KIBERXAVFSIZLIK VA ZAMONAVIY TAHDIDLAR: IT TIZIMLARIDA HIMOYA USULLARI

O.L.Ochilov *– Qarshi Xalqaro Universiteti*
E-mail: oqilbekochilov@gmail.com

Annotatsiya: Ushbu maqolada kiberxavfsizlik tushunchasi, zamonaviy tahdidlar va IT tizimlarida qo‘llaniladigan himoya usullari tahlil qilingan. Malware, ransomware, phishing, DDoS hujumlari va ichki xodimlar tahdidi kabi zamonaviy kiberxavfsizlik tahdidlari yoritilgan. Maqolada texnik, tashkiliy va huquqiy himoya chora-tadbirlari orqali axborot tizimlarini himoya qilishning samarali usullari ko‘rib chiqilgan. Tadqiqot natijalari kiberxavfsizlikni ta’minlash orqali tashkilotlar va foydalanuvchilar ma’lumotlarining xavfsizligi, tizimlarning samaradorligi va ishonchliligini oshirish mumkinligini ko‘rsatadi.

Kalit so‘zlar: Axborot texnologiyalari, kiberxavfsizlik, IT tizimlari, axborot xavfsizligi, zamonaviy tahdidlar, malware, ransomware, phishing, DDoS, himoya usullari, texnik chora-tadbirlar, tashkiliy chora-tadbirlar, huquqiy chora-tadbirlar, tarmoqlar xavfsizligi, ma’lumotlar maxfiyligi, IT infratuzilma.

Cybersecurity and Modern Threats: Protection Methods in IT Systems

This article analyzes the concept of cybersecurity, modern threats, and protection methods applied in IT systems. Contemporary cybersecurity threats such as malware, ransomware, phishing, DDoS attacks, and insider threats are examined. The article discusses technical, organizational, and legal measures for effectively protecting information systems. The study results demonstrate that implementing cybersecurity measures can enhance the security of organizational and user data, improve system efficiency, and ensure reliability.

Keywords: Information technologies, cybersecurity, IT systems, information security, modern threats, malware, ransomware, phishing, DDoS, protection methods, technical measures, organizational measures, legal measures, network security, data privacy, IT infrastructure.

Raqamli texnologiyalarning jadal rivojlanishi bilan birga, axborot tizimlariga bo‘lgan tahdidlar ham sezilarli darajada oshmoqda. Bugungi kunda kiberxavfsizlik (cybersecurity) masalalari nafaqat kompaniyalar va tashkilotlar, balki davlatlar darajasida ham dolzarb hisoblanadi. Kiberhujumlar, ma’lumotlarni o‘g‘irlash, zararli dasturlar (malware), tarmoq buzilishi kabi tahdidlar biznes va davlat tizimlariga katta zarar yetkazishi mumkin. Mazkur maqolaning maqsadi — kiberxavfsizlik tushunchasi, zamonaviy tahdidlar va IT tizimlarida qo‘llaniladigan himoya usullarini tahlil qilishdir.

Kiberxavfsizlik — bu axborot tizimlarini, tarmoqlarni va ma’lumotlarni ruxsatsiz kirish, o‘zgartirish yoki yo‘qotishdan himoya qilish tizimi. Uning asosiy elementlari quyidagilar:

- Ma’lumotlar maxfiyligi (Confidentiality) — ma’lumotlarga faqat ruxsat etilgan shaxslar kirishi;
- Ma’lumotlar yaxlitligi (Integrity) — ma’lumotlarning o‘zgarmasligi va aniqligi;
- Mavjudlik (Availability) — tizimlar va ma’lumotlarga kerakli vaqtda kirish imkoniyati.

Kiberxavfsizlikning samarali bo‘lishi uchun texnik, tashkiliy va huquqiy chora-tadbirlarning uyg‘unligi muhimdir. Zamonaviy tahdidlar turlari:

- Malware va viruslar – zararli dasturlar orqali tizimga zarar yetkazish.
- Ransomware (to‘lov talab qiluvchi dasturlar) – foydalanuvchi ma’lumotlarini shifrlab, qayta tiklash uchun to‘lov talab qilish.
- Phishing (soxtalashtirilgan elektron pochta va saytlar) – foydalanuvchi ma’lumotlarini o‘g‘irlash.
- DDoS hujumlar (Distributed Denial of Service) – serverlar va xizmatlarni ishdan chiqarish.
- Ichki xodimlar tahdidi – tashkilot ichidagi xodimlarning nojo‘ya harakatlari orqali xavfsizlikni buzish.

IT tizimlarida himoya usullari

Texnik chora-tadbirlar:

1. Firewall va IDS/IPS tizimlari — tarmoqqa ruxsatsiz kirishlarni aniqlash va bloklash;
2. Shifrlash texnologiyalari (Encryption) — ma’lumotlarni shifrlash orqali himoya qilish;
3. Antivirus va antimalware dasturlar — zararli dasturlarni aniqlash va yo‘q qilish;
4. Zaxira nusxalari (Backup) — ma’lumotlarning yo‘qolishiga qarshi chora.
5. Tashkiliy chora-tadbirlar
6. Xodimlarni kiberxavfsizlik bo‘yicha o‘qitish;
7. Ruxsat va kirish darajalarini boshqarish;
8. Xavfsizlik siyosatini ishlab chiqish va amalga oshirish.
9. Huquqiy va normativ chora-tadbirlar
10. Axborot xavfsizligi bo‘yicha davlat standartlari va qonunchilik;
11. Maxfiy ma’lumotlarni himoya qilish bo‘yicha normativ hujjatlar;
12. Kiberhujumlarga qarshi yuridik javobgarlik.

Ta’lim sohasida

Bulutli texnologiyalar masofaviy ta’limni rivojlantirishda muhim rol o‘ynaydi. Google Classroom, Moodle kabi platformalar o‘quv jarayonini samarali tashkil etish imkonini beradi. Talabalar o‘quv materiallariga istalgan vaqtda kirishlari mumkin.

Biznes va tadbirkorlikda

Kompaniyalar bulutli texnologiyalar yordamida buxgalteriya, mijozlar bilan ishlash (CRM), hujjat aylanishi tizimlarini joriy etmoqda. Bu esa xarajatlarni kamaytirib, ish unumdorligini oshiradi.

Sog‘liqni saqlash sohasida

Elektron tibbiy kartalar, tahlil natijalari va bemorlar ma’lumotlarini xavfsiz saqlashda bulutli texnologiyalar keng qo‘llanilmoqda. Shifokorlar ma’lumotlarga tezkor kirish imkoniyatiga ega bo‘ladi.

Davlat boshqaruvi tizimida

Elektron hukumat tizimlarida bulutli texnologiyalar xizmatlar tezkorligi va shaffofligini ta’minlaydi. Fuqarolar onlayn tarzda hujjat topshirish va ma’lumot olish imkoniga ega bo‘lmoqda.

Afzalliklari:

- Moliyaviy tejamkorlik
- Yuqori tezlik va samaradorlik
- Texnik xizmat ko‘rsatishning soddaligi

Muammolari:

- Axborot xavfsizligi masalalari
- Internetga bog‘liqlik
- Ma’lumotlar maxfiyligi bilan bog‘liq xavflar

Shu sababli bulutli texnologiyalarni joriy etishda axborot xavfsizligiga alohida e’tibor qaratish lozim.

Xulosa qilib aytganda, kiberxavfsizlik zamonaviy IT tizimlarining ajralmas qismiga aylangan. Zamonaviy tahdidlar doimiy ravishda rivojlanib borayotganligi sababli texnik, tashkiliy va huquqiy himoya chora-tadbirlarini uyg‘un amalga oshirish muhimdir. Kiberxavfsizlikni ta’minlash orqali tashkilotlar va foydalanuvchilar ma’lumotlarining xavfsizligi, tizimlarning samaradorligi va ishonchliligi oshadi. Kelajakda sun’iy intellekt va Big Data texnologiyalari kiberxavfsizlikni yanada takomillashtirishda muhim rol o‘ynashi kutilmoqda.

Foydalanilgan adabiyotlar:

1. Tursunov S., Nazarov I. *Ta’limda axborot texnologiyalari.* – Toshkent: Adabiyot uchqunlari, 2019.
2. Isroilov B.S. Bulutli texnologiyalar va shaxsga doir ma’lumotlar himoyasi, Ustozlar Uchun jurnal.
3. Soibov N. Bulutli texnologiyalar orqali korxona buxgalteriya tizimini raqamlashtirish va samaradorlikka erishish, GREEN ECONOMY AND DEVELOPMENT jurnali.
4. Mamasoliyev A.A., Abdullayev S. Bulutli hisoblash xavfsizligi: muammolar va ularning yechimlari.
5. Fayzullayev J.M. Bulutli texnologiyalar, Central Asian Journal of Academic Research.
6. Mell, P., Grance, T. The NIST Definition of Cloud Computing. NIST Special Publication, 2011.
7. Armbrust, M., et al. A View of Cloud Computing. Communications of the ACM, 2010.
8. OECD. *Education and Digitalisation: OECD Digital Education Outlook 2021*. – Paris: OECD Publishing.
9. Mishra, S., & Panda, S. *Development and Access to Online Educational Resources.* – Commonwealth of Learning, 2017.
10. O‘zbekiston Respublikasi Prezidentining 2020-yil 28-oktabrdagi PQ–4884-son qarori: *2020–2023-yillarda raqamli iqtisodiyot va elektron hukumatni rivojlantirish konsepsiyasi.*