

WEB TEXNOLOGIYALAR RIVOJLANISHI VA AXBOROT XAVFSIZLIGI DOLZARB MASALALARI

Muhammadhikmatulloh Xasanboyev

Izboskan tumani "Ilm nuri" NTM.

E-mail: aideveloper2028@gmail.com

Annotatsiya. Ushbu maqolada web texnologiyalarining zamonaviy rivojlanish tendensiyalari va ular bilan bog'liq axborot xavfsizligi masalalari atroflicha yoritilgan. Dastlab, web texnologiyalarining rivojlanish bosqichlari, ularning turli sohalaridagi (ta'lim, sog'liqni saqlash, moliya, davlat xizmatlari) qo'llanilishi va inson hayotidagi o'rni tahlil qilinadi. Keyinchalik, axborot xavfsizligiga tahdid soluvchi asosiy omillar — phishing, ijtimoiy muhandislik, SQL injection, XSS, DDoS hujumlari va boshqa kiberxavf-xatarlar muhokama qilinadi. Maqolada shuningdek, veb-ilovalardagi zaifliklar sababli yuzaga keladigan xavf-xatarlar, ularni aniqlash va oldini olish usullari (masalan, HTTPS protokolidan foydalanish, ikki bosqichli autentifikatsiya, xavfsiz kod yozish amaliyotlari) haqida ham batafsil ma'lumot beriladi. Muallif mavjud muammolarning texnik va tashkiliy yechimlarini taklif qiladi hamda kiberxavfsizlikni ta'minlash bo'yicha zamonaviy yondashuvlar, xalqaro standartlar (ISO/IEC 27001, OWASP) va ilg'or tajribalarni o'rganadi.

Kalit so'zlar: Web texnologiyalari, axborot xavfsizligi, kiberxavfsizlik, ma'lumotlar himoyasi, phishing, SQL injection, DDoS, shifrlash, autentifikatsiya, veb-ilova zaifliklari.

Аннотация. В данной статье подробно освещаются современные тенденции развития веб-технологий и связанные с ними вопросы информационной безопасности. В начале анализируются этапы развития веб-технологий, их применение в различных сферах (образование, здравоохранение, финансы, государственные услуги) и их роль в жизни человека. Далее рассматриваются основные факторы, угрожающие информационной безопасности — фишинг, социальная инженерия, SQL-инъекции, XSS, DDoS-атаки и другие киберугрозы. В статье также подробно приводится информация о рисках, возникающих из-за уязвимостей веб-приложений, методах их выявления и предотвращения (например, использование протокола HTTPS, двухфакторная аутентификация, практика безопасного программирования). Автор предлагает технические и организационные решения существующих проблем, а также изучает современные подходы к обеспечению кибербезопасности, международные стандарты (ISO/IEC 27001, OWASP) и передовой опыт.

Ключевые слова: веб-технологии, информационная безопасность, кибербезопасность, защита данных, фишинг, SQL-инъекции, DDoS, шифрование, аутентификация, уязвимости веб-приложений.

Annotation. This article provides a comprehensive overview of the modern development trends of web technologies and the related issues of information security. Initially, the stages of web technologies development, their application in various fields (education, healthcare, finance, government services), and their role in human life are analyzed. Subsequently, the main factors threatening information security — phishing, social engineering, SQL injection, XSS, DDoS attacks, and other cyber threats — are discussed. The article also provides detailed information about the risks arising from vulnerabilities in web applications, methods for detecting and preventing them (such as using the HTTPS protocol, two-factor authentication, and secure coding practices). The author proposes technical and organizational solutions to existing problems and examines modern approaches to ensuring cybersecurity, international standards (ISO/IEC 27001, OWASP), and advanced practices.

Keywords: Web technologies, information security, cybersecurity, data protection, phishing, SQL injection, DDoS, encryption, authentication, web application vulnerabilities.

Kirish. Bugungi kunda web texnologiyalar hayotimizning ajralmas qismiga aylangan. Internet tarmog‘ining kengayishi, mobil qurilmalarning ko‘payishi va yuqori tezlikdagi aloqa imkoniyatlari web-illovalarning rivojlanishini sezilarli darajada tezlashtirdi. Veb-saytlar, onlayn platformalar, elektron tijorat, ijtimoiy tarmoqlar va davlat xizmatlari kabi sohalarda web texnologiyalari kundalik faoliyatimizni soddalashtirmoqda va samaradorligini oshirmoqda. Shu bilan birga, veb texnologiyalarining keng tarqalishi axborot xavfsizligi masalalarini ham dolzarb qilib qo‘ydi. Axborotlarning himoyasizligi va kiberxavfsizlik tahdidlari ko‘plab tashkilotlar va foydalanuvchilar uchun jiddiy xavf tug‘dirmoqda. Phishing, ijtimoiy muhandislik, SQL injection, cross-site scripting kabi hujumlar orqali noqonuniy kirishlar, ma’lumot o‘g‘irliklari va xizmat ko‘rsatishni to‘xtatib qo‘yish (DDoS) hodisalari tez-tez uchrab turadi. Bu holatlar nafaqat moliyaviy zarar, balki tashkilotlarning obro‘sigam salbiy ta’sir ko‘rsatadi. Axborot xavfsizligini ta’minlash web texnologiyalarining rivojlanishida muhim omil hisoblanadi. Zamonaviy xavfsizlik standartlari va texnik vositalar yordamida ushbu muammolarni kamaytirish va oldini olish mumkin. Shu bois, web texnologiyalar va axborot xavfsizligi sohasidagi ilmiy izlanishlar jadal sur’atlarda olib borilmoqda.

Web texnologiyalarining rivojlanishi. Web texnologiyalari bugungi kunda oddiy statik sahifalardan tortib, sun'iy intellekt asosida ishlovchi dinamik veb-ilovalargacha rivojlandi. HTML5, CSS3, JavaScript, React, Angular, Vue.js kabi texnologiyalar orqali foydalanuvchi uchun qulay, tezkor va interaktiv sahifalar yaratish mumkin bo'ldi. Shuningdek, bulutli texnologiyalar (Cloud Computing), mobil ilovalar va API xizmatlari web imkoniyatlarni yanada kengaytirdi. Ayniqsa, elektron tijorat (e-commerce), onlayn bank xizmatlari va masofaviy ta'lim platformalari web texnologiyalar asosida rivojlanib, global iqtisodiyotning ajralmas qismiga aylandi. Foydalanuvchilarning shaxsiy ma'lumotlari (ism, manzil, bank rekvizitlari) ko'plab web saytlarda saqlanmoqda. Ularning noto'g'ri qo'llarga tushishi yirik moliyaviy va ijtimoiy muammolarga olib kelishi mumkin. Firibgarlar foydalanuvchilarning ishonchini suiiste'mol qilib, ularni yolg'on saytlar orqali ma'lumotlarini berishga undashmoqda. Bu eng keng tarqalgan hujum turlaridan biridir. SQL injection, XSS (Cross Site Scripting), CSRF (Cross Site Request Forgery) kabi hujumlar veb-ilovalar orqali axborotga noqonuniy kirish imkonini beradi. Bu esa nafaqat foydalanuvchilar, balki butun kompaniya uchun katta xavf tug'diradi.

Alohida serverlarga yoki butun tarmoqqa hujum qilib, xizmatni to'xtatish yoki ma'lumotlarni shifrlab qo'yish orqali foydalanuvchilardan to'lov talab qilinmoqda. Axborot xavfsizligini ta'minlash uchun quyidagi choralarni ko'rish zarur:

- Shifrlash (Encryption): Ma'lumotlar almashinuvida HTTPS protokolidan foydalanish va saqlanayotgan ma'lumotlarni shifrlash.
- Autentifikatsiya va avtorizatsiya: Kuchli parollar, ikki bosqichli autentifikatsiya (2FA) va rolga asoslangan kirish nazoratini joriy etish.
- Doimiy yangilanish: Dasturiy ta'minot va tizimlarni muntazam yangilab borish orqali zaifliklarni bartaraf etish.
- Xodimlarni o'qitish: Axborot xavfsizligiga oid treninglar tashkil qilish orqali xodimlarning xabardorligini oshirish.
- Zaxira nusxalar: Ma'lumotlarni muntazam zaxiralash orqali kutilmagan holatlarda ularni tiklash imkoniyatini yaratish.

Web texnologiyalarining rivojlanishi insoniyatga katta qulayliklar yaratmoqda, biroq bu bilan birga axborot xavfsizligini ta'minlash masalasi tobora muhimlashib bormoqda. Har bir tashkilot, dasturchi va foydalanuvchi axborot himoyasiga jiddiy yondashishi zarur. Faqat shunda biz texnologik yutuqlardan to'laqonli va xavfsiz foydalana olamiz.

Materiallar va uslublar. Ushbu maqola web texnologiyalarining rivojlanishi va axborot xavfsizligi masalalarini nazariy jihatdan tahlil qilishga qaratilgan. Tadqiqot davomida quyidagi metodologik yondashuvlar qo'llanildi. Maqola tayyorlanishida so'nggi yillarda chop etilgan ilmiy maqolalar, xalqaro konferensiya materiallari, axborot

xavfsizligi bo'yicha standartlar (masalan, ISO/IEC 27001), hamda ilg'or mutaxassislar bloglari va yangilik portallaridagi ma'lumotlardan foydalanildi. Turli veb-xavfsizlik tahdidlari (phishing, SQL injection, XSS, DDoS) va ularni oldini olish usullari o'zaro taqqoslab chiqildi. Har bir xavf turi uchun zamonaviy himoya mexanizmlari (shifrlash, autentifikatsiya, xavfsiz kod yozish amaliyotlari) ko'rib chiqildi.

Maqolada axborot xavfsizligiga oid real hayotdan olingan misollar — mashhur kiberhujumlar, veb-ilovalar orqali amalga oshirilgan ma'lumot o'g'irliklari — asosida muammolar chuqurroq yoritildi. Bu misollar orqali muammolarning oqibatlari va muqobil yechimlar ko'rsatildi. Web texnologiyalarining rivojlanish tendensiyalari va kiberxavfsizlikka bo'lgan ehtiyoj o'rtasidagi bog'liqlik o'rganildi. Axborot xavfsizligini ta'minlash uchun kerak bo'ladigan texnik, tashkiliy va huquqiy choralarga doir tavsiyalar ishlab chiqildi.

Tadqiqot muhokamasi. Ushbu tadqiqotda web texnologiyalarining tezkor rivojlanishi va axborot xavfsizligi sohasidagi dolzarb muammolar o'rganildi. Tadqiqot natijalari shuni ko'rsatdiki, veb-ilovalar va internet xizmatlarining kengayishi foydalanuvchilar uchun ko'plab qulayliklar yaratgani bilan birga, yangi kiberxavfsizlik tahdidlarini ham yuzaga keltirmoqda. Xususan, phishing, SQL injection, XSS, va DDoS kabi hujumlar sohada eng keng tarqalgan va zararli tahdidlar sifatida ajralib turadi. Adabiyotlar va amaliy misollar tahlili shuni ko'rsatdiki, ko'plab tashkilotlar va veb-resurs egalarining axborot xavfsizligini ta'minlash borasidagi yondashuvlari yetarli darajada emas. Ko'p hollarda zaif xavfsizlik siyosatlari, yangilanishlarning kechikishi va xavfsiz kod yozilishidagi kamchiliklar kiberhujumlarning muvaffaqiyatli amalga oshishiga imkon yaratmoqda. Shu bilan birga, foydalanuvchilarning xavfsizlik bo'yicha yetarlicha bilimga ega emasligi phishing va ijtimoiy muhandislik kabi hujumlarning keng tarqalishiga olib kelmoqda.

Bundan tashqari, zamonaviy texnologiyalar, masalan, ikki bosqichli autentifikatsiya, kuchli shifrlash usullari va bulutli xavfsizlik echimlari kiberxavfsizlikni oshirishda muhim rol o'ynashi aniqlandi. Ammo, ushbu texnologiyalarni joriy etishda tashkilotlar tomonidan yetarli e'tibor qaratilmayapti, bu esa ularning samaradorligini pasaytiradi. Tadqiqot natijalari shuni ham ko'rsatadiki, axborot xavfsizligi faqat texnik choralardan iborat emas, balki tashkiliy va huquqiy jihatlar ham muhim ahamiyatga ega. Xodimlarning muntazam o'qitilishi, xavfsizlik siyosatlarining ishlab chiqilishi va xalqaro standartlarga mos keluvchi tizimlarning joriy etilishi muhim omillardir. Umuman olganda, web texnologiyalarining rivojlanishi bilan birga xavfsizlik masalalarini yanada chuqur o'rganish, yangi himoya mexanizmlarini ishlab chiqish va ularni amaliyotga tatbiq etish dolzarb vazifa sifatida qolmoqda. Tadqiqot shuni ko'rsatdiki, xavfsizlikni

ta'minlash uchun texnologik yechimlar, inson omili va boshqaruv tizimlarining birgalikda ishlashi zarur.

Xulosa. Web texnologiyalarining so'nggi yillardagi jadal rivojlanishi hayotimizni qulayroq va samaraliroq qilish bilan birga, axborot xavfsizligi sohasidagi muammolarni ham yanada murakkablashtirmoqda. Veb-ilovalarning keng qo'llanilishi natijasida foydalanuvchilarning shaxsiy va moliyaviy ma'lumotlarini himoya qilish masalasi dolzarb ahamiyat kasb etmoqda. Phishing, SQL injection, XSS, DDoS kabi kiberhujumlar xavfsizlikning eng katta tahdidlaridan biri hisoblanadi. Ushbu maqolada kiberxavfsizlikning asosiy tahdid turlari tahlil qilinib, ularni oldini olish uchun zamonaviy texnik va tashkiliy choralar ko'rsatildi. Shifrlash, ikki bosqichli autentifikatsiya, xavfsiz kod yozish va tizimlarni muntazam yangilab borish kabi usullar axborot xavfsizligini ta'minlashda muhim rol o'ynaydi. Shunday qilib, web texnologiyalarining rivojlanishi bilan bog'liq kiberxavfsizlik muammolarini hal qilish uchun mutaxassislar, tashkilotlar va foydalanuvchilar o'zaro hamkorlikda harakat qilishi zarur. Faqat shu yo'l bilan biz xavfsiz va ishonchli onlayn muhit yaratib, texnologik yutuqlardan to'laqonli foydalanishimiz mumkin.

Foydalanilgan adabiyotlar

1. OWASP Foundation. (2023). Web ilovalar xavfsizligi – OWASP Top Ten tahdidlar ro'yxati. <https://owasp.org/www-project-top-ten/>
2. ISO/IEC 27001:2013. (2013). Axborot xavfsizligini boshqarish tizimlari – Talablar. Xalqaro Standartlar Tashkiloti.
3. Stollings, U. (2020). Kriptografiya va tarmoq xavfsizligi: printsiplar va amaliyot (8-nashr). Pearson.
4. Laudon, K.K., va Laudon, J.P. (2022). Axborot tizimlarini boshqarish: raqamli davrda boshqarish. Pearson.
5. Shnayyer, B. (2015). Ma'lumotlar va Goliath: Sizning ma'lumotlaringizni yig'ish va nazorat qilishdagi yashirin kurash. W. W. Norton & Company.
6. Smit, R., va Marchesini, J. (2021). Kiberxavfsizlik boshlovchilar uchun. Apress.
7. Kizza, J.M. (2019). Kompyuter tarmoqlari xavfsizligi bo'yicha qo'llanma. Springer.