

## ZAMONAVIY DUNYODA MA'LUMOTLAR XAVFSIZLIGI YOXUD KIBER HUJUMLARDAN SAQLANISH

**Aldashev Ilhomjon**

*Farg'ona davlat universiteti o'qituvchisi*

**Qosimova Ismigul**

*Farg'ona davlat universiteti filologiya fakulteti 1-kurs talabasi*

**Annotatsiya:** *Ushbu maqolada ma'lumotlar xavfsizligi va kiber hujumlardan saqlanish, shu bilan birga ularga sabab bo'ladigan holatlar haqida so'z yuritilgan.*

**Tayanch so'zlar:** *xavf, xavfsizlik, hacker, ma'lumotlar xavfsizligi, kiber hujum, electron pochta, veb-sayt, virus, Phishing, Accidental data exposure, insider tahdid.*

XXI asr texnologiyalar asri bo'layotgani barchamiz uchun sir emas. Hozirgi davrni zamonaviy texnologiyalarsiz tasavvur qilish qiyin. Ular inson hayotidan shunday o'rin egallaganki, kundalik hayotimizni texnologiyalardan foydalanmay o'tkazolmaymiz.

Shu bilan birga texnologiyalar qanchalik rivojlangani sari ulardan foydalanishdagi xavfsizlik ham dolzarb va zarur bo'lib qolmoqda. Ayniqsa, zamonaviy korxonalar tomonidan qo'llanilayotgan SaaS ilovalari sonining ko'pligi ichki va tashqi identifikatsiyalar tomonidan almashiladigan va boshqariladigan maxfiy ma'lumotlarga kirish va xavfsizligini boshqarish jarayonida qiyinchiliklarga olib keladi, Sizning kompaniyangizda ma'lumotlarga kiruvchi va foydalanuvchi odamlar qanchalik ko'p bo'lsa, moliyaviy jarimalar, biznesni buzish, brendga zarar yetkazish kabi xavfsizlikni buzish va salbiy oqibatlarga sabab bo'lish muammolari shunchalik yuqori bo'ladi.

Ma'lumotlar xavfsizligi nega kerak?

Axborotlar xavfsizligini ta'minlashning asosiy maqsadi ma'lumotlarning konfidensialligi, yaxlitligi, mavjudligini hisobga olgan holda, tashkilot faoliyatiga hech qanday zarar yetkazmasdan himoyalashdir. Korxonalar, muassasa, tashkilotlarning intellektual mulkini himoya qilish, turli salbiy oqibatlardan saqlash uchun ham muhimdir.

Axborot xavfsizligining markazida ma'lumotni himoyalash faoliyati, uning maxfiyligi mavjudligini ta'minlash, shuningdek, tanqidiy vaziyatda har qanday murosaga yo'l qo'ymaslik yotadi. Ayniqsa, hozirgi kunlarda zararli dasturlar orqali insonning shaxsiy mulkini va tashkilotlar ma'lumotini o'zlashtirish kabi muammolar avj olmoqda.

Zararli dasturlar deganda, kompyuter va tarmoqqa zarar yetkazish uchun mo'ljallangan dasturiy ta'minot tushuniladi. Zararli dastur viruslar, troyanlar va to'lov dasturlari kabi ko'plab shakllarni olishi mumkin. Mana shunday xavflar orqali ma'lumotlarga zarar yetmoqda. Xavfsizlikka zarar yetkazadigan tahdidlarning bir necha turlari mavjud:

1. Ichki tahdid (Indiser threats) tashkilot tizimi va ma'lumotlariga qonuniy kirish huquqiga ega bo'lgan o'sha tashkilotning o'ziga tegishli bo'lgan xodimlar tomonidan amalga oshirilgan va kelib chiqadigan xavflarni bildiradi. Bunday tahdidlar qasddan yoki tasodifiy ma'lumotlarning buzilishi, sabotaj va maxfiy ma'lumotlarni o'g'irlashdan va sotishdan iborat bo'ladi.

2. Fishing (Phishing) bu soxta veb-saytlar yoki qonuniy ko'rinadigan elektron pochta orqaliparollar va moliyaviy kabi maxfiy axborotlarni olish, insonlarni aldash faoliyatidir. Fishing hujumlarida, asosan, insonlarning shaxsiy ma'lumotlarini oshkor qilish usulidan foydalaniladi.

3. Accidental data exposure (Tasodifiy ma'lumotlarga duch kelish) bu jarayon maxfiy ma'lumotlarni ruhsatsiz shaxslarga tasodifan taqdim etilganda sodir bo'ladigan hujumdur. Bu noto'g'ri sozlangan bulutli saqlash sozlamalari, noto'g'ri qabul qiluvchilarga elektron pochta xabarlarini yuborish yoki maxfiy axborotlarni turli xil veb-saytlarga yuborish va joylash orqali kelib chiqadi.

Ma'lumotlar xavfsizligiga to'xtalar ekanmiz, kiber xavfsizlik atamasini ham chetta qoldirmasligimiz kerak. Kiber xavfsizlik o'zi nima?

Kiber xavfsizlik internet yoki elektron tarmoq, veb-sahifalar orqali ma'lumotlar, tizimlar, dasturlar va qurilmalarni kiber hujumlar, hockeringlar, viruslar, matware, identifikatsiya olish va boshqa kiber xavfsizlik xavf himoyalariga qarama-qarshi himoya qilishning qavmlarini tashlik etish, rivojlantirish va saqlash sohasidagi texnologik va amaliy faoliyatni ifodalovchi tarmoqning bir qismidir.

Kiber xavfsizlikni bilmaslik oddiy odamlarda turli xil muammolarga olib keladi. Ko'pchilik foydalanuvchilar kompyuter, mobil qurilma va boshqa texnologik voitalardan foydalansa-da, ular qurilmalaridagi maxfiylik sozlamalari va onlayn hisoblari haqida to'liq ma'lumotlarga ega emaslar. Bu esa ularning xavfsizlik bilan ta'minlanmaganini anglatadi. Shuningdek, aksariyat foydalanuvchilar maxfiy ma'lumotlari parollari sifatida oddiy sonlardan, masalan, "12345678", kabi yoinki ID raqamlaridan foydalanadi. Bu esa kiber hujumlar uchun oson o'lja hisoblanadi va hockerlar tomonidan osonlik bilan o'zlashtirishga imkoniyat yaratadi.

Kiber hujumlardan saqlanish uchun quyidagilarga amal qilish mqsadga muvofiqdir:

1. Yuqorida aytilganlarni hisobga olgan holda, birinchi navbatda, hujumlardan omon qolish uchun parolni yangilash eng muhim yechimlardan biridir. O'zingizning onlayn hisobingizdagi parollarni tez-tez yangilash va har bir sayt uchun alohida parol ishlatish va bu parolni qayta ishlatmaslik muhimdir.

2. Kompyuteringiz va qurilmangizning dasturiy ta'minotini kengaytirilgan antivirus va antipyyware dasturlari yordamida muhofaza qiling.

3. Maxfiy ma'lumotlaringizni, shu jumladan, bank, karta ma'lumotlarini yoping va boshqa maxfiy ma'lumotlarni tasdiqlangan saytlar, ilovalar yoki banklar orqali oling.

Shu bilan birga, kiber xavfsizlik haqida savodxonlikni, bilimni oshirish va bu haqida to'liq o'rganish eng asosiysi va eng keraklisidir. Sababi biz texnologik jarayonda

yashamoqdamiz va internet, texnologiyalar kundan kun rivojlanib, takomillashib bormoqda.

#### **FOYDALANILGAN ADABIYOTLAR:**

1. Modern APICASB for SaaS Applications. [www.docontrol.io/](http://www.docontrol.io/)
2. The National Cyber Security Centre. [www.ncsc.gov.uk/](http://www.ncsc.gov.uk/)
3. Johnson John. The evolution of British Sigint 1653-1939. (Her Majesty's stationary Office 1998)
4. I.Aldashev "Media ta'limning o'quv jarayoniga tatbig'i" Results of National Scientific Research International Journal 2023
5. .Aldashev "O'qituvchi ishida ijodiy yondashish xususiyatlari" Results of National Scientific Research International Journal 2023 Volume 2| Issue 4
6. I.Aldashev, S.Aldasheva "Dars samaradorligini oshirishda axborot texnologiyalarining o'rni" - ... and practical conference" the time of..., 2022 Related articles
7. Modern information technologies in education is a new opportunity I.Aldashev - Economy and society, 2020 Cited by 8 Related articles