XXL ASRDA KO‘P UCHRAYOTGAN KIBRXO'JUMLAR VA ULARNING OLDINI OLISH HAQIDA

Salimova Zahro Ulug'bek qizi
Alfraganus unversiteti raqamli texnologiyalar fakulteti 1-kurs talabasi

Annotatsiya*: Ushbu maqola asosiy va birlamchi kiberxavfsizlik tushunchalari, kiberjinoyatchilik nima ekanligi, axborot va uning xavfsizligi, axborotning tashqi hujumlardan himoya qilish usullari, axborot xavfsizligini ta`minlashda kriptografik usullarning ahamiyati, ushbu sohada O`zbekiston Respublikasi davlat siyosati, huquqiy asoslari haqida.*

Аннотация*: В данной статье речь идет об основных и первичных понятиях кибербезопасности, что такое киберпреступность, информации и ее безопасности, методах защиты информации от внешних атак, значении криптографических методов в обеспечении информационной безопасности, государственной политике Республики Узбекистан в это поле, правовые основы.*

Abstract*: This article is about the basic and primary concepts of cyber security, what is cybercrime, information and its security, methods of protecting information from external attacks, the importance of cryptographic methods in ensuring information security, the state policy of the Republic of Uzbekistan in this field, legal bases.*

Kalit so`zlar*: kiberxavfsizlik, kibermakon, kiberjinoyatchilik, axborot xavfsizligi, axborot xavfsizligiga tahdid, axborotning kriptografik himoyasi.*

Ключевие слова*: кибербезопасность, киберпространство, киберпреступность, информационная безопасность, угроза информационной безопасности, криптографическая защита информации.*

Key words*: cyber security, cyberspace, cybercrime, information security, threat to information security, cryptographic protection of information.*

Ilm-fanning yangi texnologiyalari keng rivojlanib, biz insonlar kundalik hayotiga katta tezlikda kirib kelmoqda. Ijtimoiy hayotda ushbu texnologiyalar (uyali aloqa vositalari, shaxsiy kompyuterlar, turli gadjetlar va b.) dan keng ko`lamda, inson o`z mushkullarini yengil qilish maqsadida, iqtisodiy jihatdan manfaat topishda, kommunikatsiya qurilmalari orqali o`zaro olis masofadan turgan holda axborot almashishda samarali foydalanib kelmoqda. Shu bilan birgalikda, ushbu qurilmalardan foydalanish chog`ida ularni ham dasturiy, ham texnik tomondan ishonchli himoya qilish bugungi kunda juda muhim va dolzarb masaladir. Ana shunday muammolar ushbu soha mutaxassislarini ham nazariy, ham amaliy jihatdan bartaraf etishga qaratilgan dasturlar, rejalar, ilmiy maqolalar ishlab chiqishga va ularni amaliyotda qo`llashga undaydi va majbur etadi.

Kiberxavfsizlik hozirda yangi kirib kelgan tushunchalardan biri bo'lib, unga berilgan turlicha ta'riflar mavjud. Xususan, CSEC2017 Joint Task Force manbasida[12] 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. Tarmoqlar sohasida faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta'rif bergan: Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberxujumlar odatda maxfiy axborotni boshqarish, almashtirish yoki yo'q qilishni, foydalanuvchilardan pul undirishni, normal ish faoliyatini buzishni maqsad qiladi[13]. Hozirgi kunda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar soni va turlarining kattaligi va buzg'unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda. "Kiberxavfsizlik" atamasiga O'zbekiston Respublikasining Prezidenti tomonidan 2022-yil 15-aprelda tasdiqlangan *"Kiberxavfsizllik to`g`risida" gi O'RQ-764-son* qonunining 3-moddasida quyidagicha ta`rif berilgan:

"Kiberxavfsizlik — kibermakonda shaxs, jamiyat va davlat manfaatlarining tashqi va ichki tahdidlardan himoyalanganlik holati" dir[14]. "Kiberxavfsizlik to'g'risida" O'zbekiston Respublikasi Qonunining 3-moddasida ta'rif berilishicha, kibermakon — axborot texnologiyalari yordamida yaratilgan virtual muhit. Kibermakon kompyuter tarmoqlari orqali amalga oshiriladigan muloqot maydonini ifodalovchi voqelik sifatida 1990-yildan keng miqyosda rivojlanib, takomillashib kelmoqda. Kibermakon tushunchasini dastlab kanadalik yozuvchi Wilam Gibson 1982-yil o`zining "Burning Chrome" nomli hikoyasida yozadi. Ijtimoiy nuqtai nazardan kibermakon deganda kompyuter tarmog'i orqali bir-biri bilan bog'langan va bir vaqtning o'zida turli geografik nuqtada kesishuvchi har qanday mavjud kompyuterning grafik sifatidagi ma'lumotlariga o'ralashib qolgan kishilar jamoasi tushuniladi.

Kiberxavfsizlik tushunchasi bilan bir qatorda *"Kiberjinoyat"* atamasi ham mavjud. Xo`sh, Kiberjinoyat aslida nima? Ingliz tilidan "Cybercrime"[15] tushunchasi o`zbek tiliga "Kiberjinoyat" deya tarjima qilinib kirib kelgan.

Kiberjinoyatchilikning qay darajada insoniyatga tahdid solishi mumkinligini quyidagi statistika (2023-yil may) orqali ko`rishimiz mumkin.

Kiberjinoyatlar statistikasi sarlavhasi

- Bir yil ichida 1 milliardga yaqin elektron pochta xabarlari fosh qilindi, bu har 5 internet foydalanuvchisidan 1 tasiga salbiy ta'sir ko'rsatdi;

[12] S.R.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O`quv qo`llanma. – T.: "Aloqachi", 2020, 221 bet
[13] S.R.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O`quv qo`llanma. – T.: "Aloqachi", 2020, 221 bet
[14] *Lex.uz Qonunchilik ma'lumotlari milliy bazasi, 16.04.2022-y., 03/22/764/0313-son*
[15] Cybercrime *(eng.) – kiberjinoyat*

- 2022 yilda ma’lumotlar buzilishi (data breaches) korxonalarga o‘rtacha 4,35 million dollarga tushdi;
- 2022-yilning birinchi yarmida dunyo bo‘ylab 236,1 millionga yaqin to‘lov dasturlari hujumi sodir bo‘ldi;
- 2021-yilda har 2 amerikalik internet foydalanuvchisidan 1 nafarining akkauntlari buzilgan;
- Buyuk Britaniya korxonalarining 39 foizi 2022-yilda kiberhujumga uchraganini ma’lum qildi;
- Taxminan 10 ta AQSH tashkiloti kiberhujumlardan sug‘urta qilmaydi;
- 2022 yilning birinchi yarmida 53,35 million AQSh fuqarosi kiberjinoyatlardan jabrlangan;
- 2022-yilda kiberjinoyat Buyuk Britaniya korxonalariga o‘rtacha 4200 funt sterlingga tushgan;
- 2020-yilda zararli dastur (malware)[16] hujumlari 2019 yilga nisbatan 358 foizga oshdi;
- Yuridik va jismoniy shaxslar duch keladigan eng keng tarqalgan kiber tahdid bu fishingdir[17].

Ushbu ko`rsatkichlardan anglashimiz miumkinki, virtual dunyoda sodir bo`layotgan tahdidlarning salmog`i kamayish o`rniga yildan yilga sezilarli miqyosda ortib bormoqda. Yana shuni qoshimcha qilsam;

- ✓ 2025 yilga kelib, kiberhujumlar har yili dunyoga 7 trillion funt sterlingdan ko'proq zarar keltirishi bashorat qilinmoqda.;
- ✓ O'rtacha ma'lumotlarning buzilishi tashkilotlarga 2,8 million funt sterlingga tushadi;
- ✓ Korxonalar resurslari va fayllarining atigi 5 foizi kiberjinoyatchilardan yetarli darajada himoyalangan.

Kiberjinoyatlarning oshib borishida turli sabab va vaziyatlar mavjud. Inson ilmiy salohiyati kundan kunga oshib borishi, atrof-olam haqidagi, tibbiyot, fan va ta`lim tizimidagi kata yutuqlar, shu jumladam Internet global tarmog`idagi yuksak kashfiyotlar ularni raqamlashtirish natijasidagi ko`plab ma`lumotlar bazasining shakllanishi natijasida inson faoliyatining samaradorligi, vaqt tejalishi, sarmoyaning o`sishi ortib bormoqda. Albatta bu yaxshi, ammo ushbu bilimlardan noto`g`ri va o`z moddiy manfaatlai yo`lida foydalanish qayg`uli va oqibati esa ko`plab insonlarga katta talofatlar va nohushliklar olib kelishi achinarli hol.

So'nggi yillarda global kiberxavfsizlik landshaftida tahdidlar kuchaygan. Pandemiya tufayli kiberjinoyatchilar noto'g'ri taqsimlangan tarmoqlardan foydalanishdi, chunki

[16] Malware (eng.)- zararli dastur yoki "zararli dasturiy ta'minot" - bu tizimlar uchun zararli bo'lgan har qanday zararli dastur yoki kodni tavsiflovchi umumiy atama.

[17] Phishing (*ing.* “B*aliq ovi”*) – shaxsiy ma`lumotlar, bank rekvizitlari hamda bank karta ma`lumotlari, shu jumladan parollarni va boshqa shu kabi muhim ma`lumotlarni soxta habarlar yordamida egallashdan iborat “ov”.

korxonalar uzoqdan ish muhitiga o'tishdi. 2020-yilda zararli dastur hujumlari 2019-yilga nisbatan 358 foizga oshgan.

Fishing Internetda sodir etilgan jinoyatlarning eng keng tarqalgan shakli bo'lib qolmoqda. 2021-yilda 323 972 internet foydalanuvchisi fishing hujumlari qurboni bo‘lgan. Bu shuni anglatadiki, ma'lumotlar buzilgan foydalanuvchilarning yarmi fishing hujumiga uchragan. Pandemiya avj olgan davrda fishing hodisalari 220 foizga oshgan.

2021-yilda 1 milliardga yaqin elektron pochta xabarlari fosh etildi, bu har 5 internet foydalanuvchisidan 1 tasiga ta’sir ko‘rsatdi. Bu fishing hujumlarining davom etishini qisman tushuntirishi mumkin.

Ish joyidagi o'zgarishlar va yanada ilg'or kirib borish usullari kiber jinoyatchilarni qo'llab-quvvatlaganligi sababli, korxonalar uchun ma'lumotlar buzilishining narxi doimiy ravishda oshdi. 2022-yilda ma’lumotlar buzilishi korxonalarga o‘rtacha 4,35 million dollarga tushadi, bu 2021 yildagi 4,24 million dollardan ko‘p.

Axborot xavfsizligi deganda tabiiy yoki sun`iy xarakterdagi tasodifiy yoki qasddan qilingan ta`sirlardan axborot va uni qo`llab-quvvatlab turuvchi infratuzilmaning himoyalanganligi tushuniladi. Bunday ta`sirlar axborot munosabatlariga, jumladan, axborotdan foydalanuvchilar yoki ularning egalariga, axborotni muhofaza qiluvchi maxsus tashkilotlarning faoliyatiga jiddiy zarar yetkazadi. O`zbekiston Respublikasining 2022-yil 12-dekabrdagi

”Axborot erkinligi prinsiplari va kafolatlari to`g`risida” gi qonunida[18] Axborot borasidagi xavfsizlik — axborot sohasida shaxs, jamiyat va davlat manfaatlarining himoyalanganlik holati deb ta`kidlab o`tilgan. Ushbu himoyalanganlik holatining qay darajada ekanligi unga qiinayotgan turli xil ko`rinishdagi va usullardagi hujumlarni bartaraf etishi orqali o`lchanadi.

Axborot xavfsizligiga tahdid bu – axborot xavfsizligining buzilishiga imkon beruvchi yoki real xatarlarni vujudga keltiruvchi sharoit va omillarning to`plamidir. Axborotning qanchalik muhimligi uning yo`qotilgan yoki zarar yetkazilgandan keyin ijtimoiy, iqtisodiy, siyosiy va boshqa muhit va sohalarga qay darajada xavf tug`dirilishi bilan o`lchanadi. Birgina misol, sizning shaxsiy ma`lumotlaringiz fishing (Phishing) asosida o`g`irlansa bu oqibatida yetkazilgan yoki yetkazilishi mumkin bo`lgan zarar chegarasi faqatgina siz va atrofizdagi odamlar (oila a`zolar, do`stlar, yaqin tanishlar va boshqalar…) gagina bo`ladi. Agarda, ushbu axborot davlat darajasidagi muhim, davlat sirlari bilan bog`liq bolsa, ushbu axborot qanday tartibda va qay usullarda (DDOS va DOS hujumlar, smishing, vishing, fishing, kiberbulling…) zarar yetkazilganligidan qat`iy nazar oqibat anchayin katta va keng ko`lamli doirani qamrab oladi.

Axborotni himoya qilish tizimi ob’ektlarda axborot xavfsizligini ko’p sonli mumkin bo’lgan xavflardan himoya qilish uchun yaratiladi. U yoki bu xavfni blokirovkalash uchun himoya qilishning usullarini va vositalarini ma’lum bir to’plami ishlatiladi. Ularning ba’zi birlari axborotni bir vaqtning o’zida bir nechta xavflardan himoya qiladi. Usullarning ichida universal usullar ham mavjuddir, ular istalgan himoya qilish tizimi uchun asosiy hisoblanadi. Bu

[18] O‘zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2003-y., 1-son, 2-m:

axborotni himoya qilishning huquqiy usullaridir, bu ixtiyoriy vazifali himoya qilish tizimini rasmiy ravishda ko`rishni va ishlatishni asosi bo’lib xizmat qiladi. Tashkiliy usullar - ular odatda bir nechta xavflarni bartaraf (qaytarish) etish uchun ishlatiladi. Texnik usullar - ular tashkiliy va texnik tadbirlarga asoslangan holda ko’pchilik xavflardan axborotlarni himoya qiladi.

Axborotni himoya qilishni *huquqiy usullarida* huquqiy xarakterli masalalar ko’rib chiqiladi:

- kompyuter jinoyatchiligi uchun jazolash me’yorlarini ishlab chiqish;
- dasturlovchilarni mualliflik huquqlarini himoya qilish;
- jinoiy va fuqarolik qonunchiligini, hamda kompyuter jinoyatchiligi sohasida sud ishini mukammallashtirish;
- kompyuter tizimlari ishlab chiquvchilar ustidan jamoat nazorati masalalari;
- bu masalalar bo’yicha mos xalqaro shartnomalarni qabul qilish va h.k.

Himoya qilishni *texnik usullari* apparatli, dasturli va apparat-dasturliga bo’linadilar. Elektron hisoblash texnikasiga mo’ljallangan xavfsizliklarni ta’minlashni asosiy yo’nalishlari quyidagilardir:

- virusga qarshi himoya qilish;
- istalmagan elektromagnit va akustik maydon va nurlanishlar orqali ushlab olishni bartaraf etish;
- kriptografik usullar asosida xabarlarni yuqori tuzilishli berkligini ta’minlash.[19]

Axborot himoya qilishda kriptografiyaning o`rni juda muhim va dolzarb hisoblanadi. Kriptografik usullardan foydalangan holda shaxsiy ma`lumotlarni, barcha turdagi davlat manfaatiga daxldor raqamli axborotlarni va boshqa ko`plab axborotlarni kelasida yuz berishi mumkin bo`lgan hujumlardan, vaholanki, kiberjinoyatchilik olamidagi turli tahdidlardan himoya qilishimiz mumkin. Kriptografiya ma'lumotni o'zgartirish usullari bilan shug'ullanadi, bu dushmanga uni ushlangan xabarlardan ajratib olishga imkon bermaydi. Shu bilan birga, kiberjinoyatchi endi aloqa kanali orqali uzatiladigan shifr yordamida o'zgartirish natijasida himoyalangan ma'lumotni buzishdek qiyin vazifaga duch keladi. Shifrni ochish (расшифровка) - bu ochiq kodni olish jarayonida qo'llaniladigan shifrni yechish usulini aniq bilmasdan shifrlangan xabardan ma`lumot olishga bo`lgan urinish.

Kriptografik himoyalash usullari turli darajada mavjud. Shu jumladan, uning turlari ham bor. Quyidagi shifrlash usullaridan hozirda ko`plab rivojlangan mamlakatlar tomonidan qo`lanib kelmoqda. Bular:

Rossiyaning axborotni shifrlash standarti. Rosssiya Federatsiyasida hisoblash mashinalari, komplekslari va tarmoqlarida axborotni kriptografik o’zgartirish algoritmlariga davlat standarti (GOST 2814-89) joriy etilgan. Bu algoritmlar maxfiylik darajasi ixtiyoriy bo’lgan axborotni hech qanday cheklovsiz shifrlash imkonini beradi. Algoritmlar apparat va dasturiy usullarida amalga oshirilishi mumkin.

[19] https://elib.buxdu.uz/

AQSHning axborotni shifrlash standarti. AQSHda davlat standarti sifatida DES (Data Encryption Standart)[20] standarti ishlatilgan. Bu standart asosini tashkil etuvchi shifrlash algoritmi IBM firmasi tomonidan ishlab chiqilgan bo'lib, AQSH Milliy Xavfsizlik Agentligining mutaxasislari tomonidan tekshirilgandan so'ng davlat standarti maqomini olgan. DES standartidan nafaqat federal departamentlar, balki nodavlat tashkilotlar, nafaqat AQSHda, balki butun dunyoda foydalanib kelingan.

Xulosa qilib aytganda, bugungi raqamlashib borayotgan axborot tizimlari, telekommunikatsiya qurilmalari, ushbu sohadagi yuqori texnologiyali gadjetlar insoniyatning jismoniy va ma`naviy ehtiyojlarini qondirish maqsadida o`ylab topilib, ishlab chiqariladi ularning salohiyatidan kelib chiqib turli vazifalarni bajarishda qo`laniladi ammo ushbu raqamlashib borayotgan qurilma va dasturlar doim ham ezgu maqsadlarda foyadalanilmayotganligini yuqorida ta`kidlab o`tildi.

O`z manfaatlari yo`lida moddiy boylik o`zlashtiruvchi yoki g`arazli maqsadlarda turli shaxslar, xalqaro miqyosdagi davlatlar o`rtasida o`zaro nizolarni keltirib chiqarib ko`plab odamlarning o`limiga bir tomondan sabab bo`lmoqda. Har qanday axborot ma`lum bir doirada o`z darajasiga ega, shu jumladan, uning yo`qotilishi , o`g`irlanishi, zarar yetkazilishi ham ma`lum bir oqibatlarni olib keladi. Shuning uchun, ma`lumotlarni bunday hujumlar orqali egallashdan, yo`q qilinishdan, uning yordamida uchinchi shaxslar manfaatlariga noqonuniy daromad yoki hayotiga, sha`niga, sog`ligi va shaxsiy hayotiga tahdid solishidan muhofaza qilish zarur.

FOYDALANILGAN ADABIYOTLAR:

1. S.R.Ganiyev, A.A.Ganiyev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O`quv qo`llanma. – T.: "Aloqachi", 2020, 221 bet.

2. O'zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2003-y., 1-son, 2-m:

3. https://elib.buxdu.uz/

4. Введение в криптографию. Под редакцией В. В. Ященко. Издание четвертое, дополненное. Москва. Издательство МЦНМО. 2012 год

5. http:/Phishing.org/

6. *https://azkurs.org/*

7. William Gibson "Neuromancer"

8. https://aag-it.com/ The latest 2023 Cyber Crime Statistics (updated May 2023)

[20] DES (Data Encryption Standart) - eng. "Ma'lumotlarni shifrlash standarti"