Date: 19th October-2025

KOMPYUTER VIRUSLARI VA ULARNING ISHLASH MEXANIZMLARI

Yorqulov Shohinur Baxtiyor o‘g‘li
Mustafoyeva Anora Ulug‘bek qizi
Sharifjonova Durdona Malikjon qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalar unversiteti Samarqand filiali talabalari

Annotatsiya: Ushbu maqolada kompyuter viruslari, ularning kelib chiqish sabablari va ishlash mexanizmlari haqida so‘z yuritiladi. Maqolada viruslarning turlari, ular qanday qilib tizimlarga kirib borishi va foydalanuvchi ma’lumotlariga zarar yetkazishi yoritilgan. Shuningdek, zararli dasturlarni aniqlash va oldini olish usullari, antivirus dasturlarining ahamiyati ham tahlil qilingan. Maqola kompyuter xavfsizligini ta’minlashda foydalanuvchining roli va zamonaviy himoya texnologiyalarining o‘rni haqida tushuncha beradi.

Аннотация: В данной статье рассматриваются компьютерные вирусы, причины их возникновения и механизмы работы. Описываются основные типы вирусов, способы их проникновения в систему и нанесения вреда пользовательским данным. Также анализируются методы обнаружения и предотвращения вредоносных программ, а также значение антивирусных средств. Статья направлена на формирование представления о роли пользователя и современных технологий защиты в обеспечении компьютерной безопасности.

Annotation: This article discusses computer viruses, their causes, and mechanisms of operation. It describes the main types of viruses, how they infiltrate computer systems, and the ways they damage user data. The article also analyzes methods for detecting and preventing malware, emphasizing the importance of antivirus software. It aims to highlight the role of users and modern security technologies in maintaining computer safety and protecting digital information.

Hozirgi kunda kompyuterlar va internet hayotimizning ajralmas qismiga aylangan. Shu bilan birga, raqamli texnologiyalar bilan birga turli xavf-xatarlar ham paydo bo‘lmoqda. Kompyuter viruslari — shunday xavf-xatarlardan biri bo‘lib, ular tizimga kirib foydalanuvchi ma’lumotlariga zarar yetkazishi, dasturlarni ishlamas qilishi yoki ma’lumotlarni yo‘qotishi mumkin.Kompyuter viruslari dastlab 1970–1980 yillarda paydo bo‘lgan bo‘lsa-da, bugungi kunda ular turli shakllarda — fayl viruslari, makro viruslar, troyanlar va ransomware kabi ko‘rinishlarda uchraydi. Viruslar tizimga kirish usullari va ishlash mexanizmlari jihatidan farq qilsa-da, ularning asosiy maqsadi — kompyuter tizimiga zarar yetkazish yoki foydalanuvchidan ma’lumotlarni yashirin tarzda olishdir.

Ushbu maqolaning maqsadi — kompyuter viruslarining turlari, ularning ishlash prinsiplari va oldini olish usullari haqida tushuncha berish, shuningdek, zamonaviy antivirus vositalarining ahamiyatini yoritishdir.

International Conferences
Open Access | Scientific Online | Conference Proceedings
INTERNATIONAL CONFERENCES OF PRACTICE

International Conferences
Open Access | Scientific Online | Conference Proceedings
INTERNATIONAL CONFERENCES OF PRACTICE

Kompyuter viruslari — bu kompyuter tizimiga kirib, dasturlar, fayllar yoki tizim jarayonlariga zarar yetkazadigan dasturiy kodlar. Ular o‘zini ko‘paytirish xususiyatiga ega va foydalanuvchining roziligi yoki bexosdan ularni ishga tushirishi orqali tarqaladi.

Viruslar dastlab 1970–1980 yillarda paydo bo‘lgan bo‘lsa-da, internet va global tarmoqlar rivojlanishi bilan ular tez tarqaladigan xavfli tahdidga aylandi. Ilk mashhur viruslardan biri “Brain” bo‘lib, 1986-yilda IBM PC kompyuterlarida tarqalgan. Shundan keyin viruslar turli shakllarda rivojlandi va ularning murakkabligi oshdi.

Kompyuter viruslarining turlari

Viruslar turli usul va maqsadga ega bo‘lishi mumkin. Asosiy turlari quyidagilardan iborat:

Fayl viruslari — dastur fayllariga biriktiriladi va ular ishga tushganda aktivlashadi.

Makro viruslar — hujjat va ofis fayllarida yashirinadi, masalan, Word yoki Excel fayllari.

Troyanlar — foydalanuvchiga foydali dastur sifatida ko‘rinadi, ammo yashirin zarar yetkazadi.

Ransomware (shifrlash viruslari) — foydalanuvchi ma’lumotlarini shifrlab, pul evaziga ochilishini talab qiladi.

Worm (qurtlar) — tizimlar orqali o‘zini ko‘paytiradi va tarmoq bo‘ylab tarqaladi.

Ishlash mexanizmi

Kompyuter viruslari ishlash jarayonida quyidagi bosqichlarni bajaradi:

1. Kirish — foydalanuvchi dasturini ishga tushirishi yoki zararli faylni yuklashi orqali tizimga kiradi.

2. Ko‘payish — o‘zi bilan birga boshqa fayllarga yoki tizimga nusxa ko‘chiradi.

3. Faollashish — ma’lum shartlar (sana, dastur ishga tushishi yoki ma’lum buyruq) bajarilganda virus aktivlashadi.

4. Zarar yetkazish — fayllarni o‘chirish, ma’lumotlarni shifrlash, tizimni sekinlashtirish yoki foydalanuvchi ma’lumotlarini o‘g‘irlash.

Himoya va profilaktika usullari

Kompyuter viruslaridan himoyalanishda bir nechta samarali usullar mavjud:

Antivirus dasturlari — viruslarni aniqlash, bloklash va yo‘q qilish.

Tizim yangilanishlari — operatsion tizim va dasturiy ta’minotni muntazam yangilash.

Xavfsiz foydalanish qoidalari — noma’lum fayllarni yuklamaslik, shubhali elektron pochtalarga e’tibor bermaslik.

Zaxira nusxalar (backup) — muhim ma’lumotlarni alohida saqlash orqali yo‘qotish xavfini kamaytirish.

Tarmoq monitoringi — tarmoqdagi shubhali faoliyatlarni kuzatish va bloklash.

Zamonaviy tendensiyalar

Bugungi kunda kompyuter viruslari yanada murakkablashmoqda. Sun’iy intellekt va mashina o‘rganish texnologiyalari yordamida viruslar tizimni chetlab o‘tish, foydalanuvchi xatti-harakatlarini tahlil qilish va o‘zini yashirish qobiliyatiga ega

bo‘lmoqda. Shu sababli, antivirus dasturlari va xavfsizlik tizimlari ham shu texnologiyalar yordamida doimiy yangilanib, viruslarni aniqlash va bloklash imkonini oshirmoqda.

Kompyuter virusi — internet orqali suzib yuradigan, kompyuter programmalarini yo‘q qilib, ishlamay qolishiga sabab bo‘ladigan programma. Hozirgi kunda bu viruslarga qarshi Antiviruslar ishlab chiqarilgan. Viruslar haqida dastlabki ma’lumotlar amerikalik T. J. Raynning 1977-yilgi fantastik asarida uchraydi. Bu asarda 7000 kompyuter virusdan zararlanganligi haqida so‘z boradi. Virus ham tuzilishiga ko‘ra dastur, lekin zararli. Hozirda viruslar juda keng klassifikatsiya ega. Ular keng qamrovda faoliyat olib bormoqda. Masalan: Kasperskiy antivirusi 1,5 million virusni aniqlay oladi (2009-yil ma’lumoti). Dunyodagi birinchi virus dasturi 1988-yili Karnell Universiteti aspiranti Robert Moris(kichik) tomonidan Internet tarmog‘iga joylashtirilgan. Bu virus o‘z faoliyatini Unix operatsion tizimi xato-kamchiliklaridan g‘arazli maqsadlarda foydalanish bilan amalga oshirgan. Robert Moris tuzgan virus juda katta ko‘lamli zarar keltirdi. Robert moris esa uzoq muddatli qamoq jazosiga mahkum etildi, lekin uning nomi bir umrga tarixda qoldi.

Kompyuter virusi — EHM ning xavfli „dasturi“. Kompyuter egasini ogoxlantirmay va uning istagiga qarshi uning dasturiga „joylashtiriladi“ va zaryadlangan faylni navbatdagi qo‘yishda ko‘payadi. Kompyuter virusi kompyuterning risoladagi ish me’yorini buzadi, ma’lumotlarni o‘chirib yuboradi, displey (monitor) ekranidagi tasvirni buzadi, hisoblash jarayonini sekinlashtiradi. Kompyuter virusi dasturini ishlab chiquvchilar 20-asr 80-yillari boshida AQShda paydo bo‘ldi, keyin dunyoning barcha mamlakatlariga tarqaldi. Kompyuter virusiga qarshi kurashish uchun maxsus dasturlar ishlab chiqiladi.

Viruslar kompyuterlarda o'zini har xil tutadi. Ba'zi birlari kompyuteringizni kerakmas fayllar bilan to'latsa, yana ba'zilari operativ xotirani ko'p qismini ishlatib, kompyuteringizni qotirib qo'yadi, viruslarning bir qismi esa, kerakli fayllaringizni yoki tizim fayllarini o'chirib sizga zarar yetkazadi. Shulardan saqlanish uchun viruslarning turini bilib olish lozim, ya'ni qaysi virus nima ish qiladi va bundan saqlanish o'z o'zidan kelib chiqadi. Quyida ularning turlari keltirilgan(turlari ref.uz dan olindi):

Troyanlar (Trojan Horses) – Qadimgi yunonlarning **Troya**ga yurishlari davrida qo'llagan hiylasi, ya'ni troyaliklarni otga ishqiboz ekanligidan foydalanib, ularga **katta yog'och ot** sovg'a qilishlari va bu otning troyaliklar mag'lubiyatiga olib kelishi voqeasidan olingan nom. Hozirda troya oti iborasi "**hosiyatsiz sovg'a**" degan ma'noni bildiradi. Kompyuter va internet dunyosida troyanlar "**hosiyatsiz dastur**" deb nomlanishi maqsadga muvofiq. Troyanlar odatda internet orqali tarqaladi. Troyanlar kompyuteringizga o'rnashib olib, dastlab foydali dastur sifatida o'zlarini tanishtiradilar, lekin ularning asl vazifasi foydalanuvchiga noma'lumligicha qoladi. Yashirin ravishda ular o'zlarining yaratuvchisi (cracker – yovuz haker) tomonidan belgilangan harakatlarni amalga oshiradilar. Troyanlar o'z-o'zidan ko'paymaydi, lekin kompyuteringiz xavfsizligini ishdan chiqaradi: troyanlar kerakli ma'lumotlaringizni o'chirib yuborishi, kompyuterdagi ma'lumotlarni kerakli manzilga jo'natishi, kompyuteringizga internetdan ruxsatsiz ulanishlarni amalga oshirishi mumkin.

International Conferences
Open Access | Scientific Online | Conference Proceedings
INTERNATIONAL CONFERENCES OF PRACTICE

International Conferences
Open Access | Scientific Online | Conference Proceedings
INTERNATIONAL CONFERENCES OF PRACTICE

Chuvalchang viruslar (Worms) – Chuvalchang viruslar o'z nomiga mos ravishda juda tez o'z-o'zidan ko'payadigan viruslardir. Odatda bu viruslar internet yo'li intranet tarmoqlari orasida tarqaladi. Tarqalish usuli sifatida elektron xatlar yoki boshqa tez tarqaluvchi mexanizmlardan foydalanadi. Ular haqiqatan ham kompyuteringizdagi ma'lumotlar va kompyuter xavfsizligiga katta ziyon yetkazadi. Chuvalchang viruslar operatsion tizimning nozik joylaridan foydalanish yoki zararlangan elektron xatlarni ochish yo'li bilan kompyuteringizga o'rnashib olishi mumkin.

Boot sektor viruslari (Bootsector viruses) – Bu viruslar kompyuterning ishlay boshlashi (загрузка) uchun foydalaniladigan qattiq diskning maxsus qismini ishdan chiqaradi. Bu virus kompyuteringizni zararlaganidan keyin, kompyuter ishlamay qolishi mumkin. Odatda floppy disklar orqali tarqaladi.

Makro viruslar (Macro viruses) – Macro viruslar bu – o'zlarining tarqalishi uchun boshqa bir dasturning makro dasturlash tilidan foydalanadigan viruslardir. Ular odatda **Microsoft Word** yoki **Excel** hujjatlarini zararlaydi.

Operativ xotirada yashovchi viruslar (Memory Resident Viruses) — Bu viruslar kompyuteringizning operativ xotirasida (RAM) yashaydi va zararli harakatini amalga oshiradi. Odatda ularni ishga tushirish uchun boshqa virusdan foydalaniladi. Ular o'zlarining ishga tushishga yordam bergan virus yopilgan bo'lsa ham kompyuter xotirasida qoladi, shuning uchun ham ularga yuqoridagi nom berilgan.

Rootkit viruslari (Rootkit viruses) – Rootkitlar viruslar orasida o'zlarining eng xavfliligi va yashirinishga ustaligi bilan alohida ajralib turadi. Rootkitlar kompyuteringizni yovuz hakerlar tomonidan qo'lga olinishi uchun foydalaniladi. Ba'zi rootkitlarni antivirus dasturlari ham aniqlay olmaydi, chunki ular o'zlarini operativ tizim fayllari sifatida ko'rsatishadi. Rootkitlar odatda troyanlar tomonidan kompyuteringizga o'rnatiladi.

O'zgaruvchan viruslar (Polymorphic viruses) – Bu viruslar nafaqat o'z-o'zidan ko'payadi, balki ko'paygan paytda o'zlarining kodlarini ham o'zgartirib turishadi. O'zgaruvchan viruslarni aniqlash ham ba'zi antiviruslar uchun qiyin kechishi mumkin.

International Conferences
Open Access | Scientific Online | Conference Proceedings
INTERNATIONAL CONFERENCES OF PRACTICE

Vaqt bombasi viruslari (Time or Logic Bombs) – Bu viruslar muayyan sana yohud payt kelganida yoki foydalanuvchi tomonidan muayyan harakat amalga oshirilganida ishga tushadigan viruslardir. Misol uchun Kulgi kunida(1 aprel) yoki Yangi yilda kompyuteringizdagi ma'lumotlarni o'chirib tashlab sizga "**sovg'a**" taqdim etishi mumkin.

Xulosa qilib shuni aytish mumkinki kompyuter viruslari — zamonaviy raqamli muhit uchun jiddiy va doimiy tahdid bo‘lib qolmoqda. Ularning turlari (fayl viruslari, makro viruslar, ziyonli dasturlar, qurtlar, troyanlar va ransomware) va ishlash mexanizmlari turlicha bo‘lsa-da, ularning asosiy xususiyati — tizimga kirib o‘zini ko‘paytirish va foydalanuvchiga yoki tashkilotga moddiy hamda ma’naviy zarar yetkazishdir. Internetning keng tarqalishi, tashqi qurilmalar va ijtimoiy muhit viruslarning tez tarqalishini osonlashtirdi, ayniqsa foydalanuvchilarning xavfsizlik bo‘yicha yetarli bilimga ega emasligi zarar xavfini kuchaytiradi.

Bugungi kunda samarali himoya qatlamli yondashuvni talab qiladi: muntazam tizim va dastur yangilanishlari, ishonchli antivirus va kiberxavfsizlik yechimlari, foydalanuvchilarni o‘qitish hamda zaxira nusxalarini yaratish. Shu bilan birga, sun’iy intellekt va bulut asosidagi xavfsizlik vositalari yangi va murakkab tahdidlarni aniqlashda muhim rol o‘ynamoqda. Lekin texnologik himoyaning o‘zi yetarli emas — tashkilot va shaxslar xavfsizlik madaniyatini shakllantirishi, xavfsiz internet foydalanish qoidalariga amal qilishi va favqulodda vaziyatlarda harakat rejasiga ega bo‘lishi kerak.

Natijada, kompyuter viruslariga qarshi samarali kurash texnik vositalar, ishlab chiqilgan siyosat va muntazam ta’limning uyg‘unlashgan kombinatsiyasini talab etadi. Foydalanuvchilar va tashkilotlar bu jihatlarni jiddiy qabul qilsa, raqamli muhitdagi xavflarni sezilarli darajada kamaytirish mumkin.

FOYDALANGAN ADABIYOTLAR:

1. Fred Cohen — “Computer Viruses — Theory and Experiments” (dastlabki tadqiqot darajasi va virus tushunchalari bo‘yicha klassik manba).
2. John R. Vacca — Computer and Information Security Handbook (kiberxavfsizlikka oid keng qamrovli qo‘llanma).
3. Ross J. Anderson — Security Engineering: A Guide to Building Dependable Distributed Systems (xavfsizlik printsiplari va tizim loyihalash).
4. Andrew S. Tanenbaum — Computer Networks (tarmoqlar va qurtlar/tarmoq orqali tarqaladigan tahdidlar haqida nazariy asos).
5. William Stallings — Cryptography and Network Security (ma’lumotlarni himoya qilish va kriptografiya asoslari).
6. NIST (National Institute of Standards and Technology) — kiberxavfsizlik bo‘yicha tavsiyalar va amaliy ko‘rsatmalar (masalan, autentifikatsiya, zahira va holatlarni tiklash bo‘yicha tavsiyalar).
7. CERT/CC (Computer Emergency Response Team) hisobotlari va xabarnomalari — yangi tahdidlar va hujumlar tahlili.