OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

RAQAMLI TEXNOLOGIYALAR 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

“KIBERXAVFSIZLIKNING RIVOJLANISH ISTIQBOLLARI VA TENDENSIYALARI”

MODULI BO‘YICHA

O‘ Q U V –U S L U B I Y M A J M U A

Toshkent - 2025

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

“KIBERXAVFSIZLIKNING RIVOJLANISH ISTIQBOLLARI VA TENDENSIYALARI” (BARCHA YO‘NALISHLAR UCHUN)

MODULI BO‘YICHA

O‘ Q U V –U S L U B I Y M A J M U A

Toshkent – 2025

Modulning o‘quv-uslubiy majmuasi Oliy ta’lim, fan va innovatsiyalar vazirligining 2024 yil 27 dekabrdagi №485-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, DSc, dotsent

Taqrizchilar: **M.Kodirov** - Islom Karimov nomidagi TDTU, Axborot texnologiyalari kafedrasi dotsenti, PhD.

O.M.Allanov – Muhammad al-Xorazmiy nomidagi TATU Kiberxavfsizlik va Kriminalistika kafedra mudiri, Ph.D.

O‘quv-uslubiy majmua O‘quv dasturi Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Kengashining qarori bilan tasdiqqa tavsiya qilingan (2024-yil 27-noyabrdagi 3/4 (745/746)- 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.

O‘zbekiston Respublikasi Prezidentining 2019-yil 8-oktyabrdagi PF-5847-son Farmoni bilan tasdiqlangan “O‘zbekiston Respublikasi Oliy ta‘lim tizimini 2030-yilgacha rivojlantirish konsepsiyasi”da oliy ta‘lim jarayonlariga raqamli texnologiyalar va zamonaviy o‘qitish usullarni joriy etish, yoshlarni ilmiy faoliyatga keng jalb etish, korrupsiyaga qarshi kurashish, muhandislik-texnik ta‘lim yo‘nalishlarida tahsil olayotgan talabalar ulushini oshirish, kredit-modul tizimini joriy etish, o‘quv rejalarida amaliy ko‘nikmalarni oshirishga qaratilgan mutaxassislik fanlari bo‘yicha amaliy mashg‘ulotlar ulushini oshirish bo‘yicha aniq vazifalar belgilab berilgan.

O‘zbekiston Respublikasi Prezidentning 2019-yil 8-oktyabrdagi Farmoni bilan tasdiqlangan “O‘zbekiston Respublikasi oliy ta‘lim tizimini 2030-yilgacha rivojlantirish konsepsiyasi”ga ko‘ra mamlakatdagi oliy ta‘lim muassasalarining 85 foizi 2030-yilgacha bosqichma-bosqich kredit-modul tizimiga o‘tishi rejalashtirilgan. Bu yaqin yillar davomida mamlakatdagi deyarli barcha oliy ta‘lim muassasalarining kredit-modul tizimida faoliyat yurita boshlashidan darak beradi.

Hozirgi kunda dunyo miqyosida axborot texnologiyalarining jadal sur’atlar bilan rivojlanib borishi, aholi uchun juda ko’p imkoniyatlarni yaratishi bilan birga, ushbu texnologiyalar yordamida almashinadigan axborotlarning noqonuniy tarqalishi, o’g’irlanishi, noqonuniy tarzda axborotga egalik qilib, yolg’on axborotga o’zgartirib qo’yilishi kabi bir qator dolzarb masalalarni ham kelib chiqishiga sabab bo’lmoqda.

O’zbekiston Respublikasi Prezidentining 2022 yil 28 yanvardagi “2022 – 2026 - yillarga mo’ljallangan Yangi O’zbekistonning taraqqiyot strategiyasi to’g’risida”gi PF 60-sonli farmoni bilan tasdiqlangan “2022 – 2026 yillarga mo’ljallangan yangi O’zbekistonning taraqqiyot strategiyasi”da “Shaxsiy va sir saqlanishi lozim bo’lgan ma’lumotlarni Internet tarmog’ida oshkor qilish bilan bog’liq daxlsizlik huquqi buzilishining oldini olish” va “Kiberjinoyatchilikning oldini olish tizimini yaratish” bilan bog’liq bo’lgan bir qator vazifalar belgilangan.

Shuningdek, mamlakatimizning barcha sohalarida islohotlarni amalga oshirish, odamlarning dunyoqarashini o‘zgartirish, yetuk va zamon talabiga javob beradigan mutaxassis kadrlarni tayyorlashni hayotning o‘zi taqozo etmoqda. Respublikada ta‘lim tizimini mustahkamlash, uni zamon talablari bilan uyg‘unlashtirishga katta ahamiyat berilmoqda. Bunda mutaxassis kadrlarni tayyorlash, ta‘lim va tarbiya berish tizimi islohatlar talablari bilan chambarchas bog‘langan bo‘lishi muhim ahamiyat kasb etadi. Zamon talablariga javob bera oladigan mutaxassis kadrlarni tayyorlash, Davlat talablari asosida ta‘lim va uning barcha tarkibiy tuzilmalarini takomillashtirib borish oldimizda turgan dolzarb masalalardan biridir.

Modulning maqsadi va vazifalari

Modulning maqsadi: qayta tayyorlash va malaka oshirish kursi tinglovchilarini Kiberxavfsizlikning zamonaviy asoslari haqidagi bilimlarini takomillashtirish, Kiberxavfsizlikning rivojlanishi va muhim tendensiyalari haqida ko’nikmalarga ega bo’lish shuningdek, ularda zamonaviy kiberxavfsizlik asoslari to‘g‘risida ko‘nikma va malakalarini tarkib toptirish.

Modulning vazifalari:

- Kiberxavfsizlikning zamonaviy tushunchalari va konsepsiyalarini o’rganish;
- Kiberxavfsizlikning rivojlanishi va muhim tendensiyalari haqida xabardor bo’lish;
- Kiberhujumlarning milliy xavfsizlik va iqtisodiy barqarorlikka ta’sirlarini o’rganish;
- Kiberxavfsizlikning global xavfsizlik muammolari bilan bog’liqligi haqida ma’lumotlarga eha bo’lish;
- Kiberxavfsizlikning rivojlanish istiqbollarini o’rganish;
- Internet of Things (IoT) da kiberxavfsizlikdan amaliy foydalanish;
- Sun’iy intellekt va kiberxavfsizlikning birgalikda qo’llanilishi;
- Tahdidlarni oldini olish va kiberxavfsizlik sohasidagi yangi yondoshuvlardan foydalanish;
- Tahdid razvedkasini amalga oshirish va kibermudofaa strategiyalarini o’rganish;
- Kiberxavfsizlik siyosatini ishlab chiqish, xavfsizlik operatsiyalari va kiber urush;

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

“Kiberxavfsızlikning rivojlanısh istıqbollari va tendensiyalari” modulini o‘zlashtirish jarayonida amalga oshiriladigan masalalar doirasida:

- **Tinglovchi:**

- Kiberxavfsizlikning zamonaviy tushunchalari va konsepsiyalarini haqida ma’lumotlarga ega bo’ladi va shu boradagi bilimlarini boyitadi;
- Hozirgi kundagi Kiberxavfsizlikning sohasidagi rivojlanayotgan va muhim tendensiyalari haqida xabardor bo’lishadi;
- Kiberhujumlarning milliy xavfsizlikka ta’siri va iqtisodiy barqarorlikka ta’sirlarini o’rganishadi;
- Kiberxavfsizlikning global xavfsizlik muammolari bilan bog’liqligi haqida ma’lumotlarga ega bo’lishadi;
- Kiberxavfsizlikning rivojlanish istiqbollarini o’rganishadi;
- Internet of Things (IoT) da kiberxavfsizlikdan amaliy foydalanish ko’nikmalriga ega bo’lishadi;
- Sun’iy intellekt va kiberxavfsizlikning birgalikda qo’llanilishini amalga oshirishadi;
- Tahdidlarni oldini olish va kiberxavfsizlik sohasidagi yangi yondoshuvlardan foydalanishni o’rganishadi;
- Dasturiy vositalar orqali tahdid razvedkasini amalga oshirish va kibermudofaa strategiyalarini o’rganishadi;
- Tashkilotlar uchun Kiberxavfsizlik siyosatini ishlab chiqishadi, xavfsizlik operatsiyalari va kiber urush haqida ma’lumotlarga ega bo’lishadi;

Modulni tashkil etish va o‘tkazish bo‘yicha tavsiyalar.

“Kiberxavfsizlikning rivojlanish istiqbollari va tendensiyalari” 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

“Kiberxavfsizlikning rivojlanish istiqbollari va tendensiyalari” moduli bo‘yicha mashg‘ulotlar o‘quv rejasidagi “Ta’lim tizimida kiberxavfsizlikning muammosi va strategiyasi” modeli va “Oliy ta’lim jarayonini boshqarishning axborot tizimlari”, “Ta’lim menejerining innovatsion kompetentligi” kabi modullar bilan uzviy aloqadorlikda olib boriladi.

Modulning oliy ta’limdagi o‘rni

Modulni o‘zlashtirish orqali tinglovchilar hozirda kiberxavfsizlikning rivojlanayotgan sohalarini o‘rganish, ularni tahlil etish, amalda qo‘llash va baholashga 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.	Kiberxavfsizlikning rivojlanishi va muhim tendensiyalari	2	2			
2.	Kiberhujumlarning milliy xavfsizlik va iqtisodiy barqarorlikka ta’siri	2	2			
3.	Kiberxavfsizlikning global xavfsizlik muammolari bilan bog’liqligi. Kiberxavfsizlikning rivojlanish istiqbollari	4	4			
4.	Kvant hisoblash va 5G tarmoqlari kabi rivojlanayotgan texnologiyalarni himoya qilish.	2		2		
5.	Sun’iy intellekt va kiberxavfsizlik	2		2		
6.	Internet of Things (IoT) va kiberxavfsizlik	2		2		
7.	Tahdidlarni oldini olish va kiberxavfsizlik sohasidagi yangi yondoshuvlar	4		2	2	
8.	Tahdid razvedkasi va kibermudofaa strategiyalari	6		2	4	
	Jami:	**24**	**8**	**10**	**6**	

NAZARIY MASHG‘ULOTLAR MAZMUNI

1-MAVZU: KIBERXAVFSIZLIKNING RIVOJLANISHI VA MUHIM TENDENSIYALARI (2 soat)

Avtomatlashtirishning kiberxavfsizlikda muhim ahamiyat kasb etishi. Sun’iy intellektning (AI) salohiyati, Bulutli tizimlardagi potentsial zaifliklar, ma’lumotlarning buzilishi, 5G tarmog‘i va IoT: texnologiya va xavflarning yangi

davri, Maqsadli Ransomware, Davlat homiyligidagi kiber urush, Ijtimoiy muhandislik hujumlari, real vaqt rejimida ma'lumotlarni monitoring qilish.

2-MAVZU: KIBERHUJUMLARNING MILLIY XAVFSIZLIK VA IQTISODIY BARQARORLIKKA TA'SIRI (2 soat)

Moliyaviy faoliyat va axborot texnologiyalarning o'zaro bog‘iqligi, Raqamli moliyaviy xizmatlar, Kiberxavfsizlikning milliy xavfsizlikdagi o‘rni, Davlat miqyosidagi tizimlarga kiberhujumlar, Kiberhujumlarning iqtisodiy infratuzilmalarga yetkazadigan zara ko'lamalari.

3-MAVZU: KIBERXAVFSIZLIKNING GLOBAL XAVFSIZLIK MUAMMOLARI BILAN BOG'LIQLIGI (4 soat)

Xalqaro huquq nuqtai nazaridan kiber jinoyatlar, global xavfsizlik tahdidlarini hal qilish muammolari, milliy va xalqaro darajada kiberjinoyatlar, xalqaro hamkorlik, xalqaro va milliy miqyosda qo‘llaniladigan qoidalar va siyosatlar, kiberjinoyatchilik va global xavfsizlik tahdidlariga qarshi kurash.

Kiberxavfsizlik kelajagi, Kiber tahdid va xavf-xatarlarning yangi to‘lqinlari, bulutli xizmatlar va aqlli texnologiyalar, ma'lumotlarni himoya qilish bo'yicha yangi strategiyalar, Kiberxavfsizlikda kvant texnologiyalar, Kripto va NFT firibgarliklari.

AMALIY MASHG‘ULOTLAR MAZMUNI

1-AMALIY MASHG‘ULOT

1-MAVZU: KVANT HISOBLASH VA 5G TARMOQLARI KABI RIVOJLANAYOTGAN TEXNOLOGIYALARNI HIMOYA QILISH (2 soat)

5G tarmoq arxitekturasi va uning xavfsizligini ta'minlanganligi, Kvant hisoblash texnologiyalari xavfsizligi, Kvant kriptografiya, 5G tarmog'ida tahdidlar va ularni bartaraf etishda yechimlar, Kvant texnologiyalaridan kiberxavfsizlikda foydalanish.

2-MAVZU: SUN'IY INTELLEKT VA KIBERXAVFSIZLIK (2 soat)

Sun'iy intellektning istiqbollari, kiberxavfsizlikda SI ning afzalliklari, SI orqali Buzilish xavfini bashorat qilish, yangi tahdidlarni SI yordamida aniqlash, kiberxavfsizlikda botlardan foydalanish, zamonaviy kiberxavfsizlik masalarini yechishda sun'iy intellektdan foydalanish.

3-MAVZU: INTERNET OF THINGS (IOT) VA KIBERXAVFSIZLIK (2 soat)

IoT, IIoT (Industrial IoT, Sanoat IoT), IoT da kibertahdidlar va zaifliklar, IoT da autentifikatsiya, IoT hujum maydoni, tahdidlar va xavfsizlik yechimlari, Internet orqali bulut hujumlari, SI xavfsizlik muammolari.

4-MAVZU: TAHDIDLARNI OLDINI OLISH VA KIBERXAVFSIZLIK SOHASIDAGI YANGI YONDOSHUVLAR. (2 soat)

Kiberxavfsizlikni zamonaviy bartarf etish yo'llari, rivojlanayotgan kibertahdidlar, Kiberxavfsizlikka ko'p qirrali yondashuvlar, xavfsiz va bardoshli modelga o'tish, xavfsizlik strategiyasi.

5-MAVZU: TAHDID RAZVEDKASI VA KIBERMUDOFAA STRATEGIYALARI. (2 soat)

Tahdid razvedkasini amalga oshirish vositalari, pentesting tushunchasi, Kali Linux Operatsion tizimidan foydalanish, Kibermudofa strategiyasini ishlab chiqish.

KO‘CHMA MASHG‘ULOT

Tahdidlarni oldini olish va kiberxavfsizlik sohasidagi yangi yondoshuvlar (2 soat)

TATU Texnologiyalar transferi, inkubatsiya va akseleratsiya bo‘limi o‘quv laboratoriyasida olib borilayotgan loyihalar misolida imkoniyatlarini namoyish etish.

Tahdid razvedkasi va kibermudofaa strategiyalari (4 soat)

TATU o’quv-ilmiy laboratoriyasida olib borilayotgan loyihalar misolida imkoniyatlarini namoyish etish.

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. MODULNI O‘QITISHDA FOYDALANILADIGAN INTERFAOL TA’LIM METODLARI

“Blum kubigi” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborotlar tizimini qabul qilish va bilimlarni o‘zlashtirilishini yengillashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun “Ochiq” savollar tuzish va ularga javob topish mashqi vazifasini belgilaydi.

Metodni amalga oshirish tartibi:

1. Ushbu metodni ko‘llash uchun, oddiy kub kerak bo‘ladi. Kubning har bir tomonida quyidagi so‘zlar yoziladi:

- **Sanab bering, ta’rif bering (oddiy savol)**
- **Nima uchun (sabab-oqibatni aniqlashtirovchi savol)**
- **Tushintirib bering (muammoni har tomonlama qarash savoli)**
- **Taklif bering (amaliyot bilan bog‘liq savol)**
- **Misol keltiring (ijodkorlikni rivojlantirovchi savol)**
- **Fikr bering (tahlil kilish va baxolash savoli)**

2. O‘qituvchi mavzuni belgilab beradi.
3. O‘qituvchi kubikni stolga tashaydi. Qaysi so‘z chiqsa, unga tegishli savolni beradi.

“KWHL” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborotlar tizimini qabul qilish va biliimlarni tizimlashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun mavzu bo‘yicha qo‘yidagi jadvalda berilgan savollarga javob topish mashqi vazifasini belgilaydi.

Izoh. *KWHL:*

Know – nimalarni bilaman?

Want – nimani bilishni xohlayman?

How - qanday bilib olsam bo‘ladi? Learn - nimani o‘rganib oldim?

“KWHL” metodi	
1. Nimalarni bilaman:	***2. Nimalarni bilishni xohlayman, nimalarni bilishim kerak:***
3. Qanday qilib bilib va topib olaman:	***4. Nimalarni bilib oldim:***

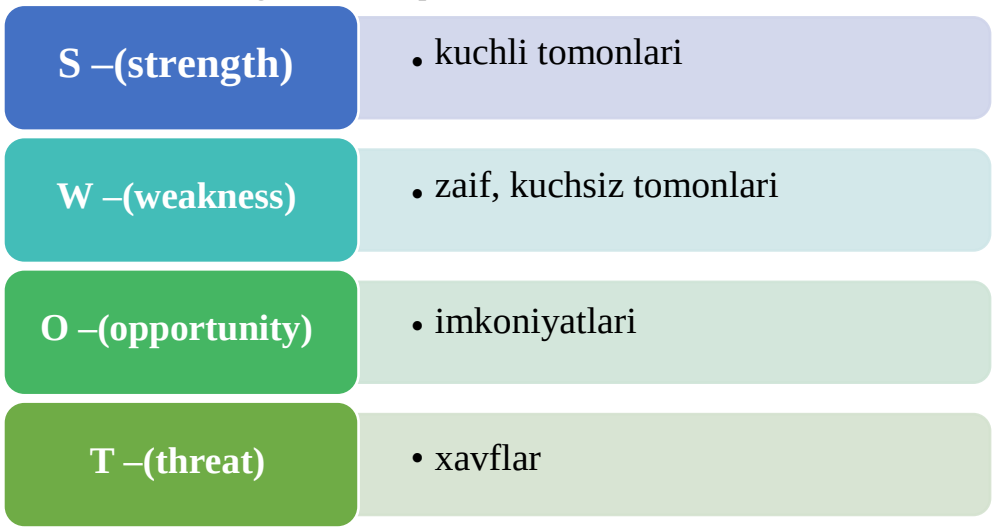
“W1H” metodi

Metodning maqsadi: Mazkur metod tinglovchilarda yangi axborotlar tizimini qabul qilish va biliimlarni tizimlashtirish maqsadida qo‘llaniladi, shuningdek, bu metod tinglovchilar uchun mavzu bo‘yicha qo‘yidagi jadvalda berilgan oltita savollarga javob topish mashqi vazifasini belgilaydi.

What?	Nima? (ta’rifi, mazmuni, nima uchun ishlatiladi)	
Where?	Qayerda (joylashgan, qayerdan olish mumkin)?	
What kind?	Qanday? (parametrlari, turlari mavjud)	
When?	Qachon? (ishlatiladi)	
Why?	Nima uchun? (ishlatiladi)	
How?	Qanday qilib? (yaratiladi, saqlanadi, to‘ldiriladi, tahrirlash mumkin)	

“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.



“VEER” 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. “Veer” 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:

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

trening maqsadi, shartlari va tartibi bilan ishtirokchilarni tanishtirgach, 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, zaruriy axborotlr bilan to‘ldiriladi va mavzu vakunlanadi.

Muammoli savol					
1-usul		**2-usul**		**3-usul**	
afzalligi	kamchiligi	afzalligi	kamchiligi	afzalligi	kamchiligi
Xulosa:					

“Keys-stadi” metodi

“Keys-stadi” - inglizcha so‘z bo‘lib, (“case” – aniq vaziyat, hodisa, “stadi” – 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 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 iyerarxiyasini 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

“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.

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

Test	**Muammoli vaziyat**
Tushuncha tahlili (simptom)	**Amaliy vazifa**

“Insert” metodi

Metodni amalga oshirish tartibi:

- o‘qituvchi mashg‘ulotga qadar mavzuning asosiy tushunchalari mazmuni yoritilgan 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	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.

III-BO‘LIM

NAZARIY MATERIALLAR

III. NAZARIY MATERIALLAR

1-ma’ruza Kiberxavfsizlikning rivojlanishi va muhim tendensiyalari (2 soat)

Reja:

1.1. Kiberxavfsizlikning fundamental tushunchalari.
1.2. Kiberxavfsizlik siyosati va uni boshqarish.
1.3. Xavf-xatarlarni boshqarish.
1.4. Hujum insidentlari va ularga qarshi reaksiya.
1.5. Kiberxavfsizlik tendensiyalari
1.6. Kiberxavfsizlik razvedkasi
1.7. Zamonaviy Xavfsizlik Operatsion Markazi
1.8. Fishinga qarshi zamonaviy SOAR dan foydalanish

Tayanch iboralar: *Kiberxavfsizlik**,** Konfidensiallik, Yaxlitlik, Foydalanuvchanlik, Ma’lumotlar xavfsizligi, Dasturiy ta’minotlar xavfsizligi, Tashkil etuvchilar xavfsizligi, Aloqa xavfsizligi, Tizim xavfsizligi, Inson xavfsizligi, kiberxavfsizlik risklari, Risklarni identifikatsiya qilish, Hodisa, Insident , Hujum, ITRM modeli. Kiberxavfsizlikda biznes**,** Tendensiyalar, Kazvedka hujumi, KTR, XOM, NIST, Fishing, SOAR, kriptoanaliz, kriptografiya.*

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.

Kiberxavfsizlik siyosati tashkilotning maqsadi va vazifasi hamda xavfsizlikni ta’minlash sohasidagi chora-tadbirlar tavsiflanadigan yuqori sathli rejasidir.

Kiberxavfsizlik konsepsiyasi axborot xavfsizligi muammosiga rasmiy qabul qilingan qarashlar tizimi va uni zamonaviy tendensiyalarni hisobga olgan holda yechish yo‘llaridir.

Tarmoq sohasida faoliyat yuritayotgan Cisco tashkiloti esa kiberxavfsizlikka quyidagicha ta’rif bergan: Kiberxavfsizlik – tizim, tarmoq va dasturlarni raqamli hujumlardan himoyalash amaliyoti. Ushbu kiberhujumlar odatda maxfiy axborotni boshqarishni, almashtirishni yoki yo‘q qilishni; foydalanuvchilardan pul undirishni;

normal ish faoliyatini buzishni maqsad qiladi. Hozirda samarali kiberxavfsizlik choralarini amalga oshirish insonlarga qaraganda qurilmalar va ularning turlari sonining kattaligi va buzg‘unchilar salohiyatini ortishi natijasida amaliy tomondan murakkablashib bormoqda. Tarmoq skanerlari masofaviy yoki lokal tashxis dasturi bo‘lib, u tarmoqning turli elementlarida har xil zaifliklarni aniqlaydi. Ilova skanerlari aniq MBBT, Web-brauzerlari va boshqa amaliy tizimlarga mo‘ljallangan.

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

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 (butunlilik) – 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. Axborot yaxlitliligini ta’minlahda xesh funskiyalardan foydalaniladi. Xesh funksiya ixtiyoriy uzunlikdagi (bit yoki bayt birliklarida) ma’lumotni biror fiksirlangan uzunlikdagi (bit yoki bayt birliklarida) qiymatga o‘tkazuvchi funksiyadir.

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).

Avtorizatsiya identifikatsiya, autentifikatsiya jarayonlaridan o‘tgan foydalanuvchi uchun tizimda bajarishi mumkin bo‘lgan amallarga ruxsat berish jarayonidir.

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. Risk hodisadan kelib chiqadigan oqibatlar va voqea-hodisa yuzaga kelishi ehtimolligi birikmasini o‘zida ifodalaydi. Risklarni identifikatsiya qilishdan maqsad potensial zarar yetkazadigan ehtimoliy insidentlarni prognozlash va bu zarar qay tarzda olinishi mumkinligi to‘g‘risida tasavvurga ega bo‘lish hisoblanadi. Riskni aniqlash tadbirlari Risklarni aniqlash; risklarni identifikatsiya qilish; risklarni tahlil qilish; risklarni baholashni o’z ichiga oladi. Risklarni aniqlash axborot aktivlarining ahamiyatini belgilaydi, mavjud (yoki mavjud bo‘lishi mumkin) qo‘llaniladigan tahdidlar va zaifliklarni identifikatsiya qiladi, mavjud boshqarish vositalarini va ularning identifikatsiya qilingan risklarga ta’sirini identifikatsiya qiladi, potensial oqibatlarni aniqlaydi va nihoyat, ustuvorliklarga muvofiq, muayyan risklarni joylashtiradi va kontekstni o‘rnatishda aniqlangan risklarni baholash mezonlari bo‘yicha ularni tasniflaydi.

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. Risklarni davolash aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayonidir.

Kiberxavfsizlikda yoki axborot xavfsizligida risklarga salbiy ko‘rinishda qaraladi.

Identifikatsiya subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim etish jarayoni hisoblanadi.

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.

Insident - standart operatsiyalar qatoriga qo‘shilmaydigan hamda xizmat holatini uzib qo‘yish yoki xizmat sifati yomonlashishi holatlariga olib keladigan har qanday hodisaga aytiladi. Xavfsizlik insidenti koordinatori insidentga javob qaytarish jarayonini boshqaradi va komandani to‘plash uchun javobgar shaxsdir. Insidentni tergov qilish insident holatini tergov qilish harakatidir. Insidentga javob qaytarish xavfsizlikni buzilish ketma-ketligi yoki hujumni boshqarish va yechish uchun ishlab chiqilgan usuldir.

Hodisa - shaxs yoki ishchi jarayonni, jarayonni, o‘rab olgan muxit va tizimni normal holatini o‘zgartirishni nazorat etishdir. *Normal hodisa* kritik komponentalarga ta’sir qilmaydi yoki ko‘rsatma (rezolyusiya)ni boshlanishidan oldin o‘zgartirishni nazorat etishni talab qiladi.

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 xarakteristikalari (xususiyatlarini) saqlanishini ta’minlovchi axborotning himoyalanish darajasi holati.

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

Aktiv - himoyalanuvchi axborot yoki resurslar. 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 oshirilishi 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-harakatlari 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‘oz ko‘rinishidagi, elektron va insonlar fikrlashida, og‘zaki va vizual) 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.

“*Ma’lumotlar xavfsizligi*” bilim sohasining maqsadi ma’lumotlarni saqlash, ishlash va uzatishda himoyani ta’minlash. Mazkur bilim sohasida himoyani to‘liq amalga oshirish uchun matematik va analitik algoritmlardan foydalaniladi. Ma’lumotlar xavfsizligi ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi.

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

“*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 xatti-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.

Kiberxavfsizlikda inson omili.

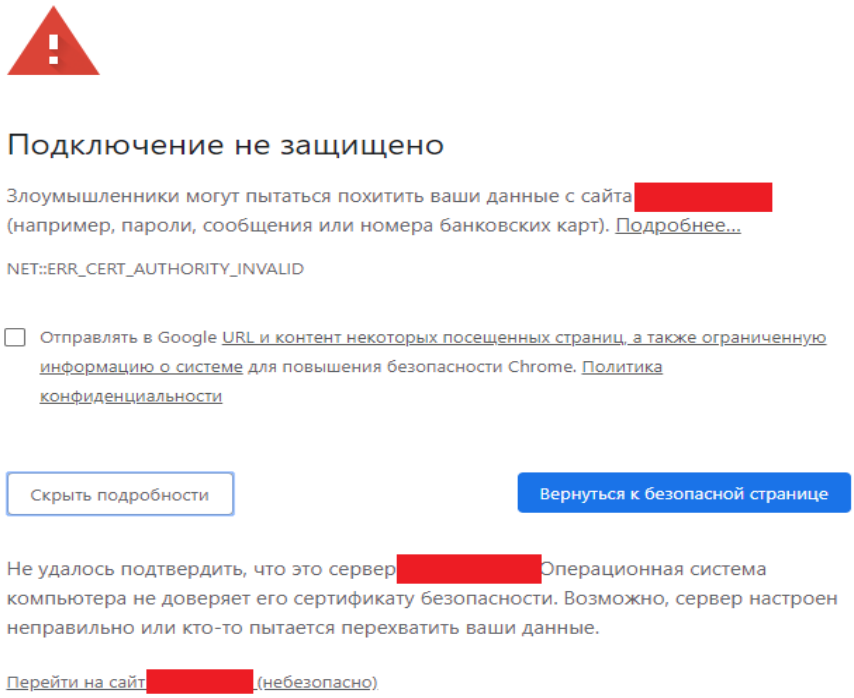
Foydalanuvchilarga kiberxavfsizlik tizimidagi eng zaif nuqta sifatida qaraladi. Foydalanuvchilar tomonidan har qanday yuqori darajadagi xavfsizlik ham buzilishi mumkin. Masalan, Bob amazon.com onlayn do‘konidan biror narsani sotib olmoqchi, deylik. Buning uchun Bob turli kriptografik usullarga tayanadigan SSL (Secure XOMkets 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. Quyida bir nechta hujum turlari keltiriladi.

Web-hujumlar web texnologiyalar orqali tashkilotning tizimiga ruxsatsiz ta’sir ko‘rsatishdir.

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.



1.4-rasm. SSL protokolidagi xavfsizlik ogohlantirishi

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 ko‘p hollarda bo‘lishi mumkin bo‘lgan zaifliklar sonini oshiradi. Boshqa tomondan,

insonning sohaga tegishli so‘nggi texnologik bilimlarni o‘zlashtirishi har doim ham yetarli bo‘lmaydi.

– *Risklarni bartaraf etishni va ular haqida xabar berishning yetarli bo‘lmasligi* kiberxavfsizlikda takrorlanuvchi va kutilmagan buzilishlarga sababchi bo‘ladi. Insonlar odatda tashkilotlariga jiddiy xavf soluvchi risk mavjudligini bilishsada, uni oshkor qilishmaydi. Buning asosiy sababi sifatida risk bevosita shaxsning o‘ziga, uni moliyaviy holatiga ta’sir etmasligini yoki oshkor qilinganida shaxsning obro‘si tushishini keltirishadi.

– *Madaniyat va munosabatlardagi muammolarga* tashkilotning o‘zi yoki tashkilot ichki ma’lumotlarini biluvchi norozi va e’tiborsiz xodimning paydo bo‘lishi sababchi bo‘lishi 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 mashg‘ulotlariga kam mablag‘ sarflanishi* boshqarilayotgan xavfsizlik risklari to‘g‘risidagi ma’lumotning kamligi sababchi bo‘ladi. Odatda, soha korxonalaridagi xodimlar mustaqil ravishda kiberxavfsizlik qoidalarini o‘rganishmaydi. Shuning uchun kiberxavfsizlik qoidalarini xodimlarga maxsus mashg‘ulotlar shaklida yetkazish zarur bo‘ladi. Bu esa tashkilotdan xavfsizlik mashg‘ulotlariga yetarlicha mablag‘ sarflanishni talab qiladi.

– *Hisobga olish nuqtasining yagona emasligi* natijasida xavfsizlikning to‘laqonli 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 bo‘ladi. Biroq, tashkilotlardagi xavfsizlik nazoratining murakkabligi bois, nazorat odatda taqsimlangan holda boshqariladi.

– *Ijtimoiy injineriya* asosida xavfsizlik nazoratini aylanib o‘tishda foydalanuvchidan, an’anaviy josuslik texnikasi yordamida, ma’lumotlar qo‘lga 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.

Inson faoliyati xavfsizligi.

Ijtimoiy (sotsial) injineriya - turli psixologik usullar va firibgarlik amaliyotining to‘plami, uning maqsadi firibgarlik yo‘li bilan shaxs to‘g‘risida maxfiy ma’lumotlarni olish. Maxfiy ma’lumotlar - foydalanuvchi ismi/ parollari,

shaxsiy ma’lumotlari, ayblov dalillari, bank karta raqamlari va moliyaviy yoki obro‘sini yo‘qotadigan har qanday ma’lumot.

Mazkur atama xakerlik sohasidan kirib kelgan, *xaker* - kompyuter tizimidagi zaifliklarni qidiradigan odam, boshqacha aytganda “buzg‘unchi”. Hozirgi vaqtda xakerlar har qanday tizimdagi asosiy 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 to‘plangan 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 to‘pladi. U shuningdek, akangizning telefon raqamini ham biladi. Shundan so‘ng, ushbu ma’lumotlar asosida o‘z rejasini tuza boshladi.

Reja: Xaker sizga kechki vaqtda telefon qilib, sizga (sizni ismingiz o‘rniga faqat akangiz ataydigan biror “laqab” ham bo‘lishi mumkin) men akangman deb tanishtiradi va o‘zini ko‘chada bezorilarga duch kelganini, ular barcha narsalarini (telefon, pul, plastik kartochka va h.k.) olib qo‘yganini aytadi. Bundan tashqari, u o‘ziga bir qiz yordam berganini, biroq, uning yonida puli yo‘qligini aytadi. Shu bilan birga, ushbu qizni yonida plastik kartasi borligini va sizdan ushbu plastik kartaga kasalxonaga yetib borish uchun zarur bo‘lgan 20 000 so‘m pulni ko‘chirib berishni talab qiladi. Mazkur holatlarning 80 foizida xakerlar muvaffaqqiyatga erishganlar va bu ishlarni amalga oshirish malakali xaker uchun qiyinchilik tug‘dirmaydi.

Mazkur holda akangizni ovozini ajratish imkoniyati haqida gap borishi mumkin. Biroq, inson turli hayojon va shovqin bo‘lgan muhitda bo‘lishi mumkin. Bundan tashqari, agar siz uxlab yotgan vaqtingizda telefon bo‘lsa, ovozni aniqlashingiz yanada qiyinlashadi.

Ushbu holatda xaker tomonidan foydalanilgan fikrlarni ko‘rib chiqaylik:

1. Shaxsini yaxshi yashirgan va real misollarga asoslangan (masalan, sizning rasmlaringiz, faqat sizning yaqinlaringiz biladigan joylar va h.k.) yaxshi afsona o‘ylab 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 bog‘liq tahdidlarni quyidagicha tasniflash mumkin:

Telefon bilan bog‘liq tahdidlar. Telefon hanuzgacha tashkilotlar ichida va ular o‘rtasidagi aloqaning eng keng tarqalgan usullaridan biri hisoblanadi. Shuning uchun, u sotsial injineriya uchun samarali vosita bo‘lib qolmoqda. Telefonda

gaplashayotganda, suhbatdoshining shaxsini tasdiqlashning imkoni yo‘q. Bu hujumchilarga xodimning, xo‘jayinning maxfiy yoki muhim tuyuladigan ma’lumotlarga ishonishi mumkin bo‘lgan har qanday shaxsning o‘rnida bo‘lish imkonini beradi. Bunda, zo‘ravonlik 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 foydalanishini oldini olish uchun ishlab 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 xabar almashish – ma’lumotlarni uzatishning nisbatan yangi usuli. 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 tamoyillarini 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 etadilar:

- 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 tamoyillarini aniqlash kerak.

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

Kompyuterlar. Korporativ kompyuterlarda qaysi dasturlardan foydalanish mumkinligini ko‘rsatadigan qat’iy tamoyillarni belgilash, foydalanuvchilar kompyuterlariga to‘g‘ridan-to‘g‘ri hujumlardan himoya qilish.

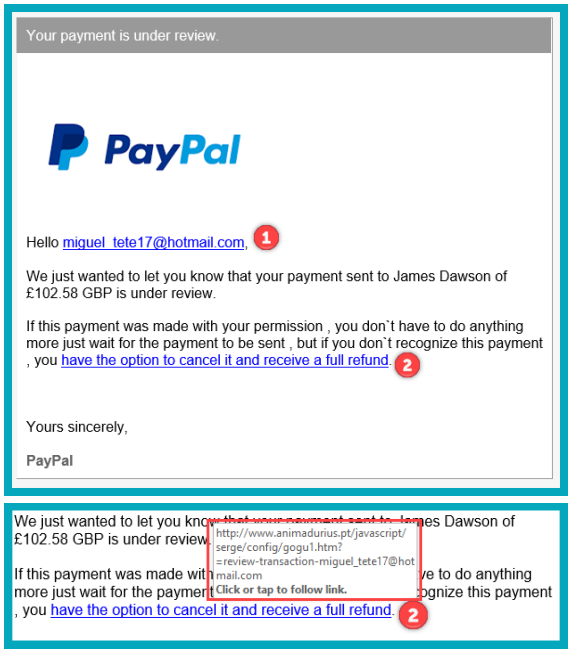
Ichki tarmoq. Korxona tizimlariga ta’sir qiladigan tarmoq, u mahalliy, global yoki simsiz bo‘lishi mumkin. So‘nggi yillarda masofadan ishlaydigan usullarning ommaviylashi sababli, ichki tarmoqlarning chegaralari sezilarli darajada o‘zboshimchalik bilan kengaytirildi. Kompaniya xodimlari har qanday tarmoq muhitida xavfsiz ishlarni tashkil qilishda nima qilish kerakligini tushunishlari lozim.

Tarmoq perimetri. Kompaniyaning ichki tarmoqlari va tashqi, masalan, Internet yoki hamkor tashkilotlar tarmoqlari o‘rtasidagi chegara. Tarmoq sathidagi ma’lumotlar birligining nomi paket. OSI modelidagi kanal sathi MAC manzillari bilan shug‘ullanadi. Switch OSI modelining 2-qatlamida ishlaydi. Hub OSI modelining 1-qatlamida ishlaydi. IPv4 manzilining uzunligi 4 bayt bo’lsa, IPv6 manzilining uzunligi 128 baytni tashkil etadi.

Sotsial injineriyaga tegishli ko‘plab hujumlar mavjud, quyida ularning ayrimlari keltirilgan:

Fishing. Fishing (ing. Phishing – baliq ovlash) Internetdagi firibgarlikning bir turi bo‘lib, uning maqsadi foydalanuvchining maxfiy ma’lumotlaridan (login/parol) foydalanish imkoniyatiga ega bo‘lish. Bu hozirda keng tarqalgan sotsial injineriya sxemalaridan biri hisoblanadi. Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan hujum fishingdir. Katta hajmdagi shaxsiy ma’lumotlarni keng tarqalishi, fishing “shamolisiz” amalga oshmaydi. Fishingning

eng keng tarqalgan namunasi sifatida jabrlanuvchining elektron pochtasiga yuborilgan rasmiy ma’lumot ko‘rinishidagi bank yoki to‘lov tizimining soxta xabarini ko‘rsatish mumkin. Bunday elektron pochta xabarlari odatda rasmiy web-saytga o‘xshash va shaxsiy ma’lumotlarni talab qiladigan shakldagi qalbaki web sahifaga havolani o‘z ichiga oladi (1.5-rasm). Rasmda keltirilgan birinchi holatda mijozning yoki foydalanuvchining ismi va familiyasini yozish o‘rniga pochta manzili yozilgan bo‘lsa, ikkinchi holatda ko‘rsatilgan havola ustiga sichqoncha olib borilganida, haqiqiy manzilni (www.PayPal.com) emas, balki, boshqa manzilni ko‘rish mumkin.



1.5-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 xabarini 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.

Ma’lumotlarni tinglash va uzatish jarayonidagi o‘zgarishlar hujumi Eavesdropping deb nomlanadi. Dasturiy hujumlar, xususan, virus, qurt yoki DOS hujumi dasturiy yoki apparat ta’minotni buzadi. MiTM o’rtadagi odam hujumidir.

IDS hujumlarni aniqlash tizimining qisqartmasi, IPS esa Hujumni bartaraf etish tizimining qisqartmasi

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 (1.6-rasm).

Kompyuter viruslari kompyuter tizimlarida tarqalish va o‘z-o‘zidan qaytadan tiklanish (replikatsiya) xususiyatlariga ega bo‘lgan bajariluvchi yoki sharxlanuvchi kichik dasturlardir. Quyida kompyuter viruslarining bir necha turlari keltirilgan.

Fayl viruslari bajariluvchi fayllarga turli usullar bilan kiriti ladi (eng ko‘p tarqalgan viruslar xili), yoki fayl yo‘ldoshlarni (kompan’on viruslar) yaratadi yoki faylli tizimlarni (link viruslar) tashkil etish xususiyatidan foydalanadi.

Makroviruslar axborotni ishlovchi zamonaviy tizimlarning makro dasturlarini va fayllarini, xususan MicroSoft Word, MicroSoft Excel va h. kabi ommaviy muharrirlarning fayl xujjatlarini va elektron jadvallarini zaharlaydi.

Tarmoq viruslari o‘zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi. Ba’zida ular "qurt" xilidagi dasturlar deb yuritishadi va Internet qurtlarga (Internet bo‘yicha tarqaladi), IRCqurtlarga (chatlar, Inter-net Relay Chat) bo‘linadi.

Rezident viruslar faollashganlaridan so‘ng to‘laligicha yoki qisman yashash muhitidan (tarmoq, yuklama sektori, fayl) hisoblash mashinasining asosiy xotirasiga ko‘chadi.

Rezident bo‘lmagan viruslar faqat faollashgan vaqtlarida hisoblash mashinasining asosiy xotirasiga tushib, zaxarlash va zararkunandalik vazifalarini bajaradi.

Viruslar-«yo‘ldoshlar» fayllarni o‘zgartirmaydi. Uning ta’sir mexanizmi bajariluvchi fayllarning nusxalarini yaratishdan iboratdir.

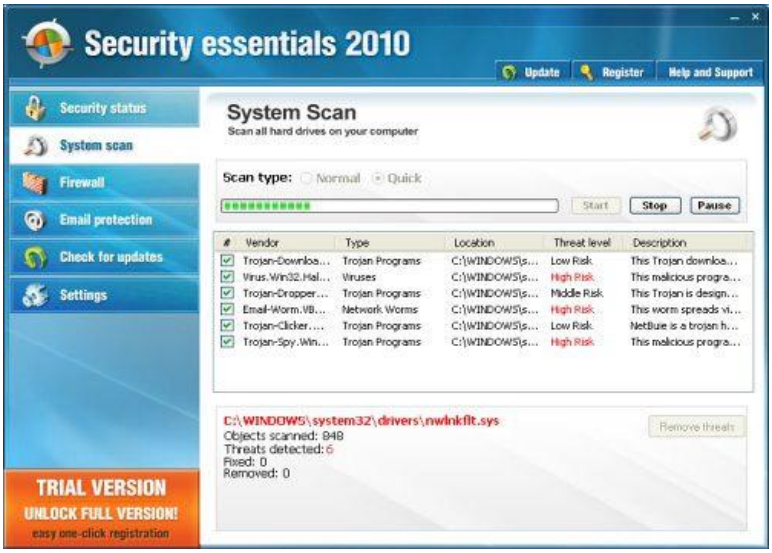
Viruslar-«qurtlar» (worm) tarmoq orqali ishchi stansiyaga tushadi, tarmoqning boshqa abonentlari bo‘yicha virusni jo‘natish adreslarini hisoblaydi va virusni uzatishni bajaradi.

Adware marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko‘rish rejimini kuzutib boruvchi dasturiy ta’minot.

Spyware foydalanuvchi ma’lumotlarini qo‘lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.

Rootkits zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma’lum harakatlarini yashiradi.

Backdoors zararli dasturiy kodlar bo‘lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o‘tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo‘lish.



1.6-rasm. “Security Essentials 2010” antivirus dasturi

Talaba viruslar odatda, rezident bo‘lmagan viruslar qatoriga kiradi, ularda ko‘pincha xatoliklar mavjud bo‘ladi, osongina taniladi va yo‘qotiladi.

«Stels» viruslar (ko‘rinmaydigan viruslar) operatsion tizimning shikastlangan fayllarga murojaatlarini ushlab qolish yo‘li bilan o‘zini yashash makonidagiligini yashiradi va operatsion tizimni axborotning shikastlanmagan qismiga yo‘naltiradi.

Polimorf viruslar doimiy tanituvchi guruxlar-signaturalarga ega bo‘lmaydi.

IVR (InteraKTRve 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 va h.k.

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, 2003-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 imkoniyatiga ega bo‘ladi.

Yelka orqali qarash. 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.k.

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»;

Kiberxavfsizlik biznesning asosiy talabi bo‘lib, korxonangizni o‘zgartirish va biznesingizni qo‘llab-quvvatlash uchun ishonchli poydevor yaratadi. Hozirgi, misli ko‘rilmagan geosiyosiy o‘zgarishlar bunday yangilangan e'tiborni yanada muhimroq qiladi.

Kiberxavfsizlik tendentsiyalari u barcha nuqtai nazardan kiberxavfsizlik bilan shug'ullanadigan mutaxassislarning umumiy tajribasini o‘z ichiga oladi. Birgalikda u kiberxavfsizlik strategiyalarini shakllantirishga yordam beradigan tushunchalar to‘plami bo‘lib xizmat qiladi.

An'anaga ko‘ra, kiberxavfsizlik ITga yo‘naltirilgan soha sifatida qaraladi va shu tarzda ustuvor hisoblanadi. Biz tez-tez kiberxavfsizlik texnologik muammo sifatida qaraladigan davlat va xususiy kompaniyalarni uchratamiz. Natijada, xavfsizlikning etishmasligi butun tashkilotga jiddiy ta'sir ko‘rsatishi mumkin bo‘lgan ta'sir ko‘pincha e'tiborga olinmaydi..

Kibertahdid razvedkasi (KTR) tahdidlarni aniqlash va ularga javob berish uchun innovatsion vositalar bilan birlashtirilgan tahlilchilarga asoslangan metodologiyadir. Asosiysi, KTR - bu dushmanning qobiliyati, niyati va imkoniyatlarini tushunish biznesidir, bu tahdid sub'ektlari nimani xohlashini va unga erishish uchun ular foydalanadigan son-sanoqsiz taktikalar, usullar va protseduralardir. KTR hujum sodir bo‘lishidan oldin qayerda sodir bo‘lishini aytib beradigan kristalli sharmi yoki bu sizning xavfsizlik vositalaringizga infratuzilmangizga allaqachon kirib borgan tahdidlarni aniqlashga yordam beradigan murosa ko‘rsatkichlaridir.

Kiberetika - kompyuterlar bilan bog‘liq falsafiy soha bo‘lib, foydalanuvchilarning hatti – harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta’sir ko‘rsatishini o‘rganadi.

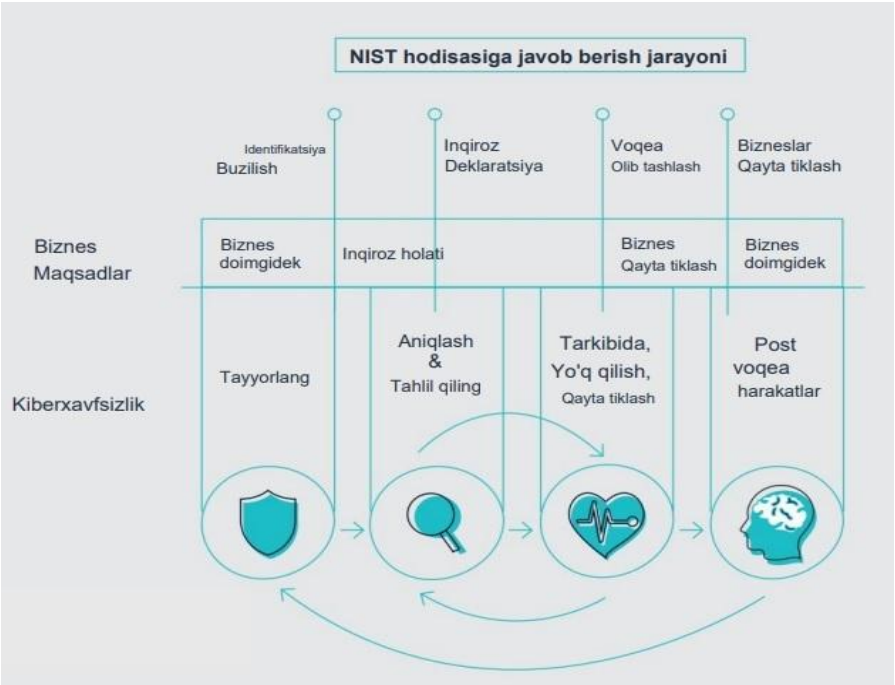
Hodisalarni kengayishi va ko‘payishi (Eskalatsiya) jiddiy ta’sir ko‘rsatadi yoki amalga oshirilgan ko‘rsatma (rezolyusiya) o‘zgartirishni nazorat etish

jarayonini kuzatishini ta’minlab berishi shart. Avariyaviy hodisa shaxs xavfsizligi va sog‘ligiga ta’sir ko‘rsatadi.

Passiv razvedka hujumlari trafik orqali axborotni to‘plashga harakat qiladi. Aktiv razvedka hujumlari portlarni va operatsion tizimni skanerlashni o‘z ichiga oladi.

KTR ni taktik, operatsion va strategik razvedkaga bo‘lish mumkin. Ushbu turli toifalarni va ularning mo‘ljallangan auditoriyalarini tushunish KTRning kiber hodisalarga javob berish (IR) va undan tashqarida qanday foyda keltirishi mumkinligini tushunish uchun kalit hisoblanadi. Taktik tahdidlar bo‘yicha razvedka turlarning eng texnikidir va ko‘pincha mashina tomonidan o‘qilishi mumkin - masalan, bular "ma'lum-yomon" IP manzillarni, fayl xeshlarini, URL manzillarini va boshqalarni aniqlashni avtomatlashtirish uchun ishlatilishi mumkin bo‘ladi..

O‘tmishda tahdid aktyori tomonidan ko‘rsatilgan ish tartibini tushunish bizga kelajakda ularning xatti-harakati va javobini bashorat qilish uchun ko‘proq imkoniyat beradi. Va nihoyat, strategik razvedka mavjud bo‘lib, u tashkilot yo‘nalishi bo‘yicha qaror qabul qilishda etakchilikka yordam berishga qaratilgan - bu xavflarni boshqarish, biznes strategiyasi, resurslarni taqsimlash va byudjet ustuvorligini ko‘rib chiqishda yordam beradigan razvedkadir. Voqealarga javob berishda Milliy Standartlar va Texnologiyalar Instituti (NIST) faoliyatning to‘rt bosqichini belgilaydi: tayyorgarlik, aniqlash va tahlil qilish, oldini olish, yo‘q qilish va tiklash va voqeadan keyingi faoliyat (1.7-rasm). Keling, KTR ushbu bosqichlarning har birini qanday qo‘llab-quvvatlashini ko‘rib chiqaylik.



1.7-rasm.NIST hodisasiga javob berish jarayoni

Kiber inqiroz va "muntazam" inqiroz o‘rtasidagi farqni tushunish muhimdir. Tashkilotlarda ko‘pincha inqiroz rejasi yoki jamoasi mavjud, ammo bu siz duch keladigan noyob dilemmalar tufayli etarli bo‘lmasligi mumkin. Ransomware hujumi kabi kiber inqiroz paytida texnik tajriba va strategik qaror qabul qilishni talab qiladigan muhim qarorlar qabul qilinishi kerak. Bu qarorlar, masalan, tizimlar yoki tarmoqlarni uzish, xaker bilan muzokaralar olib borish, ma'lumotni ommaga yetkazish kerakmi va albatta: siz tovlamachilik uchun to‘lovni to‘lashga tayyormisiz (va qodir)mi? Aslini olganda, texnik muammo bo‘lsa-da, to‘lov dasturi hujumi ko‘pincha ta'sir va miqyosga ega bo‘lib, bu sizning biznesingizning asosini jiddiy ravishda buzadi. Shuni yodda tutingki, bugungi kunda ko‘p darajali tovlamachilik xakerlari ko‘proq qo‘llaniladi. Siz nafaqat kirish imkoni bo‘lmagan tizimlar bilan, balki sotilishi, ommaga oshkor etilishi yoki boshqa zararli maqsadlarda ishlatilishi mumkin bo‘lgan ma'lumotlarni o‘g'irlash bilan ham shug'ullanayotgan bo‘lishingiz mumkin; hammasi xakerlarning talablarini qondirish uchun tashkilotingizga bosimni kuchaytiradi. Bu erda qiyinchilik shundaki, kiber bo‘lmagan mutaxassislar texnik mavzu bo‘yicha keng qamrovli va potentsial yuqori ta'sirli qarorlar qabul qilishlari kerak.

Inqirozni to‘g'ri boshqarish uchun qaysi rollarni jalb qilish va bu rollarning vazifalari va mas'uliyati aniq bo‘lishi kerak. Bu sizning texnik mutaxassislaringiz va yuqori rahbariyatingizni jalb qilishni talab qiladi va siz inqirozni boshqarish uchun zarur bo‘lgan ma'lumot va kirishni to‘plashda kim ishtirok etishini va muvofiqlashtirish va qaror qabul qilish jarayoni qanday amalga oshirilishini tasvirlashingiz kerak bo‘ladi.

Zamonaviy Xavfsizlik Operatsion Markazining (XOM) vazifasi tez o‘sib borayotgan va o‘zgaruvchan tahdidlar manzarasidan oldinda turishdir. 2021-yilda Checkpoint kiberhujumlarning 2020-yilga nisbatan 50 foizga o‘sishini kuzatdi. Bu tendentsiyalar XOM lar uchun ish yukining ortib borishiga va malakali XOM xodimlarining yetishmasligiga olib keladi. XOM xodimlari uchun haddan tashqari ish yuki xavfsizlik ogohlantirishlariga zudlik bilan javob berishga qisqa muddatli e'tiborni qaratishi mumkin. Eng yomoni, har bir ogohlantirishga o‘z vaqtida javob berishga vaqt ham yo‘q. Bu tajovuzkorlarga aniqlanmaslik va qo‘shimcha zarar etkazish imkonini beradi, agar darhol javob berilsa, ularni minimallashtirish mumkin edi. Bundan tashqari, qisqa muddatli e'tibor jarayonlar va standart operatsion tartib-qoidalarni yaratish va takomillashtirish uchun XOMlarning etuklashishiga to‘sqinlik qiladi. Bu faqat xavfsizlik ogohlantirishlariga javob berish uchun zarur bo‘lgan vaqt va kuchni oshiradi, natijada pastga tushadigan spiral paydo bo‘ladi.

Eng qadimiy kibertahdidlardan biri va hali ham rivojlanayotgan bu fishingdir. Bu har bir tashkilotga o‘z odamlariga hujum qilish orqali ta'sir qiladi, odatda eng

zaif bo‘g'in deb ataladi. Tashkilotlar o‘zlarini, xodimlarini, mijozlarini va yetkazib beruvchilarini kiberhujumlarning salbiy ta'siridan himoya qilishlari uchun fishing hujumlarini yumshatish juda muhimdir. Fishing elektron pochta xabar qilinishi mumkin bo‘lgan katta hajm va ularni tahlil qilish uchun tez-tez takrorlanadigan va qo‘lda bajariladigan vazifalar allaqachon haddan tashqari yuklangan xodimlarga ko‘proq ish yukini oshiradi.

Fishing SOAR XOM samaradorligini oshirishi mumkin bo‘lgan sohalardan biridir. Buni SOARning ikkita asosiy komponenti bilan izohlash mumkin: Orkestratsiya va Avtomatlashtirish. Orkestratsiya jarayonlaringizni raqamli ish oqimlariga tartibga solish yoki standartlashtirishni anglatadi. To‘g'ri va puxta o‘ylangan jarayonlarga ega bo‘lish samarali SOAR uchun muvaffaqiyatning asosiy omillaridan biridir. SOARni amalga oshirish, shuningdek, tashkilotlarni, agar hali bajarilmagan bo‘lsa, ish oqimlarini belgilashga majbur qiladi. Bir tomondan, orkestratsiya sifatni yaxshilashga olib keladi, chunki har bir fishing hisoboti standartlashtirilgan, kelishilgan tarzda ko‘rib chiqiladi. Boshqa tomondan, ushbu standartlashtirish SOARning ikkinchi asosiy komponenti - avtomatlashtirish uchun eshiklarni ochadi. Avtomatlashtirishdan boshlanganda, raqamli fishing ish oqimlarining har bir vazifasi avtomatlashtirish imkoniyatlari uchun tahlil qilinishi kerak. Ba'zi amaliy avtomatlashtirish misollari:

• Artefaktlarni (masalan, URL-manzillar, IP-lar) qo‘shimcha tafsilotlar yoki onlayn manbalardan olingan obro‘-e’tibor ma’lumotlari bilan boyitish;

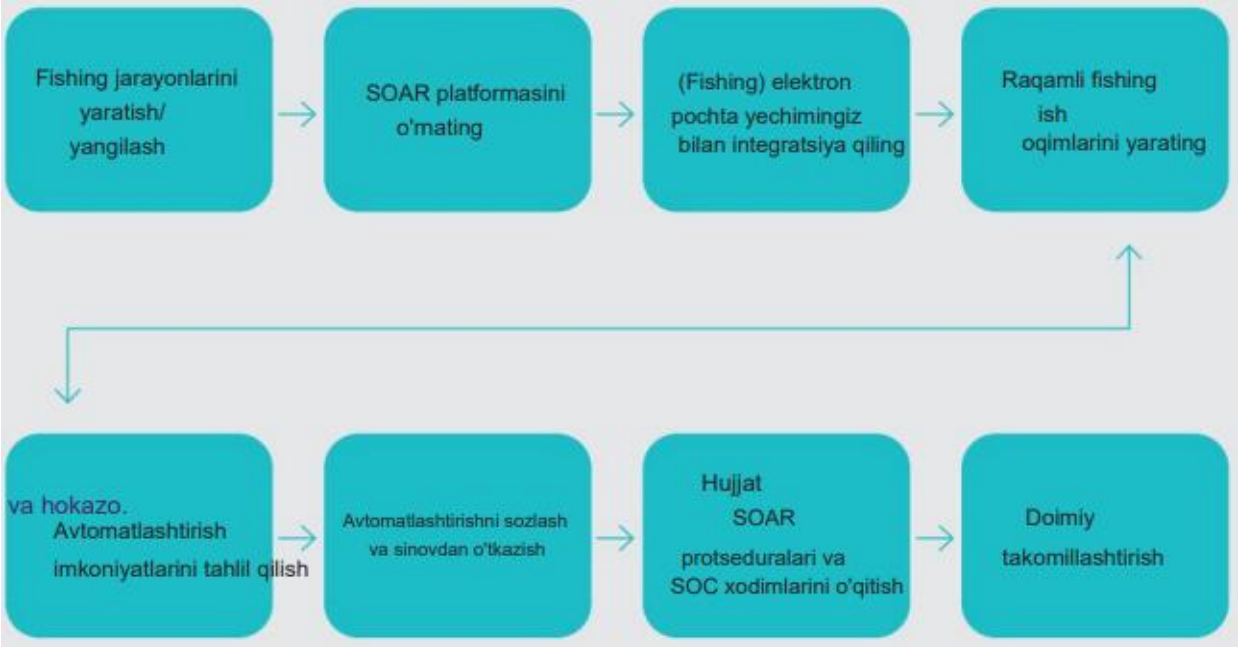
• URL manzillarini fishing ma’lumotlar bazalariga hisobot berish (masalan, Microsoft, Google, Phishtank);

• Zararli domen yoki URL manzilini o‘chirish uchun bildirishnoma va olib tashlash so‘rovlarini (NTD) bajarish.

Analitiklar ularni qo‘lda bajarishlari kerak bo‘lganda, bu misollar ko‘pincha takrorlanadigan va o‘z-o‘zidan talab qilinadigan vazifalar deb hisoblanishi mumkin. Tahlilchilar artefaktlarni to‘plashlari, barcha onlayn manbalarga tashrif buyurishlari, qidiruvlarni amalga oshirishlari, natijalar to‘plashlari, elektron pochta xabarlarini yaratishlari va hokazolar kerak. SOAR yordamida bu qidiruvlarni avtomatlashtirish mumkin va natijalar bitta konsolda taqdim etiladi.

NTDlarni tartibga solish va avtomatlashtirish tufayli bir xil hajmdagi fishing hisobotlari bilan ishlash va hujumlar bilan shug'ullanish uchun kamroq tahlilchilar talab qilinadi. Dastlabki tahlilni avtomatlashtirish orqali SOAR javob vaqtini qisqartiradi va tahlilchilarga qimmatli vaqtlarini murakkabroq masalalarga sarflash imkonini beradi.

Quyida fishing hisobotlaringiz bilan ishlash uchun SOAR dan foydalanmoqchi bo‘lganingizda bir qator zarur qadamlarni taklif qiluvchi kontseptual sharh keltirilgan (1.8-rasm).



1.8-rasm.SOAR dan foydalanish konseptual sharhi.

Umumiy qoida shundaki, AI inson fikrlashdan tezroq. Biz buni tahlil hajmi (DT) yoki javob tezligi (TTR) uchun foydalanishni afzal ko‘ramiz. Shu nuqtai nazardan qaraganda, tezlik yagona haqiqiy ko‘rsatkichdir. Afsuski, bu biroz murakkabroqdir.

AI asosan tahlilni osonlashtirish va yashash vaqtini qisqartirish uchun ishlatilsa, yaxshi aniqlanish xavfsizlik hodisasi bo‘lmagan narsani tekshirishga sarflangan vaqtga olib keladi, chunki voqea ortidagi maqsad zarar keltirmaslik edi. Bu samarasiz tuyulsa-da, u hali ham atrofmuhitni muhofaza qilishda foyda keltirishi mumkin. Tasdiqlangan jarayondan tashqari o‘z ishini bajarayotgan tizim ma'muri hali ham murojaat qilishni talab qilishi mumkin.

Biroq, agar sun'iy intellekt avtomatlashtirilgan javobga va tuzatish vaqtini qisqartirishga qaratilgan bo‘lsa, yaxshi aniqlanishga javob normal IT operatsiyalarini buzishi mumkin. Misol tariqasida, agar AT operatsiyalari guruhlari tizim zaifligini tuzatishga urinayotgan bo‘lsa, lekin AI bu o‘zgarishni zararli deb hisoblasa, AI ushbu operatsiyalarni istisno qilish uchun qayta kalibrlanmaguncha, tuzatish jarayoni buziladi va ishlamaydi.

Ikkala stsenariyning oldini olish uchun asosiy e'tibor bu turdagi noto‘g'ri pozitivlarga AI javobiga bunday istisnolarni amalga oshirish uchun maxsus protseduralarga ega bo‘lishdir. Ammo asosiy sabab aniqlash kontekstini tushunishda yotadi.

Ba'zi sun'iy intellektga asoslangan vositalar sun'iy intellektni tajovuzkorlarning so‘nggi uslublari bo‘yicha yangilab turadigan xizmatlarni taqdim etsa-da, shuni yodda tutish kerakki, hech bir xizmat tashkilotingiz ishtirokisiz o‘zingizning operatsion kontekstingizni faol ravishda qabul qila olmaydi.

Ushbu strategiyani belgilash muhim bo‘lgan sohalarni aniqlashni talab qiladi.

Bu sohalar ko‘pincha sizning xavfsizlik strategiyangiz bilan chambarchas bog'liq. Misol uchun, tashkilotingizning xavf ishtahasi yoki hodisani sud-tibbiy baholashga bo‘lgan ehtiyojini olaylik.

Bulutli infratuzilmaga global kiberhujumlar tahdidining kuchayishi va tashkilotlar o‘z ish yuklarini bulutga o‘tkazish tezligining oshishi bilan miqyosda yuqori darajadagi xavfsizlik holatini saqlab qolish muammosi paydo bo‘ladi. Ushbu muammoni hal qilishning asosiy komponenti bulutli muhit xavfsizligini yaxshilash va saqlash uchun avtomatlashtirishdan foydalanishdir.

Keng miqyosdagi muhitlar tufayli umumiy xavfsizlik muammolarini avtomatlashtirish strategiyalari bilan hal qilish mumkin.

Avtomatlashtirish keng miqyosli bulutlarni joylashtirishning (qisman qo‘lda) ishlashining ortib borayotgan murakkabligini hal qilish va teng bo‘lmagan taqsimlangan tajriba muammolarini engish uchun ishlatilishi mumkin. Avtomatlashtirishni qo‘llash platforma, dastur va operatsion xavfsizlik kabi turli sohalarga ta'sir qilishi mumkin.

Biroq, avtomatlashtirishdan foydalanish jarayonlar yaxshi aniqlangan va xavfsizlik strategiyasi biznes maqsadlariga mos keladigan sohalarda yaxshi ishlaydi.

Ko‘pgina ommaviy bulut provayderlari bulut sotuvchisiga asosiy infratuzilmani tuzatish mas’uliyatini yuklaydigan boshqariladigan yoki PaaS xizmatlarini taklif qiladi. Garchi ular xavfsizlik mas'uliyatini yo‘q qilmasalar ham, ular asosiy operatsion tizimning yangilanib turishini ta'minlaydi va DevOps jamoalariga rivojlanishga ko‘proq vaqt sarflash imkonini beradi.

Biroq, ba'zi ishlanmalardan foydalanish holatlari hali ham DevOps guruhlari asosiy OTga kirishlari mumkin bo‘lgan infratuzilmani talab qiladi va tashkilotlar ushbu infratuzilmani yangilab turish uchun javobgardir. Yangilash muhim xavfsizlik yamoqlari doimiy ravishda, ish yuklarining minimal uzilishi bilan joylashtirilishini ta'minlash uchun bulutda mahalliy avtomatlashtirish vositalaridan foydalangan holda boshqaruvni osonlashtirish mumkin. Ushbu yamoqlarni orkestrlash vositalari muhim yoki xavfsizlik yangilanishlari, ish yukining uzilishini minimallashtirish uchun ushbu yamoqlarni bajarish kerak bo‘lgan mos vaqtlar va avtomatlashtirilgan jarayonga kiritilgan operatsion tizim turlari kabi yamoqlarning toifalarini belgilash uchun o‘zgartirilishi mumkin.

Avtomatlashtirish strategiyasi etuklashgani va avtomatlashtirilgan boshqaruvlar kerakli xavfsizlik holatini ta'minlashda samaraliroq bo‘lishi bilan, ma'lum bo‘lgan noto‘g'ri konfiguratsiyalar va zaifliklarning paydo bo‘lish ehtimoli atrofmuhitda kamayishi kerak.

Bundan tashqari, avtomatlashtirilgan jarayonlar bunday tahdidlarni dasturiy ravishda aniqlash va ularni o‘z ichiga olish va keng miqyosda resurslarni himoya qilish orqali yangi tahdidlar uchun kengaytirilishi mumkin. Ko‘proq komponentlar avtomatlashtirilganligi sababli, xavfsizlik guruhlari harakatni boshqa joyga o‘zgartirishi mumkin.

SAP landshafti aqlli korxonalarning ajralmas qismiga aylandi, chunki SAP ilovalari korxonalarga o‘zlarining turli bo‘limlarini osonlikcha boshqarishning uzluksiz usulini taqdim etadi. Raqamli iqtisodiyot kompaniyalar uchun transformatsiya va kengayish imkoniyatlarini yaratgan holda, SAP mijozlarni SAP ga o‘tishga va moslashuvchan, kengaytiriladigan bulutga asoslangan tizimning afzalliklaridan foydalanishga undaydi. Biroq, murakkab SAP landshaftidagi so‘nggi kiber tahdidlar tahdidlar va zaifliklarni aniqlash va himoya qilish uchun doimiy monitoring zarurligini isbotlaydi.

SAP mahalliy sharoitda xavfsiz qo‘llash bo‘yicha tavsiyalarga muvofiq masalan, shifrlash, autentifikatsiya va h.k.) ko‘plab o‘rnatilgan qurilmalarga ega bo‘lganligi sababli, sanoat mavjud konfiguratsiyalardagi zaifliklarni aniqlash va tuzatishga ko‘p mablag' sarflamadi. Natijada muhim biznesni buzish va hatto a'lumotlarni o‘g'irlash va ma'lumotlarni o‘chirish kabi muhim voqealarga olib kelishi mumkin. Ushbu o‘zgaruvchan SAP muhitlarida SAP xavfsizlik konfiguratsiyalarida yangi tahdidlar va zaif tomonlarni aniqlash juda muhim bo‘ldi. Muhim muhim tizimlar uchun SAP zaifliklarini bartaraf etishga ustuvor ahamiyat berilishi kerak. Bu mahsuldorlik, samaradorlik va muvofiqlikni oshiradi , shu bilan birga xavflarni, xarajatlarni va tekshirish, aniqlash va bartaraf etish uchun vaqtni kamaytiradi.

Integratsiyalar kengroq SAP landshaftini to‘liq qamrab olishni ta'minlaydi: SAP Roles Security, SAP Application & Database Security va SAP Hosting Security (1.9-rasm).

1.9-rasm.

Yuqoridagi xavfsizlik jihatlari SAP landshaftini himoya qilish uchun minimal imkoniyatlar to‘plamini o‘z ichiga oladi. Korxonalar o‘zlarining biznes jarayonlari xavfsiz va xavfsiz ekanligiga juda zarur bo‘lgan ishonchga ega bo‘lgach, ular o‘zlarining energiya va vaqtlarini asosiy biznes sohalariga sarflashlari mumkin.

Nazorat savollari

1. Axborot xavfsizligining hayotiy timsollari va ularning vazifalari.
2. Kiberxavfsizlik tushunchasiga izoh bering.
3. Kiberxavfsizlik fan sifatida qanday tuzilishga ega?
4. Kiberxavfsizlikning asosiy tushunchalari.
5. Axborotning konfidensialligini ta’minlash deganda nimani tushunasiz?
6. Axborotni yaxlitligini ta’minlash deganda nimani tushunasiz?
7. Kiberxavfsizlik nima uchun biznesning asosiy talabidir?
8. Ko‘pgina ommaviy bulut provayderlari qanday xizmatlar taklif qiladi?
9. Qisqa muddatli jarayonlari va standart operatsion tartib-qoidalarni yaratish va takomillashtirish uchun nima kerak?
10. Kiber tahdidlar va zaifliklarni aniqlash va himoya qilish uchun qanaqa monitoring zarur?
11. Fishing SOARning qanday asosiy komponentlari bor?
12. SAP xavfsizlik konfiguratsiyalarida yangi tahdidlar va zaif tomonlarni aniqlash nima uchun samarali hisoblanadi?

Adabiyotlar va internet saytlari:

1. Олифер В.Г.,Олифер Н.А. “Безопасность компьютерных сетей”2017 г.
2. Роджер А. Гримс “Взламываем хакера” Часть I. (Учимся у экспертов барьбе с хакерами).
3. Роджер А. Гримс “Взламываем хакера” Часть II. (Учимся у экспертов барьбе с хакерами).

2-ma’ruza. Kiberhujumlarning milliy xavfsizlik va iqtisodiy barqarorlikka ta’siri (2 soat).

Reja:

2.1. Kiber urush tushunchasi.
2.2. Kiberxavfsizlik va uning iqtisodiyotga ta’siri.
2.3. Moliyaviy tizimlar va ularning provayderlari.

Tayanch iboralar: *Kiber urush, Kiberterrorizm, Kiberjosuslik, Kiberjinoyat, Moliyaviy tizimlar, iqtisodiy barqarorlik, FMI.*

"Kiber urush" - bu davlat xavfsizligiga jiddiy tahdid solmaydigan yoki davlat xavfsizligiga tahdid soladigan tahdidga javoban amalga oshiriladigan davlat yoki hech qanday davlat ishtirokchisisiz kibermakonda amalga oshirilgan harakatlar orqali siyosatning kengayishi. Bu, asosan, axborot va axborot tizimlariga siyosiy sabablarga koʻra hujumlarni oʻz ichiga olgan Internetga asoslangan mojarodir. Kiberhujumlar rasmiy veb-saytlar va tarmoqlarni oʻchirib qoʻyishi, muhim xizmatlarni toʻxtatishi yoki oʻchirib qoʻyishi, maxfiy ma'lumotlarni oʻg'irlashi yoki oʻzgartirishi va moliyaviy tizimlarni ishdan chiqishiga olib kelishi mumkin.

Axborot texnologiyalari global iqtisodiyotni oʻzgartirdi va odamlar va bozorlarni tasavvur qilib boʻlmaydigan yoʻllar bilan bog'ladi. Axborot texnologiyalari markaziy bosqichga ega boʻlishi bilan butun dunyo mamlakatlari iqtisodiy rivojlanish va inklyuziv oʻsish uchun innovatsion g'oyalar bilan tajriba oʻtkazmoqda. Shuningdek, u buzilish uchun yangi zaifliklar va imkoniyatlarni yaratdi. Kiberxavfsizlik tahdidlari turli xil manbalardan kelib chiqadi va jismoniy shaxslar, korxonalar, milliy infratuzilma va hukumatlarga qaratilgan buzg'unchilik faoliyatida namoyon boʻladi. Ularning ta'siri jamoat xavfsizligi, millat xavfsizligi va butun dunyo bilan bog'liq boʻlgan iqtisodiyotning barqarorligi uchun katta xavf tug'diradi. Buzilishning kelib chiqishini, jinoyatchining shaxsini yoki uning sabablarini aniqlash qiyin boʻlishi mumkin va harakat deyarli har qanday joydan sodir boʻlishi mumkin. Ushbu atributlar Axborot texnologiyalaridan buzg'unchilik faoliyati uchun foydalanishni osonlashtiradi. Bugungi kunda kiberxavfsizlik tahdidlari eng jiddiy iqtisodiy va milliy xavfsizlik muammolaridan biri hisoblanadi.

Kiber urush ekotizimlari:

a) Kiberterrorizm – “zarar yetkazish yoki keyingi ijtimoiy, mafkuraviy, diniy, siyosiy yoki shunga oʻxshash maqsadlarga yoki qoʻrqitish maqsadida kompyuterlar va/yoki tarmoqlarga qarshi qasddan buzgʻunchilik faoliyati yoki uning tahdidini qoʻllash” deb qaralishi mumkin. bunday maqsadlarga erishish uchun har qanday shaxs.

b) Kiber firibgarlik - odatda jinoyatchilar uchun pul yoki tegishli daromad olishga qaratilgan kiber hujumlar. Fishing hujumlari soxta veb-saytlar bilan birgalikda foydalanuvchining shaxsiy ma'lumotlarini o‘g'irlaydi va shu bilan birga ularning hisobidan pul o‘g'irlaydi.

c) Kiber josuslik - jinoyatchilardan ma'lumot olishga qaratilgan kiber hujumlar. Kiberfiribgarlik bilan bog'liq holda, kiber josuslikning maqsadi olingan ma'lumotlarni sotish bo‘lishi mumkin.

d) Kiber ta'qib yoki bezorilik - biznes yoki hukumatni emas, balki shaxslarni qo‘rqitish va qo‘rqitish uchun mo‘ljallangan kiber hujumlar. Odatda ular ijtimoiy tarmoqlarga asoslangan - Facebook yoki Twitter.

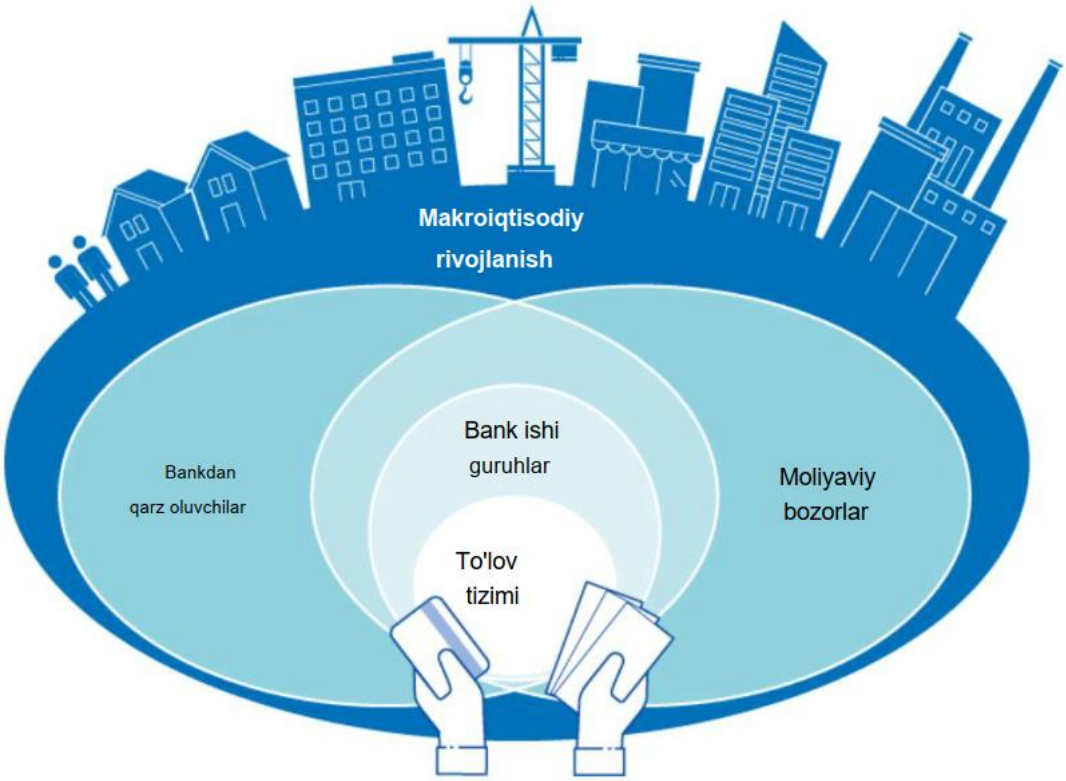
e) Kiber hujum - kiberhujumlar hujum qilinayotgan ma'lumotlar yoki jihozlarga zarar yetkazishga qaratilgan. Zarar jismoniy shikastlanish yoki muhim fayl yoki ma'lumotlarni o‘chirish bo‘lishi mumkin.

Kiberhujumlar jamiyatda tobora ko‘proq e'tiborni tortmoqda. Ushbu hujumlar hokimiyat va kompaniyalar hamda xususiy shaxslarga ta'sir qilishi mumkin. Moliyaviy sektor ham bundan mustasno emas. Xalqaro hisob-kitoblar banki ma'lumotlariga ko‘ra, moliya sektori boshqa tarmoqlarga qaraganda ko‘proq kiberhujumlarga duch kelmoqda.

Jadval 2.1. Kiberhujumlar xavfi yuqori bo‘lgan 5 ta davlat

Kiberhujumlar - eng zaif davlatlar			
Kiberhujumlar xavfi yuqori bo‘lgan beshta davlat		**Kiberhujumlar xavfi past bo‘lgan beshta davlat**	
Mamlakatlar	Risk %	Mamlakatlar	Risk %
Jazoir	30.7	Fransiya	5.2
Boliviya	20.3	Kanada	4.6
Pokiston	19.9	Avstraliya	4.1
Xitoy	18.5	AQSH	3
Hindiston	16.9	Buyuk Britaniya	2.8

Moliya sektori moliya tizimida faoliyat yurituvchi agentlardan iborat. Bularga, masalan, funksiyalari moliya tizimi va pirovardida Shvetsiya iqtisodiyoti uchun hal qiluvchi ahamiyatga ega bo‘lgan banklar va infratuzilma kompaniyalari kiradi. Moliyaviy kompaniyalar alohida funksiya va alohida maqomga ega bo‘lganligi sababli, ular maxsus tartibga solingan holda tartibga solinadi. Moliya tizimining umumiy tuzilishi va uning barqaror makroiqtisodiy rivojlanish uchun ahamiyatini ko‘rsatishning bir usuli quyida keltirilgan 2.1-rasmdagi kabidir.



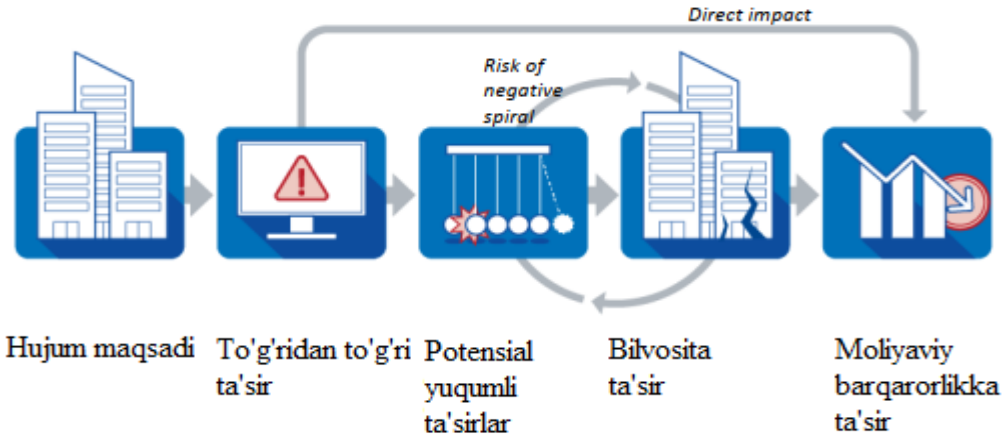
2.1-rasm. Moliya tizimining tuzilishini tasvirlash

Moliya tizimining markazida to‘lov tizimlari va boshqa moliya bozori infratuzilmalari (FMI) turadi. Bular banklar bilan chambarchas bog'liq bo‘lib, ular birgalikda moliya tizimining o‘zagini tashkil qiladi. Moliyaviy infratuzilma va banklar moliya bozorlarining faoliyat yuritishi va tizimda yetarli kredit ta'minoti uchun asos bo‘lib xizmat qiladi. Iqtisodiyotning ishlashi uchun moliya tizimi muhim funksiyalar deb ataladigan keng ko‘lamli asosiy iqtisodiy funksiyalarni ishonchli va mustahkam tarzda bajarishi kerak. Bunga, masalan, to‘lovlar va hisob-kitoblar, banklararo kreditlar, tranzaksiya va jamg'arma hisobvaraqlari, derivativlar va qimmatli qog'ozlar savdosi kabi xizmatlar ko‘rsatish kiradi. Shunday ekan, pirovard natijada barqaror makroiqtisodiy rivojlanishning zaruriy sharti faoliyat yuritayotgan moliyaviy tizimdir.

Bugungi kunda Shvetsiya moliya tizimining muhim funksiyalari deyarli faqat raqamli vositalar bilan ta'minlanadi. Keng qamrovli raqamlashtirish banklar va FMIlarning xizmatlar ko‘rsatishda to‘liq IT muhitiga bog'liq bo‘lishiga olib keldi. Shu bilan birga, bu muhitlar tez o‘sib bordi va tobora o‘zaro bog'liq va murakkab bo‘lib qoldi. Bu banklar va FMIlarning IT tizimlariga, balki ularning uchinchi tomon yetkazib beruvchilariga va telekommunikatsiya va energiya ta'minoti kabi texnik infratuzilmalarga ham tegishli. Ushbu rivojlanish moliyaviy tizimning zaifligini oshirdi va shuningdek, tahdidlar landshaftining kengayishi va rivojlangan kiberhujumlarning ko‘payishi bilan birga sodir bo‘ldi.

Kiberhujumlar moliyaviy bozor ishtirokchilariga ta'sir qilishi mumkin bo‘lganidek, ular moliyaviy barqarorlikka ham potentsial ta'sir ko‘rsatishi va tizimli xavfni tashkil qilishi mumkin. Moliya tizimining milliy iqtisodiyot uchun ahamiyatini hisobga olgan holda, moliya sektoriga kiberhujum oxir-oqibatda faoliyat yuritayotgan iqtisodiyotga tahdid solishi mumkin.

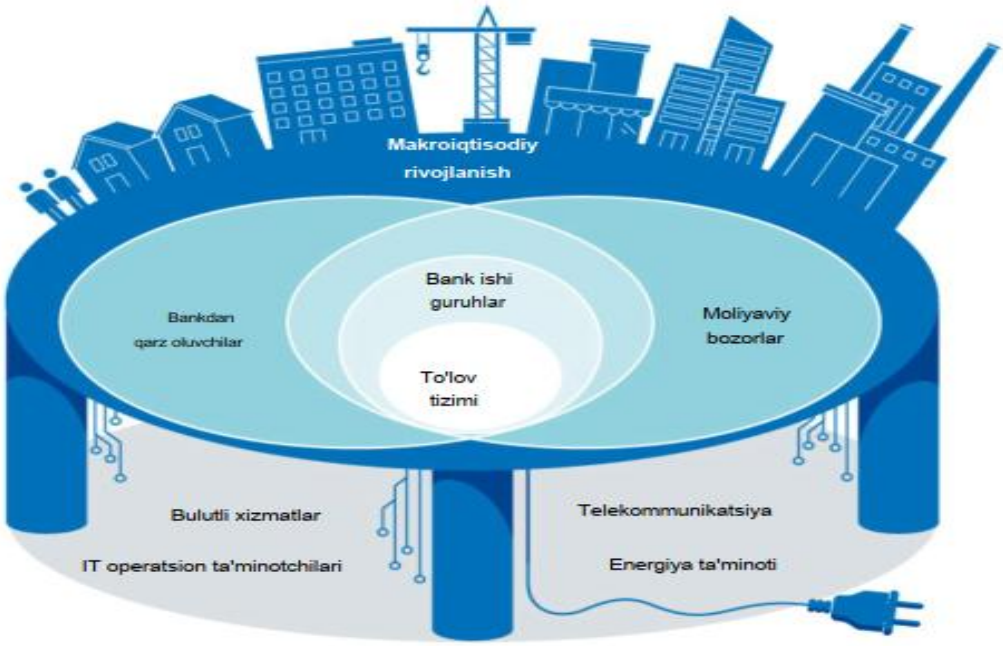
Quyidagi 2-rasmda kiberhujumni besh xil bosqichga qanday ajratish mumkinligi ko‘rsatilgan: hujumning maqsadi, hujumning bevosita ta'siri, hujumning potentsial yuqumli ta'siri, hujumning bilvosita ta'siri va hujumning umumiy ta'siri. moliyaviy barqarorlikka hujum. Moliyaviy barqarorlik nuqtai nazaridan, kiberhujum bir yoki bir nechta agentlarga ta'sir qilganda boshlanadi, deyish mumkin. Bular moliyaviy agentlar yoki moliya sektoriga uchinchi tomon yetkazib beruvchilar bo‘lishi mumkin. Keyingi jihat - bu to‘g'ridan-to‘g'ri ta'sir, ya'ni bu agentlarga hujumdan qanday ta'sir qilish, masalan, ba'zi xizmatlar mavjud bo‘lmasligi. Keyinchalik, bu ta’sirlar moliyaviy tizimda yanada tarqalishi mumkin, bu esa o‘z navbatida bilvosita bir xil agentga ko‘proq ta'sir qilishi yoki boshqalarga ta’sir qilishi mumkin. Yakuniy bosqich - bu individual agentlarga ta'sir shunchalik kuchli bo‘lib, moliyaviy barqarorlikka ham ta'sir qiladi.



2.2-rasm. Kiberhujum moliyaviy barqarorlikka qanday ta'sir qilishi mumkin

Kiberhujumni moliyaviy barqarorlik nuqtai nazaridan tahlil qilganda, uni bir yoki bir nechta agentlarning ta'sirlanishi bilan boshlangan hujum sifatida ko‘rish mumkin, 2.2-rasmdagi hujum maqsadiga qarang. Kiberhujum dastlab bitta tizimli muhim moliyaviy kompaniyaga, bir nechta moliyaviy kompaniyalarga yoki moliya sektoriga uchinchi tomon yetkazib beruvchiga qaratilgan. Moliyaviy sektor uchun uchinchi tomon yetkazib beruvchilar, masalan, IT operatsiyalari, dasturiy ta'minot, bulut xizmatlari, energiya ta'minoti va aloqa bilan bog'liq bo‘lganlardir. Buni 1-rasmdagi rasmda yoritish uchun biz uni shunday kengaytirishimiz kerakki, uchinchi tomon xizmatlari ham moliyaviy tizim va

pirovardida makroiqtisodiyot funksiyalarini qo‘llab-quvvatlovchi muhim xizmatlar sifatida kiritiladi (2.3-rasm).



2.3-rasm. Kritik xizmatlar moliya tizimining funksiyalarini qo‘llab-quvvatlaydi

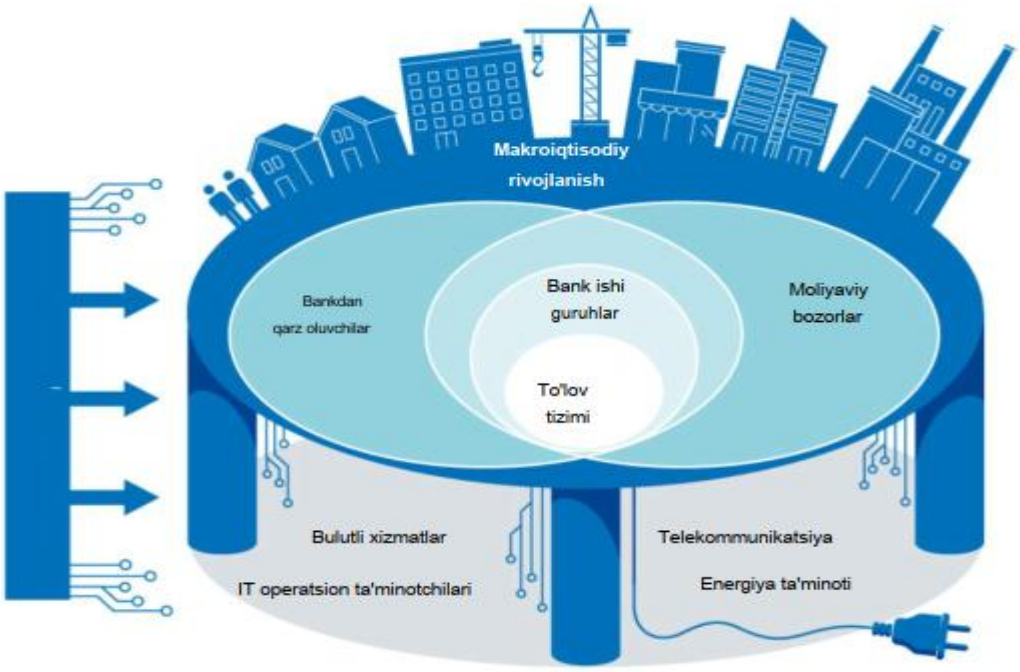
Yuqorida aytib o‘tilganidek, moliyaviy barqarorlikka ta'sir qilishning bir necha usullari mavjud va bu bosqich ushbu ta'sirni umumlashtiradi. Ushbu tahlildan olingan xulosamiz shuni ko‘rsatadiki, kiberhujum moliyaviy tizimda tizimli inqirozga olib kelishi mumkin. Bu ham oldingi tahlillar bilan mos keladi.

2.2-rasmdagi strelkalar bilan ko‘rsatganimizdek, kiberhujumlar moliyaviy barqarorlikka to‘g'ridan-to‘g'ri yoki bilvosita yoki ikkalasining kombinatsiyasi orqali ta'sir qilishi mumkin. Moliyaviy agentlarga yoki ularning uchinchi tomon yetkazib beruvchilariga kiberhujum moliyaviy barqarorlikka to‘g'ridan-to‘g'ri ta'sir qiladigan darajada muhim moliyaviy funksiyalarga ta'sir qilishi mumkin. Bundan tashqari, dastlabki hujum faqat cheklangan zarar etkazishi mumkin, ammo taqillatish effektlari oxir-oqibat moliyaviy barqarorlikka ta'sir qiladigan darajada tarqaladi va kuchayadi.

Ko‘pgina muvaffaqiyatli kiber hujumlar faqat bitta moliyaviy agentga ta'sir qiladi va cheklangan zarar keltiradi. Tizimli inqirozlarga olib kelgan kiberhujumlarning ma'lum holatlari yo‘q. Biroq, bu ular buni qila olmaydi, degani emas. Muvaffaqiyatli kiberhujum asosiy agentni buzish yoki moliyaviy tizim orqali ta'sirlarni tarqatish uchun etarli resurslarga ega bo‘lgan tizimli xavf tug'dirishi mumkin. Shu nuqtai nazardan, moliyaviy bozorlar, kompaniyalar va keng jamoatchilikning moliyaviy tizimning ishlashiga ishonchi bo‘lishi uchun ishonch kanali ayniqsa muhimdir.

Kibertahdidlar moliyaviy tizimda tahdid operatori moliyaviy agentga yoki uning uchinchi tomon yetkazib beruvchilariga qarshi qaratilgan zararli harakatlarni amalga oshirish niyati va qobiliyatiga ega bo‘lganda paydo bo‘ladi. Ushbu harakatlar kiberdomen yoki kiberfazo deb ataladigan, ya'ni ular bilan bog'liq ma'lumotlar va ma'lumotlar bilan o‘zaro bog'liq bo‘lgan o‘zaro bog'langan AT infratuzilmalaridan iborat global axborot muhitida amalga oshiriladi. Biroq, agar tahdid qiluvchi shaxs zarar etkazish qobiliyatiga ega bo‘lsa ham, hech qanday maqsad bo‘lmasa, u odatda tahdid emas. Xuddi shunday, zarar etkazish niyatida bo‘lgan tahdid aktyori, agar u qobiliyatga ega bo‘lmasa, tahdid hisoblanmaydi.

Garchi tahdid nisbatan tushunarli elementlarga ega bo‘lsa-da, muayyan faoliyatga nisbatan tahdid manzarasini tahlil qilish qiyin. Buning muhim izohi shundaki, tahdid landshaftlari ko‘pincha vaqt o‘tishi bilan farqlanadi va tez o‘zgarishi mumkin. Umuman olganda, kim zarur qobiliyatga ega ekanligini baholash qiyin va bu tez-tez kiber domenda o‘zgarib turadi. Axborotni manipulyatsiya qilish, yo‘q qilish va o‘g'irlash usullariga hech qachon to‘liq tayanib bo‘lmaydi. Tahdidchi tomonidan foydalaniladigan raqamli vositalar va zaifliklar doimiy emas, shu bilan birga himoya qilinadigan IT muhitlari ham doimiy ravishda o‘zgarib turadi. Bundan tashqari, tahdid ishtirokchilari boshqa tahdid subyektlarining vositalarini qayta ishlatishga moyil bo‘lib, ma'lum imkoniyatlarni ham sotib olishlari mumkin.30 Bundan tashqari, zamonaviy IT muhiti ko‘pincha o‘z tashkilotidan tashqari ko‘plab boshqa tomonlarga ham bog'liq. Bundan tashqari, quyida 2.4-rasmda ko‘rsatilganidek, moliyaviy tizimga ham, uning muhim yetkazib beruvchilariga ham tahdidlar manzarasi mavjud.



2.4-rasm. Kibertahdidning moliyaviy tizimga ham, uning muhim xizmat ko‘rsatuvchi provayderlarga ham qaratilishi

Tahdidchining usullari va imkoniyatlari vaqt o‘tishi bilan rivojlanishi va o‘zgarishi mumkin bo‘lganidek, tahdid qiluvchining niyati ham o‘zgarishi mumkin. Tashqi siyosat va xavfsizlik siyosatidagi yoki ommaviy axborot vositalarining e'tiboridagi o‘zgarishlar tahdid ishtirokchilarining niyatlariga ta'sir qilishi mumkin bo‘lgan voqealar misolidir. Shuning uchun tahdid manzarasi qisqa muddatli bo‘lib, doimo yangilanib turishi kerak. Bank, moliya va sug'urta sektorlarining murakkabligi ushbu sektorga tahdid manzarasini baholashni qiyinlashtiradi. Biroq, Evropa Ittifoqining kiberxavfsizlik agentligi, ENISA, kelgusi o‘n yil ichida kiberxavfsizlik xavfining ortib borayotgan murakkabligi va hujum maydonining kengayishi, ya'ni tezkor raqamlashtirish natijasida tajovuzkor uchun mumkin bo‘lgan kirish nuqtalari tufayli kiberxavfsizlik xavflarini baholash va izohlash yanada qiyin bo‘lishini kutmoqda.

Tahdidchilar, yuqorida aytib o‘tganimizdek, turli xil niyat va imkoniyatlarga ega. Masalan, uyushgan jinoiy guruhlar moliyaviy maqsadlarga erishish uchun kiberhujumlarni boshlashi mumkin, bunda moliyaviy daromad harakatlantiruvchi kuch hisoblanadi, mafkuraviy sabablarga ko‘ra faollar faollik bilan shug'ullanish uchun kiberhujumlarni boshlashi mumkin va davlat yoki davlat tomonidan qo‘llab-quvvatlanadigan aktyorlar kiberhujumlarni boshlashi mumkin.

Maqsad sifatida josuslik, sabotaj yoki ta'sir ko‘rsatadigan siyosiy sabablarga ko‘ra kiber hujumlar. Har xil harakatlantiruvchi kuchlar, maqsadlar va imkoniyatlar turli xil tahdid sub'ektlari o‘z ishlarida qanchalik uzoq muddatli, ilg'or, maqsadli yoki opportunistik bo‘lishlari haqida gap ketganda, o‘zlarini juda boshqacha tutishi mumkinligini anglatadi. Bu shuni anglatadiki, turli xil tahdid subyektlari ma'lum darajada har xil himoya turlarini talab qiladi.

Moliyaviy sektor agentlari birgalikda tashkil etadigan jamiyatning muhim infratuzilmasi uchun asosiy tahdid davlat va davlat tomonidan homiylik qilinadigan tahdid subyektlaridir. Bugungi kunda davlat aktyorlari, agar niyat paydo bo‘lsa, uni o‘chirib qo‘yish uchun Shvetsiya jamiyati uchun muhim bo‘lgan raqamli infratuzilmada o‘z o‘rnini egallashga harakat qilmoqda. Shu nuqtai nazardan, Shvetsiya oldida turgan tahdid manzarasi kengayib, yanada murakkablashdi va parallel ravishda siyosiy, harbiy va iqtisodiy aktivlarni nishonga olishi taxmin qilinmoqda. Boshqacha qilib aytadigan bo‘lsak, davlat yoki davlat tomonidan homiylik qilinadigan aktyorlar Shvetsiyadagi markaziy jamiyat funksiyalariga zarar etkazadigan kiberhujumlarni amalga oshirish niyati va qobiliyatiga ega. Bu Shvetsiya moliya tizimi o‘zining himoya choralarini moslashtirishi kerak bo‘lgan tahdidlardir. Davlat subyektlari tomonidan tahdidlar yanada rivojlangan va qoida tariqasida, boshqa tahdid subyektlari tahdidlariga qaraganda ko‘proq himoyani talab qilganligi sababli, ushbu turdagi tahdid "o‘lchov tahdidi" deb nomlanadi. Ushbu

turdagi ilg'or qobiliyatga ega bo‘lgan tahdid ishtirokchilari uchun Internetga ulangan hamma narsa mavjud va ularga kirish mumkin. Bundan tashqari, boshqa ko‘plab kiber tahdidlardan farqli o‘laroq, bu hujumlar ko‘pincha aniqlanmaslik uchun mo‘ljallangan. Shuning uchun dastlabki bosqichda rivojlangan hujumchini to‘xtatishga harakat qilish etarli emas. Tizimdagi agentlar ham yakka tartibda va birgalikda va imkon qadar bunday hujumlarni aniqlash, javob berish va ularni tiklash qobiliyatini rivojlantirish orqali ularni yanada qiyinlashtirishi kerak. Bunday qobiliyatni rivojlantirish va qo‘llab-quvvatlash nisbatan qiyin va vaqt talab qiladi. Muhim tashkiliy va madaniy birinchi qadam bu bosqin sodir bo‘ladi, allaqachon sodir bo‘lgan va hatto hozir sodir bo‘layotgan bo‘lishi mumkin bo‘lgan operatsiyalarda “taxmin buzilishi” mentalitetini o‘rnatishdir. Boshqacha qilib aytganda, ilg'or kiberhujumlarning oldini olish, boshqarish va ularni qayta tiklash choralari mavjud himoya choralari muvaffaqiyatsizlikka uchraganida aniqlash qobiliyatining yuqori darajasini, shuningdek, ushbu kamchiliklarning o‘zini va ularning oqibatlarini bartaraf etish qobiliyatini o‘z ichiga olishi kerak. Moslashuvchanlikni oshirish bo‘yicha ishlarning yana bir muhim qismi - bu kiberxavf bilan bog‘liq yaxshi muvofiqlashtirish va moliyaviy tizimning zaifligini kamaytirish uchun uzoq muddatli rejalashtirish. Bu muvofiqlashtirish moliya sektoridagi ham xususiy, ham davlat agentlarini jalb qilishi kerak. Bundan tashqari, muvofiqlashtirish yanada mustahkamlikka olib kelishi uchun moliyaviy barqarorlik mas’uliyati bo‘lgan organlar ham, kiberxavfsizlik uchun mas'ul organlar ham jalb qilinishi kerak.

Nazorat savollari

1. Qaysi sub’ektlar kiberhujumlarni boshlashi mumkin?
2. Tahdidchilar asosan qaysi vositalar yordamida kiberhujumlarni amalga oshirishadi?
3. Moliya tizimi nima uchun muhim funksiyalarni bajarishi kerak?
4. Moliyaviy sektor agentlari nima uchun muhim tahdid sub'ektlaridir?
5. Kiberhujumlar moliyaviy barqarorlikka qanday ta'sir qilishi mumkin?
6. Kiber urushning ekotizimlari nimalarni o‘z ichiga oladi?

Adabiyotlar va internet saytlari:

1. Роджер А. Гримс “Взламываем хакера” Часть III. (Учимся у экспертов барьбе с хакерами).
2. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информatsii: Учебник для вузов / – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

3. Нестеров С. А. Информатsiонная безопасность и защита информатsiи: Учеб.пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с.

4-ma’ruza. Kiberxavfsizlikning global xavfsizlik muammolari bilan bog’liqligi (2 soat).

Reja:

3.1. Xalqaro miqyosdagi kiberxavfsizlik muammolari
3.2. Axborot qurollari va undan himoyalanish.
3.3. Turli davlatlarda kiberxavfsizlik mummolari va yechimlari.

Tayanch iboralar: *Axborot quroli, Kontrrazvedka, Davlat siri, Kiberjinot, Xalqaro kiberxavfsizlik, Mamlakatga kibertahdid.*

Kiberxavfsiz dunyoni yaratish uchun biz jinoyatchilar kabi tez va global integratsiyalashgan bo‘lishimiz kerak. Mahalliy resurslar bilan global tahdidga duch kelishning o‘zi etarli bo‘lmaydi. Mamlakatlar o‘z sa'y-harakatlarini muvofiqlashtirish uchun ichki va xalqaro miqyosda ko‘proq harakat qilishlari kerak.

Sanoat ko‘plab sohalarda etakchi o‘rinni egallaganligi - texnik va risklarni boshqarish standartlarini ishlab chiqish, ma'lumot almashish forumlarini chaqirish va katta resurslarni sarflash uchun tahsinga loyiqdir. Xalqaro tuzilmalar, jumladan, 7 ta kiberekspertlar guruhi va Bazel qo‘mitasi moliyaviy sektor nazoratchilari uchun xabardorlikni oshirmoqda va sog‘lom amaliyotlarni aniqlamoqda. Ammo, ayniqsa, global nuqtai nazardan qarasak, ko‘p ish qilish kerak. Xalqaro hamjamiyat birlashishi va milliy darajada amalga oshirilayotgan ishlarni kuchaytirishi mumkin bo‘lgan to‘rtta yo‘nalish mavjud:

Birinchidan , biz xavf-xatarlarni ko‘proq tushunishimiz kerak : tahdidlarning manbai va tabiati va ular moliyaviy barqarorlikka qanday ta'sir qilishi mumkin. Xatarlarni yaxshiroq tushunish uchun bizga tahdidlar va muvaffaqiyatli hujumlarning ta'siri haqida ko‘proq ma’lumotlar kerak.

Ikkinchidan , biz tahdidlar haqida razvedka, hodisalar haqida xabar berish va chidamlilik va javob berish bo‘yicha eng yaxshi amaliyotlar bo‘yicha hamkorlikni yaxshilashimiz kerak. Xususiy va davlat sektori o‘rtasida axborot almashishni yaxshilash kerak, masalan, banklarning moliyaviy nazorat va huquqni muhofaza qilish organlariga muammolar haqida hisobot berishidagi to‘siqlarni kamaytirish orqali.

Hujum zaiflik orqali axborot tizimlari xavfsizligini buzishga oshirilgan harakatdir. Tarmoq hujumi kompyuter tarmoqlari orqali tashkilotning tizimiga ruxsatsiz ta’sir ko‘rsatishdir. Hujumni ko’p turlari mavjud.

Ma’lumotlarni qayta tiklash axborot tashuvchilarda ma’lumotlarni qayta tiklash jarayonidir

To‘liq nusxa yaratish tizimni va undagi barcha fayllarni nusxasini yaratish jarayonidir.

Differensial nusxa yaratish o‘zgartirilgan fayllarni nusxasini olish jarayonidir

Mamlakatdagi turli davlat idoralari uzluksiz muloqot qilishlari kerak. Va eng qiyin, mamlakatlar o‘rtasida ma'lumot almashishni yaxshilash kerak.

Uchinchidan , tartibga solish yondashuvlari yanada izchillikka erishishi kerak. Bugungi kunda mamlakatlarda turli standartlar, qoidalar va atamalar mavjud. Ushbu nomuvofiqlikni kamaytirish ko‘proq muloqotni osonlashtiradi. Nihoyat, hujumlar kelishini bilib, davlatlar ularga tayyor bo‘lishlari kerak . Inqirozga tayyorgarlik ko‘rish va ularga javob berish protokollari milliy va transchegaraviy darajada ishlab chiqilishi kerak, bu esa operatsiyalarga imkon qadar tezroq javob berish va tiklash imkoniyatiga ega bo‘lishi kerak. Inqiroz mashqlari jarayonlar va qarorlarni qabul qilishdagi kamchiliklar va zaif tomonlarni ochib berish orqali chidamlilik va javob berish qobiliyatini shakllantirishda hal qiluvchi ahamiyatga ega bo‘ldi.

Kiberhujum dunyoning istalgan nuqtasidan yoki bir vaqtning o‘zida ko‘p joydan kelishi mumkinligi sababli, inqirozga javob berish protokollari mintaqalar va global miqyosda ifodalanishi kerak.

Ya'ni, tegishli idoralar inqiroz paytida, yaqin atrofdagi va, ideal holda, uzoq mamlakatlarda ham “kimga qo‘ng'iroq qilishni” bilishi kerak. Kichik yoki rivojlanayotgan mamlakatlar uchun bu xalqaro e'tiborni talab qiladigan muammo. Ko‘pchilik moliyaviy aloqalar uchun global banklar tomonidan taqdim etilgan moliyaviy xizmatlar yoki vakillik liniyalariga tayanadi. Transchegaraviy javob protokollarini ishlab chiqish mamlakatlarga inqirozdagi o‘z rollarini tushunishga yordam beradi va inqiroz yuzaga kelganda muvofiqlashtirilgan javobni ta'minlaydi.

Bu erda XVF muhim rol o‘ynashi mumkin. Ko‘pgina standartlarni belgilovchi institutlarga qaraganda ancha kengroq vakillik bilan XVF rivojlanayotgan bozor va rivojlanayotgan mamlakatlarning tashvishlarini global darajaga ko‘tarish qobiliyatiga ega. Har qanday joy hujumni boshlash uchun qulay joy bo‘lgani uchun, ma’lumot almashish, harakatlarni muvofiqlashtirish va salohiyatni oshirish uchun boshqa mamlakatlar bilan hamkorlik qilishdan ilg‘or iqtisodlari oliy manfaatdordir.

XVF da biz ushbu salohiyatni oshirishi kerak bo‘lgan mamlakatlar bilan ishlaymiz, kiberxavfsizlik tahdidlarini tan olish va samarali kurashish uchun zarur bo‘lgan ko‘nikmalar va tajribalarni rivojlantiramiz. Xalqaro hamkorlarimiz ham shunday qilmoqdalar va biz davlat va xususiy sektordagi bir qator manfaatdor tomonlar bilan muntazam ishlaymiz.

Muvaffaqiyatli kiberhujumlar, ayniqsa shaxsiy va moliyaviy ma'lumotlar buzilgan taqdirda, ishonchsizlikni keltirib chiqarish orqali moliyaviy rivojlanishga to‘sqinlik qilishi mumkin.

Agar biz bozorlarni rivojlantiradigan va moliyaviy inklyuzivlikni kengaytiradigan yangi texnologiyalardan foyda olishni istasak, ishonchni saqlashimiz, axborot-kommunikatsiya texnologiyalari xavfsizligini ta'minlashimiz kerak. Kiberxavfsizlik bilan har doim ko‘proq narsa qilish kerak, chunki o‘zgarishlar tezligi hayratlanarli darajada tezdir.

3.1-rasm. 2022-yil eng muhim kiberxavfsizlik muammolari

Mamlakatning tahdidlarga mos aks ta’sir ko‘rsatish layoqatiga ega bo‘lgan axborot xavfsizlik tizimini yaratish uchun, rivojlangan chet el mamlakatlarida axborot urushining zamonaviy konsepsiyalari, o‘ziga xos xususiyatlari, axborot qurolining turlari va qo‘llash samaradorligi, shuningdek, chet el mamlakatlarida axborot xavfsizligini ta’minlash masalalari qay tarzda yechilishi haqida aniq bir tasavvurga ega bo‘lish kerak.

Axborot quroli deb nomlanuvchi vositalar:

– axborot massivlarini yo‘q qilish, buzish yoki o‘g‘irlash;

– himoya tizimlarini yengish;

– qonuniy foydalanuvchilar huquqlarini cheklash;

– kompyuter tizimlarini, texnik vositalarni ishini izdan chiqarish;

– shular kabi boshqa amallarni bajaradi.

Hozirda hujumkor axborot quroliga quyidagilarni keltirish mumkin:

– ko‘payish, dasturlarga kirish, aloqa liniyalari, ma’lumot uzatish tarmog‘i orqali uzatish, boshqaruv tizimini ishdan chiqarish va shu kabi boshqa qobiliyatlarga ega bo‘lgan kompyuter viruslari;

– mantiqiy bomba – dasturiy o‘rnatma qurilmalari, signal bo‘yicha yoki aniq vaqtda harakatga keltirish uchun harbiy yoki fuqarolik infratuzilma axborot-boshqaruv markazlariga oldindan kirgiziladi;

– telekommunikatsiya tarmoqlarida axborot almashishini susaytiruvchi, davlat yoki harbiy boshqarish kanallarida axborotni soxtalashtiruvchi vositalar;

– tekshiruvchi dasturlarni neytrallash vositalari;

– obyektning dasturiy ta’minotiga raqib tomonidan ongli ravishda turli xatoliklarni kiritish.

Axborot qurolini qo‘llash oqibatini kamaytirish yoki oldini olish uchun quyidagi chora-tadbirlarni ko‘rish kerak:

– axborot resurslarini fizik asosini tashkil etuvchi material-texnik obyektlarni himoyalash;

– ma’lumotlar bazasi va bankini normal va uzluksiz ishlashini ta’minlash;

– ruxsat etilmagan kirishlardan, buzish yoki yo‘q qilishdan axborotlarni himoyalash;

– axborot sifatini (vaqtidaligini, aniqligini, to‘laligini va foydalana olishlikni) saqlab qolish.

Axborot qurolidan himoyalovchi dasturiy tasnifdagi amaliy tadbirlarga quyidagilar kiradi:

1. Xalqaro tarmoq orqali turli xil axborot almashinuvida iqtisodiy va boshqa tuzilmalarning ehtiyojini bashoratlash va monitoringini tashkil qilish. Buning uchun transchegara, shu qatorda Internet orqali ham, almashinuvni nazorat qilish uchun maxsus tuzilmalarni yaratish; ochiq tarmoqlarda axborot xavfsizligi tahdidlarini bartaraf etish bo‘yicha davlat va nodavlat idoralarning chora-tadbirlarini koordinatsiya qilish; xalqaro hamkorlikni tashkil etish mumkin.

2. Axborot resurslarining xavfsizligi talablariga rioya qilgan holda milliy va korporativ tarmoqlarni jahon ochiq tarmog‘lariga ulanishini ta’minlovchi axborot texnologiyalarni takomillashtiruvchi davlat dasturini ishlab chiqish.

3. Jahon axborot tarmoqlarida ishlash uchun ommaviy foydalanuvchilarni va axborot xavfsizligi bo‘yicha mutaxassislarni tayyorlash va malakasini oshirish kompleks tizimini tashkil qilish.

4. Ochiq jahon tarmoqlari foydalanuvchilarining mas’uliyatlari va majburiyatlari, reglament huquqi va axborot resurslari bilan foydalanish qoidalarining milliy qonunchilik qismini ishlab chiqish. Jahon ochiq tarmoqlari ishlashining me’yoriy-huquqiy ta’minotini va xalqaro qonunchiligini ishlab chiqishda faol ishtirok etish. AQSh ning milliy xavfsizligini ta’minlash tizimi.

Milliy xavfsizlik agentligi (MXA-NBA) – radioelektron tutib qolish sohasida jahonda peshqadam hisoblanadi. Agentlikning maqsadi – texnik vositalar yordamida AQSh ning milliy xavfsizligini ta’minlash.

AQSh ning tashqi xavfsizligini ta’minlashda Markaziy razvedka boshqarmasi (MRB-SRU)ga asosiy o‘rinlardan biri ajratilgan. U yerda boshqa davlatlar tomonidan milliy axborot infratuzilmaga qilinadigan tahdidlar haqidagi axborotlarni qidirish va qayta ishlash bo‘yicha razvedkaning imkoniyatlarini kengaytirishga yo‘naltirilgan reja ishlab chiqilgan va tatbiq qilingan. Agentura ishiga oid an’anaviy usullardan tashqari, MRB texnik yo‘l orqali yopiq ma’lumotlar bazasiga kirishni va ochiq manbalarning tahliliga katta e’tibor qaratadi. Keyingi vaqtlarda MRB axborot va kompyuter texnologiyalari bo‘yicha mutaxassislarni, jumladan xakerlar orasidan tanlashni amalga oshirmoqda. Federal tekshirishlar byurosi (FTB-FBR) ham, eng avvalo AQSh infratuzilmasini himoyalash nuqtai nazaridan axborot urushi doktrinasini tatbiq qilishda ishtirok etadi. AQSh da kompyuter jinoyatchiligiga qarshi kurashish maqsadida 1996-yili “Kompyuterlarni qo‘llash orqali firibgarlik va suiiste’mol qilishlar to‘g‘risida”gi federal qonun qabul qilingan va ushbu turdagi jinoyatchilik bilan kurashish bo‘yicha FTB tarkibida bo‘linma tashkil etish ko‘zda tutilgan. FTB telekommunikatsiya tarmog‘i orqali amalga oshiriladigan ayg‘oqchilik, maxfiy ma’lumotlarni oshkor qilish, davlat instansiyalarni aldash, terrorizm, xiyla ishlatish va firibgarlik kabi noxush holatlarni tekshirish bilan shug‘ullanadi. Uning tarkibiga kompyuter jinoyatchiligi bilan shug‘ullanuvchi yettita bo‘linma kiradi, ularning shtati 300 kishini tashkil qiladi. AQSh ning Mudofaa vazirligi (MV) xalqaro Internet tarmog‘ining ajdodi hisoblanib, birinchi bo‘lib mamlakatning xavfsizligiga yangi tahdidning va axborot qurolining kuchini anglab yetdi va hozirgi vaqtda harbiy sohada axborot urushi doktrinasini tatbiq qilishda yetakchi o‘rinni egallaydi. MV ilmiy kengashining ekspertlar komissiyasi axborot urushi hodisasiga qarshi harbiy telekommunikatsiya va kompyuter tarmoqlari xavfsizligini ta’minlovchi shoshilinch choralarni qabul qilish lozimligi haqida doklad tayyorladi. Pentagon harbiy avtomatlashtirilgan axborot tizimlarini “qizil buyruqlar” deb ataluvchi zaiflikka tekshirish uchun harbiy kompyuter tarmoqlarini himoyasini ta’minlash bilan shug‘ullanish maqsadida xakerlarni ishga qabul qiladi. Hozirgi kunda AQSh idoralari faoliyatidagi umumiy tendensiya axborot urushi olib borishning asosiy tashkiliy va konseptual prinsiplarini ishlab chiqish, axborot texnologiyalarni qo‘llab yangi ish usullarini qidirish hisoblanadi.

Buyuk Britaniyadagi axborotni himoyalash tizimi. Buyuk Britaniyada axborot xavfsizligini ta’minlash davlat tizimini yaratishda axborot urushi dushmanning axborot tizimiga ta’sir etuvchi va bir vaqtda mamlakatning shaxsiy tizimlarini himoyalovchi harakatlar deb qaraladi. Buyuk Britaniyaning Razvedka va xavfsizlik

bo‘yicha parlament komiteti Britaniya maxsus xizmatlari ustidan nazorat idorasi sifatida 1994-yilda tashkil etilgan. Bu komitet “Razvedka xizmatlari to‘g‘risida”gi qonunga muvofiq uchta maxsus xizmat: Maxfiy xizmat (MI5), SIS razvedkasi va Hukumat aloqa markazi tomonidan budjet mablag‘larining sarflanishini, bu xizmatlarning boshqarilishini va ularning olib borayotgan siyosatini nazorat qilish uchun tuzilgan. Secret Intelligence Service/MI6 – Buyuk Britaniyaning asosiy razvedka xizmati. SIS Tashqi ishlar vazirligi (TIV) tizimiga kiritilgan bo‘lib xorijda 87 ta qarorgohga va Londonda shtab-kvartiraga ega. SISni Bosh direktor boshqaradi va u bir vaqtning o‘zida Tashqi ishlar vazirining o‘rinbosari ham hisoblanadi. Shunday qilib, formal ravishda SIS Buyuk Britaniyaning TIV nazorati ostida hisoblanadi, biroq, shu bilan birga u to‘g‘ridan-to‘g‘ri premyer-ministrga chiqishi mumkin.

Kontrrazvedka xizmati – Military Intelligence-5 (MI-5) 1909-yilda ichki xavfsizlikni ta’minlash bilan shug‘ullanuvchi maxfiy xizmatlar Byurosining ichki departamenti sifatida tuzilgan.

Hukumat aloqa markazi Buyuk Britaniyaning maxsus xizmatlar tizimida radioayg‘oqchilik uchun javob beradi. Markaz TIV tarkibiga kiritilgan bo‘lib, xodimlarining soni va axborotni topish hajmi bo‘yicha mamlakatning yirik idoralaridan biri hisoblanadi.

Germaniyaning axborotni himoyalash tizimi. Axborot oqimlarining xavfsizligini ta’minlashga mas’ul koordinatsiyalovchi hukumat idorasi bo‘lib 1991-yilda tashkil etilgan Federal xavfsizlik xizmati (BSI) hisoblanadi. Bu xizmat axborot texnikasi sohasidagi xavfsizlikni ta’minlaydi. Hozirgi vaqtda BSI faoliyatining umumiy konsepsiyasi NATO va YES bilan yaqin hamkorlikda quyidagi funksiyalarni bajarilishini ko‘zda tutadi:

– axborot texnologiyalarni joriy etishdagi ehtimoliy xavfni baholash;

– milliy kommutatsiya tizimlarining himoyalash darajasini baholash uchun mezonlar, usullar va sinov vositalarini ishlab chiqish;

– axborot tizimlarining himoyalanish darajasini tekshirish va muvofiqlik sertifikatlarini berish;

– muhim davlat obyektlariga axborot tizimlarini joriy etish uchun ruxsatnoma berish;

– davlat idoralari, politsiya va boshqa idoralarda axborot almashinishda maxsus xavfsizlik choralarini amalga oshirish;

– sanoat vakillariga maslahatlar berish.

Xavfsizlikni ta’minlovchi boshqa davlat idoralari:

– Germaniyaning federal razvedka xizmati (Bundesnachrichten-dienst /BND/). BND federal kansler boshqarmasiga bo‘ysunadigan bo‘linma hisoblanadi. BNDning shtat tarkibi 7000 kishidan ziyodni tashkil etadi, ulardan 2000ga yaqini

bevosita xorijda razvedka ma’lumotlarini yig‘ish bilan band. Xodimlar orasida taxminan 70 ta turli soha vakillari: harbiy xizmatchilar, huquqshunoslar, tarixchilar, muhandislar va texnik mutaxassislar mavjud.

– Konstitutsiyani himoyalash federal byurosi (Verfassungsschutz /BfV/). Ushbu byuro BND va BSI bilan bir qatorda mamlakatning uchta maxsus xizmatlaridan biri hisoblanadi va u Germaniyaning ichki ishlar vazirligiga bo‘ysunadi. Barcha federal yerlarda mahalliy ichki ishlar vazirligiga bo‘ysunadigan o‘zining mos xizmatlari mavjud. Har yili to‘plangan axborotlar asosida Konstitutsiyaga rioya etilganligi doirasidagi ish holati haqida hukumatga hisobot taqdim etiladi, unda xulosalar va tavsiyalar qilinadi. Hukumat, o‘z navbatida, aniq choralarni amalga oshirish kerakligi haqida qaror qabul qiladi. Axborotning yarmidan ko‘pini maxsus xizmat ochiq manbalardan: ommaviy axborot vositalarida chop etilgan nashrlar, Internet, majlis va mitinglarda ishtirok etish orqali yig‘adi. Axborotning bir qismi ayrim kishilardan va boshqa idoralardan kelib tushadi. Fransiyada axborotni himoyalash tizimi. Fransiya kibermaydonda o‘zining fuqarolarini nazorat qilish bo‘yicha tuzilma tashkil etgan. Fransuzlar «Eshelon» nomli Amerika tizimiga o‘xshash o‘z tizimini yaratdilar. U deyarli barcha xususiy global kommunikatsiyalarni tutib qolishga yo‘naltirilgan. Milliy xavfsizlikni ta’minlash bo‘yicha siyosatning strategik yo‘nalishlarini ishlab chiqish bilan CLUSIF (Club de la securite informatique francaise) birlashmasi shug‘ullanadi. U o‘zining statusi bo‘yicha informatika sohasida ishlovchi yuridik va fizik shaxslarning ochiq assotsiatsiyasi hisoblanadi. CLUSIF davlat tomonidan to‘liq qo‘llab quvvatlanadi va maxsus xizmatlar bilan yaqin aloqaga ega. Fransiyaning maxsus xizmati strukturasi. Fransiya razvedka uyushmasining umumiy shtati, uchta har xil vazirlikka bo‘ysunuvchi xizmatlarda ishlaydigan 12779 ga yaqin xodimlardan iborat. Uchta xizmat Tashqi xavfsizlikning Bosh direksiyasi (DGSE); Harbiy razvedka boshqarmasi (DRM) va Harbiy kontrrazvedka boshqarmasi (DPSD) Mudofaa vazirligi himoyasida faoliyat olib boradi. Maxsus xizmatlarga jandarmeriyani (Gendarmerie) ham kiritish mumkin. Uning vazifalaridan biri bo‘lib razvedka faoliyatini yuritish hisoblanadi – jandarmeriyaning har bir qismida razvedka bo‘limi mavjud. Ikkita maxsus xizmat: kontrrazvedka (DST) va Bosh razvedka xizmati (RG) Ichki ishlar vazirligiga bo‘ysungan.

Rossiya Federatsiyasi (RF)ning axborot xavfsizligini ta’minlovchi davlat idoralari strukturasi. Axborot xavfsizligining davlat siyosatini ishlab chiqish, qonunlar, normativ-me’yoriy hujjatlar tayyorlash, axborotni muhofaza qilishni ta’minlash bo‘yicha o‘rnatilgan me’yorlarni bajarilishi ustidan nazoratni davlat idoralari amalga oshiradilar. RF Prezidenti axborot xavfsizligini ta’minlovchi davlat idoralariga boshchilik qiladi. U Xavfsizlik kengashini boshqaradi va davlatda axborot xavfsizligini ta’minlashga doir farmonlarni tasdiqlaydi. Mamlakatning

davlat xavfsizligiga oid boshqa masalalar bilan bir qatorda axborot xavfsizligi tizimining umumiy boshqaruvini RF Prezidenti va Hukumati amalga oshiradi. RF Prezidenti huzuridagi Xavfsizlik Kengashi davlat xavfsizligi masalalari bilan bevosita shug‘ullanuvchi hokimiyat idorasi hisoblanadi. Xavfsizlik Kengashi tarkibiga Axborot xavfsizligi bo‘yicha idoralararo komissiya kiradi. Komissiya davlatning axborot xavfsizligi sohasida Prezident farmonlarini tayyorlaydi, qonun chiqarish tashabbusi bilan chiqadi, vazirlik va idoralar rahbarlarining faoliyatini muvofiqlashtiradi. Axborot xavfsizligi bo‘yicha idoralararo komissiyaning ishchi idorasi bo‘lib RF Prezidenti huzuridagi Davlat texnik komissiyasi hisoblanadi. Bu komissiya qonun loyihalarini tayyorlashni amalga oshiradi, normativ me’yoriy hujjatlarni ishlab chiqadi, axborotni muhofaza qilish vositalarini (kriptografik vositalardan tashqari) sertifikatlashtirishni tashkil etadi, himoya vositalarini ishlab chiqish sohasidagi faoliyatni litsenziyalashtiradi va axborotni muhofaza qilish bo‘yicha mutaxassislarni o‘qitadi. Axborotni muhofaza qilish sohasida izlanishlar olib boruvchi davlat ilmiy-tadqiqot tashkilotlari faoliyatini muvofiqlashtiradi. Bu komissiya Davlat sirini himoyalash bo‘yicha idoralararo komissiya ishini ham ta’minlaydi. Davlat sirini himoyalash bo‘yicha idoralararo komissiyasiga davlat sirini tashkil etadigan ma’lumotlardan foydalanish, axborotni muhofaza qilish vositalarini yaratish hamda davlat sirini himoyalash bo‘yicha xizmat ko‘rsatish bilan bog‘liq korxona, muassasa va tashkilotlarni litsenziyalashni boshqarish vazifasi yuklatilgan. RF vazirlik va idoralarida axborot xavfsizligi siyosatining mos darajalarini boshqarishni ta’minlovchi iyerarxiyaga asoslangan tuzilmalar mavjud. Bu tuzilmalar, turli-xil nomlangani bilan o‘xshash funksiyalarni bajaradilar.

Nazorat savollari

1. Fransiya razvedka uyushmasining umumiy shtati qancha?
2. Kontrrazvedka xizmati qachon tuzilgan?
3. Britaniyaning Razvedka va xavfsizlik bo‘yicha parlament komiteti nima uchun tashkil etildi?
4. Markaziy razvedka boshqarmasi (MRB-SRU) nima uchun ishlab chiqilgan?
5. Federal tekshirishlar byurosi (FTB-FBR) nima uchun tashkil etildi?
6. Axborot qurolidan himoyalovchi dasturiy tasnifdagi amaliy tadbirlarga nimalar kiradi?

Adabiyotlar va internet saytlari:

1. Нестеров С. А. Информатsионная безопасность и защита информатsии: Учеб.пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с.

2. Чефранова А.О., Игнатов В.В., Уривский А.В. и др. Технология построения VPN: курс лекций: Учебное пособие.- Москва: Прометей, 2009. -180 с.
3. Шаньгин В. Ф. Защита информatsii в компьютерных системах и сетях - М: ДМК Пресс, 2012. - 596 с.

1-Amaliy mashg’ulot. Kiberxavfsizlikning rivojlanish istiqbollari (2 soat).

Reja:

4.1. Kiberxavfsizlikning rivojlanish tarixi.
4.2. Kiberxavfsizlikning rivojlanish istiqboli.
4.3. Kiberxavfsizlik kelajagiga ta'sir qiladigan tendentsiyalar.

Tayanch iboralar: Narsalar Interneti (IoT)**,** *Bulutli texnologiyalar, sun’iy intellektt, Xizmat sifatida kiberjinoyat (CaaS), Avtomatlashgan zararli dasturlar, kvant texnologiyalar.*

Kiberxavfsizlikning rivojlanish tarixi.

Kiberxavfsizlik tarixi kompyuter va axborot texnologiyalarining paydo bo‘lishi bilan boshlangan. Internetning rivojlanishi va tarqalishi ham kiberxavfsizlik tahdidlarining paydo bo‘lishiga olib keldi. Kiberxavfsizlikning asosiy satrlari bilan ba'zi muhim davrlarni quyidagicha umumlashtirishimiz mumkin:

1960-yillar: Kompyuterlar birinchi marta paydo bo‘lganida, kiberxavfsizlik tushunchasi hali go‘daklik davrida edi. Bu davrda kompyuter tarmoqlari ko‘proq yopiq va cheklangan edi, shuning uchun kiber hujumlar va tahdidlar ham kamroq tarqalgan.

1970-yillar: Bu davrda kompyuter tarmoqlari rivojlanishda davom etdi va biznesda yanada kengroq qo‘llanila boshlandi. Ammo xavfsizlik choralari hali ham etarli emas edi va oddiy hujumlar paydo bo‘la boshladi.

1980-yillar: Shaxsiy kompyuterlarning keng tarqalishi va Internetdan tijorat maqsadlarida foydalanishning ortishi ham kiberxavfsizlik tahdidlarini diversifikatsiya qildi. Viruslar va qurtlar kabi zararli dasturlarning birinchi holatlari shu davrda paydo bo‘la boshladi.

1990-yillar: Internetdan foydalanish tez sur'atlar bilan o‘sib, kompyuter tarmoqlari global miqyosda ulana boshlagan davr edi. Bu davrda kiberhujumlar yanada murakkab va keng tarqalgan. Tijoriy kiberhujumlar ham ortib bormoqda.

2000-yillar: Axborot texnologiyalarining jadal rivojlanishi kiberxavfsizlik sohasida yanada murakkab tahdidlarning paydo bo‘lishiga olib keldi. Kiberjinoyat, kiberterrorizm va davlat homiyligidagi kiberhujumlar kabi tahdidlarning har xil turlari diqqatni jalb qila boshladi.

2010-yillar: Mobil qurilmalarga qarshi kiberhujumlar smartfonlar va boshqa mobil qurilmalarning tarqalishi bilan ortdi. Shu bilan birga, katta ma'lumotlar, bulutli hisoblash va narsalar interneti (IoT) kabi texnologiyalardan foydalanish xavfsizlikka yangi muammolarni keltirib chiqardi.

Hozirgi va kelajak: Bugungi kunda kiberxavfsizlik global muammoga aylandi. Davlatlar, kompaniyalar va shaxslar kiberhujumlardan yaxshiroq himoya va mudofaa strategiyalarini ishlab chiqishga harakat qilmoqda. Sun'iy intellekt, mashinani o‘rganish va katta ma'lumotlar tahlili kabi texnologiyalar kiberxavfsizlikda yanada samarali mudofaa va hujumlarni aniqlash uchun ishlatiladi. Kelajakda kvant kompyuterlari va boshqa ilg'or texnologiyalarning paydo bo‘lishi bilan kiberxavfsizlik sohasida yangi muammolar va imkoniyatlar paydo bo‘ladi. Shu sababli, xavfsizlik choralarini doimiy ravishda takomillashtirish va kiberxavfsizlik sohasida xabardorlikni oshirish muhim vazifa bo‘lib qoladi.

Kiberxavfsizlikning rivojlanish istiqboli

Kiberxavfsizlik kelajagiga nazar tashlaydigan bo‘lsak, yodda tutish kerak bo‘lgan bitta muhim ogohlantirish bor: hammasi bir zumda o‘zgarishi mumkin.

Yildan yilga sanoat o‘zgarib bormoqda. Kibertahdidlar rivojlanadi va ulardan himoya vositalari bu o‘zgarishlarni aks ettiradi va tobora murakkablashib borayotgan tarmoqlarni yaxshiroq himoya qilish uchun o‘z huquqida rivojlanadi.

Kiberxavfsizning rivojlanishi bir qator omillarning o‘zaro ta'sirida shakllanadi:

Texnologiyani rivojlantirish: Texnologiyaning jadal rivojlanishi yangi kiber tahdidlar va hujum usullarini keltirib chiqaradi. Shu sababli, xavfsizlik bo‘yicha mutaxassislar va mudofaa mexanizmlari kiberhujumchilar tomonidan qo‘llaniladigan yangi texnologiyalarga qarshi bosqichma-bosqich borishlari kerak.

Raqamlashtirishning kuchayishi: Internet va raqamli texnologiyalardan keng foydalanish kundalik hayotimizning bir qismiga aylandi. Bu shaxsiy va korporativ ma'lumotlarni onlayn almashish va saqlash imkonini beradi. Shunga ko‘ra, kiberxavfsizlik choralari va xabardorligini oshirish ahamiyat kasb etdi.

Kiberhujumlarning murakkabligi: Kiberhujumlar texnologiya taraqqiyoti bilan yanada murakkab va murakkablashdi. Murakkab kiberhujumlar maqsadlarni diversifikatsiya qilishi va avval noma'lum usullardan foydalangan holda xavfsizlik devorlarini chetlab o‘tishi mumkin.

Katta ma'lumotlar va ma'lumotlar tahlili: Katta ma'lumotlar tahlili hujumchilar va mudofaa mutaxassislari uchun muhim vositadir. Ma'lumotlar tahlili hujum tendentsiyalarini aniqlash, tahdidlarni aniqlash va mudofaa strategiyasini ishlab chiqishda yordam beradi.

Inson omili: Kiberxavfsizlikning eng zaif bo‘g'ini odatda inson omilidir. Ijtimoiy muhandislik hujumlari va noto‘g'ri xatti-harakatlar zaifliklardan foydalanishning keng tarqalgan usuli bo‘lishi mumkin. Shu sababli, ta'lim va xabardorlik kampaniyalari kiberxavfsizlikda muhim rol o‘ynaydi.

Davlat darajasidagi javob: Hukumatlar muhim infratuzilmalar va milliy xavfsizlikni himoya qilish uchun kiberxavfsizlik siyosati va qoidalarini ishlab

chiqadi va kuchaytiradi. Davlat darajasidagi aralashuv kiberhujumchilarga qarshi yanada samarali mudofaani ta'minlaydi.

Sanoat standartlari va hamkorlik: Kiberxavfsizlik sohasida sanoat standartlarini yaratish va xavfsizlik yechimlarini ishlab chiqish tahdidlarga qarshi yanada samarali kurashda muhim rol o‘ynaydi. Bundan tashqari, xususiy sektor, ilmiy muassasalar va hukumatlar o‘rtasidagi hamkorlik va bilim almashish kiberxavfsizlik bo‘yicha kuchli himoyani ta'minlaydi.

Natijada, texnologiya taraqqiyoti, raqamlashtirish, kiberhujumlarning murakkabligi va xavfsizlik bo‘yicha xabardorlikni oshirish kabi bir qator omillarning o‘zaro ta'siri natijasida kiberxavfsizning rivojlanishi shakllanadi. Doimiy ravishda o‘zgarib turadigan tahdidlarga qarshi kuchliroq kiberxavfsizlik ekotizimini yaratishga harakat qilish kerak.

Kiberxavfsiz rivojlanayotgan sohada quyidagi tendentsiyalar ahamiyat kasb etdi:

Sun'iy intellekt va mashinani o‘rganish: Sun'iy intellekt va mashinani o‘rganish kiberxavfsizlikda katta rol o‘ynaydi. Sun'iy intellektga asoslangan xavfsizlik tizimlari tahdidlarni aniqlash va mudofaa choralarini avtomatlashtirish uchun katta hajmdagi ma'lumotlarni tahlil qiladi.

Narsalar Interneti (IoT) xavfsizligi: IoT qurilmalari uylardan tortib sanoat ob'ektlarigacha ko‘p sohalarda qo‘llaniladi. Biroq, bu qurilmalar xavfsizlik nuqtai nazaridan zaif havolalarni yaratishi mumkin. IoT qurilmalari xavfsizligini ta'minlash uchun yanada qat'iy choralar va standartlar ishlab chiqilishi kerak.

Bulutli xavfsizlik: Bulutli hisoblash - bu ma'lumotlar va xizmatlar markazlashtirilmagan serverlarda saqlanadigan va qayta ishlanadigan xizmat modeli. Foydalanuvchilar bulutga asoslangan xizmatlarga tobora ko‘proq murojaat qilar ekan, bulut xavfsizligi muhimroq.

Autentifikatsiya va biometrik xavfsizlik: autentifikatsiya usullari an’anaviy parolga asoslangan usullardan biometrik tanib olish texnologiyalariga o‘tmoqda. Barmoq izi, yuzni tanish va ovozni aniqlash kabi biometrik usullar autentifikatsiyani yanada xavfsizroq qilish imkonini beradi.

Autentifikatsiya foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini anikdash jarayonidir.

Kiber urush va davlat darajasidagi hujumlar: Davlatlar o‘rtasidagi kiber urush va josuslik xavfsizlikda, shuningdek, an'anaviy harbiy mojarolarda muhim rol o‘ynaydi. Davlat tomonidan homiylik qilinadigan kiberhujumlar muhim infratuzilma va milliy xavfsizlikni nishonga olishi mumkin.

Inson omili va xabardorlik: Inson omili hali ham Kiber xavfsizligining eng zaif bo‘g'inidir. Ijtimoiy muhandislik hujumlari va foydalanuvchi xatolari kiberhujumlar muvaffaqiyatli bo‘lishining muhim sabablari hisoblanadi. Shu

sababli, foydalanuvchilarning xavfsizlik bo‘yicha xabardorligini oshirish va treninglar orqali xabardorlikni oshirish muhimdir.

Xalqaro hamkorlik: Kiberxavfning etishmasligi chegaradan oshib ketadigan muammodir va xalqaro hamkorlik uni samarali hal qilish uchun muhimdir. Tahdidlar haqidagi ma’lumotlar va ilg‘or tajribalarni almashish orqali mamlakatlar va xalqaro tashkilotlar kuchli global kiberxavfsizlik muhitini yaratishi mumkin.

Kiberxavfsiz rivojlanayotgan sohada texnologiya va kiberhujumlar o‘rtasida doimiy poyga bor. Shu sababli, kiberxavfsizlik bo‘yicha mutaxassislar va tashkilotlar doimiy ravishda tahdidlarga qarshi yangilanib turishlari va faol choralar ko‘rish orqali kelajakdagi hujumlarga tayyor bo‘lishlari kerak.

Kiberxavfsizlikning kelajagi bu - kvant va bulutli hisoblashdir

Kvant hisoblash - bu kiberxavfsizlikni keskin oshirishi mumkin bo‘lgan rivojlanayotgan texnologiya. Kvant kompyuterlari kvant fizikasining noyob xususiyatlaridan foydalanib, hisob-kitoblarni an'anaviy kompyuterlarga qaraganda ancha tez va samaraliroq bajaradi. Kvant kriptografiyasi va kiberxavfsizlikning kelajagi kvant ilovalari orqali kriptografiya va kiberxavfsizlik sohasidagi eng so‘nggi tadqiqotlar va ishlanmalarni ta'minlovchi ajoyib ilmiy manbadir.

Kvant kompyuterlarining asosiy afzalliklaridan biri oddiy kompyuter hisoblab bo‘lmaydigan murakkab muammolarni hal qilish qobiliyatidir. Masalan, kvant kompyuterlari juda xavfsiz shifrlash algoritmlarini buzish uchun ishlatilishi mumkin. Ular antivirus dasturlari kabi ilg'or kiberxavfsizlikni himoya qilish choralarini buzish uchun ham ishlatilishi mumkin. Bu xakerlarga tarmoqlarga kirib, qimmatli ma'lumotlarni o‘g'irlash imkonini beradi. Agar kiberhujum muvaffaqiyatli bo‘lsa, bu halokatli oqibatlarga olib kelishi mumkin, jumladan, iqtisodning ommaviy ravishda buzilishi va hatto mamlakatlar o‘rtasidagi urush.

Kvant hisoblash ham sun'iy intellektga (AI) katta ta'sir ko‘rsatishi mumkin. AI atrofdagi dunyo haqida o‘rganish va bashorat qilish uchun katta ma'lumotlar bazalariga tayanadi. Kvant kompyuterlari AI texnologiyalarida sezilarli yaxshilanishlarga olib kelishi mumkin bo‘lgan katta hajmdagi ma'lumotlarni sindirishning yangi usulini taklif qiladi. Kvant hisoblashning rivojlanishi juda ko‘p vaqt va kuch talab qiladi, ammo bu texnologiya haqiqatga tez yaqinlashayotganga o‘xshaydi.

Bulutli hisoblash - bu uzoq serverlarga tayanadigan ma'lumotlarni saqlash va qayta ishlashning rivojlanayotgan modeli. Bu korxonalarga o‘zlarining IT infratuzilmalarining bir qismini tushirishga imkon beradi, shu bilan birga oxirgi foydalanuvchilarga o‘z ma'lumotlarini joylashtirish uchun ishonchli va xavfsiz platformaga kirish imkonini beradi.

Kiber tahdid landshafti rivojlanib borar ekan, tashkilotlar qabul qilishi kerak bo‘lgan xavfsizlik choralari ham shunday bo‘ladi. Va bugungi kunda bulutli

hisoblash kiber xavfni kamaytirishning eng samarali usullaridan biridir. Buning sababi shundaki, u bir qator muhim afzalliklarni taqdim etadi:

- Bu, birinchi navbatda, kompaniyalarga ularni qo‘llab-quvvatlash uchun zarur bo‘lgan infratuzilmaga sarmoya kiritmasdan turib, yangi ilovalar yaratish va ishga tushirish imkonini berish orqali joylashtirish vaqtlarini tezlashtiradi.
- Ikkinchidan, bulutli hisoblash apparat yoki dasturiy ta'minotni tenglamadan olib tashlash orqali xarajatlarni kamaytiradi. Bu operatsion xarajatlarni kamaytiradi va boshqa biznes tashabbuslari uchun qimmatli resurslarni bo‘shatadi.
- Uchinchidan, bu kompaniyalarga kerak bo‘lganda ko‘proq server sig'imini qo‘shish orqali o‘z operatsiyalarini osonlik bilan kengaytirish imkonini beradi.
- To‘rtinchidan, mijozlarga xizmatlarni to‘g'ridan-to‘g'ri sotish imkonini berib, daromad olish uchun yangi kanallarni ochadi.
- Beshinchidan, bulutli hisoblash kompaniyalarga ma'lumotlar bo‘yicha olimlar va AI ekspertlari kabi uchinchi tomon provayderlari orqali ixtisoslashgan ekspertizadan foydalanish imkonini beradi. Bu ularning raqobatdosh ustunligini oshirishga va tobora kuchayib borayotgan sanoat landshaftida egri chiziqdan oldinda bo‘lishga yordam beradi.

Kiberxavfsizlik kelajagida AI va ML ning roli

AI (sun'iy intellekt) - bu inson idrokini taqlid qiluvchi texnologiya uchun soyabon atama. AIdan moliya, sog‘liqni saqlash va kiberxavfsizlik kabi turli sohalardagi vazifalarni avtomatlashtirish uchun foydalanish mumkin. Bundan tashqari, boshqa odamlar bilan o‘zaro munosabatimizni yaxshilash uchun ham foydalanish mumkin. Misol uchun, sun'iy intellekt chatbotlari bizga samaraliroq muloqot qilishimizga yordam beradi va ular yaxshi qarorlar qabul qilishimizga ham yordam beradi.

Sun'iy intellekt va kiberxavfsizlik kelajagi bir-biriga bog'langan, chunki AI kiberxavfsizlikka katta ta'sir ko‘rsatadi. Yaratilgan ma'lumotlar miqdori qanchalik ko‘p bo‘lsa, kiber tahdidlar soni shunchalik ko‘p bo‘ladi. Oqibatda, insoniyatga ulgurmaslik tobora qiyinlashib bormoqda. AI kiberxavfsizlikning ko‘plab jihatlarini, jumladan, hodisalarga javob berish, zararli dasturlarni aniqlash va hokazolarni yaxshilash imkoniyatiga ega.

AI hatto yangi fikrlash usullariga olib kelishi mumkin. Shu sababli ushbu sohadagi so‘nggi o‘zgarishlardan xabardor bo‘lish juda muhimdir. Bundan tashqari, kiberxavfsizlik masalasida hushyor bo‘lish muhim. Yuqorida aytib o‘tganimizdek, AI texnologiyalari ko‘pincha zararli shaxslar tomonidan maxfiy ma'lumotlarga kirish uchun qo‘llaniladi. Shunday ekan, har doim hushyor turish va tizimingiz yaxshi himoyalanganligiga ishonch hosil qilish muhimdir.

Kiberxavfsizlikda mashinani o‘rganishning roli yangi tushuncha emas. Biroq, texnologiyaning rivojlanishi va tahlil qilish uchun katta ma'lumotlar to‘plami bilan bu soha undan qanday foydalanish bo‘yicha katta yutuqlarga erishmoqda. Eng ko‘p qiziqish uyg'otadigan sohalardan biri bu anomaliyalarni aniqlash bo‘lib, u odatiy bo‘lmagan naqshlarni qidiradi. Bu noodatiy tarmoq faolligidan noodatiy foydalanuvchilar uchun noodatiy joylardan tizimga kirishigacha bo‘lgan har qanday narsa bo‘lishi mumkin. Bundan keyin nima bo‘lishini bashorat qilish uchun bashoratli tahlilda ham foydalanish mumkin.

Boshqa foydalanish anomaliyalarni aniqlash va xavfni baholashni o‘z ichiga oladi. Xavfni baholash foydalanuvchi xatti-harakatlariga qarab, ular tarmoq uchun xavf tug'diradimi yoki yo‘qmi. Anomaliyani aniqlash tarmoqdagi noodatiy faoliyatni qidiradi va bu hodisalarni keyingi tekshirish uchun belgilab beradi. Mashinani o‘rganish kelajakdagi voqealar haqida bashorat qilish usuli sifatida ham ishlatilishi mumkin, masalan, qachon buzilish sodir bo‘lishi yoki muayyan xatti-harakatlar hujumga olib kelishi mumkin.

Ko‘proq tashkilotlar ushbu tahlil vositalarini tatbiq etar ekan, ular nima qila olishida cheklov yo‘q. Mashinani o‘rganish tashkilotlarga nafaqat tahdidlarni aniqlashga, balki ularning faoliyatiga ta'sir qilish imkoniyatiga ega bo‘lgunga qadar ularni yumshatishga yordam berish potentsialiga ega. Sun'iy intellekt yoki mashinani o‘rganish kiberxavfsizlikning kelajagi ekanligi aniq.

Kiberxavfsizlik kelajagiga ta'sir qiladigan tendentsiyalar

Keling, kiberxavfsizlik sanoatining kelajagini ko‘rib chiqaylik:

1. Xizmat sifatida kiberjinoyat (CaaS)

Cybercrime-as-a-service (CaaS) onlayn taklif qilinadigan kiberjinoyat xizmatlaridan foydalanishni anglatadi. CaaS potentsiali juda katta, chunki u jinoyatchilarga jinoyat sodir etmasdan o‘z mahoratini monetizatsiya qilish yo‘lini taklif qiladi. Masalan, xaker boshqa shaxs tomonidan boshqa birovning kompyuter tarmog‘iga yoki qurilmalari tarmog‘iga kirib, ularga zararli dasturlarni o‘rnatish uchun yollanishi mumkin.

2. Zararli dasturlarni avtomatlashtirish

Zararli dasturlarni avtomatlashtirish zararli dasturlarni tadqiq qilishning bir yoki bir nechta jihatlarini avtomatlashtirishdir. Avtomatlashtirilgan vazifalar manba kodini tahlil qilish, tarmoq trafigini tahlil qilish va oxirgi nuqtani aniqlashni o‘z ichiga olishi mumkin. Ushbu usul zararli dasturlarning yangi turlarini topishni osonlashtirishi mumkin, ammo u xatolarni kiritish imkoniyatiga ham ega. Tahlil vazifalarini bajarish uchun zarur bo‘lgan vaqt va resurslarni qisqartirish uchun avtomatlashtirish texnologiyasidan foydalanish mumkin. Ayrim tashkilotlar qisqa vaqt ichida minglab fayllarni skanerlaydigan zararli dasturlarni aniqlashning avtomatlashtirilgan vositalaridan foydalanishni boshladi.

3. Polimorf zararli dastur

Polimorf zararli dastur - bu an'anaviy antivirus dasturlariga chidamli bo‘lish uchun mo‘ljallangan zararli dasturning yangi turi. Polimorf zararli dasturlar juda ko‘p turli xil fayllar shaklini oladi, lekin u har doim bir xil tarzda tarqaladi: elektron pochta orqali. Uni qonuniy fayllar sifatida osongina yashirish mumkinligi sababli, u tez va hech kim nima bo‘layotganini bilmasdan tarqalishi mumkin.

Ushbu turdagi tahdidlardan himoyalanishning eng yaxshi usuli bu sizning kompyuteringiz doimo eng so‘nggi antivirus dasturi bilan yangilanganligiga ishonch hosil qilishdir.

Agar siz o‘zingizni polimorf zararli dastur tomonidan buzilgan tizimda topsangiz, uni imkon qadar tezroq olib tashlashga harakat qiling. Agar siz ushbu turdagi muammolarni o‘zingiz hal qila olmasangiz, yordam beradigan IT mutaxassisiga murojaat qiling.

4. Uchinchi tomon xavflari

Uchinchi tomon xavf-xatarlari kiberxavfsizlik uchun eng aniq va potentsial ravishda eng zararli hisoblanadi. Bularga uchinchi tomon xodimlari, hamkorlar va sotuvchilar tomonidan yuzaga keladigan xavflar kiradi. Uchinchi tomon xavfini to‘rt toifaga bo‘lish mumkin: insayder tahdidlar (xodimlarni o‘g‘irlash, poraxo‘rlik va h.k.), tashqi tahdidlar (xakerlar, kiberhujumlar va h.k.) va muvofiqlik risklari (masalan, ma’lumotlarning buzilishi).

Insayder tahdidlar odatda xodimlarning ma'lumotlarni o‘g'irlashi yoki tizimlarni buzish bilan bog'liq. Tashqi tahdidlar xakerlar yoki boshqa begonalardan keladi. Muvofiqlik xavfi odatda ma'lumotlar xavfsizligi siyosati va protseduralari bilan bog'liq. Uchinchi tomon xavflarining hammasi ham zararli kampaniyaning bir qismi emas. Misol uchun, uchinchi tomon sotuvchilari tomonidan qilingan xatolar mijozlar ma'lumotlarining oshkor bo‘lishiga olib kelishi mumkin.

5. Inson elementi

Inson elementi kiberxavfsizlik uchun eng katta tahdiddir. Ayniqsa, yosh avlodlar uchun texnologiyalardan foydalanish imkoniyatlarining oshishi kiberjinoyatlar va xavfsizlikni buzish holatlarining ko‘payishiga olib kelmoqda. Odamlar texnologiyadan qulayroq bo‘lib, undan foydalanishdan kamroq qo‘rqqanlari sababli, ular xakerlar qarshisida ham himoyasiz bo‘lib bormoqda.

Kompaniyalar o‘z xodimlarini kiber tahdidlardan himoya qilish uchun choralar ko‘rishlari kerak. Kiber tahdidlar haqida xabardorlikni oshirish ham sodir bo‘ladigan hujumlar sonini kamaytirishga yordam beradi. Xodimlar o‘zlari ko‘rgan har qanday muammolar haqida xabar berishlari mumkin bo‘lgan xavfsiz muhitni yaratib, kompaniyalar o‘z tizimlari xavfsizligini ta'minlashga yordam berishi mumkin.

6. Xavfsizlikka tahdidlarning kuchayishi

Kiberxavfsizlik tahdidlari tez sur'atlar bilan ortib bormoqda, har kuni tobora koʻproq kiberhujumlar sodir boʻlmoqda. Bu hujumlar identifikatorni oʻgʻirlashdan tortib hukumat va korporativ tizimlarga xakerlik hujumigacha boʻlgan turli shakllarda boʻlishi mumkin. Bundan tashqari, botnetlar, soxta yangiliklar va toʻlov dasturlari kabi "yangi" tahdidlar soni ortib bormoqda.

Kiberxavfsizlik tahdidlarini butunlay yoʻq qilishning imkoni boʻlmasa-da, ma'lumotlaringiz va ma'lumotlaringizni himoya qilish uchun ehtiyot choralarini koʻrish muhimdir. Buning eng yaxshi yoʻli dasturiy ta'minotni muntazam yangilab turish va xavfsizlik tizimingiz yangilanganligini ta'minlashdir.

7. Kripto va NFT firibgarliklari

NFTs yoki oʻzgartirilmaydigan tokenlar kriptovalyutalarning yangi turi boʻlib, kriptovalyutalarni sotish usullarini soddalashtirishga qaratilgan. NFTlar boshqa kriptovalyutalarga qaraganda osonroq sotilishi uchun yaratilgan, chunki noyob oʻn oltilik identifikator har bir tokenni ifodalaydi.

Bu texnologiya foydalanuvchilarga oddiygina QR kodni skanerlash yoki token manzilini hamyoniga qoʻlda kiritish orqali NFT sotib olish va sotish imkonini beradi. NFT’laringizni xavfsiz QR kod bilan shifrlash yaxshiroqdir. Onlayn QR kod ishlab chiqaruvchi dasturiy ta'minot yordamida siz raqamli uzatish uchun xavfsiz va xavfsiz QR kodlarini yaratishingiz mumkin. Ular, shuningdek, hamyonlar oʻrtasida oʻtkazish oson va firibgarlikka chidamli, chunki har bir token noyobdir. Biroq, ular Bitcoin kabi boshqa kriptovalyutalar kabi xavfsiz emas, chunki ular ulushning ishonchli isboti oʻrniga "ish isboti" deb nomlangan algoritmdan foydalanadilar. Shuning uchun foydalanuvchilar oʻzlarining NFTlarini xavfsiz raqamli hamyonda saqlashlari kerak.

8. Nolinchi ishonch tamoyillarini qabul qiling

Ishonchsizlik tamoyillarini qabul qilish tashkilot xodimlari tarmoq va tizim ma'murlariga ishonishlari shart emasligini anglatadi. Ular har qanday tarmoqqa kirish potentsial zararli deb taxmin qilishlari va shunga muvofiq harakat qilishlari mumkin. Ushbu yondashuv fishing hujumlaridan, ma'lumotlarni manipulyatsiya qilishdan va boshqa kiber tahdidlardan himoya qilish uchun moʻljallangan. Ushbu yondashuvni qoʻllagan tashkilotlar xavfsizroq boʻladi, chunki ular oʻz xodimlariga maxfiy ma'lumotlarni tasodifan oshkor qilish yoki qurilmalariga zararli dasturlarni oʻrnatishni oldini olishlari mumkin.

9. Javob berish imkoniyatlarini takomillashtirish

Kibertahdid landshafti rivojlanishda davom etar ekan, tashkilotlar uchun kuchli kiberxavfsizlik pozitsiyasiga ega boʻlishlarini ta'minlash juda muhimdir. Tashkilotlarga tahdidlarni tezda aniqlash va ularga javob berishga yordam beradigan texnologiyaga sarmoya kiritish javob berish imkoniyatlarini yaxshilashning asosiy usullaridan biridir. Masalan, yangi avlod xavfsizlik devorlari kiruvchi trafikni tezda

aniqlashi va bloklashi mumkin, buzg'unchilikni aniqlash tizimlari tashkilotlarni shubhali harakatlar haqida ogohlantirishi mumkin. Tashkilotlar ushbu texnologiyalarga sarmoya kiritish orqali o‘zlarini kelajakdagi tahdidlarga yaxshiroq tayyorlashlari mumkin.

Nazorat savollari

1. Sun’iy intellekt va kiberxavfsizlik kelajagi bir-biriga qanday bog‘langan?
2. Kiberxavfsizlikni keskin oshirishi mumkin bo‘lgan rivojlanayotgan texnologiya qaysi?
3. Inson elementi qanday tahdidlarni yaratishi mumkin?
4. NFT'lar qanday xavfsizlashtirilishi mumkin?
5. Kiberxavfsizlikning eng zaif bo‘g'ini nima hisoblanadi?

Adabiyotlar va internet saytlari:

1. Cyber security policy guidebook. Jennifer L. Bayuk. Jason Healey. Paul Rohmeyer, et.c. Willey publisher.2018-y. 288 p. ISBN 978-1-118-02780-6.

2. I. M. Karimov, N. A. Turgunov, F. Kadirov, Axborot xavfsizligi asoslari: Ma’ruzalar kursi, T.: O‘zbekiston Respublikasi IIV Akademiyasi, 2013. – 123 b.

3. Олифер В.Г.,Олифер Н.А. “Безопасность компьютерных сетей”2017 г.

IV-BO‘LIM

AMALIY MASHG‘ULOT MATERIALLARI

IV. AMALIY MASHG’ULOT MATERIALLARI

1-Amaliy mashg’ulot. Kvant hisoblash va 5G tarmoqlari kabi rivojlanayotgan texnologiyalarni himoya qilish (2 soat).

So‘nggi bir necha yil ichida kvant hisoblashning kriptografik tizimlarga ta'siri ko‘p muhokama qilinmoqda. Keng miqyosli, umumiy maqsadlar haqida umumiy kelishuv mavjud emas. Ularni rivojlantirish uchun katta sa'y-harakatlar davom etmoqda. Bundan tashqari, keng muhokama qilinganidek, agar bunday kompyuterlar mavjud bo‘lsa, bugungi kunda ko‘plab kriptografik tizimlarning xavfsizligiga ta'siri sezilarli bo‘ladi.

Bu shuni ko‘rsatadiki, kriptografiyaning har bir asosiy qo‘llanilishi uchun kvant hisoblashning ta'sirini diqqat bilan ko‘rib chiqish kechiktirmasdan amalga oshirilishi kerak.

Ushbu ko‘rib chiqish, agar kvant kompyuteri mavjud bo‘lsa, tizimning qaysi qismlari zaif ekanligini va tizimning bu qismi buzilgan taqdirda qanday ta'sir qilishini baholashi kerak.

Bunday ko‘rib chiqish, shuningdek, tizimning har bir qismida ishlatiladigan kriptografiyani almashtirish uchun qancha vaqt ketishini ko‘rib chiqishi kerak; ushbu baholash spetsifikatsiyalarni yangilash uchun zarur bo‘lgan vaqtni, o‘rnini bosuvchi ilovalarni ishlab chiqarish vaqtini va "sohada" barcha mavjud ilovalarni almashtirish vaqtini o‘z ichiga olishi kerak.

Umumiy vaqt dastur domeniga qarab juda katta bo‘lishi mumkin. Masalan, kredit va debet kartalarining ishlash muddati odatda uch-besh yilni tashkil qiladi, shuning uchun barcha bunday kartalarni yangi texnologiya bilan almashtirish o‘n yil yoki undan ko‘proq vaqtni olishi mumkin (va bu ulardan foydalanishni qo‘llab-quvvatlovchi infratuzilmani almashtirish uchun zarur bo‘lgan vaqtni ham hisobga olmaydi).

Mobil telekommunikatsiya infratuzilmasining xavfsizligi dastlab 1980-yillarda ishlab chiqilgan va birinchi marta 1991-yilda ishga tushirilgan GSM tizimi paydo bo‘lganidan beri kriptografiyadan foydalanishga tayanadi (GSM ko‘pincha mobil telekommunikatsiyaning 2-avlodi uchun 2G deb ataladi). 5G mobil telekommunikatsiya standartlarining so‘nggi avlodi bo‘lib, 3GPP tashkiloti 1 tomonidan ishlab chiqarilgan va 5G tizimlari hozir butun dunyo bo‘ylab qo‘llanilmoqda. Mobil telekommunikatsiya tizimlari butun dunyoda juda keng qo‘llaniladi va 5G jamiyat bilan yanada yaqinroq integratsiyalashgandir.

Bu shuni anglatadiki, 5G tizimlarining xavfsizligi juda muhim masala. Ushbu kuzatuvlar kvant hisoblashning 5G mobil xavfsizligiga ta'sirini ko‘rib chiqadigan ushbu maqolaga turtki bo‘ldi. 5G texnologiyasi allaqachon joriy etilayotgani va kelgusi bir necha yil ichida ushbu texnologiyaga katta sarmoyalar kiritilishi mumkinligini hisobga olsak, bunday ko‘rib chiqish ayniqsa o‘z vaqtida ko‘rinadi. Ma'lum bo‘lishicha, agar kvant kompyuteri mavjud bo‘lsa, tizimning hozirda ko‘rsatilgan asosiy qismlari zaif bo‘ladi. Ushbu batafsil tahlilni amalga oshirish taklif qilinayotgan joriy tizim xavfsizligini oshirish bo‘yicha bosqichma-bosqich

yondashish imkonini berdi, bu esa silliq va soddalashtirilgan migratsiya yo‘lini ta'minlaydi.

5G xavfsizligi evolyutsiyasidagi ustuvorliklarni ko‘rib chiqishdan saboq olishimiz mumkin bo‘lgandan tashqari, ushbu tadqiqot xavfsizlik uchun kriptografiyaga tayanadigan boshqa keng tarqalgan texnologiyalar uchun “kvantdan keyingi” sharhlarni o‘tkazishda ham yordam beradi deb umid qilamiz.

Kvant hisoblashning zamonaviy kriptografiyaga ta’siri.

Kriptanaliz. Agar keng ko‘lamli umumiy maqsadli kvant kompyuterlari qurilgan bo‘lsa, hozirda ishlatiladigan kriptografiyaga ta'siri juda muhim bo‘ladi.

Xususan, simmetrik (maxfiy kalit) va assimetrik (ochiq kalit) kriptografik algoritmlarga ta'sir qiluvchi ikkita kvant algoritmi (ya'ni kvant kompyuterida bajariladigan algoritmlar) ishlab chiqilgan.

1994 yilda nashr etilgan Shor algoritmi (Shor, 1994), bugungi kunda keng qo‘llaniladigan barcha assimetrik algoritmlarning xavfsizligiga juda katta ta'sir ko‘rsatadi. Buni to‘ldiruvchi, Groverning 1997 algoritmi (Grover, 1997) har qanday simmetrik algoritmning xavfsizligiga ta'sir qiladi, garchi unchalik jiddiy bo‘lmasa ham. Ushbu algoritmlarning ta'siri, ularni bajarish uchun kvant kompyuterini hisobga olgan holda, quyidagicha umumlashtirilishi mumkin.

• Katta butun sonlarni faktoring qilish yoki diskret logarifmlarni (shu jumladan elliptik egri chizmalarni) hisoblash qiyinligiga asoslangan barcha assimetrik kriptografik algoritmlar hozirda foydalanilayotgan kalit uzunliklari uchun xavfsiz bo‘lmaydi. Natijada, hozirda foydalanilayotgan barcha assimetrik sxemalarni keng ko‘lamli umumiy maqsadli kvant kompyuteri yordamida buzish mumkin edi. Bundan tashqari, hozirda foydalanilayotgan sxemalarni xavfsiz qilish uchun zarur bo‘lgan kalit uzunligining (katta) o‘sishi algoritmlardan foydalanishni ko‘p hollarda amalga oshirib bo‘lmaydigan qilib qo‘yadi.

• Barcha nosimmetrik kriptografik algoritmlar amalda kalit uzunligini sezilarli darajada qisqartiradi (printsipial jihatdan u ikki baravar qisqartiriladi, lekin amalda qisqarish bundan bir oz kamroq bo‘ladi). Ya'ni, kvant kompyuteri yordamida simmetrik algoritm uchun k-bitli kalitni 2 k / 2 hisoblash tartibida, ya'ni oddiy kompyuter yordamida zarur bo‘lgan 2 k hisoblash tartibining kvadrat ildizini topish mumkin edi. Biroq, kvant holatida bu "hisoblashlar" juda murakkab bo‘lishi mumkin, shuning uchun oddiy kvadrat ildiz argumenti unchalik to‘g'ri emas - kvant hujumlari an'anaviy kompyuterlar yordamida qo‘pol kuch qidiruvi kabi parallel bo‘lmaydi. Biroq, kvant hujumining aniq murakkabligini baholashda noaniqlik darajasini hisobga olgan holda, biz konservativ yondashuvni qo‘llaymiz; ya'ni o‘rnatilgan amaliyotga muvofiq, biz printsipga amal qilamiz, agar kvant kompyuter mavjud bo‘lsa va qachon, a128-bitli kalit bugungi kunda 64-bitli kalit bilan bir xil xavfsizlik darajasini taklif qiladi, ya'ni u xavfsiz bo‘lmaydi. . Ushbu tamoyilga amal qilgan holda, bugungi kunda 128 bitli kalit tomonidan taqdim etilgan xavfsizlik darajasiga erishish uchun 256 bitli kalitlarga o‘tish kerak bo‘ladi.

Qulay stenografiya sifatida biz har qanday potentsial raqib keng ko‘lamli umumiy maqsadli kvant kompyuterlariga kirish huquqini qo‘lga kiritgan vaqtni PQ davri deb aytamiz.

Kelajakda hozirda ishlatiladigan kriptografik algoritmlar xavfli bo‘lib qolsa, kelajakdagi ta'sir qanday bo‘lishini ko‘rib chiqish qiziq. Faqat uzatilgan ma'lumotlarning yaxlitligini tekshirish uchun ishlatiladigan, ya'ni foydalanish uzoq muddatli ta'sir ko‘rsatmaydigan algoritmlar uchun, agar yangi "xavfsiz" algoritmlar o‘z vaqtida joriy etilsa, hech qanday jiddiy muammolar bo‘lmaydi. Biroq, shifrlash va kalitlarni o‘rnatish algoritmlarining ahamiyati halokatli bo‘lishi mumkin.

Agar kelajakda xavfli bo‘lib qoladigan algoritm yordamida shifrlangan shifrlangan matn ushlanib qolsa va saqlangan bo‘lsa, u kelajakda shifrlash algoritmi buzilgan vaqtda shifrlanishi mumkin. Ya'ni, maxfiyligi har qanday uzoq muddatli ahamiyatga ega bo‘lgan ma'lumotlar, agar kvant kompyuterlari qurilgan bo‘lsa, xavfli bo‘lib qoladigan algoritmlardan foydalanish orqali himoyasiz holga keltirilmoqda.

Shunga o‘xshab, xavfsiz havola orqali almashinadigan ma'lumotlardan foydalanib, kelajakda buzilishi mumkin bo‘lgan asosiy o‘rnatish texnikasi qo‘llanilgan deylik. Agar kalitlar almashinuvi qayd etilsa, bunday usul yordamida o‘rnatilgan kalit yordamida shifrlangan har qanday nozik ma'lumotlar kvant kompyuteri mavjud bo‘lganda, buzilish xavfi ostida bo‘ladi.

Algoritmlarni almashtirish.

Bugungi kriptografiya xavfsizligi uchun potentsial halokatli oqibatlarni hisobga olgan holda, bir qator agentliklar yangi kriptografiya standartlarini ishlab chiqish ustida ishlamoqda. Nosimmetrik kriptografiyaning hozirgi holati 256 bitli kalitlardan foydalanishga imkon beradi, shuning uchun bu domenda katta o‘zgarishlar talab etilmaydi, faqat uzunroq kalitlarga (ya'ni 256 bit yoki undan ko‘p) o‘tishni majburlashdan tashqari.

Biroq, assimetrik kriptografiya uchun vaziyat unchalik oson emas, chunki assimetrik kriptografiyaning deyarli barcha joriy ilovalari xavfli bo‘lib qoladigan algoritmlardan foydalanadi. Bu bir qator standartlar tashkilotlarini (jumladan, NIST, ETSI va ISO/IEC JTC 1/SC 27/WG 2) kelajakdagi "postkvant" dunyosida xavfsiz bo‘lib qoladigan assimetrik kriptografik algoritmlar to‘plamini ishlab chiqish ustida ish boshlashiga olib keldi.

Bugungi kunga kelib, NIST ishi eng ta'sirli bo‘ldi, uning Post-Kvant Kriptografiyasi Standartlashtirish loyihasi natijalari SC 27/WG 2 kabi boshqa standartlar organlari tomonidan yaqindan kuzatilmoqda.

Ushbu loyihaning ko‘lami va holati eng yaxshi loyiha veb-sahifasidan iqtibos keltirish orqali umumlashtiriladi. Quyidagi chaqiruv 2017 yil noyabr oyida e'lon qilindi.

NIST bir yoki bir nechta kvantga chidamli ochiq kalitli kriptografik algoritmlarni so‘rash, baholash va standartlashtirish jarayonini boshladi. Hozirgi vaqtda ochiq kalitli kriptografik algoritmlar FIPS 186-4, Raqamli imzo standarti, shuningdek, SP 800-56A revision, Diskret logarifm kriptografiyasi va SP6B Revision-1-dan foydalangan holda juft kalitlarni yaratish sxemalari bo‘yicha tavsiyalar maxsus nashrlarida ko‘rsatilgan. Butun sonli faktorizatsiya kriptografiyasidan foydalangan holda juftlik kalitlarini o‘rnatish sxemalari bo‘yicha tavsiya. Biroq, bu algoritmlar katta hajmdagi kvant kompyuterlarining hujumlariga nisbatan zaifdir. Yangi ochiq kalitli kriptografiya standartlari bir yoki bir nechta

qo‘shimcha tasniflanmaganlarni belgilaydi. Ommaga oshkor qilingan raqamli imzo, ochiq kalitlarni shifrlash va kalitlarni yaratish algoritmlari butun dunyo bo‘ylab mavjud bo‘lib, hukumatning nozik ma'lumotlarini yaqin kelajakda, shu jumladan kvant kompyuterlari paydo bo‘lgandan keyin ham himoya qilishga qodir.

Ushbu jarayonning birinchi bosqichi sifatida NIST nomzod algoritmlari uchun qabul qilinadigan minimal talablar, topshirish talablari va baholash mezonlari loyihasi bo‘yicha jamoatchilik fikrini so‘radi. Qabul qilingan fikr-mulohazalar ushbu sharhlar natijasida kiritilgan o‘zgarishlarning qisqacha mazmuni bilan birga e'lon qilindi. Ushbu chaqiruv jamoatchilik sharhlari va kriptotahlillarni o‘z ichiga olgan bir qator turlar orqali standartlashtiriladigan to‘plamga qisqartirish jarayonida bo‘lgan yangi algoritmlar bo‘yicha ko‘plab takliflarga olib keldi.

5G texnologiyasi xavfsizligi

5G xavfsizligi 3GPP 5G xavfsizlik spetsifikatsiyalarining 15-versiyasida (R15) belgilangan (3GPP, 2019c). E'tibor bering, R15 hozir barqaror va yaqinda uni R16 bilan almashtirish bo‘yicha ish boshlandi; ammo, ta'riflagan tizimning juda oz qismi R16 da o‘zgartirilgan ko‘rinadi. Hozirgi vaqtda aniqlangan 5G xavfsizligini 3G (UMTS) va 2G (GSM) xavfsizlik qoidalarining evolyutsiyasi bo‘lgan 4G xavfsizligining evolyutsiyasi sifatida ko‘rish mumkin. Biroq, 4G dan uchta asosiy farq:

• autentifikatsiya usulida moslashuvchanlik: foydalanuvchi uskunasi (UE), mobil telefon, xizmat ko‘rsatuvchi tarmoqqa autentifikatsiya qilinishi mumkin (rasmiy ravishda ushbu tarmoqning SEcurity Anchor FunKTRon (SEAF), tarmoqning autentifikatsiya serveri funksiyasi (AUSF) bilan hamkorlik qiladi. xavfsizlik funksiyalari) yoki o‘zi 4G AKA evolyutsiyasi bo‘lgan 5G AKA (Autentifikatsiya va kalit kelishuvi) protokoli yoki Internet EAP-AKA ′ protokoli 3 dan foydalangan holda;

• mustahkam mobil identifikator maxfiyligi: ochiq kalit shifrlashdan foydalanish doimiy foydalanuvchi identifikatorini tarmoq bo‘ylab aniq matnda yuborish zaruratini yo‘q qiladi;

• ma'lumotlar yaxlitligini himoya qilish: bu havo interfeysi orqali yuborilgan ma'lumotlarning yaxlitligini (shu jumladan raqamlashtirilgan ovoz) himoya qilish uchun autentifikatsiya paytida o‘rnatilgan seans kalitidan olingan kalitlardan foydalanishni o‘z ichiga oladi.

Bu erda 5G AKA protokoli qo‘llaniladigan holatga e'tibor qaratilgan, ammo to‘liq tahlil qilish uchun EAP-AKA ' ishini ham ko‘rib chiqish kerakligi aniq. Quyida tavsiflanganidek, xavfsizlik qoidalarini to‘rtta asosiy qismga bo‘lish mumkin:

• AKA : bu UE va xizmat ko‘rsatuvchi tarmoq o‘rtasida almashinuvni o‘z ichiga oladi, buning natijasida ikki tomon o‘zaro autentifikatsiya qilinadi va ikki ob’ekt o‘rtasida maxfiy seans kaliti o‘rnatiladi;

• Kalitni chiqarish: AKA davomida o‘rnatilgan seans kalitidan maqsadli kalitlarni chiqarishni o‘z ichiga oladi;

• Mobil identifikatorning maxfiyligi: bu UE hech qachon havo interfeysi orqali shifrlash yoki ajratilmaydigan vaqtinchalik identifikatorlardan foydalanish

orqali aniq matnli doimiy foydalanuvchi identifikatorini yubormasligini ta'minlashni o‘z ichiga oladi;

• Seans xavfsizligi: seans kalitidan olingan alohida maxfiy kalitlar UE va xizmat ko‘rsatuvchi tarmoq o‘rtasidagi havo interfeysi orqali yuborilgan ma'lumotlarni himoya qilish uchun ishlatiladi.

Barcha xavfsizlik xizmatlarining asosida abonent kartaga asoslangan Universal obunachi identifikatsiya moduliga (USIM) ega bo‘lishi talabi yotadi, u olinadigan yoki UEga ulangan bo‘lishi mumkin. Ushbu USIM uzoq muddatli 128 bitli 4 maxfiy kalitni AKA da foydalanish uchun saqlaydi, u ham uy tarmog'ining Autentifikatsiya hisob ma'lumotlari ombori va qayta ishlash funksiyasi (ARPF) tomonidan saqlanadi.

USIM shuningdek, identifikatorni shifrlash uchun foydalaniladigan uy tarmog'ining ochiq kalitini ham saqlaydi.

Nihoyat, keyingi tahlillar uchun etarli ma'lumot berish maqsadida quyidagi tavsiflar biroz soddalashtirilganiga e'tibor bering. Xususan, biz uzatish va rouming bilan bog'liq xavfsizlik masalalari bo‘yicha spetsifikatsiyadagi keng ko‘lamli qoidalarni ko‘rib chiqmadik. Shuningdek, biz SEAF funksiyalarini tegishli Kirish va harakatchanlikni boshqarish funksiyasidan (AMF), bu har qanday holatda ham SEAF bilan birga joylashishi.

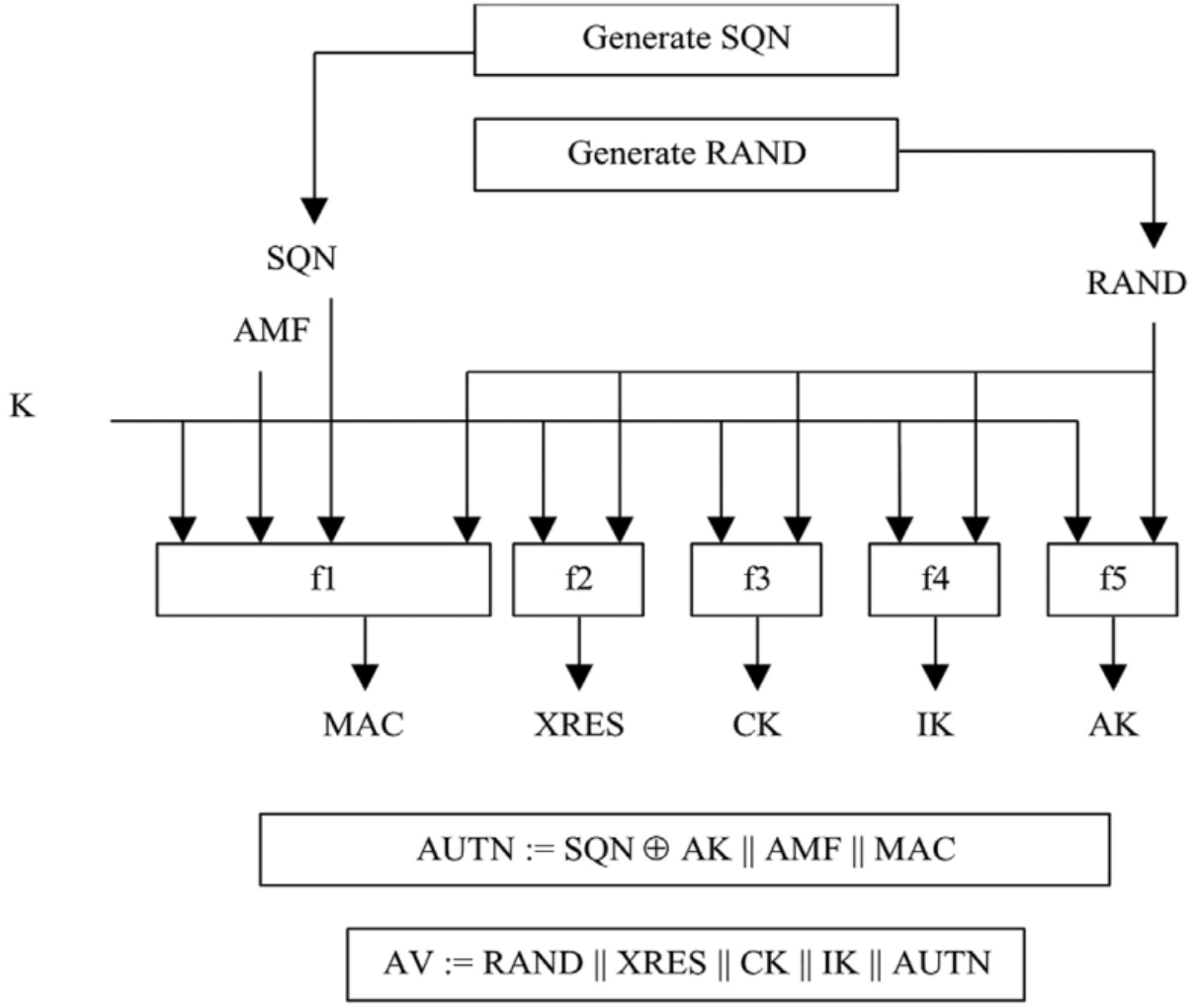
5G AKA protokolini 5G xavfsizligining yadrosi deb hisoblash mumkin. Bu 4G AKA protokoliga juda o‘xshaydi; bitta kichik o‘zgarish uy tarmog'ini xizmat ko‘rsatuvchi tarmoqqa UEning "muvaffaqiyatli autentifikatsiya isboti" bilan ta'minlashdir.

Barcha oldingi tizim avlodlarida bo‘lgani kabi (2G–4G), uy tarmog'ining ARPF so‘rov bo‘yicha xizmat ko‘rsatuvchi tarmoq AUSF-ni 5G HE autentifikatsiya vektori (AV) bilan ta'minlaydi. Ushbu 5G HE AV quyidagi tarzda ishlab chiqariladi (xizmat ko‘rsatuvchi tarmoqning AUSF tomonidan 5G HE AV dan hisoblangan 5G AV dan farqlash uchun u 5H HE AV deb ataladi;

5-qiymatli vektor (RAND, XRES, CK, IK, AUTN) birinchi bo‘lib 3G va 4G uchun AV-lar yaratilgani kabi aniq hisoblab chiqiladi. 3G/4G AV ni hisoblash 1-rasmda umumlashtirilgan. Aniqroq: RAND 128 bitli tasodifiy qiymat; XRES, CK va IK RAND va abonent maxfiy kaliti K funksiyasi sifatida hosil qilingan 128 bitli qiymatlardir; va AUTN 128 bitli autentifikatsiya tokenidir. AUTN 48-bitli SQN AK qatorini o‘z ichiga oladi, bunda SQN bu ARPF tomonidan boshqariladigan hisoblagichdan olingan tartib raqami, AK esa RAND va abonent maxfiy kaliti K funksiyasi sifatida yaratilgan 48-bitli shifrlash qatoridir. AUTN yana ikkita maydonni o‘z ichiga oladi: 16-bitli autentifikatsiyani boshqarish maydoni (AMF) va 64-bitli xabar autentifikatsiya kodi (MAC). MAC RAND, AMF, SQN va abonent maxfiy kaliti K funksiyasi sifatida hisoblanadi. AMFning 16 bitidan sakkiztasi xususiy maqsadlarda mavjud bo‘lib, ular, masalan, foydalanilayotgan f 1–f 5 algoritmlar to‘plamini ko‘rsatish uchun ishlatilishi mumkin (pastga qarang); qolgan sakkiztasidan yettitasi kelajakda foydalanish uchun ajratilgan. AMFdan foydalanish bo‘yicha qo‘shimcha ma’lumot olish uchun 3GPP TS 33.102 (3GPP, 2018a) F va H ilovalariga qarang.

MAC, XRES, CK, IK va AK ni olish uchun ishlatiladigan funksiyalar mos ravishda f 1, f 2, f 3, f 4 va f 5 bilan belgilanadi va maxfiy kalitga asoslangan MAC va kalit hosil qilish mexanizmlaridir. Ushbu algoritmlarni tanlash uyali aloqa operatoriga qoldiriladi, chunki ular faqat USIM va ARPFda amalga oshiriladi, ikkalasi ham operator tomonidan boshqariladi.

Biroq, ushbu algoritmlarga qo‘yiladigan talablar 3GPP TS 33.105 (3GPP, 2018b) da belgilangan va standart algoritmlar to‘plami taqdim etilgan.

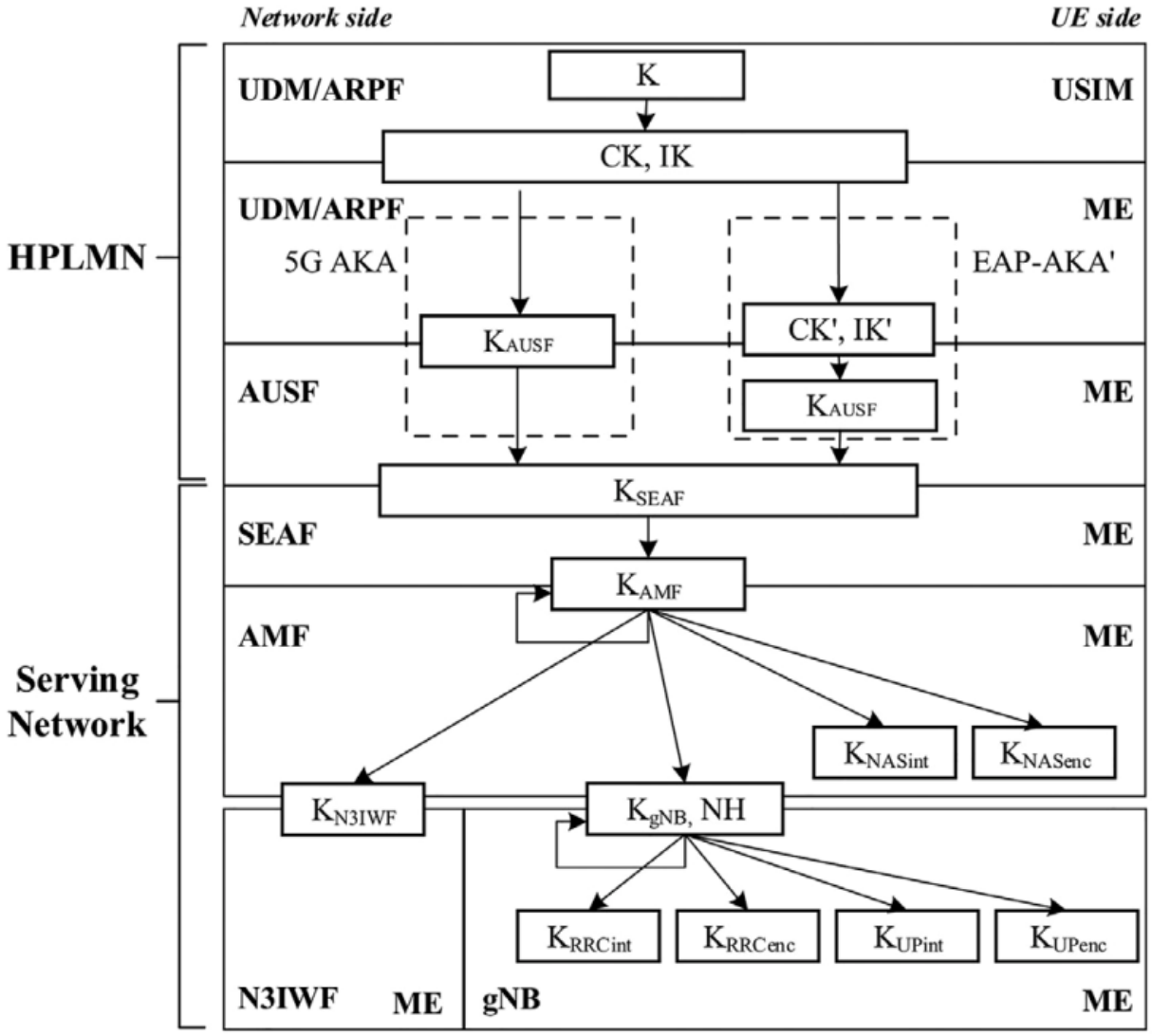


1.1-rasm. 3G/4G AV ni yaratish (TS 33.102 (3GPP, 2018a))

Mobil identifikatsiya maxfiyligi. 5Gda doimiy foydalanuvchi identifikatori obunaning doimiy identifikatori (SUPI) deb ataladi va u hech qachon foydalanuvchi interfeysi bo‘ylab aniq matnda yuborilmaydi. Buning o‘rniga, autentifikatsiyani boshlashda UE o‘zini SUPI ning shifrlangan versiyasi (obunaning yashirin identifikatori (SUCI)) yoki, agar mavjud bo‘lsa, avval o‘rnatilgan vaqtinchalik identifikator (5G-Globally Unique Ident TemporaryGUTI) yordamida o‘zini identifikatsiya qiladi. SUCI ni uzatish, agar u 5G-GUTI muammosini hal qila olmasa, xizmat ko‘rsatuvchi tarmoq tomonidan ham talab qilinishi mumkin.

SUCI “himoya sxemasi” (odatda assimetrik shifrlash sxemasi) va abonent uy tarmog‘ining ochiq kaliti yordamida SUPIdan yaratiladi, bunda himoya sxemasi

yoki ECIES (elliptik egri chiziqli shifrlash sxemasi 3GPP (2019c))) yoki uy tarmog‘ining tanlovi sxemasi. ECIES spetsifikatsiyasi rasmiy standartga emas, balki SECG spetsifikatsiyalariga 7 amal qiladi. Shifrlash USIM-ning xohishiga ko‘ra USIM yoki ME-da amalga oshirilishi mumkin.



2.2-rasm. Kalit hosila ierarxiyasi (TS 33.501 (3GPP, 2019c).

Albatta, agar shifrlash MEda sodir bo‘lsa, unda standartlashtirilgan sxemadan foydalanish kerak. Uy tarmog‘ining ochiq kaliti ishonchli manba orqali UE uchun mavjud bo‘lishi kerak, masalan. USIMda taqdim etish orqali. SUCI ni xizmat ko‘rsatish tarmog'iga yuborayotganda, UE uy tarmog'ining identifikatorini ham yuboradi. Shuni esda tutingki, shifrlash tasodifiy bo‘lib, bir xil SUPIdan yaratilgan ikkita SUCI bir-biridan farq qiladi va ajralmas bo‘ladi (albatta, ularni parolini hal qila oladigan uy tarmog'i bundan mustasno).

Keyin SUCI xizmat ko‘rsatuvchi tarmoq tomonidan tegishli uy tarmog'idan autentifikatsiya ma’lumotlarini so‘rash uchun ishlatiladi. Uy tarmog'i o‘zining shaxsiy parolini ochish kaliti yordamida SUPI-ni SUCI-dan tiklashi mumkin. Yangi 5G-GUTI havo interfeysi orqali UEga yuborilganda, u shifrlangan havola orqali yuboriladi.

Seans xavfsizligi

Biz 5G xavfsizlik mexanizmlarining qisqacha mazmunini UEga va undan yuborilgan har xil turdagi ma'lumotlarni himoya qilish uchun turli xil kalitlardan qanday foydalanishni ko‘rib chiqamiz. Avvalgidek, bu biroz soddalashtirilgan tavsif bo‘lib, ba’zi maxsus holatlar e'tiborga olinmaydi.

Oqim shifrlash kalit oqimi COUNT, shifr kaliti K NASenc, tashuvchi identifikatori va uzatish yo‘nalishini ko‘rsatuvchi bit (yuqoriga yoki pastga ulanish) funksiyasi sifatida hisoblanadi. Xuddi shunday, MAC COUNT funksiyasi, yaxlitlik kaliti K NASint, tashuvchi identifikatori, uzatish yo‘nalishini ko‘rsatadigan bit va xabar sifatida hisoblanadi.

Kelajakda 5G xavfsizligi

Yuqoridagi tahlilning asosiy maqsadi PQ davrining paydo bo‘lishining 5G xavfsizlik xususiyatlariga ta'sirini tushunish edi.

Endi ushbu tahlildan 5G tizimlari PQ davrida yetarli darajadagi xavfsizlikni ta’minlashga qodir bo‘lishini ta’minlash uchun bajarilishi kerak bo‘lgan qadamlar bo‘yicha bir qator tavsiyalarni ishlab chiqish uchun foydalaniladi.

Uzoq muddatli USIM maxfiy kalitiga hujumlar yuqorida ta'kidlab o‘tilganidek, bitta AKA chaqiruv-javob juftligini tutib olish K maxfiy kalitini ochish uchun hujumning asosi sifatida ishlatilishi mumkin. Buning oqibatlari quyidagilarni o‘z ichiga oladi:

• O‘tmishdagi (va kelajakdagi) ushlangan barcha shifrlangan ovoz va ma'lumotlar trafigi, agar darhol oldingi AKA protokoli namunasi davomida yuborilgan RAND qiymati ham ushlangan bo‘lsa, shifrlanishi mumkin edi;

• Faol “o‘rtadagi odam” tutuvchisi ma’lumotlarni o‘zgartirish va keyin MACni mos ravishda o‘zgartirish orqali ma’lumotlar va signalizatsiya trafikini muvaffaqiyatli boshqarishi mumkin (bu, masalan, agar UE konfiguratsiyasi oldini olish uchun o‘zgartirilsa, uzoq muddatli xizmat ko‘rsatishni rad etishga olib kelishi mumkin) manipulyatsiya qilingan signalizatsiya xabarlaridan foydalanish);

Bu bitta abonent xavfsizligi uchun halokatli bo‘lishi aniq bo‘lsa-da, hujum har bir USIM uchun takrorlanishi kerak. Hujumning har bir misoli 264 kvant operatsiyalari tartibini o‘z ichiga olishini hisobga olsak, juda oz sonli USIMlar uchun K kalitini tiklash hech bo‘lmaganda o‘rta muddatli istiqbolda amalda imkonsiz bo‘lishi mumkin.

Bunga qo‘shimcha ravishda, tarmoq bo‘ylab yuborilgan nozik ma'lumotlar shifrlanishi va yaxlitligi dastur qatlamida yoki darhol ostida himoyalanishi mumkin, masalan. SSL/TLS kabi protokoldan foydalanish. Masalan, HTTPS (Rescorla, 20 0 0) dan foydalanish (asosan HTTP TLS orqali ishlaydi) barcha veb-trafiklar uchun odatiy holga aylanib bormoqda. Natijada, bunday hujum orqali nozik ma'lumotlarning buzilishi ehtimoli kichik (albatta, amalda HTTPS xavfsizligi soxta sertifikatlarni qabul qilish orqali buzilishi mumkin).

2-Amaliy mashg’ulot. Sun’iy intellekt va kiberxavfsizlik (2 soat).

Ilm-fan va axborot-kommunikatsiya texnologiyalari jadal taraqqiy etib borayotgan bugungi sharoitda dunyoning rivojlangan mamlakatlarida davlat va jamiyat boshqaruvi, iqtisodiyot, sanoat, ijtimoiy himoya, ta’lim, tibbiyot, bandlik,

qishloq ho’jaligi, mudofaa, xavfsizlik, turizm va boshqa sohalarda zamonaviy axborot texnologiyalari va sun’iy intellekt imkoniyatlaridan keng foydalanish urfga kirmoqda.

O’zbekistonda ham axborotlashtirish va raqamli iqtisodiyotni rivojlantirish orqali 2030 yilga qadar innovatsion taraqqiy etgan yetakchi davlatlar qatoridan o’rin egallash ustuvor vazifa sifatida belgilangan.

Qayd etish joizki, “Ilm, ma’rifat va raqamli iqtisodiyotni rivojlantirish yili”da axborot texnologiyalari va raqamlashtirish borasida jiddiy o’zgarishlar amalga oshirilib, bir qator muhim dasturlar qabul qilindi.

Xususan, O’zbekiston Respublikasi Prezidentining “Raqamli iqtisodiyot va elektron hukumatni keng joriy etish chora-tadbirlari to’g’risida”gi, “Aholiga davlat ijtimoiy xizmatlari va yordam taqdim etish tartib-taomillarini avtomatlashtirish bo’yicha qo’shimcha chora-tadbirlar to’g’risida”gi hamda «Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to’g’risida»gi qarorlari va boshqa normativ-huquqiy hujjatlar mamlakatimizda raqamlashtirishni jadallashtirish va ijtimoiy-iqtisodiy sohalarga zamonaviy texnologiyalarni joriy qilishga qaratilgan.

O‘zbekiston respublikasi prezidentining 2021 yil 17 fevralda qabul qilingan «Sun’iy intellekt texnologiyalarini jadal joriy etish uchun shart-sharoitlar yaratish chora-tadbirlari to’g’risida»gi qarori bilan 2021-2022 yillarda sun’iy intellekt texnologiyalarini o’rganish va joriy etish bo’yicha choratadbirlar dasturi bunga yaqqol misol bo‘la oladi.

2022-yil 25-fevralda O‘zbekistonda kiberxavfsizlik sohasidagi munosabatlarni tartibga solish maqsadida “Kiberxavfsizlik to‘g‘risida”gi qonun qabul qilindi.

Qonunda kiberxavfsizlikni ta’minlashning asosiy prinsiplari sifatida quyidagilar keltirilgan:

– qonuniylik;

– kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi;

– kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv;

– kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi;

–O‘zbekiston Respublikasining kiberxavfsizlikni ta’minlashda xalqaro hamkorlik uchun ochiqligi.

Kiberxavfsizlik sohasidagi yagona davlat siyosatini O‘zbekiston Respublikasi Prezidenti belgilaydi. O‘zbekiston Respublikasi Davlat xavfsizlik xizmati kiberxavfsizlik sohasidagi vakolatli davlat organi xisoblanadi.

Kiberxavfsizlik hodisalari vakolatli davlat organi yoki kiberxavfsizlikni ta’minlash bo‘yicha ishchi organning mansabdor shaxslari tomonidan tekshiriladi.

Kiberxavfsizlik hodisasi sodir bo‘lgan axborot resursining yoki axborot tizimining egasi, agar u tekshiruv o‘tkazish uchun zarur bo‘lgan resurslarga va texnik imkoniyatlarga ega bo‘lsa, kiberxavfsizlik hodisasining tekshiruvini o‘tkazishi mumkin. Bunda vakolatli davlat organi tekshiruv natijalari to‘g‘risida xabardor qilinishi kerak.

Kiberxavfsizlik subyektlari tomonidan kiberxavfsizlik hodisalariga nisbatan choralar ko‘rish quyidagi shakllarda amalga oshirilishi mumkin:

– dasturiy ta’minotdagi va qurilmalardagi zaifliklarni hamda xatoliklarni bartaraf etish;

– zararli dasturlarni yo‘q qilish, ularning tarqalishini cheklash, kiberhujumlar manbaini texnik jihatdan cheklash;

– axborotlashtirish obyektlarini mavjud kibertahdidlardan ajratib qo‘yish;

– huquqni muhofaza qiluvchi organlarga kiberxavfsizlik hodisalari to‘g‘risida ma’lumotlar taqdim etish.

Sun’iy intellektni(SI) rivojlantirish hamda davlat organlari va boshqa tashkilotlar faoliyatida, shuningdek ushbu sohada normativ-huquqiy bazani tayyorlashda maslahatchi sifatida qatnashish uchun «Sber» guruhining (Rossiya) yetakchi mutaxassislari va ekspertlari jalb qilindi. Kiberjinoyatlar soni doimiy va tez ortib bormoqda. Shunday qilib, o‘tgan yil davomida Rossiya iqtisodiyotining xakerlar faoliyatidan ko‘rgan yo‘qotishlari taxminan 6 trillion rublni tashkil etdi. Mutaxassislarning fikricha, hujumchilar ko‘pincha axborot xavfsizligi bo‘yicha mutaxassislar va huquq-tartibot xodimlaridan bir emas, bir necha qadam oldinda bo‘ladi.

Sun'iy intellekt odamlar qila olmaydigan narsani qila olmaydi. Axir, sun'iy intellektning butun asosi inson xatti-harakatlariga taqlid qiladigan mashina yaratishdir. Ammo sun'iy intellekt ishlarni tezroq bajarishi va inson uchun juda ko‘p mehnat talab qiladigan katta hajmdagi ma'lumotlarni tahlil qilishi mumkin. SI zararli dasturlarning belgilarini aniqlash uchun murakkab naqshni aniqlash vositalaridan avtomatik ravishda foydalanishi mumkin. Sun'iy intellekt kuchli texnologiya bo‘lmasada va barcha tahdidlarni aniqlay olmasa ham, bu texnologiya mutaxassislarning ogohlantirishlarni o‘rganishga sarflash vaqtini qisqartiradigan muhim vositadir. Va bu, ehtimol, SIning eng muhim afzalligi.

So‘nggi 3-5 yil ichida kibermakondagi rivojlanish va o‘zgarishlar tezligi nafaqat tajribasiz foydalanuvchilarni, balki IT va axborot xavfsizligi sohasidagi tajribali mutaxassislarni ham hayratga solmoqda. Hatto qayta ishlangan ma'lumotlar

miqdori, Internetga ulangan qurilmalar yoki ilovalar/xizmatlar sonida ham emas, balki tushunchalar va texnologiyalarning o‘zida ham, har tomonlama raqamlashtirish va ko‘pchilik korxonalarning onlayn rejimga o‘tishida ham eksponensial rivojlanish kuzatilmoqda. 2020 yildagi pandemiya bu tendentsiyani faqat tezlashtirdi. Yuqori va o‘ta yuqori darajali dasturlash tillaridan, kuchli freymworklar va ishlab chiqish muhitlaridan keng foydalanish, bulutli infratuzilmalar hamda virtualizatsiya va konteynerlashtirish texnologiyalarining rivojlanishi misli ko‘rilmagan qisqa vaqt ichida yangi ilovani “yig‘ish” imkonini beradi. Kibertahdidlar ham tezlikda ko‘paymoqda, chunki buzg’unchilar ham shunday yuqori samarali ishlab chiqish vositalaridan o‘z maqsadlari uchun foydalanadilar. Bu kiber qarshi choralar darajasini yangi bosqichga olib chiqadi: agar ilgari buzg'unchilar bilan to‘qnashuvni onglarning kurashi va ma'lumotni himoya qilishning moslashtirilgan vositalari deb ta'riflash mumkin bo‘lsa, endi uni sun'iy kiber intellektlar orasida bo‘ladigan "mashinalar jangi" deb atash mumkin. Sun’iy intellekt haqidagi tasavvur va bu sohadagi izlanishlar — «aqlli mashinalar» ishlab chiqarishga ilmiy èndoshish birinchi bo’lib Stanford universitetining (AQSh) professori Djon Makkarti tashabbusi asosida 1956 yili tashkil topgan ilmiy tugarakda paydo bo’ldi. Axborot xavfsizligi va kiberxavfsizlik sohasida sun'iy intellektdan foydalanish 2000 yillarning boshlarida juda oddiy narsalardan, ya’ni ma'lum bir profil mutaxassislari, xususan, virustahlilchilarining ishini osonlashtiradigan tizimlarni qurish bilan boshlandi. Bu vaqtga kelib, zararli fayllar namunalari soni shunchalik ko‘payib ketdiki, qo‘lda yoki oddiy avtomatlashtirilgan tahlil endi etarli emas edi. Bular zararli koddagi naqshlarni (o‘xshashlikni) aniqlagan va hech bo‘lmaganda minimal atributga ruxsat beruvchi tizimlar edi. Ya'ni, ular teskari mutaxassislar va virus tahlilchilariga ma'lum ma'lumotlarni taqdim etdilar, bu esa u yoki bu zararli dasturlarni ma'lum bir guruh yoki sinfga tayinlash imkonini berdi. Aslida, bu klasterlash va katta ma'lumotlar bilan ishlash edi.

Sun’iy intellektni(SI) rivojlantirish hamda davlat organlari va boshqa tashkilotlar faoliyatida, shuningdek ushbu sohada normativ-huquqiy bazani tayyorlashda maslahatchi sifatida qatnashish uchun «Sber» guruhining (Rossiya) yetakchi mutaxassislari va ekspertlari jalb qilindi. Kiberjinoyatlar soni doimiy va tez ortib bormoqda. Shunday qilib, o‘tgan yil davomida Rossiya iqtisodiyotining xakerlar faoliyatidan ko‘rgan yo‘qotishlari taxminan 6 trillion rublni tashkil etdi. Mutaxassislarning fikricha, hujumchilar ko‘pincha axborot xavfsizligi bo‘yicha mutaxassislar va huquq-tartibot xodimlaridan bir emas, bir necha qadam oldinda bo‘ladi.

Axborot xavfsizligi sohasida sun'iy intellektdan foydalanish 2000 yillarning boshlarida juda oddiy narsalardan, ya’ni ma'lum bir profil mutaxassislari, xususan, virus tahlilchilarining ishini osonlashtiradigan tizimlarni qurish bilan boshlandi. Bu

vaqtga kelib, zararli fayllar namunalari soni shunchalik ko‘payib ketdiki, qo‘lda yoki oddiy avtomatlashtirilgan tahlil endi etarli emas edi. Bular zararli koddagi naqshlarni (o‘xshashlikni) aniqlagan va hech bo‘lmaganda minimal atributga ruxsat beruvchi tizimlar edi. Ya'ni, ular teskari mutaxassislar va virus tahlilchilariga ma'lum ma'lumotlarni taqdim etdilar, bu esa u yoki bu zararli dasturlarni ma'lum bir guruh yoki sinfga tayinlash imkonini berdi. Aslida, bu klasterlash va katta ma'lumotlar bilan ishlash edi.

Axborot xavfsizligini ta’minlashda sun’iy intellektdan foydalanish, quyidagi ikki omilga asoslanadi: kiber voqea sodir bo‘lgan taqdirda tezkor choralar ko‘rish zarurati va kibermudofaa bo‘yicha malakali mutaxassislarning etishmasligi. Darhaqiqat, zamonaviy voqelikda xodimlar ro‘yxatini zarur tajribaga ega bo‘lgan malakali axborot xavfsizligi mutaxassislari bilan to‘ldirish juda qiyin va keng ko‘lamli axborot xavfsizligi hodisalari tez rivojlanishi mumkin: daqiqalar ko‘pincha hisoblanadi. Agar kompaniyada axborot xavfsizligi bo‘yicha tahlilchilarning kechayu kunduz navbatchilik smetasi bo‘lmasa, u holda kiber hodisalarga tezkor avtonom javob berish tizimisiz ish vaqtidan tashqarida yuqori sifatli himoyani ta'minlash qiyin bo‘ladi. Bundan tashqari, tahdidni amalga oshiruvchilar o‘z hujumlaridan oldin chalg'itishni amalga oshirishi mumkin - masalan, DDoS hujumini boshlash yoki tarmoqni faol skanerlash. DDoS hujumlari uchun ARP protokol ishlatiladi Bunday vaziyatlarda sun'iy intellektga asoslangan kiber hodisalarga javob berish tizimi yordam beradi, bu bir vaqtning o‘zida ko‘p sonli axborot xavfsizligi hodisalarini qayta ishlash, axborot xavfsizligi bo‘yicha tahlilchilarning muntazam harakatlarini avtomatlashtirish va inson aralashuvisiz hodisalarga tezkor javob berish imkonini beradi.

Bugungi kunga kelib SIning axborot xavfsizligini ta'minlash doirasi ancha keng. Internetda yangi tahdidlarni ko‘rsatishi yoki oldindan bashorat qilishi mumkin bo‘lgan katta hajmdagi ma'lumotlarni tahlil qiladigan global kompaniyalar mavjud. Ushbu kompaniyalarda ma'lumotlar to‘plamlarini to‘playdigan, SI-sinf texnologiyasidan foydalangan holda ularni tahlil qiladigan, klaster ma'lumotlarini aniqlaydigan va tahdidlarni bashorat qiladigan tizimlar mavjud. Ushbu texnologiyalarsiz bunday hajmdagi ma'lumotlarni qayta ishlash deyarli mumkin emas. Bu yerda, albatta, neyron tarmoqlar ham, klasterlash ham juda keng qo‘llaniladi. SI tizimlari tahdidlarni kuzatish uchun ham qo‘llaniladi, ya’ni ochiq va yopiq manbalardan to‘plangan ma'lumotlar asosida axborot xavfsizligi tahdidlarini bashorat qilish uchun foydalaniladi. Shunday qilib, so‘nggi yigirma yil ichida axborot xavfsizligi sohasida sun'iy intellektni qo‘llash vazifalari ko‘lami sezilarli darajada o‘sdi.

Bugungi kunga kelib sun'iy intellekt endi qandaydir sehr emas, balki kiber tahdidlardan himoya qilishda samarali yordamchidir.

Bugungi texnologik jihatdan rivojlangan davrda Kiberxavfsizlikni tahlil qilish va takomillashtirish endi faqatgina insonlar tomonidan amalga oshirilmaydi. Ushbu misli ko‘rilmagan muammoga javoban, sun’iy intellektga (AI) asoslangan kiberxavfsizlik vositalari paydo bo‘ldi, ular axborot xavfsizligi guruhlariga xakerlik xavfini kamaytirishga va xavfsizlik darajasini yuqori darajada oshirishga yordam beradi.

Sun’iy intellekt va mashinalarni o‘rganish (Machine Learning) axborot xavfsizligi sohasidagi eng muhim texnologiyalarga aylandi, chunki ular millionlab hodisalarni tezda tahlil qilish va turli xil tahdidlarni aniqlash qobiliyatiga ega. Zero-day (nol kunlik) zaifliklardan foydalanadigan zararli dasturlardan tortib, fishing hujumiga yoki zararli kodni yuklashga olib kelishi mumkin bo‘lgan xavfli xatti-harakatlarni aniqlashga qodir. Ushbu texnologiyalar o‘tmishdagi tajribalarga asoslanib, endilikda hujumlarning yangi turlarini aniqlash uchun vaqt o‘tishi bilan takomillashib bormoqda.

Afsuski, hozirgi vaqtda sun’iy intellekt juda mashhur, ammo ko‘pincha noto‘g’ri ishlatiladigan zamonaviy so‘zdir. Hozirda ko‘plab kompaniyalar sun’iy intellekt tomoniga o‘tish yo‘llarini qidirmoqdalar. Ammo bugungi kunda sun’iy intellekt bo‘yicha ko‘plab takliflar aslida sun’iy intellekt testi talablariga javob bermaydi. Ular ma’lumotlarni tahlil qiladigan va ma’lum natijalarni aniqlashga imkon beradigan texnologiyalardan foydalanishsa-da, bu AI emas. Sof AI vazifalarni avtomatlashtirish uchun kognitiv qobiliyatlarni ko‘paytirishdan iborat.

Sun’iy intellekt tizimlari iterativ va dinamikdir. Ular ko‘proq ma’lumotlarni tahlil qilish davomida aqlli bo‘lib, tajribadan “o‘rganadilar” va borgan sari qobiliyatli va avtonom bo‘lib boradilar.

Boshqa tomondan, ma’lumotlarni tahlil qilish (DA) – bu ixtisoslashgan tizimlar va dasturiy ta’minot yordamida ulardagi ma’lumotlar to‘g’risida xulosa chiqarish uchun katta ma’lumotlar to‘plamlarini o‘rganadigan statik jarayon hisoblanadi.

Sun’iy intellekt deganda olingan ma’lumotlar asosida tushunishi, o‘rganishi va harakat qilishi mumkin bo‘lgan texnologiyalar tushuniladi. Bugungi kunda sun’iy intellekt uchta usulda ishlaydi:

Assisted intelligence (Yordamchi intellekt) – hozirgi kunda odamlar va kompaniyalar ishini yaxshilashga yordam beradi.

Augmented intelligence (Tarmoqli intellekt) – odamlar va kompaniya qila olmaydigan ishlarni qilishga imkon beradi.

Autonomous intelligence (Avtonom intellekt) – o‘z-o‘zidan ishlaydigan mashinalar misol bo‘la oladi va bunga kelajakda mustaqil ravishda o‘z-o‘zini boshqara oladigan transport vositalarini aytishimiz mumkin.

Aytishimiz mumkinki, sun’iy intellekt ma’lum darajada inson aql-idrokiga ega: ma’lum bir fan sohasiga tegishli bilimlar zaxirasi, yangi bilimlarni egallash mexanizmlari va ushbu bilimlarni qo‘llash mexanizmlari kabi. Mashinani o‘rganish, ekspert tizimlar, neyron tarmoqlar va chuqur o‘rganish sun’iy intellekt texnologiyalariga misol bo‘la oladi:

Mashinani o‘rganish (Machine learning) keng ko‘lamli missiyaga emas, balki ma’lum bir vazifani hal qilishga qaratilgan bo‘lgandagina yaxshi ishlaydi.

Ekspert tizimlari – bu ixtisoslashgan sohalardagi muammolarni hal qilish uchun mo‘ljallangan dasturlar. Bu tizimlar haqiqiy mutaxassislarning fikrlashiga taqlid qilib, diqqat bilan tanlangan bilimlar to‘plamidan foydalangan holda noaniq qoidalarga asoslangan fikrlash orqali muammolarni hal qilishadi va qaror qabul qilishadi.

Neyron tarmoqlar kompyuterga kuzatuv ma’lumotlaridan o‘rganish imkonini beruvchi biologik dasturlash paradigmasidan foydalanadi.

Chuqur o‘rganish (Deep learning) ma’lum bir vazifaga xos algoritmlardan farqli o‘laroq, o‘quv ma’lumotlarini taqdim etishga asoslangan mashinani o‘rganish usullarining bir qismidir. Bugungi kunda chuqur o‘rganish orqali tasvirni aniqlash ko‘pincha avtonom transport vositalari, skanerlash tahlili va tibbiy diagnostika kabi sohalarda keng qo‘llaniladi.

Kiberxavfsizlikda sun’iy intellektni qo‘llash

Sun’iy intellekt kiberxavfsizlik borasidagi eng qiyin muammolarimizni hal qilishga yordam bera oladi. Bugungi kunda doimiy ravishda rivojlanib borayotgan kiberhujumlar va qurilmalarning tarqalishi sharoitida tahdidlarni aniqlashni avtomatlashtirish va ularga an’anaviy dasturiy ta’minotga asoslangan yondashuvlarga qaraganda samaraliroq javob berish orqali “yomon odamlarni kuzatib borish” uchun mashinani o‘rganish va sun’iy intellektdan foydalanish mumkin.

Shu bilan birga, kiberxavfsizlik bir qator noyob muammolar bilan birga keladi:

- Ulkan hujum maydoni
- Har bir tashkilotda 10 yoki 100 minglab qurilma
- Yuzlab hujum vektorlari
- Malakali xavfsizlik mutaxassislarining yetishmasligi

Avtomatik sun’iy intellektga asoslangan kiberxavfsizlik holatini boshqarish tizimi ushbu muammolarning ko‘pini hal qilishga qodir.

Quyida sun’iy intellektning turli darajalari bilan tanishing:

Axborot texnologiyalari aktivlarini inventarizatsiya qilish – axborot tizimlariga har qanday kirish huquqiga ega bo‘lgan barcha qurilmalar, foydalanuvchilar va ilovalarning to‘liq va aniq inventarizatsiyasini olish. Inventarizatsiya qilishda biznesning tanqidiyligini tasniflash va o‘lchash ham katta rol o‘ynaydi.

Tahdidlarni fosh qilish – xakerlar ham o‘zgarishlar va tendentsiyalarni boshqalar kabi kuzatadilar. Sun’iy intellektga asoslangan kiberxavfsizlik tizimlari nafaqat sizning korxonangizga hujum qilinganida, balki sizning korxonangizga hujum sodir bo‘lish ehtimoli mavjud bo‘lgan holatlarda ham sizga dolzarb bilimlarni taqdim etishi mumkin.

Samarali nazorat – ishonchli xavfsizlik tizimini saqlab qolish uchun foydalaniladigan turli xil himoya vositalari va xavfsizlik jarayonlarining ta’sirini tushunish muhimdir. Sun’iy intellekt sizning axborot xavfsizligi jihatdan dasturingizning kuchli tomonlari va unda bo‘shliqlar mavjudligini tushunishga yordam beradi.

Xakerlik xavfini bashorat qilish – axborot texnologiyalarining aktivlari inventarizatsiyasi, tahdidlarga ta’sir qilish va boshqaruv samaradorligini hisobga olgan holda, sun’iy intellektga asoslangan tizimlar zaif tomonlarni bartaraf etish uchun resurslar va vositalarni taqsimlashni rejalashtirishingiz uchun qanday va qayerda xakerlik hujumiga duchor bo‘lishingiz mumkinligini taxmin qilishi mumkin. Sun’iy intellekt tahlilidan olingan tahliliy tavsiyalar tashkilotingizning kiber barqarorligini oshirish uchun nazorat va jarayonlarni sozlash hamda takomillashtirishga yordam beradi.

Hodisalarga javob berish – sun’iy intellektga asoslangan tizimlar xavfsizlikka oid ogohlantirishlarga ustuvor ahamiyat berish va ularga javob berish, hodisalarga tezkor javob berish va zaifliklarni yumshatish va oldini olish uchun yaxshilangan konteksni taqdim etishi mumkin.

Sun’iy intellektning dastlabki tarafdorlari

Google: Gmail 18 yil oldin ishga tushirilgandan beri elektron pochta xabarlarini filtrlash uchun mashinani o‘rganish usullaridan foydalanmoqda. Bugungi kunda mashinani o‘rganish deyarli barcha xizmatlarida, ayniqsa deep learning’da qo‘llaniladi, bu algoritmlarga o‘rganish va evolyutsiya jarayonida yanada mustaqil bo‘lish va o‘zini o‘zi boshqarish imkonini beradi.

“Ilgari biz shunday dunyoda yashar edik, u yerda sizda qancha ko‘p ma’lumot bo‘lsa, shuncha ko‘p muammolarga duch kelar edinggiz. Endi esa deep learning bilan, ma’lumotlar qanchalik ko‘p bo‘lsa, shuncha yaxshi bo‘ladi.” deydi Googlening suiiste’mol qilish bo‘yicha tadqiqot guruhi rahbari Eli Bershteyn.

IBM / Watson: IBM jamoasi “bilimlarni mustahkamlash” vazifalari va mashinani o‘rganishga asoslangan tahdidlarni aniqlash uchun o‘zining Watson kognitiv o‘rganish platformasidan tobora ko‘proq foydalanmoqda.

“Bugungi kunda xavfsizlikni boshqarish markazida amalga oshirilayotgan ishlarning aksariyati odatiy yoki takrorlanadigan ishdir, shuning uchun agar biz uning bir qismini mashinani o‘rganish bilan avtomatlashtira olsak nima bo‘ladi?”– deydi Koos Lodeveyks, IBM Security kompaniyasining xavfsizlik operatsiyalari va ularga javob berish bo‘yicha vitse-prezidenti va texnik direktori.

Juniper Networks: tarmoq hamjamiyati zamonaviy tarmoqlarning barqaror bo‘lmagan iqtisodiyot muammolarini hal qilish uchun ilg’or g’oyalarni xohlaydi. Juniper ushbu muammoning yechimini ishlab chiqarishga tayyor, iqtisodiy jihatdan maqsadga muvofiq o‘zini o‘zi boshqarish tarmog’i Self-Driving Network sifatida ko‘radi.

“Dunyo avtonom tarmoqlarga tayyor. Sun’iy intellekt, mashinani o‘rganish va maqsadga asoslangan tarmoqlardagi yutuqlar bizni avtomatlashtirish avtonomiyaga yo‘l ochadigan ostonaga olib keldi.” Kevin Xatchins, strategiya va mahsulotlarni boshqarish bo‘yicha katta vitse-prezident.

Balbix Breach Control platformasi (hozirda Balbix Security Cloud deb nomlanadi) Real vaqt rejimida xavflarni doimiy ravishda bashorat qilish, xavfga asoslangan zaifliklarni boshqarish va buzilishlarni oldindan nazorat qilish uchun sun’iy intellektga asoslangan kuzatuvlar va tahlillardan foydalanadi. Platforma kiberxavfsizlik guruhlarini ishonchli xavfsizlik tizimini saqlab qolish uchun bajarishi kerak bo‘lgan ko‘plab vazifalarni bajarishda samaraliroq qilishga yordam beradi.

So‘nggi yillarda sun’iy intellekt axborot xavfsizligi bo‘yicha mutaxassislarning sa’y-harakatlarini kuchaytirish uchun zarur texnologiyaga aylandi. Xavfsizlik nuqtai nazaridan, sun’iy intellekt xavflarni aniqlashi va birinchi o‘ringa qo‘yishi, tarmoqdagi har qanday zararli dasturni darhol aniqlashi, hodisalarga javob berishi va bosqinlarni boshlanishidan oldin aniqlashi mumkin.

3-Amaliy mashg’ulot. Internet of Things (IoT) va kiberxavfsizlik (2 soat).

Buyumlar Interneti (Internet of Things, IoT) atamasi dastlab 1999-yilda MIT xodimi Kevin Eshton tomonidan RFID texnologiyasi ilgari surilganida paydo bo‘lgan. Shundan so‘ng IoT har bir fizik obyektni (ya’ni, buyumlarni) Internet tarmog’idagi tugunga aylantirish, fizik dunyo bilan mashinadan-odamga, mashinadan-mashinaga aloqasini osonlashtirishda istiqbolli texnologiya sifatida sezilarli suratga ega bo‘ldi. Fizik va raqamli muhitlarni o‘zaro ulash va

integratsiyalash orqali IoT aqlli shaharlar, aqlli uylar, Sanoat 4.0 va Jamiyat 5.0 kabi qiziqarli ilova hamda xizmatlarni butunlay yangi sinfini taqdim etmoqda.

So‘ngi 20 yillikda, xususan, oxirgi 10 yillikda IoT eng salmoqli ilmiy tadqiqotlar olib boriladigan sohaga aylandi. Microsoft Academic ma'lumotlariga ko‘ra 2000-yilda IoT bo‘yicha atiga 26 ta nashr, 2009-yilda 160 ta nashr bo‘lgan bo‘lsa, so‘ngi yillarda bu raqamlar jadallik bilan o‘sdi. Xususan, 2016-yilda 10 926 ta, 2017-yilda 15 765 ta, 2018-yilda 21 906 va 2019-yilda 26 885 ta IoT sohasiga oid ilmiy maqolalar va nashrlar chop etilgan. Ushbu maqolada IoT sohasida, xususan, xavfsizlik sohasida hozirda olib borilayotgan dolzarb ilmiy tadqiqotlar yo‘nalishlari bilan yaqindan tanishib chiqiladi. Tahlil qilingan ilmiy maqolalar va nashrlardan olingan ma'lumotlarga asoslanib, hozirda IoT sohasida dolzarb sanalgan ilmiy tadqiqot yo‘nalishlarining top 10 taligini quyidagicha keltirish mumkin:

1. Energiyani yig'ish. IoT vositalari kichik quvvat manbalariga egaligi bois, davomli holda ularni almashtirish talab etiladi. Bu esa foydalanishda samaradorlikni tushishiga olib keladi. Shu sababli, IoT tizimlari uchun tabiiy yoki suniy resurslardan foydalanishi mumkin bo‘lgan energiyani elektr energiyaga aylantirish mexanizmini yaratish dolzarb tadqiqot sohasi hisoblanadi.

2. IoT ma'lumotlarini boshqarish. IoT tarmog'i ko‘p sonli tugunlardan iboratligi, tugunlarning turli fizik imkoniyat va xususiyatga egaligi ular tomonidan yetkaziluvchi ma'lumotlarning ham turlichaligiga sabab bo‘ladi. Bu turdagi ma'lumotlarni boshqarish, analiz qilish va ularni ishlash alohida yondashuv talab etadi.

3. IoT-da qidiruv. Millardlab obyektlar ichidan keraklisini topish IoT tizimida mavjud bo‘lgan jiddiy muammolardan biri hisoblanadi. Buning sababi, IoT tizimidagi qidiruv tizimi oddiy Web tizimga nisbatan farq qilishi bilan belgilanadi.

4. IoT-da xavfsizlik, shaxsiylik va kafolat. IoT tizimlarini rivoji bilan parallel ravishda xavfsizlik va shaxsiylik masalasi dolzarblashib bordi. IoT qurilmarining hisoblash, quvvat va tarmoq imkoniyatlarini cheklanganligi bois, ular uchun himoya mexanizmini yaratishda alohida yondashuvni talab etdi. Shu sababli, IoT tizimi uchun mos himoya mexanizmini ishlab chiqish, turli ilovalar uchun shaxsiy ma'lumotni himoyalash va tizimni davomli ishlashini kafolatlashga oid ilmiy tadqiqot sohasi dolzarb hisoblanadi.

5. Xizmatga yo‘naltirilgan hisoblash va IoT. Xizmatga yo‘naltirilgan. hisoblash xizmatga yo‘naltirilgan arxitekturaga asoslangan bo‘lib, interaktiv xizmatlar to‘plamida dasturiy ta'minot ilovalari va infratuzilmalarini tashkil etishga qaratilgan. Xizmatga yo‘naltirilgan hisoblashda texnologiyalar IoT tomonidan yuzaga keltirilgan ko‘plab fundamental muammolarni hal qilishga yordam beradi. Biroq, IoT tizimlarida qurilmalarning resurs va imkoniyatlarini cheklanishi, ulami standart xizmatga yo‘naltirilgan hisoblash standartlari va usullaridan foydalanishga

imkoniyat bermaydi. Shu sababli, IoT muhiti uchun mos bo‘lgan xizmatga yo‘naltirilgan hisoblash usullarini tadqiq etish dolzarb hisoblanadi. 6. Ijtimoiy IoT. So‘nggi paytlarda aqlli obyektlardan ijtimoiy jihatdan xabardor obyektlarga o‘tish orqali IoT paradigmasining navbatdagi evolyutsion bosqichini olib borish uchun juda ko‘p mustaqil tadqiqot faoliyati amalga oshirildi.

Bu yangi xizmatlarni kashf qilish, tajriba almashish va bir-birining imkoniyatlaridan foydalanish maqsadida, lekin, ular bilan cheklanmagan holda, o‘zini namoyon qiladigan va odamlarga taqlid qiluvcha atrofdagi tengdoshlar bilan muloqot qilish qobiliyatiga ega bo‘lgan IoT obyektlarining yangi avlodini yaratishni nazarda tutadi.

Ushbu yangi paradigma obyektlarga o‘z ijtimoiy tarmoqlarini yaratish va boshqa obyektlar va ularning xizmatlarini kashf qilish imkonini beruvchi do‘st obyektlarning ijtimoiy tarmoq tuzilmasi bo‘ylab harakatlanish imkonini beruvchi yangi istiqbol bo‘lgan narsalarning ijtimoiy Interneti (XOMial IoT) deb nomlanadi. SloT ijtimoiy hisoblashdan na'muna olgan holda masshtablash, ishonch va resurslarni aniqlash sohasiga oid IoT muammolarini yengillashtirishga harakat qiladi.

7. IoT tavsiyasi. IoT muhitida ma'lumotlarni keskin ortishi bilan lot qurilmalarini qidirish, ulardan foydalanish va ularga bog‘lanish har qachongidan ham murakkab. Bu esa foydalanuvchidan talabiga mos IoT qurilmasini qidirish mashaqqatini talab etadi. Ushbu paradigmaga ko‘ra esa, loT tizimlarini o‘zi imkoniyati va qayd ma'lumotlari asosida kerakli resursni o‘zi tavsiya etishi va yetkazib berishi mumkin. Shu sababli, ushbu soha hozirda dolzarb tadqiqot yo‘nalishlaridan biriga aylanmoqda.

8. Chetki hisoblash (Edge computing) va IoT. Chetki hisoblash taqsimlangan hisoblash topologiyalarining bir qismi bo‘lib, u hisoblash va saqlashni qurilmalarga yaqinlashtirishga asoslanadi. Bu qat'iy kechikmaslik talablari qo‘yilgan ilovalar uchun juda foydali. Bunga ko‘ra ma'lumotlarni ishlashning aksariyat hajmi chetki vositalarda amalga oshirilib, faqat talab etilgan kichik hajmdagi ma'lumot markaziy bulutga yetkazilishi sababli o‘tkazish qobiliyatiga bo‘lgan talabni kamaytiradi, iqtisodiy va resurs tomonidan tejamkor hisoblanadi. Bu esa, o‘z navbatida chetki hisoblashga asoslangan IoT ilovalarini ishlab chiqish sohasi dolzarb ilmiy tadqiqot yo‘nalishi ekanligini ko‘rsatadi.

9. Suhbatdosh IoT. Odamlar o‘rtasida ta'sir qilish odatda so‘zlar orqali amalga oshiriladi. So‘ngi yillarda olib borilayotgan ilmiy izlanishlar texnologiyalari ham inson tabiy tilidan foydalangan holda boshqarish mumkinligini ko‘rsatmoqda. Bularni dastlabki amaliy natijalari aqlli uy ilovalarida qo‘llanilmoqda. Biroq, mazkur sohada inson-mashina muloqotini ta'minlashda qator kamchiliklar, suhbat konteksidagi kamchiliklar, suhbat dialogida mulohaza yurita olmaslik, murakkab

gap birikmalarini tahlil qila olmaslik, mavjudki, ularni bartaraf etish uchun koʻp soni ilmiy tadqiqotlarni olib borish talab etiladi.

10. IoT tizimida ma'lumotlarni xulosalash (Summarization in IoT). IoT rivoji bilan sensorlardan olingan ma'lumotlar miqdorining ortishi va Internet foydalanuvchilarining oʻsishi Internet orqali ma'lumotlarni siqish zaruriyatini keltirib chiqaradi. Tabiiy tilda ma'lumotlarni ishlash nuqtai nazaridan, umumlashtirish ma'lumotlarni siqishning samarali usuli boʻlib, u bir yoki bitta matn toʻplamidan qisqa va ixcham xulosa chiqarishga imkon beradi. Xuddi shunday, IoT tizimlari uchun koʻp sonli ma'lumotlarni siqish usulini ishlab chiqish dolzarb masalalardan biri.

Xususan, IoT tizimida axborot xavfsizligi masalasi dolzarb boʻlib, unda quyidagi ilmiy tadqiqot yoʻnalishlari boʻyicha hozirda keng qamrovli ilmiy izlanishlar olib bonlmoqda

IoT muammolarini yechishda blokcheyn texnologiyasidan foydalanish ;

Sin'iy intellektga asoslangan xavfsizlik va ma'lumotlar xavfsizligi;

IoT-da shaxsiylik, ma'lumotlarni himoya qilish va xavfsizlik masalalari; IoT-da shaxsiylik va xavfsizlik testlari, sertifikatlash va yorliqlash";

Xavfsizlik va ma'lumotlarni himoyalashda riskni baholash va qarshi kurashish;

Identifikatsiya va autentifikatsiya muammolari;

IoT xavfsizligi uchun simsiz sensor tarmoqlar (WSN); IoT da suqilib kirishlarni aniqlash;

IoT uchun knptografiya, kalitlar boshqarish, autentifikatsiya va avtorizatsiya,

IoT-da fizik, MAS va tarmoq hujumlaridan himoyalash; - IoT-da sathlararo hujumlarni oldini olish;

- IoT-da QoS-ni optimallashtirish bilan xavfsizlik,

- IoT-da shaxsiylikka asoslangan holda kanaldan foydalanish, IoT kriminalistikasi,

- IoT-da katta ma'lumotlar va ma'lumot yaxlitligi; -IoT-da aloqa xavfsizligi;

IoT-da xavfsizlik standartlari.

Buyumlar Interneti (IoT) yigirma yildan koʻproq vaqt davomida tadqiqot va ishlanmalarning juda faol sohasi boʻlib kelmoqda. Garchi standartlashtirish, tijorat ishlanmalari va tadqiqotlami oʻz ichiga olgan juda koʻp ilmiy izlanishlar olib borilgan boʻlsada, IoT qurilmalarining keng koʻlamli va xilma-xilligi, IoT muhitining ochiqligi hamda shaxsiylik va maxfiylik kamchiliklari tufayli hali ham koʻplab muammolar ochiqligicha qolmoqda. Ushbu maqolada IoT boʻyicha 10 ta asosiy tadqiqot mavzulari, xavfsizlik sohasida esa qator ilmiy izlanish yo 'nalishlari aniqlandi va ushbu sohada keyingi ilmiy tadqiqotlarni olib borishga harakat qilinadi muhitining ochiqligi hamda shaxsiylik va maxfiylik kamchiliklari tufayli hali ham

ko‘plab muammolar ochiqligicha qolmoqda. Ushbu maqolada IoT bo‘yicha 10 ta asosiy tadqiqot mavzulari, xavfsizlik sohasida esa qator ilmiy izlanish yo 'nalishlari aniqlandi va ushbu sohada keyingi ilmiy tadqiqotlarni olib borishga harakat qilinadi.

4-Amaliy mashg’ulot. Tahdidlarni oldini olish va kiberxavfsizlik sohasidagi yangi yondoshuvlar (2 soat).

Har qanday taraqqiy etgan jamiyat hayotida axborotning ahamiyati uzluksiz ortib bormoqda. Uzoq o‘tmishdan davlatning harbiy-strategik ahamiyatiga molik bo‘lgan ma’lumotlar qat’iy sir tutilgan va himoyalangan. Hozirgi vaqtda ishlab chiqarish texnologiyalariga va mahsulotlarni sotishga tegishli axborot tovar ko‘rinishiga ega bo‘lib, ichki va tashqi bozorda unga bo‘lgan talab ortib bormoqda. Axborot texnologiyalari avtomatlashtirish va axborotni muhofaza qilish yo‘nalishlarida muntazam mukammallashib bormoqda. Zamonaviy axborot texnologiyalarining taraqqiyoti sanoat shpionaji, kompyuter jinoyatchiligi, konfedensial ma’lumotlarga ruxsatsiz kirish, o‘zgartirish, yo‘qotish kabi salbiy hodisalar bilan birgalikda kuzatilmoqda. Shuning uchun axborotni muhofaza qilish har qanday mamlakatda muhim davlat vazifasi hisoblanadi. O‘zbekistonda axborotni muhofaza qilishning zaruriyati axborotni muhofaza qilishning davlat tizimi yaratilishida va axborot xavfsizligining huquqiy bazasini rivojlantirishda o‘z ifodasini topmoqda. «Axborotlashtirish to‘g‘risida», «Davlat sirlarini saqlash to‘g‘risida», «Elektron hisoblash mashinalari dasturlari va ma’lumotlar bazalarini huquqiy himoya qilish to‘g‘risida» va boshqa qonunlar hamda bir qator Hukumat qarorlari qabul qilindi va amalga tatbiq etildi. Axborotni muhofaza qilish axborotni ixtiyoriy ko‘rinishda yo‘qotishda (o‘g‘irlash, buzish, qalbakilashtirish) ko‘riladigan zararning oldini olishni ta’minlashi lozim. Axborotni muhofaza qilish choralari axborot xavfsizligiga oid amaldagi qonun va me’yoriy hujjatlar asosida va axborotdan foydalanuvchilarning manfaatlariga ko‘ra tashkil etilishi zarur. Yuqori darajada axborotni muhofaza qilishni kafolatlash uchun muntazam ravishda murakkab ilmiy-texnik vazifalarni hal etish va himoya vositalarini takomillashtirish talab etiladi.

Axborotni muhofaza qilishning maqsadi va konseptual asoslari. Umuman olganda axborotni muhofaza qilishning maqsadini quyidagicha ifodalash mumkin:

– axborotni tarqab ketishi, o‘g‘irlanishi, buzilishi, qalbakilashtirilishini oldini olish;

– shaxs, jamiyat, davlatning xavfsizligiga tahdidni oldini olish;

– axborotni yo‘q qilish, modifikatsiyalash, buzish, nusxa olish, blokirovka qilish kabi noqonuniy harakatlarning oldini olish;

– axborot resurslari va axborot tizimlariga noqonuniy ta’sir qilishning boshqa shakllarini oldini olish, hujjatlashtirilgan axborotga shaxsiy mulk obyekti sifatida huquqiy rejimni ta’minlash;

– axborot tizimida mavjud bo‘lgan shaxsiy ma’lumotlarning maxfiyligini va konfedensialligini saqlash orqali fuqarolarning konstitutsiyaviy huquqlarini himoyalash;

– davlat sirlarini saqlash, qonunchilikka asosan hujjatlashtirilgan axborotlar konfedensialligini ta’minlash;

– axborot jarayonlarida hamda axborot tizimlari, texnologiyalari va ularni ta’minlash vositalarini loyihalash, ishlab chiqish va qo‘llashda subyektlarning huquqlarini ta’minlash.

Nusxa yaratish Axborot tashuvchilarda ma’lumotlar nusxasini yaratish jarayonidir.

Axborotni muhofaza qilishning samaradorligi uning o‘z vaqtidaligi, faolligi, uzluksizligi va kompleksligi bilan belgilanadi. Himoya tadbirlarini kompleks tarzda o‘tkazish axborotni tarqab ketishi mumkin bo‘lgan xavfli kanallarni yo‘q qilishni ta’minlaydi. Ma’lumki, birgina ochiq qolgan axborotni tarqab ketish kanali butun himoya tizimining samaradorligini keskin kamaytirib yuboradi. Axborotni muhofaza qilish sohasidagi ishlar holatining tahlili shuni ko‘rsatadiki, muhofaza qilishning to‘liq shakllangan konsepsiyasi va tuzilishi hosil qilingan, uning asosini quyidagilar tashkil etadi:

– sanoat asosida ishlab chiqilgan, axborotni muhofaza qilishning o‘ta takomillashgan texnik vositalari;

– axborotni muhofaza qilish masalalarini hal etishga ixtisoslashtirilgan tashkilotlarning mavjudligi;

– ushbu muammoga oid yetarlicha aniq ifodalangan qarashlar tizimi;

– yetarlicha amaliy tajriba va boshqalar.

Biroq, xorijiy matbuot xabarlariga ko‘ra ma’lumotlarga nisbatan jinoiy harakatlar kamayib borayotgani yo‘q, aksincha barqaror o‘sish tendensiyasiga ega bo‘lib bormoqda.

Himoyalangan axborotga tahdidlar tushunchasi va uning tuzilishi. Umumiy yo‘nalishga ko‘ra axborot xavfsizligiga tahdidlar quyidagilarga bo‘linadi: – O‘zbekistonning ma’naviy ravnaqi sohalarida, ma’naviy hayot va axborot faoliyatida fuqarolarning konstitutsiyaviy huquqlari va erkinliklariga tahdidlar; – mamlakatning axborotlashtirish, telekommunikatsiya va aloqa vositalari industriyasini rivojlanishiga, ichki bozor talablarini qondirishga, uning mahsulotlarini jahon bozoriga chiqishiga, shuningdek mahalliy axborot resurslarini yig‘ish, saqlash va samarali foydalanishni ta’minlashga nisbatan tahdidlar; – Respublika hududida joriy etilgan hamda yaratilayotgan axborot va

telekommunikatsiya tizimlarining me’yorida ishlashiga, axborot resurslari xavfsizligiga tahdidlar.

Axborot hisoblash tizimlarida axborot xavfsizligini ta’minlash nuqtai nazaridan o‘zaro bog‘liq bo‘lgan uchta tashkil etuvchini ko‘rib chiqish maqsadga muvofiq:

1) axborot;

2) texnik va dasturiy vositalar;

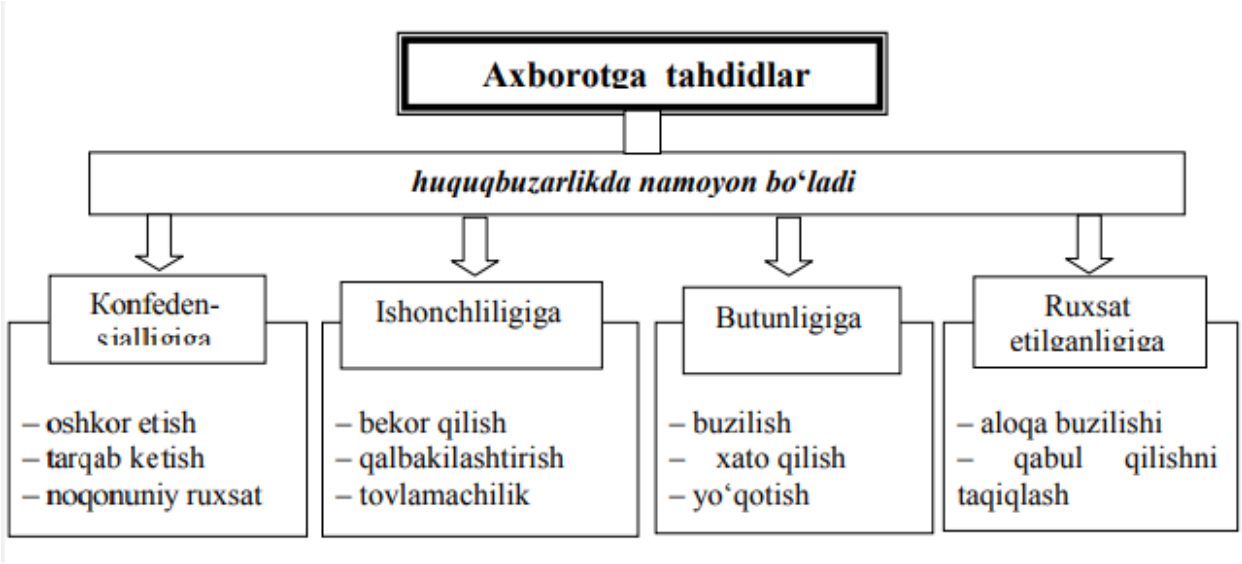
3) xizmat ko‘rsatuvchi personal va foydalanuvchilar.

Har qanday axborot hisoblash tizimlarini tashkil etishdan maqsad foydalanuvchilarning talablarini bir vaqtda ishonchli axborot bilan ta’minlash hamda ularning konfedensialligini saqlash hisoblanadi. Bunda axborot bilan ta’minlash vazifasi tashqi va ichki ruxsat etilmagan ta’sirlardan himoyalash asosida hal etilishi zarur. Axborot tarqab ketishiga konfedensial ma’lumotning ushbu axborot ishonib topshirilgan tashkilotdan yoki shaxslar doirasidan nazoratsiz yoki noqonuniy tarzda tashqariga chiqib ketishi sifatida qaraladi. Tahdidning uchta ko‘rinishi mavjud.

1. Konfedensiallikning buzilishiga tahdid shuni anglatadiki, bunda axborot unga ruxsati bo‘lmaganlarga ma’lum bo‘ladi. Bu holat konfedensial axborot saqlanuvchi tizimga yoki bir tizimdan ikkinchisiga uzatilayotganda noqonuniy foydalana olishlikni qo‘lga kiritish orqali yuzaga keladi.

2. Butunlikni buzishga tahdid hisoblash tizimida yoki bir tizimdan ikkinchisiga uzatilayotganda axborotni har qanday qasddan o‘zgartirishni o‘zida mujassamlaydi. Jinoyatchilar axborotni qasddan o‘zgartirganda, bu axborot butunligi buzilganligini bildiradi. Shuningdek, dastur va apparat vositalarning tasodifiy xatosi tufayli axborotga noqonuniy o‘zgarishlar kiritilganda ham axborot butunligi buzilgan hisoblanadi. Axborot butunligi – axborotning buzilmagan holatda mavjudligidir.

3. Xizmatlarning izdan chiqish tahdidi hisoblash tizimi resurslarida boshqa foydalanuvchilar yoki jinoyatchilar tomonidan ataylab qilingan harakatlar natijasida foydalana olishlilikni blokirovka bo‘lib qolishi natijasida yuzaga keladi. Axborotdan foydalana olishlilik – axborot aylanuvchi, subyektlarga ularni qiziqtiruvchi axborotlarga o‘z vaqtida qarshiliklarsiz kirishini ta’minlab beruvchi hamda ixtiyoriy vaqtda murojaat etilganda subyektlarning so‘rovlariga javob beruvchi avtomatlashtirilgan xizmatlarga tayyor bo‘lgan tizimning xususiyatidir.



4.1-rasm. Axborotga tahdidlar

Axborot xavfsizligiga tahdidlarning toifalanishi. Axborot xavfsizligiga tahdidlar darajasiga kora quyidagicha toifalanishi mumkin:

a) shaxs uchun:

– axborotlarni qidirish, olish, uzatish, ishlab chiqish va tarqatish bo‘yicha fuqarolarning konstitutsiyaviy huquqlari va erkinliklarini buzilishi;

– fuqarolarni shaxsiy hayot daxlsizligi huquqidan mahrum qilish;

– g‘ayriixtiyoriy zararli axborotlardan fuqarolarning o‘z sog‘liqlarini himoya qilish huquqlari buzilishi;

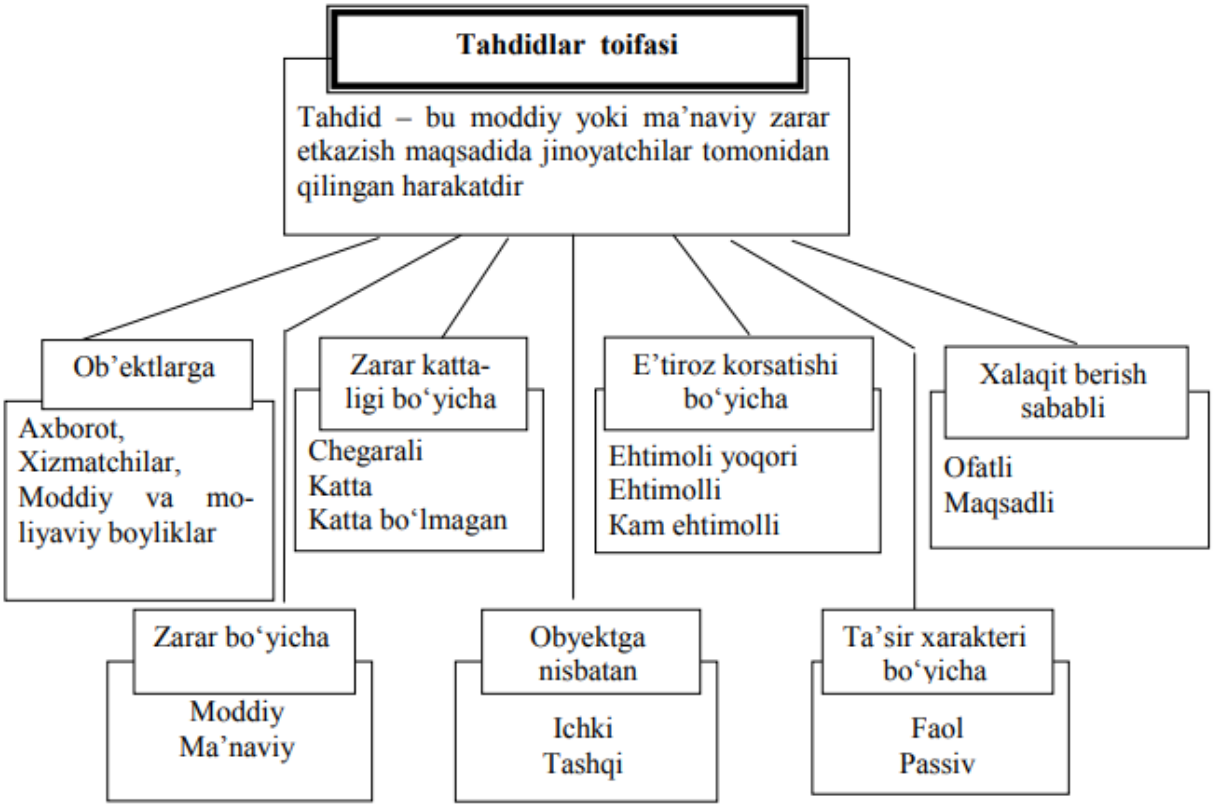
– intellektul mulk obyektlariga tahdid.

b) jamiyat uchun:

– axborotlashtirilgan jamiyatni qurishga to‘siqlar;

– jamiyatning ma’naviy yangilanish, uning ma’naviy boyliklarini saqlash, fidoyilik va xolislik, mamlakatning ko‘p asrlik ma’naviy an’analarini rivojlantirish, milliy, madaniy merosni targ‘ib qilish, axloq me’yorlari huquqlaridan mahrum qilish;

– zamonaviy telekommunikatsiya texnologiyalarini taraqqiy etishi, mamlakat ilmiy va ishlab chiqarish potensialini rivojlantirish va saqlab qolishga qarshilik qiluvchi muhitni yaratish.



4.2-rasm.Tahdidlar toifasi.

v) davlat uchun:

– shaxs va jamiyat manfaatlari himoyasiga qarshi harakatlar;

– huquqiy davlat qurishga qarshilik;

– davlat boshqaruv organlari ustidan jamoat nazorati institutlarini shakllantirishga qarshi harakatlar;

– shaxs, jamiyat va davlat manfaatlarini ta'minlovchi davlat boshqaruv organlari tomonidan qarorlarni tayyorlash, qabul qilish va tatbiq etish tizimini shakllantirishga qarshilik;

– davlat axborot tizimlari va davlat axborot resurslari himoyasiga to'siqlar;

– mamlakat yagona axborot muhiti himoyasiga qarshi harakatlar. Axborot himoyasiga metodologik yondashuv

– bu konfedensial axborotlarni saqlash vazifasini turli bosqichlarda yechish bo'yicha asos bo'luvchi g'oyalar, muhim tavsiyalardir. Ular axborotni me'yoriy himoya qilish bazalarini yaratishda inobatga olinadi. Shuningdek, qonun va qonunosti aktlarini qabul qilishda me'yor sifatida tatbiq qilinadi hamda ularni bajarish majburiy xarakterga ega bo'ladi. Axborotni muhofaza qilish tamoyillarini uchta guruhga bo'lish mumkin: huquqiy, tashkiliy hamda texnik razvedkadan himoyalanishda va hisoblash texnikasi vositalarida axborotga ishlov berishda axborotni muhofaza qilishdan foydalanish.

Axborotni muhofaza qilish tizimlaridan foydalanish amaliyoti shuni ko‘rsatmoqdaki, faqatgina kompleks axborotni muhofaza qilish tizimlari samarali bo‘lishi mumkin. Unga quyidagi chora-tadbirlar kiradi:

1. Qonunchilik. Axborot himoyasi sohasida yuridik va jismoniy shaxslarning, shuningdek davlatning huquq va majburiyatlarini qat’iy belgilovchi qonuniy aktlardan foydalanish.

2. Ma’naviy-etik. Obyektda qat’iy belgilangan o‘zini tutish qoidalarining buzilishi ko‘pchilik xodimlar tomonidan keskin salbiy baholanishi joriy etilgan muhitni hosil qilish va qo‘llab quvvatlash.

3. Fizik. Himoyalangan axborotga begona shaxslarning kirishini taqiqlovchi fizik to‘siqlar yaratish.

4. Ma’muriy. Tegishli maxfiylik rejimi, kirish va ichki rejimlarni tashkil etish.

5. Texnik. Axborotni muhofaza qilish uchun elektron va boshqa uskunalardan foydalanish.

6. Kriptografik. Ishlov berilayotgan va uzatilayotgan axborotlarga noqonuniy kirishni oldini oluvchi shifrlash va kodlashni tatbiq etish.

7. Dasturiy. Foydalana olishlilikni chegaralash uchun dastur vositalarini qo‘llash. Fizik, apparatli, dasturli va hujjatli vositalarni o‘z ichiga oluvchi barcha axborot tashuvchilarga kompleks holda himoya obyekti sifatida qaraladi. Odatda, so‘nggi vaqtlarda axborotdan foydalanish, saqlash, uzatish va qayta ishlashda turli ko‘rinishdagi axborot tizimlarida amalga oshirilmoqda. Axborot tizimi – bu odatda matnli yoki grafik axborotlarni yig‘ish, saqlash, qidirish va qayta ishlashga mo‘ljallangan amaliy dasturiy, ba’zan esa apparat-dasturiy nimtizimdir. Ma’lumotlarning axborot tizimida mavjud bo‘lishining moddiy asosi bu elektron va elektron-mexanik qurilmalar, shuningdek axborot tashuvchilardir. Axborot tashuvchilari sifatida qog‘oz, magnit va optik tashuvchilar, elektron sxemalar foydalanilishi mumkin. Demak, qurilma va nimtizimlarni hamda axborot tashuvchilarini himoya qilish zarur.

Kodlashtirish - axborotni bir tizimdan boshqa tizimga ma’lum bir belgilar yordamida belgilangan tartib bo‘yicha o‘tkazish jarayonidir.

Kalit - matnni shifrlash va shifrini ochish uchun kerakli axborot.

Kriptoanaliz kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi. Kriptografiyadan simmetrik va assimmetrik kriptotizimlar qo’llaniladi, Simmetrik shifr ma’lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalaniladi. Assimmetrik shifr shifrlash va deshifrlash uchun ikkita kalitdan foydalaniladi. Bundan tashqari ma’lumotni yashirtilganligini yashirish ya’ni steganografiya ham mavjud. Steganografiyaning asosiy g‘oyasi maxfiy ma’lumotlarning mavjudligi haqidagi shubhani oldini olishdir.

Turli axborot tizimlarida foydalanuvchilar xizmat ko‘rsatuvchi personal hisoblanib, axborot manbai va tashuvchilari bo‘lishi mumkin. Shuning uchun himoya obyekti tushunchasi keng ma’noda talqin 17 etiladi. Himoya obyekti deganda nafaqat axborot resurslari, apparat va dasturiy vositalar, xizmat ko‘rsatuvchi personal va foydalanuvchilar, balki bino hamda u joylashgan hudud ham tushuniladi. Axborotni muhofaza qilishning asosiy obyektlariga quyidagilar kiradi:

– davlat sirlari bilan bog‘liq va konfedensial ma’lumotlarni o‘zida saqlovchi axborot resurslari;

– vositalar va axborot tizimlari (hisoblash texnikasi vositalari, tarmoqlar va tizimlar), dasturiy vositalar (operatsion tizimlar, ma’lumotlar bazalarini boshqarish tizimlari, amaliy dasturiy ta’minot), avtomatlashtirilgan boshqaruv tizimlari, aloqa va ma’lumotlarni uzatish tizimlari, ruxsati chegaralangan axborotni qabul qilish, uzatish va qayta ishlash texnik vositalari (ovoz yozish, ovoz kuchaytirish, ovoz eshitish, so‘zlashuv va televizion qurilmalar, hujjatlarni tayyorlash, ko‘paytirish vositalari hamda boshqa grafik, matn va harfli-raqamli ma’lumotlarni qayta ishlash vositalari), konfedensial va davlat sirlari toifasiga oid bevosita qayta ishlovchi tizim va vositalar.

Bunday tizim va vositalarni ko‘pincha axborotlarni qabul qilish, qayta ishlash va saqlash texnik vositalari (AQITV) deb atashadi. AQITV tarkibiga kirmaydigan, biroq konfedensial ma’lumotlar qayta ishlanuvchi hududga joylashgan texnik vosita va tizimlar ham mavjud. Bunday texnik vosita va tizimlar yordamchi texnik vosita va tizimlar (YOTVT) deb ataladi. Ularga quyidagilar kiradi: telefon, aloqa ovoz kuchaytirgich texnik vositalari, yong‘in va qo‘riqlash signalizatsiyasi tizimlari, radioaloqa tizimida ma’lumotlarni uzatish vositalari, nazorato‘lchov qurilmalari, xo‘jalik elektr asboblari va boshqalar, shuningdek ular joylashgan bino. AQITVga statsionar jihozlar, periferiya qurilmalari, ulash liniyalari, taqsimlovchi va kommunikatsion qurilmalar, elektr manba tizimlarini o‘ziga biriktirgan tizim sifatida qarash mumkin. Konfedensial ma’lumotlarni qayta ishlashga mo‘ljallangan texnik vositalar, shuningdek ular joylashgan bino ham AQITV obyektini ifodalaydi. Axborot xavfsizligini ta’minlashga yo‘naltirilgan himoya harakatlari qator kattaliklar bilan tavsiflanishi mumkin: tahdid xarakteri, harakat usullari, uning tarqalganligi, o‘rab olish masshtabi kabilar. Tahdid xarakteriga ko‘ra himoya harakatlari ma’lumotlarni oshkor bo‘lishi, chiqib ketishi va noqonuniy kirishdan himoya qilishga yo‘naltiriladi. Harakat usullariga ko‘ra ularni kamomad yoki boshqa zararlarni: ogohlantirish, aniqlash, oldini olish va tiklash kabilarga taqsimlash mumkin. O‘rab olish bo‘yicha himoya harakatlari hududga, 18 binoga, inshoatga, qurilmalarga yoki ularning alohida elementlariga yo‘naltirilgan bo‘lishi mumkin. Himoya tadbirlarining masshtabi esa obyekt, guruh yoki individual himoya

bo‘yicha tavsiflanadi. Axborot himoyasi turlari ikki asosiy belgiga ko‘ra tasniflanadi: birinchidan, axborot xususiyligi, aniqrog‘i qo‘riqlanadigan sirlar turiga ko‘ra; ikkinchidan, axborot himoyasi uchun qo‘llaniluvchi kuchlar, vositalar va usullar guruhlari bo‘yicha. Birinchi guruhga quyidagi asosiy yo‘nalishlar kiritilishi mumkin: davlat sirlarini himoya qilish, davlatlararo maxfiy ma’lumotlarni himoya qilish, tadbirkorlik sirlarini himoya qilish, xizmat sirlarini himoya qilish, mutaxassislik sirlarini himoya qilish va xususiy ma’lumotlarni himoya qilish. Ikkinchi guruhga quyidagi asosiy yo‘nalishlar kiradi: axborotlarni huquqiy himoyalash, axborotlarni tashkiliy himoyalash, axborotlarni muhandislik-texnik himoyalash.

Huquqiy himoyalash – bu huquqiy asosda axborot himoyasini ta’minlovchi maxsus qonunlar, boshqa me’yoriy hujjatlar, qoidalar, jarayonlar va tadbirlar.

Tashkiliy himoya – bu bajaruvchilarga yetkazilishi mumkin bo‘lgan ixtiyoriy zararni bartaraf etuvchi yoki yengillashtiruvchi, bajaruvchilarning me’yoriy-huquqiy asosdagi o‘zaro muomalasi va ishlab chiqarish faoliyatini qat’iy belgilash.

Muhandislik-texnik himoya – bu faoliyatga yetkaziluvchi zararlarga qarshilik qiluvchi turli texnik vositalardan foydalanishdir. Axborot himoyasi vositalarini va usullarini tasniflash. Axborotni muhofaza qilishda foydalaniluvchi asosiy usullar quyidagilar hisoblanadi: yashirish, ranjirlash, noto‘g‘ri ma’lumot berish, bo‘laklash, sug‘urta qilish, hisobga olish, kodlash va shifrlash. Yashirish – axborotni muhofaza qilish usuli sifatida amaliyotda ma’lumotlarni himoyalashning asosiy tashkiliy usullaridan biri hisoblanadi, maxfiy ma’lumotlarga ruxsat etilgan shaxslar sonini chegaralaydi. Yashirish axborotlarni himoya qilishda juda keng qo‘llaniluvchi usullardan biri hisoblanadi. Ranjirlash axborot himoya usuli sifatida, birinchidan, maxfiy ma’lumotlarni maxfiylik darajasi bo‘yicha taqsimlaydi, va ikkinchidan himoyalangan axborotga ruxsatni chegaralaydi. Noto‘g‘ri ma’lumot berish – axborot himoya usullaridan biri bo‘lib, biror obyekt haqidagi haqiqiy ma’lumot o‘rniga atayin yolg‘on ma’lumot tarqatishni anglatadi. Axborotni bo‘laklash usuli axborotni bo‘laklarga bo‘lib, uning biror qismi orqali to‘liq ma’lumot olib bo‘lmaslikni anglatadi. Bu usul harbiy texnika va qurollanish vositalarini ishlab chiqarishda, shuningdek yangi mahsulotlarni ishlab chiqarishda keng qo‘llaniladi.

Sug‘urta qilish – axborotni muhofaza qilish usuli sifatida endigina tan olinmoqda. Uning ma’nosi axborot egasi huquqlari va manfaatlarini yoki axborot vositalarini an’anaviy tahdidlar va axborot xavfsizligi tahdidlaridan himoya qilishni bildiradi. Ushbu usul tijorat sirlarini saqlashda ko‘proq qo‘llanilishi ehtimoli mavjud. Axborotni sug‘urta qilishda u dastlab, auditorlik tekshiruvidan o‘tishi va xulosaga ega bo‘lishi talab etiladi. Axborotlarni ma’naviy-ma’rifiy himoyalash usuli axborotni muhofaza qilishda juda muhim rol o‘ynaydi. Aynan inson, u korxona yoki tashkilot xodimi, maxfiy ma’lumotlardan voqif bo‘lib, o‘z xotirasida ko‘plab

ma’lumotlarni jamlaydi va ba’zi hollarda axborot chiqib ketishi manbaiga aylanishi mumkin hamda uning aybi bilan o‘zgalar ushbu axborotga noqonuniy ega bo‘ladilar. Axborotlarni ma’naviy-ma’rifiy himoyalash usuli quyidagilarni nazarda tutadi:

– xodimni tarbiyalash, u bilan ma’lum sifatlarni, qarashlarni shakllantirishga yo‘naltirilgan maxsus ishlarni olib borish (vatanparvarlik, axborotni muhofaza qilish uning shaxsan o‘zi uchun ham qanday ahamiyat kasb etishini tushuntirish);

– xodimni axborotni muhofaza qilish qoidalari va usullariga o‘rgatish, konfedensial axborot tashuvchilar bilan amaliy ishlash ko‘nikmalarini shakllantirish. Hisobga olish axborotni muhofaza qilishning muhim usullaridan biri bo‘lib, konfedensial ma’lumotlar tashuvchilarning hamda undan foydalanuvchilarning ixtiyoriy vaqtda qayerda joylashganligi haqida ma’lumot olish imkonini beradi. Ushbu usulsiz himoya muammosini hal etish juda qiyin. Sir saqlanuvchi axborotlarni hisobga olish tamoyillari:

– himoyalanuvchi axborotlarni tashuvchilarning barchasini ro‘yxatga olish majburiyligi;

– muayyan axborot tashuvchini ro‘yxatga olish bir marta bo‘lishligini (takrorlanmasligini) ta’minlash;

– ro‘yxatda konfedensial ma’lumot tashuvchining ayni vaqtda qaysi manzildaligini ko‘rsatish;

– har bir himoyalangan axborot tashuvchining saqlanishiga yagona javobgarlik va hisobda ushbu axborotni ishlatgan foydalanuvchi haqida ma’lumotni aks ettirish.

Kodlash – himoyalanuvchi axborotni raqibdan yashirish maqsadida, axborotni kanal orqali uzatish jarayonida o‘zgalar tomonidan tutib olinishi xavfi mavjud bo‘lganda, uni kodlash usuli yordamida ochiq matnni shartli axborotga aylantirish usulidir. Kodlash uchun odatda belgilar to‘plami (belgilar, raqamlar va boshqalar), shuningdek axborotni tushunarsiz belgilar to‘plami ko‘rinishiga aylantirish imkonini beruvchi ma’lum qoidalar tizimi foydalaniladi. Bu axborotni o‘qish uchun esa uni yana o‘z xoliga keltirish, ya’ni kodni ochish (kalit) kerak bo‘ladi. Axborotni kodlash texnik vositalar yordamida yoki qo‘lda amalga oshirilishi mumkin.

Shifrlash – axborotni muhofaza qilish usuli bo‘lib, ko‘pincha axborotlarni radioqurilmalar vositasida uzatishda, raqib tomonidan tutib olish xavfi bo‘lganda qo‘llaniladi. Axborotni shifrlash, uni o‘zgalar tomonidan tutib olinganda ham kalitsiz ma’nosini tushunib bo‘lmaydigan holatga o‘tkazishni anglatadi.

Axborotni muhofaza qilish vositalari – bu axborotni muhofaza qilish masalalarini hal etish uchun foydalaniluvchi muhandislik-texnik, elektr, elektron, optik va boshqa qurilma vositalar to‘plamidir. Axborotni muhofaza qilishning kadr va resurs ta’minoti. Davlat sirlarini tashkil etuvchi axborotni muhofaza qilishni tashkil etuvchi kadrlar tayyorlash tizimiga quyidagilar kiradi:

1. Tashkilot va bo‘linma rahbarlari.

2. Axborotni muhofaza qilish bo‘yicha maxsus komissiyalar.

3. Yagona xavfsizlik xizmati tarkibiga kiruvchi ixtisoslashgan bo‘linmalar. Boshqa sohalar kabi axborotni muhofaza qilish sohasi ham kadrlar tayyorlashdan tashqari moddiy, iqtisodiy va axborot resurslari bilan ta’minlanishi kerak. Moddiy resurslar axborotni muhofaza qilishda maxsus ahamiyatga ega. Unga maxsus ajratilgan bino, maxsus qurilmalar, qabul qilingan me’yorlar asosida attestatsiya qilingan kompyuter va orgtexnika, apparat vositalari, dastur vositalari, axborotni muhofaza qilish vositalari va boshqalar.

Axborot resurslari – bu tashkilot miqyosida axborotni muhofaza qilish bo‘yicha optimal boshqaruv yechimlari qabul qilinadigan axborot. Unga quyidagilar kiradi:

– huquqiy axborot (xavfsizlik muammolari bo‘yicha me’yoriy baza);

– tijorat axborotlari (ishlab chiqariladigan mahsulot va unda axborotni muhofaza qilish bo‘yicha ko‘rsatiladigan xizmatlar haqida axborot);

– ilmiy-texnik axborot (xavfsizlik bo‘yicha mamlakat va chet el davlatlari siyosati haqida axborot);

– ishlab chiqarish texnologiyasi jarayonlari bo‘yicha axborot;

– tashkilotning axborot xavfsizligi holati, unga tahdidlar bo‘yicha axborot-tahliliy faoliyat natijasida olingan tahliliy axborot. Moddiy resurslar. Axborotni muhofaza qilishni loyihalashtirishni, uni ishga tushirishni moddiy ta’minotsiz amalga oshirib bo‘lmaydi. Bu ish murakkab sharoitlarda amalga oshiriladi: xavfsizlik sohasida raqobatchilik, xizmat ko‘rsatuvchining kam xarajat qilib ko‘p foyda olish istagi, xavfsizlik bo‘yicha sifatsiz ishlarni amalga oshirishi va hokazo. Axborot xavfsizligi uning egalari tomonidan himoyalanuvchi axborotning tarqab ketish, buzilish, yo‘q qilish va modifikatsiya qilishni oldini olish maqsadiga yo‘naltirilgan kompleks chora-tadbirlarni ifodalaydi. Axborotni muhofaza qilish tizimi deganda davlat axborotni muhofaza qilish tizimini hamda muayyan obyektlardagi himoya tizimlarini tushunish kerak. Davlat axborotni muhofaza qilish tizimiga quyidagilar kiradi:

– davlat me’yoriy hujjatlari, standartlar, boshqaruv hujjatlari va talablari;

– axborotni muhofaza qilish bo‘yicha konsepsiya, talablar, me’yoriy-texnik hujjatlar va ilmiy-uslubiy tavsiyalarni ishlab chiqish;

– davlat mulki bo‘lgan axborotni muhofaza qilishga yo‘naltirilgan chora-tadbirlarning tashkil etilishi, bajarilishi va amal qilinishi tartibi, shuningdek jismoniy va yuridik shaxslar ixtiyorida bo‘lgan axborotni muhofaza qilish bo‘yicha tavsiyalar;

– axborotni muhofaza qilish vositalarini sinash va sertifikatsiyalashni tashkillashtirish;

– axborotni muhofaza qilish uchun tashkilot va sohaviy koordinatsion tuzilmalarni tashkil etish;

– axborotni muhofaza qilishni tashkil etish bo‘yicha ishlarni nazorat qilish;

– chet el fuqarolari bo‘lgan yuridik va jismoniy shaxslarning davlat mulki bo‘lgan axborotdan yoki davlat tomonidan axborotni tarqatishga chegara qo‘yilgan yuridik va jismoniy shaxslar ma’lumotlaridan foydalana olish tartibini aniqlash. Axborotlashtirishning muayyan obyektlarida axborotni muhofaza qilishning maqsadlari ehtimoli bo‘lgan tahdidlarning ro‘yxati bilan belgilanadi. Har qanday axborotni muhofaza qilish tizimi o‘zining xususiyatiga ega bo‘lish bilan birga umumiy talablarga javob berishi kerak. Axborotni muhofaza qilishga ko‘proq qo‘yiladigan umumiy talablar quyidagilardir: Axborotni muhofaza qilish tizimi – bir butunlikda bo‘lishi;

– axborotning, axborot vositalarining xavfsizligini va axborot munosabatidagilar manfaatlarining himoyasini ta’minlashi;

– tizimning ichida uning elementlari orasida axborot aloqasini ta’minlashi;

– axborot faoliyatining texnologik kompleksini o‘ziga qamrab olishi;

– foydalanish vositalari bo‘yicha turli, axborotdan foydalana olishlilik bo‘yicha ko‘p darajali iyerarxik ko‘rinishda bo‘lishi;

– axborot xavfsizligi choralarini o‘zgartirish va to‘ldirishga ochiq bo‘lishi;

– nostandart bo‘lishi (himoya vositalarini tanlashda buzg‘unchining himoya imkoniyatlari bilan tanish emasligiga ishonishmaslik);

– texnik xizmat ko‘rsatishga oddiy va foydalanish uchun qulay bo‘lishi;

– ishonchli bo‘lishi kerak (texnik vositalardagi ixtiyoriy buzilish axborotning tarqab ketish kanali bo‘lib qolishi mumkin). Boshqa tizimlar kabi axborotni muhofaza qilish tizimi o‘z ta’minotining ma’lum turlariga ega bo‘lishi kerak. Shu sababli bu tizim quyidagilarga ega bo‘lishi mumkin:

– huquqiy ta’minot (bunga bajarilishi majburiy bo‘lgan me’yoriy hujjatlar, ko‘rsatmalar, yo‘riqnomalar, talablar kiradi);

– tashkiliy ta’minot (bunda axborotni muhofaza qilish ma’lum bir tuzilmaviy birliklar orqali qo‘llanilishi nazarda tutiladi: hujjatlar himoyasi xizmati; qo‘riqlash, kirishga ruxsat berish xizmati; texnik vositalar yordamida axborotni muhofaza qilish xizmati; axborot-tahliliy faoliyat va boshqalar);

– apparat ta’minoti (bunda axborotni muhofaza qilish hamda muhofaza qilish tizimi faoliyatini ta’minlash uchun texnik vositalardan keng miqyosda foydalanish nazarda tutiladi);

– axborot ta’minoti (ushbu ta’minot tarkibiga tizimning faoliyatini ta’minlovchi vazifalarni hal yotuvchi ma’lumotlar, axborotlar, ko‘rsatkichlar, kattaliklar kiradi. Shuningdek, unga xavfsizlik ta’minoti xizmati faoliyati bilan

bog‘liq bo‘lgan turli xarakterdagi ko‘rsatkichlar: ruxsat berish, ro‘yxatga olish, saqlash kabilar ham kiradi);

– dasturiy ta’minot (bunga konfedensial axborot manbalariga noqonuniy kirish yo‘llari hamda axborotni chiqib ketish kanallari mavjudligiga baho beruvchi turli axborot, hisobga olish, statistik va hisoblash dasturlari kiradi);

– matematik ta’minot (bu himoya uchun zarur bo‘lgan har xil hisoblarni amalga oshirishda, buzg‘unchilar texnik vositalarining xavfi tomonidan me’yorlar, hududlarga baho beruvchi matematik usullarni qo‘llashni nazarda tutadi);

– lingvistik ta’minot (axborotni muhofaza qilish sohasida mutaxassislar va foydalanuvchilar tomonidan qo‘llaniluvchi maxsus til vositalarining to‘plami);

– me’yoriy-uslubiy ta’minot (bunga axborotni muhofaza qilishni ta’minlovchi organlar, xizmatlar, vositalar faoliyati me’yorlari va reglamentlari, axborotni muhofaza qilish qattiq talab etiladigan sharoitlarda foydalanuvchilar tomonidan o‘z vazifalarini bajarishda faoliyatni ta’minlovchi turli uslublar kiradi).

5-Amaliy mashg’ulot. Tahdid razvedkasi va kibermudofaa strategiyalari (2 soat)

Tarmoq razvedkasi - mijozning axborot tizimi, axborot tizimining resurslari, foydalaniladigan qurilmalar va dasturiy ta'minot, ularning zaif tomonlari, himoya vositalari, shuningdek, axborot tizimiga kirish chegarasi to‘g'risidagi ma'lumotlarni olish va qayta ishlash.

Tarmoq razvedkasi DNS so‘rovlari, ping tekshiruvi va portni skanerlash shaklida bo‘ladi. DNS so‘rovlari ma'lum bir domenga kim egalik qilishini va ushbu domenga qanday manzillar tayinlanganligini tushunishga yordam beradi. DNS tomonidan topilgan manzillarga ping jo‘natish sizga ma'lum bir muhitda qaysi xostlar ishlayotganligini ko‘rish imkonini beradi. Xostlar ro‘yxatini hisobga olgan holda, xaker ushbu xostlar tomonidan qo‘llab-quvvatlanadigan xizmatlarning to‘liq ro‘yxatini tuzish uchun portni skanerlash vositalaridan foydalanadi. Va nihoyat, xaker xostlarda ishlaydigan ilovalarning xususiyatlarini tahlil qiladi. Natijada, xakerlik uchun ishlatilishi mumkin bo‘lgan ma'lumotlar olinadi.

Zamonaviy tarmoq razvedkasi, faoliyatning maqsadlari, ko‘lami va vazifalarni bajarish uchun qo‘yilgan vazifalar xarakteriga qarab quyidagilarga bo‘linadi:

- strategik.
- taktik;

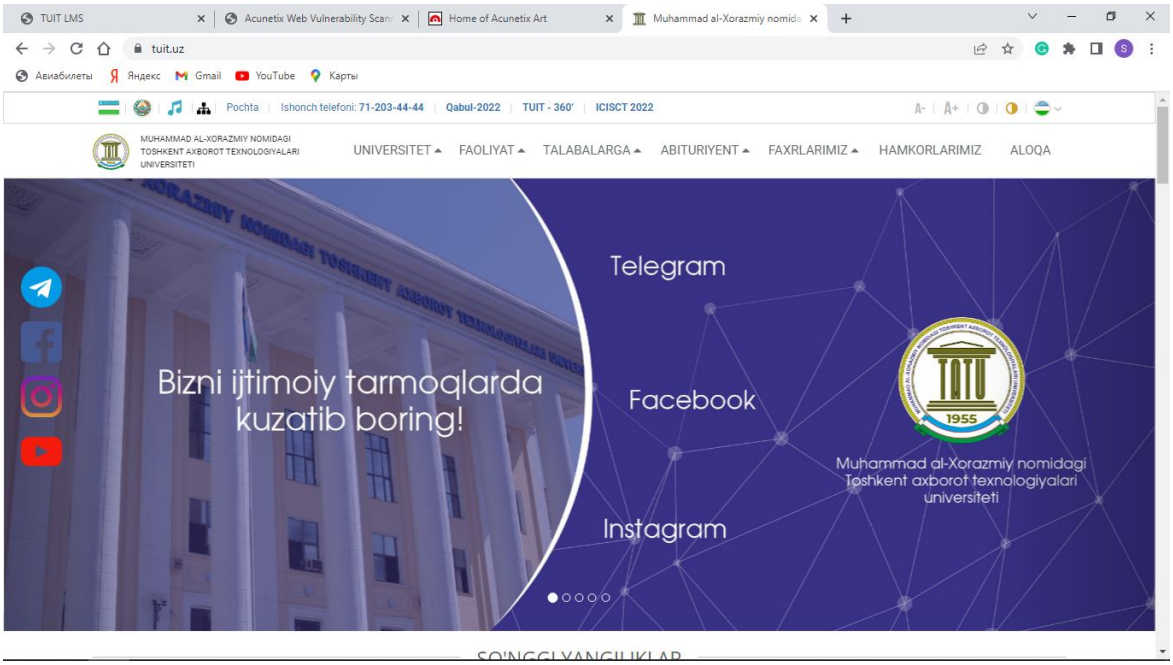
Taktik razvedka hujumchilarning harakatlarini ta'minlaydi. Bularga tajovuzkorlar ham, axborot tizimini sinovdan o‘tkazuvchi mutaxassislar ham kiradi. Taktik razvedka quyidagi ma'lumotlarni ochib beradi:

- texnik jihozlar,

- dasturiy ta'minot uskunalari,
- pochta serveridagi zaifliklar,
- xizmatlar va pochta mijozlari,
- tarmoq segmentlarining chegaralari,
- foydalanilgan aloqa kanallari (turi, tarmoqli kengligi),
- axborot tizimlariga hujumni rejalashtirish va amalga oshirish bo‘yicha maqbul qarorlarni qabul qilishga yordam beradigan tarmoq va/yoki serverga davlat (geografik, tijorat) egalik qilish.

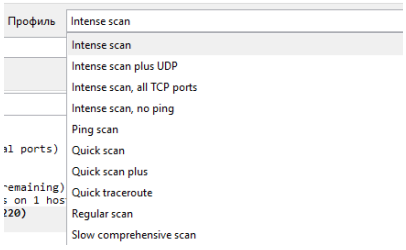
Ushbu ma'lumotlar elektron vositalar orqali uzatiladigan ma'lumotlarni ushlab turish orqali olinadi.

Nmap. Nmap dasturiy vositasi tarmoqda mavjud domenning host tizimi, portlari, foydalanuvchi xizmatlari va ulardagi xavfsizlik vositalari haqida axborot yig’uvchi vosita hisoblanadi. Undan foydalanish interfeysning soddaligi tufayli qulaydir. Dastlab bravzer orqali biz tekshirmoqchi bo‘lgan saytimiz manzili aniqlab olinadi.



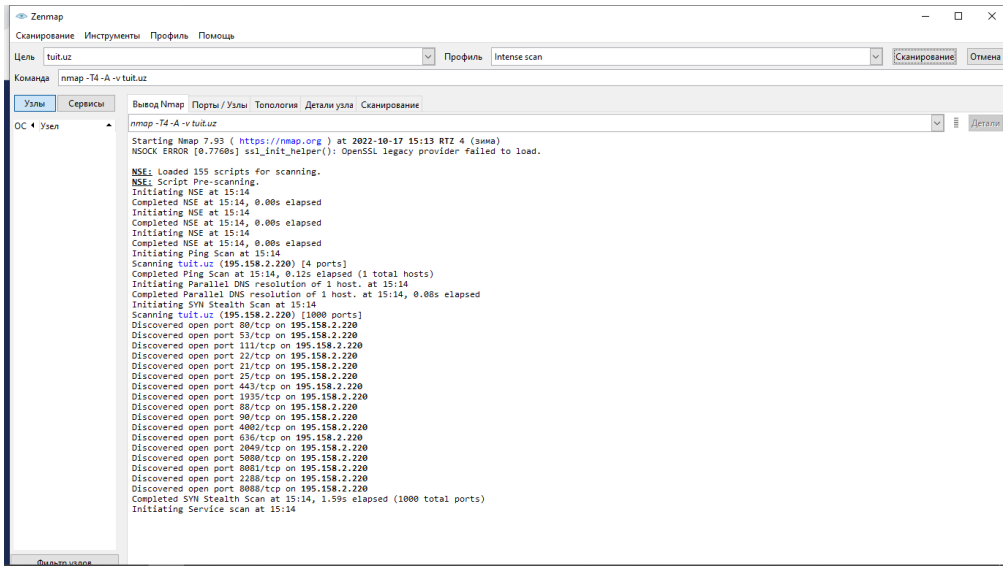
5.1-rasm. Sayt manzilini aniqlash

Aniqlangan manzil Nmap dasturiga qo‘yiladi. Buning uchun dasturda “Nishon (Цель - Target)” qismi mavjud bo‘lib, u tekshirilishi lozim bo‘lgan sayt manzilini qabul qiladi. So‘ngra “Skanerlash” tugmasi bosiladi. Bundan oldin “Profil” qismidan bizga kerakli bo‘lgan skanerlash turi tanlanadi.



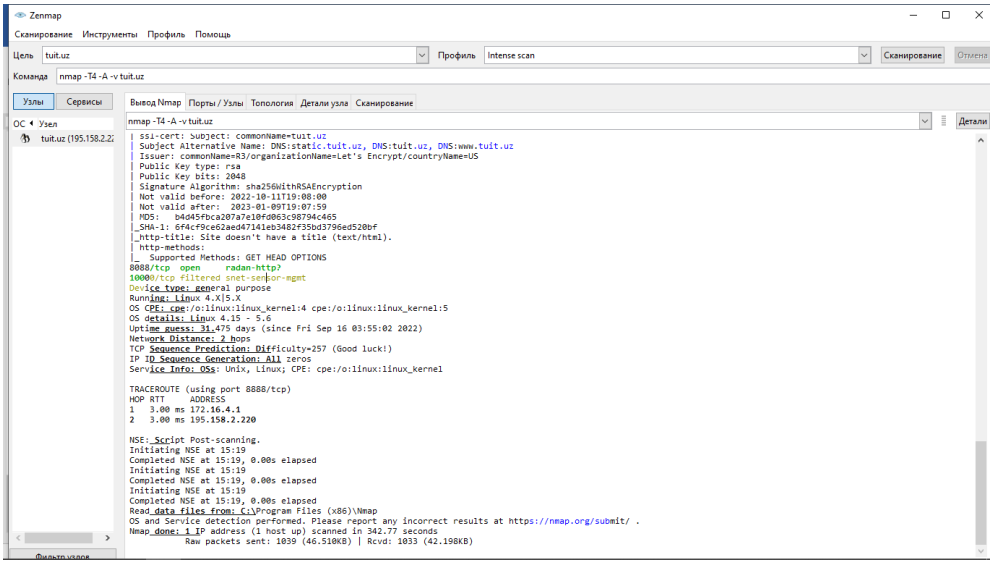
5.2-rasm. Skanerlash profillari

“Skanerlash” tugmasi bosilganidan so‘ng, dastur biz kiritgan manzilni tekshirish boshlaydi. Tekshirish “Nmap Done” xabari chiqmagunigacha davom etadi.



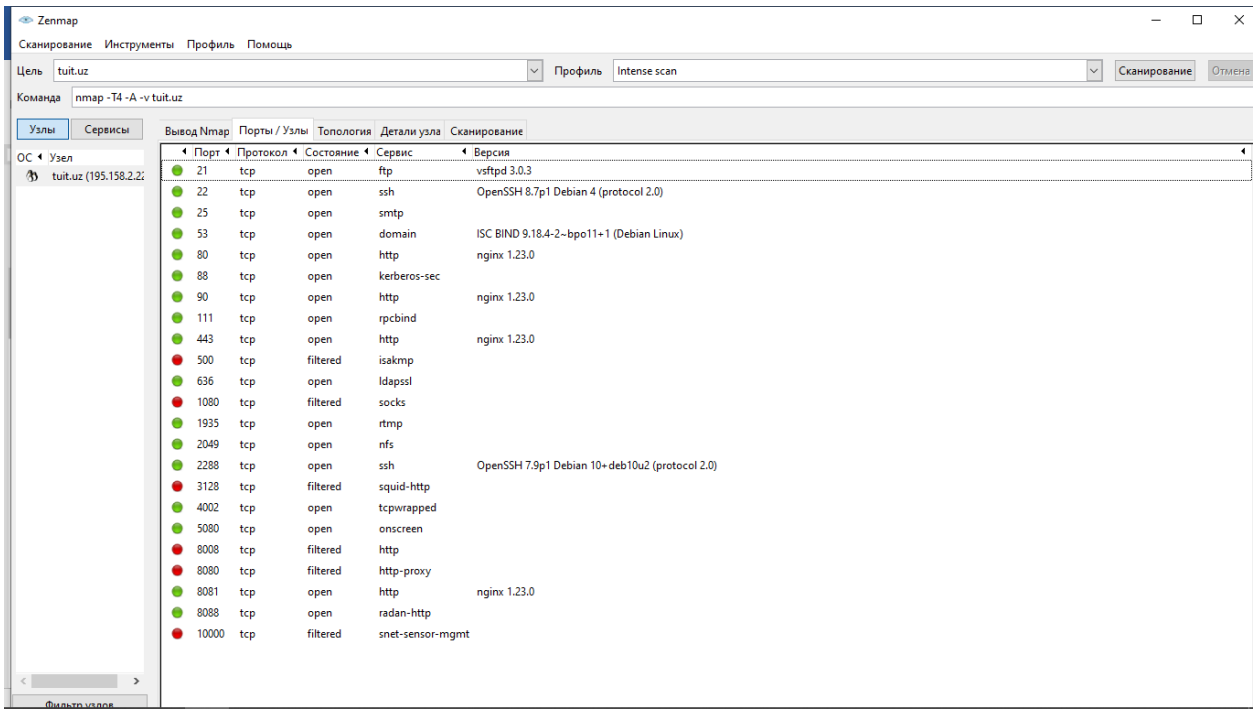
5.3-rasm. Skanerlash jarayoni

Dasturning asosiy oynasida skanerlash jarayoni tugaguniga qadar barcha xabarlar ketma-ketligi berib boriladi.



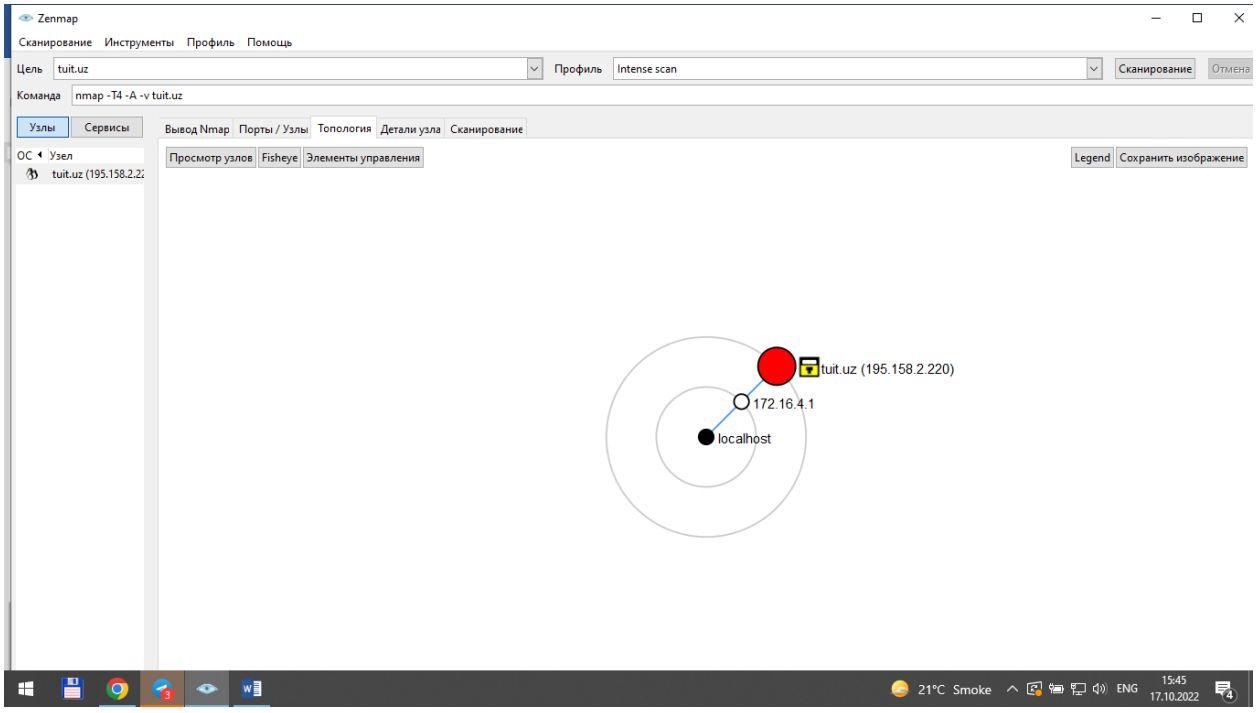
5.4-rasm. Skanerlash yakunlangan holati

Dasturning “Portlar (Ports - Порты)” bo‘limida biz skanerlagan sayt o‘rnatilgan hostdagi ochiq yoki firewall yordamida bloklangan portlar ro‘yhati, ulardan foydalanuvchi xizmatlar, portlar holati, protokoli va versiyasi haqida ma’lumot olishimiz mumkin.



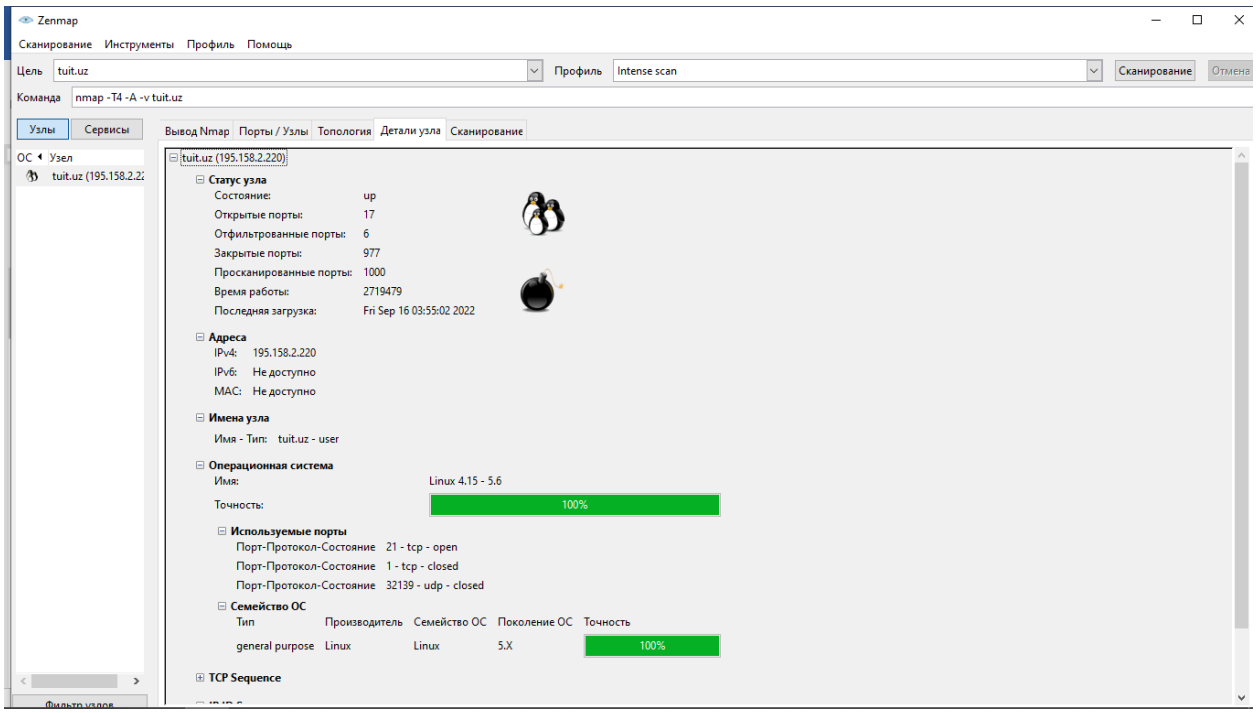
5.6-rasm. Portlar (Ports - Порты) bo‘limi

Dasturning “Topologiya” bo‘limida bizning tarmoq qurilmamizdan sayt faoliyat olib boruvchi hostgacha asosiy yo‘nalishni ko‘rishimiz mumkin.



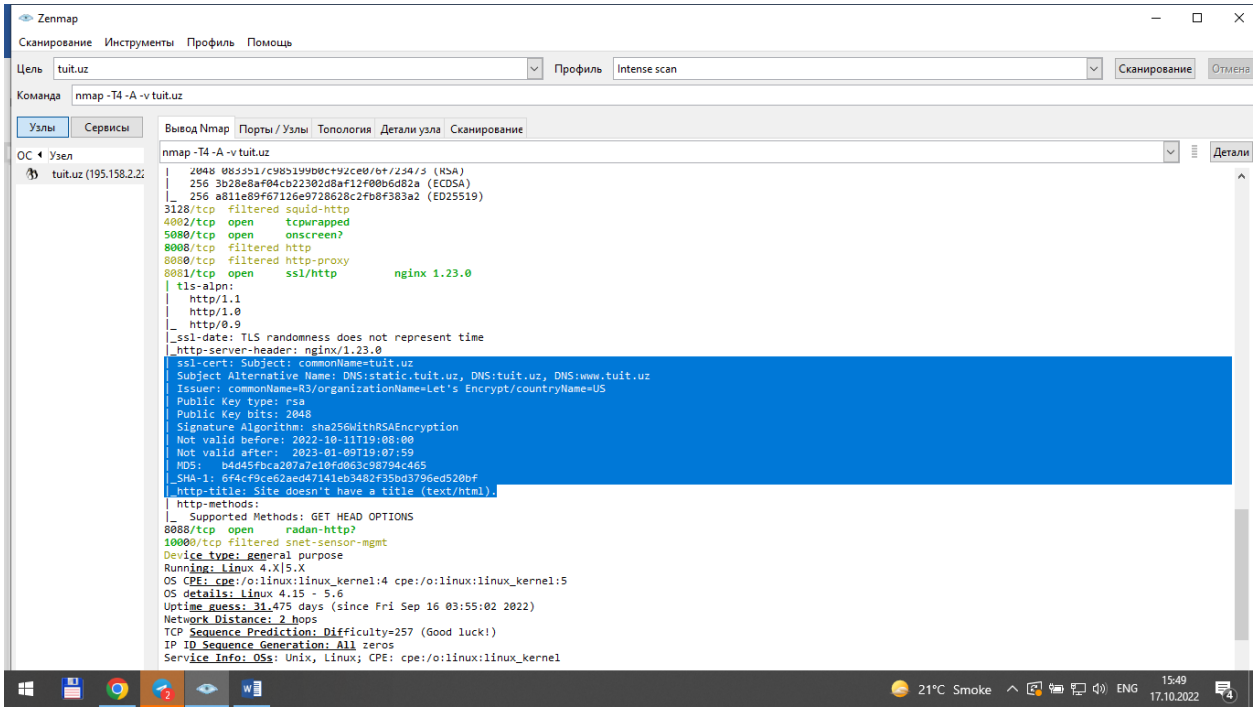
5.7-rasm. Topologiya oynasi

“Uzel parametrlari (Getaway detail – Детали узла)” bo‘limida hostda o‘rnatilgan OT va skanerlashning umumiy natijalarini ko‘rish mumkin.

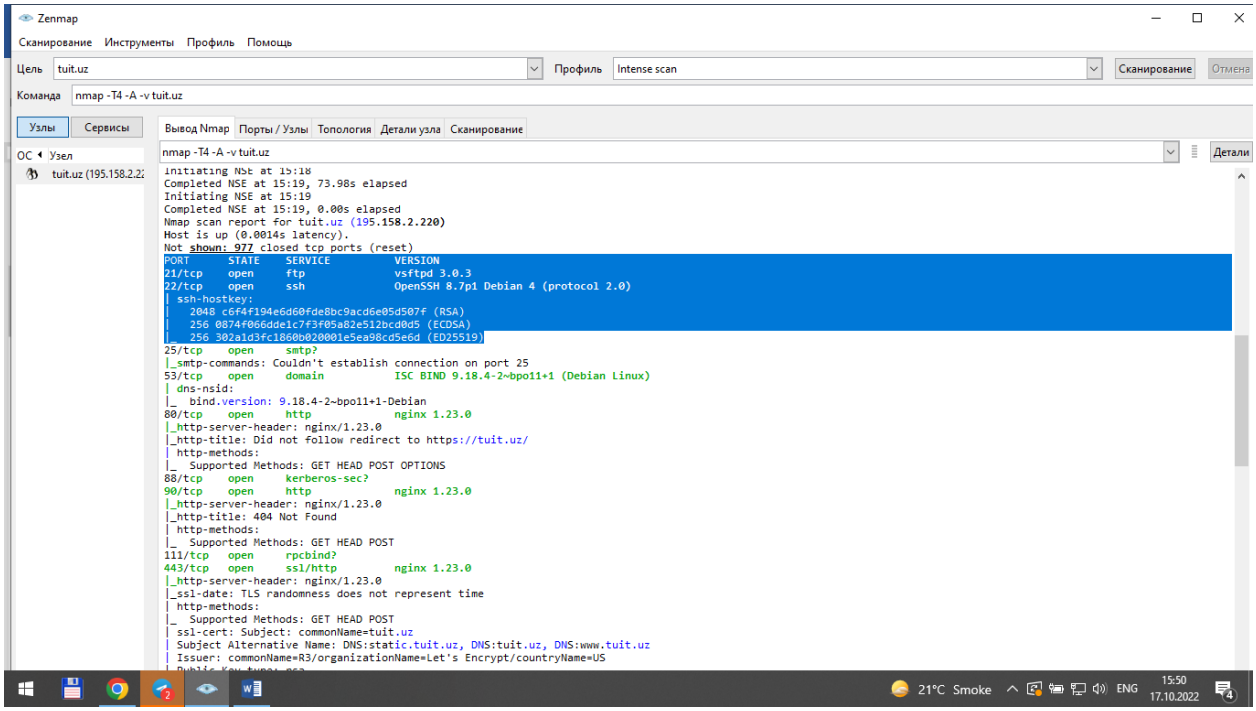


5.8-rasm. Uzel parametrlari bo‘limi

Dasturning asosiy oynasida saytdagi xavfsizlik parametrlari haqida to‘liqroq ma’lumot olish mumkin. Masalan, ssl sertifikati, kalitlar haqida ma’lumot, ssh protokoli va hokazo.



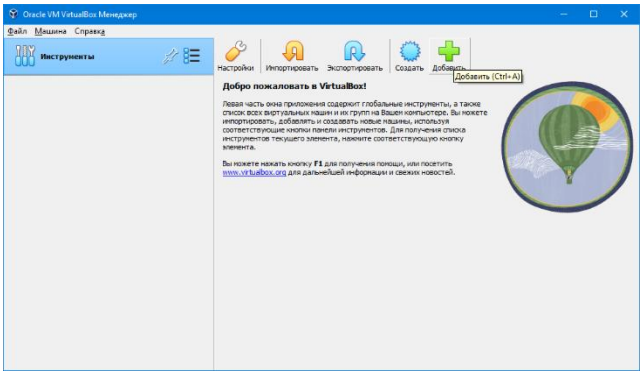
5.9-rasm. SSL sertifikati haqida ma’lumot



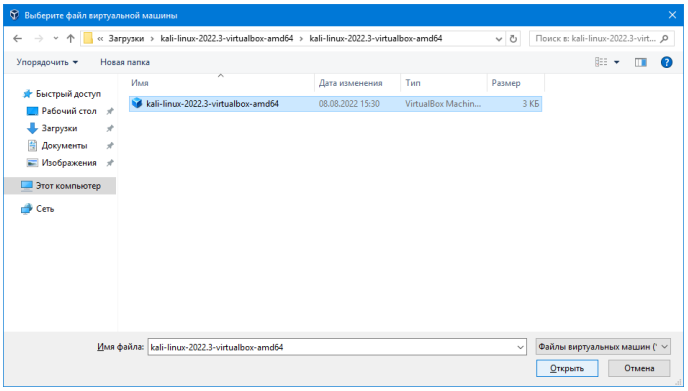
5.10-rasm. ftp va ssh haqida ma’lumot

Kali Linux OT yordamida razvedka hujumlarini amalga oshirish

Dastlab kali linux OT ni virtual mashinaga o‘rnatib olamiz. Buning uchun virtual disk obrazini VirtualBox dasturining “Qo‘shish - Добавить” tugmasini bosish orqali ko‘rsatamiz.

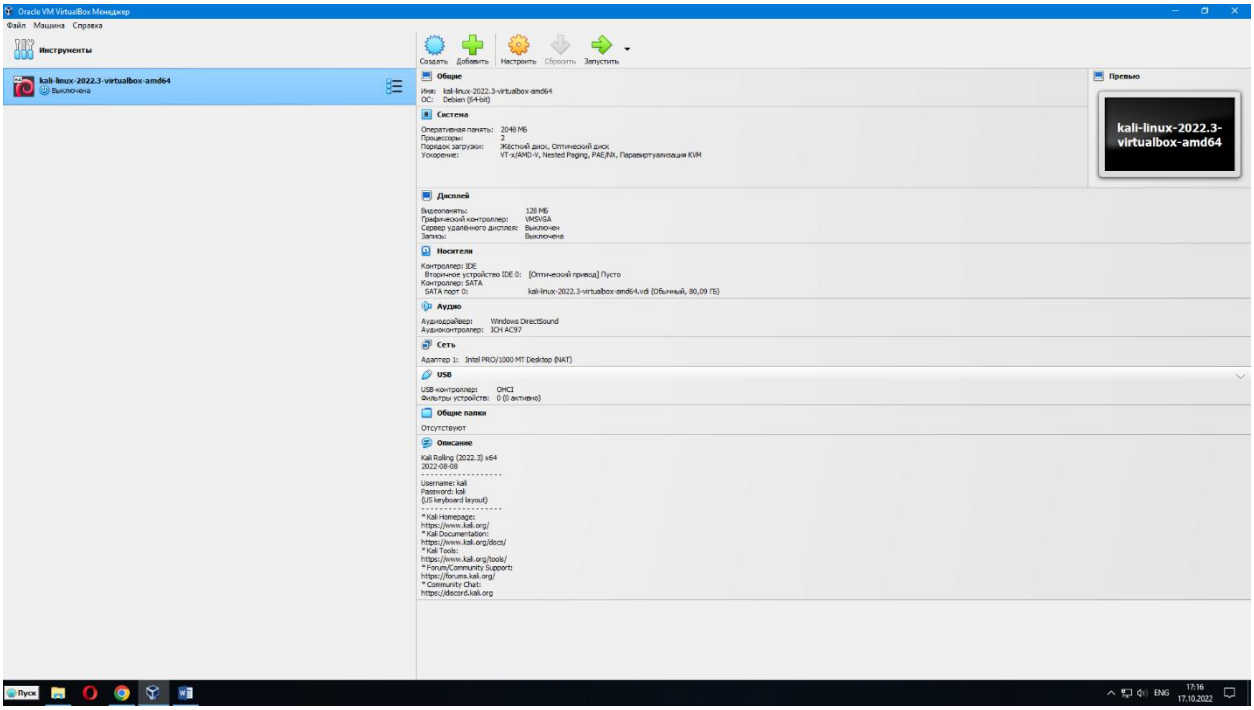


5.11-rasm. VirtualBox asosiy oynasi va unga virtual tizim obrazini qo‘shish

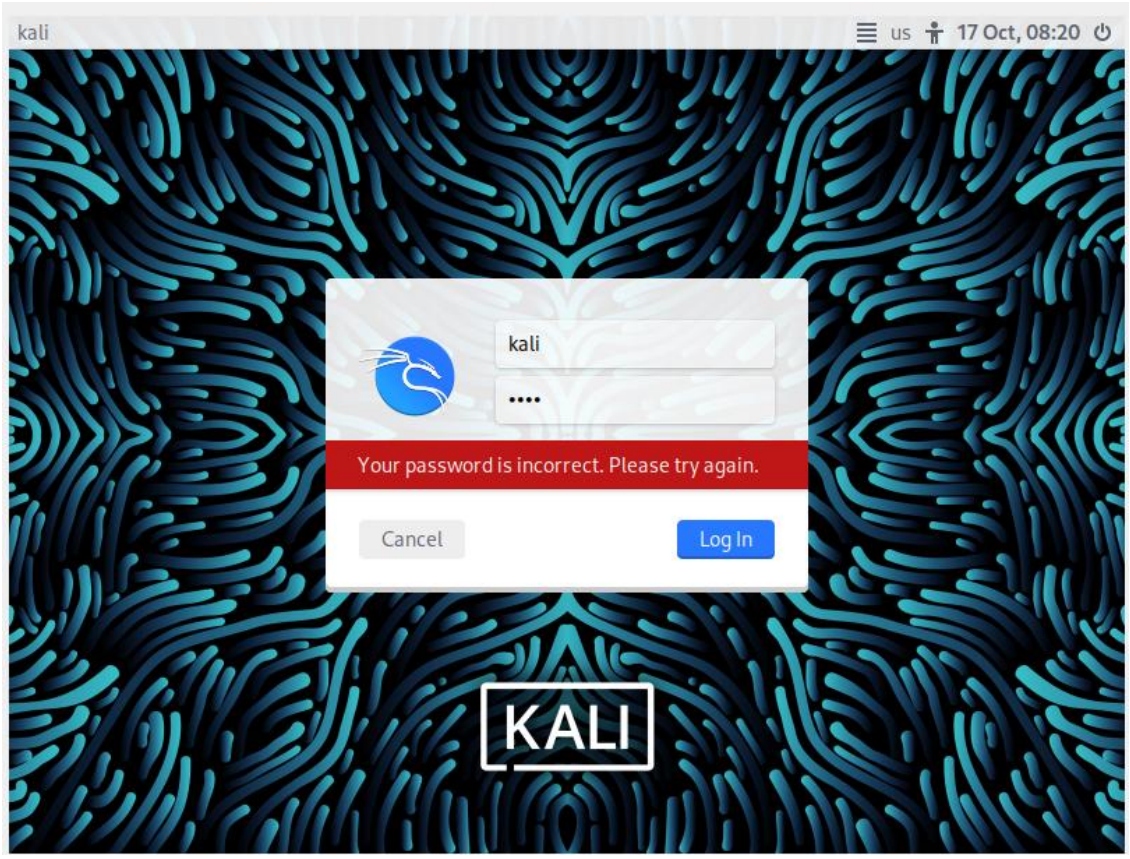


5.12-rasm. Virtual tizim obrazini tanlash

Virtual disk obrazi dastur yordamida tanib olinganida “Ishga tushurish - Запустить” tugmasi bosiladi va OT ishga tushiriladi. Ishga tushgan OT da login va parol sifatida “**kali**” so‘zi qo‘llaniladi.

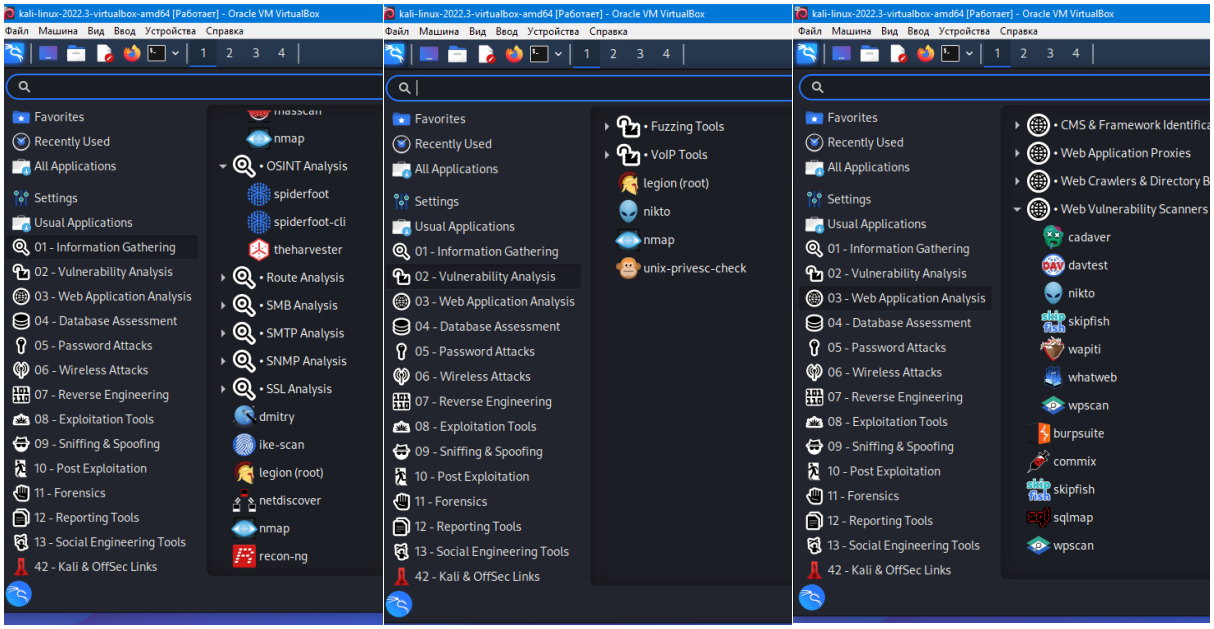


5.13-rasm. Kali Linuxning o‘rnatilish parametrlari



5.14-rasm. Kali Linuxga kirish

Kali Linux OT tizimlar va dasturlarni testlash uchun dasturlarni o‘zida mujassamlashtiradi. Biz ular ichidan “Nikto” va “Legion” dasturlari yordamida razvedkani amalga oshiramiz.

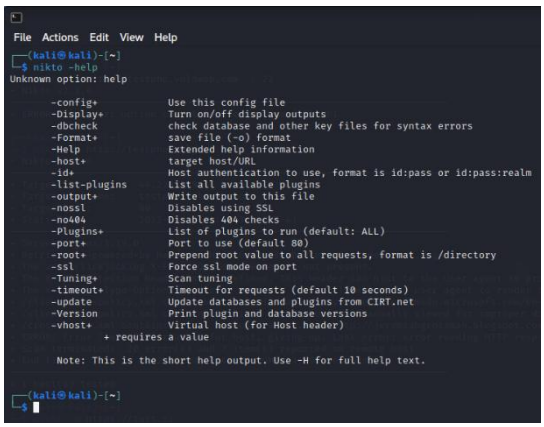


5.15-rasm. Razvedka hujumlari amalga oshirish vositalari

Nikto - tezkor xavfsizlik yoki ma'lumot tekshiruvlarini amalga oshirish uchun rfp ning LibWhisker-dan foydalangan holda Perl-da yozilgan ulanadigan veb-server skaneri.

Xususiyatlari:

- Osonlik bilan yangilanadigan CSV formatidagi tekshiruvlar ma'lumotlar bazasi
- Hisobotlarni oddiy matn yoki HTML formatida chiqarish
- Mavjud HTTP versiyalari avtomatik almashtirish
- Umumiy va maxsus server dasturlarini tekshirish
- SSL-quvvatlash (libnet-ssleay-perl orqali)
- Proksi-serverni qo‘llab-quvvatlash (autentifikatsiya bilan)
- Cookie-fayllarni qo‘llab-quvvatlash

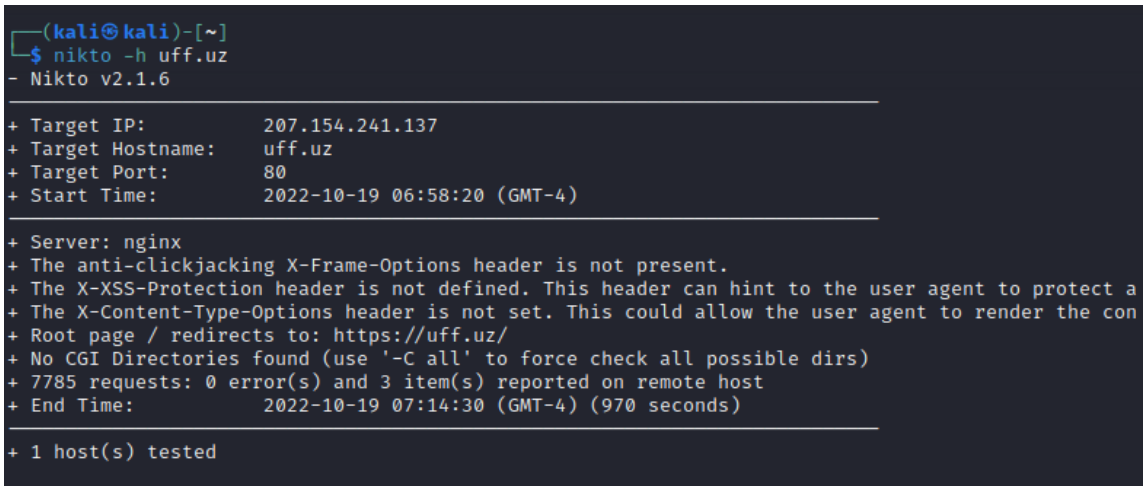


5.16-rasm. Nikto dasturidan foydalanish yordam komandalari

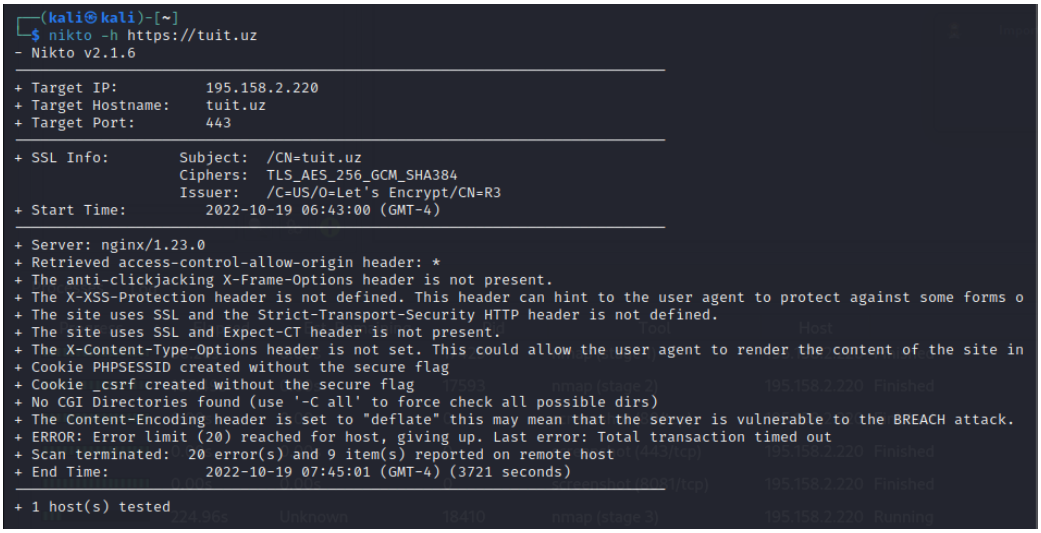
Ushbu dasturiy vosita web tizimlarni hujumlarga bardoshliligini baholash uchun ham ishlatiladi va asosan XSS turidagi hujumlarga zaifliklar mavjudligini tekshiradi. Web tizim IP manzilini aniqlab olgach hujum ssenariylarini ishga tushuradi. Topilgan zaifliklar haqida batafsil ma’lumot olish imkoniyatini beradi.

Dastur yordamida 3 ta web saytni sinab ko‘ramiz.

5.17-rasm. Birinchi saytni skanerlash uning natijalari



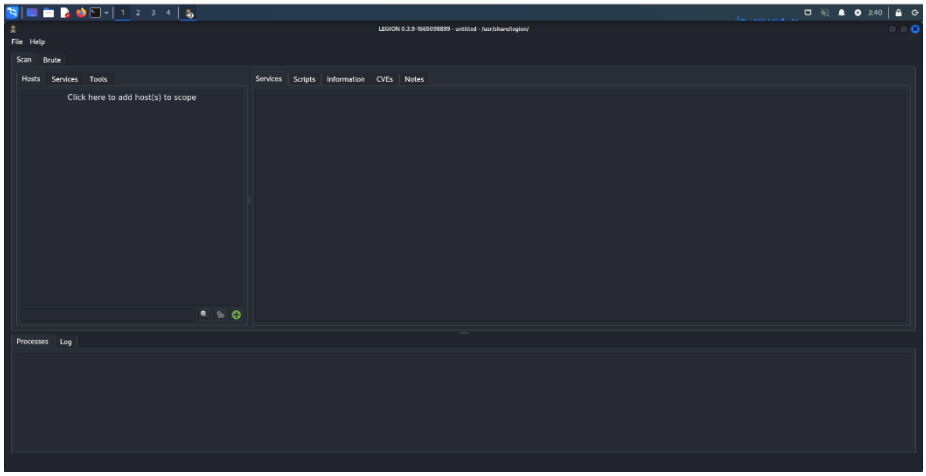
5.18-rasm. Ikkinchi saytni skanerlash uning natijalari



5.19-rasm. Uchinchi saytni skanerlash uning natijalari

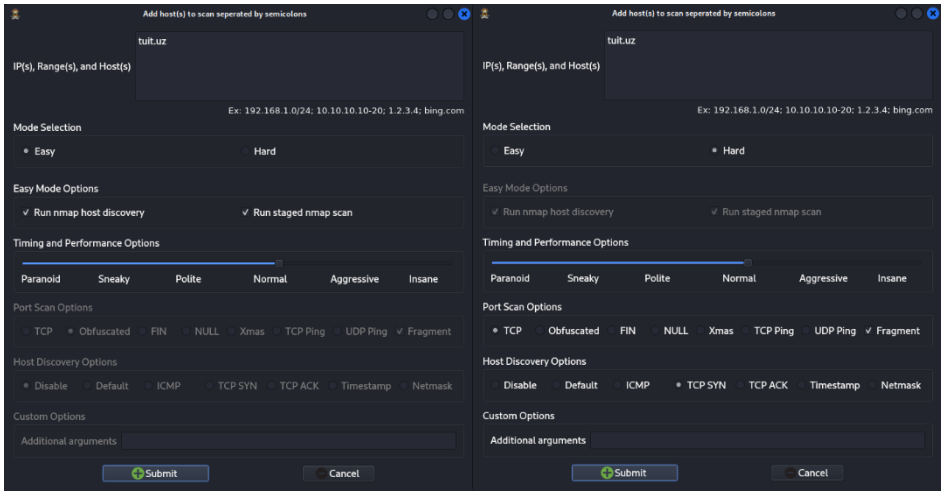
Keyingi dasturiy vosita “Legion” deb nomlanadi. Ushbu paket ochiq, ishlatish uchun qulay, o‘ta kengaytiriladigan va yarim avtomatlashtirilgan tarmoqqa kirishni

tekshirish vositasini o‘z ichiga oladi, bu axborot tizimlarini aniqlash, razvedka qilish va ekspluatatsiya qilishda yordam beradi.

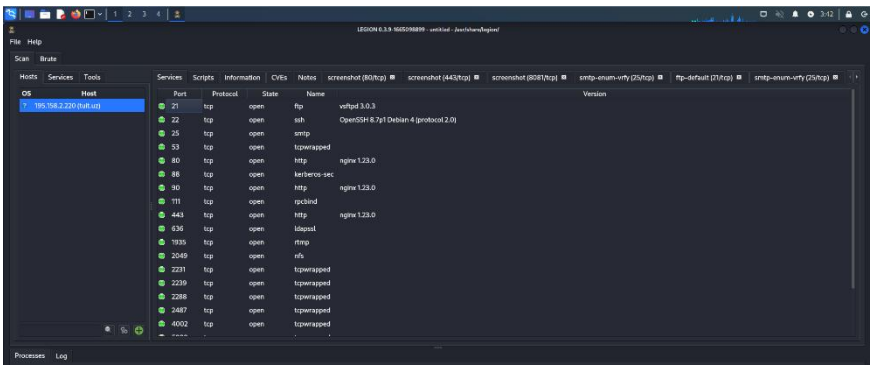


5.20-rasm. Dasturning asosiy oynasi

Dastur ishga tushirilgandan so‘ng tekshirilishi lozim bo‘lgan tizim nomi kiritiladi. Tekshirish rejimi va samaradorlik ko‘rsatiladi.



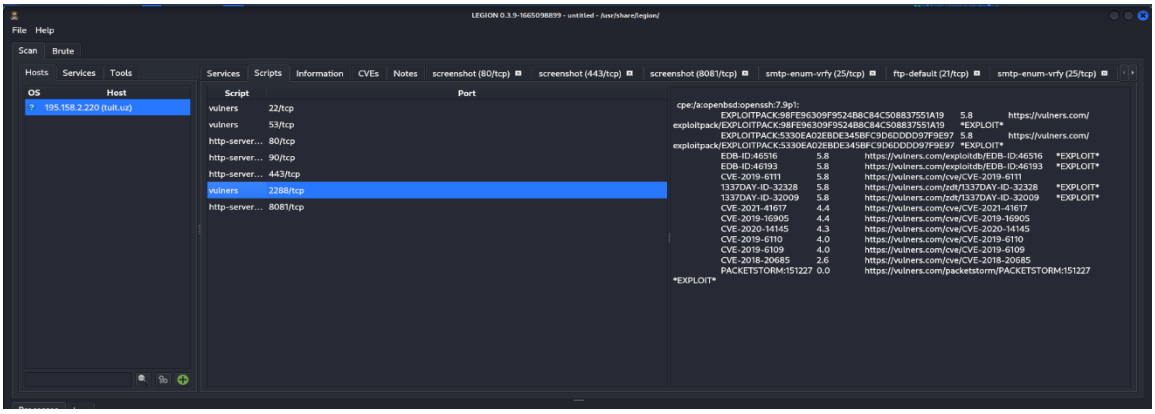
5.21-rasm. Skanerlash parametrlarini kiritish



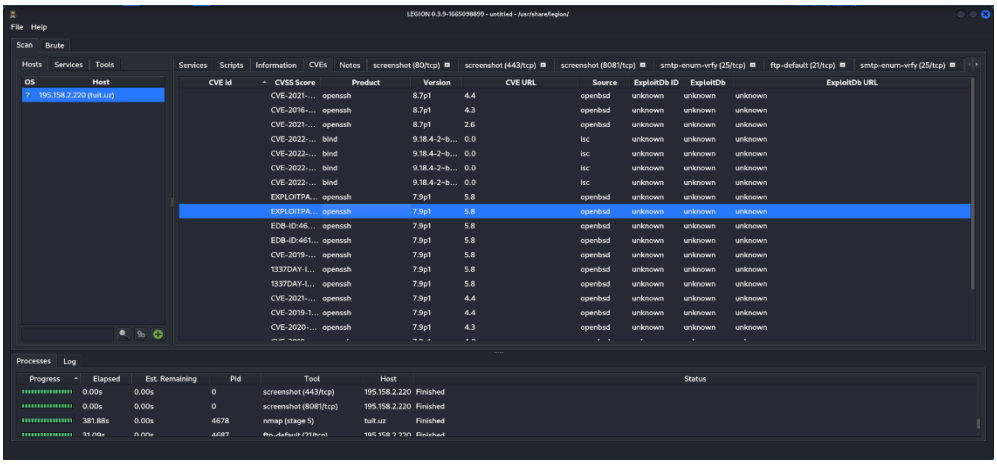
5.22-rasm. Portlar va xizmatlar

Skanerlash yakunlanganidan so‘ng tizimdagi ochiq portlar, ulardan foydalanuvchi xizmatlar, holati, zaif scriptlar, CVE (Common Vulnerabilities and Exposures – Asosiy zaifliklar va ta’sirlar) haqida tartibli va to‘liq ma’lumot olish mumkin.

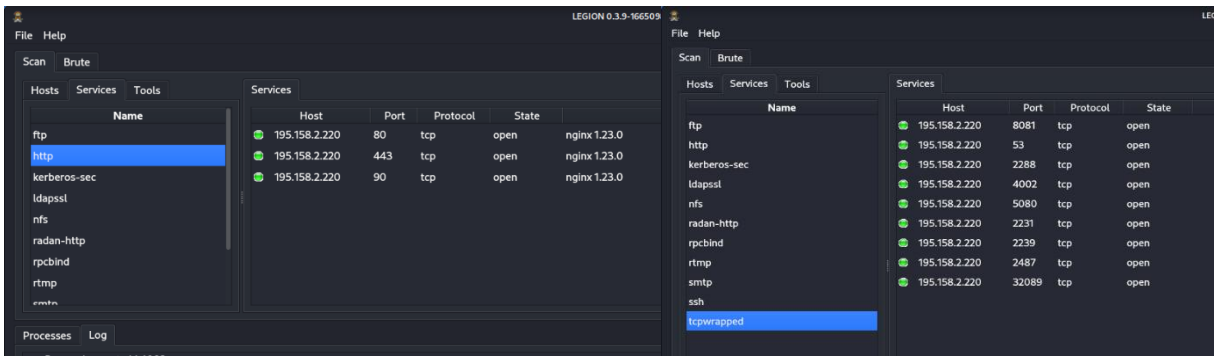
5.23-rasm. Umumlashtiruvchi axborot



5.24-rasm. Zaif scriptlar



5.25-rasm. CVE ro‘yhati



5.26-rasm. Tarmoq portlarini tasniflangan holda ajratish

KO‘CHMA MASHG‘ULOT

Tahdidlarni oldini olish va kiberxavfsizlik sohasidagi yangi yondoshuvlar (2 soat)

TATU Texnologiyalar transferi, inkubatsiya va akseleratsiya bo‘limi o‘quv laboratoriyasida olib borilayotgan loyihalar misolida imkoniyatlarini namoyish etish.

Tahdid razvedkasi va kibermudofaa strategiyalari (4 soat)

TATU o’quv-ilmiy laboratoriyasida olib borilayotgan loyihalar misolida imkoniyatlarini namoyish etish.

V-BO‘LIM
GLOSSARIY

V. GLOSSARY

Konfidentsiallik – Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o’qilishini” ta’minlaydi va tizim ma’lumotlarining tarqalishini ruxsat etilgan foydalanish bilan cheklash qobiliyati tushuniladi.

Yaxlitlik (butunlik) – qayd etilgan va xabar qilingan ma’lumotlarning haqiqiyligi, to‘g‘riligi va manbasini saqlab qolish qobiliyatini anglatadi, ya’ni, axborotni ruxsat etilmagan o’zgartirishdan yoki “yozish” dan himoyalashdir.

Foydalanuvchanlik – funktsional imkoniyatlarni o‘z vaqtida yetkazib berishni anglatgan holda ma’lumotni aniq va ishonchli ekanligiga ishonch hosil qilish, ma’lumot, axborot va tizimdan foydalanishning mumkinligi, ya’ni, ruxsat etilmagan “bajarish” dan himoyalashdir.

Siyosat - so‘zi kiberxavfsizlik bilan bog‘liq bo‘lgan turli vaziyatlarga nisbatan qo‘llaniladi. U axborotni tarqatish, axborotni himoya qilish bo‘yicha xususiy korxona maqsadlari, texnologiyani boshqarish uchun kompyuter operatsiyalari usullari va elektron qurilmalardagi konfiguratsiya o‘zgaruvchilari bilan bog‘liq qonun va qoidalarga murojaat qilish uchun ishlatiladi.

Port skanerlari - tizimdagi ochiq portlarni aniqlaydi. Bu testerlarga ular kirishga harakat qilayotgan tarmoqda ishlayotgan operatsion tizim va ilovalarni aniqlashga yordam beradi. Port skanerlari razvedkada qo‘llaniladi va potentsial hujum vektorlari uchun g‘oyalarni taqdim etishi mumkin.

Zaiflik skanerlari - serverlar, operatsion tizimlar va ilovalardagi ma’lum zaifliklarni, shuningdek sinovda ishlatilishi mumkin bo‘lgan noto‘g‘ri konfiguratsiyalarni qidiradi. Zaiflik skanerlari tomonidan taqdim etilgan hisobotlar penetratsion sinovchilarga tizimga dastlabki kirish huquqini beruvchi foydalaniladigan zaiflikni tanlashda yordam beradi.

Tarmoq sniffer - tarmoq trafigidagi ma’lumotlarni, shu jumladan uning manbasini, manzilini, tarmoqda aloqa qiladigan qurilmalarni, ishlatiladigan protokollar va portlarni kuzatib boradi. Bu ma’lumotlar shifrlangan yoki yo‘qligini tekshirish va penetratsiya testi paytida foydalanish mumkin bo‘lgan aloqa yo‘llarini aniqlash uchun foydali bo‘lishi mumkin.

Veb-proksi - penetratsion testerlarga o‘z brauzeri va tashkilot veb-serverlari o‘rtasidagi trafikni ushlab turish va o‘zgartirish imkonini beradi. Bu saytlararo skript (XSS) yoki saytlararo so‘rovlarni soxtalashtirish (CSRF) kabi hujumlarni faollashtirishi mumkin bo‘lgan yashirin shakl maydonlarini va boshqa HTML xususiyatlarini aniqlash imkonini beradi.

Parolni buzish - parolni xeshlash maqsadli tizim yoki tarmoqdagi imtiyozlarni oshirish vositasi sifatida tajovuzkorlar uchun umumiy maqsaddir.

Parolni buzish vositalari penetratsion testerlarga tashkilot xodimlariga xavf tug‘diradigan zaif parollardan foydalanayotganligini aniqlash imkonini beradi.

Kali Linux - bu kirish testini, xavfsizlikni tekshirishni va tegishli faoliyatni osonlashtiradigan operatsion tizim. Bu ochiq manba sifatida taqdim etilgan va Offensive Security tomonidan qo‘llab-quvvatlanadigan Debian-ga asoslangan Linux distributividir.

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

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

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

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

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

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

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

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.

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

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

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.

«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.

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.

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.

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

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.

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.

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

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.

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.

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.

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.

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

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.

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

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

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.

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

VI-BO‘LIM

ADABIYOTLAR RO‘YXATI

VI. ADABIYOTLAR RO‘YHATI

I. O‘zbekiston Respublikasi Prezidentining asarlari:

1. Mirziyoyev Sh.M. Buyuk kelajagimizni mard va olijanob xalqimiz bilan birga quramiz. – T.: “O‘zbekiston”, 2017. – 488 b.

2. Mirziyoyev Sh.M. Milliy taraqqiyot yo‘limizni qat’iyat bilan davom ettirib, yangi bosqichga ko‘taramiz. 1-jild. – T.: “O‘zbekiston”, 2017. – 592 b.

3. Mirziyoyev Sh.M. Xalqimizning roziligi bizning faoliyatimizga berilgan eng oliy bahodir. 2-jild. –T.: “O‘zbekiston”, 2018. – 507 b.

4. Mirziyoyev Sh.M. Niyati ulug‘ xalqning ishi ham ulug‘, hayoti yorug‘ va kelajagi farovon bo‘ladi. 3-jild.– T.: “O‘zbekiston”, 2019. – 400 b.

5. Mirziyoyev 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-sentyabrda 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-sentyabr “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-oktyabr “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 Mirziyoyevning 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. Maxsus adabiyotlar:

16. S.K. Ganiev, A.A.Ganiev, Z.T.Xudoyqulov Kiberxavfsizlik asoslari. O‘quv qo‘llanma. T.: “Aloqachi” nashriyoti, Toshkent 2020-y.

17. Pardeep Kumar, Vishal Jain, Vasaki Ponnusamy Artificial Intelligence and Cybersecurity: Current Trends and Future Prospects: 12 September 2021. https://doi.org/10.1002/9781119761655.ch22.

18. Oliy ta’limning me’yoriy - huquqiy xujjatlari to‘plami. -T., 2013.

19. Cyber security policy guidebook. Jennifer L. Bayuk. Jason Healey. Paul Rohmeyer, et.c. Willey publisher.2018-y. 288 p. ISBN 978-1-118-02780-6.

20. Mwaffaq Alhija. Cyber security: between challenges and prospects. - India, November 2020.

21. Shaping our Own Future in the European Higher Education Area // Convention of European Higher Education Institutions. - Salamanca, 2001, 29-30 march.

IV. Internet saytlar:

22. http://edu.uz – O‘zbekiston Respublikasi Oliy ta’lim, fan va innovasiyalar vazirligi..

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

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

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

26. http://natlib.uz – Alisher Navoiy nomidagi O‘zbekiston Milliy kutubxonasi.

VII. NAZORAT SAVOLLARI

№	Savollar
1	Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti
2	Cisco kompaniyasining Kiberxavfsizlik tushunchasiga bergan ta’rifi qanday?
3	Ma’lumotlar xavfsizligi nima?
4	Ma’lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta’minlashni maqsad qiladi
5	Foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi dasturiy ta’minotlarni ishlab chiqish va foydalanish jarayoniga e’tibor qaratadi
6	katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko‘rsatishga e’tibor qaratadi
7	Tashkil etuvchilar o‘rtasidagi aloqani himoyalashga etibor qaratib, o‘zida fizik va mantiqiy ulanishni birlashtiradi.
8	Dasturiy ta’minotlar xavfsizligi nima?
9	Tashkil etuvchilar xavfsizligi nima?
10	Aloqa xavfsizligi nima?
11	Tizim xavfsizligi nima?
12	Inson xavfsizligi nima?
13	Tashkilot xavfsizligi
14	Jamoat xavfsizligi
15	kiberxavfsizlik bilan bog‘liq inson hatti harakatlarini o‘rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma’lumotlarni va shaxsiy hayotni himoya qilishga e’tibor qaratadi
16	tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqqiyatli bajarishini madadlash uchun risklarni boshqarishga e’tibor qaratadi
17	u yoki bu darajada jamiyatda ta’sir ko‘rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi
18	axborot xavfsizligi muammosiga rasmiy qabul qilingan qarashlar tizimi va uni zamonaviy tendensiyalarni hisobga olgan holda yechish yo‘llari
19	Kiberxavfsizlik konsepsiyasi
20	Kiberxavfsizlik siyosati
21	tashkilotning maqsadi va vazifasi hamda xavfsizlikni ta’minlash sohasidagi chora-tadbirlar tavsiflanadigan yuqori sathli rejasi
22	Hodisa nima bu?
23	Normal hodisa
24	Hodisalarni kengayishi va ko‘payishi (Eskalatsiya)

25	Avariyaviy hodisa
26	shaxs yoki ishchi jarayonni, jarayonni, o‘rab olgan muxit va tizimni normal holatini o‘zgartirishni nazorat etishdir
27	kritik komponentalarga ta’sir qilmaydi yoki ko‘rsatma (rezolyusiya)ni boshlanishidan oldin o‘zgartirishni nazorat etishni talab qiladi.
28	Hodisalarni ko‘payishi tizimga jiddiy ta’sir ko‘rsatadi yoki amalga oshirilgan ko‘rsatma (rezolyusiya) o‘zgartirishni nazorat etish jarayonini kuzatishini ta’minlab berishi shart.
29	shaxs xavfsizligi va sog‘ligiga ta’sir ko‘rsatadi.
30	Insident bu?
31	Xavfsizlik insidenti koordinatori
32	Insidentni tergov qilish
33	Insidentga javob qaytarish
34	standart operatsiyalar qatoriga qo‘shilmaydigan hamda xizmat holatini uzib qo‘yish yoki xizmat sifati yomonlashishi holatlariga olib keladigan har qanday hodisaga aytiladi.
35	insidentga javob qaytarish jarayonini boshqaradi va komandani to‘plash uchun javobgar shaxsdir.
36	insident holatini tergov qilish harakati
37	xavfsizlikni buzilish ketma-ketligi yoki hujumni boshqarish va yechish uchun ishlab chiqilgan usuldir
38	Kodlashtirish
39	Kalit
40	Kriptoanaliz
41	Simmetrik shifr
42	Assimmetrik shifr
43	axborotni bir tizimdan boshqa tizimga ma’lum bir belgilar yordamida belgilangan tartib bo‘yicha o‘tkazish jarayoni
44	matnni shifrlash va shifrini ochish uchun kerakli axborot.
45	kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o‘rganadi.
46	ma’lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalaniladi
47	shifrlash va deshifrlash uchun ikkita kalitdan foydalaniladi
48	steganografiyaning asosiy g‘oyasi
49	Xesh funksiya
50	Risklarni davolash bu?
51	Tarmoq skanerlari
52	Ilova skanerlari

53	kompyuter tizimlarida tarqalish va o‘z-o‘zidan qaytadan tiklanish (replikatsiya) xususiyatlariga ega bo‘lgan bajariluvchi yoki sharxlanuvchi kichik dasturlardir
54	Fayl viruslari
55	Yuklama viruslar
56	Makroviruslar
57	Tarmoq viruslari
58	bajariluvchi fayllarga turli usullar bilan kiritiladi (eng ko‘p tarqalgan viruslar xili), yoki fayl yo‘ldoshlarni (kompan’on viruslar) yaratadi yoki faylli tizimlarni (linkviruslar) tashkil etish xususiyatidan foydalanadi.
59	o‘zini diskning yuklama sektoriga (boot sektoriga) yoki vinchesterning tizimli yuklovchisi (Master Boot Record) bo‘lgan sektorga yozadi. Yuklama viruslar tizim yuklanishida boshqarishni oluvchi dastur kodi vazifasini bajaradi.
60	axborotni ishlovchi zamonaviy tizimlarning makro dasturlarini va fayllarini, xususan MicroSoft Word, MicroSoft Excel va h. kabi ommaviy muharrirlarning fayl xujjatlarini va elektron jadvallarini zaharlaydi.
61	o‘zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi. Ba’zida ular "qurt" xilidagi dasturlar deb yuritishadi, Internet qurtlarga (Internet bo‘yicha tarqaladi), IRCqurtlarga (chatlar, Internet Relay Chat) bo‘linadi
62	Rezident viruslar
63	Rezident bo‘lmagan viruslar
64	faollashganlaridan so‘ng to‘laligicha yoki qisman yashash muhitidan (tarmoq, yuklama sektori, fayl) hisoblash mashinasining asosiy xotirasiga ko‘chadi.
65	faqat faollashgan vaqtlarida hisoblash mashinasining asosiy xotirasiga tushib, zaxarlash va zararkunandalik vazifalarini bajaradi.
66	Viruslar-«yo‘ldoshlar»
67	viruslar-«qurtlar» (worm).
68	fayllarni o‘zgartirmaydi. Uning ta’sir mexanizmi bajariluvchi fayllarning nusxalarini yaratishdan iboratdir
69	tarmoq orqali ishchi stansiyaga tushadi, tarmoqning boshqa abonentlari bo‘yicha virusni jo‘natish adreslarini hisoblaydi va virusni uzatishni bajaradi
70	talaba viruslar
71	«stels» viruslar (ko‘rinmaydigan viruslar)
72	polimorf viruslar
73	Risk
74	Riskni aniqlash tadbirlari

75	Risklarni aniqlash
76	Risklarni identifikatsiya qilishdan maqsad
77	hodisadan kelib chiqadigan oqibatlar va voqea-hodisa yuzaga kelishi ehtimolligi birikmasini o‘zida ifodalaydi.
78	Risklarni aniqlash; risklarni identifikatsiya qilish; risklarni tahlil qilish; risklarni baholash.
79	axborot aktivlarining ahamiyatini belgilaydi, mavjud (yoki mavjud bo‘lishi mumkin) qo‘llaniladigan tahdidlar va zaifliklarni identifikatsiya qiladi, mavjud boshqarish vositalarini va ularning identifikatsiya qilingan risklarga ta’sirini identifikatsiya qiladi, potensial oqibatlarni aniqlaydi va nihoyat, ustuvorliklarga muvofiq, muayyan risklarni joylashtiradi va kontekstni o‘rnatishda aniqlangan risklarni baholash mezonlari bo‘yicha ularni tasniflaydi
80	potensial zarar yetkazadigan ehtimoliy insidentlarni bashoratlash va bu zarar qay tarzda olinishi mumkinligi to‘g‘risida tasavvurga ega bo‘lish hisoblanadi.
81	Identifikatsiya
82	Autentifikatsiya
83	Avtorizatsiya
84	Nusxa yaratish
85	Ma’lumotlarni qayta tiklash
86	To‘liq nusxa yaratish
87	Differensial nusxa yaratish
88	Tarmoq hujumi
89	Hujum
90	Sotsial injineriya bu?
91	web-hujumlar
92	Adware
93	Spyware
94	Rootkits
95	Backdoors

96	Kiberetika
97	Passiv razvedka hujumlari
98	Aktiv razvedka hujumlari
99	fishing
100	Tashkilot va odamlarning maxsus va shaxsiy ma’lumotlarini olishga qaratilgan hujum
101	“Axborot xavfsizligi” tushunchasining uchta tarkibiy qismi nimalardan iborat?
102	Tarmoq sathidagi ma’lumotlar birligining nomi nima?
103	Ma’lumotlarni tinglash va uzatish jarayonidagi o‘zgarishlar hujumi ko‘rsatilgan variantni tanlang.
104	OSI modelidagi qaysi sath MAC manzillari bilan shug‘ullanadi?
105	Switch OSI modelining qaysi qatlamida ishlaydi?
106	Hub OSI modelining qaysi qatlamida ishlaydi?
107	Virus, qurt yoki DOS hujumi dasturiy yoki apparat ta’minotni buzadi?
108	Xizmatni rad etish hujumini belgilang?
109	O‘rta hujumdagi odamni toping?
110	Hujumlarni aniqlash tizimining qisqartmasi ko‘rsatilgan qatorni toping?
111	Hujumni bartaraf etish tizimining qisqartmasi ko‘rsatilgan qatorni toping?
112	OSI modelida nechta qatlam mavjud?
113	DDoS hujumlari uchun qanday protokol ishlatiladi?
114	IPv4 manzilining uzunligi necha baytga teng?
115	IPv6 manzilining uzunligi necha bitg?