2 aprel (№ 02070)

IQTISODIY BARQARORLIKNI TA'MINLASH: RIVOJLANGAN DAVLATLAR AMALIYOTI ORQALI O'ZBEKISTONDA KIBERXAVFSIZLIK CHORA-TADBIRLARINI MUSTAHKANLASH

Toshkent Davlat Iqtisodiyot Universiteti "Moliya" kafedrasi o'qituvchisi
oliyakuvatova0808@gmail.com

Husenov Muhriddin Bahriddinovich
Toshkent Davlat Iqtisodiyot Universiteti Moliya fakulteti talabasi
mukhriddinhusenov@gmail.com
DOI: *https://doi.org/10.55439/EIT/vol12_iss2/a30*

Annotatsiya
Hozirgi raqamli texnologiyalar jadal rivojlanayotgan asrda, kiberxavfsizlik, milliy iqtisodiyotimiz uchun milliy xavfsizlik va barqarorlikni ta'minlash uchun muhim tarkibiy qismga aylandi. O'zbekiston o'z iqtisodiyotini barqaror holatga olib kelishga harakat qilayotgan ekanki, bu yo'lda kiberxavfsizlikka alohida urg'u qaratilishi lozim. Bu chora-tadbirlarni amalga oshirish uchun rivojlangan mamlakatlar bosib o'tgan yo'llar o'rganilib, eng maqbullari mamlakatimiz uchun tatbiq qilinishi lozim
Kalit so'zlar: Kiberxavfsizlik, raqamli iqtisodiyot, raqamli texnologiyalar, IT, raqamli savodxonlik, iqtisodiy barqarirorlik, kibertahdidlar, milliy xavfsizlik.

ENSURING ECONOMIC STABILITY: STRENGTHENING CYBER SECURITY MEASURES IN UZBEKISTAN THROUGH THE PRACTICE OF DEVELOPED COUNTRIES.

Kuvatova Oliya Sheraliyevna
Teacher of Tashkent State University of Economics, teacher of the Finance Department

Husenov Muhriddin Bahriddinovich
Tashkent State University Institute of Economics, Student of the Faculty of Finance

Abstract
In today's rapidly evolving age of digital technologies, cyber security has become an essential component for ensuring national security and stability for our national economy. As Uzbekistan is trying to bring its economy to a stable state, special emphasis should be placed on cyber security. In order to implement these measures, the paths taken by developed countries should be studied, and the most suitable ones should be implemented for our country.
Keywords. Cyber security, digital economy, digital technologies, IT, digital literacy, economic stability, cyber threats, national security.

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ СТАБИЛЬНОСТИ: УКРЕПЛЕНИЕ МЕР КИБЕРБЕЗОПАСНОСТИ В УЗБЕКИСТАНЕ ЧЕРЕЗ ПРАКТИКУ РАЗВИТЫХ СТРАН

Куватова Олия Шералиевна
Ташкентский Государственный Экономический Университет Преподаватель кафедры Финансы

Хусенов Мухриддин Бахриддинович
Ташкентский Государственный Экономический Университет Студент Финансового факультета

Аннотация
В сегодняшний быстро развивающийся век цифровых технологий кибербезопасность стала важным компонентом обеспечения национальной безопасности и стабильности нашей национальной экономики. Поскольку Узбекистан пытается привести свою экономику в стабильное состояние, особое внимание следует уделить кибербезопасности. Для реализации этих мер необходимо изучить пути, по которым идут развитые страны, и реализовать наиболее подходящие для нашей страны.
Ключевые слова: Кибербезопасность, цифровая экономика, цифровые технологии, ИТ, цифровая грамотность, экономическая стабильность, киберугрозы, национальная безопасность.

KIRISH

R
a
q
H
a
m
l
i
K
o
’
p
g
i
n
a
d
a
v
l
a
t
l
a
r
q
a
t
o
r
i
O
’
z
b
e
k
i
s
t
o
n
h
a
m
r
a
q
a
m
l
i
t
r
a
n
s
f
o
r
m
a
t
s
i
y
a
j
a
r
a
y
o
n
i
n
i
j
a
d
a
l

M
K

B

’zining tadqiqotlarida kiberxavflarning uy-xo’jalik, kichik bizneslar va milliy iqtisodiyotga

S

T
M

ahlili

Kiberhujum – ma’lum kompyuterdan boshqa bir kompyuterlar, tizim, web-saytlar yoki to’g’irlash maqsadida qaratilgan hujumdir. Kiberhujumlardan ko’zlanadigan maqsadlar:

- Qurilmalarga ruxsatsiz kirish imkoniyatiga ega chiqish va uning ichidagi ma’lumotlarga ega bo’lish.
- Tizimlarni butunlay ishdan chiqarish, faoliyatiga tiklab bo’lmas darajada zarar yetqazish, xususan web-saytlarning butunlay to’xtashi.
- Birovlarning qurilmasiga kirib, u shaxs nomidan noqonuniy amallar bajarish
- Tashkilotlar kompyuter tarmog’iga viruslar, zararli kodlar o’rnatish orqali yaxlit tizimga zarar yetqazish
- Rahbar ruhsatisiz yoki uning topshirig’isiz tizimlarga kirishga urinish, uning ichidagi ma’lumotlarni o’zgartirish, tizim ko’rinishini o’zgartirish.

Kiberhujumlar turlari va ularning metodologiyasi (1-jadval):

Kichik turdagi hujumlar - bunday turdagi hujumlar, asosan avtomatlashtirilgan tarzda tizimlarga to’xtovsiz botlar yordamida so’rov yuborish orqali, ma’lum tarmoqni vaqtinchalik ishdan chiqarish uchun qaratilgan bo’ladi. Ikkinchi nom, DDoS nomini olgan ushbu tahdid turi serverlarni so’rovlar bilan to’ldiradi va faoliyatini ma’lum muddatga (mutaxasislar bartaraf qiluguncha) qiyinlashtiradi. Bu davrda ushbu tizim foydalanuvchilari vaqtinchalik noqulayliklarga duch kelishadi.

Ma’lumotlar o’g’irlanishi – shaxslarning shaxsiy ma’lumotlari, korxona tashkilotlarning moliyaviy hisobotlari yoki shu kabi faoliyatiga bog’liq ma’lumotlarga egalik qilishga qaratilgan ushbu hujum turi uyushtirilgan jinoyat turiga kirib, aniq maqsadli kishilar tomonidan amalga oshiriladi. Bu oddiy hujumlardan farqli o’laroq, hujum qiluvchi ushbu tizimga ichki yoki tashqi omillar orqali tizim himoya qismini chetlab o’tishi lozim bo’ladi.

1-jadval

Kiberhujumlar turlari va ularning farqlanishi

Kibertahdid turi	**Kichik turdagi hujumlar**	**Ma'lumotlar o'g'irlanishi**	**Kiber jinoyatlar**	**Hakerlik harakatlari**	**Masshtabli hujumlar**
Maqsadi	Tahlikaga tushirish, Faoliyatni vaqtincha cheklash	Iqtisodiy, siyosiy manfaat	Moliyaviy manfaat	Reputatsion zarar, Siyosiy maqsadlar	Faoliyatlarga chek qo'yish
Misol	Bot spamlar, DDoS	Uyushgan, aniq maqsadli hujumlar	Plastik karta, bank hisoblardagi mablag'lar o'g'irlanishi	Web-saytlar ishdan chiqarilishi	Ma'lumotlarni o'g'irlash, butkul yo'qotish

Xarakter	Avtomatlashgan	Doimiy, Rejalashtirilgan	Tez-tez, Vaziyat yaratilib	Rejalashtirilgan	Muammoli vaziyatlar
Maqsadlilik					

Kiber jinoyatlar hozirgi kunda eng keng tarqalagan hujum turlaridan bo’lib, bu turdagi harakat qurboni har qanday kishi bo’lishi mumkin. Bu usul bir muncha sodda ko’rinishga ega bo’lib, jabrlanuvchilar raqamli savodxonlikdan xabardor emasliklari tufayli yuzaga keladi. Jinoyatchilar turli email, SMS xabarnoma, telefon qo’ng’iroqlar, messenjer yoki ijtimoiy tarmoqlar orqali shubhali havola biriktirilgan xabarlar orqali o’z qopqonlariga tushirishadi. Bulardan ko’zlangan maqsad kishilarning shaxsiy ma’lumotlariga ega chiqish, bank ma’lumotlari orqali hisoblaridagi pul mablag’larini o’zlashtirish hisoblanadi, agarda qurbon shaxs biror tashkilotning qurilmasi orqali bu qopqonga tushsa bu tashkilot uchun boshqa muammolar keltirib chiqaradi.

Hakerlik harakatlari – kamdan-kam uchraydigan, ammo rejalashtirilgan va jiddiy zararlarga olib keluvchi tahdid turi hisoblanib, ma’lum anonim guruhlar tomonidan brendlar, hukumat tashkilotlari reputatsiyasiga keskin salbiy ta’sir ko’rsatish maqsad qilingan bo’ladi.

Masshtabli hujumlar – bunday turdagi hujumlar siyosiy motiv bilan uyushtirilib, katta hajmda yuz beradi. Misol, uchun 2022-yilda boshlangan Rossiya-Ukraina urushida ikki davlatning hakerlik guruhlari tomonidan davlat infrastrukturalari tomon yo’nalgan hujumlarni olishimiz mumkin. [8] [9]

Jahon Iqtisodiy Forumining (WEF) xabar berishicha, 2023-yilda dunyo bo’ylab kiberjinoyatlar soni o’sgani va yetqazilgan zarar miqdori 11 trillion AQSH dollari ekanligi ma’lum qilindi. Maqolada bu raqamlar keyinchalik yanada o’sishda davom etishi va 2027-yilga kelib bu raqamlar 27 trillion dollarga yetishi mumkin ekanligi haqida xabar qilingan. [10]

Quyida 2023-yildagi eng yirik moliyaviy zarar keltirgan hakerlik hujumlarini ko’rishimiz mumkin:

- Buyuk Britaniyaning Royal Mail xalqaro pochta xizmati 2023-yil boshida hakerlar hujumiga uchrab, 11500 ga yaqin pochta ofislari faoiliyatiga to’sqinlik qilindi. Hakerlar. Royal Mail kompaniyasidan 80 million AQSH dollari miqdorda pul undirishga harakat qilishdi [11]
- Buyuk Britaniya saylov komissiyasi tomonidan saqlanadigan 40 millionga yaqin ovoz beruvchilarning shaxsiy ma’lumotlari o’g’irlanganligi haqida xabar berildi. [12]
- “Caesars Entertainment” nomi ostida faoliyat yurituvchi AQSH ko’ngilochar kazinosi ham hakerlar tomonidan foydalanuvchilar ma’lumotlari o’g’irlangani haqida xabar qilgan edi va qora bozorga tarqab ketishini oldini olish evaziga 15 million AQSH dollari miqdorda tovon pul to’lab berishga rozilik bildirgan edi. [13]

“National Cybersecurity Index” xalqaro tashkilotining 177 ta davlatlardan taqdim qilgan statistik ma’lumotlariga ko’ra, O’zbekiston 94-o’rinni egallab, raqamli texnologiyalar o’sish sur’atiga nisbatan qoniqarsiz kiberxavfsizlik ko’rsatkichiga ega ekanligini ko’rishimiz mumkin (2-jadval):

2-jadval

Dunyo davlatlarining milliy kiberxavfsizlik indeksi reytingi. [14]

O'rni	Davlat nomi	Milliy kiberxavfsizlik indeksi	Raqamli rivojlanish darajasi

1	Belgiya	94.81	74.07
2	Litva	93.51	67.34
3	Estoniya	93.51	75.59
4	Chexiya	90.91	69.21
5	Germaniya	90.91	80.01
…	…	…	…
92	Meksika	37.66	51.46
93	Veytnam	36.36	47.69
94	**O'zbekiston**	**36.36**	**49**
95	Janubiy Afrika	36.36	49.24

Yurtimizda olib borilayotgan jadal rivojlanishlar ruhida bu ko’rsatkich nisbatan past hisoblanib, bu kuchsiz yovuz maqsadli jinoiy guruhlar uchun qulay zamin yaratishi mumkin.

Kibertahdidlardan himoyalanish chora-tadbirlari doimo aktual mavzu bo’lib kelgan. Individual shaxslar o’z ma’lumotlari va shaxsiy mablag’larini himoyalash, kompaniya, banklar, moliyaviy sektorlar o’z reputatsiyalarini saqlab qolish, hukumat tashkilotlari o’z fuqarolari, hamda davlatning milliy xavfsizligini himoya qilish uchun doimo sergak turmoqliklari lozim. Mamlakat bo’ylab undagi kiberhujum qurbonlarining keskin kamaytirishning eng asosiy va muhim sanalgan yo’lidan biri bu kishilarning raqamli savodxonligini oshirish hisoblanadi. Bu risklarni nolga tushirishgacha kafolatlamasada, har bir shaxs o’z xatti-harakatlarini oqibatlarini anglagan holda, turli xil qopqonlar, spam-xabarlar, virus joylangan fayllarni chetlab o’ta olish qobiliyatiga ega bo’ladi. Bu jarayon muhim hisoblangani bilan bir qancha qyinichiliklarga ega va kiberxavfsizlik jarayonini ta’minlashda dastlabki bosqich bo’lib hisoblanadi:

1. *Ta’lim standartlari ishlab chiqish*. Mamlakat darajasida aholi qaysi qismi qanday turdagi hujumlar qurboni bo’layotganini statistikasi tahlil qilinib, targetlash usuli orqali maxsus dasturlar ishlab chiqish eng qulay yo’l hisoblanadi. Ammo, bu juda katta mehnat talab qilinganligi tufayli, ba’zi mamlakatlar yosh jihatdan guruhlarga ajratgan holda yosh qatlamdan boshlab internetdan foydalanish etikasi o’rgatilib boriladi. Bu guruhlash tajribasini Buyuk Britaniya, Avstraliya, Estoniya, Singapur kabi davlatlarda muvaffaqiyatli qo’llanilayotganini guvohi bo’lishimiz mumkin.

Buyuk Britaniya hukumati ostida tashkil topgan “Milliy Kiberxavfsizlik Markazi” (NCSC) tomonidan yoshlar uchun “CyberFirst” loyihasi tashkil etilgan. [15] Ushbu loyiha o’smirlarni 7-11, 11-14, 14-18 yosh guruhlariga ajratgan holda alohida o’quv dasturlari orqali bolalarni yoshlikdan internet orqali kutilishi mumkin bo’lgan xavflar haqida turli xil ko’rinishdagi o’quv kurslar, seminar treninglar, amaliy-mashg’ulot yoki musobaqalar orqali ta’lim jarayonini olib borishadi.

Shuningdek savodxonlikni oshirish bilan shug’ullanuvchi subyekt faqatgina hukumat bo’libgina qolmay, balki barcha moliyaviy muassasalar o’z risklarini kamaytirish uchun ma’suliyatni bo’yniga olgan holda xodimlari uchun qo’shimcha o’quv mashg’ulotlari, profilaktika jarayonlari olib borishi maqsadga muvofiq bo’ladi.

2. *Rejalashtirish va tayyorgarlik*. Kiberxavfsizlik “agar …” yoki “qachon?” masalasi emas, u muqarrar hodisa bo’lib har bir raqamli sektor bilan integratsiyalashgan korxona e’tibor qaratishi lozim bo’lgan soha hisoblanadi. Bu o’z ichiga yaxshi IT kompaniya bilan ishlash, ishonchli tashkilotlar tomonidan ishlab chiqilgan rasmiy operatsion tizimlardan foydalanish, ishonchli himoya tizimlaridan foydalanish, lozim bo’lganda ikki bosqichli

himoyalarni qo’llash kabilarni o’z ichiga oladi. O’z-o’zidan ushbu tayyorgarliklar, tashkilot o’z tizimi ustidan tartibli nazorat imkonini berib, xavf tug’ilgan holatlarda ham o’z kritik nuqtalarini muvaffaqiyatli ravishda himoya qilishi va barcha standartlarni qoniqtirishiga olib keladi.

3. *Aniqlashtirish va qayta tiklanish.* Kiberhujum sodir bo’lganda unga qarshi tezkor reaksiya bera olish zararlarning minimal bo’lishini kafolatlaydi. Hujum bo’layotgan jarayonda korxona o’z tizimining (masalan, server) qaysi qismiga hujum yo’naltirilayotganini aniqlashi va shu qism zarar yetishidan avval o’chirib qo’yilishi, ya’ni karantin holatiga olinishi kerak. Bu ma’lum muddatdan keyin, qayta tiklash jarayoni bosqichini osonlashtirishga xizmat qiladi.

4. Hamjihatlik. Kiberxavfsizlik sohasi faqat tor doiradagi kishilarning muammosi bo’libgina qolmay, butun mamlakat bo’ylab har bir shaxs va tashkilot muammosi hisoblanadi. Shu bois, kiberxavfsizlik sohasida erishilgan yutuq va natijalar o’zaro ulashilib birdamlikda harakat qilish, qisqa muddatda yuqori natijalar erishilinishiga olib keladi.

Ushbu bosqichlardan tashqari, qo’shimcha e’tiborga olinishi kerak bo’lgan kichik, ammo muhim internetdan foydalanish etikasi qoidalari mavjud bo’lib, bularga doimo amal qilinishi shartdir. Bilamizki, O’zbekistonda juda ko’p tashkilotlar internet orqali ham o’z xizmatlarini ko’rsatishadi, o’z hisobot, operatsion faoliyatini yuritish uchun asosan, Windows operatsion tizimi, Microsoft Office dasturlari (Word, Excel, PowerPoint …) kabi dasturlardan keng foydalaniladi. Shuni kuzatishimiz mumkinki, ko’p tashkilotlar bu dastur va tizimlarning “qaroqchi”, ya’ni o’g’irlangan versiyalarida ish yuritishadi. Ushbu dasturlarning ishlab chiqaruvchilari tomonidan taklif qilingan rasmiy obunalardagi to’lovlardan qochish maqsad qilingan bu xatti-harakatlar oddiy holdek ko’rinsada, eng avvalo qonuniy jihatdan noto’g’ri, so’ng tashkilotlar va ularning mijozlarining ma’lumotlarini katta xavf ostiga qo’yish hisoblanadi. Xususan, 2023-yilning oxirgi chorakida shov-shuvga aylangan xabarlardan biri bo’lgan, 200000 ga yaqin O’zbekistonlik fuqarolarining ma’lumotlari tarqalishining [16] ortida ham aynan shu “qaroqchi” dasturlar sabab qilib ko’rsatilmoqda.

Xulosa va Takliflar

Dunyo raqamli texnologiyalar sohasida rivojlanishda davom etar ekan, kiberxavfsizlik mavzusi eng dolzarb mavzularidan biriga aylanib boraveradi. Hozirda bizga ma’lum eng mashhur kiberhujum turlari bu fishinglar, DDoS hujumlar, turli xil ko’rinishga ega kompyuter viruslari, ma’lumotlar o’g’irlanishi, yirik masshtabli hakerilik hujumlari ekanligidan xabarimiz bor. Bu muammolar barcha rivojlangan va rivojlanayotgan davlatlarning asosiy muammosi bo’lib kelmoqda, shuningdek O’zbekistonning o’z istiqbolli strategiyalari uchun bu juda muhim o’ringa ega. O’zbekiston Respublikasi prezidenti tomonida taklif bildirigan “O’zbekiston – 2030” loyihasida barcha sohalarda raqamli texnologiyalar bilan integratsiyalashuv jarayonini qo’llash topshirig’i berilgan. Shuni unutmasligimiz lozimki, bu o’z-o’zidan turli tashqi tahdidlar paydo bo’lishiga olib keladi, shu bois kiberxavfsizlik sohasida qilinishi kerak bo’lgan islohotlar ham ushbu maqsadlar ichida yuqori qatorlarda turmog’ligi darkordir. Zeroki, beqaror kiberxavfsizlik holati O’zbekistonni dunyodagi reytinglarda orqaga tortibgina qolmay, balki ichki milliy xavfsizligi, iqtisodiy muammolar, aholi orasida sarosimalar keng yoyilishiga olib keladi.

Bir mamlakat hududida kiberxavfiszlik holatini barqaror holatga olib kelish uchun bir qancha qiyinchiliklarga duch kelinishi tabiiy hol hisoblanib, u kelajakdagi o’sish uchun tayanch vazifasini bajarib beradi. Maqola davomida ko’rdikki, eng avvalo O’zbekiston fuqarolari orasida individual xabardorlikni oshirishdir. Bu fuqarolarning har bir harakati

uchun o’zi javobgar ekanligi tushunchasini ilgari surib, kiber olam haqidagi dastlabki tushunchalarga ega bo’lishi lozimligi haqidagi g’oyani ilgari suradi. Shuningdek, rivojlangan davlatlar misolidan olib qaraganimizda, kiber-ta’lim jarayoni bolalarning o’smirlik yoshlaridan boshlab ishlab chiqilgan turli xil o’quv-dasturlari, musobaqalar orqali amalga oshiriladi.

Keyingi bosqichlarda, bir shaxsning ma’suliyat darajasini kengaytirib buni korxona-tashkilotlar darajasida, undan keyin butun davlat miqyosida amalga oshirilishi maqsadga muvofiq bo’ladi.

Xulosa qilib aytganda, umumiy jarayon qanchalik qiyin ko’rinmasin bu O’zbekistonning kelajakdagi strategiyalari uchun muhim ustun bo’lib xizmat qiladi. O’zbekiston oldida turgan kiberxavfsizlikka oid muammolarning yechimi davlat idoralari, xususiy va iqtisodiy sektor tuzilmalari, ilmiy doiralar va fuqarolarni jalb etgan holda ko’p qiralli yondashuvni talab etadi.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasi Prezidentining 05.10.2020 yildagi PF-6079-son “Raqamli O’zbekiston – 2030” strategiyasi tasdiqlash va uni samarali amalga oshirish tadbirlari to’g’risidagi farmoni. https://lex.uz/docs/5030957

2. 2020-yil 15-iyundagi “O‘zbekiston Respublikasida kiberxavfsizlikni ta’minlash tizimini yanada takomillashtirishga doir qo‘shimcha chora-tadbirlar to‘g‘risida”gi PQ-4751-son qarori

3. Walls, A., Perkins, E., & Weiss, J. (2013). Definition: Cybersecurity, 5. https://www.gartner.com/doc/2510116/def inition-cybersecurity

4. Barzilay, M. (2013, 2013-08-05). A simple definition of cybersecurity. http://www.isaca.org/KnowledgeCenter/Blog/Lists/Posts/Post.aspx?ID=29 6

5. R Böhme, S Laube, M Riek - Variance, 2019 “A Fundamental Approach to Cyber Risk Analysis”

6. OECD Global Forum on Digital Security for Prosperity, 7 June 2021

7. OECD, The Global Forum on Digital Security for Prosperity in 2024

8. M.Hunder, J.Landay, S.Bern. Reuters “Ukraine's top mobile operator hit by biggest cyberattack of war” https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/

9. Kela Cyber Intelligence center, “Russia-Ukraine war: pro-Russian hacktivist activity two years on” https://www.kelacyber.com/russia-ukraine-war-pro-russian-hacktivist-activity-two-years-on/

10. Emma Charlton, WEF, “2023 was a big year for cybercrime – here’s how we can make our systems safer” https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/

11. https://www.theguardian.com/business/2023/jan/11/royal-mail-services-suffer-severe-disruption-after-cyber-incident

12. The Electrol Comission, UKhttps://www.electoralcommission.org.uk/privacy-policy/public-notification-cyber-attack-electoral-commission-systems

13. BleepingComputerhttps://www.bleepingcomputer.com/news/security/caesars-entertainment-confirms-ransom-payment-customer-data-theft/

14. National cybersecurity index https://ncsi.ega.ee/ncsi-index/?order=rank&archive=1

15. National cyber security center, UK https://www.ncsc.gov.uk/cyberfirst

16. “Интернетга 200 мингдан ортиқ ўзбекистонлик фойдаланувчиларнинг маълумотлари тарқалиб кетди” https://uznews.uzuz//posts/68778