KIBERXAVFSIZLIK. RAQAMLI DUNYODA HIMOYALANISH USULLARI

КИБЕ БЕЗОПАСНОСТЬ. СПОСОБЫ ОСТАВАТЬСЯ В БЕЗОПАСНОСТИ В ЦИФРОВОМ МИРЕ

CYBERSECURITY. WAYS TO PROTECT YOURSELF IN THE DIGITAL WORLD

Mirzaakbarov Dilshodbek Dovlatboyevich

Farg‘ona davlat universiteti axborot texnologiyalari kafedrasi o‘qituvchisi

mdilshodbek@mail.ru

https://orcid.org/0000-0002-5146-0467

Alijonova Barnoxon Valijon qizi

Farg’ona Davlat Universiteti, Chet tillari

fakulteti, 1-bosqich 24.108-guruh talabasi

Annotatsiya. Ushbu maqolada kiberxavfsizlikning raqamli dunyoda o‘rni va himoya qilish usullari to‘liq tahlil qilinadi. Raqamli texnologiyalar va internet tarmog‘ining tez o‘sishi kiberhujumlar va axborot xavfsizligi tahdidlarini yanada jiddiylashtirdi. Maqolada kiberhujumlar turlari, jumladan viruslar, troyanlar, phishing va DDoS hujumlari, shuningdek, ularni oldini olish va himoya qilishda qo‘llaniladigan metodlar yoritilgan. Kriptografiya, tarmoq xavfsizligi, xavfsizlikni boshqarish tizimlari (SIEM) va foydalanuvchi xavfsizligi kabi himoya usullari hamda sun'iy intellekt va mashina o‘rganish texnologiyalarining kiberxavfsizlikda roli o‘rganilgan. Bunga qo‘shimcha ravishda, yuridik nuqtai nazardan kiberxavfsizlikni mustahkamlash uchun zarur bo‘lgan siyosatlar va me'yoriy hujjatlar ko‘rib chiqiladi.

Kalit so‘zlar : kiberxavfsizlik, himoya usullari, tarmoq xavfsizligi, kriptografiya, sun'iy intellekt, mashina o‘rganish, kiberhujumlar, DDoS hujumlari, phishing, xavfsizlik siyosati

Аннотация. В этой статье проводится всесторонний анализ кибербезопасности и методов защиты в цифровом мире. С быстрым развитием цифровых технологий и интернета кибератаки и угрозы информационной безопасности становятся все более актуальными. Статья описывает различные виды кибератак, включая вирусы, трояны, фишинг и DDoS-атаки, а также методы предотвращения и защиты от них. Рассматриваются методы защиты, такие как криптография, сетевой безопасность, системы управления безопасностью (SIEM) и безопасность пользователей. Также рассматривается роль технологий искусственного интеллекта и машинного обучения в кибербезопасности. В статье рассматриваются юридические аспекты укрепления кибербезопасности через политику и нормативные акты.

Ключевые слова: кибербезопасность, методы защиты, сетевая безопасность, криптография, искусственный интеллект, машинное обучение, кибератаки, DDoS-атаки, фишинг, политика безопасности

Kiberxavfsizlik va uning asosiy tamoyillari

Annotation. This article provides a comprehensive analysis of cybersecurity and protection methods in the digital world. With the rapid growth of digital technologies and the internet, cyberattacks and information security threats have become increasingly critical. The article highlights the different types of cyberattacks, including viruses, trojans, phishing, and DDoS attacks, and discusses methods to prevent and protect against them. Protection methods such as cryptography, network security, security management systems (SIEM), and user security are explored. Additionally, the role of artificial intelligence and machine learning technologies in cybersecurity is examined. The article also considers the legal aspect of strengthening cybersecurity through policies and regulations.

Keywords: cybersecurity, protection methods, network security, cryptography, artificial intelligence, machine learning, cyberattacks, DDoS attacks, phishing, security policie.

Kirish

Kiberxavfsizlik – bu ma’lumotlarni, tizimlarni va tarmoqlarni zararli hujumlardan himoya qilish jarayonidir. Bu har bir tashkilot yoki jismoniy shaxs uchun zarur bo‘lgan muhim soha hisoblanadi. Raqamli texnologiyalar rivojlanishi bilan kiberxavfsizlik nafaqat maxfiylikni, balki ma’lumotlar yaxlitligini va mavjudligini ta’minlashni ham o‘z ichiga oladi. Bu tamoyillar asosida har bir tashkilot o‘zining xavfsizlik siyosatini va me'yorlarini belgilaydi.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Kiberxavfsizlik masalasi so‘nggi yillarda jahon miqyosida dolzarb muammolardan biriga aylanganligi sababli, bu sohada bir qator xalqaro va mahalliy tadqiqotlar olib borilgan. Xususan, B. Schneierning “Applied Cryptography” asari hamda C. Easttomning “Network Defense and Countermeasures” nomli ishlari raqamli xavfsizlikni ta’minlash, himoya tizimlarini yaratish va xavflarni aniqlash usullarini chuqur yoritib beradi. O‘zbekistonda esa, A. Karimov, S. Abdug‘aniyev va M. Raximov kabi mutaxassislarning ilmiy ishlari axborot xavfsizligi, kiberhujumlar va ularning oqibatlarini yumshatish usullariga bag‘ishlangan. Ushbu maqolani yozishda sifatli (qualitative) tadqiqot metodidan foydalanildi. Tadqiqot davomida mavjud ilmiy maqolalar, darsliklar va texnik hisobotlar tahlil qilindi. Shuningdek, kiberhujumlar turlari, ularning amalga oshish mexanizmlari, oldini olishda qo‘llaniladigan texnologiyalar (kriptografiya, SIEM tizimlari, sun’iy intellekt yondashuvlari) bo‘yicha amaliy holatlar o‘rganildi. Metodologik yondashuv sifatida taqqoslash (komparativ), tahliliy sharhlash hamda holatli tadqiqot (case-study) usullaridan foydalanildi. Bu yondashuvlar mavzuning nazariy asoslarini aniqlash va amaliy misollar orqali asoslash imkonini berdi.

NATIJA VA MUHOKAMA

Olib borilgan tahlillar shuni ko‘rsatdiki, raqamli texnologiyalarning tez sur’atlarda rivojlanishi inson hayotini yengillashtirgani bilan birga, kiberxavfsizlik tahdidlarini ham kuchaytirmoqda. Ayniqsa, DDoS hujumlari, phishing, zararli dasturlar (virus, trojan, spyware) orqali amalga oshirilayotgan xurujlar korxonalar, davlat tashkilotlari va jismoniy shaxslar uchun jiddiy xavf tug‘dirmoqda. Maqolada ko‘rib chiqilgan usullar – kriptografiya, xavfsizlikni boshqarish tizimlari (SIEM), sun’iy intellektga asoslangan

tahdidlarni aniqlash modellari – zamonaviy kiberhujumlarning oldini olishda muhim rol o‘ynaydi. Ayniqsa, mashina o‘rganish texnologiyalari yordamida tahdidlarni oldindan aniqlash va avtomatik javob berish imkoniyatlari himoya samaradorligini oshiradi. Muhokamalardan kelib chiqqan xulosa shuki, raqamli muhitda samarali himoyalanish uchun faqat texnik choralar emas, balki foydalanuvchilarning axborot madaniyati, parol siyosati, muntazam yangilanishlar va xavfsizlik protokollariga rioya qilinishi ham muhim omillardandir. Shuningdek, kiberxavfsizlik faqat axborot texnologiyalari sohasi doirasidagina emas, balki huquqiy, ijtimoiy va psixologik jihatlarni ham qamrab olishi lozim. Bu esa sohaga tizimli yondashuv zarurligini ko‘rsatadi.

Kiberhujumlar va ularning turlari

Kiberhujumlar ko‘plab shakllarda bo‘lishi mumkin. Bular orasida:

Viruslar – tizimga kirib, foydalanuvchilarga zarar yetkazadigan dasturlar.

Troyanlar – foydalanuvchi xohlamagan dasturlar, lekin ular tizimga kirishni ta’minlaydi.

Phishing – foydalanuvchilardan maxfiy ma'lumotlarni o‘g‘irlash uchun ular bilan yolg‘on muloqot qilish.

DDoS hujumlari (Distributed Denial of Service) – tizimni ishlay olmaydigan darajaga keltirish uchun xizmatlarni to‘sish.

Himoyalanish usullari

Himoyalanish usullari zamonaviy texnologiyalar yordamida amalga oshiriladi. Eng ommabop usullar:

Kriptografiya – ma’lumotlarni shifrlash va faqat ruxsat etilgan foydalanuvchilar uchun ochish.

Tarmoq xavfsizligi – xavfsizlik devorlari (firewall) va boshqa tarmoq xavfsizligi protokollarini qo‘llash.

Xavfsizlikni boshqarish tizimlari (SIEM) – tizimlarning xavfsizligini kuzatish va tahlil qilish.

Foydalanuvchi xavfsizligi – foydalanuvchilarga xavfsiz parollar, ikki faktorli autentifikatsiya va boshqa himoya usullarini ta’minlash.

Sun'iy intellekt va mashina o‘rganishning roli

Sun'iy intellekt (AI) va mashina o‘rganish (ML) texnologiyalari kiberxavfsizlikni mustahkamlashda juda katta rol o‘ynaydi. AI yordamida tarmoqlarda g‘ayritabiiy xatti-harakatlarni aniqlash va tahdidlarni oldindan bashorat qilish mumkin. ML esa tizimlarga tahdidlar to‘g‘risida o‘rganish va yangi hujum usullarini aniqlashda yordam beradi.

Kiberxavfsizlik siyosatlari va yuridik asosi

Kiberxavfsizlikni mustahkamlash uchun davlatlar va kompaniyalar tomonidan qabul qilingan siyosatlar hamda me'yoriy hujjatlar katta ahamiyatga ega. Yuridik nuqtai nazardan, ma’lumotlarni himoya qilish va himoya choralarini ko‘rish uchun turli qonunlar va qonunchilikka rioya qilish zarur.

Xulosa

Xulosa qilib aytganda, raqamli texnologiyalarning jadal rivojlanishi bilan birga kiberxavfsizlik muammolari ham keskin tus olmoqda. Tadqiqotlar natijasi shuni ko‘rsatadiki, kiberhujumlarning xilma-xilligi, murakkabligi va avtomatlashtirilgan shakllari insoniyat uchun jiddiy tahdidlar tug‘dirmoqda. Ushbu tahdidlarning oldini olishda zamonaviy texnologiyalar, xususan, kriptografiya, SIEM tizimlari, sun’iy intellekt va mashina o‘rganish kabi vositalar muhim rol o‘ynaydi. Shuningdek, samarali kiberxavfsizlik faqat texnik himoya bilan cheklanmasdan, foydalanuvchilarning ongli harakati, doimiy axborot savodxonligi, xavfsizlik siyosatiga qat’iy rioya etish va davlatlararo hamkorlik kabi omillar bilan mustahkamlanishi kerak. Har qanday tashkilot yoki foydalanuvchi raqamli dunyoda xavfsiz faoliyat yuritish uchun kompleks yondashuvni tanlashi lozim. Kelgusida ushbu mavzu doirasida tahlillarni chuqurlashtirib, milliy va xalqaro tajribalarni solishtirish, turli sektorlar uchun mos himoya strategiyalarini ishlab chiqish dolzarb masalalardan biri bo‘lib bo‘lib qoladi

Foydalanilgan adabiyotlar

1. Jalilov, A. (2020). Kiberxavfsizlik va axborot tizimlarining himoyasi. Tashkent: Informatika va axborot texnologiyalari institutining nashriyoti.

2. Xudoyberganov, S. (2018). Axborot xavfsizligi va tarmoqni himoya qilish metodlari. Tashkent: Ma'lumotlar xavfsizligini ta'minlash markazi

3. Maqsudov, O., & Tashkentov, M. (2019). Raqamli xavfsizlik: Kiberhujumlarga qarshi kurashish. Tashkent: O'zbekiston Milliy Universiteti nashriyoti.

4. Salimov, D. (2021). Internet xavfsizligi va himoya tizimlari. Tashkent: Xalqaro axborot texnologiyalari universiteti nashriyoti

5. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. 7th Edition. Pearson Education. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd Edition. Wiley.

6. Bertino, E., & Sandhu, R. (2005). Database Security: Concepts, Approaches, and Challenges. IEEE Computer Society Press.

7. Shostack, A. (2014). Threat Modeling: Designing for Security. Wiley.

8. Bianchi, G., et al. (2021). Artificial Intelligence in Cybersecurity: A Survey. Journal of Cybersecurity, 7(1).