Andijon davlat texnika instituti
“Axbororot texnologiyalar “kafedrasi
Phd, Dotsent, Atajonova Saidaxon
Borataliyevna taqrizi ostida

Quldashev Erkinjon
Professor, Andijon davlat texnika institute O‘zbekiston
+998901732165
muhammaderkinov@gmail.com
Maxsudjonova Xikmatxon Iqboljon qizi
Talaba, Andijon davlat texnika institute O‘zbekiston
+9988806123332
xikmatxonmaxsudjonova@gmail.com

KIBERTAHDIDLAR VA AXBOROT XAVFSIZLIGI

Annotatsiya: Ushbu maqolada zamonaviy dunyoda kibertahdidlarning axborot xavfsizligiga ta’siri va ushbu tahdidlarga qarshi kurashish choralari tahlil qilinadi. Raqamli texnologiyalar rivojlanishi bilan kibertahdidlarning soni va turlari ortib bormoqda, bu esa axborot tizimlari va foydalanuvchilar xavfsizligiga jiddiy tahdid tug‘diradi. Kibertahdidlar davlat organlari, xususiy sektor va oddiy foydalanuvchilar uchun katta xavf bo‘lib, ular moliyaviy yo‘qotishlar, shaxsiy ma’lumotlarning o‘g‘irlanishi va tizimlarning ishdan chiqishiga sabab bo‘lishi mumkin. Ushbu maqolada kibertahdidlarning asosiy turlari, ularning zararli ta’siri, himoya strategiyalari va axborot xavfsizligini ta’minlashda zamonaviy texnologiyalarning o‘rni batafsil ko‘rib chiqiladi. Shuningdek, kibertahdidlarga qarshi samarali kurashish choralari va foydalanuvchilarning kiberxavfsizlik bo‘yicha xabardorligini oshirish muhimligi ham tahlil qilinadi. Raqamli texnologiyalar rivojlanishi bilan kibertahdidlarning xilma-xilligi ortib bormoqda, bu esa korxonalar, davlat tashkilotlari va jismoniy shaxslar uchun jiddiy xavf tug‘diradi. Maqolada kibertahdidlarning asosiy turlari, ularning oldini olish usullari va axborot xavfsizligini ta’minlashning zamonaviy texnologiyalari ko‘rib chiqiladi.

Kalit so‘zlar: kibertahdid, axborot xavfsizligi, kiberjinoyatlar, ma’lumotlar himoyasi, tarmoq xavfsizligi.

Kirish Axborot texnologiyalarining jadal rivojlanishi natijasida raqamli muhitda ishlovchi barcha subyektlar kibertahdidlarga duch kelmoqda. Raqamli transformatsiya jarayoni kundalik hayotimizning barcha jabhalariga ta’sir ko‘rsatib, davlat idoralari, biznes tashkilotlari va jismoniy shaxslarning axborot resurslaridan foydalanish usullarini o‘zgartirmoqda. Shu bilan birga, internet va bulutli texnologiyalarning keng qo‘llanilishi axborot xavfsizligiga bo‘lgan talabni keskin oshirmoqda. Bunday sharoitda kiberjinoyatchilikning ortishi va zararli dasturlar, fishing hujumlari, DDoS xurujlari kabi tahdidlarning ko‘payishi axborot resurslarini himoya qilishni muhim masalaga aylantirdi.

Kiberjinoyatchilar turli texnologik yutuqlardan foydalangan holda, himoyasiz axborot tizimlariga hujum qilib, foydalanuvchilarning shaxsiy ma’lumotlarini o‘g‘irlash, moliyaviy firibgarlik sodir etish va muhim infratuzilmalarni izdan chiqarishga qaratilgan xurujlar uyushtirmoqdalar. Shu sababli axborot xavfsizligini ta’minlash faqat texnologik masala bo‘lib qolmay, balki global darajadagi muammo sifatida ko‘rilmoqda.

Ushbu maqolada kibertahdidlarning asosiy turlari, ularning axborot xavfsizligiga ta’siri va ularga qarshi kurashish usullari tahlil qilinadi. Bundan tashqari, raqamli muhitda xavfsizlikni ta’minlash bo‘yicha ilg‘or texnologiyalar va amaliy chora-tadbirlar ham ko‘rib chiqiladi. Kibertahdidlar bu – zarar yetkazish yoki noqonuniy ma’lumot olish maqsadida amalga oshiriladigan kiberhujumlar hisoblanadi. Ular hukumat tizimlariga, tijorat kompaniyalariga va oddiy foydalanuvchilarga katta zarar yetkazishi mumkin. Ushbu maqolada kibertahdidlarning asosiy turlari, ularning xavflari va ularga qarshi kurashish strategiyalari tahlil qilinadi.

Usullar Ushbu maqolada kibertahdidlar va axborot xavfsizligiga oid tadqiqotlar, ilmiy maqolalar hamda rasmiy hisobotlar tahlil qilindi. Tadqiqot davomida ilmiy-analitik yondashuv asosida mavjud adabiyotlar o‘rganildi hamda zamonaviy kibertahdidlarning tabiati va ularga qarshi kurashish usullari chuqur tahlil qilindi. Bundan tashqari, sohada olib borilgan ilg‘or tadqiqotlarning natijalari ham ko‘rib chiqilib, ularning samaradorligi baholandi.

Kibertahdidlarni o‘rganish jarayonida quyidagi yondashuvlardan foydalanildi:

1. **Adabiyotlar tahlili** – mavjud ilmiy maqolalar, tadqiqotlar va xalqaro tashkilotlarning axborot xavfsizligi bo‘yicha hisobotlari o‘rganildi.
2. **Statistik ma’lumotlarni tahlil qilish** – oxirgi yillarda qayd etilgan kibertahdidlar, ularning iqtisodiy va ijtimoiy ta’siri hamda global miqyosdagi xavfsizlik strategiyalarining samaradorligi baholandi.
3. **Ekspert fikrlari** – axborot xavfsizligi bo‘yicha mutaxassislar tomonidan bildirilgan fikrlar va tavsiyalar tahlil qilindi.
4. **Amaliy tajribalar va real misollar** – yirik kompaniyalarga, davlat tashkilotlariga va jismoniy shaxslarga qaratilgan kiberhujumlar bo‘yicha misollar o‘rganildi va ulardan olinadigan saboqlar tahlil qilindi.

Tahlil jarayonida eng ommaviy va xavfli kibertahdidlar, jumladan, fishing, zararli dasturlar, DDoS hujumlari va tarmoqlarga noqonuniy kirish holatlari ko‘rib chiqildi. Shuningdek, himoya vositalari va xavfsizlikni ta’minlash strategiyalarining samaradorligi baholandi. Ushbu metodologiya asosida olingan natijalar maqolaning keyingi qismlarida batafsil tahlil qilinadi. Shuningdek, zamonaviy kibertahdidlarga oid misollar va ularning oldini olish choralari ko‘rib chiqildi. Tadqiqotda kiberjinoyatlar, ma’lumotlar himoyasi va tarmoq xavfsizligini ta’minlash bo‘yicha ilg‘or amaliyotlar o‘rganildi.

Natijalar Tadqiqot natijalari shuni ko‘rsatdiki, zamonaviy kibertahdidlar tobora murakkablashib, ularning ta’siri global miqyosda sezilmoqda. Kibertahdidlarning eng keng tarqalgan turlari quyidagilardan iborat:

1. **Fishing** – foydalanuvchilarning shaxsiy ma’lumotlarini o‘g‘irlash maqsadida soxta elektron pochta yoki veb-sahifalar orqali amalga oshiriladi. So‘nggi yillarda fishing xurujlarining soni sezilarli darajada oshdi, bu esa korxonalar va shaxsiy foydalanuvchilarning katta miqdordagi ma’lumotlarini xavf ostida qoldirdi.
2. **Zararli dasturlar (malware)** – viruslar, troyanlar va reklama dasturlari kabi zararli kodlar orqali ma’lumotlarni buzish, o‘g‘irlash yoki tizimlarni ishdan chiqarish uchun ishlatiladi. Tadqiqot natijalari shuni ko‘rsatmoqdaki, global miqyosda har kuni minglab yangi zararli dasturlar yaratilmoqda.
3. **DDoS hujumlar** – server yoki tarmoq tizimiga ortiqcha yuklama berib, ularni ishdan chiqarishga qaratilgan. Ayniqsa, davlat muassasalari va yirik korxonalar bu hujumlardan jabr ko‘rmoqda. 2023-yilda kuzatilgan eng yirik DDoS hujumlardan biri dunyoning yetakchi kompaniyalarining tarmoqlariga zarar yetkazgan.

4. **Ma’lumotlarni o‘g‘irlash (data breach)** – xakerlar tomonidan kompaniyalarning maxfiy ma’lumotlari buzib kirilib, jamoatchilikka tarqatilishi yoki sotilishi. Tadqiqot natijalariga ko‘ra, bu hujumlarning aksariyati zaif parollar yoki zaif xavfsizlik tizimlari natijasida sodir bo‘lgan.
5. **Tarmoq buzilishi** – noqonuniy ravishda korporativ yoki davlat tarmoqlariga kirish holatlari. Bu turdagi xurujlar davlat xavfsizligiga jiddiy tahdid tug‘dirib, ba’zi hollarda strategik axborotlarning tarqalishiga olib keladi.

Tahlil natijalari shuni ko‘rsatdiki, aksariyat kibertahdidlar foydalanuvchilarning xavfsizlik choralariga yetarlicha e’tibor bermasligi yoki tizimlarning himoya darajasi pastligi tufayli sodir bo‘lmoqda. Xususan:

- **Foydalanuvchilarning xabardorligi past** – aksariyat hujumlar foydalanuvchilarning e’tiborsizligi yoki kiberhujum usullaridan bexabarligi sababli amalga oshirilgan.
- **Himoya mexanizmlarining sustligi** – eskirgan xavfsizlik tizimlari va yangilanishlarning o‘z vaqtida amalga oshirilmasligi natijasida ko‘plab ma’lumotlar o‘g‘irlash va buzilish xavfi ostida qolgani aniqlandi.
- **Zamonaviy texnologiyalarning yetarlicha qo‘llanilmasligi** – sun’iy intellekt va blokcheyn texnologiyalaridan foydalangan tizimlarning ancha samarali himoyaga ega ekanligi kuzatilgan, ammo ularning ko‘pchilik tashkilotlar tomonidan joriy etilmagani aniqlangan.

Ushbu natijalar kibertahdidlarga qarshi kurashish choralari samaradorligini oshirish zarurligini ko‘rsatmoqda. Axborot xavfsizligi strategiyalarining yanada mustahkamlanishi, foydalanuvchilar uchun xavfsizlik bo‘yicha o‘quv dasturlarini tashkil etish va zamonaviy himoya vositalaridan keng foydalanish kibertahdidlarga qarshi kurashda muhim omillardan biri bo‘lib xizmat qiladi. Fishing foydalanuvchilarni aldash orqali ularning shaxsiy ma’lumotlarini qo‘lga kiritish usuli bo‘lib, odatda soxta elektron pochta yoki veb-sahifalar orqali amalga oshiriladi. Zararli dasturlar (viruslar, troyanlar, reklama dasturlari) esa tizimga kirib, axborotni yo‘q qilish, shikast yetkazish yoki ruxsatsiz foydalanish imkonini beradi. DDoS hujumlar esa server yoki tarmoq tizimiga ortiqcha yuklama berish orqali ularni ishdan chiqarishga qaratilgan. Ushbu tahdidlarga qarshi kurashish uchun kuchli parollar qo‘llash, ikki faktorli autentifikatsiya, xavfsizlik devorlari (firewall), antivirus dasturlaridan foydalanish va muntazam ravishda tizim yangilanishlarini o‘tkazish muhim ahamiyat kasb etadi.

Muhokama Axborot xavfsizligini ta’minlashning zamonaviy texnologiyalari orasida sun’iy intellekt asosida ishlovchi xavfsizlik tizimlari, blokcheyn texnologiyalari va bulutli xavfsizlik xizmatlari alohida ajralib turadi. Zamonaviy kiberhujumlar tobora murakkablashib borayotgani sababli, an’anaviy xavfsizlik choralaridan tashqari, ilg‘or texnologiyalardan foydalanish zaruriyati ortib bormoqda.

Sun’iy intellekt kiberhujumlarni oldindan aniqlash, anomaliyalarni tahlil qilish va real vaqtda avtomatik javob berish imkonini yaratadi. Ushbu texnologiya zararli dasturlarni aniqlashda va tarmoqlarning himoyasini kuchaytirishda muhim rol o‘ynaydi. Bundan tashqari, sun’iy intellekt asosida ishlovchi tizimlar xakerlar tomonidan qo‘llaniladigan yangi hujum usullarini prognoz qilish va ularning oldini olishda ham samarali hisoblanadi.

Blokcheyn texnologiyalari esa ma’lumotlarning buzilmasligini va o‘zgartirilmasligini ta’minlashda qo‘llaniladi. Markazlashmagan saqlash tizimi sababli, blokcheynda saqlanayotgan ma’lumotlar yuqori darajada himoyalangan bo‘ladi. Bu texnologiya moliyaviy operatsiyalar, shaxsiy ma’lumotlar va davlat hujjatlarini himoya qilish uchun keng qo‘llanilmoqda.

Bulutli xavfsizlik xizmatlari esa tashkilotlar va shaxsiy foydalanuvchilar uchun samarali himoya vositalaridan biri bo‘lib, ma’lumotlarni markazlashgan holda xavfsiz saqlash imkonini beradi.

Bulutli texnologiyalar yordamida foydalanuvchilar o‘z ma’lumotlarini istalgan joydan xavfsiz tarzda boshqarishlari mumkin, shu bilan birga, ma’lumotlarni zahiralash va uzatish jarayonlari shifrlangan holda amalga oshiriladi.

Shuningdek, foydalanuvchilarning kiberxavfsizlik bo‘yicha xabardorligini oshirish ham muhim ahamiyatga ega. Statistika shuni ko‘rsatmoqdaki, kiberhujumlarning aksariyati inson omili tufayli sodir bo‘ladi, ya’ni foydalanuvchilar zaif parollardan foydalanish, phishing xabarlariga ishonish yoki shubhali ilovalarni yuklab olish kabi xatolarga yo‘l qo‘yadilar. Shu sababli, korxona va tashkilotlarda muntazam ravishda axborot xavfsizligi bo‘yicha treninglar o‘tkazilishi lozim.

Raqamli dunyoda ishonchli va himoyalangan muhit yaratish uchun davlatlar va tashkilotlar o‘zaro hamkorlik qilishlari, qonuniy bazani mustahkamlashlari hamda ilg‘or texnologiyalarni joriy etishlari lozim. Xalqaro hamkorlik doirasida kiberjinoyatchilikka qarshi kurashish bo‘yicha maxsus qonunlar qabul qilinishi, shuningdek, axborot xavfsizligini ta’minlash bo‘yicha xalqaro standartlar ishlab chiqilishi zarur. Kiberxavfsizlik bo‘yicha global hamkorlik va innovatsion texnologiyalarni joriy etish orqali raqamli dunyoda xavfsizlikni ta’minlash mumkin. Sun’iy intellekt kiberhujumlarni oldindan aniqlash va ularga javob berishda samarali bo‘lsa, blokcheyn texnologiyalari ma’lumotlarning buzilmasligini ta’minlaydi. Shuningdek, foydalanuvchilarning kiberxavfsizlik bo‘yicha xabardorligini oshirish ham muhim ahamiyatga ega. Raqamli dunyoda ishonchli va himoyalangan muhit yaratish uchun davlatlar va tashkilotlar o‘zaro hamkorlik qilishlari, qonuniy bazani mustahkamlashlari hamda ilg‘or texnologiyalarni joriy etishlari lozim.

Xulosa Kibertahdidlar hozirgi kunda global muammo bo‘lib, ular nafaqat alohida shaxslar va tashkilotlarga, balki butun davlatlarning milliy xavfsizligiga ham jiddiy tahdid tug‘dirmoqda. Zamonaviy texnologiyalar rivojlanishi bilan birga, kiberjinoyatchilik usullari ham takomillashib bormoqda. Shu sababli, axborot xavfsizligini ta’minlash nafaqat texnik, balki huquqiy va ijtimoiy chora-tadbirlarni ham o‘z ichiga olgan kompleks yondashuvni talab qiladi.

Ushbu tahdidlarga qarshi samarali kurashish uchun ilg‘or texnologiyalardan foydalanish, xavfsizlik protokollariga qat’iy rioya qilish va foydalanuvchilarning kiberxavfsizlik bo‘yicha xabardorligini oshirish zarur. Sun’iy intellekt, blokcheyn va bulutli xavfsizlik texnologiyalaridan foydalanish axborot tizimlarining himoyasini sezilarli darajada oshirish imkonini beradi. Shuningdek, tashkilotlar va davlat muassasalari kiberhujumlarning oldini olish uchun xavfsizlik strategiyalarini doimiy ravishda takomillashtirib borishlari lozim.

Foydalanuvchilarning xabardorligi kiberxavfsizlikning muhim omillaridan biri hisoblanadi. Amaliy tajribalar shuni ko‘rsatmoqdaki, aksariyat kiberhujumlar inson omiliga bog‘liq bo‘lib, oddiy himoya choralariga rioya qilmaslik sababli sodir bo‘ladi. Shu sababli, muntazam ravishda axborot xavfsizligi bo‘yicha o‘quv dasturlari va treninglar tashkil etish orqali foydalanuvchilarni himoya darajasini oshirish mumkin.

Foydalanilgan adabiyotlar:

1. Гостев В. А. "Кибербезопасность: угрозы и методы защиты" – Москва, 2022.
2. Anderson R. "Security Engineering: A Guide to Building Dependable Distributed Systems" – Wiley, 2020.
3. Юсупов Р.Х., Тошбаев А. "Ахборот хавфсизлиги ва криптографик ҳимоя" – Тошкент, 2021.
4. Schneier B. "Applied Cryptography" – John Wiley & Sons, 2019.
5. Абдуллаев Н. "Кибертаҳдидлар ва уларга қарши кураш чоралари" – Тошкент, 2023.