ZAMONAVIY TELEKOMMUNIKATSIYADA KIBERXAVFSIZLIK

“Informatika va aloqa” kafedrasi katta o‘qituvchisi
podpolkovnik To‘rayev Baxtiyor Temirovich

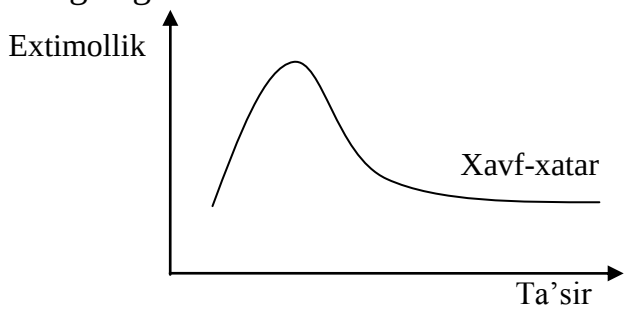
Samarqand oily harbiy avtomobil qo‘mondonlik muhandislik bilim yurti

Bugungi kunda Telekommunikasiyalar sohasi millionlab insonlar o‘rtasida o‘zaro ma’lumotlar almashinuvini amalga oshirishi mumkin bo‘lgan, keng tarmoqli xizmatlarni taqdim qilmoqda. Xizmatlarning rivojlanishi, telekommunikasiyalarda kiberxavflarning tez suratda o‘rtishiga sabab bo‘lmoqda. Bu o‘z navbatida kiberxavflarni qidirish, toppish va tahlil qilishning zamonaviy vositalarini, shuningdek yuqori malakali xodimlarni talab qiladi.

Telekommunikatsiya – barcha turdagi belgilarni, signallarni, xabarlarni, yozma matnlarni, rasmlarni, ovozlarni va videolarni yoki xar qanday turdagi ma’lumotlarni – sim, radio, optika yoki boshqa elektromagnitli tizimlar orqali uzatish va qabul qilish, ya’ni ma’lumotlar almashinuvi tushuniladi. Qachonki aloqa ishtirokchilari o‘rtasida, texnologiyalardan foydalangan holda ma’lumot almashinuvi amalga oshirilsa, **telekommunikatsiya** vujudga keladi. Telekommunikasiyalarda kiberxavfsizlik atamasini tushunish uchun biz, avvalo **kibertaxdid** atamasini bilishimiz kerak.

Kibertaxdid ma’lum bir xavf emas, balki bu texnologiyalar, vosita va usullar, hujum yo’nalishlari va boshqalar bilan farqlanadigan taxdidlar guruhidir. Biz bu taxdidlarni ikki xil o‘xshash xususiyatlaridan kelib chiqqan xolda ko‘rib chiqamiz: a) ularning barchasida katta ta’sir qilish potensiali mavjud b) qachonlardir ularni extimoldan uzoq deb xisoblashgan.

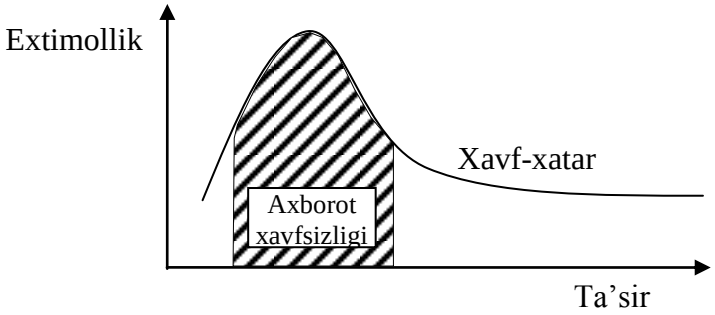
Biz buni tushunishimiz uchun, birinchi navbatda ana’naviy tahdidlarni ko‘z oldimizga keltiramiz. Tahdidni paydo bo‘lishi extimolligi va potensial ta’sir qilishi o‘rtasidagi bog‘liqlik 1-rasmda oddiy grafik tarzida ko‘rsatilgan. Grafikning o‘ng tamonidan tahdidlarning paydo bo‘lishi extimolligi pastligi bilan, ta’sir qilishi juda yuqori bo‘lgan guruhni kuzatishimiz mumkin.



1-rasm.

Ushbu grafikdan, tashkilotlar xavf-xatarlarni oldini olish va yo‘qotishga katta kuch va vositalarini yo‘naltiradigan, xavf-xatarlarni o‘z ichiga olgan hudud sifatida tahdidlar jamlangan o‘chiq zonasini belgilaymiz. Ba bu o‘choq zonasidagi

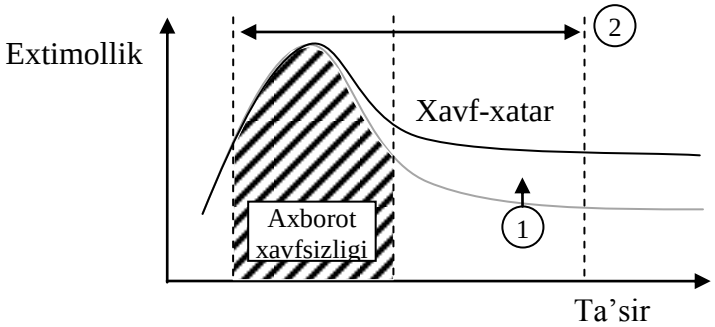
xavf-xatarlarni oldini olishga qaratilgan xarakatlarni **AXBOROT XAVFSIZLIGI** deb nomlaymiz. Bu xavf-xatarlar an'anaviy zararli dasturlarni (viruslar, troyanal, josus-dasturlar va x.k.), standart fishing-hujumlarni, xizmat ko'rsatishning inkor qilinishini, standart xakerlar xarakatlarini o'z ichiga oladi.



2-rasm.

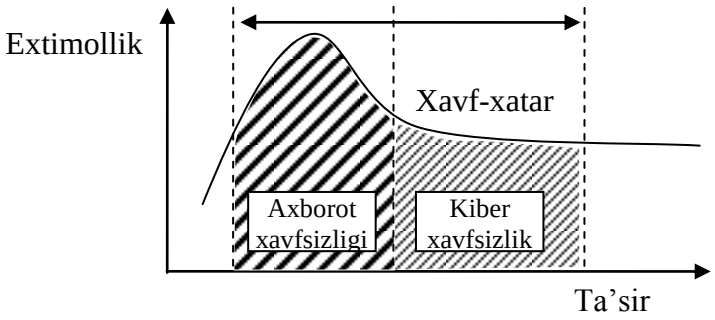
Albatta oxirgi paytlarda texnologiyalarning yuksalishi natijasida ba'zi narsalar o'zgardi, bu o'z navbatida tahdidlarning ko'rinishini, rivojlanishini va o'z shaklini, shuningdek ta'sir qilish doirasini o'zgartirishiga sabab bo'lmoqda. 3-rasmda xavf-xatarlarni juda yuqori suratlarda, shiddatli hujumlarini ortib borayotganini ko'rishimiz mumkin.

Xozirgi rivojlanayotgan zamonda, hujum qilishning o'ziga xos strategiyalari, usullari va ko'rinishlarining paydo bo'layotganligini, ularning ta'sir qilish doiralarining kengayishini, jinoyatchilarning motivasiyasi oshayotganligini, hamda xavf-xatarlarni aniqlashning takomillashgan vositalarining paydo bo'layotgaligi kabi xolatlarni ko'rish mumkin. Aytilgan gaplarni xisobga olgan xolda, biz bu yangi yuqori shakllangan xavf-xatar guruhlarining vujudga kelishi natijasida, axborot xavfsizligi sohasidagi ba'zi o'zgarishlarga iqror bo'lishimiz kerak. 3-rasmdan tahdidlarni paydo bo'lishi doirasini kengayishi va ta'sir qilish extimolligining ortib borayotganini ko'rishimiz mumkin.



3-rasm.

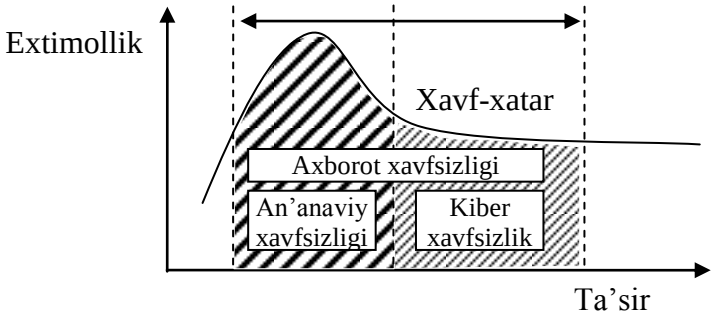
Bu yangi turdagi juda yuqori ta'sir qiluvchi xavf-xatarlar guruhi, ya'ni oddiy qilib **kibertahdid** deb nomlanadigan xatarlar hozirda bizning diqqatimizni o'ziga qaratmoqda. Bu kibertahdidlarni oldini olishga qaratilgan barcha chora tadbirlar va xarakatlarni biz **kiberxavfsizlik** deb atashimiz mumkin (4-rasm).



4-rasm.

Bu turdagi xavf-xatarlar turli turdagi g‘ayrioddiy xarakatlarni: aniq tashkilotlarni, maxsus mo‘ljallangan zararkunanda dasturlarni, o‘g‘irlangan sertifikatlarni ishlatishni, josuslar va axborotchilarni, qattiq diskdagi bo‘sh qolgan, zaiflashgan, e’tibordan chetta qolgan bo‘shliqlardan foydalanishni, xizmatlarni taqdim qiluvchiga hujum qilish va boshqa xarakatlarni o‘z ichiga oladi.

Bazilar axborot xavfsizligi va kiberxavfsizlini ikki turli soha sifatida tushunadi, ammo men kiberxavfsizlik axborot xavfsizligining bir bo‘lagi sifatida qaralishi tarafdoriman.



Xulosa sifatida shuni aytish mumkinki, **Kiberxavfsizlik bu** – hozirgi vaqtlargacha mavjud bo‘lmagan yoki ularni haqiqatdan uzoq deb xisoblangan, ular bizning e’tiborimizni olishi mumkin deb o‘ylamagan kibertahdidlarni oldini olishga yo‘naltirilgan qarashlarning yig‘indisidir.

Foydalanilgan adabiyotlar

1. B.To‘rayev, Elektron hujjat almashinuvini kriptografik himoyalash. Toshkent -2015.
2. Мельников В.Н., Клейменов С.А. Информационная безопасность и защиты информации. Москва 2008.
3. Телекоммуникации и сети: В.А.Галкин, Москва 2003.
4. https://twitter.com/BaMenny. A simple definition of cybersecurity.
5. http://www.linkedin.com/in/mennyb.