



## VIRUSLARGA QARSHI VOSITALAR.

---

*Xushbaqov Elchin*

*Mirzarasulov Javohir*

*Ilmiy rahbar: Yusupova Zebiniso Xusniddinova*

*Sanoyev Zafar Isomiddinovich*

*Dotsent PhD*

**Annotatsiya:** ushbu maqolada antivirus vositalarining evolyutsiyasi, ularning kiberxavfsizlikning o'zgaruvchan landshaftidagi ahamiyati va zararli dasturlarni aniqlash va oldini olishda qo'llaniladigan usullar ko'rib chiqilgan. Adabiyot tahlili antivirus echimlarining tarixiy rivojlanishiga kirib, asosiy bosqichlarni ta'kidlaydi. Usullar bo'limida zamonaviy antivirus vositalari tomonidan qo'llaniladigan texnologik yondashuvlar muhokama qilinadi va natijalar bo'limida ularning samaradorligi keltirilgan. Muhokama bo'limi sohadagi muammolar va yutuqlarni ko'rib chiqadi, kelajakda takomillashtirish bo'yicha xulosalar va takliflarga olib keladi.

**Kalit so'zlar:** Antivirus vositalari, kiberxavfsizlik, zararli dastur, tahdidlarni aniqlash, so'nggi nuqta himoyasi, xavfsizlik dasturi.

Internet bizning kundalik hayotimizda hal qiluvchi rol o'ynaydigan raqamli asrda zararli dasturlar va kiberhujumlar xavfi katta. Antivirus vositalari kiber tahdidlarning tobora o'sib borayotgan murakkabligiga moslashish uchun vaqt o'tishi bilan rivojlanib, ushbu zararli shaxslardan himoya qilishning asosiga aylandi. Ushbu maqola raqamli muhitni himoya qilishda antivirus vositalarining tarixi, metodologiyasi va samaradorligini chuqur o'rganishga qaratilgan.

Antivirus vositalarining genezisini hisoblashning dastlabki kunlarida o'z-o'zini takrorlaydigan dasturlar yoki kompyuter viruslari tushunchasi paydo bo'lgan paytdan boshlash mumkin. Birinchi antivirus dasturlari ma'lum zararli dasturlarni aniqlash uchun imzoga asoslangan aniqlash usullaridan foydalangan holda nisbatan sodda edi. Kiber tahdidlar rivojlanib borgan sari, kiber tahdidlarning dinamik landshaftiga mos kelish uchun evristika, xatti-harakatlarni tahlil qilish va bulutga asoslangan aniqlashni o'z ichiga olgan antivirus echimlari ham rivojlandi.

Adabiyotlarni tahlil qilish antivirusni ishlab chiqishda an'anaviy imzoga asoslangan aniqlashdan mashinani o'rganish va sun'iy intellekt kabi ilg'or texnikaga o'tish kabi muhim daqiqalarni qamrab oladi. Shuningdek, u antivirus vositalarining



to'lov dasturlari, fishing hujumlari va polimorfik zararli dasturlar kabi tahdidlarning muayyan turlarini yumshatishdagi rolini o'rganadi.

Zamonaviy antivirus vositalari zararli dasturlarni aniqlash va oldini olish uchun ko'p qirrali yondashuvni qo'llaydi. Imzoga asoslangan aniqlash fayllarni ma'lum ma'lumotlar bazasi bilan taqqoslashni o'z ichiga oladi zararli dastur imzolar, evristika esa potentsial tahdidlarni aniqlash uchun dasturlarning xatti-harakatlarini tahlil qiladi. Mashinani o'rganish algoritmlari naqsh va anomaliyalarni aniqlash uchun tobora ko'proq foydalanilmoqda, bu esa yanada moslashuvchan va dinamik himoya mexanizmini ta'minlaydi. Bulutga asoslangan aniqlash jamoaviy razvedkadan foydalanadi, bu antivirus vositalariga Real vaqtda paydo bo'lgan tahdidlarni tezda aniqlash va ularga javob berishga imkon beradi.

Ushbu bo'lim shuningdek, so'nggi nuqta himoyasining rolini o'rganadi, antivirus vositalarining operatsion tizimlar va tarmoq infratuzilmalari bilan qanday qilib xavfsizlikni har tomonlama qamrab olishini ta'minlaydi.

Antivirus vositalari-bu zararli dasturlarni aniqlash, oldini olish va olib tashlash uchun mo'ljallangan dasturiy ta'minot (zararli dastur) kompyuter tizimlaridan. Ular raqamli qurilmalarning xavfsizligi va yaxlitligini ta'minlashda hal qiluvchi rol o'ynaydi. Antivirus vositalarining ba'zi asosiy jihatlari:

- Haqiqiy vaqtda himoya: aksariyat antivirus vositalari Real vaqtda skanerlashni ta'minlaydi, ya'ni ular sizning tizimingizni zararli dasturlarning har qanday belgilari uchun faol ravishda kuzatib boradi va uning bajarilishi yoki tarqalishining oldini olish uchun choralarni ko'radi.
- Virus ta'riflari: virusga qarshi vositalar tahdidlarni aniqlash va olib tashlash uchun virus ta'riflariga, ma'lum zararli dastur imzolari ma'lumotlar bazasiga tayanadi. Ushbu ta'riflar so'nggi tahdidlar bilan dolzarb bo'lib qolish uchun muntazam ravishda yangilanadi.
- Evristik tahlil: ma'lum virus imzolaridan tashqari, ko'plab antivirus dasturlari yangi yoki noma'lum tahdidlarni ularning xatti-harakatlariga qarab aniqlash uchun evristik tahlildan foydalanadi. Bu ilgari ko'rilmagan zararli dasturlarni aniqlashga yordam beradi.
- Xulq-atvor tahlili: ba'zi ilg'or antivirus vositalari dasturlarning Real vaqt rejimida ishlashini tahlil qiladi. Agar dastur shubhali harakat qilsa yoki zararli dasturlarning xususiyatlarini namoyish qilsa, u belgilanishi va tegishli ravishda ko'rib chiqilishi mumkin.
- Xavfsizlik devori integratsiyasi: ba'zi antivirus vositalari tarmoq trafiginii kuzatish va boshqarish uchun xavfsizlik devori imkoniyatlarini o'z ichiga



oladi, bu sizning kompyuteringizga ruxsatsiz kirishni oldini olish orqali umumiy xavfsizlikni oshiradi.

- **Avtomatik yangilanishlar:** muntazam yangilanishlar antivirus vositalarining samaradorligi uchun juda muhimdir. Yangilanishlar dasturiy ta'minotning yangi va rivojlanayotgan tahdidlarga qarshi kurashish uchun so'nggi virus ta'riflari va xavfsizlik yamoqlariga ega bo'lishini ta'minlaydi.
- **Karantin:** potentsial tahdid aniqlanganda, virusga qarshi vositalar ko'pincha zararlangan fayllarni karantin ostiga oladi. Bu ularni tizimning qolgan qismidan ajratib, keyingi zararni oldini oladi.
- **Skanerlash imkoniyatlari:** Antivirus dasturi odatda turli xil skanerlash imkoniyatlarini, shu jumladan to'liq tizimni skanerlash, tezkor skanerlash va maxsus skanerlashni ta'minlaydi, bu foydalanuvchilarga puxtalik darajasini tanlashga imkon beradi.
- **Elektron pochta va veb-himoya:** ba'zi antivirus vositalari elektron pochta xabarlarini skanerlash va zararli qo'shimchalarni blokirovka qilish xususiyatlarini o'z ichiga oladi. Shuningdek, ular zararli dasturlarni joylashtirish uchun ma'lum bo'lgan veb-saytlarga kirishni belgilash yoki blokirovka qilish orqali veb-himoyani ta'minlashi mumkin.
- **Ko'p qurilmalarni qo'llab-quvvatlash:** ko'pgina antivirus vositalari foydalanuvchilarga bitta obuna bilan bir nechta qurilmalarni (masalan, kompyuterlar, smartfonlar va planshetlar) himoya qilishga imkon beradigan ko'p qurilmalarni qo'llab-quvvatlaydi.

Mashhur antivirus vositalariga quyidagilar kiradi:

- Norton Antivirus
- McAfee
- Kasperskiy
- Bitdefender
- Avast
- AVG
- Oyna himoyachisi (oyna operatsion tizimlariga o'rnatilgan)

Tizimning muvofiqligi, xususiyatlari, ishlashga ta'siri va foydalanuvchi interfeysi kabi omillarni hisobga olgan holda, o'ziga xos ehtiyojlaringizga qarab antivirus vositasini tanlash juda muhimdir. Bundan tashqari, operatsion tizim va dasturiy ta'minotni yangilab turish, shubhali havolalardan qochish va kuchli, noyob parollardan foydalanish kabi kiberxavfsizlik gigienasiga rioya qilish antivirus vositalari tomonidan taqdim etilgan himoyani to'ldiradi.



Ularning samaradorligiga qaramay, antivirus vositalari nol kunlik ekspluatatsiya, faylsiz zararli dastur va ilg'or doimiy tahdidlar (apt) tomonidan qo'llaniladigan qochish texnikasi kabi muammolarga duch kelmoqda. Muhokama bo'limi ushbu muammolarni hal qiladi, joriy antivirus metodologiyalarining cheklovlarini baholaydi va takomillashtirish uchun potentsial yo'llarni o'rganadi. Antivirus vositalarining umumiy samaradorligini oshirishda foydalanuvchi ta'limi va proaktiv xavfsizlik choralarining roli ham ko'rib chiqiladi.

#### **Xulosa va takliflar:**

Xulosa qilib aytganda, antivirus vositalari o'zlarining kamtar boshlanishidan ancha uzoqlashib, kiber tahdidlarga qarshi murakkab himoya mexanizmlariga aylandi. Adabiyot tahlili tarixiy kontekstni ta'kidlaydi, usullar va natijalar bo'limlari antivirus texnologiyasining zamonaviy manzarasini namoyish etadi. Muhokama bo'limi muammolarni tan oladi va rivojlanayotgan kiber tahdidlarga qarshi doimiy innovatsiyalar zarurligini ta'kidlaydi.

Kelgusida takomillashtirish bo'yicha takliflar orasida ilg'or sun'iy intellekt, mashinani o'rganish va xulq-atvorni tahlil qilish texnikasi integratsiyasi kiradi. Kiberxavfsizlik bo'yicha mutaxassislar, dasturiy ta'minot ishlab chiquvchilari va oxirgi foydalanuvchilar o'rtasidagi hamkorlik mustahkam mudofaa ekotizimini yaratish uchun juda muhimdir. Doimiy yangilanishlar, tahdid razvedkasini almashish va foydalanuvchilarni xabardor qilish dasturlari raqamli muhitni himoya qilishda antivirus vositalarining samaradorligini yanada oshirishi mumkin.

Texnologiya rivojlanib borar ekan, bizning mudofaa mexanizmlarimiz ham shunday bo'lishi kerak. Antivirus vositalari ushbu raqamli jangda birinchi o'rinda turadi, kiber tahdidlarning o'zgaruvchan landshaftidan himoya qilish uchun moslashadi va rivojlanadi.

#### **Adabiyotlar.**

1. Borisov L. B. tibbiy mikrobiologiya, virusologiya, immunologiya-5-e Ed. o'tish: saytda harakatlanish, qidiruv O'tish: saytda harakatlanish, qidiruv O'tish: saytda harakatlanish, qidiruv
2. Generalov I. I. tibbiy virusologiya. O'tish: saytda harakatlanish, qidiruv
3. Prozorkina N. V., Rubashkina P. A. mikrobiologiya, virusologiya va immunologiya asoslari: - Rostov nd: Feniks, 2002. -416s.
4. Knorre E. s-ilm-fan yoritgichlarida yashash: ilmiy va badiiy adabiyot. O'tish: Saytda Harakatlanish, Qidiruv Lit., 2002.-159 bilan.
5. Rubinskiy Ao, Vysotskaya Iv, Glagolev sm, - biologiya chuqur o'rganish bilan maktablarning 10-11 sinflari uchun umumiy biologiya darsligi-M.: ma'rifat, 2005
6. <http://medbookaide.ru/books/fold9001/book2047/p1.php/>