Axborot xavfsizligi tushunchasi, tamoillari va standartlari

Turapov U.U. (Toshkent davlat agrar universiteti, “Axborot tizimlari va texnologiyalari” kafedrasi dotsenti)

Botirova M. R. (Toshkent davlat agrar universiteti, “Axborot tizimlari va texnologiyalari” yo’nalish 4 bosqich talabasi)

ANNOTASIYA. Mazkur maqolada qo‘yilgan asosiy maqsad “Kiberxavfsizlik asoslari”dan himoyalash usullari, “Kiberxavfsizlik asoslari”ning dolzarbligi va asosiy atamalarini o‘rganishdan iborat. Tashkilotlar uchun “Kiberxavfsizlik asoslari”da himoyaning buzilishlari, uning oqibatlari va “Kiberxavfsizlik asoslari” siyosati muommolari o’rganib chiqilgan. Simmetrik o‘rin almashtirish algoritmlari yordamida shifrlash axborotga nisbatan bo‘ladigan xavf-xatarlar va zaifliklar hamda ularni boshqarish usullari haqida to’liq ma’lumotlar berib o’tilgan.

Tayanch iboralar: kiberxavfsizlik, kiberhujum, axborot xavfsizligi, axborotning maxfiyligi, axborot xavfsizligi standartlari, zararli dasturlar.

АННОТАЦИЯ. Основная цель данной статьи — изучение методов защиты в рамках «Основ кибербезопасности», актуальности «Основ кибербезопасности» и основных терминов. В «Основах кибербезопасности» для организаций рассматриваются нарушения защиты, их последствия и проблемы политики «Основ кибербезопасности». Предоставляется полная информация о рисках и уязвимостях шифрования с использованием симметричных алгоритмов подстановки информации, а также о методах управления ими.

Ключевые слова: кибербезопасность, кибератака, информационная безопасность, конфиденциальность информации, стандарты информационной безопасности, вредоносное ПО.

ANNOTATION. The primary purpose of this article is to examine the protection methods within the Cybersecurity Fundamentals Framework, the relevance of the Framework, and key terminology. The Cybersecurity Fundamentals Framework for Organizations addresses security breaches, their consequences, and the challenges of the Framework's policies. It provides comprehensive information on the risks and vulnerabilities of symmetric encryption algorithms, as well as methods for managing them.

Keywords: cybersecurity, cyberattack, information security, information confidentiality, information security standards, malware.

Axborot xavfsizligi – axborot resurslarini ruxsatsiz kirish, o‘zgartirish, yo‘q qilish yoki oshkor qilishdan himoya qilish maqsadida amalga oshiriladigan chora-tadbirlar va vositalar majmuasidir. Ushbu tushuncha zamonaviy axborot jamiyatida markaziy o‘rin tutadi, chunki ma’lumotlar bugungi kunda eng qimmatli resurslardan biriga aylangan.

Axborot xavfsizligi tushunchasi dastlab faqat harbiy va razvedka sohalari bilan bog‘liq bo‘lgan. Raqamli texnologiyalarning rivojlanishi bilan birga u barcha sohalarga yoyildi. ISO/IEC 27000:2018 xalqaro standarti axborot xavfsizligini quyidagicha ta’riflaydi: axborotning maxfiyligi, yaxlitligi va mavjudligini saqlash. Bu uch xususiyat axborot xavfsizligining asosini tashkil etadi va “CIA triadasi”

nomi bilan keng tanilgan (bunda C – Confidentiality (maxfiylik), I – Integrity (yaxlitlik), A – Availability (mavjudlik) so‘zlarining bosh harflarini anglatadi).

CIA triadasi 1980-yillarda ishlab chiqilgan bo‘lib, bugungi kunda ham axborot xavfsizligi tizimlarini loyihalash va baholashda asosiy mezon sifatida qo‘llaniladi. Bu model nafaqat texnik jihatdan, balki tashkiliy va huquqiy jihatdan ham axborotni himoya qilishning asosiy yo‘nalishlarini belgilab beradi.

Jadvaldan ko‘rinib turibdiki, CIA triadasining har uchala elementi bir-biri bilan chambarchas bog‘liq va ular birgalikda axborot xavfsizligining to‘liq manzarasini hosil qiladi. Maxfiylikning buzilishi ko‘pincha yaxlitlikka zarar yetkazadi, mavjudlikning pasayishi esa o‘z navbatida tizimga ishonchni kamaytiradi. Shu sababli axborot xavfsizligi tizimini loyihalashda uchala omilni bir butun tarzda ko‘rib chiqish zarur.

So‘nggi yillarda CIA triadasiga qo‘shimcha elementlar kiritish takliflari ham ilgari surilgan. Jumladan, haqiqiylik (autentiklik) – ma’lumotlarning manbai ishonchli ekanligini tasdiqlash; hisobdorlik – foydalanuvchining har bir amali qayd etilishi; inkor etmaslik – bitimni amalga oshirgan shaxsning uni rad eta olmasligi kabi tushunchalar zamonaviy axborot xavfsizligi tizimiga tobora ko’proq kirib kelmoqda.

Axborot xavfsizligining asosiy tamoyillari. Axborot xavfsizligini ta’minlash bir qator fundamental tamoyillarga asoslanadi. Bu tamoyillar tizimni loyihalash, joriy etish va boshqarish jarayonlarida asos bo‘lib xizmat qiladi. Ularni to‘g‘ri tushunish va amaliyotda qo‘llash har qanday tashkilotning axborot xavfsizligi tizimini mustahkamlashda hal qiluvchi ahamiyatga ega.

Mazkur tamoyillar bir-birini to‘ldiradi va ular birgalikda yaxlit axborot xavfsizligi tizimini hosil qiladi. Masalan, eng kam huquq tamoyili va ishonchsizlik tamoyili birgalikda qo‘llanganda, tashkilot ichidagi tahdidlar (ya’ni “ichki tahdidlar”) xavfi sezilarli darajada kamayadi. Qavat-qavat himoya tamoyili esa tashqi hujumlardan himoyalanishda asosiy rol o‘ynaydi.

Axborot xavfsizligi standartlari. Axborot xavfsizligini tizimli ta’minlash uchun xalqaro hamjamiyat bir qator standartlar va normativlar ishlab chiqdi. Bu standartlar tashkilotlarga axborot xavfsizligi tizimini to‘g‘ri qurishda yo‘l-yo‘riq beradi, xavflarni baholash usullarini belgilaydi va nazorat mexanizmlarini tavsiflaydi.

ISO/IEC 27001 standarti axborot xavfsizligini boshqarish tizimiga qo‘yiladigan talablarni belgilaydigan eng keng tarqalgan xalqaro standartdir. Bu standart tashkilotlarga axborot xavfsizligi xavflarini aniqlash, baholash va boshqarish uchun tizimli yondashuvni taqdim etadi. Bugungi kunda dunyoning 150 dan ortiq mamlakatida 40 000 dan ziyod tashkilot ushbu sertifikatga ega.

Amerika Qo‘shma Shtatlarining Milliy Standartlar va Texnologiyalar Instituti (NIST) tomonidan 2014-yilda ishlab chiqilgan Kiberxavfsizlik Doirasi besh asosiy funksiyani o‘z ichiga oladi: Aniqlash, Himoya qilish, Kashf etish, Javob berish va tiklash. Bu doira AQSh federal tashkilotlari uchun majburiy bo‘lib, xususiy sektorda ham keng qo‘llaniladi. O‘zbekiston Respublikasida ham axborot xavfsizligi sohasida milliy standartlar shakllanib bormoqda. O‘z DSt ISO/IEC 27001:2015 standarti ISO/IEC 27001 asosida ishlab chiqilgan bo‘lib, mamlakatimiz tashkilotlari uchun axborot xavfsizligini boshqarish tizimini joriy qilish uchun asos bo‘lib xizmat qilmoqda. Bundan tashqari, O‘zbekistonda “Axborot xavfsizligi to‘g‘risida”gi Qonun (2022-yil), Milliy kiberxavfsizlik strategiyasi va tegishli hukumat qarorlari soha rivojiga mustahkam huquqiy zamin yaratgan.

1.3-jadval

Xalqaro axborot xavfsizligi standartlari taqqoslamasi

Standart nomi	Manbai	Qo‘llanish doirasi	Asosiy yo‘nalish	Xususiyati
ISO/IEC 27001	Xalqaro (ISO)	Barcha tashkilotlar	Axborot xavfsizligi boshqaruv tizimi talablari	Eng keng tarqalgan, sertifikatlash imkoni bor
NIST CSF 2.0	AQSh (NIST)	Asosan AQSh federal tashkilotlari	Aniqlash, Himoya, Kashf etish, Javob, Tiklash bosqichlari	Moslashuvchan, bepul, keng qo‘llaniladi
PCI DSS v4.0	Xalqaro (PCI SSC)	To‘lov kartalari bilan ishlovchilar	12 asosiy talab, kartalar ma’lumotlarini himoya qilish	Moliya sektorida majburiy
COBIT 2019	Xalqaro (ISACA)	IT boshqaruvi sohasidagi tashkilotlar	IT boshqaruvi va nazorat maqsadlari	Korporativ IT boshqaruvi uchun ideal
O‘z DSt ISO/IEC 27001:2015	O‘zbekiston	O‘zbek tashkilotlari	ISO/IEC 27001 asosida milliy standart	Milliy qonunchilik talablariga mos

Manba: ISO, NIST, PCI SSC va O‘zbekiston Respublikasi standartlash organi ma’lumotlari asosida tuzilgan.

Jadvaldan ko‘rinib turibdiki, har bir standart o‘zining maqsadli auditoriyasi va qo‘llanish doirasiga ega. O‘zbekiston tashkilotlari uchun eng maqbul yondashuv – ISO/IEC 27001 talablari bilan milliy qonunchilik talablarini birlashtirgan holda kompleks axborot xavfsizligi tizimini qurishdir.

Kiberhujumlarning tasnifi va asosiy turlari. *Kiberhujum* – bu raqamli vositalar yordamida axborot tizimlariga, tarmoqlarga yoki qurilmalarga ruxsatsiz kirishga yoki ularga zarar yetkazishga qaratilgan, ataylab amalga oshiriladigan harakatdir. Kiberhujumlarning maqsadlari xilma-xil bo‘lishi mumkin: ma’lumotlarni o‘g‘irlash, tizimning ishlashiga xalaqit berish, maxfiy axborotni oshkor qilish, moliyaviy boylik ortirish yoki siyosiy ta’sir o‘tkazish.

Kiberhujumlarning ko‘lami va murakkabligi yildan-yilga ortib bormoqda. Zamonaviy tajovuzkorlar o‘z harakatlarini yashirishda, yangi zaifliklardan foydalanishda va hujumlarni avtomatlashtirishda sun’iy intellekt va ilg‘or texnologiyalardan tobora ko‘proq foydalanmoqda. Bugungi kunda kiberhujumlar nafaqat yakka tartibdagi shaxslar, balki tashkilotlashgan guruhlar, hattoki ba’zi davlatlar tomonidan ham amalga oshirilmoqda.

Kiberhujumning asosiy bosqichlari (Hujum zanjiri). Kiberhujumlar odatda ma’lum bir ketma-ketlikda amalga oshiriladi. Bu ketma-ketlik “hujum zanjiri” (Cyber Kill Chain) deb ataladi va birinchi marta Lockheed Martin kompaniyasi tomonidan 2011-yilda tavsiflab berilgan. Hujum zanjiridagi bosqichlarni chuqur tushunish axborot tizimini himoya qilishda juda muhim ahamiyatga ega: har bir bosqichda hujumni aniqlash va toxtatish imkoniyati mavjud.

1.4-jadval

Kiberhujumning asosiy bosqichlari – Hujum zanjiri modeli

Bosq.	Bosqich nomi	Tavsifi	Aniqlash usuli
1	Razvedka (Reconnaissance)	Tajovuzkor nishon tizim haqida ma’lumot to‘playdi: domenlar, IP manzillar, xodimlar ro‘yxati, tashkilot tuzilishi.	Tarmoq skanerlashni aniqlash, g‘ayritabiiy so‘rovlarni kuzatish
2	Qurol tayyorlash (Weaponization)	Topilgan zaiflikka mos keladigan zararli dastur yoki ekspluatatsiya vositasi tayyorlanadi.	Zararli dastur imzolarini aniqlash, hujum uskunalarini kuzatish
3	Yetkazib berish (Delivery)	Zararli dastur nishonga yetkaziladi: fishing xabarlari, zararli saytlar, ifloslangan qurilmalar orqali.	Elektron pochta filtrlash, veb-filtrlash, USB qurilmalarni nazorat qilish
4	Ishga tushirish (Exploitation)	Zararli kod nishon tizimida bajariladi, zaiflikdan foydalanib tizimga kirish ta’minlanadi.	Intruziyani aniqlash tizimlari, anomal xatti-harakatlarni kuzatish
5	O‘rnatish (Installation)	Tajovuzkor tizimda doimiy yashirin orqa eshik (backdoor) o‘rnatib, qayta kirishni ta’minlaydi.	Fayl tizimidagi o‘zgarishlarni kuzatish, yangi jarayonlarni nazorat qilish
6	Boshqarish (Command & Control)	Tajovuzkor yuqtirilgan tizim bilan maxfiy aloqa kanali o‘rnatib, uni masofadan boshqaradi.	G‘ayritabiiy tarmoq trafigini aniqlash, DNS so‘rovlarini tahlil qilish
7	Maqsadni amalga oshirish (Actions on	Tajovuzkor asosiy maqsadini amalga oshiradi: ma’lumot o‘g‘irlash, tizimni	Ma’lumotlar harakatini kuzatish,

	Objectives)	buzish, to‘lov talab qilish.	noodatiy faollikni aniqlash

***Manba**: Lockheed Martin Cyber Kill Chain modeli asosida muallif tomonidan tuzilgan.*

Hujum zanjirining har bir bosqichida mudofaachi tizimni himoya qilish imkoniyatiga ega. Ayniqsa, dastlabki bosqichlarda hujumni aniqlash va to‘xtatish oxirgi bosqichlardagiga nisbatan ancha kam zarar bilan kechadi. Shu sababli zamonaviy kiberxavfsizlik mutaxassislari proaktiv yondashuv – ya’ni hujumdan oldin aniqlash va oldini olishga alohida e’tibor qaratadi.

Kiberhujumlarning tasnifi. Kiberhujumlarni turli mezonlar asosida tasniflash mumkin. Bu tasnif mutaxassislarga tahdidlarni to‘g‘ri baholash, tegishli himoya choralarini tanlash va resurslarni samarali taqsimlash imkonini beradi.

1.5-jadval

Kiberhujumlarning tasnifi

Tasnif mezoni	Kichik tur	Qisqacha tavsifi
Maqsad bo‘yicha	**Ma’lumot o‘g‘irlash**	Shaxsiy, moliyaviy, davlat ma’lumotlarini ruxsatsiz olish
	Tizimni buzish	Xizmatlarni to‘xtatish, infratuzilmani ishdan chiqarish
	Moliyaviy foyda olish	To‘lov talabnomalari, firibgarlik operatsiyalari
	Josuslik	Raqobat ustunligini qo‘lga kiritish, davlat sirlarini olish
Sub’ekt bo‘yicha	**Davlat tomonidan moliyalanadigan hujumlar**	Millat davlatlari maxsus xizmatlari amalga oshiradigan murakkab, maqsadli hujumlar
	Tashkilotlashgan guruhlar	Kiberjinoyatchilik hamjamiyatlari; moliyaviy maqsadlarda harakat qiladi
	Ichki tahdidlar	Xodimlar yoki sobiq xodimlar tomonidan amalga oshiriladi

	Yakka tartibdagi tajovuzkorlar	Ko‘pincha taniqlilik yoki shaxsiy manfaat maqsadida harakat qiladi
Usul bo‘yicha	**Dastur zaifliklaridan foydalanish**	Tizim yoki dasturlardagi kamchiliklarni ishlatish
	Ijtimoiy muhandislik	Insonning ishonuvchanligidan foydalanib axborot olish yoki harakatga undash
	Tarmoq hujumlari	Tarmoq protokollarini nishon qilib, trafikni ushlab qolish yoki buzish
	Jismoniy kirish	Qurilmalarga to‘g‘ridan-to‘g‘ri jismoniy murojaat orqali ma’lumot olish

Manba: *ENISA (Yevropa Ittifoqi Kiberxavfsizlik Agentligi) va muallif tahlili asosida tuzilgan.*

Kiberhujumlarni tasniflash ularning mohiyatini to‘g‘ri tushunishga va tegishli himoya choralarini tanlashga yordam beradi. Amaliyotda kiberhujumlar ko‘pincha bir necha mezon bo‘yicha bir vaqtda tavsiflanishi mumkin: masalan, moliyaviy maqsadli, ijtimoiy muhandislik usulida amalga oshirilgan, tashkilotlashgan guruhning hujumi.

Asosiy kiberhujum turlari va ularning ta’siri. Zamonaviy kiberxavfsizlik amaliyotida eng ko‘p uchraydigan va eng katta zarar yetkazadigan kiberhujum turlari quyidagilardir:

Zararli dastur (Malware) hujumlari. Zararli dastur – kompyuter tizimiga zarar yetkazish, ma’lumot o‘g‘irlash yoki tizimni nazorat ostiga olish maqsadida yaratilgan dasturiy ta’minotdir. Zararli dasturlarning asosiy turlari: viruslar (o‘zini ko‘paytiruvchi), qurtlar (tarmoq orqali tarqaluvchi), troyanlar (foydali dastur ko‘rinishida yashirinuvchi), josuslik dasturlari (foydalanuvchi harakatlarini kuzatuvchi) va reklama dasturlari kiradi.

To‘lov talab qiluvchi zararli dastur (Ransomware). Bu zararli dastur turi qurbonning ma’lumotlarini shifrlaydi va ularni qaytarish evaziga pul to‘lovini talab qiladi. 2021-yilda Colonial Pipeline kompaniyasiga bo‘lgan hujumda 4,4 million dollar to‘lov undirilib, AQShdagi yoqilg‘i ta’minoti bir necha kun izdan chiqdi. Bu hujum zamonaviy kibertahdidlarning moddiy infratuzilmaga ham jiddiy xavf tug‘dirishini yaqqol ko‘rsatdi.

Fishing hujumlari (Fishing/Phishing). Bu usulda tajovuzkor qonuniy tashkilot yoki shaxs nomidan soxta xabarlar yuborib, qurbonni maxfiy ma’lumotlarni (parol, bank kartasi raqami) oshkor qilishga yoki zararli havola yoki faylni ochishga aldaydi. Verizon kompaniyasining 2023-yilgi tahliliy hisobotiga ko‘ra, barcha kiberhujumlarning 36 foizida fishing usulidan foydalanilgan.

Xizmatni blokirovka qilish hujumi (DDoS). Distributed Denial of Service – bu hujum turida veb-sayt yoki onlayn xizmati juda ko‘p so‘rov bilan to‘ldirib tashlanadi va natijada u oddiy foydalanuvchilarga javob berish imkoniyatini yo‘qotadi. 2016-yilda Dyn DNS provayderiga bo‘lgan

DDoS hujumi Twitter, Reddit, Netflix kabi yirik internet xizmatlarining bir necha soat ishdan chiqishiga sabab bo‘ldi.

SQL kiritish hujumi (SQL Injection). Bu hujum turida tajovuzkor veb-ilova orqali ma’lumotlar bazasiga noto‘g‘ri SQL buyruqlarini kiritadi va natijada ma’lumotlarga ruxsatsiz kirish, ularni o‘zgartirish yoki o‘chirish imkoniyatiga ega bo‘ladi. Kiberhujumlarning taxminan 65 foizi ma’lumotlar bazasi zaifliklaridan foydalanadi.

O‘rtadagi odam hujumi (Man-in-the-Middle). Bu hujumda tajovuzkor ikki taraf o‘rtasidagi aloqaga yashirin tarzda kiradi va ular bilmagan holda axborot almashuvini kuzatadi yoki o‘zgartiradi. Ko‘pincha ommaviy Wi-Fi tarmoqlarida amalga oshiriladi.

Nol kunlik zaiflik (Zero-day) hujumlari. Bu hujum turiga dasturiy ta’minot ishlab chiqaruvchisi hali bilmagan zaifliklardan foydalaniladi. “Nol kun” atamasi ishlab chiqaruvchida zaiflikni tuzatish uchun hech qanday vaqt qolmaganligini bildiradi. Bunday hujumlar ayniqsa xavfli, chunki ularga qarshi tayyor himoya choralari mavjud bo‘lmaydi.

1.5-jadval

Asosiy kiberhujum turlari va ularning ta’siri

Hujum turi	Xavflilik darajasi	Ta’siri	Asosiy himoya	Qo‘shimcha ma’lumot
Zararli dastur	**O‘rta / Yuqori**	Ma’lumot o‘g‘irlash, tizimni nazorat ostiga olish	Antivirus, tarmoq devori, foydalanuvchi ta’limi	Nafaqat kompyuter, balki mobil qurilmalar ham nishon
To‘lov zararli dasturi	**Juda yuqori**	Ma’lumotlarni shifrlash, faoliyatni to‘xtatish, moliyaviy zarar	Muntazam zaxira nusxalar, xodimlarni o‘qitish	To‘lov o‘rtacha 1,5 mln dollar (2023-yil)
Fishing hujumi	**O‘rta / Yuqori**	Login ma’lumotlarini o‘g‘irlash, tizimga kirish	Ikki bosqichli tekshiruv, pochta filtrlash	Hujumlarning 36% fishing orqali boshlanadi
DDoS hujumi	**O‘rta**	Xizmat uzilishi, daromad yo‘qotish, obro‘ zarar ko‘rishi	CDN, trafik filtrlash, tarmoq bandligi zaxirasi	Eng katta hujum: 3,47 Tbps (2021-yil, Amazon)
SQL kiritish	**Yuqori**	Ma’lumotlar bazasiga ruxsatsiz kirish, ma’lumotlarni o‘chirish	Kiritishni tekshirish, tayyor so‘rovlar	65% veb-hujumlarida qo‘llaniladi

O‘rtadagi odam	**O‘rta / Yuqori**	Maxfiy ma’lumotlarni ushlab qolish, sessiyani egallash	HTTPS, VPN, sertifikatlarni tekshirish	Ommaviy Wi-Fi tarmoqlarda keng tarqalgan
Nol kunlik zaiflik	**Juda yuqori**	Tizimga to‘la kirish, uzoq muddatli josuslik	Zaifliklarni bashorat qilish, tizimni tezda yangilash	Dark web da bahosi 2,5 mln dollargacha
Ijtimoiy muhandislik	**Yuqori**	Maxfiy ma’lumot olish, texnik himoyani chetlab o‘tish	Xodimlarni muntazam o‘qitish, xabardorlikni oshirish	Hujumlarning 98% inson omiliga bog‘liq

Manba: Verizon DBIR 2023, IBM Cost of a Data Breach 2023, Kaspersky Lab ma’lumotlari asosida tuzilgan.

Jadvaldan ko‘rinib turibdiki, kiberhujumlarning aksariyati inson omiliga tayanadi. Bu esa axborot xavfsizligini ta’minlashda faqat texnik vositalar bilan cheklanmaslik, balki xodimlarni doimiy o‘qitish va xabardorlik darajasini oshirishga alohida e’tibor qaratish lozimligini ko‘rsatadi.

1.6-jadval.

Dunyo miqyosida kiberhujumlar ko‘rsatkichlari (2020–2024)

Yil	O‘rtacha zarar (buzilish boshiga)	Ransomware hujumlari soni	Aniqlanish muddati (o‘rtacha)	Jahon miqyosidagi kiberjinoyatchilik zarari
2020	3,86 million dollar	1 081 ta ziyod	304 kun	157 milliard dollar
2021	4,24 million dollar	1 862 ta	287 kun	6,9 trillion dollar
2022	4,35 million dollar	4 145 ta	277 kun	8,4 trillion dollar
2023	4,45 million dollar	5 400 ta ziyod	258 kun	8,0 trillion dollar
2024*	4,88 million dollar	6 000+ (taxminiy)	240 kun (taxminiy)	9,2 trillion dollar

				(taxminiy)

*Manba: IBM Cost of a Data Breach hisobotlari (2020–2023), Cybersecurity Ventures (2024-yil taxminiy). * – taxminiy ma'lumotlar.*

Jadval ma'lumotlari kiberhujumlardan yetkaziladigan iqtisodiy zararning yildan-yilga keskin o'sib borayotganini ko'rsatmoqda. 2020-yildan 2023-yilga qadar bitta ma'lumotlar xavfsizligi buzilishidan yetkaziladigan o'rtacha zarar 15,5 foizga oshgan. To'lov zararli dastur hujumlarining soni esa to'rt yil ichida taxminan besh baravar ko'paygan. Bu raqamlar axborot xavfsizligiga sarflanadigan xarajatlarni investitsiya emas, balki zaruriy xarajat deb qarash lozimligini yaqqol ko'rsatadi.

Xulosa

Xulosada axborot xavfsizligining nazariy asoslari ko'rib chiqildi. CIA triadasi – maxfiylik, yaxlitlik va mavjudlik – axborot xavfsizligining uch ustunini tashkil etadi. Xalqaro standartlar (ISO/IEC 27001, NIST CSF, PCI DSS) ushbu tamoyillarni amaliyotda joriy etish uchun tizimli asos hisoblanadi Kiberhujumlar esa zamonaviy raqamli dunyodagi eng jiddiy tahdidlardan biri bo'lib, ularning tasnifini va hujum zanjirini bilish samarali mudofaa strategiyasini ishlab chiqish uchun ma'lumotlar ko'rib chiqildi.

Qo'llanilgan adabiyotlar

1. O'zbekiston Respublikasi standartlashtirish agentligi. O'z DSt ISO/IEC 27001:2015. Toshkent: O'zstandart, 2015.
2. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Hoboken: Pearson, 2019. 816 b.
3. ISO/IEC 27000:2018. Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva: ISO, 2018.
4. Parker D.B. Fighting Computer Crime: A New Framework for Protecting Information. New York: John Wiley & Sons, 1998. 512 b.
5. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Requirements. Geneva: ISO, 2022.
6. ISO Survey 2023. The ISO Survey of Management System Standard Certifications. URL: https://www.iso.org/the-iso-survey.html (murojaat sanasi: 12.02.2024).
7. NIST. Framework for Improving Critical Infrastructure Cybersecurity (CSF), Version 2.0. Gaithersburg, MD: NIST, 2024. URL: https://doi.org/10.6028/NIST.CSWP.29 (murojaat sanasi: 20.02.2024).
8. IBM Security. Cost of a Data Breach Report 2023. Op. cit.
9. Verizon. 2023 Data Breach Investigations Report (DBIR). Basking Ridge, NJ: Verizon Communications, 2023. URL: https://www.verizon.com/business/resources/reports/dbir (murojaat sanasi: 25.02.2024).
10. Woolf N. DDoS attack that disrupted internet was largest of its kind in history. The Guardian, 2016-yil 26-oktabr. URL: https://www.theguardian. com/technology/2016/oct/26/ddos-attack-dyn (murojaat sanasi: 14.03.2024).