KIBERXAVFSIZLIK ASOSLARI VA ZAMONAVIY TAHDIDLAR

A.B. Aliqulov –
Qarshi xalqaro universiteti o'qituvchisi
E_mail: abbosaliqulov1253@gmail.com
A.B. Aliqulov –
Lecturer at Qarshi International University

Annotatsiya: *Maqolada kiberxavfsizlikning asosiy tamoyillari, zamonaviy tahdidlar (phishing, ransomware, DDoS, zero-day) va ularning oldini olish usullari tahlil qilinadi. Xalqaro standartlar va foydalanuvchi xatti-harakatlarining ahamiyati yoritilib, real holat asosida amaliy xulosalar chiqariladi. Tadqiqot axborot tizimlari xavfsizligini ta'minlashda nazariy va amaliy ahamiyatga ega.*

Kalit so'zlar: *kiberxavfsizlik, phishing, ransomware, CIA triadasi, axborot xavfsizligi, DDoS, kriptografiya.*

Аннотация: *В статье анализируются основные принципы кибербезопасности, современные угрозы (фишинг, программы-вымогатели, DDoS, уязвимости нулевого дня) и методы их предотвращения. Освещается значение международных стандартов и поведения пользователей. На основе анализа реального инцидента формулируются практические выводы. Исследование представляет теоретическую и практическую ценность для обеспечения безопасности информационных систем.*

Ключевые слова: *кибербезопасность, фишинг, программы-вымогатели, триада CIA, информационная безопасность, DDoS, криптография.*

Abstract: *The article analyzes the fundamental principles of cybersecurity, modern threats (phishing, ransomware, DDoS, zero-day vulnerabilities), and methods of prevention. It highlights the importance of international standards and*

user behavior. Practical conclusions are drawn based on the analysis of a real-life incident. The study holds both theoretical and practical significance for ensuring information system security.

Keywords: *cybersecurity, phishing, ransomware, CIA triad, information security, DDoS, cryptography.*

Kirish

Axborot texnologiyalari tez sur’atlar bilan rivojlanib borayotgan hozirgi zamonda raqamli xavfsizlik masalasi global miqyosda dolzarb bo‘lib bormoqda. Zamonaviy jamiyat faoliyatining barcha jabhalarida - moliya, sog‘liqni saqlash, ta’lim, davlat boshqaruvi va boshqa sohalarda - axborot tizimlari keng qo‘llanilmoqda. Bunday sharoitda axborotning ishonchliligi, maxfiyligi va butunligiga tahdid soluvchi kiberxurujlar tobora ko‘paymoqda.

Tadqiqotlarning ko‘rsatishicha, so‘nggi yillarda kiberxavfsizlikka oid voqealar soni sezilarli darajada ortmoqda. Masalan, 2023-yilda dunyo bo‘yicha o‘tkazilgan tahlillarga ko‘ra, kompaniyalarning 80% dan ortig‘i hech bo‘lmaganda bir marta kiberhujumga duch kelgan. Bu esa kiberxavfsizlikni nafaqat texnik, balki strategik va ijtimoiy muammo sifatida ko‘rib chiqishni taqozo etadi. Mazkur maqolada kiberxavfsizlikning nazariy asoslari, zamonaviy kiberxavf-xatarlar tahlili va ularga qarshi kurashish usullari ilmiy jihatdan o‘rganiladi. Shuningdek, real holat (WannaCry virusi) misolida tahdidlarning amaliy oqibatlari yoritiladi va xulosalar chiqariladi.

Adabiyotlar tahlili

Kiberxavfsizlik (ing. cybersecurity) - bu axborot texnologiyalari va kompyuter tizimlaridan foydalanganda ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini ta’minlashga qaratilgan chora-tadbirlar tizimidir. Bugungi raqamli jamiyatda kiberxavfsizlik nafaqat texnik himoya vositasi, balki milliy xavfsizlik,

iqtisodiy barqarorlik va shaxsiy hayot daxlsizligining asosiy omillaridan biri sifatida qaralmoqda.

Kiberxavfsizlik texnologik infratuzilmani, tarmoqlarni, dasturiy ta’minotlarni va foydalanuvchilarni turli xil tahdidlardan himoya qilishni nazarda tutadi. U nafaqat texnik vositalar, balki boshqaruv siyosati, xodimlar o‘rtasida axborot madaniyatini shakllantirish hamda huquqiy mexanizmlarni ham o‘z ichiga oladi. Kiberxavfsizlikni tashkil etuvchi asosiy prinsiplar ko‘pincha CIA triadasi (Confidentiality, Integrity, Availability) orqali izohlanadi:

Maxfiylik (Confidentiality): ma’lumotlarga faqat ruxsat etilgan shaxslar kirish huquqiga ega bo‘lishi kerak.

Yaxlitlik (Integrity): ma’lumotlar o‘zgarmasligi va ishonchliligini saqlash.

Mavjudlik (Availability): tizimlar zarur vaqtda foydalanuvchilar uchun ochiq bo‘lishi lozim.

1-rasm: CIA triadasi[1]

[1] https://www.stationx.net/what-is-the-cia-triad/

Mazkur triada axborot tizimlarining holatini tahlil qilish, tahdidlarni baholash va himoya strategiyasini ishlab chiqishda asos bo‘lib xizmat qiladi.

Shuningdek, xalqaro standartlar, jumladan ISO/IEC 27001 axborot xavfsizligini boshqarish tizimini yaratish va takomillashtirishga qaratilgan.

Tadqiqot metodologiyasi

Kiberxavfsizlikni ta’minlash - bu tizimli, kompleks va doimiy jarayon bo‘lib, texnik, tashkiliy va inson omillarini birlashtiradi. Faoliyat sohasidan qat’i nazar, har bir tashkilot yoki foydalanuvchi axborot xavfsizligiga oid asosiy chora-tadbirlarni ko‘rishi zarur. Maqolada zamonaviy tahdidlar misolida (phishing, ransomware, DDoS, zero-day) ularning turlari, sabablari va oqibatlari o‘rganiladi. Bundan tashqari, himoyalanish usullari, xalqaro standartlarga muvofiqlik va foydalanuvchi xatti-harakatlarining o‘rni ham tahlil etiladi.

Tahlil va natijalar muhokamasi

Zamonaviy tahdidlar ichida quyidagilar alohida o‘rin tutadi:

- Phishing va ijtimoiy muhandislik orqali foydalanuvchilarning shaxsiy ma’lumotlarini qo‘lga kiritish;
- Ransomware dasturlari orqali tizimni bloklab, to‘lov talab qilish;
- DDoS hujumlari orqali xizmatlar faoliyatini izdan chiqarish;

Zero-day zaifliklar orqali aniqlanmagan zaif joylardan foydalanish.

- Kiberxavfsizlikni ta'minlash usullari quyidagilarni o‘z ichiga oladi:
- Tarmoq xavfsizligi (Firewall, IDS/IPS, VPN)
- Kriptografik vositalar (simmetrik, assimmetrik shifrlash, elektron raqamli imzo)
- Xodimlarni o‘qitish, xavfsizlik siyosatini shakllantirish va 2FA kabi choralar

Amaliy misol sifatida 2017-yilgi WannaCry hujumi[2] tahlil qilinib, uning sabablari, zarar ko‘rgan tizimlar, zaifliklar va natijalari ko‘rsatildi. Ushbu

[2] https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

hujumdan quyidagi saboqlar chiqarildi: doimiy yangilanish, zaxira nusxalar, xodimlarni tayyorlash va ilg‘or monitoring vositalari joriy etilishi zarur.

Xulosa

Kiberxavfsizlik bugungi kunda axborot tizimlari ishonchliligini ta'minlashda strategik ahamiyat kasb etmoqda. Tadqiqot davomida nazariy asoslar, zamonaviy tahdidlar, himoya choralarining samaradorligi hamda real holatdagi misol tahlil qilindi. Xulosa qilib aytganda, tashkilotlar quyidagilarga e'tibor qaratishi lozim:

- Xavfsizlik siyosatini ishlab chiqish va yangilab borish;
- Yangilanishlarni vaqtida o‘rnatish;
- Zaxira nusxalarni muntazam saqlash;
- Foydalanuvchilarni o‘qitish va madaniyatni shakllantirish;
- Texnik himoya vositalarini joriy qilish.

Tadqiqot natijalari kiberxavfsizlik sohasida nazariy bilimlar va amaliy faoliyatni uyg‘unlashtirishga xizmat qiladi.

Adabiyotlar

1. Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress Publishing.

2. Stallings, W. (2017). Network Security Essentials: Applications and Standards (6th ed.). Pearson Education.

3. ISO/IEC 27001:2022 - Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization.

4. Ильин, И.В. (2021). Кибербезопасность: учебник для вузов. Москва: Юрайт.

5. Symantec. (2019). Internet Security Threat Report. Retrieved from: https://www.broadcom.com/company/newsroom/press-releases

6. Kaspersky Lab. (2023). Ransomware attacks report: global trends and statistics. URL: https://www.kaspersky.com/blog/ransomware-report

7. Microsoft. (2017). WannaCrypt ransomware attack: Analysis and recommendations. URL: https://blogs.microsoft.com/microsoftsecure/wannacrypt-ransomware/

8. Федеральная служба по техническому и экспортному контролю (ФСТЭК). (2022). Методические рекомендации по защите информации в автоматизированных системах.

9. Parker, D. B. (2002). Fighting Computer Crime: A New Framework for Protecting Information. John Wiley & Sons.

10. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4(2), 92–100. DOI:10.4236/jis.2013.42011