KIBERXAVFSIZLIK TEXNOLOGIYALARINING ZAMONAVIY TENDENSIYALARI

Nabiyeva Dilrabo Abduraupovna
Iqtisodiyot va Pedagogika Universiteti o'qtuvchisi
Urinov Shoxboz Ergash o'g'li
Iqtisodiyot va Pedagogika Universiteti Filologiya tillarni o'qitish (Rus tili) yunalishi talabasi

Annotasiya: *Kiberxavfsizlik texnologiyalarining zamonaviy tendensiyalari bugungi kunda tezkor rivojlanish va yangi xavf-xatarlar bilan bog'liq. Texnologiyalar va internet tarmoqlarining kengayishi bilan birga, kiberxavfsizlik sohasidagi tahdidlar ham tobora murakkablashmoqda. Sun'iy intellekt (SI) va mashinaviy o'qitish (MO) texnologiyalari xavfsizlikni yanada samarali qilishda muhim rol o'ynamoqda, chunki ular tarmoqdagi tahdidlarni aniqlash va ularga tezkor javob berish imkonini beradi.*

Kalit so'zlar: *Kiberxavfsizlik, Zero Trust, Sun'iy intellect, Ransomware, Kriptografiya, Ma'lumotlarni himoya qilish, Cloud security, IoT xavfsizligi, Xavfsizlik tarmog'I, Kiberhujumlar.*

Annotation. *Modern trends in cyber security technologies today are associated with rapid development and new threats. As technology and internet networks expand, so do cyber security threats. Artificial intelligence (AI) and machine learning (ML) technologies are playing an important role in making security more effective, as they enable detection of network threats and rapid response to them.*

Keywords: *Cyber Security, Zero Trust, Artificial Intelligence, Ransomware, Cryptography, Data Protection, Cloud Security, IoT Security, Security Network, Cyber Attacks.*

Kirish. Kiberxavfsizlik sohasidagi zamonaviy tendensiyalar doimiy ravishda o'zgarib bormoqda, chunki texnologiyalar va tarmoqlar rivojlanib, yangi tahdidlar

paydo bo'layotgan bir paytda, ularni oldini olish va ularga qarshi kurashish uchun ilg'or texnologiyalarni qo'llash zarurati ortmoqda. Quyidagi tendensiyalar kiberxavfsizlikning hozirgi rivojlanish yo'nalishlarini aks ettiradi.

Sun'iy intellekt va mashinaviy o'qitish: Sun'iy intellekt (SI) va mashinaviy o'qitish (MO) texnologiyalari kiberxavfsizlikda tahdidlarni aniqlash va ularga qarshi kurashishning yangi usullarini yaratmoqda. SI tizimlari tarmoqdagi noma'lum va yangi xavflarni aniqlashda samarali bo'lib, avtomatik ravishda xavf-xatarlarni tahlil qilish va ularga tezkor javob berish imkoniyatini beradi. MO yordamida tizimlar o'z vaqtida yangi tahdidlarni o'rganib, o'z-o'zini yangilash va moslashish qobiliyatiga ega bo'ladi.

Zero Trust (Hech qanday ishonch yo'q) yondoshuvi: Zero Trust modeli kiberxavfsizlikni ta'minlashda yangi yondoshuv sifatida paydo bo'ldi. Ushbu yondoshuvda tarmoqda hech qanday qurilmaga, foydalanuvchiga yoki tizimga ishonch berilmaydi, shuning uchun har bir so'rov va harakat doimiy ravishda tekshiriladi. Bu modelning asosiy g'oyasi, foydalanuvchi yoki qurilmaning ichki yoki tashqi bo'lishidan qat'i nazar, har bir faoliyatni tekshirish va tasdiqlash zarurati hisoblanadi.

Bulutli xavfsizlik: Bulutli xizmatlar tobora ommalashgan sari, ularning xavfsizligini ta'minlash ham muhim ahamiyat kasb etmoqda. Bulutli xavfsizlik, bulutda saqlanayotgan ma'lumotlar va resurslarni himoya qilish uchun ilg'or texnologiyalarni qo'llashni talab qiladi. Bu, ayniqsa, korporativ ma'lumotlar, mijozlar ma'lumotlari va muhim tizimlarning xavfsizligini ta'minlashda dolzarb masaladir. Bulutda xavfsizlikni boshqarish uchun ko'plab vositalar, masalan, shifrlash, autentifikatsiya va monitoring tizimlari ishlatiladi.

IoT xavfsizligi: Internet of Things (IoT) qurilmalari har kuni ko'payib bormoqda, bu esa yangi xavf-xatarlarni keltirib chiqaradi. IoT qurilmalari o'zaro tarmoq orqali bog'lanib, ularga kirish imkoniyatini yaratadi. Bu qurilmalarning xavfsizligini ta'minlash uchun maxsus protokollar va himoya tizimlari ishlab chiqilmoqda. IoT xavfsizligi, asosan, qurilmalarning shifrlanishi, autentifikatsiyasi va tarmoqdagi faoliyatni kuzatish bilan bog'liq.

Ransomware hujumlari: Ransomware (talabnomali zararli dasturlar) kiberxavfsizlikdagi eng katta tahdidlardan biri bo'lib qolmoqda. Bu hujumlar qurilmalar va tizimlarni blokirovka qilish yoki ma'lumotlarni shifrlash orqali amalga oshiriladi, va keyinchalik hujumni amalga oshirgan shaxslar ma'lumotlarni qaytarib olish uchun pul talab qiladilar. Yangi kiberxavfsizlik texnologiyalari bu turdagi hujumlarni aniqlash va ularga qarshi kurashish uchun ilg'or himoya vositalarini taklif etmoqda.

Xavfsizlikni boshqarish tizimlari (SIEM): SIEM (Security Information and Event Management) tizimlari xavfsizlikni boshqarish va kuzatish uchun ishlatiladi. SIEM tizimlari tarmoqdagi barcha xavfsizlik voqealarini bir joyga to'playdi, ular tahlil qilinadi va xatoliklar yoki tahdidlar aniqlanadi. Bu tizimlar, shuningdek, kiberhujumlar va ichki xavf-xatarlarni aniqlash uchun real vaqt rejimida ishlaydi.

Xavfsizlikni avtomatlashtirish: Kiberxavfsizlikni avtomatlashtirish texnologiyalari xavfsizlik jarayonlarini tezlashtirish va samarali qilishga yordam beradi. Avtomatlashtirilgan tizimlar tahdidlarni aniqlash, ularga javob berish va xavfsizlikni yangilashni tezda amalga oshiradi. Bu jarayonlarni avtomatlashtirish, ayniqsa, katta tarmoqlar va tizimlar uchun zarur, chunki ularning xavfsizligini qo'lda boshqarish qiyin bo'lishi mumkin.

Shifrlash va maxfiylik: Ma'lumotlarni shifrlash va foydalanuvchi maxfiyligini ta'minlash kiberxavfsizlikning asosiy elementlaridan biridir. Shifrlash, ma'lumotlarni xavfsiz tarzda uzatish va saqlash imkonini beradi, shu bilan birga, ma'lumotlarni o'g'irlash yoki manipulyatsiya qilishning oldini oladi. Maxfiylikni himoya qilish, ayniqsa, shaxsiy ma'lumotlar va moliyaviy tranzaksiyalarni himoya qilishda muhimdir.

Kiberxavfsizlik texnologiyalari turli sohalar va tizimlar o'rtasida integratsiyani talab qiladi. Xavfsizlikni ta'minlashda hamkorlik va tizimlar o'rtasidagi o'zaro aloqalar muhim ahamiyatga ega. Bu, ayniqsa, global tarmoqlar va bulutli xizmatlar orqali ma'lumotlarni almashish va ularni himoya qilishda dolzarbdir.

Kiberxavfsizlik texnologiyalarining zamonaviy tendensiyalari texnologiyalar va tahdidlarning tezkor o'zgarishiga moslashgan holda rivojlanmoqda. Sun'iy intellekt, zero trust arxitekturasi, bulutli xavfsizlik va IoT xavfsizligi kabi yangi yondoshuvlar kiberxavfsizlikni ta'minlashda innovatsion imkoniyatlarni yaratmoqda. Kiberhujumlar, xususan ransomware va DDoS hujumlari, yangi texnologiyalarni ishlab chiqishni va xavfsizlikni yanada kuchaytirishni talab qilmoqda. Kelajakda kiberxavfsizlik texnologiyalarining rivojlanishi va yangi yondoshuvlar xavfsizlikni yanada samarali qilishda davom etadi.

Kiberxavfsizlik texnologiyalarining zamonaviy tendensiyalari doirasida yana bir qancha muhim yo'nalishlar va rivojlanishlar mavjud. Kiberxavfsizlik sohasidagi yangi yondoshuvlar va texnologiyalar tahdidlarni aniqlash, oldini olish va ularga qarshi kurashishda yanada samarali vositalarni taqdim etadi. Quyida kiberxavfsizlikning yana bir qancha zamonaviy tendensiyalari keltirilgan.

Tarmoqlarni segmentatsiya qilish, ya'ni tarmoqni kichikroq va xavfsizroq qismlarga ajratish, xavfsizlikni yaxshilashning samarali usuli hisoblanadi. Har bir segmentda xavfsizlikni mustahkamlash va tarmoqdagi potentsial tahdidlarga qarshi samarali choralar ko'rish mumkin. Tarmoqni segmentatsiya qilish orqali, agar biror qismini buzib kirishsa, butun tizimni xavf ostiga qo'yishning oldini olish mumkin.

Zamonaviy tashkilotlar kiberhujumlarni simulyatsiya qilish va sinovdan o'tkazish orqali o'z tizimlarining zaif joylarini aniqlashga harakat qilmoqda. Bu usul "Red Team" (hujumchi guruh) va "Blue Team" (himoya guruh) usullariga asoslanadi. Red Team tizimni buzishga urinishadi, Blue Team esa bu hujumlarga qarshi himoya qiladi. Bu amaliyotlar orqali kiberhujumlarning oldini olish va tizimni mustahkamlash mumkin.

Blockchain texnologiyasi kiberxavfsizlikda yangi imkoniyatlar yaratmoqda. Blockchainning xususiyatlari, masalan, ma'lumotlarni o'zgartirishning imkonsizligi va tarqatilgan tizimda saqlanishi, uni ma'lumotlarni xavfsiz saqlash va himoya qilishda foydali qiladi. Kiberxavfsizlikda blockchain, ayniqsa, identifikatsiya va autentifikatsiya tizimlarida, shuningdek, ma'lumotlarni saqlash va uzatishda qo'llanilmoqda.

Raqamli identifikatsiya va biometrik autentifikatsiya texnologiyalari kiberxavfsizlikda eng yangi va samarali vositalardan biri hisoblanadi. Biometrik tizimlar, masalan, barmoq izlari, yuzni tanish, irisni skanerlash kabi usullar foydalanuvchilarni aniqlashda xavfsizlikni oshiradi. Bu texnologiyalarni qo'llash orqali foydalanuvchilarning identifikatsiyasi yanada ishonchli va xavfsiz bo'ladi.

Kiberxavfsizlikning samarali boshqarilishi uchun barcha xavfsizlik vositalarini birlashtirish zarur. SIEM (Security Information and Event Management) tizimlari xavfsizlikni boshqarish va tahlil qilishda yordam beradi, ammo ularni boshqa xavfsizlik tizimlari bilan integratsiya qilish, masalan, IDS/IPS (Intrusion Detection/Prevention Systems), firewall, va DLP (Data Loss Prevention) tizimlari bilan birlashtirish, yanada kuchliroq himoya tizimini yaratadi. Bunday integratsiya tizimlar o'rtasida o'zaro aloqalarni va tezkor javob berishni ta'minlaydi.

Mobil qurilmalar va ilovalar kiberxavfsizlikning yangi muammolarini keltirib chiqarmoqda. Ularning xavfsizligini ta'minlash uchun maxsus mobil xavfsizlik texnologiyalari ishlab chiqilmoqda. Mobil ilovalar uchun xavfsizlik protokollari, shifrlash, autentifikatsiya va xavfsizlikni monitoring qilish kabi vositalar mavjud. Mobil qurilmalar va ilovalar foydalanuvchilari uchun maxfiylikni saqlash va himoya qilish uchun yangi standartlar va texnologiyalar ishlab chiqilmoqda.

Tarmoqni monitoring qilish va xavf-xatarlarni aniqlash zamonaviy kiberxavfsizlikning ajralmas qismiga aylangan. Tarmoqda sodir bo'layotgan barcha voqealarni real vaqt rejimida kuzatish, ma'lumotlarni tahlil qilish va tahdidlarni aniqlash uchun ilg'or vositalar ishlab chiqilmoqda. Bu tizimlar tarmoqdagi har bir harakatni kuzatadi va noma'lum yoki shubhali faoliyatni darhol aniqlaydi, shuningdek, tahdidga qarshi tezkor javob beradi.

Kiberxavfsizlikni avtomatlashtirish texnologiyalari tahdidlarni tezda aniqlash va ularga qarshi kurashish imkoniyatini beradi. Sun'iy intellekt (SI) va mashinaviy o'qitish (MO) algoritmlari yordamida xavfsizlik tizimlari tahdidlarni o'z vaqtida aniqlash va ularga avtomatik javob berish imkoniyatiga ega bo'ladi. Bu,

ayniqsa, katta tarmoqlar va korporativ tizimlar uchun muhimdir, chunki ular ko'plab tahdidlarni va xavf-xatarlarni tezda tahlil qilishni talab qiladi.

Raqamli huquqlar va shaxsiy ma'lumotlarni himoya qilish kiberxavfsizlikning muhim yo'nalishlaridan biridir. Yangi qonunlar va me'yorlar, masalan, GDPR (General Data Protection Regulation) va CCPA (California Consumer Privacy Act), shaxsiy ma'lumotlarni himoya qilishni kuchaytirishga qaratilgan. Bu qonunlar tashkilotlarga foydalanuvchilarning shaxsiy ma'lumotlarini qanday yig'ish, saqlash va ulardan foydalanishni boshqarish bo'yicha aniq talablar qo'yadi.

Kiberxavfsizlikning samarali bo'lishi uchun xodimlar va foydalanuvchilarni ta'limlash va xabardor qilish zarur. Kiberxavfsizlikka oid treninglar va kurslar, xodimlarga xavfsizlik protokollarini to'g'ri qo'llashni, phishing va boshqa xakerlik usullaridan ehtiyot bo'lishni o'rgatadi. Kiberxavfsizlikni ta'minlashning muvaffaqiyatli bo'lishi uchun barcha darajadagi xodimlar va foydalanuvchilar o'z vazifalarini bilishlari kerak.

Kiberxavfsizlik texnologiyalarining zamonaviy tendensiyalari doimo o'zgarib bormoqda va yangi tahdidlar paydo bo'lgani sayin, ularni oldini olish va xavfsizlikni ta'minlash uchun ilg'or texnologiyalarni qo'llash zarurati ortmoqda. Yangi usullar, masalan, sun'iy intellekt, zero trust yondoshuvi, blockchain va mobil xavfsizlik, kiberxavfsizlikning samarali bo'lishiga yordam beradi. Bunday texnologiyalar kiberhujumlarni aniqlash va ularga qarshi kurashishda yanada kuchliroq vositalar yaratadi, bu esa tashkilotlar va foydalanuvchilarning xavfsizligini oshiradi.

Zero Trust (ZT) arxitekturasi — bu kiberxavfsizlikning eng yangi va samarali yondoshuvlaridan biri hisoblanadi. ZT yondoshuvi "Hech kimga ishonma" degan prinsipga asoslanadi. Tarmoqdagi barcha foydalanuvchilar va qurilmalar har doim tekshiriladi, va faqat kerakli ruxsatlar bilan ishlashga imkoniyat beriladi. Bu yondoshuvni amalga oshirishda foydalanuvchi autentifikatsiyasi, shifrlash, va ma'lumotlar oqimini to'liq nazorat qilish muhim o'rin tutadi. Zero Trust arxitekturasi,

ayniqsa, masofaviy ishchilar va bulutli muhitda xavfsizlikni ta'minlashda samarali hisoblanadi.

Ransomware hujumlari so'nggi yillarda kiberxavfsizlikning asosiy tahdidlariga aylangan. Ushbu hujumlar orqali xakerlar tizimlarga kirib, foydalanuvchining ma'lumotlarini shifrlaydi va uni tiklash uchun fidya talab qiladi. Ransomware hujumlarini oldini olish uchun tashkilotlar mustahkam shifrlash, ma'lumotlar zaxirasini yaratish, va foydalanuvchilarni phishing hujumlariga qarshi ogohlantirish kabi choralarni ko'rishlari kerak. Bundan tashqari, fidya dasturlariga qarshi kurashishda sun'iy intellekt va mashinaviy o'qitish algoritmlari yordamida tahdidlarni aniqlash va oldini olish mumkin.

Bulutli hisoblash va saqlashning keng tarqalishi kiberxavfsizlikni yangi darajaga olib chiqdi. Bulutli xavfsizlik, ma'lumotlarni saqlash va uzatishda xavfsizlikni ta'minlash uchun yangi texnologiyalarni ishlab chiqishga olib keldi. Bulutli xavfsizlikni ta'minlashda, shifrlash, ma'lumotlarni uzatishda xavfsizlik protokollarini kuchaytirish, va bulutda ishlayotgan foydalanuvchilarning identifikatsiyasini ta'minlash zarur. Bulutli xavfsizlikning yana bir muhim tendensiyasi — "Xavfsizlikni xizmat sifatida" (Security as a Service, SECaaS) modelining rivojlanishi. Bu model orqali tashkilotlar xavfsizlik xizmatlarini tashqi provayderlardan oladi va o'z tizimlarini bulutda xavfsiz ishlashini ta'minlaydi.

IoT qurilmalari, ya'ni Internetga ulanish imkoniyatiga ega bo'lgan qurilmalar, kiberxavfsizlikning yangi muammolarini keltirib chiqarmoqda. IoT qurilmalarining xavfsizligi, ayniqsa, shaxsiy hayot va korporativ ma'lumotlarni himoya qilishda muhim rol o'ynaydi. IoT qurilmalarini himoya qilish uchun mustahkam autentifikatsiya, shifrlash, va xavfsizlikni monitoring qilish kabi texnologiyalarni qo'llash zarur. Shu bilan birga, IoT qurilmalari uchun maxsus xavfsizlik protokollari ishlab chiqilmoqda, chunki ular ko'pincha kamroq xavfsiz va himoyasiz bo'lishi mumkin.

Sun'iy intellekt va mashinaviy o'qitish kiberxavfsizlikda tahdidlarni aniqlash va oldini olishda yanada samarali vositalar yaratmoqda. AI va ML algoritmlari tarmoqda sodir bo'layotgan shubhali faoliyatni avtomatik tarzda aniqlashga yordam

beradi. Masalan, foydalanuvchi harakatlarini tahlil qilib, uning odatdagi xatti-harakatlaridan chetga chiqqan harakatlar aniqlanadi va tezkor javob beriladi. Shuningdek, AI yordamida kiberhujumlarni oldindan prognozlash va ularga qarshi kurashish mumkin.

Xavfsizlikni boshqarishning avtomatlashtirilgan tizimlari, masalan, SOAR (Security Orchestration, Automation, and Response) tizimlari, kiberxavfsizlikni samarali boshqarish va tezkor javob berish imkoniyatini beradi. SOAR tizimlari kiberhujumlarni aniqlash, ularni tahlil qilish va tezkor javob berish jarayonlarini avtomatlashtiradi. Bu, ayniqsa, katta tarmoqlar va korporativ tizimlar uchun juda muhimdir, chunki ular juda ko'p xavf-xatarlarni boshqarishni talab qiladi.

Kiberxavfsizlikni ta'minlashda tashkilotlar o'rtasida integratsiya va hamkorlikning o'rni ham muhim. Kiberhujumlar va tahdidlar global miqyosda tarqalganligi sababli, bir tashkilotning xavfsizligi butun tarmoqning xavfsizligiga ta'sir qiladi. Shuning uchun, turli tashkilotlar o'rtasida ma'lumot almashish va hamkorlik qilish zarur. Bu, ayniqsa, yirik korporatsiyalar va davlat organlari uchun muhimdir, chunki ular o'rtasida kiberxavfsizlik bo'yicha tajriba va ma'lumot almashish kiberhujumlarga qarshi kurashishda samarali bo'ladi.

Kiberxavfsizlikda xavfni baholash va riskni boshqarish muhim vazifalardan biridir. Tashkilotlar o'z tizimlarining xavf-xatarlarini baholash va ular uchun mos xavfsizlik choralarini ko'rishlari kerak. Riskni boshqarish jarayonida tashkilotlar tizimlaridagi zaifliklarni aniqlash, kiberxavfsizlikni kuchaytirish uchun zarur choralarni belgilash va xavf-xatarlarni oldini olish bo'yicha rejalar ishlab chiqish zarur.

Kiberxavfsizlik texnologiyalarining zamonaviy tendensiyalari kiberhujumlar va tahdidlar bilan samarali kurashish uchun yangi usullarni va yondoshuvlarni ishlab chiqishga olib keldi. Sun'iy intellekt, zero trust arxitekturasi, bulutli xavfsizlik, IoT xavfsizligi, va boshqa ilg'or texnologiyalar kiberxavfsizlikni ta'minlashda samarali vositalar yaratmoqda. Kiberxavfsizlikni ta'minlash uchun tashkilotlar xavfsizlikni boshqarish, xavfni baholash, va xodimlarni o'qitish kabi ko'plab choralarni amalga oshirishi kerak.

Umumiy xulosa. Kiberxavfsizlik texnologiyalarining zamonaviy tendensiyalari global miqyosda kiberhujumlar va tahdidlarga qarshi samarali kurashish uchun yangi va ilg'or usullarni ishlab chiqmoqda. Zero Trust arxitekturasi, sun'iy intellekt va mashinaviy o'qitish, bulutli xavfsizlik, IoT qurilmalari xavfsizligi kabi yondoshuvlar kiberxavfsizlikni ta'minlashda katta rol o'ynaydi. Kiberhujumlar, ayniqsa, ransomware hujumlari va kiberjinoyatlar, tashkilotlar va foydalanuvchilar uchun doimiy xavf tug'diradi. Shu bilan birga, xavfsizlikni boshqarishning avtomatlashtirilgan tizimlari, xavfni baholash va riskni boshqarish, hamda kiberxavfsizlikni yoshlarni o'qitish va ta'lim berish kabi sohalarda ham katta e'tibor qaratilmoqda. Bulardan tashqari, yangi standartlar va me'yorlar kiberxavfsizlikni ta'minlashda muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR RUYXATI

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley.
2. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.
3. Rouse, M. (2021). What is Zero Trust Security?. TechTarget. https://www.techtarget.com
4. Kaspersky. (2020). Ransomware: A Global Threat. Kaspersky Lab. https://www.kaspersky.com
5. IBM. (2021). Artificial Intelligence in Cybersecurity. IBM Security. https://www.ibm.com
6. CISCO. (2020). The Future of Cybersecurity: Trends and Predictions. Cisco. https://www.cisco.com
7. NIST. (2020). Cybersecurity Framework. National Institute of Standards and Technology. https://www.nist.gov