“KIBERXAVFSIZLIK MARKAZI”
DAVLAT UNITAR KORXONASI

2022

YIL YAKUNLARI

Mundarija

Kirish

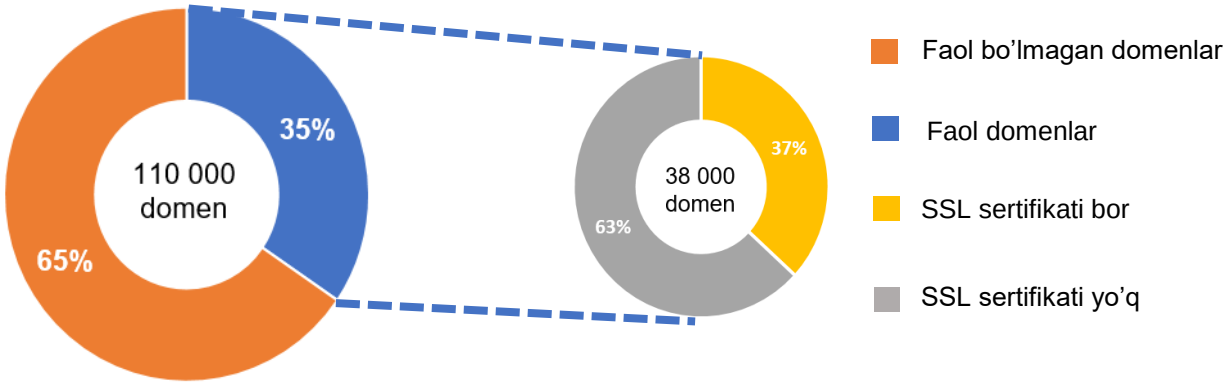
Dunyo miqyosida jadal sur’atlarda rivojlanib borayotgan axborot texnologiyalarining muhim o’rni, ishtirokini bugun hayotimizning har bir jabhasida ko’rish mumkin. Aytish joizki, mamlakatimizning har bir fuqarosi bevosita yoki bilvosita axborot-aloqa texnologiyalarining faol foydalanuvchisi hisoblanadi. Yil sayin elektron resurslar axborot foydalanuvchilarining asosiy manbasi bo’lib bormoqda. Internet resurslari va foydalanuvchilari soni oshib borishi aholi manfaatlari, yoshlar ta’lim-tarbiyasi, intellektual salohiyatining yuksalishida xizmat qilib kelmoqda.

Shuningdek, horijiy investorlarning mamlakatimizning ijtimoiy-siyosiy va iqtisodiy hayotining barcha jabhalariga oid ochiq ob’ektiv va keng qamrovli ma’lumotlar olishga bo’lgan ehtiyojlarini qondirishda milliy kibermakonda faoliyat olib borayotgan rasmiy axborot manbalari va resurslarining salmoq va sifat jihatidan to’laqonli ishlashiga bo’lgan talabning tobora ortib borayotganligini ko’rsatmoqda.

Ushbu jarayon o’z o’rnida Internet tarmog’ining “.UZ” milliy domen zonasida ro’yhatdan o’tgan mamlakatimiz xalq xo’jaligining turli sohalarida faoliyat olib borayotgan davlat boshqaruvi organlari va xo’jalik yurituvchi tashkilotlarining axborot infratuzilmasida vujudga kelishi mumkin bo’lgan kiberxavfsizlikka oid zamonaviy xavf-xatarlar hamda zaifliklarni aniqlash va bartaraf etish bilan birgalikda, tegishli davlat organi va xo’jalik sub’ektlari haqidagi ma’lumotlar manbai bo’lgan Internet tarmog’idagi ularning rasmiy veb-saytlarining uzluksiz, barqaror va shu bilan birga axborot istemolchilarining talab darajasida ishlashini ta’minlash masalalarini yanada dolzarblashtirdi.

Tahdidlar

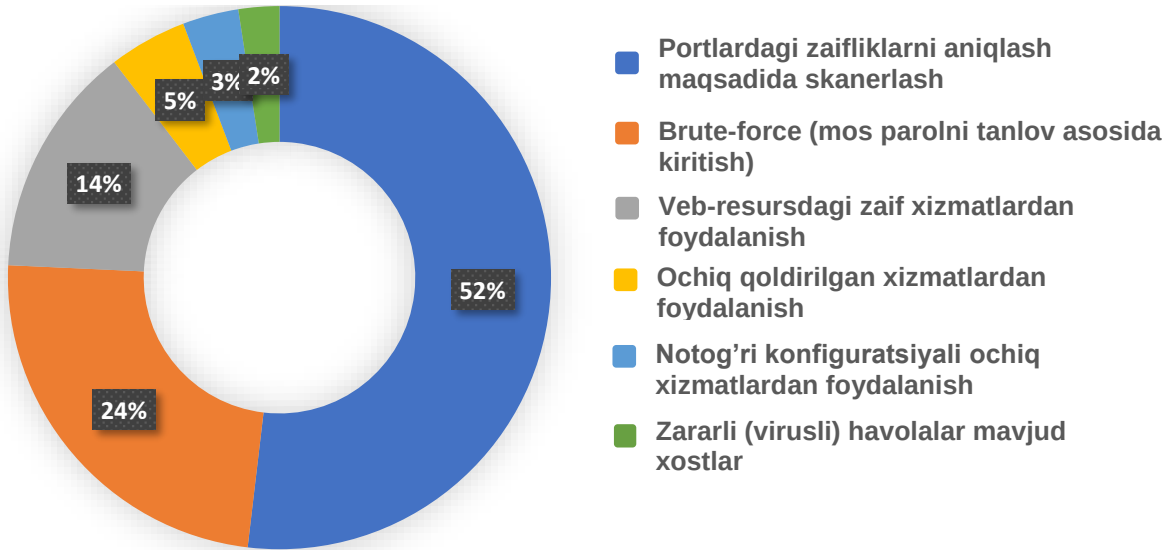
2022-yil holatiga ko‘ra, O‘zbekiston Respublikasining internet tarmog’i “.UZ” segmentida 110 000 dan ortiq veb-sayt domenlari ulangan bo‘lib, shulardan 38 000 dan ortig‘i faol domenlardir. Ularning 14 000 dan ortig‘i xavfsiz ya’ni SSL sertifikati bilan himoyalangan domenlar (1-rasm).



1-rasm. Domenlar hamda ularda SSL sertifikatining mavjudligi yuzasidan ma’lumot.

Shuningdek, milliy kibermakonda zararli tarmoq faoliyati bilan bog‘lik 65 million hodisa aniqlandi.

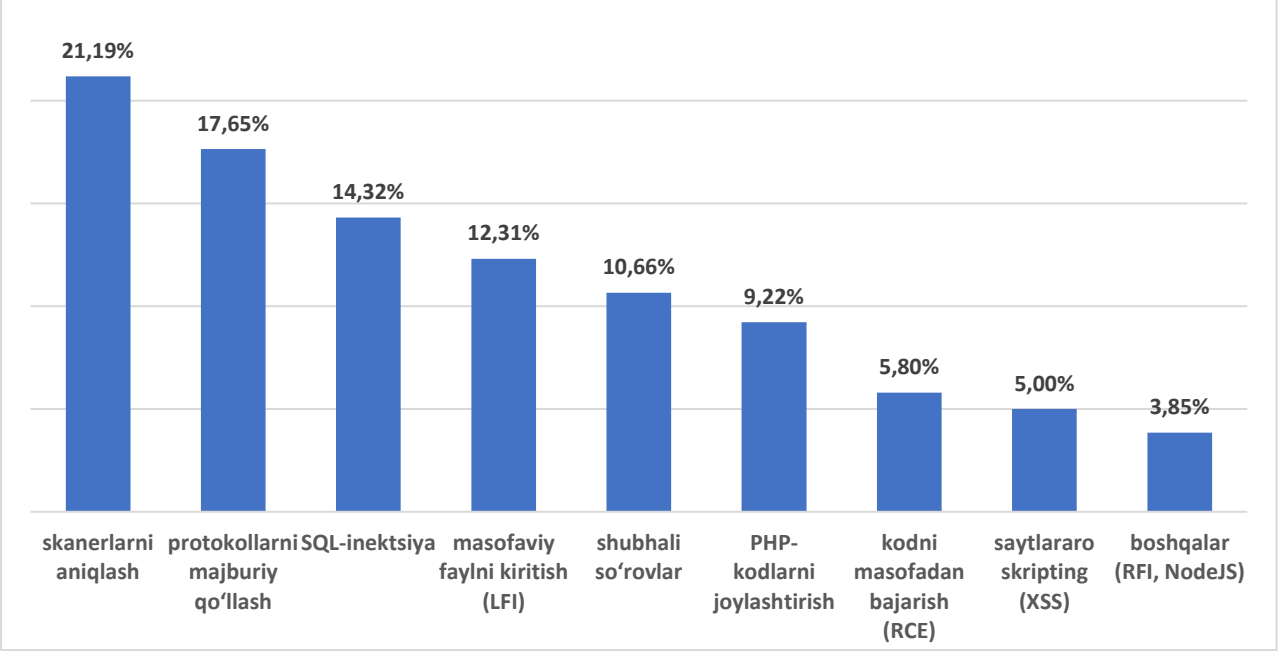
Ularni quyidagi kesimda turlarga ajratish mumkin (2-rasm).



2-rasm. Aniqlangan kibertahdidlarning asosiy turlari.

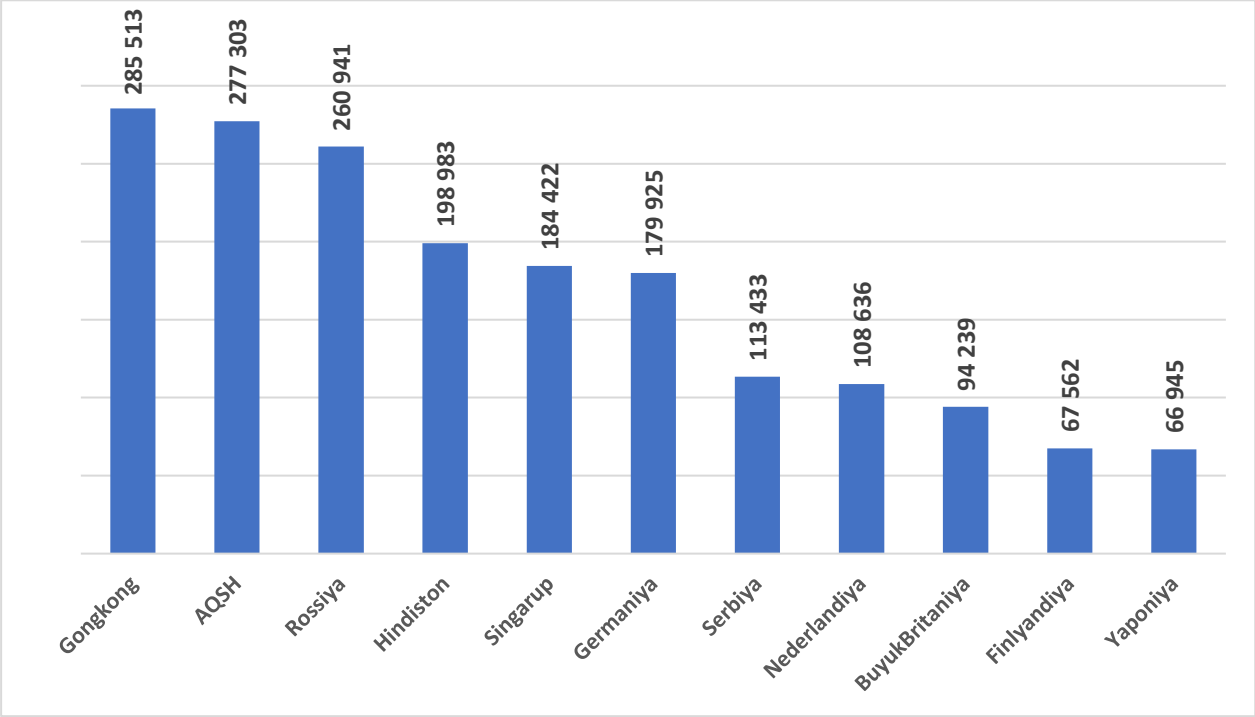
Bundan tashqari, Markaz tomonidan Yagona kiberxavfsizlik uzeli doirasida davlat organlari va tashkilotlari veb-resurslarini himoya qilish (Web Application Firewall) tizimi sinov tariqasida ishga tushirilgan bo’lib, hozirgi kunda mazkur tizimga 36 ta davlat organlari va tashkilotlarining 39 ta veb-resurslari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

Ushbu tizim orqali 50 dan ortiq xorijiy mamlakatlar hududlaridan amalga oshirilgan 4 510 318 ta kiberxavfsizlik tahdidlari aniqlangan va bartaraf etilgan (3-rasm).



3-rasm. Aniqlangan va bloklangan kiberhujumlar.

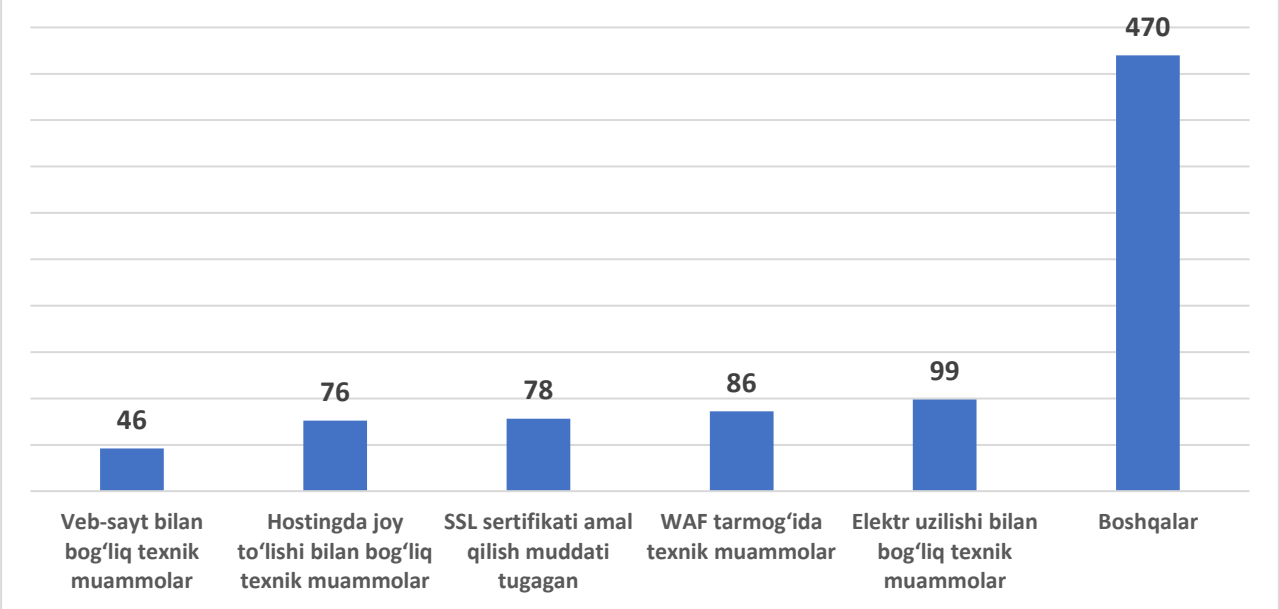
Aniqlangan va bloklangan kiberhujumlarning asosiy qismi Gongkong, AQSH, Rossiya, Hindiston va boshqa davlatlar hududidan amalga oshirilgan (4-rasm).



4-rasm. Kiberhujumlar amalga oshirilgan davlatlar

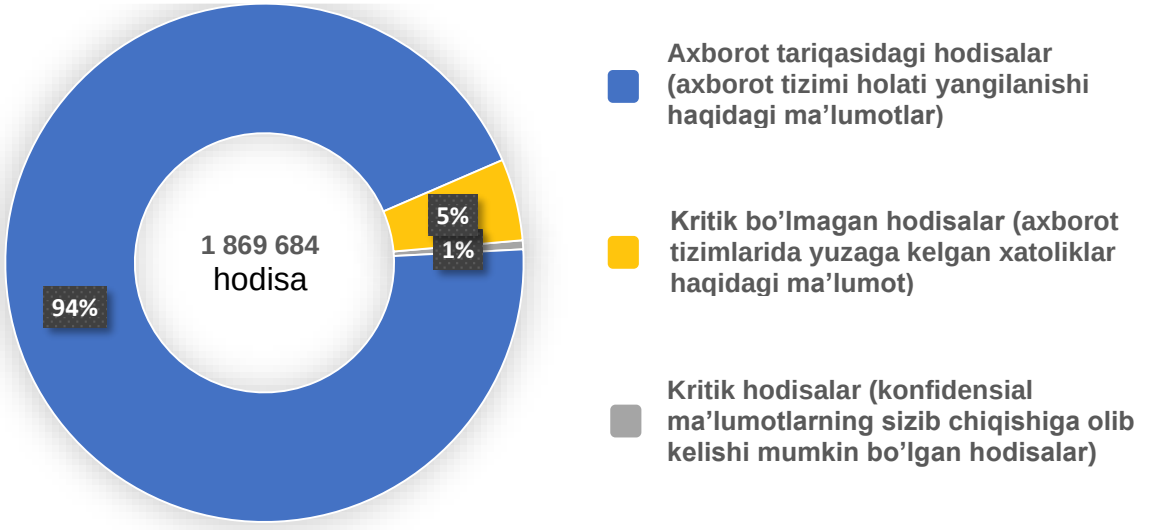
Insidentlar va hodisalar

Internet tarmog‘ining milliy segmentida joylashgan davlat va xo‘jalik boshqaruvi organlarining rasmiy veb-saytlarida **855 ta** hodisa aniqlangan bo‘lib, buning natijasida davlat idoralarining veb-saytlari umumiy hisobda **1 570 659** daqiqa davomida ishdan chiqishiga olib kelgan (5-rasm).



5-rasm. Aniqlangan xodisalar asosiy turlari.

Idoralararo ma’lumot uzatish tarmog’iga ulangan davlat idoralarining axborot tizimlari va resurslarining uzluksiz monitoringi davomida umumiy **1 869 684** xavfsizlik hodisalari aniqlanib, ulardan **9 709** tasida konfidensial ma’lumotga ruxsatsiz kirish hamda ularning sizib chiqishiga olib kelishi mumkin bo’lgan hodisalardir (6-rasm).

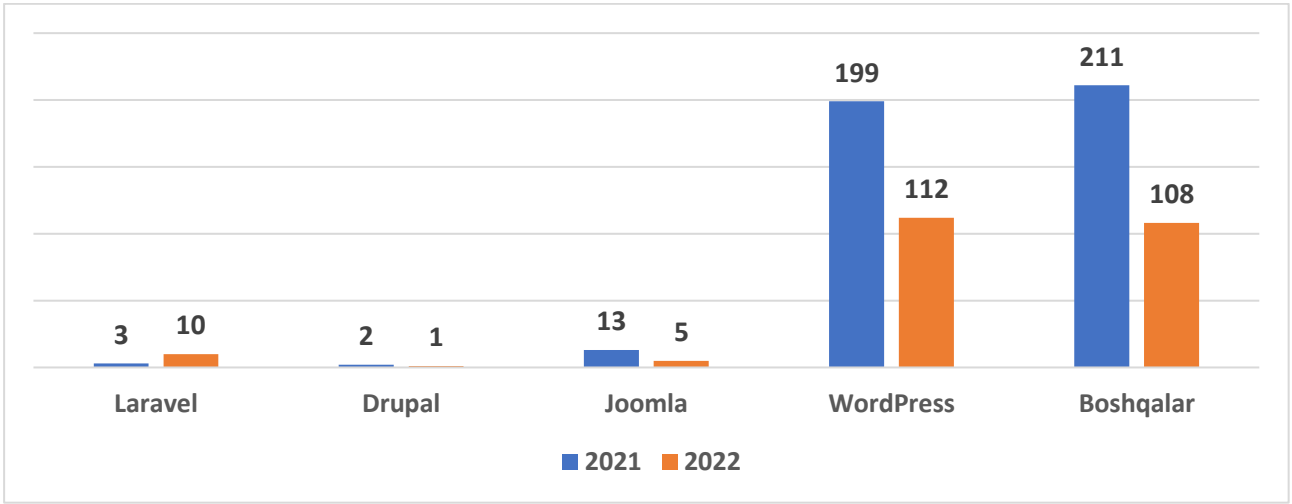


6-rasm. Axborot tizimlarida aniqlangan hodisalar turlari.

“.UZ” domen zonasidagi veb-saytlarning uzluksiz monitoringi davomida **236 ta** kiberxavfsizlik insidenti aniqlanib, ularning asosiy qismi *ruxsatsiz kontent yuklash* (**191** ta) hamda *asosiy oynani ruxsatsiz o’zgartirish* (**19** ta) bilan bog’liq bo’lgan insidentlardir.

Aniqlangan insidentlarning tahlili shuni ko’rsatmoqdaki, davlat idoralarining veb-saytlari (**50** ta) xususiy sektor vakillarining veb-saytlaridan (**186** ta) ko’ra, **3 barobar** kamroq hujumlarga uchragan.

Shuningdek, tahlillar davomida, eng ko’p kiberhujumlarga uchragan (zaif bo’lgan) veb-saytlar, “Laravel”, “Drupal”, “Joomla”, “WordPress” kontentni boshqarish tizimlarida ishlab chiqilgani aniqlandi (7-rasm).



7-rasm. 2022 – 2021 yillarda aniqlangan insidentlar (kontentni boshqarish tizimlari kesimida).

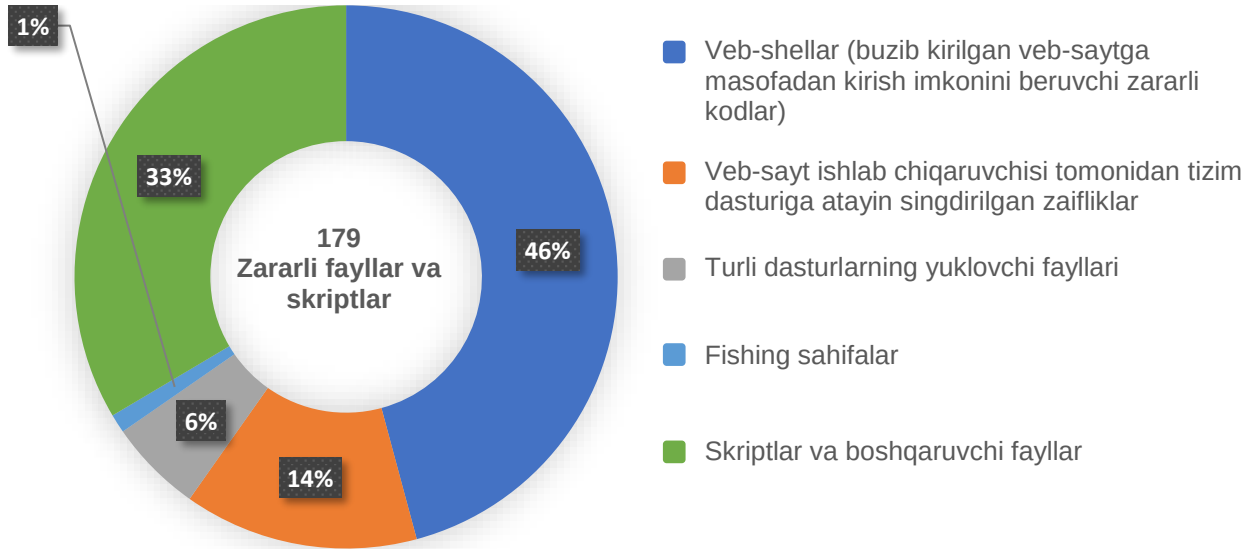
Kiberxavfsizlik insidentlarini tekshirish

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 plaginlar va dasturiy ta'minot komponentlarining eskirgan versiyalari (CMS, mavzu shablonlari, kutubxonalar va boshqalar)dan foydalanish. Xususan, aksariyat hollarda pochta xizmatlari va masofaviy ulanish modullarida kritik darajadagi zaifliklar aniqlandi (**34%**);
- veb-saytlar ishida qo'llanilmaydigan dasturiy vositalarning, shu jumladan, ishonchli bo’lmagan manbalardan yuklab olingan konfiguratsiya fayllarining ortiqchaligi (**8%**);
- parol siyosatiga amal qilinmaslik (**58%**).

Xususan, tekshiruvlar natijasida axborot tizimlari va resurslari, shuningdek, ulardan foydalanuvchilarning kiberxavfsizligiga tahdid solishi mumkin bo’lgan **179** ta zararli fayl va skriptlar aniqlandi (8-rasm).



8-rasm. Aniqlangan zararli fayllar va skriptlarning asosiy turlari.

Shu bilan birga, **97%** holatda noqonuniy faoliyat manbalari xorijiy davlatlarning manzil maydonlari ekanligi aniqlandi. Shu bilan birga, tajovuzkorlar o'zlarining haqiqiy manzillarini yashirish uchun proksi-serverlardan foydalanishlari va qidiruvni murakkablashtirish uchun proksi-serverlar zanjirlaridan foydalanishlarini inobatga olish zarur.

Respublikamiz kibermakonida bunday katta hajmdagi noqonuniy faoliyatning yuqoriligi, milliy axborot tizimlari va resurslarining aksariyat egalari va ma’murlari tomonidan axborot va kiberxavfsizlik talablariga e’tiborsizlik bilan munosabatda bo‘lishi bilan bog‘liq bo‘lib, buning natijasida davlat idoralari hamda fuqarolarning shaxsiy ma’lumotlarga ruxsatsiz aralashish xavfi sezilarli darajada oshadi.

Zaifliklar

2022 yil davomida Davlat va xo'jalik boshqaruvi organlari, shuningdek xususiy sektor vakillarining **44 ta** axborot tizimini axborot va kiberxavfsizlik talablariga muvofiqligi yuzasidan ekspertizadan o'tkazildi.

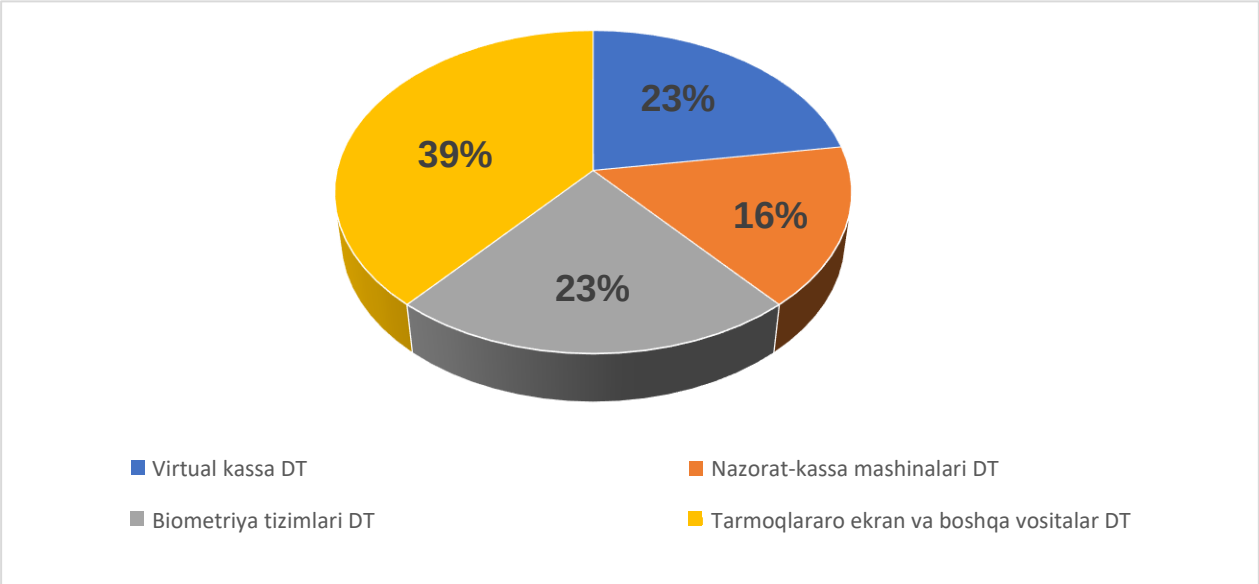
O'tkazilgan ekspertizalar natijasida jami **116 ta** axborot xavfsizligi zaifligi va kamchiligi aniqlandi. Xususan:

- yuqori darajadagi **5 ta** zaiflik va **56 ta** kamchilik;
- **42 ta** o'rta darajadagi kamchilik;
- **13 ta** quyi darajadagi kamchiliklar.

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.

Sertifikatlashtirish

Kiberxavfsizlikni ta'minlash yo'nalishida foydalaniladigan apparat, dasturiy, dasturiy-apparat vositalarining normativ hujjatlarda belgilangan talablarga muvofiqligini tasdiqlash maqsadida xorijiy va mahalliy ishlab chiqaruvchilarning **31 ta** dasturiy mahsuloti, jumladan, biometrik identifikatsiya tizimlari, tarmoqlararo ekran va boshqa kiberxavfsizlik vositalarining dasturiy ta'minotlariga muvofiqlik sertifikatlari berildi (9-rasm).



9-rasm. Dasturiy vositalar sertifikatsiyasi.

Xulosa

Yuqoridagilarning barchasi O'zbekistonda kibertahdidlar kuchayib borayotganidan dalolat bermoqda. Shuningdek, yuqoridagilardan xulosa qilgan holda, bugungi kunda kibermakondagi xavfsizlikka, xususan, axborot tizimlari va veb-saytlarning xavfsizlik darajasini oshirish va kiberxavfsizlikni ta'minlash, shuningdek, foydalanuvchilarning axborot-kommunikatsiya texnologiyalari va axborot xavfsizligi sohasidagi bilim darajasini muntazam oshirib borishga alohida e'tibor qaratish lozim.