KIBERXAVFSIZLIK SOHASIDAGI SO‘NGGI TEXNOLOGIYALAR VA YANGILIKLAR

Siddiqov Murodali Yo‘ldoshali o‘g‘li
Isaxonov Xushnidbek Murodiljon o‘g‘li
Sotvoldiyev Asadbek Abrorjon o‘g‘li
Muhammad al-Xorazmiy nomidagi TATU Farg‘ona Filiali talabalari

Annotatsiya: *Ushbu maqolada biz kiberxavsizlik sohasidagi so‘nggi yangiliklar bilishimiz mumkin. Shuningdek bu texnologiyalarni qayerdan topish, ko‘rish to‘g‘risidagi ma’lumotlarni bilib olamiz.*

Kalit so‘zlar: *Sun‘iy intellekt, Endi-to-End Maxfiylik, Blockchain texnologiyasi, biometrik identifikatsiya, Zero Trust xavfsizlik modeli*

Bugungi kunda texnologiyalar tez sur’atlar bilan rivojlanib, insoniyat hayotida buyuk o‘zgarishlar sodir bo‘lishiga va yanada taraqqiy etishiga sabab bo‘lmoqda. Biroq mazkur sharoitda nafaqat texnologiyalar rivojlanmoqda, balki COVID-19 epidemiyasi tufayli dunyoda yana ko‘p narsa o‘zgardi, ta’bir joiz bo‘lsa odamlarning hayot tarzi va fikrlashi ham anchaginia o‘zgardi. Xususan, IT mutaxassislari ertaga kontaktsiz dunyoda ularning roli o‘zgarmasligini anglashdi. Shu boisdan, 2022-23-yillarda IT mutaxassislari doimiy ravishda o‘z ustilarida ishlab, izlanib ilm o‘rganishlari, bilim yo‘nalishlarini o‘zgartirishlari va qayta o‘rganishlari talab etiladi (agar xohlamasalar ham, zarurat tufayli).

Sun’iy intellekt 2022-yilda tabiiy tillarni qayta ishlash va mashinani o‘rganishni rivojlantirish bilan yanada kengayishi kutilmoqda. Sun’iy intellekt bizni yaxshiroq tushunishi va ushbu texnologiya yordamida murakkabroq vazifalarni bajarishi mumkin. Taxminlarga ko‘ra, 5G kelajakda bizning yashash va ishlash tarzimizda inqilob yasaydi.

2023-yilda kiberxavfsizlik sohasidagi texnologiyalarda ko'proq o'zgarishlar bo‘lib, so‘nggi yillarda ham ma’lumot xavfsizligini oshirish uchun yangi

yondashuvlar va texnologiyalar ishlab chiqilyapti. Quyidagi so‘nggi kiberxavfsizlik texnologiyalari bir qancha yo‘nalishlarda ishlatiladi:

1. Sun’iy Intellekt (SI) va Masofaviy O‘qitish: Sun’iy intellekt (SI) va masofaviy o‘qitish texnologiyalari, xakerlarning eng so‘nggi usullarini aniqlash va ularni oldini olishda yordam beradi. AQShning kiberxavfsizlik sohasidagi kompaniyalari, SI ni mahalliy va global xavfsizlik tizimlarini kuchaytirish uchun qo‘llaydi.

2. Endi-to-End Maxfiylik (E2EE): Bu texnologiya, ma’lumotlar o‘rnatilgan joydan olish va ularni o‘zi o‘rtasida maxfiy ravishda uzatish orqali maxfiylikni ta’minlash uchun ishlatiladi. E2EE, ma’lumotlar tashqi tomondan kirgandan keyin ham maxfiy bo‘lishini ta’minlaydi.

3. Blockchain Teknologiyasi: Blokchain, transaktsiyalarni qayd etish, ularni tasdiqlash va shifrlashda qo‘llaniladi. Maxfiylik va amalni tasdiqlashda blokchain texnologiyasi ishlatilishi, xavfsizlikni oshiradi va ma'lumotlar o‘zgarishsizlikni ta’minlaydi.

4. Biometrik Identifikatsiya: Biometrik identifikatsiya usullari (qo‘llab-quvvat, odam yuzi, tom o‘shaq, iris, va boshqa biometrik ma’lumotlar) kiberxavfsizlik sohasida o‘z o‘rnini olishda o‘zgartirilgan. Ushbu identifikatsiya usullari maxfiylikni oshirish uchun qo‘llaniladi.

5. Internet of Things (IoT) Xavfsizligi: Bir qancha qurilmalarning (smart qurilmalar, smart uy, smart mashinalar, va h.k.) ulanishining o‘sishi bilan, IoT xavfsizligi katta muammolar yaratdi. So‘nggi texnologiyalar, IoT qurilmalari uchun maxfiylikni ta’minlash va ularni xakerlardan himoya qilish uchun ishlab chiqilyapti.

6. Xavfsizlik Siyosati va Monitoring (SSM): Kiberxavfsizlik siyosati va monitoring texnologiyalari, tarmoqni kuzatish, xakerlarning faoliyatini aniqlash va ularga qarshi kurashish uchun qo‘llaniladi.

7. Zero Trust xavfsizlik modeli: Bu model asosan barcha tarmoq elementlariga ishonch qilishni rad etadi va har bir foydalanuvchi, qurilma yoki tizimga kirish uchun tasdiqlashni talab qiladi. Zero Trust, tarmoqni maxfiy va xavfsiz qilish uchun tuyuladi.

8. Kiberxavfsizlik xizmatlari: So‘nggi yillarda, kiberxavfsizlik xizmatlarining ommaviy doirada kengayishini ko‘rib chiqmoqda. Tadbirkorlar, kiberxavfsizlik sohasida xizmat ko‘rsatuvchi kompaniyalardan xavfsizlik xizmatlari sotib olishadi.

Bu texnologiyalar kiberxavfsizlik sohasidagi so‘nggi yangiliklarning faqat bir qismini tashkil etadi. Kiberxavfsizlik sohasidagi yangi yondashuvlar va texnologiyalar har kuni paydo bo'lishi mumkin.

Kiberxavfsizlik bizning davrimizda, ayniqsa sodir bo‘layotgan barcha texnologik yutuqlar bilan chambarchas bog‘langan. O’z resurslarini ularni xohlaydigan boshqa mamlakatlardan himoya qilish uchun hech qanday armiyasi y‘oq mamlakatni tasavvur qiling. Mamlakat zaif bo‘lishi shubhasiz, to‘g‘rimi? Siz shunday mamlakatda yashashni xohlarmidingiz?

Siz hozir deyarli har kuni o‘qish va ish uchun foydalanayotgan texnologiya va internet bilan ham xuddi shunday; kiberxavfsizlik bo‘lmasa, sizning shaxsiy ma’lumotlaringiz, joylashuvingiz, fotosuratlaringiz, kamerangiz va boshqa ko‘p narsalaringiz himoyalanmagan bo‘lardi va natijada, bu sizning shaxsiy hayotingiz haqidagi muhim ma’lumotlarni jinoyatchilar uchun tayyor o‘ljaga aylantiradi. Agar jinoyatchilar bunday ma’lumotlarga kirish imkoniga ega bo‘lsa, ular sizning kredit kartalaringizdan foydalanishi, pulingizni o’g’irlashi va hatto shaxsni o‘g‘irlashi mumkin.

Yana bir misol, agar sizda kompyuterlar va ma’lumotlarga tayanadigan shaxsiy biznesingiz bor va siz ushbu kompaniyani qurish uchun juda ko‘p mehnat qildingiz. Ammo kiberxavfsizlik bo‘lmasa, kompaniyangiz biznesdan chiqib ketishi va bir kechada barcha pul, ma’lumotlar va obro‘sini yo‘qotishi mumkin.

Yuqorida kiberxavfsizlik nima uchun muhim ekanligiga ikkita misol keltirdik. Ammo bugungi virtual hayotimizda bunga juda ko‘plab misollar keltirishimiz mumkin. Umuman olganda, biz kiberxavfsizlikni i**nternetning harbiy qismi** deb o‘ylashimiz mumkin.

Kiberxavfsizlikdagi dolzarb mavzularda xodimlarning kiberjinoyatlarning oldini olishdagi ahamiyati ham qayd etilgan. Texnologiyadagi yutuqlarga qaramay,

inson xatolari muvaffaqiyatli kiberhujumlarning eng muhim omillaridan biri bo‘lib qolmoqda. Kiberjinoyatchilar ko‘pincha xodimlarning o‘rnatilgan kiberxavfsizlik protokollaridan xabardor emasligi yoki ularga rioya qilmasligidan foydalanadilar. Eng keng tarqalgan xato - bu kiber jinoyatchilar tomonidan osonlik bilan foydalaniladigan zaif parol sozlamalari.

Tashkilotlar xodimlarni potentsial tahdidlarni tan olish va ularni amalga oshirishga o‘rgatish uchun kuchli kiberxavfsizlik bo‘yicha o‘quv dasturlariga sarmoya kiritishlari kerak. Kuchli parol amaliyotlari ommaviy qurilmalardan foydalanish va dasturiy ta’minot va qurilmalarni yangilab turish muhimligini tushunish. Tashkilotlarda kiberxavfsizlik madaniyatini rag‘batlantirish inson xatolaridan kelib chiqadigan xavflarni sezilarli darajada kamaytirishi mumkin.

Asrimizning global muammolari qatoriga yangidan-yangi turlari bilan tilga olinayotgan kiberjinoyatchilik kirib kelganiga ham ancha bo'ldi. Uning bizga ma’lum bo‘lgan virusli dasturlarni tarqatish, parollarni buzib kirish, kredit karta va boshqa bank rekvizitlaridagi mablag‘larni o‘zlashtirish talon-toroj qilish, shuningdek, internet orqali qonunga zid axborotlar, xususan, bo‘hton, ma‘naviy buzuq ma’lumotlarni tarqatish bilan bashariyat hayotiga katta xavf solayotganidan ko‘z yuma olmaymiz.

«Kiberjinoyatchilik» tushunchasi axborot-kommunikatsiya texnologiyalari vositalaridan foydalangan holda, virtual tarmoqda dahshat solish, virus va boshqa zararli dasturlar, qonunga zid axborotlar tayyorlash va tarqatish, elektron xatlarni ommaviy tarqatish (spam), xakerlik hujumi, veb-saytlarga noqonuniy kirish, firibgarlik, ma’lumotlar butunligi va mualliflik huquqini buzish, kredit kartochkalari raqami hamda bank rekvizitlarini o‘g‘irlash (fishing va farming) va boshqa turli huquqbuzarliklar bilan izohlanadi.

Shu o‘rinda kiberterrorizm va uning jamiyat hayotiga solayotgan xavfining ko‘lami ham oshib borayotganini ta’kidlash joiz. Kiberterroristik harakat (kiberhujum) - kompyuterlar va axborot kommunikatsiya vositalari yordamida amalga oshirilgan, odamlarning hayoti va sog‘lig‘iga bevosita xavf tug‘diradigan yoki potentsial xavf tug‘dirishi mumkin bo‘lgan, moddiy ob’ektlarga katta zarar

etkazishi yoki shunga olib kelishi mumkin bo‘lgan, ijtimoiy xavfli oqibatlarning boshlanishi yoki maqsadi bo‘lgan siyosiy sababdir. Zamonaviy terrorchilar uchun kibermakondan foydalanishning jozibadorligi kiberhujumni amalga oshirish katta moliyaviy xarajatlarni talab qilmasligi bilan bog‘liq.

Ekspertlarning xulosasiga ko‘ra, bu rivojlanayotgan davlatlarning taraqqiyotiga ko‘maklashish, umuminsoniy demokratik tamoyillarni qaror toptirish niqobi ostida fuqarolar ongiga ta’sir o‘tkazish, ularni turli yo‘llar bilan o‘z maqsadlari sari bo‘ysundirish orqali amalga oshirilmoqda.

Afsuski, bu jarayonda kiberhujumlarni uyushtirish, bu yo‘lda internet global tarmog‘ining mislsiz imkoniyatlaridan foydalanishga urinishlar tobora avj olmoqda.

Internetda mavjud ijtimoiy tarmoqlar, ularning ishlab chiqaruvchilari va homiylarining suveren davlat ichki ishlariga «aralashishlari» qanday rol o‘ynashi oxirigacha o‘rganilmaganligi bois ba’zan bunday «aralashuv» mazkur davlatga qarshi ekanligi hali hanuz e’tirof etilgani yo’q.

Ijtimoiy tarmoqlar egalari ushbu tarmoqlar sahifalarida davlat tuzumini ag‘darishga da’vat qilingani uchun javobgarlikka tortilishining xalqaro miqyosdagi huquqiy asoslari yaratilmagan. Vaholanki, har bir qilingan jinoiy xatti-harakat yoki harakatsizlik mazmun-mohiyatiga ko‘ra, albatta, javobsiz va jazosiz qolmasligi kerak.

Internet saytlari to‘satdan paydo bo‘lib, ko‘pincha formatini, so‘ngra manzilini o‘zgartiradi. Shu bois ayrim ekspertlar internetning butkul ochiqligi kabi dastlabki kontseptsiyalardan voz kechib, uning yangi tizimiga o‘tishni taklif etmoqda.

Yangi modelning asosiy mohiyati tarmoqdan foydalanuvchilarning anonimligidan voz kechishdir. Bu tarmoqning jinoiy tajovuzlardan yanada ko‘proq himoyalangan bo'lishini ta’minlashga imkon berdi.

Misol tariqasida, yopiq tarmoq tizimiga o‘tgan Xitoy davlatini va bunday jarayonga tayyorgarlik ko‘rayotgan Rossiya davlatini keltirishimiz mumkin.

Jahon hamjamiyatiga integratsiyalashayotgan mamlakatimizda axborot kommunikatsiya texnologiyalari, axborot tizimlari va zamonaviy kompyuter texnologiyalaridan samarali foydalanish bo‘yicha izchil davlat siyosati olib

borilmoqda.

Bugungi kunda mamlakatimizda joriy etilayotgan zamonaviy raqamli texnologiyalar, fuqarolarimizga qator qulayliklar va imkoniyatlar eshigini ochmoqda.

Mazkur jarayon bilan bir qatorda, yaratilayotgan raqamli texnologiyalar va axborot tizimlarining xavfsizligini ta’minlash muammosi ham mavjud, albatta. Bu eng dolzarb masalalardan biri - kiberxavfsizlikni ta’minlash, sodir etilishi mumkin bo‘lgan kiberjinoyatlarning oldini olish va unga qarshi kurashish masalasi hisoblanadi.

Kundan-kunga takomillashib ketayotgan kiberjinoyatchilikka qarshi kiberxavfsizlikni ta’minlashda quyidagi asosiy talablarni bajarish orqali ulardan himoyalanish, ya’ni kiberxavfsizlikni ta’minlashimiz mumkin:

- xodimlarga axborot xavfsizligi asoslarini o‘rgatish;
- foydalanayotgan dasturiy mahsulotlarning zaifliklarini doimiy sinovdan o‘tkazish;
- ishonchli antivirus dasturidan foydalanish;
- litsenziyalangan rasmiy dasturlardan foydalanish;
- axborot tizimlarini himoyalashda ko‘p faktorli autentifikatsiyadan foydalanish;
- parollardan foydalanishda kuchli parolni saqlash siyosatiga rioya qilish;
- muntazam ravishda kompyuter qattiq disklaridagi ma’lumotlarni shifrlash.

Shu o‘rinda, mamlakatimizda kiberjinoyatlarning oldini olish va unga qarshi kurashni olib boruvchi vakolatli davlat idoralariga ham muayyan vazifalar yuklanishini alohida ta’kidlash lozim.

Xususan, ular kiberjinoyatchilikka qarshi kurash faoliyatida O‘zbekiston Respublikasi va uning xalqini axborot texnologiyalari va kommunikatsiyalari orqali

amalga oshirilayotgan yoki bunga imkon berayotgan shaxs, jamiyat va davlat xavfsizligini va ularning manfaatlari tashqi hamda ichki kibertahdidlardan himoya qilinishini ta’minlash, mazkur sohada qonuniylik va qonun ustuvorligini mustahkamlash, kiberjinoyatlar va kiberhuquqbuzarliklarning oldini olish, ularni aniqlash va barham berish kabi vazifalarni amalga oshirishi darkor.

Shuningdek, kiberjinoyatlar va kiberhuquqbuzarliklarni tergov qilish va ularni aniqlash, bartaraf etish hamda oldini olish bo‘yicha zarur qarorlar qabul qilish, kiberjinoyatchilikka qarshi kurashish bo‘yicha normativ-huquqiy hujjatlar loyihalarini ishlab chiqishda ishtirok etish, kiberterrorizm, kiberekstremizm, uyushgan jinoyatchilikka qarshi kurashish, davlat organlari manfaatlariga hamda kiberxavfsizligiga tahdid soluvchi kiberhatarlarni aniqlash va ularga qarshi kurashish, kiberjinoyatlar bo'yicha tergovga qadar tekshiruv va dastlabki tergovni o‘tkazish, tezkor-qidiruv faoliyatini amalga oshirish, fuqarolarning huquq va erkinliklariga tahdid soluvchi kiberjinoyatlarning sodir etilishiga imkon yaratuvchi sabablar hamda shart-sharoitlarni aniqlash va bartaraf etish kabi muhim vazifalarni bajarishlari lozim.

FOYDALANILGAN ADABIYOTLAR

1. SARVINOZ, T. (2023). DESIGN OF THE PREPARATION PROCESS SYSTEM FOR EVALUATION SYSTEMS IN SCHOOLS. International Multidisciplinary Journal for Research & Development, 10(11).

2. Toxirova, S. (2023, November). Python dasturida lug’atlar bilan ishlash. In Conference on Digital Innovation:" Modern Problems and Solutions".

3. Toxirova, S. (2023). MA'LUMOTLAR TUZILMASI VA ALGORITMLAR TUSHUNCHASI. Engineering problems and innovations.

4. Mahmudova, M., & Toxirova, S. (2023, October). MULTISERVISLI TARMOQ XAVFSIZLIGIDA NEYRON TARMOQLARINI O ‘RNI. In Conference on Digital Innovation:" Modern Problems and Solutions".

5. Tojiboev, I., Rayimjonova, O. S., Iskandarov, U. U., Makhammadjonov, A. G., & Tokhirova, S. G. (2022). ANALYSIS OF THE FLOW

OF INFORMATION OF THE PHYSICAL LEVEL OF INTERNET SERVICES IN MULTISERVICE NETWORKS OF TELECOMMUNICATIONS. Мировая наука, (3 (60)), 26-29.

6. TOJIBOEV, I., RAYIMJONOVA, O., ISKANDAROV, U., MAKHAMMADJONOV, A., & TOKHIROVA, S. МИРОВАЯ НАУКА. МИРОВАЯ НАУКА Учредители: ООО" Институт управления и социально-экономического развития", (3), 26-29.

7. Muhammadjonov, A., & Toxirova, S. (2023). YARIMO ‘TKAZGICHLARNING TURLARI. Ichki va tashqi yarimo ‘tkazgichlar. Research and implementation.

8. Обухов, В. А. Тохирова Сарвиноз Гайратжон кизи, & Исахонов Хушнидбек Муродилжон угли.(2023). ПРОГРАММЫ ДЛЯ РАСПОЗНАВАНИЯ ТЕКСТА. Ta’lim Innovatsiyasi Va Integratsiyasi, 7 (1), 52–57. ПРОГРАММЫ ДЛЯ РАСПОЗНАВАНИЯ ТЕКСТА. Ta’lim Innovatsiyasi Va Integratsiyasi, 7(1), 52-57.

9. Обухов, В. А. Тохирова Сарвиноз Гайратжон кизи, & Сотволдиев Асадбек Аброржон угли. (2023). МЕТОДЫ РАСПОЗНАВАНИЯ И ЭТАПЫ ОБРАБОТКИ ИЗОБРАЖЕНИЯ. Ta’lim Innovatsiyasi Va Integratsiyasi, 7 (1), 40–44.

10. Muhammadjonov, A., & TURLARI, T. S. Y. T. ICHKI VA TASHQI YARIMO ‘TKAZGICHLAR. Research and implementation.–2023.

11. Porubay, O., & Khasanova, M. (2023). Model of innovative progress in the power sector. Engineering problems and innovations.

12. Порубай О. В., Хасанова М. У. К. Обзор процесса принятия решений в условиях риска и неопределенности //Universum: технические науки. – 2022. – №. 7-1 (100). – С. 17-19.

13. Porubay, O., & Khasanova, M. (2023). Formation of new technologies for innovation management in the modern competitive environment. Engineering problems and innovations.

14. Porubay, O., & Khasanova, M. (2023). Model of innovative progress in the power sector. Engineering problems and innovations.

15. Porubay O., Siddikov I., Madina K. Algorithm for optimizing the mode of electric power systems by active power //2022 International Conference on Information Science and Communications Technologies (ICISCT). – IEEE, 2022. – С. 1-4.

16. Porubay O., Khasanova M. Machine learning as a tool of modern pedagogical technologies //Science and innovation. – 2022. – Т. 1. – №. B3. – С. 840-843.

17. Порубай О. В., Хасанова М. У. Концепция безопасности в теории и практике принятия решений //Просвещение и познание. – 2022. – №. 7 (14). – С. 11-20.

18. Порубай О. В., Хасанова М. СИСТЕМЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ С ИНТЕЛЛЕКТУАЛЬНЫМИ МЕХАНИЗМАМИ ПОИСКА ДЛЯ ОПЕРАТИВНОДИСПЕТЧЕРСКОГО УПРАВЛЕНИЯ В ЭЛЕКТРОЭНЕРГЕТИКЕ. – 2021.

19. Порубай, О. В., & Хасанова, М. (2022). ВНЕДРЕНИЕ ИННОВАЦИОННЫХ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ В ВЫСШИЕ УЧЕБНЫЕ ЗАВЕДЕНИЯ. In Статистический анализ социально-экономического развития субъектов Российской Федерации (pp. 225-228).

20. Tokhirova Sarvinoz Gayratjon Kizi, Sotvoldiyev Asadbek Abrorjanovich, & Isakhanov Khushnidbek Murodiljanovich. (2023). DATA STRUCTURE AND ALGORITHM ANALYSIS PROCESS. Best Journal of Innovation in Science, Research and Development, 2(11), 722–724. Retrieved from https://www.bjisrd.com/index.php/bjisrd/article/view/943

21. Tokhirova Sarvinoz Gayratjon Kizi. (2023). Ethernet and Fast Ethernet network architecture. Best Journal of Innovation in Science, Research and Development, 175–179. Retrieved from https://www.bjisrd.com/index.php/bjisrd/article/view/985

22. MILLIY IQTISODIYOT VA UNING MAKROIQTISODIY KO‘RSATKICHLARI. (2023). Journal of Technical Research and Development,1(2),402-409. https://jtrd.mcdir.me/index.php/jtrd/article/view/81

23. МИКРОПРОЦЕССОРНЫЕ СИСТЕМЫ И ИХ ПРОИСХОЖДЕНИЕ. (2023). Journal of Technical Research and Development, 1(2), 32-37.https://jtrd.mcdir.me/index.php/jtrd/article/view/80

24. МИКРОПРОЦЕССОРНЫЕ СИСТЕМЫ И ИХ ПРОИСХОЖДЕНИЕ. (2023). Journal of Technical Research and Development, 1(2), 32-37. https://jtrd.mcdir.me/index.php/jtrd/article/view/80