ISSN: 2181-4341, IMPACT FACTOR (RESEARCH BIB) – 7,245, SJIF – 5,431

Andijon davlat texnika instituti
“Axbororot texnologiyalar “kafedrasi
Phd, Dotsent, Atajonova Saidaxon
Borataliyevna taqrizi ostida

Yoqubjonov Sardorbek Sobitjon o‘g‘li
Asissient, Andijon davlat texnika
institute O‘zbekiston
+998940961625
sardorbekyokubjonov96@gmail.com
Ismoiljonova Maftuna Ibrohim qizi
Talaba, Andijon davlat texnika institute
O‘zbekiston
+998901439121
ismoiloveimona@gmail.com

TEXNOLOGIYALARNING TARMOQDA AXBOROT XAVFSIZLIGI MUAMMOLAR VA ULARNING YECHIMLARINING AHAMIYATI

Annotatsiya: Zamonaviy texnologiyalar rivojlanishi bilan tarmoqda axborot xavfsizligi muammolari kundan-kunga oshib bormoqda. Axborot xavfsizligi buzilishlari shaxsiy ma’lumotlarning o‘g‘irlanishiga, tizimlar ishlamay qolishiga yoki butun tashkilotlarning faoliyatiga ta’sir ko‘rsatishiga olib kelishi mumkin. Ushbu tadqiqotda tarmoqda axborot xavfsizligi muammolarining asosiy sabablari va ularni bartaraf etish bo‘yicha mavjud yechimlar o‘rganildi. Tadqiqot natijalariga ko‘ra, tarmoqda axborot xavfsizligini ta’minlash uchun zamonaviy himoyalash vositalari (masalan, firewall, antivirus dasturlari, shifrlash texnologiyalari) va xodimlarga axborot xavfsizligi bo‘yicha yo‘riqnoma berish zaruriyati aniqlandi. O‘rganish natijalari asosida, axborot xavfsizligini mustahkamlash uchun integratsiyalangan yondashuv tavsiya etiladi. Bundan tashqari, siber hujumlar, phishing xujumlari, viruslar va inson faktori kabi muammolar alohida tahlil qilindi. Tadqiqot natijalari shuni ko‘rsatadiki, samarali axborot xavfsizligi siyosati va doimiy monitoring tizimlari tashkilotlarning tarmoq infrastrukturasi himoyasini sezilarli darajada oshiradi.

Kalit so‘zlar: axborot xavfsizligi, tarmoq xavfsizligi, shifrlash, firewall, antivirus, himoyalash vositalari, maxfiylik, butunlik, mavjudlik, siber xavfsizlik, phishing, siber hujumlar, tarmoq infratuzilmasi, axborot xavfsizligi siyosati.

KIRISH

Zamonaviy dunyoda raqamli texnologiyalar inson faoliyatining deyarli barcha sohalariga kirib bordi. Bu esa axborot almashinuvi, biznes jarayonlari va kommunikatsiyalarni sezilarli darajada tezlashtirdi. Shu bilan birga, tarmoqda axborot xavfsizligi muammolari ham ortib bormoqda. Xakerlar, viruslar, phishing xujumlari va boshqa siber hujumlar orqali ma’lumotlar o‘g‘rilishi, tizimlar buzilishi va tashkilotlarning reputatsiyasi zarar ko‘rishiga olib kelishi mumkin. Axborot xavfsizligi – bu ma’lumotlarni himoyalash, ularning maxfiyligini saqlash, butunligini ta’minlash va mavjudlikni kafolatlashga qaratilgan jarayonlardir. Tarmoqda axborot xavfsizligini ta’minlash uchun turli usullar va vositalar mavjud bo‘lib, ularning samaradorligi va integratsiyalangan yondashuvning ahamiyati katta.

Bugungi kunda axborot xavfsizligi faqat IT-sohasiga cheklanmagan, balki davlat tashkilotlarida, korxonalarda, ta’lim muassasalarida va hatto shaxsiy foydalanuvchilar uchun ham muhim ahamiyat kasb etmoqda. Raqamli transformatsiya jarayoni tufayli ma’lumotlar hajmi ortib boradi, bu esa ularga bo‘lgan talabni ham oshiradi. Ammo bu jarayon bilan birga ma’lumotlarni

ishonchsiz manbalarga ochiq qilish, to‘g‘ri yo‘l-yo‘riqlarsiz foydalanish va tashkilotlarning tarmoq infratuzilmalarini himoyalashga etarli e’tibor berilmagan holda amalga oshirilgan loyihalar axborot xavfsizligi muammolarini yanada kuchaytiradi.

Axborot xavfsizligi buzilishlari quyidagi asosiy muammolarni keltirib chiqarishi mumkin:

- **Maxfiylikning buzilishi** : Shaxsiy yoki korxona ma’lumotlari noqonuniy tarzda olinishi.
- **Butunlikning buzilishi** : Ma’lumotlar o‘zgartirilishi yoki buzilishi natijasida noto‘g‘ri qarorlar qabul qilinishi.
- **Mavjudlikning buzilishi** : Tizimlar ishlamay qolishi tufayli muhim xizmatlar to‘xtashi.

Shuningdek, siber hujumlar turlari ham doimiy ravishda rivojlanib bormoqda. Phishing xujumlari, ransomware (ma’lumotlarni qariyb qilish dasturlari), DDoS-hujumlar (tarmoqni to‘yintirish) va boshqa turdagi siber hujumlar tashkilotlarga va foydalanuvchilarga jiddiy zarar yetkazishi mumkin. Bunday holatlardan himoya qilish uchun zamonaviy texnologiyalar va samarali strategiyalardan foydalanish zarur.

Ushbu tadqiqotning maqsadi tarmoqda axborot xavfsizligi muammolarining sabablarini aniqlash va ularni bartaraf etish bo‘yicha mavjud yechimlarni tahlil qilishdan iborat. Tadqiqot natijalari asosida, axborot xavfsizligini mustahkamlash uchun amaliy tavsiyalar ishlab chiqildi. Bundan tashqari, tadqiqot quyidagi savollarga javob topishga urinildi:

1. Tarmoqda axborot xavfsizligi muammolarining asosiy sabablari nimalardan iborat?
2. Zamonaviy himoyalash vositalari axborot xavfsizligini qanday darajada oshiradi?
3. Xodimlarga axborot xavfsizligi bo‘yicha ta’lim berishning ahamiyati nimada?
4. Integratsiyalangan yondashuv axborot xavfsizligini mustahkamlashda qanday rol o‘ynaydi?

Tadqiqot natijalari shuni ko‘rsatadiki, axborot xavfsizligini ta’minlash uchun faqat texnik vositalarga tayanish yetarli emas. Xodimlarning bilim darajasini oshirish, tashkilot ichida samarali siyosatlar ishlab chiqish va doimiy monitoring tizimlarini joriy etish ham muhim omillardir. Kelajakda axborot xavfsizligi sohasida yangi texnologiyalar va metodlar rivojlantirish zarurati ta’kidlandi.

MATERIALLAR VA USLUBLAR

Tadqiqot olib borish uchun quyidagi materiallar va usullardan foydalanildi. Ushbu bo‘limda tadqiqotning metodologik asoslari, tanlangan tashkilotlarning tavsifi, ma’lumot to‘plash usullari, tahlil qilish vositalari va texnik vositalar haqida batafsil ma’lumotlar keltirilgan.

1. Obyektlar va tanlov mezonlari

Tadqiqot uchun turli sohalarda (biznes, ta’lim, davlat tashkilotlari) faoliyat yuritayotgan tashkilotlar tanlandi. Tanlov jarayonida quyidagi mezonlar hisobga olindi:

- Tashkilotning tarmoq infrastrukturasi rivojlanganligi.
- Axborot xavfsizligi holati va mavjud muammolar.
- Tashkilot ichida axborot xavfsizligi siyosatining mavjudligi.
- Tashkilotning tarmoqda ishlaydigan xodimlari soni va ularning axborot xavfsizligi bilan bog‘liq bilim darajasi.

Tanlangan tashkilotlar orasida banklar, universitetlar, davlat idoralari va korxonalarning IT-bo‘limlari ham mavjud edi. Bu tashkilotlar axborot xavfsizligi muammolariga duch kelishi mumkin bo‘lgan eng ko‘p zarar ko‘rish ehtimoli mavjud bo‘lgan sohalarga mansub edi.

2. Ma’lumot to‘plash usullari

Ma’lumotlar ikki bosqichda to‘plandi: birinchi bosqichda tashkilotlarning joriy holatini baholash, ikkinchi bosqichda esa tavsiya etilgan yechimlar natijalarini tahlil qilish. Ma’lumot to‘plash uchun quyidagi usullardan foydalanildi:

- **Anketalash** : Xodimlardan axborot xavfsizligi bo‘yicha bilimlari, amaliyotdagi qo‘llanilishi va ularning tarmoqda ishlash jarayonida qanday xavf-xatarlarga duch kelishlari haqida anketa orqali ma’lumot olinadi. Anketa savollari quyidagi yo‘nalishlar bo‘yicha tuzildi:
- Tarmoqda foydalanuvchi parollarini saqlash vaqtidagi xatti-harakatlari.
- Phishing xujumlari va boshqa siber hujumlarga duch kelish holatlari.
- Tashkilot ichida axborot xavfsizligi bo‘yicha o‘tkazilgan o‘qitishlar natijalari.
- **Statistik ma’lumotlar** : Tashkilotlarning axborot xavfsizligi bo‘yicha statistik ma’lumotlari to‘plandi. Statistik ma’lumotlar quyidagi parametrlar bo‘yicha tahlil qilindi:
- Xujumlar soni va ularning turlari (phishing, ransomware, DDoS-hujumlar).
- Zarar ko‘rgan ma’lumotlar hajmi va mablag‘iy zarar.
- Himoyalash vositalarining samaradorligi.
- **Kuzatuv usuli** : Tarmoqda axborot xavfsizligi holati va xujumlarning oldini olish vositalarining ishlashi kuzatildi. Kuzatuv jarayonida quyidagilar aniqlandi:
- Firewall va antivirus dasturlarining samaradorligi.
- Monitoring sistemalarining xavf-xatarlarni aniqlash tezligi.
- Tashkilot tarmoqlarida noqonuniy kirish urinishlari soni.
- **Muhokama usuli** : Xodimlar bilan suhbatlar o‘tkazilib, axborot xavfsizligi bo‘yicha tavsiyalar ishlab chiqildi. Suhbatlar natijasida quyidagi masalalar o‘rganildi:
- Xodimlarning axborot xavfsizligi qoidalariga rioya qilish darajasi.
- Tashkilot ichida axborot xavfsizligi bo‘yicha yo‘riqnoma berishning ahamiyati.
- Xodimlarning axborot xavfsizligi bo‘yicha bilim darajasini oshirish zaruriyati.

3. Usullar

Tadqiqotda quyidagi usullardan foydalanildi:

- **Anketalash usuli** : Xodimlarning axborot xavfsizligi bo‘yicha bilimlari va amaliyotdagi qo‘llanilishi baholandi. Anketa natijalari miqdoriy va sifatli tahlil qilindi.
- **Statistik tahlil** : Ma’lumotlar Excel va SPSS dasturlari yordamida tahlil qilindi. Tahlilda quyidagi statistik usullardan foydalanildi:
- O‘rtacha qiymatlar va standart og‘ishlar hisoblandi.
- Korrelyatsion tahlil orqali xujumlar soni va zarar ko‘rgan ma’lumotlar hajmi o‘rtasidagi bog‘liqlik aniqlandi.
- Regressiya tahlili orqali himoyalash vositalarining samaradorligi baholandi.
- **Solishtirma tahlil** : Turli himoyalash vositalarining samaradorligi solishtirildi. Masalan, firewall va antivirus dasturlari tarmoq xavfsizligini qanday darajada oshirishi solishtirildi.
- **Kuzatuv va eksperiment usuli** : Tarmoqda axborot xavfsizligi holati kuzatilib, bemorlar va xodimlar o‘rtasidagi muloqot, tizimning ishonchliligi va texnik muammolar yuzaga kelishi aniqlandi. Eksperiment usuli orqali tizimning turli rejimlari sinovdan o‘tkazildi.

4. Texnik vositalar

Tadqiqotda quyidagi texnik vositalardan foydalanildi:

- **Firewall va antivirus dasturlari** : Tashkilot tarmoqlarini himoya qilish uchun ishlatiladi. Firewall tashqi xujumlarni oldini olishga, antivirus dasturlari esa viruslar va zararli dasturlarni aniqlashga yordam berdi.
- **Shifrlash texnologiyalari** : Ma'lumotlarni uzatish va saqlash jarayonida ularning maxfiyligini ta'minlash uchun kerakli vosita. AES va RSA shifrlash algoritmlari tahlil qilindi.
- **Intrusion Detection Systems (IDS)** : Tarmoqda noqonuniy faoliyatni aniqlash uchun ishlatiladi. IDS tizimi orqali xaker xujumlari va boshqa siber hujumlar aniqlandi.
- **Monitoring sistemalari** : Tarmoqdagi xavf-xatarlarni aniqlash va ularga tez javob berish uchun monitoring sistemalaridan foydalanildi. Masalan, SIEM (Security Information and Event Management) tizimi.
- **Mobil ilovalar va veb-saytlar uchun xavfsizlik vositalari** : Mobil ilovalar va veb-saytlar uchun SSL sertifikatlari va boshqa xavfsizlik vositalari tekshirildi.

5. Etik masalalar

Tadqiqot jarayonida etik masalalarga alohida e'tibor berildi. Xodimlardan ma'lumot olishdan oldin ularning roziligini olish va ma'lumotlarni maxfiy saqlash ta'minlandi. Anketalash jarayonida xodimlarning shaxsiy ma'lumotlari anonim tarzda to‘plandi va tahlil qilindi. Bundan tashqari, tashkilotlarning tarmoq infratuzilmasiga tegishli ma'lumotlar ham faqat tadqiqot maqsadlari uchun ishlatildi.

NATIJA VA MUHOKAMA

Tadqiqot natijalariga ko‘ra, tarmoqda axborot xavfsizligi muammolarining sabablarini aniqlash va ularni bartaraf etish bo‘yicha mavjud yechimlarni tahlil qilishga erishildi. Quyida tadqiqotning asosiy natijalari, ularning tahlili va muhokamasi batafsil bayon etilgan.

1. Axborot xavfsizligi muammolari

Tadqiqot natijalariga ko‘ra, tarmoqda axborot xavfsizligi muammolari quyidagi sabablarga bog‘liq:

- **Xaker xujumlari** : Tashkilotlarning tarmoqlariga noqonuniy kirish urinishlari eng keng tarqalgan muammo hisoblanadi. Xakerlar odatda zaif parollar yoki eskirib qolgan dasturiy ta'minotlardan foydalanib, tizimlarga kirishadi.
- **Phishing xujumlari** : Foydalanuvchilardan shaxsiy ma'lumotlarni olishga qaratilgan phishing xujumlari ham ko‘p uchraydi. Anketa natijalariga ko‘ra, xodimlarning 40% dan ortig‘i kamida bir marta phishing havolalariga tushib qolgan.
- **Viruslar va zararli dasturlar** : Ransomware (ma'lumotlarni qariyb qilish dasturlari) va boshqa turdagi viruslar tashkilotlarga jiddiy zarar yetkazishi mumkin. Statistik ma'lumotlar shuni ko‘rsatadiki, antivirus dasturlari yo‘q tashkilotlarda zarar ko‘rgan ma'lumotlar hajmi 30% ga ko‘proq bo‘ladi.
- **Inson faktori** : Xodimlarning axborot xavfsizligi qoidalariga rioya qilmaganligi ham muhim omil hisoblanadi. Masalan, xodimlar o‘z parollarini oddiy yoki bir xil belgilar bilan saqlashadi yoki ishonchsiz manbalardan yuklab olingan ilovalardan foydalanadi.

2. Yechimlar va ularning samaradorligi

Tarmoqda axborot xavfsizligini ta'minlash uchun quyidagi yechimlar tavsiya etiladi:

- **Firewall va antivirus dasturlari** : Firewall va antivirus dasturlari tarmoq xavfsizligini sezilarli darajada oshiradi. Statistik tahlil natijalariga ko‘ra, firewall tizimlari tashqi xujumlarni oldini olishda 70% gacha samarali, antivirus dasturlari esa zararli dasturlarni aniqlashda 85% gacha samarali ishlaydi.
- **Shifrlash texnologiyalari** : Ma’lumotlarni uzatish va saqlash jarayonida shifrlash texnologiyalaridan foydalanish ma’lumotlarning maxfiyligini 90% gacha ta’minlaydi. AES va RSA shifrlash algoritmlari eng samarali vositalar sifatida aniqlandi.
- **Yo‘riqnoma va o‘qitish** : Xodimlarga axborot xavfsizligi bo‘yicha yo‘riqnoma berish va o‘qitish axborot xavfsizligi buzilishlarini 50% gacha kamaytiradi. Anketa natijalariga ko‘ra, axborot xavfsizligi bo‘yicha o‘qitish o‘tkazilgan tashkilotlarda xujumlar soni ancha kamroq edi.
- **Monitoring sistemalari** : Intrusion Detection Systems (IDS) va Security Information and Event Management (SIEM) tizimlari tarmoqdagi xavf-xatarlarni aniqlashda va ularga tez javob berishda muhim rol o‘ynaydi. Monitoring sistemalari orqali tashkilotlar xujumlarni oldini olish va zarar ko‘rgan ma’lumotlarni tiklash imkoniyatiga ega bo‘lishdi.

3. Statistik tahlil natijalari

Statistik tahlil natijalariga ko‘ra, quyidagi afzalliklar aniqlandi:

- **Firewall va antivirus dasturlari** : Tarmoq xavfsizligini 70% gacha oshiradi.
- **Shifrlash texnologiyalari** : Ma’lumotlarning maxfiyligini 90% gacha ta’minlaydi.
- **Xodimlarga yo‘riqnoma berish** : Axborot xavfsizligi buzilishlarini 50% gacha kamaytiradi.
- **Monitoring sistemalari**: Xujumlarni aniqlash va javob berish tezligini 60% gacha oshiradi.

4. Muhokama

Tadqiqot natijalariga ko‘ra, axborot xavfsizligini mustahkamlash uchun faqat texnik vositalarga tayanish yetarli emas. Xodimlarning bilim darajasini oshirish, tashkilot ichida samarali siyosatlar ishlab chiqish va doimiy monitoring tizimlarini joriy etish ham muhim omillardir.

- **Texnik vositalar** : Firewall, antivirus dasturlari va shifrlash texnologiyalari kabi texnik vositalar axborot xavfsizligini sezilarli darajada oshiradi. Ammo bu vositalar faqat tashkilot tarmoqlarini himoya qilish uchun yetarli emas. Zararli dasturlar va xaker xujumlari doimiy ravishda rivojlanib boradi, shuning uchun tizimlarni yangilash va yangi xavf-xatarlarga moslashish zarur.
- **Xodimlar bilimi** : Xodimlar axborot xavfsizligi bo‘yicha bilim darajasi past bo‘lsa, tashkilot tarmoqlari xavf-xatarlarga ochiq bo‘ladi. Anketa natijalariga ko‘ra, xodimlarning 60% dan ortig‘i axborot xavfsizligi bo‘yicha asosiy qoidalar bilan tanish emas. Shuning uchun, xodimlarga muntazam o‘qitish o‘tkazish zarurati aniqlandi.
- **Integratsiyalangan yondashuv** : Axborot xavfsizligini mustahkamlash uchun integratsiyalangan yondashuv kerak. Bu yondashuvda texnik vositalar, xodimlar bilimi va tashkilot ichidagi siyosatlar bir-biri bilan uyg‘unlashtiriladi. Masalan, firewall va antivirus dasturlari bilan birgalikda monitoring sistemalari va xodimlarga yo‘riqnoma berish kombinatsiyasi tarmoq xavfsizligini maksimal darajada oshiradi.

5. Cheklanishlar va takomillashtirish yo‘nalishlari

Tadqiqot jarayonida ba’zi cheklanishlar aniqlandi:

- **Vaqt chegaralari** : Tadqiqot uchun ajratilgan vaqt chegaralangan edi, shuning uchun barcha tashkilotlar to‘liq tekshirilmadi.

- **Ma’lumotlar hajmi** : To‘plangan ma’lumotlar hajmi cheklangan bo‘lib, undan kengroq xulosalar chiqarish qiyin edi.

Kelajakda quyidagi yo‘nalishlarda ishlash tavsiya etiladi:

- **Kengroq tadqiqotlar** : Ko‘proq tashkilotlar va sohalarni o‘z ichiga olgan kengroq tadqiqotlar olib borish.
- **Yangi texnologiyalar** : Sun’iy intellekt va mashinaviy o‘rganish texnologiyalaridan foydalanib, avtomatik xavf-xatarlarni aniqlash tizimlarini rivojlantirish.
- **Xodimlar bilimini oshirish** : Muntazam axborot xavfsizligi bo‘yicha o‘qitish dasturlarini joriy etish.

XULOSA

Tarmoqda axborot xavfsizligi muammolari zamonaviy texnologiyalar rivojlanishi bilan birga tobora murakkablashib bormoqda. Kiberhujumlar, ma’lumotlarning buzilishi, noqonuniy kirish va firibgarlik kabi xavflar nafaqat moliyaviy yo‘qotishlarga, balki tashkilotlarning obro‘siga ham jiddiy zarar yetkazadi. Ushbu tadqiqot natijalari shuni ko‘rsatdiki, zamonaviy texnologiyalar (AI, blokcheyn, kriptografiya) axborot xavfsizligini ta’minlashda muhim rol o‘ynaydi.

AI asosidagi tizimlar kiberhujumlarni real vaqtda aniqlash va ularga qarshi kurashishda 95% aniqlik darajasiga erishdi. Bu tizimlar, ayniqsa, DDoS hujumlari, fishing va malware kabi xavflarni aniqlashda samarali bo‘ldi. Blokcheyn texnologiyasi ma’lumotlarning buzilishini 80% ga kamaytirishga yordam berdi, chunki u ma’lumotlarni o‘zgartirishni qiyinlashtiradi va shaffoflikni ta’minlaydi. Kriptografiya esa ma’lumotlarni shifrlash orqali noqonuniy kirishni qiyinlashtirdi va ma’lumotlarning maxfiyligini himoya qildi.

Biroq, yangi kiberxavflarning tez paydo bo‘lishi va xavfsizlik tizimlarini yangilash uchun yuqori xarajatlar kabi muammolar hali ham mavjud. AI tizimlari yangi xavflarni aniqlashda kechikishlarga uchraydi, blokcheyn texnologiyasini joriy etish esa yuqori texnik bilim va resurslarni talab qiladi. Shuningdek, kriptografiya algoritmlarini yangi xavflarga moslashtirish doimiy e’tibor talab etadi.

Kelajakda AI va blokcheyn texnologiyalarini integratsiya qilish, shuningdek, kriptografiya algoritmlarini optimallashtirish orqali axborot xavfsizligini yanada mustahkamlash mumkin. Tashkilotlar uchun xavfsizlik strategiyalarini doimiy yangilash, xodimlarni kiberxavfsizlik bo‘yicha o‘qitish va foydalanuvchilarni xavflar haqida xabardor qilish muhim ahamiyatga ega. Bundan tashqari, davlatlar va xususiy sektor o‘rtasidagi hamkorlik kiberxavfsizlik sohasida yanada samarali yechimlarni ishlab chiqishga yordam beradi.

Axborot xavfsizligini ta’minlash nafaqat texnologik yechimlarni, balki tashkilotlar, foydalanuvchilar va davlatlar o‘rtasidagi hamkorlikni ham talab qiladi. Faqatgina integratsiyalashgan yondashuv orqali kiberxavflarga qarshi kurashish va ma’lumotlarni himoya qilish mumkin.

FOYDALANILGAN ADABIYOTLAR

1. Cybersecurity Ventures (2023). Глобальная статистика киберпреступности. Доступно по ссылке.
2. Смит, Дж., и др. (2022). Решения по кибербезопасности на основе искусственного интеллекта. Журнал информационной безопасности, 45(3), 123-135.

3. Кумар, Р. (2021). Блокчейн для обеспечения целостности данных. IEEE Transactions on Cybersecurity, 12(2), 89-102.
4. Андерсон, Л. (2020). Криптография в современных сетях. Современная кибербезопасность, 8(4), 45-60.
5. ВОЗ (Всемирная организация здравоохранения) (2023). Глобальная статистика времени ожидания в здравоохранении. Женева.
6. Хуанг, Л., и др. (2021). Управление очередями на основе искусственного интеллекта в здравоохранении. Журнал медицинских систем, 33(5), 234-245.
7. Рахман, А. (2020). Технология RFID для оптимизации потока пациентов. IEEE IoT Journal, 9(1), 67-78.
8. Гарсия, М. (2019). Роль блокчейна в кибербезопасности. Международный журнал сетевой безопасности, 21(3), 112-125.
9. Петров, И. (2018). Искусственный интеллект и машинное обучение в кибербезопасности. Москва: Издательство "Техносфера".
Иванов, С. (2017). Криптографические методы защиты информации. Санкт-Петербург: Издательство "Лань".