

KIBER XAFSIZLIK TUSHUNCHASI VA UNING VAZIFALARI

M.E. Sanayev Samarqand Iqtisodiyot va Servis Instituti, Assistant

Annotatsiya: Kiberxavfsizlik atamasi endi kirib kelgan atama emas , lekin ba'zilarimiz bu nimani anglatishini yoki nima uchun bunday deb atalishini bilmasligimiz mumkin. Shunday qilib, kiberxavfsizlikning ma'nosini to'liq tushunish uchun keling, so'zni ikki qismga ajratamiz: "kiber" va "xavfsizlik". " *Kiber* " atamasi odatda kompyuterlar, axborot texnologiyalari yoki internet bilan bog'liq narsalarni anglatadi. Buni yaxshiroq tushunish uchun uni *kompyuterlar* va *internetga* tegishli maxsus so'z sifatida tasavvur qiling.

Kalit so'z: kiberxavfsizlik, cisco tashkiloti, hujum, milliy xavfsizlik, konfidensiallik, risk, axborot xavfsizligi.

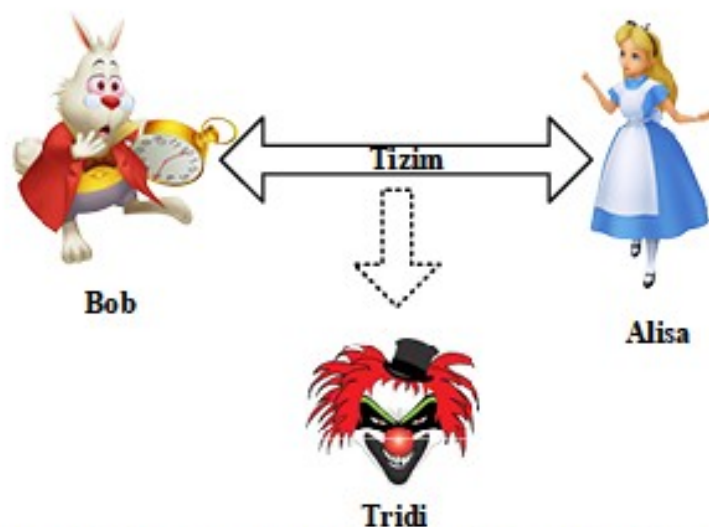
CONCEPT OF CYBER SECURITY AND ITS DUTIES

M.E.Sanayev Samarkand Institute of Economics and Service, Assistant

Abstract: The term cyber security is not a catchy term anymore, but some of us may not know what it means or why it is called that. So, to fully understand the meaning of cyber security, let's divide the word into two parts: "cyber" and "security". **Keyword:** cyber security, cisco organization, attack, national security, confidentiality, risk, information security.

Kirish: Xavfsizlik – bu xavf yoki tahdiddan xoli bo'lish va xavfsiz bo'lish holatini anglatadi. Shunday qilib, agar ikkita so'zni birlashtirsak, "kiberxavfsizlik" kompyuterlarni, tarmoqlarni va internetga ulangan har qanday qurilmani har qanday xavf yoki tahdiddan xavfsiz saqlashni anglatadi.

Nima uchun kiberxavfsizlik muhim? Kiberxavfsizlik bizning davrimizda,



1.1-rasm. Axborot xavfsizligining hayotdagi timsollari

ayniqsa sodir bo'layotgan barcha texnologik yutuqlar bilan chambarchas bog'langan. O'z resurslarini ularni xohlaydigan boshqa mamlakatlardan himoya qilish uchun hech qanday armiyasi yo'q mamlakatni tasavvur qiling. Mamlakat zaif bo'lishi shubhasiz, to'g'rimi? Siz shunday mamlakatda yashashni xohlaringiz? **Kiberxavfsizlik sohasiga kirish uchun dasturlashni bilish kerakmi?** Siz endigina kiberxavfsizlik sohasiga qadam qo'yayotganingizda dasturlash ilmini mukammal tarzda bilishingiz zarur emas. Ammo keyinchalik bu soha bilan astoydil shug'ullanishni boshlasangiz, sizga albatta dasturlashni o'rganish hamda bilish talab etiladi. Chunki shunday murakkab kiber jinoyatlar mavjudki, ularning oldini olish yoki qarshi turish uchun siz professional dasturchi bo'lishingiz shart.

Axborotni ishlash, uzatish va to'plashning zamonaviy usullarining rivojlanishi foydalanuvchilar axborotini yo'qolishi, buzilishi va oshkor etilishi bilan bog'liq tahdidlarning ortishiga olib kelmoqda. Shu sababli, kompyuter tizimlari va tarmoqlarida axborot xavfsizligini ta'minlash axborot texnologiyalari rivojining yetakchi yo'nalishlaridan biri hisoblanadi.

Axborot xavfsizligi hayotda mavjud timsollarga asoslanadi. Hayotda qonuniy faoliyat olib boruvchi shaxslar mavjud, ular 1.1-rasmda Alisa va Bob timsolida aks ettirilgan. Biroq, hayotda qonuniy faoliyat yurituvchi insonlarning faoliyatiga qiziquvchi, ularning ishlariga xalaqit beruvchi insonlar ham mavjud va ular 1.1-tasvirda Tridi timsolida tasvirlangan. Tridi timsoli barcha g'arazli niyatlarni amalga oshiruvchi shaxslarni ifodalaydi.

Darslikning keyingi bo‘limlarini yoritishda quyidagi hayotiy senariyni ko‘raylik. Ushbu hayotiy senariy Alisaning onlayn banki (AOB) deb ataladi. Bunga ko‘ra, Alisa onlayn bankning biznes faoliyatini amalga oshiradi. Mazkur senariyda Alisaning xavfsizlik muammosi nima?

Alisaning mijozi bo‘lgan Bobning xavfsizlik muammosichi? Alisa va Bobning xavfsizlik muammolari bir xilmi? Tridi nuqtai nazaridan qaraganda qanday xavfsizlik muammolari mavjud? Ushbu savollarga keyingi qismlarda javob berib o‘tiladi.

Kompyuter tizimlari va tarmoqlarida axborotni himoyalash va axborot xavfsizligiga tegishli bo‘lgan ayrim tushunchalar bilan tanishib chiqaylik.

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.

Tarmoq sohasida faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta’rif bergan: Kiberxavfsizlik – tizim,

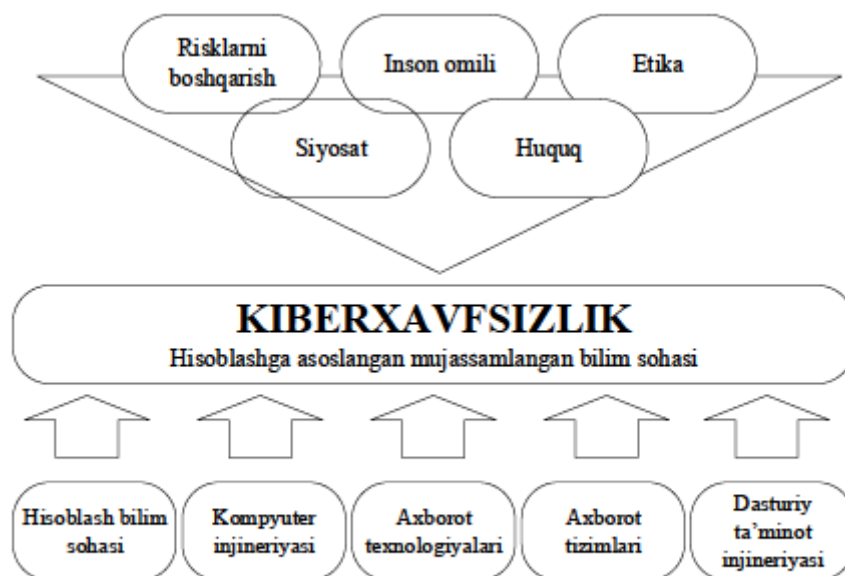
tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberhujumlar odatda maxfiy axborotni boshqarishni, almashtirishni yoki yo‘q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi. Hozirda samarali kiberxavfsizlik choralari amalga oshirish insonlarga qaraganda qurilmalar va ularning turlari sonining kattaligi va buzg‘unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda.

Kiberxavfsizlik bilim sohasining zaruriyati birinchi meynfreym kompyuterlar ishlab chiqarilganidan boshlab paydo bo‘la boshlagan.

Bunda mazkur qurilmalarning va ularning vazifalarining himoyasi uchun ko‘p sathli xavfsizlik choralari amalga oshirilgan. Milliy xavfsizlikni ta’minlash zaruriyatini oshib borishi kompleks va texnologik murakkab ishonchli xavfsizlik choralari paydo bo‘lishiga sabab bo‘ladi.

Hozirda axborot texnologiyalari sohasida faoliyat yuritayotgan har bir mutaxassisning kiberxavfsizlikning fundamental bilimlariga ega bo‘lishi talab

etiladi. Kiberxavfsizlik fani sohasining tuzilishini quyidagicha tasvirlash mumkin (1.2-rasm).



1.2-rasm. Kiberxavfsizlik fani sohasining tuzilishi

Kiberxavfsizlikni fundamental atamalarini aniqlashda turli yondashuvlar mavjud. Xususan, CSEC2017 JTF manbasida kiberxavfsizlikning quyidagi 6 ta atamasi keltirilgan: Konfidentsiallik – axborot yoki uni eltuvchisining shunday holatiki, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi.

Konfidentsiallik axborotni ruxsatsiz “o‘qish”dan himoyalash bilan shug‘ullanadi. AOB senariysida Bob uchun konfidentsiallik juda muhim.

Ya’ni, Bob o‘z balansida qancha pul borligini Tridining bilishini istamaydi. Shu sababli Bob uchun balans xususidagi ma’lumotlarning konfidentsialligini ta’minlash muhim hisoblanadi.

Yaxlitlik – axborotning buzilmagan ko‘rinishida (axborotning qandaydir qayd etilgan holatiga nisbatan o‘zgarmagan shaklda) mavjud bo‘lishi ifodalangan xususiyati. Yaxlitlik axborotni ruxsatsiz “yozish”dan (ya’ni, axborotni o‘zgartirishdan) himoyalash yoki kamida o‘zgartirilganligini aniqlash bilan shug‘ullanadi. AOB senariysida Alisaning banki qayd yozuvining yaxlitligini Trididan himoyalash shart.

Masalan, Bob o‘zining akkauntida balansning o‘zgarishidan yoki Alisa akkauntida balansning oshishidan himoyalashi shart.

Shu o‘rinda konfidentsiallik va yaxlitlik bir xil tushuncha emasligiga e’tibor berish kerak. Masalan, Tridi biror ma’lumotni o‘qiy olmagan taqdirda ham uni sezilmaydigan darajada o‘zgartirishi mumkin.

Foydalanuvchanlik – avtorizatsiyalangan mantiqiy obyekt so‘rovi bo‘yicha axborotning tayyorlik va foydalanuvchanlik holatida bo‘lishi xususiyati. Foydalanuvchanlik axborotni (yoki tizimni) ruxsatsiz “bajarmaslik”dan himoyalash bilan shug‘ullanadi. AOB senariysida AOB web saytidan Bobning foydalana olmasligi Alisaning banki va Bob uchun foydalanuvchanlik muammosi hisoblanadi. Sababi, mazkur holda Alisa pul o‘tkazmalaridan daromad ola olmaydi va Bob esa o‘z biznesini amalga oshira olmaydi. Foydalanuvchanlikni buzishga qaratilgan hujumlardan eng keng tarqalgani – xizmat ko‘rsatishdan voz kechishga undovchi hujum (Denial of service, DoS).

Risk – potensial foyda yoki zarar bo‘lib, umumiy holda har qanday vaziyatga biror bir hodisani yuzaga kelish ehtimoli qo‘shilganida risk paydo bo‘ladi. ISO “risk – bu noaniqlikning maqsadlarga ta’siri” sifatida ta’rif bergan.

Masalan, universitetga o‘qishga kirish jarayonini ko‘raylik.

Umumiy holda bu jarayonni o‘zi risk hisoblanmaydi. Faqatgina abituriyent hujjatlarini va kirish imtihonlarini topshirganida, u o‘qishga kirishi yoki kira olmasligi mumkin. Bu o‘z navbatida qabul qilinish yoki qabul qilinmaslik riskini yuzaga kelishiga sabab bo‘ladi.

Kiberxavfsizlikda yoki axborot xavfsizligida risklarga salbiy ko‘rinishda qaraladi.

Hujumchi kabi fikrlash – bo‘lishi mumkin bo‘lgan xavfni oldini olish maqsadida qonuniy foydalanuvchining hujumchi kabi fikrlash jarayoni.

Tizimli fikrlash – kafolatlangan amallarni ta’minlash uchun ijtimoiy va texnik cheklovlarning o‘zaro ta’sirini hisobga oladigan fikrlash jarayoni.

Bundan tashqari quyidagi tushunchalar ham kiberxavfsizlik sohasini o‘rganishda muhim hisoblanadi.

Axborot xavfsizligi – axborotning holati bo‘lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta’sir etishga yoki ruxsatsiz undan foydalanishga yo‘l qo‘yilmaydi. Yoki, axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidentsiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalaniish darajasi holati.

Axborotni himoyalash – axborot xavfsizligini ta’minlashga yo‘naltirilgan choralar kompleksi. Amalda axborotni himoyalash deganda ma’lumotlarni kiritish, saqlash, ishlash va uzatishda uning yaxlitligini, foydalanuvchanligini va agar, kerak bo‘lsa, axborot va resurslarning konfidentsialligini madadlash tushuniladi.

Aktiv - himoyalaniuvchi axborot yoki resurslar. Yoki, tashkilot uchun qimmatli barcha narsalar.

FOYDALANILGAN ADABIYOTLAR:

1. Eshquvvat o'g'li M.S, Zafar qizi Z.B AREAS OF APPLICATION OF ARTIFICIAL INTELLIGENCE ISSN: 2181-4027_SJIF: 4.995 Volume-27, Issue-2, February-2023. 61-64.
2. Eshquvvat o'g'li M.S, Naim o'g'li M. D, Xamrobek o'g'li N.N, DATA MININGDA CRISP-DM METODOLIGIYASI TASNIFI Частъ-11_ Том-1_ Декабрь-2023 43-46.
3. Файзиев Б.М., Бегматов Т.И., Санаев М.Э. ОБРАТНАЯ ЗАДАЧА ПО ОПРЕДЕЛЕНИЮ КИНЕТИЧЕСКОГО КОЭФФИЦИЕНТА В МОДЕЛИ ФИЛЬТРАЦ ИИ ТОМ TATU SF MA'RUZALAR TO'PLAMI 9 aprel 2022-yil 11-13.
4. Файзиев Б.М., Бегматов Т.И., Санаев М.Э ИДЕНТИФИКАЦИЯ КОЭФФИЦИЕНТА КИНЕТИКИ В МОДЕЛИ ФИЛЬТРАЦИИ СУСПЕНЗИИ В ПОРИСТОЙ СРЕДЕ 144-145.
5. Файзиев Б.М., Бегматов Т.И., Санаев М.Э. ИДЕНТИФИКАЦИЯ КОЭФФИЦИЕНТА КИНЕТИКИ В МОДЕЛИ ФИЛЬТРАЦИИ СУСПЕНЗИИ В ПОРИСТОЙ СРЕДЕ ХАЛҚАРО ИЛМИЙ-АМАЛИЙ АНЖУМАН МАТЕРИАЛЛАРИ 2022 йил, 11-12 май 360-361.
6. Eshquvvat o'g'li.M.S, Shodiyor o'g'li.Sh.J, Raxmonqul o'g'li.A.T, MA'LUMOTLARNI SINFLASHTIRISHDA BIRCH ALGORITMI АНАМИЯТИ Частъ-11_ Том-1_ Декабрь -2023 39-42.
7. Eshquvvat o'g'li.M.S, Elmurza o'g'li.Z.B, Anvar o'g'li.B.A DATA MININGDA SEMMA METODOLIGIYASI TASNIFI Частъ-11_ Том-1_ Декабрь -2023 35-38.
8. Naim o'g'li M. D., Abdishukur o'g'li S. A. THE NUMPY LIBRARY OF THE PYTHON PROGRAMMING LANGUAGE IS AN OPTIMAL SOLUTION FOR WORKING WITH ARRAYS //JOURNAL OF INNOVATIONS IN SCIENTIFIC AND EDUCATIONAL RESEARCH. – 2022. – Т. 2. – №. 13. – S. 195-197.
9. Naim o'g'li M. D., Baxtiyor o'g'li E. S. DATA SCIENCE METHODOLOGY IN LEARNING PROGRAMMING //JOURNAL OF INNOVATIONS IN SCIENTIFIC AND EDUCATIONAL RESEARCH. – 2022. – Т. 2. – №. 13. – S. 207-210.
10. Amanbayevna A. S., Naim o'g'li M. D. GEOMETRIC MODELING AND VISUALIZATION OF SELF-SIMILAR STRUCTURES BASED ON FRACTAL THEORY //JOURNAL OF INNOVATIONS IN SCIENTIFIC AND EDUCATIONAL RESEARCH. – 2022. – Т. 2. – №. 13. – S. 187-188.
11. Ernazarov, A. E. Features of defining goals and objectives in training. Society and innovations-Obshchestvo i innovatsii-Society and innovations.
12. Ergashevich, E. A. AJMR. AJMR.
13. Artikovich, A. S., Arulmoly, C., Kiruthika, A., Mody, P., Elopura, P., Kamsi, R., & Ergashevich, E. A. AJMR. AJMR.

14. Ergashevich, E. A. (2017). Implementation of Modern Pedagogical Technologies in the Process of Training Sessions. Asian Journal of Multidimensional Research (AJMR), 6(5), 37-47.
15. Ernazarov, A. E. Specific features of training. International Journal on Integrated Education, 3(5), 30-34.
16. ERGASHEVICH, E. A. (2020). Methods of Modern Organization and Implementation of Training. JournalNX, 6(05), 311-315.
17. Ergashevich, E. A. (2017). Clarification of the purpose and design of the training sessions. World Scientific News, (80), 101-115.
18. Ergashevich, E. A., & Zufar o'g'li, A. M. (2024). Zamonaviy Axborot Texnologiyalari Infratuzilmasining Tarkibiy qismlari. Journal of Innovation in Education and Social Research, 2(1), 154-157.
19. Ergashevich, E. A. (2024). OLIY TA'LIM MUASSASALARIDA FANLARNI O'QITISHDA O'QUV MAQSADLARI ANIQLASHNING AHAMIYATI. Miasto Przyszłości, 44, 196-199.
20. Ergashevich, E. A. (2024). Internet Texnologiyalaridan Ta'lim Jarayonida Samarali Foydalanish Yo'llari. Journal of Innovation in Education and Social Research, 2(1), 97-101.