KIBERXAVFSIZLIK TUSHUNCHASI, MOHIYATI VA TA'LIM TIZIMIDAGI AHAMIYATI

Aslonov Jasur Sharifovich
Buxoro innovatsiyalar universiteti 2 – kurs magistranti.

https://doi.org/10.5281/zenodo.19200661

Annotatsiya. *Maqolada kiberxavfsizlik tushunchasining mohiyati, uning zamonaviy ta'lim tizimidagi ahamiyati va o'rni ilmiy tahlil qilingan. Kiberxavfsizlikning nazariy asoslari, asosiy tamoyillari va ta'lim muassasalarida axborot xavfsizligini ta'minlash zarurligi ko'rsatib berilgan. Xalqaro va milliy miqyosda ta'lim sohasida kiberxavfsizlikni ta'minlash bo'yicha zamonaviy yondashuvlar, kibertahdidlar tasnifi va ularning ta'lim jarayoniga ta'siri tahlil qilingan.*

Kalit so'zlar: *kiberxavfsizlik, axborot xavfsizligi, ta'lim tizimi, kibertahdid, ma'lumotlarni himoya qilish, raqamli ta'lim, axborot infratuzilmasi, shaxsiy ma'lumotlar, kiber madaniyat, xavfsizlik siyosati.*

Аннотация. *В статье научно проанализированы сущность понятия кибербезопасности, его значение и роль в современной системе образования.*

Рассмотрены теоретические основы кибербезопасности, основные принципы и необходимость обеспечения информационной безопасности в образовательных учреждениях. Проанализированы современные подходы к обеспечению кибербезопасности, классификация киберугроз и их влияние на образовательный процесс.

Ключевые слова: *кибербезопасность, информационная безопасность, система образования, киберугроза, защита данных, цифровое образование, информационная инфраструктура, персональные данные, киберкультура, политика безопасности.*

Annotation. *The article scientifically analyzes the essence of the concept of cybersecurity, its significance and role in the modern education system. The theoretical foundations of cybersecurity, basic principles and the necessity of ensuring information security in educational institutions are examined. Modern approaches to ensuring cybersecurity in education, classification of cyber threats and their impact on the educational process are analyzed.*

Key words: *cybersecurity, information security, education system, cyber threat, data protection, digital education, information infrastructure, personal data, cyber culture, security policy.*

Zamonaviy dunyoda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi va raqamli transformatsiyaning kengayishi ta'lim tizimini tubdan o'zgartirmoqda. Onlayn ta'lim platformalari, masofaviy o'qitish tizimlari, bulutli texnologiyalar va sun'iy intellekt vositalari ta'lim jarayonining ajralmas qismiga aylanmoqda. Biroq, raqamlashuv jarayoni bilan bir qatorda kibertahdidlar ham keskin ortib, ta'lim muassasalari kiberxujumlarning asosiy nishonlaridan biriga aylanmoqda. IBM Security hisobotiga ko'ra, 2023-yilda ta'lim sohasiga qarshi kiberxujumlar soni 44 foizga oshgan va bir insidentning o'rtacha zarar miqdori 3,65 million AQSh dollarini tashkil etgan [1]. Ushbu maqolada kiberxavfsizlik tushunchasining mohiyati, uning ta'lim tizimidagi ahamiyati va zamonaviy yondashuvlar ilmiy tahlil qilinadi.

Kiberxavfsizlik tushunchasi XX asr oxirida shakllangan bo'lib, dastlab harbiy va davlat sohasida qo'llanilgan, keyinchalik esa barcha tarmoqlarga, jumladan ta'lim sohasiga ham keng tarqalgan.

Xalqaro Telekommunikatsiya ittifoqi (ITU) kiberxavfsizlikni “kibermuhitda tashkilotlar va foydalanuvchilar mulkini himoya qilish uchun qo‘llanilishi mumkin bo‘lgan vositalar, siyosatlar, xavfsizlik konsepsiyalari, xavfsizlik kafolatlari, yo‘riqnomalar, risklarni boshqarish yondashuvlari, harakatlar, treninglar, eng yaxshi amaliyotlar, sug‘urta va texnologiyalar majmui” sifatida ta’rif etgan [2]. Bu keng qamrovli ta’rif kiberxavfsizlikning nafaqat texnik, balki tashkiliy, huquqiy va insoniy jihatlarini ham o‘z ichiga olishini ko‘rsatadi.

Uilyam Stallings axborot xavfsizligining uchta asosiy tamoyilini – maxfiylik (confidentiality), yaxlitlik (integrity) va foydalanish imkoniyati (availability) – CIA triada sifatida ishlab chiqqan va bu tamoyillar kiberxavfsizlikning nazariy asosini tashkil etgan [3].

Maxfiylik ma’lumotlarning faqat vakolatli shaxslar tomonidan ko‘rilishini, yaxlitlik ma’lumotlarning ruxsatsiz o‘zgartirilmasligini, foydalanish imkoniyati esa ma’lumot va tizimlarga zarur paytda kirishning ta’minlanishini anglatadi. Ta’lim kontekstida bu tamoyillar talabalar va o‘qituvchilarning shaxsiy ma’lumotlari, baholash natijalari, ilmiy tadqiqot ma’lumotlari va ta’lim muassasasining boshqaruv axborotining xavfsizligini ta’minlashda namoyon bo‘ladi.

Ross Anderson axborot xavfsizligi muhandisligi sohasida fundamental tadqiqotlar olib borib, xavfsizlik tizimlarining texnik va insoniy omillarining o‘zaro ta‘sirini chuqur o‘rganilishi zarurligini asoslab bergan [4]. Andersonning fikricha, ko‘pchilik xavfsizlik buzilishlari texnik zaifliklar emas, balki inson omili – foydalanuvchilarning bilim va ko‘nikmalar yetishmasligi, ijtimoiy muhandislik hujumlari va xavfsizlik siyosatiga rioya qilmaslik tufayli sodir bo‘ladi.

Ta’lim muassasalarida bu muammo ayniqsa dolzarb, chunki talabalar va o‘qituvchilarning kiberxavfsizlik bo‘yicha bilim darajasi ko‘pincha yetarli emas va ular fishing, zararli dasturlar va ijtimoiy muhandislik hujumlariga oson nishon bo‘lishi mumkin.

Bryus Shnaier kriptografiya va kompyuter xavfsizligi sohasidagi yetakchi mutaxassis sifatida xavfsizlikni faqat texnologiya emas, balki jarayon sifatida tushunish zarurligini ta‘kidlagan [5]. Shnaierning fikricha, hech qanday texnologik yechim yolg‘iz o‘zi to‘liq xavfsizlikni ta’minlay olmaydi – samarali kiberxavfsizlik texnologiya, siyosat va odamlarning uyg‘un birlashuvini talab etadi. Bu yondashuv ta’lim sohasida ayniqsa muhim, chunki ta’lim muassasalari minglab foydalanuvchilarga (talabalar, o‘qituvchilar, ma’muriyat, texnik xodimlar) xizmat ko‘rsatadi va ularning har birining xavfsizlik xulq-atvori butun tizimning xavfsizligiga ta‘sir ko‘rsatadi.

Ta’lim tizimida kiberxavfsizlikning ahamiyati bir necha muhim jihatda namoyon bo‘ladi.

Birinchidan, ta’lim muassasalari katta hajmdagi shaxsiy ma’lumotlarni – talabalar va xodimlarning shaxsiy identifikatsiya ma’lumotlari, moliyaviy ma’lumotlar, akademik natijalar, tibbiy ma’lumotlar – saqlaydi va qayta ishlaydi. Bu ma’lumotlarning sizib chiqishi jiddiy huquqiy va moliyaviy oqibatlarga olib kelishi mumkin. Ikkinchidan, ta’lim jarayonining uzluksizligi – kiberxujum natijasida ta’lim platformalari ishdan chiqishi minglab talabalarning o‘quv jarayonini to‘xtatib qo‘yishi mumkin. Uchinchidan, ilmiy tadqiqot ma’lumotlarining xavfsizligi – universitetlarda olib borilayotgan ilmiy tadqiqot natijalari, patentlar va intellektual mulk axborotining himoya qilinishi zarur.

Kibertahdidlarning ta’lim sohasidagi ko‘rinishlari turli-tuman bo‘lib, ularni bir necha asosiy guruhga bo‘lish mumkin. Fishing hujumlari – talabalar va o‘qituvchilarga soxta elektron xatlar yuborib, ularning login va parol ma’lumotlarini o‘g‘irlash eng keng tarqalgan tahdid turi hisoblanadi. Verizon kompaniyasining ma’lumotlariga ko‘ra, ta’lim sohasidagi xavfsizlik buzilishlarining 36 foizi fishing hujumlari orqali amalga oshirilgan [6].

Ransomware (to‘lov dasturlari) hujumlari ta’lim muassasalarining ma’lumotlarini shifrlash va fidya talab qilish orqali jiddiy zarar yetkazmoqda. DDoS (taqsimlangan xizmat ko‘rsatishni rad etish) hujumlari ta’lim platformalari va veb-saytlarni ishdan chiqarish orqali ta’lim jarayonini to‘xtatishi mumkin.

Raqamli ta’limning kengayishi kiberxavfsizlik muammolarini yanada murakkablashtirdi.

COVID-19 pandemiyasi davrida masofaviy ta’limga tezkor o‘tish ko‘plab ta’lim muassasalari uchun kiberxavfsizlik bo‘yicha yetarli tayyorgarlik ko‘rilmagan holda amalga oshirildi. Zoom, Google Meet va Microsoft Teams kabi video konferensiya platformalarining keng qo‘llanilishi yangi xavfsizlik muammolarini keltirib chiqardi – “Zoombombing” hodisalari, ruxsatsiz kirishlar va ma’lumot sizilishlari qayd etildi. Keyingi davrda gibrid va onlayn ta’lim modellari barqarorlashib, bu platformalarga bog‘liqlik oshdi, bu esa kiberxavfsizlikni ta’minlashning zaruriyatini yanada oshirdi.

Ta’lim muassasalarida kiberxavfsizlikni ta’minlash bir qator o‘ziga xos qiyinchiliklarga ega. Birinchidan, ta’lim muassasalari “ochiq tizim” tamoyiliga asoslangan – ular bilim va ma’lumot almashishni rag‘batlantiradi, bu esa kiberxavfsizlik talablari bilan ziddiyat yaratishi mumkin. Ikkinchidan, foydalanuvchilarning katta soni va ularning texnik bilim darajasining turlichaligi xavfsizlik siyosatini amalga oshirishni qiyinlashtiradi. Uchinchidan, ta’lim muassasalarining byudjeti ko‘pincha cheklangan bo‘lib, kiberxavfsizlikka ajratiladigan mablag‘lar moliyaviy va tijorat sektoriga nisbatan kam. To‘rtinchidan, BYOD (Bring Your Own Device) siyosati – talabalar va o‘qituvchilarning shaxsiy qurilmalaridan foydalanishi tarmoq xavfsizligini ta’minlashni murakkablashtiradi.

NIST (AQSh Milliy standartlar va texnologiyalar instituti) kiberxavfsizlik doiraviy modelini (Cybersecurity Framework) ishlab chiqqan bo‘lib, u beshta asosiy funktsiyadan iborat: aniqlash (Identify), himoya qilish (Protect), aniqlash (Detect), javob berish (Respond) va tiklash (Recover) [7]. Bu model ta’lim muassasalari uchun ham samarali qo‘llanilishi mumkin. Aniqlash bosqichida ta’lim muassasasining axborot aktivlari va ularning xavfsizlik darajasi aniqlanadi.

Himoya qilish bosqichida kirish nazorati, ma’lumotlarni shifrlash va xodimlarni o‘qitish amalga oshiriladi. Kiberxujumlarni aniqlash, ularga tezkor javob berish va tizimni tiklash qolgan bosqichlarning vazifasi hisoblanadi.

Ta’limda kiberxavfsizlik madaniyatini shakllantirish texnik chora-tadbirlar bilan bir qatorda muhim ahamiyatga ega. Kiberxavfsizlik madaniyati ta’lim ishtirokchilarining xavfsizlik bo‘yicha bilim, ko‘nikma va xulq-atvor me’yorlarining yig‘indisi sifatida ta‘riflanadi. Yon van Niekerk va Rossou von Solms kiberxavfsizlik madaniyatini tashkiliy madaniyatning ajralmas qismi sifatida ko‘rib chiqib, uni texnik, tashkiliy va insoniy o‘lchamlarda shakllantirish zarurligini asoslaganlar [8]. Ta’lim muassasalarida kiberxavfsizlik madaniyatini shakllantirish uchun muntazam treninglar, simulyatsiya mashqlari, axborot kampaniyalari va gamifikatsiya vositalari qo‘llaniladi.

O‘zbekistonda ta’lim sohasida kiberxavfsizlikni ta’minlash masalasi so‘nggi yillarda dolzarb bo‘lib bormoqda. Mamlakatda “Kiberxavfsizlik to‘g‘risida”gi Qonun (2022) qabul qilinib, axborot tizimlarini himoya qilishning huquqiy asoslari belgilangan. Ta’lim muassasalarida Hemis, Moodle va boshqa raqamli platformalar keng joriy etilishi bilan bir qatorda, bu tizimlarning xavfsizligini ta‘minlash zarurligi ham ortmoqda. Biroq, ta’lim muassasalarida kiberxavfsizlik bo‘yicha mutaxassislarning yetishmasligi, byudjet cheklovlari va foydalanuvchilarning kiberxavfsizlik bilim darajasining pastligi asosiy muammolar sifatida qaralmoqda.

Xalqaro miqyosda ta’limda kiberxavfsizlikni ta’minlash bo‘yicha bir qator samarali modellar ishlab chiqilgan. Yevropa Ittifoqining ENISA (Yevropa Tarmoq va Axborot Xavfsizligi agentligi) ta’lim muassasalari uchun maxsus kiberxavfsizlik yo‘riqnomalari ishlab chiqqan. AQShda EDUCAUSE tashkiloti oliy ta’lim muassasalari uchun kiberxavfsizlik dasturini (Higher Education Information Security Council) amalga oshirmoqda. Buyuk Britaniyada National Cyber Security Centre ta’lim sohasida kiberxavfsizlikni oshirish bo‘yicha maxsus dastur yuritmoqda [9]. Bu tajribalar O‘zbekiston ta’lim tizimida kiberxavfsizlikni ta’minlash strategiyasini ishlab chiqishda muhim manba bo‘lishi mumkin.

Shaxsiy ma’lumotlarni himoya qilish ta’limda kiberxavfsizlikning eng muhim jihatlaridan biri hisoblanadi. Ta’lim muassasalari talabalarning to‘liq ismi, tug‘ilgan sanasi, yashash manzili, telefon raqami, elektron pochta, bank rekvizitlari, akademik natijalari va ba‘zan tibbiy ma’lumotlarini saqlaydi. AQShda FERPA (Family Educational Rights and Privacy Act), Yevropa Ittifoqida GDPR (General Data Protection Regulation) kabi qonunlar ta’lim sohasida shaxsiy ma’lumotlarni himoya qilishning huquqiy asosini tashkil etadi [10]. O‘zbekistonda ham “Shaxsiy ma’lumotlar to‘g‘risida”gi Qonun qabul qilingan bo‘lib, ta’lim muassasalari bu qonun talablariga to‘liq rioya qilishi zarur.

Sun’iy intellekt va mashinali o‘rganish texnologiyalari kiberxavfsizlik sohasida yangi imkoniyatlar ochmoqda. AI-asosidagi xavfsizlik tizimlari anomal xatti-harakatlarni aniqlash, kibertahdidlarni bashorat qilish va avtomatik javob berish imkoniyatiga ega. Biroq, shu bilan birga, sun’iy intellekt kiberjinoyatchilar tomonidan ham qo‘llanilmoqda – deepfake texnologiyalari, AI-asosidagi fishing hujumlari va avtomatlashtirilgan zaifliklarni qidirish vositalari yangi tahdidlarni keltirib chiqarmoqda. Ta’lim muassasalari uchun AI-asosidagi xavfsizlik yechimlarini joriy etish bilan bir qatorda, AI xavflarini ham hisobga olish zarur.

Xulosa va Takliflar:

Kiberxavfsizlik zamonaviy ta’lim tizimining ajralmas va muhim komponenti bo‘lib, uning ahamiyati raqamli transformatsiyaning chuqurlashuvi bilan tobora ortmoqda. W.Stallings, R.Anderson, B.Schneier kabi olimlarning nazariy yondashuvlari va NIST, ITU, ENISA kabi xalqaro tashkilotlarning standartlari kiberxavfsizlikning nazariy-metodologik asoslarini tashkil etadi. Ta’lim muassasalari uchun kiberxavfsizlikni ta’minlash nafaqat texnik chora-tadbirlar, balki kiberxavfsizlik madaniyatini shakllantirish, huquqiy bazani mustahkamlash va barcha ta’lim ishtirokchilarining bilim va ko‘nikmalarini oshirishni talab etadi. O‘zbekiston ta’lim tizimida kiberxavfsizlikni ta’minlash bo‘yicha kompleks strategiyani ishlab chiqish va amalga oshirish bugungi kunning eng dolzarb vazifalaridan biri hisoblanadi.

Foydalanilgan adabiyotlar

1. IBM Security. Cost of a Data Breach Report 2023. – Armonk: IBM Corporation, 2023. – 78 p.
2. International Telecommunication Union. Global Cybersecurity Agenda. – Geneva: ITU, 2020. – 48 p.
3. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – London: Pearson, 2020. – 768 p.
4. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – 3rd ed. – Indianapolis: Wiley, 2020. – 1232 p.
5. Schneier B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. – New York: W.W. Norton, 2018. – 288 p.

6. Verizon. Data Breach Investigations Report 2023. – New York: Verizon, 2023. – 89 p.
7. NIST. Cybersecurity Framework Version 2.0. – Gaithersburg: NIST, 2024. – 32 p.
8. Van Niekerk J., Von Solms R. Information Security Culture: A Management Perspective // Computers & Security. – 2010. – Vol. 29, No. 4. – P. 476–486.
9. National Cyber Security Centre. Cyber Security for Schools. – London: NCSC, 2023. – 24 p.
10. European Union. General Data Protection Regulation (GDPR). – Brussels: EU, 2016.