INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

ZAMONAVIY ILM-FAN VA TA'LIM: MUAMMO VA YECHIMLAR

ILMIY-AMALIY KONFERENSIYA

Google Scholar doi zenodo OpenAIRE

+998335668868
https://innoworld.net

2025

«INNOVATIVE WORLD» ILMIY TADQIQOTLARNI QO'LLAB-QUVVATLASH MARKAZI

«ZAMONAVIY ILM-FAN VA TADQIQOTLAR: MUAMMO VA YECHIMLAR» NOMLI 2025-YIL № 5-SONLI ILMIY, MASOFAVIY, ONLAYN KONFERENSIYASI

ILMIY-ONLAYN KONFERENSIYA TO'PLAMI
СБОРНИК НАУЧНЫХ-ОНЛАЙН КОНФЕРЕНЦИЙ
SCIENTIFIC-ONLINE CONFERENCE COLLECTION

www.innoworld.net
O'ZBEKISTON-2025

AXBOROT XAVFSIZLIGI SOHASIDA RAQAMLASHTIRISH MUAMMOLARI VA ISTIQBOLLARI

Isomiddinov Ma'rufjon Umid o'g'li

Xujakulov Anvar Karomatullo o'g'li

Qarshi davlat texnika universiteti, "Axborot tizimlari va texnologiyalari" kafedrasi assistent o'qituvchisi.

Safarboyeva Komila Zokir qizi

Qarshi Davlat Texnika Universiteti PAT-615 22 guruh 4-bosqich talabasi.

Annotatsiya. Mazkur maqolada axborot xavfsizligini tashkil etish — axborot xavfsizligiga tahdidlarni aniqlash, axborotni himoya qilish bo'yicha chora-tadbirlarni rejalashtirish, amalga oshirish va axborotni muhofaza qilish holatini kuzatishga qaratilgan harakatlar majmui.

Kalit so'zlar: axborot xavfsizligi, metodologiya, qayta ishlash, saqlash

Axborot xavfsizligi axborotni ruxsatsiz kirish, foydalanish, oshkor qilish, buzish, o'zgartirish, tadqiq qilish, yozib olish yoki yo'q qilishning oldini olish amaliyotidir. Ushbu universal kontseptsiya ma'lumotlar qanday shaklda bo'lishidan qat'iy nazar (masalan, elektron yoki, jismoniy) amal qiladi. Axborot xavfsizligini ta'minlashning asosiy maqsadi ma'lumotlarning konfidensialligi, yaxlitligi va mavjudligini muvozanatli, qo'llashning maqsadga muvofiqligini hisobga olgan holda va tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoya qilishdir. Bunga, birinchi navbatda, asosiy vositalar va nomoddiy aktivlar, tahdid manbalari, zaifliklar, potensial ta'sirlar va mavjud xavflarni boshqarish imkoniyatlarini aniqlaydigan ko'p bosqichli xavflarni boshqarish jarayoni orqali erishiladi. Bu jarayon xavflarni boshqarish rejasining samaradorligini baholash bilan birga olib boriladi.

Ushbu faoliyatni standartlashtirish maqsadida ilmiy va kasbiy hamjamiyatlar texnik axborot xavfsizligi choralari, yuridik javobgarlik, shuningdek, foydalanuvchi va ma'murlarni tayyorlash standartlari sohasida asosiy metodologiya, siyosat va tarmoq standartlarini ishlab chiqishga qaratilgan doimiy hamkorlik asosida ish olib boradi. Ushbu standartlashtirishga asosan ma'lumotlarga kirish, qayta ishlash, saqlash va uzatishni tartibga soluvchi keng ko'lamli qonunlar va qoidalar ta'sir ko'rsatadi. Biroq, tashkilotda agar doimiy takomillashtirish madaniyati to'g'ri shakllantirilmagan bo'lsa, har qanday standartlar va metodologiyalarni joriy etish yuzaki ta'sir ko'rsatishi mumkin Axborot xavfsizligining markazida axborotni himoya qilish faoliyati — uning maxfiyligi, mavjudligi va yaxlitligini ta'minlash, shuningdek, tanqidiy vaziyatda har qanday murosaga yo'l

qo'ymaslik masalasi yotadi. Bunday holatlarga tabiiy, texnogen va ijtimoiy ofatlar, kompyuterning ishdan chiqishi, jismoniy o'g'irlik va boshqalar kiradi. Dunyodagi aksariyat tashkilotlarning ish jarayonlari hanuz qog'oz asosidagi xujjatlarga asoslangan[6], bo'lib, tegishli axborot xavfsizligi choralarini talab qilsa-da, korxonalarda raqamli texnologiyalarni joriy etish bo'yicha tashabbuslar soni barqaror o'sib bormoqda . Bu esa axborotni himoya qilish uchun axborot texnologiyalari (IT) xavfsizligi bo'yicha mutaxassislarni jalb qilishni talab qiladi. Ushbu mutaxassislar axborot xavfsizligi texnologiyasini (ko'p hollarda kompyuter tizimlarining bir turini) ta'minlaydi. Bu kontekstda kompyuter nafaqat maishiy shaxsiy kompyuterni, balki har qanday murakkablik va maqsadli raqamli qurilmalar, ya'ni elektron kalkulyatorlar va maishiy texnika kabi ibtidoiy va izolyatsiya qilinganlardan tortib, sanoat boshqaruv tizimlari va kompyuter tarmoqlari orqali ulangan superkompyuterlargacha bo'lgan raqamli qurilmalarni anglatadi. Yirik korxona va tashkilotlar o'z bizneslari uchun axborotning hayotiy ahamiyati va qiymati tufayli, qoida tariqasida, o'z xodimlariga axborot xavfsizligi bo'yicha mutaxassislarni yollaydilar. Ularning vazifasi barcha texnologiyalarni maxfiy ma'lumotlarni o'g'irlash yoki tashkilotning ichki tizimlarini nazorat qilishga qaratilgan zararli kiberhujumlardan himoya qilishdir.

Axborot xavfsizligi bandlik sohasi sifatida so'nggi yillarda sezilarli darajada rivojlandi va o'sdi. U tarmoq va tegishli infratuzilma xavfsizligi, dasturiy ta'minot va ma'lumotlar bazasini himoya qilish, axborot tizimlari auditi, biznesning uzluksizligini rejalashtirish, elektron yozuvlarni aniqlash va kompyuter kriminalistikasi kabi ko'plab professional ixtisosliklarni yaratdi. Axborot xavfsizligi bo'yicha mutaxassislar mehnat bozorida yuksak barqaror bandlikka va yuqori talabga ega. Bir qator tashkilotlar (ISC)[2] tomonidan olib borilgan keng ko'lamli tadqiqotlar natijasida ma'lum bo'lishicha, 2017-yilda axborot xavfsizligi sohasi rahbarlarining 66 % o'z bo'limlarida ishchi kuchining keskin yetishmasligini tan olishgan va 2022-yilga kelib bu sohada mutaxassislarning tanqisligi darajasi butun dunyoda 1 800 000 kishini tashkil etishini taxmin qilgan. Axborot xavfsizligiga tahdidlar turli shakllarda bo'lishi mumkin. 2018-yil uchun eng jiddiy tahdidlar „xizmat ko'rsatish usulidagi jinoyatlar" (inglizcha: *Crime-as-a-Service*), Internet mahsulotlari, ta'minot zanjirlari va tartibga solish talablarining murakkabligi bilan bog'liq bo'lgan tahdidlar bo'lgan . „Xizmat ko'rsatish usulidagi jinoyatlar" yirik jinoiy hamjamiyatlar uchun darknet bozorida jinoiy xizmatlar paketini yangi paydo bo'lgan kiberjinoyatchilarga arzon narxlarda taqdim etishning bir namunasidir. Bu yuqori texnik murakkablik yoki yuqori narx tufayli ilgari erishib bo'lmagan xakerlik hujumlarini amalga oshirish imkonini beradi. Bu esa kiberjinoyatni ommaviy hodisaga aylantiradi. Ko'pgina tashkilotlar Internet mahsulotlarini faol tatbiq qilmoqdalar. Bu qurilmalar ko'pincha xavfsizlik talablarisiz ishlab chiqilganligi bois, kiberhujumlar uchun

qo'shimcha imkoniyatlar yaratadi. Bundan tashqari, internet xizmatlarining jadal rivojlanishi va murakkablashuvi uning shaffofligini pasaytiradi, bu esa noaniq belgilangan huquqiy qoidalar va shartlar bilan birgalikda tashkilotlarga qurilmalar tomonidan to'plangan mijozlarning shaxsiy ma'lumotlaridan o'z ixtiyoriga ko'ra, ular bilmagan holda foydalanish imkonini beradi. Bundan tashqari, tashkilotlarning o'zlari IoT qurilmalari tomonidan to'plangan ma'lumotlarning qaysi biri tashqariga uzatilishini kuzatishi mushkul masaladir. Ta'minot zanjirlariga tahdid shundaki, tashkilotlar o'zlarining yetkazib beruvchilari bilan turli xil qimmatli va nozik ma'lumotlarni almashishadi, natijada ular ustidan bevosita nazorat yo'qoladi. Shunday qilib, ushbu ma'lumotlarning maxfiyligi, yaxlitligi yoki mavjudligini buzish xavfi sezilarli darajada oshadi. Bugungi kunda regulyatorlarning tobora ko'payib borayotgan yangi talablari tashkilotlarning hayotiy axborot aktivlarini boshqarishni sezilarli darajada murakkablashtirmoqda. Masalan, 2018-yilda Evropa Ittifoqida qabul qilingan „Umumiy ma'lumotlarni himoya qilish qoidalari" (inglizcha: *General Data Protection Regulation, GDPR*) har qanday tashkilotdan istalgan vaqtda o'z faoliyati yoki ta'minot zanjirining istalgan qismida joylashtirilgan shaxsiy ma'lumotlarning mazmuni, ularni qayta ishlash usullari, saqlanish va himoyalanish tartibi va qanday maqsadlar uchun xizmat qilishini ko'rsatishni talab qiladi. Bundan tashqari, ushbu ma'lumot nafaqat vakolatli organlar tomonidan tekshirish paytida, balki ushbu ma'lumotlar egasining birinchi talabiga binoan ham taqdim etilishi lozim. Bunday muvofiqlikka rioya qilish muhim byudjet mablag'lari va resurslarini tashkilotning boshqa axborot xavfsizligi vazifalaridan chetlashtirishni talab qiladi. Shaxsiy ma'lumotlarni qayta ishlashni soddalashtirish uzoq muddatli istiqbolda axborot xavfsizligini yaxshilashni nazarda tutsa ham, qisqa muddatda tashkilotning xatarlari sezilarli darajada oshadi.

Foydalanilgan adabiyotlar:

1. "Kompyuter xavfsizligi: tamoyillar va amaliyot" (Uilyam Stallings va Lori Braun)
2. Kriptografiya va tarmoq xavfsizligi: tamoyillar va amaliyot" (Uilyam Stallings)
3. "Xavfsizlik muhandisligi: ishonchli taqsimlangan tizimlarni yaratish bo'yicha qo'llanma" (Ross J. Anderson)
4. "Tarmoq xavfsizligi asoslari: ilovalar va standartlar" (Uilyam Stallings)
5. "Amaliy kriptografiya: C tilidagi protokollar, algoritmlar va manba kodi" (Bryus Shnayer)
6. "Kiberxavfsizlik va kiberurush: hamma bilishi kerak bo'lgan narsa" (P.W. Singer va Allan Fridman)
7. "Veb-ilova xakerining qo'llanmasi: Xavfsizlik kamchiliklarini topish va ulardan foydalanish" (Dafydd Stuttard va Markus Pinto)