



RAQAMLI DUNYODA HIMOYA

Niyazova Arofat Axrorovna

TDTU 3-son akademik litsey fizika va informatika fanlari o'qituvchisi

Xozirgi kunda kiberxavfsizlik raqamli davrning barqarorligi uchun strategik zaruratga aylandi. Milliardlab qurilmalar bir-biri bilan ma'lumot almashayotgan, ma'lumotlar oqimi tez sur'atlarda oshayotgan bir dunyoda shaxslar va tashkilotlar xavfsizligini ta'minlash iqtisodiy va ijtimoiy jihatdan muhim ahamiyatga ega. Aqlli telefonlarimizdan tortib sanoat boshqaruv tizimlariga, bulut xizmatlaridan davlat tarmoqlarigacha bo'lgan barcha qatlamlarda kiber tahdidlarga qarshi himoya raqamli ekotizimning sog'lom ishlashi uchun ajralmasdir.

Kiber hujumlar tobora xilma-xil va murakkab bo'lib bormoqda. Oddiy zararli dasturlardan tortib davlat tomonidan qo'llab-quvvatlanadigan murakkab doimiy tahdidlargacha bo'lgan keng spektrda hujumlar mavjud. Bu holat mudofaa mexanizmlarining ham doimiy ravishda rivojlanishini talab qiladi. Endi faqat antivirus va xavfsizlik devorlari kabi klassik choralar yetarli emas; xulq-atvor tahlili, mashina o'rganishga asoslangan tahdidlarni aniqlash, Zero avtomatik hodisalarga javob berish tizimlari kabi innovatsion yechimlar ishga tushirilmoqda. Shu yo'l bilan tashkilotlar faqat hujumlarga javob berish bilan cheklanmay, tahdidlarni oldindan bashorat qila oladi va ularni amalga oshirishdan oldin oldini oladi.

Shaxsiy darajada kiberxavfsizlik kimlik o'g'irligidan tortib ijtimoiy muhandislik hujumlarigacha bo'lgan xavflarga qarshi qalqon vazifasini bajaradi. Kuchli va noyob parollarni ishlatish, ko'p omilli autentifikatsiyani yoqish, shubhali havolalardan qochish va dasturlarni muntazam yangilab turish asosiy himoya choralaridir. Raqamli gigiyenani hayot tarziga aylantirish jamiyat darajasida kiberbarqarorlikni oshiradi. Treninglar va xabardorlik kampaniyalari foydalanuvchilarning eng zaif bo'g'in bo'lishdan chiqib, xavfsizlikning faol ishtirokchisiga aylanishiga yordam beradi.

Tashkiliy darajada kiberxavfsizlik faqat IT bo'limining emas, balki butun tashkilotning mas'uliyatidir. Direktorlar kengashidan oldingi saflardagi xodimlargacha hamma xavfsizlik madaniyatini qabul qilishi kerak. Siyosat va protseduralarni yangilab turish, muntazam kirish testlarini o'tkazish, hodisalarga javob rejaları va zaxiralash strategiyalarini yuritish tashkilotlarga risklarni minimallashtirishga yordam beradi. Shuningdek, ta'minot zanjiri xavfsizligi va uchinchi tomon risklarini boshqarish tobora ko'proq bog'langan muhitda muhimdir. Chunki bitta zaiflik butun ekotizimga ta'sir ko'rsatishi mumkin.



Davlatlar va xalqaro tashkilotlar uchun kiberxavfsizlik milliy xavfsizlikning ajralmas qismi hisoblanadi. Energetika tarmoqlari, moliyaviy tizimlar, sogʻliqni saqlash infratuzilmalari, transport tarmoqlari va harbiy aloqalar kabi tanqidiy soha-larning raqamlashtirilishi bu sohalarida amalga oshiriladigan kiberhujumlarning ijtimoiy va iqtisodiy inqirozlarga olib kelish ehtimolini oshiradi. Shu sababli mam-lakatlar davlat muassasalarini va xususiy sektorni qamrab oluvchi milliy strategiya-lar ishlab chiqadi, hamkorlikni ragʻbatlantiradi va chegaradan oʻtuvchi tahdidlarga qarshi kurashishda maʼlumot almashishni kuchaytiradi.

Tahdidlarning xilma-xilligi va murakkabligi ortib borar ekan, mudofaa tomonida ham innovatsiyalar muqarrar boʻladi. Hujumchilar sunʼiy intellekt, avtomatlashtirish va deepfake kabi texnologiyalardan foydalanar ekan, himoya tomoni ham mashina oʻrganish bilan qoʻllab-quvvatlanadigan tahdidlarni aniqlash, xulq-atvor tahlili va prognozli xavfsizlik yechimlarini ishlab chiqadi. Bu raqamli qurollanish poygasidir va innovatsiyalar hujum hamda mudofaa tomonida tez surʼatlarda rivojlanadi. Xavfsizlik jamoalari tahdid razvedkasi va avtomatik javob mexanizmlarini integratsiya qilib, ushbu poygada ustunlikka erishishga harakat qiladi.

Huquqiy va etik doiralar ham kiberxavfsizlikning ajralmas oʻlchovidir. Maʼlumotlarni himoya qilish qonunlari, maxfiylik huquqlari va xalqaro meʼyorlar tobora muhim ahamiyat kasb etmoqda. Kompaniyalar faqat texnik jihatdan emas, balki huquqiy jihatdan ham muvofiqlikni taʼminlashi kerak. GDPR kabi reglamentlar yoki mahalliy maʼlumotlarni himoya qilish qonunlari mijoz ishonchini mustahkamlaydi va mumkin boʻlgan sanksiyalarni oldini oladi. Etik jihatdan xavfsizlik mutaxassislarning masʼuliyati katta; ularning bilim va vositalari notoʻgʻri ishlatilsa jiddiy zarar keltirishi mumkin.

Kiberxavfsizlikning kelajagi proaktiv yondashuvlarda yotadi. Tahdidlarni amalga oshishidan oldin aniqlash, hujumlarni bashorat qilish va hodisalarga javob berishni avtomatlashtirish klassik mudofaa tushunchasidan chiqib ketadi. Zero Trust arxitekturasini har bir kirishni potentsial xavf sifatida koʻrib, hujum yuzasini kamaytiradi. Kvant shifrlash, biometrik autentifikatsiya va blokcheyn asosidagi xavfsizlik protokollari kelajakdagi xavfsizlik arxitekturalarining qurilish bloklariga aylanishi mumkin. Ushbu rivojlanishlar xavfsizlikni xarajat markazidan raqobat ustunligiga va ishonch omiliga aylantiradi.

Inson resurslari ham bu sohada katta ahamiyatga ega. Malakali mutaxassislarni tayyorlash, doimiy oʻqitish va sertifikatlash dasturlarini amalga oshirish sohadagi kadrlar yetishmovchiligini bartaraf etish uchun zarur. Ayollarning va turli sohalardan mutaxassislarning ishtiroki turli qarashlar va innovatsion yechimlarni olib keladi. Kiberxavfsizlik jamoaviy ishdir; muhandislik, psixologiya, huquq va biznes sohalaridagi mutaxassislarning



hamkorligi yanada keng qamrovli va samarali strategiyalarni yaratadi.

Xulosa qilib aytganda, kiberxavfsizlik raqamli davrning ajralmas mudofaa chizig'idir. Shaxslardan tortib kompaniyalargacha, davlatlardan xalqaro tashkilotlardagacha hamma ushbu sohada xabardor bo'lishi va choralar ko'rishi kerak. Kiberxavfsizlikni strategik ustuvorlikka aylantirgan jamiyatlar nafaqat risklarini kamaytiradi, balki raqamli dunyoning taklif qilayotgan imkoniyatlarini ham xavfsiz foydalanish imkoniyatiga ega bo'ladi. Bu xavfsiz, barqaror va inklyuziv raqamli ekotizimni yaratishning kalitidir. Har bir tashkilot va har bir shaxs bugun raqamli qalqonini mustahkamlashni boshlaganda umumiy xavfsizlik madaniyati paydo bo'ladi va bu madaniyat hammamizga foyda keltiradi.

FOYDALANILGAN ADABIYOTLAR

1. “Kiberxavfsizlik asoslari” (Xoliqov Sh.A., Musayev A.I., 2024)
2. **“Kiber xavfsizlik: zamonaviy tahdidlar va ularni bartaraf etish usullari” (IQRO jurnali, 2025)** Mualliflar: Muxarramov A.N., Ruzibayev E.X., Sapparboy F.Z.
3. “Kiber xavfsizlik: global tahdidlar va milliy himoya” (JasuXasanov Zenodo, 2024)
4. Kodirov Z. Z, Ismoilov E. T., kiberxavfsizlik – vaqt talabi sifatida, “Iqtisodiyot va jamiyat” №6(109)-1 2023.
5. Levashov V. kiber kuch: kompyuter xavfsizligi bo'yicha keng qamrovli qo'llanma. Spb.: Piter, 2023 yil.
6. Jabbarova K. F., global tahdidlar kontekstida dunyodagi kiberxavfsizlikning zamonaviy jihatlari, // Iqtisodiyot va boshqaruv. 2017. T. 6. № 2(19)