HOZIRGI KUNDA KIBER HUJUMLAR VA KIBER QONUNLAR

Davronova Sevinch
Muhammad al-Xorazmiy nomidagi TATU
Qarshi filiali AKT yo‘nalishi talabasi

ANNOTATSIYA

Kiberhujum tizimga ruxsatsiz, buzib kirish orqali mo‘ljallangan nishonni o‘g‘irlashi, o‘zgartirishi yoki yo‘q qilishi mumkin. Bu turdagi hujumlar shaxsiy kompyuterga josuslik dasturlarini o‘rnatishdan tortib, biror davlat infratuzilmasini butkul yo‘q qilishga urinish kabi maqsadlarda sodir etilishi mumkin. Yuridik ekspertlar atamani jismoniy shikastlanish hodisalari bilan cheklab qo‘yishga moyil bo‘lib, odatiy ma’lumotlar buzilishi va kengroq xakerlik harakatlaridan ajratishga intilishadi.

Kalit so‘zlar: *axborot texnologiyalari,kiberhujumlar, kiberqonunlar, hakkerlar, kiberterrozim.*

So‘ngi yillarda mamlakatimizda ijtimoiy-iqtisodiy, sog‘liqni saqlash, ta’lim, huquqni muhofaza qilish va boshqa sohalarga zamonaviy informatsion texnologiyalar keng tadbiq etilmoqda. Bu esa kundalik hayotimizda o‘ziga xos qulayliklar yaratishi bilan birgalikda “Kiberjinoyat” tushunchalarini hayotimizga olib kirdi.Bugungi kunda ijtimoiy injiniring yordamida va virusli fayllarni pochta orqali jo‘natish orqali qilinadigan kiberhujumlar keng tarqalgan.

Kiberhujumlar — kompyuter axborot tizimlari, kompyuter tarmoqlari infratuzilmalar yoki shaxsiy kompyuter qurilmalariga qaratilgan har qanday hujum. Hujumni amalga oshiruvchi shaxs ma’lumotlarga, funksiyalarga yoki tizimning boshqa kirish cheklangan

joylariga ruxsatsiz, potensial ravishda yomon niyatda kirishga harakat qiladi. Kontekstga qarab, kiberhujumlarm kiberurush yoki kiberterrorizmning bir qismi sifatida tavsiflanishi mumkin. Kiberhujum suveren davlatlar, shaxslar, guruhlar, miyatlar yoki tashkilotlar tomonidan qo‘llab-quvvatlanishi yoki anonim manba asosida yuzaga chiqishi mumkin. Kiberhujum paytida foydalaniluvchi qurol-asboblar kiberqurollar deb ataladi. So‘nggi bir necha yil ichida kiberhujumlar soni yuqori hajmda tashkil etilmoqda.

Kiberhujumlar, hozirda, tobora murakkab va xavfli tusga egadir.Ushbu hujumlarning oldini olish uchun foydalanuvchi xatti-harakatlari tahlili va Xavfsizlik ma’lumotlari va hodisalarni boshqarish mumkin hisoblanadi. So‘nggi yillarda esa kiberhujumlarning ko‘lami va chidamliligi tez sur’atlar bilan oshib keldi. Jahon Iqtisodiy Forumi 2018-yilgi hisobotida ta’kidlaganidek: „Kiberhujumlar soni biz ularga qarshi kurashish qobiliyatimizga qaraganda tezroq rivojlanmoqda“.

•“Internet kundan-kunga hayotimizning ajralmas qismiga aylanib bormoqda. Fuqarolar, korporatsiyalar, hukumatlar bir-biri bilan inernetda aloqa qiladi. Kommunikatsiya, tijorat, hamkorlik global tarmoq bilan bog‘liq. Bugungi kunda jinoiy niyatdagilar uchun imkoniyatlar bisyor”, - deydi AQSh Ichki xavfsizlik vazirligidan Jonatan Xoumer.

Internetga qaramlik hamda raqamli informatsiya jinoyatchilar uchun ko‘proq moliyaviy daromad degani. Ular fayllarni qulflab, egasidan pul talab qiladi.“Shantaj qilish oson bo‘lib qoldi, chunki kompyuter sistemalariga buzib kirish uchun kerakli programmalar qora bozorda muhayyo”, - deydi informatsion texnologiyalar bo‘yicha mutaxassis Klifford Nyuman. **Kiberqonunlar.** Qonun (huquq) — inson, jamiyat va davlat manfaatlari nuqtai nazaridan eng muhim hisoblanadigan ijtimoiy munosabatlarni mustahkamlash, rivojlantirish va tartibga solish vositasi. Qonunning nima maqsadga qaratilganini u yo‘naltirilgan munosabatga qarab aniqlash mumkin. Shu bois qonunlar turli sohaga oid maqsadlarga ega bo‘lishi mumkin. Umumiy nomda kiberjinoatchilikni tartibga solishni maqsad qilgan qonunlar kiberqonunlar deb ataladi. Qonunni ishlab chiquvchilar va uni himoya qiluvchilar

butun dunyo bo‘ylab kiberjinoyatchilikni aniq belgilaydigan va kiber dalillarni qabul qilishni to‘liq madadlovchi kiberqonunlar zarurligi haqida ogohlantirib keladilar. Xususan, Respublikamizda ham “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili”da amalga oshirishga oid davlat dasturi to‘g‘risida”gi O‘zbekiston Respublikasi Prezidenti Farmoni loyihasi va 2020 yil Davlat dasturi loyihasida 2020–2023 yillarga mo‘ljallangan kiberxavfsizlikka doir milliy strategiya va “Kiberxavfsizlik to‘g‘risida”gi qonun loyihasi ishlab chiqish rejalashtirilgan. Hujjatga asosan xavfsizlikni, millatlararo totuvlik va diniy bag‘rikenglikni ta’minlash, shuningdek, tashqi siyosat sohasida: 2020 yil 1 sentyabrga qadar kiberxavfsizlikning huquqiy asoslarini shakllantirish bo‘yicha choralar ko‘riladi, shu jumladan 2020–2023 yillarga mo‘ljallangan kiberxavfsizlikka doir milliy strategiya va “Kiberxavfsizlik to‘g‘risida”gi qonun loyihasi ishlab chiqiladi; Kiberqonunlar har bir davlatning milliy qonun me’yorlari asosida shakllantiriladi yoki ularning bir qismini tashkil qiladi. Quyida Respublikamizdagi qonun hujjatlarida kiberjinoyatni oldini olish va tartibga solishga aloqador bo‘lgan bandlar keltirilgan. ***Milliy qonunlar.*** 2002 yil 12 dekabrda O‘zbekiston Respublikasining 439-II – sonli “Axborot erkinligi prinsiplari va kafolatlari to‘g‘risida”gi qonuni qabul qilindi. Ushbu qonun 16 moddadan iborat bo‘lib, unda xususan, quyidagilar belgilangan: Ushbu Qonunning asosiy vazifalari axborot erkinligi prinsiplari va kafolatlariga rioya etilishini, har kimning axborotni erkin va moneliksiz izlash, olish, tekshirish, tarqatish, foydalanish va saqlash huquqlari ro‘yobga chiqarilishini, shuningdek axborotning muhofaza qilinishini hamda shaxs, jamiyat va davlatning axborot borasidagi xavfsizligini ta’minlashdan iborat. ***Axborot erkinligi*** O‘zbekiston Respublikasining Konstitutsiyasiga muvofiq har kim axborotni moneliksiz izlash, olish, tekshirish, tarqatish, undan foydalanish va uni saqlash huquqiga ega. Axborot olish faqat qonunga muvofiq hamda inson huquq va erkinliklari, konstitutsiyaviy tuzum asoslari, jamiyatning axloqiy qadriyatlari, mamlakatning ma’naviy, madaniy va ilmiy salohiyatini muhofaza qilish, xavfsizligini ta’minlash maqsadida cheklanishi mumkin.

Xulosa qilib shuni ta’kidlab o‘tish zarurki: XXI asr “Axborot texnologiyalari asri” da deyarli har bitta inson internet tarmoqlari, mobil qurilmalar va kompyuterlardan foydalanishadi. Afsuski, hammasi ham ishlatayotgan qurilmasidagi funksiyalarning 90%ini ishlatishni bilishmaydi. Bu esa juda og‘ir vaziyatlarga olib keladi. Hozirgi kunda esa buning oldini olishini uchun turli xil tadbirlar olib borilmoqda. Misol uchun: Toshkent Axborot Texnologiyalari Universiteti Qarshi Filialida **cyber102** tadbiri olib borildi. Tadbirning asosiy maqsadi shundan iboratki, odamlar o‘rtasida kiberxavfsizlik nima? Kiberhujum nima? Ular hakkerligini qanday bilish mumkin? Va shu kabi savollarga javob topildi. Va yana shuni ta’kidlab o‘tish lozimki, hech kim login parollaringizni, bank karta raqamalaringizni bermasligingiz kerak. Zero, hammamizni o‘zimizni o‘zimiz himoya qilishimiz kerak. Chunki kiberjinoyatchilarni topish ham oson ish emas.

FOYDALNILGAN ADABIYOTLAR

1.innemore, Martha; Hollis, Duncan B (2020), „Beyond Naming and Shaming: Accusations and International Law in Cybersecurity“, European Journal of International Law, doi:10.2139/ssrn.3347958

2.Sanaei, M. G., Isnin, I. F., & Bakhtiari, M. (2013). Performance Evaluation of Routing Protocol on AODV and DSR Under Wormhole Attack. International Journal of Computer Networks and Communications Security, Volume 1, Issue 1, Andoza:ISSN.

3.TURSUNOVA A.H (2023). TA’LIM JARAYONIDA INTELLEKTUAL–KREATIV QOBILIYATLARINI RIVOJLANTIRISHNING MAZMUNIY XUSUSIYATLARI. OLIM ,1(6), 18–21.

4. TURSUNOVA A.H THE ADVANTAGES AND FEATURES OF TEACHING AND LEARNING ONLINE IN THE EDUCATION PROCESS https://cyberleninka.ru/article/n/the-advantages-and-features-of-teaching-and-learning-online-in-the-education-process