respublikasi Jinoyat kodeksi;
3. O‘zbekiston Respublikasi Prezidentining 2025-yil 30-apreldagi “Axborot texnologiyalari yordamida sodir etiladigan jinoyatlarga qarshi kurashish faoliyatini yanada kuchaytirishga qaratilgan chora-tadbirlar to‘g‘risida”gi PQ-153-son qarori;

MDH MAMLAKATLARIDA KIBERXAVFSIZLIKNI HUQUQIY JIHATDAN TA’MINLASHNING ILMIY-NAZARIY ASOSLARI

Abdixamidov G‘.Z.
O‘zbekiston Respublikasi Ichki ishlar vazirligi
Kriminologiya ilmiy-tadqiqot instituti ilmiy xodimi

Annotatsiya. Ushbu tezisda MDH mamlakatlarida kiberxavfsizlikni huquqiy jihatdan ta’minlashning ilmiy-nazariy asoslari, normativ-huquqiy yondashuvlari va institutsional mexanizmlari tahlil qilinadi. Kiberxavfsizlik zamonaviy sharoitda faqat axborot texnologiyalarini himoya qilish vositasi emas, balki davlat suvereniteti, konstitutsiyaviy tartib, kritik infratuzilma barqarorligi va fuqarolarning axborot huquqlarini ta’minlovchi kompleks huquqiy institut sifatida baholanadi. Tezisda O‘zbekiston, Rossiya, Qozog‘iston va boshqa MDH davlatlarining kiberxavfsizlikka oid qonunchilik yondashuvlari qiyosiy jihatdan ko‘rib chiqiladi. Xususan, O‘zbekiston Respublikasining “Kiberxavfsizlik to‘g‘risida”gi qonuni, Rossiya Federatsiyasining kritik axborot infratuzilmasi xavfsizligiga oid qonunchiligi hamda Qozog‘istonning axborotlashtirish sohasidagi huquqiy modeli ilmiy tahlil qilinadi.

Kalit so‘zlar: Kiberxavfsizlik; MDH mamlakatlari; axborot xavfsizligi; kiberhuquq; kritik axborot infratuzilmasi; kiberhodisalarga javob berish; huquqiy tartibga solish.

XXI asrda kiberxavfsizlik masalasi davlat boshqaruvi, iqtisodiyot, mudofaa, jamoat xavfsizligi va ijtimoiy barqarorlikni ta’minlashning muhim shartlaridan biriga aylandi. Raqamli transformatsiya davlat xizmatlari, moliya, transport, energetika, sog‘liqni saqlash, ta’lim va huquqni muhofaza qilish tizimlarining axborot-kommunikatsiya infratuzilmalariga bog‘liqligini keskin oshirdi. Shu sababli kiberxavfsizlik endilikda faqat texnik himoya vositalari majmui emas, balki davlat suvereniteti va milliy xavfsizlikni ta’minlovchi mustaqil huquqiy institut sifatida qaralmoqda. Ayniqsa, MDH mamlakatlari uchun mazkur masala umumiy tarixiy-huquqiy makon, transchegaraviy axborot oqimlari va xavfsizlik tahdidlarining o‘xshashligi sababli alohida dolzarblik kasb etadi. Xalqaro elektraloqa ittifoqining 2024-yilgi Global Cybersecurity Index hisobotida kiberxavfsizlik huquqiy, texnik, tashkiliy, salohiyatni rivojlantirish va xalqaro hamkorlik mezonlari asosida baholanishi ushbu sohaning kompleks xususiyatga ega ekanligini ko‘rsatadi [1]. MDH mintaqasidagi ayrim davlatlarning kiberxavfsizlik bo‘yicha institutsional ko‘rsatkichlari yaxshilangani bu yo‘nalishda ijobiy siljishlar mavjudligini tasdiqlaydi [2]. Biroq xalqaro reytinglardagi o‘sish huquqiy mexanizmlar to‘liq va samarali ishlayotganini anglatmaydi. Chunki kiberxavfsizlikdagi asosiy masala faqat normativ hujjat mavjudligida emas, balki uning real tahdidlar, idoralararo muvofiqlashuv va kritik infratuzilma boshqaruvi bilan uyg‘un ishlashidadir.

Kiberxavfsizlik tushunchasi huquqiy nazariya nuqtayi nazaridan axborot tizimlari, raqamli xizmatlar, elektron ma’lumotlar va kommunikatsiya tarmoqlarining xavfsiz ishlashini ta’minlovchi normalar majmui sifatida qaraladi. Biroq mazkur tushuncha zamonaviy sharoitda faqat ma’lumotlarni ruxsatsiz kirishdan himoya qilish bilan cheklanmaydi. U davlatning raqamli suvereniteti, fuqarolarning shaxsiy ma’lumotlari, kritik infratuzilma uzluksizligi va jamiyatning axborot barqarorligi bilan bevosita bog‘liqdir. MDH mamlakatlari huquqiy makonida kiberxavfsizlik ko‘pincha “axborot xavfsizligi”, “kritik axborot infratuzilmasi”, “elektron hukumat xavfsizligi”, “shaxsiy ma’lumotlarni himoya qilish” va

“kiberjinoyatchilikka qarshi kurash” tushunchalari orqali tartibga solinadi. Bu yondashuv ma’lum darajada tarixiy va institutsional asosga ega bo‘lsada, ayrim hollarda kiberxavfsizlikning mustaqil huquqiy institut sifatida shakllanishini sekinlashtiradi. Chunki axborot xavfsizligi ko‘proq axborot mazmuni, kommunikatsiya siyosati va axborot oqimlarini boshqarishga qaratilgan bo‘lsa, kiberxavfsizlik texnik, tashkiliy, huquqiy va operativ himoya mexanizmlarini birlashtiradi. Shu sababli ilmiy-nazariy yondashuvda bu ikki tushunchani mutlaq aynanlashtirish emas, balki ularning kesishuvchi va farqlanuvchi jihatlarini aniq ajratish zarur.

O‘zbekiston Respublikasida kiberxavfsizlikka oid mustaqil qonunchilik bazasining shakllanishi 2022-yil 15-apreldagi “Kiberxavfsizlik to‘g‘risida”gi O‘RQ-764-son Qonun bilan yangi bosqichga ko‘tarildi [3]. Mazkur qonun kiberxavfsizlik sohasidagi munosabatlarni tartibga solish, vakolatli davlat organini belgilash, kiberxavfsizlik obyektlari va subyektlarini aniqlash hamda davlat organlari va tashkilotlarining majburiyatlarini belgilashga xizmat qiladi. Qonunda Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi sifatida belgilanganligi mazkur sohaning milliy xavfsizlik bilan bevosita bog‘liqligini ko‘rsatadi [3]. Huquqiy jihatdan bu yondashuv kiberxavfsizlikni idoraviy texnik masala emas, balki davlat xavfsizligi arxitekturasining tarkibiy qismi sifatida talqin qilish imkonini beradi. Shu bilan birga, qonunning amaliy samaradorligi uning shaxsiy ma’lumotlar, elektron hukumat, telekommunikatsiya, davlat siri, jamoat xavfsizligi va kritik infratuzilma bilan bog‘liq boshqa huquqiy normalar bilan uyg‘un ishlashiga bog‘liq. O‘zbekiston tajribasining ijobiy jihati shundaki, maxsus qonun mavjudligi sohaning institutsional chegaralarini belgilab berdi. Biroq amaliy jihatdan idoralararo axborot almashinuvi, kiberhodisa reporting, majburiy audit va sektorlararo standartlar yanada chuqurlashtirilishi zarur.

Rossiya Federatsiyasi tajribasi MDH makonida kritik axborot infratuzilmasini huquqiy himoya qilishning nisbatan rivojlangan modelini namoyon etadi. 2017-yil 26-iyuldagi 187-FZ-son Federal qonun davlat organlari, sanoat, energetika, transport, aloqa, moliya, sog‘liqni saqlash va boshqa muhim sohalardagi axborot tizimlarini himoya qilishga qaratilgan [4]. Mazkur qonun kritik axborot infratuzilmasi subyektlari uchun xavfsizlik talablari, toifalash, kiberhodisalar haqida xabar berish va davlat

nazorati mexanizmlarini belgilaydi [4]. Rossiya modelining nazariy ahamiyati shundaki, unda himoya qilinadigan obyekt faqat server yoki tarmoq sifatida emas, balki davlat va jamiyat faoliyati uchun zarur bo‘lgan funksional tizim sifatida ko‘riladi. Bunday yondashuv favqulodda vaziyatlar, harbiy-siyosiy keskinliklar va geosiyosiy raqobat sharoitida muhim ahamiyat kasb etadi. Shu bilan birga, modelning yuqori markazlashganligi xususiy sektor bilan hamkorlik, ochiq audit va xalqaro axborot almashinuvi masalalarida muvozanatni talab qiladi. MDH mamlakatlari uchun Rossiya tajribasi kritik infratuzilmani toifalash va majburiy xavfsizlik talablarini belgilash borasida ilmiy-amaliy namuna bo‘lib xizmat qiladi.

Qozog‘iston Respublikasida kiberxavfsizlik “axborotlashtirish”, “kritik axborot-kommunikatsiya infratuzilmasi” va shaxsiy ma’lumotlarni himoya qilish sohalari orqali tartibga solinadi. “Axborotlashtirish to‘g‘risida”gi qonun davlat organlari, jismoniy va yuridik shaxslar o‘rtasidagi axborotlashtirish sohasidagi munosabatlarni tartibga soladi [5]. 2020-yilda tasdiqlangan kritik axborot-kommunikatsiya infratuzilmasi xavfsizligini ta’minlash qoidalari xavf tahlili, zaifliklarni boshqarish, audit va kiberhodisalar bo‘yicha xabar berish kabi talablarni o‘z ichiga oladi [6]. Qozog‘iston yondashuvining kuchli jihati shundaki, u raqamli transformatsiya, elektron hukumat va iqtisodiy modernizatsiyani axborot xavfsizligi bilan bog‘lashga intiladi. Biroq tez raqamlashtirilayotgan moliyaviy texnologiyalar, davlat ma’lumotlar bazalari va transport-logistika tizimlarida huquqiy talablarning amaliy ijrosi muntazam sinovdan o‘tadi. Shu bois Qozog‘iston tajribasi kiberxavfsizlikni faqat repressiv javob chorasi emas, balki raqamli iqtisodiyot barqarorligini ta’minlovchi boshqaruv modeli sifatida talqin qilish imkonini beradi. Bunday model O‘zbekiston uchun ham elektron hukumat, davlat xizmatlari va xavfsizlik tizimlarining kiberbarqarorligini ta’minlashda muhim metodik ahamiyatga ega.

MDH mamlakatlarida kiberxavfsizlikning huquqiy ta’minoti odatda bir nechta funksional qatlamlar orqali shakllanadi. Birinchi qatlam konstitutsiyaviy va strategik asoslar bo‘lib, u milliy xavfsizlik, davlat suvereniteti va inson huquqlari bilan bog‘liq umumiy prinsiplarni belgilaydi. Ikkinchi qatlam maxsus kiberxavfsizlik yoki axborot xavfsizligi qonunchiligi bo‘lib, u vakolatli organlar, subyektlar va obyektlarni

aniqlaydi. Uchinchi qatlam kritik infratuzilma himoyasi bo‘lib, energetika, transport, moliya, aloqa, sog‘liqni saqlash va davlat boshqaruvi tizimlarini qamrab oladi. To‘rtinchi qatlam kiberjinoyatchilikka qarshi javobgarlik bo‘lib, noqonuniy kirish, zararli dasturlar tarqatish, ma’lumotlarni o‘g‘irlash va tizimlarga zarar yetkazish uchun sanksiyalarni belgilaydi. Beshinchi qatlam xalqaro hamkorlik va kiberhodisalarga javob berish mexanizmlaridan iborat bo‘lib, transchegaraviy tahdidlar sharoitida alohida ahamiyat kasb etadi. Ushbu qatlamlarning birortasi zaif bo‘lsa, butun huquqiy tizimda institutsional bo‘shliq yuzaga keladi. Shuning uchun kiberxavfsizlikni huquqiy ta’minlash faqat qonun qabul qilish bilan emas, balki ko‘p pog‘onali boshqaruv siklini shakllantirish bilan baholanishi kerak.

Xulosa

MDH mamlakatlarida kiberxavfsizlikni huquqiy jihatdan ta’minlash turli darajada rivojlangan bo‘lsa-da, umumiy tendensiya maxsus qonunchilik, kritik infratuzilma himoyasi va kiberhodisalarga javob berish mexanizmlarini kuchaytirish tomon yo‘nalgan. O‘zbekistonning 2022-yilda “Kiberxavfsizlik to‘g‘risida”gi qonunni qabul qilgani milliy huquqiy tizimda muhim institutsional burilish bo‘ldi [3]. Rossiya tajribasi kritik axborot infratuzilmasini toifalash va majburiy himoya talablarini belgilash borasida muhim ahamiyatga ega [4]. Qozog‘iston modeli esa axborotlashtirish va kritik axborot-kommunikatsiya infratuzilmasini yagona raqamli boshqaruv doirasida bog‘lashga intiladi [5; 6]. Shu bilan birga, MDH mamlakatlarida kiberxavfsizlik tushunchasining axborot xavfsizligi, shaxsiy ma’lumotlar, davlat siri va kiberjinoyatchilik bilan chegaralarini aniq ajratish dolzarb vazifa bo‘lib qolmoqda. O‘zbekiston sharoitida kiberxavfsizlik huquqini sektorlararo, riskga asoslangan va amaliy ijroga yo‘naltirilgan model sifatida rivojlantirish maqsadga muvofiqdir.

Foydalanilgan adabiyotlar:

1. International Telecommunication Union. (2024). Global Cybersecurity Index 2024. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

2. International Telecommunication Union Regional Office for CIS. (2025). CIS countries’ progress in the Global Cybersecurity Index 2024.

ITU. https://www.itu.int/en/ ITU-D/ Regional-Presence/CIS/Pages/ News/14.01.2025.aspx

3. O‘zbekiston Respublikasi. (2022). “Kiberxavfsizlik to‘g‘risida”gi O‘RQ–764-son Qonun. Lex.uz. https://lex.uz/docs/5960604

4. Russian Federation. (2017). Federal Law No. 187-FZ on the Security of the Critical Information Infrastructure of the Russian Federation. Presidential Library / official legal sources. https://www.prlib.ru/en/node/692141

5. Republic of Kazakhstan. (2015). Law on Informatization. Adilet Legal Information System. https://adilet.zan.kz/eng/docs/Z1500000418

6. ICLG. (2025). Digital Business Laws and Regulations: Kazakhstan 2025. Global Legal Group. https://iclg.com/practice-areas/digital-business-laws-and-regulations/kazakhstan

ROSSIYA-UKRAINA URUSHI SHAROITIDA KIBERXAVFSIZLIK TAHDIDLARI VA O‘ZBEKISTONDA OMMAVIY TADBIRLAR XAVFSIZLIGINI TAKOMILLASHTIRISH MASALALARI

Iminov A.A.
Jamoat xavfsizligi universiteti mustaqil izlanuvchisi bo‘limi katta ofitseri
Abdixamidov G‘.Z.
O‘zbekiston Respublikasi Ichki ishlar vazirligi Kriminologiya ilmiy-tadqiqot instituti ilmiy xodimi

Annotatsiya. Ushbu tezisda 2022-2026-yillarda kiberxavfsizlik tahdidlarining keskin ortishi, Rossiya-Ukraina urushi fonida transport-logistika tizimlariga qarshi kiberoperatsiyalar kuchayishi va mazkur jarayonlarning O‘zbekiston uchun amaliy ahamiyati tahlil qilinadi. Tezisda zamonaviy kiberhujumlar endilikda faqat moliyaviy yoki axborot tizimlariga emas, balki harbiy yuk tashish, qo‘shinlar harakati, temiryo‘l, aeroport, port, avtomobil yo‘laklari va ommaviy tadbirlarni boshqaruvchi raqamli infratuzilmalarga ham qaratilayotgani asoslanadi. O‘zbekiston bo‘yicha 2024-yilda kiberhujumlar va axborot texnologiyalari orqali sodir etilgan jinoyatlar sonining oshgani kiberxavfsizlikni jamoat xavfsizligi tizimi bilan integratsiya qilish zarurligini ko‘rsatadi. Milliy gvardiya tomonidan ommaviy tadbirlar xavfsizligini ta’minlashda videokuzatuv,

MUNDARIJA

KIRISH SO‘ZI.....3
I SHO‘BA Zamonaviy telekommunikatsiya tizimlarinining rivojlanish tendensiyalari.....5
Beysenov K.S. Zamonaviy ta’lim tizimida innovatsion texnologiyalarning yangi avlodga ta’siri.....5
Короткова Л.А. Приемный модуль для тв-сигнала.....9
Мустанов О.Г. Разработка структуры и функций грузовых терминалов.....13
Хатамов Б.Б. Гибридные телекоммуникационные системы беспилотных летательных аппаратов: интеграция радиочастотных и оптических каналов.....18
Yusupov U.A., Tashmanov Y.B. Harbiy obyektlar xavfsizligini ta’minlashda makroegilish hodisasiga asoslangan tolali-optik massa datchiglarining tahlili.....24
Xurramov J.A. Aviatsiya radioaloqa tizimlarini raqamlashtirish: Analog tizimlardan raqamli (digital voice) tizimlarga o‘tish muammolari.....31
Tursimuratov S.S. Favqulodda vaziyatlarda tolali-optik bog‘lamli uchuvchisiz uchish apparatlari yordamida moslashuvchan havo aloqa tarmoqlarini tashkil etish.....38
Туганов Г., Абдуллаев Ж. Проблемы развития системы ориентации и управления дронов, беспилотных летательных аппаратов. преимущество и недостатки при применении в локальных войнах.....44
Shaymardonov J.Z. Transport vositalari kuzatuv tizimida GPS texnologiyalaridan foydalanishning nazariy asoslari.....56
Iminov A.A. Ommaviy tadbirlar vaqtida zamonaviy axborot-telekommunikatsiya texnologiyalarining ilmiy-nazariy tahlili (Rossiya federatsiyasining 9-may paradi misolida).....67
Abdullayev U.I. Axborot kommunikatsiya xizmatlarining tavsifi.....78
Mamadoliev M.O. Zamonaviy uchish apparatlarida elektr tizimida uchraydigan nosozliklar va ularning tahlili.....86
Yakubov S.X. Azizov A.N. Deformatsiyalanadigan qattiq jismlar mexanikasida optimallashtirish masalalarini yechish usullari.....91
Исаев Р.И. Перспективы развития оптических сетей связи: Эволюция сетей оптического доступа и оптических транспортных сетей.....96
Yusupov U.A., Erkinov J.A. Optik tola egilishlari yordamida aktiv tolalar, uzatilayotgan signal yo‘nalishi va to‘lqin uzunligini aniqlash.....102
II SHO‘BA Kiberxavfsizlikni ta’minlashning dolzarb muammolari va yechimlari.....108
Sadikov Sh.M., Ablayeva O.Z. .Uz domen zonasining statistik tahlili va rivojlanish tendensiyalari.....108

Turaxodjayev N.S. Ma'lumotlardan ruxsatsiz foydalanishni oldini olish tizimlarini yaratishdagi mavjud axborot xavfsizligi muammolari.....113
Shukurov O.P. Kiberxavfsizlikni ta'minlashda sun'iy intellektdan foydalanish va uning ahamiyati.....119
Beysenov K.S. Kiberxavfsizlikni ta'minlashning dolzarb muammolari va ularning yechimlari.....122
Aliyeva Z.M. Axborot texnologiyalari sohasidagi kiber jinoyatlar.....129
Abdixamidov G'.Z. MDH mamlakatlarida kiberxavfsizlikni huquqiy jihatdan ta'minlashning ilmiy-nazariy asoslari.....133
Iminov A.A., Abdixamidov G'.Z. Rossiya-Ukraina urushi sharoitida kiberxavfsizlik tahdidlari va O'zbekistonda ommaviy tadbirlar xavfsizligini takomillashtirish masalalari.....138
Ermaxamatov X.X. Qurilma konfiguratsiyasidagi zaifliklarni sun'iy intellekt usullari yordamida aniqlash va bartaraf etishning dolzarb muammolari.....145
Samarov X., Barotova Z. A Comparative analytical evaluation of classical, hybrid and ensemble learning methods in intrusion detection systems.....150
Turaxodjayev N.S. Huquqni muhofaza qiluvchi axborot tizimlarida ruxsatlarni chegaralash mexanizmlari: turlari, cheklovlari va rivojlanish yo'nalishlari...153
Toshpulatov Sh. Passive vulnerability detection in web applications: techniques and limitations.....159
Шамшиева Б.М. Сравнительный анализ активных и пассивных методов выявления уязвимостей.....163
Xayrullayev A. Obidov O. Virtual telekommunikatsiya muhitida suricata va wazuh integratsiyasi asosida tarmoq trafigi va kibertahdidlar monitoringi.....168
Хакимбеков Д.Т. Анализ методов обнаружения deepfake и определение перспективных направлений исследований.....178
Nigmatov Z.Z., Akramov B.A. Intelligent monitoring of military equipment using zigbee-based iot systems.....182
Haydarov E.D., Mirzoyeva F.U. Korporativ tarmoqlardagi zararli ta'sirlarni aniqlash muammolari va ularni bartaraf etishdagi yondashuvlar.....192
Ismatov N.N. Bulutli texnologiyalarda ma'lumotlarning sizib chiqish riskini kamaytirish mexanizmlarini ishlab chiqish.....203
Nigmatov Z.Z., Yaxyoyev A.A. Telekommunikatsiya tarmoqlarida kiberhujumlarni aniqlash va oldini olishda IDS/IPS tizimlari samaradorligini baholash.....211
Ulashov J.Z. Zamonaviy bosqichda kiberxavfsizlikni ta'minlash muammolari.....224
Raximov S.Sh. Kiberxavfsizlikning himoya vositalari.....228
Parpiyeva A.J. Ommabop tarmoq snifferlarining tahlili.....232

Мадумарова М.Х. Актуальность усовершенствования информационно-креативной компетенции военнослужащих при обеспечении кибербезопасности.....237
Ganiyev A.A., Jalolov M.S. Korporativ tarmoqlarda ko‘p uchraydigan kiberxavfsizlik zaifliklari haqida.....246
Xayitov D.D., Sodiqov D.S. Cognitive firewall: Miya–kompyuter interfeyslarida fikr maxfiyligi va kognitiv hujumlardan himoyalanishning yangi paradigmasi.....251
Zikirjonov M.D., Abdulxayev N.M. Kiberxavfsizlikda sun’iy intellektning o‘rni.....265
Bobomurodov D.A. O‘quvchilarga harbiy fanlarni o‘qitishda kiberxavfsizlikni ta’minlash yo‘llari.....270
Tursunova M.A. Telemeditsina tizimlarida shaxsiy ma’lumotlar xavfsizligiga tahdidlar tahlili.....273
Samarov X.K. Nizomov A.O‘. Kiberxavfsizlikda big data muammolari: Machine learning asosida tahdidlarni aniqlash va tahlil qilish yondashuvlari.....279
Alimov H.B., Usmanbayev D.S. Tarmoq xavfsizligida sun’iy intellektning kelajagi: avtonom tahdidlarni aniqlash va javob berish tizimlari.....284
Ganiyev A.A. Jalolov M.S. Korporativ tarmoqlarda phishing url manzillar aniqlashni algoritmik yondashuvlar haqida.....289
Ablayeva O.Z. “.UZ” Domenidagi kiberxavfsizlik tahdidlarini aniqlash va oldini olish algoritmlari.....292
Shoimov N.B. O‘zbekiston Respublikasi prezidentining «O‘zbekiston Respublikasining kiberxavfsizlik strategiyasini belgilash va kiberjinoyatchilikning oldini olish tizimini takomillashtirish to‘g‘risida»gi farmoni — kiberxavfsizlikni ta’minlashning asosi.....297
Xoliqov Sh.A. Kiberxavfsizlikda profayling.....302
Akramov B.I. Harbiy boshqaruv punktlarida uzluksiz tarmoq monitoringini tashkil etish: zabbix tizimining xavfsizlik imkoniyatlarini tahlil qilish.....310
III SHO‘BA Qo‘shinlarni avtomatlashtirilgan boshqaruv tizimlarida sun’iy intellektni qo‘llash istiqbollari.....314
Мурадов Ф.А. Метод оценки боевых возможностей беспилотных летательных аппаратов противника на основе машинного обучения.....314
Xakimova D.B. Uchuvchisiz uchish apparatlari tizimlarining klassifikatsiyasi va ularning xususiyatlari.....326
Шамсиев А.А. Применение ии в автоматизированном системе управление войсками.....330
Хатамов Б.Б. Применение методов машинного обучения для интеллектуальной поддержки принятия решений в асув тактического звена управления.....333

Zikirjonov M.D., Abdulxayev N.M. Sun'iy intellekt va axborot texnologiyalarining zamonaviy jamoatdagi o'rni va rivojlanish istiqbollari....339
Uzaqov V.R., Mamajonov I.R. Sun'iy intellekt texnologiyalarini harbiy boshqaruvda qo'llashning zamonaviy yo'nalishlari va istiqbollari.....343
Muxammedinov K.K. Dasturiy konfiguratsliyalanadigan tarmoqda resurslarni intelektual segmentlash uchun mininet imkoniyatlari.....348
Tashmanov Y.B. Favqulodda holatlarda yirik savdo majmualarining xavfsizligini ta'minlashda raqamli texnologiyalar.....352
Babadjanov S.S., Ashurov U.M. Mashinali o'rganishning vizual evolyutsiyasi: orange muhitida ma'lumotlarni kodsiz tahlil qilish texnologiyalari.....356
Tashmanov Y.B. Transport vositalarining yo'l harakati xavfsizligini ta'minlashda sun'iy intellekt texnologiyalarining ahamiyati.....361
Xamidov G'.S. O'zbekistonda sun'iy intellekt asosida tezkor-qidiruv faoliyatini rivojlantirish va jinoyatchilikka qarshi kurash samaradorligini oshirish yo'nalishlari.....365
Bekmurodov I.R. Harbiy texnikada sun'iy intellektning texnologik inqilobi va strategik ustuvorliklari.....370
Серебряков В.О., Наумов Д.И. Китайский опыт использования искусственного интеллекта в военной сфере.....373
Xamidov G'.S. Tezkor-qidiruv faoliyatida qidiruvdagi shaxslarni aniqlashda sun'iy intellekt texnologiyalaridan foydalanishning nazariy va amaliy jihatlari.....379
Nurjanov F.R. Niqob va yorug'lik sharoitida yuz tasviri asosida shaxsni identifikatsiyalashda sun'iy intellekt usullari.....386
Xudoyqulova S.I., Ramonova S.K. Oliy matematika va sun'iy intellekt.....399
Jumaniyozov T.Sh. Oliy harbiy ta'lim muassasalarida sun'iy intellekt texnologiyalari hamda kiberxavfsizlikning o'rni.....404
Berdiyev M.I., Rajabov O.O. Jamoat xavfsizligi tizimlarida audio-vizual anomaliyalarni aniqlash uchun kontekstga moslashuvchan sun'iy intellekt modeli.....409
Tursunboyev A.A. Harbiy xizmatchilari maqomini takomillashtirishda sun'iy intellektning o'rni va ahamiyati.....420
TAKLIF VA TAVSIYALAR.....428

ZAMONAVIY TELEKOMMUNIKATSIYA MUAMMOLARI VA INNOVATSION YECHIMLARI: XALQARO TAJRIBA, NAZARIYA VA AMALIYOT

xalqaro ilmiy-amaliy anjumani
MATERIALLAR TO‘PLAMI

2026-yil 29-aprel

I QISM

Muharrir: Tashmanov Ye.B.
Texnik muharrir: Rahmonov A.A.

Bosishga ruxsat etildi: 11.05.2026. Buyurtma: № 53. Format 60x90/16
Times New Roman garniturasi bilan raqamli bosma usulida bosildi.
Hajmi: 27,5 sh.b.t., 20,15 t-h.t Adadi: 2 nusxa.

O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti bosmaxonasi