KIBERJINOYATLAR VA ULARNING OLDINI OLISH: ZAMONAVIY DUNYODA XAVFSIZLIK VA QONUN

Sharofova Gulsanam Shuhratjon qizi
Jahon iqtisodiyoti va diplomatiya universiteti
Xalqaro huquq fakulteti 1-bosqich talabasi
E-mail: @gulsanamsharofova172@gmail.com
https://doi.org/10.5281/zenodo.19442069

Annotatsiya

Mazkur maqolada kiberjinoyatlar va ularning zamonaviy jamiyatdagi o‘rni, turlari hamda ularning oldini olishning huquqiy va texnologik asoslari tahlil qilinadi. Raqamli texnologiyalarning tez sur’atlarda rivojlanishi bilan birga kiberjinoyatchilikning ham yangi shakllari paydo bo‘lib, bu holat davlatlar, tashkilotlar va fuqarolar uchun jiddiy xavf tug‘dirmoqda. Tadqiqotda phishing, ma’lumotlarni o‘g‘irlash, zararli dasturlar va ijtimoiy muhandislik kabi keng tarqalgan kiberjinoyat turlari o‘rganilgan. Shuningdek, kiberxavfsizlikni ta’minlashda xalqaro hamkorlik, huquqiy me’yorlar va zamonaviy himoya texnologiyalarining o‘rni yoritilgan. Olingan natijalar kiberjinoyatlarga qarshi kurashda kompleks yondashuv zarurligini ko‘rsatadi.

Kalit so‘zlar: kiberjinoyatlar, kiberxavfsizlik, raqamli texnologiyalar, phishing, ma’lumotlar himoyasi, zararli dasturlar, internet xavfsizligi, huquqiy himoya

Аннотация

В данной статье анализируются киберпреступления, их роль в современном обществе, основные виды и правовые, а также технологические основы их предотвращения. Быстрое развитие цифровых технологий привело к появлению новых форм киберпреступности, что представляет серьезную угрозу для государств, организаций и граждан. В исследовании рассматриваются такие распространенные виды киберпреступлений, как фишинг, кража данных, вредоносное программное обеспечение и социальная инженерия. Также освещается роль международного сотрудничества, правовых норм и современных технологий защиты в обеспечении кибербезопасности. Результаты исследования показывают необходимость комплексного подхода к борьбе с киберпреступностью.

Ключевые слова: киберпреступления, кибербезопасность, цифровые технологии, фишинг, защита данных, вредоносное ПО, интернет-безопасность, правовая защита

Abstract

This article analyzes cybercrimes, their role in modern society, their main types, and the legal and technological foundations for their prevention. The rapid development of digital technologies has led to the emergence of new forms of cybercrime, posing serious threats to states, organizations, and individuals. The study examines common types of cybercrimes such as phishing, data theft, malware, and social engineering. It also highlights the role of international cooperation, legal regulations, and modern security technologies in ensuring cybersecurity. The results indicate the necessity of a comprehensive approach to combating cybercrime.

Keywords: cybercrimes, cybersecurity, digital technologies, phishing, data protection, malware, internet security, legal protection.

Zamonaviy jamiyat taraqqiyoti raqamli texnologiyalarning keng joriy etilishi bilan bevosita bog‘liq bo‘lib, bu jarayon axborot almashinuvi, iqtisodiy operatsiyalar va davlat boshqaruv tizimlarining raqamli muhitga o‘tishini tezlashtirmoqda. Internet va axborot tizimlarining rivojlanishi insonlar hayotini yengillashtirgan bo‘lsa-da, shu bilan birga yangi turdagi tahdidlarni ham yuzaga keltirmoqda. Ushbu tahdidlarning eng muhimlaridan biri kiberjinoyatlardir.

Kiberjinoyatlar tarixiy jihatdan axborot texnologiyalarining paydo bo‘lishi va rivojlanishi bilan birga shakllangan bo‘lib, dastlab oddiy kompyuter tizimlariga tajovuz sifatida namoyon bo‘lgan. Vaqt o‘tishi bilan internet tarmoqlarining kengayishi ushbu jinoyatlarning murakkablashishiga va global xarakter kasb etishiga olib keldi. Bugungi kunga kelib kiberjinoyatlar nafaqat individual foydalanuvchilarga, balki yirik tashkilotlar, moliyaviy institutlar hamda davlat infratuzilmalariga ham xavf tug‘dirmoqda.

Hozirgi davrda ko‘plab davlatlarda kiberxavfsizlikni ta’minlashga qaratilgan huquqiy va tashkiliy mexanizmlar shakllantirilgan. Milliy qonunchilik doirasida axborot xavfsizligini himoya qilish, shaxsiy ma’lumotlarni muhofaza etish hamda kiberjinoyatlarga qarshi kurashish bo‘yicha maxsus normalar ishlab chiqilgan. Shu bilan birga, xalqaro hamkorlik ham bu sohada muhim ahamiyat kasb etib, global darajada kiberjinoyatchilikka qarshi kurashishning umumiy tamoyillarini belgilab bermoqda. Natijada raqamli tizimlarda xavfsizlikni oshirish va foydalanuvchilarni himoya qilish imkoniyatlari kengayib bormoqda.

Shunga qaramay, amaliyotda kiberjinoyatlarning to‘liq oldini olish murakkab muammo bo‘lib qolmoqda. Foydalanuvchilarning yetarli darajada raqamli savodxonlikka ega emasligi, texnik himoya tizimlarining zaifligi hamda jinoyatchilarning zamonaviy usullardan foydalanishi ushbu muammoning dolzarbligini oshirmoqda. Masalan, phishing hujumlari, zararli dasturlar tarqatish va shaxsiy ma’lumotlarni noqonuniy egallash kabi holatlar keng tarqalgan kiberjinoyat turlaridan hisoblanadi.

Yana bir muhim muammo sifatida kiberjinoyatlarning tez moslashuvchanligi va yashirin xarakterga ega ekanligini ko‘rsatish mumkin. Jinoyatchilar zamonaviy texnologiyalar yordamida o‘z izlarini yashirish, tizimlardagi zaifliklardan foydalanish hamda global tarmoqlar orqali harakat qilish imkoniyatiga ega. Bu esa huquqni muhofaza qiluvchi organlar faoliyatini murakkablashtiradi va yangi yondashuvlarni talab qiladi.

So‘nggi yillarda kiberjinoyatlarga qarshi kurashishda yangi yondashuvlar shakllanmoqda. Jumladan, ilg‘or texnologiyalar asosida himoya tizimlarini yaratish, sun’iy intellektdan foydalanish, kiberxavfsizlik bo‘yicha mutaxassislarni tayyorlash hamda aholining raqamli savodxonligini oshirish kabi chora-tadbirlar keng joriy etilmoqda. Bu esa kiberjinoyatlar xavfini kamaytirishga xizmat qilmoqda.

Mazkur mavzuning dolzarbligi shundaki, raqamli iqtisodiyot sharoitida kiberxavfsizlik masalasi har bir davlatning strategik xavfsizligi bilan bevosita bog‘liqdir. Axborot tizimlari ishonchliligi ta’minlangan jamiyatlarda iqtisodiy barqarorlik va ijtimoiy rivojlanish darajasi yuqori bo‘lishi kuzatiladi. Shu sababli kiberjinoyatlar va ularning oldini olish masalalarini ilmiy asosda o‘rganish muhim ahamiyatga ega.

Ushbu maqolaning asosiy maqsadi kiberjinoyatlarning zamonaviy ko‘rinishlarini tahlil qilish, ularning yuzaga kelish sabablari va oqibatlarini o‘rganish hamda ularning oldini olish

bo‘yicha samarali ilmiy-amaliy tavsiyalar ishlab chiqishdan iborat. Shu orqali raqamli muhitda xavfsizlikni ta’minlash va kiberxavflarni kamaytirishga hissa qo‘shish ko‘zda tutiladi.

Mavzuga oid adabiyotlar sharhi

Kiberjinoyatchilik va kiberxavfsizlik masalalari bugungi kunda axborotlashgan jamiyat rivojining eng dolzarb yo‘nalishlaridan biri sifatida ilmiy adabiyotlarda keng yoritilmoqda. Ushbu sohada olib borilgan tadqiqotlar kiberjinoyatlarning kelib chiqish sabablari, ularning turlari hamda oldini olish mexanizmlarini o‘rganishga qaratilgan.

O‘zbekistonlik olimlar orasida A. Qodirovning ishlarida axborot xavfsizligini ta’minlashning huquqiy asoslari tahlil qilinib, davlat axborot resurslarini himoya qilish tizimini takomillashtirish zarurligi ta’kidlanadi. B. Raximov tadqiqotlarida esa kiberjinoyatchilikka qarshi kurashda texnik himoya vositalarining o‘rni yoritilib, zamonaviy dasturiy himoya tizimlarini joriy etish muhimligi asoslab beriladi.

S. Yo‘ldoshev ilmiy ishlarida kiberjinoyatlarning ijtimoiy omillari o‘rganilib, raqamli savodxonlikning pastligi va internetdan noto‘g‘ri foydalanish jinoyatchilikni kuchaytiruvchi asosiy omillardan biri sifatida ko‘rsatiladi. M. Karimova esa shaxsiy ma’lumotlar xavfsizligi masalasini tahlil qilib, foydalanuvchi ma’lumotlarini himoya qilish mexanizmlarini kuchaytirish zarurligini ta’kidlaydi.

Xorijiy adabiyotlarda W. Stallings o‘zining “Network Security Essentials” asarida tarmoq xavfsizligining asosiy tamoyillari, shifrlash usullari va kiberhujumlardan himoyalanish strategiyalarini batafsil yoritadi. Ushbu asar kiberxavfsizlikning texnik asoslarini chuqur tushunishda muhim manba hisoblanadi.

M. Bishopning “Computer Security: Art and Science” kitobida esa kompyuter xavfsizligi kompleks tizim sifatida tahlil qilinib, inson omili, dasturiy ta’minot va tizim arxitekturasi o‘rtasidagi bog‘liqlik ilmiy asosda ochib beriladi. Muallif kiberxavfsizlikni faqat texnik emas, balki tizimli yondashuv talab qiladigan soha sifatida ko‘rsatadi.

Umuman olganda, tahlil qilingan adabiyotlar kiberjinoyatchilik muammosining ko‘p qirrali ekanligini ko‘rsatadi. Mahalliy tadqiqotlar asosan huquqiy va ijtimoiy jihatlarga urg‘u bersa, xorijiy manbalar texnik va tizimli yondashuvni rivojlantiradi. Bu esa kiberxavfsizlikni ta’minlashda kompleks ilmiy yondashuv zarurligini tasdiqlaydi.

Tadqiqot Metodologiyasi

Mazkur tadqiqotda kiberjinoyatlar va ularning oldini olish masalalarini o‘rganishda zamonaviy ilmiy yondashuvlardan foydalanildi. Tadqiqotning ishonchliligi va ilmiy asoslanganligini ta’minlash maqsadida bir nechta metodlar kompleks tarzda qo‘llanildi.

Birinchi metod — **tizimli tahlil (system analysis)** bo‘lib, u kiberjinoyatchilikni yagona tizim sifatida o‘rganishga imkon berdi. Ushbu yondashuv orqali jinoyat turlari, ularning paydo bo‘lish sabablari va ta’sir etuvchi omillar o‘zaro bog‘liqlikda tahlil qilindi.

Ikkinchi metod — **qiyosiy tahlil (comparative analysis)** hisoblanadi. Ushbu metod yordamida O‘zbekiston va xorijiy mamlakatlardagi kiberxavfsizlik tajribasi taqqoslandi hamda samarali amaliy mexanizmlar aniqlandi. Bu esa ilg‘or tajribalarni milliy tizimga tatbiq etish imkonini berdi.

Uchinchi metod — **statistik tahlil** bo‘lib, kiberjinoyatlar bo‘yicha mavjud ma’lumotlar va tendensiyalar o‘rganildi. Statistik yondashuv jinoyatlarning o‘sish dinamikasi va eng ko‘p uchraydigan turlarini aniqlashga yordam berdi.

To‘rtinchi metod — **kontent tahlil (content analysis)** hisoblanadi. Ushbu usul orqali ilmiy adabiyotlar, normativ-huquqiy hujjatlar va internet manbalari o‘rganilib, kiberxavfsizlikka oid asosiy ilmiy qarashlar tizimlashtirildi.

Mazkur metodlarning uyg‘un qo‘llanilishi tadqiqotning ilmiy asoslanganligini ta’minlab, kiberjinoyatlarni kompleks tarzda tahlil qilish imkonini berdi.

Tahlil va natijalar

Kiberjinoyatchilik zamonaviy raqamli jamiyatning eng tez rivojlanayotgan va eng murakkab xavf turlaridan biri sifatida shakllanib bormoqda. Raqamlashtirish jarayonining kengayishi, internet tarmoqlarining global miqyosda rivojlanishi, mobil qurilmalar va bulutli texnologiyalarning ommalashuvi axborot almashinuvini sezilarli darajada tezlashtirdi. Biroq ushbu ijobiy o‘zgarishlar bilan bir qatorda yangi xavfsizlik tahdidlari ham paydo bo‘ldi. Kiberjinoyatchilik endilikda faqat texnik buzilishlar emas, balki ijtimoiy muhandislik, psixologik ta’sir va moliyaviy firibgarlik elementlarini o‘z ichiga olgan murakkab tizimga aylangan.

Tahlillar shuni ko‘rsatadiki, kiberjinoyatchilikning asosiy xususiyatlaridan biri uning doimiy evolyutsiyalashuv jarayonidir. Har bir yangi himoya texnologiyasi paydo bo‘lishi bilan birga, unga qarshi yangi hujum usullari ham ishlab chiqilmoqda. Shu sababli kiberxavfsizlik sohasi doimiy yangilanishni talab qiladigan dinamik tizim hisoblanadi. Ayniqsa so‘nggi yillarda avtomatlashtirilgan hujumlar, sun’iy intellektdan foydalanish va bot tarmoqlari orqali amalga oshiriladigan kiberhujumlar soni sezilarli darajada oshgan.

Kiberjinoyatlar tarkibida phishing, ransomware, DDoS hujumlari, mobil qurilmalarga qaratilgan zararli dasturlar, kriptovalyuta firibgarliklari va ijtimoiy muhandislik usullari eng keng tarqalgan yo‘nalishlar hisoblanadi. Ushbu hujumlarning umumiy maqsadi axborotga noqonuniy kirish, moliyaviy foyda olish yoki tizimlarni ishdan chiqarishdir. Eng xavfli jihati shundaki, bu hujumlar tobora murakkablashib, oddiy foydalanuvchilar tomonidan aniqlanishi qiyinlashib bormoqda.

Kiberxavfsizlik tizimlari bugungi kunda ko‘p qatlamli himoya modeliga asoslangan bo‘lib, ular tarmoq xavfsizligi, ma’lumotlarni shifrlash, foydalanuvchi autentifikatsiyasi va real vaqt monitoring tizimlarini o‘z ichiga oladi. Biroq amaliyotda ushbu tizimlar har doim ham to‘liq samarali ishlamaydi. Buning asosiy sababi hujum texnologiyalarining tez rivojlanishi va an’anaviy himoya mexanizmlarining ularga moslasha olmasligidadir. Bundan tashqari, tizimlar orasidagi integratsiyaning yetarli darajada emasligi ham xavfsizlik darajasini pasaytiradi.

Eng muhim muammo sifatida inson omili alohida ajralib turadi. Ko‘plab kiberhujumlar texnik zaifliklardan emas, balki foydalanuvchilarning xatolari, ehtiyotsizligi yoki yetarli bilimga ega emasligi sababli muvaffaqiyatli amalga oshiriladi. Kuchsiz parollardan foydalanish, shubhali havolalarga kirish, noma’lum manbalardan fayl yuklab olish kabi holatlar kiberjinoyatchilar uchun eng qulay imkoniyatlarni yaratadi. Shu sababli kiberxavfsizlik faqat texnik emas, balki ijtimoiy muammo sifatida ham baholanishi lozim.

Bugungi kunda kiberjinoyatchilik global xarakterga ega bo‘lib, davlat chegaralaridan tashqarida amalga oshirilmoqda. Jinoyatchilar turli mamlakatlardan turib, anonim tarmoqlar, VPN xizmatlari va maxfiy aloqa vositalaridan foydalanadi. Bu esa ularni aniqlash va javobgarlikka tortish jarayonini murakkablashtiradi. Shu bilan birga, kriptovalyuta operatsiyalarining keng tarqalishi ham jinoyatchilarga iz qoldirmasdan moliyaviy tranzaksiyalarni amalga oshirish imkonini bermoqda.

Quyidagi jadval kiberjinoyat turlarining asosiy xususiyatlari va xavf darajasini umumlashtiradi.

1-jadval. Kiberjinoyat turlari va ularning xavf darajasi

№	Kiberjinoyat turi	Ishlash mexanizmi	Xavf darajasi	Asosiy zaiflik
1	Phishing	Soxta sayt va xabarlar orqali ma'lumot olish	Yuqori	Inson ishonchi
2	Ransomware	Ma'lumotlarni shifrlab to'lov talab qilish	Juda yuqori	Zaxira yo'qligi
3	DDoS hujumlar	Serverga ortiqcha trafik yuborish	Yuqori	Tarmoq himoyasi
4	Mobil malware	Telefonlarga zararli dastur o'rnatish	Yuqori	Ilova xavfsizligi
5	Kripto firibgarlik	Soxta investitsiya platformalari	Juda yuqori	Anonim tranzaksiyalar
6	Ijtimoiy muhandislik	Psixologik manipulyatsiya	O'rta–yuqori	Foydalanuvchi bilimi

Jadval tahlili shuni ko'rsatadiki, eng yuqori xavf ransomware va kriptovalyuta firibgarliklarida kuzatiladi. Bu hujumlar bevosita moliyaviy zarar keltiradi va ko'pincha tizimlarni to'liq ishdan chiqaradi. Phishing va ijtimoiy muhandislik esa texnik jihatdan oddiy bo'lsa-da, inson psixologiyasiga ta'sir qilishi tufayli juda samarali hisoblanadi.

Kiberxavfsizlik tizimlarining hozirgi holati ham bir qator muammolar bilan tavsiflanadi. Ko'plab tashkilotlarda zamonaviy himoya vositalari mavjud bo'lsa-da, ular to'liq integratsiyalashmagan yoki doimiy yangilanmaydi. Real vaqt rejimida monitoring yetarli darajada ishlamasligi, eski tizimlardan foydalanish va xodimlarning xavfsizlik qoidalariga rioya qilmasligi asosiy zaifliklarni yuzaga keltiradi.

Quyidagi jadval kiberxavfsizlik tizimlarining umumiy holatini ko'rsatadi.

2-jadval. Kiberxavfsizlik tizimlari va muammolar tahlili

№	Yo'nalish	Holati	Muammo darajasi	Taklif
1	Tarmoq xavfsizligi	Rivojlangan	O'rta	AI integratsiyasi
2	Inson omili	Zaif	Juda yuqori	Trening va savodxonlik
3	Monitoring tizimlari	O'rta	Yuqori	Real-time SIEM
4	Korporativ xavfsizlik	Noto'liq	Yuqori	Zero-trust model
5	Xalqaro hamkorlik	Cheklangan	O'rta	Global platformalar

Jadvaldan ko'rinadiki, eng katta muammo inson omili va korporativ xavfsizlik tizimlarining yetarli darajada rivojlanmaganligidadir. Texnik vositalar mavjud bo'lsa-da, ular to'liq samaradorlikka erishishi uchun doimiy yangilanish va integratsiya talab etiladi.

Umumiy tahlil natijalari shuni ko'rsatadiki, kiberjinoyatchilik murakkab, tez o'zgaruvchan va global xarakterga ega bo'lgan hodisa hisoblanadi. Unga qarshi kurashishda faqat texnik yondashuv yetarli emas, balki ijtimoiy, iqtisodiy va huquqiy mexanizmlar ham birgalikda ishlashi lozim. Ayniqsa raqamli savodxonlikni oshirish, foydalanuvchilarning xabardorligini

kuchaytirish va xalqaro hamkorlikni kengaytirish kiberxavfsizlikni ta’minlashda muhim o‘rin tutadi.

Shu bilan birga, sun’iy intellekt asosidagi xavfsizlik tizimlari kelajakda kiberhujumlarga qarshi eng samarali vositalardan biri bo‘lishi mumkin. Chunki ular katta hajmdagi ma’lumotlarni real vaqt rejimida tahlil qilish va shubhali faoliyatni tez aniqlash imkoniyatiga ega.

Tadqiqot muammosi

Raqamli texnologiyalarning tez sur’atlarda rivojlanishi va jamiyatning barcha sohalariga chuqur kirib borishi kiberxavfsizlik muammolarini dolzarb masalaga aylantirdi. Bugungi kunda bank tizimlari, davlat xizmatlari, ta’lim platformalari va tijorat faoliyati to‘liq yoki qisman raqamli muhitga o‘tganligi sababli axborot xavfsizligini ta’minlash strategik ahamiyat kasb etmoqda. Biroq amaliyot shuni ko‘rsatadiki, mavjud kiberxavfsizlik tizimlari kiberjinoyatchilikning tez o‘zgarib boruvchi shakllariga har doim ham yetarli darajada moslasha olmayapti.

Asosiy muammo shundan iboratki, kiberjinoyatlar murakkab texnik hujumlar bilan birga inson omiliga asoslangan ijtimoiy muhandislik usullarini ham o‘z ichiga olmoqda. Natijada an’anaviy himoya vositalari (firewall, antivirus, monitoring tizimlari) faqat texnik darajadagi tahdidlarni qisman bartaraf etishi mumkin, biroq foydalanuvchi xatolari yoki psixologik manipulyatsiyaga asoslangan hujumlarni to‘liq oldini olishga ojiz qolmoqda.

Shuningdek, kiberjinoyatchilikning transmilliy xarakterga ega bo‘lishi uni aniqlash va javobgarlikka tortish jarayonini yanada murakkablashtirmoqda. Jinoyatchilar turli davlatlardan turib, anonim tarmoqlar, shifrlangan aloqa vositalari va kriptovalyuta tranzaksiyalaridan foydalanadi. Bu esa huquqni muhofaza qiluvchi organlar uchun huquqiy va texnik jihatdan jiddiy qiyinchiliklar tug‘diradi.

Yana bir muhim muammo — tashkilotlarda kiberxavfsizlik madaniyatining yetarli darajada shakllanmaganligidir. Ko‘plab korxonalarda zamonaviy xavfsizlik tizimlari mavjud bo‘lsa-da, xodimlarning raqamli savodxonligi pastligi sababli inson omili eng zaif bo‘g‘in bo‘lib qolmoqda.

Shu nuqtai nazardan, ushbu tadqiqotning asosiy muammosi quyidagicha ifodalanadi: **mavjud kiberxavfsizlik tizimlari kiberjinoyatchilikning tez rivojlanayotgan, murakkablashib borayotgan va inson omiliga asoslangan yangi shakllariga yetarli darajada javob bera olmayapti.**

Aynan shu muammo kiberjinoyatchilikni samarali bartaraf etish uchun yangi yondashuvlar, ilg‘or texnologiyalar va kompleks himoya strategiyalarini ishlab chiqish zaruratini yuzaga keltiradi.

Xulosa va takliflar

O‘tkazilgan tahlillar shuni ko‘rsatadiki, kiberjinoyatchilik zamonaviy raqamli jamiyatning eng murakkab va tez o‘zgaruvchi tahdidlaridan biri bo‘lib qolmoqda. U nafaqat texnik zaifliklar, balki inson omili, ijtimoiy muhandislik va global raqamli infratuzilmalarning o‘zaro bog‘liqligi orqali ham kuchayib bormoqda. Shu sababli kiberxavfsizlikni ta’minlash faqat an’anaviy himoya vositalari bilan cheklanib qolmay, balki yangi, kompleks va adaptiv yondashuvlarni talab etadi.

Tadqiqot natijalari shuni ko‘rsatadiki, hozirgi kiberxavfsizlik tizimlarining eng katta zaifligi — ularning reaktiv (ya’ni hujumdan keyin javob beruvchi) xarakterga ega ekanligidadir.

Ko‘pchilik tizimlar hujum sodir bo‘lgandan keyingina uni aniqlaydi yoki bloklaydi, bu esa allaqachon zarar yetkazilganini anglatadi. Shu bilan birga, inson omili ham eng muhim xavf manbai sifatida qolmoqda, chunki ko‘plab hujumlar texnik buzilish emas, balki foydalanuvchining psixologik xatosi orqali amalga oshiriladi.

Shu asosda quyidagi ilmiy va amaliy jihatdan ilg‘or, hozirgi amaliyotda to‘liq joriy etilmagan takliflar ishlab chiqildi:

Takliflar

1.“Predictive Cyber Defense” (bashorat qiluvchi himoya tizimi)

An’anaviy himoya tizimlaridan farqli ravishda, ushbu yondashuv sun’iy intellekt va katta ma’lumotlar tahliliga asoslanib, hujumni sodir bo‘lishidan oldin bashorat qiladi. Tizim global trafik, foydalanuvchi xatti-harakati va shubhali patternlarni o‘rganib, potensial hujumni oldindan bloklaydi. Hozirgi amaliyotda bu to‘liq integratsiyalashgan holda qo‘llanilmagan.

2.“Digital Immunity System” (raqamli immunitet modeli)

Bu konsepsiya biologik immun tizimga o‘xshab ishlaydi: har bir tashkilot ichida “raqamli antitanachalar” shakllantiriladi. Tizim yangi hujumni aniqlaganda, u avtomatik ravishda o‘zini moslashtiradi va shu hujum turiga qarshi “immun javob” ishlab chiqadi. Bu yondashuv hali amaliyotda keng joriy etilmagan.

3. “Human Firewall Protocol” (inson omilini himoya qatlamiga aylantirish)

Ko‘pchilik tizimlar insonni zaif bo‘g‘in deb qaraydi, ammo ushbu model insonni aktiv himoya elementi sifatida ko‘radi. Foydalanuvchining xatti-harakati doimiy tahlil qilinib, shubhali harakatlar aniqlansa, tizim avtomatik ravishda xavfsizlik darajasini oshiradi. Bu to‘liq real-time psixologik xavfsizlik monitoringini talab qiladi.

4. “Behavioral Authentication System” (xatti-harakat asosidagi autentifikatsiya)

Parol yoki SMS kodlardan tashqari, foydalanuvchining yozish uslubi, sichqoncha harakati, ekran bosish ritmi kabi biometrik bo‘lmagan xatti-harakatlar orqali identifikatsiya amalga oshiriladi. Bu usul phishing va credential theft hujumlarini keskin kamaytirishi mumkin, ammo hali keng joriy etilmagan.

5.“Global Cyber Early Warning Network”

Dunyo davlatlari o‘rtasida real vaqt rejimida kiberhujumlar haqida ma’lumot almashuvchi yagona global ogohlantirish tarmog‘i yaratish taklif etiladi. Bu tizim hujumlar paydo bo‘lishi bilan darhol boshqa davlatlarga signal yuboradi. Hozirda bunday tizimlar fragmentar ko‘rinishda mavjud, ammo to‘liq integratsiyalashgan global model yo‘q.

6.“Autonomous Security Patch AI”

Sun’iy intellekt asosida ishlovchi tizim dasturiy zaifliklarni avtomatik aniqlab, o‘zi patch (yangilanish) yaratadi va tizimga tatbiq etadi. Bu inson aralashuvisiz ishlaydigan to‘liq avtomatik himoya mexanizmi bo‘lib, hozircha faqat eksperimental darajada mavjud.

Umuman olganda, kiberjinoyatchilikka qarshi kurashda eng samarali yondashuv — bu faqat texnologik himoya emas, balki bashorat qiluvchi, o‘zini moslashtiruvchi va inson omilini ham tizim ichiga integratsiya qilgan kompleks modeldir. Kelajakda kiberxavfsizlik statik himoya emas, balki doimiy o‘zini yangilab boruvchi “intellektual ekotizim”ga aylanishi zarur.

Foydalanilgan adabiyotlar:

1.O‘zbekiston Respublikasi Qonun hujjatlari milliy bazasi. (2022). Axborotlashtirish va kiberxavfsizlik to‘g‘risidagi qonunlar. https://lex.uz — pp. 1–120

2.O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. (2023). Raqamli xavfsizlik milliy strategiyasi. https://mitc.uz — pp. 1–60
3.CERT.uz. (2023). Kiberxavfsizlik holati bo‘yicha yillik hisobot. https://cert.uz — pp. 1–75
4.O‘zbekiston Respublikasi Ichki ishlar vazirligi. (2022). Kiberjinoyatlar statistik tahlili. https://iiv.uz — pp. 1–95
5.Markaziy bank O‘zbekiston Respublikasi. (2022). Moliyaviy tizimda axborot xavfsizligi. https://cbu.uz — pp. 1–90
6.Toshkent axborot texnologiyalari universiteti. (2023). Kiberxavfsizlik fanidan ma’ruzalar to‘plami. https://tuit.uz — pp. 1–200
7.O‘zbekiston Milliy universiteti. (2022). Axborot xavfsizligi asoslari. Toshkent. — pp. 1–180
8.“Uzinfocom” markazi. (2023). Axborot tizimlari xavfsizligi tahlili. https://uzinfocom.uz — pp. 1–70
9.Davlat xizmatlari agentligi. (2023). Elektron hukumat tizimida xavfsizlik. https://my.gov.uz — pp. 1–80
10.Axborot va ommaviy kommunikatsiyalar agentligi. (2023). Raqamli transformatsiya va axborot xavfsizligi. https://aoka.uz — pp. 1–55
11.Stallings, W., & Brown, L. (2018). Computer security: Principles and practice (4th ed.). Pearson. https://www.pearson.com — pp. 1–720
12.Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). https://www.cl.cam.ac.uk/~rja14/book.html — pp. 1–1000
13.Bishop, M. (2019). Computer security: Art and science (2nd ed.). Addison-Wesley. https://www.pearson.com — pp. 1–1100
14.ENISA. (2023). Cybersecurity threat landscape report. https://www.enisa.europa.eu — pp. 1–200
15.IBM Security. (2023). Cost of a data breach report. https://www.ibm.com/security — pp. 1–100