RAQAMLI TA'LIM MUHITIDA MA'LUMOTLAR XAVFSIZLIGINI TA'MINLASHNING ZAMONAVIY TEXNOLOGIYALARI

Zulxumor Ravshanova
Osiyo xalqaro universiteti magistranti
https://doi.org/10.5281/zenodo.20611508

Annotatsiya. Ushbu maqolada raqamli ta'lim muhitida ma'lumotlar xavfsizligini ta'minlashning zamonaviy texnologiyalari tahlil qilingan. Tadqiqotda identifikatsiya, autentifikatsiya va avtorizatsiya mexanizmlarining zamonaviy modellari, ma'lumotlarni shifrlash texnologiyalari, monitoring va audit tizimlari hamda axborot xavfsizligi hodisalariga javob berish usullari o'rganilgan. Shuningdek, ta'lim muassasalarida axborot xavfsizligini ta'minlashning amaliy jihatlari yoritilib, mavjud kiberxavflarni kamaytirish bo'yicha tavsiyalar ishlab chiqilgan.

Kalit so'zlar: raqamli ta'lim muhiti, axborot xavfsizligi, autentifikatsiya, avtorizatsiya, shifrlash, monitoring, audit, kiberxavfsizlik.

Abstract. This article analyzes modern technologies for ensuring information security in digital educational environments. The study examines identification, authentication, and authorization mechanisms, data encryption technologies, monitoring and auditing systems, as well as incident response approaches. Furthermore, the practical aspects of information security management in educational institutions are discussed, and recommendations are proposed to reduce cybersecurity risks.

Keywords: digital educational environment, information security, authentication, authorization, encryption, monitoring, auditing, cybersecurity.

Bugungi kunda ta'lim tizimida raqamli texnologiyalarning keng joriy etilishi natijasida elektron ta'lim platformalari, masofaviy ta'lim tizimlari va bulutli xizmatlardan foydalanish ko'lami sezilarli darajada kengayib bormoqda. Ushbu jarayon ta'lim sifatini oshirish, o'quv resurslariga tezkor kirishni ta'minlash va ta'lim jarayonini samarali tashkil etish imkonini bermoqda .

Raqamli ta'lim muhitida katta hajmdagi ma'lumotlar, jumladan talabalar, o'qituvchilar va ta'lim muassasalariga oid axborotlar elektron shaklda saqlanadi hamda uzatiladi. Shu sababli mazkur ma'lumotlarning maxfiyligi, yaxlitligi va foydalanish imkoniyatini ta'minlash muhim vazifalardan biri hisoblanadi .

So'nggi yillarda kiberhujumlar sonining ortishi, zararli dasturlarning takomillashuvi hamda ma'lumotlarni noqonuniy egallash holatlarining ko'payishi ta'lim muassasalarida axborot xavfsizligini ta'minlashga qaratilgan zamonaviy texnologiyalarni joriy etishni talab etmoqda . Ayniqsa, masofaviy ta'lim

tizimlarining rivojlanishi foydalanuvchilarni autentifikatsiyalash, ma'lumotlarni shifrlash va xavfsizlik hodisalarini monitoring qilish masalalarining ahamiyatini yanada oshirdi . Raqamli ta'lim muhitida ma'lumotlar xavfsizligini ta'minlash identifikatsiya, autentifikatsiya va avtorizatsiya mexanizmlaridan foydalanish, zamonaviy kriptografik algoritmlarni qo'llash, monitoring va audit tizimlarini joriy etish hamda hodisalarga tezkor javob berish mexanizmlarini shakllantirish orqali amalga oshiriladi . Shu nuqtai nazardan mazkur maqolada raqamli ta'lim muhitida ma'lumotlar xavfsizligini ta'minlashning zamonaviy texnologiyalari tahlil qilinadi va ularning amaliy ahamiyati yoritiladi.

Identifikatsiya, autentifikatsiya va avtorizatsiyaning zamonaviy texnologiyalari.

Raqamli ta'lim muhitida axborot xavfsizligini ta'minlashning muhim shartlaridan biri foydalanuvchilarni ishonchli identifikatsiya qilish va ularning tizim resurslaridan foydalanish huquqlarini nazorat qilish hisoblanadi. Ushbu vazifalar identifikatsiya, autentifikatsiya va avtorizatsiya mexanizmlari orqali amalga oshiriladi. Identifikatsiya foydalanuvchining tizimga o'zini tanishtirish jarayoni bo'lsa, autentifikatsiya uning haqiqiyligini tekshirishga xizmat qiladi .

Zamonaviy axborot tizimlarida quyidagi autentifikatsiya usullari keng qo'llaniladi:

Parol asosidagi autentifikatsiya;

Ikki faktorli autentifikatsiya (2FA);

Biometrik autentifikatsiya;

Token va smart-karta asosidagi autentifikatsiya;

Bir martalik parollar (OTP).

Ushbu usullar orasida ikki faktorli autentifikatsiya eng ishonchli himoya vositalaridan biri hisoblanadi. Ushbu usul foydalanuvchidan nafaqat parolni, balki qo'shimcha tasdiqlovchi vositani ham talab qiladi. Natijada hisoblarni buzish va ruxsatsiz kirish ehtimoli sezilarli darajada kamayadi. Hozirgi kunda ko'plab LMS platformalarida ikki faktorli autentifikatsiya texnologiyasi muvaffaqiyatli joriy etilgan .

Autentifikatsiyadan muvaffaqiyatli o'tgan foydalanuvchilarning vakolatlarini boshqarish avtorizatsiya mexanizmlari orqali amalga oshiriladi. Eng keng tarqalgan model RBAC (Role-Based Access Control) modeli bo'lib, unda foydalanuvchilarga ularning lavozimi yoki vazifasiga qarab huquqlar beriladi . Masalan:

Administrator	**Tizimni to‘liq boshqarish;**
O‘qituvchi	Kurslarni yaratish va boshqarish;
Talaba	O‘quv materiallaridan foydalanish.

RBAC modeli ta’lim muassasalarida axborot resurslaridan foydalanishni samarali nazorat qilish va ma’lumotlarning maxfiyligini ta’minlash imkonini beradi.

Ma’lumotlarni shifrlash va himoyalash texnologiyalari

Raqamli ta’lim muhitida ma’lumotlarni himoyalashning eng samarali vositalaridan biri kriptografik texnologiyalardan foydalanish hisoblanadi. Kriptografiya ma’lumotlarni maxsus matematik algoritmlar yordamida shifrlash orqali ularni ruxsatsiz foydalanishdan himoya qiladi. Ayniqsa, elektron ta’lim platformalarida saqlanayotgan talabalar ma’lumotlari, baholash natijalari va shaxsiy axborotlarning xavfsizligini ta’minlashda shifrlash texnologiyalarining ahamiyati katta .

Bugungi kunda quyidagi algoritmlar keng qo‘llanilmoqda:

AES (Advanced Encryption Standard);
RSA (Rivest-Shamir-Adleman);
ECC (Elliptic Curve Cryptography);
TLS/SSL protokollari[1].

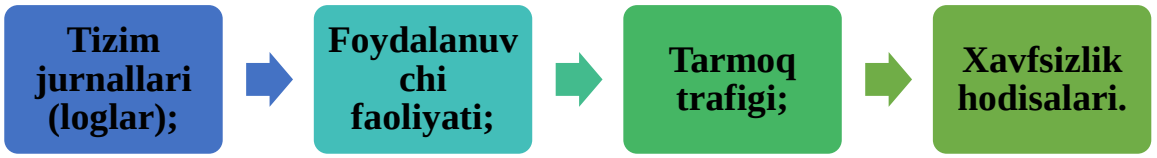
AES algoritmi ma’lumotlarni saqlash jarayonida yuqori darajadagi himoyani ta’minlaydi. RSA algoritmi esa ochiq kalitli kriptografiya asosida ishlaydi va xavfsiz kalit almashinuvida qo‘llaniladi. ECC algoritmi kichik hajmdagi kalitlardan foydalanish orqali yuqori darajadagi xavfsizlikni ta’minlaydi. TLS/SSL protokollari esa internet orqali uzatilayotgan ma’lumotlarni himoya qilishga xizmat qiladi. Bulutli texnologiyalar asosida ishlovchi ta’lim platformalarida ushbu texnologiyalardan foydalanish ma’lumotlarning maxfiyligi va yaxlitligini saqlash imkonini beradi.

Monitoring, audit va hodisalarga javob berish texnologiyalari

Axborot xavfsizligini ta’minlashda monitoring va audit tizimlari muhim o‘rin tutadi. Ular tizim faoliyatini doimiy nazorat qilish, xavfsizlik bilan bog‘liq hodisalarni aniqlash hamda ehtimoliy tahdidlarning oldini olish imkonini beradi. Monitoring vositalari orqali foydalanuvchilar faoliyati va tarmoq infratuzilmasining holati real vaqt rejimida kuzatib boriladi .

[1] Paar C., Pelzl J. *Understanding Cryptography: A Textbook for Students and Practitioners.* Berlin: Springer-Verlag, 2010. – P. 51–72.

Monitoring jarayonida quyidagi obyektlar nazorat qilinadi:



Audit esa axborot tizimlarining xavfsizlik standartlari va talablariga muvofiqligini baholash imkonini beradi. Audit natijalari asosida mavjud zaifliklar aniqlanadi va ularni bartaraf etish bo‘yicha tavsiyalar ishlab chiqiladi. Zamonaviy tashkilotlarda SIEM (Security Information and Event Management) tizimlari qo‘llanilib, turli manbalardan kelayotgan xavfsizlik ma’lumotlari markazlashtirilgan holda yig‘iladi va tahlil qilinadi .

Kiberhujumlar yoki axborot xavfsizligi hodisalari yuz berganda Incident Response (IR) jarayonlari amalga oshiriladi. Mazkur jarayon quyidagi bosqichlarni o‘z ichiga oladi:

1.Hodisani aniqlash;
2.Hodisani tahlil qilish;
3.Zararni cheklash;
4.Muammoni bartaraf etish;
5.Tizimni tiklash;
6.Yakuniy hisobot tayyorlash.

Ushbu bosqichlarning ketma-ket va samarali bajarilishi ta’lim muassasalari axborot tizimlarining uzluksiz ishlashini ta’minlash hamda ma’lumotlar xavfsizligini yuqori darajada saqlash imkonini beradi.

Xulosa. Raqamli ta’lim muhitining jadal rivojlanishi ta’lim muassasalarida ma’lumotlar xavfsizligini ta’minlash masalasining dolzarbligini oshirmoqda. Tadqiqot natijalari identifikatsiya, autentifikatsiya va avtorizatsiya mexanizmlaridan samarali foydalanish foydalanuvchilarni ishonchli aniqlash va axborot resurslariga ruxsatlarni boshqarishda muhim ahamiyatga ega ekanligini ko‘rsatdi. Shuningdek, AES, RSA va ECC kabi kriptografik algoritmlar hamda TLS/SSL protokollari ma’lumotlarning maxfiyligi va yaxlitligini ta’minlashda samarali vosita hisoblanadi. Monitoring, audit va Incident Response texnologiyalarining qo‘llanilishi esa xavfsizlik tahdidlarini o‘z vaqtida aniqlash va ularning salbiy oqibatlarini kamaytirish imkonini beradi. Xulosa qilib aytganda, zamonaviy xavfsizlik texnologiyalarini kompleks ravishda joriy etish ta’lim

muassasalarida ishonchli, xavfsiz va barqaror raqamli ta'lim muhitini shakllantirishning muhim omili hisoblanadi.

Foydalanilgan adabiyotlar:

1. Bishop M. Computer Security: Art and Science. Addison-Wesley, 2019. - P. 27-35.
2. Cichonski P., Millar T., Grance T., Scarfone K. Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2). Gaithersburg, MD: National Institute of Standards and Technology, 2012. - P. 19-42.
3. Easttom C. Computer Security Fundamentals. 5th Edition. Hoboken, NJ: Pearson IT Certification, 2022. - P. 187-201.
4. Ferraiolo D.F., Kuhn D.R., Chandramouli R. Role-Based Access Control. 2nd Edition. Norwood, MA: Artech House, 2007. - P. 45-58.
5. Grassi P.A., Garcia M.E., Fenton J.L. Digital Identity Guidelines: Authentication and Lifecycle Management (NIST Special Publication 800-63B). Gaithersburg, MD: National Institute of Standards and Technology, 2023. - P. 16-28.
6. Grassi P.A., Garcia M.E., Fenton J.L. Digital Identity Guidelines: Authentication and Lifecycle Management (NIST Special Publication 800-63B). Gaithersburg, MD: National Institute of Standards and Technology, 2023. - P. 33-39.
7. ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems - Requirements. - P. 1-12.
8. NIST SP 800-63B. Digital Identity Guidelines: Authentication and Lifecycle Management. National Institute of Standards and Technology, 2023. - P. 5-14.
9. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Berlin: Springer-Verlag, 2010. - P. 51-72.
10. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson Education, 2023. - P. 3-8.
11. Stallings W. Cryptography and Network Security: Principles and Practice. 8th Edition. Harlow: Pearson Education Limited, 2023. - P. 231-245.
12. Whitman M.E., Mattord H.J. Principles of Information Security. 7th ed. Boston: Cengage Learning, 2022. - P. 15-21.