INTELLEKTUAL O‘QITISH TIZIMLARIDA TIZIM XAVFSIZLIGINI TA’MINLOVCHI MODELLAR VA ALGORITMLAR

Maxamadov Rustam Xabibullaevich
IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi katta o‘qituvchisi, mustaqil izlanuvchi
Djamatov Mustafa Xatamovich
IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi katta o‘qituvchisi, f.-m.f.n.

Annotatsiya: Ushbu maqola intellektual o‘qitish tizimlarida tizim xavfsizligini ta’minlash bo‘yicha ilg‘or modellar va algoritmlarni tahlil qilinadi. Maqolada kriptografik shifrlash usullari, axborot xavfsizligi modellarini tahlil qilish, va sun’iy intellekt yordamida tahdidlarni aniqlash kabi yondashuvlar ko‘rib chiqiladi. Tadqiqot natijalari shuni ko‘rsatadiki, AES shifrlash algoritmi, Clark-Wilson modeli va mashinali o‘qitish asosida tahdidlarni bashorat qilish eng samarali usullar hisoblanadi. Kelajakda blokcheyn texnologiyalari va Zero Trust Security modeli asosida tizim xavfsizligini yanada mustahkamlash mumkin.

Kalit so‘zlar: Intellektual o‘qitish tizimlari, axborot xavfsizligi, kriptografik algoritmlar, AES va RSA shifrlash, Bell-LaPadula modeli, sun’iy intellekt asosida tahdidlarni aniqlash, mashinali o‘qitish, intellektual tizimlar.

Аннотация: В данной статье анализируются передовые модели и алгоритмы обеспечения безопасности систем в интеллектуальных обучающих системах. В статье рассматриваются такие подходы, как методы криптографического шифрования, анализ моделей информационной безопасности и обнаружение угроз с использованием искусственного интеллекта. Результаты исследования показывают, что наиболее эффективными методами являются алгоритм шифрования AES, модель Кларка-Уилсона и прогнозирование угроз на основе машинного обучения. В перспективе возможно дальнейшее усиление безопасности систем на основе технологий блокчейна и модели Zero Trust Security.

Ключевые слова: Интеллектуальные обучающие системы, информационная безопасность, криптографические алгоритмы, шифрование AES и RSA, модель Белла-ЛаПадулы, обнаружение угроз на основе искусственного интеллекта, машинное обучение.

Abstract: This article analyzes advanced models and algorithms for ensuring system security in intelligent learning systems. The article considers approaches such as cryptographic encryption methods, analysis of information security models, and threat detection using artificial intelligence. The results of the study show that the AES encryption algorithm, the Clark-Wilson model and threat prediction based

ISSN 3030-3907

on machine learning are the most effective methods. In the future, it is possible to further strengthen system security based on blockchain technologies and the Zero Trust Security model.

Keywords: Intelligent learning systems, information security, cryptographic algorithms, AES and RSA encryption, Bell-LaPadula model, threat detection based on artificial intelligence, machine learning.

Kirish

O‘qitish jarayonlarida kursantlarning kasbiy hamda individual rivojlanishi jarayonini tashkil etishga nisbatan innovatsion yondashuv sifatida ixtisoslik fanlarini intellektual tizimlar asosida o‘qitishning maqsadi, tarkibi va qo‘llash texnologiyalarini ishlab chiqish hozirgi kunning dolzarb muamolaridan biri hisoblanadi. O‘qitishning intellektual tizimi sun’iy intellekt metodlari va vositalarining avtomatlashtirilgan o‘qitish sohasida qo‘llanishining amaliy natijasi bo‘lib, ta’lim tizimlarining yangi avlodi hisoblanib, ularning xavfsizligini ta’minlash zaruratga aylanmoqda.

Intellektual o‘qitish tizimlari zamonaviy ta’limning rivojlanayotgan sohasi bo‘lib, ularda sun’iy intellekt, moslashuvchan dasturiy ta’minot va shaxsiylashtirilgan ta’lim jarayonlari asosida o‘quv jarayoni optimallashtiriladi[1]. Biroq, bu tizimlar kiberxavfsizlik tahdidlari bilan ham to‘qnash keladi, jumladan:

- ma’lumotlar maxfiyligi buzilishi – shaxsiy ma’lumotlar hackerlar tomonidan o‘g‘irlanishi mumkin.
- zararli hujumlar – sun’iy intellekt tizimlariga kiberhujumlar tashkillashtirilishi ehtimoli mavjud.
- foydalanuvchilar autentifikatsiyasi – tizimda noto‘g‘ri identifikatsiya va parollar bilan kirish xavfi mavjud[2].

Ushbu maqolada intellektual o‘qitish tizimlari xavfsizligini oshirish uchun kriptografik shifrlash usullari, axborot xavfsizligi modellarini tahlil qilish va sun’iy intellekt yordamida tahdidlarni aniqlash kabi muhim yondashuvlar batafsil ko‘rib chiqiladi.

USULLAR

Axborot xavfsizligini ta’minlash va boshqarish uchun quyidagi kriptografik shifrlash usullari va modellarni tahlil qilib chiqamiz:

AES (Advanced Encryption Standard) algoritmi - intellektual o‘qitish tizimlarida o‘quvchilar ma’lumotlari, o‘quv kurslari va foydalanuvchilar autentifikatsiyasi kabilar himoyalanadi. AES algoritmi simmetrik shifrlash usuli bo‘lib, har bir ma’lumot 256-bit uzunlikdagi kalit yordamida shifrlanadi. AES-256 versiyasi yuqori xavfsizlik darajasini ta’minlaydi.

Uning matematik formulasi quyidagicha:

ISSN 3030-3907

$$C=E(K,P)$$

Bu yerda:

C – shifrlangan matn

E – AES shifrlash funksiyasi

K – maxfiy kalit

P – ochiq matn

AES shifrlashning asosiy afzalliklari quyidagilardan iborat:

- yuqori tezlik – kam resurs talab qiladi;

- foydalanuvchi autentifikatsiyasi - AES algoritmi foydalanuvchi parollarini shifrlashda ishlatiladi. Shaxsiy ma'lumotlar hash funksiyasi bilan saqlanadi va tizimga kirish vaqtida AES yordamida dekriptirovka qilinadi[3];

- kiberhujumlardan himoya (kiberhujumlarga qarshilik qilish) – intellektual o'qitish tizimlarida AES shifrlash modeli quyidagi tahdidlarga qarshi qo'llaniladi: MITM (Man-in-the-middle) hujumlariga qarshi – ma'lumotlarni shifrlangan holda uzatish.SQL Injection hujumlariga qarshi – shifrlangan foydalanuvchi ma'lumotlarini ishlatish. Ransomware hujumlarini oldini olish – AES bilan zaxira nusxalarni shifrlash. Brute-force hujumlariga qarshi - chidamli va yuqori darajadagi himoya ta'minlash;

- ma'lumotlar bazasini himoyalash - intellektual o'qitish tizimlarida talabalar reytinglari, test natijalari va foydalanuvchi profillari AES orqali shifrlanadi. Buning uchun SQL ma'lumotlar bazasida AES-256 shifrlash integratsiya qilinadi.

RSA (Rivest-Shamir-Adleman) – asimmetrik shifrlash usuli bo'lib, ochiq va maxfiy kalitlar yordamida ma'lumotlarni himoya qilishga asoslangan. Intellektual o'qitish tizimlarida talaba va o'qituvchilarning shaxsiy hisoblarini himoya qilish uchun RSA algoritmi ishlatiladi. RSA ochiq va maxfiy kalit asosida ishlaydi, bu esa tizimga faqat tasdiqlangan foydalanuvchilar kirishiga imkon beradi.

RSA shifrlash algoritmining matematik formulasi:

$$C=P^e \bmod N$$

Bu yerda:

C – shifrlangan matn

P – ochiq matn

^{e} – ochiq kalit

N – modul

RSA shifrlash algoritmining afzalliklari quyidagilardan iborat:

- shaxsiy ma'lumotlar himoyasi - talabalar o'quv natijalari, imtiyozli kirish huquqlari, va xavfsizlikka aloqador hujjatlar RSA yordamida shifrlanadi. RSA algoritmi ma'lumotlarni faqat ruxsat berilgan foydalanuvchilar o'qishi va o'zgartira olishini ta'minlaydi[4];

ISSN 3030-3907

- tizimda autentifikatsiya jarayonini mustahkamlaydi - RSA yordamida hujjatlarning autentikligi kafolatlanadi va foydalanuvchilar tomonidan buzib o‘zgartirish oldini olinadi;
- elektron imzolarni yaratish imkoniyati - Intellektual o‘qitish tizimlarida o‘qituvchilar va talabalar o‘rtasidagi rasmiy hujjatlar RSA orqali elektron imzo bilan tasdiqlanadi. Hujjatlarga elektron imzo qo‘yish uchun RSA yordamida xesh-funksiyalar ishlatiladi.

Axborot xavfsizligi modellarini qisqacha tahlil qilamiz:

Clark-Wilson modeli - bu model ma’lumotlarning ishonchliligini va integratsiyasini ta’minlashga asoslangan. Har bir operatsiya tasdiqlash mexanizmi orqali o‘tadi.

Uning asosiy matematik formulasi quyidagicha:

$$I(T)=A(U)+P$$

Bu yerda:
I(T) – tranzaksiyalarning ishonchliligi
A(U) – foydalanuvchi huquqlari
P – ma’lumotlarni tasdiqlash mexanizimi
Clark-Wilson modeli quyidagilarni ta’minlaydi:
- ma’lumotlar uzatish xavfsizligi ta’minlash;
- tizimga buzib kirish ehtimolini minimallashtirish;
- Intellektual o‘qitish tizimi platformalarida ishonchli integratsiya qilish.

Bell-LaPadula modeli - bu model ma’lumotlar maxfiyligi va huquqlar boshqaruvi uchun ishlatiladi. Foydalanuvchilar faqat belgilangan darajadagi ma’lumotlarni o‘qishi va o‘zgartirishi mumkin.

Uning matematik formulasi quyidagicha:

$$S \leq 0$$

Bu yerda:
S – subyekt (foydalanuvchi)
O – obyekt (ma’lumotlar darajasi)
Bell-LaPadula modeli quyidagilarni ta’minlaydi:
- maxfiylik siyosatini nazorat qiladi;
- ma’lumotlar oqimi xavfsizligini ta’minlaydi;
- kiberhujumlarga qarshilik qiladi.

Sun’iy intellekt asosida tahdidlarni aniqlash:

Sun’iy intellekt kiberxavfsizlikda anomaliyalarni aniqlash, hujumlarni prognoz qilish va himoya strategiyalarini moslashtirish uchun ishlatiladi.

Mashinali o‘qitish algoritmlari

Ma’lumotlar tahdidlarini aniqlash uchun Supervised Learning usullari ishlatiladi[6].

Uning matematik formulasi quyidagicha:

$$P(T)=X/(X+Y)$$

ISSN 3030-3907

Bu yerda:
P(T) – tahdidni aniqlash ehtimoli;
X – zararli hujumlar soni;
Y – normal tizim holatlari.
Mashinali o‘qitishning afzalliklari quydagilardan iborat:
- avtomatik tahdidlarni aniqlash;
- real vaqtda hujumlarni bashorat qilish;
- tizim xavfsizligini doimiy ravishda optimallashtirish.
Unsupervised Learning algoritmi

Bu usul ma’lumotlarni katta hajmda tahlil qilib, anomaliyalarni aniqlashga yordam beradi.

$$A = \frac{1}{n}\sum_{i=0}^{n}(X_i - X)^2$$

Bu yerda:
A – anomaliyalar darajasi (ya’ni dispersiya, variatsiya o‘lchovi);
X_i – ma’lumotlar to‘plamidagi i-element;
X – ma’lumotlarning o‘rtacha qiymati;
n – ma’lumotlar soni (butun to‘plamdagi elementlar soni).
Unsupervised Learning algoritmining afzalliklari quyidagilardan iborat[7]:
- kiberhujumlarni ilgari aniqlash;
- mustaqil ravishda tahdidlarni aniqlash;
- intellektual o‘qitish tizimlarini himoyalash.
Grafik analizlar (Graphical Analysis)

Quyidagi grafiklar intellektual o‘qitish tizimlarida xavfsizlikni ta’minlash bo‘yicha asosiy tendensiyalarni hisoblanadi:

Ma’lumotlar shifrlash samaradorligi – AES algoritmi 99.7% darajada ma’lumotlarni himoya qiladi. Sun’iy intellekt asosida tahdidlarni aniqlash – kiberhujumlarni 89% aniqlik bilan prognoz qilishga yordam beradi[7]. RBAC modeli esa foydalanuvchi huquqlarini boshqarish – tizimning 83% ishonchliligini oshiradi[8].
Matematik modellar (Mathematical Models)

Intellektual o‘qitish tizimlarida xavfsizlikni ta’minlash uchun quyidagi matematik modellar qo‘llaniladi:
Shifrlash modeli:

$$C=E(K,P)$$

Bu yerda:
C – shifrlangan matn
E – AES shifrlash funksiyasi
K – maxfiy kalit

ISSN 3030-3907

P – ochiq matn

Sun’iy intellekt asosida tahdidlarni aniqlash modeli:

$$P(T)=X/(X+Y)$$

Bu yerda:

P(T) – tahdidni aniqlash ehtimoli;

X – zararli hujumlar soni;

Y – normal tizim holatlari.

RBAC modeli:

$$A(U) = \bigcup_{i=1}^{n} R_i$$

Bu yerda:

$A(U)$ – foydalanuvchi U ning umumiy huquqlari

R_i – foydalanuvchi i - rolga ega bo‘lganda beriladigan huquqlar

$\bigcup$ – barcha rollar bo‘yicha huquqlar to‘plami

MUHOKAMA VA NATIJALAR

Yuqori model va algoritmlarni tahlil qilib, ularning azfalliklari, kamchiliklari, qo‘llanilish sohasi va intellektual tizimdagi roli quyidagi jadvalda keltiramiz

1-jadval

Model va algoritmlarning qiyosiy tahlili

Model / Algoritm	Qo‘llanilish yo‘nalishi	Afzalliklari	Kamchiliklari	Intellektual tizimdagi roli
AES	Ma’lumotlarni shifrlash	Tez, 256-bit kalit, samarali, past resurs sarfi	Kalit almashinuvi uchun alohida mexanizm zarur	Ma’lumotlar, test natijalarini shifrlashda qo‘llaniladi
RSA	Autentifikatsiya, elektron imzo	Ochiq/maxfiy kalit, xavfsiz uzatish, imzo yaratish	Sekin ishlaydi, katta kalit kerak	Kirish nazorati, hujjatlarni imzolash
Clark–Wilson modeli	Ma’lumotlar yaxlitligi va transaktsiya	Tranzaksiyani nazorat qilish, ruxsatli amallar	Maxsus interfeys va audit tizimi kerak	Ma’lumotlar ishonchliligini saqlash

ISSN 3030-3907

		doirasida ishlash		
Bell–LaPadula modeli	Maxfiylik siyosati	Maxfiylikni qat'iy saqlash, harbiy tizimlar uchun mos	Ma'lumotlar integratsiyasiga e'tibor bermaydi	Ma'lumotlarni o'qish/yozishni darajali boshqarish
RBAC	Kirish huquqlari boshqaruvi	Rollar asosida soddalashtirilgan tizim	Murakkab rollar va ierarxiyalarni boshqarish qiyin	Talaba/o'qituvchi/admin huquqlarini aniq taqsimlash
K-Means	Klasterizatsiya	Soddaligi, katta ma'lumotlarga mos	Klaster soni oldindan belgilanadi, sferik shakllarga mos	Foydalanuvchi xatti-harakatini guruhlash

Yuqoridagi ma'lumotlarni tahlil qilish natijalari shuni ko'rsatadiki, sun'iy intellekt va kriptografik metodlar eng samarali himoya vositalari hisoblanadi:

- AES shifrlash algoritmi – Intellektual o'qitish tizimlarida eng xavfsiz va tezkor usul ekanligi isbotlandi[9].
- Clark-Wilson modeli – Intellektual o'qitish tizimlarining uzluksiz ishlashini ta'minladi.
- Mashinali o'qitish algoritmlari – kiberhujumlarni aniqlashni 89% aniqlik bilan amalga oshirdi.

Shuningdek, kelajakda quyidagi takomillashtirish zarur:

- blockchain asosida ma'lumotlar himoyasi – buzib kirish ehtimolini kamaytiradi.
- biometrik autentifikatsiya – foydalanuvchi maxfiyligini oshirishga yordam beradi.
- zero trust security model – global Intellektual o'qitish tizimlarida xavfsizlikni mustahkamlaydi[10].

XULOSA VA TAKLIFLAR

Intellektual o'qitish tizimlarining xavfsizligini ta'minlash uchun quyidagi yondashuvlar eng samarali ekanligi aniqlandi: AES va RSA shifrlash algoritmlari – ma'lumotlarni yuqori darajada himoya qiladi. Clark-Wilson va Bell-LaPadula modellar – tizimda xavfsizlik siyosatini saqlaydi. Mashinali o'qitish va sun'iy intellekt asosida tahdidlarni aniqlash – kiberhujumlarni prognoz qiladi. Kelajakda

ISSN 3030-3907

quyidagi takomillashtirishlar amalga oshirilishi lozim: Blockchain asosida ma'lumotlar himoyasi – buzib kirish ehtimolini kamaytiradi. Biometrik autentifikatsiya – foydalanuvchi maxfiyligini oshiradi. Zero Trust Security Model – global intellektual o'qitish tizimlarida xavfsizlikni mustahkamlaydi.

FOYDALANILGAN ADABIYOTLAR

1. Umarov Sh.A., Abduqodirov A.. Axborot xavfsizligi tizimlarini intellektuallashtirish masalalari. Al-Farg'oniy avlodlari, 15(3), 45–60.2024
2. Kenjaboyev O. T., Allanazarov, A. Sh.. Axborot tizimi xavfsizligi. Toshkent: Uzsmart. 2013
3. Turdimatov, M.M., Sadirova X.X.. Axborotni himoyalashda chetlab o'tishning mumkin bo'lgan ehtimollik holatini baholash usullari. Cybersecurity Journal, 27(2), 112–130.2023
4. Umarov Sh. A., Sun'iy intellekt asosida tahdidlarni aniqlash. Farg'ona: Fan va texnologiya. 2019
5. Muxtarov F. M., Toshpulatov S. M.. Sun'iy intellekt vositalarini ta'limni nazorat qilish va baholashda qo'llash. Information Systems Review, 19(4), 78–95.2023
6. Khabibullayevich, M. R., & Khatamovich, D. M. (2025). Modern intellectual systems: status, functions, technologies and development tendencies. American Journal Of Applied Science And Technology, 5(02), 52-55.
7. Li, Bingcheng, Dingkang Li, and Mingyuan Zhu. "Application analysis of data encryption technology". Applied and Computational Engineering 50, no. 1 (March 25, 2024): 199–205. http://dx.doi.org/10.54254/2755-2721/50/20241502.
8. Abdullayev A., Qosimova U., Axborot xavfsizligi asoslari. Uslubiy qo'llanma. Studylib.net. 2009.
9. AES: ma'lumotlarni shifrlash. URL: https://uz.birmiss.com/aes-malumotlarni-shifrlash/
10. Toshpulatov Sh. M.. Blockchain va Zero Trust Security modeli. Samarqand: Innovatsion texnologiyalar nashriyoti. 2022

ISSN 3030-3907