

AXBOROT TIZIMLARINI WEB VIRUS HUJUMLARIDAN HIMOYA QILISHNING ADAPTIV USULLARI VA ALGORITMLARI

Shoraimov Husanboy Uktamboyevich, Tashpulatova Nadira Batirovna,

Muxsinov Shamil Shavkatovich, Sharipov Baxodir Akilovich

Annotatsiya: Mazkur maqolada axborot tizimlarini web virus hujumlaridan himoya qilishning adaptiv usullari va algoritmlari tadqiq qilingan. Zamonaviy web asosidagi axborot tizimlariga nisbatan amalga oshirilayotgan zararli hujumlar, xususan, Cross-Site Scripting (XSS), iframe injection, web-shell joylashtirish, obfuskatsiyalangan JavaScript kodlari va boshqa zararli skriptli ta'sirlar tizim xavfsizligiga jiddiy tahdid tug'dirishi asoslab berilgan. Tadqiqot davomida web virus hujumlarining shakllanishi va tarqalish dinamikasi ehtimollik-risk modeli asosida tahlil qilingan hamda Markov–Poyya taqsimoti yordamida hujumlarning rivojlanish ehtimollari modellashtirilgan. Web muhitda yuzaga keluvchi tahdidlarni aniqlash uchun timsollarni tanib olish nazariyasiga asoslangan moslanuvchan (adaptiv) algoritmlar ishlab chiqilgan.

Taklif etilgan yondashuvda foydalanuvchi so'rovlari, web-trafik oqimi, zararli skriptli faollik va web ilovalardagi anomal xatti-harakatlarni monitoring qilish mexanizmlaridan foydalanilgan. Bundan tashqari, signaturaviy, evristik va statistik tahlil elementlari hamda mashinali o'rganish usullari integratsiyalashgan holda web virus hujumlarini real vaqt rejimida aniqlash va bloklash algoritmlari taklif etilgan. Tadqiqot natijasida ishlab chiqilgan Web Virus Protection dasturiy vositasi orqali web asosidagi axborot tizimlarida zararli kodlarni aniqlash aniqligi oshirilgan va virusli hujumlarning oldini olish samaradorligi yaxshilangan.

Olingan natijalar web asosidagi axborot tizimlarida xavfli faoliyatni erta aniqlash, xavfsizlik monitoringini avtomatlashtirish va tizim barqarorligini oshirish imkonini beradi. Taklif etilgan usul va algoritmlar O'zbekistonning milliy axborot infratuzilmasi sharoitlariga moslashtirilgan bo'lib, davlat va xususiy sektordagi web tizimlar xavfsizligini ta'minlashda amaliy ahamiyat kasb etadi.

Kalit so‘zlar: web virus, kiberxavfsizlik, axborot tizimi xavfsizligi, web hujumlar, XSS, iframe injection, web-shell, JavaScript obfuskatsiyasi, ehtimollik-risk modeli, Markov–Poyya taqsimoti, adaptiv algoritmi, timsollarni tanib olish, mashinali o‘rganish, web trafik monitoringi, Web Virus Protection, zararli kodlarni aniqlash, axborot xavfsizligi.

Kirish

Hozirgi raqamli transformatsiya sharoitida axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida web asosidagi axborot tizimlari davlat boshqaruvi, bank-moliya sektori, elektron tijorat, sog‘liqni saqlash, ta’lim va sanoat tarmoqlarida keng qo‘llanilmoqda. Internet texnologiyalariga asoslangan axborot tizimlarining funksional imkoniyatlari kengaygani sari ularning xavfsizligini ta’minlash masalasi ham dolzarb ahamiyat kasb etmoqda. Ayniqsa, web muhit orqali amalga oshiriladigan virusli hujumlar axborot tizimlarining maxfiyligi, yaxlitligi va uzluksiz ishlashiga jiddiy tahdid tug‘diruvchi omillardan biri sifatida namoyon bo‘lmoqda.

So‘nggi yillarda web-ilovalarga qaratilgan zararli hujumlar sezilarli ravishda murakkablashib, an’anaviy antivirus va himoya tizimlari imkoniyatlaridan chetlab o‘tuvchi yangi usullar shakllanmoqda. Jumladan, Cross-Site Scripting (XSS), iframe injection, web-shell joylashtirish, SQL Injection, obfuskatsiyalangan JavaScript kodlari, zararli skriptlar orqali foydalanuvchi sessiyalarini egallash va web-serverlarni masofadan boshqarishga imkon beruvchi tahdidlar keng tarqalmoqda. Mazkur hujumlar nafaqat foydalanuvchi ma’lumotlarini noqonuniy egallash, balki server konfiguratsiyasini buzish, web-resurslarni bloklash hamda zararli dasturiy kodlarning avtomatik tarqalishiga sabab bo‘lmoqda.

Global miqyosda web virus hujumlariga qarshi turli himoya mexanizmlari ishlab chiqilgan bo‘lsa-da, ularning aksariyati signaturaviy tahlilga asoslangan bo‘lib,

faqat oldindan ma'lum bo'lgan tahdidlarni aniqlash imkonini beradi. Dinamik tarzda shakllanuvchi, obfuskatsiya qilingan yoki yangi mutatsiyalangan zararli kodlar uchun esa ushbu tizimlar samaradorligi yetarli darajada emas. Bundan tashqari, ko'plab xorijiy himoya tizimlari mahalliy infratuzilma xususiyatlari va O'zbekiston axborot tizimlari arxitekturasiga to'liq moslashmagan. Bu esa web virus hujumlarini aniqlash va bloklashning moslanuvchan, ehtimollik modellariga asoslangan, real vaqt rejimida ishlovchi algoritmlarini ishlab chiqish zaruratini yuzaga keltiradi.

Axborot tizimlarida virusli hujumlarning tarqalish jarayoni murakkab stoxastik xususiyatga ega bo'lib, ularning shakllanishi va rivojlanishi ehtimollik nazariyasi asosida modellashtirilishi mumkin. Shu nuqtai nazardan, virusli hujumlarning dinamikasini baholash, xavf ko'rsatkichlarini aniqlash hamda tahdidlarning tarqalish tezligini oldindan prognozlash muhim ilmiy-amaliy masalalardan biri hisoblanadi. Tadqiqotlarda Markov zanjirlari, Bayes ehtimollik modeli, mashinali o'rganish algoritmlari va statistik tahlil metodlaridan foydalanilgan bo'lsa-da, aynan web-virus hujumlarining tarqalish dinamikasini Markov–Poyya ehtimollik taqsimoti asosida modellashtirish va unga mos himoya algoritmlarini ishlab chiqish masalalari yetarlicha o'rganilmagan.

O'zbekiston Respublikasida raqamli xizmatlar hajmining kengayishi, davlat va xususiy sektorda web-platformalar sonining ortishi hamda "Raqamli O'zbekiston – 2030" strategiyasi doirasida axborot tizimlarini rivojlantirish jarayonlari web xavfsizlik masalasining dolzarbligini yanada oshirmoqda. Davlat organlari, bank tizimlari, elektron hukumat platformalari va korporativ web-resurslarda kiberxavfsizlik talablarining kuchayishi mavjud tahdidlarni oldindan aniqlash va ularga mos himoya mexanizmlarini yaratishni taqozo etmoqda. Shu bilan birga, web-virus hujumlarining milliy axborot tizimlariga ta'sirini kamaytirishga qaratilgan ilmiy asoslangan yondashuvlarni ishlab chiqish amaliy zaruratga aylangan.

Mazkur maqolada web virus hujumlarining shakllanishi va tarqalish mexanizmlari tizimli ravishda tahlil qilinib, ularning rivojlanish dinamikasi ehtimollik-risk modeli asosida modellashdirilgan. Tadqiqotda web asosidagi axborot tizimlariga tahdid soluvchi zararli skriptlar, iframe asosidagi zararli yoʻnaltirishlar, web-shell va obfuskatsiyalangan JavaScript kodlarini aniqlash uchun timsollarni tanib olish nazariyasiga asoslangan adaptiv algoritmlar taklif etilgan. Bundan tashqari, web trafik monitoringi, signaturaviy va evristik tahlil elementlari hamda mashinali oʻrganish usullari integratsiyasi asosida tahdidlarni real vaqt rejimida aniqlash va avtomatik bloklash modeli ishlab chiqilgan.

Tadqiqotning asosiy maqsadi axborot tizimlarini web virus hujumlaridan himoya qilish samaradorligini oshirish, web muhitda tarqaluvchi zararli kodlarning rivojlanish dinamikasini baholash hamda moslanuvchan himoya algoritmlarini ishlab chiqishdan iborat. Ushbu maqsadga erishish uchun web-virus hujumlarining ehtimollik-risk modeli ishlab chiqilib, xavf koʻrsatkichlarini baholash, sezgirlik tahlilini amalga oshirish va Web Virus Protection dasturiy vositasi asosida real vaqt monitoringi mexanizmlari taklif etiladi.

Mazkur tadqiqot natijalari davlat va xususiy sektordagi web asosidagi axborot tizimlari xavfsizligini oshirish, zararli faoliyatni erta bosqichda aniqlash hamda virusli hujumlarning tizim faoliyatiga salbiy taʼsirini kamaytirishda muhim ilmiy-amaliy ahamiyat kasb etadi.

Tadqiqot metodologiyasi

Mazkur tadqiqotda axborot tizimlarini web virus hujumlaridan himoya qilish samaradorligini oshirishga qaratilgan usul va algoritmlarni ishlab chiqish uchun kompleks metodologik yondashuvdan foydalanildi. Tadqiqot jarayonida web virus hujumlarining shakllanishi, tarqalishi, tizimga taʼsiri va ularni aniqlash mexanizmlari nazariy hamda amaliy jihatdan oʻrganildi. Tadqiqot metodologiyasi bir-biri bilan uzviy bogʻliq boʻlgan bir nechta bosqichlardan tashkil etildi: tahdidlarni tizimli tahlil qilish, matematik modellashdirish, risk baholash,

timsollarni tanib olish asosidagi aniqlash algoritmlarini ishlab chiqish, mashinali o'rganish metodlarini qo'llash va eksperimental sinovlar o'tkazish.

Tadqiqotning dastlabki bosqichida web muhitda uchraydigan virusli hujumlarning shakllanish mexanizmlari tizimli tahlil qilindi. Xususan, Cross-Site Scripting (XSS), SQL Injection, iframe injection, web-shell joylashtirish, obfuskatsiyalangan JavaScript kodlari va zararli skriptlar orqali amalga oshiriladigan hujumlarning ishlash tamoyillari o'rganildi. Ushbu hujumlarning web asosidagi axborot tizimlariga ta'sir etish bosqichlari, foydalanuvchi–brauzer–server o'rtasidagi o'zaro bog'liqlik va zararli kodlarning tarqalish dinamikasi tahlil qilindi. Natijada web-virus hujumlarining asosiy belgilarini tavsiflovchi parametrlar majmuasi shakllantirildi.

Tadqiqotda web virus hujumlarining rivojlanish jarayonlarini modellashtirish uchun ehtimollar nazariyasi va matematik statistika usullaridan foydalanildi. Virusli tahdidlarning tarqalishi tasodifiy va dinamik xarakterga ega ekanligini hisobga olib, ularni modellashtirishda Markov–Poyya ehtimollik taqsimoti asosiy matematik apparat sifatida tanlandi. Mazkur model web viruslarning web-ilovalarda bir obyektidan boshqa obyektlarga o'tish ehtimolini, zararli kodning ko'payish intensivligini hamda virusli hujumlarning vaqt bo'yicha rivojlanishini baholash imkonini berdi. Model quyidagi asosiy parametrlar orqali tavsiflandi:

- a -tizimdagi xavfsiz (zararlanmagan) obyektlar soni;
- b -zararli ta'sirga uchragan obyektlar soni;
- n -foydalanuvchi so'rovlari yoki web obyektlarga murojaatlar soni;
- c -zararli kod ta'sirida hosil bo'ladigan yangi zararli obyektlar koeffitsienti.

Mazkur parametrlar asosida web-viruslarning tarqalish ehtimoli va xavf darajasi hisoblandi. Tadqiqot davomida hujumlarning ehtimollik-risk modeli ishlab chiqilib, tizim xavfsizligi ko'rsatkichlari quyidagi tamoyil asosida baholandi:

$$\text{Risk} = P \times U$$

bu yerda:

P -tahdidning yuzaga kelish ehtimoli;

U -web virus hujumi natijasida yetkaziladigan zarar darajasi.

Risk modeli yordamida web asosidagi axborot tizimlarida tahdidlarning kritik darajasi, ularning tarqalish ehtimoli va tizim barqarorligiga ta'siri baholandi. Bundan tashqari, sezgirlik (sensitivity) tahlili yordamida xavf ko'rsatkichlariga ta'sir qiluvchi omillarning ustuvorligi aniqlandi. Sezgirlik tahlili asosida tizim xavfsizligiga eng katta ta'sir qiluvchi parametrlar belgilandi va himoya algoritmlarini optimallashtirish imkoniyati yaratildi.

Web virus hujumlarini aniqlash metodologiyasining asosiy qismi sifatida timsollarni tanib olish nazariyasi qo'llanildi. Mazkur yondashuv orqali zararli skriptlar, web-shell kodlari, iframe manipulyatsiyalari hamda obfuskatsiyalangan JavaScript kodlarining strukturaviy va semantik xususiyatlari o'rganildi. Zararli faollikni ifodalovchi shablonlar (patternlar) bazasi shakllantirilib, foydalanuvchi so'rovlari va web-trafik oqimlari ushbu timsollar bilan taqqoslash asosida tahlil qilindi. Bu esa an'anaviy signaturaviy yondashuvlardan farqli ravishda yangi va oldindan noma'lum bo'lgan tahdidlarni ham aniqlash imkonini berdi.

Shuningdek, tadqiqot metodologiyasida mashinali o'rganish (machine learning) usullaridan foydalanildi. Web trafik oqimlari va foydalanuvchi xatti-harakatlarini tahlil qilish uchun klassifikatsiya algoritmlari qo'llanilib, normal va anomal faoliyatlarni farqlovchi model ishlab chiqildi. Eksperimental ma'lumotlar asosida zararli so'rovlar va oddiy foydalanuvchi faoliyatlari o'rtasidagi farqlar aniqlanib, false positive va false negative ko'rsatkichlarini minimallashtirishga qaratilgan optimallashtirish ishlari amalga oshirildi.

Tadqiqotning amaliy bosqichida ishlab chiqilgan metod va algoritmlar asosida Web Virus Protection dasturiy vositasi yaratildi. Mazkur dasturiy majmua web trafik monitoringi, log-fayllarni tahlil qilish, zararli JavaScript kodlarini

aniqlash, iframe asosidagi zararli yo'naltirishlarni bloklash va foydalanuvchi so'rovlarini xavflilik darajasiga ko'ra baholash imkoniyatlarini birlashtirdi. Dasturiy vosita real vaqt rejimida ishlashga moslashtirilib, web tizimlarida virusli tahdidlarni avtomatik ravishda aniqlash va bloklash imkonini berdi.

Tadqiqot natijalarining ishonchliligini ta'minlash maqsadida eksperimental sinovlar laboratoriya va real web muhitlarda amalga oshirildi. Tajribalar davomida ishlab chiqilgan algoritmlarning aniqlik darajasi, javob berish tezligi, tizim resurslariga yuklamasi va tahdidlarni aniqlash samaradorligi baholandi. Olingan natijalar statistik tahlil asosida qayta ishlanib, taklif etilgan metodologiyaning amaliy samaradorligi asoslandi.

Shunday qilib, tadqiqot metodologiyasi web virus hujumlarini ehtimollik-risk modeli asosida modellashtirish, timsollarni tanib olish nazariyasi yordamida aniqlash va mashinali o'rganish usullari asosida adaptiv himoya algoritmlarini ishlab chiqishga qaratilgan kompleks ilmiy yondashuv sifatida shakllantirildi. Mazkur metodologiya web asosidagi axborot tizimlarida kiberxavfsizlikni oshirish hamda web-virus tahdidlarini erta bosqichda aniqlash imkonini beradi.

Natijalar

Tadqiqot jarayonida web asosidagi axborot tizimlarini virusli hujumlardan himoya qilishga qaratilgan adaptiv usullar va algoritmlar ishlab chiqildi hamda ularning samaradorligi nazariy va amaliy jihatdan baholandi. Ishlab chiqilgan metodologiya asosida web virus hujumlarining shakllanishi, tarqalish mexanizmlari va tizim xavfsizligiga ta'siri ehtimollik-risk modeli yordamida modellashtirildi. Natijada web muhitdagi zararli faoliyatlarni aniqlash uchun timsollarni tanib olish nazariyasiga asoslangan moslanuvchan algoritmik model taklif etildi.

Tadqiqot davomida web virus hujumlarining asosiy turlari — Cross-Site Scripting (XSS), iframe injection, web-shell joylashtirish, SQL Injection va obfuskatsiyalangan JavaScript kodlari tahlil qilinib, ularning web tizimlarga ta'sir

qilish mexanizmlari o'rganildi. Tahlillar natijasida web hujumlarining xos belgilarini ifodalovchi parametrlar majmuasi shakllantirildi hamda zararli faoliyatni tavsiflovchi shablonlar bazasi ishlab chiqildi.

Virusli hujumlarning tarqalish dinamikasini modellashtirish uchun Markov–Poyya ehtimollik modeli qo'llanildi. Mazkur model asosida web viruslarning tizim bo'ylab tarqalish intensivligi, zararli obyektlarning ko'payish ehtimoli va xavf darajasining o'zgarish dinamikasi baholandi. Modellashtirish natijalari web tizimlarida foydalanuvchi so'rovlari sonining ortishi va zararli obyektlar ulushining ko'payishi bilan tahdidlarning tarqalish xavfi sezilarli oshishini ko'rsatdi.

Tadqiqot doirasida ishlab chiqilgan adaptiv algoritmlar web trafik oqimlarini monitoring qilish, zararli skriptlarni aniqlash, iframe asosidagi zararli yo'naltirishlarni bloklash hamda obfuskatsiyalangan JavaScript kodlarini tahlil qilish imkonini berdi. Algoritmarda signaturaviy, evristik va statistik tahlil usullari integratsiyalashgan holda qo'llanilib, oldindan noma'lum bo'lgan zararli kodlarni aniqlash samaradorligi oshirildi.

Tadqiqot natijalari asosida Web Virus Protection dasturiy vositasi ishlab chiqildi. Dasturiy vosita quyidagi asosiy funksional imkoniyatlarni o'z ichiga oldi:

1-jadval

Web Virus Protection dasturiy vositasining funksional imkoniyatlari

№	Funksional modul	Vazifasi
1	Trafik monitoringi	Web trafik va foydalanuvchi so'rovlarini real vaqt rejimida tahlil qilish
2	Zararli skriptlarni aniqlash	XSS, iframe injection va JavaScript hujumlarini aniqlash
3	Web-shell	Serverga joylashtirilgan zararli fayllarni aniqlash

	monitoringi	
4	Adaptiv tahlil moduli	Yangi tahdidlarni timsollar asosida aniqlash
5	Avtomatik bloklash	Xavfli faoliyatni darhol cheklash va bloklash

Eksperimental sinovlar natijalari ishlab chiqilgan algoritmlar samaradorligini tasdiqladi. Tajribalar davomida web virus hujumlarini aniqlash aniqligi, javob qaytarish tezligi va tizim resurslariga yuklama ko'rsatkichlari baholandi.

2-jadval

Taklif etilgan algoritm samaradorligining tahlili

Ko'rsatkich	An'anaviy tizim	Taklif etilgan algoritm
XSS hujumlarini aniqlash aniqligi	81%	95%
Obfuskatsiyalangan JS aniqlash	68%	91%
False Positive darajasi	14%	5%
Tahdidga javob berish vaqti	4.8 sek	1.9 sek
Real vaqt monitoring samaradorligi	O'rta	Yuqori

Natijalardan ko'rinib turibdiki, ishlab chiqilgan adaptiv algoritmlar yordamida web virus hujumlarini aniqlash aniqligi oshirildi, noto'g'ri aniqlashlar (false positive) kamaytirildi hamda tizimning tahdidlarga javob qaytarish tezligi sezilarli yaxshilandi. Ayniqsa, obfuskatsiyalangan JavaScript kodlari va yangi turdagi zararli skriptlarni aniqlash samaradorligi an'anaviy signaturaviy tizimlarga nisbatan yuqori ekanligi aniqlandi.

Bundan tashqari, xavf tahlili natijalari shuni ko'rsatdiki, web asosidagi axborot tizimlarida virusli hujumlarni erta aniqlash va avtomatik bloklash tizim xavfsizligini sezilarli darajada oshiradi hamda web tizimlarning barqaror ishlashiga ijobiy ta'sir ko'rsatadi.

Xulosa

Mazkur tadqiqotda axborot tizimlarini web virus hujumlaridan himoya qilishning adaptiv usullari va algoritmlari ishlab chiqildi hamda ularning samaradorligi ilmiy jihatdan asoslandi. Tadqiqot natijasida web asosidagi axborot tizimlariga tahdid soluvchi virusli hujumlarning shakllanish va tarqalish mexanizmlari tizimli ravishda tahlil qilindi.

Web virus hujumlarining ehtimollik-risk modeli ishlab chiqilib, Markov–Poyya taqsimoti asosida zararli kodlarning tarqalish dinamikasi modellashirildi. Ushbu model web virus tahdidlarining rivojlanishini oldindan baholash va tizim xavf darajasini aniqlash imkonini berdi.

Tadqiqot davomida timsollarni tanib olish nazariyasiga asoslangan adaptiv algoritmlar ishlab chiqilib, ular yordamida web tizimlarda uchraydigan XSS, iframe injection, web-shell va obfuskatsiyalangan JavaScript asosidagi tahdidlarni aniqlash samaradorligi oshirildi. Mashinali o'rganish, signaturaviy va evristik yondashuvlar integratsiyasi natijasida yangi va noma'lum tahdidlarni aniqlash imkoniyati yaratildi.

Ishlab chiqilgan Web Virus Protection dasturiy vositasi web trafik monitoringi, xavfli foydalanuvchi faolligini tahlil qilish, zararli kodlarni aniqlash va real vaqt rejimida bloklash funksiyalarini amalga oshirish imkonini berdi. Tajriba natijalari taklif etilgan algoritmlarning amaliy samaradorligini tasdiqlab, tahdidlarni aniqlash aniqligi oshgani hamda xavfsizlik monitoringiga sarflanadigan vaqt qisqarganini ko'rsatdi.

Tadqiqot natijalari O'zbekistonning web asosidagi axborot tizimlari xavfsizligini ta'minlash, milliy axborot infratuzilmasini himoyalash va web virus hujumlarining salbiy oqibatlarini kamaytirishda muhim ilmiy-amaliy ahamiyat kasb etadi.

Adabiyotlar

1. G‘aniyev S.K., Karimov M.M. Axborot xavfsizligi asoslari. – Toshkent: Aloqachi, 2020.
2. Ostapenko A.G., Zheleznyak V.P. Risk Analysis of Virus Attacks on Client-Server Systems. – Voronezh, 2008.
3. Pozdniakov S.S. Informatsionnaya bezopasnost kompyuternix sistem. – Moskva: Nauka, 2017.
4. Kaspersky E. Computer Virus Threats in Web Systems. – Moscow, 2021.
5. Symantec Security Report. Internet Security Threat Report. – California, 2023.
6. Cyren Threat Intelligence Report. Web Malware and Threat Analytics. – 2024.
7. Stallings W. Network Security Essentials. – Pearson Education, 2021.
8. Bishop M. Computer Security: Art and Science. – Addison Wesley, 2019.
9. Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2018.
10. Sodiqov T., Islomov Sh.Z. Web ilovalarda axborot xavfsizligi muammolari // Muhammad al-Xorazmiy avlodlari. – 2023.
11. OWASP Foundation. OWASP Top 10 Web Application Security Risks. – 2024.
12. IBM X-Force Threat Intelligence Index. – 2024.
13. McAfee Labs Threat Report. – 2024.
14. Karimov M.M., Mamatov N.S. Kiberxavfsizlik asoslari va himoya mexanizmlari. – Toshkent, 2022.
15. Shoraimov X.U. Web virus hujumlarini aniqlash va himoya qilish algoritmlari // Respublika ilmiy-amaliy konferensiya materiallari. – 2025.