2023

ЯКУНЛАРИ

“КИБЕРХАВФСИЗЛИК МАРКАЗИ”
ДАВЛАТ УНИТАР КОРХОНАСИ

Мундарижа

Кириш

Мамлакатимизда жадал олиб борилаётган ислоҳотларнинг асосий тамойили бўлмиш инсон қадрини юксалтириш, инсон капиталининг ривожланишини таъминлашга қаратилган чора-тадбирларнинг тамал мезони сифатида миллий иқтисодиётимизнинг рақобатдошлигини ва самарадорлигини оширишнинг рақамли усулларини кенг қамровли жорий этилиши, республикамизнинг муҳим ахборот инфратузилмаси, шу жумладан, давлат ва хўжалик бошқаруви органлари ахборот тизим ва ресурсларининг киберхавфсизлигини таъминлаш масалаларини стратегик поғонага кўтариб, сезиларли даражада долзарблаштирди.

Шу ўринда алоҳида таъкидлаш жоизки, сўнги пайтларда халқаро ахборот хавфсизлигининг замонавий манзарасида жиддий ўзгаришларни келтириб чиқараётган жаҳон миқёсида асосий “куч марказлари” ўртасидаги геосиёсий қарама-қаршиликларнинг кескинлашуви асносида, глобал кибермакон юзага келаётган сиёсий-харбий тўқнашувларнинг асосий майдонларидан бирига айланиб улгурганлиги, республикамиз муҳим ахборот инфратузилмасининг киберхавфсизлик ҳолатига таъсир кўрсатувчи глобал омил сифатида юзага чиқмоқда.

Мазкур вазиятда, турли эксперт ҳисоб-китобларга кўра, дунё миқёсида яқин уч йилда кибержиноятчиликдан кўрилган глобал зарар йилига 15%га ўсиб борган холда, жорий йилда 8 триллион АҚШ долларини, 2025 йилга бориб эса 10,5 триллион АҚШ долларини ташкил этиши таҳмин қилинмоқда. Шу билан бирга, тобора рақамлаштирилаётган ташкилот ва корхоналарнинг, “нарсалар интернети” қурилмалари ва турли тоифадаги истеъмолчиларни турли кибержиноятлардан ҳимоя қилиш зарурати 2021 йилдан 2025 йилгача бўлган давр мобайнида умумжаҳон даражасида киберхавфсизлик маҳсулотлари ва хизматларига йўналтириладиган харажатлар миқдорини 1,75 триллион АҚШ долларга етишига олиб келиши таъкидланмоқда.

“Киберхавфсизлик маркази” ДУКда (кейинги ўринларда – Марказ) мавжуд маълумотларнинг таҳлилига кўра, республикамизда давлат ва хўжалик бошқаруви органларининг ахборот тизимларида рақамлаштириш тадбирларини шиддат билан амалга оширилиши билан бир қаторда бу тизимларга бўлган кибертаҳдидларнинг хавфлилик даражасининг жиддийлашуви ҳамда сон-сифат кўрсаткичлари жиҳатидан ўсиш тенденцияси кузатилмоқда.

Техник топшириқ экспертизаси

Ахборот тизимларини ишлаб чиқиш бўйича техник топшириқларни экспертизадан ўтказиш йўналишида 365 та экспертиза хизматлари кўрсатилди, (1-диаграмма).

1-диаграмма. Ўтказилган экспертизалар сони йиллар кесимида (21.12.2023й. ҳолатига).

Ахборот тизимининг техник топшириққа мослик экспертизаси

Ахборот тизимларининг техник топшириққа мослиги юзасидан 93 та экспертиза хизматлари кўрсатилди (2-диаграмма).

2023 йил якуний натижаларига кўра, ушбу экспертиза турига доир хизматларни кўрсатиш 2022 йилга нисбатан 24% га ортгани қайд этилди.

2-диаграмма. Ўтказилган экспертизалар сони йиллар кесимида.

Ахборот тизимининг киберхавфсизлик талабларига мослик экспертизаси

Тегишли ташкилотлар мурожаати, иш режалари ва шахсий ташаббуслар асосида 86 та ахборот тизими ва ресурсларида ахборот хавфсизлиги таъминланганлик ҳолати бўйича ўрганиш ва таҳлил қилиш ишлари олиб борилиб, 740 та заифлик аниқланди. Уларнинг соҳалар кесимидаги кўринишини (3-диаграмма)да кўриш мумкин. Марказнинг тавсиялари ва амалий ёрдами асосида 260 та заифлик бартараф этилди.

3-диаграмма. Аниқланган заифликлар сони соҳалар кесимида

Экспертиза жараёнида аниқланган ҳолатларнинг таҳлили мазкур тизимларда қуйидаги салбий оқибатларга олиб келиш мумкин бўлган бир қатор заифлик ва камчиликлар мавжудлигини кўрсатди. Уларнинг аҳамиятга моликлари қуйидагилар:

- Ўзбекистон Республикаси фуқароларининг шахсга доир маълумотлари ноқонуний ошкор бўлиши ва улардан фойдаланиш;
- ахборот тизим ва ресурслари жойлашган серверлардан, шунингдек уларнинг созламалари, бошқарув панели, маълумотлар базаларини бошқариш тизимлари ва функционал имкониятларидан ноқонуний фойдаланиш;
- конфиденциал турдаги маълумотларга ноқонуний эга бўлиш;
- республика олий, ўрта ва халқ таълими тизимларида жорий этилган хизматлардан, ноқонуний фойдаланиш, шунингдек ноқонуний равишда талабалар ва ўқувчиларга доир маълумотларга эга бўлиш ҳамда имтиҳон натижаларига таъсир кўрсатиш.

Мазкур заифликлар келиб чиқишининг асосий сабаблари:

- ахборот тизими ва ресурсларни ишлаб чиқиш жараёнида йўл қўйилган хатоликлар;
- ахборот тизими ва ресурсларини ишлаб чиқишда ахборот ва киберхавфсизлик талабларини инобатга олмаслик;
- ахборот тизими ва ресурсларини ишлаб чиқишда заифликка эга дастурий маҳсулотлардан фойдаланиш;
- ишончли ва тажрибага эга бўлмаган ташкилотларга ишлаб чиқиш учун лойиҳаларни топшириш;
- ахборот тизими ва ресурсларни ишлаб чиқилгандан сўнг аутсорс компания мутахассислари ёки ташкилотнинг АКТ мутахассислари томонидан мунтазам равишда техник қўллаб қувватлаш ишлари олиб борилмаслиги;
- АКТ ва киберхавфсизлик соҳасида малакали мутахассислар етишмовчилиги;
- киберхавфсизлик масалаларини ҳал этишда етарли даражада молиялаштирилмаслик.

Заифликлар бартараф этилмаганлигининг асосий сабаблари:

- ташкилотларда малакали ходимларнинг етишмаслиги;
- давлат органлари раҳбарияти, масъул ходимлар томонидан мавжуд заифлик ва камчиликларни бартараф этилиши бўйича мунтазам назорат ўрнатмаганлиги;
- ташкилотларда молиявий барқарорликнинг йўқлиги;
- ахборот тизимлари ва ресурсларини ўз вақтида ва мунтазам равишда киберхавфсизлик талабларига мувофиқлиги бўйича экспертизадан ўтказишга эътиборсизлик.

Аттестация ва аудит

11 та ташкилотнинг *Ахборотлаштириш объектлари*да* ахборот хавфсизлиги аудити ўтказилди (4-диаграмма).

Ўтказилган аудит тадбирлари давомида жами 5 та сервер хонаси, 70 та сервер қурилмаси ҳамда 651 та ишчи станциялар ўрганиб чиқилди.

Шу билан бирга, мавжуд маълумотлар таҳлилига кўра, 2023 йилда республика миқёсида ушбу хизматни таклиф қилувчи хусусий сектор субъектлари сони ҳамда улар томонидан мазкур хизматларни кўрсатиш салмоғи ортганлиги қайд этилди.

4-диаграмма. Ўтказилган Аудитлар йиллар кесимида.

**Ахборотлаштириш объектлари - бу турли даражадаги ва мақсаддаги ахборот тизимлари, телекоммуникация тармоқлари, ахборотга ишлов беришнинг техник воситалари, ушбу воситалар ўрна-тилган ва фойдаланиладиган хоналар.*

Сертификация

Дастурий таъминотларни сертификатлаштириш хизматини кўрсатиш 2022 йилга нисбатан 13% пасайганлиги кузатилган бўлсада, мазкур хизматлар юзасидан тузилган янги шартномалар салмоғи 25,9% га ортганлиги қайд этилди (5-диаграмма).

Хусусан, дастурий таъминотларни сертификатлаштириш бўйича 34 та шартнома имзоланган бўлиб, улардан 26 таси якунига етказилди.

5-диаграмма. Сертификатланган дастурий воситалар сони йиллар кесимида.

Сертификатланган 26 та дастурий таъминотлардан ахборот ва киберхавфсизлигини таъминлаш бўйича қуйидаги дастурий таъминотлар сертификатланди:

- Махфий маълумотларнинг тарқалишини олдини олиш тизими “Falcongaze SecureTower” (6.6.697 версияли);
- “Cisco FPR-2140”, “Cisco FPR-2130”, “Cisco FirePower 1010”, “Cisco FirePower 1140”, “Cisco FirePower 1150” тармоқлараро экранлари учун “Cisco FX-OS” (7.0.1 версияли), “Cisco FX-OS” (7.0.1 версияли), “Cisco FX-OS” (7.2.5 versiyali);
- “FortiGate 601F” ҳамда “FortiGate 1801F” тармоқлараро экранлари учун “FortiOS” (7.2.5 версияли);
- “Updive SIEM” хавфсизлик маълумотлари ва ҳодисаларни бошқариш тизимининг таркибидаги сервер қисми (1.3.26 версияли), клиент қисми (1.5.3 версияли) ва агент қисми (1.3 версияли);
- “СерчИнформ SIEM” хавфсизлик маълумотлари ва хавфсизлик тадбирларини бошқариш тизимининг (1.47.222.5 версияси).

Ахборот хавфсизлиги сиёсати доирасида

Ахборот хавфсизлиги сиёсати (АХС)ни ишлаб чиқишда ташкилотларга кўмаклашиш бўйича 20 та шартнома асосида идораларнинг “Ахборот хавфсизлиги сиёсатлари” ишлаб чиқилди ва Ваколатли орган билан келишишда кўмак берилди.

45 та янги ишлаб чиқилган ёки таҳрирланган АХС кўриб чиқилиб, таклиф ва тавсиялар берилди.

Марказ томонидан АХС ишлаб чиқиш бўйича давлат идораларига кўрсатилаётган маслахат ва кўмаклашиш тадбирларининг жадаллашгани боис, ташкилотларнинг ўз ташаббуслари асосида, ишлаб чиқилган лойиҳалар сони 2022 йилга нисбатан 29% га ортганлиги қайд этилди. Ўз ўрнида, жорий йилда ташкилотларнинг Марказга шартнома асосида АХС ишлаб чиқишга доир мурожаатлари 29% га камайган (6-диаграмма).

6-диаграмма. Ишлаб чиқилган АХСлар сони йиллар кесимида.

Давлат идораларига консалтинг хизматлари кўрсатиш

Ахборот ва киберхавфсизлик соҳасида консалтинг хизматлари кўрсатиш доирасида 6 та ташкилотда ишлар якунланди.

Давлат ва хўжалик бошқаруви органларининг ихтисослаштирилган бўлинмалари ҳамда бошқа ташкилотларга ахборот ва киберхавфсизликни таъминлаш масалалари ва улардаги камчиликларни бартараф этиш бўйича 986 та маслаҳат ёрдами, шу жумладан 92 та ҳолатда жойига чиққан ҳолда, амалга оширилди. Ахборот ва киберхавфсизлик масалаларига оид мавзуларда 17 та давлат ташкилотларида семинарлар, тренинглар ва амалий машғулотлар ўтказилди.

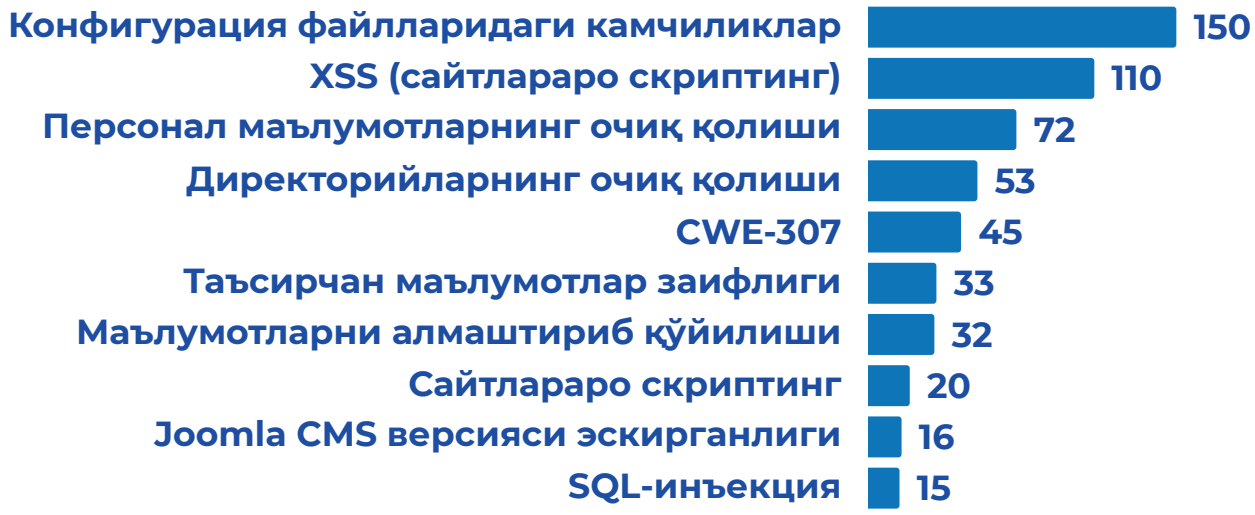
Веб-ресурсларда аниқланган заифликлар

1. Интернет тармоғи миллий сегментидаги расмий веб-ресурсларини ахборот ва киберхавфсизлик талаблари бўйича текшириш доирасида

Расмий веб-ресурсларни ахборот ва киберхавфсизлик талаблари бўйича давомида умумий ҳисобда 677 та веб-ресурсда жами бўлиб 1186 та заифлик аниқланди. Улардан 1022 таси давлат органлари веб-ресурсларига тўғри келади.

Шунингдек, Марказ мутахассислари кўмаклари ёрдамида мазкур заифликлардан 587 таси бартараф этилди. Улардан энг кўп учраган турлари (7-диаграмма) да кўрсатилган. Бартараф этилмаган заифликлар юзасидан “Ўзкомназорат” Инспекцияси билан ҳамкорликда ишлар ташкил қилинди.

Бунинг натижасида 2023 йилда давлат ташкилотларига тегишли веб-ресурларда аниқланиб бартараф этилмаган 46 та заифликларнинг 36 таси бартараф этилди, 7 та веб-ресурснинг иш фаолияти вақтинча тўхтатилди.



7-диаграмма. Аниқланган заифлик турлари

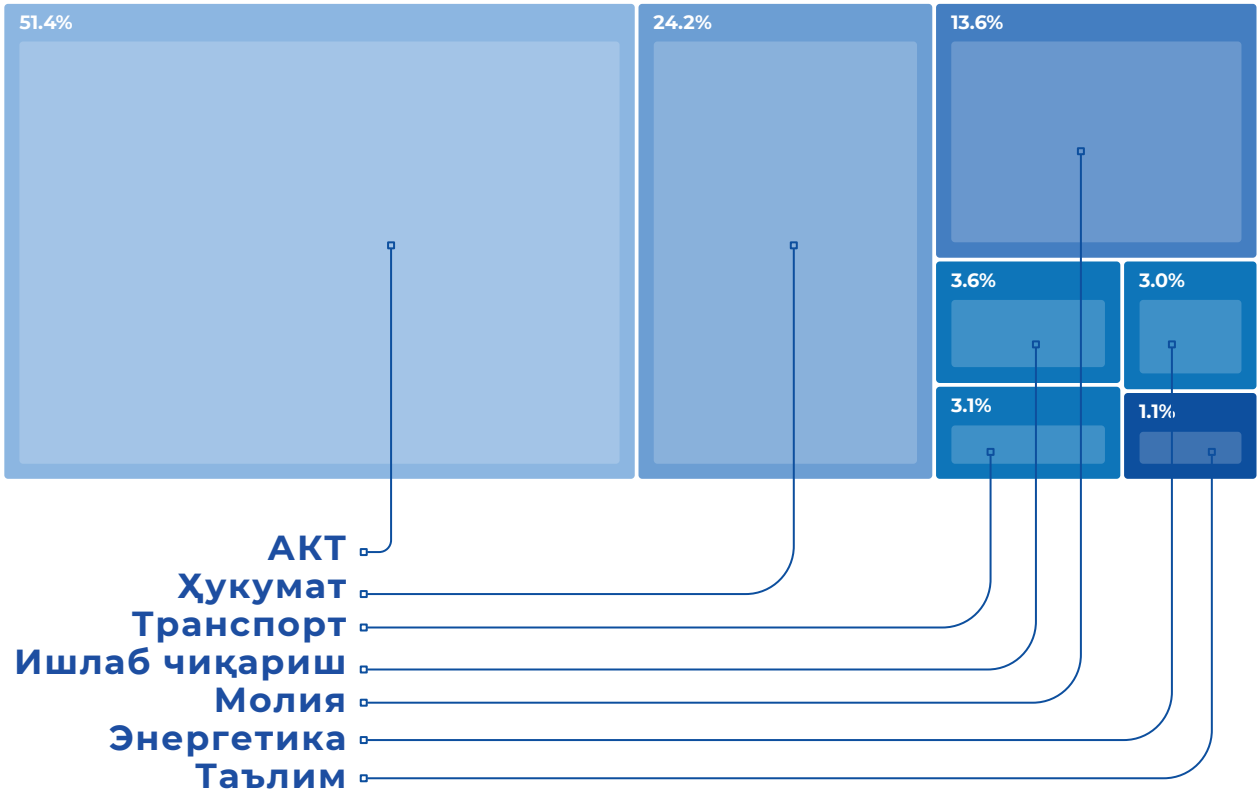
Жамланган статистик маълумотлар таҳлилига кўра, жорий йилда аниқланган заифликлар сони 2022 йил кўрсаткичларига нисбатан 3% га камайган бўлсада, веб-сайтларни ишлаб чиқишда дастурчилар томонидан веб-ресурсда юқори хавф даражасидаги заифликларнинг салмоғи 521 та (23% га ошгани)ни ва аксинча, ўрта ва қуйи даражадаги заифликлар, мос равишда 126 та (41%) ва 47 та 40% га камайганини кузатиш мумкин.

2. Марказнинг TI тизими доирасида

Ҳозирги кунда мазкур тизимга 179 дан ортиқ давлат органлари ва ташкилотлари ҳамда алоқа операторлари ва провайдерларининг ахборот тизимлари ва ресурслари уланган.

2023 йил мобайнида TI тизимида кибертаҳдидлар тўғрисидаги маълумотлар соҳалар кесимида энг кўп “АКТ” – 51.4%, “Ҳукумат” – 24.2% ва “Молия” – 13.6% соҳалари бўйича кузатилган (8-диаграмма).

Тизимда кузатилган умумий кибертаҳдидлар ҳақидаги маълумотларнинг 21.3% критик характерга эга бўлиб улар “маълум заифликлар (known vulnerabilities)”, “потенциал таҳдидлар (potential threats)” ва “эҳтимолий компроментация (suspected compromise)” категорияларига мансубдир.



8-диаграмма. Заифликлар соҳалар кесимида

2.1. Марказнинг TI тизими доирасида

Аниқланган заифликларнинг қуйидаги турлари энг кўп учрамоқда:

- CVE-2018-10549 (51 та ташкилот). Ушбу заифлик “бегона скриптлар кодини амалга ошириш” (Cross-Site Scripting - XSS) ва дастурий таъминотнинг маълум бир версиясида топилган. Ушбу заифлик масофавий ҳужумчиларга фойдаланувчи сессияси контекстида ўзбошимчалик билан скриптларни киритиш ва бажариш имконини беради, бу еса, маълумотларнинг ўғирланиши, ахборот яхлитлигининг бузилиши ҳамда бошқа ҳужумлар амалга оширилиши каби салбий оқибатларга олиб келиши мумкин.
- CVE-2019-9641 (51 та ташкилот). Нотўғри қайта ишланган кириш коднинг ўзбошимчалик билан бажарилишига олиб келиши мумкин бўлган заифлик. Тажовузкор заиф тизимга код киритиши ва бажариши мумкин, бу маълумотлар хавфсизлиги ва яхлитлигига жиддий хавф туғдиради.
- CVE-2017-7272 (51 та ташкилот). Масофавий тажовузкорга хизматни рад этишни амалга оширишга имкон берувчи заифлик. Заиф тизимга махсус тайёрланган сўровларни юбориш орқали тизим ёки унинг таркибий қисмларининг ишламай қолишига олиб келиши мумкин, бу эса қонуний фойдаланувчилар учун хизматларнинг мавжудлигига салбий таъсир қилади.
- CVE-2022-31813 (30 та ташкилот). Ушбу заифлик манба сервер/дастурий иловада IP-га асосланган аутентификацияни четлаб ўтиш учун ишлатилиши мумкин.
- CVE-2022-22720 (30 та ташкилот). Компьютерлар ёки серверларга масофадан кириш учун фойдаланиладиган дастурий таъминотдаги заифликдир. Ушбу заифлик тажовузкорларга компьютер ёки серверга тегишли аутентификациясиз масофадан киришга имкон беради, бу эса хавфсизлик ва маълумотлар махфийлигининг бузилишига олиб келади.

2.2. Марказнинг TI тизими доирасида

2023 йил мобайнида 2 637 458 та кибертаҳдидлар тўғрисидаги маълумотлар тизим ёрдамида қайта ишланиб, жами 19 294 ҳолатда киберхавфсизлик ҳодисаси юзага келишига олиб келиши мумкин бўлган заифлик ва камчиликлар хусусида тегишлилиги бўйича давлат идоралари ва операторларга хабарномалар тақдим этилди. Бунинг натижасида давлат органларида 150 дан ортиқ критик даражадаги заифликлар бартараф этилишига эришилди.

Хусусан:

- SSL POODLE заифлиги SSL 3.0 хавфсизлик протоколидаги заифлик бўлиб, тажовузкорга фойдаланувчи ва веб-сервер ўртасида узатиладиган шифрланган маълумотларни ушлаб олиш ва шифрини очиш имконини беради;
- CVE-2017-7679, CVE-2018-1312, CVE-2021-31206, CVE-2021-34473 заифликлардан фойдаланган ҳолда, тажовузкорлар тизимга киришлари ва уни бузишлари мумкин. Ушбу заифликлар “хизмат кўрсатишда рад этиш” ҳужумига олиб келиши, маълумотларни ўғирлаш ёки тизимда зарарли ҳаракатларни амалга ошириш учун ишлатилиши ёки ташкилотнинг мақсадли тизимида масофавий код бажарилишига олиб келиши мумкин;
- тизимга уланиш учун ташкилотлар томонидан тақдим этилган IP-манзилларга боғланган камера камчиликлари бартараф этилди. Ушбу камера заифликлари тажовузкорга камерага рухсатсиз киришни таъминлаши ва реал вақт режимида камера томонидан кўрсатилган тасвирни кузатиш имконини беради;
- CVE-2021-39275, CVE-2021-44790, CVE-2022-22720, CVE-2022-26377, CVE-2022-31813 заифликлардан фойдаланиш орқали сервер/дастурий иловада IP-га асосланган аутентификацияни четлаб ўтишга, сўровларни қайта йўналтиришга ва бошқа рухсатсиз ҳаракатларни амалга ошириш имконини яратади;
- CVE-2021-21974 заифлигини ташкилот тизимида масофадан мақсадли код бажарилишига олиб келиши мумкин;
- Ташкилот тизимидаги файлларни иҳтиёрий ва тасодифий ўчириб ташлаш билан боғлиқ бўлган CVE-2020-28039 заифлиги тузатилди.

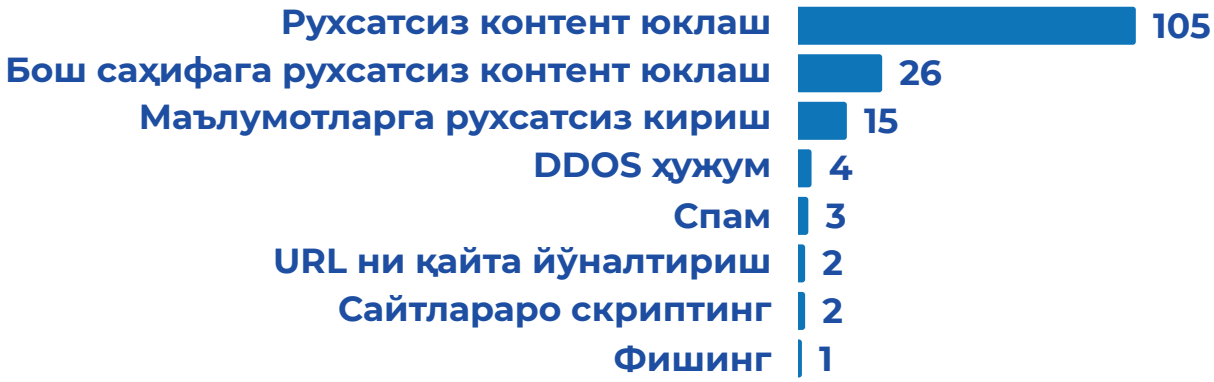
3. Аниқланган заифлик ва камчиликларнинг бартараф этилиши натижасида олди олинган салбий омиллар:

- Марказ томонидан бир қанча давлат идораларининг ахборот тизим ва ресурсларини ахборот ва киберхавфсизлик талабларига мувофиқлиги экспертизаси юзасидан амалга оширилган тадбирлар жараёнида қатор камчилик ва заифликлар аниқланиши натижасида умумий ҳисобда 25.7 миллиондан зиёд Ўзбекистон Республикаси фуқароларининг шахсий маълумотларини сизиб чиқишига, ахборотларнинг йўқ қилиниши ҳамда қалбакилаштирилишига, тизимнинг маълумотлар омбори, корпоратив почта хизмати ҳамда сервер қурилмасига тўлиқ кириш имкониятини қўлга киритиш ҳамда сервер қурилмасида жойлашган маълумотлар омборини юклаб олиш имкон берувчи салбий ҳолат ва омиллар бартараф этилди;
- мобил алоқа операторларининг 120 мингдан ортиқ мижознинг шахсий кабинетларидан рухсатсиз фойдаланиш;
- 13 мингдан ортиқ мижознинг банк тўлов карталарида мавжуд 3 миллиард сўм пул миқдори билан боғлиқ оммавий молиявий операцияларни амалга ошириш орқали катта миқдордаги пул қийматини бир вақтнинг ўзида бошқа ҳисобларга йўналтириш;
- 50 мингдан ортиқ банк операцияларини амалга ошириш билан боғлиқ фойдаланувчилар имкониятидан ноқонуний (рухсатсиз) фойдаланиш (банк мижозларининг шахсий кабинетлари орқали пул ўтказмаларини амалга ошириш, хорижий валютани конвертация қилиш ва ҳ.к.);
- 1,25 млндан ортиқ конфиденциал маълумотларга ноқонуний эга бўлиш (паспортлар, туғилганлик ҳақида гувоҳно-малар, ID карталар, тиббий маълумотлар ва ҳ.к.);
- 8,5 мингдан ортиқ молиявий транзакциялар тўғрисидаги маълумотларга ноқонуний эга бўлиш (ойлик маош қайдномалар, ҳисоб варақалар, миллий ва хорижий валютадаги тўлов ҳужжатлар ва ҳ.к.) каби салбий оқибатлар олди олинди.

Веб-ресурсларда юзага келган киберхавфсизлик ҳодисалари

Интернет тармоғи миллий сегментидаги веб-ресурсларнинг доимий мониторинги жараёнида жами 158 та (2022 йилга нисбатан 32% га кам) киберхавфсизлик ҳодисаси аниқланди. (9-диаграмма) Улардан 38 таси давлат органлари веб-ресурслари ҳисобига тўғри келди. Қуйида аниқланган ҳодисаларнинг асосий турлари келтирилган (10-диаграмма).

9-диаграмма. Киберхавфсизлик ҳодисалари сони йиллар кесимида.



10-диаграмма. Аниқланган киберхавфсизлик ҳодисалари турлари

Давлат идоралари веб-ресурсларида аниқланган киберхавфсизлик ҳодисалари ўрганилганда веб-ресурсларда мавжуд бўлган қуйидаги заифликлар сабабли юзага келганлиги кузатилди:

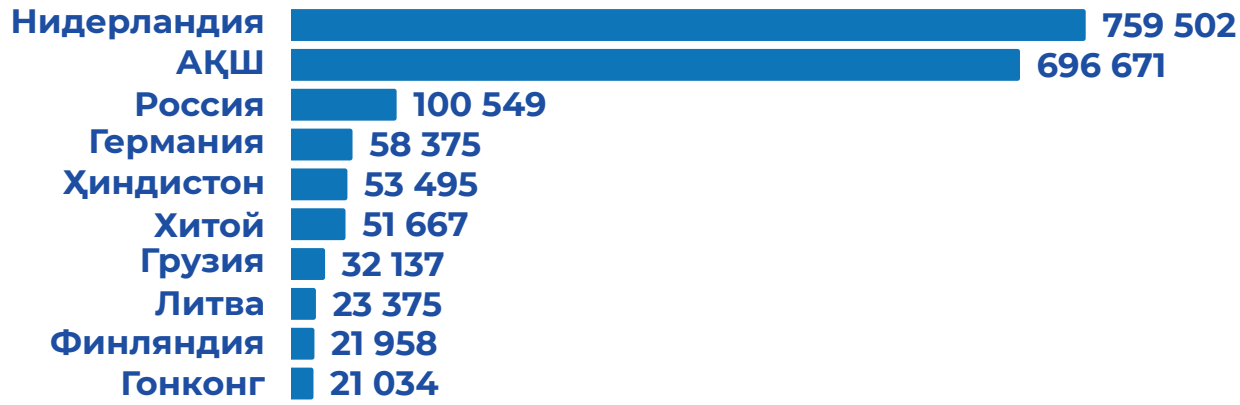
- фойдаланувчи контентини текшириш ва фильтрлашнинг мавжуд эмаслиги;
- кодлашдаги заифликлар (PHP-плагинлари, csfr-заифликлари, кросс-браузер заифликлари ва бошқалар);
- заиф парол ҳимояси.

Веб-ресурсларга бўлган киберҳужумлар

Статистик маълумотлар таҳлилига кўра, Марказнинг автоматлаштирилган тизимлари ёрдамида ҳисобот йилида қайд этилган тармоқ ҳужумларининг интенсивлигида сезиларли ўсиш тенденцияси мавжуд бўлиб, 2022 йилга нисбатан мазкур кўрсаткич 148% га ортган (11-диаграмма).

11-диаграмма. Веб-ресурсларга бўлган киберҳужумлар йиллар кесимида.

2023 йилда амалга оширилган киберҳужумларнинг географик жиҳатдан тааллуқлилиги таҳлилига кўра, қуйида келтирилган давлатлар ҳудудидаги IP-манзиллардан энг кўп киберҳужумлар уюштирилганлиги кузатилди (12-диграмма).



12-диаграмма. Веб-ресурсларга бўлган киберҳужумлар давлатлар кесимида.

Мониторинг тизимига уланган веб-ресурсларга уюштирилган киберҳужумларнинг турлари орасида энг қўп қўлланилганлари қуйидагича тақсимланди (13-диаграмма)

13-диаграмма. Киберҳужумлар турлари кесимида.

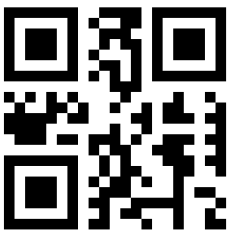
Веб-ресурсларда юзага келган техник носозликлар

Давлат органлари веб-ресурслари мониторинги натижасида 140 та давлат идорасининг веб-ресурсларида умумий ҳисобда 1129 марта (2022 йилга нисбатан 36% га кўп) турли техник носозликлар туфайли ишдан чиқиши қайд этилди (14-диаграмма). Носозликлар бартараф этилиши учун кетган жами вақт 22660 соат 22 дақиқани ташкил этган. қуйида техник носозликлар асосий турлари келтириб ўтилган (15-диаграмма).

14-диаграмма. Веб-ресурслардаги техник носозликлар йиллар кесимида.

15-диаграмма. Веб-ресурслардаги техник носозликлар сабаблари.

Марказ томонидан қайд этилган у ёки бу расмий веб-сайтнинг ишида вужудга келган муаммолар, жумладан, ушбу ахборот ресурсига киришнинг чекланиб қолиши билан боғлиқ фактлар юзасидан Марказ ходимлари томонидан зудлик билан тегишли ташкилотларнинг масъул ходимлари билан боғланиш, тезкор хабар бериш ва киберҳодиса сабаблари ҳақида бирламчи маълумотлар олиш амалиёти татбиқ этилган.



Ўзбекистон Республикаси, 100115,
Ташкент ш., Тарас Шевченко кўчаси, 20

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

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