KOMPYUTER JINOYATLARI VA KIBERXAVFSIZLIK: RAQAMLI JAMIYATDA HUQUQIY, TEXNOLOGIK VA IJTIMOIY JIHATLAR

Ro'ziyeva Anora Muhamadiyor qizi
G'ijduvon tuman 2-son politexnikumi Informatika va AT fani o'qituvchisi
Bukhara, Uzbekistan

Annotatsiya: Mazkur ilmiy maqolada kompyuter jinoyatlarining (kiberjinoyatlar) turlari, ularning global va milliy iqtisodiy, ijtimoiy va huquqiy ta'sirini o'rganish, shuningdek, kiberxavfsizlik tizimlarining samaradorligini oshirish choralarini taklif etishdir. Bu mavzu zamonaviy raqamli iqtisodiyotning rivojlanishi, 5G texnologiyalari, IoT (Internet of Things) va sun'iy intellektning keng tarqalishi kontekstida o'ta dolzarbdir.
Kiber jinoyatchilikka qarshi aholining barcha qatlami orasida huquqiy ong va madaniyatni rivojlantirish, ya'ni fuqarolarga kiber jinoyatchilikning tashqi belgilari va ulardan qanday birlamchi himoyalanish mumkinligi haqida ma'lumotlarni yetkazish orqali imunitet hosil qilish masalalari tahlil qilingan

Abstract: This scientific article examines the relevance and significance of transitioning to a "green economy" for Uzbekistan and its regions in ensuring sustainable development, as well as the scientific and methodological foundations for improving the process of making managerial decisions regarding the attraction of "green investments," efficient resource use, environmental protection, and social justice.
Globally, the "green economy" is based on principles of justice, sustainability, and efficiency. In Uzbekistan, it involves analyzing ecological issues, enhancing competitiveness in this field, reducing resource dependency, and supporting the process through international cooperation and investments. Consequently, practical recommendations have been developed to achieve effective solutions for economic, social, and ecological balance through the "green economy."

Аннотация: В данной научной статье рассматриваются актуальность и значение перехода к «зеленой экономике» для Узбекистана и его регионов в обеспечении устойчивого развития, а также научно-методические основы совершенствования процесса принятия управленческих решений по привлечению «зеленых инвестиций», эффективному использованию ресурсов, охране окружающей среды и обеспечению социальной справедливости.
В глобальном масштабе «зеленая экономика» основывается на принципах справедливости, устойчивости и эффективности. В Узбекистане это предполагает анализ экологических проблем, повышение конкурентоспособности в данной сфере, снижение зависимости от ресурсов, поддержку процесса международным сотрудничеством и инвестициями. В результате разработаны практические рекомендации, направленные на достижение эффективных решений для экономического, социального и экологического баланса через «зеленую экономику».

Kalit so'zlar: Kiber jinoyat, elektron pochta, Internet-auksion, milliy kiberxavfsizlik, internet, texnologiya, 5G texnologiyalari, IoT (Internet of Things) va sun'iy intellekt, operatsion tizimlar, to‘lov protsessor.
Key words: Green economy, sustainable development, green investments, resource efficiency, environmental protection, green energy.
Ключевые слова: Зеленая экономика, устойчивое развитие, зеленые инвестиции, эффективность ресурсов, охрана окружающей среды, зеленая энергетика.

Kirish (Введение/ Introduction). Tadqiqotlar shuni ko'rsatadiki, o'rtacha tashkilotda 800 dan ortiq bulut ilovalari mavjud bo'lib, ularning aksariyati biznesga tayyor emas. Oxirgi ikki yil ichida bu o‘rtacha ko‘rsatkich o‘sishda davom etmoqda. Aksariyat tashkilotlar bu faktni 80–90 foiz deb baholamoqda. Mavjud muhit haqida aniqroq tasavvurga ega bo'lish uchun ko'pchilik tashkilotlarning birinchi qadami Shadow IT havfini baholashdan iborat. Tashkilotda aniqlangan eng xavfli ilovalarga kirish orqali IT ma'murlari kompaniya uchun umumiy xavfni kamaytirishi mumkin. Bu aniqlash uchun qo'shimcha foydalanish tahlilini talab qiladi. Ushbu qo'shimcha tushuncha qatlami bilan IT tashkilotlari xavfni kamaytirish strategiyalarini ishlab chiqishi mumkin, masalan, alohida foydalanuvchilar yoki bo'limlarga muqobil ilovalarni topishga o'rgatish yoki eng xavfli ilovalarga kirishni cheklash siyosatini qo'llash lozim. Topilgan ilovalarning biznesga tayyorligini aniqlash uchun tashkilotlar ushbu ilovalar kompaniyaning xavfsizlik siyosati, muvofiqlik siyosati yoki boshqa korporativ talablarni hisobga olgan holda foydalanishga mos kelishini bilishi kerak. Ushbu tushunchalar yordamida tashkilotlar qaysi ilovalarni sanktsiyalash, qaysilariga ruxsat berish va nazorat qilish va qaysi birini butunlay blokirovka qilish haqida ongli qarorlar qabul qilishlari mumkin.

Hozirda kiber hujumlarning eng samarali usuli sifatida zararli dastur hujumlari hisoblanmoqda. Bunday holda, kompyuter tizimi yoki tarmog‘i kompyuter virusi yoki boshqa zararli dastur bilan zararlangan bo‘ladi. Shundan so‘ng, kiber jinoyatchilar kompyuterdan maxfiy ma’lumotlarni o‘g‘irlash, ma’lumotlarni buzish va boshqa jinoiy harakatlarni amalga oshirish uchun foydalanishlari mumkin.

Ushbu turdagi kiberjinoyatlarning mashhur namunasi 2017-yilning may oyida WannaCry ransomware dasturidan foydalangan holda global kiberhujumdir. Bunday dasturlar kiberjinoyatchilarga garovga olingan ma’lumotlar yoki qurilmalar uchun to‘lov talab qilish imkonini beradi. WannaCry Microsoft Windows operatsion tizimida ishlaydigan kompyuterlardagi zaiflikdan foydalangan. O‘shanda 150 ta mamlakatdagi 230 000 ta kompyuter to‘lov dasturidan zarar ko‘rgan. Kiberjinoyatchilar qurbonlari o‘z fayllariga kirish huquqini yo‘qotdilar va kirish huquqini tiklash uchun bitkoinlarda to‘lov talab qilingan xabarni oldilar.

Tahlil va natijalar (Анализ и результаты. Analysis and results)

Kiberjinoyat deganda kompyuter va Internetdan foydalanib, shaxsning shaxsini o‘g‘irlash, kontrabandani sotish yoki qurbonlarni bezovta qilish yoki zararli dasturlar orqali operatsiyalarni to‘xtatish maqsadida sodir etilgan jinoyat sifatida ta’riflash mumkin.

Axborot xavfsizligi va kiberjinoyat hujumlariga qarshilik mahalliy qattiq disklar va elektron pochta platformalarini shifrlash, virtual xususiy tarmoq (VPN) va shaxsiy, xavfsiz domen nomlari tizimi (DNS) serveridan foydalanish orqali ham yaratilishi mumkin.

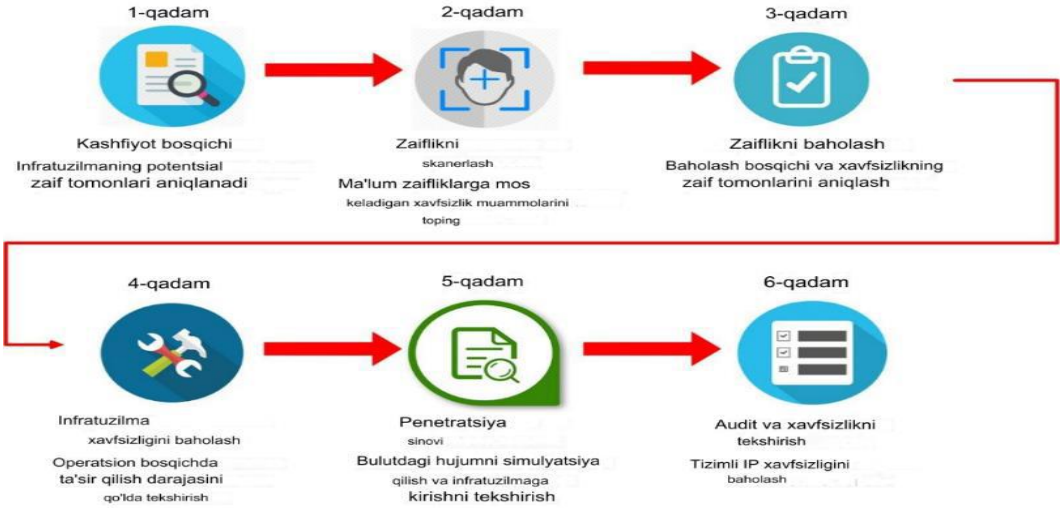
Ma'lumotlarning maxfiyligi va xavfsizligi har doim har qanday tashkilot e'tibor beradigan eng yuqori xavfsizlik choralari bo'lib qoladi. Biz hozirda barcha ma'lumotlar raqamli yoki kiber shaklda saqlanadigan dunyoda yashayapmiz. Ijtimoiy tarmoq saytlari foydalanuvchilar o'zlarini do'stlari va oila a'zolari bilan xavfsiz muloqot qilish uchun joy beradi. Uy foydalanuvchilari uchun kiberjinoyatchilar shaxsiy ma'lumotlarni o'g'irlash uchun ijtimoiy tarmoq saytlarini nishonga olishni davom ettiradilar. Nafaqat ijtimoiy tarmoqlarda, balki bank operatsiyalari paytida ham inson barcha zarur xavfsizlik choralarini ko'rishi kerak.

Quyida kiberxavfsizlikka katta ta'sir ko'rsatayotgan ba'zi texnologiyalar keltirilgan:

Veb-serverlar: Ma'lumot olish yoki zararli kodni tarqatish uchun veb-ilovalarga hujumlar tahdidi saqlanib qolmoqda. Kiberjinoyatchilar o'zlarining zararli kodlarini buzilgan veb-serverlar orqali tarqatadilar. Ammo ko'pchiligi ommaviy axborot vositalarining e'tiborini tortadigan ma'lumotlarni o'g'irlash hujumlari ham katta xavf tug'diradi. Endi biz veb-serverlar va veb-ilovalarni himoya qilishga ko'proq e'tibor qaratishimiz kerak. Veb-serverlar, ayniqsa, ma'lumotlarni o'g'irlash uchun kiber jinoyatchilar uchun eng yaxshi platformadir. Shu sababli, ushbu jinoyatlar qurboni bo'lmaslik uchun har doim xavfsizroq brauzerdan foydalanish kerak, ayniqsa muhim tranzaktsiyalar paytida.

Bulutli hisoblash va uning xizmatlari. Hozirgi kunda barcha kichik, o'rta va yirik kompaniyalar asta-sekin bulutli xizmatlarga o'tmoqda. Boshqacha aytganda, dunyo asta-sekin bulutlar tomon harakatlanmoqda. Ushbu so'nggi tendentsiya kiberxavfsizlikda katta muammo tug'diradi, chunki trafik an'anaviy tekshirish nuqtalarini chetlab o'tishi mumkin. Bundan tashqari, bulutda mavjud ilovalar soni ortib borayotganligi sababli, qimmatli ma'lumotlarning yo'qolishining oldini olish uchun veb-ilovalar va bulut xizmatlari uchun siyosat boshqaruvlari ham rivojlanishi kerak bo'ladi. Bulutli xizmatlar o'z modellarini ishlab chiqsa-da, xavfsizlik bilan bog'liq muammolar ko'p. Bulut ulkan imkoniyatlarni taqdim etishi mumkin, biroq siz doimo bulut etuklashgani sari uning xavfsizligi bilan bog‘liq muammolar ortib borishini hisobga olishingiz kerak

Bulutli texnologiyalarda kiberxavfsizlikni ta’minlash qadamlari



Mobil tarmoqlar: Bugun biz dunyoning istalgan burchagida istalgan odam bilan bog'lanishimiz mumkin. Ammo bu mobil tarmoqlar uchun xavfsizlik juda katta muammo. Hozirgi kunda xavfsizlik devorlari va boshqa xavfsizlik choralari odamlarning planshetlar, telefonlar, shaxsiy kompyuterlar va h.k. kabi qurilmalardan foydalanishi tufayli tobora zaiflashib bormoqda. Ularning barchasi foydalaniladigan ilovalarda mavjud bo'lganlardan tashqari yana qo'shimcha xavfsizlik choralarini talab qiladi. Biz har doim ushbu mobil tarmoqlarning xavfsizlik masalalari haqida o'ylashimiz kerak. Boshqa mobil tarmoqlar ushbu kiberjinoyatlarga juda sezgir, shuning uchun ular bilan xavfsizlik bilan bog'liq muammolar mavjud bo'lsa, juda ehtiyot bo'lish kerak.

Shifrlash - bu xabarlarni (yoki ma'lumotlarni) tinglovchilar yoki xakerlar ularni o'qiy olmasligi uchun kodlash jarayonidir. Shifrlash sxemasida xabar yoki ma'lumot shifrlash algoritmi yordamida shifrlanadi va uni o'qib bo'lmaydigan shifrlangan matnga aylantiradi. Bu odatda shifrlash kaliti yordamida amalga oshiriladi, bu xabar qanday kodlanganligini aniqlaydi. Eng asosiy darajadagi shifrlash ma'lumotlarning maxfiyligi va yaxlitligini himoya qiladi. Ammo shifrlashdan foydalanishning ko'payishi kiberxavfsizlik uchun qo'shimcha muammolarni keltirib chiqaradi. Shifrlash, shuningdek, tarmoqlar (masalan, Internet, elektron tijorat), mobil telefonlar, simsiz mikrofonlar, simsiz interkomlar va boshqalar orqali uzatiladigan ma'lumotlar kabi tranzitdagi ma'lumotlarni himoya qilish uchun ham qo'llaniladi. Shuning uchun kodni shifrlash orqali siz mavjud yoki yo'qligini bilib olishingiz mumkin. ma'lumotlarning sizib chiqishidir.

Antivirus dasturlari - viruslar va qurtlar kabi zararli dasturlarni aniqlaydigan, oldini oladigan va zararsizlantirish yoki o'chirish uchun choralar ko'radigan kompyuter dasturi. Aksariyat antivirus dasturlari avtomatik yangilash xususiyatini o'z ichiga oladi, bu dasturga yangi virus profillarini yuklab olish imkonini beradi, shunda ular yangi viruslar aniqlangandan so'ng darhol tekshiriladi. Antivirus dasturi har bir tizim uchun zarur va asosiy zaruratdir.

Kiberxavfsizlik sifatida kompyuter tizimlari, tarmoqlar, ma’lumotlar va foydalanuvchilarning fizikiy va raqamli xavflardan himoyalanishi tushuniladi. 2022-yilda O‘zbekiston Kiberxavfsizlik Agentligi tashkil etildi, hamda uning asosiy vazifalari

kiberhujumlarni monitoring qilish, davlat tizimlarini himoya qilish va xalqaro hamkorlikni rivojlantirishdan iboratdir.

Shuningdek, Muhammad al-Xorazmiy nomidagi Toshkent Axborot Texnologiyalari Universiteti va “Uzinfocom” kompaniyasi tomonidan kiberxavfsizlik bo‘yicha 2023-yilda 500 dan ortiq mutaxassislar tayyorlandi. 2024-yilda O‘zbekistonda kiberhujumlar soni 30% ga o‘sib, asosan davlat tizimlariga (banklar, davlat xizmatlari) qaratilgan.

O‘zbekistonda 2020-2024 yillarda kiberjinoyat holatlari 3 barobarga ko‘paygan, xususan, phishing va ransomware hujumlari 70% ni tashkil etadi (Ichki ishlar vazirligi, 2024).

Cybersecurity Ventures hisobotlariga ko‘ra, 2025-yilda global kiberjinoyatlar tufayli zarar 10,5 trillion dollarni tashkil etishi kutilmoqda. O‘zbekistonda 2022-yilda kiberjinoyatlar tufayli iqtisodiy zarar 50 million dollar atrofida baholangan (O‘zbekiston Respublikasi Ichki ishlar vazirligi ma’lumotlariga asoslanib), hamda 2023-yilda global miqyosda kiberjinoyat holatlari 85% ga o‘sishni ko‘rsatgan.

2023-yilda O‘zbekistonda bank sektoriga qaratilgan ransomware hujumi natijasida 5 million dollarlik zarar yetkazilgan. Hujum “DarkSide” guruhining ishi sifatida aniqlangan. 2022-yilda “Colonial Pipeline” hujumi (AQSh) ransomware tufayli 4,4 million dollar to‘langan, bu kiberxavfsizlik tizimlarining zaifliklarini ko‘rsatgan.

O‘zbekiston Respublikasi Jinoyat kodeksining 284-286-modadalari bilan bir qatorda, “Kiberxavfsizlik to‘g‘risida”gi 2022-yilgi qonun kiberjinoyatlarning oldini olish uchun asosiy huquqiy asos hisoblanadi. O‘zbekistonda kiberjinoyatlar bo‘yicha sud qarorlarining kamligi (2023-yilda 15 ta holat sudga yuborilgan, lekin faqat 5 tasi jazo bilan yakunlangan) va qonunchilikdagi zaifliklar (masalan, deepfake’lar uchun alohida qoidalar yo‘qligi). Biroq, sun’iy intellekt asosidagi yangi hujumlar uchun qonunchilikning zaif jihatlari (masalan, deepfake’lar bilan bog‘liq qoidalar yo‘qligi) aniqlanadi.

Kiberxavfsizlik tizimlarining asosiy prinsiplar:

Qonuniylik va huquqiy tartib: Kiberxavfsizlik qonunlari bilan muvofiqlik (O‘zbekistonning PQ-4751-qarori, 2021).

Texnologik mustahkamlash Firewall, intrusion detection systems (IDS), sun’iy intellekt asosidagi monitoring tizimlari.

Xalqaro hamkorlik Shanghai Hamkorlik Tashkiloti (SHT), BMT Kiberxavfsizlik bo‘yicha guruhi va Yevropa Ittifoqi bilan hamkorlik.

Xabardorlik Aholi va korxonalar o‘rtasida kiberxavfsizlik madaniyatini rivojlantirish.

Sun’iy intellekt asosidagi kiberhujumlar (AI-driven attacks) kiberxavfsizlik tizimlarini yangi darajadagi sinovlarga duchor qilmoqda. Masalan, 2024-yilda ChatGPT misra’lari orqali yozilgan phishing xatlar 80% samaradorlikka erishgan.

Xulosa (Заключение/ Conclusion). Yuqoridagilardan kelib chiqib, kiberjinoyatlarning keng tarqalishi va xorijiy, ko‘p, o‘zgaruvchan yoki noma’lum yurisdiksiyalarda joylashgan bo‘lishi mumkin bo‘lgan elektron dalillarni olishning murakkablashishi bilan huquqni muhofaza qilish organlarining vakolatlari hududiy

chegaralar bilan cheklanadi. Natijada, davlatlarning vakolatli organlariga ma’lum bo‘lgan kiberjinoyatlarning faqat kichik bir qismi bilan kurashish mumkin bo‘lib qoladi. Bunga qarshi turish uchun xalqaro shartnomalarga qo‘shilish, hukumatlararo o‘zaro yordamning yo‘lga qo‘yilishi kiberjinoyatlarga qarshi samarali kurashishda muhim ro‘l o‘ynaydi.

O‘zbekistonda kiberxavfsizlik sohasining yaxshilanishi uchun quyidagi takliflarimni berib o`tmoqchiman.

1.**Mavjud qonunchilikdagi bo`shliqlarni aniqlash va yangilash**: Kiberxavfsizlik bo`yicha qonunchilikni takomillashtirishning birinchi bosqichi bo`shliq va kamchiliklarni aniqlash uchun amaldagi qonun va me`yoriy hujjatlarni qayta ko`rib chiqishdan iborat. Bo‘shliqlar aniqlanishi kerak.

2. **Ogohlikka chaqirish va ta'lim berish orqali kiberxafvsizlikni oshirish**: Kiberxavfsizlik nafaqat hukumatning, balki shaxslar va tashkilotlarning ham amalga oshirishi kerak bo`lgan vazifalaridan biri hisoblanadi. Shu bois keng jamoatchilik, korxonalar va davlat amaldorlari o`rtasida kiberxavfsizlik bo`yicha xabardorlikni oshirish va ta`limni kuchaytirish zarur.

3. **Milliy kiberxavfsizlik strategiyasini yaratish**: Kiberxavfsizlikning keng qamrovli milliy strategiyasi barcha manfaatdor tomonlarning kibert ahdidlarga qarshi birgalikda ishlashi uchun ishlab chiqilishi kerak.

4. **Kiberxavfsizlik agentligini tashkil etish**: Milliy kiberxavfsizlik strategiyasini muvofiqlashtirish va amalga oshirish uchun kiberxavfsizlik uchun mas'ul bo‘lgan markazlashtirilgan agentlik tashkil etilishi kerak. Ushbu agentlik kibertahdidlarni samarali hal qilish uchun yetarli darajada xodimlar va resurslar bilan ta'minlanishi kerak.

5. **Axborot almashishni yaxshilash**: Samarali kiberxavfsizlik uchun turli manfaatdor tomonlar o‘rtasida ma’lumot almashish muhim ahamiyatga ega. Shu sababli, davlat idoralari, xususiy kompaniyalar va boshqa manfaatdor tomonlar o‘rtasida tahdidlar haqidagi razvedka va kiberxavfsizlik ma’lumotlarini almashishni rag‘batlantirish va himoya qilish uchun qonunlar ishlab chiqilishi kerak, hamda kiberxavfsizlik uchun kvant shifrlash texnologiyalarini joriy etish.

6. **Kiberxavfsizlik hodisalariga javob rejasini ishlab chiqish**: Hodisalarga javob berish rejasi kiber hodisalarga javob berish uchun asos yaratish uchun ishlab chiqilishi kerak. Reja hodisalar haqida xabar berish, hodisalarni tekshirish va hodisalardan tiklanish tartiblarini o‘z ichiga olishi kerak.

7. **Davlat-xususiy sheriklikni rag‘batlantirish**: Davlat-xususiy sheriklik kiberxavfsizlikni yaxshilashda samarali bo`lishi mumkin. Hukumat kiberxavfsizlik siyosati va tashabbuslarini ishlab chiqish va amalga oshirish uchun xususiy sektor bilan hamkorlik qilishi kerak, shuningdek Aholi o‘rtasida kiberxavfsizlik bo‘yicha xabardorlikni oshirish uchun milliy kampaniyalar (masalan, “Kiberxavfsiz O‘zbekiston” loyihasi) joriy etish.

FOYDALANILGAN ADABIYOTLAR (ЛИТЕРАТУРЫ/ REFERENCES):

1. https://tashviqot.uz/index.php/2022/10/04/2506/
2. https://library-tsul.uz/viktimologiya-rustambayev-m-x-niyozova-s-s-2021

3. The NIST Definition of Cloud Computing [Electronic resource] // URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.
4. Cybercrime [Electronic resource] // https://earthweb.com/cybercrime-statistics/
5. https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime
6. Web Server and its Types of Attacks [Electronic resource] // URL: https://www.greycampus.com/opencampus/ethical-hacking/web-server-and-its-types-of-attacks.
7. https://zamon.uz/detail/ozbekistonda-songgi-3-yilda-kiberjinoyatlar-keskin-oshgan-ozbekiston
8. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
9. Convention on Cybercrime, Article https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/