



International Conference on Educational Discoveries and Humanities

Hosted online from Moscow, Russia

Website: econfseries.com

16th February, 2025

**AXBOROT TIZIMLARINI HIMOYA QILISHDA RAQAMLI
TEKNOLOGIYALAR: DOLZARB MASALALAR VA INNOVATSION
YECHIMLAR**

Otamuratova Latofat Umar qizi

Yangi asr universiteti Ta'limda axborot texnologiyalari universiteti

1-bosqich magistranti

E-mail: otamuratovalatofat4@gmail.com

Annotatsiya:

Ushbu maqola axborot tizimlarini himoya qilishda raqamli texnologiyalarning o'rnini va ahamiyatini tahlil qiladi. Maqolada axborot tizimlarining xavfsizligini ta'minlashda yuzaga kelayotgan dolzarb masalalar, jumladan, kiberxavf-xatarlarning rivojlanishi, tizimlarning murakkabligi, insider tahdidlari va ma'lumotlar uzatishdagi xavfsizlik masalalari yoritilgan. Shuningdek, axborot tizimlarini himoya qilishda qo'llanilayotgan innovatsion yechimlar, xususan, sun'iy intellekt, blokcheyn texnologiyasi, kriptografiya, bulutli texnologiyalar va Zero Trust modeli kabi ilg'or texnologiyalar keltirilgan. Maqola, shuningdek, kiberxavfsizlikni kuchaytirish uchun raqamli yechimlarning samarali qo'llanishi zarurligini ta'kidlaydi va axborot tizimlarining himoyasini yanada mustahkamlash uchun zamonaviy yondashuvlarni taklif etadi. Maqola axborot xavfsizligi sohasida ilmiy tadqiqotlar va amaliy ishlanmalar uchun qo'shimcha tavsiyalar beradi.

Kalit so'zlar: Sun'iy intellekt, blokcheyn texnologiyasi, kriptografiya, bulutli texnologiyalar, axborot texnologiyalarini himoya qilish, Zero Trust modeli

Annotation:

This article analyzes the role and importance of digital technologies in protecting information systems. It discusses the emerging critical issues in ensuring the security of information systems, including the development of cybersecurity threats, system complexity, insider threats, and security concerns related to data transmission. The article also presents innovative solutions used in protecting information systems, particularly advanced technologies such as artificial intelligence, blockchain



International Conference on Educational Discoveries and Humanities

Hosted online from Moscow, Russia

Website: econfseries.com

16th February, 2025

technology, cryptography, cloud technologies, and the Zero Trust model. Additionally, it emphasizes the need for the effective application of digital solutions to strengthen cybersecurity and proposes modern approaches to further enhance the protection of information systems. The article provides additional recommendations for scientific research and practical developments in the field of information security.

Keywords: Artificial Intelligence, Blockchain Technology, Cryptography, Cloud Technologies, Information Technology Protection, Zero Trust Model.

Аннотация:

Эта статья анализирует роль и значимость цифровых технологий в защите информационных систем. В статье рассматриваются актуальные проблемы обеспечения безопасности информационных систем, включая развитие киберугроз, сложность систем, внутренние угрозы и вопросы безопасности передачи данных. Также представлены инновационные решения, применяемые для защиты информационных систем, в частности, такие передовые технологии, как искусственный интеллект, блокчейн, криптография, облачные технологии и модель Zero Trust. Статья подчеркивает необходимость эффективного применения цифровых решений для усиления кибербезопасности и предлагает современные подходы для дальнейшего укрепления защиты информационных систем. Также статья дает дополнительные рекомендации для научных исследований и практических разработок в области информационной безопасности.

Ключевые слова: Искусственный интеллект, блокчейн-технология, криптография, облачные технологии, защита информационных технологий, модель Zero Trust.

Kirish

Axborot tizimlari zamonaviy jamiyatda iqtisodiyotning, davlat boshqaruvining, ta'lim va sog'liqni saqlash sohalarining, shuningdek, shaxsiy hayotning ajralmas



International Conference on Educational Discoveries and Humanities

Hosted online from Moscow, Russia

Website: econfseries.com

16th February, 2025

qismiga aylangan. Shu bilan birga, axborot tizimlarining xavfsizligi va himoyasi masalalari ham yuqori ahamiyat kasb etadi. Raqamli texnologiyalar va kiberxavfsizlikning tez rivojlanishi, yangi tahdidlarga va xatarlar turkumlariga olib kelmoqda. Shunday qilib, axborot tizimlarini himoya qilishda raqamli texnologiyalarni samarali qo'llash dolzarb masalalardan biri hisoblanadi.

Axborot tizimlarini himoya qilishning ahamiyati

Axborot tizimlarining himoyasizligi tashkilotlar va davlatlar uchun jiddiy oqibatlariga olib kelishi mumkin. Ma'lumotlar oqimi, personal ma'lumotlarining xavfsizligi va tizimlar o'rtasidagi o'zaro aloqalar zamonaviy kiberxavf-xatarlar, shuningdek, hujumchilarning yangi usullari bilan xavf ostida qolmoqda. Shunday qilib, axborot tizimlarini himoya qilishda yangi innovatsion yechimlarga ehtiyoj ortib bormoqda. Yaxshi tashkil etilgan xavfsizlik choralarisiz ma'lumotlarning o'g'irlanishi, tizimlarning ishdan chiqishi va hatto iqtisodiy zararlarga olib keladigan kiberhujumlar sodir bo'lishi mumkin[1].

Raqamli texnologiyalarning rolini oshirish

Bugungi kunda axborot tizimlarini himoya qilishda turli xil raqamli texnologiyalar qo'llanilmoqda. Ular quyidagi sohalarda faoliyat yuritmoqda:

Sun'iy intellekt (SI) – Sun'iy intellekt asosida ishlab chiqilgan xavfsizlik tizimlari tahdidlarni tahlil qilishda va kiberhujumlarni oldini olishda yordam beradi. Masalan, anomaliyalarga asoslangan tizimlar real vaqtda xavfli holatlarni aniqlaydi, o'zgarishlarni kuzatadi va himoya choralarini ko'radi.

Blokcheyn texnologiyasi – Ma'lumotlar va tranzaksiyalar xavfsizligini ta'minlashda blokcheyn texnologiyasi keng qo'llanilmoqda. Blokcheynning shifrlash tizimi orqali ma'lumotlarning o'zgartirilishi va o'g'irlanishi oldini olish mumkin[4].

Kriptografiya – Kriptografiya yordamida ma'lumotlarni shifrlash, saqlash va uzatishda axborot xavfsizligini ta'minlash uchun murakkab algoritmlar ishlatiladi.



International Conference on Educational Discoveries and Humanities

Hosted online from Moscow, Russia

Website: econfseries.com

16th February, 2025

Yangi avlod kriptografik usullari yordamida xavfsizlikni yanada kuchaytirish mumkin[3].

Bulutli texnologiyalar – Bulutli hisoblash tizimlari axborotlarni saqlash va ularni uzatishning yanada xavfsiz va samarali usulini taklif etadi. Bulut texnologiyalarining afzalligi shundaki, ular ma'lumotlarni real vaqt rejimida himoya qilish va kuzatish imkonini beradi.

Kiberhujumlarni aniqlash tizimlari (IDS) – Kiberhujumlarni aniqlash tizimlari, xususan, anomaliyalarga asoslangan IDS-lar yordamida tizimdagi xavfli holatlarni aniqlash va ularga tezkor javob berish mumkin[2].

Dolzarb masalalar

Axborot tizimlarini himoya qilishda bir qator dolzarb masalalar mavjud. Ulardan ba'zilar quyidagilardir:

Kiberxavf-xatarlarning rivojlanishi – Kiberxavfsizlik sohasidagi tahdidlar har yili yangi xususiyatlar bilan boyib bormoqda. Yangi avlod viruslari, ransomware hujumlari, phishing va DDoS (Distributed Denial of Service) hujumlari kabi tahdidlar axborot tizimlari uchun katta xavf tug'dirmoqda.

Tizimlarning murakkabligi – Axborot tizimlarining murakkabligi va integratsiyasi xavfsizlikni ta'minlashni qiyinlashtiradi. Tizimlar o'rtasidagi o'zaro aloqalar, murakkab ma'lumotlar bazalari va tashqi xizmatlar xavfsizlikni ta'minlashni yanada murakkablashtiradi.

Insider tahdidlari – Tashkilot ichidagi xodimlar tomonidan amalga oshirilgan hujumlar (insider threat) ham axborot tizimlarining xavfsizligini tahdid qiluvchi muammolardan biridir. Bunday tahdidlarni oldini olish uchun samarali kuzatuv tizimlari va xodimlar bilan doimiy treninglar o'tkazish zarur.



International Conference on Educational Discoveries and Humanities

Hosted online from Moscow, Russia

Website: econfseries.com

16th February, 2025

Ma'lumotlarni saqlash va uzatishda xavfsizlik – Ma'lumotlarni saqlash va uzatishda xavfsizligi ta'minlash masalasi dolzarb. Bulutli saqlash tizimlaridan foydalanish, shifrlash va autentifikatsiya mexanizmlari bu borada samarali vositalar hisoblanadi.

Innovatsion yechimlar

Axborot tizimlarini himoya qilishda innovatsion yechimlar doimiy ravishda takomillashmoqda. Ulardan ba'zilar quyidagilardir:

Zero Trust (Ishonchsizlik asosida xavfsizlik modeli) – Zero Trust modeli barcha tarmoq foydalanuvchilari va qurilmalari ishonchli emas deb hisoblaydi va har bir kirish uchun alohida tekshiruv o'tkazadi. Bu usulda barcha tizimlar va foydalanuvchilarga nisbatan teng xavfsizlik choralarini qo'llash tavsiya etiladi.

Kengaytirilgan analitika va mashina o'rganish – Kengaytirilgan analitika va mashina o'rganish algoritmlari yordamida axborot tizimlari xavfsizlik nuqtai nazaridan doimiy ravishda tahlil qilinadi va tahdidlar tezkor ravishda aniqlanadi.

Biometrik autentifikatsiya – Biometrik tizimlar, masalan, barmoq izlari, yuzni tanish, ko'z retinasini skanerlash kabi metodlar orqali foydalanuvchi autentifikatsiyasi xavfsizligini ta'minlaydi. Bu usullar o'zgartirish va soxtalashtirishga qarshi samarali himoya chorasini hisoblanadi.

Kiberxavfsizlikni boshqarish platformalari – Kiberxavfsizlikni boshqarish uchun barcha tizimlarni yagona platformada birlashtirish, ular o'rtasidagi xavfsizlikni ta'minlashda integratsiya qilish imkoniyatini yaratadi[1].

Xulosa

Axborot tizimlarini himoya qilishda raqamli texnologiyalarning roli kuchayib bormoqda. Sun'iy intellekt, blokcheyn, kriptografiya, bulutli texnologiyalar kabi innovatsion yechimlar axborot tizimlari xavfsizligini ta'minlashda muhim vosita hisoblanadi. Shuningdek, kiberxavfsizlikdagi dolzarb masalalar va tahdidlar doimiy



International Conference on Educational Discoveries and Humanities

Hosted online from Moscow, Russia

Website: econfseries.com

16th February, 2025

ravishda o'zgarib borayotgani sababli, tizimlarni himoya qilishda innovatsion va zamonaviy yondashuvlar, texnologik yechimlar samarali qo'llanilishi zarur.

Foydalanilgan Adabiyotlar

1. Cybersecurity and Cyberwar: What Everyone Needs to Know” . P.W. Singer . Allan Friedman (2013).
2. Tim Mather, Subra Kumaraswamy, Shahed Latif, (2009) “Cloud Security and Privacy an. Enterprise Perspective on Risks and Compliance”.
3. “Cryptography and Network Security: Principles and Practice” William Stallings(2016).
4. “Blockchain Basics: A Non-Technical Introduction in 25 Steps” . Daniel Drescher(2017).
5. Artificial Intelligence: A Modern Approach” (2004). Stuart J, Russell, Peter Norvig.