O‘ZBEKISTON RESPUBLIKASI ADLIYA VAZIRLIGI
X.SULAYMONOVA NOMIDAGI RESPUBLIKA SUD EKSPERTIZASI MARKAZI

ZARARLI DASTURLAR VA ULARDAN HIMOYALANISH YO'LLARI

(*Fuqarolar uchun qo‘llanma*)

Toshkent 2026

Mualliflar jamoasi: X. Sulaymonova nomidagi Respublika sud ekspertiza markazi Sud-kompyuter texnikaviy ekspertizasi bo‘limi boshlig‘i D.Sh. Ataniyazov, bo‘lim yetakchi eksperti J.Z. Abdukarimov, bo‘lim eksperti D.R.Eshpo‘latov

Ushbu qo‘llanma Zararli dasturlar va ulardan himoyalanish yo'llari bo‘yicha fuqarolar tomonidan foydalanish uchun tayyorlangan.

KIRISH

Bugungi kunda jahon miqyosida axborot texnologiyalari jadal sur'atlar bilan rivojlanmoqda. Internetga ulanish tobora kengayib, milliardlab qurilmalar global tarmoqqa qo'shilmoqda. Biroq bu jarayon bilan bir qatorda, kiber tahdidlar ham misli ko'rilmagan darajada oshib bormoqda. Zararli dasturlar (malware) bu tahdidlarning eng tarqalgan va eng xavfli turlaridan birini tashkil etadi.

GLOBAL STATISTIKA — 2025-2026 YIL MA'LUMOTLARI

(*Symantec, Kaspersky va NIST ma'lumotlariga ko'ra: Har kuni dunyoda 450,000+ yangi zararli dastur namunasi aniqlanadi. 2025-yilda kiberjinoyatlar iqtisodiyotga yetkazgan zarar 8 trillion AQSh dollaridan oshdi. O'rta Osiyo mintaqasida kiberataklarning 62%i zararli dasturlar orqali amalga oshirildi. O'zbekistonda 2024-2025 yillarda kiberhujumlar soni 340%ga oshdi.*)

Zararli dasturlar nafaqat shaxsiy foydalanuvchilarga, balki davlat muassasalari, tijorat tashkilotlari, moliya institutlari va kritik infratuzilmalarga ham katta zarar yetkazmoqda. Milliy xavfsizlik, iqtisodiy barqarorlik va fuqarolarning shaxsiy ma'lumotlarini himoya qilish masalalari tobora muhim ahamiyat kasb etmoqda.

Muammo	Ko'rsatkich (2026)
Har sekundda yangi zararli dastur	**~5.2 ta namuna**
Ransomware hujumlari o'sishi (2023-2025)	**+127%**
O'rtacha zarar (korporativ sektor, 1 hujum)	**$4.45 million**
Jahon bo'yicha zararli dastur bilan yuqtirish	**Har 39 sekundda 1 hujum**
O'zbekistonda axborot xavfsizligi tahdidlari	**340% o'sish (2025)**

Zararli dasturlarning turlari

Zararli dasturlar (malware) — kompyuter, telefon, server va tarmoq qurilmalariga zarar yetkazish, ma’lumotlarni o‘g‘irlash yoki foydalanuvchini kuzatish maqsadida yaratilgan dasturiy vositalardir. Ular axborot xavfsizligiga katta tahdid soladi va kiberjinoyatchilar tomonidan keng qo‘llaniladi. Zararli dasturlar bir necha turlarga bo‘linadi. Virus eng mashhur turlaridan biri bo‘lib, boshqa fayllarga yopishib tarqaladi va tizim faoliyatini buzadi. Worm (qurt) esa mustaqil ravishda tarmoq orqali tarqalib, kompyuterlarni zararlaydi. Trojan dasturlari foydali dastur ko‘rinishida yashirinib, foydalanuvchini aldash orqali tizimga kiradi hamda maxfiy ma’lumotlarni o‘g‘irlaydi. Ransomware fayllarni shifrlab, ularni qayta ochish uchun pul talab qiladi. Spyware foydalanuvchini yashirin kuzatadi, keylogger esa klaviaturada terilgan ma’lumotlarni yozib boradi. Rootkit tizim ichida yashirinib

ishlaydi va zararli faoliyatni aniqlashni qiyinlashtiradi. Botnet esa bir nechta zararlangan qurilmalarni bitta markazdan boshqarishga imkon beradi. Zararli dasturlar email, internet, soxta saytlar, pirat dasturlar va fleshka orqali tarqaladi. Ulardan himoyalanish uchun antivirus dasturlaridan foydalanish, tizimni muntazam yangilash, noma’lum fayllarni ochmaslik va kuchli parollardan foydalanish zarur. Zararli dasturlar nafaqat oddiy foydalanuvchilarga, balki davlat tashkilotlari va korxonalarga ham katta iqtisodiy va axborot xavfi tug‘diradi.

Tur / Nomi	Tavsif	Xavf darajasi	Tarqalish %
Virus	Fayllarga yopishib, foydalanuvchi harakati bilan tarqaladigan o'z-o'zini ko'paytiradigan kod	**Yuqori**	**17.4%**
Troyan (Trojan Horse)	Foydali dastur niqobi ostida yashiringan, orqa eshik ochuvchi zararli dastur	**Juda Yuqori**	**22.1%**
Ransomware	Fayllarni shifrlaydi va to'lov talab qiladi; eng tez o'suvchi tahdid	**Kritik**	**18.6%**
Spyware	Foydalanuvchi ma'lumotlarini yashirin ravishda to'playdi va uzatadi	**Yuqori**	**12.3%**
Worm (Qurt)	Tarmoq orqali avtomatik tarqaladigan, fayllarni zararlaydi	**O'rta-Yuqori**	**9.8%**
Rootkit	Operatsion tizim darajasida yashirinadi, antivirus uchun ko'rinmas bo'ladi	**Kritik**	**6.2%**
Adware	Ko'rsatilmagan reklamalar ko'rsatadi, maxfiylikni buzadi	**Past-O'rta**	**8.4%**
Botnet	Masofadan boshqariladigan zombi tarmoqlari, DDoS hujumlar uchun ishlatiladi	**Yuqori**	**5.2%**

Kompyuter viruslari — bu o'z kodini boshqa fayllarga yoki dasturlarga ko'chirib, ularni zararlash qobiliyatiga ega bo'lgan zararli dasturlardir. Ular odatda ijro etiladigan fayllar (.exe, .com), Microsoft Office hujjatlari yoki yuklash sektorlari (boot sector) orqali tarqaladi.

- Fayl viruslari: .exe va .com fayllarini zararlaydi (masalan, CIH/Chernobyl virusi)
- Makro viruslar: Word, Excel kabi Office hujjatlariga joylashadi (masalan, Melissa)
- Boot sektori viruslari: Diskni yuklash sektorini zararlaydi (masalan, Michelangelo)

- Polimorf viruslar: Har safar o'z kodini o'zgartirib antivirus skanerlarini aldaydi
- Metamorf viruslar: Butun kodini qayta yozib, imzoni to'liq o'zgartiradi

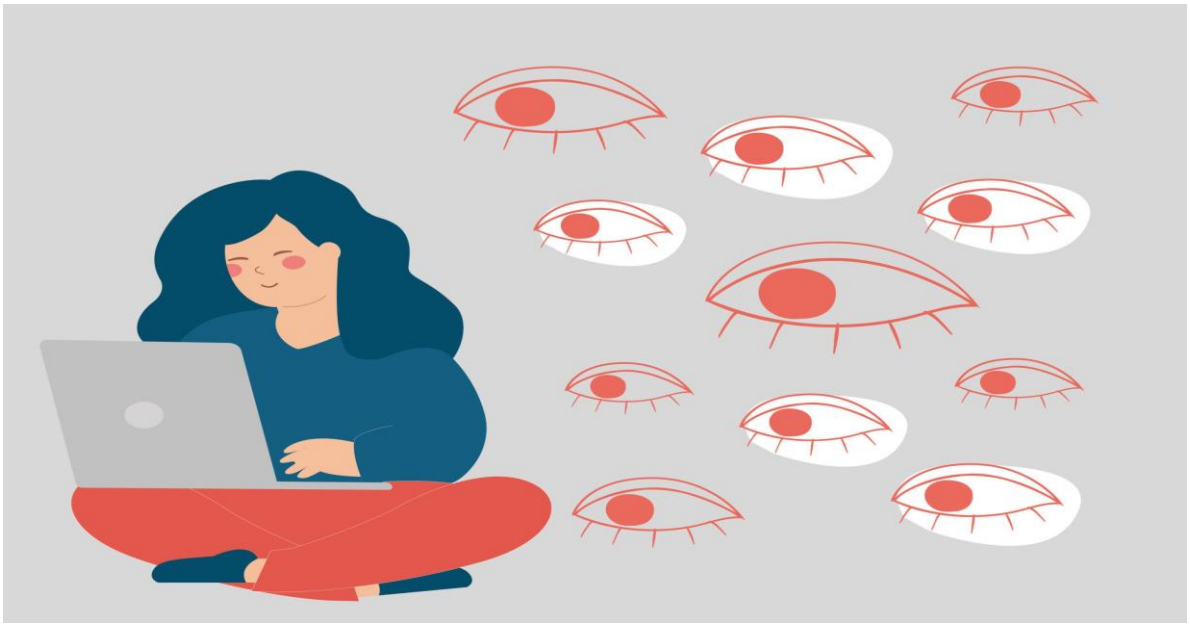
Troyanlar — foydalanuvchilarni aldash uchun qonuniy dastur ko'rinishida tarqatiladigan zararli dasturlar. Ular o'zini ko'paytirmaydi, ammo tizimga o'rnatilgandan so'ng xakerlarga orqa eshik (backdoor) ochadi, maxfiy ma'lumotlarni o'g'irlaydi yoki tizimni buzadi. MITRE ATT&CK ma'lumotlariga ko'ra, troyanlar barcha kiber hujumlarning 22.1%ini tashkil etadi.

- Remote Access Trojan (RAT): Masofadan to'liq boshqaruv imkonini beradi
- Banking Trojan: Internet-banking va to'lov tizimlarini nishonga oladi (Zeus, Emotet)
- Downloader Trojan: Boshqa zararli dasturlarni yuklab o'rnatadi
- Infostealer: Parollar, kredit karta ma'lumotlari va boshqa shaxsiy axborotlarni o'g'irlaydi

Ransomware 2025-yilda eng ko'p zarar yetkazgan zararli dastur turi bo'lib, global zarar 20 milliard dollardan oshdi. O'rtacha to'lov miqdori: $1.54 million (korporativ sektor). Fayllar tiklanishiga kafolat: Faqat 65% hollarda to'lovdan keyin fayllar qaytariladi. Hujumdan keyin o'rtacha tiklash vaqti: 21 kun. Ransomware fayllarni kuchli kriptografik algoritmlar (RSA-2048, AES-256) yordamida shifrlaydi va kalit uchun kriptovalyuta to'lovini talab qiladi. Eng mashhur namunalar: WannaCry (150+ mamlakat, $4 mlrd zarar), NotPetya, REvil, Conti, LockBit.

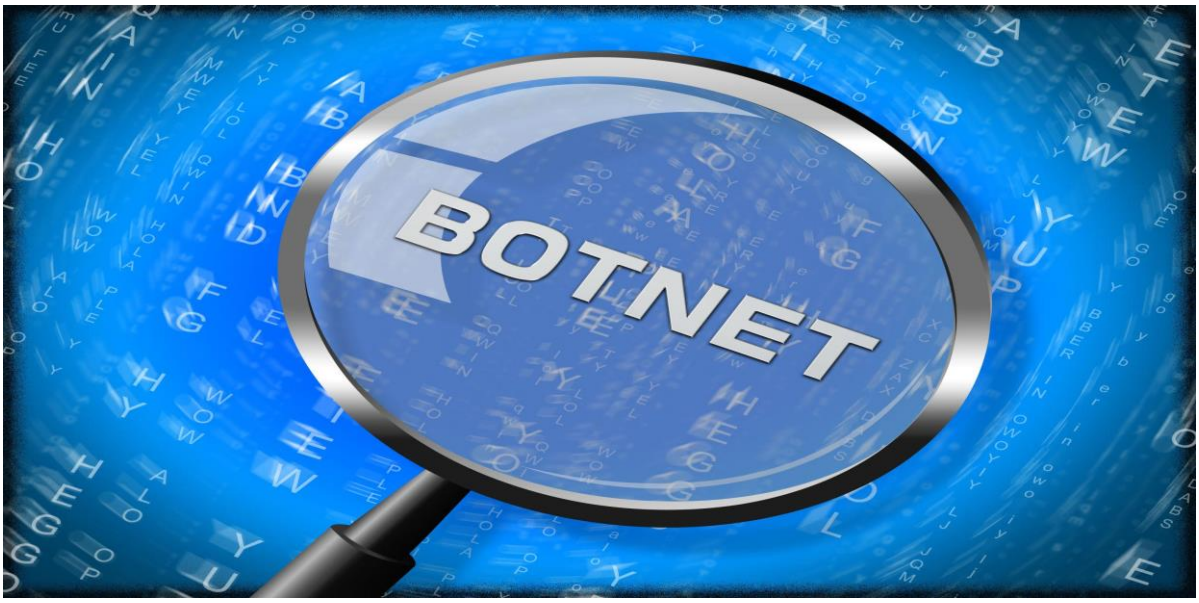
Josuslik dasturlari foydalanuvchi xabarsiz holda uning faoliyatini kuzatib boradi: tugmachalarni yozib oladi (keylogger), ekran tasvirini oladi, mikrofon va kamerani yoqadi, joylashuv ma'lumotlarini uzatadi va veb-brauzer tarixini o'g'irlaydi.

- Keylogger: Barcha klaviatura bosishlarini yozib saqlaydi
- Screen Capture: Muayyan intervallarda ekran suratini oladi
- GPS Tracker: Qurilma joylashuvini uzatadi
- Cookie Stealer: Autentifikatsiya ma'lumotlarini o'g'irlaydi



Rootkit — operatsion tizimning eng pastki darajalarida, ba'zan esa BIOS/UEFI darajasida yashirinib oladigan va o'zini hamda boshqa zararli dasturlarni antivirus vositalaridan berkitadigan eng xavfli malware turi. Ularni aniqlash va yo'qotish juda qiyin.

Botnet — xakerlar tomonidan masofadan boshqariladigan zararlangan qurilmalar (bot) tarmog'i. Botnetlar DDoS hujumlari (saytlarni ishdan chiqarish), spam yuborish, kriptovalyuta qazib olish va boshqa zararli faoliyat uchun ishlatiladi. Mirai botneti 2016-yilda 600,000+ qurilmani zararlagan va Amazon, Netflix, Twitter kabi yirik saytlarni ishdan chiqargan.



ZARARLI DASTURLARDAN KELADIGAN OQIBATLAR

Zararli dasturlar oqibatlari ko'lamiga ko'ra bir necha darajaga bo'linadi: shaxsiy (individual), tashkiliy (korporativ), milliy va xalqaro. Quyida har bir daraja bo'yicha batafsil tahlil keltirilgan.

Shaxsiy foydalanuvchilar uchun:

- Moliyaviy yo'qotishlar: Internet banking parollari o'g'irlanishi, kredit karta ma'lumotlari oshkor bo'lishi, to'lov dasturlari talabi
- Shaxsiy ma'lumotlar sizib chiqishi: Passport ma'lumotlari, tibbiy yozuvlar, shaxsiy fotosurat va videolar
- Identifikatsiya o'g'riligiga (identity theft) uchrash xavfi
- Qurilma ishlash qobiliyatining pasayishi yoki butunlay ishdan chiqishi
- Maxfiy suhbatlar va yozishmalar nazorat ostiga olinishi

Tashkilotlar va korxonalarga ta'siri:

(*KORPORATIV SEKTOR BO'YICHA GLOBAL STATISTIKA (IBM Security, 2025)Ma'lumotlar sizib chiqishi o'rtacha narxi: $4.45 million per instsident. Ransomware to'lovi + tiklash xarajatlari: $1.85 million (o'rtacha). Bitta kiberxujumdan keyin tashkilotning obro'si tiklash muddati: 1-3 yil. Ma'lumotlar sizib chiqishini aniqlash uchun o'rtacha vaqt: 207 kun*.)

- Biznes jarayonlarining to'xtab qolishi va mahsuldorlik yo'qotishi
- Mijozlar ma'lumotlari bazasining o'g'irlanishi va oshkor bo'lishi
- Huquqiy mas'uliyat va jarimalar (GDPR bo'yicha maksimal jarima: 20 million evro)
- Intellektual mulk va tijorat sirlari o'g'irlanishi
- Bank va moliya tizimlarida firibgarlik operatsiyalari
- Ishchilarning ish vaqti yo'qotishi va IT infratuzilma tiklash xarajatlari

Davlat darajasidagi kiberhujumlar — zamonaviy gibrid urushning ajralmas qismi bo'lib, ular kritik infratuzilmani (elektr tarmoqlari, suv ta'minoti, transport tizimlari, moliya tizimi) nishonga oladi.

- Kritik infratuzilma sabotaji: Ukraina (2015-2016) da elektr stansiyalariga hujum — 230,000 iste'molchi elektrsiz qoldi
- Davlat sirlarining oshkor bo'lishi va milliy xavfsizlikka tahdid
- Milliy iqtisodiyotga yetkaziladigan katta zarar (NotPetya — $10 mlrd global zarar)
- Saylov jarayonlariga aralashish va demokratik institutlarni zaiflashtirish

Aholining davlat tizimlariga ishonchini yo'qotishi.

Zararli dasturlar nafaqat texnik, balki ijtimoiy va psixologik oqibatlar ham keltirib chiqaradi. Kiberhujumga uchragan shaxslar stress, tashvish va ishonch yo'qotishi kabi ruhiy holatlarga duch keladi. Tashkilotlar esa o'z xodimlariga va mijozlariga nisbatan mas'uliyatdan kelib chiqadigan korporativ psixologik bosim bilan kurashishga majbur bo'ladi.

ZARARLI DASTURLARDAN HIMOYALANISH YO'LLARI

Zararli dasturlardan himoyalanish — ko'p qatlamli (multi-layered) yondashuv talab etadigan jarayon bo'lib, texnik vositalar, tashkiliy choralar va foydalanuvchi

xulq-atvorini o'zgartirish orqali amalga oshiriladi. NIST Cybersecurity Framework asosida himoya 5 yo'nalishda quriladi: Aniqlash (Identify), Himoya (Protect), Kuzatish (Detect), Javob berish (Respond) va Tiklash (Recover).

NIST Bosqich	Asosiy Faoliyat	Vositalar / Metodlar
1. Aniqlash	Aktivlar inventarizatsiyasi, risklar baholash	CMDB, Risk assessment tools
2. Himoya	Kirish nazorati, shifrlash, yangilanishlar	IAM, MFA, Patch management
3. Kuzatish	Anomaliyalarni real vaqtda aniqlash	SIEM, IDS/IPS, EDR
4. Javob berish	Instsidentlarga javob rejasi	IR Plan, SOAR platformalari
5. Tiklash	Zaxira nusxalardan tiklash, tahlil	BCP/DRP, Forensics

Zamonaviy antivirus yechimlari an'anaviy imzoga asoslangan aniqlash bilan birga, sun'iy intellekt va xulq-atvorga asoslangan (behavioral analysis) tahlil texnologiyalarini qo'llaydi. Dunyoning eng yaxshi reytingdagi antivirus yechimlari (AV-TEST, AV-Comparatives 2025):

- Bitdefender Total Security — Aniqlash darajasi: 99.9% (AV-TEST Oltin mukofoti)
- Kaspersky Premium — Aniqlash darajasi: 99.8%, ayniqsa ransomware himoyasi kuchli
- Norton 360 — Aniqlash darajasi: 99.7%, qo'shimcha VPN va dark web monitoring
- ESET NOD32 — Eng past resurs sarfi bilan yuqori aniqlash (99.5%)
- Malwarebytes Premium — Real-time himoya + zaxira tozalash vositasi sifatida samarali.

EDR — qurilmalar darajasida real vaqtda tahdidlarni aniqlash, tahlil qilish va ularga javob berish platformasi. An'anaviy antivirusdan farqli ravishda, EDR xulq-atvor tahlili va sun'iy intellekt asosida noma'lum tahdidlarni ham aniqlaydi. Yetakchi yechimlari: CrowdStrike Falcon, SentinelOne, Microsoft Defender for Endpoint.

Security Information and Event Management (SIEM) — barcha tizimlardan loglarni markazlashtirib to'playdi, anomaliyalarni aniqlaydi va kiberinstsidentlarga tezkor javob berish imkonini yaratadi. IBM QRadar, Splunk Enterprise Security, Microsoft Sentinel eng keng tarqalgan yechimlardir.

(***MUHIM STATISTIKA*** *Kiberataklarning 60%i ma'lum zaifliklardan foydalanadi. Bu zaifliklarning 85%iga patch (yamaq) chiqarilgan bo'ladi, ammo foydalanuvchilar uni o'rnatmagan bo'ladi. Shuning uchun tizimlarni muntazam yangilab turish eng muhim himoya chorasidir.*)

Kiberataklarning 95%iga yaqini inson omilidan foydalanadi — fishing, ijtimoiy muhandislik (social engineering), noto'g'ri konfiguratsiya va boshqalar. Texnik vositalar yetarli emas — insonni o'qitish ham shunday muhim.

YAKUNLOVCHI QISM — MAVZUNING DOLZARBLIGI

Axborot xavfsizligi sohasidagi mutaxassislarning yagona fikri shuki: kibertahdidlar insoniyat tarixidagi eng tez o'suvchi muammo bo'lib qoldi. Zararli dasturlar endi faqat alohida shaxslarga emas, balki butun davlatlar infratuzilmasiga, iqtisodiy tizimlarga va demokratik jarayonlarga tahdid solmoqda.

Sun'iy Intellekt (AI) asosidagi malware: Tezda moslashadigan, o'z-o'zini o'rgatadigan zararli dasturlar paydo bo'lmoqda. Deepfake hujumlari: Yolg'on audio/video orqali ijtimoiy muhandislik hujumlari keskin ortmoqda. IoT zaifliklari: 2030-yilga kelib 50 milliard ulanilgan qurilma kiberataklarning yangi maydoniga aylanadi. Post-kvant kriptografiya tahdidi: Kvant kompyuterlar mavjud shifrlash algoritmlarini buzishi mumkin. Supply Chain hujumlari: SolarWinds (2020) va Kaseya (2021) singari zanjir bo'ylab tarqaladigan hujumlar ko'paymoqda.

O'zbekiston Respublikasi uchun axborot xavfsizligi — milliy rivojlanish strategiyasining ajralmas qismidir. 2021-yilda qabul qilingan 'Yangi O'zbekiston' strategiyasi va 2022-yilgi 'Raqamli O'zbekiston 2030' dasturi davlat va xususiy sektor raqamlashtiriladigan ekan, kiberhimoya ham shu sur'atda rivojlanishi zarur.

Tafsiyalar:

Foydalanuvchi turi	Eng Muhim 3 Tavsiya	Zaruriy Vositalar
Oddiy foydalanuvchi	Antivirus, MFA yoqish, backup	Windows Defender, Authenticator App
Tashkilot xodimi	Fishing taniш, kuchli parol, VPN	Parol menejeri, korporativ VPN
IT mutaxassisi	EDR, SIEM, patch management	CrowdStrike/SentinelOne, Splunk
IT rahbariyat/CISO	Risk assessment, incident response, audit	ISO 27001, NIST CSF, Pen testing