INNOVATIVE PUBLICATION
Journal of Effective Learning and Sustainable Innovation
Vol.4 №5 (2026). MAY
innovativepublication.uz

KIBERXAVFSIZLIK ASOSLARINI O‘QITISH

Shermetov Bunyod Ozodovich
Qo‘shko‘pir tuman 4-son texnikumi
Bunyodshermetov917@gmail.com

Annotatsiya: Bugungi raqamli evolyutsiya sharoitida oliy ta’lim muassasalari katta hajmdagi kritik ma’lumotlarni boshqarishi sababli kiberhujumlarning asosiy nishoniga aylanmoqda. Tadqiqotlar shuni ko‘rsatadiki, aksariyat kiberhodisalar texnik nosozliklardan ko‘ra ko‘proq inson omili, ijtimoiy muhandislik va foydalanuvchilarning yetarli darajada bilimga ega emasligi oqibatida yuzaga kelmoqda. Mazkur maqolada kiberxavfsizlik asoslarini o‘qitishning dolzarb muammolari va ularning yechimlari tizimli ravishda tahlil qilinadi. Tadqiqot doirasida talabalar va xodimlarning kiber-xabardorligini oshirishga qaratilgan konseptual o‘qitish asosi (Framework) taklif etiladi. Shuningdek, maqolada ta’lim jarayonida foydalanuvchilarning o‘quv metodikasini qabul qilishiga ta’sir etuvchi psixologik omillar – ishonch, xavotir va apatiya kabi ko‘rsatkichlarning o‘rni ko‘rib chiqiladi. Natijalar OTMlarda kiberxavfsizlik madaniyatini shakllantirish va zamonaviy tahdidlarga qarshi barqaror ta’lim tizimini yaratish bo‘yicha amaliy tavsiyalar beradi.
Kalit so‘zlar: kiberxavfsizlik ta’limi, oliy ta’lim, kiber-xabardorlik, inson omili, o‘qitish metodikasi, kiber-madaniyat, konseptual model.

Kirish. Bugungi shiddatli texnologik evolyutsiya davrida raqamli transformatsiya jarayoni nafaqat sanoat korxonalari, balki oliy ta’lim muassasalari uchun ham ixtiyoriy tanlovdan strategik zaruriyatga aylandi. Global miqyosda raqamli infratuzilmaga yo‘naltirilgan xarajatlarning 2026-yilga kelib 3,4 trillion dollarga yetishi kutilayotgan bir paytda, kiberjinoyatchilikning ham xuddi shunday sur’atda o‘sib borayotgani, xususan, kiberjinoyatlar keltiradigan zarar miqdori 11,36 trillion dollarga yetishi prognoz qilinayotgani jiddiy xavotir uyg‘otmoqda. Oliy ta’lim sektori katta hajmdagi intellektual mulk, ilmiy tadqiqotlar va shaxsiy ma’lumotlarni o‘zida jamlaganligi sababli kiberhujumchilar uchun eng jozibador yo‘nalishlardan biriga aylanib ulgurdi; xususan, so‘nggi yillarda ta’lim muassasalariga qilingan zararli dasturlar hujumi o‘tgan davrlarga nisbatan 157 foizga oshganligi ushbu sohaning zaifligini ko‘rsatadi[1,2]. Ushbu muammoning tub ildizi ko‘p hollarda texnik himoya tizimlarining yetishmasligida emas, balki kiber-tahdidlarning 80 foizidan ortig‘iga sabab bo‘layotgan inson omili – foydalanuvchilarning kiberxavfsizlik asoslari bo‘yicha

yetarli darajada bilim va ko‘nikmaga ega emasligida yotadi. OTMlarda foydalanuvchilar oqimining doimiy yangilanib turishi va fishing yoki ijtimoiy muhandislik kabi murakkab hujum vektorlarining ko‘payishi uzluksiz o‘qitish tizimini yaratishni taqozo etadi. Garchi NIST, ISO va CIS kabi xalqaro standartlar kiber-xabardorlikni oshirish bo‘yicha umumiy yo‘riqnomalarni taqdim etsa-da, ular oliy ta’limning o‘ziga xos dinamik muhitiga, talaba va professor-o‘qituvchilarning individual ehtiyojlariga to‘liq moslashtirilmagan [3, 4]. Shu sababli, foydalanuvchilarning xulq-atvoriga ta’sir etuvchi psixologik omillarni, jumladan, apatiya, ishonch va xavotir kabi ko‘rsatkichlarni hisobga oluvchi, kiberxavfsizlik asoslarini o‘qitishning moslashtirilgan konseptual modelini ishlab chiqish bugungi kunning eng dolzarb vazifalaridan biri hisoblanadi. Mazkur tadqiqot oliy ta’lim muassasalarida kiberxavfsizlik madaniyatini shakllantirish va foydalanuvchilarning kiber-savodxonligini tizimli ravishda oshirish orqali institutsional xavfsizlik darajasini mustahkamlashga qaratilgan metodologik yechimlarni taklif etadi.

Metodlar. Ushbu tadqiqotda oliy ta’lim muassasalari uchun kiberxavfsizlik asoslarini o‘qitish metodikasini ishlab chiqishda deduktiv yondashuvdan foydalanildi. Mazkur metodologiya mavjud kiberxavfsizlik nazariyalari va xalqaro standartlarni tahlil qilish orqali ta’lim sohasiga xos bo‘lgan xususiy yechimlarni shakllantirish imkonini beradi. Tadqiqotning metodologik asosi sifatida kiberhujumlar dinamikasini aks ettiruvchi miqdoriy (quantitative) ma’lumotlar hamda xalqaro xavfsizlik ramkalari va avvalgi ilmiy ishlar natijalaridan olingan sifatli (qualitative) ma’lumotlar tahlili tanlab olindi. Tadqiqot strategiyasi ikki bosqichli arxiv tahlili va qiyosiy o‘rganishga tayanadi [5].

Dastlabki bosqichda Statista, IBM, Deloitte va Verizon kabi nufuzli tashkilotlarning 2018–2026 yillardagi yillik hisobotlari o‘rganilib, oliy ta’lim sohasidagi kiber-tahdidlar, fishing hujumlari va ma’lumotlarning sizib chiqish tendentsiyalari tahlil qilindi. Bu oliy ta’lim sektori uchun maxsus moslashtirilgan o‘qitish metodikasiga bo‘lgan ehtiyojni statistik jihatdan asoslashga xizmat qildi. Tadqiqotda "Oliy ta’limda kiberxavfsizlik", "Kiber-xabardorlik tizimlari", "Akademik muassasalarda inson omili" kabi kalit so‘zlar yordamida qidiruv ishlari olib borildi [6,7].

Ikkinchi bosqichda kiberxavfsizlik bo‘yicha global standartlar hisoblangan NIST SP 800-50, ISO/IEC 27001 va 27002, shuningdek, COBIT 19 tizimlari qiyosiy tahlil qilindi. Bunda asosiy e’tibor ushbu standartlarning foydalanuvchi xabardorligini oshirish va o‘qitish jarayonlariga oid qismlariga qaratildi. Mazkur ramkalarning umumiy tavsiyalari oliy ta’lim muassasalarining dinamik muhitiga, xususan, talabalar, professor-o‘qituvchilar va ma’muriy xodimlarning individual profillariga moslashtirildi. Tadqiqot natijalari Science Direct, Research Gate va Elsevier kabi ilmiy

ma’lumotlar bazalaridagi avvalgi tadqiqotlar bilan solishtirilib, o‘qitish samaradorligiga ta’sir etuvchi psixologik va texnik omillar umumlashtirildi. Olingan ma’lumotlar asosida oliy ta’lim muassasalari uchun doimiy takomillashib boruvchi, mosuvchan kiberxavfsizlik o‘qitish tizimi (Framework) shakllantirildi [8,9].

Kiberxavfsizlik xabardorligi va o‘qitish tizimi (CA&TF)

Kiberxavfsizlik xabardorligi va o‘qitish tizimi (CA&TF) o‘zaro uzviy bog‘liq bo‘lgan uchta asosiy blokdan tashkil topadi. Ushbu tizim kiberxavfsizlik asoslarini shunchaki nazariy bilim sifatida emas, balki kundalik raqamli madaniyatning ajralmas qismi sifatida o‘qitishni ko‘zda tutadi.

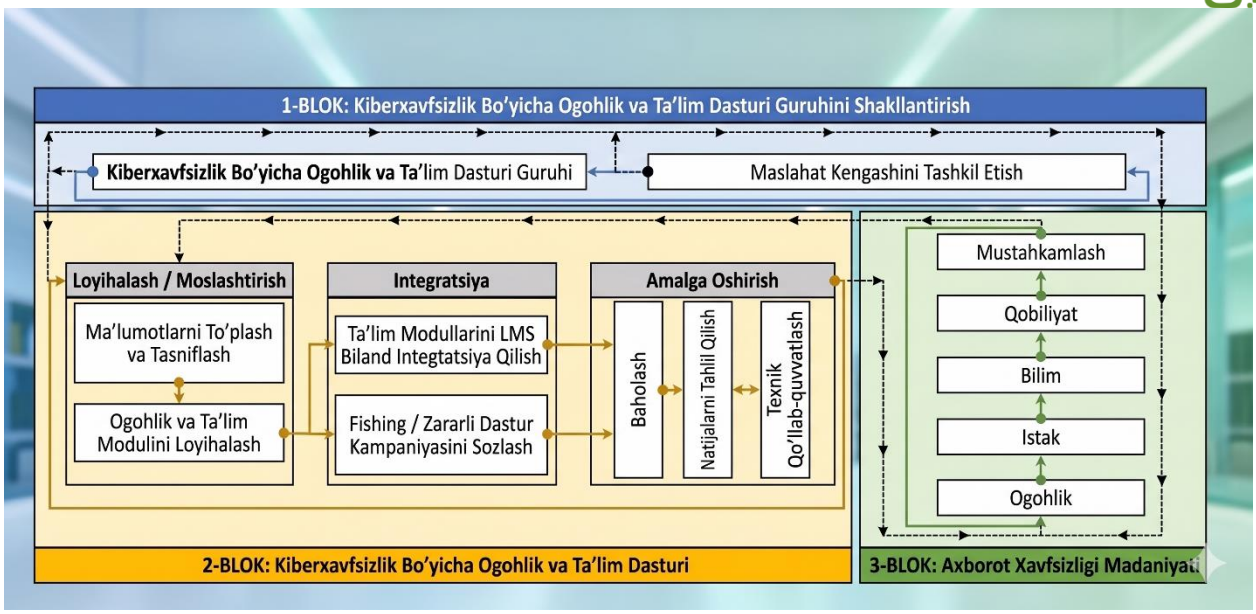
Birinchi blok dasturning poydevorini yaratishga yo‘naltirilgan bo‘lib, u kiberxavfsizlik bo‘yicha o‘qitish va xabardorlik dasturini (CA&TP) boshqaruvchi ishchi guruhni shakllantirishni o‘z ichiga oladi. Bu bosqichda asosiy e’tibor tashkilotning strategik maqsadlarini tahlil qilish va dasturga jalb qilinadigan asosiy manfaatdor tomonlarni aniqlashga qaratiladi. Bu, o‘z navbatida, o‘qitish jarayonini muassasaning ichki tartib-qoidalari va funksional ehtiyojlariga to‘liq moslashtirish imkonini beradi [10, 11].

Ikkinchi blok kiberxavfsizlik asoslarini o‘qitish dasturini bevosita loyihalash, integratsiya qilish va amaliyotga tatbiq etish bosqichidir. Bu blok doirasida foydalanuvchilarning turli profillari uchun shaxsiylashtirilgan o‘quv modullari yaratiladi. Mazkur modullar kiber-gigiyena, ijtimoiy muhandislikdan himoyalanish va ma’lumotlarni xavfsiz boshqarish kabi fundamental mavzularni o‘z ichiga oladi. Dasturning integratsiyasi o‘quv jarayoniga zamonaviy texnologiyalarni, xususan, simulyatsiyalar va interaktiv baholash tizimlarini joriy etish orqali amalga oshiriladi [12].

Uchinchi blok axborot xavfsizligi madaniyatini shakllantirishga qaratilgan. Bu bosqichda o‘qitish jarayoni faqat darslar bilan cheklanib qolmay, balki foydalanuvchilarni doimiy ogohlikda ushlab turuvchi qo‘shimcha tadbirlar, jumladan, seminarlar va amaliy kiber-mashqlar orqali boyitiladi. Ushbu blokning o‘ziga xosligi shundaki, u kiberxavfsizlik bilimlarini tor doiradan tashqariga olib chiqadi va mutaxassislarni kelgusi ish muhitidagi kiber-tahdidlarga tayyorlaydi. Natijada, foydalanuvchilar nafaqat o‘z bilimlarini amalda qo‘llaydilar, balki kiber-madaniyat tashuvchisi sifatida uni boshqa muassasa va sohalarga ham yoyadilar [13, 14].

Tizimning ushbu uch blokli sxemasi avvalgi tadqiqotlar va xalqaro kiberxavfsizlik ramkalarining zamonaviy axborot muhitiga moslashtirilgan integratsiyalashgan talqini hisoblanadi.

INNOVATIVE PUBLICATION
Journal of Effective Learning and Sustainable Innovation
Vol.4 №5 (2026). MAY
innovativepublication.uz



1-rasm. Kiberxavfsizlik xabardorligi va o'qitish tizimining (CA&TF for HEIs) yuqori darajadagi sxemasi.

Kiberxavfsizlik asoslarini o‘qitish dasturi faqat texnik mutaxassislar tomonidan boshqarilishi yetarli emas. Dasturni turli guruhlar (foydalanuvchilar, ma’murlar, rahbarlar) ehtiyojlariga moslashtirish uchun maslahat kengashini tashkil etish tavsiya etiladi. Ushbu kengash tarkibiga tashkilotning turli bo‘limlaridan vakillar kiritilishi maqsadga muvofiq [15, 16].

Maslahat kengashining asosiy vazifalari quyidagilardan iborat:

Auditoriya tahlili: Turli guruhlarning bilim darajasi va ehtiyojlarini aniqlash.

Dasturni moslashtirish: O‘quv modullarini har bir sohaga mos ravishda tahrirlash bo‘yicha takliflar berish.

Aloqa va hamkorlik: O‘qitish jarayonini barcha bo‘limlar o‘rtasida ommalashtirish va foydalanuvchilar bilan samarali qayta aloqani o‘rnatish.

Maslahat kengashi a’zolarining o‘z tajribalari va muassasaning o‘ziga xos xususiyatlaridan kelib chiqib qo‘shadigan hissalari o‘qitishning umumiy sifatini oshirishga xizmat qiladi.

Kiberxavfsizlik asoslarini o‘qitish tizimining ikkinchi bloki dasturni bevosita loyihalash, tizimga integratsiya qilish va amaliyotga tatbiq etish jarayonlarini o‘z ichiga oladi. Ushbu blokning samaradorligi, birinchi navbatda, "Loyihalash va Moslashtirish" bosqichida ma’lumotlarning qanchalik to‘g‘ri tasniflanishiga bog‘liqdir. Dastur doirasida auditoriya guruhlari ularning tizimdagi roli, vakolatlari va axborot bilan ishlash darajasiga ko‘ra tabaqalashtiriladi. Xususan, asosiy guruhlar sifatida talabalar, professor-o‘qituvchilar, ma’muriy xodimlar, rahbariyat hamda IT va

xavfsizlik bo‘limi mutaxassislari ajratib ko‘rsatiladi. Har bir guruhning ehtiyojlarini aniqlashda ularning kundalik faoliyatidagi risk darajasi asosiy mezon hisoblanadi [17]. Masalan, kiberxavfsizlik asoslarini o‘qitishda talabalar uchun ko‘proq kiber-gigiyena va ijtimoiy muhandislikdan himoyalanish mavzulari dolzarb bo‘lsa, moliya yoki ma’muriy bo‘lim xodimlari uchun ma’lumotlarning maxfiyligi va imtiyozli kirish huquqlarini boshqarish bo‘yicha chuqurlashtirilgan modullar talab etiladi. Bunday yondashuv o‘quv dasturini shunchaki umumiy nazariy bilimlar to‘plamidan har bir foydalanuvchi profiliga moslashtirilgan amaliy ko‘nikmalar tizimiga aylantiradi. Dasturni loyihalashda o‘rnatilgan maqsadlar va o‘lchanadigan metrikalar o‘qitish samaradorligini monitoring qilib borish imkonini beradi [18].

Loyihalashdan so‘ng integratsiya bosqichida ushbu modullar mavjud ta’lim platformalari (LMS) bilan muvofiqlashtiriladi va amaliy mashqlar, jumladan, fishing simulyatsiyalari bilan boyitiladi. Yakuniy amalga oshirish bosqichi esa bilimni baholash, natijalarni tahlil qilish va foydalanuvchilarga doimiy texnik yordam ko‘rsatish orqali kiberxavfsizlik ko‘nikmalarini mustahkamlaydi. Bu jarayon NIST va ISO kabi xalqaro standartlarning talablariga mos ravishda, foydalanuvchilarning bilim darajasini uzluksiz oshirib borishni ta’minlaydi.

Kiberxavfsizlikni o‘qitish faqat texnik choralar bilan cheklanib qolmay, balki dastur jamoasini shakllantirish, o‘quv modullarini loyihalash va axborot xavfsizligi madaniyatini rivojlantirishni qamrab oluvchi uch blokli yaxlit tizimga asoslanishi lozim. Kiber-tahdidlarning 80% dan ortig‘iga sabab bo‘layotgan inson omili, ya'ni foydalanuvchilarning kiberxavfsizlik asoslari bo‘yicha yetarli bilimga ega emasligi, o‘qitish metodikasini shaxsiylashtirish zaruriyatini keltirib chiqaradi. O‘qitish samaradorligini oshirish uchun foydalanuvchilar ularning tashkilotdagi roli va risk darajasiga ko‘ra talabalar, professor-o‘qituvchilar va ma’murlar kabi guruhlarga ajratilishi, o‘quv modullari esa har bir guruhning ehtiyojlariga moslashtirilishi zarur. Kiberxavfsizlik madaniyati xabardorlik, istak, bilim, qobiliyat va mustahkamlash bosqichlaridan iborat model asosida bosqichma-bosqich shakllantirilib, doimiy o‘quv sikli va amaliy mashqlar orqali mustahkamlab borilishi strategik ahamiyatga ega. Mazkur yondashuv nafaqat foydalanuvchilarning kiber-savodxonligini oshiradi, balki muassasaning kiber-tahdidlarga qarshi umumiy chidamliligini ta’minlovchi institutsional muhitni yaratadi.

Foydalanilgan adabiyotlar ro‘yxati

[1] Statista Research Department, "Spending on digital transformation technologies and services worldwide from 2017 to 2026 (in trillion U.S. dollars)," Statista, Hamburg, Germany, 2022.

[2] Statista Research Department, "Global annual growth rate of spending on cyber security from 2019 to 2026, by industry sector," Statista, Hamburg, Germany, 2023.
[3] IBM Security, *X-Force Threat Intelligence Index 2023*, Armonk, NY, USA: IBM, 2023, p. 42.
[4] K. Amorosa and B. Yankson, "Human error—A critical contributing factor to the rise in data breaches: A case study of higher education," *Holistica J. Bus. Public Adm.*, vol. 14, pp. 110–132, 2023.
[5] R. Armas, *Information Security Awareness in Higher Education: The Need for a Tailor-Made Suit*, Agadir, Morocco: C2SA, 2023.
[6] N. Ben-Asher and C. Gonzalez, *Effects of Cyber Security Knowledge on Attack Detection*, Amsterdam, The Netherlands: Elsevier, 2015, pp. 51–61.
[7] N. Ikram, N. Ikram, H. Murtaza, and M. Javed, "Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's model," *Comput. Secur.*, vol. 125, p. 103049, 2023.
[8] J. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 39, 2021.
[9] IBM Security, *Cost of a Data Breach Report 2023*, Armonk, NY, USA: IBM, 2023, p. 20.
[10] SonicWall, *2023 SonicWall Cyber Threat Report*, San Jose, CA, USA: SonicWall, 2023.
[11] Microsoft Security Intelligence, "Global threat activity," Microsoft, Redmond, WA, USA, 2023.
[12] CheckPoint, "Check Point press releases," Tel Aviv-Yafo, Israel, 2023. [Online]. Available: https://www.checkpoint.com/press/2022/check-point-softwares-2022-security-report-global-cyber-pandemics-magnitude-revealed/. [Accessed: Aug. 8, 2022].
[13] A. Arina, "Cyber security strategies for higher education institutions," *J. Eng. Sci.*, vol. 23, pp. 72–92, 2021.
[14] F. Astudillo, F. Astudillo-Salinas, L. Tello-Oquendo, F. Sanchez, and G. Lopez-Fonseca, "Information security management frameworks and strategies in higher education institutions: A systematic review," *Ann. Telecommun.*, vol. 76, pp. 255–270, 2021.
[15] EDUCAUSE, "Cybersecurity and privacy guide," Louisville, CO, USA, 2023. [Online]. Available: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/security-policies. [Accessed: July 16, 2023].

[16] J. Hash and M. Wilson, "Building an information technology security awareness and training program," NIST, Gaithersburg, MD, USA, Special Publication 800-50, 2003.

[17] P. Klein and P. Toth, "A role-based model for federal information technology/cybersecurity training," NIST, Gaithersburg, MD, USA, Special Publication 800-16, 2014.

[18] *Information Technology—Security Techniques—Information Security Management Systems—Requirements*, ISO/IEC Standard 27001, 2013.