KIBERJINOYAT VA KIBERXUJUMLARDAN HIMOYALANISHNING SAMARALI USULLARI

Yo‘ldoshev Abror Alisher o‘g‘li
Toshkent Davlat Texnika Universiteti
E-mail: abroryoldoshev979@gmail.com
Telefon: +998(94) 630 74 82
+998(91) 017 58 03

ANNOTATSIYA: *Zararli dasturlar (viruslar, qurtlar, troyanlar, spyware va boshqalar) tizim xavfsizligiga jiddiy tahdid soladi. Bu dasturlar tarmoq orqali tarqalar ekan, tizimlarni buzib, shaxsiy ma'lumotlarni o'g'irlashi yoki tizimni ishdan chiqarishi mumkin. Zararli dasturlardan himoyalanish uchun antivirus dasturlarini o'rnatish, shubhali manbalardan ilovalarni yuklamaslik, tizimni doimiy yangilab turish va xavfsiz internet ulanishlari uchun VPN kabi xavfsizlik choralari zarur.*

Kalit so‘zlar: *Kiberjinoyat, kiberhujum, zararli dasturlar, antivirus, kiberxavfsizlik, phishing, parol xavfsizligi, VPN, shifrlash va tarmoq monitoringi kabilar kiberhujumlar va jinoyatlarga qarshi kurashda muhim tushunchalar hisoblanadi. Bu so'zlar, tizimni himoya qilish va shaxsiy ma'lumotlarni xavfsiz saqlash uchun zarur bo'lgan choralarga asoslanadi.*

Kiberjinoyat — kompyuter va tarmoqning birgalikdagi aloqasi ostida sodir etiluvchi jinoyat turi. Kompyuter jinoyat paytida maqsadli yo‘naltirilgan qurol vazifasini bajarib beradi. Kiberjinoyat kimningdir xavfsizligi va moliyaviy saviyasiga zarar yetkazish maqsadida sodir etiladi.

Kiberhujum – kompyuter axborot tizimlari, kompyuter tarmoqlari, infratuzilmalar yoki shaxsiy kompyuter qurilmalariga qaratilgan har qanday hujumkor manyovr[1]. Hujumni amalga oshiruvchi shaxs ma’lumotlarga, funksiyalarga yoki tizimning boshqa kirish cheklangan joylariga ruxsatsiz, potensial ravishda yomon niyatda kirishga harakat qiladi[2]. Kontekstga qarab, kiberhujumlar kiberurush yoki kiberterrorizmning bir qismi sifatida tavsiflanishi mumkin. Kiberhujum suveren davlatlar, shaxslar, guruhlar, jamiyatlar 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.

2023-yilda O‘zbekiston jiddiy kiberxavfsizlik muammosi bilan qarama-qarshi vaziyatda, ayni vaqtda, veb-resurslarimizga **11,2 milliondan ortiq kiberhujumlar** amalga oshirildi. Ushbu kiberhujumlarning geografik kelib chiqish tahlili ba’zi tendensiyalarga yo’l ochdi. IP manzillardan olingan ma’lumotlarga ko’ra, 759 500 kiberhujum “vatani” Niderlandiya bo‘ldi. Bunday mamlakatlar qatorini shunday davom

ettirish mumkin: AQSH, Rossiya, Germaniya, Hindiston va Xitoy. Ushbu tahdidlar O‘zbekistonga qaratilgan hakerlik hujumlarining qariyb **90 foizini** tashkil etadi. Natijada kiberxavfsizlikni ta’minlashda transmintaqaviy hamkorlik zarur elementga aylanadi.

Zararli dasturlarning bir necha xil turlari mavjud bo‘lib, ular quyida keltirilgan:

1. **Viruslar.** Bu boshqa dasturlarning kodiga, tizim xotira sohalariga, yuklash sektorlariga kirib boruvchi va ularni ishdan chiqaruvchi zararli dastur.

2. **Qurtlar**. Qurtlar viruslarga o‘xshaydi, lekin ular tarmoq orqali tarqalishi mumkin. Ular tarmoqdagi kompyuterlarni skanerlashi va ularga o‘zini nusxalashi mumkin.

3. **Troyanlar**. Troyanlar foydali dasturlar sifatida yashiringan zararli dasturlardir. Bunday dasturlarni yuklab olib, o‘rnatilganida, ular tizimga kirishi va konfidensial ma’lumotlarni o‘g‘irlashi mumkin.

4. **Advar.** Reklama dasturi (inglizcha - “advertising software”) foydalanuvchi ruxsatisiz reklamalarni ko‘rsatuvchi zararli dastur. Bu tiziminni sekinlashtirishi va ish faoliyatini yomonlashtirishi mumkin.

5. **Spam.** Zararli veb-saytlar yoki viruslarga havolalar bo‘lishi mumkin bo‘lgan elektron pochta xabari. Agar ushbu havolalar bosilsa, kompyuter zararlanishi mumkin.

6. **Rootkitlar.** Rootkitlar - bu kompyuterdagi tizim fayllariga kira oladigan yashirin dasturlar. Ular ma’lumotlarni o‘zgartirishi, yashirishi, tizim boshqaruvini qo‘lga olishi mumkin, bu esa ularni aniqlash va uchirib tashlashni qiyinlashtiradi.

7. **Spyware.** Josuslik dasturi - bu foydalanuvchi onlayn faoliyatini, jumladan u tashrif buyurgan veb-saytlar, kiritgan parollar va shaxsiy ma’lumotlarni kuzatishi mumkin bo‘lgan zararli dastur.

Zararli dasturlardan himoyalanish uchun quyidagi amallarni bajarish tavsiya etiladi:

1. Kompyuterlar va mobil qurilmalarga antivirus dasturlarini o‘rnatish va uni muntazam ravishda eng so‘nggi versiyasiga yangilash.

2. Faqat ishonchli manbalardan olingan rasmiy va tasdiqlangan ilovalar va dasturlardan foydalanish.

3. Notanish va ishonchsiz manbalardan olingan elektron pochta ilovalarini yoki fayllarni hech qachon ochmaslik.

4. Agar kerak bo‘lsa, parol yoki boshqa autentifikatsiya vositalaridan foydalangan holda kompyuter yoki mobil qurilmaga kirishni cheklash.

5. Operatsion tizim va boshqa dasturiy ta’minotni so‘nggi versiyalarga yangilash.

6. Umumiy Wi-Fi tarmoqlaridan foydalanganda ehtiyot bo‘lish. Parollar yoki bank kartasi ma’lumotlari kabi maxfiy ma’lumotlarni kiritmaslik.

7. Kompyuterda zararli dastur mavjudligini muntazam ravishda tekshirib turish va agar ular topilsa, ularni o‘chirib tashlash.

8. Foydalanuvchilarni shubhali havolalarni bosmaslik yoki noma’lum jo‘natuvchilarning ilovalarini ochmaslik kabi asosiy xavfsizlik tamoyillariga o‘rgatish.

Kiberjinoyat va kiberxujumlardan himoyalanishda samarali usullar bir qancha strategiyalarni o'z ichiga oladi. Quyida ba'zi asosiy va samarali usullarni keltiraman:

1. Kuchli parollar va ikki bosqichli autentifikatsiya (2FA).Kuchli parollar yaratish juda muhim. Parolni kamida 12 ta belgidan iborat qiling, va unda raqamlar, harflar, va maxsus belgilardan foydalaning. Parolni faqat o'zingiz bilishingiz kerak, va uni doimiy ravishda yangilab turish maqsadga muvofiq.Ikki bosqichli autentifikatsiya (2FA)ni yoqish orqali hisoblaringizni qo'shimcha xavfsizlik bilan himoyalang. Bu usul foydalanuvchidan foydalanuvchi nomi va parolni kiritganidan keyin, telefon orqali yuboriladigan qo'shimcha kodni ham talab qiladi.

2. Antivirus va zararkunandalardan himoya qilish dasturlaridan foydalanish.Antivirus dasturlari va zararkunandalardan himoya qilish dasturlarini muntazam yangilab turish zarur. Ular sizning tizimingizni zararli dasturlardan himoya qiladi va xujumlarni oldini oladi.Firevall (yong'in devori)ni yoqish orqali, tarmoqda kiruvchi va chiqadigan ma'lumotlarni nazorat qilib, zararli hujumlarning oldini olish mumkin.

3. Xavfsiz internet ulanishi va VPN (Virtual Private Network).VPN (Virtual Private Network) xizmatlaridan foydalanish internetda anonimlikni saqlashga yordam beradi va hackerlar tomonidan kuzatilish ehtimolini kamaytiradi.Jamoat Wi-Fi tarmog'idan foydalanishda ehtiyotkorlik bilan yondoshuv zarur, chunki ular kiberhujumlar uchun eng zaif nuqtalar bo'lishi mumkin.

4. Elektron pochta va SMS orqali keluvchi xatarlarga ehtiyotkorlik bilan yondoshuv.Phishing hujumlaridan saqlaning. Elektron pochta yoki SMS orqali so'rovlar, maxfiy ma'lumotlarni so'rash, yoki shubhali havolalarni bosishdan saqlaning.Elektron pochta xabarlari yoki SMS xabarlaridagi havolalarni bosishdan oldin, xatni yuborgan shaxsni yoki tashkilotni tekshirish zarur.

5. Ma'lumotlarni shifrlash.O'zingizning shaxsiy va moliyaviy ma'lumotlaringizni shifrlash orqali xavfsizligini oshiring. Shuningdek, ma'lumotlarni doimiy ravishda zaxira qilish (backup) ham muhimdir.Shaxsiy ma'lumotlaringizni onlayn platformalarda kamroq baham ko'ring, ayniqsa ijtimoiy tarmoqlarda.

6. Tizim va dasturlarning doimiy yangilanishi.O'chirilgan xavfsizlik teshiklaridan foydalanish orqali kiberjinoyatchilar tizimingizga kirishlari mumkin. Shuning uchun tizimlar va dasturlarni muntazam yangilab turish muhim.Patches va xavfsizlik yangilanishlarini o'rnatish orqali hujumlarga qarshi oldindan choralar ko'rishingiz mumkin.

7. Xavfsiz tarmoq aloqalari va internet faoliyati monitoringi.O'zingizning tarmog'ingizni va qurilmangizni xavfsizlikni nazorat qilish uchun monitoring qilish zarur. Tarmoqda sodir bo'layotgan barcha faoliyatni kuzatish va noma'lum faoliyatni darhol aniqlash yordam beradi.

8. Onlayn xavfsizlikni oshirish uchun ta'lim va xabardorlik.Kiberhujumlar va kiberjinoyatlar haqidagi xabardorlikni oshirish uchun o'zingizni va atrofdagilarni ta'lim olishga undang. Bu, xususan, ish joyida, maktablarda va boshqa muhitlarda foydalidir.

9. Xavfsiz dasturlarni tanlash va foydalanish.Dastur va ilovalarni faqat rasmiy manbalardan yuklab oling. Rasmiy do'konlar yoki ishlab chiqaruvchi saytlar tashqarisida dastur yuklash xavfli bo'lishi mumkin.Onlayn hisoblarni tekshirishda xavfsiz va tasdiqlangan ilovalarni ishlatish muhimdir.

Shu tarzda, kiberjinoyatlar va kiberxujumlardan himoyalanish uchun turli darajadagi choralarni ko'rish zarur, va bu doimiy e'tibor va yangilanishni talab qiladi.

Xulosa:Kiberjinoyat va kiberhujumlardan himoyalanish uchun har bir foydalanuvchi, tashkilot va davlat o'zining axborot tizimlarini kuchli xavfsizlik choralar bilan ta'minlashi kerak. Kuchli parollar, ikki bosqichli autentifikatsiya, antivirus dasturlari va ma'lumotlarni shifrlash kabi usullar yordamida tizim xavfsizligini oshirish mumkin. Bunda ta'lim va xabardorlik ham muhim rol o'ynaydi. Kiberhujumlar va jinoyatlarning oldini olishda global va transmintaqaviy hamkorlik zarur, chunki kiberxavfsizlik faqat milliy emas, balki xalqaro miqyosda ham qo'llab-quvvatlanishi kerak

FOYDALANILGAN ADABIYOTLAR:

1.O‘zbekiston Respublikasi Kiberxavfsizligi - 2020-yil hisoboti // https://csec.uz/uz/news/maqolalar/ozbekiston-respublikasi-kiberxavfsizligi-2020-yil-his

2. https://www.statista.com/statistics/1280009 /cost-cybercrimeworldwide/# statisticContainer

3. https://www.vesti.ru/finance/article/248146

4. Берова Д.М., Кибератаки как угроза информационной безопасности. 2018 // https://cyberleninka.ru/article/n/kiberatakikak-ugroza-informatsionnoy-bezopasnosti

5. Шифровальщик LockBit – что нужно знать // https://www.kaspersky.ru/resource center/threats/lockbit-ransomware

6.Kevin Mitnick. The Art of Invisibility: The World’s Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data, 2017, pages 320

7. Christopher Hadnagy. Social Engineering: The Science of Human Hacking, 2018, pages 322

8. Thomas Kranz. Making Sense of Cybersecurity, 2022, pages 288