

KIBERXAVFSIZLIK VA AXBOROT XAVFSIZLIGI*Anvar Isakovich Musaev**O'zbekiston Respublikasi Jamoat Xavfsizligi universiteti Axborot texnologiyalari kafedrasida dotsenti, texnika fanlari nomzodi(PhD)*

Annotatsiya. Ushbu maqolada hozirgi paytda juda keng tarqalib borayotgan tushuncha kiberxavfsizlik to'g'risida so'z yuritilgan. Ushbu tushuncha "axborot xavfsizligi" tushunchasi bilan birgalikda sinonim termin sifatida qo'llanilmoqda. Lekin ushbu terminlarni tushuntirishda klassik hisoblangan "axborot xavfsizligi" tushunchasi bilan tushuntirish qiyinchilik tug'diradi. Shu sababli kiberxavfsizlik terminiga boshqacha yo'nalishda paradigim sifatida qaralishi yoritilgan.

Kalit so'zlar: kibernetika, kiberxavfsizlik, xaker, kiberhujum, axborot xavfsizligi, tizim, ob'ekt, konfidentsiallik, butunlik.

Аннотация. В данной статье рассматривается понятие кибербезопасности, которое на данный момент очень распространено. Это понятие используется как синоним вместе с понятием «информационная безопасность». Однако эти термины трудно объяснить классическим понятием «информационная безопасность». Поэтому поясняется, что термин кибербезопасность следует рассматривать как парадигму отдельного направления.

Ключевые слова: кибернетика, кибербезопасность, хакер, кибератака, информационная безопасность, система, объект, конфиденциальность, целостность.

Annotation. This article discusses the concept of cyber security, which is very widespread at the moment. This concept is used as a synonymous term together with the concept of "information security". However, it is difficult to explain these terms with the classical concept of "information security". Therefore, it is explained that the term cyber security should be considered as a paradigm of a separate direction.

Key words: cybernetics, cyber security, hacker, cyber attack, information security, system, object, confidentiality, integrity.

Kirish. Barchamiz internet tarmog'idan kundalik faoliyatimizda foydalanishga o'rganib qolganmiz. Internet tarmog'idan kompyuter va mobil qurilmalar orqali axborot qidiramiz, o'qiyamiz va kerakli bo'lgan axborotlarni yuklab olamiz. Ushbu faoliyatimizni amalga oshirilishida Internetda mavjud bo'lgan servislar va content saqlovchi manbalardan foydalanamiz. Ushbu servislar va content manbalari ishonarli yoki ishonarli emasligi natijasida xavfsizligimizga tahdidlar paydo bo'ladi.

Internet tarmoq'idan foydalanish davomida xavfsizlik talablariga amal qilishga harakat qilamiz. Bu talablar eng asosiysi qurilmaga zararli content ya'ni virus bilan zararlangan content yuklashdan ehtiyot bo'lish bilan cheklanamiz. Bu xavfsizlikni axborot xavfsizligini ta'minlayapmiz deb hisoblaniladi. Shu bilan birgalikda hozirgi paytda ommaviy axborot vositalarida ko'proq kiberxavfsizlik,

kiberhujum va xaker terminlari ko'proq ommalashib bormoqda. Ushbu tushunchalar axborot xavfsizligi tushunchasi bilan birga qo'llanilmoqda. Bu esa ikki tushunchaning farqlashni talab qiladi.

Metodologiya. Ushbu terminlarning qo'llanilishining ilmiy asoslari ham turlicha hisoblanadi. Kiberxavfsizlik tushunchani o'rganar ekanmiz ushbu termin ikki qismdan iboratligini ko'ramiz, bular "kiber" va "xavfsizlik" terminlaridir.

Kiber so'zi kibernetika (qadimgi yunoncha Κυβερνητική-kemalarni boshqarish san'ati) so'zidan olingan bo'lib bu tushunchani fanga fransuz olimi, fizik, matematik Andre-Mari Amper 1834 yili kiritgan bo'lib, bunda kibernetikani samarali boshqaruv deb atagan. Ushbu tushunchani asosan davlat boshqaruv tizimi bilan bog'lagan bo'lib, bu boshqaruv natijasida ushbu kibernetik nuqtai nazaridan asoslangan davlat tomonidan o'z fuqarolari uchun turli xil yangiliklarni yaratish oson amalga osiriladi.

Shundan so'ng 1948 yil amerikalik matematik olim, kibernetika va sun'iy intellekt asoschisi Norbert Viner tomonidan kibernetika birinchi marta zamonaviy fan sifatida taklif qilingan. Bunda kibernetikaga qora quti va shunga o'xshash tizimlar, shuningdek tirik organizm, mashina va tashkilotlarda boshqaruv tizimi, aloqa va o'z-o'zini tashkillashtirishda yuzaga keluvchi teskari aloqani o'rganishni o'z ichiga oladi. Kibernetika biror tizimning (raqamli, mexanik yoki biologik) har qanday axborotni qayta ishlashi, ushbu axborot ta'siriga javob berishi natijasida o'zining ham tarkibi yoki vazifasiga o'zgarish kiritilishi, yoki o'zining boshqa ta'sir orqali o'zgartirilishi natijasida unga qo'yilgan ikkita vazifa bo'lgan axborotni qayta ishlashi va ushbu ta'sirga javob berish vazifasini yanada yaxshiroq bajarishiga e'tibor qaratadi.

Tizimning "Xavfsizligi" yoki "Xavfsizlik darajasi" so'zi bu har qanday tizimning kelajakda bor bo'lishiga, kelajakda yashab qolishiga to'sqinlik qiluvchi ta'sirlarning umumiy ko'rsatkichidir.

"Kiber" so'zi ixtiyoriy moddiy va jonli tizimda samarali boshqaruvni bildiradi. Har qanday tizimda boshqaruvning ushbu tizim uchun foydali yoki zararli natijaga olib kelishi bilan ushbu tizimning kelajakda bor bo'lishi, yashab qolishi yoki yo'q bo'lishini, ishdan chiqishini keltirib chiqaradi. Agar bu tizim o'z boshqaruvining tarkibiy qismlari bo'lgan alohida qismlarining oldiga qo'yilgan vazifalarni samarali, foydali yoki zararli ekanligini aniqlab, bu qismlarning ular oldiga qo'yilgan vazifalarni bajarish usullarini takomillashtirishi yoki keraksiz deb topilgan qismlarni olib tashlash bilan umumiy tizimning kelajakda bor bo'lishi, yashab qolishini ta'minlansa, demak bu tizimning umumiy xavfsizligi kiber tomonidan ta'minlangan, ya'ni kiberxavfsizligi ta'minlangan deyiladi.

Shu bilan birga tizim tushunchasini ham berib o'tishimiz kerak. **Tizim** so'zi lotincha "systēma", qadimgi yunoncha "σύστημα" "bir necha tarkibiy qismlardan (elementlardan) tashkil topgan bir butun to'plam; yig'indi" ma'nosini beradi. Tizim – bu o'zaro bog'liq va yagona maqsadga erishish uchun ma'lum qoidalar asosida o'zaro munosabatda bo'ladigan sodda elementlardan iborat to'plamning

yaxlit bir butun ob'ekt sifatida baholanishidir. To'plam tarkibidagi har bir sodda element ham o'z navbatida tizim bo'lishi mumkin.

Muhokama. Kiberxavfsizlik tushunchasi tizimning boshqaruv tizimiga nisbatan qo'llaniladi. Kiberxavfsizlik - bu fan bo'lib har qanday tizimning kelajakda bor bo'lishini ta'minlash maqsadida, uning umumiy boshqaruv qismiga o'zgartirish kiritishi mumkin bo'lgan foydali va zararli ta'sirlarni o'rganadi.

Xozirgi paytda kiberxavfsizlik raqamlashtirilgan tizimlar uchun muhim xususiyatga aylandi. Muhim xususiyatga aylanishiga o'z navbatida har qanday raqamlashtirilgan tizimlarga bo'lgan tarmoq orqali masofadan ta'sir o'tkazish usullarining ko'payib borayotganligi, xattoki bu zararli ta'sirlar tizimning ishdan chiqishiga, faoliyatining to'xtashiga (yo'q bo'lishiga), faoliyatining o'zgarishiga (modifikatsiya) yoki tizimning umuman boshqa maqsadga (redirect) yo'naltirilishiga sabab bo'layotganligi bilan izohlanadi.

Hozirgi vaqtga qadar adabiyotlarda axborot xavfsizligi tushunchasi keng muomalada va ilmiy sohada qo'llanilib kelmoqda. Axborot xavfsizligi 3 ta asosiy tamoyili bo'lib bular axborotning konfidentsialligini (Confidentiality), axborotning butunligini (Integrity) va axborotning foydalanishga doimiy tayyorligini (Availability) ta'minlashga qaratiladi. Axborot xavfsizligining asosiy ob'ekti **axborot** xisoblanadi.

Shundan xulosa qilib aytish mumkinki murakkab tizimlardan tashkil etilgan ob'ektlarining xavsizligin ta'minlashda axborot xafsiligi tushunchasidan foydalanish samarali hisoblanmaydi va qo'shimcha tushunchalar kiritishga asosiy ob'ekt sifatida axborotni emas balki tizimga nisbatan qo'llash ko'proq samarali bo'ladi. Shu sababli kiberxavfsizlik tushunchasi murakkab tizimlar uchun maqbul paradigma hisoblanadi. Kiberxavfsizlikning asosiy ob'ekti bular yaxlit tizimlar olinadi va ob'ektlarga nisbatan qo'llaniladi.

Xulosa. Shu sababli "axborot xavfsizligining ob'ekti - Axborot", "kiberxavfsizlikning ob'ekti - tizim" hisoblanadi. Axborot xavfsizligida paradigmasi orqali hozirgi paytdagi mavjud bo'lgan xavflar, jinoyatlarni kriptovalyutalar orqali moliyalashtirish, ijtimoiy muhandislik orqali axborotni egallash, "fishing-smishing-voicemishing-farming" orqali firibgarlik, bank kartalari bilan bog'liq xavflar, tizimning yoki shaxsning faoliyatini axborot xavfsizligiga bog'liq bo'lmagan holda to'xtatish, ya'ni "feyk" xabarlar tarqatish, "deepfake" axborotlarini tayyorlash va tarqatish, shaxs, jamiyat va davlat faoliyati uchun zararli axborotlarni ijtimoiy tarmoqlar orqali tarqatish, ijtimoiy tarmoqlarda maxfiy guruxlar tuzish, botnetlar orqali ob'ektlarni noqonuniy egallashi kabi xavflarni **to'laqonli tushuntib bera olmaydi**. Bu tushunchalarni **Kiberxavfsizlik** tushunchasi orqali tushuntirish samarali hisoblanadi.

Zamonaviy olamda raqamlashtirilgan tizimlarning jamiyat hayoti uchun muhimligi, ajralmas qismga aylanganligi bunday tizimlarning kiberxavfsizligini ta'minlashni oldingi o'ringa olib chiqadi, davlat va jamiyatning bu tizimlarning kiberxavfsizligini ta'minlashga resurslar sarf qilinishini majburiylikni keltirib chiqaradi. Sarf qilinuvchi resurslar moddiy, ilmiy va inson resurslariga bo'linadi.

Inson resurslari ta'lim darajasi bilan bog'liq bo'lib, ushbu sohada bilimli va salohiyatli insonlar, milliy kadrlarning faoliyat yuritishi, mehnat qilishi kerakligini bildiradi.

References

1. Wiener N . Cybernetics or Control and Communication in the Animal and the Machine. — New York: The Technology Press and John Wiley & Sons, Inc. — Paris: Hermann et Cie, 1948.
2. Kibermakonda sodir etilayotgan jinoyatlarga qarshi kurash: muammolar va yechimlar, Respublika ilmiy-amaliy konferensiya materiallari to'plami, (24 fevral 2022 yil), Toshkent: MALIK PRINT CO, 2022. -482 b.
3. Akbarov D.Ye., «Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi» Toshkent, "O'zbekiston markasi" nashriyoti, 2009 – 432 bet.
4. Akbarov D.Ye., Musayev A.I. Mavjud uzluksiz shifrlash algoritmlari asoslarini tadqiqi va ularning turkumlari, Toshkent, Axborotkommunikatsiyalar: tarmoqlar, texnologiyalar, yechimlar, "UNICON.UZ", 2009 y. 36-45 b.
5. Шукуров, М. Н. (2021). Курашчиларнинг организмига кластерланган махсус тайерлов техник машқларининг таъсири. Наманган Давлат Илмий Ахборотномаси, 366-369.
6. Latyshev, M., & Holovach, I. (2021). Improvement of the Technical and Tactical Preparation of Wrestlers with the Consideration of an Individual Combat Style. SportMont, (19), 23-28.
7. Tajibayev, S. (2020). Improvement Of Technical And Tactical Movements Of Wrestlers On The Basis Of Differential Approach, Taking Into Account The Morphological Characteristics. Scienceweb academic papers collection.
8. Khojaniyozov, B. I. (2021). Teaching wrestling as anational sport in higher educational universities. ACADEMICIA: An International Multidisciplinary Research Journal, 11(7), 259-266.
9. Холиқов, Б. Х. (2020). МАЛАКАЛИ КУРАШЧИЛАРНИ ТАЙЁРЛАШДА ТЕХНИК УСУЛЛАРНИ БАЖАРИШ СИФАТИНИНГ ЎРНИ. Fan-Sportga, (5), 41-43.
10. Mizamovich, P. R. (2022). Enhancing the Technical Preparation in Kurash. Texas Journal of Multidisciplinary Studies, 12, 54-55.
11. Mizamovich, P. R. (2022). Development of Physical Qualities of Kurash Wrestling Girls. Eurasian Research Bulletin, 12, 55-57.
12. Artikov, Z. S., & Khakimov, D. U. (2022). MECHANISMS FOR IMPROVING ATTRACTION INVESTMENT OPPORTUNITIES FOR THE DEVELOPMENT OF THE SAMARKAND REGION. Results of National Scientific Research, 1(6), 368-378.
13. Khidirovich, K. B. (2022, April). DEVELOPING TECHNICAL AND TACTICAL TRAINING OF SKILLED WRESTLERS. In E Conference Zone (pp. 193-195).

14. Холиқов, Б. Х. (2022). МАЛАКАЛИ КУРАШЧИЛАРНИНГ ЖИСМОНИЙ ВА ТЕХНИК-ТАКТИК ТАЙЁРГАРЛИК ВОСИТАЛАРИ НИСБАТИНИ ОПТИМАЛЛАШТИРИШ. Fan-Sportga, (1), 28-31.
15. Artikov, Z. S. (2022). BELBOG ‘LI KURASHCHILARDA MUVOFIQLIK VA SPORT MAHORATINI TAKOMILLASHTIRISH. Scientific progress, 3(1), 594-597.
16. Romanova, S., Maryanova, S., & Naumov, A. (2021, November). Analysis of the Key Financial Factors Affecting the Profitability of Enterprises in the Context of the Digitalization of the Economy. In Second Conference on Sustainable Development: Industrial Future of Territories (IFT 2021) (pp. 260-265). Atlantis Press.
17. Artikov, Z. S. (2022). 13-14 YOSHLI BELBOG’LI KURASHCHILARNING KUCH SIFATLARINI TARBIYALASH. Scientific progress, 3(1), 598-603.
18. Холиқов, Б. Х. (2021). КУРАШЧИЛАРНИНГ ТЕХНИК ТАЙЁРГАРЛИГИДА ЯНГИ ЗАМОНАВИЙ ТЕХНОЛОГИЯЛАРДАН ФОЙДАЛАНИШ УСЛУБИЯТИ. Fan-Sportga, (3), 23-24.