KIBERXAVFSIZLIK: ZAMONAVIY TAHDIDLAR VA ULARGA QARSHI KURASH YO'LLARI

Mamadaliyev Kamronbek Sherzod o'g'li
Cyber university of Uzbekistan mamadaliyevkamron02@gmail.com

Annotatsiya: *Mazkur maqola zamonaviy kibertahdidlarning evolyutsiyasi, ularning murakkablashuvi va global miqyosda kiberxavfsizlikni ta'minlashning dolzarb masalalariga bag'ishlangan. Raqamli transformatsiya jarayonlarining jadallashuvi, sun'iy intellekt va narsalar interneti (IoT) texnologiyalarining keng joriy etilishi kiberhujumlar geografiyasining kengayishiga va ularning yangi, yanada xavfli shakllarining paydo bo'lishiga olib keldi. Maqolada zamonaviy kibertahdidlarning asosiy turlari, jumladan, ransomeware, fişing, DDoS hujumlari, davlat homiyligidagi hujumlar tahlil qilingan. Shuningdek, ushbu tahdidlarga qarshi kurashishning samarali usullari, jumladan, sun'iy intellektga asoslangan himoya tizimlari, nol ishonch arxitekturasi va postkvant kriptografiyasi masalalari yoritilgan. O'zbekiston Respublikasining kiberxavfsizlikni ta'minlash borasidagi qonunchilik asoslari va amaliy chora-tadbirlari, xususan, "Kiberxavfsizlik to'g'risida"gi Qonun va Prezident qarorlari tahliliy nuqtai nazardan keltirilgan.*

Kalit so'zlar: *kiberxavfsizlik, kibertahdid, ransomeware, fişing, DDoS, sun'iy intellekt, nol ishonch arxitekturasi, kriptografiya, O'zbekiston qonunchiligi.*

KIRISH

Dunyoda raqamli texnologiyalarning jadal sur'atlar bilan rivojlanishi insoniyat hayotining barcha jabhalarini tubdan o'zgartirmoqda. Sun'iy intellekt, bulutli hisoblashlar va narsalar interneti kabi innovatsion yechimlar iqtisodiyot, davlat boshqaruvi va sog'liqni saqlash kabi muhim sohalarning samaradorligini oshirishga xizmat qilmoqda. Biroq, ushbu texnologik taraqqiyotning salbiy oqibatlari ham mavjud bo'lib, ular orasida eng xavflisi bu – kibertahdidlarning tobora murakkablashuvi va ularning ko'lamining kengayishidir. Endilikda kiberhujumlar nafaqat yirik korporatsiyalar yoki davlat institutlariga, balki oddiy fuqarolarga, kichik biznes sub'ektlariga va hatto strategik ahamiyatga ega infratuzilma ob'ektlariga ham qaratilmoqda. Cybersecurity Ventures kompaniyasining hisob-kitoblariga ko'ra, kiberjinoyatchilik dunyo iqtisodiyotiga yiliga 10,5 trillion dollargacha zarar keltirishi mumkin. Bu esa kiberxavfsizlikni ta'minlash masalasini har bir davlatning milliy xavfsizlik strategiyasining ustuvor yo'nalishiga aylantirmoqda.

Ushbu maqolaning maqsadi – zamonaviy kibertahdidlarning asosiy turlari va ularning xususiyatlarini tahlil qilish, shuningdek, ushbu tahdidlarga qarshi kurashishning eng samarali usullarini o'rganishdan iborat. Maqolada, shuningdek, O'zbekiston Respublikasida kiberxavfsizlik sohasida amalga oshirilayotgan islohotlar va qabul qilinayotgan huquqiy-me'yoriy hujjatlar tahliliy nuqtai nazardan yoritiladi.

1. ZAMONAVIY KIBERTAHDIDLAR TASNIFI

Kibertahdidlar tushunchasi keng qamrovli bo'lib, ularni turli mezonlar asosida tasniflash mumkin. Quyida eng dolzarb va xavfli kibertahdidlarning ayrim turlari tahlil qilingan.

Ransomeware so'nggi yillarda eng keng tarqalgan va eng ko'p zarar keltirayotgan kibertahdid turlaridan biri hisoblanadi. Ushbu zararli dastur kompyuter tizimiga kirib, undagi ma'lumotlarni shifrlaydi va ularni qayta tiklash evaziga qurbondan to'lov talab qiladi. Ransomeware hujumlari nafaqat yirik korxonalar va davlat idoralariga, balki shifoxonalar, maktablar va universitetlarga ham qaratilmoqda. 2021-yilda AQShning eng yirik neft quvuri operatori Colonial Pipeline kompaniyasiga qilingan hujum butun mamlakat bo'ylab yoqilg'i ta'minotida uzilishlarga olib keldi. Hujumchilar tomonidan qo'llaniladigan usullar ham murakkablashib bormoqda: ular "ikki tomonlama to'lov" taktikasini qo'llaydilar, ya'ni ma'lumotlarni shifrlash bilan birga, ularni o'g'irlab, to'lov talabi bajarilmasa, internetda ommaga e'lon qilish bilan tahdid qiladilar.

Fişing – bu kiberjinoyatchilarning ishonchli tashkilot yoki shaxs nomidan foydalanib, foydalanuvchilarning maxfiy ma'lumotlarini olishga qaratilgan hujum turidir. Odatda, bu soxta elektron pochta xabarlari, SMS-xabarlar yoki telefon qo'ng'iroqlari orqali amalga oshiriladi.

Soxta xabarlar qurbonlarni haqiqiy veb-saytlarga o'xshash soxta veb-saytlarga yo'naltiradi va ular o'z ma'lumotlarini kiritishga majbur qiladi. Ijtimoiy muhandislik esa fişingning yanada murakkab shakli bo'lib, unda hujumchilar inson psixologiyasidan foydalanib, maxfiy ma'lumotlarni olishga yoki ma'lum bir harakatni amalga oshirishga undaydilar. Sun'iy intellekt texnologiyalarining rivojlanishi bilan fişing hujumlari yanada ishonchli va aniqlash qiyin bo'lib qoldi. Hujumchilar sun'iy intellekt yordamida tanish odamlarning ovozini yoki videotasvirini soxtalashtirishi va shu orqali firibgarlik qilishi mumkin.

DDoS hujumlari – bu bir vaqtning o'zida katta miqdordagi so'rovlar yuborish orqali server, veb-sayt yoki tarmoq resurslarini ishdan chiqarishga qaratilgan hujumdir. Bu hujum natijasida qonuniy foydalanuvchilar xizmatlardan foydalana olmaydilar. DDoS hujumlari ko'pincha shantaj, raqobatchilarni yo'q qilish yoki siyosiy norozilik bildirish maqsadida amalga oshiriladi. So'nggi yillarda narsalar interneti qurilmalari sonining keskin o'sishi DDoS hujumlari quvvatini yanada oshirdi. Hujumchilar xavfsizlik darajasi past bo'lgan minglab IoT qurilmalarini zararlab, ulardan botnet tarmog'ini shakllantiradi va yirik miqyosdagi hujumlarni amalga oshiradi.

Davlat homiyligidagi kiberhujumlar zamonaviy geosiyosiy sharoitda alohida xavf tug'dirmoqda. Bu turdagi hujumlar odatda boshqa davlatlarning strategik ob'ektlariga, davlat idoralariga, mudofaa sanoati korxonalariga va saylov tizimlariga qaratilgan bo'ladi. Ularning maqsadi – maxfiy ma'lumotlarni o'g'irlash, infratuzilmani ishdan chiqarish, siyosiy jarayonlarga aralashish yoki raqib davlatga nisbatan ustunlikka erishishdir. Stuxnet qurti, 2007 yilda Estoniyaga qilingan kiberhujumlar va 2016 yilda AQSh saylovlariga aralashish holatlari davlat homiyligidagi kiberhujumlarning eng mashhur misollaridir.

2. KIBERTAHDIDLARGA QARSHI KURASHISH USULLARI

Kibertahdidlarning murakkablashuvi ularga qarshi kurashish usullarini ham doimiy ravishda takomillashtirishni talab qiladi. Quyida zamonaviy kiberhimoyaning asosiy yo'nalishlari tahlil qilingan.

Sun'iy intellekt va mashinaviy o'qitish texnologiyalari kiberxavfsizlik sohasida inqilobiy o'zgarishlar qilmoqda. An'anaviy himoya vositalari ma'lum bo'lgan tahdidlarga qarshi kurashishda samarali bo'lsa, SI va MOga asoslangan tizimlar yangi, noma'lum tahdidlarni aniqlash va ularga real vaqt rejimida javob berish imkoniyatiga ega. Ushbu tizimlar tarmoqdagi katta hajmdagi ma'lumotlarni tahlil qilib, anomaliyalarni aniqlaydi va shu orqali potentsial hujumlarni erta bosqichida oldini oladi. Masalan, SI yordamida firibgarlik operatsiyalarini aniqlash, zararli dasturlarni ularning xatti-harakatlariga qarab klassifikatsiya qilish va avtomatik ravishda hujumlarga qarshi choralar ko'rish mumkin.

Nol ishonch arxitekturasi zamonaviy kiberhimoyaning eng muhim konsepsiyalaridan biridir. An'anaviy perimetrga asoslangan xavfsizlik modeli bulutli texnologiyalar, masofaviy ish va mobil qurilmalarning keng tarqalishi sharoitida o'z samaradorligini yo'qotmoqda. "Nol ishonch" modelining asosiy tamoyili – hech kimga, hatto tashkilotning ichki tarmog'idagi foydalanuvchi yoki qurilmaga ham, oldindan ishonch bildirmaslikdir. Har bir so'rov, uning kelib chiqishidan qat'iy nazar, doimiy ravishda tekshiruvdan o'tkaziladi va autentifikatsiya qilinadi. Nol ishonch arxitekturasi mikro-segmentatsiya, ko'p faktorli autentifikatsiya va doimiy monitoring kabi texnologiyalarga asoslanadi.

Kriptografiya ma'lumotlarni himoya qilishning asosiy usuli hisoblanadi. Hozirgi kunda keng qo'llanilayotgan RSA va elliptik egri chiziq kriptografiyasi kabi algoritmlar kvant kompyuterlari tomonidan xavf ostida. Kelajakda kvant kompyuterlarining paydo bo'lishi ushbu algoritmlarni bir necha soniya ichida buzishi mumkin. Shu sababli, hozirda postkvant kriptografiyasi sohasida jadal tadqiqotlar olib borilmoqda. AQSh Milliy standartlar va texnologiyalar instituti postkvant kriptografiyasi standartlarini ishlab chiqish bo'yicha tanlov o'tkazmoqda.

Xodimlarning xabardorligi va kibergigiyena muhim ahamiyat kasb etadi. Texnologik yechimlar qanchalik mukammal bo'lmasin, inson omili kiberxavfsizlikning eng zaif halqasi bo'lib qolmoqda. Ko'plab kiberhujumlar, ayniqsa fişing hujumlari, xodimlarning e'tiborsizligi yoki bilimsizligi tufayli muvaffaqiyatli amalga oshadi. Shu sababli, tashkilotlarda xodimlarning kiberxavfsizlik bo'yicha muntazam ravishda o'qitilishi va ularning xabardorligini oshirish muhimdir. Kibergigiyenaga kuchli parollardan foydalanish, ikki faktorli autentifikatsiyani yoqish, shubhali havolalarni bosmaslik va dasturiy ta'minotni muntazam yangilab turish kiradi.

Xalqaro hamkorlik va axborot almashinuvi kibertahdidlarga qarshi kurashda muhim rol o'ynaydi. Turli davlatlarning huquqni muhofaza qilish organlari, kiberxavfsizlik agentliklari va xususiy kompaniyalari o'rtasida tahdidlar, zaifliklar va hujumchilarning usullari haqida tezkor ma'lumot almashish kiberhujumlarning oldini olish samaradorligini oshiradi. INTERPOL va EUROPOL doirasida kiberjinoyatchilikka qarshi qo'shma operatsiyalar o'tkazilmoqda. "Budapesht konvensiyasi" kabi xalqaro shartnomalar kiberjinoyatchilikka qarshi kurashda huquqiy asos bo'lib xizmat qiladi.

3. O'ZBEKISTONDA KIBERXAVFSIZLIK SOHASIDAGI ISLOHOTLAR

O'zbekiston Respublikasi raqamli transformatsiya jarayonlarining faol ishtirokchisi sifatida kiberxavfsizlikni ta'minlash masalasiga alohida e'tibor qaratmoqda. Mamlakatda so'nggi yillarda bu borada muhim qadamlar tashlanmoqda.

Huquqiy asoslarni mustahkamlash borasida keng ko'lamli ishlar amalga oshirilmoqda. 2022 yilda qabul qilingan "Kiberxavfsizlik to'g'risida"gi Qonun ushbu sohadagi asosiy huquqiy hujjat hisoblanadi. Qonunda kiberxavfsizlik sohasidagi asosiy tushunchalar, davlat organlarining vakolatlari, kiberxavfsizlik talablari va kiberhodisalarga munosabat bildirish tartibi belgilangan. Shuningdek, O'zbekiston Respublikasi Prezidentining 2025-yil 15-apreldagi "Kiberxavfsizlikni ta'minlash tizimini yanada takomillashtirish chora-tadbirlari to'g'risida"gi qarori mamlakatda kiberxavfsizlikni ta'minlashning yangi bosqichini boshlab berdi.

Institutsiional rivojlanish va infratuzilma sohasida muhim o'zgarishlar amalga oshirilmoqda. Prezident qarori asosida Kiberxavfsizlik sohasidagi vakolatli davlat organi etib Milliy gvardiya harbiy xizmatchilaridan iborat maxsus bo'linma belgilandi. Ushbu organ quyidagi asosiy vazifalarni bajaradi: davlat organlari va tashkilotlarining axborot tizimlarida kibertahdidlarni aniqlash va oldini olish; kiberhujumlarni bartaraf etish va ularning oqibatlarini minimallashtirish; kiberxavfsizlik sohasidagi normativ-huquqiy hujjatlar loyihalarini ishlab chiqish; xalqaro hamkorlikni rivojlantirish va ilg'or xorijiy tajribani joriy etish.

Kadrlar tayyorlash va ilmiy salohiyatni oshirish masalasiga ham alohida e'tibor qaratilmoqda. O'zbekistonda bir qator oliy ta'lim muassasalarida "Kiberxavfsizlik" yo'nalishi bo'yicha mutaxassislar tayyorlanmoqda. Toshkent shahrida faoliyat yuritayotgan "INHA" universiteti, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti va boshqa ta'lim dargohlarida zamonaviy o'quv laboratoriyalari tashkil etilgan.

Shuningdek, malakali mutaxassislarni tayyorlash maqsadida xalqaro hamkorlik doirasida qator loyihalar amalga oshirilmoqda.

XULOSA

Zamonaviy kibertahdidlar tobora murakkablashib, ularning ko'lami va yetkazayotgan zarari yil sayin oshib bormoqda. Ransomeware, fişing, DDoS hujumlari va davlat homiyligidagi kiberhujumlar eng xavfli tahdidlar sirasiga kiradi. Ushbu tahdidlarga qarshi kurashishda texnologik yechimlar bilan bir qatorda tashkiliy va huquqiy chora-tadbirlar ham muhim ahamiyat kasb etadi. Sun'iy intellektga asoslangan himoya tizimlari, nol ishonch arxitekturasi va postkvant kriptografiyasi kabi ilg'or texnologiyalar kiberxavfsizlikning kelajagini belgilaydi.

O'zbekiston Respublikasida kiberxavfsizlikni ta'minlash borasida muhim qadamlar tashlanmoqda. "Kiberxavfsizlik to'g'risida"gi Qonun va Prezident qarorlari asosida yagona davlat siyosati shakllantirilmoqda, vakolatli organ tashkil etilib, uning vazifalari belgilab berilgan. Biroq, mavjud muammolarni hal etish va xalqaro standartlarga to'liq erishish uchun quyidagi yo'nalishlarda ishlarni davom ettirish zarur: malakali kadrlar tayyorlash tizimini takomillashtirish; davlat-xususiy sheriklikni rivojlantirish; xalqaro hamkorlikni kengaytirish; fuqarolarning kiberxavfsizlik madaniyatini oshirish. Faqatgina kompleks

yondashuv va barcha manfaatdor tomonlarning hamkorligi orqaligina zamonaviy kibertahdidlarga qarshi samarali kurashish va raqamli makonda xavfsizlikni ta'minlash mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni, 2022 yil.
2. O'zbekiston Respublikasi Prezidentining "Kiberxavfsizlikni ta'minlash tizimini yanada takomillashtirish chora-tadbirlari to'g'risida"gi PQ–165-son qarori, 2025 yil 15 aprel.
3. Axmedov B.A. Axborot xavfsizligi asoslari. – Toshkent: "Fan va texnologiya", 2021. – 248 b.
4. Karimov I.K. Kiberjinoyatchilikka qarshi kurashishning huquqiy mexanizmlari. – Toshkent: TDYU nashriyoti, 2023. – 186 b.
5. Stallings W. Cryptography and Network Security: Principles and Practice. 8th Edition. – Pearson, 2020. – 832 p.
6. Cybersecurity Ventures. Official Annual Cybercrime Report, 2023.
7. European Union Agency for Cybersecurity (ENISA). Threat Landscape Report, 2024.
8. NIST. Post-Quantum Cryptography: Final Report, 2024.
9. Symantec. Internet Security Threat Report, Volume 25, 2024.
10. Kaspersky Lab. Ransomware and Critical Infrastructure Report, 2024.