AXBOROT XAVFSIZLIGI VA KIBERXAVFSIZLIK MUAMMOLARI

Shahriyor Qurbonaliyev Anvarjon o'g'li
Namangan davlat universiteti
Axborot tizimlari va texnalo'giyalari yo'nalishi 1-kurs talabasi
Ilmiy rahbar: Namangan davlat universiteti "Raqamli ta`lim texnologiyalari" kafedrasi o'qituvchisi ***Ubaydullayeva Dilorom Maxmudjon qizi***

Annotatsiya. Ushbu maqolada axborot xavfsizligi va kiberxavfsizlik masalalari, ularning zamonaviy jamiyatdagi ahamiyati hamda dolzarb muammolari yoritib berilgan. Axborot tizimlarini kiberxavflardan himoyalash usullari va xavfsizlikni ta'minlash yo'llari tahlil qilingan.

Kalit so'zlar: Axborot xavfsizligi, kiberxavfsizlik, kiberhujumlar, axborotni himoyalash, kompyuter tarmoqlari, internet xavfsizligi, ma'lumotlar maxfiyligi.

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И КИБЕРБЕЗОПАСНОСТИ

Шахриёр Курбоналиев, сын Анваржона
Студент 1 курса направления «Информационные системы и технологии»
Наманганского государственного университета
Научный руководитель:
преподаватель кафедры «Цифровые образовательные технологии»
Наманганского государственного университета
Убайдуллаева Дилором Махмуджон кизи

Аннотация. В данной статье рассматриваются вопросы информационной безопасности и кибербезопасности, их значение в

современном обществе, а также актуальные проблемы в данной сфере. Проанализированы методы защиты информационных систем от киберугроз и пути обеспечения безопасности.

INFORMATION SECURITY AND CYBERSECURITY ISSUES

Shahriyor Qurbonaliyev, son of Anvarjon
1st-year student of the field Information Systems and Technologies
Namangan State University
Scientific supervisor:
Lecturer of the Department of Digital Educational Technologies
Namangan State University
Ubaydullayeva Dilorom Maxmudjon qizi

Abstract. This article discusses issues of information security and cybersecurity, their significance in modern society, and current challenges in this field. Methods of protecting information systems from cyber threats and ways to ensure security are analyzed.

Kirish

Bugungi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalariga chuqur kirib bormoqda. Xususan, davlat boshqaruvi, ta’lim tizimi, sog‘liqni saqlash, bank-moliya sohasi, sanoat va xizmat ko‘rsatish yo‘nalishlarida axborot tizimlari hamda raqamli texnologiyalardan keng foydalanilmoqda. Axborot almashinuvi tezligi va hajmining ortishi zamonaviy jamiyatning ajralmas qismiga aylangan.

Axborot resurslarining ko‘payishi bilan bir qatorda ularni himoyalash masalasi ham muhim ahamiyat kasb etmoqda. Axborot xavfsizligi tushunchasi axborotning

maxfiyligi, yaxlitligi va mavjudligini ta’minlashga qaratilgan chora-tadbirlar majmuasini anglatadi. Axborot xavfsizligi ta’minlanmagan holatlarda ma’lumotlarning yo‘qolishi, buzilishi yoki ruxsatsiz tarqalishi turli salbiy oqibatlarga olib kelishi mumkin.

Zamonaviy axborot jamiyatida kiberxavfsizlik masalasi axborot xavfsizligining muhim tarkibiy qismi sifatida namoyon bo‘lmoqda. Kiberxavfsizlik axborot tizimlari, kompyuter tarmoqlari va foydalanuvchilarning shaxsiy ma’lumotlarini turli kiberxurujlardan himoyalashni o‘z ichiga oladi. Internet tarmog‘ining global miqyosda rivojlanishi, raqamli xizmatlarning ko‘payishi kiberjinoyatlar sonining ortishiga ham sabab bo‘lmoqda.

Hozirgi kunda zararli dasturlar, viruslar, fishing hujumlari, ma’lumotlarni o‘g‘irlash, tarmoqlarga ruxsatsiz kirish kabi kiberxavflar keng tarqalgan. Ushbu tahdidlar alohida foydalanuvchilargagina emas, balki yirik tashkilotlar, bank tizimlari va davlat axborot resurslari faoliyatiga ham jiddiy zarar yetkazmoqda. Natijada axborot tizimlarining ishonchliligi va barqarorligi xavf ostida qolmoqda.

Axborot xavfsizligini ta’minlash nafaqat texnik vositalar yordamida, balki tashkiliy, huquqiy va kadrlar tayyorlash bilan bog‘liq choralarni ham qamrab oladi. Foydalanuvchilarning axborot madaniyatini oshirish, xavfsizlik qoidalariga rioya qilish ham kiberxavflarning oldini olishda muhim rol o‘ynaydi. Shu bois ushbu sohada olib borilayotgan ilmiy tadqiqotlar va amaliy ishlanmalar dolzarb hisoblanadi.

Mazkur maqolaning asosiy maqsadi axborot xavfsizligi va kiberxavfsizlik muammolarini chuqur tahlil qilish, zamonaviy kiberxavflarning asosiy turlarini aniqlash hamda axborot tizimlarini himoyalashning samarali usullarini yoritib berishdan iborat. Shuningdek, maqolada axborot xavfsizligini ta’minlashning istiqbolli yo‘nalishlari va amaliy ahamiyati ko‘rib chiqiladi.

Asosiy qism

1.Axborot xavfsizligi tushunchasi

Axborot xavfsizligi — bu axborot resurslarini, tizimlarini va ma’lumotlarni ruxsatsiz kirish, o‘zgartirish, yo‘q qilish yoki tarqatilishdan himoya qilish tizimi. Zamonaviy dunyoda axborot inson faoliyatining ajralmas qismi hisoblanadi. Shu sababli, axborot xavfsizligi muhim ahamiyat kasb etadi.

Axborot xavfsizligini ta’minlash quyidagi asosiy elementlarni o‘z ichiga oladi:

- Maxfiylik — ma’lumot faqat ruxsat etilgan foydalanuvchilar tomonidan ko‘rilishi;
- To‘liqlik — ma’lumotlar o‘zgartirilmasdan va butunligini saqlab qolishi;
- Mavjudlik — ma’lumotlar va tizimlar zarur paytda foydalanuvchilar uchun mavjud bo‘lishi. Kiberxavfsizlik va uning ahamiyati

2. Kiberxavfsizlik — bu axborot tizimlarini kiberhujumlardan, zararli dasturlardan va boshqa xavflardan himoya qilish jarayoni. Zamonaviy jamiyatda internet va raqamli texnologiyalarning keng tarqalishi kiberxavfsizlikni dolzarb masalaga aylantirdi.

Kiberxavfsizlikning asosiy yo‘nalishlari:

Tizimlarni himoya qilish — serverlar, kompyuterlar va tarmoqlarni zararli dasturlardan saqlash;

1. **Ma’lumotlarni shifrlash** — axborotni himoyalash uchun maxfiy kodlash texnologiyalarini qo‘llash;
2. **Foydalanuvchilarni o‘qitish** — xavfsiz internet va raqamli xizmatlardan foydalanish bo‘yicha treninglar tashkil etish.

3. Zamonaviy muammolar va tahdidlar

Axborot xavfsizligi sohasida bir nechta dolzarb muammolar mavjud:

- **Kiberhujumlar** — firibgarlik, xakerlik va zararli dasturlar;

- **Ma’lumotlarning yo‘qolishi** — texnik nosozlik yoki insoniy xatolik natijasida;
- **Shaxsiy ma’lumotlarning oshkor bo‘lishi** — foydalanuvchilar identifikatsiyasi va maxfiyligi buzilishi.

Bu muammolarni hal qilish uchun kompaniyalar va davlat organlari muntazam ravishda xavfsizlik protokollarini yangilab borishi va yangi texnologiyalarni joriy qilishi zarur.

4. Axborot xavfsizligini ta’minlash usullari

Axborot xavfsizligini ta’minlashda quyidagi asosiy usullar qo‘llaniladi:

- Texnik usullar — antivirus dasturlar, firewall, shifrlash texnologiyalari;
- Tashkiliy usullar — xavfsizlik siyosati, xodimlarni o‘qitish va monitoring;
- Huquqiy himoya — axborot qonunlari, shartnomalar va me’yoriy hujjatlar.

Shu bilan birga, raqamli texnologiyalarning rivojlanishi bilan yangi tahdidlar paydo bo‘lishi kiberxavfsizlikning doimiy yangilanishini talab qiladi.

Nazariy tahlil

1. Ilmiy tadqiqotlar va manbalar tahlili

Axborot xavfsizligi va kiberxavfsizlik sohasida ko‘plab ilmiy tadqiqotlar olib borilgan. Xususan:

- **Axborot xavfsizligi nazariyasi** — axborot tizimlarida ma’lumotlarni himoya qilishning nazariy asoslari, xavfsizlik protokollari va standartlari. Tadqiqotchilar ma’lumotlarning maxfiyligini, to‘liqligini va mavjudligini ta’minlash metodlarini ishlab chiqqan.
- **Kiberxavfsizlik tadqiqotlari** — zamonaviy kiberhujumlar va tahdidlarni aniqlash, ularning oldini olish usullari va xavfsizlik mexanizmlarini ishlab chiqish bo‘yicha ilmiy ishlar.

O‘tkazilgan tadqiqotlar shuni ko‘rsatadiki, axborot tizimlarini himoya qilishda texnologik va tashkiliy choralarni birgalikda qo‘llash samaraliroq natija beradi.

2. Kiberhujumlar turlari va xavf tahlili

Nazariy tahlil shuni ko‘rsatadiki, kiberhujumlar quyidagi turlarga bo‘linadi:

- **Viruslar va zararli dasturlar** — tizimlarni buzish va ma’lumotlarni yo‘q qilish maqsadida ishlatiladi;
- **Phishing va firibgarlik** — foydalanuvchilarning shaxsiy ma’lumotlarini o‘zlashtirish;
- **DDoS hujumlari** — server va tarmoqlarni ishga tushmas holga keltirish.

Har bir hujum turi uchun xavf darajasi va oqibatlari tahlil qilinadi. Masalan, moliyaviy tashkilotlarda phishing hujumlari katta iqtisodiy zarar keltiradi, davlat tizimlarida esa DDoS hujumlari axborot oqimini to‘xtatishi mumkin.

3. Nazariy asoslar va xavfsizlik standartlari

Axborot xavfsizligi sohasida bir qancha xalqaro standartlar mavjud:

- **ISO/IEC 27001** — axborot xavfsizligi boshqaruvi standarti;
- **NIST Cybersecurity Framework** — kiberxavfsizlikni baholash va boshqarish tizimi;
- **GDPR** — shaxsiy ma’lumotlarni himoya qilish bo‘yicha Yevropa standartlari.

Bu standartlar nazariy jihatdan xavfsizlikni ta’minlashning eng yaxshi amaliyotlarini belgilaydi va tashkilotlarga xavfsizlik siyosatini ishlab chiqishda yo‘l-yo‘riq beradi.

4. Metodologik yondashuvlar

Nazariy tahlilda axborot xavfsizligini ta’minlash metodologiyalari ham tahlil qilinadi:

- **Texnik metodlar** — antiviruslar, firewall, shifrlash algoritmlari;

- **Tashkiliy metodlar** — xodimlarni o‘qitish, xavfsizlik siyosati, monitoring;
- **Huquqiy metodlar** — qonunlar, me’yoriy hujjatlar va shartnomalar.

Ilmiy tadqiqotlar shuni ko‘rsatadiki, metodlarni birgalikda qo‘llash xavfsizlik tizimining samaradorligini oshiradi.

Tadqiqot metodlari

1. Tadqiqot usullari

Ushbu maqolada axborot xavfsizligi va kiberxavfsizlik sohasidagi muammolarni o‘rganish uchun quyidagi tadqiqot metodlari qo‘llanildi:

- Nazariy tahlil — ilmiy adabiyotlar, maqolalar va standartlar tahlil qilindi, mavjud kiberxavfsizlik texnologiyalari va protokollari o‘rganildi;
- Solishtirma metod — turli xavfsizlik choralarining samaradorligi taqqoslandi;
- Statistik metod — mavjud kiberhujumlar, zararli dasturlar va ma’lumot yo‘qotish holatlari bo‘yicha statistik ma’lumotlar yig‘ildi va tahlil qilindi.

2. Ma’lumot yig‘ish

Tadqiqot davomida quyidagi manbalardan foydalangan:

- Xalqaro standartlar va tavsiyalar (ISO/IEC 27001, NIST Cybersecurity Framework);
- Ilmiy maqolalar va tadqiqot ishlari;
- Korporativ va davlat axborot tizimlari bo‘yicha mavjud statistik ma’lumotlar;
- Amaliy kuzatuvlar va kiberhujumlar holatlari.

3. Tahlil usullari

Tadqiqot natijalarini tahlil qilishda quyidagi metodlardan foydalanildi:

- **Kvalitativ tahlil** — kiberxavfsizlik muammolarining sabab va oqibatlarini aniqlash;

- **Kvantitativ tahlil** — ma’lumotlar bazasidan yig‘ilgan statistik ma’lumotlarni sonli ko‘rsatkichlar orqali o‘rganish;
- **Grafik va diagrammalar yordamida tahlil** — tahdidlar, hujumlar va xavfsizlik choralarini vizual ko‘rsatish.
- **4. Tadqiqotning amaliy jihati**

Metodlar yordamida kiberxavfsizlik tizimlarida uchraydigan muammolar aniqlanib, ularni bartaraf etish bo‘yicha samarali chora-tadbirlar ishlab chiqildi. Shu bilan birga, ilmiy tahlil orqali axborot xavfsizligini ta’minlashning eng maqbul metodologiyasi aniqlangan.

Natijalar

1. Tadqiqot natijalari

Ushbu tadqiqot davomida axborot xavfsizligi va kiberxavfsizlik sohasidagi muammolar tahlil qilindi. Tadqiqot natijalari shuni ko‘rsatdiki:

- Kiberhujumlar tobora ortib bormoqda. So‘nggi yillarda zararli dasturlar va phishing hujumlari soni sezilarli darajada oshgan;
- Tashkiliy choralar yetarli emas. Ko‘plab tashkilotlarda xodimlarni kiberxavfsizlik bo‘yicha yetarlicha o‘qitilmagan, xavfsizlik siyosati to‘liq ishlab chiqilmagan;
- Texnologik himoya muammolari mavjud. Antivirus dasturlari, firewall va shifrlash vositalari ko‘plab holatlarda eskirgan yoki to‘liq qo‘llanilmayapti;
- Shaxsiy ma’lumotlar xavfi yuqori. Foydalanuvchilarning shaxsiy ma’lumotlari ruxsatsiz tarqalish va o‘g‘irlanish xavfi ostida.
- **2. Muammolarni tahlil qilish**

Tadqiqot natijalariga ko‘ra, asosiy muammolar quyidagilardan iborat:

1. Kiberhujumlar va zararli dasturlarni aniqlash va oldini olish tizimlari yetarli darajada rivojlanmagan;

2. Axborot xavfsizligi standartlari va me’yoriy hujjatlar tashkilotlarda to‘liq tatbiq etilmayapti;

3. Foydalanuvchilar va xodimlar orasida xavfsiz internet va raqamli xizmatlardan foydalanish bo‘yicha yetarlicha bilim mavjud emas.

3. Natijalarni tahlil qilish

Natijalar shuni ko‘rsatadiki, axborot xavfsizligini ta’minlash uchun:

- Zamonaviy texnologik vositalarni joriy etish;
- Tashkiliy choralarni kuchaytirish, xodimlarni muntazam o‘qitish;
- Shaxsiy ma’lumotlarni himoya qilish bo‘yicha qat’iy standartlar va siyosatlarni ishlab chiqish zarur.

Ushbu natijalar amaliy jihatdan tashkilot va foydalanuvchilar uchun axborot xavfsizligini oshirish, kiberxavfsizlik muammolarini kamaytirish va raqamli tizimlarni samarali ishlashini ta’minlashga yordam beradi.

Xulosa

Ushbu maqolada axborot xavfsizligi va kiberxavfsizlik muammolari tahlil qilindi. Tadqiqot natijalari shuni ko‘rsatdiki, zamonaviy axborot tizimlari ko‘plab kiberhujumlar va tahdidlarga duch kelmoqda. Kiberxavfsizlikni ta’minlash uchun texnologik, tashkiliy va huquqiy choralarni birgalikda qo‘llash zarur. Shu bilan birga, foydalanuvchilarni o‘qitish va shaxsiy ma’lumotlarni himoya qilish siyosatini kuchaytirish axborot xavfsizligini oshirishda muhim ahamiyatga ega.

Foydalanilgan adabiyotlar

1. ISO/IEC 27001:2013 — Information Security Management Systems (ISMS) Standard.

2. NIST Cybersecurity Framework, National Institute of Standards and Technology, USA.

3. Stallings, W. *Cryptography and Network Security: Principles and Practice*. Pearson, 2020.

4. Schneier, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley, 2015.

5. Kim, D. & Solomon, M. *Fundamentals of Information Systems Security*. Jones & Bartlett Learning, 2016.