



ЎЗБЕКИСТОН РЕСПУБЛИКАСИ КИБЕРХАВФСИЗЛИГИ



2020 ЙИЛ ҲИСОБОТИ

МУНДАРИЖА

Кириш

Таҳдидлар

Ҳодиса ва воқеалар

Киберхавфсизлик ҳодисаларни текшириш

Заифликлар

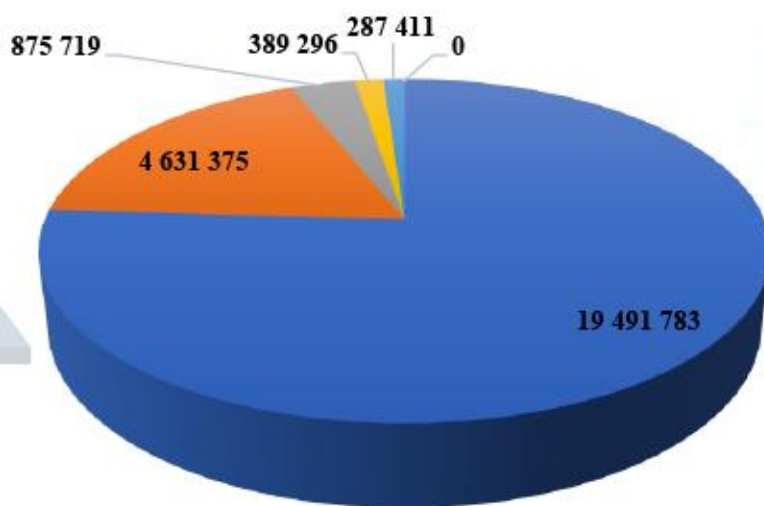
Сертификатлаш

Кириш

Мамлакатимиз рақамлаштириш асрига ишонч билан қадам қўйди ва бунга ҳукумат томонидан қаратилаётган эътибор асос бўла олади. Доимий тарзда амалга оширилаётган интернет тезлиги ва сифатини ошириш, замонавий ахборот-коммуникация технологияларини ҳаётимизга тадбиқ қилиш, ахборотлаштириш тизимларини такомиллаштириш билан биргаликда, ҳукумат алоҳида эътиборни киберхавфсизлик соҳасига ҳам қаратмоқда. “Киберхавфсизлик маркази” давлат унитар корхонаси юртимизда кибер муҳитни хавфсиз ва соғломлигини таъминлаш, ахборотлаштириш тизимларини доимий ва узлуксиз ишлашини қўллаб қувватлаш, ва зарарли кибер хужумлардан ҳимоя қилиш учун ўз олдига бир қатор мақсад ва вазифаларни қўйган. Ўрнатилган мақсад ва вазифаларни тўлақонли бажариш учун Марказ томонидан миллий интернет сегментида ахборот ва киберхавфсизлик ҳодисаларини доимий мониторинг қилиб бориш йўлга қўйилган.

Таҳдидлар

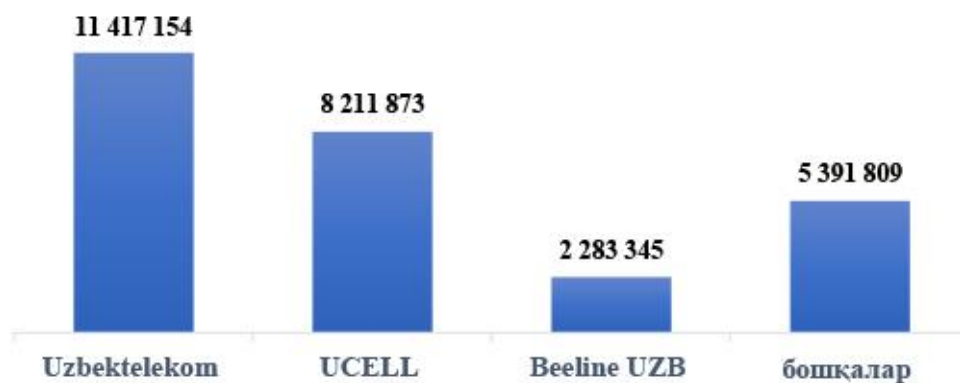
Мониторинг натижаларига кўра, ўтган 2020 йил давомида миллий интернет сегментида ахборот ва киберхавфсизликка таҳдид солувчи 27 000 000 дан ортиқ зарарли ва шубҳали тармоқ ҳодисалари кузатилди (1 – Расм). Улардан:



- ботнет тизимлардаги фаоллик
- қора рўйхатларга тушиш
- ҳимоясиз (очик) SWMP протоколи
- ҳимоясиз (очик) NTP протоколи
- ҳимоясиз (очик) HTTP протоколи
- бошқалар

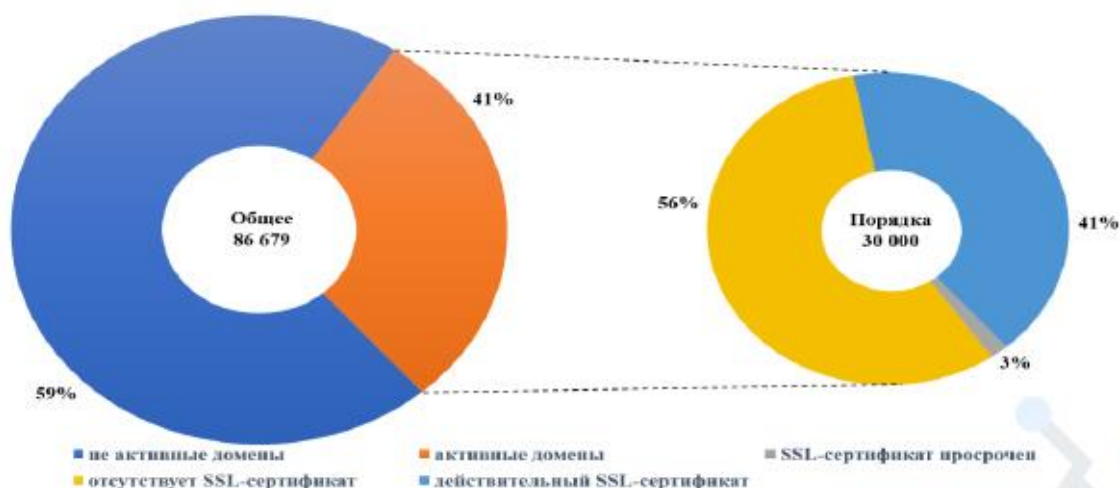
(1 – Расм: Кузатилган таҳдидларнинг асосий салмоғи)

Юқорида келтирилган таҳдидларнинг асосий қисми Uzbektelecom, Ucell ва Beeline компанияларининг манзиллар гуруҳидалиги аниқланди (2 – Расм).



(2 – Расм: Тахдидларнинг асосий қисми кузатилган компаниялар)

2020 йил охирига келиб 86 679та “.UZ” миллий доменлар рўйхатдан ўтказилган ва ҳозирда улардан қарийб 30 000 таси фаол. Шунингдек, доменларнинг 12 500 тасида SSL-Сертификатлари мавжуд, аммо уларнинг 300тасида сертификатларнинг муддати ўтган (3 – Расм)..



(3 – Расм: Фаол доменлар рақамларда)

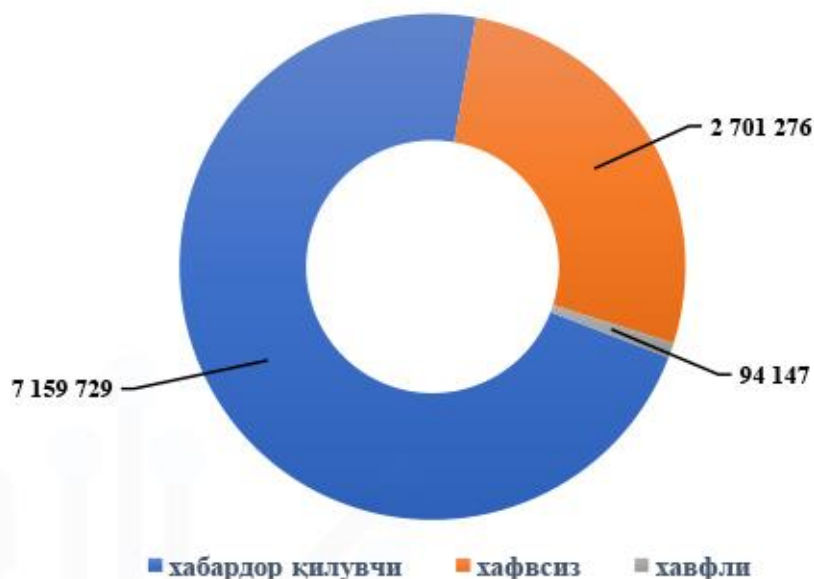
Ҳодиса ва воқеалар

Ўтган 2020 йил давомида ахборот тизимлари ва веб-сайтларнинг хавфсизлигини таъминлаш доирасида 680та ҳодиса рўй берган (4 – Расм), шу жумладан носозликлар 1 000 000 дақиқа вақт мобайнида веб-сайтларнинг ишдан чиқиш ҳолати кузатилган.



(4 – Расм, Ҳодиса ва воқеаларнинг турлари)

Шу билан бирга, идоралараро маълумотлар узатиш тармоғига уланган ахборот тизимларида 9 955 152 та ҳодиса қайд қилинган бўлиб (5-расм), шундан 94 147 таси махфий маълумотлар базасининг бузилиши ва конфиденциал маълумотларнинг тарқалишига олиб келувчи хавфли ҳодиса эканлиги аниқланди (6-расм).



(5 – Расм. Идоралараро маълумотлар узатиш тармоғига уланган тизимларда аниқланган ҳодисалар)



(6 – Расм. Хавфли ҳодисалар)

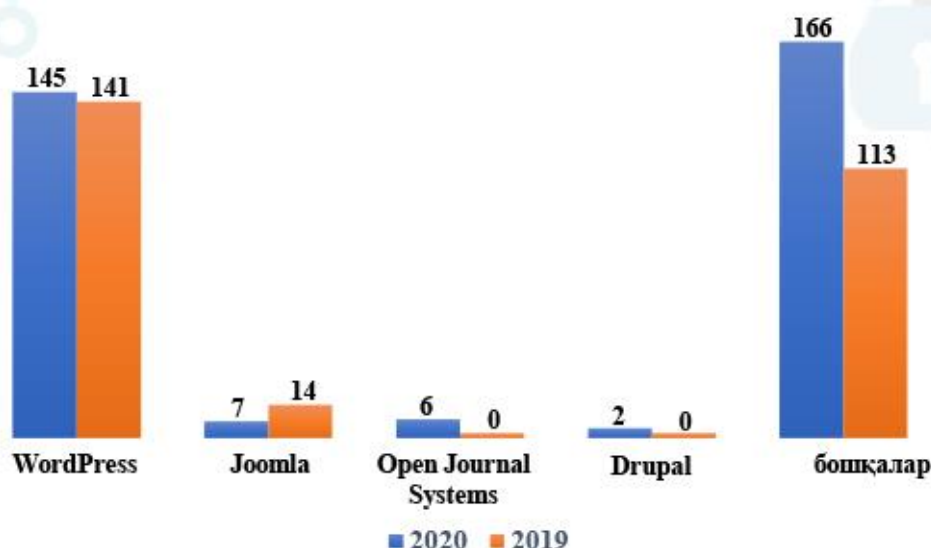
Миллий “.UZ” домен ҳудудида юз берадиган воқеалар мониторингидан ташқари, ҳодисалар ҳам қайд қилиниб борилади. Шу вақт давомида 342 ҳодиса аниқланиб, улардан 306таси веб-сайтларга руҳсатиз контент юклаш ва қолган 36таси эса бузилган веб-сайтнинг асосий саҳифаси ноқонуний ўзгартириб (deface) қўйилиши эканлиги аниқланди.

Шуни таъкидлаш керакки, давлат сектори (81 та ҳодиса) хусусий секторга нисбатан (261 та ҳодиса) 3 барабар камроқ ҳужумга дуч келган. 2019 йилдаги рақамларга солиштирганда ўтган йилда руҳсатсиз контент юклаш ҳодисаси камроқ ва веб-сайтнинг асосий саҳифасини ноқонуний ўзгартириш ҳодисаси эса кўпроқ кузатилганини кўриш мумкин (7 – Расм).



(7 – Расм. 2019-2020 йилда кузатилган ҳодисалар фарқи)

Ҳодисаларни таҳлил қилишда шу кузатилдики, «WordPress», «Joomla», «Open Journal Systems» и «Drupal» контент бошқарув тизимларида (CMS) заифликлар кўп бўлиб, уларга тез-тез ҳужумлар амалга оширилади (8 – Расм)



(8 – Расм. 2019-2020 йилда кузатилган ҳодисалардаги фарқ)

Киберхавфсизлик ҳодисаларни текшириш

Зарарли таркибга эга бўлган контентни аниқлаш ва уни ҳуқуқбузарликка алоқадорлигини таҳлил қилиш учун махсус ҳодисавий текшириш жараёнлари амалга оширилди, уларнинг келиб чиқиш сабаблари ўрганилди (9 – Расм).

Хусусан, текширувлар натижасида 2690 дан ортиқ зарарли файллар ноқонуний равишда юклангани аниқланиб, бузғунчи деструктив ҳаракатлар

амалга оширилган интернет манзиллар қуйидаги мамлакатларга тегишлилиги аниқланди: Руминия, Германия, Миср, Словакия Республикаси, АҚШ, Индонезия, Хитой, Россия Федерацияси, Буюк Британия, Франция, Саудия Арабистони, Тунис, Украина, Голландия, Жанубий Корея, Канада, Франция, Туркия, Полша, Ветнам, Ҳиндистон.

Энг кўп деструктив ҳаракатлар амалга оширилган интернет манзиллари қаторига Америка Қўшма Штатларида, Германия, Россия Федерацияси, Голландия ва Туркия мамлакатлари киради.

Таъкидлаш жоизки, 2019 йилнинг шу даврига нисбатан давлат ва хўжалик бошқаруви органлари веб-сайтларига нисбатан содир этилган ҳодисалар сони 144 фоизга ўсган.



(9 – Расм. Ҳодисалар содир бўлш сабаблари ва хужум векторлари)

Заифликлар

2020 йилда миллий ".UZ" домен ҳудудининг замонавий ахборот тизимлари ва ресурслари хавфсизлигини ошириш бўйича чора-тадбирларни амалга ошириш давомида 297 та тадқиқот ва экспертиза ўтказилди.

Амалга оширилган ишлар натижасида 695та заифликлар аниқланиб (10 – Расм), заифликлар ҳақида ахборот тизим ва ресурс эгалари дарҳол хабардор қилинди. Аниқланган заифликларнинг асосий қисми:

- Ўта хавfli даражадаги – 466та;
- Ўрта хавfli даражадаги – 205та;
- Паст хавfli даражадаги – 24та.



(10 – Расм, Аниқланган заифликларнинг асосий турлари)

Юқорида келтирилган заифликларлар ўз вақтида бартараф этилиб, Ўзбекистон Республикаси фуқароларининг конфиденциал маълумотларининг ўғирланиши олди олинди.

Сертификатлаш

Ахборот хавфсизлигини бошқариш тизимлари, техник воситалар, дастурий маҳсулотлар, ахборот-коммуникация технологиялари, телекоммуникация ускуналари ва бошқа техник воситалар, шу жумладан ахборот хавфсизлигини таъминлаш воситаларининг сифатини тасдиқлаш мақсадида Марказ томонидан маҳсулотларнинг ахборот ва киберхавфсизлиги бўйича меъёрий ҳужжатлар талабларига мувофиқлиги сертификатлашдан ўтказилади.

2020 йил давомида 45 та дастурий таъминот мувофиқлик сертификатларини олди (11-расм), ва шу қаторда улар ичида «Cent OS Linux 8» умумий мақсадли операцион тизимининг 5.8.14 версияси ҳам муваффақиятли сертификатлаш жарарёнидан ўтди.



(11 – Расм, Мувофиқлик сертификатини бериш)



KIBERXAVFSIZLIK MARKAZI



info@csec.uz



www.csec.uz



(55) 502-10-10