Axborot xavfsizligi va internetdagi tahdidlarga qarshi kurashish

Azimjonov Hasanboy Botirali o'gli
Farg'ona davlat texnika universiteti talabasi
Elektron pochta: azimjonovhasanboy212@gmail.com

Annotatsiya: Ushbu maqolada axborot xavfsizligi tushunchasi, internetdagi zamonaviy tahdidlar, kiberhujumlarning turlari hamda ularga qarshi kurashishning samarali usullari yoritilgan. Shuningdek, zamonaviy axborot tizimlarining yuragi hisoblangan ma'lumotlar bazalari, Big Data (katta ma'lumotlar) tizimlarining xavfsizligi, bulutli texnologiyalarda ma'lumotlarni himoyalash hamda sun'iy intellektning kiberxavfsizlikdagi roli tahlil qilingan. Foydalanuvchilar va tashkilotlar xavfsizligini ta'minlashda texnologik va huquqiy himoya choralarining ahamiyati asoslab berilgan.

Kalit so'zlar: Axborot xavfsizligi, kiberxavfsizlik, internet tahdidlari, phishing, zararli dastur, ma'lumotlar bazasi (DBMS), Big Data, shifrlash, autentifikatsiya, kiberjinoyat, bulutli texnologiyalar, sun'iy intellekt.

Modern Methods of Combating Information Security and Internet Threats

Abstract. This article discusses the concept of information security, modern Internet threats, types of cyberattacks, and effective methods to combat them. It also analyzes the security of databases, which are the core of modern information systems, Big Data security, data protection in cloud technologies, and the role of artificial intelligence in cybersecurity. The importance of technological and legal protection measures in ensuring the security of users and organizations is scientifically justified.

Keywords: Information security, cybersecurity, internet threats, phishing, malware, database (DBMS), Big Data, encryption, authentication, cybercrime, cloud technologies, artificial intelligence.

Современные методы борьбы с угрозами информационной безопасности в Интернете

Аннотация. В данной статье рассматриваются понятие информационной безопасности, современные интернет-угрозы, виды кибератак и эффективные методы борьбы с ними. Также анализируется безопасность баз данных, являющихся ядром современных информационных систем, защита Big Data (больших данных), облачных технологий и роль искусственного интеллекта в кибербезопасности. Обосновано значение технологических и правовых мер защиты для обеспечения безопасности пользователей и организаций.

Ключевые слова: Информационная безопасность, кибербезопасность, интернет-угрозы, фишинг, вредоносное ПО, база данных (СУБД), Big Data, шифрование, аутентификация, киберпреступность, облачные технологии, искусственный интеллект

KIRISH

Zamonaviy raqamli jamiyatning jadal rivojlanishi axborot texnologiyalarining barcha sohalarga keng kirib borishiga olib keldi. Internet tarmog'i bugungi kunda nafaqat axborot almashinuvi vositasi, balki iqtisodiyot, ta'lim, davlat boshqaruvi va ijtimoiy hayotning ajralmas qismiga aylandi. Biroq, raqamli texnologiyalarning bunday keng qo'llanilishi bilan bir qatorda, axborot xavfsizligiga tahdid soluvchi omillar ham keskin ortib bormoqda [1].Axborot xavfsizligi — bu ma'lumotlarning maxfiyligi,

yaxlitligi va mavjudligini ta’minlashga qaratilgan kompleks chora-tadbirlar tizimidir. Bugungi kunda internet orqali amalga oshirilayotgan kiberhujumlar, zararli dasturlar (malware), fishing (phishing), ijtimoiy muhandislik (social engineering) kabi tahdidlar foydalanuvchilar va tashkilotlar uchun jiddiy xavf tug‘dirmoqda [2]. Ayniqsa, shaxsiy ma’lumotlarning o‘g‘irlanishi, bank kartalari va hisob raqamlariga ruxsatsiz kirish holatlari ko‘payib bormoqda [3].

Internetdagi tahdidlarning eng xavfli jihatlaridan biri ularning tez moslashuvchanligi va murakkabligidir. Kiberjinoyatchilar zamonaviy texnologiyalardan foydalangan holda himoya tizimlarini chetlab o‘tishga harakat qilmoqdalar. Bu esa axborot xavfsizligi sohasida doimiy yangilanib boruvchi himoya mexanizmlarini joriy etishni talab etadi [4].Shuningdek, foydalanuvchilarning axborot savodxonligi darajasi ham muhim omil hisoblanadi. Ko‘plab kiberhujumlar texnik zaifliklardan emas, balki inson omili — e’tiborsizlik, ehtiyotsizlik yoki yetarli bilimga ega emaslik sababli yuzaga keladi [5]. Shu bois, axborot xavfsizligi madaniyatini shakllantirish va internetdan xavfsiz foydalanish ko‘nikmalarini rivojlantirish bugungi kunning dolzarb vazifalaridan biridir.

O‘zbekiston Respublikasida ham axborot xavfsizligini ta’minlash, kiberjinoyatlarga qarshi kurashish hamda raqamli savodxonlikni oshirish bo‘yicha keng ko‘lamli islohotlar amalga oshirilmoqda. Bu jarayon jamiyatning barcha qatlamlarini qamrab olgan holda, milliy kiberxavfsizlik tizimini mustahkamlashga xizmat qilmoqda [6].

ADABIYOTLAR TAHLILI

Axborot xavfsizligi va internetdagi tahdidlarga qarshi kurashish masalasi zamonaviy ilmiy tadqiqotlarda keng o‘rganilayotgan yo‘nalishlardan biri hisoblanadi. Ushbu sohada olib borilgan tadqiqotlar asosan kiberxavfsizlikning nazariy asoslari, texnik himoya vositalari va ijtimoiy omillarni o‘z ichiga oladi [7]. J. P. Lantolf va M. E. Poehner tomonidan ishlab chiqilgan sociokultural yondashuvga ko‘ra, bilimlarni egallash jarayoni ijtimoiy muhit va hamkorlik asosida shakllanadi. Bu yondashuv axborot xavfsizligi sohasida foydalanuvchilarning xulqi va inson omilining kiberxavflarga ta’sirini tushunishda muhim ahamiyatga ega [7].

Shuningdek, J. P. Lantolf va S. L. Thorne tadqiqotlarida til va rivojlanish jarayonlari ijtimoiy-madaniy kontekstda o‘rganilib, inson faoliyatining vositalar orqali shakllanishi ta’kidlanadi. Ushbu qarashlar internet muhitida foydalanuvchilarning xatti-harakatlari va xavfsizlik madaniyatini shakllantirishda ham qo‘llanilishi mumkin [8].

G. T. Makhkamova esa bo‘lajak ingliz tili o‘qituvchilarining kasbiy va metodik kompetensiyasini rivojlantirishni o‘rganar ekan, zamonaviy ta’lim jarayonida axborot texnologiyalaridan samarali foydalanish zarurligini ta’kidlaydi. Bu esa raqamli muhitda xavfsiz ishlash ko‘nikmalarining ham muhimligini ko‘rsatadi [9]. A. Walqui va G. C. Bunch tomonidan olib borilgan tadqiqotlarda o‘quvchilarga sifatli ta’lim muhitini yaratish va o‘quv jarayonini boyitish masalalari yoritilgan. Ushbu yondashuv raqamli ta’lim platformalarida xavfsiz va samarali foydalanish muhimligini asoslaydi [10].

METODOLOGIYA

Mazkur tadqiqotda axborot xavfsizligi va internetdagi tahdidlarga qarshi kurashish muammosini o‘rganishda nazariy va tahliliy metodlar qo‘llanildi. Tadqiqot jarayonida ilmiy adabiyotlarni tahlil qilish, umumlashtirish va tizimlashtirish usullaridan foydalanildi [11].Shuningdek, kiberxavfsizlik sohasidagi asosiy konseptlar — axborotning maxfiyligi, yaxlitligi va mavjudligi (CIA modeli) asosida yondashuv ishlab chiqildi. Bu yondashuv internet muhitidagi tahdidlarni aniqlash va ularning oldini olish mexanizmlarini tushunishda muhim ahamiyatga ega hisoblanadi [12].

Tadqiqotda qiyosiy tahlil metodi ham qo‘llanilib, turli ilmiy manbalarda keltirilgan kiberhujum turlari, himoya usullari va xavfsizlik strategiyalari o‘zaro solishtirildi. Bu esa muammoning ko‘p qirrali ekanligini aniqlash imkonini berdi [13]. Bundan tashqari, tizimli yondashuv asosida axborot xavfsizligi komponentlari o‘zaro bog‘liqlikda o‘rganildi. Internetdagi tahdidlar texnik, tashkiliy va inson omili nuqtai nazaridan kompleks ravishda tahlil qilindi [14].

NATIJA VA MUHOKAMA

Tadqiqot natijalari shuni ko‘rsatadiki, axborot xavfsizligi zamonaviy raqamli muhitda eng dolzarb muammolardan biri bo‘lib qolmoqda. Internetdagi tahdidlar soni va murakkabligi yildan-yilga ortib bormoqda, bu esa foydalanuvchilar va tashkilotlar uchun qo‘shimcha xavf tug‘dirmoqda [15]. Tahlillar asosida aniqlanishicha, kiberhujumlarning eng ko‘p uchraydigan turlari fishing (phishing), zararli dasturlar (malware), parol buzish va ijtimoiy muhandislik (social engineering) hisoblanadi. Ushbu hujumlarning aksariyati texnik zaifliklardan ko‘ra inson omili orqali amalga oshirilishi kuzatildi [16].

Natijalarga ko‘ra, axborot xavfsizligini ta’minlashda texnik himoya vositalari (firewall, antivirus, shifrlash) muhim o‘rin tutadi, biroq ular yetarli emas. Eng samarali yondashuv — texnik, tashkiliy va inson omilini birgalikda qamrab olgan kompleks xavfsizlik tizimini joriy etishdir [17]. Muhokama jarayonida shuni ham aniqlash mumkinki, foydalanuvchilarning raqamli savodxonligi past bo‘lsa, hatto eng zamonaviy himoya tizimlari ham to‘liq samarali bo‘la olmaydi. Shu sababli, kiberxavfsizlik madaniyatini shakllantirish va foydalanuvchilarni muntazam o‘qitish zarur [18].

Shuningdek, davlat darajasida kiberxavfsizlik siyosatini kuchaytirish, milliy axborot tizimlarini himoya qilish va kiberjinoyatlarga qarshi kurashish mexanizmlarini takomillashtirish muhim ahamiyatga ega ekanligi tasdiqlandi [19].

XULOSA

Axborot xavfsizligi va internetdagi tahdidlarga qarshi kurashish bugungi kunda raqamli jamiyatning eng muhim va dolzarb muammolaridan biri hisoblanadi. Internet texnologiyalarining keng qo‘llanilishi axborot almashinuvini tezlashtirgan bo‘lsa-da, shu bilan birga turli kiberxavflarning ortishiga ham sabab bo‘lmoqda. Tadqiqot natijalariga ko‘ra, kiberhujumlarning asosiy turlari fishing, zararli dasturlar, parol buzish va ijtimoiy muhandislik usullari hisoblanadi. Ushbu tahdidlar ko‘pincha texnik zaifliklardan emas, balki inson omili, ya’ni foydalanuvchilarning ehtiyotsizligi va yetarli bilimga ega emasligi natijasida yuzaga keladi. Shuningdek, axborot xavfsizligini ta’minlashda texnik himoya vositalari muhim o‘rin tutadi, biroq ular yakka o‘zi yetarli emas. Eng samarali yondashuv sifatida texnik, tashkiliy va inson omillarini o‘z ichiga olgan kompleks xavfsizlik tizimini joriy etish zarurligi aniqlanadi.

Bundan tashqari, raqamli savodxonlikni oshirish va foydalanuvchilarda kiberxavfsizlik madaniyatini shakllantirish internetdagi tahdidlarning oldini olishda muhim ahamiyatga ega. Shu sababli, doimiy o‘qitish va xabardorlikni oshirish choralari dolzarb hisoblanadi. Umuman olganda, axborot xavfsizligini ta’minlash uzluksiz jarayon bo‘lib, u doimiy yangilanib boruvchi himoya tizimlari, kuchli nazorat va foydalanuvchilarning mas’uliyatli yondashuvini talab qiladi.

FOYDALANILGAN ADABIYOTLAR

[1] W. Stallings, *Kriptografiya va tarmoq xavfsizligi: tamoyillar va amaliyot*, 7-nashr. Boston, AQSh: Pearson, 2017.

[2] C. P. Pfleeger va S. L. Pfleeger, *Hisoblash tizimlarida xavfsizlik*. Boston, AQSh: Pearson, 2015.

[3] A. S. Tanenbaum va D. J. Wetherall, *Kompyuter tarmoqlari*, 5-nashr. Boston, AQSh: Pearson, 2011.

[4] M. Bishop, *Kompyuter xavfsizligi: san'at va fan*. Boston, AQSh: Addison-Wesley, 2018.

[5] E. Casey, *Raqamli dalillar va kompyuter jinoyatlari*. Boston, AQSh: Academic Press, 2011.

[6] D. Easttom, *Kompyuter xavfsizligi asoslari*. Nyu-York, AQSh: Pearson, 2019.

[7] A. Anderson, *Xavfsizlik muhandisligi: ishonchli tizimlar yaratish*. Wiley, 2020.

[8] NIST, *Kiberxavfsizlik tizimi (CSF) 1.1 versiya*. Gaithersburg, AQSh: NIST, 2018.

[9] ITU, *Global kiberxavfsizlik indeksi hisoboti*. Jeneva, Shveytsariya: ITU, 2020.

[10] O'zbekiston Respublikasi Prezidentining qarori, "Kiberxavfsizlikni rivojlantirish choralari to'g'risida," Toshkent, 2021.

[11] O'zbekiston Respublikasi Axborot texnologiyalari vazirligi, *Raqamli O'zbekiston — 2030 strategiyasi*. Toshkent, 2020.

[12] O'zbekiston Respublikasi Statistika agentligi, *Raqamli iqtisodiyot rivojlanishi hisoboti*. Toshkent, 2023.

[13] S. Garfinkel, *Practical UNIX and Internet Security*. O'Reilly Media, 2018.

[14] B. Schneier, *Applied Cryptography*. Wiley, 2015.

[15] J. P. Lantolf va M. E. Poehner, *Sociokultural nazariya va til rivojlanishi*. Routledge, 2022.

[16] R. Ellis, *Task-Based Language Learning*. Oxford University Press, 2018.

[17] M. Fullan, *Ta'limdagi o'zgarishlarning yangi ma'nosi*. Teachers College Press, 2016.

[18] D. Coyle va O. Meyer, *CLIL va chuqur o'qitish*. Cambridge University Press, 2021.

[19] G. Kessler, *CALL asoslari va amaliyoti*. TESOL International Association, 2018.