

ЎЗБЕКИСТОНДА АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШДА МИЛЛИЙ ҚОНУНЧИЛИГИМИЗНИНГ ЎРНИ ВА ХАЛҚАРО ҲАМКОРЛИК ТАҲЛИЛИ

Мирхамидов Бобир Миртохирович

ЖИДУ магистранти

Аннотация: Ушбу мақолада ИТ соҳасидаги жиноятларга қарши курашишда давлатларнинг минтақавий, халқаро-ҳуқуқий тартибга солиниши, халқаро-ҳуқуқий базасини шакллантирилиши ҳамда халқаро ҳамкорлиги масалалари таҳлил қилинган. Шу билан бирга, сўнгги йиллардаги асосий динамика ва статистик маълумотлар акс эттирилиб, ўрганилган маълумотлар асосида сўнгги йилларда ахборот хавфсизлигини таъминлашда халқаро ташкилотлар томонидан амалга оширилган ҳамда ушбу йўналишда қабул қилинган ҳуқуқий нормалари тўғрисида хулосалар чиқарилади.

Калит сўзлар: Ўзбекистон, ИТ, ахборот хавфсизлиги, киберхавфсизлик, конституция, қонун, қарор, жиноий жавобгарлик, конвенция, жиноят кодекс, халқаро, ахборот-коммуникация, ҳамкорлик.

Ахборотни ҳуқуқий ҳимоялаш заҳира сифатида давлат ва халқаро миқёсида тан олинган ҳамда халқаро шартнома, конвенция ва декларацияларда аниқланади. Давлат миқёсида ахборотни ҳуқуқий ҳимоялаш давлат ва ташкилот ҳужжатлари орқали назорат қилинади. Бизнинг мамлакатимизда бундай меъёрий ҳужжатларга Конституция, Ўзбекистон Республикаси Қонунлари, Давлат ва Ҳукумат қарорлари, фармонлари ҳамда фуқаролик, маъмурий ва жиноят кодексларида келтирилган тегишли моддалар киради. Ташкилот меъёрий ҳужжатларига эса ушбу ташкилот доирасида амал қилинувчи буйруқ, йўриқнома, кўрсатма кабилар киради.

Ахборот хавфсизлиги ва маълумотларни ҳимоялаш соҳасида меъёрий ҳуқуқий ҳужжатларни қабул қилиш ва амал қилишда тизимли кетма-кетлик. Хавфсизликни таъминлаш муаммоси комплекс характерига эга. Уни ҳал қилиш учун ҳуқуқий ҳамда ташкилий чоралар ва дастурий-техник таъминотни биргаликда кўриш талаб этилади (мисол учун корхона бошқаруви миқёсида унинг компьютер ахборот тармоғида ахборот хавфсизлигини таъминлаш учун хавфсизлик сиёсатини ишлаб чиқиш ҳамда керакли ресурслар талаб этилади).

Ҳозирда давлат ҳокимияти ва бошқаруви органларининг асосий фаолият йўналишлари бўйича уларга юклатилган вазифаларнинг кенг кўламли эканлигини ҳисобга олсак, уларнинг фаолиятни зарур ахборот билан таъминлаш жараёнини тўғри ташкил этиши жуда муҳим ҳисобланади. Чунки, бу давлат органлари фуқароларнинг ҳуқуқ ва эркинликлари, жамият ва давлатнинг қонуний манфаатларини таъминлаш борасидаги тўлиқ ва ишончли ахборот билан таъминланишига имкон яратади. Бу борада халқаро даражада давлат органлари ва бошқа турли идоралар ҳамда бизнес фаолияти учун ахборот хавфсизлигини қандай таъминлаш борасида стандартлар ишлаб чиқилган.

Мамлакатимизда ахборот хавфсизлигини таъминлаш юзасидан бир нечта Қонун, Давлат ва ҳукумат Фармони, Қарорлар ва бошқа норматив-ҳужжатлар ишлаб чиқилди. Жумладан,

- Ўзбекистон Республикаси Конституцияси (янги таҳрири 2023 йил 30 апрелдаги)

- Ўзбекистон Республикасининг 1993 йил 7 майдаги “Давлат сирларини сақлаш тўғрисида”ги 848-ХП сон Қонуни;

- Ўзбекистон Республикасининг 1994 йил 6 майдаги “Электрон ҳисоблаш машиналари учун яратилган дастурлар ва маълумотлар базаларининг ҳуқуқий ҳимояси тўғрисида”ги 1060-ХП сон Қонуни;
 - Ўзбекистон Республикасининг 2002 йил 12 декабрдаги “Ахборот эркинлиги принциплари ва кафолатлари тўғрисида”ги 439-П сонли Қонуни,
 - Ўзбекистон Республикасининг 2003 йил 11 декабрдаги “Ахборотлаштириш тўғрисида”ги 560-П сон Қонуни;
 - Ўзбекистон Республикасининг 2004 йил 29 апрелдаги “Электрон ҳужжат айланиши тўғрисида”ги 611-П сон Қонуни;
 - Ўзбекистон Республикасининг 2006 йил 4 апрелдаги “Автоматлаштирилган банк тизимида ахборотни муҳофаза қилиш тўғрисида”ги ЎРҚ-30 сон Қонуни,
 - Ўзбекистон Республикасининг 2019 йил 2 июлдаги “Шахсга доир маълумотлар тўғрисида”ги 547-сон Қонуни,
 - Ўзбекистон Республикасининг 2022 йил 15 апрелдаги “Киберхавфсизлик тўғрисида”ги ЎРҚ-764-сон Қонуни,
 - Ўзбекистон Республикаси Президентининг 2007 йилдаги 3 апрелдаги «Ўзбекистон Республикасида ахборотни криптографик муҳофаза қилишни ташкил этиш чора-тадбирлари тўғрисида» ПҚ-614-сон қарори,
 - Ўзбекистон Республикаси Президентининг 2020 йил 5 октябрдаги ПФ-6079-сон фармони (“Рақамли Ўзбекистон – 2030” стратегияси қабул қилиниб, уни самарали амалга ошириш чора-тадбирлари белгиланиши натижасида бир томондан АКТ такомиллашиб ва кенгайиб борган бўлса, иккинчи томондан, ахборот хавфсизлиги моддий техникавий базасини ривожлантириш жараёнлари ҳам ривожлана бошлади),
 - Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги ПФ-60 сон фармони (“2022-2026 йилларга мўжалланган янги Ўзбекистоннинг тараққиёт стратегияси” дастурининг “Мамлакатимиз хавфсизлигини ва мудофаа салоҳиятини кучайтириш, очиқ, прагматик ва фаол ташқи сиёсат олиб бориш”),
 - Ўзбекистон Республикаси Президентининг 2023 йил 11 сентябрдаги ПФ-158 сон фармони (“Ўзбекистон – 2030” стратегияси” дастурининг “Мамлакатимиз хавфсизлиги ва мудофаа салоҳиятини кучайтириш бўйича ислохотлар”),
 - Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2017 йил 17 октябрдаги “Ўзбекистон Республикаси ахборот технологиялари ва коммуникацияларини ривожлантириш вазирлигининг ахборот хавфсизлиги ва жамоат тартибини таъминлашга кўмаклашиш маркази фаолиятини ташкил этиш чора-тадбирлари тўғрисида” 838-сон Қарори,
 - Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2018 йил 5 сентябрдаги “Бутунжаҳон интернет тармоғида ахборот хавфсизлигини янада такомиллаштириш чора-тадбирлари тўғрисида” 707-сонли Қарори,
 - Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2018 йил 22 октябрдаги “Болаларни уларнинг соғлиғига зарар етказувчи ахборотдан ҳимоя қилиш тўғрисида”ги Ўзбекистон Республикаси қонунини амалга ошириш чора-тадбирлари тўғрисида” 848-сон Қарори,
 - Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2011 йил 7 июлдаги 296-сон қарори,
- Шу билан бирга, мамлакатимизда ахборот хавфсизлигини таъминлаш ва кибержиноятчиликни олдини олиш масалалари давлат сиёсати даражасига кўтарилган. Ўзбекистон Республикаси қонунчилигида ҳам

IT жиноятлари мустақамланган (Жиноят кодекс XXI боб).

IT жиноятлари билан боғлиқ бўлиши мумкин бўлган кўплаб ноқонуний хатти-ҳаракатлар мавжуд. Қонун устуворлигининг замонавий шароитида жиноий жавобгарликка тортилиши керак бўлган аниқ жиноятлар рўйхатини ишлаб чиқиш унчалик долзарб эмасдек кўринади. Ҳатто жиноятларнинг энг кенг рўйхати ҳам тўлиқ эмас ва келажакда уни тўлдириш ёки ўзгартириш керак, чунки ўрганилаётган соҳа жуда кенг ва ўзгарувчандир. Кўрсатилган нуқтаи назарлар жуда ўринли ва шунинг учун жиноий жавобгарликка тортилиши мумкин бўлган ноқонуний хатти-ҳаракатларнинг аниқ рўйхатини ишлаб чиқиш ўрнига, типологияга асосланган ёндашувдан фойдаланиш керак. Хусусан, олтита асосий жиноят турини назарда тутувчи IT соҳасидаги жиноятларнинг Ўзбекистон Республикаси қонунчилиги нуқтаи назаридан кўриб чиқиш мақсадга мувофиқдир:

- Асосий тажовузнинг предмети IT бўлган жиноятлар: Ахборотлаштириш қоидаларини бузиш (Ўзбекистон Республикаси Жиноят кодексининг 278¹-моддаси),
- Компьютер ахборотидан қонунга хилоф равишда (рухсатсиз) фойдаланиш (Ўзбекистон Республикаси Жиноят кодексининг 278²-моддаси).
- Компьютер тизимидан, шунингдек телекоммуникация тармоқларидан қонунга хилоф равишда (рухсатсиз) фойдаланиш учун махсус воситаларни ўтказиш мақсадини кўзлаб тайёрлаш ёхуд ўтказиш ва тарқатиш (Ўзбекистон Республикаси Жиноят кодексининг 278³-моддаси),
- Компьютер ахборотини модификациялаштириш (Ўзбекистон Республикаси Жиноят кодексининг 278⁴-моддаси), Компьютер саботажи (Ўзбекистон Республикаси Жиноят Кодексининг 278⁵-модда),
- Зарар келтирувчи дастурларни яратиш, ишлатиш ёки тарқатиш (Ўзбекистон Республикаси Жиноят Кодексининг 278⁶-модда).

- O‘z DSt ISO/IEC 27002 стандартининг 5–бобида “Ўзбекистон Республикаси ҳудудида ахборот хавфсизлиги сиёсатини ишлаб чиқиш бўйича услубий қўлланмалар” ҳам 2013-2020 йилларда Ўзбекистон Республикаси Миллий ахборот-коммуникация тизимини ривожлантиришни мувофиқлаштириш бўйича Республика комиссиясининг 2016 йил 23 февралдаги 7 баёнини билан тасдиқланган.

Шунингдек, IT соҳасидаги маъмурий жавобгарликни Ўзбекистон Республикаси қонунчилиги нуқтаи назаридан кўриб чиқиш мақсадга мувофиқдир, яъни Ўзбекистон Республикаси Маъмурий жавобгарлик тўрисидаги кодекслари: Жумладан,

- Ахборотдан фойдаланиш қоидаларини бузиш. (Маъмурий жавобгарлик тўрисидаги кодексининг 155-моддаси).
- Компьютер тизимидан фойдаланиш қоидаларини бузиш (Маъмурий жавобгарлик тўрисидаги кодексининг 155¹-моддаси).

Юқорида таъкидлаб ўтилган, Қонун, Қарор, Фармон ва бошқа ҳуқуқий норматив-ҳужжатлар мамлакатимизда ахборот хавфсизлигини таъминлаш катта аҳамиятга эга.

Ҳозирги кунда мамлакатимизда ахборот хавфсизлигини таъминлашда “Киберхавфсизлик маркази” ДУК фаолият олиб бормоқда. “Киберхавфсизлик маркази” ДУК томонидан 2023 йилнинг 1-ярим йиллиги мобайнида Ўзбекистон Республикаси давлат идораларининг 81 та расмий вебресурслари амалдаги ахборот ва киберхавфсизлик талабларига жавоб бериши даражасини аниқлаш бўйича экспертизадан ўтказилган. Экспертиза натижаларига кўра, жами бўлиб мазкур ресурсларда 316 та турли хавф тоифаларига оид киберхавфсизлик заифликлари аниқланган. Аниқланган заифликларнинг

81% (255 та) юқори даражали хавф тоифасига тегишли эканлиги кузатилган. 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 кодиди қўлга киритиш имкониятини вужудга келтириши боис, веб-ресурсларга киберхавфсизлик тамойилларини изчил тадбир этилиши талабини долзарблаштиради.

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 этилган. Аниқланган ҳолатлар юзасидан манфаатдор ташкилотларга ушбу заифликларни бартараф этиш борасида тегишли тавсиялар тақдим этилган. 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.

Марказнинг тармоқ ҳужумларига қарши автоматлаштирилган ҳимоя тизимларида жамланган маълумотларнинг таҳлилига кўра, киберҳимоядаги давлат ташкилотлари веб-ресурсларига жами 17 мингга яқин ҳолатда тармоқ ҳужумлари амалга оширилганлиги қайд этилди ва ўз вақтида блокраниши таъминланди. Веб-ресурсларга уюштирилган жами киберҳужумлар турлари кесимида умумий кўрсаткичдан қуйида кўрсатилган уллушларда тақсимланганлиги аниқланди. Бунда, сканерларни аниқлаш, SQL-инъекция, масофавий файлни киритиш (LFI), PHP - кодларни жойлаштириш ва сайтлараро скриптинг (XSS) каби киберҳужум турларини қўллаш ҳолатлари орگانлиги кузатилди.

Ўзбекистон Республикаси халқаро миқёсида ахборот хавфсизлиги таъминлашда бир қанча етакчи давлатларда фаолият юритаётган ахборот хавфсизлик тизимлари билан бир ҳуқуқда фаолият олиб бормоқда. Жумладан,

1. “FIRST” хавфсизликни биргаликда яхшилаш халқаро ташкилоти (<https://www.first.org/>);
2. Халқаро электр алоқа иттифоқи (МСЭ) (<https://www.itu.int/ru/Pages/default.aspx#/ru>);
3. Россия Федерациясида Москва шаҳрида жойлашган F.A.C.C.T.(facet.ru)
4. Жанубий Корея интернет ва хавфсизлик агентлиги “KISA” (<https://www.kisa.or.kr/>);
5. Латвия давлатидаги “CERT.LT” (<https://www.cert.lv/lv/>);
6. Япония давлатининг Токио шаҳрида жойлашган Япония компьютер ходисаларига жавоб бериш гуруҳини мувофиқлаштириш маркази “JPCERT.CC” (<https://www.jpccert.or.jp/english/>);
7. Польша давлати Варшава шаҳрида жойлашган “CERT.PR.” (<https://cert.pl/en/>);
8. Хитой Халқ Республикасининг “CNCERT/CC” (<https://cert.gov.kz/>);
9. Қозғистон Республикаси Остона шаҳрида жойлашган “KZ-CERT” (<https://cert.gov.kz/>);
10. Омон Султонолигининг Ал-Атайба шаҳрида “OIC-CERT” (cert@ita.gov.om) раислиги ҳамда Малайзия давлатида “OIC-CERT” (secretariat@oic-cert.org) доимий котибиятдир.

2023 йил октябрь ойида Ўзбекистон Республикасида “CSS 2023” икки кунлик конференция бўлиб ўтган, конференцияда 24 давлатдан 130 та компаниялар иштирок этган. У Марказий Евроосиё бўйлаб миллий хавфсизлик марказлари, киберхавфсизлик бўйича ечимлар провайдерлар ва ҳукумат, тижорат ва саноат корхоналарининг охириги фойдаланувчиларини янги бизнес алоқаларини яратиш, технологияларни намоиш этиш ва илгари суриш, янги ўзаро алоқалар ва мулоқотларни яратиш учун бирлаштирилади. Саммитнинг икки кунда киберхавфсизлик соҳасида Ўзбекистон ҳамда Туркменистон давлатлари ўртасида меморандум имзоланди. Ушбу Англашув Меморандуми “Киберхавфсизлик маркази” ҳамда “Туркменарагатнашиқ” (Turkmenaragatnashiq) агентлиги ҳузуридаги Давлат киберхавфсизлик хизматлари ўртасида имзоланиб, ўзаро манфаатлар асосида киберхавфсизлик соҳасида ҳамкорлик қилишга келишиб олинган. Меморандумнинг мақсади “Компьютер ҳужумлари, ахборот хавфсизлигига таҳдидларнинг оқибатларини аниқлаш, олдини олиш ва бартараф этиш, шу жумладан ахборот хавфсизлиги соҳасида ихтисослашган мутахассисларни тайёрлаш мақсадида тажриба алмашиш ва ахборот хавфсизлик даражасини оширишга қаратилган ўзаро ҳамкорликни ташкил этиш, ахборот ресурсларини вируслар ва хакерлар ҳужумларидан ҳимоя қилиш, барча даражадаги ходимларнинг замонавий кибертаҳдидлардан хабардорлик даражасини ошириш, ахборот хавфсизлигини таъминлаш ва бошқаришнинг замонавий тизимларидан фойдаланишдан иборат”лиги кўрсатган.

Мамлакатимиз ушбу ташкилотлар билан бир овозга эга бўлган ҳолда доимий равишда ахборот хавфсизлиги бўйича ҳамкорликда ишлар олиб боради.

2019 йил 27 мартда, яъни орадан икки йил ўтгач Ўзбекистон жаҳон киберхавфсизлик рейтингда 52-ўринни эгаллади. Очiq манбаларни ўрганиш, MSE тузилмасида турли ташкилотлар билан ўзаро ҳамкорлик қилиш, Ўзбекистон Республикасининг халқаро муносабатларини, жумладан, киберхавфсизлик масалаларида кенг кўламли ишлари, мамлакатимиз жаҳон ҳамжамиятида ижобий баҳо берилди ва эътироф этилди¹. Мамлакатларнинг киберхавфсизликка бўлган мажбуриятини баҳоловчи “Global Cybersecurity Index” (GCI)нинг 2021 йил 10 октябрдаги маълумотида биноан Ўзбекистон глобал киберхавфсизлик бўйича 194 мамлакат рейтингда 70-ўринни эгаллаб, унинг индекси максимал 100 баллдан 71,11 баллни ташкил этди. Ўзбекистон энг юқори баллни ҳуқуқий чоралар сегментида олди (19,27 балл), энг паст баллни эса ташкилий чораларга тегишли (10,05 балл) бўлди. Шунингдек, мамлакатга техник чора-тадбирлар соҳаси учун 12,56 балл, салоҳиятни ривожлантириш чора-тадбирлари учун 15,68 ва ҳамкорлик чоралари учун эса 13,56 балл берилди. Таъкидланишича, Марказий Осиё давлатлари орасида киберхавфсизлик бўйича Ўзбекистон Қозоғистондан (рейтингда 31-ўринда) кейин иккинчи ўринни қайд этган (Қирғизистон 92-ўринни, Тожикистон 138-ўринни, Туркменистон эса 144-ўринни эгаллади). Рейтинг биринчи учталини

1. АҚШ (100 балл) биринчи,
2. Буюк Британия ва Саудия Арабистони (ҳар бири 99,54 балл),
3. Эстония (99,48 балл) ўринни олиб кучли учликни ташкил қилди. Рейтингда охириги ўрин Шимолий Кореяга тегишли бўлди (1,35 балл)².

¹ "Экономика и социум" №4(107)-2 2023 www.iupr.ru 451

² "Экономика и социум" №4(107)-2 2023 www.iupr.ru 451

“NCSI” веб-сайтида эълон қилинган маълумотларга кўра, 2023 йил октябрь ойида Ўзбекистон Республикаси Миллий киберхавфсизлик индексида 176 давлат орасида 94 ўринни эгаллади³. Рейтингни тузишда “Global Cybersecurity Index”и, ахборот-коммуникация технологияларини ривожлантириш индекс, тармоқ тайёрлиги каби мезонлар инобатга олинган.

Мамлакатимизда ахборот хавфсизлиги рейтинги йил сайин пастга тушиб кетаётганлиги ҳамда мамлакатимизда ахборот хавфсизлигини таъминлаш юзасидан “Янги Ўзбекистоннинг 2022-2026 йилларга мўлжалланган тараққиёт стратегиясида 2022 йил октябрга қадар “2023-2026 йилларга мўлжалланган Ўзбекистон Республикасининг киберхавфсизлик стратегияси”ни ишлаб чиқиш вазифаси қўйилди. Унда, “UZ№ домен зонаси Интернетмаконининг киберхавфсизлигини таъминлашнинг асосий йўналишлари ҳамда электрон ҳукумат, энергетика, рақамли иқтисодиёт тизимлари ва муҳим ахборот инфратузилмасига тааллуқли бошқа йўналишларни ҳамоя қилиш бўйича комплекс вазифалар белгиланади. Шунингдек, кибержиноятчилик учун жиноий жавобгарликни қайта кўриб чиқиш кўзда тутилган ҳамда ҳужжатда ахборот майдонидаги киберхужум ва таҳдидларни мониторинг қилиш тизимини янада такомиллаштириш вазифалари белгиланди. Унга биноан киберхавфсизликнинг Ягона тармоғининг техник инфратузилмасини кенгайтириш, кибернетикада инновациялар ИТ-парки” фаолиятини янада жадаллаштириш, ИТ-паркнинг ҳудудлардаги рақамли технологиялар ўқув марказлари негизда ёшларни киберхавфсизлик асослари бўйича ўқитилишини таъминлаш ҳамда ҳар йили талаба ва ўқувчилар орасида киберхужумлар аниқлаш бўйича республика миқёсида конкурслар ўтказишни назарда тутиш қайд этилди.

Ўзбекистон Республикаси Президент Ш.М.Мирзиёев ташаббуси билан 2022 йил 21 апрелда парламент томонидан “Киберхавфсизлик тўғрисида”ги Қонуннинг қабул қилиниши мамлакатда ахборот хавфсизлигини таъминлаш соҳасидаги катта бурилиш бўлди. Мазкур қонуннинг қабул қилиниши мамлакатда ахборот-коммуникация воситаларини ички ва ташқи киберхужумлардан ҳамоя қилиш соҳасининг ҳуқуқий асосларини ҳар томонлама мустаҳкамлади. Қонун 8 та боб ва 40 та моддадан иборат бўлиб, унда мамлакатнинг киберхавфсизлигини таъминлашнинг қуйидаги асосий принциплари белгиланди: қонунийлик, кибермаконда шахс, жамият ва давлат манфаатларини ҳамоя қилишнинг устуворлиги, киберхавфсизлик соҳасини тартибга солишга нисбатан ягона ёндашув, киберхавфсизлик тизимини яратишда маҳаллий ишлаб чиқарувчилар иштирокининг устуворлиги, Ўзбекистон Республикасининг киберхавфсизликни таъминлашда халқаро ҳамкорлик учун очиқлиги. Шунингдек, қонунда Киберхавфсизлик соҳасидаги ягона давлат сиёсатини Ўзбекистон Республикаси Президенти белгилаши мустаҳкамланди. Қонунга биноан, киберхавфсизлик субъектлари томонидан киберхавфсизлик ходисаларига нисбатан чоралар кўриш дастурий таъминотдаги ва қурилмалардаги заифликларни ҳамда хатоликларни бартараф этиш, зарарли дастурларни йўқ қилиш, уларнинг тарқалишини чеклаш, киберхужумлар манбаини техник жиҳатдан чеклаш, ахборотлаштириш объектларини мавжуд кибертаҳдидлардан ажратиш бўйича, ҳуқуқни муҳофаза қилувчи органларга киберхавфсизлик ходисалари тўғрисида маълумотлар тақдим этиш каби шаклларда амалга оширилиши мумкин.

³ “Global Cybersecurity Index” 2023, https://daryo/uz/en/category/uzbekistan?utm=from_top_menu

Шу билан бирга, Ўзбекистон Республикаси Президентининг 2023 йил 11-сентябрдаги ПФ-158-сон фармони билан тасдиқланган “Ўзбекистон-2030 стратегияси” дастурининг “Мамлакатимиз хавфсизлиги ва муҳофаа салоҳиятини кучайтириш бўйича ислохотларни олиб бориш” деб номланган V устувор йўналишининг бандларида кўрсатиб ўтилган. Жумладан, миллий ахборот майдонида қонунчиликка риоя этилишини таъминлаш, ахборотдан фойдаланиш маданиятини юксалтириш ҳамда аҳолини ёт ва деструктив маълумотлар таъсиридан ҳимоя қилиш, радикаллашувнинг олдини олиш. Интернет жаҳон ахборот тармоғидан тўсиқларсиз фойдаланиш учун зарур шарт-шароитларни яратиш, миллий интернет маконида киберхавфсизликни таъминлаш ҳамда фуқароларнинг интернетдан фойдаланиш борасидаги саводхонлигини ошириш; Қуролли Кучларнинг рақамли салоҳиятини ошириш ва ахборот хавфсизлигини таъминлаш, ҳарбий хизматчиларнинг замонавий ахборот-коммуникация технологияларидан фойдаланиш борасидаги билим ва кўникмаларини ошириш. Қўшинларнинг жанговар руҳи ва салоҳиятини юксалтириш, замонавий жанг ва ҳарбий можаролар ҳамда хорижий армияларнинг илғор тажрибасини ўрганиш асосида қўшинларнинг жанговар шайлиги ва маҳоратини ривожлантириш. Қуролли Кучлар куч тузилмалари билан ҳамкорликни кучайтириш, биргаликдаги ҳаракатларнинг самарадорлиги ва мувофиқлашганлик даражасини ошириш. Юқори малакали ҳарбий кадрларни тайёрлаш тизимини мунтазам равишда такомиллаштириб бориш, ўқув жараёнларига ҳарбий тайёргарликнинг замонавий усулларини кенг жорий этиш; давлат чегарасини қўриқлаш тизимида замонавий технологиялар, коммуникация воситалари ва техник (муҳандислик) иншоотларни кенг жорий қилиш. Давлат чегараси хавфсизлигини таъминлаш жараёнини сунъий интеллект технологияларидан фойдаланган ҳолда янада автоматлаштириш. Чегара бузувчилари ҳаракатларини сустлаштириш ва қийинлаштириш жиҳатдан жиҳозланганлик даражасини ошириш.

Давлатимиз томонидан ахборот хавфсизлиги таъминлаш юзасидан бир қанча ишлар олиб бораётганлиги ва ушбу йўналишга катта эътибор қаратилмоқда. Кибержиноятчиликнинг олдини олиш тизимини яратиш масаласи белгиланганлигининг ўзи ҳам ушбу мавзунинг долзарблигидан далолат беради.

IT соҳасидаги трансмиллий жиноятларни фош этиш ва тергов қилишда ҳуқуқни муҳофаза қилувчи органлар қатор муаммоларга дуч келмоқда, жумладан, жиноят содир этилган жой ва юрисдикцияни аниқлаш, хорижий давлатларнинг ваколатли органларидан олинган рақамли далиллардан фойдаланиш ва бошқалар. Шу муносабат билан, Ўзбекистон Республикаси ҳуқуқни муҳофаза қилиш органларининг IT соҳасидаги жиноятларни очиш ва тергов қилиш фаолиятини такомиллаштириш истиқболларини белгилаш алоҳида аҳамиятга эга.

Фойдаланилган адабиётлар рўйхати:

1. Ўзбекистон Республикаси Конституцияси (янги таҳрири 2023 йил /30 апрель) [Электрон ресурс]:[lex/uz](http://lex.uz)
2. Ўзбекистон Республикаси Президентининг 2023 йил 11 сентябрдаги ПФ-158 сон фармони, [Электрон ресурс]:<https://lex.uz/docs/6600413>
3. Ўзбекистон Республикасининг 2022 йил 15 апрелдаги “Киберхавфсизлик тўғрисида”ги ЎРҚ-764-сон Қонуни, [Электрон ресурс]: <https://lex.uz/uz/docs/5960604>
4. "Экономика и социум" №4(107)-2 2023 www.iupr.ru 451
5. “Global Cybersecurity Index” 2023, https://daryo.uz/en/category/uzbekistan?utm=from_top_menu

6. Н.А.Нугмонов “Формирование международного информацион-ного права: вопросы теории и практики:” Монография – Ташкент, УМЭД, 2018.228с
7. Global Risks Report 2020 // Jahon iqtisodiy forumining rasmiy sayti. [URL:https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf](https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf)