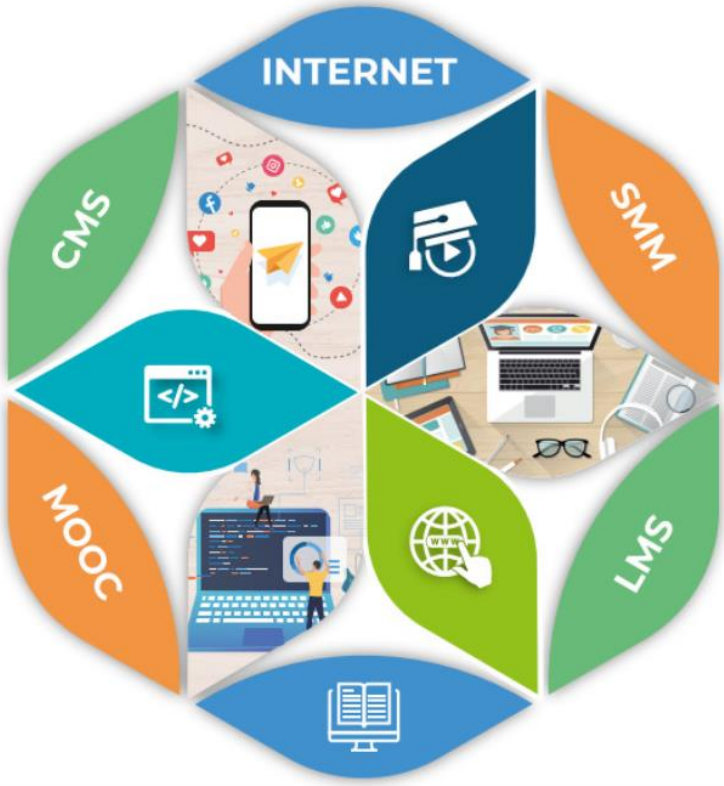
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI PEDAGOG KADRLARNI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISH TARMOQ MARKAZI



“TA’LIM TIZIMIDA KIBERXAVFSIZLIKNING MUAMMOLARI VA STRATEGIYASI”
moduli bo’yicha
O’QUV-USLUBIY MAJMUA

O‘ZBEKISTON RESPUBLIKASI OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

OLIY TA’LIM TIZIMI PEDAGOG VA RAHBAR KADRLARINI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISHNI TASHKIL ETISH BOSH ILMIY - METODIK MARKAZI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI HUZURIDAGI PEDAGOG KADRLARNI QAYTA TAYYORLASH VA ULARNING MALAKASINI OSHIRISH TARMOQ MARKAZI

“AXBOROT XAVFSIZLIGI” yo‘nalishi

“TA’LIM TIZIMIDA KIBERXAVFSIZLIKNING MUAMMOLARI VA STRATEGIYASI”

MODULI BO‘YICHA

O‘ Q U V –U S L U B I Y M A J M U A

Toshkent – 2024

Modulning o‘quv-uslubiy majmuasi Oliy ta’lim, fan va innovatsiyalar vazirligining 2023 yil 25 avgustdagi №391-sonli buyrug‘i bilan tasdiqlangan o‘quv dasturi va o‘quv rejasiga muvofiq ishlab chiqilgan.

Tuzuvchilar:	**Sh.R.G‘ulomov–** Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik fakulteti dekani, Ph.D., dotsent.
	D.Sh.Usmanbayev – Muhammad al-Xorazmiy nomidagi TATU Axborot xavfsizligi kafedrasi assistenti.
	Sh.B.Sayfullayev - Muhammad al-Xorazmiy nomidagi TATU Axborot xavfsizligi kafedrasi assistenti.
Taqrizchilar:	**O.M.Allanov –** Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik va Kriminalistika kafedra mudiri, Ph.D.
	N.B.Nasrullayev - Muhammad al-Xorazmiy nomidagi TATU Nurafshon filiali direktori, dotsent.

O‘quv-uslubiy majmua O‘quv dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining qarori bilan tasdiqqa tavsiya qilingan (2023-yil 26 maydagi 7 (729)- sonli bayonnoma)

MUNDARIJA

I-BO‘LIM
ISHCHI DASTUR

I. ISHCHI DASTUR

KIRISH

O‘zbekiston Respublikasi Prezidentining 2017-yil 7 fevraldagi PF-4947-sonli Farmoni bilan tasdiqlangan “2017-2021-yillarda O‘zbekiston Respublikasini rivojlantirishning beshta ustuvor yo‘nalishi bo‘yicha Harakatlar Strategiyasi”da milliy kadrlarning raqobatbardoshligi va umumjahon amaliyotiga asoslangan oliy ta’lim milliy tizimining sifati oshishiga, Bolonya jarayoni ishtirokchi mamlakatlari diplomlarini o‘zaro tan olishga, o‘qituvchi va talabalar bilan almashuv dasturlarini amalga oshirishga ko‘maklashuvchi 1999 yil 19-iyundagi Bolonya deklaratsiyasiga qo‘shilish masalasini ko‘rib chiqish belgilab qo‘yilgan.

Ma’lumki davlatimiz rahbari Shavkat Mirziyoyev tomonidan 2020 yilni “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili” deb e’lon qildi. 2020 yil 2 martda esa Prezidentimizning “2017–2021 yillarda O’zbekiston Respublikasini rivojlantirishning beshta ustuvor yo’nalishi bo’yicha Harakatlar strategiyasini “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili”da amalga oshirishga oid davlat dasturi to’g’risida”gi Farmoni bilan “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili” Davlat dasturi qabul qilindi. Davlat dasturi beshta asosiy yo’nalishlardan iborat bo’lib, dasturning beshinchi yo’nalishida 2020-2023 yillarga mo’ljallangan Kiberxavfsizlikka doir milliy strategiya hamda “Kiberxavfsizlik to’g’risida”gi qonun loyihasini ishlab chiqish belgilanib qo’yilgan.

Prezidentimizning 2018 yil 19 fevraldagi “Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to’g’risida”gi Farmoni Hukumatimiz tomonidan raqamli iqtisodiyotni rivojlantirish bo’yicha muhim chora-tadbirlar ishlab chiqilishiga va hayotga tatbiq etilishiga asos bo’ldi. Raqamli ma’lumotlarni boshqarishda axborot xavfsizligini ta’minlash muhim omil sanaladi. Bunda asosiy e’tibor raqamli ma’lumotlarga ruxsatsiz kirish, ularni axborot vositachilaridan himoya qilgan holda xavfsizligini ta’minlash va axborotlar uzatishning soddaligini ta’minlashga qaratilishi lozim.

Respublikamizda xam axborot texnologiyalarining rivojlanishi bilan bir qatorda xo‘jalik va davlat boshqaruvi organlarida axboorot xavfsizligini, xususan, kompyuter bilan bog‘liq bo‘lgan xavfsizlik muammolarini bartaraf etish yo‘nalishiga alohida e‘tibor qaratilmoqda. 2017-2021 yillarda O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasida vazifalar belgilab olindi, shular qatorida «...axborot xavfsizligini ta‘minlash va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o‘z vaqtida va munosib qarshilik ko‘rsatish» va kiber jinoyatchilikni fosh etish masalalariga alohida e‘tibor qaratilgan. Bundan tashqari, “Ilm, ma‘rifat va raqamli iqtisodiyotni rivojlantirish yili” da amalga oshirishga oid Davlat dasturi to‘g‘risidagi O‘zbekiston Prezidenti Farmonida “2020 yil 1 sentyabrga qadar kiberxavfsizlikka doir milliy strategiya va qonun loyihasi ishlab chiqish” vazifalari belgilangan.

Ushbu dasturda ta’lim tizimida kiberxavfsizlik muammolari va strategiyasi aspektlarini huquqiy, tashkiliy va texnik sathlari, ta’lim tizimidagi kiberxavfsizlik

sohasida xalqaro, milliy va idoraviy me’yoriy-huquqiy baza, ta’lim tizimida kiberxavfsizlik tuzilishi va strukturasi, strategiya, kiberxavfsizlik siyosati va uni amalga oshirish, ta’lim tizimidagi kiberxavfsizlik sohasida axborotni himoyalashda zarur bo‘ladigan axborot xavfsizligini baholash mezonlari, axborot xavfsizligiga bo‘ladigan tahdidlar, hujumlar darajasini aniqlash, axborot xavfsizligini tashkil etuvchilari va ularning ahamiyati bayon etilgan.

Modulning maqsadi va vazifalari

Modulning maqsadi: qayta tayyorlash va malaka oshirish kursi tinglovchilarini ta’lim tizimida kiberxavfsizlikning muammolari va strategiyasi haqidagi bilimlarini takomillashtirish, oliy ta’lim muassasalarida kiberxavfsizlikni ta’minlash aspektlarini huquqiy, tashkiliy va texnik sathlarini tashkil etish, normativ hujjatlarni qo‘llashda kiberxavfsizlik muammolarni aniqlash, tahlil etish, shuningdek, ularda oliy ta’limda kiberxavfsizlik muammolari va strategiyasi to‘g‘risida ko‘nikma va malakalarini tarkib toptirish.

Modulning vazifalari:

- ta’lim tizimida kiberxavfsizlikni ta’minlash sohasidagi asosiy bilimlarni shakllantirish;
- ta’lim tizimidagi kiberxavfsizlik muammolari va strategiyasi haqidagi bilimlarni shakllantirish;
- ta’lim tizimidagi kiberxavfsizlik muammolari va strategiyasining bazaviy tashkil etuvchilari to‘g’risida bilimlarni shakllantirish.

Modul bo‘yicha tinglovchilarning bilim, ko‘nikma, malaka va kompetensiyalariga qo‘yiladigan talablar

“Ta’lim tizimida kiberxavfsizlikning muammolari va strategiyasi” modulini o‘zlashtirish jarayonida amalga oshiriladigan masalalar doirasida:

Tinglovchi:

- ta’lim tizimida kiberxavfsizlikni ta’minlash sohasida foydalaniladigan kompyuter texnologiyalarini obyektlari;
- ta’lim tizimidagi kiberxavfsizlik muammolari va strategiyasi xususiyatlari to‘girisida nazariy ma’lumotlar;
- ta’lim tizimidagi kiberxavfsizlik muammolari va strategiyasining bazaviy tashkil etuvchilari to‘g’risida bilimlar;
- ta’lim tizimida kiberxavfsizlik sohasidagi kompyuter-texnik ekspertiza obyektlari;
- Davlat ta’lim standartlari, tegishli ta’lim (mutaxassislik) yo‘nalishlari bo‘yicha davlat ta’lim standarti, o‘quv rejalar va fan dasturlari va ularga qo‘yiladigan talablarni, o‘quv rejalari va o‘quv fanlari dasturlarini takomillashtirish tamoyillarini, o‘quv yuklamalarini rejalashtirish va ularning bajarilishini nazorat qilish metodlari haqidagi **bilimlarga ega bo‘lishi**;

- ta;lim tizimida kiberxavfsizlikni ta’minlash bilan bog’liq vazifalarni shakllantirish, maqsadlarni qo‘yish;

- ta’lim tizimida kiberxavfsizlikni ta’minlash tizimlarini rivojlanish tendensiyalarini tahlillash;

- qo‘yilgan vazifalar yechish bo‘yicha kiberxavfsizlik to‘g‘risida bilimlarni qo‘llash;

- O‘zbekiston Respublikasi Prezidentining Oliy ta’lim tizimiga oid qabul qilgan farmonlari, qarorlari va farmoyishlari hamda O‘zbekiston Respublikasi Vazirlar Mahkamasining Oliy ta’lim tizimiga tegishli normativ-huquqiy hujjatlari asosida ta’lim-tarbiya jarayonlarini tashkillashtirish;

- O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligining ta’lim-tarbiya jarayonini tashkil etishga oid normativ-huquqiy hujjatlari asosida Davlat ta’lim standartlari, tegishli ta’lim (mutaxassislik) yo‘nalishlari bo‘yicha davlat ta’lim standarti, o‘quv rejalar va fan dasturlarini takomillashtirish;

- o‘quv yuklamalarni rejalashtirish va ularning bajarilishini nazorat qilish **ko‘nikma va malakalarini egallashi;**

- ta;lim tizimida kiberxavfsizlikni ta’minlash sohasida tahlil o‘tkazish usullari;

- ta;lim tizimida kiberxavfsizlik sohasida qo‘llaniladigan zamonaviy texnologiyalar to‘g‘risida bilimlar;

- Davlat ta’lim standartlari, o‘quv rejalar va fan dasturlar asosida fanning ishchi dasturini ishlab chiqish **kompetensiyalarni egallashi lozim.**

Modulni tashkil etish va o‘tkazish bo‘yicha tavsiyalar

“Ta’lim tizimida kiberxavfsizlikning muammolari va strategiyasi” moduli ma’ruza va amaliy mashg‘ulotlar shaklida olib boriladi.

Kursni o‘qitish jarayonida ta’limning zamonaviy metodlari, axborot-kommunikatsiya texnologiyalari qo‘llanilishi, shuningdek, ma’ruza darslarida zamonaviy kompyuter texnologiyalari yordamida taqdimot va elektron-didaktik texnologiyalarni;

- o‘tkaziladigan amaliy mashg‘ulotlarda texnik vositalardan, blis-so‘rovlar, aqliy hujum, guruhli fikrlash, kichik guruhlar bilan ishlash, va boshqa interfaol ta’lim metodlarini qo‘llash nazarda tutiladi.

Modulning o‘quv rejadagi boshqa modullar bilan bog‘liqligi va uzviyligi

“Ta’lim tizimida kiberxavfsizlikning muammolari va strategiyasi” moduli bo‘yicha mashg‘ulotlar “Kiberxavfsizlik asoslari”, “Axborotni xavf-xatarlarini boshqarishga kirish” kabi modullar bilan uzviy aloqadorlikda olib boriladi.

Modulning oliy ta’limdagi o‘rni

Modulni o‘zlashtirish orqali tinglovchilar ta’lim tizimida mavjud kiberxavfsizlik bilan bog’liq muammolari va tizimlarni qo‘llash bilan doir kasbiy kompetentlikka ega bo‘ladilar.

MODUL BO‘YICHA SOATLAR TAQSIMOTI

№	Modul mavzulari	Auditoriya o‘quv yuklamasi				
		Jami	Nazariy	Amaliy mashg‘ulot	Ko‘chma mashg‘ulot	Mustaqil ta’lim
1.	**Kiberxavfsizlikka kirish** Kiberxavfsizlikning tarixi va uning jamiyatga ta’siri. Kiberxavfsizlikning asosiy tushunchalari: kiberxavfsizlik, risk, risklarni boshqarish, kiberqonun, kiberetika, kiberjinoyat. Konfidensiallik, yaxlitlik va foydalanuvchanlik tushunchalari. Kiberxavfsizlikda risklarni boshqarish konsepsiyasi. Tashkilotga nisbatan kiberxavfsizlik tahdidlari. Xavfsizlikni ta’minlashning turli usullari: fizik, texnologik va tashkiliy.	2	2			
2.	**Kibertahdidlar va zaifliklar** Kibertahdidlar, hujumlar, zaifliklar va uning xususiyatlari. Kibertahdid turlari. Zararli hujum manbalari. Zararli dasturlarning turlari. Hujum turlari: simsiz, dasturiy, ijtimoiy injineriya, buferni to‘lib toshishi.	2	2			
3.	**Kompyuter va tarmoq arxitekturasi** Tarmoqqa oid asosiy tushunchalar, tarmoq turlari va tarmoq topologiyalari. Simsiz va simli tarmoq turlari. Tarmoq xavfsizligiga oid tushunchalar: IDS, IPS, Router, Firewall, antivirus dasturiy vositalari. Tarmoqlararo ekran va uning turlari, ularni sozlash. VPN, uning vazifasi va uni amalga oshirish tartibi. Hujumlarni aniqlash va bartaraf etish vositalari.	2	2			
4.	**Ijtimoiy injineriya** Ijtimoiy injineriya va uni hozirgi kiberjinoyatchilikdagi ahamiyati. Soxta veb saytlar, fishing elektron xabarlar.	2	2			

	Fishing va uning ko‘rinishlari. Ijtimoiy injineriyaga real misollar. Ijtimoiy injineriyadan himoyalanish usullari.					
5.	**Simsiz tarmoq vositalarini sozlash** Turli simsiz tarmoq vositalari va ularning vazifasi. Tarmoq vositalarini (WI-FI router) xavfsizlik sozlanmalarini sozlash.	10		6	4	
6.	**Axborot xavfsizligi risk modellar** Axborot xavfsizligida risk tushunchasini aniqlash va risk modeli	6		4	2	
	Jami:	**22**	**8**	**10**	**6**	

NAZARIY MASHG‘ULOTLAR MAZMUNI

1-MAVZU: KIBERXAVFSIZLIKKA KIRISH (2 soat)

Kiberxavfsizlikning tarixi va uning jamiyatga ta’siri. Kiberxavfsizlikning asosiy tushunchalari: kiberxavfsizlik, risk, risklarni boshqarish, kiberqonun, kiberetika, kiberjinoyat. Konfidensiallik, yaxlitlik va foydalanuvchanlik tushunchalari. Kiberxavfsizlikda risklarni boshqarish konsepsiyasi. Tashkilotga nisbatan kiberxavfsizlik tahdidlari. Xavfsizlikni ta’minlashning turli usullari: fizik, texnologik va tashkiliy.

2-MAVZU: KIBERTAHDIDLAR VA ZAIFLIKLAR (2 soat)

Kibertahdidlar, hujumlar, zaifliklar va uning xususiyatlari. Kibertahdid turlari. Zararli hujum manbalari. Zararli dasturlarning turlari. Hujum turlari: simsiz, dasturiy, ijtimoiy injineriya, buferni to‘lib toshishi.

3-MAVZU: KOMPYUTER VA TARMOQ ARXITEKTURASI (2 soat)

Tarmoqqa oid asosiy tushunchalar, tarmoq turlari va tarmoq topologiyalari. Simsiz va simli tarmoq turlari.Tarmoq xavfsizligiga oid tushunchalar: IDS, IPS, Router, Firewall, antivirus dasturiy vositalari. Tarmoqlararo ekran va uning turlari, ularni sozlash. VPN, uning vazifasi va uni amalga oshirish tartibi. Hujumlarni aniqlash va bartaraf etish vositalari.

4-MAVZU: IJTIMOIY INJINERIYA (2 soat)

Ijtimoiy injineriya va uni hozirgi kiberjinoyatchilikdagi ahamiyati. Soxta veb saytlar, fishing elektron xabarlar. Fishing va uning ko‘rinishlari. Ijtimoiy injineriyaga real misollar. Ijtimoiy injineriyadan himoyalanish usullari.

AMALIY MASHG‘ULOTLAR MAZMUNI

1-MAVZU: SIMSIZ TARMOQ VOSITALARINI SOZLASH (6 soat)

Turli simsiz tarmoq vositalari va ularning vazifasi. Tarmoq vositalarini (WI-FI router) xavfsizlik sozlanmalarini sozlash.

2-AMALIY MASHG‘ULOT
MAVZU: AXBOROT XAVFSIZLIGIDA RISK MODELLARI (4 soat)

Axborot xavfsizligida risk tushunchasini aniqlash va risk modellari

O‘QITISH SHAKLLARI

Mazkur modul bo‘yicha quyidagi o‘qitish shakllaridan foydalaniladi:

- ma’ruzalar, amaliy mashg‘ulotlar (ma’lumotlar va texnologiyalarni anglab olish, motivatsiyani rivojlantirish, nazariy bilimlarni mustahkamlash);
- davra suhbatlari (ko‘rilayotgan loyiha yechimlari bo‘yicha taklif berish qobiliyatini rivojlantirish, eshitish, idrok qilish va mantiqiy xulosalar chiqarish);
- bahs va munozaralar (loyihalar yechimi bo‘yicha dalillar va asosli argumentlarni taqdim qilish, eshitish va muammolar yechimini topish qobiliyatini rivojlantirish).

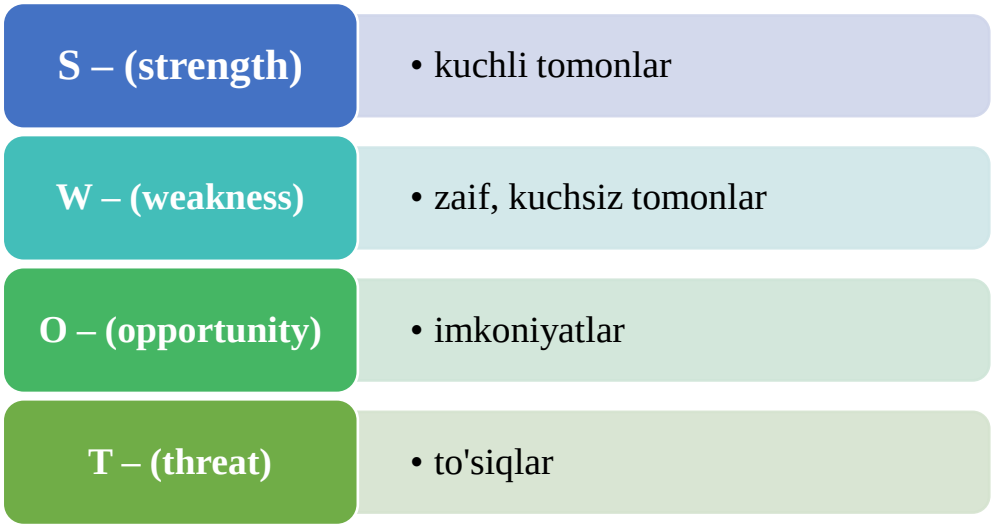
II-BO‘LIM

MODULNI O‘QITISHDA FOYDALANILADIGAN INTERFAOL TA’LIM METODLARI

II. FANNI O‘QITISHDA FOYDALANILADIGAN INTREFAOL TA’LIM METODLARI

“SWOT-tahlil” metodi.

Metodning maqsadi: mavjud nazariy bilimlar va amaliy tajribalarni tahlil qilish, taqqoslash orqali muammoni hal etish yo‘llarni topishga, bilimlarni mustahkamlash, takrorlash, baholashga, mustaqil, tanqidiy fikrlashni, nostandart tafakkurni shakllantirishga xizmat qiladi.



Namuna: Aloqa kanallari uchun SWOT tahlilini ushbu jadvalda tushiring.

S	Tarmoqlararo ekran	Korporativ tarmoqlarni masofadan buladigan tarmoq hujumlaridan himoyalash va tarmoq trafigini nazoratlash imkonini beradi.
W	Tarmoqlararo ekran	Faqat ichki tarmoqni internetdan bo‘ladigan hujumlardan himoyalash imkonini beradi. Ammo ichki tarmoqni o‘zidan bo‘ladigan hujumlardan himoyalash imkonini bermaydi.
O	Tarmoqlararo ekran	Tarmoq paketlarini to‘liq nazoratlash imkonini beradi.
T	To‘siqlar	SSL protokoli paketlarini tahlillash imkonini yo‘qligi.

“Xulosalash” (Rezyume, Veyer) metodi

Metodning maqsadi: Bu metod murakkab, ko‘ptarmoqli, mumkin qadar, muammoli xarakteridagi mavzularni o‘rganishga qaratilgan. Metodning mohiyati

shundan iboratki, bunda mavzuning turli tarmoqlari bo‘yicha bir xil axborot beriladi va ayni paytda, ularning har biri alohida aspektlarda muhokama etiladi. Masalan, muammo ijobiy va salbiy tomonlari, afzallik, fazilat va kamchiliklari, foyda va zararlari bo‘yicha o‘rganiladi. Bu interfaol metod tanqidiy, tahliliy, aniq mantiqiy fikrlashni muvaffaqiyatli rivojlantirishga hamda o‘quvchilarning mustaqil g‘oyalari, fikrlarini yozma va og‘zaki shaklda tizimli bayon etish, himoya qilishga imkoniyat yaratadi. “Xulosalash” metodidan ma’ruza mashg‘ulotlarida individual va juftliklardagi ish shaklida, amaliy va seminar mashg‘ulotlarida kichik guruhlardagi ish shaklida mavzu yuzasidan bilimlarni mustahkamlash, tahlili qilish va taqqoslash maqsadida foydalanish mumkin.

Metodni amalga oshirish tartibi:

5-6 kishidan iborat kichik guruhlarga trener-o‘qituvchi ishtirokchilarni ajratiladi;

trening maqsadi, har bir guruhga umumiy muammoni tahlil qilinishi zarur bo‘lgan qismlari tushirilgan tarqatma materiallarni tarqatadi;

har bir guruh o‘ziga berilgan muammoni atroflicha tahlil qilib, o‘z mulohazalarini tavsiya etilayotgan sxema bo‘yicha tarqatmaga yozma bayon qiladi;

navbatdagi bosqichda barcha guruhlar o‘z taqdimotlarini o‘tkazadilar. Shundan so‘ng, trener tomonidan tahlillar umumlashtiriladi va mavzu yakunlanadi.

“Keys-stadi” metodi

“Keys-stadi” - inglizcha so‘z bo‘lib, (“case” – aniq vaziyat, hodisa, “study” – o‘rganmoq, tahlil qilmoq) aniq vaziyatlarni o‘rganish, tahlil qilish asosida o‘qitishni amalga oshirishga qaratilgan metod hisoblanadi. Mazkur metod dastlab 1921 yil Garvard universitetida amaliy vaziyatlardan iqtisodiy boshqaruv fanlarini o‘rganishda foydalanish tartibida qo‘llanilgan.

Keysda ochiq axborotlardan yoki aniq voqea-hodisadan vaziyat sifatida

tahlil uchun foydalanish mumkin. Keys harakatlari o‘z ichiga quyidagilarni qamrab oladi: Kim (Who), Qachon (When), Qaerda (Where), Nima uchun (Why), Qanday/ Qanaqa (How), Nima-natija (What).

“Keys metodi” ni amalga oshirish bosqichlari

Ish bosqichlari	Faoliyat shakli va mazmuni
1-bosqich: Keys va uning axborot ta’minoti bilan tanishtirish	yakka tartibdagi audio-vizual ish; keys bilan tanishish(matnli, audio yoki media shaklda); axborotni umumlashtirish; axborot tahlili; muammolarni aniqlash
2-bosqich: Keysni aniqlashtirish va o‘quv topshirig‘ni belgilash	individual va guruhda ishlash; muammolarni dolzarblik ierarxiyasini aniqlash; asosiy muammoli vaziyatni belgilash
3-bosqich: Keysdagi asosiy muammoni tahlil etish orqali o‘quv topshirig‘ining yechimini izlash, hal etish yo‘llarini ishlab chiqish	individual va guruhda ishlash; muqobil yechim yo‘llarini ishlab chiqish; har bir yechimning imkoniyatlari va to‘siqlarni tahlil qilish; muqobil yechimlarni tanlash
4-bosqich: Keys yechimini yechimini shakllantirish va asoslash, taqdimot.	yakka va guruhda ishlash; muqobil variantlarni amalda qo‘llash imkoniyatlarini asoslash; ijodiy-loyiha taqdimotini tayyorlash; yakuniy xulosa va vaziyat yechimining amaliy aspektlarini yoritish

Keys. Xemming kodi va uni qurish. Talaba Xemming kodini qurish muolajasini amalga oshirdi va uning natijasida xatolik yuz berdi.

Keysni bajarish bosqichlari va topshiriqlari:

- Keysdagi muammoni keltirib chiqargan asosiy sabablarni belgilang (individual va kichik guruhda) .
- Xatolikni bartaraf etuvchi ishlar ketma-ketligini belgilang (juftlikdagi ish).

“FSMU” metodi

Texnologiyaning maqsadi: Mazkur texnologiya ishtirokchilardagi umumiy fikrlardan xususiy xulosalar chiqarish, taqqoslash, qiyoslash orqali axborotni o‘zlashtirish, xulosalash, shuningdek, mustaqil ijodiy fikrlash ko‘nikmalarini shakllantirishga xizmat qiladi. Mazkur texnologiyadan ma’ruza mashg‘ulotlarida, mustahkamlashda, o‘tilgan mavzuni so‘rashda, uyga vazifa berishda hamda amaliy mashg‘ulot natijalarini tahlil etishda foydalanish tavsiya etiladi.

Texnologiyani amalga oshirish tartibi:

-qatnashchilarga mavzuga oid bo‘lgan yakuniy xulosa yoki g‘oya taklif etiladi;

-har bir ishtirokchiga FSMU texnologiyasining bosqichlari yozilgan qog‘ozlarni tarqatiladi:

F	• fikringizni bayon eting
S	• fikringizni bayoniga sabab ko'rsating
M	• ko'rsatgan sababingizni isbotlab misol keltiring
U	• fikringizni umumlashtirish

- ishtirokchilarning munosabatlari individual yoki guruhiy tartibda taqdimot qilinadi.

FSMU tahlili qatnashchilarda kasbiy-nazariy bilimlarni amaliy mashqlar va mavjud tajribalar asosida tezroq va muvaffaqiyatli o‘zlashtirilishiga asos bo‘ladi.

Namuna.

Fikr: “Axborot xavfsizligi siyosati, korxonaning axborot xavfsizligini ta’minlashda asosiy xujjat hisoblanadi”.

Topshiriq: Mazkur fikrga nisbatan munosabatingizni FSMU orqali tahlil qiling.

“Assesment” metodi

Metodning maqsadi: mazkur metod ta’lim oluvchilarning bilim darajasini baholash, nazorat qilish, o‘zlashtirish ko‘rsatkichi va amaliy ko‘nikmalarini tekshirishga yo‘naltirilgan. Mazkur texnika orqali ta’lim oluvchilarning bilish faoliyati turli yo‘nalishlar (test, amaliy ko‘nikmalar, muammoli vaziyatlar mashqi, qiyosiy tahlil, simptomlarni aniqlash) bo‘yicha tashhis qilinadi va baholanadi.

Metodni amalga oshirish tartibi:

“Assesment” lardan ma’ruza mashg‘ulotlarida talabalarning yoki qatnashchilarning mavjud bilim darajasini o‘rganishda, yangi ma’lumotlarni bayon qilishda, seminar, amaliy mashg‘ulotlarda esa mavzu yoki ma’lumotlarni o‘zlashtirish darajasini baholash, shuningdek, o‘z-o‘zini baholash maqsadida individual shaklda foydalanish tavsiya etiladi. Shuningdek, o‘qituvchining ijodiy yondashuvi hamda o‘quv maqsadlaridan kelib chiqib, assesmentga qo‘shimcha topshiriqlarni kiritish mumkin.

Namuna. Har bir katakdagi to‘g‘ri javob 5 ball yoki 1-5 balgacha baholanishi mumkin.

Test

1. Axborot xavfsizligi konsepsiyasini ishlab chiqish necha bosqichni o‘z ichiga oladi?

- A. 3 bosqichni
- B. 4 bosqichni
- C. 5 bosqichni

Qiyosiy tahlil

- Himoya tizimini ishonchliligini tahlil qiling?

Tushuncha tahlili

- “Kriptotizim”ni izohlang...

Amaliy ko‘nikma

- “1914 143 1524 1181 1241 1573” yuqoridagi ma’lumotni RSA usulida deshifrlang.

“Tushunchalar tahlili” metodi

Metodning maqsadi: mazkur metod talabalar yoki qatnashchilarni mavzu buyicha tayanch tushunchalarni o‘zlashtirish darajasini aniqlash, o‘z bilimlarini mustaqil ravishda tekshirish, baholash, shuningdek, yangi mavzu buyicha dastlabki

bilimlar darajasini tashhis qilish maqsadida qo‘llaniladi.

Metodni amalga oshirish tartibi:

- ishtirokchilar mashg‘ulot qoidalari bilan tanishtiriladi;
- o‘quvchilarga mavzuga yoki bobga tegishli bo‘lgan so‘zlar, tushunchalar nomi tushirilgan tarqatmalar beriladi (individual yoki guruhli tartibda);
- o‘quvchilar mazkur tushunchalar qanday ma’no anglatishi, qachon, qanday holatlarda qo‘llanilishi haqida yozma ma’lumot beradilar;
- belgilangan vaqt yakuniga yetgach o‘qituvchi berilgan tushunchalarning tugri va tuliq izohini uqib eshittiradi yoki slayd orqali namoyish etadi;
- har bir ishtirokchi berilgan tugri javoblar bilan uzining shaxsiy munosabatini taqqoslaydi, farqlarini aniqlaydi va o‘z bilim darajasini tekshirib, baholaydi.

Namuna: “Moduldagi tayanch tushunchalar tahlili”

Tushunchalar	**Sizningcha bu tushuncha qanday ma’noni anglatadi?**	**Qo‘shimcha ma’lumot**
Informatsiya	Muayyan obekt xususidagi bilimlarimiz noaniqlik darajasini pasaytirishga imkon beruvchi har qanday axborot(ma’lumot).	
Ma’lumot	Texnika vositalari yordamida qidirish,qabul qilish, saqlash, ishlov berish, uzatish mumkin bo‘lgan shaklga keltirilgan har qanday informatsiya.	
Axborot xavfsizligi	Axborot va axborot tashuvchilarni himoyasini ta’minlash.	
Huquqiy himoya	Axborot xavfsizligini ta’minlashning huquqiy ta’minoti.	
Shifrlash	Xabarni ma’lum algoritm bo‘yicha o‘qib bo‘lmaydigan holatga keltirish.	
Deshifrlash	Qabul qilingan xabarni ma’lum algoritm orqali qayta tiklash.	

Izoh: Ikkinchi ustunchaga qatnashchilar tomonidan fikr bildiriladi. Mazkur tushunchalar haqida qo‘shimcha ma’lumot glossariyda keltirilgan.

“Insert” metodi

Metodning maqsadi: Mazkur metod o‘quvchilarda yangi axborotlar tizimini

qabul qilish va bilmlarni o‘zlashtirilishini yengillashtirish maqsadida qo‘llaniladi, shuningdek, bu metod o‘quvchilar uchun xotira mashqi vazifasini ham o‘taydi.

Metodni amalga oshirish tartibi:

- o‘qituvchi mashg‘ulotga qadar mavzuning asosiy tushunchalari mazmuni yoritilgan input-matnni tarqatma yoki taqdimot ko‘rinishida tayyorlaydi;
- yangi mavzu mohiyatini yorituvchi matn ta’lim oluvchilarga tarqatiladi yoki taqdimot ko‘rinishida namoyish etiladi;
- ta’lim oluvchilar individual tarzda matn bilan tanishib chiqib, o‘z shaxsiy qarashlarini maxsus belgilar orqali ifodalaydilar. Matn bilan ishlashda talabalar yoki qatnashchilarga quyidagi maxsus belgilardan foydalanish tavsiya etiladi:

Belgilar	**1-matn**	**2-matn**	**3-matn**
“V” – tanish ma’lumot.			
“?” – mazkur ma’lumotni tushunmadim, izoh kerak.			
“+” bu ma’lumot men uchun yangilik.			
“– ” bu fikr yoki mazkur ma’lumotga qarshiman?			

Belgilangan vaqt yakunlangach, ta’lim oluvchilar uchun notanish va tushunarsiz bo‘lgan ma’lumotlar o‘qituvchi tomonidan tahlil qilinib, izohlanadi, ularning mohiyati to‘liq yoritiladi. Savollarga javob beriladi va mashg‘ulot yakunlanadi.

Venn Diagrammasi metodi. Metodning maqsadi: Bu metod grafik tasvir orqali o‘qitishni tashkil etish shakli bo‘lib, u ikkita o‘zaro kesishgan aylana tasviri orqali ifodalanadi. Mazkur metod turli tushunchalar, asoslar, tasavurlarning analiz va sintezini ikki aspekt orqali ko‘rib chiqish, ularning umumiy va farqlovchi jihatlarini aniqlash, taqqoslash imkonini beradi.

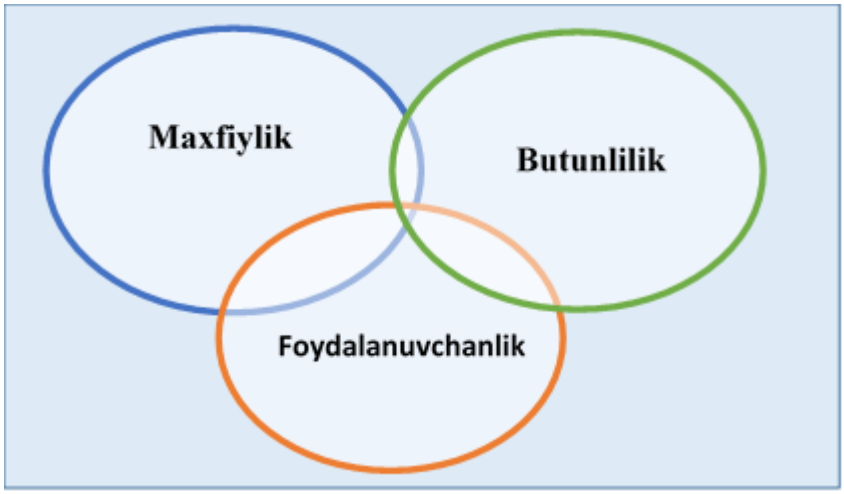
Metodni amalga oshirish tartibi:

- ishtirokchilar ikki kishidan iborat juftliklarga birlashtiriladilar va ularga

koʻrib chiqilayotgan tushuncha yoki asosning oʻziga xos, farqli jihatlarini (yoki aksi) doiralar ichiga yozib chiqish taklif etiladi;

- navbatdagi bosqichda ishtirokchilar toʻrt kishidan iborat kichik guruhlarga birlashtiriladi va har bir juftlik oʻz tahlili bilan guruh a'zolarini tanishtiradilar;
- juftliklarning tahlili eshitilgach, ular birgalashib, koʻrib chiqilayotgan muammo yohud tushunchalarning umumiy jihatlarini (yoki farqli) izlab topadilar, umumlashtiradilar va doirachalarning kesishgan qismiga yozadilar.

Namuna: Informatsiyaning struktura oʻlchovi



"Blis-oʻyin" metodi

Metodning maqsadi: oʻquvchilarda tezlik, axborotlar tizmini tahlil qilish, rejalashtirish, prognozlash koʻnikmalarini shakllantirishdan iborat. Mazkur metodni baholash va mustahkamlash maksadida qoʻllash samarali natijalarni beradi.

Metodni amalga oshirish bosqichlari:

1. Dastlab ishtirokchilarga belgilangan mavzu yuzasidan tayyorlangan topshiriq, ya'ni tarqatma materiallarni alohida-alohida beriladi va ulardan materialni sinchiklab oʻrganish talab etiladi. Shundan soʻng, ishtirokchilarga toʻgʻri javoblar tarqatmadagi «yakka baho» kolonkasiga belgilash kerakligi tushuntiriladi. Bu bosqichda vazifa yakka tartibda bajariladi.

2. Navbatdagi bosqichda trener-oʻqituvchi ishtirokchilarga uch kishidan iborat kichik guruhlarga birlashtiradi va guruh a'zolarini oʻz fikrlari bilan guruhdoshlarini tanishtirib, bahslashib, bir-biriga ta'sir oʻtkazib, oʻz fikrlariga

ishontirish, kelishgan holda bir to‘xtamga kelib, javoblarini «guruh bahosi» bo‘limiga raqamlar bilan belgilab chiqishni topshiradi. Bu vazifa uchun 15 daqiqa vaqt beriladi.

3. Barcha kichik guruhlar o‘z ishlarini tugatgach, to‘g‘ri harakatlar ketma-ketligi trener-o‘qituvchi tomonidan o‘qib eshittiriladi, va o‘quvchilardan bu javoblarni «to‘g‘ri javob» bo‘limiga yozish so‘raladi.

4. “To‘g‘ri javob” bo‘limida berilgan raqamlardan «yakka baho» bo‘limida berilgan raqamlar taqqoslanib, farq bulsa “0”, mos kelsa “1” ball quyish so‘raladi. Shundan so‘ng “yakka xato” bo‘limidagi farqlar yuqoridan pastga qarab qo‘shib chiqilib, umumiy yig‘indi hisoblanadi.

5. Xuddi shu tartibda “to‘g‘ri javob” va “guruh bahosi” o‘rtasidagi farq chiqariladi va ballar “guruh xatosi” bo‘limiga yozib, yuqoridan pastga qarab qo‘shiladi va umumiy yig‘indi keltirib chiqariladi.

6. Trener-o‘qituvchi yakka va guruh xatolarini to‘plangan umumiy yig‘indi bo‘yicha alohida-alohida sharhlab beradi.

7. Ishtirokchilarga olgan baholariga qarab, ularning mavzu bo‘yicha o‘zlashtirish darajalari aniqlanadi.

“Ochiq kalitli kriptotizimlar algorimlarini dasturlash” ketma-ketligini joylashtiring. O‘zingizni tekshirib ko‘ring!

Harakatlar mazmuni	Yakka baho	Yakka xato	To‘g‘ri javob	Guruh bahosi	Guruh xatosi
Ikkita 200 dan katta bo‘lgan tub son p va q tanlanadi					
Kalitning ochiq tashkil etuvchisi n hosil qilinadi n=pq					
Quyidagi formula bo‘yicha Eyler funksiyasi hisoblanadi: f(p,q)=(p-1)(q-1)					
f(p,q) qiymati bilan o‘zaro tub bo‘lgan katta tub son e tanlab olinadi.					
Quyidagi shartni qanoatlantiruvchi d soni aniqlanadi e*d=1(modf(p,q))					
Shifrlangan axborot quyidagi formula bo‘yicha aniqlanuvchi Y(i) sonlarning ketma-ketligi					

ko‘rinishida olinadi: $Y(i)=(X(i))^e(\mathrm{mod}n)$					
Axborotni deshifrlashda quyidagi munosabatdan foydalaniladi: $X(i)=(Y(i))^d(\mathrm{mod}n)$					

“Brifing” metodi

“Brifing”- (ing. briefing-qisqa) biror-bir masala yoki savolning muhokamasiga bag‘ishlangan qisqa press-konferensiya.

O‘tkazish bosqichlari:

1. Taqdimot qismi.

2. Muhokama jarayoni (savol-javoblar asosida).

Brifinglardan trening yakunlarini tahlil qilishda foydalanish mumkin. Shuningdek, amaliy o‘yinlarning bir shakli sifatida qatnashchilar bilan birga dolzarb mavzu yoki muammo muhokamasiga bag‘ishlangan brifinglar tashkil etish mumkin bo‘ladi.Talabalar yoki tinglovchilar tomonidan yaratilgan mobil ilovalarning taqdimotini o‘tkazishda ham foydalanish mumkin.

“Portfolio”metodi

“Portfolio” – (ital. portfolio-portfel, ingl.hujjatlar uchun papka) ta’limiy va kasbiy faoliyat natijalarini autentik baholashga xizmat qiluvchi zamonaviy ta’lim texnologiyalaridan hisoblanadi. Portfolio mutaxassisning saralangan o‘quv-metodik ishlari, kasbiy yutuqlari yig‘indisi sifatida aks etadi. Jumladan, talaba yoki tinglovchilarning modul yuzasidan o‘zlashtirish natijasini elektron portfoliolar orqali tekshirish mumkin bo‘ladi. Oliy ta’lim muassasalarida portfolioning quyidagi turlari mavjud:

Faoliyat turi	**Ish shakli**	
	Individual	**Guruhiy**
Ta’limiy faoliyat	Talabalar portfoliosi, bitiruvchi, doktorant, tinglovchi portfoliosi va boshq.	Talabalar guruhi, tinglovchilar guruhi portfoliosi va boshq.
Pedagogik faoliyat	O‘qituvchi portfoliosi, rahbar xodim portfoliosi	Kafedra, fakultet, markaz, OTM portfoliosi va boshq.

III-BO‘LIM

NAZARIY MATERIALLAR

III. NAZARIY MASHG‘ULOTLAR MATERIALLARI

1-MAVZU. KIBERXAVFSIZLIKKA KIRISH (2 soat)

Reja:

1.1. Kiberxavfsizlikning tarixi va uning jamiyatga ta’siri.

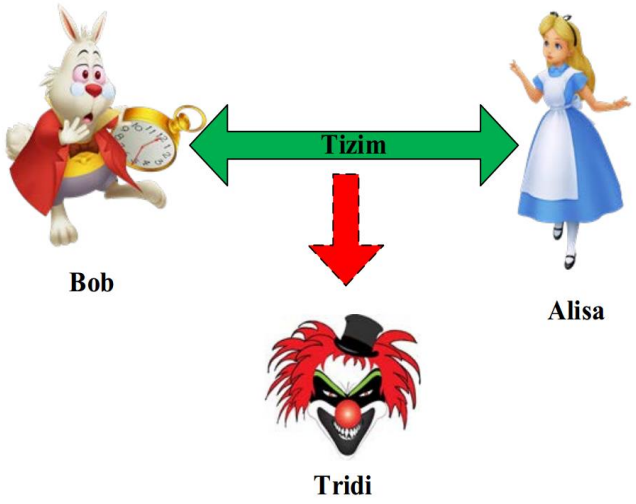
1.2. Kiberxavfsizlikda risklarni boshqarish konsepsiyasi.

1.3. Xavfsizlikni ta’minlashning turli usullari.

Tayanch iboralar: *Kiberxavfsizlik, Konfidensiallik, Yaxlitlik, Foydalanuvchanlik, Ma’lumotlar xavfsizligi, Dasturiy ta’minotlar xavfsizligi, Tashkil etuvchilar xavfsizligi, Aloqa xavfsizligi, Tizim xavfsizligi, Inson xavfsizligi*.

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 akslantirilgan. 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.



1.1-rasm. Axborot xavfsizligining hayotdagi timsollari

Ushbu majmuaning 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 kiberxujumlar odatda maxfiy axborotni boshqarishni, almashtirishni yoki yo‘q qilishni; foydalanuvchilardan pul undirishni; normal ish faoliyatini buzishni maqsad qiladi. Hozirda samarali kiberxavfsizlik choralarini 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 choralarini 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).

Kiberxavfsizlikni fundamental atamalarini aniqlashda turli yondashuvlar mavjud. Xususan, CSEC2017 JTF manbasida kiberxavfsizlikning quyidagi 6 ta atamasi keltirilgan:

Konfidensiallik – axborot yoki uni eltuvchisining shunday holatiki, undan ruxsatsiz tanishishning yoki nusxalashning oldi olingan bo‘ladi. Konfidensiallik axborotni ruxsatsiz “o‘qish”dan himoyalash bilan shug‘ullanadi. AOB senariysida Bob uchun konfidensiallik juda muhim. Ya’ni, Bob o‘z balansida qancha pul borligini Tridining bilishini istamaydi. Shu sababli Bob uchun balans xususidagi ma’lumotlarning konfidensialligini 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 Tridiдan himoyalash shart. Masalan, Bob o‘zining akkauntida balansning o‘zgarishidan yoki Alisa akkauntida balansning oshishidan himoyalashi shart.

Shu o‘rinda konfidensiallik 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 (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanish darajasi holati.

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

Aktiv-himoyalanuvchiaxborotyokiresurslar. Yoki, tashkilot uchun qimmatli barcha narsalar.

Tahdid – tizim yoki tashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa. Yoki, tahdid - axborot xavfsizligini buzuvchi potensial yoki real mavjud xavfni tug‘diruvchi sharoit va omillar majmui. Tahdid tashkilotning aktivlariga qaratilgan bo‘ladi. Masalan, aktiv sifatida korxonaga tegishli biror bir saqlanuvchi hujjat bo‘lsa, u holda ushbu hujjat saqlanadigan xonaga nisbatan tahdid amalga oshirilish mumkin.

Zaiflik – bir yoki bir nechta tahdidlarni amalga oshirishga imkon beruvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik.

Boshqarish vositasi – riskni o‘zgartiradigan harakatlar bo‘lib, natijasi zaiflik yoki tahdidlarni o‘zgarishiga ta’sir qiladi. Bundan tashqari, boshqarish vositasining o‘zi turli tahdidlar foydalanishi mumkin bo‘lgan zaiflikka ega bo‘lishi mumkin. Masalan, tashkilotda saqlanayotgan qog‘oz ko‘rinishidagi axborotni yong‘indan himoyalash uchun o‘chirish vositalari boshqarish vositasi sifatida ko‘rilishi mumkin. Yong‘in bo‘lganida xodimlarning xatti-xarakatlari va yong‘inni oldini olish bo‘yicha ko‘rilgan chora-tadbirlar ham boshqarish vositasi hisoblanishi mumkin. Yong‘inga qarshi kurashish tizimining ishlamay qolish holatiga esa

boshqarish vositasidagi kamchilik sifatida qaraladi.

Axborot xavfsizligi va kiberxavfsizlik o‘rtasidagi farq.

“Kiberxavfsizlik” va “axborot xavfsizligi” atamalaridan, ko‘pincha o‘rnilari almashgan holda, foydalanishadi. Ba’zilar kiberxavfsizlikka axborot xavfsizligi, axborot texnologiyalari xavfsizligi va (axborot) risklarni boshqarish tushunchalariga sinonim sifatida qarashsa, ayrimlar esa, xususan hukumat sohasidagilar, kompyuter jinoyatchiligi va muhim infrastrukturalar himoyasini o‘z ichiga olgan milliy xavfsizlik bilan bog‘liq texnik tushuncha sifatida qaraydilar. Turli soha xodimlari tomonidan o‘z maqsadlariga moslashtirish holatlari mavjud bo‘lsada, axborot xavfsizligi va kiberxavfsizlik tushunchalari orasida ba’zi muhim farqlar mavjud.

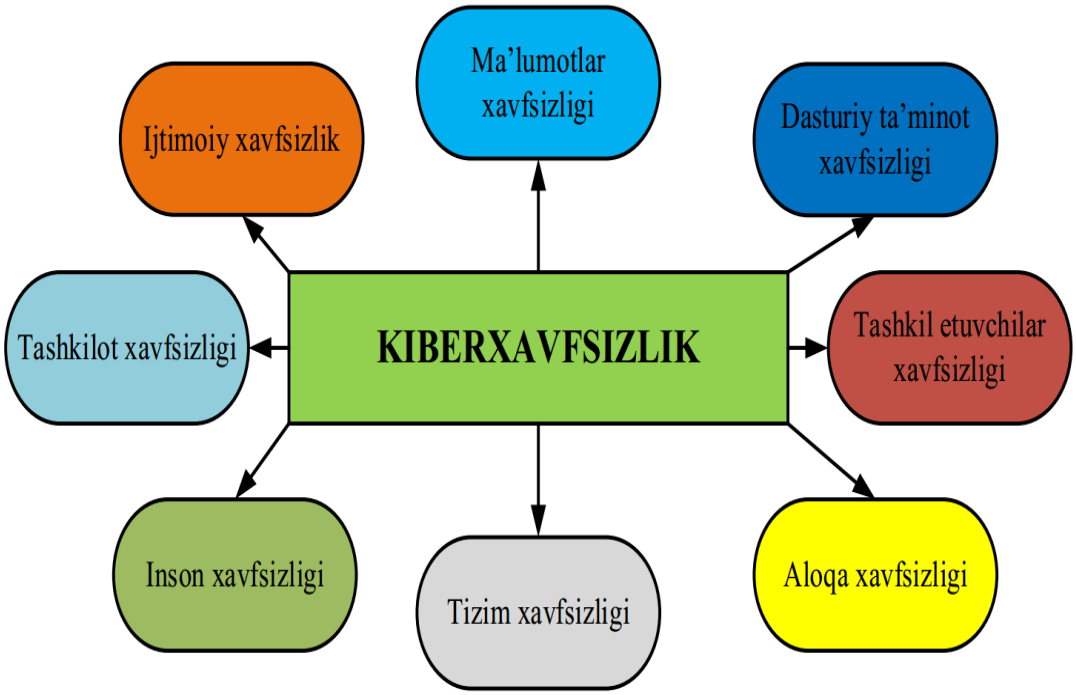
Axborot xavfsizligi sohasi, axborotning ifodalanishidan qat’iy nazar (qog‘ozko‘rinishidagi, elektron vainsonlarfikrlashida, og‘zakivavizual) intelektual huquqlarni himoyalash bilan shug‘ullanadi. Kiberxavfsizlik esa elektron shakldagi axborotni (barcha holatdagi, tarmoqdan to qurilmagacha bo‘lgan, o‘zaro birga ishlovchi tizimlarda saqlanayotgan, uzatilayotgan va ishlanayotgan axborotni) himoyalash bilan shug‘ullanadi.

Bundan tashqari, hukumatlar tomonidan moliyalashtirilgan hujumlar va rivojlangan doimiy tahidlar (Advanced persistent threats, APT) ham aynan kiberxavfsizlikka tegishli. Qisqacha aytganda, kiberxavfsizlikni axborot xavfsizligining bir yo‘nalishi deb tushunish uni to‘g‘ri anglashga yordam beradi.

Kiberxavfsizlikning bilim sohalari. CSEC2017 JTF manbasiga ko‘ra kiberxavfsizlik 8 ta bilim sohasiga bo‘lingan, o‘z o‘rnida ularning har biri qismsohalarga bo‘linadi (1.3-rasm).

“Ma’lumotlar xavfsizligi” bilim sohasining maqsadi ma’lumotlarni saqlash, ishlash vauzatishda himoyani ta’minlash. Mazkur bilim sohasida himoyani to‘liq amalga oshirish uchun matematik va analitik algoritmlardan foydalaniladi.

“Dasturiy ta’minot xavfsizligi” bilim sohasi foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy vositalarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi.



1.3-rasm. Kiberxavfsizlikning bilim sohalari

“Tashkil etuvchilar xavfsizligi” bilim sohasi katta tizimlarda integrallashgan tashkil etuvchilarni loyihalashga, sotib olishga, testlashga, tahlillashga va texnik xizmat ko‘rsatishga e’tibor qaratadi. Tizim xavfsizligi gohida tashkil etuvchilar xavfsizligidan farq qiladi. Tashkil etuvchilar xavfsizligi tizimning qanday loyihalanganligiga, yaratilganligiga, sotib olinganligiga, boshqa tarkibiy qismlar bilan bog‘langanligiga, qanday ishlayotganligiga va saqlanayotganligiga bog‘liq bo‘ladi.

“Aloqa xavfsizligi” bilim sohasi tashkil etuvchilar o‘rtasidagi aloqani himoyalashga e’tibor qaratib, o‘zida fizik va mantiqiy ulanishni mujassamlashtiradi.

“Tizim xavfsizligi” bilim sohasi tashkil etuvchilar, ulanishlar va dasturiy ta’minotdan iborat tizim xavfsizligining jihatlariga e’tibor qaratadi. Tizim xavfsizligini tushunish uchun, nafaqat uning tarkibiy qismlari va ularning bog‘lanishlarini tushunish, balki yaxlitlikni ham hisobga olish talab etiladi. Ya’ni, tizimni to‘liqligicha ko‘rib chiqish talab etiladi. Mazkur bilim sohasi, “Tashkil etuvchilar xavfsizligi” va “Aloqa xavfsizligi” bilim sohalari bilan bir qatorda, tashkil etuvchilar bog‘lanishlarining xavfsizligi va undan yuqori tizimlarda

foydalanish masalasini hal etadi.

“Inson faoliyati xavfsizligi” bilim sohasi kiberxavfsizlik bilan bog‘liq inson hatti-harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida ma’lumotlarni va shaxsiylikni himoya qilishga e’tibor qaratadi.

“Tashkilot xavfsizligi” bilim sohasi tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini madadlash uchun risklarni boshqarishga e’tibor qaratadi.

“Ijtimoiy xavfsizlik” bilim sohasi jamiyatda u yoki bu darajadagi ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi. Kiberjinoyatchilik, qonunlar, axloqiy munosabatlar, siyosat, shaxsiy hayot va ularning bir-biri bilan munosabatlari ushbu bilim sohasidagi asosiy tushunchalar hisoblanadi.

Demak, aytish mumkinki, kiberxavfsizlik sohasi axborot texnologiyalari mutaxassislari uchun zarur soha hisoblanadi.

Nazorat savollari:

1. Axborot xavfsizligi va kiberxavfsizlik o‘rtasidagi farqni tushuntirib bering.
2. Kiberxavfsizlik fani sohasining tuzilishini qanday tasvirlash mumkin?
3. Kiberxavfsizlikning bilim sohalari nimalardan iborat?
4. “Tizim xavfsizligi” va “Tashkilot xavfsizligi” bilim sohalarini tushuntirib bering?

Adabiyotlar va internet saytlari:

1. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoykulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma, – T. “Nihol print” OK, 2021. – 224 b.
2. S.K. Ganiev, Z.T. Xudoykulov, N.B. Nasrullaev. Основы кибербезопасности: Учебное пособие, – T. “Mahalla oila nashriyoti”, 2021. – 224 b.
3. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях - М: ДМК Пресс, 2012. - 596 с.

2-MAVZU. KIBERTAHDIDLAR VA ZAIFLIKLAR

Reja:

2.1. Kibertahdidlar, hujumlar, zaifliklar va uning xususiyatlari.

2.2. Zararli hujum manbalari. Zararli dasturlarning turlari.

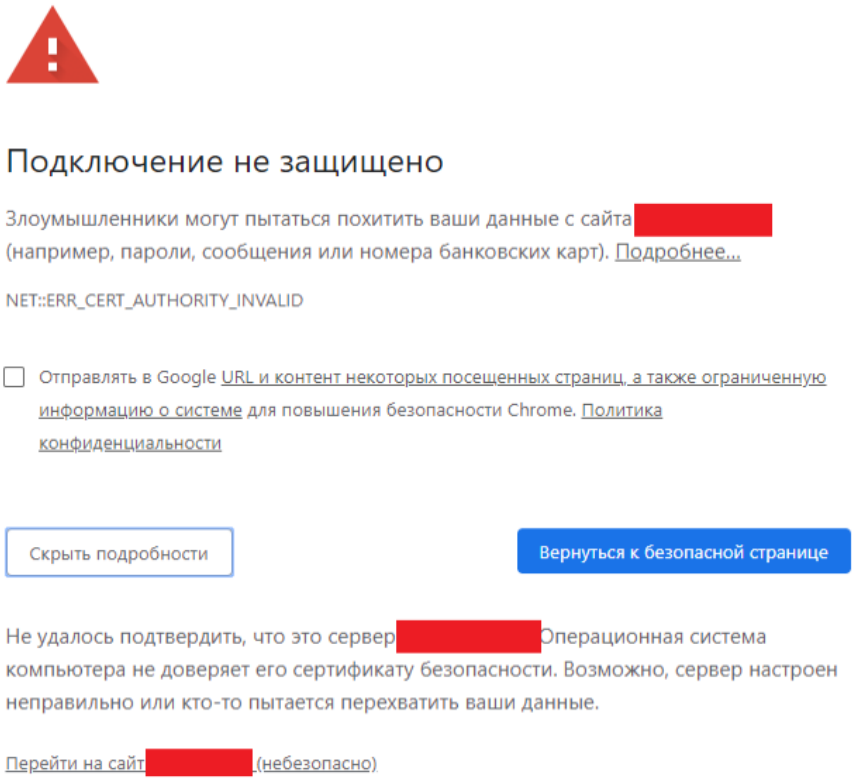
2.3. Kompyuter jinoyatchiligi.

Tayanch iboralar: *Kibertahdidlar, hujumlar, zaifliklar, zararli hujum manbalari, zararli dasturlarning turlari, hujum turlari, ijtimoiy injineriya, buferni to‘lib toshishi.*

Foydalanuvchilarga kiberxavfsizlik tizimidagi eng zaif nuqta sifatida qaraladi. Foydalanuvchilar tomonidan har qanday yuqori darajadagi xavfsizlik ham buzilishi mumkin. Masalan, Bob amazon.com onlayn do‘konidan biror narsani sotib olmoqchi, deylik. Buning uchun Bob turli kriptografik usullarga tayanadigan SSL (Secure Sockets Layer) protokoli yordamida Amazon bilan ishonchli bog‘lanish uchun web-brauzerdan foydalanishi mumkin. Ushbu protokol barcha zarur amallar to‘g‘ri bajarilganida kafolatli xavfsizlikni ta’minlaydi.

Biroq, ushbu protokolga qaratilgan ba’zi hujum turlari (O‘rtada turgan odam hujumi, Man-in-the-middle attack) mavjudki, ularning amalga oshishi uchun foydalanuvchi “ishtiroki” talab etiladi (1.4-rasm). Agar foydalanuvchi xavfsiz holatni tanlasa (Вернуться к безопасной странице) hujum amalga oshmaydi. Biroq, foydalanuvchi tomonidan xavfsiz bo‘lmagan tanlov (Перейти на сайт …. (небезопасно)) amalga oshirilganida hujum muvaffaqiyatli tugaydi.

Boshqacha aytganda, yuqori xavfsizlik darajasiga ega protokoldan foydalanilganda ham foydalanuvchining noto‘g‘ri harakati sababli xavfsizlik buzilishi mumkin.



1.4-rasm. SSL protokolidagi xavfsizlik ogohlantirishi

Odatda foydalanuvchilar esda saqlash oson bo‘lgan parollardan foydalanishga harakat qiladilar. Biroq, bunday yo‘l tutish buzg‘unchi uchun parollarni taxminlab topish imkoniyatini oshiradi. Boshqa tomondan, murakkab parollardan foydalanish va ularni turli eltuvchilarda saqlash (masalan, qog‘ozda qayd etish) esa, ushbu muammoni yanada kuchaytiradi.

Bu misollar inson omili tufayli turli joylar va holatlarda xavfsizlik muammolarining kelib chiqishi mumkinligini ko‘rsatadi. Inson omili tufayli yuzaga keladigan xavfsizlik muammolariga ko‘plab misollar keltirish mumkin. Biroq, keltirilgan holatlardagi eng muhim jihat shundaki, xavfsizlik nuqtai nazaridan “tenglamadan” inson omilini olib tashlash zarur. Boshqacha aytganda, inson omili ishtirok etmagan tizimlar ishtirok etgan tizimlarga nisbatan xavfsizroq bo‘ladi.

Eng muhim inson omillariga quyidagilar taalluqli:

− Kiberxavfsizlik sohasiga oid bilimlarni yetishmasligi katta hajmdagi oshkor zaifliklarni paydo bo‘lishiga olib keladi. Kiberxavfsizlik sohasi an’anaviy xavfsizlikka aloqador bo‘lgani bois, zarur texnologik moslashishning tezkorligi

koʻp hollarda boʻlishi mumkin boʻlgan zaifliklar sonini oshiradi. Boshqa tomondan, insonning sohaga tegishli soʻnggi texnologik bilimlarni oʻzlashtirishi har doim ham yetarli boʻlmaydi.

− Risklarni bartaraf etishni va ular haqida xabar berishning yetarli boʻlmasligi kiberxavfsizlikda takrorlanuvchi va kutilmagan buzilishlarga sababchi boʻladi. Insonlar odatda tashkilotlariga jiddiy xavf soluvchi risk mavjudligini bilishsada, uni oshkor qilishmaydi. Buning asosiy sababi sifatida risk bevosita shaxsning oʻziga, uni moliyaviy holatiga ta'sir etmasligini yoki oshkor qilinganida shaxsning obroʻsi tushishini keltirishadi.

− Madaniyat va munosabatlardagi muammolarga tashkilotning oʻzi yoki tashkilot ichki ma'lumotlarini biluvchi norozi va e'tiborsiz xodimning paydo boʻlishi sababchi boʻlishi mumkin. Kiberxavfsizlik muammolarining aksariyati ichki hisoblanib, ular xodimlar orasidagi turli kelishmovchiliklar va tashkilot ichidagi muhitning yaxshi emasligi natijasida yuzaga keladi. Bu sabablar esa, xodimning tashkilot ichki strukturasini yaxshi bilgani bois, aksariyat hollarda jiddiy muammolarga olib keladi.

− Xavfsizlik mashgʻulotlariga kam mablagʻ sarflanishi boshqarilayotgan xavfsizlik risklari toʻgʻrisidagi ma'lumotning kamligi sababchi boʻladi. Odatda, soha korxonalaridagi xodimlar mustaqil ravishda kiberxavfsizlik qoidalarini oʻrganishmaydi. Shuning uchun kiberxavfsizlik qoidalarini xodimlarga maxsus mashgʻulotlar shaklida yetkazish zarur boʻladi. Bu esa tashkilotdan xavfsizlik mashgʻulotlariga yetarlicha mablagʻ sarflanishni talab qiladi.

− Hisobga olish nuqtasining yagona emasligi natijasida xavfsizlikning toʻlaqonli amalga oshirilmasligi kuzatiladi. Amalda xavfsizlikni kafolatli ta'minlashda uning nazoratini bir nuqtada amalga oshirish muhim hisoblanadi. Yagona nuqtada amalga oshirilgan xavfsizlik nazorati taqsimlangan shakliga nisbatan ishonchli boʻladi. Biroq, tashkilotlardagi xavfsizlik nazoratining murakkabligi bois, nazorat odatda taqsimlangan holda boshqariladi.

− Ijtimoiy injineriya asosida xavfsizlik nazoratini aylanib oʻtishda foydalanuvchidan, an'anaviy josuslik texnikasi yordamida, ma'lumotlar qoʻlga

kiritiladi. Eng yaxshi kiberxavfsizlik tizimiga ega bo‘lgan tashkilotga ham ijtimoiy injineriya tahdidi xavf solishi mumkin. Ayniqsa, foydalanuvchilarni turli ijtimoiy tarmoqlarda shaxsiy ma’lumotlarini e’tiborsizlik bilan qoldirishi bu xavfning keskin ortishiga sababchi bo‘lmoqda.

Kiberjinoyatchilik – g‘arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o‘g‘irlashga yoki buzishga yo‘naltirilgan alohida shaxslarning yoki guruhlarning harakatlari.

Kiberhujumga duch kelgan tashkilot uchun kiberjinoyatlar ichki yoki tashqi bo‘lishi mumkin:

Ichki kiberjinoyatlar: tarmoqqa yoki kompyuter tizimiga, ular bilan tanish va ulardan qonuniy foydalanish huquqiga ega bo‘lgan shaxs tomonidan, amalga oshiriladi. Mazkur turdagi kiberjinoyatlar odatda tashkilotning xafa bo‘lgan va norozi xodimlari tomonidan amalga oshiriladi. Ushbu xodimlarning maqsadi esa tashkilot yoki uning rahbaridan o‘ch olish yoki ochko‘zlik bo‘lishi mumkin. Xafa bo‘lgan xodim, AT infrastrukturasi, xavfsizlik arxitekturasi va tizimi bilan yaqindan tanish bo‘lgani bois, mazkur turdagi jinoyatchilik tashkilotga jiddiy ziyon yetkazishi mumkin. Bundan tashqari, kiberjinoyatchi tashkilot tarmog‘idan foydalanish imkoniyatiga ega bo‘ladi. Shuning uchun, ichki kiberjinoyatchilik natijasida maxfiy axborotning sirqib chiqish imkoniyati yuqori bo‘ladi.

Tashqi kiberjinoyatlar: odatda tashqaridan yoki tashkilot ichkarisidan yollangan hujumchi tomonidan amalga oshiriladi. Mazkur kiberjinoyatchilik tashkilotning nafaqat moliyaviy yo‘qotishlariga, balki obro‘sining yo‘qolishiga ham sababchi bo‘ladi. Hujum tashqaridan amalga oshirilgani bois, hujumchi harakatni tashkilot AT infrastrukturasini skaner qilish va unga aloqador ma’lumotlarni to‘plashdan boshlaydi. Xususan, malakali buzg‘unchi dastlab tashkilotda foydalanilgan tarmoqlararo ekran vositasining log faylini tahlil qilishdan boshlaydi. Shu bois, tarmoq ma’muri mazkur imkoniyatni buzg‘unchiga taqdim etmasligi shart.

Kiberjinoyat amalga oshirilganida quyidagilar asosiy maqsad sifatida qaraladi:

- mablag‘, qimmatli qog‘ozlar, kredit, moddiy boyliklar, tovarlar, xizmatlar, imtiyozlar, ko‘chmas mulk, yoqilg‘i xom ashyosi, energiya manbalari va strategik xom ashyolarni noqonuniy o‘zlashtirish;

- soliq va boshqa yig‘imlarni to‘lashdan bosh tortish;

- jinoiy daromadlarni qonunlashtirish;

- qalbaki hujjatlar, shtamplar, muhrlar, blankalar, shaxsiy yutuq chiptalarini qalbakilashtirish;

- shaxsiy yoki siyosiy maqsadlarda maxfiy ma’lumotlarni olish;

- ma’muriyatning yoki ishdagi hamkasblarning g‘arazli munosabatlari uchun qasos olish;

- shaxsiy yoki siyosiy maqsadlar uchun mamlakat pul tizimini buzish;

- mamlakatdagi vaziyatni, hududiy ma’muriy tuzilishni beqarorlashtirish;

- talonchilik, raqibni yo‘q qilish yoki siyosiy maqsadlar uchun muassasa, korxona yoki tizim ish tartibini buzish;

- shaxsiy intelektual qobiliyatini yoki ustunligini namoyish qilish.

Kiberjinoyat turlarini qat’iy tasniflashning imkoni yo‘q. Quyida kriminologiya sohasiga nisbatan kiberjinoyatlarning turlari keltirilgan:

- iqtisodiy kompyuter jinoyatchiligi;

- inson va fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga qarshi qaratilgan kompyuter jinoyatchiligi;

- jamoat va davlat xavfsizligiga qarshi kompyuter jinoyatchiligi. Iqtisodiy kompyuter jinoyatchiligi amalda ko‘p uchraydi.

Ular jinoyatchilarga millionlab AQSh dollari miqdoridagi noqonuniy daromadlar keltiradi. Ular orasida keng tarqalgani firibgarlik, asosan, bank hisob raqamlari va bank kartalari orqali amalga oshiriladi. Xalqaro amaliyotda plastik kartalar bilan sodir etilgan jinoyatlar yo‘qolgan yoki o‘g‘irlangan kartalar, soxta to‘lov kartalarini yaratish yoki ulardan foydalanish, karta taqdim etmasdan bank hisob varag‘i ma’lumotlarini olish va noqonuniy foydalanish, shuningdek, karta egasi tomonidan sodir etilgan jinoyatlar bilan bog‘liq.

Kiberjinoyatlarning yana bir turi inson va fuqorolarning huquqlariga va erkinliklariga qaratilgan jinoyatlar - “kompyuter qaroqchiligi”dir. Ushbu jinoyatlar dasturiy ta’minotni noqonuniy nusxalash, ishlatish va tarqatishda namoyon bo‘ladi. Bu dasturiy ta’minot va ma’lumotlar bazasini yaratish bilan bog‘liq huquqiy munosabatlarga (mualliflik huquqiga) jiddiy zarar yetkazadi. Bundan tashqari, dasturiy ta’minot kompaniyalariga katta moliyaviy yo‘qotishlarni olib keladi.

“Microsoft Armaniston” kompaniyasining direktori Grigor Barsegyanning ta’kidlashicha, “kompyuter qaroqchiligi” ning ishlab chiqaruvchilarga yetkazgan zarari yiliga 66 milliard dollarni tashkil etgan. Uning so‘zlariga ko‘ra Armanistonlik iste’molchilar, o‘zlarining moliyaviy resurslarini tejash maqsadida, viruslarni yuqtirish xavfi yuqori bo‘lgan dasturlardan ongli ravishda foydalanganlar.

Kompyuter jinoyatchiligining oxirgi turi - jamoat yoki davlat xavfsizligiga qarshi kompyuter jinoyatchiligi, ularga davlat yoki jamoat xavfsizligiga qaratilgan xavfli xatti - harakatlar taalluqli. Ular ko‘pincha ma’lumot uzatish qoidalarining, mamlakat mudofaa tizimining yoki uning tarkibiy qismlarining buzilishi bilan bog‘liq.

Nazorat savollari:

1. Ichki va tashqi tahdidlar o‘rtasidagi farqni tushuntirib bering.
2. Tashqi kiberjinoyatlar qanday amalga oshiriladi?
3. Ichki kiberjinoyatlar nimalardan iborat?
4. “Kompyuter qaroqchiligi” atamasini tushuntirib bering.

Adabiyotlar va internet saytlari:

1. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoykulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma, – T. “Nihol print” OK, 2021. – 224 b.

2. S.K. Ganiev, Z.T. Xudoykulov, N.B. Nasrullaev. Основы кибербезопасности: Учебное пособие, – T. “Mahalla oila nashriyoti”, 2021. – 224 b.

3. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях - М: ДМК Пресс, 2012. - 596 с.

3-MAVZU. KOMPYUTER VA TARMOQ ARXITEKTURASI (2 soat)

Reja:

3.1. Tarmoqqa oid asosiy tushunchalar, tarmoq turlari.

3.2. Tarmoq xavfsizligiga oid tushunchalar.

3.3. Hujumlarni aniqlash va bartaraf etish vositalari.

Tayanch iboralar: *tarmoq, topologiya, simsiz tarmoq, IDS, IPS, tarmoqlararo ekran, antivirus, VPN, Router.*

Kompyuter tarmoqlari resurslarni almashish maqsadida bir necha kompyuterlarning birlashuvidan iborat. Fayllar, dasturlar, printerlar, modemlar va har qanday tarmoq uskunasi birgalikda foydalaniluvchi yoki taqsimlanuvchi resurslar bo‘lishi mumkin. Kompyuterlarni birlashtirish uchun ma’lumotlarni uzatuvchi turli xil vositalardan foydalaniladi: aloqa kanallari, telekommunikatsiya vositalari, retranslyatorlar va h.

Mos tarmoq servislaridan foydalanish orqali turli xil tarmoq resurslarini taqdim etish vazifasi yuklatilgan tarmoq kompyuteri server deb ataladi. Tarmoq resurslaridan va turli tarmoq servislaridan foydalanish maqsadida serverga so‘rov yuboruvchi tarmoq qurilmalari mijozlar deb ataladi. Avtonom ishlovchi yoki mijoz sifatida tarmoqqa ulangan kompyuterni, odatda, ishchi stansiyasi deb atashadi.

Kompyuter tarmoqlarini quyidagicha tasniflash mumkin:

- hududiy alomat bo‘yicha;
- ma’murlash usuli bo‘yicha;
- topologiya bo‘yicha.

Hududiy alomat bo‘yicha lokal (LAN, Local Area Network) va global (WAN, Wide Area Network) hisoblash tarmoqlari farqlanadi.

Lokal hisoblash tarmog‘i katta bo‘lmagan hududda, xonada yoki binoda joylashgan kompyuter tarmog‘idan iborat. Lokal tarmoq o‘lchami tarmoq texnik arxitekturasi va ulash xiliga (kabel turiga) bog‘liq. Odatda lokal hisoblash tarmog‘ining diametri 2,5 km. dan oshmaydi.

Global hisoblash tarmog‘i katta geografik muhitni qamrab olgan va tarkibida

aloqaning magistral liniyalari yordamida birlashtirilgan ko‘plab hisoblash tarmoqlari va masofadagi kompyuterlar bo‘lgan hududiy taqsimlangan tizimdan iborat. Megapolis va region doirasida tashkil etilgan tarmoqlar mos holda shahar tarmog‘i (MAN, Metropolitan Area Network) va regional tarmoq (PAN, Personal Area Network) deb yuritiladi. Eng mashhur global tarmoq Internet TCP/IP protokollari steki bazasiga asoslangan megatarmoq hisoblanadi. Ba’zi adabiyotlarda “korporativ tarmoq” iborasi ishlatiladi. Bu ibora orqali turli texnik, dasturiy va informatsion prinsiplarda qurilgan bir necha tarmoqlarning birlashmasi tushuniladi.

Megatarmoq Internet foydalanuvchilarini birlashtirish uchun ishlatiluvchi global tarmoq Ekstranet (extranet) deb yuritiladi. TCP/IP protokoli bazasida amalga oshirilgan, ammo megatarmoq Internetdan ajratilgan tarmoq Intranet (Intranet) deb ataladi.

Ma’murlash usuli bo‘yicha tarmoqlar “bir rutbali (одноранговый)” va “mijoz serverli” turlariga bo‘linadi. Bir rutbali tarmoqlarda barcha kompyuterlar ham mijoz, ham server bo‘lishi mumkin. UNIX tarmoqlari bunga misol bo‘ladi.

Mijoz-server texnologiyasi bo‘yicha qurilgan tarmoqlarda maxsus ajratilgan server mavjud. Ajratilgan serverlarga quyidagilar misol bo‘la oladi: fayl server, bosma server, ilovalar serverlari.

Ro‘yxatga olish serverlari (domenlar kontrollerlari), web serverlar, elektron pochta serverlari, masofadan foydalanish serverlari, terminal serverlar, telefon serverlar, proksi serverlar va h.

“Mijoz-server” tarmoqlarida markazlashgan arxitektura hisobiga ma’murlash va masshtablash funksiyalarini, xavfsizlikni va tiklanishni ta’minlash osongina amalga oshiriladi. Ammo, bunday tarmoqlarning zaif joyi (barcha markazlashgan tizimlardagi kabi) server hisoblanadi. Serverning buzilishi butun tizimning ishdan chiqishiga olib keladi. Undan tashqari, “mijoz-server” tarmoqni qurish uchun serunum kompyuter va mos operatsion server muhiti talab etiladi. Mos holda, bunday tarmoqlar professional tarmoq ma’muriga ega bo‘lishi shart.

Tarmoq topologiyasi bo‘yicha umumiy shinali (bus), xalqasimon (ring),

yulduzsimon (star), uyali (mesh) va aralash topologiyali tarmoqlar farqlanadi.

Simsiz tarmoq turlari. Ma’lumki, radio ixtiro etilganidan so‘ng, ko‘p o‘tmay telegraf aloqani simsiz amalga oshirish imkoniyati paydo bo‘ldi. Aslida, hozirgi raqamli kodni radiokanal bo‘yicha uzatishda o‘sha prinsipdan foydalanishadi, ammo ma’lumotlarni uzatish imkoniyati bir necha bor oshdi.

Zamonaviy simsiz tarmoqlarni ta’sir doirasi va vazifasi bo‘yicha quyidagilarga ajratish mumkin:

- shaxsiy (Wireless Personal Area Network, WPAN);
- lokal (Wireless Local Area Network, WLAN);
- shahar (Wireless Metropolitan Area Network, WMAN);
- global (Wireless Wide Area Network, WWAN).

Tarmoqqa qo‘yiladigan talablar:

− ochiqlilik – tarmoqning mavjud komponentlarining texnik va dasturiy vositalarini o‘zgartirmay qo‘shimcha abonent kompyuterlarini hamda aloqa liniyalarini (kanallarini) kiritish imkoniyati;

− moslashuvchanlik – kompyuterni yoki aloqa liniyalarini ishdan chiqishi natijasida struktura o‘zgarishining ishga layoqatlikka ta’sir etmasligi;

− samaradorlik – kam sarf-xarajat evaziga foydalanuvchilarga xizmat qilishning talab etiladigan sifatini ta’minlash.

Tarmoq – turli uskunalarning birlashmasi, demak ularni birgalikda ishlatish muammosi jiddiy muammolardan hisoblanadi. Ishlab chiqaruvchilarning uskuna qurilishidagi umumiy qoidalarga rioya qilmaslaridan turli tarmoqlarni qurishda taraqqiyotga erishish mumkin emas. Shu sababli kompyuter sohasidagi yuksalishlar standartlarda akslanadi. Boshqacha aytganda, har qanday texnologiya, uning mazmuni standartlarda o‘z aksini topganidagina “qonuniy” himoyaga ega bo‘ladi.

1980 – yilning boshlarida standartlash bo‘yicha qator tashkilotlar tomonidan yaratilgan model tarmoqlar rivojida muhim rol o‘ynadi. Bu model ochiq tizimlarning o‘zaro aloqa modeli (Open System Interconnection) yoki OSI modeli deb yuritiladi. OSI modeli tizimlarning o‘zaro aloqasining turli sathini belgilaydi,

ularga standart nomlar beradi va har bir sathning qanday vazifalarni bajarishini ko‘rsatadi. Ushbu modelning talablariga muvofiq tarmoqning har bir tizimi ma’lumotlar kadrini uzatish orqali o‘zaro aloqada bo‘lishlari lozim.

OSI modeliga binoan kadrlarni hosil qilish va uzatish 7 ta ketma-ket harakatlar yordamida amalga oshiriladi. Bu harakatlar “ishlash sathlari” nomini olgan.

Hozirda tarmoq xavfsizligini ta’minlovchi vositalarga tarmoqdan foydalanishni cheklashning bazaviy vositalari (tarmoqlararo ekran) va ma’lumotlarni himoyalangan holda uzatish vositalari (kriptoshlyuzlar va VPN yechimlar), hamda himoyalanganlikni ta’minlovchi qo‘shimcha tarmoq vositalari, trafikni monitoringlash vositalari, yolg‘on tarmoq nishonlari va h. taalluqli.

Tarmoqlararo ekranlash. Tarmoqlararo ekran (firewall, brandmaver) – trafikni filtrlash mexanizmiga asoslangan tarmoqdan foydalanishni cheklashning bazaviy vositasi. Filtratsiya mexanizmi o‘tuvchi trafikni ma’lum qoidalar (filtrlar) bilan taqqoslashni va tarmoq paketlarini o‘tkazish yoki o‘tkazmaslik xususida qaror qabul qilishni ko‘zda tutadi.

Tarmoqlararo ekranlarni, odatda, ishlatiladigan filtrlash texnologiyasiga va OSI modelining bazaviy sathiga nisbatan tasniflashadi (3.1-jadval).

3.1-jadval.

Tarmoqlararo ekran turlari

OSI modeli sathlari	**Filtratsiya texnologiyalari**	**Tarmoqlararo ekran turlari**
Tatbiqiy sath	Proksi	Tatbiqiy vositachi
Seans sathi	Proksi	Seans vositachisi
	Paketlar inspektori	Holat inspektori
	Paketlar filtrasiyasi	Dinamik filtr
Tarmoq sathi	Paketlar filtrasiyasi	Ekranlovchi marshrutizator, paket filtri
Kanal sathi	Trafikni segmentlash	Boshqariluvchi (ekranlovchi) kommutator

Kanal sathida ishlatiluvchi boshqariluvchi kommutatorlar, masalan, MAC-adreslar, portlar va kadrlar sarlavhalaridan olingan boshqa parametrlar asosida, trafikni filtrlash vazifasining bajarilishiga imkon beradi. Boshqariluvchi

kommutatorlarning afzalligi sifatida tarmoq qurilmalari guruhini ma’murlashning qulayligini, lokal tarmoq unumdorligining oshishini ko‘rsatish mumkin.

Funksionallikning cheklanganligi, fizik rekonfiguratsiyalashning noqulayligi va MAC-adresni almashtirish hujumiga zaifligi boshqariluvchi kommutatorlarning kamchiligi hisoblanadi.

Tarmoq sathining paket filtrlari va marshrutizatorlar IP-adres, portlar, protokol turi va h. bo‘yicha filtrlash vazifasining bajarilishiga imkon beradi. Tarmoq va transport sathlari funksionalliklarining cheklanganligi va IP-adresni almashtirish hujumiga zaifligi paket filtrlarining kamchiligi hisoblanadi.

Seans sathining paket filtrlari, seansga mos filtrlash parametrlarining katta sonini hisobga olgan holda, filtrlashni bajarishga imkon beradi.

Vositachilar - oraliq tarmoq vositalari o‘ziga tegishli ulanishni amalga oshirib, trafikni qo‘shimcha qurilmada ishlaydi. Bu o‘z navbatida quyidagi vazifalarni bajarishga imkon beradi:

- autentifikatsiyani;
- mijozlar va serverlarning asinxron muloqotini;
- adreslarning translyatsiyasini va yashirishni;
- tarmoq yukini qayta taqsimlash maqsadida adresni o‘zgartirishni;
- almashish unumdorligini oshirish maqsadida xeshlashni;
- trafikni qaydlashni.

Ayni paytda, vositachilardan foydalanilganda, trafik qo‘shimcha qurilmada takroriy ishlangani sababli, tarmoq perimetri bo‘yicha istalgan unumdorlikni ta’minlash masalasini yechish talab etiladi.

Vositachi tomonidan amalga oshiriluvchi marshrutlash texnologiyasiga alohida e’tibor berish lozim. Unga binoan tarmoq adreslarining translyatsiyasi (Network Address Translation, NAT) amalga oshiriladi, ya’ni hostning ichki adresi vositachining shaxsiy adresiga almashtiriladi. Boshqacha aytganda, NAT ichki tarmoq adreslarini tashqi tomondan yashirish siyosatini amalga oshiradi va ichki tarmoq uchun vositachiga bitta IP-adresni belgilash imkoniyatini yaratadi. Adreslarni translyatsiyalash statik va dinamik tarzda belgilanishi mumkin.

Seans sathidagi vositachilarga, yuqori unumdorlikka, adreslarni yashiruvchi samaradorli apparatga va TCP/UDP – trafikni ajratish imkoniyatiga ega SOCKet Secure (SOCKS5) vositachisi taalluqli. Tatbiqiy vositachi sifatida HTTP/HTTPS vositachilari va FTP vositachi keng tarqalgan. Ushbu vositachilar tatbiqiy protokol kontenti bo‘yicha filtrlashga imkon tug‘diradi.

Holat inspektorlari (seans sathining imkoniyati kengaytirilgan filtrlari), seans sathidagi protokollar sarlavhalaridan olinuvchi ma’lumotlar asosida, intelektual filtrlashni bajaradi. Bu yuqori sathlarda filtrlash effektini olishga imkon beradi. Bunday tarmoqlararo ekranlar vositachini o‘rnatishni talab qilmaydi. Shu sababli, tarmoq unumdorligi pasaymaydi, ammo xavfsizlikning kerakli darajasi ta’minlanadi. Holat inspektorining afzalligiga masshtablashning qulayligini ham qo‘shish mumkin.

Amaliyotda axborot resurslarining tarmoqlararo himoyasini ta’minlashda UTM (Unifield Threat Management) qurilma tushunchasini va keyingi avlod tarmoqlararo ekranlarini (Next Generation, NG firewall) uchratish mumkin.

UTM – qurilma perimetrli himoyalash masalasining kompleks yechimi hisoblanadi. Uning tarkibida tarmoqlararo ekranlash modullaridan tashqari, suqilib kirishlarni aniqlash tizimlari, oqimli antivirus, spamga qarshi yechim, kriptoshlyuz va h. mavjud bo‘lishi mumkin.

NG firewall UTMga o‘xshash va portlar bo‘yicha filtrlash texnikasini, suqilib kirishlardan ogohlantirish tizimlarini va ilovalar sathida trafikni filtrlashni birlashtirish maqsadida yaratilgan.

Virtual xususiy tarmoqlar. Virtual xususiy tarmoq (Virtual Private Network, VPN) deganda ma’lumotlarni inkapsulyatsiyalash mexanizmlari, hamda qo‘shimcha autentifikatsiya, shifrlash, yaxlitlikni nazoratlash bazasida vaqtinchalik himoyalangan aloqa kanalini yaratish yo‘li bilan uzatiluvchi ma’lumotlarni himoyalash vositasi tushuniladi. Nomidan ko‘rinib turibdiki, VPNning asosiy g‘oyasi vaqtinchalik (seans davrida) ma’lumotlarni uzatish uchun inkapsulyatsiyalash, ya’ni bir sathning tarmoq paketini yuqori sathning yagona paketiga birlashtirish yo‘li bilan himoyalangan tunnelni yaratishdan iborat. Aynan,

doimiy himoyalangan kanalni yoki ajratilgan liniyani ijaraga olishni tashkil etish oldida, vaqtinchalik tunnelni tashkil etish imkoniyatining afzalligi namoyon.

Ma’lumotlar paketining yuqori sath paketiga inkapsulyatsiyasi esa ma’lumotlarni shifrlash va ularning yaxlitligini nazoratlash talablarini osongina qondirishga imkon beradi.

Virtual xususiy tarmoqlarni, asosan OSI-modeli sathlari va ulanish usullari bo‘yicha tasniflash qabul qilingan. Ulanish bo‘yicha “nuqta-nuqta” (“uzel-uzel”), “nuqta-tarmoq” va “tarmoq-nuqta” usullari farqlanadi.

PPTP (Point-to-Point Tunneling Protocol) – “nuqta-nuqta” xilidagi kanal sathining tunnel protokoli. Ushbu protokol, tunnelga xizmat qilish uchun, qo‘shimcha TCP-ulanish yordamida PPP-kadrlarni IP-paketlarga inkapsulyatsiyalaydi.

Mijozlarni autentifikatsiyalash uchun masofaviy foydalanishning turli protokollarini, jumladan MSCHAPv2 protokolini, madadlaydi. Shifrlashda RC4 algoritmni amalga oshiruvchi MPPE protokol madadlanadi.

L2TP (Layer 2 Tunneling Protocol) – PPP-kadrlarni tarmoq sathi paketlariga inkapsulyatsiyalovchi kanal sathining tunnel protokoli. Protokolning afzalligi sifatida foydalanish ustuvorliklarini va multi protokollikni (nazariy jixatdan Ipga bog‘liq emaslikni) madadlashini ko‘rsatish mumkin. Shifrlash mexanizmi o‘zidan yuqori sathga ishonib topshiriladi, masalan IPSec apparat yordamida amalga oshirilishi mumkin. PPTPdan farqli holda, TCP/IP tarmoqlarida ushbu protokol transport protokoli UDPga moslangan.

IPSec (IP Security) protokoli ikkita rejimda – transport va tunnel rejimida ishlaydi. Transport rejimida (ushbu rejim hostlar orasidagi ulanishlarni o‘rnatishda ishlatiladi) IPSecdan, qandaydir boshqa usul, xususan, shifrlash funksiyasi bo‘lmagan L2TP tomonidan tashkil etilgan “nuqta-nuqta” xilidagi tunnellarni himoyalashda foydalanish mumkin. Tunnel rejimi shunday tunnelarni yaratishga imkon beradiki, shifrlangan butun paket (transport rejimidan farqli holda, butun paket sarlavhasi bilan shifrlangan) adresatga yetkazish uchun yuqori sathga inkapsulyatsiyalanadi.

Tarmoq xavfsizligini ta’minlovchi qo‘shimcha vositalar.

Suqilib kirishlarni aniqlash tizimlari (Intrusion Detection System, IDS). IDSning asosini tarkibida mos shablonlar, signaturalar yoki profillar bo‘lgan hujumlarning ma’lumotlar bazasi tashkil etadi va aynan ushbu baza bilan sensorlardan olingan ma’lumotlar taqqoslanadi. Shu sababli, IDSning samaradorligi hujumlarning ma’lumotlar bazasining nufuziga bog‘liq. Suqilib kirishlarni aniqlashda quyidagi usullardan foydalanish mumkin:

− signatura usuli – qandaydir hujumga xarakterli ma’lumotlar nabori bo‘yicha suqilib kirishlarni aniqlash;

− anomallarni aniqlash usuli –normal holatiga harakterli bo‘lmagan alomatlarni aniqlash;

− xavfsizlik siyosatiga asoslangan usul – xavfsizlik siyosatida belgilangan parametrlarning buzilganligini aniqlash.

Monitoring darajasi bo‘yicha IDS – tizimlar quyidagilarga bo‘linadi:

− tarmoq sathi IDSi (Network based IDS, NIDS);

− uzel sathi IDSi (Host based IDS, HIDS).

NIDS tarmoq segmentiga ulangan bir necha xostlardan keluvchi tarmoq trafigini monitoringlash orqali ushbu xostlarni himoyalashi mumkin. HIDS yagona kompyuterda yig‘ilgan, asosan operatsion tizimning va axborotni himoyalash tizimining jurnallaridan, foydalanuvchi profilidan va h. yig‘ilgan, axborot bilan ish ko‘radi. Shu sababli NIDSdan kompyuter hujumlarini oldinroq aniqlashda foydalanish qulay hisoblansa, HIDSdan ruxsatsiz foydalanishning ishonchli faktini qaydlashda foydalaniladi.

IDSning aktiv (in-line) xili suqilib kirishlarni ogohlantirish tizimi (Intrusion Prevention System, IPS) deb ataladi.

Himoyalanganlikni tahlillash vositalari. Texnik audit bo‘yicha mutaxassislar bo‘lishi mumkin bo‘lgan va real zaifliklarni aniqlashda turli himoyalanganlikni tahlillash vositalaridan foydalanishadi. Himoyalanganlikni tahlillash vositalarining quyidagi sinflari mavjud:

− zaifliklarning tarmoq skanerlari;

− web-ilovalar xavfsizligining skanerlari;

− tizim konfiguratsiyasini tahlillash vositalari;

− testlashning maxsus vositalari.

Zaifliklarning tarmoq skanerlari maxsus dasturiy vositalar bo‘lib, undagi kirish axboroti sifatida skanerlanuvchi IP-adreslarning ro‘yxati, chiqish axboroti sifatida esa aniqlangan zaifliklar xususidagi hisobot ishtirok etadi. Asosiy ishlash prinsipi – masofadagi uzelda o‘rnatilgan dasturiy ta’minotning aniq versiyasini aniqlash va zaifliklarning yangilanuvchi lokal bazasiga dasturiy ta’minotning ushbu versiyasi uchun xarakterli zaifliklar xususidagi axborotni qidirish.

Web-ilovalar xavfsizligining skanerlari maxsus dasturiy vositalar bo‘lib, web-tizimlar strukturasini tahlillaydi. Natijada axborotni kiritishning bo‘lishi mumkin bo‘lgan variantlari aniqlanadi va zaiflikdan foydalanish maqsadida so‘rov shakllantiriladi.

Tizim konfiguratsiyasini tahlillash vositalari - tizim himoyalanganligini uning sozlanishi bo‘yicha baholovchi dastur. Bu xil yechim kompleks mahsulot yoki lokal skript (senariy) sifatida ifodalanishi mumkin.

Testlashning maxsus vositalari:

− parollarni online va offline saralash dasturlari;

− zaifliklardan foydalanish freymworklari;

− ma’lum tarmoq hujumlarini amalga oshiruvchi dasturlar (masalan, ARP-spoofing);

− web-serverga uzatiluvchi HTTP so‘rovlarni o‘zgartirish uchun loakl HTTP proksilar va h.

Zaifliklarning turli onlayn – bazalari mavjud. CVE (Common Vulnerabilities and Exposures, cve.mitre.org) zaifliklar bazasi mashhur.

Ma’lumotlarning sirqib chiqishini oldini olish tizimlari (Data Leakage Prevention, DLP). Ushbu tizimlardan, tarkibida tijoriy, kasbiy yoki boshqa turdagi sir bo‘lgan ma’lumotlarning noqonuniy tarzda tashqi tarmoqqa jo‘natilishini aniqlashda va blokirovkalashda foydalaniladi. DLP tizimlar ulanish sxemasi bo‘yicha IDS – yechimlarga o‘xshash – tahlillanuvchiaxborottarmoqsathida

yokihostsathidayig‘ilishi mumkin. Axborot oqimlarini, ularda konfidensial axborotning mavjudligini aniqlash maqsadida, nazoratlashning ikkita usuli qo‘llaniladi:

- hujjatda berilgan belgilar bo‘yicha aniqlash;
- ma’lumotlar nabori kontenti bo‘yicha aniqlash.

Birinchi usul bo‘yicha axborotni dastlabki kategoriyalash va markirovkalash amalga oshiriladi. Bunda konfidensial hujjatga (masalan, faylga, ma’lumotlar bazasi yozuviga va h.) qandaydir ajralmaydigan formal alomat (masalan, nazorat yig‘indisi, inventar nomeri, konfidensiallik grifi) moslashtiriladi. So‘ngra, uzatiluvchi axborot oqimida ushbu alomat aniqlansa, mos hujjat blokirovkalanadi.

Bunday yondashish hujjatni faqat butunligicha himoyalashga qodir. Yondashishning afzalligi sifatida huquqiy risklarning pasayishini va turli xil yolg‘on nishonlar ishlashi darajasining yuqori emasligini ko‘rsatish mumkin.

Yolg‘on nishonlar yoki tuzoqlar (honeypot). Tarmoq xavfsizligini ta’minlovchi ushbu vositadan niyati buzuq tomonidan yolg‘on nishonlarni aniqlash, hamda buzib ochish usullarini tadqiqlash maqsadida hujumni yuzaga keltirishga urinishda foydalaniladi.

Yolg‘on nishonlarni tasniflashda alomat sifatida ularning interaktivligi ishlatiladi, ya’ni quyidagi tuzoqlar farqlanadi:

- interaktiv tuzoqlar;
- interaktivlik darajasi past tuzoqlar;
- interaktivlik darajasi yuqori tuzoqlar.

Interaktivlik darajasi past tuzoqlar bitta tarmoq servisining, masalan, FTP-servisning emulyatsiyasi bo‘lishi mumkin. Joylashtirilishining va nazoratlanishining osonligi bunday tuzoqlarning afzalligi hisoblansa, kamchiligi sifatida ular yordamida ko‘pincha faqat hujum faktining aniqlanishini ko‘rsatish mumkin.

Interaktivlik darajasi yuqori tuzoqlarni to‘laqonli operatsion tizimga va servislar naboriga ega virtual mashina sifatida tasavvur etish mumkin. Bunday tuzoqlar niyati buzuq xususida ancha ko‘p axborotni yig‘ishga imkon beradi

(ayniqsa, u bilan intellektual teskari bog‘lanish tashkil etilgan bo‘lsa).

Ta’kidlash lozimki, IDS va DLP – yechimlar hujumlarning ma’lum sinfiga mo‘ljallangan. Amaliyotda axborot tizimi ishlashidagi har qanday xavfsizlik va ishonchlik hodisalarni yig‘ish masalasi paydo bo‘ladi. Bunday tizimlarga quyidagilar taaluqli:

- jurnallarni boshqarish tizimlari (log management). Ushbu tizimlar axborot xavfsizligi hodisalarini markazlashgan tarzda yig‘ishni tashkil etish uchun mo‘ljallangan;
- xavfsizlik xususidagi axborotni boshqarish tizimlari (Security Information Management, SIM). Ushbu tizimlar axborot xavfsizligi hodisalarini markazlashgan tarzda yig‘ishga, hamda turli hisobotlarni shakllantirishga va tahlillashga mo‘ljallangan;
- xavfsizlik hodisalari hususidagi axborotni boshqarish tizimlari (Security Event Manager, SEM). Ushbu tizimlar vaqtning real rejimida monitoringlashga, axborot xavfsizligi hodisalarini korrelyatsiyalashga mo‘ljallangan;
- xavfsizlik va xavfsizlik hodisalari xususidagi axborotni boshqarish tizimlari (Security Information and Event Management, SIEM). Ushbu tizimlar monitoring tizimlari rivojining keyingi qadami hisoblanadi, chunki SEM va SIM funksionalliklarini kombinasiyalaydi.

Nazorat savollari

1. Kompyuter tarmog’i nima?
2. Qanday kompyuter tarmog’i turlari bor?
3. Tarmoqda xavfsizlikni ta’minlash qanday amlaga oshiriladi?
4. Tarmoqni himoyalash qurilmalariga misollar keltiring.
5. Hujumlarni aniqlash va bartaraf etishni qanday vositalarini bilasiz?

Foydalanilgan adabiyotlar va internet saytlar:

1. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoykulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma, – T. “Nihol print” OK, 2021. – 224 b.

2. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях

- M: ДМК Пресс, 2012. - 596 с.

4-MAVZU: IJTIMOIY INJINERIYA (2 soat)

Reja:

4.1. Ijtimoiy injineriya va uni hozirgi kiberjinoyatchilikdagi ahamiyati. Soxta veb saytlar, fishing elektron xabarlar.

4.2. Fishing va uning koʻrinishlari. Ijtimoiy injineriyaga real misollar. Ijtimoiy injineriyadan himoyalanish usullari.

Tayanch iboralar: *Ijtimoiy injineriya, fizik xavfsizlik, ma'lumotla, ilovalar, kompyuterlar, ichki tarmoq, tarmoq perimetri, fishing.*

Ijtimoiy (sotsial) injineriya - turli psixologik usullar va firibgarlik amaliyotining toʻplami, uning maqsadi firibgarlik yoʻli bilan shaxs toʻgʻrisida maxfiy ma'lumotlarni olish. Maxfiy ma'lumotlar – foydalanuvchi ismi/parollari, shaxsiy ma'lumotlari, ayblov dalillari, bank karta raqamlari va moliyaviy yoki obroʻsini yoʻqotadigan har qanday ma'lumot.

Mazkur atama xakerlik sohasidan kirib kelgan, xaker - kompyuter tizimidagi zaifliklarni qidiradigan odam,boshqacha aytganda "buzgʻunchi". Hozirgi vaqtda xakerlar har qanday tizimdagiasosiy zaiflik - mashina emas, balki shaxs ekanligini yaxshi tushunishadi. Inson, xuddi kompyuter singari, muayyan qonunlarga muvofiq ishlaydi. Psixologiya, hiyla-nayranglar va ta'sir mexanizmlari doirasida insoniyat tomonidan toʻplangan tajribadan foydalangan holda, xakerlar "odamlarga hujum qilishni" boshlaydilar. Gohida ularni "aql xakerlari" deb ham atashadi.

Masalan, xaker sizdan pul olmoqchi deb faraz qilaylik. Aytaylik, u sizning telefon raqamingiz va ijtimoiy tarmoqdagi akkauntingiz haqida ma'lumotga ega. Bundan tashqari, u izlanish natijasida sizning akangiz borligini ham aniqladi va akangiz haqida ham yetarlicha ma'lumot toʻpladi. U shuningdek, akangizning telefon raqamini ham biladi. Shundan soʻng, ushbu ma'lumotlar asosida oʻz rejasini tuza boshladi.

Reja: Xaker sizga kechki vaqtda telefon qilib, sizga (sizni ismingiz oʻrniga faqat akangiz ataydigan biror “laqab” ham boʻlishi mumkin) men akangman deb tanishtiradi va oʻzini koʻchada bezorilarga duch kelganini, ular barcha narsalarini (telefon, pul, plastik kartochka va h.) olib qoʻyganini aytadi.

Bundan tashqari, u oʻziga bir qiz yordam berganini, biroq, uning yonida puli yoʻqligini aytadi. Shu bilan birga, ushbu qizni yonida plastik kartasi borligini va sizdan ushbu plastik kartaga kasalxonaga yetib borish uchun zarur boʻlgan 20 000 soʻm pulni koʻchirib berishni talab qiladi. Mazkur holatlarning 80% da xakerlar muvaffaqqiyatga erishganlar va bu ishlarni amalga oshirish malakali xaker uchun qiyinchilik tugʻdirmaydi.

Mazkur holda akangizni ovozini ajratish imkoniyati haqida gap borishi mumkin. Biroq, inson turli hayojon va shovqin boʻlgan muhitda boʻlishi mumkin. Bundan tashqari, agar siz uxlab yotgan vaqtingizda telefon boʻlsa, ovozni aniqlashingiz yanada qiyinlashadi.

Ushbu holatda xaker tomonidan foydalanilgan fikrlarni koʻrib chiqaylik:

1. Shaxsini yaxshi yashirgan va real misollarga asoslangan (masalan, sizning rasmlaringiz, faqat sizning yaqinlaringiz biladigan joylar va h.) va yaxshi afsona oʻylab topdi.

2. Bularning barchasi yetarlicha tez va ishonchli tarzda aytilgan.

3. Ta’sirning juda ishonarli mexanizmidan foydalanilgan – achinishga majbur qilingan (hissiyotlarga murojaat qilish).

Sotsial injineriya bilan bogʻliq tahdidlarni quyidagicha tasniflash mumkin:

Telefon bilan bogʻliq tahdidlar. Telefon hanuzgacha tashkilotlar ichida va ular oʻrtasidagi aloqaning eng keng tarqalgan usullaridan biri hisoblanadi. Shuning uchun, u sotsial injineriya uchun samarali vosita boʻlib qolmoqda. Telefonda gaplashayotganda, suhbatdoshining shaxsini tasdiqlashning imkoni yoʻq. Bu hujumchilarga xodimning, xoʻjayinning maxfiy yoki muhim tuyuladigan ma’lumotlarga ishonishi mumkin boʻlgan har qanday shaxsning oʻrnida boʻlish imkonini beradi. Bunda, zoʻravonlik qurbonining “yordam berishdan” boshqa

imkoni qolmaydi. Hattoki, uyushtiriladigan suhbat ahamiyatsiz bo‘lib ko‘ringan taqdirda ham.

Uyali telefondan foydalanuvchilarni pul o‘g‘irlashga qaratilgan firibgarlikning turli usullari mavjud. Bunga qo‘ng‘iroqlar yoki lotereyalardagi yutuqlar, SMS-xabarlar, xatoliklar orqali pulni qaytarish to‘g‘risidagi so‘rovlar yoki jabrlanuvchining yaqin qarindoshlari muammoga duch kelganligi hamda ma’lum miqdordagi pulni zudlik bilan o‘tkazish kerakligi haqidagi xabarlarni keltirish mumkin.

Mazkur hollarda quyidagi xavfsizlik choralarini amalga oshirish talab etiladi:

- telefon qiluvchining shaxsini aniqlash;
- raqamni aniqlash xizmatidan foydalanish;
- SMS – xabardagi noma’lum havolalarga e’tibor bermaslik. Elektron pochta bilan bog‘liq tahdidlar. Ko‘pgina xodimlar har kuni korporativ va shaxsiy pochta tizimlaridan o‘nlab, hatto yuzlab elektron pochta xabarlarini qabul qilishadi. Albatta, bunday yozishmalar oqimining har bir harfiga yetarlicha e’tibor berishning imkoni yo‘q. Bu esa hujumlarni amalga oshirishni sezilarli darajada osonlashtiradi. Elektron pochta tizimlarining ko‘plab foydalanuvchilari bunday holni bir papkadan ikkinchisiga qog‘ozlarni o‘tkazishning elektron analogi sifatida qabul qilishadi va xabarlarni qabul qilishda xotirjam bo‘lishadi. Tajovuzkor pochta orqali oddiy so‘rov yuborganida, uning qurboni ko‘pincha uning xatti-harakatlari haqida o‘ylamasdan ular so‘ragan ishni bajaradi. Elektron pochtalarda xodimlarni korporativ atrof-muhit muhofazasini buzishga undaydigan giperhavolalar bo‘lishi mumkin. Bunday havolalar har doim ham da’vo qilingan sahifalarga murojaat qilmaydi.

Xavfsizlik choralarining aksariyati ruxsatsiz foydalanuvchilarning korporativ resurslardan foydalanishinioldiniolish uchunishlab chiqilgan. Buzg‘unchi tomonidan yuborilgan giperhavolaga murojaat orqali foydalanuvchining zararli dasturni korporativ tarmoqqa yuklashi ko‘plab himoya turlarini chetlab o‘tishga imkon beradi. Giperhavola, shuningdek, ma’lumot yoki yordamni talab qiladigan qalqib chiquvchi ilovalar bilan turli xostlarga murojaatni talab qilishi mumkin.

Firibgarlikni va zararli hujumlarni oldini olishning eng samarali usuli kutilmagan foydalanuvchining elektron pochtasi xabarlariga shubha bilan qarash. Ushbu yondashuvni butun tashkilotda tarqatish uchun xavfsizlik siyosatida belgilangan elektron pochtadan foydalanishning quyidagi elementlari kiritilishi kerak:

- hujjatlarga qo‘shimchalar;
- hujjatdagi giperhavolalar;
- shaxsiy yoki korporativ ma’lumotlarni kompaniya ichida so‘rash;
- shaxsiy yoki korporativ ma’lumotlarga kompaniya tashqarisidan keladigan so‘rovlar.

Tezkor xabarlardan foydalanishga asoslangan tahdidlar. Tezkor xabaralmashish - ma’lumotlarniuzatishning nisbatan yangiusuli. Ammo, u korporativ foydalanuvchilar orasida allaqachon mashhurlikka erishgan. Foydalanishning tezligi va qulayligi tufayli ushbu aloqa usuli turli xil hujumlar uchun keng imkoniyatlarni ochib beradi. Foydalanuvchilar unga telefon kabi qarashadi va uni bo‘lishi mumkin bo‘lgan dasturiy tahdidlar sifatida baholashmaydi. Tezkor xabarlar xizmatidan foydalanishga asoslangan hujumlarning ikkita asosiy turi - zararli dasturga havola va dasturning o‘zi haqida xabarning ko‘rsatilishi hisoblanadi. Tezkor xabarlar xizmatlarining xususiyatlaridan biri - aloqaning norasmiyligi, unda har qanday nomlarni moslashtirish qobiliyati bilan bir qatorda, bu omil tajovuzkorni o‘zini boshqa odam bo‘lib ko‘rsatishiga imkon beradi. Bu esa muvaffaqiyatli hujum qilish ehtimolini sezilarli darajada oshiradi. Agar kompaniya tezkor xabarlar sababli keladigan xarajatlarni kamaytirish maqsadida boshqa afzalliklardan foydalanmoqchi bo‘lsa, korporativ xavfsizlik siyosatida tegishli tahdidlardan himoya qilish mexanizmlarini ta’minlashi kerak. Korporativ muhitda tezkor xabar almashish ustidan ishonchli boshqaruvga ega bo‘lish uchun quyidagi talablar bajarilishi shart:

- tezkor xabarlar uchun bitta platformani tanlash;
- tezkor xabar yuborish xizmatini o‘rnatishda xavfsizlik sozlamalarini aniqlash;

- yangi aloqalarni o‘rnatish prinsiplarini aniqlash;
- parol tanlash standartlarini o‘rnatish;
- tezkor xabarlardan foydalanish bo‘yicha tavsiyalar berish. Sotsial injineriya mutaxassislari tashkilotlar uchun quyidagi asosiy himoya usullarini qo‘llashni tavsiya etishadi:
- muhim ma’lumotlar ko‘rinishida bo‘lgan, zararsiz ko‘rinadigan ma’lumot turlarini hisobga oladigan ishonchli ma’lumotlarni tasniflash siyosatini ishlab chiqish;
- ma’lumotlarni shifrlash yoki foydalanishni boshqarish yordamida mijoz ma’lumotlari xavfsizligini ta’minlash;
- xodimlarni sotsial injineriya ko‘nikmalariga o‘rgatish, ularni o‘zlari tanimaydigan odamlar bilan muloqotiga shubha bilan qarashni o‘rgatish;
- xodimlar orasida parollarni almashishni yoki umumiy foydalanishni taqiqlash;
- shaxsan tanish bo‘lmagan yoki biron – bir tarzda tasdiqlanmagan shaxsga korxonaga tegishli ma’lumotlarni berishni taqiqlash;
- maxfiy ma’lumotlardan foydalanishni so‘raganlar uchun maxsus tasdiqlash muolajalaridan foydalanish.

Sotsial injineriya hujumlarini oldini olishda ko‘p hollarda kompaniyalar tomonidan murakkab, ko‘p darajali xavfsizlik tizimlari qo‘llaniladi. Bunday tizimlarning ba’zi xususiyatlari va majburiyatlari quyida keltirilgan:

- *Fizik xavfsizlik.* Kompaniya binolari va korporativ resurslardan foydalanishni cheklaydigan to‘siqlar. Unutmaslik kerakki, kompaniyaning resurslari, masalan, kompaniya hududidan tashqarida joylashgan axlat konteynerlari fizik himoyalanmagan.
- *Ma’lumotlar.* Biznes ma’lumotlari: qayd yozuvlari, pochta va boshqalar bo‘lib, tahdidlarni tahlillash va ma’lumotlarni himoya qilish choralarini rejalashtirishda qog‘oz, elektron ma’lumot eltuvchilari bilan ishlash prinsiplarini aniqlash kerak.

- *Ilovalar* - foydalanuvchilar tomonidan boshqariladigan dasturlar. Atrofini himoya qilish uchun elektron pochta dasturlaridan, tezkor xabarlar xizmati va boshqa dasturlardan tajovuzkorlar qanday foydalanishlari mumkinligini koʻrib chiqish kerak.

- *Kompyuterlar*. Korporativ kompyuterlarda qaysi dasturlardan foydalanish mumkinligini koʻrsatadigan qat'iy prinsiplarni belgilash, foydalanuvchilar kompyuterlariga toʻgʻridan-toʻgʻri hujumlardan himoya qilish.

- *Ichki tarmoq.* Korxona tizimlariga ta'sir qiladigan tarmoq, u mahalliy, global yoki simsiz boʻlishi mumkin. Soʻnggi yillarda masofadan ishlaydigan usullarning ommaviylashi sababli, ichki tarmoqlarning chegaralari sezilarli darajada oʻzboshimchalik bilan kengaytirildi. Kompaniya xodimlari har qanday tarmoq muhitida xavfsiz ishlarni tashkil qilishda nima qilish kerakligini tushunishlari lozim.

- *Tarmoq perimetri.* Kompaniyaning ichki tarmoqlari va tashqi, masalan, Internet yoki hamkor tashkilotlar tarmoqlari oʻrtasidagi chegara. Sotsial injineriyaga tegishli koʻplab hujumlar mavjud, quyida ularning ayrimlari keltirilgan:

Fishing. Fishing (ing. Phishing – baliq ovlash) Internetdagi firibgarlikning bir turi boʻlib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan (login/parol) foydalanish imkoniyatiga ega boʻlish. Bu hozirda keng tarqalgan sotsial injineriya sxemalaridan biri hisoblanadi. Katta hajmdagi shaxsiy ma'lumotlarni keng tarqalishi, fishing "shamolisiz" amalgaoshmaydi. Fishingning eng keng tarqalgan namunasi sifatida jabrlanuvchining elektron pochtasiga yuborilgan rasmiy ma'lumot koʻrinishidagi bank yoki toʻlov tizimining soxta xabarini koʻrsatish mumkin. Bunday elektron pochta xabarlari odatda rasmiy web-saytga oʻxshash va shaxsiy ma'lumotlarni talab qiladigan shakldagi qalbaki web sahifaga havolani oʻz ichiga oladi (6.1-rasm).

Rasmda keltirilgan birinchi holatda mijozning yoki foydalanuvchining ismi va familiyasini yozish oʻrniga pochta manzili yozilgan boʻlsa, ikkinchi holatda

ko‘rsatilgan havola ustiga sichqoncha olib borilganida, haqiqiy manzilni (www.PayPal.com) emas, balki, boshqa manzilni ko‘rish mumkin.

4.1-rasm. Fishing hujumiga misol

Quyida keng tarqalgan fishing sxemalariga misollar keltirilgan. Mavjud bo‘lmagan havola. Fishing hujumining mazkur turida biror web saytga o‘xshash web saytga murojaat amalga oshirilishi tavsiya etiladi. Masalan, www.PayPai.com manzilini www.PayPal.com manzili sifatida yuborish mumkin. Bu holda kamdan-kam holda foydalanuvchilar “l” harfini o‘riniga “i” harfi borligiga e’tibor berishadi. Havolaga murojaat qilinganida esa www.PayPal.com web saytga o‘xshash, biroq soxta web saytga tashrif buyuriladi va talab kiritilgan to‘lov kartasi ma’lumotlari kiritiladi. Natijada, kiritilgan ma’lumotlar xaker qo‘liga tushadi.

Bunga yaqqol misol sifatida, 2003 yilda eBay foydalanuvchilariga tarqalgan fishing xabarni keltirish mumkin. Mazkur xabarda foydalanuvchilarning akkauntlari blokirovkalangani va kredit karta ma’lumotlari blokirovkadan chiqarilishi kerakligi keltirilgan va unda rasmiy web-saytga o‘xshash soxta web saytga olib boruvchi havola mavjud bo‘lgan. Ushbu fishing hujumining keltirgan zarari bir necha yuz ming dollarga teng bo‘lgan.

Taniqli korporativ brendidan foydalanishga asoslangan firibgarlik. Firibgarlikning mazkur ko‘rinishida taniqli yoki yirik kompaniyalar nomidan foydalanuvchiga xabar yuboriladi. Xabarda kompaniya tomonidan o‘tkazilgan biror tanlovda g‘alaba qozonilganligi haqidagi tabriklar bo‘lishi mumkin. Unda

shuningdek, zudlik bilan qayd yozuvi ma’lumotlari va parolni o‘zgartirish kerakligi so‘raladi. Shunga o‘xshash sxemalar texnik ko‘maklashish xizmati nomidan ham amalga oshirilishi mumkin.

Soxta lotareyalar. Mazkur fishing sxemasiga ko‘ra foydalanuvchi har qanday taniqli kompaniya tomonidan o‘tkazilgan lotereyada g‘olib bo‘lgani to‘g‘risidagi xabarni olishi mumkin. Tashqi tomondan, bu elektron xabar kompaniyaning yuqori lavozimli xodimlaridan biri nomidan yuborilganga o‘xshaydi.

Soxta antivirus va xavfsizlik dasturlari. Mazkur dasturlar firibgar dasturiy ta‘minoti yoki “chaqqon dastur” deb nomlanib, ular antivirus dasturlariga o‘xshasada, vazifasi boshqacha. Bu dasturiy ta’minot turli tahdidlar to‘g‘risidagi yolg‘on xabarnomalar asosida foydalanuvchini soxta bitimlarga jalb qilishga harakat qiladi. Foydalanuvchi ulardan foydalanganida elektron pochtada, onlayn e’lonlarda, ijtimoiy tarmoqlarda, qidiruv tizimlari natijalarida va hatto foydalanuvchi kompyuterida turli qalqib chiquvchi oynalarga duch kelishi mumkin. Quyida keltirilgan misolda, aslida Microsoft Security Essentials bo‘lishi kerak bo‘lgan, biroq o‘ziga Security Essentials 2010 nomi berilgan soxta antivirus dasturining ko‘rinishi keltirilgan (4.2-rasm).

IVR (Interactive Voice Response) yoki telefon orqali fishing. Fishing sxemasining mazkur usuli oldindan yozib olingan xabarlar tizimidan foydalanishga asoslangan, ular bank va boshqa IVR tizimlarining “rasmiy qo‘ng‘iroqlari”ni qayta tiklash uchun ishlatiladi. Bu hujumda jabrlanuvchi bank bilan bog‘lanib, qandaydir ma’lumotlarni tasdiqlash yoki yangilash kerakligi haqidagi so‘ovni qabul qiladi. Tizim PIN kodni yoki parolni kiritish orqali foydalanuvchi tasdig‘ini talab qiladi. Natijada, muhim ma’lumotlarni qo‘lgan kiritgan buzg‘unchi foydalanuvchi ma’lumotlaridan foydalanish imkoniyatiga ega bo‘ladi. Masalan, parolni almashtirish uchun “1” ni bosing va operator javobini olish uchun “2” ni bosing.

4.2-rasm. “Security Essentials 2010” antivirus dasturi

Preteksting. Mazkur fishing sxemasida xaker o‘zini boshqa shaxs sifatida ko‘rsatadi va oldindan tayyorlangan senariy (skript) bo‘yicha maxfiy axborotni olishni maqsad qiladi. Ushbu hujumda qurbonni shubhalanmasligi uchun tegishli tayyorgarlik ko‘riladi: tug‘ilgan kun, INN, pasport raqami yoki hisob raqamining oxirgi belgilari kabi ma’lumotlar topiladi. Ushbu fishing sxemasi odatda telefon yoki elektron pochta orqali amalga oshiriladi.

Kvid pro kvo (lotinchadan: Quid pro quo). Ushbu ibora ingliz tilida “xizmat uchun xizmat” degan ma’noni anglatib, sotsial injineriyaning mazkur turida xaker korporativ tarmoq yoki elektron pochta orqali kompaniyaga murojaatni amalga oshiradi. Ko‘pincha xaker o‘zini texnik xizmat ko‘rsatuvchi sifatida tanitib, texnik xodimning ish joyidagi muammolarni bartaraf etishda “yordam berishini” aytadi. Texnik muammoni “bartaraf” etish vaqtida nishondagi shaxsni buyruqlarni bajarishga yoki jabrlanuvchining kompyuteriga turli xil dasturlarni o‘rnatishga undash amalga oshiriladi. Masalan, 2022 yilda Axborot xavfsizligi dasturi doirasida o‘tkazilgan tadqiqot ofis xodimlarining 90% har qanday xizmat yoki to‘lov uchun maxfiy ma’lumotlarni, masalan, o‘zlarining parollarini, berishga tayyor bo‘lishini ko‘rsatdi.

Yo‘l-yo‘lakay olma. Sotsial injineriyaning mazkur usulida xaker maxsus zararli dastur yozilgan ma’lumot eltuvchilardan foydalanadi va zararli dasturlar yozilgan eltuvchilarni qurbonning ish joyi yaqinida, jamoat joylarida va boshqa joylarda qoldiradi. Bunda, ma’lumot eltuvchilari tashkilotga tegishli shaklda rasmiylashtiriladi. Masalan, xaker biror korporatsiya logotipi va rasmiy web-sayt

manzili tushirilgan kompakt diskni qoldirib ketadi. Ushbu disk “Rahbarlar uchun ish haqlari” nomi bilan nomlanishi mumkin. Ushbu eltuvchini qo‘lga kiritgan qurbon uni o‘z kompyuteriga qo‘yib ko‘radi va shu orqali kompyuterini zararlaydi.

Ochiq ma’lumot to‘plash. Sotsial injineriya texnikasi nafaqat psixologik bilimlarni, balki, inson haqida kerakli ma’lumotlarni to‘plash qobilyatini ham talab etadi. Bunday ma’lumotlarni olishning nisbatan yangi usuli ochiq manbalardan, ijtimoiy tarmoqlardan to‘plash.

Masalan, «Одноклассники», «ВКонтакте», «Facebook», «Instagram» kabi saytlarda odamlar yashirishga harakat qilmaydigan juda ko‘p ma’lumotlar mavjud. Odatda, foydalanuvchilar xavfsizlik muammolariga yetarlicha e’tibor bermasdan, xaker tomonidan foydalanilishi mumkin bo‘lgan ma’lumotlar va xabarlarni qarovsiz qoldiradilar.

Bunga yaqqol misol sifatida Yevgeniy Kasperskiyning o‘g‘lini o‘g‘irlanganini keltirish mumkin. Mazkur holatda jinoyatchilar o‘smirning kun tartibini va marshrutini ijtimoiy tarmoq sahifalaridagi yozuvlardan bilgani aniqlangan.

Ijtimoiy tarmoqdagi o‘z sahifasidagi ma’lumotlardan foydalanishni cheklab qo‘ygan taqdirda ham, foydalanuvchining firibgarlik qurboni bo‘lmasligiga to‘liq kafolat yo‘q. Masalan, Braziliyaning kompyuter xavfsizligi bo‘yicha tadiqiqotchisi 24 soat ichida sotsial injineriya usullaridan foydalangan holda har qanday Facebook foydalanuvchisi bilan do‘stlashish mumkinligini ko‘rsatdi. Tajriba davomida Nelson Novayes Neto dastlab jabrlanuvchiga tanish bo‘lgan odam – uning xo‘jayini uchun soxta qayd yozuvini yaratadi. Avval Neto jabrlanuvchining xo‘jayinining do‘stlariga va undan keyin to‘g‘ridan-to‘g‘ri jabrlanuvchining do‘stiga do‘stlik so‘rovini yuboradi. 7,5 soatdan so‘ng esa tadqiqotchi jarblanuvchi bilan do‘stlashadi. Natijada tadqiqotchi foydalanuvchining shaxsiy ma’lumotlarini olish ikoniyatiga ega bo‘ladi.

Yelka orqaliqarash. Ushbu hujumga ko‘ra buzg‘unchi jabrlanuvchiga tegishli ma’lumotlarini uning yelkasi orqali qarab qo‘lga kiritadi. Ushbu turdagi hujum jamoat joylarida, masalan, kafe, avtobus, savdo markazlari, aeroport va

temir yo‘l stansiyalarida keng tarqalgan. Mazkur hujumga doir olib borilgan so‘rovnomalar quyidagilarni ko‘rsatgan:

- 85% ishtirokchilar o‘zlari bilishlari kerak bo‘lmagan maxfiy ma’lumotlarni ko‘rganliklarini tan olishgan;
- 82% ishtirokchilar ularning ekranidagi ma’lumotlarini ruxsatsiz shaxslar ko‘rishi mumkinligini tan olishgan;
- 82% ishtirokchilar tashkilotdagi xodimlar o‘z ekranini ruxsatsiz odamlardan himoya qilishiga ishonishmagan.

Teskari sotsial injineriya. Jabrlanuvchining o‘zi tajovuzkorga ma’lumotlarini taqdim qilishi teskari sotsial injineriyaga tegishli holat hisoblanadi. Bu bir qarashda ma’noga ega bo‘lmagan qarash hisoblansada, aksariyat hollarda jarblanuvchining o‘zi muammolarini hal qilish uchun tajovuzkorni yordamga jalb qiladi. Masalan, jabrlanuvchi bilan birga ishlovchi tajovuzkor jabrlanuvchi kompyuteridagi biror faylni nomini o‘zgartiradi yoki boshqa katalogga ko‘chirib o‘tkazadi. Faylni yo‘‘q bo‘lganini bilgan qurbon esa ushbu muammoni tezda bartaraf etishni istab qoladi. Bu vaziyatda tajovuzkor o‘zini ushbu muammoni bartaraf etuvchi sifatida ko‘rsatadi va qurbonning muammosini bartaraf etish bilan birga unga tegishli login/ parolni ham qo‘lga kiritadi. Bundan tashqari, ushbu vazifasi bilan tajovuzkor tashkilot ichida obro‘ga ega bo‘ladi va o‘z qurbonlari sonini ortishiga erishadi. Bu holatni aniqlash esa ancha murakkab ish hisoblanadi.

Mashhur sotsial injinerlar. Kevin Mitnik tarixdagi eng mashhur sotsial injinerlardan biri, u dunyodagi mashhur kompyuter xakeri, xavfsizlik bo‘yicha mutaxassis va sotsial injineriyaga asoslangan kompyuter xavfsizligiga bag‘ishlangan ko‘plab kitoblarning ham muallifidir. Uning fikriga ko‘ra xavfsizlik tizimini buzishdan ko‘ra, aldash yo‘li orqali parolni olish osonroq.

Aka-uka Badirlar. Ko‘r bo‘lishlariga qaramasdan aka-uka Mushid va Shadi Badirlar 1990 yillarda Isroilda sotsial injineriya va ovozni soxtalashtirish usullaridan foydalangan holda bir nechta yirik firibgarlik sxemalarini amalga oshirishgan. Televideniyaga bergan intervyusida: “faqat telefon, elektr va noutbuklardan foydalanmaydiganlar uchun tarmoq xavfsizdir” deb aytishgan.

Sotsial injineriyadan himoyalanish choralari. Hujumlarni amalga oshirishda sotsial injineriya texnikasidan foydalangan tajovuzkorlar tez-tez muloyimlik, dangasalik, xushmuomilalik bilan foydalanuvchi va tashkilot xodimlarining qiziqishlaridan foydalanadilar. Hujumlarni oldini olish esa, xodimlarning aldanayotganliklarini bilmasliklari sababli, murakkab hisoblanadi.

Sotsial injineriya hujumlarini quyidagicha aniqlash mumkin:

- o‘zini do‘stingiz yoki yordam so‘rab murojaat qilgan yangi xodim sifatida tanishtirish;
- o‘zini yetkazib beruvchi, hamkor kompaniyaning xodimi yoki qonun vakili sifatida tanishtirish;
- o‘zini biror rahbar sifatida tanishtirish;
- biror zaiflikni bartaraf etuvchi yoki jabrlanuvchiga biror nimani yangilash imkoniyatini taqdim qiluvchi sotuvchi yoki ishlab chiqaruvchi sifatida tanishtirish;
- muammo yuzaga kelganida yordam beruvchi sifatida tanishtirish;
- ishonchni hosil qilish uchun ichki xotirjamlik va terminologiyadan foydalanish;
- “maktub”ga turli zararli dasturlarni qo‘shib yuborish;
- soxta ochilgan oynada login/ parolni qayta kiritishni so‘rash;
- foydalanuvchi nomi va paroli bilan saytga ro‘yxatdan o‘tish uchun biror sovg‘a taklif etish;
- jabrlanuvchi kompyuteriga yoki dasturiga kiritilgan kalitlarni yozib olish (keylogger dasturlari);
- turli xil zararli dasturiy vositaga ega ma’lumot eltuvchilarini foydalanuvchi stoliga tashlash;
- turli qo‘ng‘iroqlardagi ovozli xabarlar va h.

Hayotda ko‘plab jabhalarda sotsial injineriyaga tegishli muammolarni ko‘rish mumkin. Xususan, ommaviy madaniyatda (masalan, kinofilmlarda) sotsial injinerlikdan foydalanish holatlari tez-tez uchrab turadi. Masalan, quyidagi keltirilgan kinofilmlarda sotsial injineriyaga oid epizodlar mavjud:

– «Поймай меня, если сможешь»;

- «Поймай толстуху, если сможешь»;
- «Один дома»;
- «Хакеры»;
- «Афера Томаса Крауна»;
- «Бриллианты навсегда»;
- «Кто я».

Nazorat savollari:

1 Ijtimoiy injineriya va uni hozirgi kiberjinoyatchilikdagi ahamiyatini ko‘rsatib bering?

2. Soxta veb saytlar, fishing elektron xabarlarga ta’rif bering.

3.Fishing va uning ko‘rinishlari. Ijtimoiy injineriyaga real misollar keltiring.

4.Ijtimoiy injineriyadan himoyalanish usullarini yoritib bering.

Adabiyotlar va internet saytlari:

1. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoykulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma, – T. “Nihol print” OK, 2021. – 224 b.

2. S.K. Ganiev, Z.T. Xudoykulov, N.B. Nasrullaev. Основы кибербезопасности: Учебное пособие, – T. “Mahalla oila nashriyoti”, 2021. – 224 b.

3. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях - М: ДМК Пресс, 2012. - 596 с.

IV-BO‘LIM

AMALIY MASHG‘ULOT MATERIALLARI

IV. AMALIY MASHG‘ULOT MATERIALLARI

1-amaliy ish

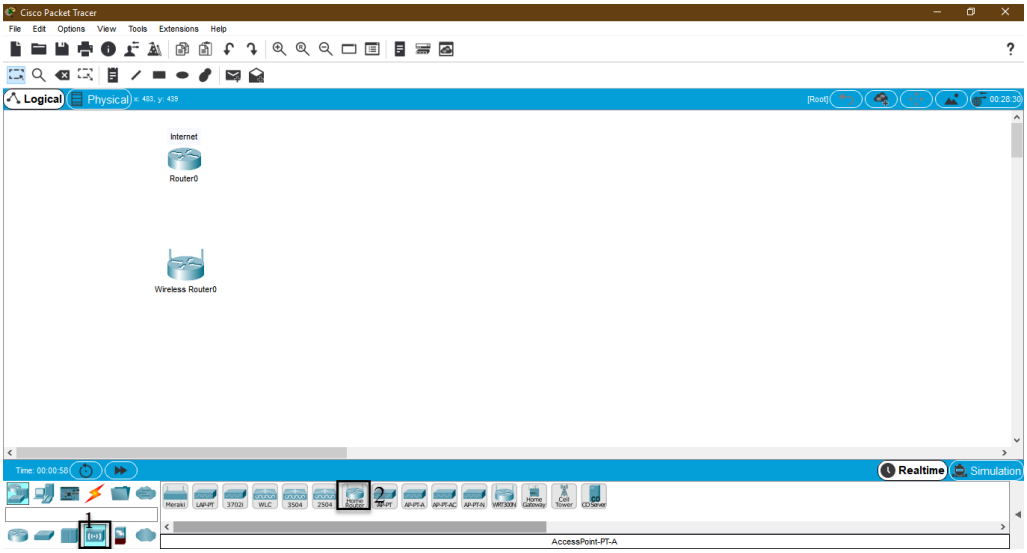
MAVZU: SIMSIZ TARMOQ VOSITALARINI SOZLASH

Ishdan maqsad:

1. Wi-Fi texnologiyasi haqida tushunchaga ega bo‘lish;

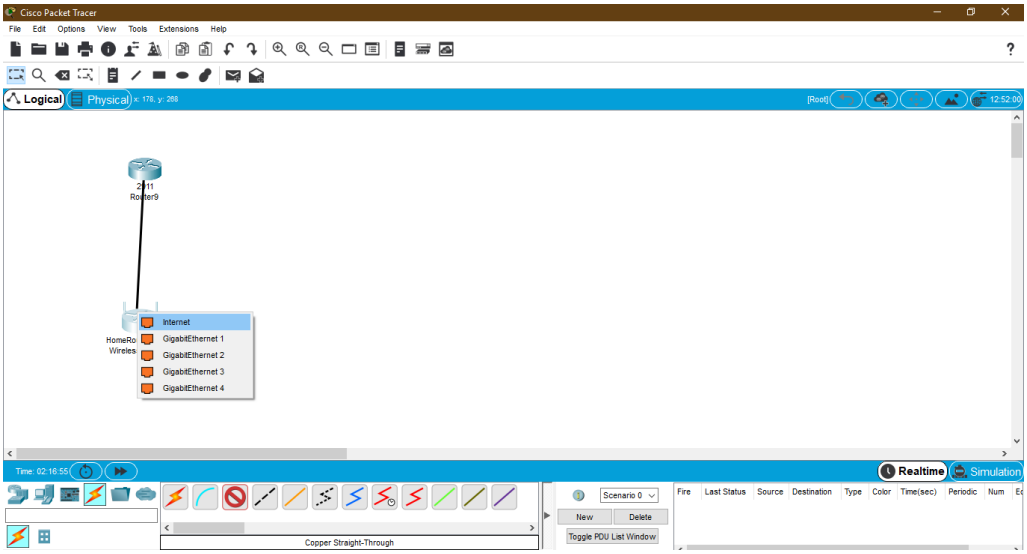
2. CPT dasturida WIFI tarmog’ini qurish.

Cisco Packet Tracer (CPT) dasturida Wi-Fi tarmoq qurish uchun dastlab 1 router qurilmasi va 1 WiFi router qurilmasi olinadi:



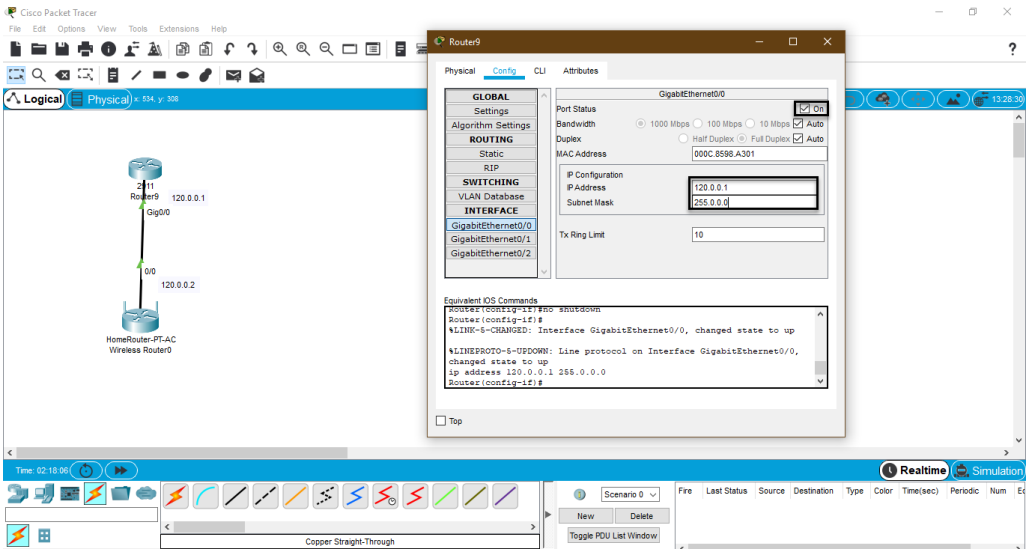
1.1-rasm

Ular o‘zaro aloqa kabeli bilan ulab chiqiladi. *Router0* da «GigabitEthernet» protiga va *WiFi router* da «Internet» portiga ulanadi:



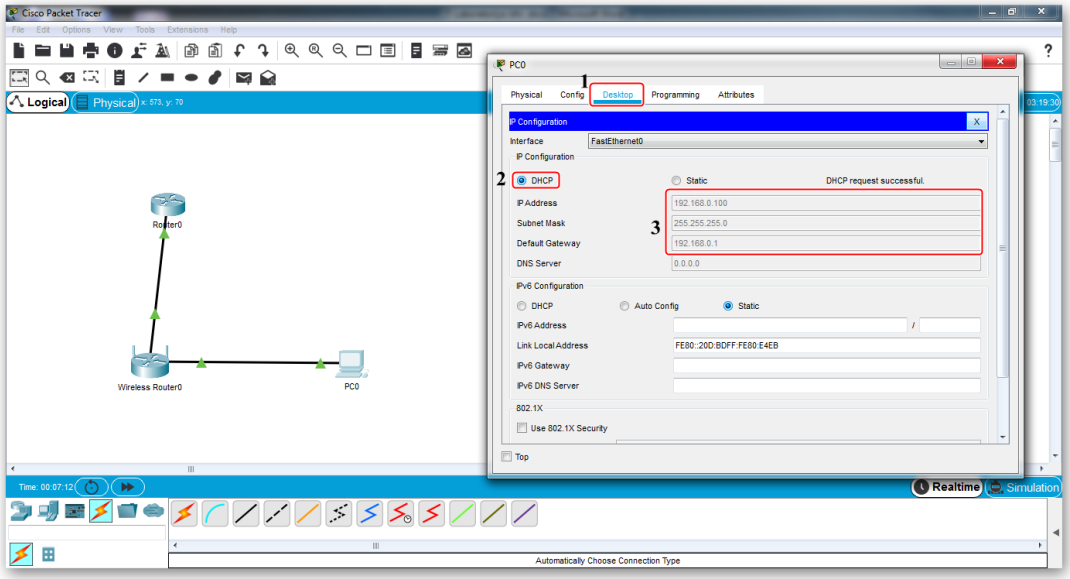
1.2-rasm

Router0 da IP address 120.0.0.1 Tarmoq maskasi 255.0.0.0 qilib sozlamalar kiritiladi:



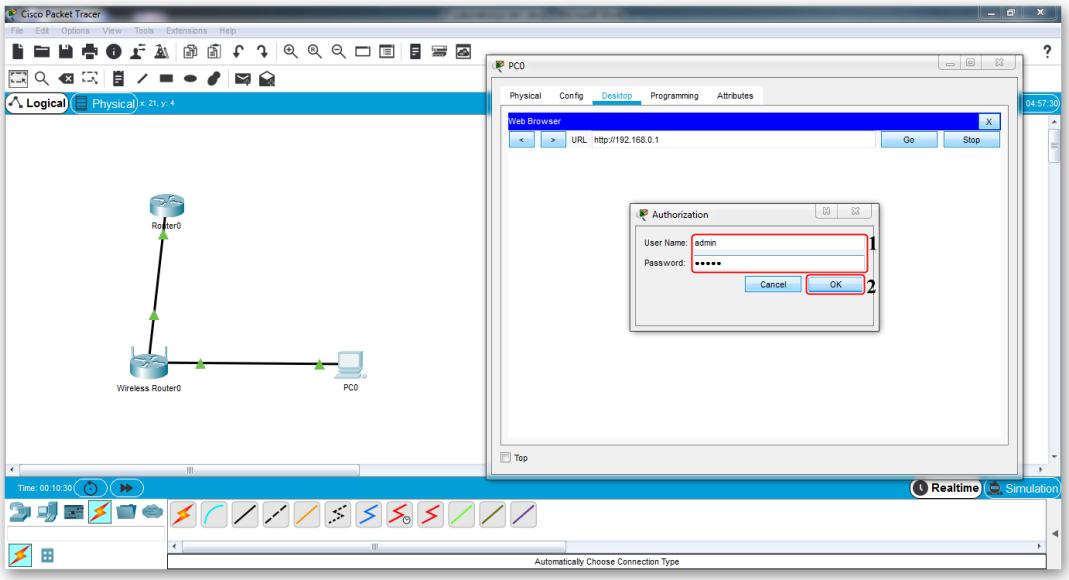
1.3-rasm

WiFi router ning LAN portiga kompyuter olib aloqa kabeli orqali ulanadi va kompyuterda IP addres sozlamalari «Static» dan «DHCP» ga o`zgartiriladi:



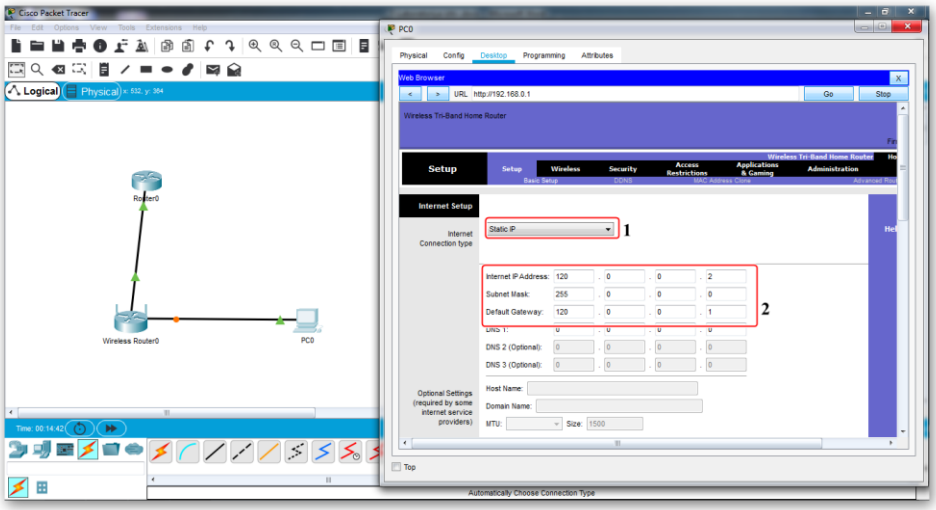
1.4-rasm

WiFi router ni sozlash uchun kompyuterda «Desktop» dan «Web browser» ga kirib domen o`rniga 192.168.0.1 IP addresi kiritiladi va «User Name» va «Password» ga «admin» kiritiladi:



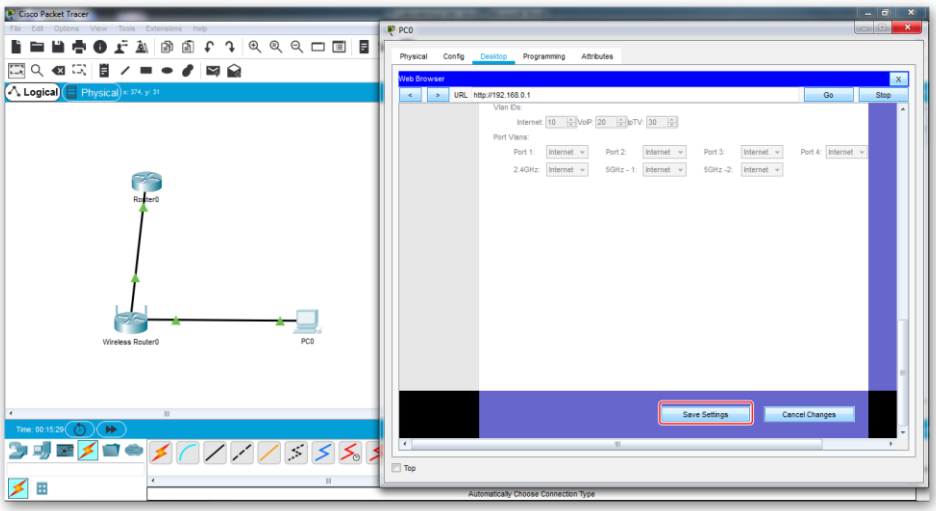
1.5-rasm

WiFi router ning admin paneliga kirilganidan so`ng «Internet» portiga IP addres sozlamalari kiritiladi. Buning uchun «Internet Connection Type» ni «Static IP» ga o`zgartiriladi va IP address 120.0.0.2, Tarmoq maskasi 255.0.0.0, Asosiy shlyuz 120.0.0.1 qilib sozlamalar kiritiladi:



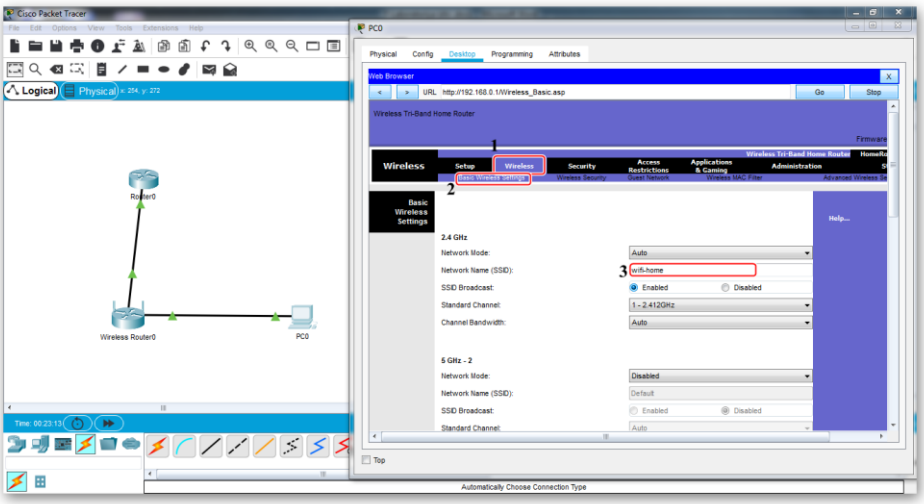
1.6-rasm

IP addres sozlamalari kiritilganidan so`ng «Save Settings» bosiladi:



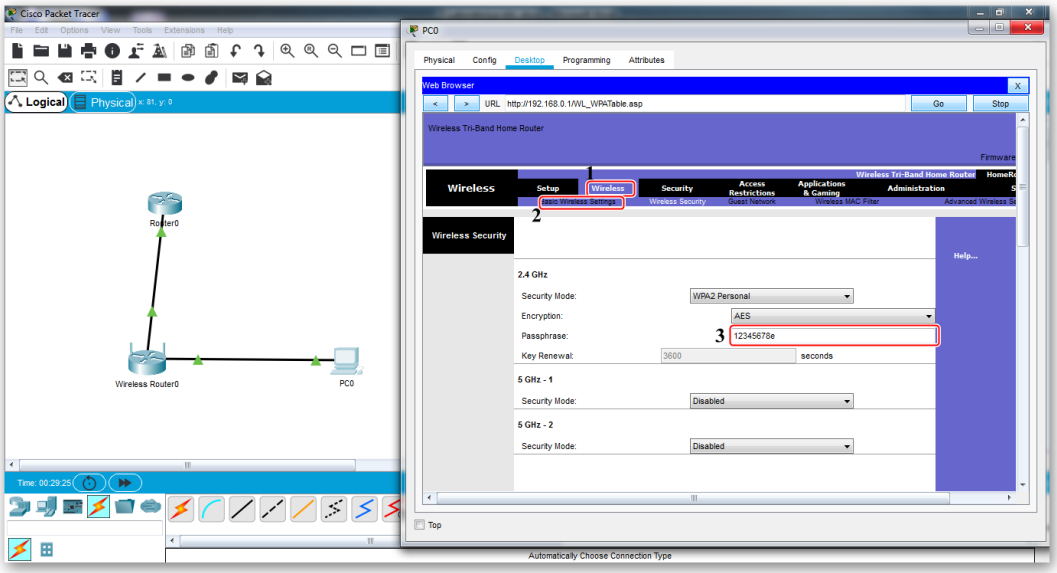
1.7-rasm

Yo`qoridagi sozlamalar o`rnatilganidan so`ng WiFi (simsiz tarmoq) sozlamalari o`rnatiladi. Buning uchun «Wireless» bo`limidan «Basic Wireless Settings» ga kirib (2.4 GHz) «Network Name (SSID)» ga wifi nomi kiritiladi va sozlamalari «Save Setting» ga bosib saqlanadi:



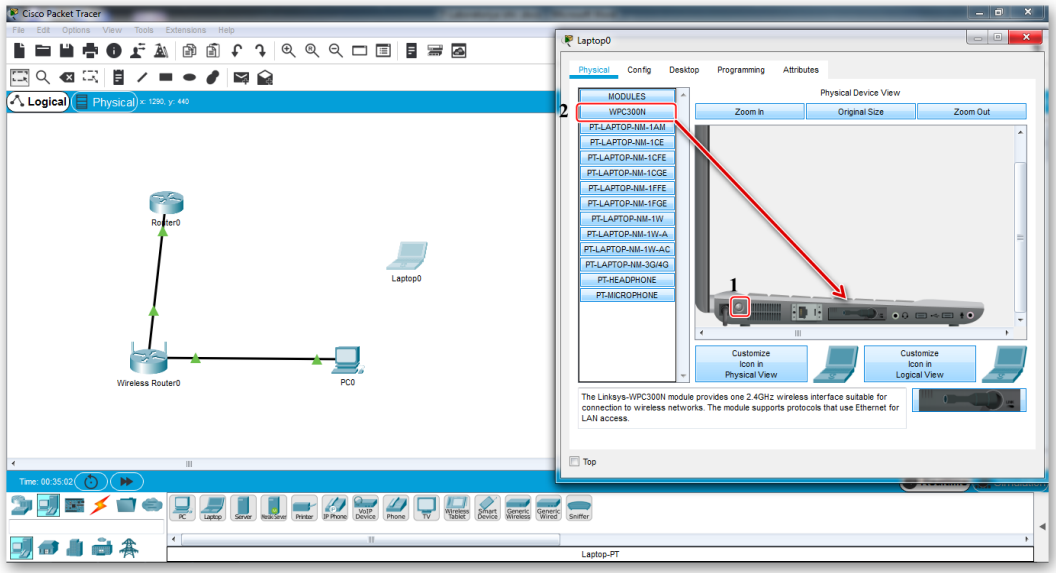
1.8-rasm

Wifi nomi o`rnatilganidan so`ng parol o`rnatiladi. Buning uchun «Wireless» bo`limidan «Wireless Security» ga kirib (2.4 GHz) «Security mode» «WPA 2 Personal» qilinadi va «Passphrase» ga parol kiritiladi. Parol kiritilganidan so`ng «Save Settings» ga bosib saqlanadi:



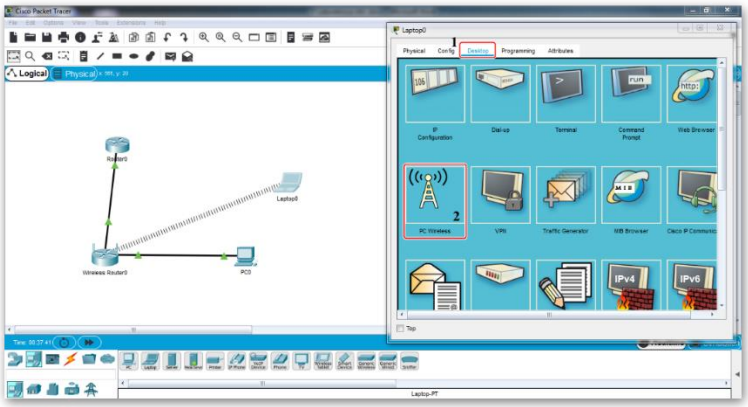
1.9-rasm

Yo`qoridagi sozlamalardan so`ng WiFi tarmoq sozlangan xisoblanadi. WiFi tarmoqga *laptop0* olib WiFi orqali ulab ko`riladi. *Laptop0* qurilmasi olib unga WiFi moduli o`rnatiladi. Buning uchun *laptop0* ni o`chirib «WPC300N» moduli o`rnatilib qayta ishga tushiriladi:



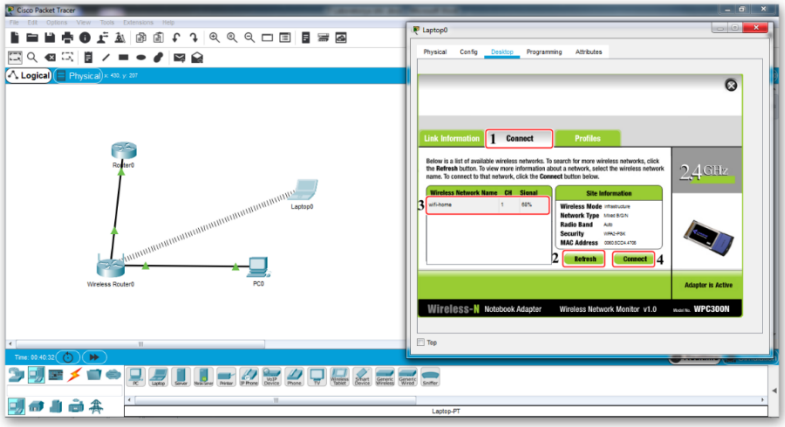
1.10-rasm

WiFi router ga *laptop0* dan ulanish uchun «Desktop» bo`limidan «PC Wireless» ga kiriladi:



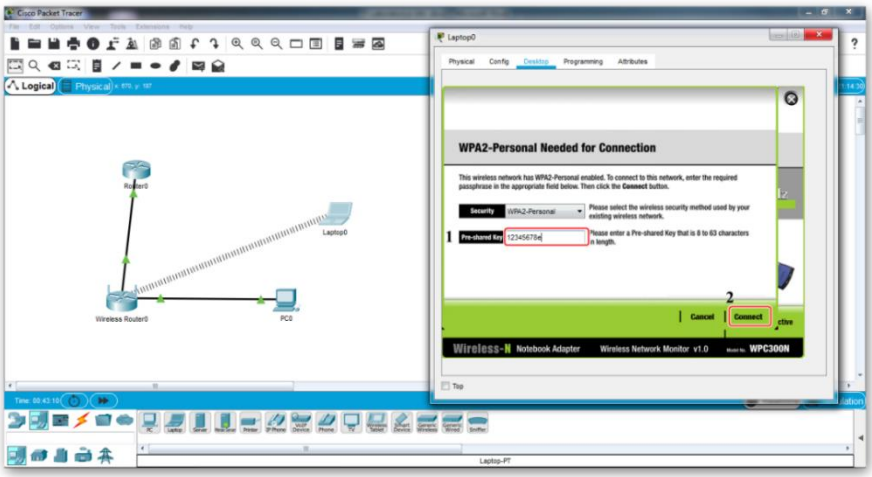
1.11-rasm

«Connect» bo`limidan «Refresh» ga bosib «wifi-home» ga ulanish uchun «connect» bosiladi:



1.12-rasm

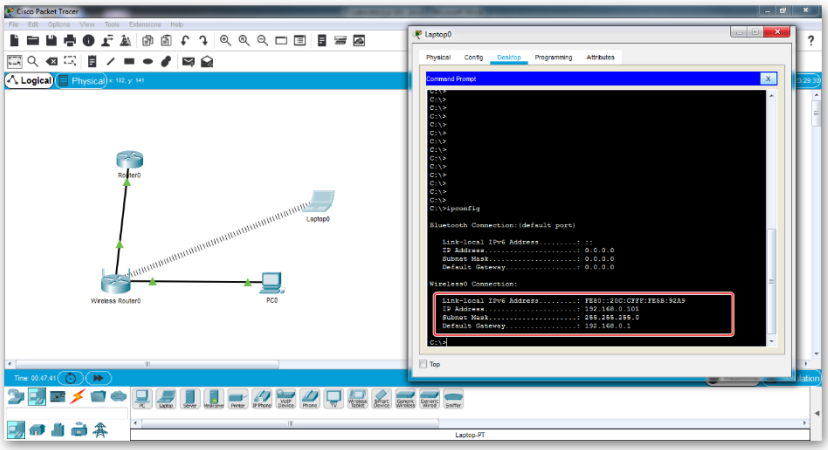
Keyingi oynada «Pre-shared Key» bo`limiga «wifi-home» paroli (12345678e) kiritib «connect» bosiladi:



1.13-rasm

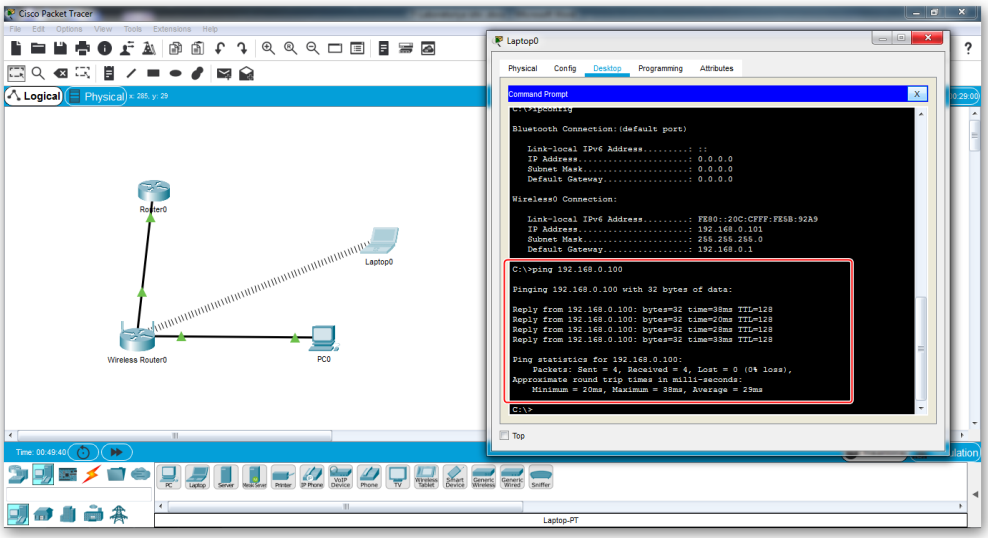
«Connect» ni bosilganidan so`ng *laptop0* wifi tarmog`iga ulanadi. IP addres

sozlamalari «DHCP» protokoli orqali avtomatik tarizda sozlanadi. Buni tekshirish uchun «Command Prompt» ga kirib *ipconfig* komandasi kiritiladi:



1.14-rasm

Aloqani tekshirish uchun aloqa kabeli orqali ulangan kompyuterga xabar (ping) yuborib tekshiriladi. Buning uchun *ping 192.168.0.100* komandasi kiritiladi:



1.15-rasm

Yuqorida rasmda xabar (ping) omadli yuborilganini bildiradi.

2-AMALIY ISH

MAVZU: AXBOROT XAVFSIZLIGIDA RISK MODELLARI

Ishdan maqsad: Sababdan Oqibatgacha xavfli hodisani rivojlanish yo‘llarini taxlili va sxematik tavsifilash usuli.

Xavflarni baholash usullari turli kutilgan va kutilmagan vaziyatlarni o‘rganish uchun kuchli vositadir. Keyinchalik, kiberxavfsizlik asoslari kursining bir qismi sifatida ba'zi amaliy mashg'ulotlarda foydalaniladigan xavflarni baholash usullari tavsiflanadi.

“Galstuk-babochka” tahlil usuli

Ushbu usul o‘rganilayotgan salbiy hodisaning sababdan oqibatga qadar rivojlanishini grafik tavsiflash va tahlil qilishdir. Ushbu usulning asosiy yo‘nalishi tekshirilayotgan hodisaga qarshi choralar va uni keltirib chiqaradigan sabablarga qaratilgan.

Ushbu usulni amalga oshirish quyidagi bosqichlarni ajratishi mumkin:

1. Grafik markazida tahlil qilish uchun hodisani aniqlash.

2. Tekshirilayotgan hodisaga olib kelishi mumkin bo‘lgan sabablar ro‘yxatini tuzish.

3. Tekshirilayotgan voqea oldidan vaziyatning rivojlanish mexanizmini tahlil qilish

4. Hodisaning rivojlanishiga olib keladigan omillar va uning oqibatlari tavsiflanishi mumkin.

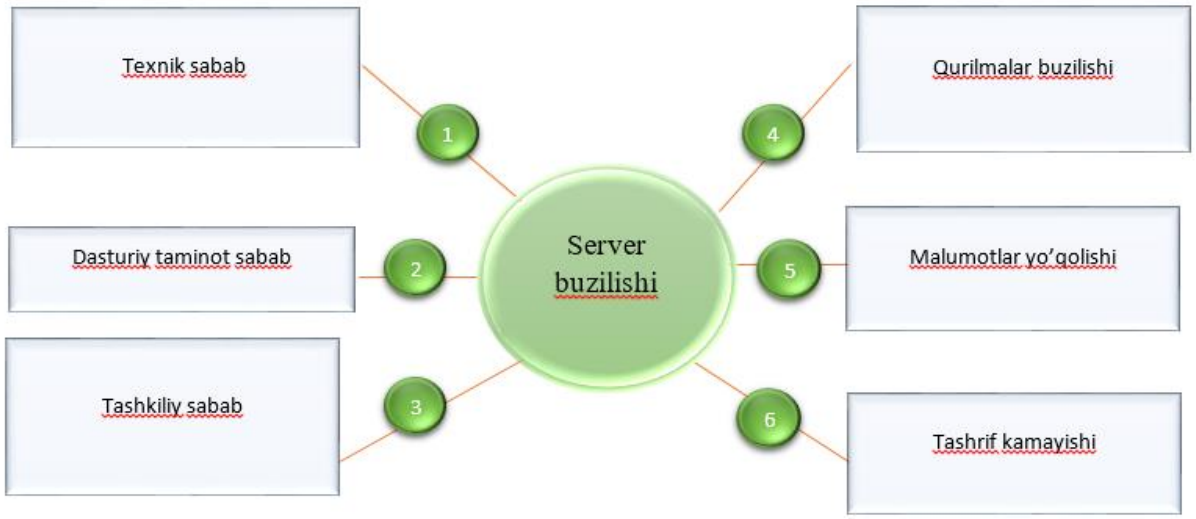
5. Hodisadan oldin deb ataladigan sabablarning rivojlanishiga to‘sqinlik qiladigan to‘siqlarni namoyish qilish profilaktika choralari. Eskalatsiya omillari uchun to‘siqlarni ham ko‘rsatishingiz mumkin.

6. Tekshirilayotgan voqea sabab bo‘lishi mumkin bo‘lgan oqibatlar ro‘yxatini tuzish.

7. O‘rganilayotgan voqeaning oqibatlarini rivojlanishiga to‘sqinlik qiladigan to‘siqlarni namoyish qilish.

“Galstuk-babochka” tahlilini o‘tkazish orqali biz xavfli hodisalar va ularning oqibatlarning oldini olish , yumshatish yoki kutilayotgan hodisalarni kuchaytirish,

tezlashtirishga yo‘naltirilgan xavfli voqealar va to‘siqlarning asosiy yo‘llarini aniq ko‘rsatadigan oddiy diagramma kiritamiz (tekshirilayotgan voqea ijobiy bo‘lgan taqdirda).



2.1-rasm.Nosozliklarni tahlil qilish

Nosozliklarni tahlil qilish usuli nomaqbul hodisaga olib keladigan omillarni aniqlash va tahlil qilish uchun foydalaniladi. O‘rganilgan omillar ular yuzaga kelishi mumkin bo‘lgan ketma-ketlikda joylashtiriladi va mantiqiy bog'liqdir.

Bularni tahli qilish uchun quyidagi bosqichlarni amalga oshirish kerak bo`ladi.

Ushbu usulni amalga oshirishni quyidagi bosqichlarni ajratishi mumkin:

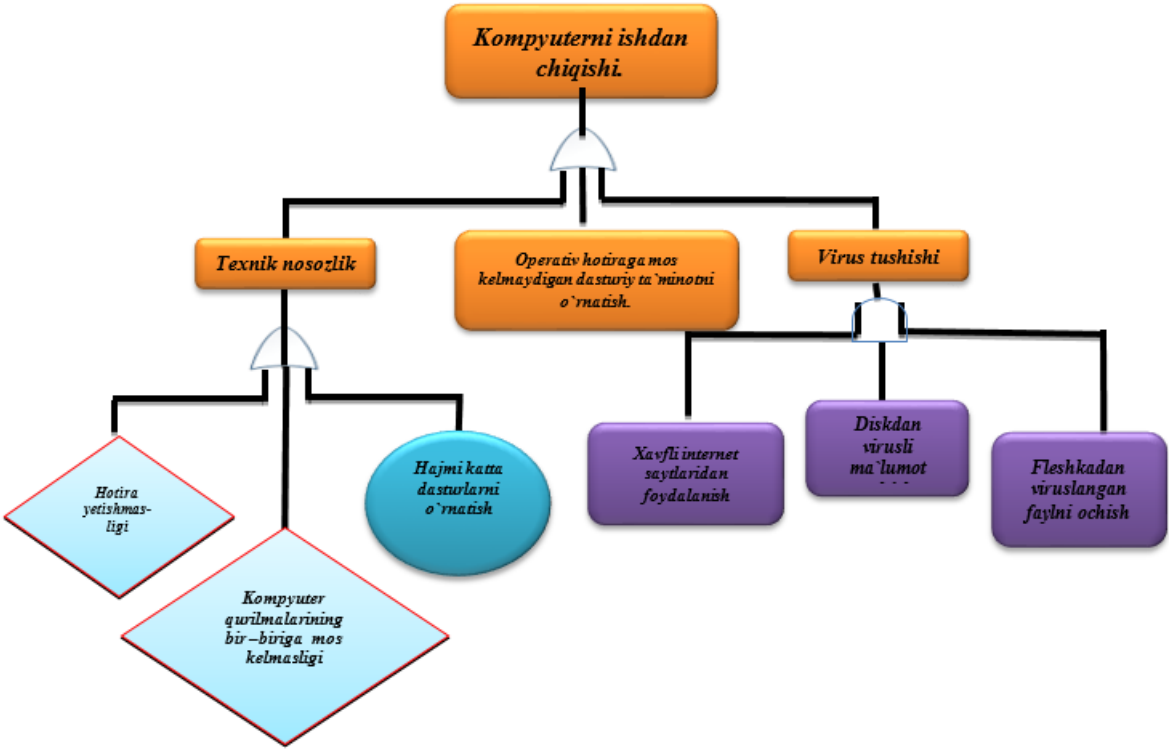
1. Tekshirilishi kerak bo‘lgan yakuniy hodisani aniqlash.

2. Yakuniy voqeadan boshlab, yakuniy hodisaga olib keladigan sabablarni topish

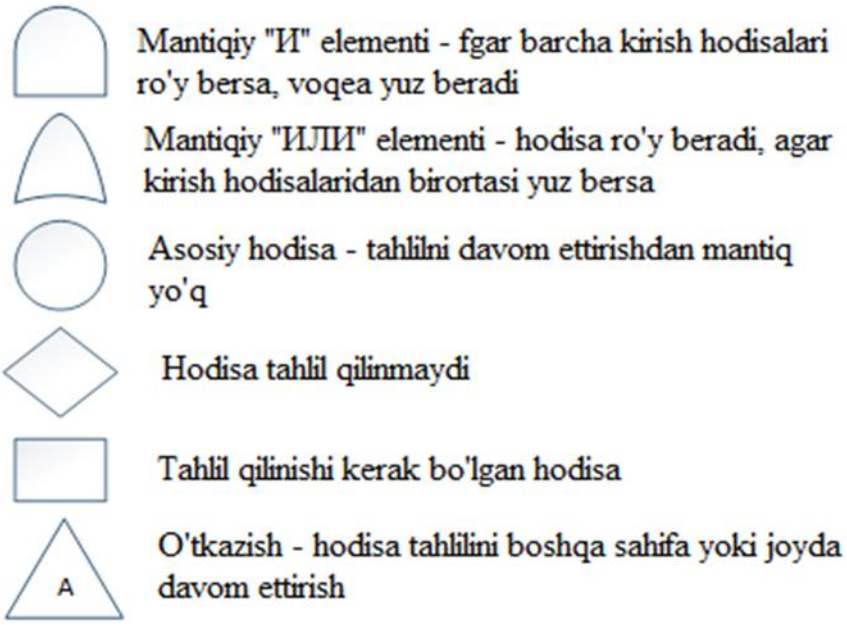
3. Belgilangan sabablarga olib kelishi mumkin bo‘lgan aniq voqealar yoki nosozliklarni aniqlash uchun ko‘rsatilgan sabablarni tahlil qilish.

4. Keyingi darajadagi sabablarni izchil tahlil qilish va hokazo, hozircha tahlil noto‘g'ri bo‘ladi.

5. Dastlabki hodisalar ehtimolini baholash, so‘ngra oxirgi voqea ehtimolini hisoblash.



2.1-rasm. Nosozliklar daraxti tahlili diagrammasining belgilanishi



Bu tahlillar bizga nega kerak degan savolga shunday javob bersak bo`ladi, Nosozliklar daraxtining tahlili bir vaqtning o‘zida bir nechta voqealar sodir bo‘lishi mumkin bo‘lgan tekshirilayotgan yakuniy voqea va vaziyatlarning vujudga kelish yo‘llarini vizual ravishda taqdim etadi. Shuningdek yakuniy voqea ehtimolini baholash imkonini beradi.

Tahdidlar	Oqibatlari	Tahdidlarni	Risk o‘lchovi	Tahdidlarni

		yuzaga kelish ehtimolligi		Ranjirlash
Tahdid A	5	2	10	2
Tahdid B	4	4	15	2
Tahdid C	3	3	9	3

Tahdid A- Texnik nosozlik

Tahdid B- Mos kelmaydigan DTni o‘rnatish

Tahdid C- Virus tushishi

V-BO‘LIM

GLOSSARIY

V. GLOSSARIY

Avtorizatsiya – tizimda foydalanuvchiga, uning ijobiy autentifikatsiyasiga asosan, ma’lum foydalanish huquqlarini taqdim etish.

Авторизация - представление пользователю определенных прав доступа на основе положительного результата его аутентификации в системе.

Authorization – granting the user certain access rights based on the positive result of authentication in the system.

Himoya ma’muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz foydalanishdan himoyalashga javobgar foydalanish subyekti.

Администратор защиты - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Security administrator - the subject of the access responsible for the protection of the automated system against unauthorized access to the information.

Tizim ma’muri – tizimni ekspluatatsiyasiga va uning ishga layoqatlik holatini ta’minlashga javobgar shaxs.

Администратор системы - лицо, отвечающее за эксплуатацию системы и поддержание ее в работоспособном состоянии.

System administrator – a person who is responsible for operation of the system and keeping it in an appropriate working condition.

Faol tahdid – tizim holatini atayin ruxsatsiz o‘zgartirish tahdidi.

Активная угроза - угроза преднамеренного несанкционированного изменения состояния системы.

Active threat – a threat that can make a deliberate unauthorized change to the system.

Shifrlash algoritmi - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm. Blokli shifrtizim holida shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.

Алгоритм шифрования - алгоритм криптографический, реализующий функцию шифрования. В случае шифрсистем блочных получается использованием алгоритма шифрования блочного базового в конкретном режиме шифрования.

Encryption algorithm - a cryptographic algorithm that implements the function of encryption. In the case of block cipher system is obtained using the algorithm of the base block encryption in a particular mode of encryption.

RSA shifrlash algoritmi – 1978 yili R. Rayvest, A Shamir va L.Adleman tomonidan taklif etilgan va asimetrik shifr tizimlarini qurishga mo‘ljallangan shifrlash algoritmi.

Алгоритм шифрования RSA - алгоритм шифрования, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом и предназначенный для построения шифрсистем асимметричных.

RSA encryption algorithm - the encryption algorithm proposed in 1978 by R. Rivest, A. Shamir and L. Adleman and is designed to build asymmetric ciphers.

Tahlil – olingan ma’lumotlarning muhimligi va vaziyat uchun isbotlanganlik qiymatini o‘rganish.

Анализ - изучение значимости полученных данных и доказательственной ценности к случаю.

Analysis – the examination of acquired data for its significance and probative value to the case.

Tarmoq tahlillagichlari (sniffer) – tarmoq trafigini “tinglash”ni va tarmoq trafigidan avtomatik tarzda foydalanuvchilar ismini, parollarni, kredit kartalar nomerini, shu kabi boshqa axborotni ajratib olishni amalga oshiruvchi dasturlar.

Анализаторы сетевые (сниффер) - программы, осуществляющие «прослушивание» трафика сетевого и автоматическое выделение из трафика сетевого имен пользователей, паролей, номеров кредитных карт, другой подобной информации.

Network analyzers (sniffer) - programs that listen on network traffic and automatic allocation of network traffic usernames, passwords, credit card numbers, and other such information.

Axborotni himoyalashning apparat vositasi – axborotni ishlovchi texnik vositasi komplekti tarkibiga kiruvchi maxsus himoyalovchi qurilma yoki moslama.

Аппаратное средство защиты информации - специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информации.

Hardware data protection - a special protective device or fixture included in the kit technical tools of information processing.

AT xavfsizlik arxitekturasi - xavfsizlikni loyihalash tizimini boshqaruvchi prinsiplariga rioya qilish uchun xavfsizlik prinsiplarining va umumiy yondashishning tavsifi.

Архитектура IT безопасности - описание принципов безопасности и общего подхода для соблюдения принципов, управляющих системой проектирования безопасности.

IT security architecture – a description of security principles and an overall approach for complying with the principles that drive the system design.

Axborot xavfsizligining arxitekturasi - tashkilot xavfsizlik jarayonlari strukturasi va ishlash rejimini, axborot xavfsizligi tizimlarini, shaxsiy va tashkiliy bo‘linmalarini, ularni tashkilot missiyasi va strategik rejalariga tenglashtirishni ko‘rsatish bilan tavsiflovchi tashkilot arxitekturasining o‘rnatilgan, ajratib bo‘lmas qismi.

Архитектура информационной безопасности - встроенная, неотъемлемая часть архитектуры предприятия, описывающая структуру и поведение процессов безопасности, систем информационной безопасности, персональных и организационных подразделений, с указанием их выравнивание с целью и стратегическими планами предприятия.

Information security architecture – an embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise’s security processes, information security systems, personnel and organizational sub-

units, showing their alignment with the enterprise's mission and strategic plans.

«Dushman o'rtada» hujumi – kriptografik protokolga hujum bo'lib, bunda dushman C ushbu protokolni ishtirokchi A va ishtirokchi B bilan bajaradi. Dushman C ishtirokchi A bilan seansni ishtirokchi B nomidan, ishtirokchi B bilan esa ishtirokchi A nomidan bajaradi. Bajarish jarayonida dushman ishtirokchi A dan ishtirokchi V ga va aksincha xabarni, ehtimol, o'zgartirib uzatadi. Xususan, abonentni autentifikatsiyalash protokoli holida «dushman o'rtada» hujumining muvafaaqiyatli amalga oshirilishi dushmanga ishtirokchi B uchun o'zini ishtirokchi A nomidan autentifikatsiyalashga imkon beradi. «Dushman o'rtada» hujumini amalga oshirish uchun protokolning ikkita seansining sinxronlanishini ta'minlash lozim.

Атака «противник в середине» — атака на протокол криптографический, в которой противник C выполняет этот протокол как с участником A, так и с участником B. Противник C выполняет сеанс с участником A от имени B, а с участником B от имени A. В процессе выполнения противник пересылает сообщения от A к B и обратно, возможно, подменяя их. В частности, в случае протокола аутентификации абонента успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для B под именем A. Для осуществления атаки «противник в середине» необходимо обеспечивать синхронизацию двух сеансов протокола.

Attack "the opponent in the middle" - attack on a cryptographic protocol in which the enemy with this protocol performs as a party A and party B with C. Enemy performs session with party A on behalf of B, and a participant on behalf of A. During runtime opponent forwards messages from A to B and back, possibly replacing them attacks. In particular, in the case of an authentication protocol is connected to the success of the attack "the opponent in the middle" allows authenticate itself to the enemy in the name of A. To carry out the attack "the opponent in the middle" is necessary to ensure the synchronization of the two sessions of the protocol.

Xizmat qilishdan voz kechish hujumi – tizim buzilishiga sabab bo'luvchi hujum, ya'ni shunday sharoitlar tug'diradiki, qonuniy foydalanuvchi tizim taqdim etgan resurslardan foydalana olmaydi yoki foydalanish anchagina qiyinlashadi.

Атака на отказ в обслуживании — атака с целью вызвать отказ системы, то есть создать такие условия, при которых легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет значительно затруднён.

Denial-of-service attack - attack intended to cause a system failure, that is, to create conditions under which legitimate users will not be able to access the system-provided resources, or this access much more difficult.

Passiv hujum – kriptotizmga yoki kriptografik protokolga hujum bo'lib, bunda dushman va/yoki buzg'unchi uzatiluvchi shifrlangan axborotni kuzatadi va ishlatadi, ammo qonuniy foydalanuvchilar harakatiga ta'sir etmaydi.

Атака пассивная — атака на криптосистему или протокол

криптографический, при которой противник и/или нарушитель наблюдает и использует передаваемые сообщения шифрованные, но не влияет на действия пользователей законных.

Passive attack - attack on a cryptosystem or a cryptographic protocol in which enemy and/or the offender observes and uses the transmitted messages are encrypted, but does not affect the user's actions legitimate.

Parollar lug'atiga asoslangan hujum – parol qiymatlarini saralashga asoslangan kriptotizimga hujum.

Атака со словарем паролей — атака на криптосистему, основанная на переборе значений пароля.

Attack with a dictionary of passwords - the attack on the cryptosystem based on iterating the value of a password.

Autentifikator – foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo'shimcha kod so'zlari, biometrik ma'lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo'lishi mumkin.

Аутентификатор - средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.

Authenticator - means of authentication that represents the distinctive attribute of the user. Means of user authentication can be additional code word, biometric data and other identifying features of the user.

Autentifikatsiya – odatda tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul uchun foydalanuvchining, qurilmaning yoki tizimning boshqa tashkil etuvchisining identifikasiyasini tekshirish; saqlanuvchi va uzatuvchi ma'lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.

Аутентификация - проверка идентификации пользователя, устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.

Authentication - checking the identification of user, device, or other component in the system, typically for decision-making about access to system resources; check the integrity of stored or transmitted data to detect unauthorized modification.

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.

Аутентификация двухфакторная — аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает

пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).

Two-factor authentication - user authentication on the basis of two unrelated factors, as a rule, on the basis of what he knows and what he knows (e.g., password-based and physical ID).

Bir martali parollar aosidagi autentifikatsiya - bir martali parollar yordamida autentifikatsiyalash texnologiyasi. Bir martali parollarni olishda quydagilar ishlatilishi mumkin: bir tomonlama funksiya asosida generatsiyalash algoritmi, maxsus qurilmalar-tokenlar, yoki bir martali parolni, foydalanuvchi tatbiqiy tizimdan foydalanishda ishlatiladigan kanaldan farqli, kanal orqali uzatishga asoslangan OOB (out of band) texnologiyasi.

Аутентификация на основе паролей одноразовых — технология аутентификации с помощью паролей одноразовых, для получения которых могут использоваться: алгоритм генерации на основе односторонней функции, специальные устройства – токены, либо технология OOB (out of band), основанная на передаче пароля одноразового с использованием дополнительного канала, отличного от того, по которому пользователь осуществляет доступ к прикладной системе.

One time password based authentication - technology authentication using one time passwords, which can be used: the generation algorithm based on one-way functions, special device – taken, or technology OOB (out of band) based on the transmission password disposable using additional channels, other than where the user accesses the application system.

Xabarlar autentifikatsiyasi – ma’lumotlarda har qanday o‘zgarishlarni aniqlash maqsadida ma’lumotlar blokiga nazorat hoshiyasini qo‘shish. Ushbu hoshiya qiymatini hisoblashda faqat ma’lumotlar priyemnigiga ma’lum kalitlar ishlatiladi.

Аутентификация сообщений - добавление к блоку данных контрольного поля для обнаружения любых изменений в данных. При вычислении значений этого поля используется ключ, известный только приемнику данных.

Message authentication - adding control data to the data field to detect any changes in the data. The values of this field using a key known only to receiver data.

Xavfsizlik - ta’siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifiy, ichki va tashqi beqarorlovchi faktorlarga qarshi tizimning tura olish xususiyati. Yana - ma’lumotlar fayllarining va dasturlarning avtorizatsiyalanmagan shaxslar (jumladan tizim xodimi), kompyuterlar yoki dasturlar tomonidan ishlatilishi, ko‘rib chiqilishi va modifikatsiyalanishi mumkin bo‘lmagan holat.

Безопасность - свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. Еще -

состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами.

Security - the property of a system to withstand external or internal destabilizing factors, the effect of which may be unwanted state or behaviour. Still - a state in which the data files and programs may not be used, viewed and modified by unauthorized persons (including the system staff), computers or software.

Axborot xavfsizligi - axborot holati bo‘lib, unga binoan axborotga tasodifiy yoki atayin ruxsatsiz ta’sir etishga yoki ruxsatsiz uning olinishiga yo‘l qo‘yilmaydi; yana - axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanish darajasi holati.

Безопасность информации - состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение; еще - состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность (конфиденциальность), целостность и доступность.

Information security - status information, which excludes accidental or deliberate tampering or unauthorized information receive it, also - the state of security level information when processing technical means to ensure the preservation of its quality characteristics (properties) such as secrecy (confidentiality), integrity, and availability.

Axborot tarmog’i xavfsizligi – axborot tarmog’ini ruxsatsiz foydalanishdan, me’yoriy harakatlariga tasodifiy yoki atayin aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.

Безопасность информационной сети - меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.

Network security - measures that protect the information network from unauthorized access, accidental or deliberate interference in normal activities or attempts the destruction of its components.

Tarmoqlararo ekran – apparat-dasturiy vositalar yordamida tarmoqdan foydalanishni markazlashtirish va uni nazoratlash yo‘li bilan tarmoqni boshqa tizimlardan va tarmoqlardan keladigan xavfsizlikka tahdidlardan himoyalash usuli; yana - bir necha komponentlardan (masalan, tarmoqlararo ekran dasturiy ta’minoti ishlaydigan marshrutizator yoki shlyuzdan) tashkil topgan ximoya to‘sig’i hisoblanadi.

Брандмауэр - метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизации доступа к сети и контроля

за ним аппаратно-программными средствами; еще - является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра).

Firewall - a method of protecting a network against security threats from other systems and networks, through centralizing network access and control hardware and software; - is a protective barrier consisting of several components (e.g., router or gateway running firewall software).

Imtiyozlar - hisoblash tizimida ma’lum obyektlardan foydalanish va ularda ishlashdan iborat foydalanuvchilarning yoki dasturning huquqlari.

Привилегии - права пользователя или программы, состоящие в доступности определенных объектов и действий в вычислительной системе.

Privilege - rights of the user or a program, consisting in the availability of certain objects and actions in a computing system.

Ilova – bevosita foydalanuvchi uchun boshqarish, monitoringlash tizimlaridan yoki ma’muriy imtiyozlardan foydalanmay aniq funksiyani bajaruvchi axborot tizimining dasturiy ta’minoti (dasturi).

Приложение – программное обеспечение (программа) информационной системы, выполняющая определенную функцию непосредственно для пользователя без доступа к системе управления, мониторинга или административным привилегиям.

Application – a software (program) hosted by an information system. In addition, software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

Virtual xususiy tarmoq - tarmoqlar orasida almashiniluvchi ma’lumotlar yoki boshqa axborotni uzatish uchun xavfsiz kommunikatsiya tunnelini ta’minlovchi, mavjud fizik tarmoqlar asosida qurilgan virtual tarmoq.

Виртуальная частная сеть - виртуальная сеть, построенная на основе существующих физических сетей, обеспечивающая безопасный туннель коммуникации для передачи данных или другой информации, передаваемой между сетями.

Virtual private network – a virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

Rollarga asoslangan ruxsatni nazoratlash - resurslardan foydalanishni boshqarish modeli bo‘lib, resurslarda ruxsat berilgan harakatlar shaxsiy subyekt identifikatorining o‘rniga rollar bilan identifikatsiyalanadi.

Контроль доступа на основе ролей - модель для управления доступом к ресурсам, когда разрешенные действия на ресурсы идентифицированы с ролями, а не с личными идентификаторами субъекта.

Role-based access control – a model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

Konfidensiallik – 1. Avtorizatsiyalanmagan shaxs tomonidan olinishi yoki foydalanishi tashkilot uchun jiddiy zarar sababi bo‘la olmaydigan ma’lumotlarning qandaydir sinfi. 2. Alohida shaxslar, modullar, jarayonlar ruxsatisiz aniqlanishi, va foydalanishi mumkin bo‘lmagan axborot xususiyati.

Конфиденциальность – 1. Некоторый класс данных, получение либо использование которых неавторизованными для этого лица не может стать причиной серьезного ущерба для организации. 2. Свойство информации, состоящее в том, что она не может быть обнаружена и сделана доступной без разрешения отдельным лицам, модулям или процессам.

Confidentiality – 1. Some class data, obtaining or the use of which by unauthorized persons could not cause serious damage to the organization. 2. The quality of information, consisting in that it cannot be detected and made available without the permission of individuals, modules or processes.

VI-BO‘LIM

ADABIYOTLAR RO‘YXATI

VI. ADABIYOTLAR RO‘YXATI

I. O‘zbekiston Respublikasi Prezidentining asarlari:

1. Mirziyoev Sh.M. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. – T.: “O‘zbekiston”, 2017. – 488 b.
2. Mirziyoev Sh.M. Milliy taraqqiyot yo‘limizni qat’iyat bilan davom ettirib, yangi bosqichga ko‘taramiz. 1-jild. – T.: “O‘zbekiston”, 2017. – 592 b.
3. Mirziyoev Sh.M. Xalqimizning roziligi bizning faoliyatimizga berilgan eng oliy bahodir. 2-jild. –T.: “O‘zbekiston”, 2018. – 507 b.
4. Mirziyoev Sh.M. Niyati ulug‘ xalqning ishi ham ulug‘, hayoti yorug‘ va kelajagi farovon bo‘ladi. 3-jild.– T.: “O‘zbekiston”, 2019. – 400 b.
5. Mirziyoev Sh.M. Milliy tiklanishdan – milliy yuksalish sari. 4-jild.– T.: “O‘zbekiston”, 2020. – 400 b.

II. Normativ-huquqiy hujjatlar:

6. O‘zbekiston Respublikasining Konstitutsiyasi.–T.:O‘zbekiston, 2018.
7. O‘zbekiston Respublikasining 2020 yil 23 sentabrda qabul qilingan “Ta’lim to‘g‘risida”gi O‘RQ-637-sonli Qonuni.
8. O‘zbekiston Respublikasi Prezidentining 2017 yil 7 fevral “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida”gi 4947-sonli Farmoni.
9. O‘zbekiston Respublikasi Prezidentining 2018 yil 21 sentabr “2019-2021 yillarda O‘zbekiston Respublikasini innovatsion rivojlantirish strategiyasini tasdiqlash to‘g‘risida”gi PF-5544-sonli Farmoni.
10. O‘zbekiston Respublikasi Prezidentining 2019 yil 27 may “O‘zbekiston Respublikasida korrupsiyaga qarshi kurashish tizimini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi PF-5729-son Farmoni.
11. O‘zbekiston Respublikasi Prezidentining 2019 yil 27 avgust “Oliy ta’lim muassasalari rahbar va pedagog kadrlarining uzluksiz malakasini oshirish tizimini joriy etish to‘g‘risida”gi PF-5789-sonli Farmoni.
12. O‘zbekiston Respublikasi Prezidentining 2019 yil 8 oktabr “O‘zbekiston Respublikasi oliy ta’lim tizimini 2030 yilgacha rivojlantirish konsepsiyasini tasdiqlash to‘g‘risida”gi PF-5847-sonli Farmoni.
13. O‘zbekiston Respublikasi Prezidenti Shavkat Mirziyoevning 2020 yil 25 yanvardagi Oliy Majlisga Murojaatnomasi.
14. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2001 yil 16 avgustdagi “Oliy ta’limning davlat ta’lim standartlarini tasdiqlash to‘g‘risida”gi 343-sonli Qarori.
15. O‘zbekiston Respublikasi Vazirlar Mahkamasining 2015 yil 10 yanvardagi “Oliy ta’limning Davlat ta’lim standartlarini tasdiqlash to‘g‘risida”gi

2001 yil 16 avgustdagi “343-sonli qororiga o‘zgartirish va qo‘shimchalar kiritish haqida”gi 3-sonli qarori.

III. Internet saytlar:

16. http:// csec.uz/uz – “Kiberxavfsizlik markazi” davlat unitar korxonasi.

17. http://lex.uz – O‘zbekiston Respublikasi Qonun hujjatlari ma’lumotlari milliy bazasi.

18. http://bimm.uz – Oliy ta’lim tizimi pedagog va rahbar kadrlarini qayta tayyorlash va ularning malakasini oshirishni tashkil etish Bosh ilmiy-metodik markazi.

19. http://ziyonet.uz – Ta’lim portali ZiyoNET.

20. http://unicon.uz – “UNICON.UZ” fan-tadqiqot markazi.