ZAMONAVIY AXBOROT TIZIMLARIDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASH TAMOYILLARI
ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ
PRINCIPLES OF DATA SECURITY IN MODERN INFORMATION SYSTEMS

Behzod Sobirjonov Qahromonovich
FarDU Axborot texnologiyalari kafedrasi katta o'qituvchisi
behzodqahramonovich@gmail.com
Qurbonaliyeva Feruzaxon Abduvohid qizi
Farg'ona davlat universiteti
Axborot tizimlari va texnologiyalari yo'nalishi 2-bosqich talabasi
feruzahonkurbonalieva@gmail.com
To'xtasinova Mahbubaxon Akmaljon qizi
Farg'ona davlat universiteti
Axborot tizimlariva texnologiyalari yo'nalishi 2-bosqich talabasi
m.tohtasinova@icloud.com

Annotatsiya:*Ushbu maqolada zamonaviy axborot tizimlarida ma'lumotlar xavfsizligini ta'minlashning asosiy prinsiplari, usullari va texnologiyalari yoritiladi. Ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini himoya qilishga qaratilgan mexanizmlar – shifrlash, autentifikatsiya, ruxsatlarni boshqarish, tarmoq xavfsizligi va xavf tahlili kabi mavzular ko'rib chiqiladi. Shuningdek, kiberhujumlar turlari va ulardan himoyalanish strategiyalari, xavfsizlik siyosatini shakllantirish hamda zamonaviy xavfsizlik standartlarining ahamiyati tahlil qilinadi. Tadqiqot axborot resurslarini himoya qilishda kompleks yondashuvning zarurligini asoslaydi.*

Kalit so'zlar: *ma'lumotlar xavfsizligi, axborot himoyasi, maxfiylik, yaxlitlik, mavjudlik, shifrlash, autentifikatsiya, avtorizatsiya, kiberxavfsizlik, xavf tahlili, himoya mexanizmlari, tarmoq xavfsizligi, hujumlar, xavfsizlik siyosati, ma'lumotlar bazasi xavfsizligi.*

Аннотация:*В данной статье рассматриваются основные принципы, методы и технологии обеспечения безопасности данных в современных информационных системах. Особое внимание уделяется механизмам защиты конфиденциальности, целостности и доступности данных, таким как шифрование, аутентификация, управление доступом, сетевые меры безопасности и анализ рисков. Также анализируются типы кибератак и стратегии противодействия им, разработка*

политики безопасности и значение современных стандартов информационной безопасности. Работа обосновывает необходимость комплексного подхода к защите информационных ресурсов.

Ключевые слова:*безопасность данных, защита информации, целостность, доступность, шифрование, аутентификация, авторизация, кибербезопасность, анализ рисков, защитные механизмы, сетевая безопасность, атаки, политика безопасности, безопасность баз данных.*

Annotation: *This article examines the key principles, methods, and technologies used to ensure data security in modern information systems. It focuses on mechanisms that protect the confidentiality, integrity, and availability of data, including encryption, authentication, access control, network security measures, and risk analysis. The study also analyzes various types of cyberattacks, defense strategies, security policy development, and the importance of modern security standards. The research highlights the necessity of a comprehensive approach to safeguarding information resources.*

Keywords:*data security, information protection, confidentiality, integrity, availability, encryption, authentication, authorization, cybersecurity, risk analysis, security mechanisms, network security, attacks, security policy, database security.*

Kirish

Bugungi kunda raqamli axborot oqimining jadal o‘sishi ma’lumotlar xavfsizligini axborot texnologiyalari sohasidagi eng muhim yo‘nalishlardan biriga aylantirmoqda. Deyarli har bir tashkilot, korxona yoki onlayn xizmat o‘z faoliyatida katta hajmdagi ma’lumotlarni qayta ishlaydi va ularning xavfsizligini ta’minlash strategik ahamiyat kasb etadi. Ma’lumotlar xavfsizligi — bu ma’lumotlarning maxfiyligini, yaxlitligini va mavjudligini saqlashga qaratilgan chora-tadbirlar majmui bo‘lib, u kiberxavfsizlikning markaziy qismidir. Raqamli makonda turli kiberhujumlarning ko‘payishi, zararli dasturlar, ijtimoiy muhandislik usullari va ma’lumotlarning o‘g‘irlanishi xavfini oshirmoqda. Shu sababli, ma’lumotlarni himoya qilish bo‘yicha samarali yondashuv va texnologiyalarni qo‘llash zamon talabi hisoblanadi.

Ma’lumotlar xavfsizligining nazariy asoslari

Zamonaviy axborot tizimlarida ma’lumotlar xavfsizligini ta’minlash masalasi texnologik rivojlanish jarayonida eng muhim yo‘nalishlardan biri sifatida qaraladi. Raqamli axborot hajmining ortishi, tarmoqlar orqali ma’lumot almashinuvi tezlashishi va xizmatlar onlayn formatga o‘tishi natijasida xavfsizlikka bo‘lgan talab ham keskin oshdi. Ma’lumotlar xavfsizligining asosiy tamoyillari sifatida maxfiylik, yaxlitlik va mavjudlik prinsiplari alohida o‘rin tutadi. Ushbu tamoyillar axborotni yetkazish, saqlash va qayta

ishlash jarayonlarida ma’lumotlarning buzilmasligi, o‘zgarmasligi hamda ruxsatsiz kirishlardan himoyalanishini ta’minlaydi.

Maxfiylik tamoyili ma’lumotlarga faqat ruxsat etilgan shaxslar tomonidan murojaat qilinishini anglatadi. Zamonaviy axborot tizimlarida bu tamoyil kriptografik usullar, shifrlash algoritmlari, kirishni boshqarish mexanizmlari va autentifikatsiya vositalari orqali amalga oshiriladi. Shifrlash ma’lumotlarni tarmoqlar orqali uzatilayotgan vaqtda ham, saqlanayotgan paytda ham xavfsizligini ta’minlayshga xizmat qiladi. Maxfiylikning ishonchli ta’minlanishi axborot tizimlarida ishlatiladigan himoya qatlamlarining to‘g‘ri tashkil etilganligiga bevosita bog‘liqdir.

Ma’lumotlar yaxlitligi esa axborotning o‘zgarmasligi va tashqi ta’sirlar natijasida buzilmasligini nazarda tutadi. Yaxlitlikni himoya qilishda raqamli imzo, xesh-funksiyalar, nazorat yig‘indilari va tranzaksiyalarni boshqarish tizimlari qo‘llanadi. Bu mexanizmlar ma’lumotlarni har qanday ruxsatsiz o‘zgarishlardan himoya qiladi va axborot ishonchliligini ta’minlaydi. Ma’lumotlarning yaxlitligiga putur yetishi natijasida tizimlar faoliyatida jiddiy xatoliklar yuzaga kelishi mumkin, shu bois ushbu tamoyil axborot tizimlarining barqaror ishlashi uchun zarur bo‘lgan asosiy omillardan biri hisoblanadi.

Mavjudlik tamoyili ma’lumotlardan istalgan vaqtda foydalanish imkoniyatining doimiy saqlanishini bildiradi. Axborot tizimlarining uzluksiz faoliyat yuritishi bugungi kunda iqtisodiy, ijtimoiy va boshqaruv jarayonlari uchun juda muhimdir. DDoS hujumlari, serverlarning ishdan chiqishi, elektr uzilishlari yoki dasturiy nosozliklar mavjudlikka eng katta xavflardan biri hisoblanadi. Shu sababli tizimlarda zaxira serverlar, avariyadan tiklash mexanizmlari, muntazam zaxiralash siyosatlari va monitoring tizimlari joriy etiladi. Ma’lumotlarning mavjudligini ta’minlash zamonaviy axborot tizimlarining barqarorligini oshiradi.

Axborot tizimlarida xavfsizlikni ta’minlashning yana bir muhim jihati autentifikatsiya va avtorizatsiya jarayonlarining to‘g‘ri tashkil etilishidir. Foydalanuvchi shaxsini aniqlash, uning tizimdagi huquqlarini belgilash, kirish darajalarini boshqarish va ruxsatlarni nazorat qilish kiberxavfsizlikning ajralmas qismidir. Ko‘p bosqichli autentifikatsiya, biometrik tizimlar, tokenlar va kalitlar kabi texnologiyalar zamonaviy xavfsizlik talablariga javob beradi.

Shuningdek, axborot tizimlarining xavfsizligini ta’minlashda monitoring, audit va nazorat mexanizmlarining ahamiyati beqiyosdir. Tizimda sodir bo‘layotgan jarayonlarni doimiy kuzatib borish, loglarni tahlil qilish, potensial xavflarni aniqlash va ularga vaqtida javob qaytarish xavfsizlikning mustahkamligini oshiradi. IDS/IPS tizimlari, SIEM platformalari va xavfsizlik jurnallari xavfli harakatlarni erta aniqlashda yordam beradi.

Zamonaviy axborot tizimlarida ma’lumotlar xavfsizligini ta’minlash tamoyillari kompleks yondashuvni talab qiladi. Birgina texnik vositalar yoki dasturiy vositalar yetarli emas, balki barcha tamoyillar o‘zaro bog‘liq holda, yagona xavfsizlik strategiyasi asosida qo‘llanilishi zarur. Shu tarzda axborot tizimlarining barqaror, ishonchli va xavfsiz ishlashi ta’minlanadi.

Xulosa

Ma’lumotlar xavfsizligi zamonaviy axborot tizimlarining ajralmas qismi bo‘lib, u axborot resurslarini turli ichki va tashqi tahdidlardan himoya qilishga qaratilgan. Ushbu maqolada xavfsizlikning nazariy asoslari, ya’ni maxfiylik, yaxlitlik va mavjudlik tamoyillari, shuningdek, ma’lumotlarni himoya qilishning asosiy mexanizmlari — shifrlash, autentifikatsiya, avtorizatsiya va tarmoq xavfsizligi nazariy jihatdan yoritildi.

Kiberhujumlarning ko‘payishi va turlicha shakllarda sodir bo‘lishi ma’lumotlar xavfsizligini ta’minlashda qatlamli va kompleks yondashuvni zarur qiladi. Shu sababli, ma’lumotlarni himoya qilish siyosati va texnologik choralarning uyg‘unligi axborot resurslarini samarali himoya qilish uchun muhim ahamiyat kasb etadi. Nazariy asoslar va amaliy mexanizmlar uyg‘unligi tashkilotlarning axborot tizimlarini ishonchli va barqaror ishlashini ta’minlashga xizmat qiladi.

FOYDALANILGAN ADABIYOTLAR

1. Stallings, W. (2020). Cryptography and Network Security: Principles and Practice. Pearson.
2. Pfleeger, C., Pfleeger, S. (2015). Security in Computing. Prentice Hall.
3. Bishop, M. (2018). Computer Security: Art and Science. Addison-Wesley.
4. Whitman, M. E., Mattord, H. J. (2018). Principles of Information Security. Cengage Learning.
5. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.
6. ISO/IEC 27001:2013. Information Security Management Systems (ISMS) Standard. International Organization for Standardization.
7. Stallings, W. (2017). Network Security Essentials: Applications and Standards. Pearson.
8. Andress, J. (2019). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress.
9. Easttom, C. (2020). Computer Security Fundamentals. Pearson IT Certification.
10. Gonzalez, R., & Vasquez, M. (2018). Cybersecurity: Principles, Techniques, and Applications. CRC Press.