KIBERXAVFSILIKNING O‘ZBEKISTONDAGI O‘RNI

Siddiqov Shaxboz Muxiddin o‘g‘li
Toshkent davlat yuridik unversiteti talabasi,
Toshkent O‘zbekiston

Annotatsiya:*Ushbu maqolada O‘zbekistonda kiberxavfsizlik tizimining hozirgi holatini va uning raqamli iqtisodiyotdagi o‘rnini aniqlash maqsad qilingan. Tadqiqot usuli sifatida 2022 yilda qabul qilingan ORQ-764-son “Kiberxavfsizlik to‘g‘risida”gi qonun hujjatlari, Milliy CERT markazlari (CERT-CBU va UZCERT) faoliyati hamda 2023–2024 yillardagi kiberhujumlar statistikasi tahlil qilindi . Tahlillar shuni ko‘rsatdiki, o‘tgan davrda 11,2 milliondan ortiq hujum urinishlari qayd etilib, eng ko‘p DDoS va TCP ACK turidagi hujumlar aniqlangan . Tadqiqot davomida kadrlar tayyorlash, milliy mahsulotlarni rivojlantirish hamda ommaviy xabardorlikni oshirish masalalari muammolar sifatida belgilandi. Qaror chiqarishda shu muammolarni bartaraf etish bo‘yicha amaliy tavsiyalar ishlab chiqildi. Xulosa sifatida, ushbu tavsiyalar amalga oshirilsa, O‘zbekistonning kiberxavfsizlik darajasi mustahkamlanib, raqamli infratuzilma va iqtisodiyoti barqaror rivojlanadi.*

Kalit so‘zlar: *Kiberxavfsizlik, DDoS , TCP ACK, kiberhujum, DNS, SMS, kiberjinoyat, hacker.*

KIRISH

Gene Spafford:“Agar kompyuter bo‘lmaganida, kompyuter jinoyatlari ham bo‘lmas edi; lekin agar odamlar bo‘lmaganida ham kompyuter jinoyatlari bo‘lmas edi. Tizimlarni himoya qilish reja va mexanizmlariga inson omilini ham kiritishimiz zarur.” P.W. Singer esa “Internet — bu insoniyat yaratgan, biroq o‘zi tushunmaydigan ilk narsa, biz ko‘rgan eng katta anarxiya tajribasidir” deb ta’kidlaydi. Bu ikki fikr kiberxavfsizlik masalasining nafaqat texnik, balki siyosiy va ijtimoiy jihatlarini ham o‘z ichiga olishini ko‘rsatadi. 2022 yil 15 aprel kuni qabul qilingan ORQ-764-sonli “Kiberxavfsizlik to‘g‘risida”gi qonun axborot infratuzilmasini himoya qilish mexanizmlarini yuridik asosga ega bo’ldi. Shu bilan birga, O‘zbekistonda 2023 yilda 11,2 milliondan ortiq kiberhujum urinishlari qayd etilgani sohaga e’tiborni kuchaytirmoqda. Ushbu maqola davlat boshqaruvi organlari, moliya sektori, telekommunikatsiya kompaniyalari hamda foydalanuvchilarnining ma’lumotlarini saqlaydigan har qanday businesslarni o’z ichiga olgan bo’lib, O‘zbekistonda kiberxavfsizlik bo’lgan talabni ortishiga olib keladi.

ASOSIY QISM

1. Huquqiy-normativ baza

O‘zbekiston Respublikasi 2022 yil 15 aprel kuni “Kiberxavfsizlik to‘g‘risida”gi asosiy qonunni (ORQ-764) qabul qildi, bu hujjat muhim axborot infratuzilmalarini aniqlash va

ularni himoya qilish talablari hamda mas’ul organlar vakolatlarini belgilaydi cybersecuritycentraleurasia.com.

2023 yil 31 mayda qabul qilingan qo‘shimcha nizom “Kritik axborot infratuzilmasi obyektlarining kiberxavfsizlik talablari”ni kengaydi, bu esa korxonalarga va davlat xizmatlariga qattiqroq standartlar joriy etishni nazarda tutadi cybersecuritycentraleurasia.com.

2. Milliy javob guruhlari

Markaziy Bankning “CERT-CBU” markazi 2021 yil iyulda tashkil etilib, to‘lov tizimlari va kredit tashkilotlari kiberxavfsizligini ta’minlash bo‘yicha real-vaqt rejimida monitoring, tahlil va chora-tadbirlarni amalga oshiradi O’zbekiston Respublikasi Markaziy Banki.

UZCERT — milliy domen segmentini qamrab oluvchi javob guruhi 2020 yilda tashkil topib, jahon CERT tarmoqlari bilan hamkorlikda kiberhujumlarga tezkor javob qaytaradi.

CERT-CBU yaqinda APWG (Anti-Phishing Working Group) a’zosiga aylanish orqali xalqaro phishing tahdidlariga qarshi o‘zaro axborot almashinuvini kengaytirdi.

3. Kiberhujumlar tahlil

2024 yildagi 12 milliondan ortiq kiberhujum urinishlari

2024 yilda O‘zbekistonda 12 milliondan ortiq kiberhujum urinishlari ro‘yxatga olingan, bu oldingi yilga qaraganda 8,5% ga ko‘payish demakdir Kun.uz.

Bu urinishlarning 35% ga yaqini to‘lov kartalari firibgarligi bilan bog‘liq bo‘lib, kiberjinoyatchilar mobil ilovalar, “Salom, opa!” (“Hello, Mom”) scam va boshqa sotsial injiniring usullaridan foydalangan Kun.uz.

Shunga asoslanib, milliy banklar va to‘lov tizimlari yanada kuchli SMS-validatsiya mexanizmlarini joriy etishni boshladi O’zbekiston Respublikasi Markaziy banki. Ushbu hujum turi kiberxavfsizlikda “Phishing” deb nomlanib, odamlarni aldash va o’ziga ishontirish yordamida moliyaviy, shaxsiy ma’lumotlarini o’g’irlash bilan shug’ullandigan shaxslar ya’ni kiberjinoyatchilar

Davlat veb-resurslariga qarshi DDoS hujumi (2019)

2019 yil 10–11 avgust kunlari mustaqil “Asiaterra.info” saytiga nisbatan tarqatilgan xizmatni rad etish (DDoS) hujumi uyushtirildi, bu mo‘ljallangan trafik hajmi 80 Gbps ga yetgani qayd etildi ACCA Media.

Hujum oqibatida sayt ikki kun davomida ishlay olmadi, foydalanuvchilarning axborot olish imkoniyati cheklandi ACCA Media.

Bu holatdan so‘ng, O‘zbekiston mustaqil internet resurslari uchun zaxira mirror saytlar tashkil etish va kontent tarqatishni ta’minlash bo‘yicha qoidalar ishlab chiqdi RadioFreeEurope/RadioLiberty. Ushbu hujum turi kiberxavfsizlik olamiga DDos hujum bilan kirgan ya’ni manshu hujumni amalga oshirayotgan hacker ishlab turgan websiteni qotirish va bir necha soat balki kunlargacha ishlatmasdan qo’yish bilan kifoyalanadi.

Bank kartalarini avtomatik egallash (SIM swap) hiylasi

SIM swap hujumlari — hujumchi qurbonning raqamli identifikatorini boshqarish uchun mobil operator tizimini aldash usuli xtncognitivesecurity.com.

Masalan, 2023 yilda bir necha holatda foydalanuvchilarning kartalarga bog‘langan telefon raqamlari o‘g‘irlanib, SMS-kod orqali autentifikatsiya bypass qilingan va jami millionlab so‘m miqdorida nolegal pul yechib olingan Kun.uz.

Bu hujumlarni oldini olish uchun operatorlar “shaxsni ta’riflash” jarayonlarini kuchaytirib, qo‘shimcha video-identifikatsiya va biometrik tekshiruvlarni joriy etmoqda O’zbekiston Respublikasi Markaziy banki

Mahalliy bank tizimida Group-IB misoli

2024 yilda AVO bank Group-IB MXDR platformasi yordamida xavfli faoliyatni aniqlash-javob tezligini 1 daqiqagacha qisqartirdi go.group-ib.com.

Platforma firibgarlik, phishing va malvariylarga qarshi real-vaqt rejimida tahlil o‘tkazib, zararlangan hostlarni izolyatsiya qildi go.group-ib.com.

Natijada moliya tashkilotining oylik tahdid javob vaqti 75% ga qisqarib, mijozlar ma’lumotlari xavfsizligi sezilarli darajada oshdi go.group-ib.com.

4. Mavjud muammolar

Kiberxavfsizlik sohasida malakali kadrlar yetishmovchiligi dolzarb muammo bo‘lib, MSP tahlillariga ko‘ra, xodimlar sonining kamligi “alert fatigue” va “burn-out” holatlarini kuchaytiradi deb malum qiladi ConnectWise.

O‘zbekiston korxonalari va aholining digital savodxonligi pastligi sabab, oddiy phishing hujumlari ham muvaffaqiyatli natija beradi; OECD hisobotida bu “kompaniyalarni raqamli va komplementar ko‘nikmalardan mahrum etadi” deb aytadi OECD.

5. Amaliy tavsiyalar

1. Kadrlarni tayyorlash. universitet va kasb-hunar kollejlarida kiberxavfsizlik bo‘yicha maxsus kurslar, laboratoriya mashg‘ulotlari va stajirovkalar tizimini joriy etish lozim deydi ConnectWise.

2. Xalqaro hamkorlik. CERT-CBU va UZCERTga qo‘shni davlatlar CERT tarmoqlari bilan doimiy “joint exercise” mashg‘ulotlari tashkillashtirish tavsiya etiladi

3. Milliy mahsulotlarni rivojlantirish. Kiberxavfsizlik apparat va dasturiy ta’minotini mahalliy ishlab chiqarish uchun subsidiya va grantlar ajratish kerak deb takidlaydi cybersecuritycentraleurasia.com.

4. Omma xabardorligini oshirish: ommaviy axborot vositalari va hukumat organlari birgalikda phishing va soxta saytlarga qarshi kampaniyalarni muntazam o‘tkazishi lozim deydi equalit.ie.

5. Texnik monitoringni kuchaytirish: barcha davlat va moliya muassasalari uchun yagona SIEM (Security Information and Event Management) platformasini joriy etish orqali real-vaqt ogohlantirishlarni avtomatlashtirish zarur.

XULOSA

Ushbu maqolada O‘zbekistonda kiberxavfsizlik sohasining qonuniy-normativ bazasi, milliy javob guruhlari faoliyati, tahdidlar statistikasi hamda amaliy misollar tahlil qilindi. 2022 yil 15 aprel kuni qabul qilingan ORQ-764-sonli “Kiberxavfsizlik to‘g‘risida”gi qonun mamlakat infratuzilmasini muhofaza qilish va xalqaro hamkorlikni mustahkamlash uchun asos yaratdi . CERT-CBU va UZCERT markazlari real-vaqt rejimidagi monitoring, tahlil va

javob choralari bilan moliya tizimi hamda milliy domen segmentini himoya qiladi . 2023 yilda qayd etilgan 11,2 milliondan ortiq kiberhujum urinishlari bu sohadagi tahdidlar darajasining sezilarli ekanligini ko‘rsatdi , 2024 yilda esa bu raqam 12 milliondan oshdi . Asosiy hujum turlari DDoS (o‘rtacha 5,59 Mpps, davomiyligi ~8 daqiqa), DNS amplification va phishing bo‘lib, bu turdagi hujumlar bank va davlat resurslariga eng ko‘p zarar yetkazmoqda .

Amaliy misollar qatorida 2019 yil avgustdagi “Asiaterra.info” saytiga qilingan 80 Gbps DDoS hujumi sayt faoliyatini ikki kunga to‘xtatib qo‘ydi ; 2023 yil noyabrda SMS-kodlarni aylanib o‘tish usulida o‘n oltita bank kartasidan jami 1 milliard so‘mlik ruxsatsiz pul yechib olish holatlari qayd etildi ; SIM swap tufayli yuzaga kelgan firibgarliklarga qarshi operatorlar video-identifikatsiya va biometrik tekshiruvlarni joriy etmoqda ; AVO bank esa Group-IB MXDR platformasi yordamida tahdid javob vaqti 75% ga qisqarishini ta’minladi .

Kelgusi rivojlanish uchun kadrlar tayyorlash, xalqaro hamkorlikni kuchaytirish, milliy mahsulotlarni qo‘llab-quvvatlash hamda jamoatchilik ongini oshirish bo‘yicha aniq amaliy tavsiyalar berildi. Xususan, oliy ta’limda kiberxavfsizlik laboratoriyalari yaratish va stajirovkalarni yo‘lga qo‘yish zarur ; qo‘shni davlatlar bilan muntazam “joint exercise” mashg‘ulotlari tashkil etish lozim ; mahalliy ishlab chiqaruvchilarga subsidiya ajratilishi kiberxavfsizlik mahsulotlari tanlovini kengaytiradi ; ommaviy axborot kampaniyalari va onlayn treninglar orqali phishing va soxta saytlarga qarshi kurash kuchaytiriladi ; yagona SIEM platformasi joriy etilishi real-vaqt ogohlantirishlarni avtomatlashtiradi .

Shu bilan birga, OECD hisobotlariga ko‘ra, digital savodxonlikni oshirish korxona va aholining kiberhujumlarga qarshi immunitetini kuchaytiradi . Infocom tahlillari O‘zbekistonda xavfsizlik choralari iqtisodiy samaradorligini oshirish uchun resurslarni iqtisodiy jihatdan oqilona taqsimlash zarurligini ko‘rsatadi . Yakunida, kiberxavfsizlikni mustahkamlash mamlakatning raqamli infratuzilmasi va iqtisodiy barqarorligiga bevosita hissa qo‘shadi, hamda milliy xavfsizlik va ijtimoiy-iqtisodiy rivojlanishning ajralmas qismiga aylanadi.

FOYDALANILGAN ADABIYOTLAR:

1.Ch.Moschovitis. (2021). Bob 19 Incident Response Tahrirchi (M.damiandes), bookname Privacy, Regulations and Cybersecurity (pp. 321-341). Nashriyot Wiley

2.H.Hoffman (2020). Bob 12 DDoS Attacks. Tahrirchi (H.H), bookname Cybersecurity Bible 4 in1 (23-24).

3.Phillip L.Wylie and Kim Crawley (2021). Bob 2 Prerequisite Skills .bookname; The Pentester Blueprint (pp. 24,28,37). Nashriyot: Wiley ISBN;978-1-119-68430-5 ISBN ; 978-1-119-68435-0(ebk) ISBN; 978-1-119-684437-4(ebk)

4. M. OccupyTheWeb (2023). Bob 8 Domain Name Service (DNS) In E. E. Tahrirchi (Ed.), bookname Network Basics For Hackers (pp.118). Nashriyot: Independently published ISBN: 979-8373290043

Electron Manbalar:
5.https://lex.uz.
6.https://yuz.uz.
7.https://cybersecuritycentraleurasia.com
8.https://uzcert.uz
9.https://Asiaterra.info
10.https://Kun.uz
11.https://cbu.uz