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

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,

akkreditatsiya, kirish nazorati, aloqa va tezkor shtab platformalari kritik axborot tizimlari sifatida baholanishi lozim..

Kalit so‘zlar: Rossiya-Ukraina urushi; kiberhodisa; logistika xavfsizligi; qo‘shinlarni tashish; ommaviy tadbirlar; Milliy gvardiya; kiberxavf pasporti; raqamli barqarorlik.

So‘nggi besh yillik tajriba kiberxavfsizlik tahdidlari bevosita harbiy-siyosiy jarayonlar, geosiyosiy raqobat va transchegaraviy logistika tizimlari bilan bog‘lanib borayotganini ko‘rsatmoqda. 2022-yil 24-fevraldan boshlangan Rossiya-Ukraina urushi kiberoperatsiyalar zamonaviy qurolli mojarolarning yordamchi emas, balki operativ-strategik tarkibiy qismiga aylanganini namoyon qildi. Ukraina davlat organlari, temiryo‘l tizimlari, energetika obyektlari, aloqa infratuzilmasi va xalqaro yordam logistikasiga qarshi kiberhujumlar harbiy harakatlar bilan parallel olib borildi. AQSh va hamkor davlatlar e’lon qilgan qo‘shma kiberxavfsizlik ogohlantirishlarida Rossiya harbiy razvedkasiga aloqador guruhlar 2022-yildan boshlab Ukraina uchun harbiy va gumanitar yordam tashuvchi G‘arb logistika, transport va texnologiya tashkilotlarini nishonga olgani qayd etilgan. Ushbu kampaniyada havo, dengiz, temiryo‘l va avtomobil transporti zanjirlari, shuningdek, chegara yaqinidagi internetga ulangan kameralar orqali yuklar harakati haqida razvedka ma’lumotlari yig‘ishga urinishlar kuzatilgan [1]. Bu holat MDH mamlakatlari uchun ham muhim saboqdir, chunki transport yo‘laklari, chegara nazorati, ommaviy tadbirlar, strategik obyektlar va harbiy-ma’muriy boshqaruv tizimlari tobora raqamli platformalarga bog‘lanmoqda. Demak, kiberxavfsizlikni ta’minlash masalasi jinoyatchilikka qarshi kurash doirasidan chiqib, davlat boshqaruvi uzluksizligi, qo‘shinlar harakati va jamoat tartibini saqlashning ajralmas qismiga aylanmoqda.

ENISA 2024-yilgi tahdidlar manzarasida mavjudlikka qarshi tahdidlar, ransomware va ma’lumotlarga qarshi hujumlarni yetakchi yo‘nalishlar sifatida ko‘rsatadi [4]. Check Point Research ma’lumotlariga ko‘ra, 2024-yil ikkinchi choragida global kiberhujumlar yilma-yil 30 foizga oshib, bir tashkilotga haftasiga o‘rtacha 1 636 ta hujum darajasiga yetgan. Hukumat va harbiy sektor esa haftasiga 2 084 ta hujum bilan eng ko‘p nishonga

olingan yo‘nalishlardan biri bo‘lgan [5]. 2024-yil uchinchi choragida o‘rtacha haftalik hujumlar bir tashkilotga 1 876 taga yetib, 2023-yilga nisbatan 75 foizlik o‘sish qayd etilgan [6]. IBM 2024-yilgi hisobotida ma’lumotlar buzilishi bo‘yicha global o‘rtacha zarar 4,88 million AQSh dollariga yetganini bildiradi [7]. Ushbu raqamlar kiberxavfsizlikka oid siyosat va huquqiy tartibga solish oddiy deklarativ prinsiplar bilan cheklanib qolmasligi kerakligini ko‘rsatadi. Davlatlar risklarni oldindan baholash, majburiy audit, zaxira infratuzilma, kiberhodisadan keyingi tiklash va javobgarlik mexanizmlarini aniq belgilashi zarur.

O‘zbekiston bo‘yicha ochiq ma’lumotlar kiberxavfsizlik tahdidlarining tez o‘sayotganini ko‘rsatadi. 2024-yilda mamlakatda 12 milliondan ortiq kiberhujum urinishlari qayd etilgani, bu 2023-yildagi 11 milliondan yuqori ekanligi bildirilgan [8]. 2024-yilning birinchi choragida milliy internet segmentida 3 290 860 dan ortiq kiberhujum qayd etilgani, 19 ta davlat organi va tashkiloti veb-resurslarida 70 ta zaiflik aniqlanib bartaraf etilgani ma’lum qilingan [15]. O‘zbekiston IIV ma’lumotlariga ko‘ra, 2024-yilda axborot texnologiyalari orqali sodir etilgan jinoyatlar 58 800 tani tashkil etib, fuqarolardan 1,909 trillion so‘mdan ortiq mablag‘ talon-toroj qilingan [9]. Bu ko‘rsatkichlar kiberjinoyatchilikning moliyaviy, ijtimoiy va institutsional zarar darajasi ortib borayotganini ko‘rsatadi. 2026-yil boshida e’lon qilingan ayrim ma’lumotlarda esa O‘zbekiston kiberxavfsizlik infratuzilmasi 2024-yilda 7 milliondan, 2025-yilda esa 107 milliondan ortiq tahdidni bloklagani aytiladi [2]. Mazkur raqamlar kiberxavfsizlikni profilaktika, aniqlash, javob berish va tiklash jarayonlari bilan birgalikda tartibga solish zarurligini ko‘rsatadi. Ayniqsa, davlat xizmatlari, bank-moliya tizimi, transport, ta’lim va jamoat xavfsizligi sohasida inson omili va texnik zaifliklar birgalikda katta xavf tug‘diradi.

Rossiya-Ukraina urushi kiberxavfsizlikka oid nazariy qarashlarda yangi konseptual vaziyatni yuzaga keltirdi. Avvallari kiberhujumlar ko‘proq banklar, davlat portallari, ommaviy axborot vositalari yoki shaxsiy ma’lumotlar bazalariga qarshi qaratilgan bo‘lsa, urush sharoitida transport, logistika va harbiy ta’minot zanjirlari asosiy nishonga aylandi. 2025-yilda AQSh Milliy xavfsizlik agentligi, FQB va hamkor davlatlar e’lon qilgan

ogohlantirishda Rossiya harbiy razvedkasi bilan bog‘liq kiberaktyorlar G‘arbning Ukraina bilan bog‘liq logistika va texnologiya tashkilotlarini nishonga olgani qayd etilgan. Ular havo, dengiz, temiryo‘l va avtomobil tashuvlari, portlar, aeroportlar, logistika firmalari hamda internetga ulangan kuzatuv kameralaridan ma’lumot olishga uringan [1]. Bunday faoliyat harbiy yuklar, gumanitar yordam, yoqilg‘i, texnika, o‘q-dori va qo‘shinlar harakatini kuzatish yoki kechiktirish imkoniyatini yaratishi mumkin. Shu bois transport-logistika tizimlarining kiberhimoyasi endilikda faqat iqtisodiy xavfsizlik emas, balki operativ mudofaa masalasidir. O‘zbekiston uchun bu tajriba chegaralar, aeroportlar, temiryo‘l tugunlari, omborlar, ommaviy tadbirlar hududi va kuch tuzilmalari harakatini boshqaruvchi tizimlarni alohida muhofaza qilish zarurligini ko‘rsatadi.

Qo‘shinlarni tashish va harbiy-logistik harakatlarni kiberxavfsizlik nuqtayi nazaridan baholashda bir nechta asosiy xavf kanali ajratiladi. Birinchi kanal - transport jadvali, marshrut, yuk tarkibi va harakat vaqti haqidagi ma’lumotlarning noqonuniy qo‘lga kiritilishidir. Ikkinchi kanal - temiryo‘l, aeroport, port, avtomobil nazorat punktlari va ombor boshqaruv tizimlariga zararli dasturlar orqali ta’sir ko‘rsatishdir. Uchinchi kanal - kuzatuv kameralariga, GPS qurilmalariga, logistika platformalariga yoki elektron hujjat aylanish tizimlariga kirib, real vaqtli razvedka ma’lumotlari olishdir. To‘rtinchi kanal - noto‘g‘ri axborot tarqatish orqali logistika qarorlarini chalkashtirish, navbatlar, kechikishlar va xavfsizlik bo‘shliqlarini yuzaga keltirishdir. Beshinchi kanal - ransomware yoki DDoS hujumlari orqali tashish jarayonining uzluksizligini buzishdir. Ukraina temiryo‘llariga 2025-yilda qilingan keng ko‘lamli kiberhujum yo‘lovchi va yuk xizmatlarida uzilishlar keltirib chiqargani, ayrim jarayonlar vaqtincha qog‘oz hujjat aylanishiga o‘tkazilganini ko‘rsatdi [8]. Bu hodisa raqamli tizimlar ishdan chiqqanda ham transport boshqaruvi ishlashini davom ettiruvchi zaxira protokollar majburiy bo‘lishi kerakligini isbotlaydi. Huquqiy jihatdan bunday protokollar favqulodda rejim, davlat sirini saqlash, shaxsiy ma’lumotlarni himoya qilish va tezkor axborot almashinuvi normalari bilan uyg‘unlashtirilishi zarur.

Ommaviy tadbirlar xavfsizligi ham kiberxavfsizlik huquqi bilan tobora kuchliroq bog‘lanmoqda. Stadion, konsert maydoni, festival, xalqaro sammit, sport musobaqasi yoki davlat bayrami kabi yirik tadbirlarda jismoniy xavfsizlik raqamli tizimlarsiz samarali ta’minlanmaydi. Kirish-chiqish nazorati, yuzni aniqlash, avtomobil raqamlarini tanish, dronlarni aniqlash, radiotelefon aloqa, tezkor shtab platformasi, evakuatsiya ogohlantirishlari va tibbiy yordam koordinatsiyasi raqamli infratuzilmaga tayanadi. Agar ushbu tizimlarga kiberhujum qilinsa, navbatlar, noto‘g‘ri yo‘naltirish, aloqa uzilishi, yolg‘on signal, ma’lumot oqishi yoki evakuatsiya boshqaruvida xatolik yuzaga kelishi mumkin. Shunday ekan, Milliy gvardiya tomonidan ommaviy tadbirlar xavfsizligini ta’minlashda kiberxavfsizlik alohida tayyorgarlik bosqichi sifatida ko‘rilishi kerak. Tadbir rejasi tarkibiga “kiberxavf pasporti”, axborot tizimlari ro‘yxati, mas’ul administratorlar, zaxira aloqa kanallari, kiberhodisaga javob algoritmi va huquqiy javobgarlik chegaralari kiritilishi maqsadga muvofiqdir. Bu yondashuv jismoniy va raqamli xavfsizlikni yagona operativ boshqaruv modeliga birlashtiradi. Natijada ommaviy tadbirlar xavfsizligi faqat kuch va vositalarni joylashtirish bilan emas, balki axborot oqimlarini himoya qilish bilan ham ta’minlanadi.

Idoralararo hamkorlik ommaviy tadbirlar kiberxavfsizligini ta’minlashda hal qiluvchi ahamiyatga ega. Kiberhodisa paytida bir vaqtning o‘zida vakolatli kiberxavfsizlik organi, ichki ishlar, prokuratura, aloqa operatorlari, transport tashkilotlari, mahalliy hokimiyat, tadbir tashkilotchilari va xavfsizlik bo‘linmalari manfaatdor bo‘ladi. Agar ularning vakolatlari oldindan aniqlanmagan bo‘lsa, kiberhodisaga javob berish sekinlashadi. Ayniqsa, ommaviy tadbirlar paytida vaqt omili hal qiluvchi ahamiyatga ega bo‘ladi. Besh daqiqalik aloqa uzilishi yoki noto‘g‘ri xabar minglab odamlar oqimini boshqarishda xavf tug‘dirishi mumkin. Shu bois huquqiy jihatdan “yagona kiber-operativ shtab” mexanizmini ishlab chiqish zarur. Bu shtab tadbir boshlanishidan oldin xavf baholash, tadbir vaqtida monitoring va tadbirdan keyin kiberhodisa tahlilini amalga oshirishi kerak. Bunday model davlat organlari o‘rtasida ma’lumot almashishning aniq tartibi, ruxsat darajalari va javobgarlik chegaralarini talab qiladi.

Kiberxavfsizlikdagi yana bir muhim masala zaxira va avtonom boshqaruv rejimidir. Rossiya-Ukraina urushi tajribasi, xususan logistika va temiryo‘l xizmatlariga qilingan hujumlar, raqamli tizimlar izdan chiqqanda qo‘lda boshqaruv va zaxira protokollar hayotiy ahamiyatga ega ekanini ko‘rsatdi [1, 2]. Ukraina temiryo‘llari hujumdan keyin ayrim yuk operatsiyalarida qog‘oz hujjat aylanishiga vaqtincha o‘tganini bildirgan. Bu holat har qanday davlat uchun aniq saboq beradi: raqamlashtirish to‘liq avtomatlashtirish degani emas, balki uzilish paytida ham ishlay oladigan gibrid tizim yaratish demakdir. Milliy gvardiya ommaviy tadbirlar xavfsizligida ham shunday modelga muhtoj. Agar internet uzilsa, mobil aloqa yuklamasi oshsa yoki server ishlamay qolsa, qo‘mondonlik, patrul, nazorat punkti va evakuatsiya guruhlari qanday tartibda ishlashi oldindan belgilangan bo‘lishi kerak. Huquqiy jihatdan bunday rejim xizmat yo‘riqnomalari, favqulodda vaziyat protokollari va axborot xavfsizligi reglamentlarida aks ettirilishi zarur. Bu kiberxavfsizlikni amaliy barqarorlik bilan bog‘laydi.

Xulosa

2022-2026-yillardagi ochiq statistikalar kiberxavfsizlik tahdidlari miqdoriy va sifat jihatdan keskin ortganini ko‘rsatmoqda. Global miqyosda 2024-yilda hujumlar chastotasi oshib, hukumat va harbiy sektor eng ko‘p nishonga olingan yo‘nalishlardan biriga aylandi. O‘zbekistonda 2024-yilda 12 milliondan ortiq kiberhujum urinishlari, 58 800 ta IT orqali sodir etilgan jinoyat va 1,909 trillion so‘mdan ortiq moddiy zarar qayd etilgani masalaning milliy darajadagi dolzarbligini ko‘rsatadi. Rossiya-Ukraina urushi esa kiberxavfsizlik transport, logistika, temiryo‘l, harbiy yuk tashish va qo‘shinlar harakatini ta’minlash bilan bevosita bog‘liq ekanini isbotladi [7; 8]. Shu sababli O‘zbekiston sharoitida ommaviy tadbirlar xavfsizligi, harbiy-ma’muriy boshqaruv va transport yo‘laklari raqamli tizimlarining kiberbarqarorligini kuchaytirish zarur. Milliy gvardiya faoliyatida kiberxavfsizlik yordamchi yo‘nalish emas, balki operativ boshqaruvning majburiy elementi sifatida qaralishi lozim.

Takliflar

Birinchidan, Milliy gvardiya tizimida “Ommaviy tadbirlar kiberxavfsizligi pasporti” institutini joriy etish maqsadga muvofiq. Ushbu pasport har bir yirik tadbir bo‘yicha foydalaniladigan axborot tizimlari, videokuzatuv kameralar, akkreditatsiya bazalari, QR-ruxsatnomalar, mobil aloqa kanallari, dron monitoringi, tezkor shtab serverlari va zaxira aloqa vositalarini to‘liq ro‘yxatga olishi kerak.

Ikkinchidan, Milliy gvardiya huzurida ommaviy tadbirlar uchun vaqtinchalik “kiber-operativ shtab” modelini shakllantirish zarur. Mazkur shtab tadbir davomida Milliy gvardiya, DXX vakolatli organlari, IIV, aloqa operatorlari, mahalliy hokimiyat, tadbir tashkilotchilari va texnik provayderlar o‘rtasida tezkor axborot almashuvini ta’minlaydi.

Uchinchidan, Milliy gvardiya o‘quv jarayoniga “kiberxavfsizlikka asoslangan ommaviy tadbirlar xavfsizligi” bo‘yicha ssenariyli trening modulini kiritish lozim. Modulda soxta QR-ruxsatnoma, videokuzatuv serveri ishdan chiqishi, dron monitoringi manipulyatsiyasi, soxta Telegram xabari, GPS marshrut ma’lumotlari sizib chiqishi va aloqa kanali uzilishi kabi real ssenariylar ishlanishi kerak.

Foydalanilgan adabiyotlar:

1. National Security Agency, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, & partners. (2025). Russian GRU targeting Western logistics entities and technology companies. Joint Cybersecurity Advisory. https://media.defense.gov/ 2025/May/21/2003719846/-1/-1/0/CSA_ RUSSIAN_GRU _TARGET_ LOGISTICS.PDF

2. Reuters. (2025). Ukraine railways say cyber attack hit its online freight services. Reuters. https://www.reuters.com /technology/ cybersecurity /ukraine-railways -say -sundays-cyber-attack-hit-its-o nline-freight- services- 2025-03-25/

3. Ministry of Internal Affairs of the Republic of Uzbekistan. (2025). Creating a safe cyberspace by combating cybercrime. Government Portal of Uzbekistan. https://gov.uz/en/iiv/news/view/52319

4. European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

5. Check Point Research. (2024). Check Point Research reports highest increase of global cyber attacks seen in last two years: A 30% increase in Q2 2024 global cyber attacks. Check Point Software. https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

6. Check Point Research. (2024). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Software. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

7. IBM. (2024). Cost of a Data Breach Report 2024: Key findings. IBM Security. https://www.ibm.com/think/insights/whats-new-2024-cost-of-a-data-breach-report

8. Kun.uz. (2025). Over 12 million cyberattacks recorded in Uzbekistan in 2024. Kun.uz. https://kun.uz/en/news/2025/02/03/over-12-million-cyberattacks-recorded-in-uzbekistan-in-2024

Kun.uz. (2024). Uzbekistan reports over 3 million cyberattacks for Q1 2024. Kun.uz. https://kun.uz/en/news/2024/04/06/uzbekistan-reports-over-3-million-cyberattacks-for-q1-2024

QURILMA KONFIGURATSIYASIDAGI ZAIFLIKLARNI SUN'IY INTELLEKT USULLARI YORDAMIDA ANIQLASH VA BARTARAF ETISHNING DOLZARB MUAMMOLARI

Ermaxamatov X.X.

Toshkent Axborot Texnologiyalari Universiteti 2-kurs magistrant

Hozirgi kunda kiberxavfsizlikni ta'minlash jarayoni axborot texnologiyalari infratuzilmalarining murakkablashuvi va raqamli qurilmalar xilma-xilligining keskin ortishi tufayli ancha murakkablashmoqda. Ish jarayonlarini raqamlashtirish natijasida korxona va tashkilotlar serverlar, tarmoq uskunalari, virtual tizimlar va bulutli xizmatlarni keng qo'llamoqda.

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