



O'zbekiston Respublikasi
Maktabgacha va maktab
ta'limi vazirligi

ISSN: 2992-9008
UDK: 37

TA'LIM VA TARAQQIYOT

Ilmiy-uslubiy jurnali



2026-YIL 5-SON

www.journal.namspi.uz

Bosh muharrir: Namangan davlat pedagogika instituti rektori B.E.Xusanov
Mas'ul muharrir: Ilmiy ishlar va innovatsiyalar bo'yicha prorektor M.R.Qodirxonov
Mas'ul muharrir o'rinbosari: Ilmiy tadqiqotlar, innovatsiyalar va ilmiy-pedagogik kadrlar tayyorlash bo'limi boshlig'i J.A.Yuldashev

TAHRIR HAY'ATI

Aniq va tabiiy fanlar: k.f.d., prof. Sh.Abdullayev, f-m.f.d., dots. R.Xakimov, k.f.d., prof. N.Vohidova, k.f.d., dots. M.Qodirxonov, b.f.d., dots. A.Batashov, f-m.f.n., dots., T.Abdullayev, p.f.n., dots. M.Eshnazarova, p.f.n., dots. G'.Nafasov, p.f.n., dots. M.Boltayeva.

Texnika fanlari: t.f.d., prof. A.Umarov, t.f.d., prof. A.Qayumov, PhD, dots. Sh.Xudoyqulov, PhD, dots. Abdunazarov.

Ijtimoiy-gumanitar fanlar: s.f.d., prof. T.Fayzullayev, tar.f.d., prof. A.Rasulov. f.f.d., prof. M.Ismoilov, i.f.d., dots. N.Sotivoldiyev, t.f.n., dots. A.Isoqboyev, f.f.n., dots. O.Mamatov, t.f.n., dots. Z.Haydarov, PhD. J.Yuldashev, PhD. A.Abdullayev.

Pedagogika fanlari: p.f.d., prof. B.Xodjayev, p.f.d., prof. X.Najmiddinova, p.f.d., prof. T.Ismoilov, p.f.d., prof. S.Abdullayev. p.f.d., prof., M.Y.Sobirova, p.f.d., prof., R.Zamilova, p.f.d., prof. Sh.Xujamberdiyeva, p.f.d., dost. M.Asqarova, PhD, dots. M.Asranboyeva.

Filologiya fanlari: fil.f.d., prof. N.Uluqov, fil.f.d., prof. H.Usmanova, f.f.d., dots. X.Shokirova, p.f.n., dots. S.Misirov, p.f.n., dots. Sh.Ubaydullayev, PhD, dots. P.Lutfullayev, PhD, dots. M.Yakubbayev.

Texnik muharrir: R.Tursunov

Tahririyat manzili: Namangan shahri, Uychi ko'chasi, 316-uy.

Pochta indeksi: 160136, **Faks:** (0369) 227-27-21,

Email: Info@namspi.uz

"Ta'lim va taraqqiyot" ilmiy-uslubiy jurnali elektron to'plam sifatida O'zbekiston Respublikasi Prezidenti Administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi (AOKA)ning 2022-yil 25-oktabrdagi № 045044 raqamli guvohnomasi asosida chop etiladi. Jurnal Oliy Attestatsiya komissiyasining 2024-yil 30-noyabrdagi (№ 364/5) yig'ilishi qaroriga asosan pedagogika fanlari bo'yicha falsafa fanlari doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan asosiy ilmiy natijalarini chop etish uchun tavsiya etilgan. UDK: 37, Xalqaro standartlashtirish raqami (ISSN): 2992-9008.

Maqolalarning ilmiy saviyasi va keltirilgan ma'lumotlar uchun mualliflar javobgar hisoblanadi.

ZAMONAVIY DRON TIZIMLARIDA KIBERHUJUMLAR TAHLILI VA AXBOROT XAVFSIZLIGINI TA'MINLASHNING INNOVATSION YECHIMLARI

Rivojiddinov Doniyor,

KIUT, o'qituvchi

e-mail: doniyorrivojiddinov@gmail.com,

+998 (95) 262 30 50

Annotatsiya: ushbu maqolada zamonaviy dron tizimlarida yuzaga kelishi mumkin bo'lgan kiberxavfsizlik tahdidlari va kiberhujumlar tahlil qilingan. Dronlarning boshqaruv, aloqa va navigatsiya tizimlariga ta'sir qiluvchi DoS, Man-In-The-Middle, GPS spoofing, jamming va wormhole kabi hujumlarning xususiyatlari ko'rib chiqilgan. Shuningdek, dron tizimlarida axborot xavfsizligini ta'minlash, ma'lumotlarni himoyalash va kiberhujumlarning oldini olish bo'yicha zamonaviy hamda innovatsion yondashuvlar yoritilgan. Maqolada dasturiy ta'minotni muntazam yangilash, VPN orqali ma'lumotlarni shifrlash, qurilmalar ulanishini cheklash va xavfsiz qaytish (RTH) funksiyasidan foydalanish kabi himoya choralarining ahamiyati asoslab berilgan.

Kalit so'zlar: dron, kiberxavfsizlik, kiberhujum, axborot xavfsizligi, DoS hujumi, Man-In-The-Middle, GPS spoofing, jamming, wormhole, dron kommunikatsiyasi, ma'lumotlarni himoyalash, innovatsion xavfsizlik.

АНАЛИЗ КИБЕРАТАК НА СОВРЕМЕННЫЕ СИСТЕМЫ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ И ИННОВАЦИОННЫЕ РЕШЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. в статье проведён анализ современных угроз кибербезопасности и кибератак, которые могут возникать в системах беспилотных летательных аппаратов (дронов). Рассмотрены особенности таких атак, как DoS, Man-In-The-Middle, GPS spoofing, jamming и wormhole, оказывающих влияние на системы управления, связи и навигации дронов. Также освещены современные и инновационные подходы к обеспечению информационной безопасности, защите данных и предотвращению кибератак в беспилотных системах. Обоснована важность таких мер защиты, как регулярное обновление программного обеспечения, шифрование данных с использованием VPN, ограничение подключаемых устройств и применение функции безопасного возврата дрона (RTH).

Ключевые слова: дрон, кибербезопасность, кибератака, информационная безопасность, DoS-атака, Man-In-The-Middle, GPS spoofing, jamming, wormhole, коммуникация дронов, защита данных, инновационные решения безопасности.

ANALYSIS OF CYBERATTACKS ON MODERN DRONE SYSTEMS AND INNOVATIVE SOLUTIONS FOR ENSURING INFORMATION SECURITY

Abstract. *this article analyzes modern cybersecurity threats and cyberattacks that may occur in unmanned aerial vehicle (UAV) systems. The study examines the characteristics of attacks such as DoS, Man-In-The-Middle, GPS spoofing, jamming, and wormhole attacks, which can affect drone control, communication, and navigation systems. The article also highlights modern and innovative approaches to ensuring information security, protecting data, and preventing cyberattacks in UAV systems. The importance of security measures such as regular software updates, data encryption using VPNs, restricting connected devices, and applying the Return To Home (RTH) function for safe drone recovery is substantiated.*

Keywords: *drone, cybersecurity, cyberattack, information security, DoS attack, Man-In-The-Middle, GPS spoofing, jamming, wormhole, drone communication, data protection, innovative security solutions.*

KIRISH

Raqamli texnologiyalar jadal rivojlanishi natijasida uchuvchisiz uchish apparatlari — dronlardan foydalanish ko'lami kengayib bormoqda. Dronlar qishloq xo'jaligi, geodeziya, qurilish, logistika, monitoring va favqulodda vaziyatlarda samarali texnologik vosita sifatida qo'llanilmoqda. Shu bilan birga, ularning boshqaruv, aloqa va navigatsiya tizimlarining raqamlashtirilishi kiberxavfsizlik bilan bog'liq yangi tahdidlarni yuzaga keltirmoqda. O'zbekistonda ham uchuvchisiz uchish apparatlaridan foydalanish va raqamli xavfsizlikni ta'minlash masalalariga alohida e'tibor qaratilmoqda. Xususan, O'zbekiston Respublikasi Prezidentining 2018-yil 29-martdagi PQ-3639-son qarorida iqtisodiyot tarmoqlarida uchuvchisiz uchish apparatlaridan maqsadli va samarali foydalanish masalalari belgilangan. Shuningdek, axborot xavfsizligi va kiberxavfsizlikni rivojlantirishga qaratilgan Prezidentning PF-6007-son Farmoni hamda PQ-4751-son qarori mazkur sohaning huquqiy va tashkiliy asoslarini mustahkamlashga xizmat qilmoqda.

Dron tizimlarining raqamli aloqa kanallariga bog'liqligi ularni DoS, Man-In-The-Middle, GPS spoofing, jamming va wormhole kabi kiberhujumlarga nisbatan zaiflashtirishi mumkin. Bunday hujumlar boshqaruv jarayonining buzilishi, navigatsiya ma'lumotlarining o'zgarishi yoki aloqa kanalining izdan chiqishiga olib kelishi ehtimoli mavjud. Shu sababli zamonaviy dron tizimlarida kiberhujumlarni aniqlash, ularning

oldini olish va axborot xavfsizligini ta'minlashning samarali mexanizmlarini ishlab chiqish dolzarb ilmiy-amaliy masalalardan biridir. Mazkur maqolada dron tizimlaridagi asosiy kiberhujumlar tahlil qilinib, ularning ta'siri hamda axborot xavfsizligini ta'minlashning innovatsion yechimlari ko'rib chiqiladi.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Uchuvchisiz uchish apparatlari yoki dronlarning keng qo'llanilishi bilan bir qatorda, ularning boshqaruv, aloqa, navigatsiya va ma'lumot almashish tizimlarining kiberxavfsizligini ta'minlash masalasi ham dolzarb ilmiy yo'nalishlardan biriga aylanmoqda. Mazkur muammo bo'yicha olib borilgan tadqiqotlar dron tizimlarining texnik imkoniyatlari bilan bir qatorda, ularning kiberhujumlarga nisbatan zaif jihatlarini ham o'rganishga qaratilgan. Axborot xavfsizligi nuqtayi nazaridan O'zbekiston Respublikasi Prezidentining PF-6007-son Farmoni hamda PQ-4751-son qarori muhim ahamiyatga ega. Ushbu hujjatlarda axborot tizimlari va resurslarini himoyalash hamda mamlakatda kiberxavfsizlikni ta'minlash tizimini takomillashtirishga doir masalalar yoritilgan. Ular dron tizimlarining kiberxavfsizligini tashkil etishda milliy huquqiy va tashkiliy asos sifatida qaralishi mumkin. G'aniyev S.K., Karimov M.M. va Tashev K.A. tomonidan tayyorlangan **"Axborot xavfsizligi"** darsligida axborotni himoyalash, axborot xavfsizligi va tegishli texnologiyalar bo'yicha nazariy asoslar keltirilgan. Mazkur manba dron tizimlarida ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta'minlash masalalarini nazariy jihatdan asoslash uchun muhim manba bo'lib xizmat qiladi. Maqolada, shuningdek, dron bozorining rivojlanish dinamikasini ko'rsatish uchun Statista ma'lumotlaridan foydalanilgan. 2021–2026-yillar oralig'idagi bozor ko'rsatkichlari dronlardan foydalanish ko'lami ortib borayotganini ko'rsatish uchun keltirilgan. Shu bilan birga, maqoladagi foydalanilgan adabiyotlar ro'yxatida Statista manbasining aniq grafik havolasi va murojaat sanasini ko'rsatish tavsiya etiladi. Tahlil qilingan adabiyotlar uchuvchisiz uchish apparatlari xavfsizligini uchta asosiy yo'nalishda o'rganish imkonini beradi: birinchidan, dronlardan foydalanishning

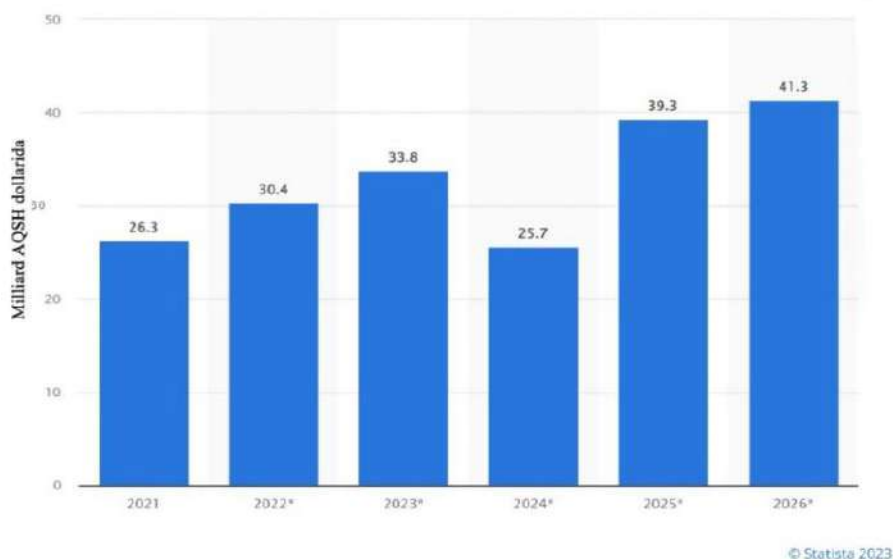
huquqiy va tashkiliy asoslari; ikkinchidan, axborot va kiberxavfsizlikning nazariy asoslari; uchinchidan, dron kommunikatsiyalariga qaratilgan amaliy kiberhujumlar **va ularning oldini olish masalalari** ushbu hujumlarning dronning boshqaruv, aloqa va navigatsiya tizimlariga ta'sirini kompleks tahlil qilishga e'tibor qaratilgan.

Mazkur tadqiqotning metodologik asosini zamonaviy uchuvchisiz uchish apparatlari tizimlarida yuzaga keladigan kiberxavfsizlik tahdidlarini **tizimli, qiyosiy va funksional tahlil qilish** tashkil etadi. Tadqiqot obyekti sifatida dronlarning boshqaruv, aloqa, navigatsiya va ma'lumot almashish tizimlari, tadqiqot predmeti sifatida esa ushbu tizimlarga nisbatan yuzaga kelishi mumkin bo'lgan kiberhujumlar va ularga qarshi axborot xavfsizligi mexanizmlari belgilandi. Tadqiqot jarayonida, avvalo, dron kommunikatsiyasining asosiy tuzilishi va axborot almashish jarayoni o'rganildi. Keyingi bosqichda **tahdidlarni tasniflash usuli** qo'llanildi. Tadqiqotda **qiyosiy tahlil usuli** yordamida turli kiberhujumlarning dron tizimining qaysi funksional qismiga ko'proq ta'sir qilishi baholandi. Jumladan, DoS va jamming asosan aloqa va xizmatlarning mavjudligiga, Man-In-The-Middle ma'lumot almashish xavfsizligiga, GPS spoofing navigatsiya aniqligiga, wormhole esa tarmoqning yaxlitligi va marshrutlash jarayonlariga xavf tug'dirishi nuqtayi nazaridan tahlil qilindi. Shuningdek, **funksional-tizimli tahlil** usulidan foydalanilib, dron tizimining asosiy komponentlari — boshqaruv kanali, aloqa kanali, navigatsiya tizimi, telemetriya va dasturiy ta'minotga kiberhujumlarning ehtimoliy ta'siri o'rganildi. Ushbu yondashuv orqali xavfsizlikni faqat bitta qurilma yoki aloqa kanalini himoyalash orqali emas, balki butun dron tizimi miqyosida tashkil etish zarurligi asoslandi. Maqolaning xulosasida ham boshqaruv kanallari, navigatsiya tizimlari, telemetriya ma'lumotlari va dasturiy ta'minotga bo'lgan tahdidlar alohida ko'rsatilgan. Tadqiqotning yana bir metodologik yo'nalishi **himoya mexanizmlarini tahlil qilishdan** iborat bo'ldi. Bunda dasturiy ta'minotni muntazam yangilash, antivirus vositalaridan foydalanish, VPN orqali aloqani shifrlash, tayanch stansiyaga ulanadigan qurilmalarni cheklash hamda RTH — "Return To Home" xavfsiz

qaytish funksiyasidan foydalanish kabi choralar kiberhujumlarga qarshi himoya mexanizmlari sifatida ko'rib chiqildi. Tadqiqotning yakuniy bosqichida **sintez va umumlashtirish usuli** asosida dronlar uchun ko'p qatlamli kiberxavfsizlik modeli taklif etildi. Ushbu yondashuv kriptografik himoya, kuchli autentifikatsiya, xavfsiz aloqa protokollari, real vaqt rejimidagi tarmoq monitoringi, sun'iy intellekt asosida anomal faoliyatni aniqlash, dasturiy ta'minotni yangilash va navigatsiya ma'lumotlarini mustaqil manbalar orqali tekshirish kabi mexanizmlarni birlashtirishga asoslanadi.

NATIJALAR VA MUHOKAMA

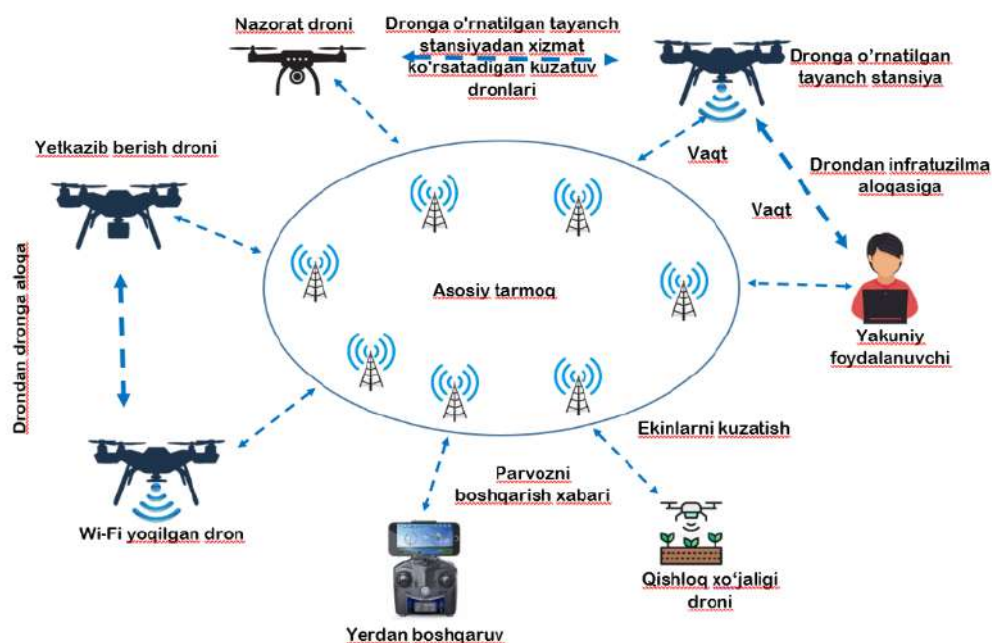
Bugungi kunda dronlarni ishlab chiqish va ulardan turli sohalarda keng foydalanish, dronlarga bo'lgan talabni oshishiga olib keldi. Bu o'z navbatida butun dunyo bo'ylab dron bozorining hajmi ortib borishiga olib kelmoqda[4]. Dron bozorining hajmi ortib borishi statista.com saytining ma'lum qilishicha 2021-yildan 2026-yilgacha butun dunyo bo'ylab dron bozorining hajmi quyidagicha tashkil qilinmoqda (**1-rasm**).



1-rasm. Dunyo bozorida dronlarni sotuv hajmi.

2021-yildan 2026-yilgacha dunyo bo'ylab dron bozorining hajmi. Dronlar xavfsizligi butun dunyo tadqiqotchilari va sanoatchilar o'rtasida asosiy muhokamaga sabab bo'luvchi mavzudir. Dronlarning bir nechta ilovalari mavjud bo'lsada, xavfsizlik muammolari va zarur arxitektura o'zgarishlari amalga oshirilmasa yaqin kelajakda dron

illovalari o'zlarining madsadlariga xizmat qila olmaydi. Shunday ekan dron aloqasi xavfsizligi muammolarni bartaraf etish va yangi yechim arxitekturalarini ishlab chiqish zarur.



2-rasm. Dron bilan aloqaning asosiy jarayoni.

Dron aloqasidagi axborot xavfsizligidagi muammolarni o'rganishdan avval dron bilan aloqa qilishning asosiy jarayonini ko'rib chiqamiz (**2-rasm**).

Dron oddiy prodsedura bilan ishlaydi [2]. U yerdagi boshqaruvchidan dronga ma'lumot havolasini va drondan sun'iy yo'ldoshga ma'lumotlar havolasini yuborishni o'z ichiga oladi.

Dron aloqasida umumiy kibertahdidlardan tashqari ba'zi maxsus xavfsizlik muammolariga duch keladi. Bu muammolardan biri uning uchuvchisiz ekanligidir va kutilmagan muammolarni dinamik va moslashuvchan holatda hal qilishi qiyin. Dronlar xavfsizligida autentifikatsiya, kirishni nazorat qilish, va ma'lumotlarni himoyalashda maxfiylikni ta'minlashda ilg'or yechimlarni qo'llash zarurati mavjud bo'lib kelgan. Sababi dronlarda resurslar juda cheklanganligidir. Yuqorida keltirilgan maxsus

xavfsizlik muammolari bilan bir qatorda dron aloqasida quyidagi xavfsizlik tahdidlarini ham bartaraf etishi zarur. Bu hujumlarni ba'zilarini keltiramiz:

Xizmatdan voz kechish hujumlari - DoS yoki xizmatdan voz kechish hujumchi tomonidan dronning normal ishlashini to'xtatish uchun ko'p sonli ortiqcha so'rovlar tufayli umumiy resurslardan qonuniy foydalanuvchilarga kirishni cheklaydi. Bu tizimning haddan tashqari yuklanishiga olib keladi va ba'zi yoki barcha qonuniy so'rovlarning rad etilishiga olib kelishi mumkin.

O'rtadagi odam (Man-In-The-Middle) xujumi – hujumi mijoz va dron o'rtasida hujumchini joylashtiradi. Hujumchi Wi-Fi Pineapple deb nomlanuvchi qurilmadan foydalanadi.

Geoma'lumotlarga taqlid - GPS-spoofing. GPS-spoofing hujumchi noto'g'ri signallarni uzatadi. Dronning GPS koordinatalarini olishning ushbu jarayonida dron GPS-dan foydalangan holda soxta geoma'lumotdan foydalanadi.

Radar: Monostatik radar muhim ob'yektlarni qidirishning eng an'anaviy usuli hisoblanadi. Radarlar uzoq masofani bosib o'ta oladigan elektromagnit signallarni yuboradi. Ushbu signallar barcha yo'nalishlarda tarqaladi va dron borligi aniqlangan joyda signallar dron yuzasidan aks etadi.

Jammerlar (Siqilish hujumi) - Jammers elektron qurilma yordamida qabul qiluvchining uchidagi signallarni blokirovka qilish uchun hujumchilar tomonidan ishlatiladigan elektron qurilmalardir.

Wormhole (chuvalchang teshigi) hujumi. Chuvalchang teshigi hujumida ikkita tajovuzkor dron tarmog'i o'rtasidagi aloqani tinglash uchun o'zlarini strategik ravishda tarmoqqa joylashtiradilar. Tajovuzkor tunnel quriladi, tajovuzkorga tarmoqning istalgan nuqtasidan hujum boshlash imkonini beradi [3].

Yuqoridagi tahdidlarga qarshi kurashish uchun bir-qancha tavsiyalar:

- dronlar dasturiy ta'minotini muntazam ravishda yangilash;
- dronda yangilangan antivirus dasturlaridan foydalanish;

- ulanishni shifrlash uchun VPN virtual xususiy tarmoqlardan foydalanish;
- asosiy stantsiyaga ulanishi mumkin bo'lgan qurilmalar sonini cheklang;
- dronni o'g'irlab ketilgan holatda "Uyga qaytish" (RTH-Return To Home) rejimidan foydalaning.

XULOSA

Zamonaviy dron tizimlarining keng qo'llanilishi ularning axborot xavfsizligini ta'minlash masalasini dolzarb ilmiy-amaliy muammolardan biriga aylantirmoqda. Tadqiqot davomida dronlarning boshqaruv kanallari, navigatsiya tizimlari, telemetriya ma'lumotlari va dasturiy ta'minotiga nisbatan yuzaga kelishi mumkin bo'lgan kiberhujumlar tahlil qilindi. Ayniqsa, aloqa kanalini buzish, GPS signalini soxtalashtirish, ma'lumotlarni tutib qolish, zararli dasturiy ta'minotdan foydalanish hamda masofadan boshqaruv tizimiga noqonuniy kirish kabi tahdidlar dronlarning barqaror va xavfsiz ishlashiga jiddiy ta'sir ko'rsatishi mumkinligi aniqlandi.

Dron tizimlarida axborot xavfsizligini kuchaytirish uchun ko'p qatlamli himoya konsepsiyasidan foydalanish maqsadga muvofiq. Bunda ma'lumotlarni kriptografik himoyalash, kuchli autentifikatsiya, xavfsiz aloqa protokollaridan foydalanish, real vaqt rejimida tarmoq monitoringini amalga oshirish, sun'iy intellekt asosida anomal faoliyatni aniqlash hamda dasturiy ta'minotni muntazam yangilab borish muhim ahamiyatga ega. Shuningdek, navigatsiya ma'lumotlarini bir nechta mustaqil manbalar orqali tekshirish va kiberhujum sodir bo'lgan taqdirda tizimning xavfsiz rejimga avtomatik o'tishini ta'minlash dronlarning ishonchliligini oshiradi. Kelgusida dronlar, sun'iy intellekt va IoT texnologiyalarining yanada integratsiyalashuvi kiberxavfsizlikka qo'yiladigan talablarni kuchaytiradi. Shu sababli dron tizimlarini loyihalash bosqichidanoq "Security by Design" tamoyilini joriy etish, kiberhujumlarni oldindan aniqlash va ularga avtomatik javob qaytaruvchi intellektual himoya mexanizmlarini ishlab chiqish muhim istiqbolli yo'nalish hisoblanadi. Natijada innovatsion kiberxavfsizlik yechimlarini kompleks

qo'llash dronlarning maxfiyligi, yaxlitligi, mavjudligi va boshqaruv xavfsizligini ta'minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasi Prezidentining 2018-yil 29-martdagi PQ-3639-son "Iqtisodiyot tarmoqlarida fuqaro aviatsiyasining uchuvchisiz uchish apparatlaridan maqsadli va samarali foydalanish chora-tadbirlari to'g'risida"gi qarori. URL: <https://lex.uz/uz/acts/-4884433>.
2. O'zbekiston Respublikasi Prezidentining 2020-yil 15-iyundagi PF-6007-son "O'zbekiston Respublikasining axborot tizimlari va resurslarini himoya qilish davlat tizimini joriy etish chora-tadbirlari to'g'risida"gi Farmoni.
3. O'zbekiston Respublikasi Prezidentining 2020-yil 15-iyundagi PQ-4751-son "O'zbekiston Respublikasida kiberxavfsizlikni ta'minlash tizimini yanada takomillashtirishga doir qo'shimcha chora-tadbirlar to'g'risida"gi qarori.
4. G'aniyev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi: darslik. – Toshkent: Fan va texnologiya, 2017. – 372 b. ISBN 978-9943-11-366-4.
5. Ullah H., Nair N.G., Moore A., Nugent C., Muschamp P., Cuevas M. 5G communication: An overview of vehicle-to-everything, drones, and healthcare use-cases // IEEE Access. – 2019. – Vol. 7. – P. 37251–37268.
6. Westerlund O., Asif R. Drone hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and privacy threats for the Internet-of-Things // 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS). – 2019. – P. 1–10.
7. Statista. Drone market statistics and forecasts. URL: <https://www.statista.com/> (murojaat sanasi va aniq grafik manbasini tekshirish tavsiya etiladi).