

INTELLIGENT MODEL BASED ON PATTERN RECOGNITION FOR DETECTING VIRAL THREATS IN WEB-BASED INFORMATION SYSTEMS

Shoraimov Husanboy Uktamboevich, Tashpulatova Nadira Batirovna, Muxsinov
Shamil Shavkatovich, Sharipov Baxodir Akilovich

Abstract

This article proposes an intelligent model based on pattern recognition theory for detecting viral threats in web-based information systems. The relevance of the research is explained by the increasing complexity of malicious attacks targeting web applications and the insufficient effectiveness of traditional signature-based protection systems in identifying new and obfuscated threats. During the study, the mechanisms of formation of web virus attacks, their propagation dynamics, and their impact on web systems were systematically analyzed.

The research focuses on Cross-Site Scripting (XSS), iframe injection, web-shell deployment, obfuscated JavaScript code, malicious URL redirections, and script-based threats as the main objects of analysis. An intelligent model based on pattern recognition theory was developed to detect web virus threats, and a multi-stage classification algorithm aimed at identifying the structural and semantic features of malicious code was proposed. The model integrates web traffic monitoring with signature-based, statistical, and heuristic analysis methods.

The proposed model operates by analyzing user behavior, web request structures, JavaScript code fragments, URL parameters, and web server logs to identify malicious activities. The developed intelligent approach enables the detection of previously unknown threats and improves the accuracy of web virus classification. Experimental results demonstrated an increase in the accuracy of web virus threat detection, a reduction in false positive detections, and improvements in real-time monitoring efficiency.

The results of this study have significant scientific and practical importance for ensuring the security of web-based information systems within the national information infrastructure of the Republic of Uzbekistan, enabling early detection of malicious activities and prevention of web virus attacks.

Keywords: web virus, information system security, cybersecurity, pattern recognition, intelligent model, web attacks, XSS, iframe injection, web-shell, obfuscated JavaScript, web monitoring, anomaly detection, malicious code classification.

Web asosidagi axborot tizimlarida virusli tahdidlarni aniqlashning timsollarni tanib olishga asoslangan intellektual modeli

Shoraimov Husanboy Uktamboyevich, Tashpulatova Nadira Batirovna, Muxsinov Shamil Shavkatovich, Sharipov Baxodir Akilovich

Annotatsiya

Mazkur maqolada web asosidagi axborot tizimlarida uchraydigan virusli tahdidlarni aniqlashning timsollarni tanib olish nazariyasiga asoslangan intellektual modeli taklif etilgan. Tadqiqotning dolzarbligi web-illovalarga qaratilgan zararli hujumlarning murakkablashuvi, an'anaviy signaturaviy himoya tizimlarining yangi va obfuskatsiyalangan tahdidlarni aniqlashdagi samaradorligi yetarli emasligi bilan izohlanadi. Tadqiqot davomida web virus hujumlarining shakllanish mexanizmlari, ularning tarqalish dinamikasi va web tizimlarga ta'siri tizimli ravishda o'rganilgan.

Tadqiqotda Cross-Site Scripting (XSS), iframe injection, web-shell joylashtirish, obfuskatsiyalangan JavaScript kodlari, zararli URL yo'naltirishlari va skript asosidagi tahdidlar asosiy tahlil obyekti sifatida qaralgan. Web virus tahdidlarini aniqlash uchun timsollarni tanib olish nazariyasiga asoslangan intellektual model ishlab chiqilib, zararli kodlarning strukturaviy va semantik belgilarini aniqlashga mo'ljallangan ko'p bosqichli klassifikatsiya algoritmi taklif etilgan. Modelda web-trafik monitoringi, signaturaviy, statistik va evristik tahlil elementlari integratsiyalashgan holda qo'llanilgan.

Taklif etilgan model zararli faoliyatni aniqlashda foydalanuvchi xatti-harakatlari, web so'rovlar tuzilmasi, JavaScript kod fragmentlari, URL parametrlar va web-server loglari asosida ishlaydi. Tadqiqot natijasida ishlab chiqilgan intellektual yondashuv oldindan noma'lum bo'lgan tahdidlarni ham aniqlash imkonini berib, web viruslarni klassifikatsiyalash aniqligini oshiradi. Tajriba sinovlari natijasida web virus tahdidlarini aniqlash aniqligi oshgani, noto'g'ri

aniqlashlar miqdori kamaygani hamda real vaqt monitoring samaradorligi yaxshilangani kuzatildi.

Mazkur tadqiqot natijalari O'zbekiston Respublikasining milliy axborot infratuzilmasida web asosidagi axborot tizimlari xavfsizligini ta'minlash, zararli faoliyatni erta aniqlash va web virus hujumlarining oldini olishda muhim ilmiy-amaliy ahamiyat kasb etadi.

Kalit so'zlar: web virus, axborot tizimi xavfsizligi, kiberxavfsizlik, timsollarni tanib olish, intellektual model, web hujumlar, XSS, iframe injection, web-shell, obfuskatsiyalangan JavaScript, web monitoring, anomaliyani aniqlash, pattern recognition, zararli kod klassifikatsiyasi.

KIRISH

Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida web asosidagi axborot tizimlari davlat boshqaruvi, bank-moliya, elektron tijorat, sog'liqni saqlash, ta'lim va sanoat sohalarining ajralmas tarkibiy qismiga aylanib bormoqda. Internet texnologiyalarining keng joriy qilinishi natijasida foydalanuvchilarga xizmat ko'rsatish sifati va tezligi sezilarli darajada oshgan bo'lsa-da, mazkur tizimlarning kiberxavfsizligini ta'minlash bilan bog'liq muammolar ham keskin ortmoqda. Ayniqsa, web-ilovalar orqali amalga oshiriladigan virusli tahdidlar axborot tizimlarining yaxlitligi, maxfiyligi va uzluksiz ishlashiga salbiy ta'sir ko'rsatuvchi asosiy omillardan biri hisoblanadi.

So'nggi yillarda web muhitda uchraydigan zararli hujumlarning shakli va murakkabligi sezilarli darajada o'zgarmoqda. Web virus hujumlari oddiy zararli skriptlardan tortib, murakkab obfuskatsiyalangan JavaScript kodlari, serverga yashirin joylashtiriladigan web-shelllar, foydalanuvchi sessiyalarini o'g'irlashga qaratilgan XSS hujumlari hamda iframe orqali zararli yo'naltirishlargacha bo'lgan ko'plab tahdidlarni qamrab olmoqda. Mazkur tahdidlar nafaqat ma'lumotlarni noqonuniy qo'lga kiritish, balki web tizim faoliyatini buzish, foydalanuvchilarni zararli resurslarga yo'naltirish va server boshqaruvini egallash imkoniyatini ham yaratadi.

Mavjud web xavfsizlik tizimlarining asosiy qismi signaturaviy tahlil tamoyiliga asoslangan bo‘lib, ular oldindan ma’lum bo‘lgan zararli kodlarni aniqlashda samarali hisoblanadi. Biroq yangi mutatsiyalangan viruslar, obfuskatsiyalangan skriptlar va noma’lum tahdidlarni aniqlashda ushbu tizimlarning imkoniyatlari yetarli emas. Bundan tashqari, an’anaviy antivirus vositalari ko‘pincha lokal kompyuter tizimlariga yo‘naltirilgan bo‘lib, web asosidagi dinamik tahdidlarni aniqlash uchun to‘liq moslashmagan.

Shu sababli web virus tahdidlarini aniqlashning intellektual usullarini ishlab chiqish, ayniqsa timsollarni tanib olish nazariyasiga asoslangan modellarni qo‘llash muhim ilmiy-amaliy ahamiyat kasb etadi. Pattern recognition yondashuvi zararli faoliyatning o‘ziga xos belgilarini aniqlash, tahdidlarni klassifikatsiyalash va noma’lum viruslarni ham topish imkonini beradi. Mazkur yondashuv web trafik oqimlari, JavaScript kodlari, URL parametrlar, foydalanuvchi xatti-harakatlari va log-fayllarni kompleks tahlil qilish orqali tahdidlarni aniqlash imkoniyatini kengaytiradi.

O‘zbekiston Respublikasida “Raqamli O‘zbekiston – 2030” strategiyasi doirasida davlat va xususiy sektordagi web platformalarning jadal rivojlanishi web asosidagi axborot tizimlarini himoyalash masalasini yanada dolzarb qilmoqda. Davlat xizmatlari, elektron hukumat tizimlari, bank platformalari va korporativ axborot tizimlarining web muhitga o‘tishi bilan virusli tahdidlarning oldini olishga qaratilgan zamonaviy himoya mexanizmlarini ishlab chiqish zarurati kuchaymoqda.

Mazkur maqolaning maqsadi web asosidagi axborot tizimlarida virusli tahdidlarni aniqlashning timsollarni tanib olishga asoslangan intellektual modelini ishlab chiqish, zararli faoliyat belgilarini klassifikatsiyalash hamda web virus hujumlarini erta bosqichda aniqlash samaradorligini oshirishdan iborat.

MAVZUGA OID ILMIY ISHLANMALAR TAHLILI

Axborot tizimlarini web virus hujumlaridan himoya qilish masalasi kiberxavfsizlik sohasining eng dolzarb ilmiy yo‘nalishlaridan biri hisoblanadi. So‘nggi yillarda web asosidagi axborot tizimlarining keng qo‘llanilishi bilan bog‘liq ravishda zararli dasturiy ta’sirlar va virusli tahdidlarning murakkabligi ortib bormoqda. Shu sababli web viruslarni aniqlash, klassifikatsiyalash va ularning oldini olish bo‘yicha ko‘plab ilmiy tadqiqotlar olib borilgan.

Xorijiy tadqiqotlarda web asosidagi tahdidlarni aniqlash masalasi ko‘proq signaturaviy tahlil, anomalayani aniqlash, mashinali o‘rganish va ehtimollik modellashtirish yondashuvlari asosida o‘rganilgan. Xususan, A.G. Ostapenko, V.P. Zheleznyak, S.S. Pozdniakov hamda boshqa olimlarning tadqiqotlarida klient-server arxitekturasi asosidagi tizimlarda virusli hujumlarning rivojlanish dinamikasi, xavf darajasini baholash va risklarni boshqarish algoritmlariga alohida e‘tibor qaratilgan. Mazkur ishlarda zararli hujumlarning vaqt bo‘yicha rivojlanishi stoxastik jarayon sifatida qaralib, Markov jarayonlari va ehtimollik taqsimotlari asosida modellashtirish usullari taklif etilgan.

Shuningdek, xalqaro kiberxavfsizlik tashkilotlari tomonidan ham web tahdidlarining xususiyatlarini tahlil qilishga qaratilgan keng ko‘lamli tadqiqotlar amalga oshirilmoqda. Jumladan, OWASP (Open Worldwide Application Security Project) tomonidan ishlab chiqilgan OWASP Top 10 reytingida web-ilovalardagi asosiy xavfsizlik zaifliklari, jumladan, Cross-Site Scripting (XSS), SQL Injection, autentifikatsiya mexanizmlaridagi kamchiliklar va zararli skriptlar bilan bog‘liq tahdidlar tizimli ravishda tasniflangan. Ushbu yondashuv web tizimlarida eng ko‘p uchraydigan zaifliklarni aniqlashda muhim metodologik asos vazifasini bajaradi.

Bundan tashqari, Kaspersky Lab, IBM X-Force, McAfee Labs, Symantec Security Response kabi xalqaro tashkilotlar tomonidan web muhitdagi zararli kodlar, obfuskatsiyalangan JavaScript skriptlari va phishing asosidagi tahdidlar muntazam ravishda monitoring qilinadi. Ularning hisobotlarida zararli kodlarning yangi modifikatsiyalari, ekspluatatsiya mexanizmlari va web-serverlarga qaratilgan tahdidlar evolyutsiyasi tahlil qilinadi. Ayniqsa, zararli JavaScript kodlarini yashirish (obfuscation) texnologiyasi va iframe asosidagi yo‘naltirish mexanizmlari bugungi kunda web xavfsizlikning eng dolzarb muammolaridan biri sifatida qayd etilgan.

So‘nggi yillarda web viruslarni aniqlashning intellektual usullariga qiziqish ortib bormoqda. Tadqiqotlarda machine learning, deep learning, artificial neural networks, decision trees, support vector machine (SVM) va Bayes klassifikatorlari asosidagi modellar qo‘llanilib, zararli faoliyatlarni avtomatik aniqlashga qaratilgan yondashuvlar taklif etilgan. Ushbu modellar foydalanuvchi xatti-harakatlari, web

trafik xususiyatlari, URL parametrlar va log-fayllarni tahlil qilish orqali normal va anomal faoliyatlarni ajratib olish imkonini beradi.

Biroq mavjud ilmiy ishlanmalar tahlili shuni ko'rsatadiki, ko'pchilik tadqiqotlar asosan ma'lum turdagi zararli kodlarni aniqlashga yo'naltirilgan bo'lib, web virus tahdidlarining dinamik o'zgaruvchan tabiati yetarli darajada hisobga olinmagan. Ayniqsa, obfuskatsiyalangan JavaScript kodlari, yangi shakllanuvchi web-shelllar hamda kompleks web hujumlarini aniqlashda mavjud tizimlarning samaradorligi cheklanganligicha qolmoqda. Ko'pgina signaturaviy tizimlar oldindan ma'lum bo'lmagan tahdidlarni aniqlash imkoniyatiga ega emasligi sababli, yangi mutatsiyalangan zararli kodlarga nisbatan himoya samaradorligi pasayadi.

Respublikamiz miqyosida ham axborot xavfsizligi va kiberxavfsizlik sohasida bir qator ilmiy tadqiqotlar amalga oshirilgan. Xususan, S.K. G'aniyev, M.M. Karimov, M.M. Musayev, N.S. Mamatov, D.T. Muxamediyeva, Sh.Z. Islomov va boshqa tadqiqotchilar tomonidan axborot xavfsizligi, zararli dasturlarni aniqlash va tarmoq tahdidlarini monitoring qilishga oid ilmiy natijalar olingan. Biroq web virus tahdidlarini aynan timsollarni tanib olish nazariyasiga asoslangan intellektual model orqali aniqlash hamda ularni O'zbekistonning web infratuzilmasiga moslashtirish masalalari hali yetarli darajada tadqiq etilmagan.

Shu nuqtai nazardan, web asosidagi axborot tizimlarida virusli tahdidlarni aniqlash uchun timsollarni tanib olish nazariyasiga asoslangan intellektual modelni ishlab chiqish, zararli faoliyatni tavsiflovchi patternlarni aniqlash hamda web trafik monitoringi orqali tahdidlarni real vaqt rejimida klassifikatsiyalash muhim ilmiy va amaliy ahamiyat kasb etadi.

Mavjud ilmiy ishlanmalar tahlili asosida quyidagi ilmiy muammo aniqlandi: web asosidagi axborot tizimlarida noma'lum va dinamik ravishda shakllanuvchi virusli tahdidlarni aniqlash uchun moslanuvchan, intellektual va pattern recognition asosida ishlovchi samarali model yetarli darajada ishlab chiqilmagan.

Mazkur muammoni bartaraf etish maqsadida ushbu tadqiqotda web virus tahdidlarini aniqlashning timsollarni tanib olishga asoslangan intellektual modeli taklif etiladi hamda uning amaliy samaradorligi asoslanadi.

TADQIQOT METODOLOGIYASI

Mazkur tadqiqotda web asosidagi axborot tizimlarida virusli tahdidlarni aniqlash samaradorligini oshirishga qaratilgan timsollarni tanib olish nazariyasiga asoslangan intellektual model ishlab chiqildi. Tadqiqot metodologiyasi web virus hujumlarining shakllanishi, rivojlanishi va aniqlanish jarayonlarini kompleks tahlil qilishga asoslanib, bir necha bosqichlardan iborat ilmiy yondashuv asosida tashkil etildi. Tadqiqot davomida tizimli tahlil, ehtimollar nazariyasi, matematik statistika, pattern recognition (timsollarni tanib olish), mashinali o'rganish elementlari va web-trafik monitoringi usullaridan foydalanildi.

Tadqiqotning birinchi bosqichida web asosidagi axborot tizimlariga xos bo'lgan virusli tahdidlar tasniflandi va ularning ishlash mexanizmlari tahlil qilindi. Tahlil obyekti sifatida Cross-Site Scripting (XSS), iframe injection, web-shell joylashtirish, obfuskatsiyalangan JavaScript kodlari, zararli URL yo'naltirishlari va serverga noqonuniy kirishga qaratilgan skriptlar tanlandi. Ushbu tahdidlarning foydalanuvchi–brauzer–server o'rtasidagi o'zaro bog'liqligi, zararli kodlarning bajarilish ketma-ketligi va web tizimlarga ta'sir etuvchi asosiy belgilari o'rganildi.

Web virus hujumlarining aniqlash mezonlarini shakllantirish maqsadida zararli faoliyatni tavsiflovchi atributlar to'plami ishlab chiqildi. Bunda foydalanuvchi so'rovlarining strukturasidagi o'zgarishlar, URL parametrlaridagi anomal belgilar, JavaScript kodlari ichidagi xavfli funksiyalar, iframe ulanishlari va server loglaridagi shubhali faoliyatlar asosiy indikatorlar sifatida tanlandi.

Tahdidlarni aniqlashning matematik apparati sifatida timsollarni tanib olish nazariyasi qo'llanildi. Mazkur yondashuvda web virus tahdidlarini aniqlash masalasi klassifikatsiya muammosi sifatida qaraldi. Ya'ni tizimga kelayotgan obyekt (web so'rov, kod fragmenti yoki trafik elementi) uning xavflilik darajasiga ko'ra sinflarga ajratiladi:

$$W=\{W_1,W_2,...,W_n\} \quad W = \{W_1, W_2, ..., W_n\} \quad W=\{W_1,W_2,...,W_n\}$$

bu yerda:

- W_1 — xavfsiz faoliyat;
- W_2 — shubhali faoliyat;
- W_3 — zararli web virus tahdidi.

Har bir web obyekt uchun xususiyatlar vektori shakllantirildi:

$$X=(x_1,x_2,x_3,...,x_n) \quad X = (x_1, x_2, x_3, ..., x_n) \quad X=(x_1,x_2,x_3,...,x_n)$$

bu yerda:

- x_1 — URL parametrlarining holati;
- x_2 — JavaScript kodi murakkabligi;
- x_3 — iframe mavjudligi;
- x_4 — zararli funksiyalar ulushi;
- x_5 — foydalanuvchi xatti-harakatlaridagi anomal holatlar.

Mazkur parametrlar asosida obyektlarning xavflilik darajasi baholanib, klassifikatsiyalash amalga oshirildi.

Tahdidlarning tarqalish ehtimolini baholash uchun **ehtimollik-risk modeli** ishlab chiqildi. Web virus hujumlarining xavf darajasi quyidagi formula asosida hisoblandi:

$$R=P \times DR = P \times D$$

bu yerda:

- R** — umumiy xavf darajasi;
- P** — web tahdid yuzaga kelish ehtimoli;
- D** — tizimga yetkaziladigan zarar darajasi.

Risk baholash modeli yordamida web asosidagi axborot tizimlarida mavjud bo'lgan zaif nuqtalarni aniqlash va ularning tizim xavfsizligiga ta'sir darajasini baholash imkoniyati yaratildi. Mazkur yondashuv web muhitda yuzaga keladigan tahdidlarning ehtimollik darajasi hamda ular natijasida tizimga yetkazilishi mumkin bo'lgan zarar miqdorini kompleks baholashga xizmat qiladi. Natijada web asosidagi axborot tizimlarida eng kritik zaifliklar aniqlanib, ularga nisbatan ustuvor himoya choralarini ishlab chiqish imkoniyati shakllantirildi. Bu esa resurslarni samarali taqsimlash, eng yuqori xavf tug'diruvchi tahdidlarga nisbatan tezkor choralar ko'rish va tizim xavfsizligini optimallashtirish imkonini beradi.

Tadqiqot davomida web virus tahdidlarini aniqlash va ularning tizimga ta'sirini kamaytirishga qaratilgan ko'p bosqichli intellektual model ishlab chiqildi. Mazkur model web muhitda yuzaga keluvchi zararli faoliyatni real vaqt rejimida kuzatish,

tahlil qilish va klassifikatsiyalashga mo'ljallangan bo'lib, bir nechta o'zaro bog'liq bosqichlardan tashkil topgan.

Modelning dastlabki bosqichida web tizimdan olinadigan ma'lumotlarni yig'ish va monitoring qilish jarayoni amalga oshiriladi. Ushbu bosqichda web-server loglari, HTTP va HTTPS so'rovlari, URL parametrlar, JavaScript kod fragmentlari hamda foydalanuvchi sessiyalariga oid ma'lumotlar muntazam ravishda kuzatib boriladi. Mazkur ma'lumotlar web tizimdagi foydalanuvchi faoliyatini aks ettiruvchi asosiy axborot manbalari bo'lib xizmat qiladi. Ayniqsa, web virus hujumlarining aksariyati foydalanuvchi so'rovlari yoki skriptlar tarkibida yashirin tarzda amalga oshirilishini hisobga olsak, monitoring bosqichi tahdidlarni aniqlashning fundamental qismi hisoblanadi.

Keyingi bosqichda yig'ilgan ma'lumotlar dastlabki qayta ishlashdan o'tkaziladi. Amaliyotda web trafik tarkibidagi ma'lumotlar ko'pincha ortiqcha belgilar, takrorlanuvchi elementlar yoki foydasiz fragmentlarni o'z ichiga oladi. Shu sababli ushbu bosqichda ma'lumotlar filtrlanadi, kod fragmentlari normalizatsiya qilinadi hamda web virus hujumlarini tavsiflovchi asosiy xavf indikatorlari ajratib olinadi. Masalan, URL tarkibidagi g'ayrioddiy parametrlar, JavaScript kodidagi yashirin funksiyalar, iframe orqali amalga oshiriladigan ulanishlar yoki shubhali sessiya faolligi alohida indikator sifatida belgilanadi. Natijada keyingi tahlil uchun optimallashtirilgan va strukturaviy jihatdan qayta ishlangan ma'lumotlar shakllantiriladi.

Shundan so'ng tizimning asosiy intellektual qismi — timsollarni tanib olish (pattern recognition) moduli ishga tushadi. Ushbu bosqichda web obyektlarning strukturaviy va semantik xususiyatlari oldindan shakllantirilgan zararli faoliyat patternlari bazasi bilan taqqoslanadi. Pattern recognition yondashuvi web viruslarning o'ziga xos xususiyatlarini aniqlashga asoslangan bo'lib, zararli JavaScript fragmentlari, XSS hujumlarida qo'llanadigan skriptlar, iframe orqali yashirin yo'naltirishlar va web-shell'larga xos funksiyalar maxsus belgilar asosida tahlil qilinadi. Mazkur yondashuvning afzalligi shundaki, tizim nafaqat oldindan ma'lum bo'lgan zararli faoliyatni, balki strukturaviy jihatdan o'xshash yangi yoki modifikatsiyalangan tahdidlarni ham aniqlash imkoniyatiga ega bo'ladi.

Tahlil natijalari asosida web obyektlarning xavflilik darajasi intellektual klassifikatsiya moduli yordamida baholanadi. Mazkur bosqichda tizim har bir obyektни xavfsiz, shubhali yoki zararli faoliyat sinfiga ajratadi. Agar web obyekt xavfli deb topilsa, uning tizimga salbiy ta'sir ko'rsatish ehtimoli va zarar darajasi alohida baholanadi. Bu esa tizimga faqat aniq tahdidlar bo'yicha emas, balki ehtimoliy xavf tug'diruvchi holatlarga nisbatan ham oldindan choralar ko'rish imkonini beradi.

Modelning yakuniy bosqichida qaror qabul qilish mexanizmi ishga tushadi. Agar tahdid darajasi oldindan belgilangan kritik qiymatdan yuqori bo'lsa, tizim avtomatik ravishda himoya mexanizmlarini faollashtiradi. Bunda zararli so'rov bloklanadi, foydalanuvchi sessiyasi vaqtincha cheklanadi yoki administratorga ogohlantirish yuboriladi. Shu bilan birga, aniqlangan tahdid haqidagi ma'lumot monitoring tizimiga saqlanib, keyingi tahdidlarni aniqlash jarayonida pattern bazasini boyitishga xizmat qiladi.

Shunday qilib, taklif etilgan ko'p bosqichli intellektual model web asosidagi axborot tizimlarida virusli tahdidlarni erta bosqichda aniqlash, ularni real vaqt rejimida monitoring qilish va avtomatik bloklash imkonini beruvchi kompleks himoya mexanizmi sifatida namoyon bo'ladi. Mazkur modelning asosiy ustunligi uning moslanuvchanligi va oldindan noma'lum bo'lgan tahdidlarni ham aniqlash imkoniyatiga egaligida namoyon bo'ladi.

Taklif etilgan metodologiyada an'anaviy signaturaviy yondashuvlardan farqli ravishda noma'lum va yangi mutatsiyalangan web viruslarni aniqlash imkoniyati yaratildi. Shu bilan birga, tizim web trafikdagi anomal holatlarni real vaqt rejimida monitoring qilish imkoniga ega bo'ldi.

TAKLIF ETILGAN INTELLEKTUAL MODEL VA ALGORITM

Tadqiqot natijasida web asosidagi axborot tizimlarida virusli tahdidlarni aniqlashning timsollarni tanib olishga asoslangan intellektual modeli ishlab chiqildi. Taklif etilgan modelning asosiy maqsadi web muhitda uchraydigan zararli faoliyatni erta aniqlash, tahdidlarni klassifikatsiyalash va web viruslarning tizim bo'ylab tarqalishini oldini olishdan iborat.

Taklif etilgan modelning strukturaviy arxitekturasini beshta asosiy moduldan iborat:

1-jadval

Intellektual modelning funksional modullari

№	Modul nomi	Vazifasi
1	Monitoring moduli	Web trafik va loglarni yig'ish
2	Tahlil moduli	JavaScript va URL parametrlarni tekshirish
3	Pattern recognition moduli	Virusli belgilarni aniqlash
4	Klassifikatsiya moduli	Tahdid darajasini aniqlash
5	Himoya moduli	Avtomatik bloklash va ogohlantirish

Taklif etilgan algoritmnining ishlash tamoyili web asosidagi axborot tizimlariga kelib tushayotgan so'rovlarni bosqichma-bosqich tahlil qilish va ularning xavflilik darajasini baholashga asoslangan. Mazkur algoritmnining asosiy maqsadi zararli faoliyatni imkon qadar erta bosqichda aniqlash hamda virusli tahdidlarning tizim bo'ylab tarqalishining oldini olishdan iborat. Shu sababli algoritmnin web muhitdagi foydalanuvchi faolligi va serverga kelayotgan ma'lumotlar oqimini doimiy monitoring qilish mexanizmi asosida tashkil etilgan.

Algoritmnin faoliyati web so'rovning tizimga kelib tushishi bilan boshlanadi. Har bir foydalanuvchi tomonidan yuborilgan HTTP yoki HTTPS so'rovi dastlab monitoring moduli orqali qabul qilinadi va dastlabki tahlildan o'tkaziladi. Ushbu bosqich web tizim uchun muhim hisoblanadi, chunki aynan foydalanuvchi so'rovlari tarkibida zararli kodlar, yashirin skriptlar yoki manipulyatsiyalangan parametrlar mavjud bo'lishi mumkin. Shu sababli tizim har bir kelayotgan so'rovni oddiy axborot almashinuvi sifatida emas, balki ehtimoliy xavf manbai sifatida ko'rib chiqadi.

Keyingi bosqichda web so'rov tarkibi chuqur tahlil qilinadi. Xususan, URL parametrlarining strukturasi, JavaScript kodlarining mavjudligi hamda iframe elementlarining ishlatilishi tekshiriladi. Amaliyot shuni ko'rsatadiki, zararli web viruslarning katta qismi aynan URL manipulyatsiyasi, JavaScript obfuskatsiyasi yoki yashirin iframe elementlari orqali tizimga kirishga harakat qiladi. Shu bois mazkur bosqichda web sahifalardagi skriptlar, parametrlar va tashqi ulanishlar maxsus

indikatorlar asosida baholanadi. Agar tizim tomonidan shubhali belgilar aniqlansa, ular keyingi tahlil bosqichiga yuboriladi.

TAJIRIBA NATIJALARI VA TAHLIL

Taklif etilgan intellektual modelning samaradorligini baholash maqsadida eksperimental tadqiqotlar laboratoriya hamda real web muhitlarda amalga oshirildi. Tajribalar davomida web asosidagi axborot tizimlariga xos bo'lgan virusli tahdidlar, xususan Cross-Site Scripting (XSS), iframe injection, web-shell joylashtirish, obfuskatsiyalangan JavaScript kodlari va zararli URL yo'naltirishlari simulyatsiya qilindi hamda taklif etilgan model yordamida aniqlash darajasi baholandi.

Eksperimental tadqiqotlarda foydalanuvchi so'rovlari, HTTP/HTTPS trafik oqimlari, server log-fayllari, JavaScript kod fragmentlari va web-serverdagi fayllar monitoring qilindi. Tajribalar uchun zararli va xavfsiz web faoliyatlardan iborat ma'lumotlar to'plami shakllantirildi. Tahlil davomida tizimning tahdidlarni aniqlash aniqligi, noto'g'ri aniqlash ko'rsatkichlari (False Positive va False Negative), javob qaytarish tezligi hamda tizim resurslariga yuklama darajasi baholandi.

Tajriba natijalari shuni ko'rsatdiki, taklif etilgan timsollarni tanib olishga asoslangan intellektual model an'anaviy signaturaviy tizimlarga nisbatan yuqori samaradorlikka ega bo'lib, ayniqsa oldindan noma'lum va obfuskatsiyalangan tahdidlarni aniqlash imkonini beradi.

2-jadval

Taklif etilgan model va an'anaviy tizimlar samaradorligi taqqoslanishi

Ko'rsatkich	An'anaviy signaturaviy tizim	Taklif etilgan intellektual model
XSS hujumlarini aniqlash aniqligi	82%	96%
iframe injection aniqlash	75%	93%
Web-shell aniqlash	69%	91%
Obfuskatsiyalangan JavaScript aniqlash	63%	89%

False Positive	15%	4%
False Negative	12%	3%
Tahdidga javob berish vaqti	4.5 sek	1.8 sek

2-jadval natijalariga ko'ra, taklif etilgan model zararli faoliyatlarni aniqlash aniqligini sezilarli darajada oshirgan. Ayniqsa, obfuskatsiyalangan JavaScript kodlari va web-shell tahdidlari kabi murakkab web viruslarni aniqlashda an'anaviy tizimlarga nisbatan yuqori natija qayd etilgan.

Bundan tashqari, foydalanuvchi xatti-harakatlarini monitoring qilish asosida anomal faoliyatlarni aniqlash samaradorligi ham oshgani kuzatildi. Pattern recognition algoritmi yordamida web so'rovlarining strukturasi, URL parametrlari va JavaScript funksiyalaridagi o'zgarishlar avtomatik ravishda tahlil qilinib, zararli faoliyatni ifodalovchi timsollar bilan taqqoslandi.

Eksperimental natijalarga ko'ra, taklif etilgan model yordamida real vaqt monitoring samaradorligi yaxshilandi va web virus tahdidlariga javob qaytarish vaqti deyarli 2.5 barobarga qisqardi. Bu esa tizim xavfsizligini oshirish va zararli faoliyatning tarqalishini dastlabki bosqichda cheklash imkonini berdi.

Tadqiqot davomida xavf ko'rsatkichlari tahlili ham amalga oshirildi. Natijalarga ko'ra, web tizimlarga eng yuqori xavf tug'diruvchi tahdidlar sifatida XSS, web-shell va obfuskatsiyalangan JavaScript asosidagi zararli kodlar qayd etildi.

3-jadval

Web virus tahdidlarining xavf darajasi bo'yicha taqsimoti

Tahdid turi	Ehtimollik darajasi	Tizimga ta'siri	Umumiy risk
XSS	Yuqori	Yuqori	Kritik
iframe injection	O'rta	O'rta	Yuqori

Web-shell	Yuqori	Juda yuqori	Kritik
Obfuskatsiyalangan JS	Yuqori	Yuqori	Kritik
URL manipulyatsiyasi	O'rta	Past	O'rta

Tahlil natijalari shuni ko'rsatdiki, web tizimlarda tahdidlarni erta aniqlash va avtomatik bloklash mexanizmlarini qo'llash xavf darajasini kamaytirishga xizmat qiladi. Ayniqsa, timsollarni tanib olishga asoslangan yondashuv yangi mutatsiyalangan tahdidlarni aniqlash imkoniyatini yaratgani sababli web viruslarning tarqalish ehtimolini pasaytiradi.

Taklif etilgan model asosida ishlab chiqilgan Web Virus Protection dasturiy vositasining konseptual ishlash mexanizmi web trafik monitoringi, zararli faoliyatni klassifikatsiyalash va avtomatik bloklashni yagona tizimda birlashtirishga imkon berdi. Bu esa web asosidagi axborot tizimlari xavfsizligini oshirish uchun kompleks himoya mexanizmini shakllantirdi.

XULOSA

Mazkur tadqiqotda web asosidagi axborot tizimlarida virusli tahdidlarni aniqlashning timsollarni tanib olishga asoslangan intellektual modeli ishlab chiqildi va uning ilmiy-amaliy samaradorligi asoslandi. Tadqiqot davomida web virus hujumlarining shakllanish mexanizmlari, tarqalish xususiyatlari va axborot tizimlariga ta'siri tizimli ravishda tahlil qilindi.

Tadqiqot natijasida web asosidagi tahdidlarni aniqlash uchun pattern recognition tamoyiliga asoslangan ko'p bosqichli intellektual model ishlab chiqildi. Taklif etilgan model yordamida foydalanuvchi so'rovlari, URL parametrlar, JavaScript kodlari, web trafik oqimlari va server loglari kompleks ravishda tahlil qilinib, zararli faoliyatni ifodalovchi timsollar aniqlanadi.

Tadqiqotning ilmiy yangiligi sifatida web virus tahdidlarini aniqlash uchun timsollarni tanib olish nazariyasiga asoslangan intellektual klassifikatsiya modeli taklif etildi hamda zararli faoliyatni xavfsiz, shubhali va kritik sinflarga ajratish algoritmi ishlab chiqildi. Mazkur yondashuv an'anaviy signaturaviy tizimlardan farqli ravishda oldindan noma'lum bo'lgan tahdidlarni aniqlash imkonini beradi.

Ekspirimental sinovlar natijalari taklif etilgan model samaradorligini tasdiqladi. Xususan, web virus tahdidlarini aniqlash aniqligi oshgani, False Positive ko'rsatkichlari kamaygani hamda real vaqt monitoring samaradorligi yaxshilangani kuzatildi. Ayniqsa, XSS, web-shell va obfuskatsiyalangan JavaScript tahdidlarini aniqlashda yuqori natijalar qayd etildi.

Mazkur tadqiqot natijalari O'zbekiston Respublikasining web asosidagi axborot tizimlari xavfsizligini ta'minlash, davlat va xususiy sektor web-platformalarini virusli tahdidlardan himoya qilish hamda kiberxavfsizlik monitoring tizimlarini takomillashtirishda muhim ilmiy-amaliy ahamiyat kasb etadi.

ADABIYOTLAR

- [1] G'aniyev S.K., Karimov M.M. **Axborot xavfsizligi asoslari**. – Toshkent: Aloqachi, 2020. – 356 b.
- [2] Karimov M.M., Musayev M.M. **Kiberxavfsizlik asoslari va himoya mexanizmlari**. – Toshkent: Fan va texnologiya, 2022. – 284 b.
- [3] Mamatov N.S., Islomov Sh.Z. **Axborot tizimlarida xavfsizlikni ta'minlash texnologiyalari**. – Toshkent, 2021. – 248 b.
- [4] Ostapenko A.G., Zheleznyak V.P. **Protsessy virusnoy ataki na klient-servernye sistemy: analiz dinamiki i upravlenie riskami**. – Voronej: Nauchnaya kniga, 2008. – 214 s.
- [5] Pozdniakov S.S. **Informatsionnaya bezopasnost kompyuternyx sistem i setey**. – Moskva: INFRA-M, 2019. – 368 s.
- [6] Stallings W. **Network Security Essentials**. – 7th ed. – Pearson Education, 2021. – 816 p.
- [7] Bishop M. **Computer Security: Art and Science**. – 2nd ed. – Addison-Wesley, 2019. – 1184 p.
- [8] Goodfellow I., Bengio Y., Courville A. **Deep Learning**. – Cambridge: MIT Press, 2018. – 800 p.
- [9] Anderson R. **Security Engineering**. – 3rd ed. – Wiley, 2020. – 1232 p.
- [10] Tanenbaum A.S., Wetherall D. **Computer Networks**. – Pearson, 2021. – 960 p.
- [11] OWASP Foundation. **OWASP Top 10: The Ten Most Critical Web Application Security Risks**. – 2024.

- [12] IBM X-Force. **Threat Intelligence Index Report**. – IBM Security, 2024.
- [13] Symantec Corporation. **Internet Security Threat Report**. – California, 2024.
- [14] Kaspersky Lab. **Kaspersky Security Bulletin: Statistics of Web Threats**. – Moscow, 2024.
- [15] McAfee Labs. **Threats Report: Advanced Web Threat Detection**. – 2024.
- [16] Cyren Security Center. **Global Threat Intelligence Report**. – 2024.
- [17] Sodiqov T., Islomov Sh.Z. **Web ilovalarda axborot xavfsizligi muammolari** // *Muhammad al-Xorazmiy avlodlari* ilmiy jurnali. – Toshkent, 2023. – №4. – B. 45–52.
- [18] Xudoyqulov Z.T., Muxamediyeva D.T. **Tarmoq tahdidlarini monitoring qilishning zamonaviy usullari** // *Axborot xavfsizligi muammolari*. – 2022. – №2. – B. 28–35.
- [19] Islomov Sh.Z., Mamatov N.S. **Web-ilovalarda zararli kodlarni aniqlash algoritmlari** // *TATU xabarlari*. – 2023. – №3. – B. 55–64.
- [20] G‘aniyev S.K., Karimov M.M., Musayev M.M. **Axborot tizimlarining kiberxavfsizlik modeli** // *Muhammad al-Xorazmiy avlodlari*. – 2022. – №5. – B. 12–21.
- [21] Shoraimov X.U. **Web asosidagi axborot tizimlarida virusli tahdidlarni aniqlash algoritmlari** // Respublika ilmiy-amaliy konferensiya materiallari. – Toshkent, 2025. – B. 112–118.