KIBERXAVFSIZLIKNI TA'MINLASH: AXBOROT TEXNOLOGIYALARI SOHASIDAGI ASOSIY USULLAR

Nabiyeva Muhrinisa Bahtiyor qizi
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Farg‘ona filiali 3-bosqich talabasi
Farg‘ona O‘zbekiston
E-mail:muhrinisannabiyeva88@gmail.com

Annotatsiya: *Ushbu maqola axborot texnologiyalari sohasidagi kiberxavfsizlikni ta'minlashning asosiy usullarini tahlil qiladi. Kriptografiya, foydalanuvchi autentifikatsiyasi, tarmoq xavfsizligi va zararli dasturlardan himoya qilish kabi texnologiyalarning kiberxavfsizlikni mustahkamlashdagi o‘rni ko‘rib chiqiladi. Maqolada ushbu usullarning samaradorligi, tarmoq xavfsizligi va foydalanuvchilarni himoya qilish uchun qo‘llaniladigan zamonaviy texnologiyalarni tahlil qilish orqali natijalar taqdim etiladi. Shuningdek, xavfsizlikni ta'minlashda doimiy yangilanishlar va inson omilining ahamiyati ta'kidlanadi. Maqola, kiberxavfsizlikni ta'minlashda innovatsion yondashuvlarning dolzarbligini va ulardan samarali foydalanish zaruratini ko‘rsatib beradi.*

Kalit so‘zlar: *Kiberxavfsizlik, axborot texnologiyalari, kriptografiya, autentifikatsiya, tarmoq xavfsizligi, zararli dasturlar, xavfsizlik choralar, innovatsion texnologiyalar, tarmoqni himoya qilish, foydalanuvchi xavfsizligi.*

Kirish: Axborot texnologiyalari sohasidagi jadal rivojlanish, ayniqsa internet va tarmoq texnologiyalarining keng tarqalishi bilan birga, yangi xavf-xatarlarga olib kelmoqda. Har bir tashkilot va shaxs ma'lumotlarini himoya qilish, tarmoq va tizim xavfsizligini ta'minlashga katta e'tibor qaratmoqda. Kiberxavfsizlik, shubhasiz, hozirgi kunda eng dolzarb masalalardan biri hisoblanadi. Ushbu maqolada kiberxavfsizlikni ta'minlashning asosiy usullari va zamonaviy texnologiyalarni muhokama qilamiz.

Adabiyotlar tahlili: Kiberxavfsizlikni ta'minlash uchun bir nechta asosiy usullar mavjud. Quyida ularning ba'zilari keltirilgan: Kriptografiya: Ma'lumotlarni shifrlash orqali himoya qilish, xususan, masofaviy aloqalarda ma'lumotlar xavfsizligini ta'minlaydi. Kriptografiya texnologiyalarining yordamida ma'lumotlarni faqat ruxsat etilgan shaxslar o'qishi mumkin. Foydalanuvchi autentifikatsiyasi: Foydalanuvchilarning identifikatsiyasi va tizimga kirishini cheklash uchun parollar, biometrik tizimlar yoki ikki faktorli autentifikatsiya (2FA) texnologiyalari qo'llaniladi.Tarmoq xavfsizligi: Tarmoqda hujumlarni aniqlash va oldini olish uchun xavfsizlik devorlari, Intrusion Detection System (IDS) va Intrusion Prevention System (IPS) kabi tizimlar ishlatiladi.Zararlangan dasturiy ta'minotdan himoya qilish: Antiviral dasturlar va zararsizlantirish tizimlari yordamida zararli dasturlardan himoya qilish amalga oshiriladi. Ushbu dasturlar tizimga kirishdan oldin zararli kodlarni aniqlaydi va ularni bloklaydi.

Kiberxavfsizlikni ta'minlashda qo‘llanilayotgan texnologiyalar va usullar sezilarli

darajada samarali bo‘lishi mumkin. Kriptografiya va autentifikatsiya metodlari orqali ma'lumotlar va foydalanuvchilarning xavfsizligi ta'minlanadi. Misol uchun, korxonalarda kriptografiya usullari joriy etilishi tufayli ma'lumotlar o‘g‘irlanishidan himoya qilinmoqda. Tarmoq xavfsizligi tizimlari tarmoqdagi anomaliyalarni kuzatib borish va o‘z vaqtida javob choralarini ko‘rish imkonini beradi. Bu, ayniqsa, tarmoqni xavfsiz holatga keltirishda muhim o‘rin tutadi.

Kiberxavfsizlikni ta'minlashda bir qator omillarni hisobga olish zarur. Birinchi navbatda, xavfsizlik choralarini doimiy ravishda yangilab turish lozim. Tez o‘zgaruvchan texnologiyalar va yangi hujum usullari xavfsizlikni yangilashni talab qiladi. Shuningdek, inson faktori ham muhim ahamiyatga ega. Foydalanuvchilarning ehtiyotsizligi yoki zaif parollarni tanlash kabi omillar tizim xavfsizligiga tahdid solishi mumkin. Shuning uchun, foydalanuvchilarni xavfsizlik bo‘yicha muntazam ravishda xabardor qilish va ularga tegishli o‘qitishlarni o'tkazish zarur.

Uslubiyot: Kiberxavfsizlik sohasida olib borilgan tadqiqotlar va ishlanmalarda ko‘plab yirik izlanishlar mavjud. Quyida ba'zi asosiy ishlanmalar va ulardagi muhim nuqtalar tahlil qilinadi:

1. Schneier, B. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World."

Bruce Schneierning asari axborot xavfsizligi va kiberxavfsizlikka doir eng muhim asarlardan biridir. Muallif, global miqyosda axborotlarni yig‘ish va shaxsiy ma'lumotlarni saqlashning xavfsizlikka ta'siri haqida batafsil ma'lumot beradi. Kitobda kriptografiya, tarmoq xavfsizligi va hukumatlarning ma'lumotlarni kuzatish metodlari haqida tahlillar keltirilgan. Schneier kiberxavfsizlikni nafaqat texnologik, balki siyosiy va ijtimoiy nuqtai nazardan ham yoritadi.

2. Anderson, R. (2020). "Security Engineering: A Guide to Building Dependable Distributed Systems."

Andersonning asari, kiberxavfsizlik tizimlarini loyihalash va qurishda ishlatiladigan metodlarni chuqur tahlil qiladi. U kriptografiya, autentifikatsiya tizimlari, va tarmoqni himoya qilishni muhim tarkibiy qismlar sifatida ta'riflaydi. Anderson shuningdek, tarmoqni himoya qilishda inson omilining ahamiyatini ta'kidlaydi va eng ko‘p uchraydigan xavf-xatarlar va hujumlar haqida ma'lumot beradi.

3. Kaspersky, E. (2019). "Cybersecurity: Protecting Critical Information Infrastructures."

Kaspersky laboratoriyasi tomonidan chiqarilgan ushbu tadqiqotda zamonaviy kiberhujumlarning turlari va ularning oldini olish metodlari tahlil qilinadi. Kitobda kiberxavfsizlikni ta'minlashda ishlatiladigan texnologiyalarning eng so‘nggi rivojlanishlari, jumladan, AI va mashinasozlik texnologiyalari haqida batafsil ma'lumot berilgan. Kaspersky, shuningdek, zararli dasturlarni aniqlash va ularning oldini olish uchun kriptografik usullar va tarmoqni kuzatib borish metodlarini qo‘llashning samaradorligini ko‘rsatadi.

4. Cheswick, W., Bellovin, S., & Rubin, A. (2003). "Firewalls and Internet Security: Repelling the Wily Hacker."

Ushbu asar internet xavfsizligi va xavfsizlik devorlarini qo‘llash bo‘yicha asosiy

manbalardan biridir. Kitobda xavfsizlik devorlarining ishlash printsiplari, ular orqali ma'lumotlar oqimining nazorati va xavf-xatarlardan himoya qilish metodlari keltirilgan. Cheswick va uning hamkasblari, shuningdek, tarmoq xavfsizligi va tarmoqdagi hujumlarni aniqlashning samarali usullarini taqdim etadi.

5. Pfleeger, C. P., & Pfleeger, S. L. (2012). "Security in Computing."

Ushbu darslikda kiberxavfsizlikning turli jihatlari, jumladan, ma'lumotlarni himoya qilish, tarmoq xavfsizligi, va zararli dasturlarni aniqlash bo‘yicha keng qamrovli tahlillar kiritilgan. Kitobda xavfsizlikni ta'minlashda dasturiy ta'minot va apparat xavfsizligi muammolari ham muhokama qilinadi. Mualliflar, shuningdek, kiberxavfsizlik tizimlarining samaradorligini baholashda qo‘llaniladigan metodlarni taqdim etadilar.

Natija: Kiberxavfsizlikni ta'minlashda amalga oshirilgan tadbirlar vatexnologiyalar keng ko‘lamda muvaffaqiyatlarga erishdi. Kriptografiya orqali ma'lumotlar shifrlanib, tarmoq xavfsizligi choralarining joriy etilishi yordamida bir qator xavf-xatarlar oldi olindi. Biroq, barcha tizimlar va metodlar bir xil darajada samarali bo‘lishi mumkin emas. Kriptografiya va autentifikatsiya metodlarining yuqori darajada qo‘llanilishi, ayniqsa, tashkilotlar va hukumatlar tomonidan ma'lumotlarni himoya qilishda sezilarli darajada muvaffaqiyatni ta'minlagan.

Bundan tashqari, zararli dasturlarni aniqlash va bloklash tizimlari yordamida tizimlar xavfsizligi bir qadar yaxshilangan bo‘lsa-da, yangi avlod hujumlarining doimiy ravishda paydo bo‘lishi, xavfsizlikning doimiy yangilanishini talab qilmoqda. Tarmoqni va tizimni real vaqtda kuzatib borish orqali ko‘plab xavf-xatarlar aniqlanib, ularga o‘z vaqtida javob berish imkoniyati yaratildi.

Kiberxavfsizlik choralarini amalga oshirishdagi muvaffaqiyatlarning asosiy omili – bu texnologiyalarning yangilanishiga e'tibor qaratish va zamonaviy xavf-xatarlarni oldini olish uchun zaruriy o‘zgartirishlarni kiritishdir. Kiberxavfsizlikning kelajakdagi rivojlanishi ko‘proq sun'iy intellekt va mashina o‘rganish kabi innovatsion texnologiyalarga asoslanadi.

Xulosa

Kiberxavfsizlikni ta'minlashda texnologiyalarning yuksalishi va innovatsion usullarni qo‘llash, tashkilotlar va shaxslarni xavfsizligini sezilarli darajada oshirish imkonini beradi. Biroq, xavfsizlik choralarini doimiy yangilab borish va foydalanuvchilarni o‘qitish masalalari ham e'tiborga olinishi lozim. Yangi xavf-xatarlar va hujumlar bilan kurashishda axborot texnologiyalarining rivojlanishi davom etayotganini hisobga olib, kiberxavfsizlikni ta'minlash doimiy jarayon bo‘lib qoladi.

FOYDALANILGAN ADABIYOTLAR:

1. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company.

2. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (2nd ed.). Wiley.

3. Kaspersky, E. (2019). Cybersecurity: Protecting Critical Information Infrastructures. Kaspersky Lab.

4. Cheswick, W., Bellovin, S., & Rubin, A. (2003). Firewalls and Internet

Security: Repelling the Wily Hacker (2nd ed.). Addison-Wesley.

5. Pfleeger, C. P., & Pfleeger, S. L. (2012). Security in Computing (4th ed.). Prentice Hall.