



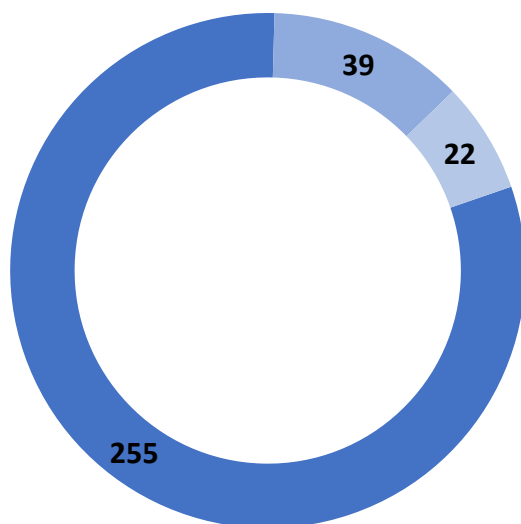
**Интернет тармоғи миллий
сегментида 2023 йил 1-ярим
йиллигида аниқланган ҳолатлар**

Веб-ресурсларнинг экспертизаси натижалари

“Киберхавфсизлик маркази” ДУК томонидан жорий йилнинг 1-ярим йиллиги мобайнида Ўзбекистон Республикаси давлат идораларининг **81** та расмий веб-ресурслари амалдаги ахборот ва киберхавфсизлик талабларига жавоб бериши даражасини аниқлаш бўйича экспертизадан ўтказилди.

Экспертиза натижаларига кўра, жами бўлиб мазкур ресурсларда **316** та турли хавф тоифаларига оид киберхавфсизлик заифликлари аниқланди.

Аниқланган заифликларнинг **81% (255 та) юқори даражали** хавф тоифасига тегишли эканлиги кузатилди. Ушбу тоифадаги заифликлар веб-ресурсларга ёхуд маълумотлар базасига маъмурлик ҳуқуқини қўлга киритган ҳолда, уларга рухсатсиз кириш ва/ёки махфий (конфиденциал) маълумотларни олиш ҳамда веб-ресурснинг манба кодини қўлга киритиш имкониятини вужудга келтириши боис, веб-ресурсларга киберхавфсизлик тамойилларини изчил тадбиқ этилиши талабини долзарблаштиради.

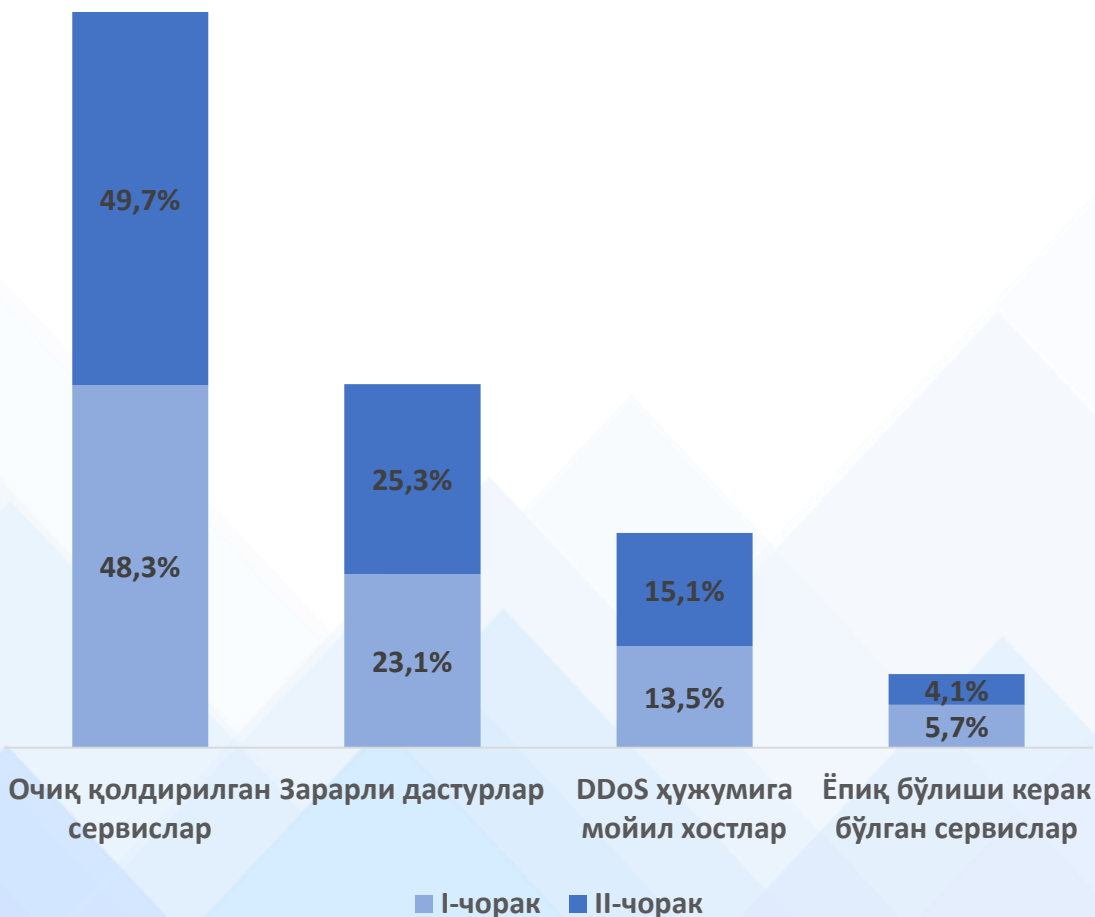


Юқори	255	81%
Ўрта	39	12%
Қуйи	22	7%

Веб-ресурсларда аниқланган заифликлар

Интернет тармоғининг миллий сегментидаги кибертаҳдидларни амалга оширишга имкон берувчи заифликларни аниқлаш тизими орқали **123** та давлат идоралари веб-ресурсларида мавжуд бўлган **552** мингдан ортиқ потенциал киберхавфсизлик заифликлари қайд этилди. Аниқланган ҳолатлар юзасидан манфаатдор ташкилотларга ушбу заифликларни бартараф этиш борасида тегишли тавсиялар тақдим этилди.

Потенциал киберхавфсизлик заифликларининг “очиқ (ҳимоясиз) қолдирилган сервислар”, “зарарли дастурлар” ва “DDoS ҳужумларига мойил хостлар” каби турлари жами қайд этилган заифликларнинг аксариятини ташкил қилмоқда. Мазкур ҳолат муҳим ахборот инфратузилмаси субъектларига ўзлари фойдаланаётган аппарат ва дастурий таъминотларда аниқланган тармоқ ва ресурс заифликлари ҳақидаги ахборотларни кузатиб бориш ҳамда мазкур киберхавфсизлик таҳдидларини амалга ошириш имкониятларини чеклашга ва бартараф этишга қаратилган превентив чора-тадбирларни кўриш амалиётини йўлга қўйишларини талаб этади.



Веб-ресурсларда кузатилган техник носозликлар

Ўтган 6 ой мобайнида Марказнинг автоматлаштирилган веб-ресурсларни мониторинг қилиш тизимига уланган **123** давлат ташкилотларининг веб-ресурслари маълум вақт оралиқларида жами бўлиб **9 616** соат ишламаганлиги қайд этилди.

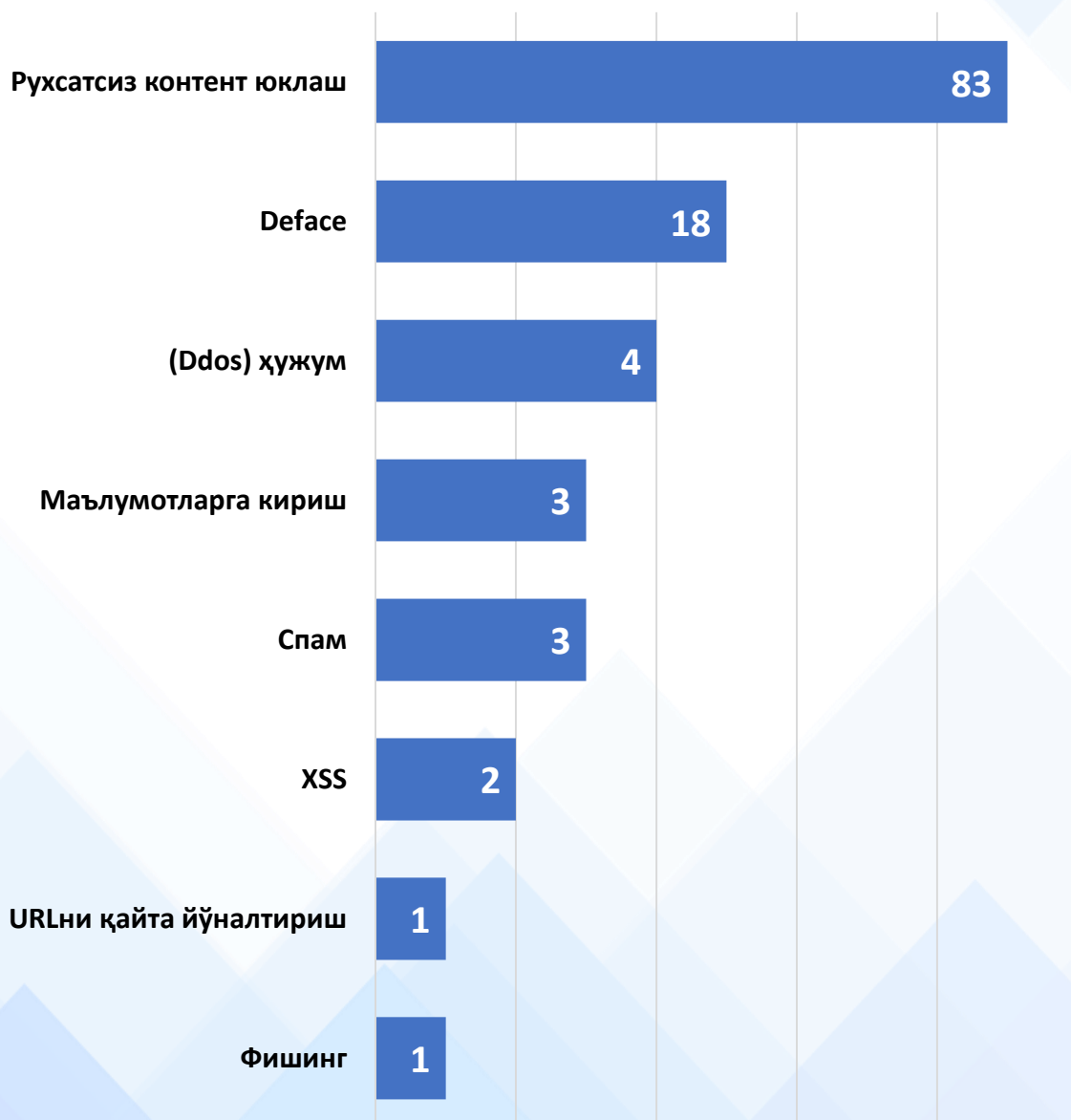
Мазкур вазият вужудга келишининг асосий сабаблари сифатида идораларининг веб-ресурсларида юзага келган қуйидаги ҳолатларни келтириш мумкин.



Веб-ресурсларда қайд этилган киберҳодисалар

Интернет тармоғининг миллий сегменти мониторинги натижаларига кўра, жорий йилнинг 1-ярим йиллиги мобайнида жами **115** та киберҳодисалар аниқланди. Ушбу киберҳодисаларнинг **25** ҳолати давлат сектори, **90** ҳолати эса хусусий сектор веб-ресурсларида юзага келган.

Веб-ресурсларда аниқланган киберҳодисаларнинг турлари қуйидаги таснифга эга.



Веб-ресурсларга нисбатан амалга оширилган киберҳужумлар

Марказнинг тармоқ ҳужумларига қарши автоматлаштирилган ҳимоя тизимларида жамланган маълумотларнинг таҳлиliga кўра, киберҳимоядаги давлат ташкилотлари веб-ресурсларига жами **17 мингга** яқин ҳолатда тармоқ ҳужумлари амалга оширилганлиги қайд этилди ва ўз вақтида блокляниши таъминланди.

Веб-ресурсларга уюштирилган жами киберҳужумлар турлари кесимида умумий кўрсаткичдан қуйида кўрсатилган улушларда тақсимланганлиги аниқланди. Бунда, *сканерларни аниқлаш*, *SQL-инъекция*, *масофавий файлни киритиш (LFI)*, *PHP - кодларни жойлаштириш ва сайтлараро скриптинг (XSS)* каби киберҳужум турларини қўллаш ҳолатлари ортганлиги кузатилди.



Дастурий маҳсулотларни сертификатлаштириш

Дастурий маҳсулотларни сертификатлаштириш бўйича қўйидаги дастурий таъминотлар учун мувофиқлик сетрификатлари берилди:

- Ахборот тизимларидан ахборот сизиб чиқишини аниқлаш ва олдини олиш учун дастурий таъминот “Falcongaze SecureTower” (6.5 версияси);
- “Cisco FPR-2140” тармоқлараро экран учун “Cisco IOS XE” (7.0.1 версияли) дастурий таъминот;
- “Cisco FPR-2130” тармоқлараро экран учун “Cisco IOS XE” (7.0.1 версияли) дастурий таъминот;
- “Cisco 9300-24T” тармоқ коммутатори учун “Cisco IOS XE” (17.03.04 версияли) дастурий таъминот;
- “Cisco 9300-48T” тармоқ коммутатори учун “Cisco IOS XE” (17.03.04 версияли) дастурий таъминот;
- “ID SYSTEM” рақамли идентификация тизимининг дастурий таъминоти сервер қисми (V1R0 версияси) ҳамда Android ва IOS операцияларига асосланган мобил иловалар (V1R0 версияси).

Ўзбекистон Республикаси,
100115, Тошкент.ш, Т.Шевченко, 20.

Телефон: (99871) 203 55 11
Факс: (99871) 277 70 66

E-mail : info@csec.uz,
Веб-сайт: www.csec.uz