DASTURIY TA‘MINOT XAVSIZLIGI.

Zaxro Salimova Ulug‘bek qizi
Alfraganus universiteti Raqamli Texnologiyalar fakulteti kompyuter injenering yunalishi 3-kurs KI-23-1 guruh talabasi
G’anixojayeva Dilfuza
Fan o'qtuvchisi:

Annotatsiya: *Mazkur maqolada dasturiy ta’minot xavfsizligini ta’minlashning nazariy asoslari, amaliy yondashuvlari va zamonaviy talablar yoritiladi. Dasturiy ta’minotning xavfsizligi tizimning ishonchliligi, himoyalanganligi, uzluksiz ishlashi hamda ma’lumotlarning butligi va maxfiyligini saqlashda muhim omil hisoblanadi. Maqolada xavfsizlikka tahdidlarning turlari, zaifliklarni aniqlash usullari, himoya mexanizmlari, kriptografiya, autentifikatsiya, avtorizatsiya, monitoинг va testlash kabi jarayonlar batafsil ko‘rib chiqiladi. Shuningdek, global miqyosdagi kiberxavfsizlik tendensiyalari, xalqaro standartlar va amaliyotlar asosida dasturiy ta’minotni xavfsiz loyihalash, ishlab chiqish va ekspluatatsiya qilish bo‘yicha asosiy tamoyillar tahlil qilinadi.*

Kalit so‘zlar: *Dasturiy ta’minot xavfsizligi, kiberxavfsizlik, zaifliklar, tahdidlar, himoya mexanizmlari, kriptografiya, autentifikatsiya, avtorizatsiya.*

Zamonaviy raqamli texnologiyalar davrida dasturiy ta’minot barcha sohalarning ajralmas qismiga aylangan bo‘lib, iqtisodiyot, tibbiyot, ta’lim, transport, moliya va davlat boshqaruvi kabi tizimlarning asosiy faoliyati to‘liq yoki qisman dasturiy mahsulotlarga tayanadi.

Ushbu jarayonning keskin kengayishi bilan birga dasturiy tizimlar xavfsizligini ta’minlash masalasi global miqyosdagi muammolardan biriga aylandi. Chunki har qanday dasturiy ta’minotning ishonchli faoliyati uning funksional imkoniyatlari bilan bir qatorda yuqori darajadagi himoyalanganlik talablariga ham bog‘liqdir.

Ma’lumotlar oqimi hajmining oshishi, ochiq tarmoqlardan keng foydalanish, mobil ilovalar sonining keskin ortishi, sun’iy intellekt va bulut texnologiyalarining rivojlanishi dasturiy mahsulotlarga nisbatan xavfsizlik talablarini yanada kuchaytirmoqda.

Hozirgi kunda kiberxavfsizlik bo‘yicha xalqaro tashkilotlar tomonidan qayd etilishicha, har yili millionlab kiberhujumlar sodir bo‘lib, ularning katta qismi aynan dasturiy ta’minotdagi zaifliklardan foydalanadi. Tahlillar shuni ko‘rsatadiki, mavjud zaifliklarning qariyb 65 foizi dastur ishlab chiqish bosqichida xavfsizlik tamoyillariga yetarli darajada amal qilinmagani natijasida yuzaga keladi.

Bu esa dasturiy ta’minotni xavfsiz tarzda loyihalash, kodlash va testlashni har bir loyiha uchun majburiy talabga aylantiradi. Katta korporatsiyalar, banklar va davlat organlarida kuzatilgan yirik ma’lumotlar sizib chiqishi holatlari zamonaviy xavfsizlikka yondashuvlar yetarlicha mukammal bo‘lmagan taqdirda katta moliyaviy zarar va ishonch yo‘qotilishiga olib kelishini amalda isbotlamoqda.

Dasturiy ta’minot xavfsizligi tushunchasi nafaqat tizimni tashqi hujumlardan himoya qilish, balki ichki xatolar, foydalanuvchi xatti-harakatlari, noto‘g‘ri konfiguratsiya, ruxsatsiz kirish, zararli kodlar, viruslar, tarmoq tahdidlari va ekspluatatsiya jarayonida yuzaga kelishi mumkin bo‘lgan boshqa xavf omillarini ham qamrab oladi. Shu sababli dasturiy mahsulotni yaratish jarayonining har bir bosqichi: tahlil, dizayn, kodlash, testlash, joriy etish va ekspluatatsiya davomida xavfsizlik mezonlariga qat’iy amal qilinishi zarur. Ayniqsa, “Security by Design” va “Secure Coding” tamoyillarining joriy etilishi zamonaviy dasturlash metodologiyalarining ajralmas qismiga aylangan.Shuningdek, global miqyosda kiberxavfsizlik standartlari, audit tizimlari, sertifikatlashtirish va monitoring mexanizmlarining takomillashib borayotgani ham dasturiy ta’minot xavfsizligining dolzarbligini oshirmoqda. Bugungi kunda ISO/IEC 27001, OWASP, NIST kabi yirik standartlar va metodologiyalar dasturiy tizimlarni himoyalashda asosiy qo‘llanma sifatida qo‘llaniladi. Bu standartlar dasturiy ta’minot ishlab chiqaruvchilar oldiga aniq talab va mezonlar qo‘yadi hamda ularning xavfsiz mahsulot yaratishiga yordam beradi.Yuqoridagi omillar shuni ko‘rsatadiki, dasturiy ta’minotni xavfsiz yaratish bugungi kunda nafaqat texnik jarayon, balki strategik ahamiyatga ega bo‘lgan kompleks faoliyatdir. Bu informatika va axborot texnologiyalari sohasida tahsil olayotgan talabalar, dasturchilar, tizim administratorlari, kiberxavfsizlik mutaxassislari va barcha IT soha vakillari uchun muhim o‘rganish yo‘nalishi sanaladi.

Bugungi kunda dasturiy ta’minot har bir sohada muhim rol o‘ynamoqda. Moliyadan tortib, tibbiyot, transport, ta’lim va davlat boshqaruvigacha bo‘lgan tizimlar dasturiy mahsulotlarga tayanadi. Shu bilan birga, dasturiy ta’minot turli xavf-xatarlar ostida qoladi. Ma’lumotlarga ko‘ra, 2024 yilda dunyo bo‘yicha millionlab kiberhujumlar sodir bo‘lgan. O‘rtacha bir tashkilot haftasiga 1 636 ta hujumga duch kelgan. Bu esa har 39 soniyada hujum amalga oshishini anglatadi.Kiberhujumlar natijasida global iqtisodiy zarar 10 trillion dollarni oshishi kutilmoqda. Dasturiy komponentlar, API’lar va ilovalar orqali amalga oshiriladigan hujumlar tobora ko‘paymoqda. 2024 yilda 22 254 ta yangi zaiflik qayd etilgan va bu 2023 yilga nisbatan 30 foizga ko‘paygan. Shuningdek, phishing hujumlari tashkilotlarda eng ko‘p sodir bo‘ladigan xavf turidir. 2023 yilda tashkilotlarning 83 foizi phishing hujumlariga duch kelgan. Global hujumlar soni yil davomida 75 foizga oshgan.Hududiy statistikaga qaraganda ham vaziyat jiddiy. Afrika mintaqasida tashkilotlar o‘rtacha haftasiga 3 370 hujumga duch kelgan. Lotin Amerikasi va Osiyo-Tinch okeani mintaqalarida ham hujumlar sezilarli ko‘tarilgan. Bu raqamlar dasturiy ta’minot xavfsizligini ta’minlashning muhimligini ko‘rsatadi.Shuning uchun dasturiy ta’minotni loyihalashdan tortib kodlash, testlash va ekspluatatsiya qilishgacha bo‘lgan jarayonlarda xavfsizlik tamoyillarini qo‘llash zarur. Masalan, “Security by Design”, xavfsiz kodlash, muntazam yangilanish va tizim monitoringi kabi yondashuvlar bugungi kunda dolzarb. Ilgari faqat tizimning funksionalligi va ishlash tezligi muammo bo‘lgan bo‘lsa, hozir ma’lumotlar maxfiyligi, tizim izchilligi va tahdidlarga chidamlilik muhim omil hisoblanadi.Mahalliy sharoitda ham dasturiy mahsulotlarni yaratishda xavfsizlik standartlari va himoya mexanizmlarini tatbiq etish talab etiladi. Shu sababli dasturiy ta’minot xavfsizligi faqat texnik masala emas, balki tashkilot, loyiha va biznes strategiyasi nuqtai nazaridan ham muhim ahamiyatga ega.

Dasturiy ta’minot xavfsizligi zamonaviy axborot texnologiyalari sohasidagi eng muhim masalalardan biridir. Xavfsizlik tushunchasi nafaqat tashqi kiberhujumlardan himoya qilishni, balki ichki xatolar, noto‘g‘ri konfiguratsiyalar, foydalanuvchi xatti-harakatlari va zararli kodlar bilan bog‘liq tahdidlarni ham qamrab oladi. Shu sababli dasturiy mahsulotni yaratish jarayonining har bir bosqichi tahlil, dizayn, kodlash, testlash, joriy etish va ekspluatatsiya xavfsizlik talablarini inobatga olgan holda amalga oshirilishi lozim.Dasturiy ta’minot xavfsizligini ta’minlashning asosiy yondashuvlaridan biri “Security by Design” prinsipi bo‘lib, bu tizimni loyihalash bosqichida xavfsizlik choralarini kiritishni anglatadi. Ushbu yondashuv orqali dasturiy mahsulot yaratilayotgan vaqtda zaifliklar aniqlanadi va ularga qarshi oldindan chora ko‘riladi. Shu bilan birga, xavfsiz kodlash (Secure Coding) tamoyili dasturchilarga kod yozishda potentsial xatoliklarni kamaytirish, ma’lumotlarning himoyalanishini ta’minlash va tizimni barqaror ishlashini kafolatlash imkonini beradi.Autentifikatsiya va avtorizatsiya mexanizmlari dasturiy ta’minotning yana bir muhim tarkibiy qismidir. Autentifikatsiya foydalanuvchini tizimga kirishdan oldin tekshirishni, avtorizatsiya esa foydalanuvchining tizim ichidagi resurslarga kirish huquqini boshqarishni ta’minlaydi. To‘g‘ri ishlangan autentifikatsiya va avtorizatsiya tizimlari tizimni ruxsatsiz kirishlardan, ma’lumotlar o‘g‘irlanishidan va boshqa xavflardan samarali himoya qiladi.Kriptografiya ham dasturiy ta’minot xavfsizligida katta ahamiyatga ega. Ma’lumotlarni shifrlash, elektron imzo, xavfsiz kommunikatsiya protokollari orqali uzatilayotgan ma’lumotlar himoyalanadi. Bugungi kunda TLS/SSL protokollari, AES shifrlash algoritmi, RSA va ECC kabi algoritmlar keng qo‘llaniladi. Shifrlash orqali ma’lumotlar maxfiyligi saqlanadi, ularni ruxsatsiz foydalanuvchi o‘qiy olmaydi.Dasturiy ta’minotning ekspluatatsiyasi davomida xavfsizlikni ta’minlash uchun monitoring va audit tizimlari joriy qilinadi. Tizimning real vaqt rejimida kuzatilishi, har qanday shubhali harakatlar yoki zaifliklar aniqlanganda darhol choralar ko‘rilishi, xavfsizlikni yuqori darajada saqlashga yordam beradi. Shu bilan birga muntazam yangilanishlar (Patch Management) tizimning zaifliklardan himoyalanishini ta’minlaydi va yangi tahdidlarga qarshi chidamliligini oshiradi.Dasturiy ta’minot xavfsizligini oshirishda dizayn naqshlarining roli ham katta. Masalan, Observer, Singleton, Adapter kabi naqshlar tizimning xavfsizlik jihatlarini yaxshilash, modul va komponentlar orasidagi bog‘liqlikni kamaytirish, shuningdek, xatoliklar yuzaga kelish ehtimolini kamaytirish imkonini beradi.Shuningdek, xavfsizlik testlashning ahamiyati ham katta.

FOYDALANILGAN ADABIYOTLAR:

1. Pfleeger, C., Pfleeger, S. Security in Computing. – New Jersey: Prentice Hall, 2015.
2. Stallings, W. Cryptography and Network Security: Principles and Practice. – Pearson, 2020.
3. McGraw, G. Software Security: Building Security In. – Addison-Wesley, 2006.
4. Viega, J., McGraw, G. Building Secure Software. – Addison-Wesley, 2001.
5. OWASP Foundation. OWASP Top Ten Project. – Online, 2023.
6. ISO/IEC 27001: Information Security Management Systems. – International Standard, 2013.

7. NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. – NIST, 2020.

8. Rouse, M. Cybersecurity Statistics and Trends. – TechTarget, 2024.

9. Kaspersky Lab. Global IT Security Threats Report. – 2023.

10.O‘zbekiston Respublikasi Axborot Texnologiyalari va Kiberxavfsizlik Agentligi statistik ma’lumotlari. – Toshkent, 2024.