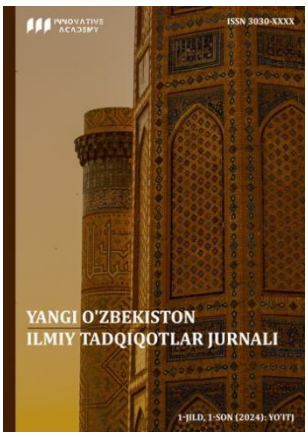

AXBOROT XAVFSIZLIGI FANINI O‘QITISHDA INNOVATSIYALAR VA ILG‘OR XORIJIY TAJRIBALAR

Qudratov Alijon Normamatovich
Guliston davlat universiteti
katta o‘qituvchi, +998975671163
a.n.qudratov@qmail.com
Bahodirov Muzrob Doniyor o‘g‘li
Guliston davlat universiteti
o‘qituvchi, +998911029292
e-mail: muzrobbakhodirov@gmail.com
https://doi.org/10.5281/zenodo.15429645

ARTICLE INFO
Qabul qilindi:26-aprel 2025 yil
Ma’qullandi:30-aprel 2025 yil
Nashr qilindi: 16-may 2025 yil
KEY WORDS
Axborot xavfsizligi, innovatsion ta’lim, virtual laboratoriya, gamifikatsiya, xorijiy tajriba, kiberta’lim, simulyator.

ABSTRACT
Ushbu maqolada axborot xavfsizligi fanini zamonaviy ta’lim jarayoniga innovatsion yondashuvlar asosida integratsiya qilish masalalari keng yoritilgan. Bugungi kunda axborot xavfsizligi sohasidagi bilim va ko‘nikmalar nafaqat IT sohasidagi mutaxassislar uchun, balki barcha soha vakillari uchun ham zaruratga aylanib bormoqda. Ayniqsa, raqamli iqtisodiyot va elektron boshqaruv tizimlarining rivojlanishi fonida axborotning ishonchli va xavfsiz muhitda saqlanishi ta’lim tizimida bu fanni chuqurlashtirib, amaliy yo‘nalishda o‘rgatishni talab etmoqda. Shu sababli, an’anaviy ta’lim metodlaridan innovatsion va texnologik yondashuvlarga o‘tish zarurati yuzaga kelmoqda.

Har bir jamiyatning kelajagi, uning ajralmas qismi bo‘lgan ta’lim tizimining qay darajada rivojlanganligi bilan belgilanadi. Bugungi kunda mustaqil taraqqiyot yo‘lidan borayotgan mamlakatimizning uzluksiz ta’lim tizimini isloh qilish va takomillashtirish, unga ilg‘or pedagogik va axborot texnologiyalarni joriy qilish va ta’lim samaradorligini oshirish davlat siyosati darajasiga ko‘tarildi. «Ta’lim to‘g‘risida»gi Qonunning qabul qilinishi bilan uzluksiz ta’lim tizimining asosi yaratildi.

Raqamli transformatsiya davrida axborot xavfsizligi masalasi global miqyosda dolzarb ahamiyat kasb etmoqda. Hozirgi kunda deyarli barcha sohalarda davlat boshqaruvi, sog‘liqni saqlash, ta’lim, moliya, sanoat va hatto ijtimoiy munosabatlarda raqamli texnologiyalar chuqur joriy qilinmoqda. Bunda axborot resurslarining ishonchliligi, maxfiyligi va butunligi, shuningdek, ma’lumotlar ustidan nazoratni saqlab qolish eng muhim omillardan biri bo‘lib qolmoqda. Ayniqsa, elektron hukumat tizimlari, moliyaviy texnologiyalar (FinTech), bulutli hisoblash texnologiyalari va katta ma’lumotlar (Big Data) asosida shakllangan xizmatlarning ommalashuvi axborot xavfsizligiga bo‘lgan ehtiyojni yanada kuchaytirmoqda.

Shu sababli bugungi kunda har bir davlat axborot xavfsizligini milliy xavfsizlikning tarkibiy qismi sifatida ko‘rib, bu yo‘nalishda malakali kadrlar tayyorlashga alohida e’tibor qaratmoqda. Kiberxavfsizlik sohasidagi tahdidlar murakkablashib borayotgan bir paytda, bu sohaga oid chuqur bilim va zamonaviy amaliy ko‘nikmalarga ega bo‘lgan mutaxassislarni yetishtirish muhim strategik vazifalardan biriga aylangan. An’anaviy o‘quv metodlari bu talabga to‘liq javob bera olmaydi. Shu bois, axborot xavfsizligi fanini zamonaviy talablarga mos holda, innovatsion yondashuvlar asosida o‘qitish zarurati dolzarb bo‘lib bormoqda.

Zamonaviy axborot xavfsizligi fanini o‘qitishning samarali uslublari, ilg‘or xorijiy tajribalar, virtual laboratoriyalar va interaktiv ta’lim platformalari asosida ta’lim jarayonini

modernizatsiya qilish yo‘llari tahlil qilinadi. Bundan tashqari, O‘zbekiston ta’lim tizimidagi mavjud holat, mavjud muammolar va bu muammolarga innovatsion yechimlar taklif qilinadi. Maqsad – raqamli asrga mos, kuchli amaliy bazaga ega bo‘lgan axborot xavfsizligi mutaxassislarini tayyorlash uchun zarur sharoitlarni yaratish va ilg‘or amaliyotni joriy etishdan iborat.

Asosiy qism Axborotni muhofaza qilish sohasida xalqaro standartlar. 1983 yil AQSH Mudofaa Vazirligi (MV) kompyuter xavfsizligi Agentligi TSec (Ishonchli tizimlarning himoyalanganligini baholash kriteriyalari) nomli hisobotini chop etdi. U boshqacha aytganda Olov rang kitob (kitob rangiga ko‘ra) deb nomlandi. Unda ko‘p foydalanuvchili kompyuter tizimlarida maxfiy ma’lumotlarni himoyalash uchun xavfsizlikning 7 ta darajasi ajratilgan. Bular: Al – kafolatli himoya, Bl, B2, B3 – ruxsatni to‘liq boshqarish, Cl, C2 – ruxsatni tanlash orqali boshqarish, D – minimal xavfsizlik.

AQSH Mudofaa Vazirligi kompyuter tizimlarini baholash maqsadida AQSH MV qoshidagi kompyuter xavfsizligi Milliy Markazi NCSC-TG-005 va NCSC-TG-011 nomli Qizil kitob (kitob rangiga ko‘ra) deb nomlangan qo‘llanmasini chiqardi.

Bunga javob tariqasida GFR axborot xavfsizligi Agentligi GreyenBook (Yashil kitob)ni tayyorladi. Unda xususiy hamda davlat miqyosida axborot xavfsizligini ta’minlashda vujudga keluvchi talablar kompleks tarzda o‘z aksini topgan.

1990 yilda Yashil kitob Germaniya, Buyuk Britaniya, Fransiya va Gollandiya davlatlari tomonidan ma’qullandi va yevropa Ittifoqiga yuborildi. Uning asosida yevropa standartini ifodalovchi ITSec (Axborot texnologiyalarining himoyalanganligini baholash kriteriyalari) yoki oq kitob tayyorlandi. Bu kitobda xavfsiz axborot tizimlarini tashkil etish kriteriyalari keltirilgan.

ITSec Oq kitobda xavfsizlik kriteriyalarining quyidagi asosiy qismlari keltirilgan:

1. Axborot xavfsizligi.
2. Tizim xavfsizligi.
3. Mahsulot xavfsizligi.
4. Xavfsizlikka tahdid.
5. Xavfsizlik funksiyasi to‘plami.
6. Xavfsizlikning kafolatlanganligi.
7. Xavfsizlikning umumiy bahosi.
8. Xavfsizlik sinflari.

ITSec yevropa kriteriyalariga ko‘ra axborot xavfsizligi olti asosiy element va uning qismlarini o‘z ichiga oladi:

1. Axborot konfedentsialligi (axborotni noqonuniy olishdan himoyalash).
2. Axborot butunligi (axborotni noqonuniy o‘zgartirishdan himoyalash).
3. Axborotdan foydalana olishlilik (axborot va tizim resurslarini noqonuniy yoki tasodifiy ushlab qolishlardan himoyalash).
4. Xavfsizlik maqsadlari (axborot xavfsizligi funktsiyalari nima uchun kerak).
5. Axborot xavfsizligi funksiyalarining tasnifi:

– identifikatsiya va autentifikatsiya (foydalanuvchining haqiqiyligini an’anaviy tekshirishgina emas, yangi foydalanuvchilarni ro‘yxatga olish, eskilarini o‘chirish, shuningdek autentifikatsiya axborotlarini o‘zgartirish va tekshirish uchun funksiyalar, shu jumladan butunlikni nazorat qiluvchi vositalar ham tushuniladi);

– foydalanish huquqini boshqarish (shu jumladan, umum foydalaniluvchi obyektlarning butunligini ta’minlash maqsadida ularga ruxsatni vaqtincha chegaralovchi xavfsizlik funksiyalari, ruxsat berish huquqini tarqatishni boshqarish kabilar);

– hisobot berishlilik (protokollashtirish);

– audit (mustaqil nazorat);

– obyektlardan qayta foydalanish;

– axborotning aniqligi (ma’lumot turli qismlarining o‘zaro mosligini ta’minlash (aloqa aniqligi) hamda axborotni uzatishda uni o‘zgarmasligini ta’minlash (kommunikatsiya aniqligi));
– xizmat ko‘rsatishning ishonchliligi (qisqa vaqt ichida vaqt bo‘yicha kritik harakatlar bajarilishini ta’minlovchi funksiyalar;
kritik bo‘lmagan, ya’ni kerakli vaqtda ma’lumotni olish imkonini berish; xatolarni topish va ularni bartaraf etish funksiyalari;
kommunikatsiya xavfsizligini ta’minlovchi rejalovchi funksiyalar);
ma’lumot almashish.
6. Xavfsizlik mexanizmlarini ifodalash.
Oq kitobda «tizim» va «mahsulot» o‘rtasida farq ifodalanadi. «Tizim» deganda ma’lum bir maqsadda va ma’lum bir doirada qo‘llaniluvchi aniq apparat - dasturiy konfiguratsiya tushuniladi. «Mahsulot» deganda esa, o‘z xohishiga ko‘ra sotib olib ixtiyoriy «tizim»ga o‘rnatilishi mumkin bo‘lgan apparat - dasturiy paket tushuniladi. «Tizim» va «Mahsulot»ning kriteriyalarini umumlashtirish maqsadida ITSecda yagona – «obyekt» atamasi kiritilgan. «Obyekt»ni ishonchli deb qabul qilish uchun, xavfsizlikni kafolatlovchi ma’lum bir darajadagi ishonch kerak bo‘ladi. U esa samaradorlik va aniqlikni o‘z ichiga oladi. Ba’zi manbalarda kafolatlanganlikni himoya vositalarining adekvatligi deb ham nomlanadi.
Himoyaning samaradorligini tekshirishda konfedentsiallik, butunlik, axborotga ruxsat etilganlik bo‘yicha xavfsizlik vazifalarining o‘zaro mosligi tahlil qilinadi. ITSec da himoya mexanizmlari quvvatining uchta darajasi (bazaviy, o‘rta, yuqori) keltirilgan.
Yevropa kriteriyalarida xavfsizlikning 10 ta sinfi o‘rnatilgan(F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-D1, F-DC, F-DX). Ularning dastlabki beshtasi Amerikaning TCSec kriteriyasidagi Cl, C2, Bl, B2, V3 larga mos keladi. F-IN sinfi axborot butunligiga bo‘lgan yuqori talabga asoslangan bo‘lib, MBBT (ma’lumotlar bazasini boshqarish tizimi)ga mos keladi, hamda ruxsatning quyidagi turlari farqlanadi: o‘qish, yozish, qo‘shish, o‘chirish, hosil qilish, qayta nomlash va obyektlarni belgilash. F-AV sinfi axborot tizimlari ish qobiliyatini ta’minlash uchun yuqori talabga mo‘ljallangan. F-D1 sinfi axborot kanallari orqali uzatiluvchi ma’lumotlarning butunligina bo‘lgan yuqori talabga mo‘ljallangan.
F-DC sinfi axborot konfedentsialligiga bo‘lgan yuqori talabga moslashgan. F-DX sinfi esa bir vaqtda F-D1 va F-DC sinflari talablariga nisbatan kuchaytirilgan talabga asoslangan.
Tahdidlarni boshqarish jarayonini quyidagi bosqichlarga bo‘lish mumkin:
1. Tahlil qilinuvchi obyektlarni tanlash va ularni ko‘rib chiqishda batafsillik darajasi.
2. Tahdidlarni baholash metodologiyasini tanlash.
3. Aktivlarni identifikatsiyalash.
4. Tahdid va uning oqibatlari tahlili, himoyaning zaifliklarini aniqlash.
5. Tahdidlarni baholash.
6. Himoya choralarini tanlash.
7. Tanlangan choralarni qo‘llash va tekshirish.
8. Qoldiq tahdidni baholash.
Ushbu munosabatlarni huquqiy boshqarish avvalo, axborot tahdidlaridan sug‘urta qilish orqali amalga oshirilishi mumkin va zarur.
AQShning milliy xavfsizligini ta’minlash tizimi. Milliy xavfsizlik agentligi (MXA-NBA) – radioelektron tutib qolish sohasida jahonda peshqadam hisoblanadi. Agentlikning maqsadi – texnik vositalar yordamida AQShning milliy xavfsizligini ta’minlash.
AQShning tashqi xavfsizligini ta’minlashda Markaziy razvedka boshqarmasi (MRB-SRU)ga asosiy o‘rinlardan biri ajratilgan. U yerda boshqa davlatlar tomonidan milliy axborot infratuzilmaga qilinadigan tahdidlar haqidagi axborotlarni qidirish va qayta ishlash bo‘yicha razvedkaning imkoniyatlarini kengaytirishga yo‘naltirilgan reja ishlab chiqilgan va tatbiq qilingan. Agentura ishiga oid an’anaviy usullardan tashqari, MRB texnik yo‘l orqali yopiq ma’lumotlar bazasiga kirishni va ochiq manbalarning tahliliga katta e’tibor qaratadi. Keyingi

vaqtlarda MRB axborot va kompyuter texnologiyalari bo‘yicha mutaxassislarni, jumladan xakerlar orasidan tanlashni amalga oshirmoqda.

AQShning Mudofaa vazirligi (MV) xalqaro Internet tarmog‘ining ajdodi hisoblanib, birinchi bo‘lib mamlakatning xavfsizligiga yangi tahdidning va axborot qurolining kuchini anglab yetdi va hozirgi vaqtda harbiy sohada axborot urushi doktrinasini tatbiq qilishda yetakchi o‘rinni egallaydi. Pentagon harbiy avtomatlashtirilgan axborot tizimlarini «qizil buyruqlar» deb ataluvchi zaiflikka tekshirish uchun harbiy kompyuter tarmoqlarini himoyasini ta’minlash bilan shug‘ullanish maqsadida xakerlarniishga qabul qiladi.

Buyuk Britaniyadagi axborotni himoyalash tizimi. Buyuk Britaniyada axborot xavfsizligini ta’minlash davlat tizimini yaratishda axborot urushi dushmanning axborot tizimiga ta’sir etuvchi va bir vaqtda mamlakatning shaxsiy tizimlarini himoyalovchi harakatlar deb qaraladi.

Buyuk Britaniyaning Razvedka va xavfsizlik bo‘yicha parlament komiteti Britaniya maxsus xizmatlari ustidan nazorat idorasi sifatida 1994 yilda tashkil etilgan. Bu komitet «Razvedka xizmatlari to‘g‘risida»gi qonunga muvofiq uchta maxsus xizmat:

Maxfiy xizmat (MI5), SIS razvedkasi va Hukumat aloqa markazi tomonidan buyudjet mablag‘larining sarflanishini, bu xizmatlarning boshqarilishini va ularning olib borayotgan siyosatini nazorat qilish uchun tuzilgan.

SecretIntelligenceService/MI6 – Buyuk Britaniyaning asosiy razvedka xizmati. SIS Tashqi ishlar vazirligi (TIV) tizimiga kiritilgan bo‘lib xorijda 87 ta qarorgohga va Londonda shtab kvartiraga ega. SISni Bosh direktor boshqaradi va u bir vaqtning o‘zida Tashqi ishlar vazirining o‘rinbosari ham hisoblanadi.

Kontrrazvedka xizmati – MilitaruIntelligence-5 (MI-5) 1909 yilda ichki xavfsizlikni ta’minlash bilan shug‘ullanuvchi maxfiy xizmatlar Buyrosining ichki departamenti sifatida tuzilgan.

Germaniyaning axborotni himoyalash tizimi. Axborot oqimlarining xavfsizligini ta’minlashga ma’sul koordinatsiyalovchi hukumat idorasi bo‘lib 1991 uilda tashkil etilgan Federal xavfsizlik xizmati (BSI) hisoblanadi. Bu xizmat axborot texnikasi sohasidagi xavfsizlikni ta’minlaydi.

Rossiya Federatsiyasi (RF)ning axborot xavfsizligini ta’minlovchi davlat idoralari strukturasi. Axborot xavfsizliginingdavlat siyosatini ishlab chiqish, qonunlar, normativ-meyoriy hujjatlar tayyorlash, axborotni muhofaza qilishni ta’minlash bo‘yicha o‘rnatilgan meyorlarni bajarilishi ustidan nazoratni davlat idoralari amalga oshiradilar.

RF Prezidenti axborot xavfsizligini ta’minlovchi davlat idoralariga boshchilik qiladi. U Xavfsizlik kengashini boshqaradi va davlatda axborot xavfsizligini ta’minlashga doir farmonlarni tasdiqlaydi.

Xulosa axborot xavfsizligi fanini o‘qitishda innovatsion yondashuvlar va ilg‘or xorijiy tajribalarning o‘rganilishi bu sohadagi mutaxassislarni sifatli tayyorlashga xizmat qiladi. Amaliy ko‘nikmalarga asoslangan ta’lim, simulyatsiya va onlayn o‘quv resurslari orqali talabalarning tayyorgarlik darajasini oshirish mumkin. O‘zbekiston ta’lim tizimida bu yo‘nalishda jadal harakatlar amalga oshirilsa, raqamli xavfsizlikning barqaror ta’minlanishiga erishiladi.

Adabiyotlar:

1. ENISA – European Union Agency for Cybersecurity: https://www.enisa.europa.eu
2. NSA – Centers of Academic Excellence in Cybersecurity: https://www.nsa.gov
3. Cybersecurity Education Curricula (ACM & IEEE recommendations)
4. TryHackMe: https://tryhackme.com
5. Abduraximov, D. B. (2019). FEATURES OF THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE EDUCATIONAL PROCESS. Bulletin of Gulistan State University, 2020(2), 28-33.