ЎЗБЕКИСТОН РЕСПУБЛИКАСИДА КИБЕРХАВФСИЗЛИКНИ ТАЪМИНЛАШ

2021

ЙИЛ ҲИСОБОТИ

info@csec.uz (55) 502-10-10 www.csec.uz

Мундарижа

Кириш

Дунёда кибермакондан фойдаланувчилар сони кундан кунга ортиб бормоқда, бу каби юқори ўсиш суръатлари ахборот-коммуникация хизматларига бўлган талаблар билан боғлиқдир.

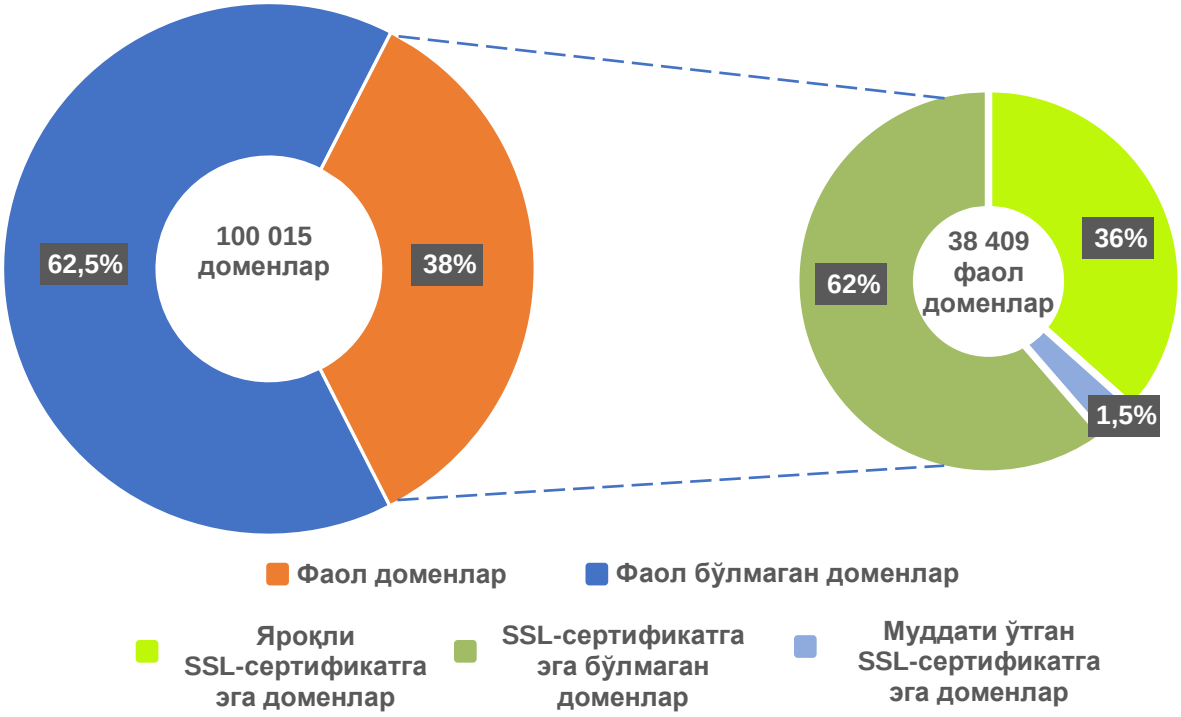
Ўзбекистон ҳам бундан мустасно эмас, фақатгина 2021 йилда давлат ва хўжалик бошқаруви органлари, маҳаллий давлат ҳокимияти органлари ва ташкилотлар фаолияти соҳаларида ахборот-коммуникация технологияларини кенг жорий этиш бўйича кўплаб лойиҳалар амалга оширилди.

Ўзбекистонда ва дунёда қўлланилаётган барча ахборот-коммуникация технологиялар ва қурилмалар жами кибермакондир. Шу каби ривожланишни хам салбий томонлари мавжуд – кибержиноят, бу жиноятчиларга пул ундириш, кибермакондан ғаразли мақсадларда фойдаланишнинг янги усулларини қўллаш имкониятини яратади.

Таъкидлаш жоизки, ахборот тизимлари ва ресурсларини ҳимоя қилишнинг оддий чоралари кўрилмагани, шунингдек, киберхавфсизликни таъминланганлик даражасининг пастлиги натижасида кибержиноятчилик даражаси ошиб бормоқда.

Таҳдидлар

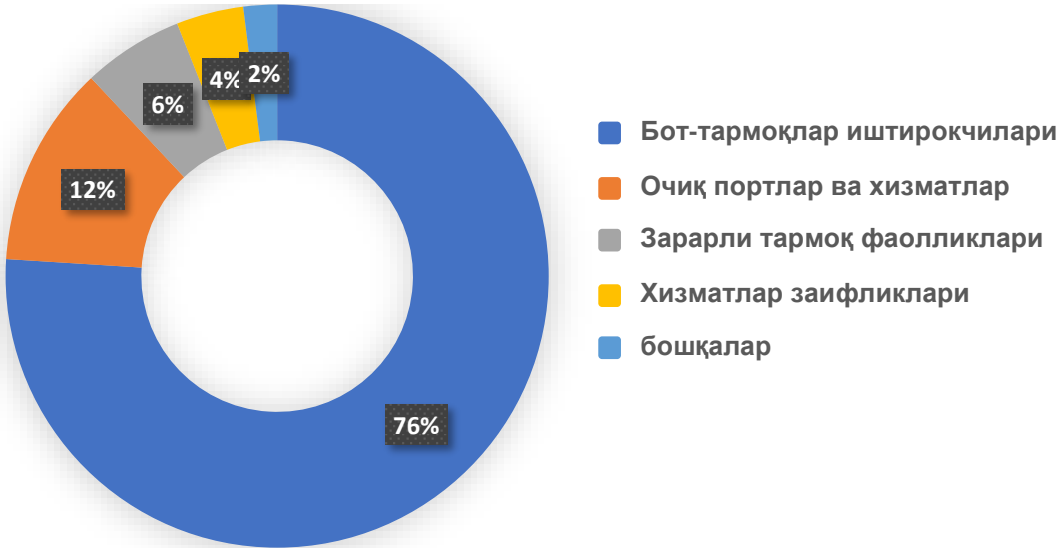
2021 йил ҳолатига кўра, Ўзбекистон Республикасининг “.uz” интернетни миллий сегментида 100 015 та домен рўйхатга олинган бўлиб, улардан 38 000 тага яқини фаолдир. 38 000 фаол доменлардан фақат 14 014 таси хавфсиз, яъни “SSL” хавфсизлик сертификатига эга. Бошқа 613 та ҳолатларда сертификатнинг амал қилиш муддати тугаган, ёки сертификат мавжуд эмас (1 - расм).



1 - расм. Доменлар ва уларнинг хавфсизлик сертификати мавжудлиги тўғрисидаги маълумот.

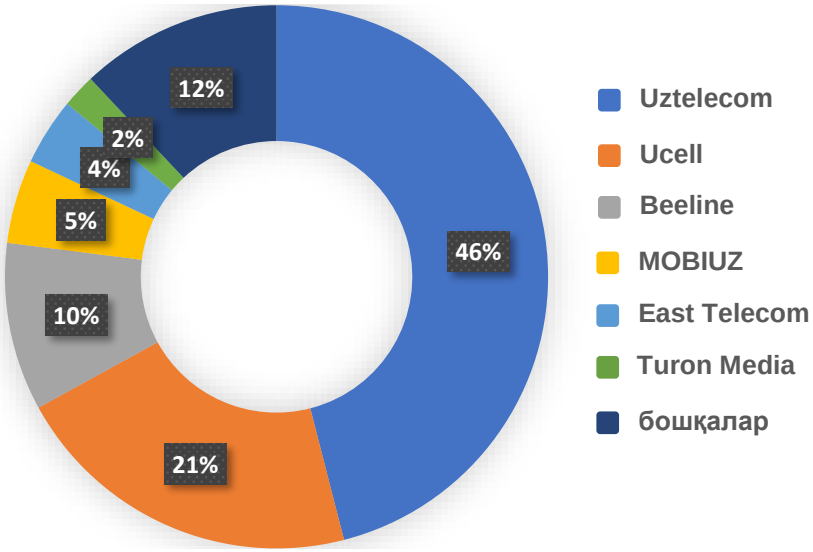
Марказ томонидан 2021 йилда Интернет тармоғининг миллий сегментини манзил майдонидан келиб чиққан 17 097 478 та зарарли ва шубҳали тармоқ фаолликлар бўйича ҳолатлар аниқланди (2 - расм).

Ушбу фаолликларнинг кўпгина қисми, яъни 76% бот-тармоқ иштирокчиларидан иборат.



2 - расм. Аниқланган таҳдидларнинг асосий турлари.

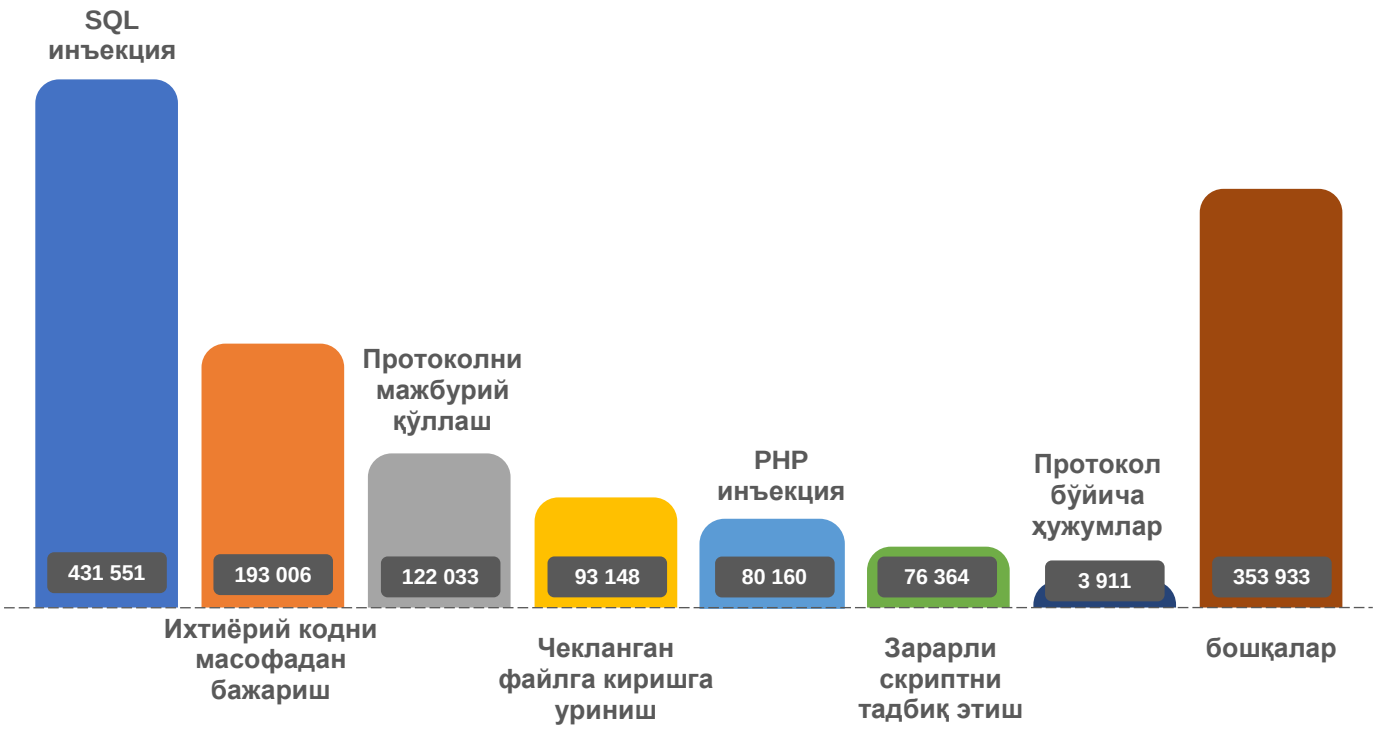
Зарарли ва шубҳали тармоқ фаолликларни асосий сони миллий операторлар ва провайдерларнинг фойдаланувчилари томонидан келиб чиққан (3 - расм).



3 - расм. Оператор ва провайдерлар кесимида зарарли тармоқ фаолликлари бўйича аниқланган ҳолатлар.

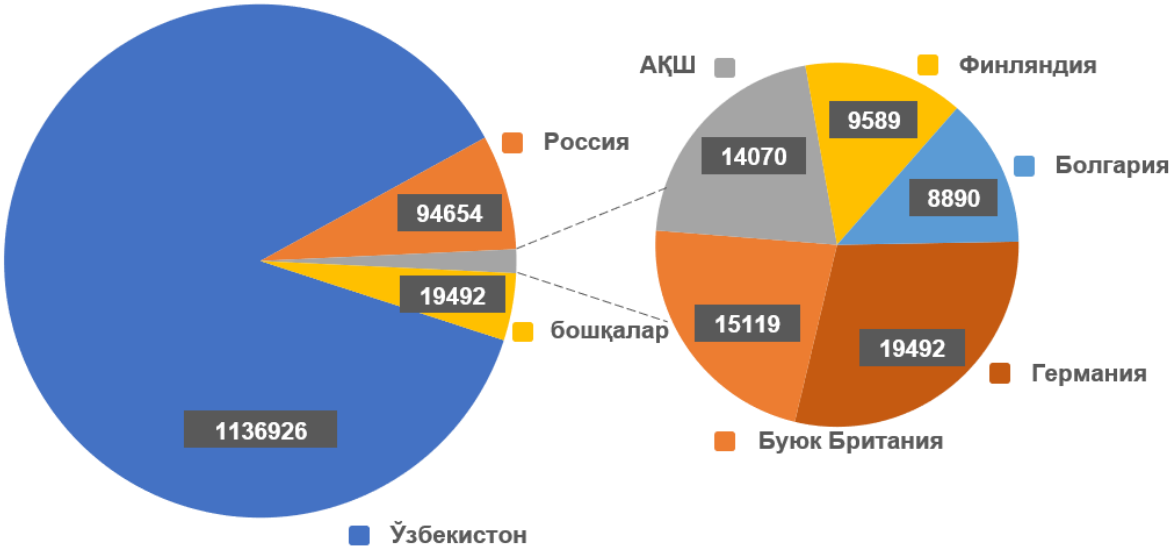
Хусусан, тармоқ аномалиялари ва аниқланган киберхавфсизлик заифликларга чоралар кўришни мувофиқлаштириш орқали 2020 йилнинг шу даврига нисбатан (20 миллиондан ортиқ кибертаҳдидлар) кибертаҳдидлар сони 20 фоизга камайди.

Бундан ташқари, Марказнинг веб-иловаларни ҳимоя қилиш тизими ёрдамида Интернет тармоғининг миллий сегментининг веб-сайтларига қилинган 1 354 106 та киберҳужумлар аниқланди ва бартараф этилди (4 - расм).



4 – расм. Аниқланган ва бартараф этилган киберҳужумлар.

Энг кўп киберҳужумлар Ўзбекистон, Россия Федерацияси, Германия ва бошқа ҳудудлардан амалга оширилган (5 - расм).



5 – расм. Манзил майдонларидан киберҳужумлар амалга оширилган мамлакатлар.

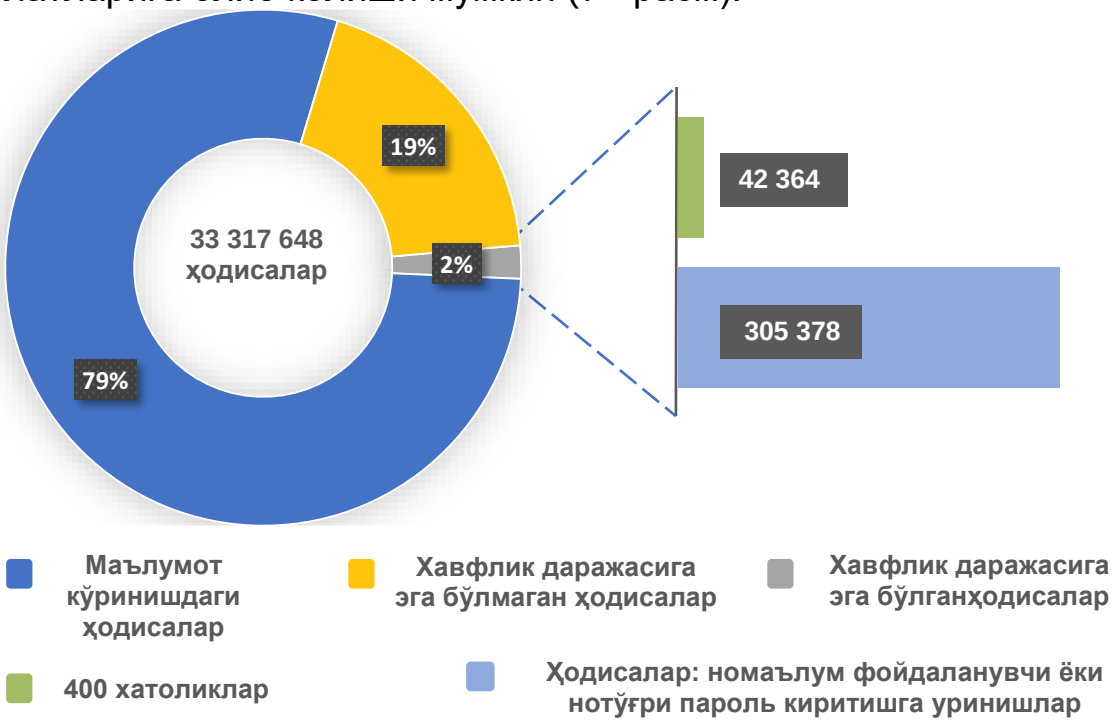
Инцидент ва ҳодисалар

Давлат органлари веб-сайтларининг хавфсиз ишлаши доирасида (ҳодисалар ва инцидентларнинг кечаю кундуз мониторинги) 2021 йилда

636 та хавфсизлик ҳодисаси аниқланган (6 - расм), бу давлат ва хўжалик бошқаруви органлари, маҳаллий давлат ҳокимияти органлари ва бошқа ташкилотларнинг веб-сайтлари қарийб 1 048 216 дақиқа иш фаолиятида бўлмаганлик (тўхтаб туриш) вақтини ташкил этади.

6 – расм. Аниқланган ҳодисаларнинг асосий турлари.

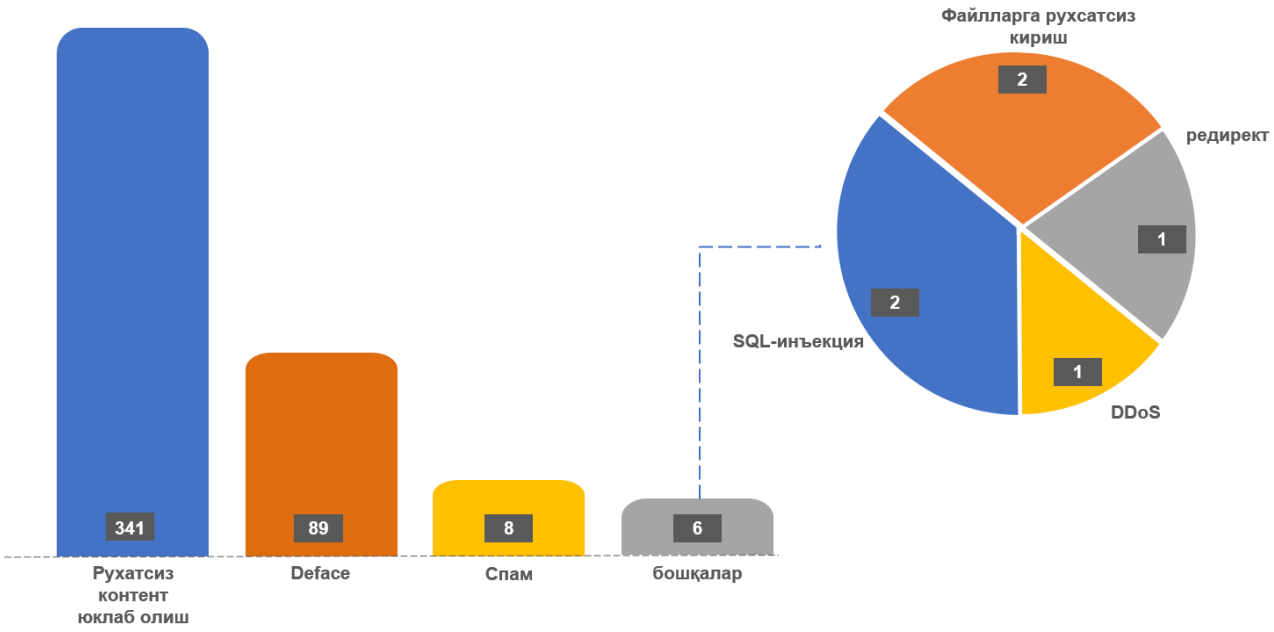
Идоралараро маълумотлар узатиш тармоғига (ИМУТ) уланган давлат органларининг ахборот тизимларини мониторинги давомида 33 317 648 та хавфсизлик ҳодисаси қайд этилган бўлиб, улардан 347 742 таси рухсатсиз кириш ва конфиденциал маълумотларнинг чиқиб кетиш ҳолатларига олиб келиши мумкин (7 - расм).



7 - расм. Ахборот тизимларда аниқланган ҳодисалар.

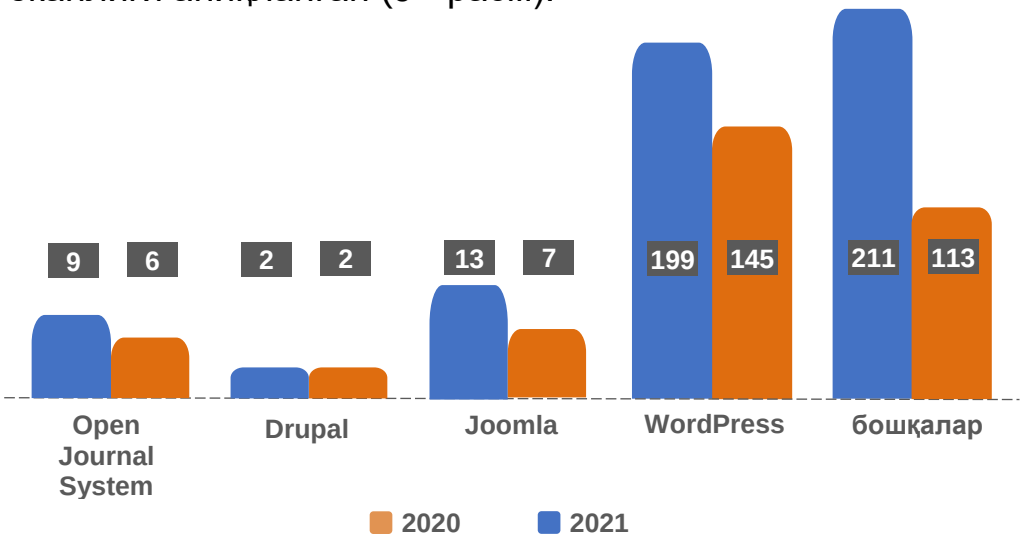
"UZ" домен зонаси веб-сайтларига нисбатан содир этилган киберхавфсизлик инцидентлари мониторинги натижасида 444 та инцидент қайд этилган бўлиб, улардан энг кўпини рухатсиз контентни юклаб олиш –341 тани ва асосий саҳифага рухсатсиз ўзгартиришлар киритиш (Deface) – 89 тани ташкил этган (8 - расм).

Инцидентларнинг таҳлили шуни кўрсатдики, давлат секторининг веб-сайтлари (134 та инцидент) хусусий секторга нисбатан 3 баравар камроқ ҳужумга учраган (310 та инцидент).



8 – Расм. Веб-сайтлардаги киберхавфсизлик инцидентлари

Инцидентларнинг батафсил таҳлили натижасида, “Wordpress”, “Joomla”, “Open Journal Systems” и “Drupal” контентни бошқариш тизимларида ишлаб чиқилган веб-сайтлар энг заиф (тез-тез ҳужумга учраган) эканлиги аниқланган (9 - расм).



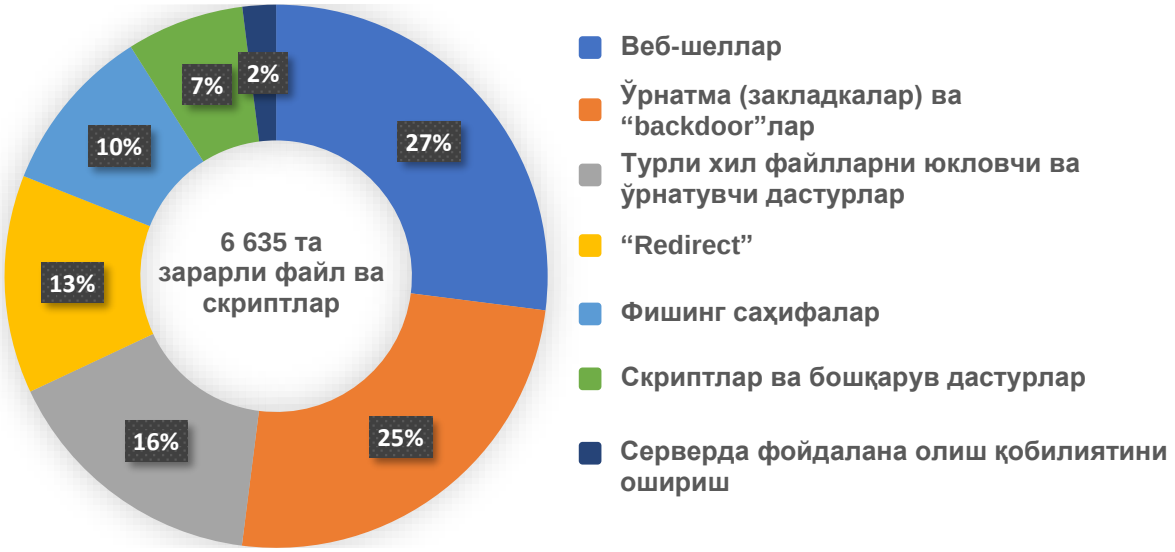
9 – расм. 2021 ва 2020 йиллардаги инцидентларни таққослаш.

Киберхавфсизлик ҳодисаларини текшириш

Зарарли контентни аниқлаш ва унинг ахборот маконидаги ҳуқуқбузарликларга алоқадорлигини таҳлил қилиш доирасида киберхавфсизлик инцидентлари текширилиб, уларни амалга ошириш сабаблари ва усуллари аниқланди.

Хакерлик ҳужумларини муваффақиятли амалга оширишнинг асосий сабаблари ва усуллари қуйидагилардан иборат: веб-иловаларда заифликларнинг мавжудлиги, хусусан, уларнинг ўз вақтида янгиланмаганлиги (72%), заиф пароллардан фойдаланиш (25%) ва бошқалар.

Хусусан, текширув натижаларига кўра, ахборот тизимлари ва ресурслари, шунингдек, улардан фойдаланувчиларнинг киберхавфсизлигига таҳдид соладиган 6635 та зарарли файл ва скриптлар аниқланди (10-расм).



10 - расм. Аниқланган зарарли файллар ва скриптларнинг асосий гуруҳлари.

Шу билан бир қаторда, 97% ҳолатларда ноқонуний фаоллик манбалари хорижий мамлакатларнинг манзил майдонлари эканлиги аниқланди. Хусусан, энг кўп ноқонуний фаоллик ҳолатлари қуйидаги давлатлар билан боғлиқ: АҚШ, Индонезия, Нидерландия, Руминия, Жазоир ва Тунис. Шу қаторида, эслатиб ўтиш жоизки, бузғунчилар ўзларининг ҳақиқий жойлашиш манзилларини яшириш учун прокси-серверлардан ишлатишларини ва қидирувни мураккаблаштириш учун прокси-сервер занжирларидан фойдаланишларини унутмаслик зарур.

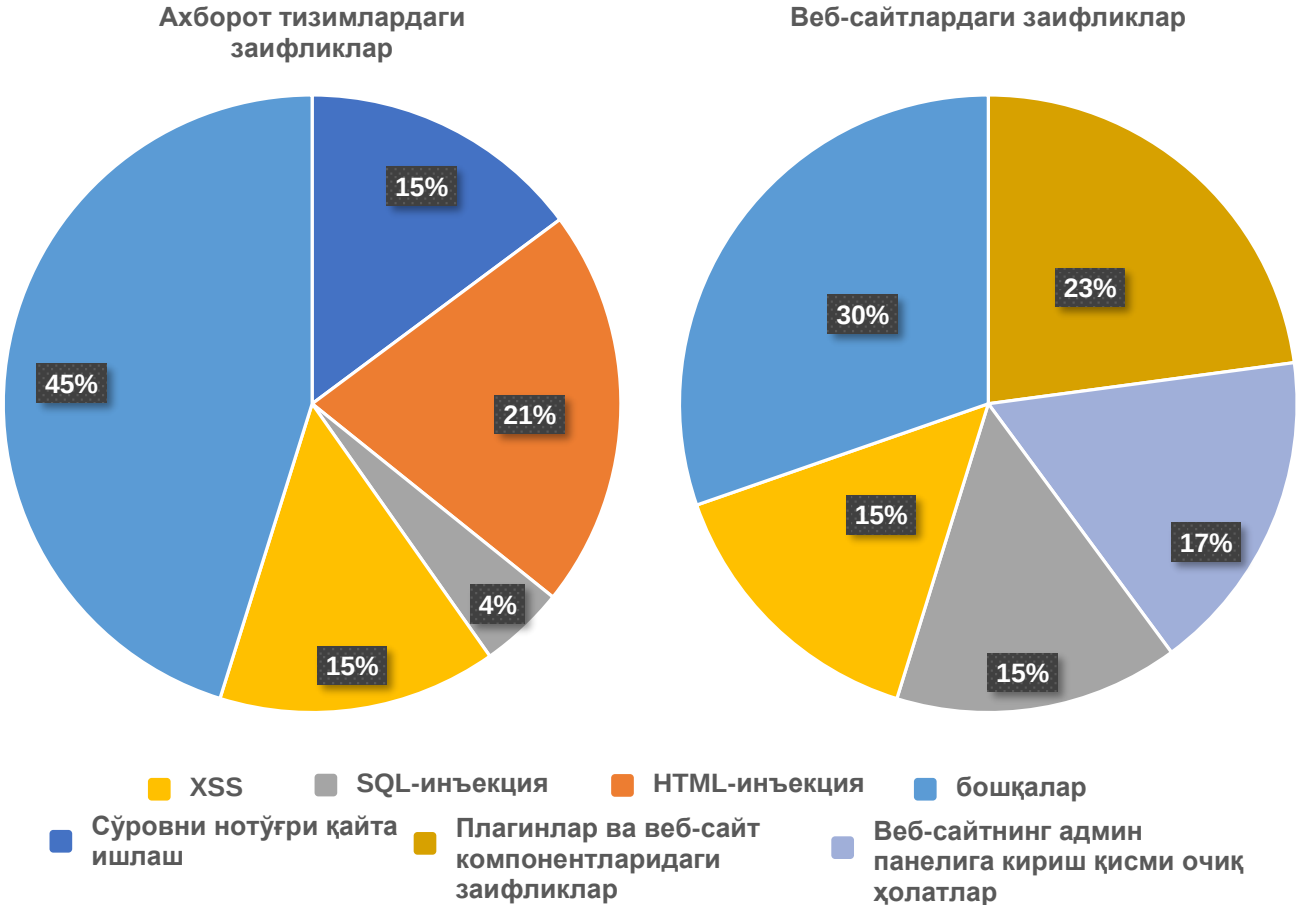
Республикамизнинг манзил маконида бундай катта ҳажмдаги ноқонуний фаолликнинг кўпайиши миллий ахборот тизимлари ва ресурсларининг аксарият эгалари ва маъмурлари томонидан ахборот ва киберхавфсизлик талабларига эътиборсизлик билан муносабатда бўлиши билан боғлиқ бўлиб, бу эса уларнинг ишига рухсатсиз аралашиш хавфини сезиларли даражада оширади.

Заифликлар

Миллий ахборот тизимлари ва ресурсларини муҳофаза қилиш даражасини ошириш бўйича чора-тадбирларни амалга ошириш давомида 2021 йилда 256 та ўрганиш ва экспертизалар ўтказилди.

Амалга оширилган ишлар натижасида 989 та киберхавфсизлик заифликлар аниқланиб, уларнинг мавжудлиги ҳақида ахборот тизимлари ва ресурслари эгаларига тезкорлик билан хабар берилди:

– Ўта хавфли даражадаги – 683 та;
– Ўрта хавфли даражадаги – 271 та;
– Паст хавфли даражадаги – 24 та.



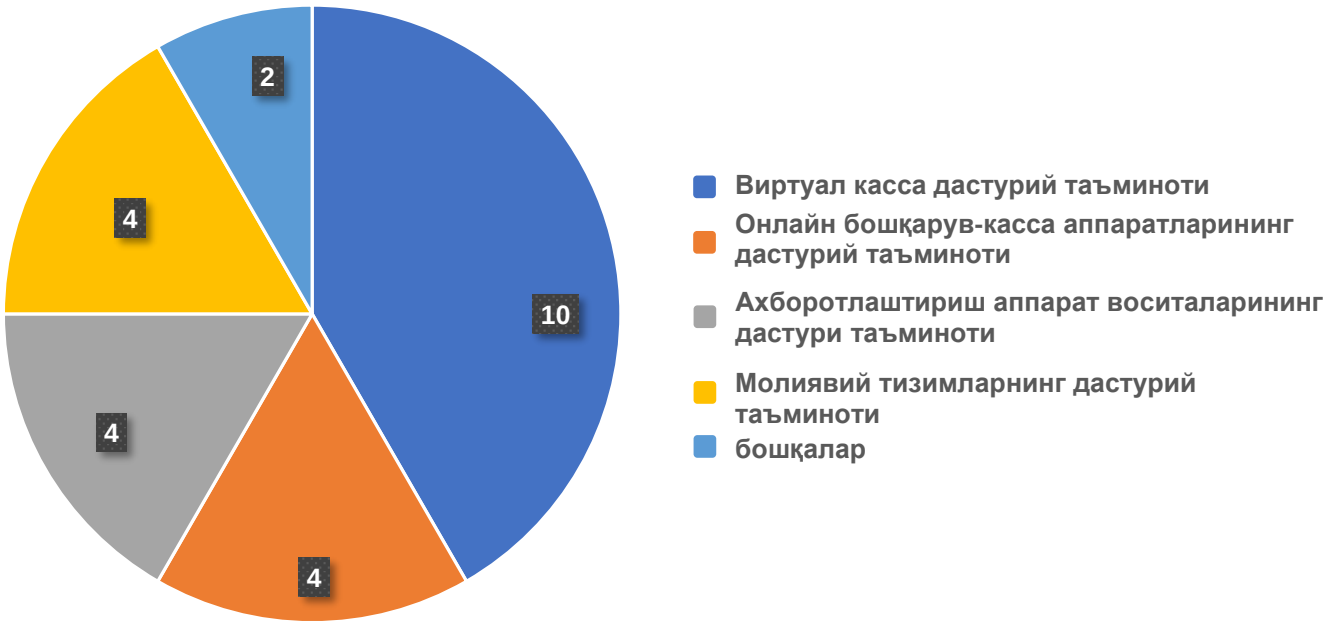
11 – расм. Аниқланган заифликларнинг асосий турлари.

Юқорида таъкидлаб ўтилган заифликларнинг бузғунчилар томонидан эксплуатация қилиниши орқали ахборот ресурсларининг яхлитлиги ва фойдалана олишликнинг бузилишига, шу жумладан Ўзбекистон Республикаси фуқароларининг шахсга доир маълумотларини чиқиб кетишига олиб келиши мумкин.

Сертификатлаш

Ахборот хавфсизлигини бошқариш тизимлари, аппарат воситалари, дастурий маҳсулотлар, ахборот-коммуникация технологиялари, телекоммуникация ускуналари ва бошқа техник воситалар, шу жумладан ахборотни ҳимоя қилиш воситалар сифатини тасдиқлаш мақсадида 21 та дастурий маҳсулот, шунингдек, 3 та хорижий ва маҳаллий аппарат-

дастурий воситалар ахборот ва киберхавфсизлик бўйича меъёрий ҳужжатлар талабларига мувофиқлиги юзасидан сертификатдан ўтказилди (12 - расм).



12-расм. Сертификатланган дастурий таъминот.

Хулоса

Юқорида таъкидлаб ўтилганларнинг барчаси Ўзбекистонда кибертаҳдидлар кучайиб бораётганидан далолат беради. Бундан хулоса қилиш қийин эмаски, бугунги кунда кибермаконда хавфсизликка, хусусан, ахборот тизимлари ва веб-сайтларнинг хавфсизлик даражасини ошириш ва киберхавфсизликни таъминлашга, шунингдек, фойдаланувчиларнинг ахборот-коммуникация технологиялари ва ахборот хавфсизлиги соҳасидаги билим даражасини мунтазам ошириб боришга алоҳида эътибор қаратиш лозим.

Шу билан қаторда, қуйидагилар тавсия этилади:

1. Лицензия ва сертификатга эга операцион тизимлар ва дастурлардан фойдаланиш.
2. Амалдаги операцион тизимлар, дастурий таъминот ва хавфсизлик компонентларининг сўнгги версияларини мунтазам янгилаб туриш. Янгилаш ишларини расмий манбалардан амалга оширилиши керак.
3. Келгусида зарарли дастурларни қидириш, ўчириб ташлаш ва улардан ҳимоя қилиш функцияларига эга хавфсизлик плагинларидан фойдаланиш.
4. Мунтазам равишда маълумотлар базалари, файллар, почта ва ҳоказолани захиралаш ишларни амалга ошириш.
5. Фойдаланилмаётган плагинларни ўчириб ташлаш - ҳар қандай янги плагин ёки кенгайтма бузғунчи томонидан ҳужум уюштириш хавфини оширади. Шу муносабат билан, фойдаланилмаган плагинларни ўчириб қўйиш ва иложи бўлса, ҳар бир алоҳида ҳолат учун плагинни ўрнатиш ўрнига ўрнатилган механизмлардан фойдаланиш тавсия этилади.

6. Пароль асосидаги аутентификациясини кучайтириш – маъмур аккаунти, хизмат кўрсатувчи провайдернинг веб-сайтидаги шахсий кабинети ва сервердаги ҳисобга олиш ёзувлари (аккаунт) учун (масалан, ажратилган ёки “co-location” хостинги учун) мураккаб ва такрорланмайдиган паролдан фойдаланиш тавсия этилади. Паролни ўзгартирганда, ҳисобга олиш ёзувлари (аккаунт) учун катта ва кичик ҳарфлар, рақамлар, махсус белгилар ва минимал узунлиги 8 белгидан иборат паролларни яратиш қоидаларидан фойдаланиш тавсия этилади. Икки факторли аутентификацияни созлаш тавсия этилади (ушбу имконият мавжуд бўлган ҳолатларда). Шунингдек, киришга уринишлар сонига чеклов қўйиш тавсия этилади (“bruteforce” ҳужумларидан ҳимоя қилиш).

7. Янгиланган вирус базаларига эга антивирус дастурлари ўрнатилган қурилмалардан (компютерлар, планшетлар) ахборот тизимига ёки веб-сайтга киришни таъминлаш.

8. Ахборот тизимлари ва ресурсларини ахборот хафсизлиги талабларига мувофиқлиги бўйича экспертизаларни ўтказиш. Экспертиза натижалари бўйича юборилган тавсиялар асосида аниқланган заифликларни ўз вақтида бартараф этиш.

9. Фойдаланувчилар (ходимлар)нинг ахборот-коммуникация технологиялари ва ахборот хавфсизлиги соҳасидаги малакаси ва билим даражасини мунтазам ошириб бориш.

10. Киберхавфсизлик ҳодисаларининг таҳдидларини ва оқибатларини бартараф этиш учун тезкор аниқлаш ва тегишли чораларни кўриш.

Юқорида санаб ўтилган ва бошқа қўшимча ҳимоя чораларини қабул қилиш киберхавфсизлик таҳдидлари хавфини сезиларли даражада камайтиради, бу эса ўз навбатида мумкин бўлган ҳужумлардан ва кейинчалик ахборот хавфсизлиги инцидентларининг сабаблари ва оқибатларини бартараф этиш заруриятидан ҳимояланиш имконини беради.