KOMPYUTER VA TARMOQADA KOMPYUTER XAVFSIZLIGINI TA'MINLASH USULLARI. AXBOROTLARNI KRIPTOGRAFIK HIMOYALASH.

Farg‘ona davlat universiteti
Chet tillar fakulteti
1-bosqich talabasi
Murodova Sevaraxon Mansurjon qizi
Ilmiy rahbar: Toshboltayev Faxriddin O'rinboyevich

Annotatsiya. Ushbu maqolada zamonaviy raqamli texnologiyalar taraqqiyoti bilan birga kompyuter va tarmoq tizimlarida yuzaga kelayotgan axborot xavfsizligi muammolari atroflicha tahlil qilinadi. Dastlab, kompyuter xavfsizligining asosiy tamoyillari, jumladan, maxfiylik, yaxlitlik va mavjudlik prinsiplariga asoslangan himoya choralari ko‘rib chiqiladi. Kompyuterlarga va tarmoq infratuzilmasiga tahdid soluvchi omillar — zararli dasturlar, fishing, xakerlik, tarmoq hujumlari kabi xavflar haqida to‘xtalinadi hamda ularning oldini olish usullari yoritiladi. Tarmoq xavfsizligini ta'minlashda autentifikatsiya, avtorizatsiya va monitoring texnologiyalarining o‘rni alohida tahlil qilinadi. Maqolaning markaziy qismi axborotlarni kriptografik himoyalashga bag‘ishlangan bo‘lib, unda shifrlashning asosiy turlari — simmetrik va assimetrik algoritmlar, ochiq va yopiq kalitli tizimlar, raqamli imzo, xesh-funksiyalar kabi texnologiyalar keng ko‘lamda bayon etiladi. Kriptografiyaning amaliyotdagi roli, ayniqsa, internet orqali axborot almashinuvida, moliyaviy operatsiyalar xavfsizligida va davlat sirlarini himoyalashda qanday xizmat qilishi misollar bilan ko‘rsatib beriladi.

Kalit so'zlar: kompyuter xavfsizligi, tarmoq xavfsizligi, kriptografiya, axborotni himoyalash, shifrlash algoritmlari, zararli dasturlar, raqamli imzo, axborot texnologiyalari xavfsizligi.

Аннотация. В данной статье подробно анализируются проблемы информационной безопасности, возникающие в компьютерных и сетевых системах вместе с развитием современных цифровых технологий. Первоначально будут

рассмотрены основные принципы компьютерной безопасности, включая меры защиты, основанные на принципах конфиденциальности, целостности и доступности. Будут рассмотрены факторы, угрожающие компьютерам и сетевой инфраструктуре, такие как вредоносные программы, фишинг, взлом, сетевые атаки, а также способы их предотвращения. Отдельно анализируется роль технологий аутентификации, авторизации и мониторинга в обеспечении безопасности сети.

Центральная часть статьи посвящена криптографической защите информации, в ней подробно описаны основные виды шифрования — такие технологии, как симметричные и асимметричные алгоритмы, системы с открытым и закрытым ключом, цифровая подпись, хеш-функции. На примерах показана роль криптографии на практике, особенно в обмене информацией через интернет, обеспечении безопасности финансовых операций и защите государственной тайны.

Ключевые слова: компьютерная безопасность, сетевая безопасность, криптография, защита информации, алгоритмы шифрования, вредоносное ПО, цифровая подпись, безопасность информационных технологий.

Abstract. This article analyzes in detail the problems of information security that arise in computer and network systems along with the development of modern digital technologies. Initially, the basic principles of computer security will be considered, including protection measures based on the principles of confidentiality, integrity and accessibility. Factors that threaten computers and network infrastructure, such as malware, phishing, hacking, network attacks, as well as ways to prevent them, will be considered. The role of authentication, authorization, and monitoring technologies in ensuring network security is analyzed separately.

The central part of the article is devoted to the cryptographic protection of information, it describes in detail the main types of encryption — technologies such as symmetric and asymmetric algorithms, public and private key systems, digital signature, hash functions. The examples show the role of cryptography in practice, especially in the exchange of information over the Internet, ensuring the security of financial transactions and protecting state secrets.

Keywords: computer security, network security, cryptography, information security, encryption algorithms, malware, digital signature, information technology security.

Kompyuter xavfsizligini ta'minlash masalasi zamonaviy axborotlashgan jamiyatda strategik muhim yo'nalishlardan biridir. U nafaqat yirik korporatsiyalar, balki kichik biznes, davlat muassasalari, va individual foydalanuvchilar uchun ham ustuvorlik kasb etadi. Kompyuter va tarmoq xavfsizligi deganda axborotni noqonuniy kirish, o'zgartirish, yo'qotish, yoki tarqatishdan himoya qilish tushuniladi. Bu soha o'z ichiga juda keng yo'nalishlarni oladi: xavfsizlik siyosatini ishlab chiqish, tizimli tahlil, xavf-xatarlarni baholash, texnik chora-tadbirlarni joriy etish va monitoring qilish, foydalanuvchi xatti-harakatlarini nazorat qilish, shuningdek, kriptografik mexanizmlarni qo'llash orqali axborotni kodlash. Dastlab, kompyuter xavfsizligining poydevori hisoblangan konseptual asoslarni ko'rib chiqamiz. Ular "CIA" modeli bilan ifodalanadi: maxfiylik (Confidentiality), yaxlitlik (Integrity), va mavjudlik (Availability). Maxfiylik ma'lumotlarga ruxsatsiz kirishni cheklaydi, yaxlitlik esa ma'lumotlarning o'zgartirilmasligi va ishonchliligini ta'minlaydi, mavjudlik esa axborot resurslarining doimiy ishlashini kafolatlaydi. Har bir prinsipning amaliy joriy etilishi uchun turli mexanizmlar ishlab chiqilgan: autentifikatsiya tizimlari, ruxsat nazorati, jurnal yuritish, tarmoq xavfsizligi devorlari, va invaziyaga qarshi tizimlar.

Kriptografik himoya metodlari zamonaviy kompyuter xavfsizligining markazida turadi. Ular axborotni shifrlash orqali ruxsatsiz foydalanishni imkonsiz qiluvchi algoritmlarni o'z ichiga oladi. Kriptografiya ikki asosiy yo'nalishga bo'linadi: simmetrik va assimmetrik shifrlash. Simmetrik shifrlashda bitta kalit orqali ma'lumotlar shifrlanadi va ochiladi. Bunda kalitni uzatish eng katta xavfni tug'diradi. Assimmetrik shifrlashda esa kalitlar juftligi mavjud bo'lib, ochiq va maxfiy kalit yordamida ma'lumotlar almashinuvi amalga oshiriladi. RSA, ElGamal, Diffie-Hellman kabi algoritmlar asosida ishlovchi tizimlar bugungi kunda keng qo'llaniladi. Ilmiy tadqiqotlar asosida aniqlanishicha, shifrlashning kvantga chidamli shakllari istiqbolli yo'nalish sifatida ko'rib chiqilmoqda. Kvant kompyuterlarining rivojlanishi bilan birga, mavjud klassik algoritmlarning zaif tomonlari ochilmoqda. Shu bois, post-quantum cryptography yo'nalishida ishlovchi

NTRU, Lattice-based cryptography, va Multivariate Polynomial cryptography asosida yangi algoritmlar ishlab chiqilmoqda. Ularning barchasi quantum kompyuterlar tomonidan parchalab bo'lmaydigan murakkab matematik muammolarga tayanadi.

Bugungi kunda xavfsizlik texnologiyalariga investitsiyalar global miqyosda sezilarli darajada ortmoqda. Gartner va IDC ma'lumotlariga ko'ra, faqatgina 2024 yilda kiberxavfsizlik bozoriga salkam 200 milliard AQSh dollari sarmoya kiritilgan. Bu sarmoyalar ko'proq AI (sun'iy intellekt) asosida ishlovchi xavfsizlik tizimlari, Zero Trust arxitekturasi, hamda avtomatlashtirilgan tarmoq monitoringi vositalariga qaratilgan. Zero Trust modeli har qanday foydalanuvchiga doimiy ishonchsizlikni asos qiladi va tizimga kirish harakatlarini doimiy tahlil qiladi. Innovatsion va hali ommalashmagan yondashuvlardan biri bu – dinami kriptografik tokenlash texnologiyasidir. Bunda foydalanuvchi sessiyasiga mos ravishda real vaqt rejimida yangi kriptografik tokenlar yaratiladi. Ular biometrik, geolokatsion va vaqt omillarini hisobga olgan holda yaratiladi. Shuningdek, shifrlash algoritmlari sun'iy intellekt tomonidan doimiy ravishda yangilanadi, ya'ni tizim real vaqtda o'zini yangilash orqali har qanday kutilmagan xavfdan oldinda harakat qiladi. Bundan tashqari, blockchain texnologiyasi ham axborot xavfsizligida yangi davrni boshlab berdi. U o'zining markazsizlashgan tuzilmasi, o'zgarmasligi va ishonchliligi bilan tanilgan. Blockchain asosida yaratilgan identifikatsiya tizimlari markaziy serverlarga bo'lgan ehtiyojni yo'qotadi va foydalanuvchilarning shaxsiy ma'lumotlarini yuqori darajada himoya qiladi. Bu tizimlar xususan saylov tizimlari, moliyaviy operatsiyalar, va sog'liqni saqlash sohalarida sinovdan o'tkazilmoqda. Axborot xavfsizligining boshqa bir muhim jihati bu foydalanuvchi xulq-atvori asosida tahdidni aniqlash tizimlaridir. Ular foydalanuvchining odatiy harakatlaridan chetga chiqqan har qanday holatni aniqlab, avtomatik blokirovka qiladi yoki xavfsizlik xabarnomasini chiqaradi. Masalan, foydalanuvchi odatda Toshkentdan tizimga ulanadi, ammo to'satdan Istanbuldan ulanmoqchi bo'lsa, tizim buni aniqlab, uni autentifikatsiyadan o'tkazadi. Bu texnologiyalar AI yordamida foydalanuvchi xatti-harakatlarining kontekstual analizini amalga oshiradi.

Shuningdek, kompyuter xavfsizligini ta'minlashda psixologik aspektlar ham muhim ahamiyatga ega. Ko'plab kiberhujumlar foydalanuvchining zaifligidan, ya'ni phishing,

social engineering orqali amalga oshiriladi. Shuning uchun foydalanuvchilarni muntazam o'qitish, ularga xavfsizlik haqida xabardorlikni oshirish bugungi kunda muhim strategik chora sifatida ko'rilmoqda. Kompyuter xavfsizligi sohasidagi ilg‘or tadqiqotlar shuni ko‘rsatmoqdaki, zamonaviy muhitda axborot himoyasini faqat mavjud texnologiyalar bilan emas, balki tizimli, kompleks va modullashtirilgan strategiyalar asosida amalga oshirish zarur. Har bir texnologik yondashuv alohida bir nuqtai nazarni ifodalaydi, lekin ular birgalikda ko‘p o‘lchamli xavfsizlik gibrid modelini shakllantiradi. Bugungi kunda ma’lumotlarni faqat kodlash yoki ruxsatni cheklash orqali himoya qilish etarli emas — xavfsizlikning proaktiv (oldini oluvchi) mexanizmlariga o‘tish zarurati mavjud.

Zamonaviy tizimlarda Adaptive Security Architecture (ASA) — ya’ni adaptiv xavfsizlik arxitekturasi joriy qilinmoqda. Bu model foydalanuvchi, qurilma, vaqt va joy omillarini birlashtirib, xavfsizlik siyosatini real vaqt rejimida avtomatik moslashtiradi. ASA foydalanuvchining xatti-harakatlaridagi har qanday anomaliyani aniqlab, algoritmik tarzda qaror qabul qiladi: masalan, hisobdan chiqish, ko‘p faktorli autentifikatsiyani majburlash yoki tranzaksiyani muzlatib qo‘yish. Bundan tashqari, Differential Privacy asosidagi kriptografik model hozirda yirik ma’lumotlar bazalarida qo‘llanilmoqda. Ushbu texnologiya shaxsiy ma’lumotlarni statistik tahlil uchun foydalanishga imkon beradi, biroq har qanday foydalanuvchining maxfiy ma’lumotlari buzilmasligiga kafolat beradi. Bu ayniqsa sog‘liqni saqlash va davlat statistikasi tizimlarida juda dolzarbdir. Differential Privacy yondashuvi ehtimolliklar nazariyasiga asoslanadi va shovqin (noise) kiritish orqali individual xususiyatlarni yashirishni ta’minlaydi.

Kriptografiyada Fully Homomorphic Encryption (FHE) deb nomlanuvchi ilg‘or texnika paydo bo‘lmoqda. Bu texnika foydalanuvchi ma’lumotlarini shifrlangan holda qayta ishlash imkonini beradi — ya’ni server hech qachon ochiq matnni ko‘rmaydi, ammo u ustida amallarni bajaradi. Bu texnologiya bulutli hisoblash tizimlari uchun mutlaq inqilobiy yechim bo‘lib, ayniqsa sog‘liqni saqlash, moliyaviy hisob-kitob va intellektual mulk sohalarida sinovdan o‘tkazilmoqda. Zero Knowledge Proof (ZKP) algoritmlari esa foydalanuvchining o‘z haqini isbotlashi uchun hech qanday maxfiy ma’lumotni ochiqlamasdan, faqat matematik dalil orqali ishonch hosil qilishga imkon beradi. Bu

texnologiya Web3 va blockchain tizimlarida jadal rivojlanmoqda, xususan, shaxsiylikni saqlab qolgan holda ishonchli tranzaksiyalarni amalga oshirishda.

Kompyuter xavfsizligining yirik tahdidlaridan biri bu — Supply Chain Attack (ta'minot zanjiriga hujum). Bunda tizimga to‘g‘ridan-to‘g‘ri emas, balki vositachilar yoki texnik ta’minotchilar orqali kirishga uriniladi. Bu xujumlar ayniqsa open-source dasturlarni modifikatsiya qilish orqali amalga oshiriladi. Bu muammoni hal qilish uchun Secure Code Provenance (kod kelib chiqishini izohlovchi) tizimlar ishlab chiqilmoqda, ular har bir fayl yoki modulning yaratish tarixi, mualliflari, va o‘zgarishlar jurnalini to‘liq saqlab boradi. Yana bir murakkab yo‘nalish — bu Adversarial Machine Learning. Bu texnologiyada sun’iy intellekt modellarini ataylab noto‘g‘ri o‘rganishga majburlovchi namunalar yaratiladi. Bu esa xavfsizlik tizimlarida yolg‘on signal, noto‘g‘ri tahlil yoki noto‘g‘ri baholashlarga olib kelishi mumkin. Adversarial Training — ya’ni sun’iy intellektni "hujumlarga qarshi immunitetli" qilish texnikasi hozircha bu muammoga yechim bo‘lishi mumkin.

Quantum Key Distribution (QKD) texnologiyasi esa kriptografiyada eng fundamental inqilobiy o‘zgarishlardan biridir. Unda axborot kvant holatlarida kodlanadi va bu holat uzatish jarayonida har qanday kuzatuvchi tomonidan aniqlanganda o‘zgaradi. Bu texnologiya shifrlash kalitlarining uzatilishini to‘liq xavfsiz holga keltirishni ta’minlaydi. Axborot xavfsizligi bu - texnologik emas, balki kompleks yondashuvni talab qiluvchi ijtimoiy, huquqiy, axloqiy va strategik muammolar to‘plamidir. Faqat kriptografik vositalar bilan emas, balki institutsional yondashuvlar, qonunchilik, xalqaro hamkorlik, va madaniyatlararo tafakkur bilan bu muammoni yengish mumkin. Shuningdek, sun'iy intellekt asosidagi xavfsizlik modelining kombinatsiyalashgan, ko'p qatlamli (layered security) yondashuvi kelajakning eng ishonchli yo'nalishi bo'lib qolmoqda. Kompyuter xavfsizligi sohasidagi ilg‘or tadqiqotlar shuni ko‘rsatmoqdaki, zamonaviy muhitda axborot himoyasini faqat mavjud texnologiyalar bilan emas, balki tizimli, kompleks va modullashtirilgan strategiyalar asosida amalga oshirish zarur. Har bir texnologik yondashuv alohida bir nuqtai nazarni ifodalaydi, lekin ular birgalikda ko‘p o‘lchamli xavfsizlik gibrid modelini shakllantiradi. Bugungi kunda ma’lumotlarni faqat kodlash yoki

ruxsatni cheklash orqali himoya qilish etarli emas — xavfsizlikning proaktiv (oldini oluvchi) mexanizmlariga o‘tish zarurati mavjud.

Zamonaviy tizimlarda Adaptive Security Architecture (ASA) — ya’ni adaptiv xavfsizlik arxitekturasi joriy qilinmoqda. Bu model foydalanuvchi, qurilma, vaqt va joy omillarini birlashtirib, xavfsizlik siyosatini real vaqt rejimida avtomatik moslashtiradi. ASA foydalanuvchining xatti-harakatlaridagi har qanday anomaliyani aniqlab, algoritmik tarzda qaror qabul qiladi: masalan, hisobdan chiqish, ko‘p faktorli autentifikatsiyani majburlash yoki tranzaksiyani muzlatib qo‘yish. Bundan tashqari, Differential Privacy asosidagi kriptografik model hozirda yirik ma’lumotlar bazalarida qo‘llanilmoqda. Ushbu texnologiya shaxsiy ma’lumotlarni statistik tahlil uchun foydalanishga imkon beradi, biroq har qanday foydalanuvchining maxfiy ma’lumotlari buzilmasligiga kafolat beradi. Bu ayniqsa sog‘liqni saqlash va davlat statistikasi tizimlarida juda dolzarbdir. Differential Privacy yondashuvi ehtimolliklar nazariyasiga asoslanadi va shovqin (noise) kiritish orqali individual xususiyatlarni yashirishni ta’minlaydi.

Kriptografiyada Fully Homomorphic Encryption (FHE) deb nomlanuvchi ilg‘or texnika paydo bo‘lmoqda. Bu texnika foydalanuvchi ma’lumotlarini shifrlangan holda qayta ishlash imkonini beradi — ya’ni server hech qachon ochiq matnni ko‘rmaydi, ammo u ustida amallarni bajaradi. Bu texnologiya bulutli hisoblash tizimlari uchun mutlaq inqilobiy yechim bo‘lib, ayniqsa sog‘liqni saqlash, moliyaviy hisob-kitob va intellektual mulk sohalarida sinovdan o‘tkazilmoqda.

Zero Knowledge Proof (ZKP) algoritmlari esa foydalanuvchining o‘z haqini isbotlashi uchun hech qanday maxfiy ma’lumotni ochiqlamasdan, faqat matematik dalil orqali ishonch hosil qilishga imkon beradi. Bu texnologiya Web3 va blockchain tizimlarida jadal rivojlanmoqda, xususan, shaxsiylikni saqlab qolgan holda ishonchli tranzaksiyalarni amalga oshirishda. Kompyuter xavfsizligining yirik tahdidlaridan biri bu — Supply Chain Attack (ta'minot zanjiriga hujum). Bunda tizimga to‘g‘ridan-to‘g‘ri emas, balki vositachilar yoki texnik ta’minotchilar orqali kirishga uriniladi. Bu xujumlar ayniqsa open-source dasturlarni modifikatsiya qilish orqali amalga oshiriladi. Bu muammoni hal qilish uchun Secure Code Provenance (kod kelib chiqishini izohlovchi) tizimlar ishlab

chiqilmoqda, ular har bir fayl yoki modulning yaratish tarixi, mualliflari, va o‘zgarishlar jurnalini to‘liq saqlab boradi. Yana bir murakkab yo‘nalish — bu Adversarial Machine Learning. Bu texnologiyada sun’iy intellekt modellarini ataylab noto‘g‘ri o‘rganishga majburlovchi namunalar yaratiladi. Bu esa xavfsizlik tizimlarida yolg‘on signal, noto‘g‘ri tahlil yoki noto‘g‘ri baholashlarga olib kelishi mumkin. Adversarial Training — ya’ni sun’iy intellektni "hujumlarga qarshi immunitetli" qilish texnikasi hozircha bu muammoga yechim bo‘lishi mumkin.

Quantum Key Distribution (QKD) texnologiyasi esa kriptografiyada eng fundamental inqilobiy o‘zgarishlardan biridir. Unda axborot kvant holatlarida kodlanadi va bu holat uzatish jarayonida har qanday kuzatuvchi tomonidan aniqlanganda o‘zgaradi. Bu texnologiya shifrlash kalitlarining uzatilishini to‘liq xavfsiz holga keltirishni ta’minlaydi.

Xulosa shuki, kompyuter va tarmoq xavfsizligi sohasidagi eng dolzarb yondashuvlar endi statik emas, balki dinamik, kontekstga moslashuvchi, sun’iy intellekt asosidagi, ehtimollik modellari va kvant mexanikasi bilan uyg‘unlashgan shakllarda rivojlanmoqda. Bu esa o‘z navbatida, nafaqat texnologik yangiliklarni, balki xavfsizlik siyosatining umuman yangicha konsepsiyasini shakllantiradi. Bunday yondashuvlar yaqinda kompyuter xavfsizligining klassik ko‘rinishini to‘liq yangilaydi. Kelajakda xavfsizlik tizimlari tarmoqqa ulangan har bir komponentni mustaqil sun’iy intellekt agentiga aylantiradi, har bir paket real vaqt rejimida tahlil qilinadi, va har bir xavf ehtimoli matematik model asosida baholanadi. Bu esa himoyani reaktiv emas, balki prediktiv — ya’ni oldindan bashorat qila oluvchi darajaga olib chiqadi.

Foydalanilgan adabiyotlar:

1. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. – 3rd ed. – New York: Wiley, 2020. – 1184 b.

2. G‘ofurov I., Abdullayev Sh. Axborot xavfsizligi: nazariyasi va amaliyoti. – Toshkent: Fan, 2021. – 320 b.

3. Jo‘rayev M. B., Rahmonqulov Z. X. Kompyuter tizimlari va tarmoqlar xavfsizligi. – Toshkent: “Ilm Ziyo”, 2020. – 256 b.

4. Katz J., Lindell Y. Introduction to Modern Cryptography. – 2nd ed. – Boca Raton: CRC Press, 2014. – 603 p.

5. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. – 20th Anniversary ed. – Wiley, 2015. – 784 p.

6. Stallings W. Network Security Essentials: Applications and Standards. – 7th ed. – Pearson Education, 2023. – 448 p.