Impact Factor: 9.9 ISSN-L: 2544-980X

Kibertahdidlar, Hujumlar, Zaifliklar Va Uning Xususiyatlari

Mirzayev Tolibjon To‘raqul o‘g‘li [1]

Rezyume: Bugungi kunda axborotni ishlash, uzatish va to‘plashning zamonaviy usullarining rivojlanishi foydalanuvchilar axborotini yo‘qolishi, buzilishi va oshkor etilishi bilan bog‘liq tahdidlarning ortishiga olib kelmoqda. Shu sababli, kompyuter tizimlari va tarmoqlarida axborot xavfsizligini ta’minlash axborot texnologiyalari rivojining yetakchi yo‘nalishlaridan biri hisoblanadi. Foydalanivchining o’z axborot manbaini himoyalay olishini ta’minlash maqsadida ushbu maqolada kibertahdidlar, hujumlar, zaifliklar va uning xususiyatlari haqida so’z yuritiladi.

Kalit so’zlar: Kibertahdidlar, hujumlar, zaifliklar, zararli hujum manbalari, zararli dasturlarning turlari, hujum turlari, ijtimoiy injineriya, buferni to‘lib toshishi.

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.

Tarmoq sohasida faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta’rif bergan:

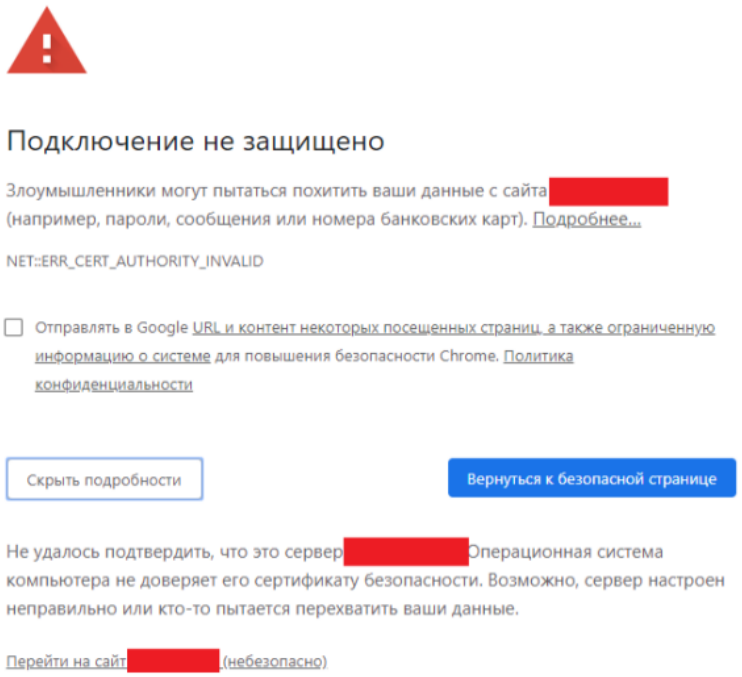
Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarishni, almashtirishni yoki yo‘q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi. Hozirda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar va ularning turlari sonining kattaligi va buzg‘unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda.

Foydalanuvchilarga kiberxavfsizlik tizimidagi eng zaif nuqta sifatida qaraladi. Foydalanuvchilar tomonidan har qanday yuqori darajadagi xavfsizlik ham

buzilishi mumkin. Masalan, yomon niyatli shaxs amazon.com onlayn do‘konidan biror narsani sotib olmoqchi, deylik. Buning uchun shaxs turli kriptografik usullarga tayanadigan SSL (Secure Sockets Layer) protokoli yordamida Amazon bilan ishonchli bog‘lanish uchun web-brauzerdan foydalanishi mumkin. Ushbu protokol barcha zarur amallar to‘g‘ri bajarilganida kafolatli xavfsizlikni ta’minlaydi. Biroq, ushbu protokolga qaratilgan ba’zi hujum turlari (O‘rtada turgan odam hujumi, Man-in-the-middle attack) mavjudki, ularning amalga oshishi uchun foydalanuvchi “ishtiroki” talab etiladi (1-rasm). Agar foydalanuvchi xavfsiz holatni tanlasa (Вернуться к безопасной странице) hujum amalga oshmaydi. Biroq, foydalanuvchi tomonidan xavfsiz bo‘lmagan tanlov (Перейти на сайт …. (небезопасно)) amalga oshirilganida hujum muvaffaqiyatli tugaydi.

Boshqacha aytganda, yuqori xavfsizlik darajasiga ega protokoldan foydalanilganda ham foydalanuvchining noto‘g‘ri harakati sababli xavfsizlik buzilishi mumkin.

[1] Buxoro viloyat hokimining raqamlashtirish bo’yicha maslahatchisi (O‘zbekiston, Buxoro).



1 -rasm. SSL protokolidagi xavfsizlik ogohlantirishi

Odatda foydalanuvchilar esda saqlash oson bo‘lgan parollardan foydalanishga harakat qiladilar. Biroq, bunday yo‘l tutish buzg‘unchi uchun parollarni taxminlab topish imkoniyatini oshiradi. Boshqa tomondan, murakkab parollardan foydalanish va ularni turli eltuvchilarda saqlash (masalan, qog‘ozda qayd etish) esa, ushbu muammoni yanada kuchaytiradi.

Bu misollar inson omili tufayli turli joylar va holatlarda xavfsizlik muammolarining kelib chiqishi mumkinligini ko‘rsatadi. Inson omili tufayli yuzaga keladigan xavfsizlik muammolariga ko‘plab misollar keltirish mumkin.

Biroq, keltirilgan holatlardagi eng muhim jihat shundaki, xavfsizlik nuqtai nazaridan “tenglamadan” inson omilini olib tashlash zarur. Boshqacha aytganda, inson omili ishtirok etmagan tizimlar ishtirok etgan tizimlarga nisbatan xavfsizroq

bo‘ladi.

Eng muhim inson omillariga quyidagilar taalluqli:

- Kiberxavfsizlik sohasiga oid bilimlarni yetishmasligi katta hajmdagi oshkor zaifliklarni paydo bo‘lishiga olib keladi. Kiberxavfsizlik sohasi an’anaviy xavfsizlikka aloqador bo‘lgani bois, zarur texnologik moslashishning tezkorligi ko‘p hollarda bo‘lishi mumkin bo‘lgan zaifliklar sonini oshiradi. Boshqa tomondan, insonning sohaga tegishli so‘nggi texnologik bilimlarni o‘zlashtirishi har doim ham yetarli bo‘lmaydi.
- Risklarni bartaraf etishni va ular haqida xabar berishning yetarli bo‘lmasligi kiberxavfsizlikda takrorlanuvchi va kutilmagan buzilishlarga sababchi bo‘ladi. Insonlar odatda tashkilotlariga jiddiy xavf soluvchi risk mavjudligini bilishsada, uni oshkor qilishmaydi. Buning asosiy sababi sifatida risk bevosita shaxsning o‘ziga, uni moliyaviy holatiga ta’sir etmasligini yoki oshkor qilinganida shaxsning obro‘si tushishini keltirishadi.
- Madaniyat va munosabatlardagi muammolarga tashkilotning o‘zi yoki tashkilot ichki ma’lumotlarini biluvchi norozi va e’tiborsiz xodimning paydo bo‘lishi sababchi bo‘lishi mumkin. Kiberxavfsizlik muammolarining aksariyati ichki hisoblanib, ular xodimlar orasidagi turli kelishmovchiliklar va tashkilot ichidagi muhitning yaxshi emasligi natijasida yuzaga keladi. Bu sabablar esa, xodimning tashkilot ichki strukturasini yaxshi bilgani bois, aksariyat hollarda jiddiy muammolarga olib keladi.

- Xavfsizlik mashg‘ulotlariga kam mablag‘ sarflanishi boshqarilayotgan xavfsizlik risklari to‘g‘risidagi ma’lumotning kamligi sababchi bo‘ladi. Odatda, soha korxonalaridagi xodimlar mustaqil ravishda kiberxavfsizlik qoidalarini o‘rganishmaydi. Shuning uchun kiberxavfsizlik qoidalarini xodimlarga maxsus mashg‘ulotlar shaklida yetkazish zarur bo‘ladi. Bu esa tashkilotdan xavfsizlik mashg‘ulotlariga yetarlicha mablag‘ sarflanishni talab qiladi.
- Hisobga olish nuqtasining yagona emasligi natijasida xavfsizlikning to‘laqonli amalga oshirilmasligi kuzatiladi. Amalda xavfsizlikni kafolatli ta’minlashda uning nazoratini bir nuqtada amalga oshirish muhim hisoblanadi. Yagona nuqtada amalga oshirilgan xavfsizlik nazorati taqsimlangan shakliga nisbatan ishonchli bo‘ladi. Biroq, tashkilotlardagi xavfsizlik nazoratining murakkabligi bois, nazorat odatda taqsimlangan holda boshqariladi.
- Ijtimoiy injineriya asosida xavfsizlik nazoratini aylanib o‘tishda foydalanuvchidan, an’anaviy josuslik texnikasi yordamida, ma’lumotlar qo‘lga kiritiladi. Eng yaxshi kiberxavfsizlik tizimiga ega bo‘lgan tashkilotga ham ijtimoiy injineriya tahdidi xavf solishi mumkin. Ayniqsa, foydalanuvchilarni turli ijtimoiy tarmoqlarda shaxsiy ma’lumotlarini e’tiborsizlik bilan qoldirishi bu xavfning keskin ortishiga sababchi bo‘lmoqda.

Kiberjinoyatchilik – g‘arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o‘g‘irlashga yoki buzishga yo‘naltirilgan alohida shaxslarning yoki guruhlarning harakatlari.

Kiberhujumga duch kelgan tashkilot uchun kiberjinoyatlar ichki yoki tashqi bo‘lishi mumkin:

Ichki kiberjinoyatlar: tarmoqqa yoki kompyuter tizimiga, ular bilan tanish va ulardan qonuniy foydalanish huquqiga ega bo‘lgan shaxs tomonidan, amalga oshiriladi. Mazkur turdagi kiberjinoyatlar odatda tashkilotning xafa bo‘lgan va norozi xodimlari tomonidan amalga oshiriladi. Ushbu xodimlarning maqsadi esa tashkilot yoki uning rahbaridan o‘ch olish yoki ochko‘zlik bo‘lishi mumkin. Xafa bo‘lgan xodim, AT infrastrukturasi, xavfsizlik arxitekturasi va tizimi bilan yaqindan tanish bo‘lgani bois, mazkur turdagi jinoyatchilik tashkilotga jiddiy ziyon yetkazishi mumkin. Bundan tashqari, kiberjinoyatchi tashkilot tarmog‘idan foydalanish imkoniyatiga ega bo‘ladi. Shuning uchun, ichki kiberjinoyatchilik natijasida maxfiy axborotning sirqib chiqish imkoniyati yuqori bo‘ladi.

Tashqi kiberjinoyatlar: odatda tashqaridan yoki tashkilot ichkarisidan yollangan hujumchi tomonidan amalga oshiriladi. Mazkur kiberjinoyatchilik tashkilotning nafaqat moliyaviy yo‘qotishlariga, balki obro‘sining yo‘qolishiga ham sababchi bo‘ladi. Hujum tashqaridan amalga oshirilgani bois, hujumchi harakatni tashkilot AT infrastrukturasini skaner qilish va unga aloqador ma’lumotlarni to‘plashdan boshlaydi. Xususan, malakali buzg‘unchi dastlab tashkilotda foydalanilgan tarmoqlararo ekran vositasining log faylini tahlil qilishdan boshlaydi. Shu bois, tarmoq ma’muri mazkur imkoniyatni buzg‘unchiga taqdim etmasligi shart.

Kiberjinoyat amalga oshirilganida quyidagilar asosiy maqsad sifatida qaraladi: mablag‘, qimmatli qog‘ozlar, kredit, moddiy boyliklar, tovarlar, xizmatlar, imtiyozlar, ko‘chmas mulk, yoqilg‘i xom ashyosi, energiya manbalari va strategik xom ashyolarni noqonuniy o‘zlashtirish; soliq va boshqa yig‘imlarni to‘lashdan bosh tortish; jinoiy daromadlarni qonunlashtirish; qalbaki hujjatlar, shtamplar, muhrlar, blankalar, shaxsiy yutuq chiptalarini qalbakilashtirish; shaxsiy yoki siyosiy maqsadlarda maxfiy ma’lumotlarni olish; ma’muriyatning yoki ishdagi hamkasblarning g‘arazli munosabatlari uchun qasos olish; shaxsiy yoki siyosiy maqsadlar uchun mamlakat pul tizimini buzish; mamlakatdagi vaziyatni, hududiy ma’muriy tuzilishni beqarorlashtirish; talonchilik, raqibni yo‘q qilish yoki siyosiy maqsadlar uchun muassasa, korxona yoki tizim ish tartibini buzish; shaxsiy intelektual qobiliyatini yoki ustunligini namoyish qilish.

Kiberjinoyat turlarini qat’iy tasniflashning imkoni yo‘q. Quyida kriminologiya sohasiga nisbatan kiberjinoyatlarning turlari keltirilgan: iqtisodiy kompyuter jinoyatchiligi; inson va fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga qarshi qaratilgan kompyuter jinoyatchiligi; jamoat va davlat xavfsizligiga qarshi kompyuter jinoyatchiligi. Iqtisodiy kompyuter jinoyatchiligi amalda ko‘p uchraydi.

Ular jinoyatchilarga millionlab AQSh dollari miqdoridagi noqonuniy daromadlar keltiradi. Ular orasida keng tarqalgani firibgarlik, asosan, bank hisob raqamlari va bank kartalari orqali amalga oshiriladi. Xalqaro amaliyotda plastik kartalar bilan sodir etilgan jinoyatlar yo‘qolgan yoki o‘g‘irlangan kartalar, soxta to‘lov kartalarini yaratish yoki ulardan foydalanish, karta taqdim etmasdan bank hisob varag‘i ma’lumotlarini olish va noqonuniy foydalanish, shuningdek, karta egasi tomonidan sodir etilgan jinoyatlar bilan bog‘liq.

Kiberjinoyatlarning yana bir turi inson va fuqorolarning huquqlariga va erkinliklariga qaratilgan jinoyatlar - “kompyuter qaroqchiligi”dir. Ushbu jinoyatlar dasturiy ta’minotni noqonuniy nusxalash, ishlatish va tarqatishda namoyon bo‘ladi.

Bu dasturiy ta’minot va ma’lumotlar bazasini yaratish bilan bog‘liq huquqiy munosabatlarga (mualliflik huquqiga) jiddiy zarar yetkazadi. Bundan tashqari, dasturiy ta’minot kompaniyalariga katta moliyaviy yo‘qotishlarni olib keladi.

Foydalanilgan adabiyotlar

1. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoykulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma, – T. “Nihol print” OK, 2021. – 224 b.
2. Imamova Shafoat Mahmudovna. A SIMULATION TRAINER'S EDUCATIONAL COMPETENCE IN THE PROCESS OF FORMING STUDENTS' PROFESSIONAL COMPETENCE// INTERNATIONAL JOURNAL ON INTEGRATED EDUCATION Volume 6, Issue 9, Sep- 2023 P.75-77.
3. Imomova Shafoat Mahmudovna. TALABALARNING KASBIY KOMPETENSIYALARINI RIVOJLANTIRISHGA YANGICHA YONDASHUVLAR// Educational Research in Universal Sciences. VOLUME 2, SPECIAL ISSUE 14, 2023, C.1075-1081
4. Imamova Sh.M. Methodology of Development of Programming Skills in Mathematical Systems in Students Based on Computer Simulation Trainers// NATURALISTA CAMPANO Volume 28 Issue 1, 2024, -pp. 551-557.
5. Imomova Shafoat Mahmudovna, Qobilov Komil Hamidovich. Oliy Ta’lim Muassasalarida Masofadan OQitish Jarayonini Takomillashtirish// Miasto Przyszłości, Vol. 31 (2023), C.312-314.
6. Imomova Shafoat Mahmudovna, Norova Fazilat Fayzulloyevna. Ta’lim jarayonlarini raqamli texnologiyalar asosida takomillashtirish// Miasto Przyszłości, Vol. 32 (2023), C.47-49.
7. S.K. Ganiev, Z.T. Xudoykulov, N.B. Nasrullaev. Основы кибербезопасности: Учебное пособие, – T. “Mahalla oila nashriyoti”, 2021. – 224 b.
8. Imomova Shafoat Mahmudovna. PEDAGOGIK TEXNIKA – KASBIY KOMPETENSIYALARNI RIVOJLANTIRISHNING ASOSIY OMILI SIFATIDA// Pedagogik mahorat. 1 tom. 2- son (2024 yil, fevral),2024, C. 56-59.