“KIBERXAVFSIZLIK MARKAZI”
DAVLAT UNITAR KORXONASI

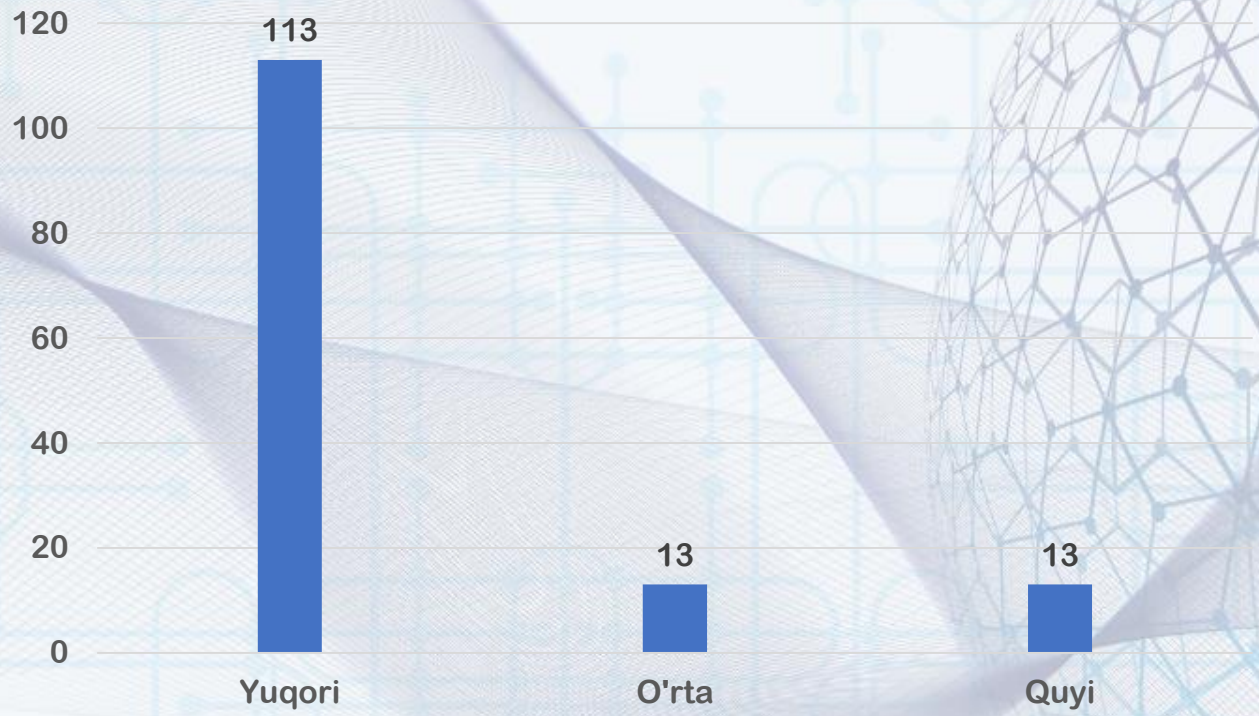
CYBER SECURITY CENTER

2023

I - chorak yakunlari

Veb-saytlar ekspertizasi

Davlat va xo'jalik boshqaruvi organlari, mahalliy davlat hokimiyati organlarining rasmiy veb-saytlarini axborot xavfsizligi talablariga asosan ekspertizadan o'tkazish bo'yicha hisobot davrida 30 ta tashkilotning veb-sayti ekspertizadan o'tkazildi. Ekspertizalar davomida umumiy 131 ta zaiflik aniqlandi. Ulardan:



1-rasm. Veb-saytlar ekspertizasi natijalari

Kiberxavfsizlik insidentlarini tekshirish

Zararli kontentni aniqlash va uning axborot makonidagi huquqbuzarliklarga aloqadorligini tahlil qilish doirasida kiberxavfsizlik insidentlari tekshirilib, ularni amalga oshirish sabablari va usullari aniqlandi.
".UZ" domen zonasidagi veb-saytlarga muvaffaqiyatli hujumlarning asosiy sabablari quyidagilar:

- veb-saytlar ishlashida zaiflik mavjud bo'lgan plaginlar va dasturiy ta'minot (CMS, mavzu shablonlari, kutubxonalar va boshqalar)dan foydalanish. Xususan, aksariyat hollarda pochta xizmatlari va masofaviy ulanish modullarida kritik darajadagi zaifliklar aniqlandi (**56%**);

- veb-saytlar ishida qo'llanilmaydigan dasturiy vositalarning, shu jumladan, ishonchli bo'lmagan manbalardan yuklab olingan fayllarining ortiqchaligi (**12%**);

- parol siyosatiga amal qilinmaslik (**7%**);

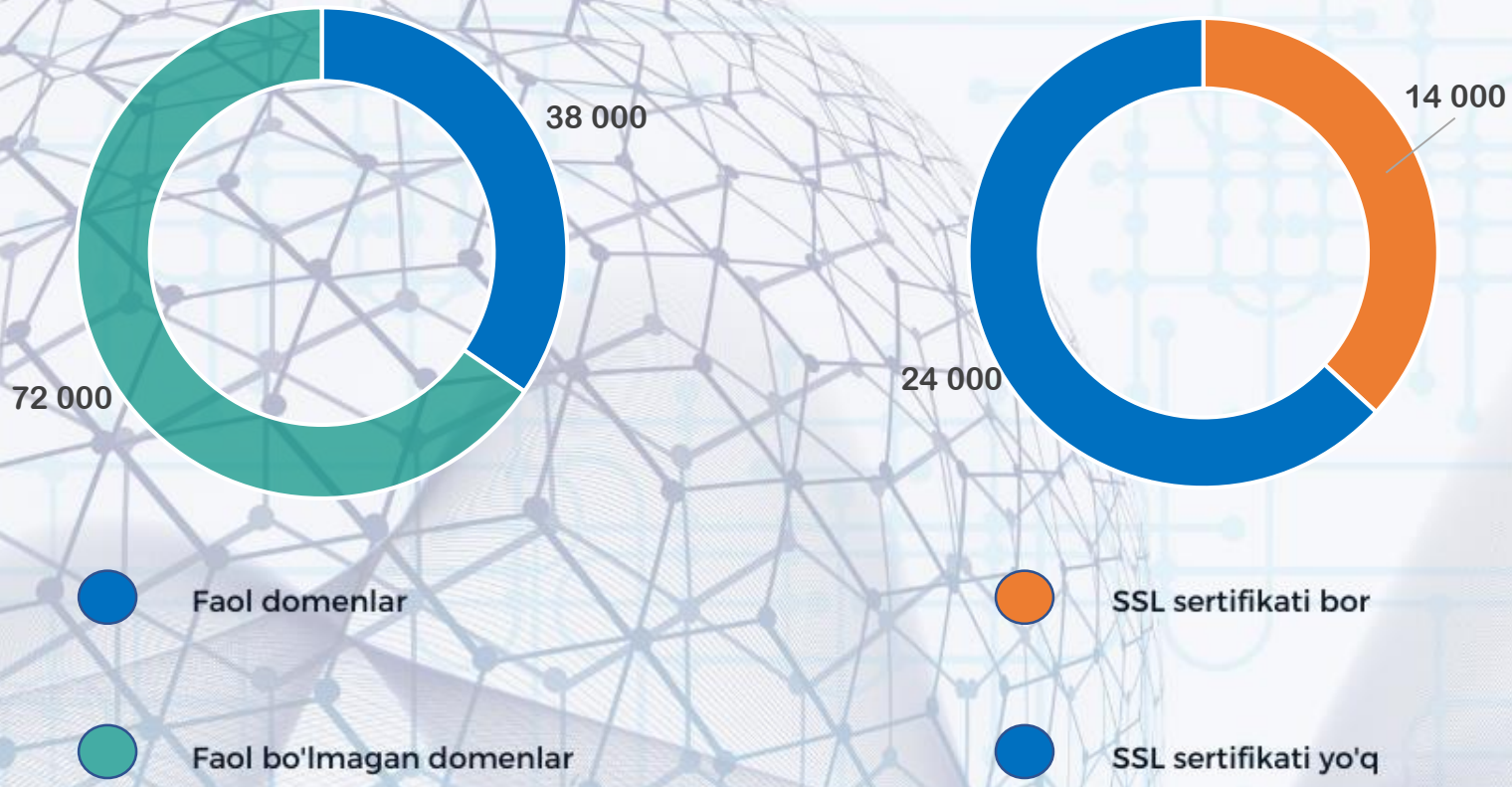
- veb-sayt fayl qismiga yuklanadigan fayllarga cheklov (filtr) qo'ymaslik (**25%**).

Xususan, tekshiruvlar natijasida axborot tizimlari va resurslari, shuningdek, ulardan foydalanuvchilarning kiberxavfsizligiga tahdid solishi mumkin bo'lgan **70 ta** zararli fayl va skriptlar aniqlandi.

Zaifliklar

2023 yil I choragi davomida Davlat va xo'jalik boshqaruvi organlari, shuningdek xususiy sektor vakillarining **6** ta axborot tizimini axborot va kiberxavfsizlik talablariga muvofiqligi yuzasidan ekspertizadan o'tkazildi.
O'tkazilgan ekspertizalar natijasida jami **5** ta yuqori darajadagi axborot xavfsizligi kamchiligi aniqlandi.
Yuqoridagi zaifliklarning kiberhujumchilar tomonidan foydalanishi natijasida, axborot resurslarining yaxlitligi va ulardan foydalanishning buzilishiga, shu jumladan, O'zbekiston Respublikasi fuqarolarining shaxsiy ma'lumotlarining sizib chiqib ketishiga olib kelishi mumkin edi.

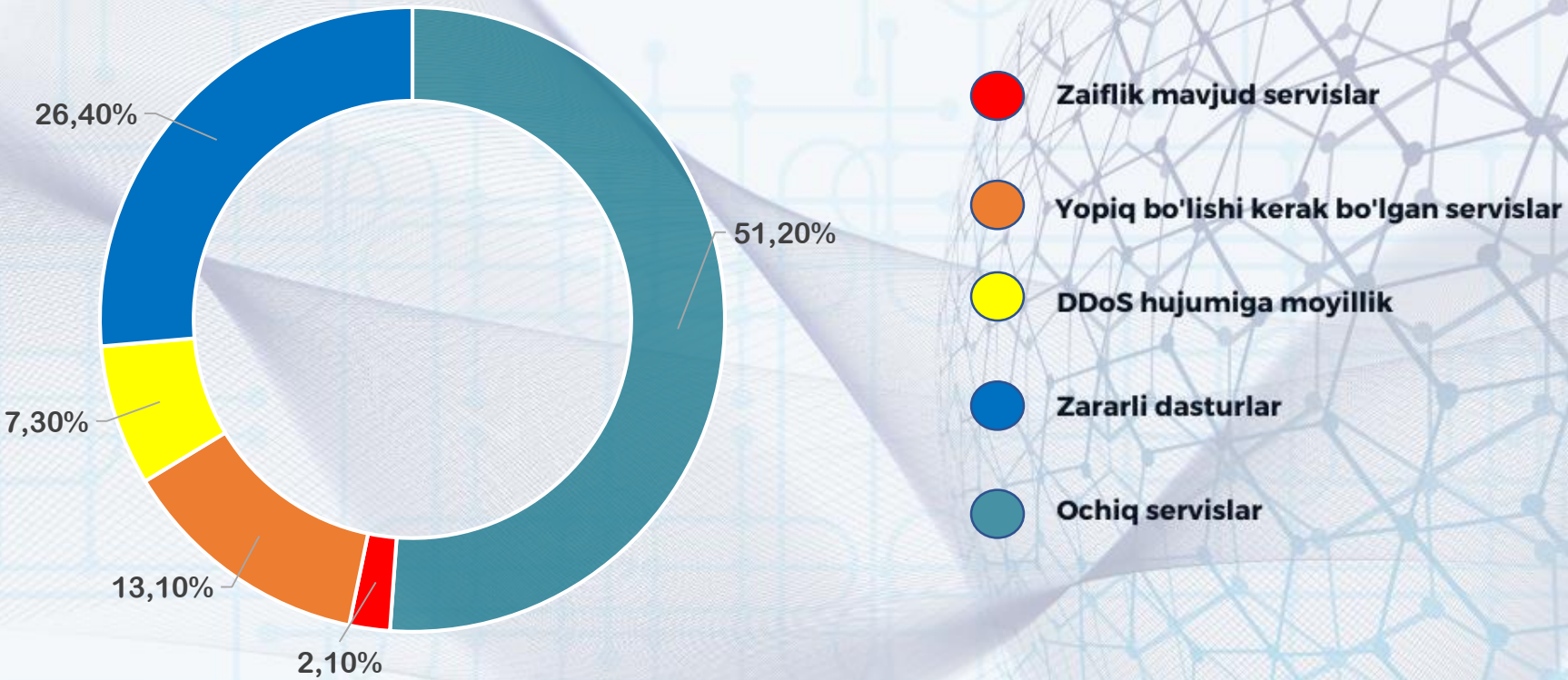
2023-yil I choragi holatiga ko'ra, O'zbekiston Respublikasining internet tarmog'i ".UZ" segmentida **110 000** dan ortiq veb-sayt domenlari ulangan bo'lib, shulardan **38 000** dan ortig'i faol domenlardir. Ularning **14 000** dan ortig'i xavfsiz ya'ni SSL sertifikati bilan himoyalangan domenlar (1-rasm).



2-rasm. Domenlar hamda ularda SSL sertifikatining mavjudligi yuzasidan ma'lumot.

Threat Intellegence monitoring tizimi

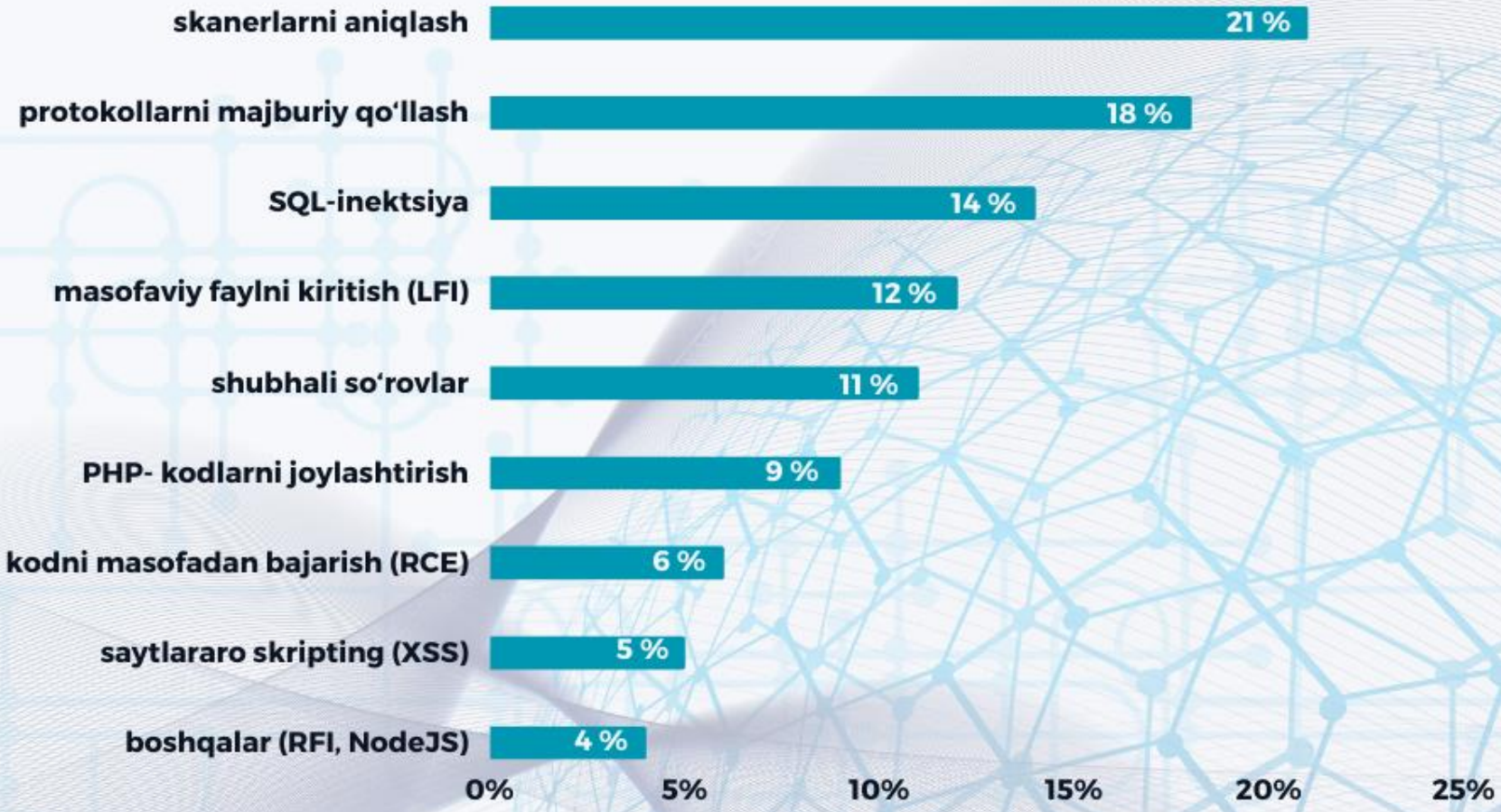
Shuningdek, milliy kibermakonda zararli tarmoq faoliyati bilan bog'lik **1 650 000** kibertahdidlar aniqlandi. Ularni quyidagi kesimda turlarga ajratish mumkin (2-rasm).



3-rasm. Aniqlangan kibertahdidlarning asosiy turlari.

WAF monitoring tizimi.

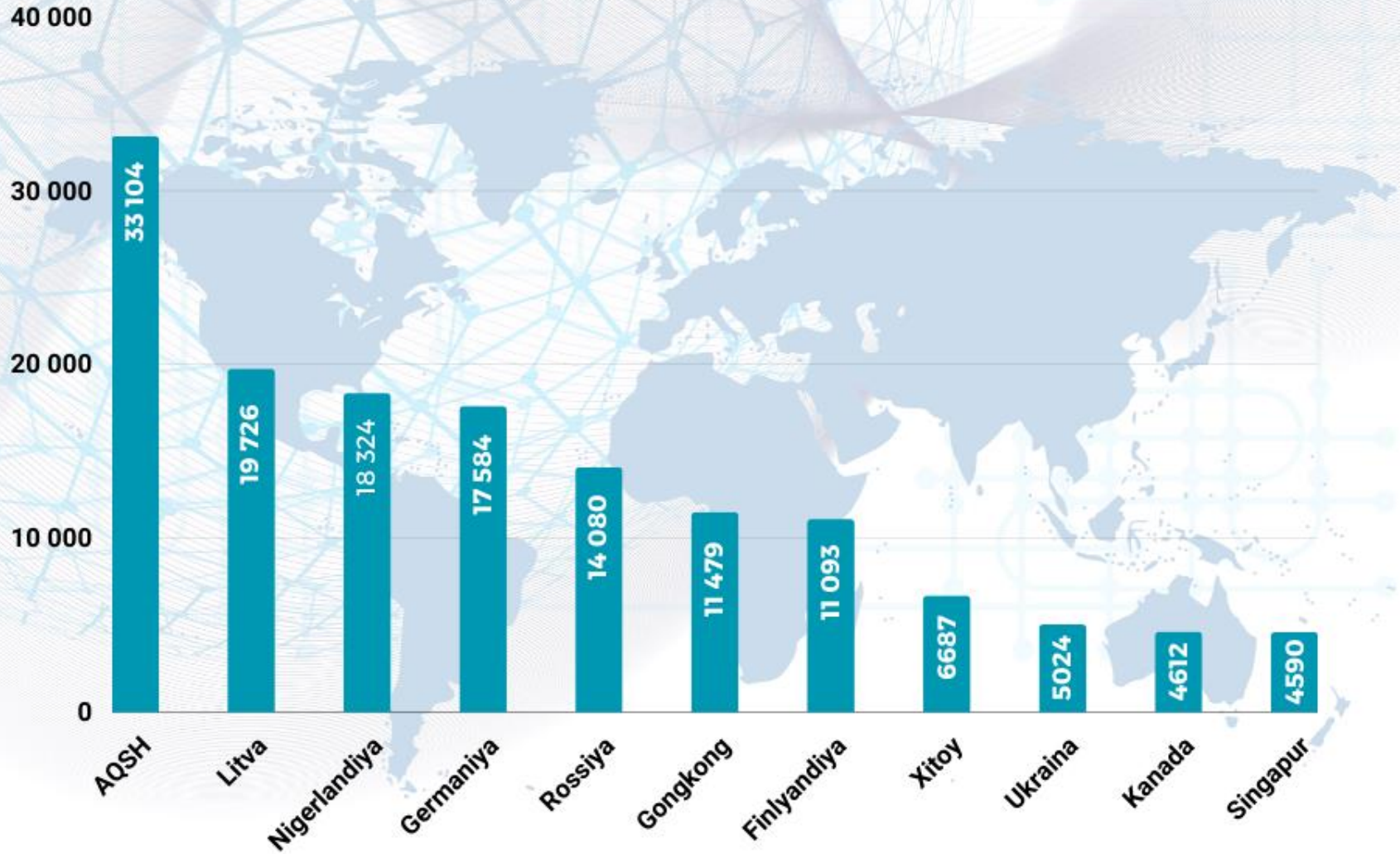
Markaz tomonidan Yagona kiberxavfsizlik uzeli doirasida davlat organlari va tashkilotlari veb-resurslarini himoya qilish (Web Application Firewall) tizimi sinov tariqasida ishga tushirilgan bo'lib, hozirgi kunda mazkur tizimga **36** ta davlat organi va tashkilotlarining **39** ta veb-resurslari ulangan.



4-rasm. Aniqlangan va bloklangan kiberhujumlar.

WAF monitoring tizimi.

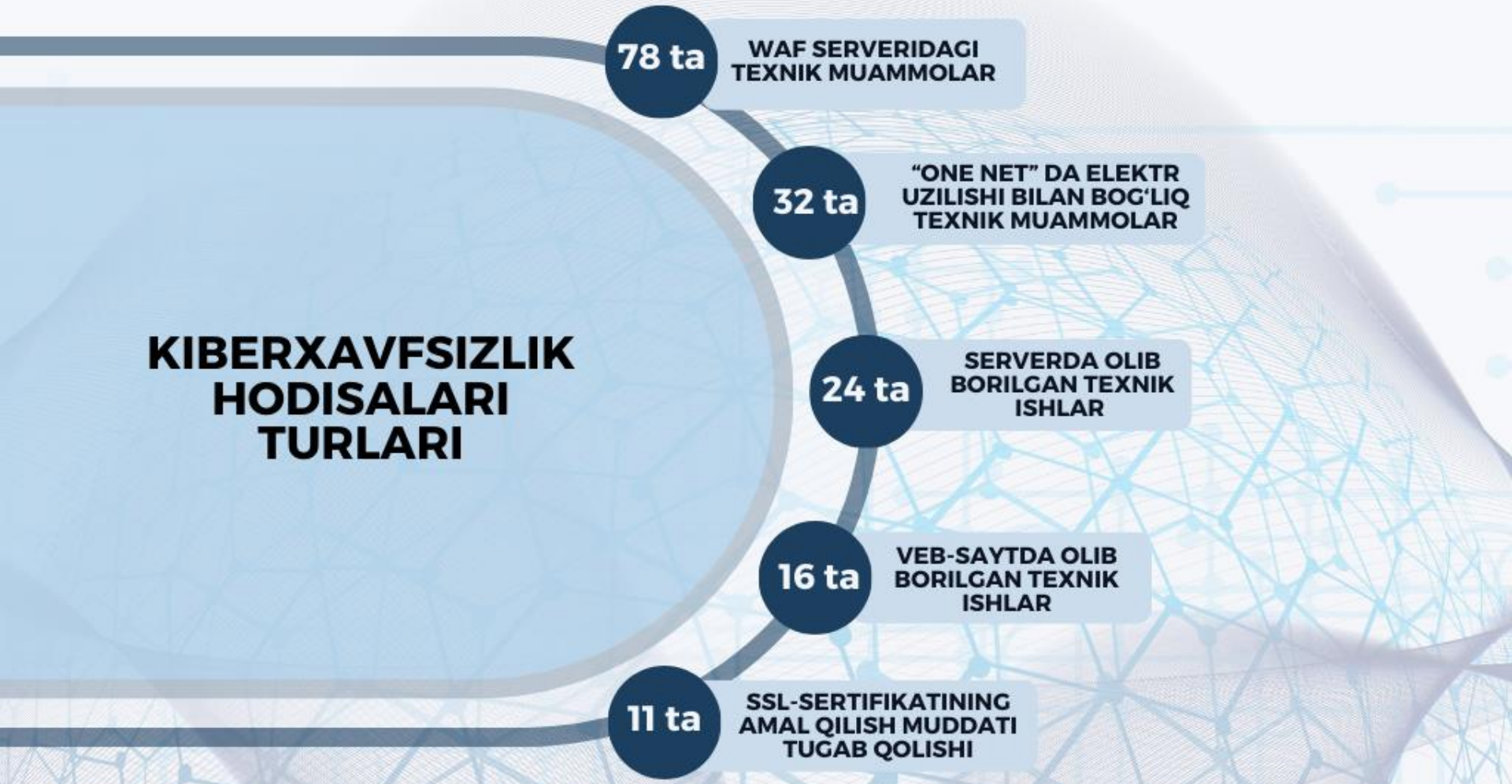
Aniqlangan va bloklangan kiberhujumlarning asosiy qismi AQSH, Litva, Niderlandiya va boshqa davlatlar hududidan amalga oshirilgan (4-rasm).



5-rasm. Kiberhujumlar amalga oshirilgan davlatlar.

Insidentlar va hodisalar

Internet tarmog‘ining milliy segmentida joylashgan davlat va xo‘jalik boshqaruvi organlarining rasmiy veb-saytlarida **249** ta hodisa aniqlangan bo‘lib, buning natijasida davlat idoralarining veb-saytlari umumiy hisobda **417 285** daqiqa davomida ishdan chiqishiga olib kelgan (5-rasm).



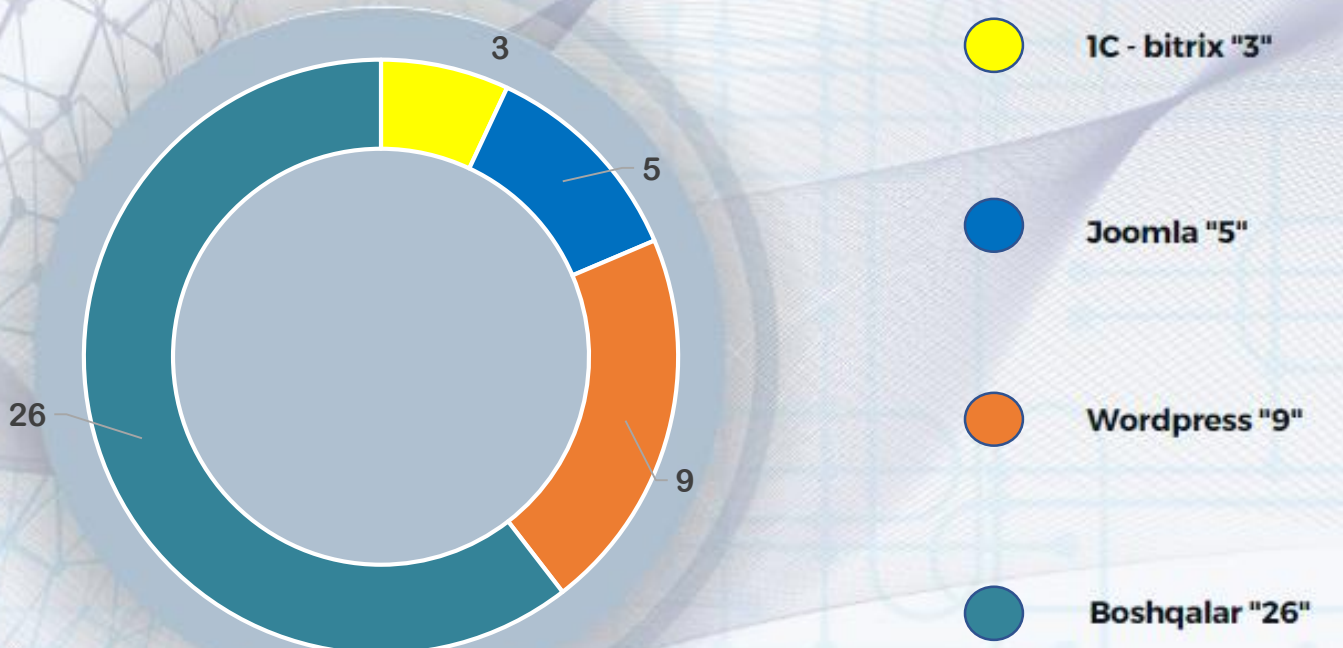
6-rasm. Aniqlangan hodisalar asosiy turlari.

Insidentlar

".UZ" domen zonasidagi veb-saytlarning uzluksiz monitoringi davomida **48** ta kiberxavfsizlik insidenti aniqlanib, ularning asosiy qismi ruxsatsiz kontent yuklash (**21** ta) hamda asosiy oynani ruxsatsiz o'zgartirish (**13** ta) bilan bog'liq bo'lgan insidentlardir.

Aniqlangan insidentlarning tahlili shuni ko'rsatmoqdaki, davlat idoralarining veb-saytlari (11 ta), xususiy sektor vakillarining veb-saytlari (**31** ta) dan ko'ra, **3** barobar kamroq hujumlarga uchragan.

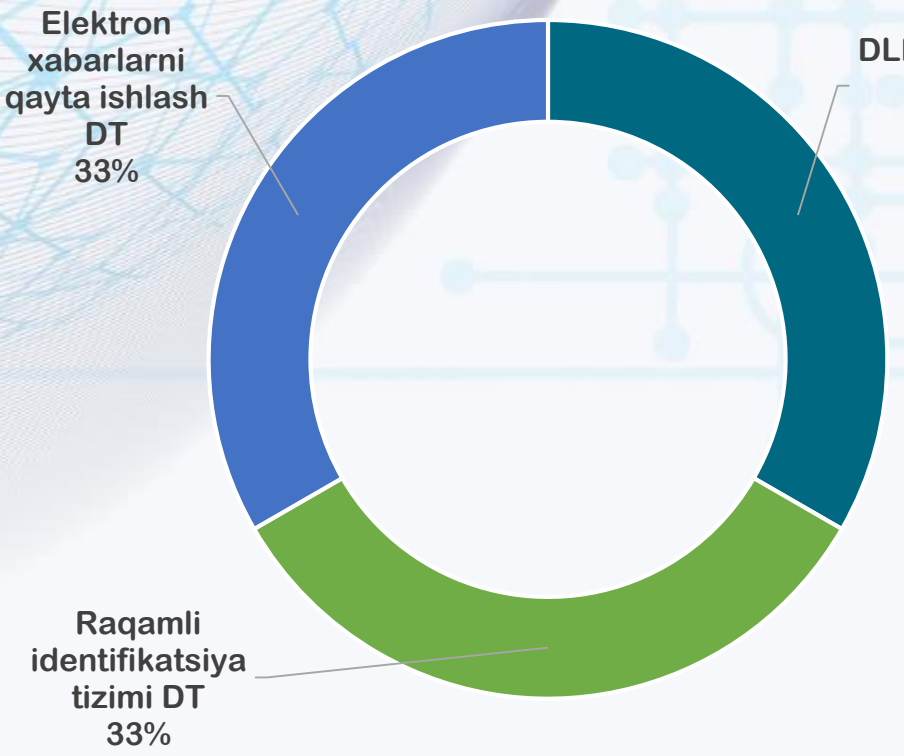
Shuningdek, tahlillar davomida, eng ko'p kiberhujumlarga uchragan (zaif bo'lgan) veb-saytlar, "**1C-bitrix**", "**Joomla**", "**WordPress**" va boshqa kontentni boshqarish tizimlarida ishlab chiqilgani aniqlandi (7-rasm).



7-rasm. Aniqlangan insidentlar (kontentni boshqarish tizimlari kesimida).

Sertifikatlashtirish

Kiberxavfsizlikni ta'minlash yo'nalishida foydalaniladigan apparat, dasturiy, dasturiy-apparat vositalarining normativ hujjatlarda belgilangan talablarga muvofiqligini tasdiqlash maqsadida xorijiy va mahalliy ishlab chiqaruvchilarning **3** ta dasturiy mahsuloti, jumladan, tarmoqlararo ekran, elektron xabarlarni qayta ishlash tizimi hamda ma'lumotlarning sizib chiqishidan himoyalash (DLP) vositasining dasturiy ta'minotlariga muvofiqlik sertifikatlari berildi (8-rasm).



8-rasm. Dasturiy vositalar sertifikatsiyasi.

Markaz tomonidan 2023-yil I choragi davomida profilaktika ishlari va kibertahdidlarni oldini olish maqsadida “UZ” domen zonasida joylashgan veb-saytlarda 124 ta zaiflik aniqlandi, shulardan 76 tasi davlat tashkilotlariga tegishli veb resurslar. Aniqlangan zaifliklar to‘g‘risida barcha veb-resurs egalari xabardor qilingan.

Lekin qayta monitoring qilish jarayonida 46 ta veb-saytlarda zaifliklar bartaraf etilmaganligi aniqlandi.

Ushbu zaifliklar veb-serverda joylashgan yashirilgan, konfidensial hamda “config” fayllarni ko‘rish va ulardan foydalanishga shuningdek serverga zararli fayl yuklash, personal yoki konfidensial malumotlar saqlanayotgan fayllarni ko‘rish, yuklab olish, parollar, kredit karta va foydalanuvchining shaxsiy ma’lumotlari kabi ma’lumotlarga ruxsatsiz kirish, ma’lumotlar bazasida saqlanayotgan ma’lumotlarni ko‘rish, ular ustida amallar bajarish va hattoki o‘chirib yuborish, veb-sahifaga rasm, matn, URL manzillarni yuklash, “cookie” larda saqlanayotgan qimmatli (login, parol va h.k.) hamda veb-sahifa maydonlariga kiritilgan ma’lumotlarni o‘g‘irlanish, shuningdek, zaifligi bor veb-saytlar orqali boshqa veb-saytlarga DoS hujumini amalga oshirish kabi holatlarga olib kelishi mumkinligini inobatga olib tashkilotlarga chiqarilgan barcha taklif va tavsiyalarning ijrosi bajarilgan taqdirda “UZ” domen zonasida joylashgan veb-resurslarga kibertahdidlarning maksimal darajada oldi olinadi.

O’zbekiston Respublikasi,
Toshkent sh. T.Shevchenko 20.

Telefon: (99871) 203 55 11

E-mail : info@csec.uz,
Veb-sayt: www.csec.uz