KIBER XAVFSIZLIK ASOSI KOMPYUTER VIRUSLARI VA ULARDAN HIMOYALANISH

Rajapova Zebiniso
Shahrisabz davlat pedagogika instituti
Matematika Informatika fakulteti 4-bosqich talabasi
Negmatova Sevinch Ergash qizi
Qarshi davlat texnika universiteti
Raqamli iqtisodiyot yo'nalishi 3 bosqich talabasi
https://doi.org/10.5281/zenodo.14922532

ARTICLE INFO

Qabul qilindi: 15-Fevral 2025 yil
Ma'qullandi: 20-Fevral 2025 yil
Nashr qilindi: 25-Fevral 2025 yil

KEYWORDS

kompyuter virusi, kompyuter viruslarining tarqalish usullari, kompyuter viruslarining turlari, kompyuter viruslarining zararli ta'siri, kompyuter viruslari tarixi va ularning iqtisodiy ta'siri, Creeper virus, Brain virus, Melissa virusi, kompyuter viruslaridan himoyalanish usullari..

ABSTRACT

Zamonaviy raqamli muhitda kompyuter viruslari kiberxavfsizlikka jiddiy tahdid solmoqda. Ular foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlash, tizim faoliyatini izdan chiqarish yoki zarar yetkazish kabi maqsadlarda yaratiladi. Ushbu maqolada kompyuter viruslarining kelib chiqishi, turlari va ishlash mexanizmlari batafsil tahlil qilinadi. Ayniqsa, eng keng tarqalgan zararli dasturlar – troyanlar, reklama viruslari, josus dasturlar, shifrlovchi viruslar va ularning foydalanuvchi qurilmalariga qanday ta'sir ko'rsatishi haqida so'z yuritiladi. Shuningdek, maqolada viruslardan samarali himoyalanish usullari ko'rib chiqiladi.

Antivirus dasturlaridan foydalanish, xavfsiz internet faoliyatini yuritish, shubhali fayllarni yuklab olmaslik, operatsion tizim va dasturlarni muntazam yangilab borish kabi choralar virus tahdidlarini sezilarli darajada kamaytirishi mumkin. Maqola kiberxavfsizlikka qiziqqan mutaxassislar, IT sohasi vakillari va oddiy foydalanuvchilar uchun foydali bo'lib, kompyuter tizimlarini himoya qilish bo'yicha muhim ko'rsatmalar beradi. Ushbu maqolani o'qish orqali siz kompyuter viruslariga qarshi kurash bo'yicha zarur bilim va ko'nikmalarga ega bo'lishingiz mumkin.

Zamonaviy texnologiyalar rivojlanishi bilan birga kiberxavfsizlik muammolari ham dolzarb masalaga aylanib bormoqda. Kompyuter viruslari foydalanuvchilarning shaxsiy ma'lumotlarini o'g'irlash, tizimga zarar yetkazish va uning ishlashiga to'sqinlik qilish kabi turli tahdidlarni yuzaga keltiradi. Ayniqsa, internetdan faol foydalanadigan kishilar, tashkilotlar va korxonalar uchun bu muammo yanada jiddiy ahamiyat kasb etadi.

Kompyuter viruslari qanday paydo bo'ladi? Ular qanday ishlaydi va foydalanuvchi qurilmalariga qanday ta'sir ko'rsatadi? Eng ko'p uchraydigan zararli dasturlar qaysilar? Viruslardan qanday samarali himoyalanish mumkin? Ushbu maqolada shu va shu kabi savollarga javob beriladi.

Kompyuter viruslari dasturiy tahdidlarning bir turi bo'lib, ular foydalanuvchi xabardor bo'lmagan holda tizimga kirib boradi va turli zararli harakatlarni amalga oshiradi. Ayrim

viruslar oddiy reklamalarni ko‘rsatish bilan cheklanib qolsa, boshqalari esa muhim ma’lumotlarni shifrlab, ularni ochish uchun to‘lov talab qiladi. Bugungi kunda zararli dasturlar ko‘lami kengayib, ularning yangi turlari tobora ko‘payib bormoqda. Shu sababli, kompyuter viruslarining qanday ishlashini, ularning asosiy turlarini va ulardan himoyalanish usullarini bilish har bir foydalanuvchi uchun juda muhimdir. Ushbu maqolada kompyuter viruslarining turlari, ularning foydalanuvchilar uchun xavfi hamda ulardan samarali himoyalanish yo‘llari haqida batafsil ma’lumot beriladi.

Kompyuter virusi — bu zararli dasturiy ta’minot (malware) turidir. U ishga tushirilganda, o‘zini takrorlab, boshqa kompyuter dasturlarini o‘zgartiradi va ularga o‘z kodini joylashtiradi.[1] Agar bu nusxalash muvaffaqiyatli amalga oshsa, zarar ko‘rgan qismlar “kompyuter virusiga chalingan” deb hisoblanadi. Bu atama biologik viruslardan olingan metaforadir.[2]

✔**Kompyuter viruslarining tarqalish usullari.** Kompyuter viruslari turli yo‘llar bilan tarqaladi:

Elektron pochta orqali – Virusli fayllar ilova shaklida jo‘natiladi va foydalanuvchi uni ochganda virus tizimga o‘tadi.

USB flesh-disklar va tashqi qurilmalar orqali – Kompyuterga ulashilgan tashqi qurilmalar orqali viruslar tarqalishi mumkin.

Shubhali veb-saytlardan yuklab olingan dasturlar orqali – Ishonchsiz manbalardan yuklab olingan dasturlar virus yuqtirgan bo‘lishi mumkin.

Tarmoq orqali – Viruslar lokal yoki internet tarmoqlari orqali tarqalishi va boshqa kompyuterlarga yuqtirilishi mumkin.

Ishonchsiz havolalar va reklamalar orqali – Foydalanuvchilar noto‘g‘ri havolalar orqali firibgar saytlariga kirib, virusli dasturlarni yuklab olishlari mumkin.

✔**Kompyuter viruslarining turlari.** Kompyuter viruslari turli usullarda ishlaydi va turlicha ta’sir ko‘rsatadi. Quyida eng keng tarqalgan virus turlari keltirilgan:

Fayl viruslari: Bu viruslar bajariladigan fayllarga (.exe, .com) joylashadi va fayl ishga tushirilganda faollashadi. Ular boshqa bajariladigan fayllarga o‘z kodini joylashtirish orqali tarqaladi.

Yuklovchi sektor viruslari (Boot Sector Virus): Bu viruslar kompyuter yuklash sektoriga joylashadi va operatsion tizim yuklanayotganda faollashadi. Kompyuter ishga tushirilishi bilan virus o‘z kodini yuklaydi.

Makroviruslar: Microsoft Word, Excel va boshqa ofis dasturlarining hujjatlariga joylashib, hujjat ochilganda ishga tushadi. Bu viruslar odatda elektron pochta orqali tarqaladi.

Troyan dasturlar (Trojan Horse): Bu virus foydalanuvchilarga foydali yoki zararsiz dastur sifatida ko‘rinadi, lekin u yashirincha zararli kodlarni ishga tushiradi. Troyanlar odatda shaxsiy ma’lumotlarni o‘g‘irlash yoki tizimni buzish uchun ishlatiladi.

[1] Piqueira, Jose R.C.; de Vasconcelos, Adolfo A.; Gabriel, Carlos E.C.J.; Araujo, Vanessa O. (2008). “Dynamic models for computer viruses”. https://linkinghub.elsevier.com/retrieve/pii/S0167404808000412 Computers & Security. 27 (7–8): 355–359. https://doi.org/10.1016%2Fj.cose.2008.07.006 ISSN 0167-4048. Archived from the original on 2022-12-28. Retrieved 2022-10-30.

[2] Alan Solomon (2011-06-14). “All About Viruses”. https://web.archive.org/web/20120117091338/http://vx.netlux.org/lib/aas10.html VX Heavens. Archived from the original on 2012-01-17. Retrieved 2014-07-17.

Qo‘shilma viruslar (Polymorphic Virus): Bu viruslar o‘z kodini doimiy o‘zgartirib, antivirus dasturlar tomonidan aniqlanishni qiyinlashtiradi.

Reklama dasturlari (Adware): Bu dasturlar foydalanuvchilarning roziligisiz reklamalar chiqaradi va ba’zan shaxsiy ma’lumotlarni yig‘adi.

Josus dasturlar (Spyware): Bu viruslar foydalanuvchilarning faoliyatini yashirincha kuzatib boradi va shaxsiy ma’lumotlarini o‘g‘irlashi mumkin.

✔ **Kompyuter viruslarining zararli ta’siri.** Kompyuter viruslari turlicha zarar yetkazishi mumkin. Eng keng tarqalgan zararlar:

Fayllarni o‘chirish yoki buzish – Muhim hujjatlar va dasturlarni yo‘q qilish.

Tizim tezligini sekinlashtirish – Kompyuter resurslarini ishlatib, uning ishlashini sustlashtiradi.

Shaxsiy ma’lumotlarni o‘g‘irlash – Parollar, kartalar ma’lumotlari va boshqa maxfiy ma’lumotlarni o‘g‘irlash.

Antivirus dasturlarini o‘chirib tashlash – Tizim himoyasini yo‘q qilib, boshqa zararli dasturlarning tarqalishiga imkon yaratish.

Tarmoq orqali boshqa kompyuterlarga virusni yuqtirish – Bir kompyuterga kirgandan so‘ng, boshqa qurilmalarga ham tarqalishi mumkin.

✔ **Kompyuter viruslari tarixi va ularning iqtisodiy ta’siri.**Kompyuter viruslari dastlab tajriba sifatida ishlab chiqilgan. Dasturchilar o‘z bilimlarini sinash maqsadida dasturlar yozib, ularning tarqalish va ishlash mexanizmlarini o‘rganishgan. Ammo vaqt o‘tishi bilan viruslar zararli qurolga aylandi va kiber jinoyatchilar ularni turli maqsadlarda ishlata boshladi. **Creeper virusi** ilk bor 1970-yillarning boshlarida Internetning ibtidosi bo‘lgan ARPANETda aniqlangan.[3] Creeper ARPANET orqali tizimga kirib, o‘zini masofaviy kompyuterga ko‘chirgan va ekranda “I’M THE CREEPER. CATCH ME IF YOU CAN!” (“Men Creeperman, qo‘lingdan kelsa meni tutib ol?”) degan xabarni chiqargan.[4] Ilk zararli viruslardan biri 1986-yilda yozilgan **Brain virusi** bo‘lib, u dastlab MS-DOS tizimiga hujum qilgan. Keyinchalik 1990-yillarga kelib, kompyuter viruslari ancha keng tarqaldi va ko‘plab foydalanuvchilarga zarar yetkazdi.

1999-yilda tarqalgan **Melissa virusi** elektron pochta orqali tarqalgan eng birinchi yirik viruslardan biri bo‘ldi. 2000-yilda esa **I LOVE YOU** nomli virus millionlab kompyuterlarga zarar yetkazdi va tahminan 10 milliard dollarlik iqtisodiy zarar keltirdi. Ushbu virus elektron pochta orqali “I LOVE YOU” sarlavhasi bilan kelgan fayl orqali tarqalgan. Shu kabi tahdidlarning ko‘payishi natijasida xavfsizlik bo‘yicha tadqiqotchilar va dasturiy ta’minot ishlab chiqaruvchilar viruslarga qarshi himoya vositalarini yaratishga majbur bo‘lishdi.

2013 yildan boshlab kompyuter viruslari har yili milliardlab dollarlik iqtisodiy zarar keltirdi.[5] Bunga javoban antivirus dasturlari sanoati paydo bo‘ldi, turli xil operatsion tizimlar foydalanuvchilariga virusdan himoyani sotdi yoki erkin tarqatdi.[6]

[3] “Virus list” https://web.archive.org/web/20061016141708/http://www.viruslist.com/en/viruses/encyclopedia?chapter=153310937Archived from the original on 2006-10-16. Retrieved 2008-02-07.

[4] “The Creeper Worm, the First Computer Virus”. https://www.historyofinformation.com/detail.php?entryid=2860 History of information. Archived from the original on 28 May 2022.

[5]“Viruses that can cost you”. https://web.archive.org/web/20130925202024/http://www.symantec.com/region/reg_eu/resources/virus_cost.html Archived from the original on 2013-09-25.

Antivirus dasturlari rivojlanishi bilan bir qatorda, xakerlar va kiberjinoyatchilar ham yangi va murakkab usullarni ishlab chiqmoqda. Bugungi kunda **fishing (phishing), ransomware (garovga oluvchi dasturlar), botnet hujumlari, zero-day** hujumlar kabi xavflar keng tarqalgan.

Ayniqsa, **ransomware dasturlarining** zararli ta'siri oshib bormoqda. Masalan, 2017-yilda tarqalgan WannaCry nomli ransomware virusi dunyo bo'ylab 200,000 dan ortiq kompyuter tizimlariga zarar yetkazdi va yirik korxonalar, hukumat idoralari, sog'liqni saqlash tizimlari faoliyatiga putur yetkazdi. Bu kabi hujumlar kiberxavfsizlikning qanchalik muhim ekanini yana bir bor ko'rsatdi.

Shu sababli, zamonaviy antivirus dasturlari endi faqatgina an'anaviy viruslarni aniqlash bilan cheklanmay, balki sun'iy intellekt va mashinaviy o'rganish texnologiyalaridan foydalangan holda real vaqtda tahdidlarni kuzatish va bloklashga qodir bo'lib bormoqda. Bundan tashqari, bulutli xavfsizlik tizimlari, tarmoq xavfsizlik devorlari (firewall) va ko'p bosqichli autentifikatsiya kabi qo'shimcha choralar ham keng qo'llanilmoqda.

Bugungi kunda kiberxavfsizlik muammolari nafaqat individual foydalanuvchilar uchun, balki yirik kompaniyalar, davlat idoralari va hatto milliy xavfsizlik uchun ham katta tahdidga aylangan. Shu sababli, dunyo bo'ylab turli hukumatlar kiberxavfsizlik choralarini kuchaytirish, qonunchilikni mustahkamlash va xalqaro hamkorlikni oshirishga harakat qilmoqda.

✔ **Kompyuter viruslaridan himoyalanish:** Kompyuter viruslari foydalanuvchining ruxsatisiz tizimga kirib, fayllarni buzishi, shaxsiy ma'lumotlarni o'g'irlashi yoki kompyuter ishini sekinlashtirishi mumkin. Ular internet, elektron pochta, flesh-disklar yoki zararli dasturlar orqali tarqaladi. Quyida kompyuteringizni viruslardan himoya qilish bo'yicha batafsil ma'lumot berilgan.

Antivirus dasturlaridan foydalanish. Antivirus dasturlari zararli fayllarni aniqlash va ularni yo'q qilish uchun ishlatiladi. Himoyalanish bo'yicha tavsiyalar:

Ishonchli antivirus dasturini o'rnatish (Kaspersky, Bitdefender, Norton, McAfee, Avast, Windows Defender kabi).

Antivirus dasturlarini doimiy ravishda yangilab borish.

Viruslarni real vaqtda kuzatish funksiyasini yoqish.

Foydalanilmayotgan dasturlar va shubhali fayllarni doimiy skanerlash.

Dasturiy ta'minotni va operatsion tizimni yangilash. Ko'pgina viruslar eski va yangilanmagan dasturlardagi zaifliklardan foydalanadi. Himoyalanish bo'yicha tavsiyalar:

Windows, macOS yoki Linux operatsion tizimlarini doimiy yangilash.

Brauzer, antivirus va boshqa dasturlarni so'nggi versiyasiga o'tkazish.

Noma'lum manbalardan fayllarni yuklab olmaslik. Viruslar ko'pincha zararli dastur sifatida yuklab olinadi yoki elektron pochta orqali yuboriladi. Himoyalanish bo'yicha tavsiyalar:

Elektron pochta orqali kelgan noma'lum havola yoki fayllarni ochmaslik.

Ishonchsiz saytlardan dastur yuklab olmaslik.

Crack yoki modifikatsiyalangan (pirat) dasturlarni yuklab olmaslik, chunki ular zararli kodlarni o'z ichiga olishi mumkin.

[6] Granneman, Scott. "Linux vs. Windows Viruses". https://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses The Register. Archived from the original on September 7, 2015. Retrieved September 4, 2015.

Kuchli parollar va autentifikatsiy. Zaif parollar xakerlar uchun kompyuterga hujum qilishni osonlashtiradi. Himoyalanish bo‘yicha tavsiyalar:

Har bir hisob uchun turli murakkab parollardan foydalanish.

Parollarda harflar (kichik va katta), raqamlar va maxsus belgilarni ishlatish.

2 bosqichli autentifikatsiyani (2FA) yoqish, ayniqsa bank, email va ijtimoiy tarmoqlar uchun.

Parollarni yozib qo‘ymaslik yoki ishonchli parol menejeridan foydalanish.

Ma’lumotlarning zaxira nusxalarini yaratish. Viruslar yoki xakerlik hujumlari natijasida muhim fayllaringiz yo‘qolishi yoki shikastlanishi mumkin. Himoyalanish bo‘yicha tavsiyalar:

Muhim fayllarni tashqi qattiq disk yoki bulutli saqlash xizmatlariga (Google Drive, OneDrive, Dropbox) yuklash.

Zaxira nusxalarni muntazam ravishda yangilash.

Ransomware viruslaridan himoyalanish uchun avtomatik zaxira nusxa olish tizimini yoqish.

Tarmoq xavfsizligini ta’minlash. Internetga ulanayotganingizda tarmoq xavfsizligiga e’tibor qaratish lozim. Himoyalanish bo‘yicha tavsiyalar:

Jamoat Wi-Fi tarmoqlaridan foydalanishda ehtiyot bo‘lish, imkon qadar VPN ishlatish.

Router parolini murakkab qilib qo‘yish va shifrlashni (WPA2/WPA3) yoqish.

Ishonchsiz flesh-disk va tashqi qurilmalarni tekshirish. USB flesh-disklar va tashqi qattiq disklarda virus bo‘lishi mumkin. Himoyalanish bo‘yicha tavsiyalar:

USB qurilmalarni kompyuterga ulashdan oldin antivirus orqali tekshirish.

“Autorun” funksiyasini o‘chirib qo‘yish, chunki viruslar avtomatik ishga tushishi mumkin.

Ishonchsiz yoki noma’lum flesh-disklardan foydalanmaslik.

Brauzer xavfsizligini oshirish. Internetdan foydalanishda brauzer xavfsizligini oshirish kerak. Himoyalanish bo‘yicha tavsiyalar: Ishonchli brauzerlardan foydalanish (Google Chrome, Mozilla Firefox, Microsoft Edge). Brauzer kengaytmalari va plaginlarini faqat rasmiy manbalardan yuklab olish.

Kompyuterdan foydalanuvchilar uchun umumiy tavsiyalar

Ishonchli va litsenziyalangan dasturlardan foydalanish.

Kompyuterga faqat kerakli dasturlarni o‘rnatish.

Tizimni muntazam skanerlash va ortiqcha fayllardan tozalash.

Kompyuterni parol bilan himoyalash va ruxsatsiz foydalanishga yo‘l qo‘ymaslik.

Kompyuter viruslaridan himoyalanish uchun har doim ehtiyotkor bo‘lish va yuqoridagi tavsiyalarga amal qilish kerak. Antivirus dasturlarini o‘rnatish, dasturlarni yangilash, noma’lum manbalardan fayl yuklamaslik va kuchli parollar ishlatish – bu sizning kompyuteringizni va shaxsiy ma’lumotlaringizni xavfsiz saqlashning eng muhim qoidalaridir.

Xulosa qilib aytganda, kompyuter viruslari dastlab eksperiment sifatida yaratilgan bo‘lsa-da, vaqt o‘tishi bilan ular zararli qurolga aylandi. Ilk viruslardan boshlab, bugungi murakkab kiber hujumlargacha bo‘lgan jarayon kiber xavfsizlik sohasining rivojlanishiga sabab bo‘ldi. Viruslar nafaqat individual foydalanuvchilarga, balki yirik korporatsiyalar va davlat idoralariga ham jiddiy zarar yetkazmoqda. Bunga javoban, antivirus dasturlari va himoya texnologiyalari rivojlanib, zamonaviy xavflarni oldindan aniqlash va bloklash

imkonini bermoqda. Biroq, kiber jinoyatchilar ham doimiy ravishda yangi va yanada ilg‘or hujum usullarini ishlab chiqmoqda. Shu sababli, kompyuter foydalanuvchilari o‘z tizimlarini muntazam yangilab borishlari, kuchli parollardan foydalanishlari, shubhali elektron xat va ilovalardan ehtiyot bo‘lishlari zarur.

Bugungi kunda kiberxavfsizlik shunchaki shaxsiy himoya vositasi bo‘lib qolmay, balki global muammo sifatida ham e’tirof etilmoqda. Davlatlar va yirik tashkilotlar bu tahdidlarni kamaytirish uchun xalqaro hamkorlikni kuchaytirish, qonunchilik bazasini mustahkamlash va texnologik innovatsiyalarni joriy etishga harakat qilmoqda. Shu bois, kompyuter foydalanuvchilari ham kiberxavfsizlik madaniyatini shakllantirishga e’tibor qaratishlari lozim.

Foydalanilgan adabiyotlar ro‘yxati:

1. Qodirov, F. "OPTIMIZATION OF TELECOMMUNICATIONS POWER SUPPLY SYSTEMS BASED ON RELIABILITY CRITERIA." Science and innovation 2.A12 (2023): 15-20.
2. F Qodirov. Aholiga tibbiy xizmatlar ko'rsatishning rivojlanishini iqtisodiy-matematik modellashtirish. Scienceweb academic papers collection . 2023/1/1.
3. F Qodirov. Zamonaviy to'lov tizimlari tahlili va elektron pul birliklari. Scienceweb academic papers collection. 2023/1/1.
4. Farrux Qodirov. Zamonaviy trenajyor va simulyatsiya qiluvchi dasturlarning hozirgi kundagi ahamiyati. Scienceweb academic papers collection. 2023/1/1
5. Farrux Qodirov. BUSINESS INNOVATION MODEL OF INCOME AND COSTS FROM THE PROVISION OF MEDICAL SERVICES TO THE POPULATION. Scienceweb academic papers collection. 2023/1/1
6. Farrux Qodirov. ECONOMIC-MATHEMATICAL MODELING OF THE DEVELOPMENT OF THE PROVISION OF MEDICAL SERVICES TO THE POPULATION. Scienceweb academic papers collection. 2023/1/1
7. Farrux Qodirov. THE PLACE OF ECONOMETRICAL MODELING OF HEALTHCARE QUALITY IMPROVEMENT IN THE DIGITAL ECONOMY. Scienceweb academic papers collection. 2023/1/1
8. Farrux Qodirov. DEVELOPMENT OF SCIENTIFIC AND TECHNOLOGICAL SYSTEM OF MANAGEMENT OF INDUSTRIAL ENTERPRISES. Scienceweb academic papers collection. 2023/1/1
9. Ergash o’g’li, Qodirov Farrux. "CREATION OF ELECTRONIC MEDICAL BASE WITH THE HELP OF SOFTWARE PACKAGES FOR MEDICAL SERVICES IN THE REGIONS." Conferencea (2022): 128-130.
10. Ergash o’g’li, Qodirov Farrux. "IMPORTANCE OF KASH-HEALTH WEB PORTAL IN THE DEVELOPMENT OF MEDICAL SERVICES IN THE REGIONS." Conferencea (2022): 80-83.
11. Qodirov, Farrux. "THE ROLE OF ICT IN THE DEVELOPMENT OF HEALTH SERVICES." RAQAMLI TRANSFORMATSIYA JARAYONIGA AXBOROT TEXNOLOGIYALARINI JORIY ETISHDA MA’LUMOTLARNI HIMOYALASH MUAMMOLARI VA YECHIMLARI RESPUBLIKA ILMIY-AMALIY ANJUMANI MA’RUZALAR TO’PLAMI (2022).
12. Фаррух Қодиров. Аҳолига хизмат кўрсатиш соҳасининг моделлаштиришни тизимли имитация қилиш. Biznes-Эксперт. Том 173. Номер №5. Страницы 102-106. Дата публикации 2022.
13. Farrux, Qodirov. "Foreign experience in the development of medical services to the population." Хоразм Маъмун академияси (2022).

14. ҚОДИРОВ, Фаррух. "АҲОЛИГА СОҒЛИҚНИ САҚЛАШ ХИЗМАТЛАРИ КЎРСАТИШНИНГ ИЖТИМОИЙ-ИҚТИСОДИЙ РИВОЖЛАНИШИ ТАҲЛИЛИ." AGRO ILM (2022).
15. Qodirov, Farrux. "VEKTOR VA SKALYAR MAYDONLAR. GRADIYENT VA YO'NALISH BO'YICHA HOSILA. DIVERGENSIYA VA ROTOR. SATH CHIZIQLARI. GRADIYENT MAYDONLAR. OQIMLAR." Analytical Journal of Education and Development (2022).
16. Qodirov, Farrux. "FURYE QATORI FUNKSIYALARNI FURYE QATORIGA YOYISH." МАТЕМАТИК ФИЗИКА ВА МАТЕМАТИК МОДЕЛЛАШТИРИШНИНГ ЗАМОНАВИЙ МУАММОЛАРИ Халқаро илмий-амалий анжуман материаллари тўплами (2021).
17. Qodirov, Farrux. "MASOFAVIY TA'LIMDA MOODLE. TUITKF. UZ PLATFORMASINING O'RNI VA AHAMIYATI." ИЖТИМОИЙ СОҲАЛАРНИ РАҚАМЛАШТИРИШДА ИННОВАЦИОН ТЕХНОЛОГИЯЛАРНИНГ ЎРНИ ВА АҲАМИЯТИ РЕСПУБЛИКА ИЛМИЙ-АМАЛИЙ АНЖУМАНИ МАЪРУЗАЛАР ТЎПЛАМИ (2020).
18. Qodirov, Farrux. "RASPBERREY PI QURILMASINING TEXNIK XUSUSIYATLARI VA UNING IMKONIYATLARI." ИЖТИМОИЙ СОҲАЛАРНИ РАҚАМЛАШТИРИШДА ИННОВАЦИОН ТЕХНОЛОГИЯЛАРНИНГ ЎРНИ ВА АҲАМИЯТИ РЕСПУБЛИКА ИЛМИЙ-АМАЛИЙ АНЖУМАНИ МАЪРУЗАЛАР ТЎПЛАМИ (2020).
19. Qodirov, Farrux. "PROTECTING WEBSITES FROM VARIOUS ATTACKS." АХБОРОТ-КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИНИ РИВОЖЛАНТИРИШ ШАРОИТИДА ИННОВАЦИЯЛАР мавзусидаги Республика илмий-амалий анжуман МАЪРУЗАЛАР ТУПЛАМИ (2019).
20. Кодиров, Ф. "PROTSESS RAZRABOTKI IGROVOGO DVIJKA UNITY." Scienceweb academic papers collection (2019).
21. Қодиров, Фаррух. "ПРОЦЕСС РАЗРАБОТКИ ИГРОВОГО ДВИЖКА UNITY." АХБОРОТ-КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИНИ РИВОЖЛАНТИРИШ ШАРОИТИДА ИННОВАЦИЯЛАР мавзусидаги Республика илмий-амалий анжуман МАЪРУЗАЛАР ТУПЛАМИ (2019).
22. Qodirov, Farrux. "" AQLLI UY" TIZIMINING IMKONIYATLARI." Scienceweb academic papers collection (2019).
23. Qodirov, Farrux. "DESCRIPTION AND PERFORMANCE OF THE PROGRAM 3D MAX STUDIO." АХБОРОТ-КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИНИ РИВОЖЛАНТИРИШ ШАРОИТИДА ИННОВАЦИЯЛАР мавзусидаги Республика илмий-амалий анжуман МАЪРУЗАЛАР ТУПЛАМИ (2019).