ISSN 3060-4567

AXBOROT XAVFSIZLIGI: RAQAMLI DUNYODA MA'LUMOTLARNI HIMOYA QILISH

Akramova Munisa A'zamjon qizi

Farg 'ona Davlat Universiteti

Chet tillari fakulteti, Filologiya va tillarni o'qitish: ingliz tili yo'nalishi

1-kurs talabasi

Ilmiy rahbar: ***Toshboltoyev Faxriddin O'rinboyevich***

Annotatsiya: *Quyidagi maqolada zamonaviy raqamli muhitda axborot xavfsizligining dolzarbligi, tahdidlar va ularga qarshi kurashish usullari, xalqaro va milliy tajribalar tahlili olib boriladi hamda axborot xavfsizligi tushunchasi, asosiy tamoyillari, texnologik va tashkiliy himoya vositalari ilmiy nuqtai nazardan ko'rib chiqiladi.*

Kalit so'zlar: *Axborot xavfsizligi, raqamli xavf, kiberxavfsizlik, shifrlash, autentifikatsiya, DDoS, kriptografiya, milliy strategiya.*

Annotation: *This article explores the relevance of information security in the modern digital environment, analyzes threats and methods of countering them, as well as international and national experiences in this field. The concept of information security, its fundamental principles, technological and organizational protective measures are examined from a scientific perspective.*

Keywords: *Information security, digital threat, cybersecurity, encryption, authentication, DDoS, cryptography, national strategy.*

Raqamli texnologiyalar jadal rivojlanib, hayotimizning har bir jabhasiga chuqur kirib bormoqda. Shuningdek, axborot resurslari va tizimlariga nisbatan xavf-xatarlar ham ortib bormoqda. Axborot xavfsizligi nafaqat texnik muammo, balki milliy xavfsizlik, iqtisodiy barqarorlik va jamiyat ishonchliligi bilan chambarchas bog'liqdir. Ayniqsa, elektron hukumat, onlayn to'lov tizimlari, shaxsiy ma'lumotlar

bazalari kabi sohalarda axborot xavfsizligini ta’minlash dolzarb muammoga aylangan.

Axborot xavfsizligi – bu axborotni ruxsatsiz kirish, o‘zgartirish, yo‘q qilish yoki tarqatilishdan himoya qilishga qaratilgan tashkiliy va texnik choralar tizimi hisoblanadi. Axborotni ishonchli saqlash va uzatish bugungi raqamli dunyoda muhim vazifalardan biridir. Shu sababli, axborot xavfsizligi nafaqat dasturchilar yoki IT-mutaxassislar uchun, balki har qanday tashkilot va foydalanuvchi uchun dolzarb masalaga aylangan.

Axborot xavfsizligining asosiy tamoyillari uchta asosiy ustunga tayanadi:

Maxfiylik (Confidentiality).Bu tamoyil axborotga faqat vakolatli shaxslar yoki tizimlar kirishini ta’minlay oladi. Maxfiylikni buzish deganda axborotni ruxsatsiz shaxslar ko‘rishi, nusxalashi yoki tarqatishi tushiniladi. Bunga qarshi kurashishda parollar, shifrlash usullari va kirish huquqlarini boshqarish tizimlari keng qo‘llaniladi.

Butunlik (Integrity).Axborotning butunligi uning ruxsatsiz o‘zgartirilmasligi, buzilmasligi yoki noto‘g‘ri ma’lumotga aylantirilmasligini anglatadi. Masalan, moliyaviy hisobotdagi raqamlarning ruxsatsiz o‘zgartirilishi jiddiy oqibatlarga olib kelishi mumkin. Shu sababli ma’lumotlar uzatilayotgan yoki saqlanayotgan paytda ularning aniqligini ta’minlash maqsadida hash-algoritmlar, raqamli imzolar kabi texnologiyalar qo‘llaniladi.

Mavjudlik (Availability).Ma’lumotlar kerakli vaqtda kerakli foydalanuvchiga mavjud bo‘lishi zarur. DDoS hujumlari yoki texnik nosozliklar bu tamoyilga jiddiy zarar yetkazishi mumkin. Bunga qarshi zaxira nusxalar, xavfsizlik devorlari (firewall), tarmoqlarni yuklamadan muhofaza qilish kabi vositalar ishlatiladi.

Ushbu tamoyillar axborot xavfsizligini ta’minlovchi har qanday tizimning asosiy poydevori hisoblanadi. Aynan shu elementlar orqali raqamli muhitda ishonchli, barqaror va xavfsiz axborot almashinuvi ta’minlanadi. Raqamli dunyoning jadal rivojlanishi axborot xavfsizligiga tahdid soluvchi omillar sonining ham ortishiga olib kelmoqda. Kiberjinoyatchilar tobora murakkab va puxta rejalashtirilgan hujumlar

ISSN 3060-4567

orqali tashkilotlar, kompaniyalar va jismoniy shaxslarning axborot tizimlariga zarar yetkazishga harakat qilmoqda. Ularning asosiy maqsadi – ma’lumotlarni o‘g‘irlash, ularni o‘zgartirish yoki yo‘q qilish, iqtisodiy zarar yetkazish yoki shantaj qilishdir. Quyida eng keng tarqalgan zamonaviy tahdidlar turlari keltirib o‘tiladi.

Kiberhujumlar (Cyberattacks). Kiberhujumlar — bu kompyuter tizimlari va tarmoqlariga qasddan zarar yetkazish yoki ruxsatsiz kirish maqsadida amalga oshiriladigan hujumlardir. Eng ko‘p tarqalgan shakllariga quyidagilar kiritish mumkin. Dastlabkisi, Phishing (Soxtalashtirilgan xabarlar) hisoblanadi va bu foydalanuvchini aldamchi havola yoki fayl orqali maxfiy ma’lumotlarini oshkor qilishga undashdir. Bu orqali foydalanuvchining login-paroli, bank ma’lumotlari va boshqa muhim axborotlar o‘g‘irlanadi.

Malware (Zararli dasturlar) – viruslar, trojanlar, ransomware (ma’lumotni shifrlab, pul talab qiluvchi dasturlar) kabi zararli dasturlar orqali tizimga zarar yetkazish yoki uni boshqaruvdan chiqarish.

DDoS hujumlari – tarmoq yoki sayt ishini izdan chiqarish uchun unga juda ko‘p so‘rovlar yuborish orqali mavjudlik tamoyilini buzish.

Ijtimoiy muhandislik (Social Engineering). Bu usulda texnik vositalardan ko‘ra inson psixologiyasidan foydalaniladi. Jinoyatchi o‘zini ishonchli shaxs sifatida ko‘rsatib, foydalanuvchini axborotni oshkor qilishga undaydi. Masalan, telefon orqali bank xodimi sifatida qo‘ng‘iroq qilib, kartadagi pulni "saqlab qolish" bahonasida kodni so‘rashi mumkin.

Ichki tahdidlar (Insider Threats). Ko‘plab xavfsizlik buzilishlari tashkilot ichidagi xodimlar tomonidan sodir etiladi. Ular ataylab yoki ehtiyotsizlik oqibatida maxfiy ma’lumotlarni filtrlashlari mumkin. Bu holat axborot xavfsizligini ta’minlashda inson omilining qanchalik muhimligini ko‘rsatadi.

Raqamli kontentning tez va ommaviy tarqalishi sababli mualliflik huquqi, shaxsiy hayot daxlsizligi va tijorat sirlariga oid ma’lumotlar osonlik bilan noqonuniy tarqatilishi mumkin. Bu nafaqat axborot xavfsizligiga, balki ijtimoiy va iqtisodiy barqarorlikka ham xavf solmoqda. Zamonaviy tahdidlarning ko‘lam va murakkabligi axborot xavfsizligiga bo‘lgan yondashuvni muntazam yangilab borishni taqozo etadi.

Bu esa texnologik vositalar bilan birga insoniy omil va tashkilot ichidagi siyosatlarni ham muhim o‘ringa qo‘yadi.

Axborot xavfsizligini ta’minlashda texnologik yechimlar muhim rol o‘ynaydi.Har bir tahdid turiga qarshi muayyan himoya vositalari mavjud bo‘lib, ular dasturiy, apparatli va tashkiliy darajalarda qo‘llaniladi. Zamonaviy va samarali himoya usullari bir necha yo‘llar bilan tahlil qilinadi:

Kriptografiya va shifrlash texnologiyalari. Kriptografiya – axborotni ruxsatsiz kirishdan himoya qilish uchun uni maxsus algoritmlar orqali shifrlash usulidir. Shifrlangan ma’lumotni faqat maxsus kalit yordamida ochish mumkin. Bugungi kunda AES (Advanced Encryption Standard), RSA va SHA kabi algoritmlar keng qo‘llanilmoqda. Shifrlash texnologiyalari orqali ma’lumotlar yuboruvchi va qabul qiluvchigina uni to‘g‘ri talqin qila oladi.

Autentifikatsiya va avtorizatsiya. Autentifikatsiya – foydalanuvchining shaxsini aniqlash jarayoni (masalan, parol, biometrik ma’lumotlar, SMS-kod orqali), avtorizatsiya esa unga tizimda qanday imkoniyatlar berilishini aniqlaydi. Hozirda ikki bosqichli autentifikatsiya (2FA) va biometrik texnologiyalar (barmoq izi, yuzni aniqlash) xavfsizlikni sezilarli darajada oshirmoqda.

Antivirüs dasturlar zararli dasturlarni aniqlash va ularni zararsizlantirishga xizmat qiladi. Xavfsizlik devorlari esa kompyuter yoki tarmoqni tashqi tahdidlardan himoya qilgan holda faqat ishonchli trafikni o‘tkazadi. Har ikki vosita foydalanuvchining xabarisiz tizimga kirib kelmoqchi bo‘lgan zararli omillarni aniqlaydi va bloklaydi. Zaxira nusxalar va uzluksizlik rejasi (backup & recovery). Axborotni yo‘qotish yoki shikastlanishining oldini olish uchun muntazam ravishda zaxira nusxalar yaratish muhim. Uzluksizlik rejasi (disaster recovery plan) esa favqulodda holatlarda tizimni tiklash uchun oldindan ishlab chiqilgan chora-tadbirlarni o‘z ichiga oladi. Bularga muqobil serverlar, bulutli saqlash tizimlari va avtomatlashtirilgan zaxiralash tizimlari kiradi.

Bulutli texnologiyalar va ularning xavfsizligi. Bulutli saqlash xizmatlari (masalan, Google Drive, OneDrive, Dropbox) foydalanuvchilarga istalgan joydan ma’lumotlarga kirish imkonini beruvchi vositalardir. Ammo bu bilan birga, yangi

ISSN 3060-4567

xavfsizlik tahdidlarini ham keltirib chiqaradi. Shuning uchun bulut xizmatlarida ma’lumotlarni shifrlash, kirish nazorati va auditoriya loglarini yuritish kabi xavfsizlik choralarini ko‘rish kerak.

Himoya usullarining har biri axborot xavfsizligining ma’lum jihatini ta’minlaydi. Ularni birgalikda, tizimli yondashuv asosida qo‘llash orqali raqamli muhitdagi xavfsizlikni sezilarli darajada oshirish mumkin.

Milliy va xalqaro tajribalar.Axborot xavfsizligini ta'minlashda har bir davlat va xalqaro tashkilot o‘ziga xos yondashuvni ishlab chiqqan. Bu yondashuvlar texnologik vositalar bilan bir qatorda huquqiy, tashkiliy va ijtimoiy mexanizmlarni ham o‘z ichiga oladi. So‘nggi yillarda O‘zbekiston axborot xavfsizligiga alohida e’tibor qaratmoqda.2017-yilda "Elektron hukumat to‘g‘risida"gi Qonun qabul qilinishi bilan birga, axborot tizimlarida xavfsizlik talablarini joriy etish bo‘yicha normativ-huquqiy asoslar shakllantirildi. 2018-yil 5-iyulda Prezident qarori bilan "Kiberxavfsizlik bo‘yicha kompleks chora-tadbirlar dasturi" tasdiqlandi. Bundan tashqari, "Axborotlashtirish to‘g‘risida"gi Qonun, "Shaxsga doir ma’lumotlar to‘g‘risida"gi Qonun, va "Kiberxavfsizlik strategiyasi" kabi hujjatlar ham raqamli xavfsizlikni huquqiy jihatdan mustahkamlashga xizmat qilmoqda. Davlat tomonidan "UZCERT" – O‘zbekiston kompyuter hodisalariga javob berish markazi tashkil etilgan bo‘lib, bu markaz kiberhujumlarning oldini olish va ularga javob berish bo‘yicha faoliyat olib bormoqda.

Dunyo miqyosida axborot xavfsizligini ta’minlash uchun qator xalqaro tashkilotlar va standartlar mavjud:

ISO/IEC 27001 – axborot xavfsizligi menejment tizimlari uchun xalqaro standart bo‘lib, tashkilotlarga xavflarni baholash, ularni boshqarish va xavfsizlik siyosatini ishlab chiqishda yordam beradi.

NIST (AQSH) – AQSh Milliy Standartlar va Texnologiyalar Instituti tomonidan ishlab chiqilgan kiberxavfsizlik bo‘yicha metodikalar butun dunyoda keng qo‘llaniladi.

ISSN 3060-4567

ITU (Xalqaro Telekommunikatsiya Ittifoqi) – BMT tarkibidagi tashkilot bo‘lib, global axborot xavfsizligi standartlarini ishlab chiqadi va davlatlar o‘rtasidagi hamkorlikni rivojlantiradi.

GDPR (Evropa Ittifoqi) – ma’lumotlarni himoya qilish va shaxsiy hayot daxlsizligini ta’minlovchi qat’iy qonun bo‘lib, foydalanuvchilarning shaxsiy ma’lumotlariga ishlov berishda aniq va qat’iy talablarni belgilaydi.

O‘zbekiston xalqaro tajribalardan ilhomlanib, o‘zining milliy xavfsizlik strategiyasini takomillashtirib kelmoqda. Biroq, rivojlangan mamlakatlarda mavjud tajribalarga nisbatan bizda texnik resurslar, malakali mutaxassislar va institutsional infratuzilmalarning yetarli darajada shakllanmagani hali dolzarb muammoligicha qolmoqda. Shu boisdan, xalqaro tajribalarni chuqur o‘rganish, ularni ilmiy asosda joriy etish zarurdir. Axborot xavfsizligi bugungi raqamli jamiyatda nafaqat texnik, balki strategik va ijtimoiy muammo sifatida ham ko‘rilmoqda. Raqamli axborot oqimlarining kengayishi, kiberhujumlar sonining ortib borishi, ma’lumotlarga nisbatan ishonchlilik darajasining pasayishi axborot xavfsizligini har bir tashkilot, tizim va fuqaro uchun ustuvor yo‘nalishga aylantirmoqda.

Ushbu maqolada axborot xavfsizligining asosiy tamoyillari, tahdid turlari, zamonaviy himoya texnologiyalari, shuningdek, milliy va xalqaro tajribalar ilmiy asosda tahlil qilindi. Tahlillar shuni ko‘rsatadiki, axborot xavfsizligini ta’minlashda texnologik vositalar bilan bir qatorda, yuridik asoslar, inson resurslari va ta’lim tizimi ham muhim o‘rin egallaydi. Har qanday xavfsizlik tizimi faqat texnik choralar bilan emas, balki foydalanuvchilarning axborot madaniyatini oshirish orqali ham samarali ishlaydi. O‘zbekiston Respublikasi bu borada muhim qadamlar tashlamoqda. Biroq xalqaro tajribalarni chuqurroq o‘rganish, zamonaviy standartlarga mos infratuzilma va kadrlar salohiyatini mustahkamlash orqali yanada barqaror va ishonchli axborot muhitini yaratish mumkin.

Shunday qilib, raqamli dunyoda muvaffaqiyatli faoliyat yuritish, rivojlanish va raqobatbardosh bo‘lish uchun axborot xavfsizligi masalasiga ilmiy, tizimli va kompleks yondashuv zarur.

ISSN 3060-4567

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley Publishing.

2. Stallings, W. (2021). Network Security Essentials: Applications and Standards. Pearson Education.

3. Европейский союз. (2018). Общий регламент по защите данных (GDPR). Официальный журнал Европейского союза.

4. CISA (Cybersecurity and Infrastructure Security Agency). (2023). Cyber Essentials Toolkit. Retrieved from: https://www.cisa.gov.

5. O‘zbekiston Respublikasi “Axborot xavfsizligi to‘g‘risida”gi Qonuni, 2020 yil 15 aprel.

6. Мазалов, Н.А., Сидоров, А.В. (2022). Кибербезопасность: теория и практика защиты информации. Москва: Научное издательство.

7. Kaspersky Lab. (2023). Annual Security Bulletin. Retrieved from: https://www.kaspersky.com.