9 – TOM 3 – SON / 2026 - YIL / 15 – MART

KIBERTAHDIDLARNI ANIQLASH VA ULARNI BARTARAF ETISHNING SHAKL VA USULLARI

Mamasaidov U.E

Harbiy Xavfsizlik va Mudofaa universiteti Janibiy operativ qo‘mondonlik fakulteti boshlig‘ining o‘ribosari, polkovnik

Annotatsiya

Ushbu maqolada kibertahdidlar ва ularning turlarini aniqlash, bartiraf etish shakl va usullari to‘g‘risida, shuningdek kibertahdidlarni aniqlash vositalari to‘g‘risida ma’lumotlar berib o‘tilgan.

Kalit so‘zlar

kibermakon, raqamli hujum, kibertahdid, firibgarlik, zararli hujumlar.

Аннотатция

В данной статье представлена информация о значении киберугрозах, формах и методах выявления и устранения их видов, а также средствах обнаружения киберугроз.

Ключевые слова

Киберпространство, цифровая атака, киберугроза, мошинничество, злонамеренные атаки.

Abstract

This article provides information on the importance of cyber threats, the forms and methods of identifying and eliminating their types, as well as cyber threat detection tools.

Keywords

cyber space, digital attack, cyber threat, fraud, malicions attacks.

Bugungi kunda jahon hamjamiyatiga integratsiyalashayotgan mamlakatimizda axborot kommunikatsiya texnologiyalari, axborot tizimlari va zamonaviy komp`yuter texnologiyalaridan samarali foydalanish bo'yicha izchil davlat siyosati olib borilmoqda. Mamlakatimizda joriy etilayotgan yangi zamonaviy raqamli texnologiyalar, fuqarolarimizga qator qulayliklar va imkoniyatlar eshigini ochmoqda. Mazkur jarayon bilan bir qatorda, yaratilayotgan raqamli texnologiyalar va axborot tizimlarining xavfsizligini ta'minlash muammosi ham mavjud. Bu bizning oldimizga qo‘yilgan eng dolzarb masalalardan biri - kiberxavfsizlikni ta'minlash, sodir etilishi mumkin bo'lgan kiberjinoyatlarning oldini olish va unga qarshi kurashish masalasi hisoblanadi.

Asosiy manbalarda kibertahdidlar kibermakondagi shaxslar, jamiyat va davlat manfaatlariga tahdid soluvchi shart-sharoitlar va omillar majmui deb yuritiladi.

Ma'lumotlarga ta'sir qiluvchi xavf omillari faqat uskunaning yoki ular boshqaradigan dasturlarning faoliyatidan kelib chiqmaydi. Kompyuterdan tashqari boshqa tahdidlar ham mavjud, ayrimlarini oldindan aytib bo'lmaydi. Bunday hollarda axborot almashiladigan kompyuter tarmoqlarini tizimlashtirish eng yaxshi himoya variantidir.

Tahdidlarning sabablari qurilma, uskunalarda yuzaga keladigan xavfsizlik kamchiliklarining asosiy sababi bo‘lib, bunda foydalanuvchilar ishtirok etishi kerak bo‘lmagan faoliyatda ularning harakatlarni cheklamaydigan noto‘g‘ri ruxsatlarga ega bo‘lishlariga bog‘liq bo‘ladi.

Zararli dasturlar deganda fayllar foydalanuvchi yoki tashkilotning roziligisiz kompyuterlarga noqonuniy kirish orqali, saqlangan ma'lumotlarga kirish va uni o'zgartirish maqsadida ishlab chiqilgan dasturlar tushuniladi.

Hozirgi paytda eng keng tarqalgan zararli dasturlarga dasturiy ta'minot yoki kompyuter viruslari, mantiqiy bomba, troyanlar, josuslik dasturlari va boshqalar kiradi.

Dasturlash xatolari xakerlar deb nomlanuvchi xavfsizlik tizimlarini buzuvchi shaxslar tomonidan dasturlarni manipulyatsiya qilish natijasida yuzaga keladi. Ularning asosiy maqsadi kompyuterlarni o'zlari hohlagancha tutib turishga majbur qilish va bu bilan qurilmaga, ham foydalanuvchilarga zarar etkazish.

Ayrim hollarda dasturlarda kamchiliklar mavjud bo'lib, ular ishlab chiqarish jarayonida yuzaga keladi, bu ham qurilmalarning xavfsizligini buzishi mumkin. Bunday kamchiliklarning oldini olish uchun vaqti-vaqti bilan kompaniyalar tomonidan operatsion tizimlar va saqlangan ilovalarga yangilanishlar kiritishga takliflar chiqariladi.

Bosqinchilar bu kompyuterda tizimlarining xavfsizligini buzishga, saqlangan ma'lumotlarga hech qanday ruxsatsiz kiradigan shaxslardir. Boshqacha aytganimizda bular Internet yoki uyali telefonlar orqali foydalanuvchilarni o'zlarining maxfiy ma'lumotlariga kirish uchun kerakli ma'lumotlarni taqdim etishida ularni aldaydigan shaxslar tomonidan qo'llaniladi.

Texnik xodimlar haqida gapirganda, biz kompyuterlarning kiber xavfsizligini ta'minlash uchun ishlaydigan shaxslarni nazarda tutamiz. Texnik xodimlar tizimni turli sabablarga ko'ra sabotaj qilishi mumkin, masalan, mehnat kelishmovchiligi, josuslik yoki ishdan bo'shatilishi kabi holatlarda.

Tahdidlarni turli yo'llar bilan guruhlanishini xarakterlash mumkin bo'lsada, hozirgi vaqtda hujumlarning uchta asosiy turi farqlanadi. Bular, kelib chiqishi bo'yicha, ta'sir doirasi bo'yicha, foydalanilgan vositalariga ko‘ra.

Asl tahdidlar bularni xalqaro CSI (Kompyuter xavfsizligi instituti) ma'lumotlariga

ko'ra, kompyuterlarning xotira qurilmalariga qilingan hujumlarning 60 dan 80% gacha ular ulangan tarmoq ichida yoki uning o'zida sodir bo'ladi.

Insayder tahdidlar global miqyosda xavf tug‘diruvchi kattaroq tahdidlar hisoblanadi, chunki ular tashkilotlarning muhim ma'lumotlarini joylashuvini aniqlaydigan ma'lumotlarni egallashga qaratilgan bo‘ladi, masalan, tashkilot yoki korxonaning kelgusidagi muhim ahamiyatga molik yirik loyihalariga bevosita kirishlar orqali ularga zarar yetkazishi yoki ulardan o‘z manfaatlari yo‘lida foydalanishlari mumkin.

Yuqoridagilardan shuni xulosa qilsak, bosqinning oldini olish tizimlari ichki tahdidlarga emas, balki tashqi tahdidlarga javob berishi kerak bo‘ladi.

Tashqi tahdidlar asosan tajovuzkor ma'lumotlarni olish va o'g'irlash uchun tarmoqning ishlash usuli o'zgarganda paydo bo'lishi mumkin. Bunday holatlar ko‘pincha tashqi tizimlarni ulanishini o'rnatishda sodir bo'lishi mumkin.

Ta'siri tufayli tahdidlar tizimga etkazilgan buzilish yoki zarar darajasiga ko'ra guruhlangan tahdidlarni ta'siri bo'yicha deb atash mumkin. Bunda, ma'lumotni o'g'irlash yoki yo'q qilish, tizimning ishlashini o'zgartirish yoki firibgarlik ushbu turdagi hujumlarga misol bo'la oladi.

Amaldagi vosita tomonidan tahdidlarni biz ishlab chiqarish usuliga qarab tajovuzkor sifatida tasniflashimiz mumkin. Bunda biz zararli dasturlar phishing (foydalanuvchilarni aldashga qaratilgan usullar), ijtimoiy muhandislik va xizmat ko'rsatishni rad etish kabi hujumlarini joylashtirishimiz mumkin.

Kelajakdagi kompyuter tahdidlari haqida gapirganda biz hozirgi vaqtda texnologik evolyutsiya semantik tarmoqning keng rivojlanishiga imkon berganligi va bu bilan kiberhujumchilarning faollashganligini ko‘ramiz.

Xulosa qilib aytganda, O‘zbekistonda kiberxavfsizlikni ta’minlash bo‘yicha olib borilayotgan tizimli va fundamental yondashuv, yagona normativ-huquqiy hujjatlar bazasini yaratish, ilg‘or xorijiy tajribani joriy etish, innovatsion usullardan keng foydalanish davlat axborot siyosatini samarali olib borishga hamda axborot xavfsizligi sohasidagi muammolarni hal etishga hizmat qiladi. Bu esa axborot kommunikatsiya va texnologiyalari tizimini zamonaviy kibertahdidlardan himoya qilish, turli darajadagi tizimlar uchun kiberxavfsizlik bo‘yicha zamonaviy mexanizmlarni joriy etish, mazkur sohada davlat organlari, korxonalar va tashkilotlarning huquqlari va majburiyatlarini belgilash, ularning faoliyatini muvofiqlashtirish kabilarni amalga oshirish orqali belgilanadi.

Yurtimizda olib borilayotgan barcha islohotlar zamirida xalqimizga qulayliklar yaratish maqsadi yotibdi. Kiberxavfsizlikni ta’minlashga alohida e’tibor qaratilishi raqamli imkoniyatlardan ishonchli va xavfsiz tarzda foydalanishga asos bo‘ladi.

FOYDALANILGAN ADABIYOTLAR VA MANBALAR:

1. «Kiberxavfsizlik to‘g‘risida»gi O‘R qonuni 2022 yil 15 mart.
2. Kiberxavfsizlik asoslari, o‘quv qo‘llanma, S.K. G‘aniyev, A.A. G‘aniyev, Z.T. Xudoyqulov, Toshkent, “Aloqachi”, 2020, 221 b.
3. Kiberxavfsizlik, maqola, R.A. Xoldarboyev, R.A. Abduvaxobova, Andijon mashinasozlik instituti, iyul, 2022 y.
4. https://Google.ru
5. https://m.zamin.uz/uz/jamiyat/
6. https://iiv.uz