KIBERXAVFSIZLIK:RAQAMLI DUNYODA MA'LUMOTLARNI HIMOYA QILISH MUAMMOLARI VA YECHIMLARI

Akbaraliyeva Munojat G'ulomjon qizi
Farg'ona davlat universiteti
Chet tillari fakulteti 1-kurs talabasi
*Ilmiy raxbar:**Mirzaakbarov Dilshodbek Dovlatboyevich***
Farg'ona davlat universiteti axborot texnologiyalari kafedrasi
katta o'qituvchisi

Annotatsiya: Ushbu maqolada kiberxavfsizlik tushunchasining mazmuni, unga oid asosiy tahdidlar va ularni bartaraf etish yo'llari tahlil qilinadi. Xususan, ma'lumotlar buzilishi, fishing, zararli dasturlar va DDoS hujumlari kabi muammolar hamda ularning oldini olish uchun texnik, ijtimoiy va siyosiy choralar ko'rib chiqiladi. O'zbekiston va xalqaro tajriba misolida kiberxavfsizlik sohasidagi dolzarb islohotlar va tavsiyalar bayon etiladi.

Kalit so'zlar: kiberxavfsizlik, axborot xavfsizligi, raqamli tahdidlar, phishing, malware, DDoS, shifrlash

Annotation: This article analyzes the concept of cybersecurity, its major threats, and possible solutions. It discusses issues such as data breaches, phishing, malware, and DDoS attacks, and explores technical, social, and legal measures to prevent them. The paper also highlights recent reforms and recommendations in the field of cybersecurity in Uzbekistan and around the world.

Keywords: cybersecurity, information security, digital threats, phishing, malware, DDoS, encryption

Аннотация: В данной статье рассматриваются понятие кибербезопасности, основные угрозы и возможные пути их устранения. Особое внимание уделяется таким проблемам, как утечка данных, фишинг, вредоносные программы и DDoS-атаки, а также техническим, социальным и правовым мерам по их предотвращению. Приводятся актуальные реформы и рекомендации в области кибербезопасности в Узбекистане и за рубежом.

Ключевые слова: кибербезопасность, информационная безопасность, цифровые угрозы, фишинг, вредоносное ПО, DDoS, шифрование

Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo'lib, unga berilgan turlicha ta'riflar mavjud. Xususan, CSEC2017 Joint Task Force manbasida kiberxavfsizlikka quyidagicha ta'rif berilgan : kiberxavfsizlik – hisoblashlarga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni to'g'ri bajarilishini kafolatlash uchun o'zida texnologiya, inson, axborot va

jarayonlarni mujassamlashtiradi. U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlillash va testlashni o'z ichiga oladi. Kiberxavfsizlik ta'limning mujassamlashgan bilim sohasi bo'lib, qonuniy jihatlarni, siyosatni, inson omilini,etika va risklarni boshqarishni o'z ichiga oladi. Tarmoqlar sohasida faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta'rif bergan [2]: Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarish, almashtirish yoki yo'q qilishni;foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi.Kiberxavfsizlik nafaqat texnologik masala, balki ijtimoiy, huquqiy va siyosiy ahamiyatga ega yo‘nalishdir. Uni ta'minlashda texnik vositalar bilan birga inson omili, foydalanuvchi madaniyati, qonunchilik bazasi va xalqaro hamkorlik ham muhim rol o‘ynaydi. Ayniqsa, O‘zbekiston kabi raqamli transformatsiyani bosqichma-bosqich joriy qilayotgan davlatlar uchun bu soha juda muhim hisoblanadi.Mazkur maqolada kiberxavfsizlik tushunchasi, asosiy muammolari, mavjud yechimlari, xalqaro tajriba hamda foydalanuvchi va jamiyat darajasida bu boradagi yondashuvlar yoritiladi. Shuningdek, axborot xavfsizligini ta'minlashda dolzarb bo‘lgan tavsiyalar ham keltiriladi.

Kiberxavfsizlik bilan bog‘liq muammolar turlicha va murakkabdir. Eng ko‘p uchraydigan tahdidlar quyidagilardan iborat:

1. Ma'lumotlar buzilishi (Data breach)

Turli kompaniyalar va tashkilotlar mijozlari yoki foydalanuvchilariga oid maxfiy ma'lumotlarni saqlaydi. Ushbu ma'lumotlar — parollar, bank ma'lumotlari, shaxsiy hujjatlar kabi nozik axborotlar — kiberjinoyatchilar uchun asosiy nishondir. Bu ma'lumotlar noqonuniy yo‘llar bilan qo‘lga kiritilib, sotilishi yoki zararli maqsadlarda ishlatilishi mumkin.

2. Phishing va soxta xabarlar

Foydalanuvchining ishonchini qozonish orqali uni aldab, shaxsiy ma'lumotlarni qo‘lga kiritish usuli. Phishing xatlari ko‘pincha rasmiy tashkilotlardan yuborilgandek ko‘rinadi va foydalanuvchini havola bosishga undaydi.

3. Zararli dasturlar (Malware)

Viruslar, troyanlar, spyware kabi zararli dasturlar qurilmaga o‘rnatiladi va u orqali ma'lumotlar o‘g‘irlanadi yoki qurilma ishdan chiqariladi. Ayniqsa, ransomware (garov dasturlari) oxirgi yillarda ko‘p tarqalgan — bu dasturlar ma'lumotlarni shifrlab qo‘yib, ularni qayta ochish uchun pul talab qiladi.

4. DDoS hujumlari

Xizmat ko‘rsatuvchi saytlar va serverlarga haddan tashqari ko‘p so‘rov yuborish orqali ularni ishdan chiqarish maqsad qilinadi. Bu, ayniqsa, onlayn xizmat ko‘rsatuvchi kompaniyalar uchun katta yo‘qotishlarga olib keladi.

Kiberxavfsizlikni ta’minlash uchun texnik vositalar, foydalanuvchi xabardorligi va davlat siyosati birgalikda harakat qilishi zarur.

1. Texnik himoya vositalari

Kuchli antivirus va xavfsizlik devorlari (firewall) ishlatilishi kerak.

Ikki bosqichli autentifikatsiya (2FA) foydalanuvchi himoyasini ancha kuchaytiradi.

Ma’lumotlarni shifrlash (encryption) va zaxira nusxalarini saqlash muhim.

2. Foydalanuvchi xabardorligi

Har bir foydalanuvchi xavfsiz parol yaratish, noma’lum havolalarga kirmaslik, shubhali ilovalarni yuklamaslik kabi oddiy, ammo muhim qoidalarga amal qilishi kerak.

Maktab, oliygoh va ish joylarida kiberxavfsizlik bo‘yicha treninglar o‘tkazilishi foydalidir.

3. Davlat va xalqaro darajadagi chora-tadbirlar

Qonunchilikda axborot xavfsizligi bilan bog‘liq qat’iy normalar belgilanishi kerak.

Xalqaro hamkorlik kiberjinoyatchilikka qarshi kurashda muhim rol o‘ynaydi.

Yevropa Ittifoqidagi GDPR kabi qonunlar ma’lumotlar himoyasiga alohida e’tibor qaratadi.

Hozirgi kunda O'zbekiston va boshqa mamlakatlarda ham kiberxavfsizlik sohasida bir qancha islohotlar amalga oshirilmoqda:

O‘zbekistonda amalga oshirilayotgan islohotlar:

1. Xalqaro hamkorlik va tajriba almashinuvi

2024-yil oktyabr oyida Toshkent shahrida “Kiberxavfsizlik sammiti – Markaziy Yevroosiyo, CSS – 2024” II Xalqaro kiberxavfsizlik sammiti bo‘lib o‘tdi. Tadbirda 30 dan ortiq mamlakatdan 60 ga yaqin kompaniya va 120 dan ortiq delegat ishtirok etdi. Sammitning asosiy maqsadi mintaqaviy kiberhamjamiyat uchun o‘zaro tajriba almashish, zamonaviy yechimlarni namoyish etish va yangi imkoniyatlarni ochishdan iborat edi.

2. Aholining xabardorligini oshirish

Kiberxavfsizlik markazi tomonidan aholini firibgarlar tuzog‘iga tushib qolmaslik uchun ikki bosqichli autentifikatsiyani o‘rnatish, SMS-xabarnomada kelgan raqamlarni hech kimga taqdim etmaslik kabi tavsiyalar berilgan. Bu chora-tadbirlar aholini Telegram va boshqa platformalarda tarqalayotgan zararli havolalardan himoya qilishga qaratilgan.

Xalqaro miqyosda amalga oshirilayotgan islohotlar:

1. AQShning xalqaro kiberxavfsizlik strategiyasi

2024-yilda AQSh hukumati xalqaro kiberxavfsizlik strategiyasini e’lon qildi. Ushbu strategiya global raqamli ekotizimni himoya qilish, huquqni hurmat qiluvchi raqamli

texnologiyalarni ilgari surish, kiberhujumlarga qarshi koalitsiyalar tuzish va sherik davlatlarning kiberxavfsizlik salohiyatini oshirishga qaratilgan.

2. CISA tomonidan kiberxavfsizlik bo‘yicha xabardorlik dasturi

AQShning Kiberxavfsizlik va infratuzilmani xavfsizligi agentligi (CISA) 2024-yilda "We Can Secure Our World" nomli jamoatchilikka xizmat ko‘rsatish e’lonini taqdim etdi. Ushbu dastur odamlarni onlayn xavfsizlikni ta’minlash uchun faol choralar ko‘rishga undaydi.

Xulosa

Kiberxavfsizlik bugungi raqamli jamiyatda axborotni himoya qilishda muhim omilga aylangan. Ma’lumotlar xavfsizligini ta’minlash faqat texnik vositalar bilan emas, balki foydalanuvchilarning xabardorligini oshirish, qonunchilikni kuchaytirish va xalqaro hamkorlik orqali ham amalga oshirilishi kerak. O‘zbekistonda va jahon miqyosida olib borilayotgan islohotlar ushbu yo‘nalishda muhim qadamlar bo‘lib, ularning samarali amalga oshirilishi raqamli muhitni yanada xavfsiz qiladi.

Foydalanilgan adabiyotlar:

1. CSEC2017 Joint Task Force. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. ACM, IEEE Computer Society.
2. Cisco. What is Cybersecurity? Cisco Official Website.
3. CISA (Cybersecurity and Infrastructure Security Agency). We Can Secure Our World – Public Awareness Campaign, 2024.
4. The White House. United States International Cyberspace and Digital Policy Strategy, 2024.
5. “CSS – 2024” II Xalqaro Kiberxavfsizlik Sammiti, Toshkent, 2024.
6. Ganiyev S.K., Ganiyev A.A., Xudoyqulov Z.T. Kiberxavfsizlik asoslari. O‘quv qo‘llanma. – Toshkent: TATU, 2020.