

1 – ma’ruza. Kirish. Kiberxavfsizlikning asosiy tushunchalari

Axborot texnologiyalari kafedrası
dosenti Ziyadullaev Davron
Shamsievich

O'quv yuklamasi

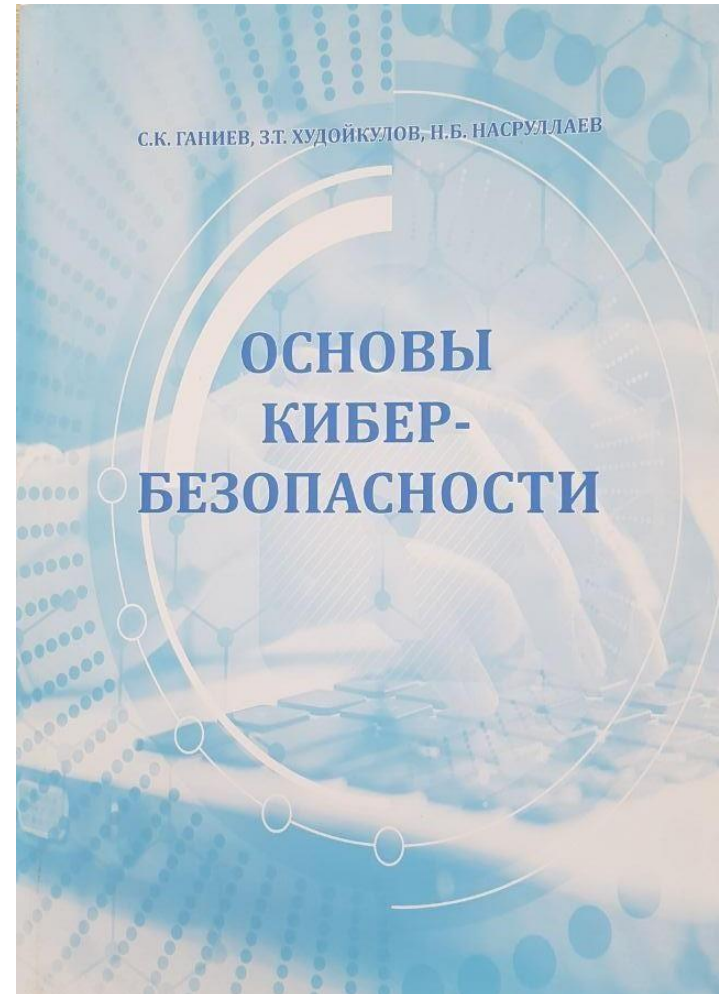
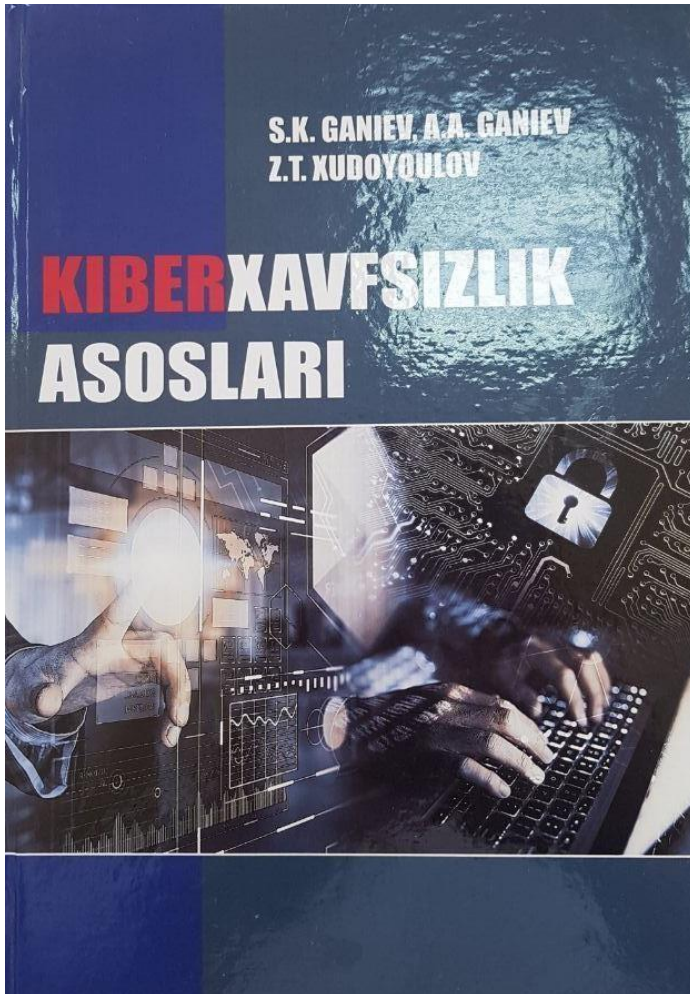
Faoliyat	Soatlar
Ma'ruza	30
Amaliy ish	42
Mustaqil ish	108
JAMI	180

Baholash

Bajariladigan ishlar	%
Semestr	50%
Referat tayyorlash	6%
Test tuzish	3+5%
Amaliy ish tayyorlash	6%
Amaliy ishlar (11)	20%
Oraliq nazorat	10%
Yakuniy ishlar	50%

*Ko'chirmachilikka yo'l qo'yilgan ishlarga ajratilgan kredit foizi **berilmaydi**.*

Foydalanilgan adabiyotlar



Xavfsizlik nima ?

- [Dictionary.com](https://www.dictionary.com) saytida “Security” so‘zi:
 1. Tahdid yoki xavfdan ozod; xavfsiz.
 2. Shubhadan, xavotirdan yoki qo‘rquvdan holi; ishonish.
- Tizim to‘g‘riligi
 - Agar kutilgan kirish amalga oshirilsa, tizim maqul natijani hosil qiladi.
- Xavfsizlik
 - Agar buzg‘unchi kutilmagan kirishni amalgi oshirsa, tizim ishida buzilish bo‘lmaydi.

Tizim to‘g‘riligi

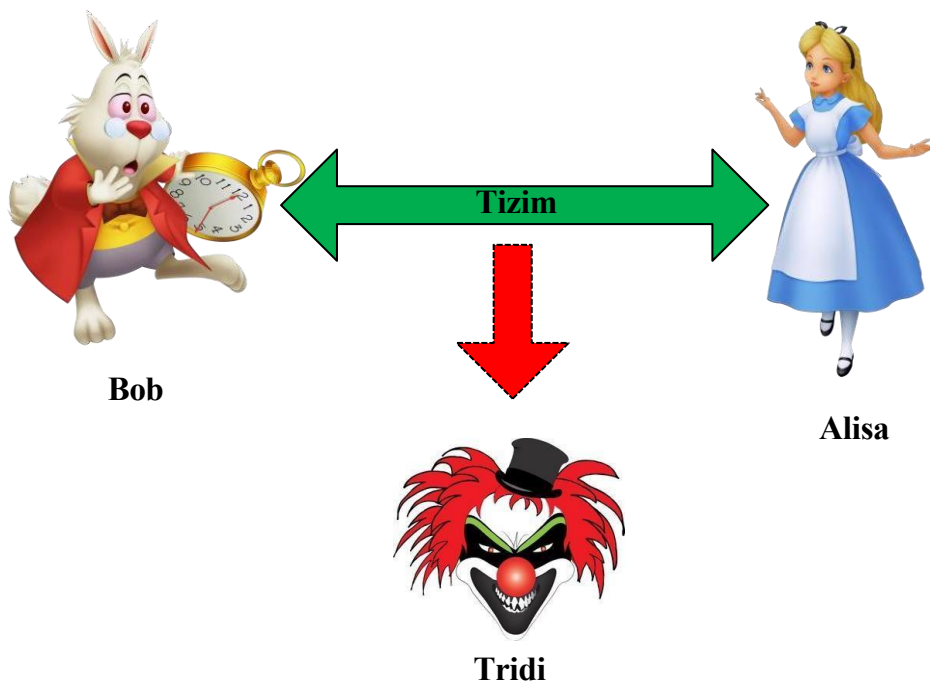
Yaxshi kirish \Rightarrow Yaxshi chiqish

Xavfsizlik

Yomon kirish \nRightarrow Yomon chiqish

Axborot xavfsizligining hayotdagi timsollari

- Hayotda qonuniy faoliyat olib boruvchi shaxslar mavjud, ular rasmda *Alisa* va *Bob* timsolida akslantirilgan.
- Biroq, hayotda qonuniy faoliyat yurituvchi insonlarning faoliyatiga qiziquvchi, ularning ishlariga xalaqit beruvchi insonlar ham mavjud va ular tasvirda *Tridi* timsolida tasvirlangan.



Alisaning onlayn banki (AOB) ssenariyeci:

1. Alisa onlayn bankning biznes faoliyatini amalga oshiradi.
2. Bob Alisaning mijosi.
3. Tridi buzg'unchi.

Kiberxavfsizlik nima?

- *Kiberxavfsizlik* hozirda kirib kelgan yangi tushunchalardan biri bo‘lib, unga turli berilgan turli ta’riflar mavjud.
- Xususan, **CSEC2017 Joint Task Force (CSEC2017 JTF)** kibyxavfsizlikka quyidagicha ta’rif bergan: *kiberxavfsizlik* – hisoblashga asoslangan bilim sohasi bo‘lib, buzg‘unchilar mavjud bo‘lgan sharoitda amallarni kafolatlash uchun o‘zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.
- U xavfsiz kompyuter tizimlarini yaratish, amalga oshirish, tahlil qilish va testlashni **o‘z ichiga oladi**.
- Kiberxavfsizlik ta’limning **mujassamlashgan** bilim sohasi bo‘lib, qonuniy jixatlarni, siyosatni, inson omilini, etika va risklarni boshqarishni **o‘z ichiga oladi**.

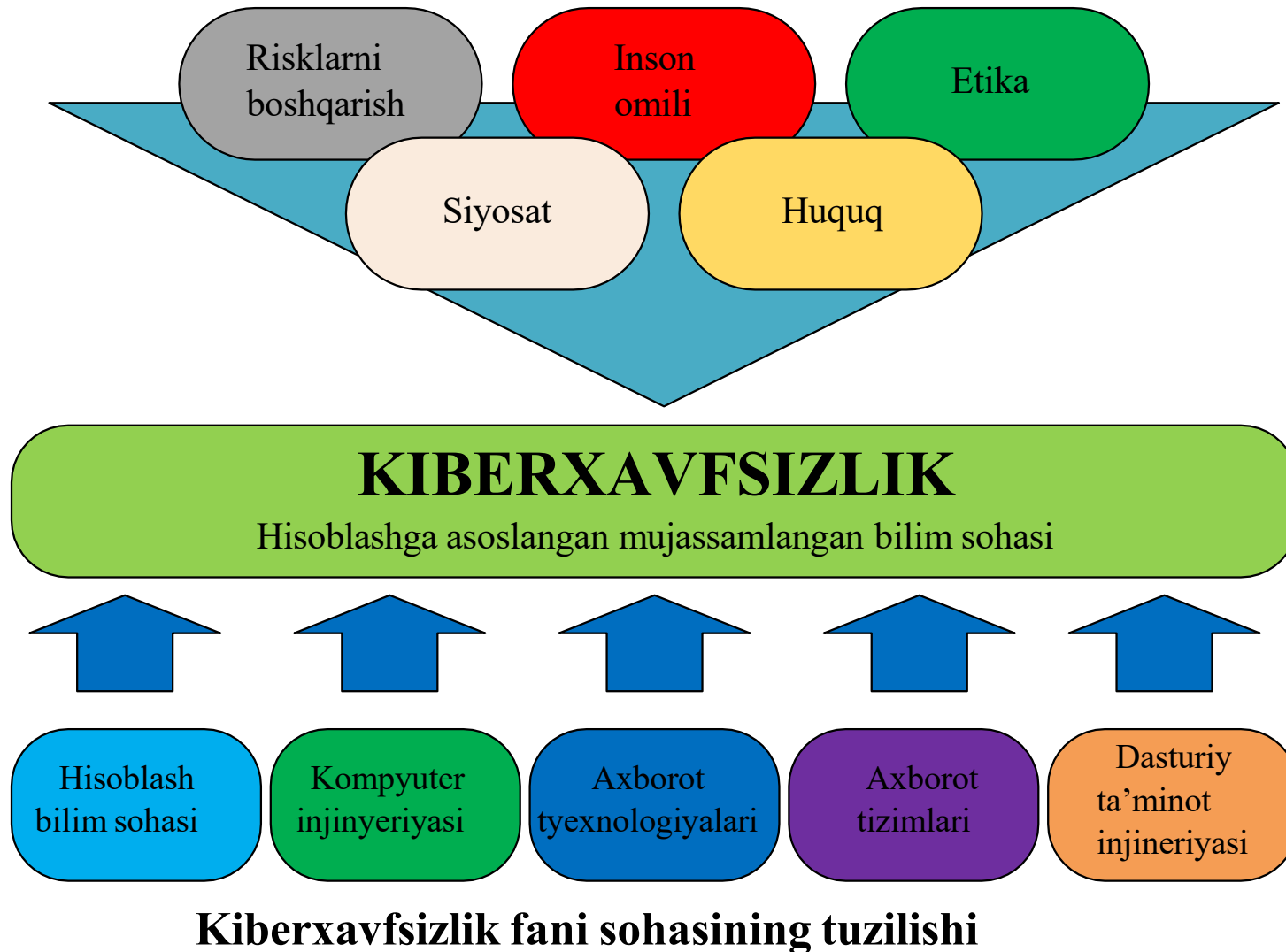
Kiberxavfsizlik nima?

- Tarmoq bo'yicha faoliyat yuritayotgan **Cisco** tashkiloti esa kiberxavfsizlikka quyidagicha ta'rif bergan: **Kiberxavfsizlik** — tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti.
- Ushbu kiberxujumlar odatda *maxfiy axborotni boshqarish, almashtirish yoki yo'q qilishni; foydalanuvchilardan pul undirishni; yoki normal ish faoliyatini uzub qo'yishni* **maqsad qiladi.**
- Hozirgi kunda samarali kiberxavfsizlik choralarini amalga oshirish *insonlarga qaraganda qurilmalar sonining ko'pligi va buzg'unchilar salohiyatini ortishi natijasida* **amaliy tomondan murakkablashib** bormoqda.

Nima uchun kiberxavfsizlik kerak ?

- **Kiberxavfsizlik bilim sohasining** zaruriyati **birinchi meynfrem kompyuterlar** ishlab chiqarilgandan boshlab paydo bo‘la boshlagan.
- Bunda mazkur qurilmalarni va ular xizmat qilgan missiyalarni himoyasi uchun **ko‘p qatlamli xavfsizlik** amalga oshirilgan.
- **Milliy xavfsizlikni ta‘minlash** zaruriyatini ortishi natijasida **kompleks va texnologik** tomondan murakkab bo‘lgan ishonchli xavfsizlik paydo bo‘ldi.

Nima uchun kiberxavfsizlik kerak ?



Kiberxavfsizlikning fundamental terminlari



Kiberxavfsizlikning fundamental terminlari

- **Konfidensiallik**

- Tizim ma'lumoti va axborotiga faqat **vakolatga ega sub'yektlar** foydalanishi mumkinligini ta'minlovchi qoidalar.
- Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan **“o'qilishini”** ta'minlaydi.

- **Yaxlitlik (butunlik)**

- Ma'lumotni aniq va ishonchli ekanligiga ishonch hosil qilish.
- Ya'ni, axborotni ruxsat etilmagan o'zgartirishdan yoki **“yozish”** dan himoyalash.

- **Foydalanuvchanlik**

- Ma'lumot, axborot va tizimdan foydalanishning mumkinligi.
- Ya'ni, ruxsat etilmagan **“bajarish”** dan himoyalash.

Kiberxavfsizlikning fundamental terminlari

- **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.
 - Kiberxavfsizlikda yoki axborot xavfsizligida **risklar salbiy ko‘rinishda** qaraladi.
- **Hujumchi kabi fikrlash** - bo‘lishi mumkin bo‘lgan xavfni oldini olish maqsadida qonuniy foydalanuvchining hujumchi kabi fikrlash jarayoni.
 - **Yaxshi insonlar “yomon inson”** kabi o‘ylashi kerak !
 - Milisiya xodimi...
 - ...kriminal haqida bilishi va tushinishi kerak
 - Ushbu kursda
 - Biz hujumchi foydalangan usullarini bilishni istaymiz.
 - Buzg‘unchi motivlari haqida o‘ylash kerak.
 - Tez – tez buzg‘unchi kabi bo‘lish.

Kiberxavfsizlikning fundamental terminlari

- **Tizimli fikrlash** - kafolatlangan amallarni ta'minlash uchun ijtimoiy va texnik cheklovlarning o'zaro ta'sirini hisobga oladigan fikrlash jarayoni.
 - Masalan, *virusga qarshi himoya uchun faqat antivirus dasturini o'rnatishning o'zi yetarli emas. Viruslar va ularni tarqalish usullari bo'yicha xodimlarga ma'lumotlar berish va seminarlar o'tkazish talab etiladi.*
- **Axborot xavfsizligi** - axborotning holati bo'lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta'sir etishga yoki ruxsatsiz undan foydalanishga yo'l qo'yilmaydi.
- **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.

Kiberxavfsizlikning fundamental terminlari

- **Maqsad** – u yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz hisoblanadi.
- **Noaniqlik** – hozisaga, uning oqibatlarini yoki uning ehtimolini bilishga aloqador axborotni yoki bilimlarni etishmasligi yoki qisman yetishmasligi holati.
- **Ta'sir** – kutilgan yoki xoxlagan hodisani salbiy yoki ijobiy tomonga og'ishi.
- **Aktiv** – tashkilot uchun qadri bo'lgan ixtiyoriy narsa bo'lib, axborot xavfsizligiga bog'liq holda aktiv sifatida tashkilotning muhim ahborotini keltirish mumkin.

Kiberxavfsizlikning fundamental terminlari

- **Zaiflik** – bu bir yoki bir nechta tahdidga sabab bo‘luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik hisoblanadi.
- **Tahdid** – tizim yokitashkilotga zarar yetkazishi mumkin bo‘lgan istalmagan hodisa.
- **Hujum** – tahdidning amalga oshirilgan ko‘rinishi.
- **Boshqarish vositasi (Control)** – bu riskni o‘zgartiradigan harakatlar bo‘lib, boshqarish natijasi zaiflik yoki tahdidga ta’sir qiladi.
 - **Bundan tashqari**, boshqarish vositasining o‘zi turli tahdidlar uchun foydalanilishi mumkin bo‘lgan zaiflikka ega bo‘lishi mumkin.

Xavfsizlik muammolari

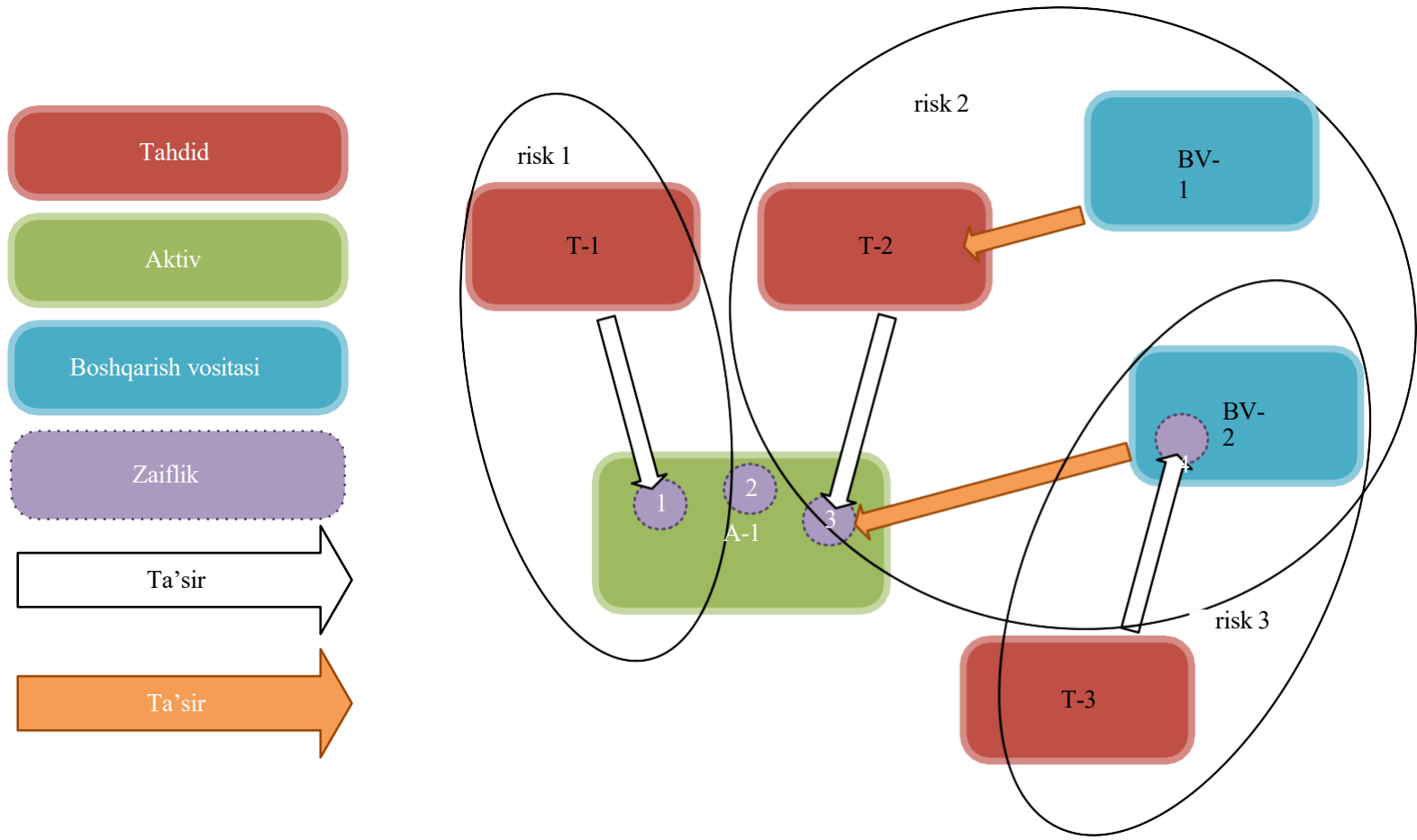


Zaiflik

Tahdid

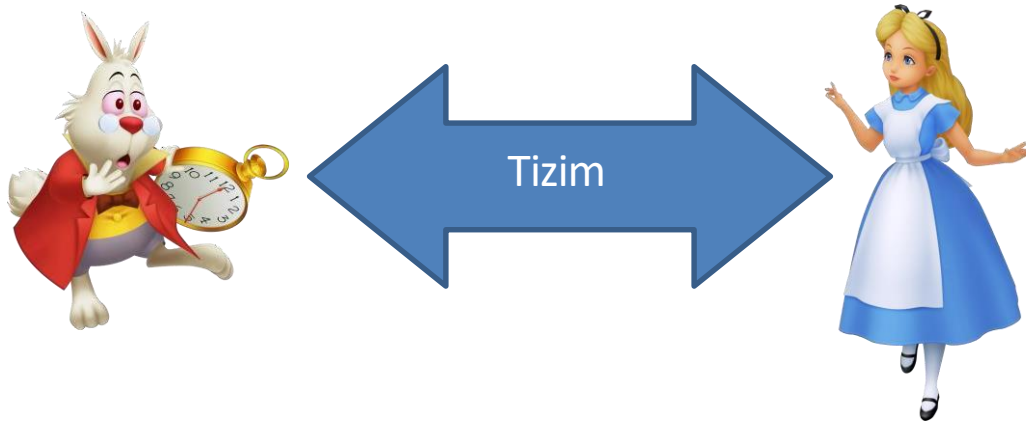
Hujum

“Tahdid-zaiflik-aktiv-boshqarish vositasi” asosida risk modeli



Kiberxavfsizlikni umumiy ko‘rinishi

- Alisa (A) va Bob (B) **yaxshi odamlar**

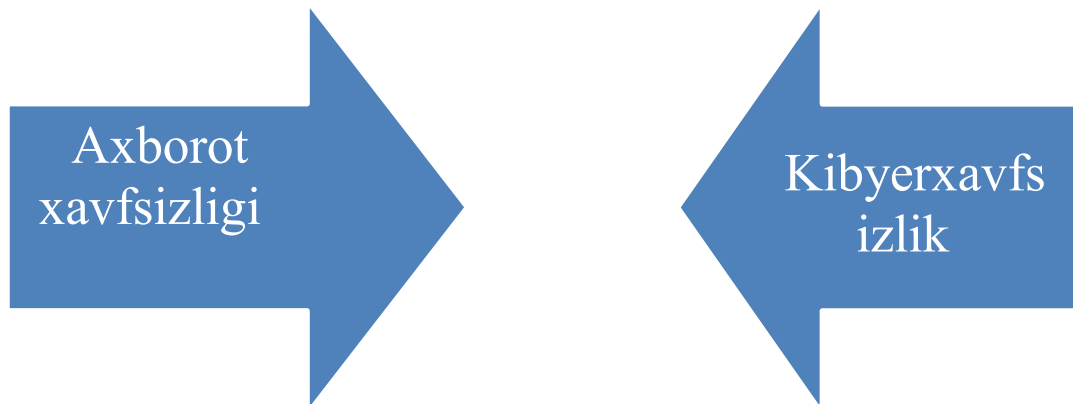


Tridi (T) yomon odam →



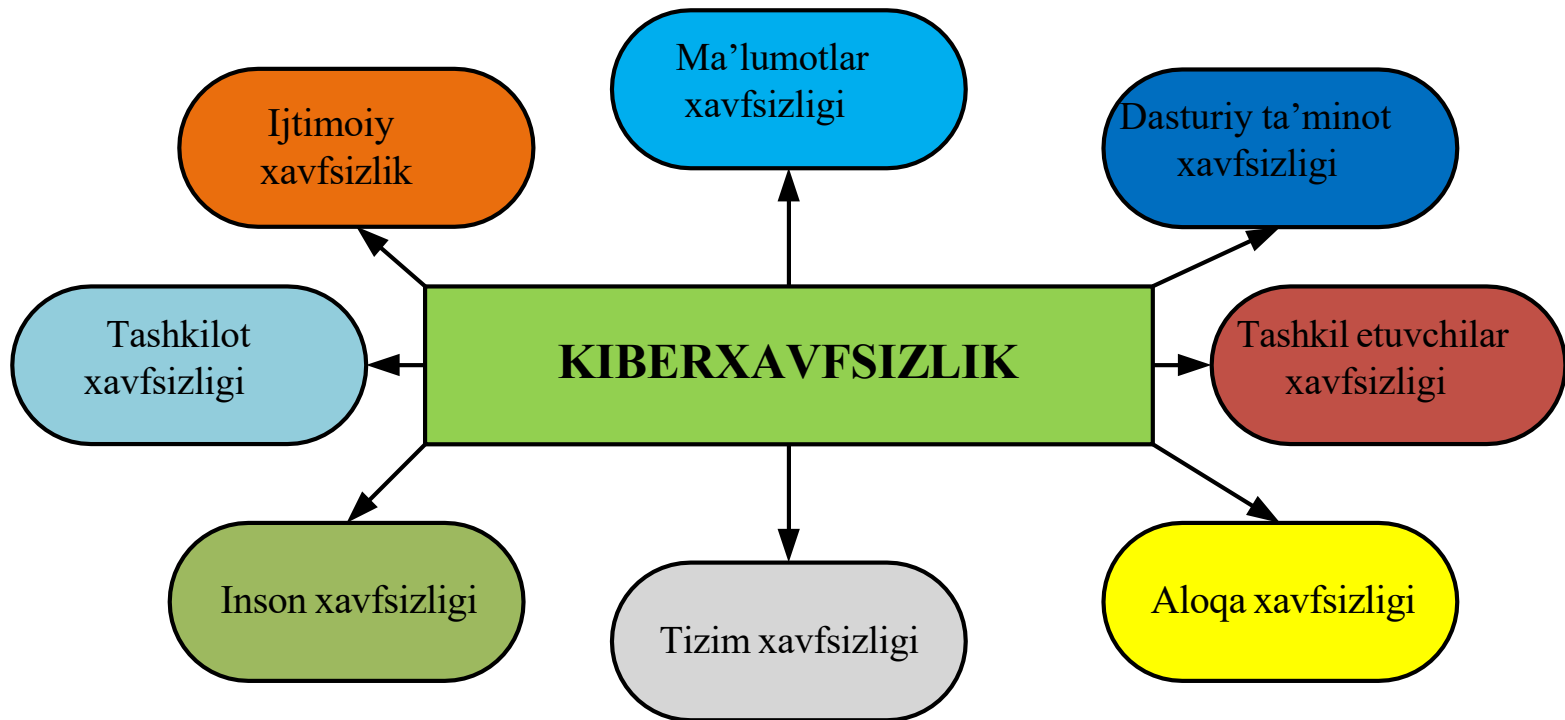
- Tridi umumiy ko‘rinishdagi “buzg‘unchi”
 - Qonuniy foydalanuvchi tizimini buzish (Butunlik, Foydalanuvchanlik)
 - Faqat Alisaga tegishli bo‘lgan axborotni o‘qish (Maxfiylik)

Axborot xavfsizligi VS kiberxavfsizlik



- *Axborot xavfsizligi* sohasi, axborotning ifodalanishidan qat'iy nazar (qog'oz ko'rinishidagi, elektron va insonlar fikrlashida, og'zaki va vizual) intellektual 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.

Kiberxavfsizlikning bilim sohalari



Kiberxavfsizlikning bilim sohalari

- “Ma’lumotlar xavfsizligi” bilim sohasi **ma’lumotlarni saqlashda, qayta ishlashda** va **uzatishda** himoyani ta’minlashni maqsad qiladi.
 - Mazkur bilim sohasi himoyani to‘liq amalga oshirish uchun **matematik** va **analitik algoritmlardan** foydalanishni talab etadi.
 - Ma’lumot *saqlangan, yuzatilish* va *ishlov berish* holatlarida bo‘lishi mumkin.
- “Dasturiy ta’minotlar xavfsizligi” bilim sohasi foydalanilayotgan tizim yoki axborot xavfsizligini ta’minlovchi **dasturiy ta’minotlarni ishlab chiqish** va **foydalanish jarayoniga** e’tibor qaratadi.

Kiberxavfsizlikning bilim sohalari

- “**Tashkil etuvchilar xavfsizligi**” bilim sohasi katta tizimlarda integrallashgan tashkil etuvchilarni **loyihalash, sotib olish, testlash, analiz qilish** va **texnik xizmat ko‘rsatishga** e’tibor qaratadi.
 - Tizim xavfsizligi tashkil etuvchilar xavfsizligidan farq qiladi.
 - Tashkil etuvchilar xavfsizligi ular *qanday loyihalanganligi, yaratilganligi, sotib olinganligi, boshqa tarkibiy qismlarga ulanganligi, qanday ishlatilganligi va saqlanganligiga* bog‘liq.
- “**Aloqa xavfsizligi**” bilim sohasi tashkil etuvchilar o‘rtasidagi **aloqani himoyalashga** etibor qaratib, o‘zida *fizik* va *mantiqiy* ulanishni birlashtiradi.

Kiberxavfsizlikning bilim sohalari

- “**Tizim xavfsizligi**” bilim sohasi **tashkil etuvchilar, ulanishlar** va **dasturiy ta’minotdan** iborat bo‘lgan tizim xavfsizligining aspektlariga e’tibor qaratadi.
 - Tizim xavfsizligini tushunish uchun nafaqat, *uning tarkibiy qismlari va ulanishini tushunishni*, balki *butunlikni* hisobga olishni talab qiladi.
- “**Inson xavfsizligi**” bilim sohasi *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.*

Kiberxavfsizlikning bilim sohalari

- “**Tashkilot xavfsizligi**” bilim sohasi tashkilotni *kiberxavfsizlik tahdidlaridan himoyalash* va *tashkilot vazifasini muvaffaqiyatli bajarishini* madadlash uchun risklarni boshqarishga e’tibor qaratadi.
- “**Jamoat xavfsizligi**” bilim sohasi u yoki bu darajada jamiyatda 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.

Kompyuter xavfsizligi muammosi

- **Ko‘plab bag mavjud dasturlar** (va ishonuvchan foydalanuvchlar)
- **Sosial injineriya** (maxfiy ma’lumotlarni oshkor qilishda xodimlardan foydalanish)
- **Boshqa tizimlar orqali buzib kirish**
- **Fizik nazoratlash**

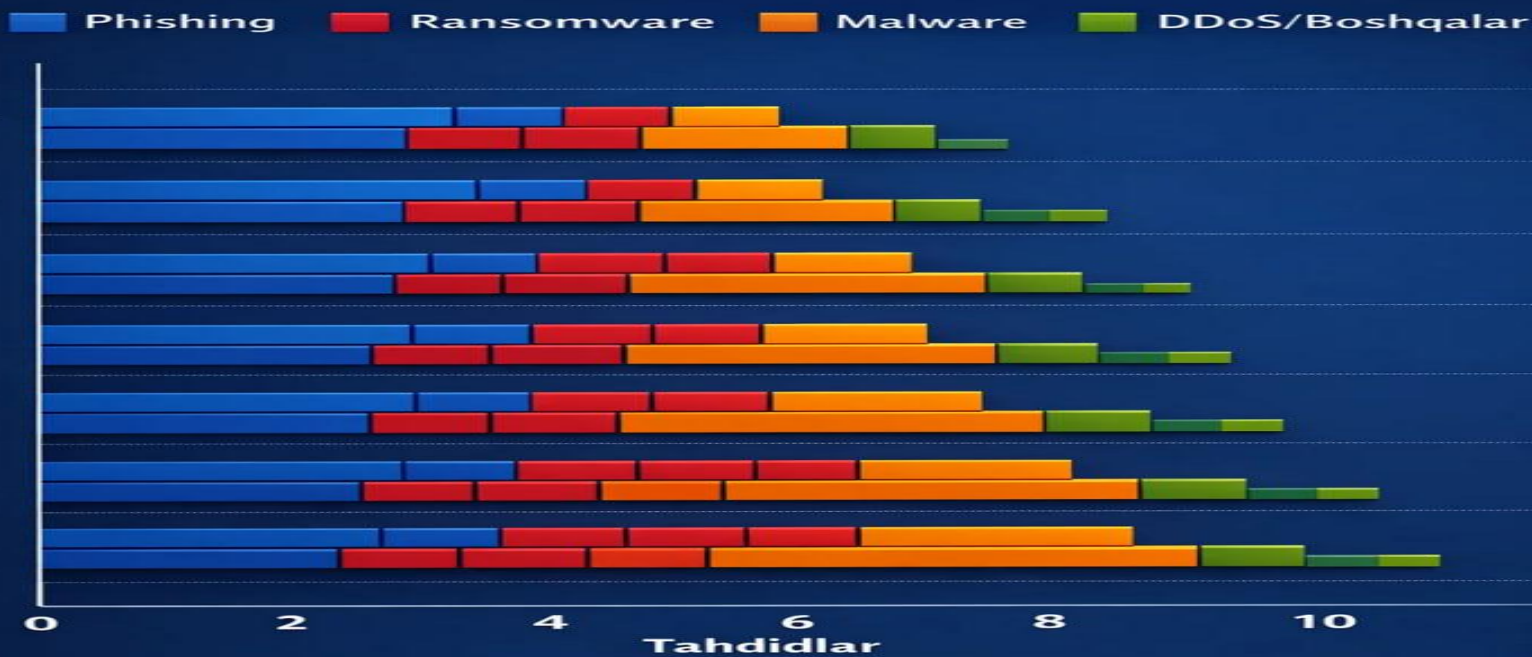
Motivatsiyalar

- Harbiy
- Terrorizm
- Foyda (masalan, pul, imtiyoz va hak.)

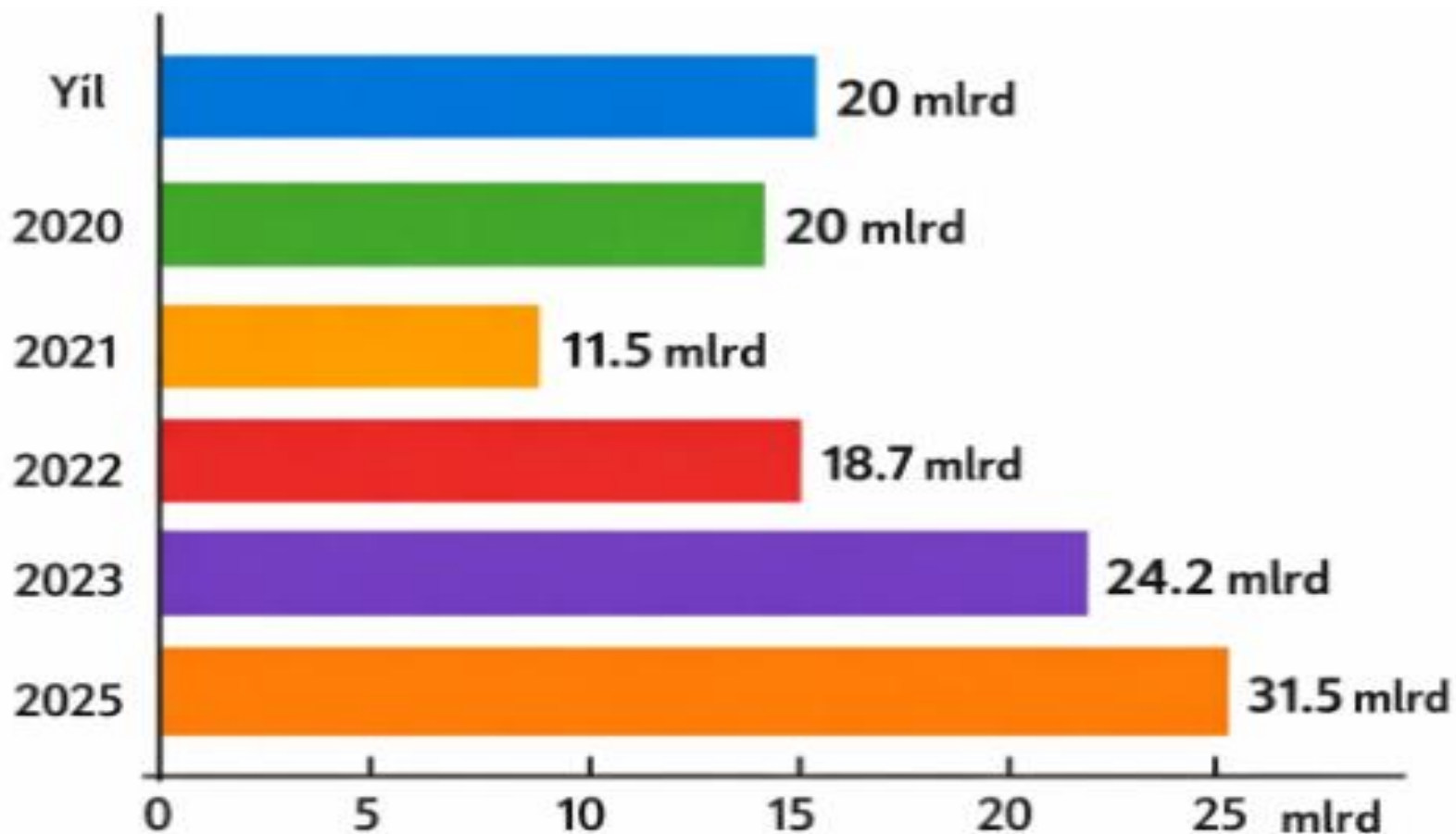
Kiberxavfsizlikka oid ba'zi statistik ma'lumotlar

https://electroiq.com/stats/cyber-security-statistics/?utm_source=chatgpt.com
Manbalariga

Kiber Tahdidlar Statistikasi

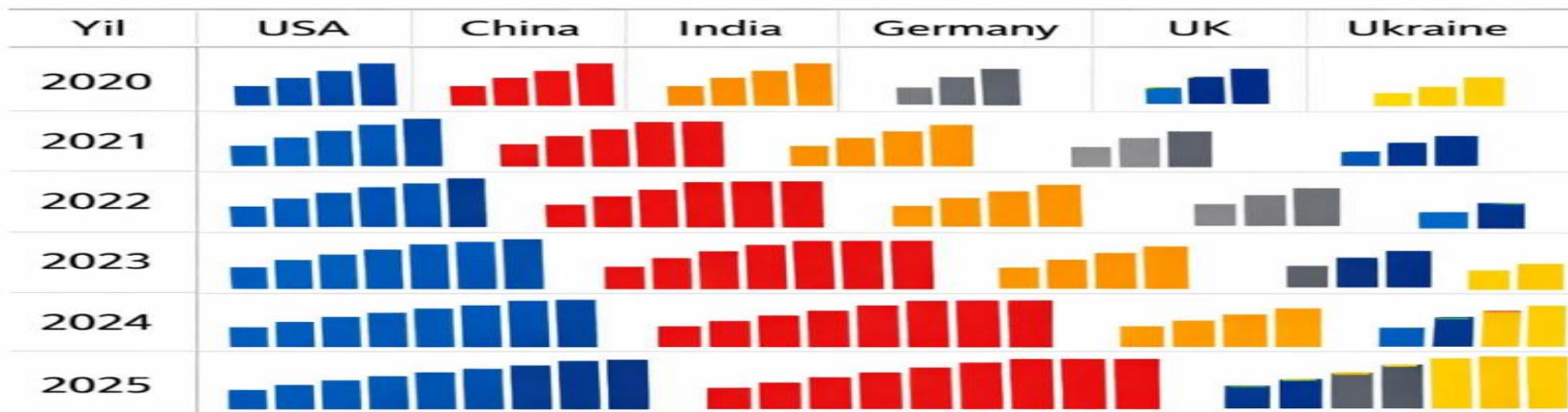


https://electroiq.com/stats/cyber-security-statistics/?utm_source=chatgpt.com
Manbalariga ko'ra ko'rilgan zararlar miqdori



https://electroiq.com/stats/cyber-security-statistics/?utm_source=chatgpt.com

Manbalariga ko'ra ko'p zarar ko'r davlatlar



https://electroiq.com/stats/cyber-security-statistics/?utm_source=chatgpt.com
Manbalariga ko'ra ko'p zarar ko'rgan sohalar

Sohalar Hujumlar ko'pi (2020–2025)



Sabablar

Sohalar	Eng ko'p uchragan hujum turi	Sabablari (izoh)
Moliyaviy xizmatlar (Banklar, FinTech)	Ransomware, Phishing	Pul va moliyaviy maqsadlar; onlayn banking ko'paydi; phishing orqali login/parollar o'g'rilanadi
Sog'liqni saqlash (Hospitals, Clinics)	Ransomware, Data Breach	Shaxsiy ma'lumotlar qimmat; eskirgan IT tizimlar; COVID-19 davrida onlayn tizimlar tezlashdi
Davlat idoralari va hukumat tizimlari	Malware, DDoS	Siyosiy/strategik ma'lumotlar mavjud; geosiyosiy ziddiyatlar; davlat xizmatlarini bloklash mumkin
Energetika va infratuzilma	Malware, Phishing	Milliy xavfsizlik bilan bog'liq; SCADA tizimlar internetga ulangan; strategik nishon
Ta'lim sohasi (Universitetlar, Online Learning)	Phishing, Malware	Talabalar va o'qituvchilarning shaxsiy ma'lumotlari; pandemiya davrida onlayn tizimlar tez joriy etildi
Savdo va E-commerce	Phishing, Ransomware	Bank karta ma'lumotlari mavjud; yuqori trafik → hujumni yashirish oson; soxta saytlar tez tarqaladi
IT va texnologiya kompaniyalari	Malware, Ransomware	Boshqa kompaniyalar uchun zanjirli nishon; server va kod bazalari mavjud; murakkab tizimlar

Kiberxavfsizlikka oid ba'zi statistik ma'lumotlar

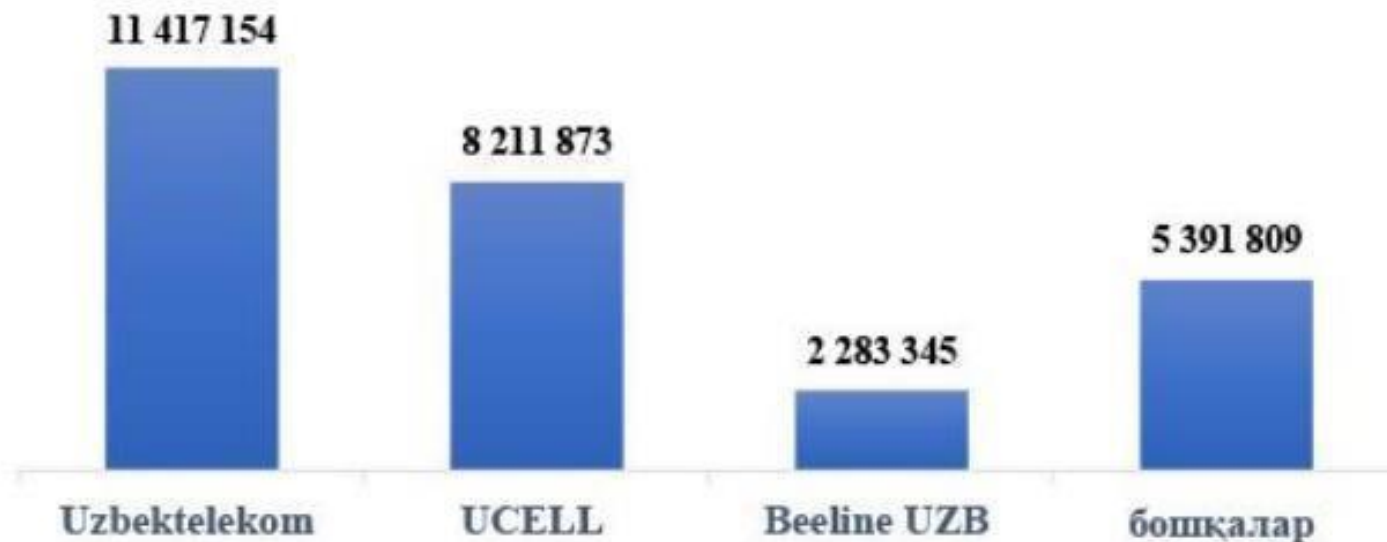
[Kiberxavfsizlik markazi ma'lumotlari]



(1 – Расм: Кузатилган таҳдидларнинг асосий салмоғи)

Kiberxavfsizlikka oid ba'zi statistik ma'lumotlar

[Kiberxavfsizlik markazi ma'lumotlari]



(2 – Расм: Тахдидларнинг асосий қисми кузатилган компаниялар)

Nazorat savollari

1. Axborot xavfsizligi tushunchasi nima va uning kiberxavfsizlik bilan bog‘liqligi qanday?
2. Konfidensiallik, yaxlitlik va foydalanuvchanlik (CIA triada) tushunchalarini tushuntiring va har birining amaliy ahamiyatini misollar bilan izohlang.
3. Kiberxavfsizlikdagi “risk” va “tahdid” tushunchalarini qanday farqlash mumkin?
4. Xujumchi (attacker) va zaiflik (vulnerability) tushunchalarini tushuntiring va ularni aniqlashning ahamiyati haqida misol keltiring.
5. Axborot xavfsizligini boshqarish vositalari (security controls) qanday turlarga bo‘linadi va ularning vazifasi nima?
6. Kiberxavfsizlikning bilim sohalari nimalardan iborat va ularning har biri tashkilot xavfsizligiga qanday hissa qo‘shadi?
7. Aktiv (asset) tushunchasi nima va uning himoyalaniishi kiberxavfsizlik tizimida qanday rol o‘ynaydi?

**E'TIBORINGIZ UCHUN
RAXMAT!!!**