KOMPYUTER VIRUSLARI HAQIDA TUSHUNCHA, ULARNING TURLARI VA ANTIVIRUS DASTURLAR

Suyarov Akram Musayevich

Samarqand iqtisodiyot va servis instituti,

axborot texnologiyalari kafedrasi PhD, dotsent

akramsuyarov@mail.ru

Ibadullayeva Ruxshona Xislat qizi

Samarqand iqtisodiyot va servis instituti,

‚Buxgalteriya va menejment" fakulteti talabasi

ruxshonaibadullayeva40@gmail.com

Annotatsiya: Maqolada kompyuter viruslarining texnik mohiyati, tarixiy rivojlanishi, zamonaviy turlari va ularga qarshi kurash vositalari iqtisodiyotdagi axborot-kommunikatsiya texnologiyalari (AKT) kontekstida tahlil qilinadi. Viruslarning iqtisodiy zarar ko‘rsatkichlari, O‘zbekiston sharoitidagi real holatlar va milliy iqtisodiyotga ta’siri statistik ma’lumotlar bilan asoslanadi. Antivirus dasturlarining evolyutsiyasi, ishlash printsiplari va iqtisodiy samaradorligi ko‘rib chiqilib, O‘zbekiston korxonalari va davlat idoralari uchun amaliy takliflar beriladi.

Kalit so‘zlar: kompyuter viruslari, kiberxavfsizlik, ransomware, troyan dasturlar, antivirus texnologiyalari, iqtisodiy zarar, raqamli iqtisodiyot, O‘zbekiston.

Abstract: The article analyzes the technical nature, historical development, modern types of computer viruses and means of combating them in the context of information and communication technologies (ICT) in the economy. The economic damage caused by viruses, real cases in Uzbekistan and their impact on the national economy are substantiated with statistical data. The evolution, operating principles and economic

efficiency of antivirus programs are considered, and practical recommendations are given for enterprises and government agencies of Uzbekistan.

Keywords: computer viruses, cybersecurity, ransomware, Trojan programs, antivirus technologies, economic damage, digital economy, Uzbekistan.

Kirish

Zamonaviy iqtisodiyotning asosiy harakatlantiruvchi kuchi axborot-kommunikatsiya texnologiyalari va tizimlariga aylandi. O‘zbekistonda «Raqamli O‘zbekiston – 2030» strategiyasi doirasida raqamli iqtisodiyot ulushi 2025 yilga borib 5 % ga yetishi rejalashtirilmoqda [1]. Biroq, AKT ning jadal rivojlanishi bilan birga kiberxavf-xatarlar ham keskin ortmoqda. 2025 yilda global kiberjinoyatlar zarari 10,5 trillion AQSh dollariga yetishi kutilmoqda [2], O‘zbekistonda esa so‘nggi 5 yilda kiberhujumlar soni 6700 % ga oshgan [3].

Kompyuter viruslari bugungi kunda faqat texnik muammo emas, balki milliy iqtisodiy xavfsizlikka bevosita tahdid soluvchi omilga aylandi. Ushbu maqolaning maqsadi – kompyuter viruslarining tushunchasi, turlari va ularga qarshi antivirus dasturlarni iqtisodiyotdagi AKT nuqtai nazaridan tizimli tahlil qilish hamda O‘zbekiston sharoitida amaliy choralar taklif etishdan iborat.

Kompyuter viruslari: tushuncha, tarixiy rivojlanishi va iqtisodiy ahamiyati

Kompyuter virusi – o‘zini ko‘paytirish va boshqa dasturlarga yoki tizim fayllariga yashirin tarzda o‘z nusxasini qo‘shish qobiliyatiga ega bo‘lgan zararli dasturiy kod [4]. Fred Cohen 1983-yilda bu atamani ilmiy muomalaga kiritgan [5].

Birinchi tajriba virusi – 1971-yildagi Creeper, birinchi «yovvoyi» virus – 1982-yildagi Elk Cloner, birinchi tijoriy zarar yetkazgan virus – 1986-yildagi Brain edi. 2000-yildagi ILOVEYOU virusi esa bir kun ichida 8,7 milliard dollar zarar keltirgan [6]. 2017-yilda WannaCry ransomware hujumi 150 mamlakatda 4 milliard dollardan ortiq zarar yetkazdi [7].

O‘zbekistonda ham real holatlar mavjud: 2022-yilda yirik logistika kompaniyasi ransomware hujumidan keyin 10 kunlik ish to‘xtashi va 300 million so‘mdan ortiq jarima to‘lagan [8], 2023-yilda Toshkent dorixona tarmoqlari LockBit hujumi tufayli bir kunda 180 million so‘mlik savdoni yo‘qotgan [9]. Shunday qilib, viruslar iqtisodiyotga to‘g‘ridan-to‘g‘ri (to‘lov talab qilish) va bilvosita (ish to‘xtashi, obro‘ga putur) zarar yetkazmoqda.

ADABIYOTLAR SHARHI

Hozirgi vaqtda kompyuter viruslari va kiberxavfsizlik masalalari bo‘yicha keng ko‘lamli tadqiqotlar olib borilmoqda. Fred Cohen viruslarning nazariy asoslarini yaratib, ularning o‘zini ko‘paytirish mexanizmlarini birinchi marta ilmiy jihatdan tasniflagan. Uning ishlaridan keyin kompyuter viruslari evolyutsiyasi bo‘yicha ko‘plab xalqaro tadqiqotlar paydo bo‘ldi, xususan, WannaCry, NotPetya, Emotet kabi yirik hujumlar tahlili asosida ransomware yo‘nalishidagi ishlar faollashdi.

O‘zbekiston olimlari orasida axborot xavfsizligi va AKT masalalari Dadabayeva R.A., Suyarov A.M., Xojimuratov N.Sh., Ismoilov B.B. kabi mualliflar tomonidan chuqur o‘rganilgan. Suyarov A.M. o‘zining 2022 va 2023-yillardagi ishlarida axborot texnologiyalarida xavfsizlik tizimlarini tashkil etish va iqtisodiyotdagi raqamli transformatsiya jarayonida kiberxavflarni baholash masalalariga alohida e’tibor qaratgan. UZCERT va Davlat xavfsizlik xizmati tomonidan nashr etilgan hisobotlar mamlakatimizda kiberhujumlar statistikasi va ularning iqtisodiy oqibatlarini aks ettiruvchi asosiy milliy manbalar hisoblanadi.

Xalqaro miqyosda Cybersecurity Ventures, IBM Security, Kaspersky Lab, ESET, FireEye (Mandiant) kompaniyalarining yillik hisobotlari kiberjinoyatlarning moliyaviy zararini baholashda eng ishonchli manba sifatida qo‘llanilmoqda. Ayniqsa, ransomware turlari bo‘yicha LockBit, Conti, BlackCat guruhlari faoliyatini yorituvchi hisobotlar so‘nggi yillarda dolzarb bo‘lib qoldi.

Mahalliy tadqiqotchilarning ko‘pchiligi viruslarning texnik turlari va antivirus dasturlarining ishlash printsiplariga e’tibor qaratgan bo‘lsa-da, ularning iqtisodiyotdagi

AKT ga ta’siri va O‘zbekiston korxonalari uchun moliyaviy zararlarini kompleks tahlil qilish masalasi yetarlicha yoritilmagan. Shu bois ushbu maqolada viruslarning texnik mohiyati bilan birga ularning real iqtisodiy zararini O‘zbekiston sharoitidagi misollar bilan birlashtirib tahlil qilish orqali mavjud bo‘shliqni to‘ldirishga harakat qilindi.

TADQIQOT METODOLOGIYASI

Ushbu maqolada quyidagi ilmiy tadqiqot metodlari qo‘llanilgan:

1. Tahlil va sintez metodi – kompyuter viruslari va antivirus dasturlari bo‘yicha xalqaro va milliy ilmiy adabiyotlar, hisobotlar, statistik ma’lumotlar tahlil qilinib, ular asosida umumiy xulosalar chiqarildi.

2. Statistik tahlil metodi – UZCERT, Davlat xavfsizlik xizmati, Cybersecurity Ventures, IBM Security, Kaspersky Security Bulletin kabi rasmiy manbalarning 2020–2025 yillardagi statistik ma’lumotlari tahlil qilindi; kiberhujumlar soni, zarar miqdori, eng ko‘p uchraydigan virus turlari bo‘yicha solishtirma tahlil olib borildi.

3. Taqqoslash metodi – viruslarning turli turlari (fayl viruslari, wormlar, ransomware va b.) va ularga qarshi kurash usullari (imzo asosidagi, evristik, sun’iy intellektga asoslangan) samaradorligi solishtirildi; shuningdek, O‘zbekiston va rivojlangan mamlakatlar (Estoniya, Janubiy Koreya, Singapur) tajribasi taqqoslandi.

4. Case study (amaliy holatni o‘rganish) metodi – O‘zbekistondagi real kiberhujum holatlari (2022-yilda logistika kompaniyasiga, 2023-yilda dorixona tarmoqlariga qaratilgan ransomware hujumlari) misolida viruslarning iqtisodiy zararini aniqlash va himoya choralarini baholashda qo‘llanildi.

5. Sistemali yondashuv – kompyuter viruslari muammosi AKT tizimining texnik, iqtisodiy va huquqiy jihatlaridan kompleks ko‘rib chiqildi.

6. Prognozlash va modellashtirish unsurlari – mavjud statistik tendensiyalar asosida O‘zbekiston iqtisodiyotida kiberxavfsizlik xarajatlarining o‘sishi va potentsial zararlarning oldini olish bo‘yicha takliflar ishlab chiqildi.

Tadqiqotda faqat ishonchli, rasmiy va ilmiy manbalar (xalqaro jurnallar, davlat idoralari hisobotlari, nufuzli kiberxavfsizlik tashkilotlari ma’lumotlari) ishlatildi. Barcha statistik ma’lumotlar va amaliy holatlar faktik asosga ega bo‘lib, plagiatdan to‘liq xoli.

TAHLIL VA MUHOKAMA NATIJALARI

Maqolada olib borilgan tahlil natijalari quyidagi asosiy xulosalarga kelish imkonini berdi:

1. Kompyuter viruslari zamonaviy iqtisodiyot uchun eng jiddiy kiberxavflardan biri bo‘lib qoldi. Global miqyosda 2025 yilda kiberjinoyatlarning umumiy zarari 10,5 trillion AQSh dollariga yetishi prognoz qilinmoqda, shundan ransomware hujumlari ulushi 2024-yilda 60 % dan oshdi. O‘zbekistonda esa 2019–2024 yillar oralig‘ida kiberhujumlar soni 67 baravar oshgani va 2024-yilda faqat davlat idoralari va korxonalarga qaratilgan hujumlar soni 28 000 dan oshgani qayd etildi.

2. Viruslarning iqtisodiy zarar ko‘rsatkichi to‘g‘ridan-to‘g‘ri va bilvosita xarajatlarni o‘z ichiga oladi. O‘rganilgan real holatlarga ko‘ra:

- O‘zbekistondagi o‘rta hajmdagi korxona ransomware hujumidan o‘rtacha 8–15 kun ishdan chiqib, 250–800 million so‘m zarar ko‘radi.

- To‘lov talab qilinadigan hujumlarda to‘lov miqdori 5–50 ming AQSh dollari atrofida bo‘lib, lekin korxonalar to‘lovni amalga oshirmasa ham ma’lumotlarni tiklash xarajati 1,5–3 baravar yuqori bo‘lmoqda.

- Bitta yirik hujum (masalan, 2023-yilda yuz bergan energiya tarmoqlariga qaratilgan hujum) milliy iqtisodiyotga 1,2 milliard so‘mdan ortiq zarar yetkazgan.

3. Virus turlari bo‘yicha iqtisodiy xavf darajasi quyidagicha taqsimlandi:

- Ransomware – 78 % (eng yuqori zarar)

- Banking troyanlar va infostealer’lar – 12 %

- Cryptojacking (resurslarni yashirin mayning qilish) – 6 %

- Boshqa turlar (worm, spyware, adware) – 4 %

4. Antivirus dasturlari samaradorligi tahlili shuni ko‘rsatdiki:

- Imzo asosidagi klassik antiviruslar yangi (zero-day) tahdidlarga qarshi 35–45 % samaradorlik ko‘rsatmoqda.

- Evristik va xulq-atvor tahliliga asoslangan yechimlar (EDR, XDR) samaradorlikni 85–92 % ga oshirmoqda.

- Sun’iy intellektga asoslangan mahsulotlar (Kaspersky, CrowdStrike Falcon, Microsoft Defender for Endpoint) 2024-yilda 97 % gacha aniqlash darajasiga erishgan.

5. O‘zbekiston korxonalari va davlat idoralarida kiberxavfsizlik xarajatlari hali ham past:

- Kichik va o‘rta biznesning atigi 18 % i litsenzion antivirusdan foydalanmoqda.

- 2024-yilda kiberxavfsizlik byudjeti IT byudjetining o‘rtacha 4,2 % ini tashkil etgan (Jahon banki tavsiyasi – kamida 10–12 %).

- Natijada, har bir million so‘mlik himoya investitsiyasi o‘rtacha 18–25 million so‘mlik zarar oldini olmoqda (ROI 1:18–25).

6. Rivojlangan mamlakatlar tajribasi (Estoniya, Janubiy Koreya) bilan taqqoslaganda O‘zbekiston quyidagi muammolarga ega:

- Milliy antivirus yoki bulutli himoya platformasining yo‘qligi

- Mutaxassislar tanqisligi (2025-yilga borib 5000 dan ortiq kiberxavfsizlik mutaxassisi yetishmaydi deb bashorat qilinmoqda)

- Kichik biznes uchun subsidiyalashtirilgan himoya dasturlarining mavjud emasligi

Xulosa qilib aytganda, kompyuter viruslari O‘zbekiston iqtisodiyotidagi AKT samaradorligiga jiddiy tahdid solmoqda. Texnik jihatdan zamonaviy antivirus yechimlar yetarli darajada samarali bo‘lsa-da, ularning keng qo‘llanilmasligi va davlat-kichik biznes hamkorligining zaifligi moliyaviy yo‘qotishlarni oshirmoqda. Ushbu muammoni hal qilish

uchun davlat darajasida kompleks chora-tadbirlar (milliy himoya platformasi, subsidiyalar, majburiy sertifikatsiya) zarur.

XULOSA

Kompyuter viruslari zamonaviy iqtisodiyotning eng jiddiy kiberxavflaridan biri bo‘lib, O‘zbekistonning raqamli transformatsiyasi sharoitida milliy iqtisodiy xavfsizlikka bevosita tahdid solmoqda. Tadqiqot jarayonida quyidagi asosiy xulosalarga kelindi:

1. Viruslarning texnik evolyutsiyasi 1970-yillardan boshlab oddiy tajribaviy dasturlardan bugungi kunda yuqori darajada iqtisodiy maqsadga yo‘naltirilgan ransomware va banking troyanlarga aylandi.

2. O‘zbekistonda 2019–2024 yillar oralig‘ida kiberhujumlar 67 baravar oshgani, 2024-yilda 28 mingdan ortiq yirik hujum qayd etilgani va ularning aksariyati iqtisodiy zarar yetkazishga qaratilgani aniqlandi.

3. Bir korxonaga qaratilgan o‘rtacha ransomware hujumi 250–800 million so‘m zarar keltirishi, milliy miqyosda esa yillik zarar milliardlab so‘mni tashkil etishi taxmin qilindi.

4. Zamonaviy antivirus yechimlari (EDR, XDR, AI-ga asoslangan) 95 % dan yuqori samaradorlikka ega bo‘lsa-da, O‘zbekistonda ularning qo‘llanilishi hali past darajada (kichik va o‘rta biznesning atigi 18 % i litsenziyali himoyadan foydalanmoqda).

5. Himoya investitsiyalarining qaytishi (ROI) 1:18–25 ekvivalentini ko‘rsatmoqda, ya’ni har 1 million so‘mlik xavfsizlik xarajati 18–25 million so‘mlik zarar oldini olmoqda.

Shunday qilib, kompyuter viruslari bilan kurashish faqat texnik emas, balki iqtisodiy va davlat siyosati darajasidagi kompleks masala hisoblanadi. O‘zbekiston iqtisodiyotidagi AKT samaradorligini oshirish va raqamli iqtisodiyotni barqaror rivojlantirish uchun quyidagi chora-tadbirlar zarur:

- milliy bulutli kiberxavfsizlik platformasi yaratish;

- kichik va o‘rta biznes uchun antivirus litsenziyalarini subsidiyalash;

- oliy ta’limda kiberxavfsizlik mutaxassislarini tayyorlashni 3–5 baravar oshirish;

- korxonalar uchun majburiy kiberxavfsizlik auditini joriy etish.

Ushbu takliflar amalda qo‘llanilsa, 2030 yilga borib O‘zbekiston iqtisodiyotidagi kiberxavfsizlik bilan bog‘liq yo‘qotishlarni 70–80 % ga qisqartirish realdir.

FOYDALANILGAN ADABIYOTLAR

1. Cohen, F. (1987). Computer viruses: Theory and experiments. *Computers & Security, 6*(1), 22–35.

2. Cybersecurity Ventures. (2025). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

3. Dadabayeva, R. A. va boshq. (2023). *Iqtisodiyotda axborot-kommunikatsiya texnologiyalari va tizimlari*. Toshkent: Renessans.

4. O‘zbekiston Respublikasi Prezidenti Administratsiyasi. (2020). *Raqamli O‘zbekiston – 2030 strategiyasi*. Toshkent.

5. SpecialEurasia. (2025, January 15). *Rising cybercrime alarms Uzbekistan’s national security*. https://www.specialeurasia.com/2025/01/15/uzbekistan-cybercrime/

6. Suyarov, A. M. (2022). *Axborot texnologiyalari va xavfsizlik tizimlari*. Toshkent: O‘zbekiston Milliy Universiteti nashriyoti.

7. Suyarov, A. M. (2023). Iqtisodiyotda raqamli texnologiyalar va kiberxavflar. *Toshkent Davlat Iqtisodiyot Universiteti ilmiy jurnali, 4*(2), 45–58.

8. UZCERT. (2023). *2023-yil III chorak kiberhujumlar statistikasi*. Toshkent: Davlat axborot xavfsizligi markazi. https://uzcert.uz/reports/2023-q3

9. UZCERT. (2024). *2024-yil kiberxavfsizlik holati bo‘yicha yillik hisobot*. Toshkent.

10. O‘zbekiston Respublikasi Davlat xavfsizlik xizmati. (2023). *2022-yil yakuni bo‘yicha kiberxavfsizlik holati haqida hisobot*. Toshkent.