Тошев Отабек Содикович
Ўзбекистон Республикаси Адлия вазирлиги ҳузуридаги Ҳуқуқий сиёсат тадқиқот институти, бўлим бошлиғи, ТДЮУ мустақил изланувчиси
Анорбоев Амириддин Улуғбек ўғли
Ўзбекистон Республикаси Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги Юридик бўлим бош юрисконсульти, ф.ф.д. (PhD)

АХБОРОТ-КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИДАН ЗАРАРЛИ МАҚСАДЛАРДА ФОЙДАЛАНИШНИНГ САЛБИЙ ОҚИБАТЛАРИ ВА АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ ИСТИҚБОЛЛАРИ

Тошев Отабек Содикович
Начальник отдела Научно-исследовательского института правовой политики при Министерстве юстиции Республики Узбекистан, самостоятельный соискатель ТГЮУ
Анорбоев Амириддин Улугбек угли
Доктор философских наук, главный юрисконсульт Юридического отдела Министерства по развитию информационных технологий и коммуникаций Республики Узбекистан

НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ВРЕДНЫХ ЦЕЛЯХ И ПЕРСПЕКТИВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Toshev Otabek
Head of the department, The Research Institute of Legal Policy under the Ministry of Justice of the Republik of Uzbekistan, independent researcher at TSUL
Anorboev Amiriddin
Deputy Head of the Department of the Ministry of Information Technologies and Communications of the Republic of Uzbekistan

NEGATIVE CONSEQUENCES OF USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES FOR HARMFUL PURPOSES AND PROSPECTS FOR INFORMATION SECURITY

Барчамизга маълумки, 2017–2021 йилларда Ўзбекистон Республикасини ривожлантиришнинг бешта устувор йўналиши бўйича Ҳаракатлар стратегиясида белгиланган истиқболдаги вазифаларни амалга ошириш мақсадида республика иқтисодиётининг рақамли секторини ривожлантириш борасида кенг кўламли чора-тадбирлар олиб борилмлқда, электрон ҳужжат айланиши тизимлари, электрон тижорат соҳасидаги норматив-ҳуқуқий база такомиллаштирилмоқда, электрон тўловлар ва ахборот-технологик платформаларда фаолият кўрсатадиган рақамли иқтисодиёт жадал ривожлантирилмоқда, “Блокчейн” технологиялари (маълумотларнинг тақсимланган реестри технологиялари), “сунъий ақл”, суперкомпьютерлар имкониятларидан фойдаланиш, шунингдек, криптоактивлар бўйича фаолият кенгаймоқда, бунда “Блокчейн” технологиялари нафақат иқтисодиётнинг кўплаб секторларига, балки давлат бошқаруви тизимига ва бошқа жамоатчилик муносабатларига аста-секин жорий этилмоқда.

Бироқ ушбу ислоҳотларга тўғаноқ бўлаётган хавфнинг мавжудлиги бу борада зарур чоралар кўришни тақозо этади. Мазкур хавф-хатарлар ичида кибержиноятчилик ўзининг кенг кўламли ва жуда катта, асосан бартараф этиш имконсиз бўлган зарар келтириши билан ажралиб туради. Ҳозирги кунда Ўзбекистонда ҳам бошқа давлатларда бўлгани каби киберҳужумлар сони ортиб бормоқда. Мамлакатда 2019 йил бошидан буён ахборот хавфсизлиги билан боғлиқ 8 миллионга яқин ҳолат қайд этилган бўлиб, уларнинг бир қисми юқори хатарга эга бўлган.

Оддийгина рақамларга эътибор берайлик, ҳар йили 556 млн.дан 1,5 млн.га яқин инсонлар кибержиноятчиликнинг қурбони бўлишмоқда ва улар кўрадиган зарар 110 млрд доллардан ортиқроқдир. Статистик маълумотларга қараганда, киберҳужумлар сони 2019 йилнинг биринчи чорагида Ўзбекистон аҳолисининг 17 фоизига, иккинчи чорагида бу кўрсаткич 26 фоизга етган.

Бу эса соҳада олиб борилаётган ислоҳотларни янада ривожлантиришни, кибержиноятчиликдан Ўзбекистон иқтисодиётини муҳофаза қилиш зарурлигини кўрсатади, энг ачинарли ҳолат шуки, йирик “Apple”, “Google” ва “Facebook” компанияларининг билдиришича, рақамли технологияларни мураккаб шифрлаш зарур ва бунда улар шифрлаш енгиллаштирилгудек бўлса, киберҳужумлар ортиб, шахсий маълумотлар йўқолиши ҳолатларининг кўпайишига сабаб бўлиши билан бирга, ўғирланган маълумотлардан дўстона муносабатда бўлмаган хорижий давлатлар махсус хизматлари фойдаланиши ҳам мумкинлигини маълум қилишган. Бу ўз навбатида шахсга доир маълумотларнинг ўзга давлатлар, айниқса, бир гуруҳ ёвуз мақсадларни кўзловчи шахсларнинг қўлига тушиши ва ушбу маълумотлар орқали уларнинг исталган шахсга таъсир ўтказиши мумкинлиги, энг олий қадрият бўлган инсон тақдирининг кейинги ривожига жуда катта хавф келтириши мумкинлигини англатади.

Кибержиноятчилик рақамли технологияларга турли усулларда зарар етказиши мумкинлиги, хусусан, хакерлар томонидан Bad Rabbit шифрловчи вируси ёрдамида Россия Федерацияси ҳудудидан туриб, турли мамлакатларда 200 дан ортиқ киберҳужумлар амалга оширганлиги, ҳатто бу ҳолат Украина, Туркия, Германия каби ривожланган давлатларда ҳам қайд этилганлиги кундалик эҳтиёжларимизни амалга ошириш учун енгиллик яратувчи технологияларнинг кейинги ривожи жуда катта хавф остида эканлигини англатади, қолаверса, бу хавф инсонларнинг ҳаётига ҳам таъсир этмай қўймайди.

Кибержиноятчиликнинг энг хавфли жиҳатларидан яна бири шуки, бу давлат томонидан амалга оширилаётган ислоҳотларда аҳолининг давлат органларига бўлган ишончи йўқолишига сабабчи бўлиши мумкин, мисол учун, АҚШда 2019 йилнинг ўзида 40 дан ортиқ Америка шаҳарларида киберҳужумлар бўлиши оқибатида, деярли барча давлат органлари ва идоралари киберҳужумнинг объектига айланиб қолган ва натижада бир вақтнинг ўзида давлат идораларининг ахборот технологиялари ва коммуникациялари ишламай қолиши оқибатида аҳолининг давлат органларига нисбатан норозилиги кучайиб кетган.

Киберҳужумларнинг ўзга мамлакат ҳудудидан туриб ҳам содир этилиши мумкинлиги, бунда рақамли технологияларнинг хавфсизлигини таъминловчи портлар ва серверлар ўзга мамлакат ҳудудида жойлашганлиги бу борада кўрилиши мумкин бўлган зарарларнинг янада улканроқ бўлишини таъминлайди.

Жумладан, сервери чет давлатда бўлган “Telegram”, “Facebook” ва бошқа тармоқларнинг ўзга давлат ҳудудида жойлашганлиги сабабли ҳам мавжуд киберҳужумнинг олдини олишни қийинлаштиради, энг ёмони киберҳужумни амалга оширган шахсларни аниқлаш имконсизлигини келтириб чиқаради, айбдор шахсларни топиш учун ушбу мессенжерларнинг муаллифларидан розилик сўрасангиз улар шахсга тегишли маълумотлар ошкор этилмаслигини таъминлаш мақсадида сўралган маълумотларни беришдан воз кечадилар.

Киберҳужум истаган ахборот технологияси ва коммуникациясига нисбатан амалга оширилиши мумкин, биргина “Telegram” тармоғини олайлик, 2019 йил 22 ноябрь куни бўлган киберҳужум оқибатида 67 фоиз фойдаланувчилар киберҳужум остида қолган, ўзбекистонлик фойдаланувчилар ҳам шулар жумласидандир.

Рақамли технологиялар ва электрон ҳукуматга амалга оширилаётган киберҳужумларни бартараф этишда ҳозир қуйидаги тўрт гуруҳга ажратилган қийинчиликлар мавжуд:

– ташкилий;
– техник;
– молиявий;
– ҳуқуқий.

Ташкилий муаммоларга қуйидагилар киради:

биринчидан, кибержиноятчилик бўйича ягона давлат бошқаруви органи ва унинг ташкилий фаолиятини тартибга солувчи қонун ҳужжатларининг мавжуд эмаслиги;

иккинчидан, кибержиноятчиликка қарши курашиш бўйича амалга ошириладиган ташкилий масалаларни амалга ошириш юзасидан аниқ механизмнинг йўқлиги;

учинчидан, бу соҳага оид кадрларнинг қўнимсизлиги ва етук мутахассисларнинг деярли йўқлиги;

тўртинчидан, яратилган имкониятлардан лозим даражада фойдаланилмаётганлиги билан боғлиқ муаммолар кўпайиб кетмоқда;

бешинчидан, киберхавфсизликни таъминлаш билан боғлиқ масалалар юқори даражада (Ўзбекистон Республикаси Олий Мажлиси палаталари ёки Президент) ҳал этилишида муаммолар мавжуд;

олтинчидан, киберхавфсизликни таъминлашга ваколатли бўлган органлар томонидан давлат органлари ва хусусий сектордаги ахборот технологиялари ва коммуникацияларининг киберхавфсизлигини комплекс таъминлаш чоралари етарли даражада амалга оширилмаяпти.

Техник муаммоларга қуйидагилар киради:

биринчидан, Ўзбекистон Республикасига кирадиган ва мавжуд ахборот технологиялари ва коммуникацияларининг замон талабларига тўлиқ жавоб бермаслиги;

иккинчидан, мавжуд технологиялардан фойдаланиш юзасидан ягона услубиётнинг мавжуд эмаслиги;

учинчидан, мавжуд ахборот технологиялари ва коммуникацияларини сертификатлаштириш, лицензиялаш, стандартлаштириш билан боғлиқ масалалар юзасидан турли хил амалиёт шаклланганлиги.

Молиявий муаммоларга қуйидагилар киради:

биринчидан, айнан ахборот-коммуникация технологияларини жорий қилишда киберхавфсизликни таъминлашга ихтисослашган техник ускуналар, компьютер ва сервер ускуналари ҳамда дастурий маҳсулотларни харид қилиш ва уларни ўрнатиш билан боғлиқ ишларни молиялаштириш механизмининг аниқ белгиланмаганлиги;

иккинчидан, хавфсиз кибермаконни таъминлаш билан боғлиқ ишларни молиялаштиришнинг ягона молиявий манбага эга эмаслиги;

учинчидан, рақамли технологияларни ривожлаштириш ва хавфсиз кибермаконни яратиш бўйича молиявий номутаносибликнинг мавжудлиги;

тўртинчидан, рақамли технологияларни кенг жорий қилиш ва киберхавфсизликни таъминлаш бўйича ажратилиши зарур бўлган пул маблағларининг ўз вақтида ажратилмаганлиги;

бешинчидан, соҳани ривожлантириш учун ажратилган пул маблағларининг мақсадли ишлатилиши ва унинг назорати билан боғлиқ муаммолар мавжудлиги.

Ҳуқуқий муаммоларга қуйидагилар киради:

биричидан, кибержиноятчиликка қарши курашиш ва киберхавфсизликни таъминлаш бўйича ягона қонунчиликнинг мавжуд эмаслиги;

иккинчидан, соҳага оид ягона миллий стратегия, концепция ва "йўл-хариталари" ишлаб чиқилмаганлиги;

учинчидан, соҳага оид ўқув курси ёки фаннинг мавжуд эмаслиги;

тўртинчидан, соҳани ўргатиш ва кадрлар тайёрлаш бўйича ягона амалиётнинг шаклланмаганлиги;

бешинчидан, соҳага оид норма ижодкорлигида изчилликнинг мавжуд эмаслиги;

олтинчиандан, соҳани ўргатиш ва ўқитиш бўйича ҳуқуқий онг ва ҳуқуқий маданиятни шакллантириш воситаларининг мавжуд эмаслиги.

Мазкур муаммолар реал ҳаётимизда учраётганлиги бўйича баъзи ҳолатларни кўриб ўтсак, шу пайтга қадар амалга оширилаётган ислоҳотлар орқали Ўзбекистон Халқаро электр алоқа иттифоқининг глобал киберхавфсизлик индексида 40 поғона юқорилаб, 175 давлат орасида 52-ўриндан жой олганлигини кўрамиз.

Ваҳоланки, амалга оширилган бу ислоҳотлар асосан техник томондан содир этилган жараёнлар бўлиб, ушбу ислоҳотларнинг ҳуқуқий таъминланиши борасида республикамиз олдида бажариши зарур бўлган ишлар бисёр.

Хусусан, Ўзбекистон Республикасининг "Киберхавфсизлик тўғрисида"ги Қонуни, ушбу қонун асосида киберхавфсизликни таъминлаш ва кибержиноятчилика қарши курашиш, киберҳуқуқбузарликларни бартараф қилиш бўйича ўрта муддатга мўлжалланган ягона миллий стретегия ишлаб чиқилиши, ушбу стратегия асосида эса ҳар йили киберхавфсизликни таъминлаш бўйича концепция ҳамда концепцияда қайд этиб ўтилган вазифаларни амалга ошириш бўйича давлат дастурлари ва "йўл-хариталари"ни ишлаб чиқиш ва амалиётга татбиқ қилиш вақти етиб келди.

Жаҳон мамлакатларининг қонунчилигига қарасак, уларда аллақачон, киберҳужумдан ҳимояланиш бўйича зарур қонун ҳужжатлари қабул қилинган ва улар ҳозир амалда. Хусусан, Германия, Буюк Британия, Канада, Литва, Люксембург, Нидерландия, АҚШ, Эстония, Япония, Хитойда стратегик ва ҳукумат ахборот тизимларини киберҳужумлар ва кибертерроризмдан, Словакия, Франция, Чехия, Литвада маълумотлар ва шахсий маълумотларни ҳимоя қилиш бўйича алоҳида қонун ҳужжатлари қабул қилинган.

Дунёда кибержиноятчилик тобора хавфли тус олиб, кунига бундай ҳолат200 мингдан ортиқ содир этилмоқда, натижада жисмоний ва юридик шахсларга 500 млрд.га яқин мулкий зарар етказилмоқда, биргина мисол, 2016 йилда Juniper Research томонидан ўтказилган тадқиқотда, 2019 йилга келиб, компьютер жиноятчилигидан етказиладиган зарар 2,1 трлн долл.

дан ортиб кетиши мумкинлиги ва ҳар ойда содир этилаётган жиноятлар 10-15% га ортиб бораётганлиги бу балога қарши аниқ тактик режалар, яъни стратегия ишлаб чиқилиши зарурлигини кўрсатади.

Хусусан, Украина Президентининг 2016 йил 15 мартдаги 96/2016-сонли Фармони билан Украина киберхавфсизлик стратегияси тасдиқланган. Шу каби стратегиялар АҚШ, Эстония, Литва, Испания, Германия, Словакия, Япония, Швейцария, Норвегия, Янги Зеландия, Ҳиндистон, Австралия, ЖАР, Канада, Финландия, Австрия, Руминия, Польша, Франция, Чехия, Нидерландия, Люксембург ва бошқа давлатларда қабул қилинган.

Кўриб ўтганимиздек, бу борада зарур ислоҳотларни амалга ошириш орқалигина мамлакатимизга бўлаётган киберҳужумларга оид балолар бартараф қилиниши мумкин.

Энг ачинарлиси, ушбу балолар бўйича аниқланган кибер ҳуқуқбузарликлар ва кибержиноятчилик бўйича айбдорларни аниқлаш, уларни жавобгарликка тортиш механизмлари Ўзбекистон қонунчилигида кўрсатиб ўтилмаганлиги ва мавжуд қонунчилигимиз бўйича Жиноят кодекси ёки Маъмурий жавобгарлик тўғрисидаги кодексда назарда тутилмаган ҳолатлар бўйича шахсларни жавобгарликка тортиш мумкин эмаслиги, киберҳужумнинг ўзга давлат ҳудудидан туриб содир этилганлиги ҳолати билан боғлиқ муаммолар қонунчилигимизни қайта кўриб чиқишни тақозо этмай қўймайди.

Шунга кўра, Ўзбекистон Республикаси Президентининг 2018 йил 14 майдаги ПҚ–3723-сонли “Жиноят ва жиноят-процессуал қонунчилиги тизимини тубдан такомиллаштириш чора-тадбирлари тўғрисида”ги қарори, 2019 йил 17 январдаги ПФ–5635-сонли Фармони билан тасдиқланган “2017–2021 йилларда Ўзбекистон Республикасини ривожлантиришнинг бешта устувор йўналиши бўйича Ҳаракатлар стратегияси”ни “Фаол инвестициялар ва ижтимоий ривожланиш йили”да амалга оширишга оид давлат дастурининг 44-банди, “Жиноят-ижроия қонунчилигини тубдан такомиллаштириш чора-тадбирлари тўғрисида” 2018 йил 7 ноябрдаги ПҚ–4006-сонли қарори ижросини таъминлаш, шунингдек, мамлакатда киберхавфсизликка қарши курашиш чораларини янада кучайтириш мақсадида Ўзбекистон Республикасининг жиноят, жиноят-процессуал, маъмурий жавобгарлик тўғрисидаги, жиноят-ижроия кодекслари қайта кўриб чиқилиши ва ушбу кодексларда кибержиноятчилик тушунчаси, турлари, улар бўйича суриштирув, дастлабки таргов, суд терговини амалга оширишнинг ўзига хос хусусиятлари, қайси кибержиноят ва киберҳуқуқбузарликлар учун жазо мавжудлиги, жазони либераллаштириш мақсадида ахборот технологиялари ва коммуникациялари бўйича махсус билимга эга шахсларга нисбатан жазо тайинлашнинг ўзига хос жиҳатлари, келтирилган зарарни қоплаш, фуқаровий даъвони таъминлаш

усулларининг ўзига хос белгилари, кибержиноятчини республика ва республика ҳудудидан ташқари ҳудудларда топиш, ушлаш, жазога тортиш билан боғлиқ қоидалар, кибержиноятчилик содир этилган вақтни аниқлашнинг ўзига хос жиҳатлари ва бошқа шу каби қоидаларни белгилаб ўтиш мақсадга мувофиқ.

Амалга оширилаётган ислоҳотлар борасида ҳозирги кунда янги Ўзбекистоннинг техник имкониятларини кенгайтириш, шахсга оид қонун ҳужжатларининг нормаларини аниқ белгилаш, давлат ва жамият хавфсизлигини турли хил ҳужумлардан бартараф қилиш мақсадида ҳозирги кунда давлат идораларидаги мавжуд “Telegram”, “Facebook” ва бошқа тармоқларнинг ўзга давлат ҳудудида жойлашганлиги ва ушбу тармоқ орқали амалга оширилаётган ҳужумларни бартараф қилиш ва бу борадаги муаммоларни ўз вақтида ечимини топиш мақсадида давлат идораларнинг расмий ижтимоий тармоқларини миллийлаштириш ва миллий контентни тубдан такомиллаштириш чораларини кўриш ва бунда Ахборот технологиялари ва коммункиацияларини ривожлантириш вазирлигининг ролини ошириш чораларини кўриш мақсадга мувофиқ.

Маълумки, Ўзбекистон Республикаси Президентининг “Ўзбекистон Республикасида рақамли иқтисодиётни ривожлантириш чора-тадбирлари тўғрисида” 2018 йил 3 июлдаги ПҚ–3832-сонли қарори билан қуйидагилар рақамли иқтисодиётнинг энг устувор вазифалари этиб белгилаб қўйилди:

– инвестициявий ва тадбиркорлик фаолиятининг турли шаклларини диверсификация қилиш учун криптоактивлар айланмаси соҳасидаги фаолиятни, жумладан, майнинг (турли криптовалюталарда янги бирликлар ва комиссия йиғимлари форматида мукофот олиш имконини берадиган тақсимлаш платформасини таъминлаш ва янги блоклар яратиш бўйича фаолият), смарт-контракт (рақамли транзакцияларни автоматик тартибда амалга ошириш орқали ҳуқуқ ва мажбуриятлар бажарилишини назарда тутувчи электрон шаклдаги шартнома), консалтинг, эмиссия, айирбошлаш, сақлаш, тақсимлаш, бошқариш, суғурталаш, крауд-фандинг (жамоавий молиялаштириш), шунингдек, “блокчейн” технологияларини жорий этиш ва ривожлантириш;

– “блокчейн” технологияларини ишлаб чиқиш ва улардан фойдаланиш соҳасида замонавий ахборот-коммуникация технологияларидан фойдаланган ҳолда амалий иш кўникмаларига эга малакали кадрларни тайёрлаш;

– криптоактивлар бўйича фаолият ва “блокчейн” технологиялари соҳасида халқаро ва хорижий ташкилотлар билан ҳамкорликни ҳар томонлама ривожлантириш, рақамли иқтисодиётда лойиҳаларни биргаликда амалга ошириш учун “блокчейн” технологияларини ишлаб чиқиш соҳасида фаолият кўрсатадиган юқори малакали хорижлик мутахассисларни жалб қилиш;

– хорижий мамлакатларнинг илғор тажрибасини ҳисобга олган ҳолда “блокчейн” технологияларини жорий этиш учун зарур ҳуқуқий базани яратиш;

– рақамли иқтисодиётни янада ривожлантириш учун инновацион ғоялар, технологиялар ва ишланмаларни жорий этиш соҳасида давлат органлари ва тадбиркорлик субъектларининг яқин ҳамкорлигини таъминлаш.

Айнан мазкур устувор вазифаларни маълум бир тизим асосида бошқариш юқоридаги ислоҳотларни амалга ошириш зарурлигини тақозо этади ва бунда соҳада ягона давлат бошқарувини белгилаш мақсадга мувофиқлигини кўрсатади.

Бу соҳада давлат бошқарувини белгилаш борасида ҳам муаммолар мавжуд, хусусан, Ўзбекистон Республикаси Давлат хавфсизлик хизмати киберхавфсизликни тартибга солиш соҳасида ваколатли орган ҳисобланади, аммо Ўзбекистон Республикаси Президентининг “Республика давлат бошқаруви органлари тизимини такомиллаштириш тўғрисида” 2003 йил 9 декабрдаги ПФ–3358-сонли Фармони талаблари бўйича Давлат хавфсизлик хизмати давлат бошқаруви органига кирмаслиги, шунингдек, кибержиноятчилик ва киберҳуқуқбузарлик бўйича давлат бошқаруви органи ҳали хануз белгиланмаганлигини, Ўзбекистон Республикаси Ахборотлаштириш ва телекоммуникациялар соҳасида назорат бўйича давлат инспекцияси (кейинги ўринларда – Ўзкомназорат) “Киберхавфсизлик маркази” ДУК билан биргаликда давлат ва хўжалик бошқаруви органлари, маҳаллий давлат ҳокимияти органлари, бошқа ташкилотлар ва идораларда ахборот-коммуникация технологияларини жорий этиш ва ривожлантириш ҳамда ахборот хавфсизлиги ҳолатини назорат қилиш, мониторинг қилиш, ўрганиш ва текширишни амалга оширишини, Жиноят кодексининг XX[1] боб-Ахборот технологиялари соҳасидаги жиноятларни тергов қилиш бўйича Жиноят-процессуал кодексда аниқ тартиб белгиланмаганлиги бу борада ҳам ислоҳотлар амалга оширишни тақозо этмай қўймайди.

Таклиф сифатида Ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлиги ёки Ички ишлар вазирлигидан бирини кибержиноятчилик ва киберхавфсизлик соҳасида ягона давлат бошқаруви органи этиб белгилаш, улардан бирини эксперт органи сифатида кўрсатиш, бунда техник чораларни кўриш бўйича мамлакат киберхавфсизлигини таъминлаш бўйича кечиктириб бўлмайдиган ишларни амалга ошириш вазифасини ДХХга юклаш ҳамда ўз фаолияти давомида киберхавфсизликка тўқнаш келишини ҳисобга олиб, Ўзкомназоратни бу борадаги ишларга кўмаклашувчи орган сифатида белгилаш таклиф қилинади.

Бу борада, олимлар Ю.Г. Булай ва Р.И. Булай кибержиноятларнинг ўзга давлат ҳудудида туриб ҳам содир этилишини инобатга олиб, халқаро ваколатли органни ташкил қилиш зарурлигини таъкидлашади,

Н. Журавленко ва Л. Шведованинг фикрларига кўра, бу борада ягона халқаро ҳужжат қабул қилиниши ва ушбу ҳужжат асосида бошқа давлатлар ўзларининг ҳужжатларини унга мувофиқлаштириши мақсадга мувофиқ.

Халқаро тажрибага назар ташласак, ҳақиқатан ҳам чет давлатларда кибержиноятчилик билан курашувчи алоҳида органлар мавжуд, хусусан, Эстониянинг Таллин шаҳрида кибержиноятчиликни ўрганиш ва тадқиқ қилиш бўйича марказ барпо этилган, АҚШда эса АҚШ Қуролли кучлари таркибидаги Киберхавфсизлик бўйича миллий марказ ((National Cyber Security Center) бу борадаги масалалар билан шуғулланади.

Фикримизча, бу соҳада ягона давлат бошқаруви органини белгилаш орқали соҳага оид бир қатор юқорида таъкидлаган муаммолар ҳал этилиши мумкин.

Мамлакатимизда олиб борилаётган ислоҳотлар замирида халқ фаровонлиги ётар экан, уни таъминлаш, аҳолининг давлат органларига бўлган ишончини янада ошириш, олиб борилаётган ислоҳотларни янада такомиллаштириш ва яратилаётган рақамли технологияларнинг хавфсизлигини таъминлаш мақсадида кибержиноятчилик бўйича ислоҳотларни янги босқичга кўтариш мақсадга мувофиқдир.

Айнан ана шундай тараққиётга эришиш учун рақамли билимлар ва замонавий ахборот технологияларини эгаллашимиз зарур ва шарт. Бу бизга юксалишнинг энг қисқа йўлидан бориш имкониятини беради. Зеро, бугун дунёда барча соҳаларга ахборот технологиялари чуқур кириб бормоқда. Юртимиз “Халқаро ахборот коммуникация технологияларини ривожлантириш индекси” бўйича 2019 йилда 8 поғонага кўтарилган бўлсада, ҳали жуда ҳам орқадамиз. Аксарият вазирлик ва идоралар, корхоналар рақамли технологиялардан мутлақо йироқ, десак, бу ҳам ҳақиқат.

Айнан мана шу камчиликларимиз ҳам кибержиноятчиларга қўл келиши ва бу орқали давлатимиз раҳбари бошчилигида олиб борилаётган ислоҳотларда давлат органларининг халқимиз олдидаги нуфузининг тушиб кетиш хавфи йўқ эмас.

Олиб борилаётган ислоҳотларимизни янги босқичга кўтариш ва соҳада туб бурилиш учун ҳам юқорида таъкидланган фикрларни амалиётга татбиқ қилиш ва бу орқали келажагимизни турли хавф-хатарлардан асраш вақти етиб келди. Зеро, халқимиз фаровонлигини таъминлаш ўз қўлимиздадир.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ:

1. Интернет сайтидан. Абдулла Арипов: “Ўзбекистонда ҳам киберҳужумлар кўпайиб боряпти”. Ўзбекистон Бош вазири Абдулла Арипов Москвада бўлиб ўтган “Очиқ инновациялар” халқаро форумининг ялпи мажлисидаги нутқидан. 22.10.2019 й., https://kun.uz/news/2019/10/22/abdulla-aripov-ozbekistonda-ham-kiberhujumlar-kopayib-boryapti.

2. Vincze E.A. Challenges in digital forensics // Police practice and research – Taylor & Francis online: An international journal. – L.; N.Y., 2016. – Vol. 17, N 2. – P. 184.

3. Интернет сайтидан: Эксперт: 26% пользователей Узбекистана столкнулись с кибератаками. https://podrobno.uz/cat/tehnp/ekspert-26-polzovateley-uzbeki/.

4. Интернет сайтидан: Ш. Саттаров. ЕИ компанияларни шифрланган ахборотни ҳукуматга “очиқ ҳолда” тақдим қилишга чақирмоқда. 08.04.2016 й., https://www.terabayt.uz/post/ei-kompaniyalarni-shifrlangan-axborotni-hukumatga-ochiq-holda-taqdim-qilishga-chaqirmoqda?page=11&per-page=10.

5. Интернет сайтидан: Н. Абдураҳимова. Group-IB компанияси Интерполга “ёмон қуён”ни тутиб бермоқчи. 02.11.2017 й., http://archive.qalampir.uz/news/group-ib-kompaniyasi-interpolga-%E2%80%9Cyomon-quyon%E2%80%9Dni-tutib-bermoqchi-13588.

6. Интернет сайтидан: В США киберпреступники “отключили” целый город. https://fakty.ua/327805-v-ssha-kiberprestupniki-otklyuchili-celyj-gorod.

7. Интернет сайтидан: Telegram дал сбой: что об этом известно. https://fakty.ua/325353-telegram-dal-sboj-chto-ob-etom-izvestno.

8. Интернет сайтидан: https://zerde.gov.kz/activity/ict/publication/2221/.

9. Интернет сайтидан: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/643426/Russian_translation_-_National_Cyber_Security_Strategy_2016.pdf.

10. Интернет сайтидан: https://ru.wikipedia.org/wiki/Канадская_служба_разведки_и_безопасности.

11. Интернет сайтидан: https://lt.sputniknews.ru/Lithuania/20180813/6740710/Pravitelstvo-lithuania-utverdilo-Natsionalnuyu-strategiyu-kiberbezopasnosti.html.

12. Интернет сайтидан: https://www.novayagazeta.ru/articles/2018/10/18/78239-haker-kaput.

13. Интернет сайтидан: https://lawandmore.nl/ru/novosti/zakon-o-kiberbezopasnosti-peredan-v-parlament-niderlandov/.

14. Интернет сайтидан: https://news.rambler.ru/politics/41266422-kongress-ssha-prinyal-zakon-o-sozdanii-agentstva-po-kiberbezopasnosti/.

15. Интернет сайтидан: https://tv.delfi.ee/rus/novosti/v-estonii-vstupayut-v-silu-tri-zakona-o-bezopasnosti-v-seti-chto-izmenitsya?id=82198971.

16. Интернет сайтидан: http://iteranet.ru/it-novosti/2014/11/13/v-yaponii-prinyala-zakon-protivodejstviya-atakam-xakerov/.

17. Интернет сайтидан: https://www.imemo.ru/index.php?page_id=502&id=2882&ret=640.

18. Интернет сайтидан: http://slovakiainvest.ru/zashchita-personalnykh- dannykh.

19. Интернет сайтидан: http://uipdp.com/solutions/services/consulting/legislation/eu/france.html.

20. Интернет сайтидан: https://www.hoteladalbert.cz/ru/gdpr/.

21. Интернет сайтидан: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.405200?jfwid=rivwzvpvg.

22. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. – P. 392.

23. Steve Morgan (January 17, 2016). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019". Forbes. Retrieved September 22.2016.

24. Ҳ.Р.Очилов. Ўзгалар мулкини компьютер воситаларидан фойдаланиб талон-торож қилганлик учун жавобгарлик. Монография // – Т.: ТДЮУ нашриёти, 2017. –б.22.

25. Указ Президента України №96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» // https://www.president.gov.ua/documents/962016-19836.

26. Интернет сайтидан: Inter nationa l str ategy for cyberspace. May 2011. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/international_strategy_for_cyberspace_US.pdf.

27. Интернет сайтидан: 2014–2017 Cyber Security Strategy https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf. // https://constitutions.ru/?p=11234.

28. Интернет сайтидан: Government of the Republic of Lithuania Resolution no 796 of 29 June 2011 on the approval of the programme for the development of electronic information security (cyber-security) for 2011–2019 // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ ncss-map/Lithuania_Cyber_Security_Strategy.pdf/.

29. Интернет сайтидан: Estrategia de Ciberseguridad Nacional // https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional.

30. Интернет сайтидан: Cyber Security Strategy for Germany // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Germancybersecuritystrategy20111.pdf.

31. Интернет сайтидан: National Strategy for Information Security in the Slovak Republic // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Slovakia_National_Strategy_for_ISEC.pdf.

32. Интернет сайтидан: Information Security Strategy for Protecting the Nation May 11, 2010 Information Security Policy Council. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/New_Strategy_English_Japan.pdf.

33. Интернет сайтидан: National strategy for Switzerland's protection against cyber risks 19 June 2012. // https://www.enisa.europa.eu/

topics/national-cyber-security-strategies/ncss-map/Switzerlands_Cyber_Security_strategy.pdf.

34. Интернет сайтидан: Cyber Security Strategy for Norway // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Norway_Cyber_Security_StrategyNO.pdf.

35. Интернет сайтидан: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/India_Cyber_Security_Strategy.pdf.

36. Интернет сайтидан: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/India_Cyber_Security_Strategy.pdf.

37. Интернет сайтидан: Cyber Security Strategy. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf.

38. Интернет сайтидан: Government Gazette Staatskoerant Republic of South Africa. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/southafricancss.pdf.

39. Интернет сайтидан: Canada's Cyber Security Strategy For a stronger and more prosperous Canada. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/canadaNCSS.pdf.

40. Интернет сайтидан: Finland's Cybe security Strategy. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf.

41. Интернет сайтидан: National ICT Security Strategy Austria. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Austria_Cyber_Security_strategy.pdf.

42. Интернет сайтидан: Strategia de securitate cibernetică a României. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf.

43. Интернет сайтидан: Rządowy program ochrony cyberprzestrzeni rzeczypospolitej polskiej na lata 2011-2016. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf.

44. Интернет сайтидан: French national digital security strategy. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf.

45. Интернет сайтидан: National cyber security strategy of the Czech Republic for the period from 2015 to 2020. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf.

46. Интернет сайтидан: The National Cyber Security Strategy. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Netherlands_Cyber_Security_strategy.pdf.

47. Интернет сайтидан: National cybersecurity strategy II. // https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Luxembourg_Cyber_Security_strategy.pdf.

48. Ўзбекистон Республикаси Президентининг 2018 йил 14 майдаги ПҚ–3723-сонли “Жиноят ва жиноят-процессуал қонунчилиги тизимини тубдан такомиллаштириш чора-тадбирлари тўғрисида”ги қарори // Қонун ҳужжатлари маълумотлари миллий базаси, 15.05.2018 й., 07/18/3723/1225-сон, 01.10.2018 й., 06/18/5547/1975-сон.

49. Ўзбекистон Республикаси Президентининг 2019 йил 17 январдаги ПФ–5635-сонли Фармони билан тасдиқланган “2017–2021 йилларда Ўзбекистон Республикасини ривожлантиришнинг бешта устувор йўналиши бўйича Ҳаракатлар стратегиясини “Фаол инвестициялар ва ижтимоий ривожланиш йили”да амалга оширишга оид давлат дастури. Манба: Қонун ҳужжатлари маълумотлари миллий базаси, 18.01.2019 й., 06/19/5635/2502-сон.

50. Ўзбекистон Республикаси Президентининг “Жиноят-ижроия қонунчилигини тубдан такомиллаштириш чора-тадбирлари тўғрисида” 2018 7 ноябрдаги ПҚ–4006-сонли қарори. Манба: Қонун ҳужжатлари маълумотлари миллий базаси, 08.11.2018 й., 07/18/4006/2166-сон.

51. Ўзбекистон Республикаси Президентининг “Ўзбекистон Республикасида рақамли иқтисодиётни ривожлантириш чора-тадбирлари тўғрисида” 2018 йил 3 июлдаги ПҚ–3832-сонли қарори. Қонун ҳужжатлари маълумотлари миллий базаси, 04.07.2018 й., 07/18/3832/1452-сон.

52. Ўзбекистон Республикаси Президентининг “Ахборот технологиялари ва коммуникацияларининг жорий этилишини назорат қилиш, уларни ҳимоя қилиш тизимини такомиллаштиришга оид қўшимча чора-тадбирлар тўғрисида” 2019 йил 14 сентябрдаги ПҚ–4452-ли қарори. Манба: ҚҲММБ, 16.09.2019 й., 07/19/4452/4207-сон.

53. Ўзбекистон Республикаси Президентининг “Республика давлат бошқаруви органлари тизимини такомиллаштириш тўғрисида” 2003 йил 9 декабрдаги ПФ–3358-сонли Фармони // Манба: Олий Мажлис Ахборотномаси, 2003 й., 11-12-сон, 178-модда; ЎР ҚҲТ, 2003 й., 23-сон, 229-модда.

54. Ўзбекистон Республикасининг 1994 йил 22 сентябрда қабул қилинган 2012-XII-сонли Қонуни билан тасдиқланган Ўзбекистон Республикасининг Жиноят кодекси // Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси, 1995 йил, № 1, 3-модда; Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси, 1996 йил, № 9, 144-модда; 1997 йил, № 2, 56-модда, № 9, 241-модда; 1998 йил, № 5-6, 102-модда, № 9, 181-модда; 1999 йил, № 1, 20-модда, № 5, 124-модда, № 9, 229-модда; 2000 йил, № 5-6, 153-модда; 2001 йил, № 1-2, 23-модда, № 9-10, 165-модда; 2002 йил, № 9, 165-модда; 2003 йил, № 1, 8-модда, № 9-10, 149-модда; 2004 йил, № 1-2, 18-модда, № 9, 171-модда; Ўзбекистон Республикаси Олий

Мажлиси палаталарининг Ахборотномаси, 2005 йил, № 9, 314-модда, № 12, 417, 418-моддалар; 2006 йил, № 6, 261-модда, № 12, 656-модда; 2007 йил, № 4, 158, 166-моддалар, № 6, 248-модда, № 9, 416, 422-моддалар, № 12, 607-модда; 2008 йил, № 4, 187, 188, 189-моддалар, № 7, 352-модда, № 9, 485, 487, 488-моддалар, № 12, 640, 641-моддалар; 2009 йил, № 1, 1-модда, № 4, 128-модда, № 9, 329, 334, 335, 337-моддалар, № 12, 470-модда; 2010 йил, № 5, 176, 179-моддалар, № 9, 341-модда, № 12, 471, 477-моддалар; 2011 йил, № 1, 1-модда; 2012 йил, № 4, 108-модда, № 9/1, 242-модда, № 12, 336-модда; 2013 йил, № 4, 98-модда, № 10, 263-модда; 2014 йил, № 1, 2-модда, № 5, 130-модда, № 9, 244-модда, № 12, 343-модда; 2015 йил, № 6, 228-модда, № 8, 310, 312-моддалар, № 12, 452-модда; 2016 йил, № 4, 125-модда, № 9, 276-модда, № 12, 383, 385-моддалар; 2017 йил, № 3, 47-модда, № 6, 300-модда, № 9, 506, 510-моддалар; 2018 йил, № 1, 4-модда, № 4, 218, 224-моддалар, № 7, 430-модда, № 10, 679-модда; 2019 йил, № 1, 3, 5-моддалар, № 3, 161-модда, № 5, 259, 267, 268-моддалар, № 7, 386-модда.

55. Ўзбекистон Республикасининг 1994 йил 22 сентябрда қабул қилинган 2013-XII-сонли Қонуни билан тасдиқланган Ўзбекистон Республикасининг Жиноят-процессуал кодекси // (Ўзбекистон Республикаси Олий Кенгашининг Ахборотномаси, 1995 йил, № 2, 5-модда; Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси, 1995 йил, № 12, 269-модда; 1997 йил, № 2, 56-модда, № 9, 241-модда; 1998 йил, № 5-6, 102-модда, № 9, 181-модда; 1999 йил, № 1, 20-модда, № 5, 124-модда, № 9, 229-модда; 2000 йил, № 5-6, 153-модда, № 7-8, 217-модда; 2001 йил, № 1-2, 11, 23-моддалар, № 9-10, 165, 182-моддалар; 2002 йил, № 9, 165-модда; 2003 йил, № 5, 67-модда; 2004 йил, № 1-2, 18-модда, № 9, 171-модда; Ўзбекистон Республикаси Олий Мажлиси палаталарининг Ахборотномаси, 2005 йил, № 12, 418-модда; 2006 йил, № 6, 261-модда; 2007 йил, № 4, 166-модда, № 6, 248, 249-моддалар, № 9, 422-модда, № 12, 594, 595, 607-моддалар; 2008 йил, № 4, 177, 187-моддалар, № 9, 482, 484, 487-моддалар, № 12, 636, 641-моддалар; 2009 йил, № 1, 1-модда, № 4, 136-модда, № 9, 335-модда, № 12, 469, 470-моддалар; 2010 йил, № 6, 231-модда, № 9, 334, 336, 337, 342-моддалар, № 12, 477-модда; 2011 йил, № 4, 103, 104-моддалар, № 9, 252-модда, № 12/2, 363-модда; 2012 йил, № 1, 3-модда, № 9/2, 244-модда, № 12, 336-модда; 2014 йил, № 9, 244-модда; 2015 йил, № 8, 310, 312-моддалар, № 12, 452-модда; 2016 йил, № 4, 125-модда, № 9, 276-модда, № 12, 385-модда; 2017 йил, № 3, 47-модда, № 6, 300-модда, № 9, 510-модда; 2018 йил, № 1, 1-модда, № 4, 224-модда.

56. Ю.Г.Булай, Р.И.Булай. Профилактика и противодействие киберпреступности, а также международным киберугрозам // Академическая мысль. 2017. №1. URL: https://cyberleninka.ru/article/n/profilaktika-i-protivodeystvie-kiberprestupnosti-a-takzhe-mezhdunarodnym-kiberugrozam (дата обращения: 18.02.2020).

57. Журавленко Н.И. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере / Н.И. Журавленко, Л.Е.Шведова // Общество и право. 2015. № 3 (53). – С. 70.

58. Градов А. Деятельность Североатлантического союза в сфере кибербезопасности / А. Градов // Зарубежное военное обозрение. 2014. № 7. – С. 13–16.

59. Берд К. Война со многими неизвестными / К. Берд // Компьютерра. 2009. № 20. – С. 26–29.

60. Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг Олий Мажлисга Мурожаатномаси. 25.01.2020 й. Манба: https://uza.uz/oz/politics/zbekiston-respublikasi-prezidenti-shavkat-mirziyeevning-oliy-25-01-2020.

61. Расулев, Абдулазиз. «Информационная безопасность в условиях пандемии коронавируса». Review of law sciences 2 (2020): 224-228.

62. Расулев А.К. «Совершенствование уголовно-правовых и криминологических мер борьбы с преступлениями в сфере информационных технологий и безопасности. д. ю. н.ю дис». (2018): 16–18.

63. Rasulev A.K. «Improvement of criminal-legal and criminological measures of fight against crimes in the sphere of information technologies and safety: Doctoral (DSc) dissertation abstract on legal sciences». (2018).