MA'LUMOTLARNI KIBERHUJUMLARDAN HIMOYA QILISH

Sevara Mirzaraximova To'xtamurod qizi, Ernazarova Nargiza Ma'rufjon qizi
Farg'ona davlat texnika universiteti 1-sonli akademik litseyi o'qituvchisi

https://doi.org/10.5281/zenodo.20227802

Annotatsiya: Ushbu maqolada ma'lumotlarni kiberhujumlardan himoya qilish va kiberhujumlarning kompyuterlar, serverlar, mobil qurilmalar, elektron tizimlar, tarmoqlarni zararli hujumlardan himoya qilish usullari to'g'risida ma'lumotlar berilgan. Ushbu maqola xavfsizlik prinsiplari, muhim xavfsizlik nazorati va kiberxavfsizlikning eng yaxshi amaliyotlarini o'z ichiga olgan xavfsizlik asoslarini tushuntiradi.

Kalit so'zlar: Elektron xavfsizlik, protokollar, virus, mobil, axborot, kiberxavfsizlik, pochta, texnologiya, biznes, kiberjinoyat.

Zamonavoy dunyoda yangi texnologiyalar, elektron xizmatlar bizning kundalik hayotimizning ajralmas qismiga aylandi. Jamiyat kundan kun axborot kommunikatsiya texnologiyalariga tobora ko'proq qaram bo'lib borayotganligini hisobga olib, ushbu texnologiyalarni himoya qilish va ulardan foydalanish milliy manfaatlar uchun hal qiluvchi ahamiyatga ega va juda dolzarb mavzuga aylanmoqda. Har bir tashkilot uchun kiberxavfsizlikni ta'minlash maqsadida mazkur soha bilan shug'ullanuvchi xodimlar jalb qilinmoqda hamda xodimlarni kiberxavfsizlikka oid bilimlar bilan doimiy tanishtirib borish uchun qator seminar treyning mashg'ulotlari tashkil etilmoqda. Maktab darsliklarida ham kiberxavfsizlik mavzularining batafsil bayon qilinganligi buning yaqqol misolidir.

Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo'lib, unga berilgan turlicha ta'riflar mavjud. Xususan, CSEC2017 Joint Task Force manbasida kiberxavfsizlikka quyidagicha ta'rif berilgan: kiberxavfsizlik – hisoblashlarga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni to'g'ri bajarilishini kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonlarni mujassamlashtiradi. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o'z ichiga oladi. Kiberxavfsizlik ta'limning mujassamlashgan bilim sohasi bo'lib, qonuniy jihatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni o'z ichiga oladi. Tarmoqlar sohasida faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta'rif bergan: Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarish, almashtirish yoki yo'q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi.

Hozirda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar va ularning turlari sonining kattaligi va buzg'unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda. Bunda mazkur qurilmalar va ularning vazifalari himoyasi uchun ko‘p sathli xavfsizlik choralari amalga oshirilgan. Milliy xavfsizlikni ta'minlash zaruriyatini oshib borishi kompleks va texnologik murakkab ishonchli xavfsizlik choralarini paydo bo‘lishiga sabab bo‘lgan.

Kiberhujumlar, kiberjinoyat, xakerliklarning zararli ta'siri raqamli dunyoda shaxsiy hayot xavfsizligini, shaxsiy ma'lumotlar daxlsizligi haqidagi qarashlarni tubdan o'zgartirib yubordi. Hozirda biz tomonimizdan "yangi sanoat inqilobi" deb nomlanayotgan jarayon yangi jamiyatni, yangi muhitni taqdim etganligi bilan bir tomondan ijobiy ahamiyat kasb etsa, ikkinchi tomondan real xavfni ham keltirib chiqarmoqda. Misli ko'rilmagan rivojlanishga qaramay, internet bizga qo'rquvning yangicha ko'rinishlarini, xavfning yangicha shakllarini olib keldi. Majir Yar va Kevin

F.Steinmetzlarning fikriga ko'ra, "Kibermakon, kompyuterlashtirilgan o'zaro aloqalar va almashinuvlar sohasi jinoyatchilar va deviant faoliyat uchun juda ko'p yangi imkoniyatlarni taqdim etadi (Yar, Majid, and Kevin F. Steinmetz, 2019). Shuningdek, aksariyat manbalarda "kiberjinoyat" tushunchasi "kiberhujumlar", "kompyuterda sodir etilgan jinoyatlar" yoki "kompyuter jinoyatlari" kabi nomlar bilan atalishi, Gudmen va Benner tomonidan XXI asrning boshidayoq ilgari surilgan edi (Goodman, Brenner, 2002). Biroq mazkur tushunchalar bir xil ma'no-mazmun anglatmasligini aytib o'tish joiz. Misol uchun, "kiberjinoyatchilik" atamasi kompyuter bilan bog'liq jinoyatlarga qaraganda torroq tushunchani ifodalashi bilan ajralib turadi. Kompyuterlar bilan bog'liq jinoyatlar esa hatto tarmoq bilan hech qanday aloqasi bo'lmagan, faqat shaxsiy kompyuter tizimlariga ta'sir qiladigan jinoyatlarni ham qamrab oladi (Gercke, 2012). Kiberjinoyatchilik transmilliy jinoyatchilikning rivojlanayotgan shaklidir. Birlashgan Millatlar Tashkilotining Jinoyatchilikning oldini olish va huquqbuzarlarni profilaktika qilish bo'yicha 10Kongressida tegishli seminar doirasida raqamli texnologiyalar orqali sodir etiladigan jinoyatlar uchun ikkita asosiy ta'rif ishlab chiqilgan edi. Tor ma'noda, kiberjinoyatchilik (kompyuter jinoyati) bu kompyuter tizimlari xavfsizligining buzib kirilishi va aynan kompyuterlar tomonidan ma'lumotlarning g'arazli maqsadlarda qayta ishlanib foydalanilishi tushuniladi.

Kiberjinoyatchilik, keng ma'noda esa, (kompyuter bilan bog'liq jinoyatlar) kompyuter tizimi yoki tarmog'i orqali yoki aynan kompyuterga va raqamli tizimlarga nisbatan sodir etilgan har qanday noqonuniy xatti-harakatlarni, shu jumladan, kompyuter tizimi yoki tarmog'i orqali noqonuniy egalik qilish va ma'lumotlarni taqdim etish yoki tarqatish kabi jinoyatlarni qamrab oladi.

Kiberxavfsizlikni fundamental atamalarini aniqlashga turli yondashuvlar mavjud. Xususan ba'zi mutaxassislar kiberxavfsizlikka oid atamalarga quyidagicha ta'rif berishgan:

Konfidensiallik - axborot yoki uni eltuvchining shunday holati bo'lib, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo'ladi. Konfidensiallik axborotni ruxsatsiz "o'qish"dan himoyalash bilan shug'ullanadi. Ayniqsa, bank sistemasida bank uchun konfidensiallik juda muhim.

Risk - potensial foyda yoki zarar bo'lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo'shilganida risk paydo bo'ladi. ISO "risk – bu noaniqlikning maqsadlarga ta'siri" sifatida ta'rif bergan.

Axborot xavfsizligi - axborotning holati bo'lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta'sir etishga yoki ruxsatsiz undan foydalanishga yo'l qo'yilmaydi. Yoki, axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta'minlovchi axborotning himoyalanish sathi holati.

Kiberxavfsizlik 8 ta bilim sohasiga bo'lingan:

Ma'lumotlar xavfsizligi; Dasturiy ta'minot xavfsizligi; Tashkil etuvchilar xavfsizligi; Aloqa xavfsizligi; Tizim xavfsizligi; Inson xavfsizligi; Tashkilot xavfsizligi; Ijtimoiy xavfsizlik.

References:

1. Ganiyev S.K. "Kiberxavfsizlik asoslari". O'quv qo'llanma.
2. O’zbekiston Respublikasi prezidentining "Axborot texnologiyalari va kommunikatsiyalarining joriy etilishini nazorat qilish, ularni himoya qilish tizimini takomillashtirish chora-tadbirlari to’g’risida"gi qarori. 2018 yil 21 noyabr, PQ-4024- son.
3. Thomas A.Johanson. "Cyber-security, Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare".

4. Akbarov D.Y.Axborot xavfsizligini ta'minlashningkriptografik usullari va ularning qo'llanilishi. – Toshkent, "O'zbekiston markasi" nashriyot, 2009-432 bet.