NIGMATOV Xikmatilla
O‘zbekiston xalqaro islomshunoslik akademiyasi Zamonaviy axborot-kommunikatsiya texnologiyalari kafedrasi professori

IZOMOVA Oyista Ilxom qizi
O‘zbekiston xalqaro islomshunoslik akademiyasi Zamonaviy axborot-kommunikatsiya texnologiyalari kafedrasi laboranti

KIBERHUJUMLARDAN HIMOYALASHDA SUN’IY INTELLEKTDAN FOYDALANISH VA TARMOQ XAVFSIZLIGINI TA’MINLASH USULLARI

МЕТОДЫ ОБЕСПЕЧЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТИ И ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ЗАЩИТЫ ОТ КИБЕРАТАК

METHODS OF ENSURING NETWORK SECURITY AND USING ARTIFICIAL INTELLIGENCE FOR PROTECTION AGAINST CYBER ATTACKS

Annotatsiya. *Raqamlashtirish jarayonida barcha korxona, tashkilot va muassasalarda saqlanayotgan, uzatilayotgan va qabul qilinayotgan ma’lumotlarni kiberhujumlardan himoyalanish uchun sun’iy intellektni qo‘llash va tarmoq havfsizligini ta’minlash uchun bugungi kunda eng zarur bo‘lgan usullar keltirilgan. Kompyuter tarmog‘ida bo‘ladigan tahdidlarni operativ ravishda aniqlashda va kiberhavfsizlik sohasida ilg‘or texnologiyalarni joriy etishda sun’iy intellektga asoslangan dasturiy vositalarni ishlab chiqish hamda tarmoq havfsizligini ta’minlashda tashkiliy, texnikaviy, dasturiy va kriptografik vositalarni qo‘llash usullari taklif etilgan.*

Kalit so‘zlar: *kiberhavfsizlik, kiberhujum, sun’iy intellekt, tahdidlar, tarmoq havfsizligi, nazariy tadqiqotlar.*

Аннотация. *В процессе цифровизации приведены наиболее необходимые на сегодняшний день методы применения искусственного интеллекта для защиты информации, хранящейся, передаваемой и принимаемой всеми предприятиями, организациями и учреждениями от кибератак, а также для обеспечения сетевой безопасности. Предложены способы разработки программных средств на основе искусственного интеллекта для оперативного выявления угроз в компьютерных сетях и внедрения передовых технологий в сфере кибербезопасности, а также применения организационных, технических, программных и криптографических средств для обеспечения сетевой безопасности.*

Ключевые слова: *кибербезопасность, кибератака, искусственный интеллект, угрозы, сетевая безопасность, теоретические исследования.*

Annotation. *In the process of digitalization, the most essential methods for applying artificial intelligence to protect data stored, transmitted, and received by all enterprises, organizations, and institutions from cyberattacks and to ensure network security are presented. The proposed approaches include the development of AI-based software tools for the rapid detection of threats in computer networks and the implementation of advanced technologies in the field of cybersecurity, as well as the use of organizational, technical, software, and cryptographic measures to ensure network protection.*

Keywords: *cybersecurity, cyberattack, artificial intelligence, threats, network security, theoretical research.*

KIRISH

Bugungi kunda O‘zbekiston xalqaro islom akademiasida ta’lim olayotgan talabalar va magistrlarga bo‘lgan talab borgan sari oshib bormoqda. Akademiyaning saytlariga va har xil tashkil etilgan elektron platformalariga kirayotganlarning sonining oshib borishi natijasida saqlanayotgan ma’lumotlarning butunligini ta’minlash, o‘chirilmaganligini, yoki o‘zgartirilib qo‘yilmaganligini ta’minlash masalalari kelib chiqmoqda [1]. Barcha muasassalarning yoki oliy yurtlarining har qanday davlat korhonalari, yoki tijorat kompaniyalarning o‘ziga yarasha har xil turdagi ma’lumotlari mavjud. Bunday turlarga maxfiy, konfidentsiyal yoki ochiq ma’lumotlar bo‘lishi mumkin.

Barcha tashkilotlar respublikamizda qabul qilingan raqamlashtirish jarayoni asosida barcha ichki va tashqi faoliyat bilan kompyuterlar bilan telekommunikatsiya tarmoqlari orqali ma’lumotlar ayirboshlashadi.

ISSN 2181-9572

Hammaga ma’lum, bugungi kunda dunyo bo‘yicha rivojlanayotgan davlatlarda zamonaviy axborot kommunikatsiya texnologiyalari asosida faoliyat olib borilmoqda. Raqamlashtirish jarayonlari iqtisodiyotning barcha jabxalarida qo‘llanishi natijasida katta moliyaviy yutuqlarga erishilmoqda.

Bugungi kunda har bir axborot o‘z qiymatiga ega bo‘lib, ularning bahosi olinayotgan, saqsalanayotgan, uzatilayotgan yoki qabul qilinayotgan axborotlarning butunligiga, o‘zgartirilmaganligiga, xatosiz berilganligiga va talab qilingan vaqtda yetkazib berilganligiga bog‘liq bo‘lib qolayapti. Bu shartlarning bajarilmaganligi axborotlardan foydalanuvchilarga juda katta ma’naviy, siyosiy, axloqiy va eng asosiysi iqtisodiy ya’niy moliyaviy zarar keltirishi barchaga ma’lum bo‘lib qoldi [2].

Albatta xozirgi raqamlashtirish davrda barcha korxonalar, tashkilotlar, vazirliklar, muassasalar, aktsiyadorlik kompaniyalar, assosatsiyalar, mas’uliyati cheklangan jamiyat va firmalar o‘zlarining faoliyati yuzasidan barcha ma’lumotlarni kompyuterlarga joylashtirib, ulardan kerak paytda foydalanib kelinmoqda, lekin ushbu ma’lumotlarni himoyalash masalalari ko‘p joylarda hisobga olinmay qolayapti /1,2/.

ASOSIY QISM

Axborot xavfsizligi tobora ko‘proq joriy etilayotgan va foydalaniladigan kompyuter tizimlarini hisobga olgan holda zamonaviy dunyoda muhim o‘rin tutadi. Har bir inson, xoh shaxs, xoh kompaniya bo‘lsin, o‘z ma’lumotlarini o‘g‘irlash, o‘chirish yoki o‘zgartirish xavfini kamaytirishga xarakat qiladi. Shu jumladan, avtomatlashtirilgan tizimda kiberxavfsizlik muhim rol o‘ynaydi.

Bugun dunyo bo‘ylab axborot xavfsizligi bilan birgalikda “kiberxavfsizlik” tushunchasi keng qo‘llanilib, uning ahamiyati borgan sari to‘liqroq e’tirof etilmoqda. Kiberxavfsizlik – bu kibermakonning barcha tashkil etuvchilari (ya’ni texnik qurilmalar va foydalanuvchilar)ni har qanday tahdidlar va kutilmagan ta’sirlardan himoyalanganlik holati hisoblanadi. Kiberhujumlar soni tez va barqaror o‘sishda davom etmoqda, hujumlarning o‘zi tobora takomillashib bormoqda va bunday kiberhujumlarning maqsadi odatda maxfiy ma’lumotlarga kirish, uni o‘zgartirish yoki yo‘q qilish, foydalanuvchilardan pul undirish, biznes va moliyaviy markazlar, davlat tashkilotlari faoliyati uchun mas’ul bo‘lgan hisoblash tizimlarining ishlashini buzishga qaratilgan bo‘lib qolmoqda.

Kiberxavfsizlik sohasida ilg‘or texnologiyalarni joriy etish hujumlarni batafsil aniqlash va ularni kiberxavfsizlik bo‘yicha mutaxassislarga qaraganda tezroq hal qilish uchun sun’iy intellektdan foydalanishga to‘g‘ri kelmoqda /3/. Bundan tashqari, kiberhujumlarning turlarini aniqlash, ularni sinflarga bo‘lish va ichki va tashqi tahdidlarni aniqlash ilmiy tadqiqot ishlarini olib borishni talab etmoqda.

Sun’iy intellekt (SI) - bu tahdidlarni aniqlay oladigan va ularni bartaraf etish va oldini olish uchun avtomatik ravishda zarur choralarni ko‘radigan texnologiya deb hisoblasa bo‘ladi. U ma’lumotlarni qayta ishlash, anomaliyalarni aniqlash va jarayonlarni avtomatlashtirish imkoniyatlari tufayli kiberhujumlardan axborotni himoya qilish darajasini sezilarli darajada oshirishi mumkin.

Kiberxavfsizlikda sun’iy intellektdan foydalanish axborotni himoya qilish darajasini sezilarli darajada oshirishi, jarayonlarni samaraliroq qilishi va kiberhujumlar xavfini kamaytirishi mumkin [7,8]. Shuni yodda tutish kerakki, SI kiber mudofaa arsenalidagi vositalardan biri bo‘lib, undan foydalanish boshqa xavfsizlik choralari bilan birlashtirilishi kerak.

Uzatilayotgan ma’lumotlarni himoya qilish uchun sun’iy intellektni qo‘llashning ba’zi usullari:

1. Har xil turdagi anomaliyalarni aniqlash:

- SI odatdagi xatti-harakatlardan chetga chiqishni aniqlash uchun trafik va foydalanuvchi xatti-harakatlarini tahlil qilishi mumkin. Misol uchun, agar foydalanuvchi odatda foydalanmaydigan ma’lumotlarga kirishga urinish kabi g‘ayrioddiy harakatlarni amalga oshira boshlasa, tizim avtomatik ravishda mumkin bo‘lgan hujum haqida signal berishi mumkin.

2. Hujumlarni bashorat qilish:

- Mashinani o‘rganish usullaridan foydalangan holda, SI tarixiy kiberhujum ma’lumotlarini tahlil qilishi va naqshlarni aniqlashi mumkin, bu esa potentsial tahdidlarni bashorat qilish va ularni oldini olish uchun o‘z vaqtida choralar ko‘rish imkonini beradi.

3. Hodisalarga javob berishni avtomatlashtirish:

- SI shubhali IP-manzillarni blokirovka qilish yoki buzilgan hisoblarni o‘chirib qo‘yish

ISSN 2181-9572

kabi hodisalarga javob berish jarayonlarini avtomatlashtirishi mumkin, bu esa tahdidlarga tezroq javob berishga imkon beradi.

4. Tarkibni filtrlash:

- SI kiruvchi xabarlar va ma'lumotlarni tahlil qilish va filtrlash, fishing yoki zararli qo'shimchalar kabi zararli tarkibni aniqlash uchun ishlatilishi mumkin.

5. Kirishni boshqarish:

- SI foydalanuvchi huquqlarini boshqarishda yordam berishi mumkin. Tizimlar foydalanuvchilarning xatti-harakatlarini tahlil qilishi va ularning roli va faoliyatiga qarab kirish darajalarini avtomatik ravishda sozlashi mumkin.

6. Tarmoq monitoringi:

- SI DDoS hujumlari yoki xakerlik urinishlari kabi kiberhujumni ko'rsatishi mumkin bo'lgan shubhali naqshlarni aniqlash orqali tarmoq faoliyatini doimiy ravishda kuzatishi mumkin.

7. Ma'lumotlarga asoslangan trening:

- SI tizimlari katta miqdordagi kiberhujum ma'lumotlari bo'yicha o'qitilishi mumkin, bu ularga aniqlash va javob berish algoritmlarini doimiy ravishda takomillashtirishga imkon beradi.

8. Ma'lumotlar buzilishidan himoya qilish:

- SI ma'lumotlar uzatilishini kuzatish va katta hajmdagi ma'lumotlarni nusxalash yoki tashqi manbalarga uzatish kabi shubhali harakatlarni aniqlash uchun ishlatilishi mumkin.

9. Aqlli tahdidlarni boshqarish tizimlari:

- Xavfsizlik ma'lumotlari va hodisalarni boshqarish tizimlari (SIEM) xavfsizlik hodisalarini yanada samarali tahlil qilish va o'zaro bog'lash uchun sun'iy intellektni birlashtirishi mumkin.

10. Xodimlarni o'qitish:

- SI xodimlarga kiber tahdidlarni aniqlashga va axborotni himoya qilish choralarini ko'rishga yordam beradigan interaktiv o'quv dasturlarini yaratish uchun ishlatilishi mumkin.

Kiber tahdidlardan himoyalangan korporativ kompyuter tarmog'ini yaratish texnik va tashkiliy choralarni o'z ichiga olgan kompleks yondashuvni talab qiladi.

Tarmoq xavfsizligini ta'minlashga yordam beradigan asosiy usullar [4-6]:

1. Xatarlarni baholash:

- Tarmoq zaifliklarini aniqlash uchun xavf tahlilini bajarish. Qaysi ma'lumotlar va tizimlar biznes uchun muhim ekanligini va ularga qanday tahdidlar ta'sir qilishi mumkinligini aniqlash.

2. Xavfsizlik siyosatini ishlab chiqish:

- Axborotni himoya qilish, kirishni boshqarish va hodisalarga javob berish qoidalari va tartiblarini o'z ichiga olgan xavfsizlik siyosatini yaratib amalga oshirish.

3. Tarmoq segmentatsiyasi:

- Muhim tizimlar va ma'lumotlarni ajratish uchun tarmoqni segmentlarga bo'linadi. Bu tahdidlar paydo bo'lganda ularning tarqalishini cheklashga yordam beradi.

4. Xavfsizlik devorlaridan foydalanish:

- Kiruvchi va chiquvchi trafikni filtrlash uchun xavfsizlik devorlarini o'rnatish. Shubhali ulanishlarni blokirovka qilish qoidalarini sozlash.

5. Kirishni aniqlash va oldini olish tizimlari (IDS / IPS):

- Tarmoq trafigini kuzatish va Real vaqtda yuzaga kelishi mumkin bo'lgan hujumlarni aniqlash uchun IDS/IPS tizimlarini ishga tushurish.

6. Ma'lumotlarni shifrlash:

- Dam olish paytida ham, tarmoq orqali uzatishda ham nozik ma'lumotlarni himoya qilish uchun shifrlashdan foydalanish. Bu ma'lumotlar ushlanib qolsa, ularga kirishni oldini olishga yordam beradi.

7. Autentifikatsiya va kirishni boshqarish:

- Muhim tizimlarga kirish uchun ko'p faktorli autentifikatsiyani (KFA) amalga oshirish. Foydalanuvchilarning faqat o'z ishlarini bajarish uchun zarur bo'lgan manbalarga kirishini cheklash.

8. Dasturiy ta'minotni yangilash:

- Ma'lum zaifliklardan himoya qilish uchun operatsion tizimlar, ilovalar va antivirus dasturlarini muntazam yangilab turish.

9. Monitoring va jurnallar:

- Foydalanuvchi faoliyati va tarmoq trafigini kuzatish uchun monitoring va jurnal tizimlarini sozlash. Bu shubhali xatti-harakatlarni aniqlashga yordam beradi.

10. Xodimlarni o'qitish:

- Xodimlar uchun fishing kabi mumkin bo'lgan tahdidlardan xabardor bo'lishlari va ularga to'g'ri munosabatda bo'lishlari uchun muntazam ravishda kiberxavfsizlik bo'yicha treninglar o'tkazish.

11. Hodisalarga javob berish rejasi:

- Kiberhujum yoki ma'lumotlar buzilgan taqdirda aniq harakatlar tartibini o'z ichiga olgan hodisalarga javob berish rejasini ishlab chiqish.

12. Ma'lumotlarni zaxiralash:

- Muhim ma'lumotlarni muntazam ravishda zaxiralash va xavfsiz joyda saqlash. Bu yo'qolgan

yoki buzilgan taqdirda ma’lumotni tiklashga yordam beradi.

13. Penetratsion test:

- Xavfsizlik zaifliklarini aniqlash va mavjud himoya choralarining samaradorligini tekshirish uchun muntazam ravishda penetratsiya testlarini o‘tkazish.

14. Tashqi manbalar:

- Maslahat olish va xavfsizlik auditini o‘tkazish uchun tashqi kiberxavfsizlik bo‘yicha mutaxassislar bilan hamkorlik qilishni aniqlash.

Ushbu amallarni bajarib, yanada xavfsiz korporativ kompyuter tarmog‘ini yaratish va kiber tahdid xavfini minimallashtirish mumkin bo‘ladi.

Bunday boshqarish tizimi nazariy tadqiqotlar asosida quyidagi yo‘nalishlardan iborat bo‘lishi kerak:

1. Yuqorida keltirilgan jismoniy, texnikaviy, dasturiy, iqtisodiy, siyosiy, ma’naviy va ma’rifiy keltirilgan zararlarni aniqlab beradigan matematik formulalarini yaratish.

2. Har bir kiberxujumdan hosil bo‘lishi mumkin bo‘lgan zararlarning matematik modellarini ishlab chiqish.

3. Kiberxavfsizlikka taaluqli bo‘lgan texnikaviy, dasturiy vositalarni va ularning turlarini aniqlab berish.

4. Kiberxujumlarning turlarini aniqlaydigan va ularga qarshi usullarini ishlab chiqish.

5. Axborotlarni xavfsizligini ta’minlash uchun tashkiliy, texnikaviy, dasturiy, kriptografik, jismoniy, xuquqiy va telekommunikatsiya tarmoqlari orqali uzatilayotgan ma’lumotlarni himoyalash vositalarini aniqlab berish.

6. Identifikatsiya va autentifikatsiya jarayonlarini takomilashtirish.

7. Kompyuter tarmoqlari orqali kirib kelayotgan viruslarga va maxsus kodlarga qarshi usullarni ishlab chiqish.

8. Himoyalangan zamonaviy ma’lumotlar omborlarini yaratish usullarini ishlab chiqish.

9. Har xil turdagi intellektual tizimlar yaratish uchun o‘z-o‘zini o‘rgatadigan va neyrotexnologiyalarga asoslangan bilimlar bazasini yaratish hisoblanadi.

XULOSA

Xulosa qilib aytish mumkinki, barcha yuqorida keltirilgan masalalar uchun texnikaviy, dasturiy va informatsion ta’minotini yaratib berish kerak bo‘ladi. Ushbu usullarni ilmiy tahlili asosida amalga oshirilganda barcha tashkilot, korxona va muassasalarning Internet platformalarida saqlanayotgan, uzatilayotgan va qabul qilinayotgan ma’lumotlarini har xil turdagi kiberhujumlardan saqlanish ihtimolini oshirilgan bo‘ladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Nigmatov X. Raqamlashtirish va intellektual tizimlarining kiberxavfsizligini ta’minlanishini boshqarish // “SCIENTIFIC foundations of raising the use of information technologies to a new level and modern problems of automation” III-international scientific conference november 20, 2024. 306-310. https://doi.org/10.5281/zenodo.14221576.
2. Nigmatov X. Tarmoqlarda kiberhujumlardan axborotlarni himoyalashda sun’iy intellektdan foydalanish // “Amaliy matematikaning zamonaviy muammolari va istiqbollari” Respublika ilmiy-amaliy konferensiya. – Qarshi, 24-25-may, 2024. 153-155 b. https://mppam2024.
3. Nigmatov X. Ma’lumotlar xavfsizligini ta’minlashda sun’iy intellektdan foydalanish // Problems of application of innovative and digital technologies in the education system international scientific – practical conference. 6-7 may, 2024. – Tashkent. – B. 738-747.
4. Nigmatov X. Tarmoq xavfsizligini aniqlash usullari. Monografiya. – Toshkent: «Fan va texnologiyalari» nashriyot bosmaxonasi, 2023. – 220 b.
5. Nigmatov X., Raxmonov Q.S., Obyektlarda axborot xavfsizligini boshqarish tizimini yaratish metodologiyasi. Monografiya. – Toshkent: “Zamon poligraf” ok bosmaxonasi, 2022. – 144 b.
6. Nigmatov X., Tarmoq xavfsizligini aniqlash usullari. Monografiya. – Toshkent: “Fan va texnologiyalari” nashriyot-matbaa uyi bosmaxonasi, 2024. – 222 b.
7. Nigmatov X., Xodjaeva M.S. Axborotlarni himoyalashda intellektual tizimlar: darslik. – Toshkent: “Lesson Press” nashriyoti, 2022. – 290 b.
8. Nigmatov X., Sodiqov U.X. Intellektual tizimlar: darslik. – Toshkent: “Zamon poligraf” OK bosmaxonasi, 2024. – 194 b.

ISSN 2181-9572