



КИБЕРХАВФСИЗЛИК ВА УНИ ТАЪМИНЛАШГА ДОИР ЧОРА- ТАДБИРЛАРНИНГ ТАКОМИЛЛАШУВИ

Юлдашев Бехзод Рузиматович

Мустақил изланувчи

<https://doi.org/10.5281/zenodo.6564394>

Аннотация: Ушбу илмий мақолада илмий жихатдан кенг ёритилган бўлиб, унда қуйидагилар келтириб ўтилган. Киберхавфсизлик ахборот технологиялари дунёсида муҳим рол ўйнайди. Ҳозирги кунда маълумотларни хавфсиз сақлаш энг катта муаммолардан биридир. Киберхавфсизлик ҳақида ўйлаганимизда ҳаёлимизга келадиган биринчи нарса кундан-кунга жадал ривожланаётган кибержиноят бўлади. Турли хил компаниялар ва ҳукуматлар кибержиноятчиликни олдини олиш учун кенг кўламли ишлар олиб бормоқдалар. Лекин бунга қарамай киберхавфсизлик ҳозирда кўпчилик учун жуда катта муаммо бўлиб қолмоқда ва шунга ўхшаш маълумотлар ёритилган.

Калит сўзлар: киберхавфсизлик, киберхужум, вирусли дастурлар, веб-сайт, кредит карта, интеграция.

Асримизнинг глобал муаммолари қаторига янгидан-янги турлари билан тилга олинаётган кибержиноятчилик кириб келганига ҳам анча бўлди. Унинг бизга маълум бўлган вирусли дастурларни тарқатиш, паролларни бузиб кириш, кредит карта ва бошқа банк реквизитларидаги маблағларни ўзлаштириш талон-торож қилиш, шунингдек, интернет орқали қонунга зид ахборотлар, хусусан, бўҳтон, маънавий бузуқ маълумотларни тарқатиш билан башарият ҳаётига катта хавф солаётганидан кўз юма олмаймиз.

«Кибержиноятчилик» тушунчаси ахборот-коммуникация технологиялари воситаларидан фойдаланган ҳолда, виртуал тармоқда даҳшат солиш, вирус ва бошқа зарарли дастурлар, қонунга зид ахборотлар тайёрлаш ва тарқатиш, электрон хатларни оммавий тарқатиш (спам), хакерлик хужуми, веб-сайтларга ноқонуний

кириш, фирибгарлик, маълумотлар бутунлиги ва муаллифлик ҳуқуқини бузиш, кредит карточкалари рақами ҳамда банк реквизитларини ўғирлаш (фишинг ва фарминг) ва бошқа турли ҳуқуқбузарликлар билан изоҳланади¹.

Шу ўринда кибертерроризм ва унинг жамият ҳаётига солаётган хавфининг кўлами ҳам ошиб бораётганини таъкидлаш жоиз. Кибертеррористик ҳаракат (киберхужум) - компьютерлар ва ахборот коммуникация воситалари ёрдамида амалга оширилган, одамларнинг ҳаёти ва соғлиғига бевосита хавф туғдирадиган ёки потенциал хавф туғдириши мумкин бўлган, моддий объектларга катта зарар етказиши ёки шунга олиб келиши мумкин бўлган, ижтимоий хавфли оқибатларнинг бошланиши ёки мақсади бўлган сиёсий сабабдир. Замонавий террорчилар учун кибермакондан фойдаланишнинг жозибadorлиги киберхужумни амалга ошириш катта молиявий харажатларни талаб қилмаслиги билан боғлиқ².

Экспертларнинг хулосасига кўра, бу ривожланаётган давлатларнинг тараққиётига кўмаклашиш, умуминсоний демократик тамойилларни қарор топтириш ниқоби остида фуқаролар онгига таъсир ўтказиш, уларни турли йўллар билан ўз мақсадлари сари бўйсундириш орқали амалга оширилмоқда.

Афсуски, бу жараёнда киберхужумларни уюштириш, бу йўлда интернет глобал тармоғининг мислсиз имкониятларидан «самарали» фойдаланишга уринишлар тобора авж олмоқда³.

Интернетда мавжуд ижтимоий тармоқлар, уларнинг ишлаб чиқарувчилари ва ҳомийларининг суверен давлат ички ишларига «аралашилари» қандай роль ўйнаши охиригача ўрганилмаганлиги боис баъзан бундай «аралашув» мазкур давлатга қарши эканлиги ҳали ҳануз эътироф этилгани йўқ.

Ижтимоий тармоқлар эгалари ушбу тармоқлар саҳифаларида давлат тузумини ағдаришга даъват қилингани учун жавобгарликка тортилишининг халқаро миқёсдаги ҳуқуқий асослари яратилмаган. Ваҳоланки, ҳар бир қилинган жиноий

¹ Васенин В.А. Информационная безопасность и компьютерный терроризм. <https://www.crime-research.ru>

² Ибрагимов В. Кибертерроризм в Интернете до и после 11 сентября 2001: угрозы и нейтрализация. <http://www.crimeresearch.ru/articles/vagif>

³ Голубев В.А. Кибертерроризм – угроза национальной безопасности. <https://www.crime-research.ru>

хатти-ҳаракат ёки ҳаракатсизлик мазмун-моҳиятига кўра, албатта, жавобсиз ва жазосиз қолмаслиги керак.

Интернет сайтлари тўсатдан пайдо бўлиб, кўпинча форматини, сўнгра манзилни ўзгартиради. Шу боис айрим экспертлар интернетнинг буткул очиқлиги каби дастлабки концепциялардан воз кечиб, унинг янги тизимига ўтишни таклиф этмоқда. Янги моделнинг асосий моҳияти тармоқдан фойдаланувчиларнинг анонимлигидан воз кечишдир. Бу тармоқнинг жиноий тажовузлардан янада кўпроқ ҳимояланган бўлишини таъминлашга имкон берди. Мисол тариқасида, ёпиқ тармоқ тизимига ўтган Хитой давлатини ва бундай жараёнга тайёргарлик кўраётган Россия давлатини келтиришимиз мумкин.

Жаҳон ҳамжамиятига интеграциялашаётган мамлакатимизда ахборот коммуникация технологиялари, ахборот тизимлари ва замонавий компьютер технологияларидан самарали фойдаланиш бўйича изчил давлат сиёсати олиб борилмоқда. Бугунги кунда мамлакатимизда жорий этилаётган замонавий рақамли технологиялар, фуқароларимизга қатор қулайликлар ва имкониятлар эшигини очмоқда. Мазкур жараён билан бир қаторда, яратилаётган рақамли технологиялар ва ахборот тизимларининг хавфсизлигини таъминлаш муаммоси ҳам мавжуд, албатта.

Бу энг долзарб масалалардан бири - киберхавфсизликни таъминлаш, содир этилиши мумкин бўлган кибержиноятларнинг олдини олиш ва унга қарши курашиш масаласи ҳисобланади. Кундан-кунга такомиллашиб кетаётган кибержиноятчиликка қарши киберхавфсизликни таъминлашда қуйидаги асосий талабларни бажариш орқали улардан ҳимояланиш, яъни киберхавфсизликни таъминлашимиз мумкин:

ходимларга ахборот хавфсизлиги асосларини ўргатиш;

фойдаланаётган дастурий маҳсулотларнинг заифликларини доимий синовдан ўтказиш;

ишончли антивирус дастуридан фойдаланиш;

лицензияланган расмий дастурлардан фойдаланиш;

ахборот тизимларини ҳимоялашда кўп факторли аутентификациядан фойдаланиш;

пароллардан фойдаланишда кучли паролни сақлаш сиёсатига риоя қилиш; мунтазам равишда компьютер қаттиқ дискларидаги маълумотларни шифрлаш.

Шу ўринда, мамлакатимизда кибержиноятларнинг олдини олиш ва унга қарши курашни олиб боровчи ваколатли давлат идораларига ҳам муайян вазифалар юкланишини алоҳида таъкидлаш лозим.

Хусусан, улар кибержиноятчиликка қарши кураш фаолиятида Ўзбекистон Республикаси ва унинг халқини ахборот технологиялари ва коммуникациялари орқали амалга оширилаётган ёки бунга имкон бераётган шахс, жамият ва давлат хавфсизлигини ва уларнинг манфаатлари ташқи ҳамда ички кибертаҳдидлардан ҳимоя қилинишини таъминлаш, мазкур соҳада қонунийлик ва қонун устуворлигини мустаҳкамлаш, кибержиноятлар ва киберҳуқуқбузарликларнинг олдини олиш, уларни аниқлаш ва барҳам бериш каби вазифаларни амалга ошириши даркор.

Ҳозир бутун дунёда бу масала алоҳида эътибор марказига кўтарилган. Шунингдек, ҳар бир давлат ўз манфаатлари нуқтаи назарида ички имкониятлари доирасида тегишли чора-тадбирларни ишлаб чиқмоқда. Жумладан мамлакатимизда ҳам ахборот хавфсизлиги масалаларига давлат сиёсати даражасида катта эътибор қаратилмоқда. Бир қатор меъёрий ҳужжатлар қабул қилинмоқда. Хусусан, Ўзбекистонда 2022 йилда “Киберхавфсизлик тўғрисида” ги қонун ишлаб чиқилди.

Янги қонуннинг мақсади:

- Ўзбекистон Республикаси кибермақонида киберхавфсизлик соҳасидаги муносабатларни тартибга солиш;
- Киберхавфсизлик соҳасидаги ваколатли органнинг ваколатлари, ҳуқуқ ва мажбуриятларини белгилаш;
- Миллий киберхавфсизлик саноатини рағбатлантириш, ривожлантириш учун ҳуқуқий базани яратиш: давлат томонидан қўллаб-қувватлаш чораларини

кўриш, киберхавфсизлик бўйича мутахассислар тайёрлаш, миллий операцион тизим ва дастурий таъминотлар яратиш ва бошқалардан иборат⁴.

Шунингдек, Ўзбекистонда кибержиноятчиликнинг олдини олиш тизими яратилади. Бу ҳақда Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг «2022—2026 йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида»ги фармонида белгилаб қўйилган.

Қайд этилишича, 2023—2026 йиллар учун Ўзбекистоннинг киберхавфсизлик стратегияси ишлаб чиқилади. Бунда «уз» домен зонаси интернет-маконининг киберхавфсизлигини таъминлашнинг асосий йўналишлари белгиланади. Электрон ҳукумат, энергетика, рақамли иқтисодиёт тизимлари ва муҳим ахборот инфратузилмасига тааллуқли бошқа йўналишларни ҳимоя қилиш бўйича комплекс вазифалар тузиб чиқилади.

Шунингдек, кибержиноятчилик учун жиноий жавобгарликни қайта кўриб чиқиш режалаштирилган. Ахборот майдонидаги киберхужум ва таҳдидларни мониторинг қилиш тизими такомиллаштирилади. Бу орқали киберхавфсизлик ягона тармоғининг техник инфратузилмаси кенгайтирилади. «Кибернетикада инновациялар IT-парки» фаолиятини янада жадаллаштириш режалаштирилган.

IT-паркнинг ҳудудлардаги рақамли технологиялар ўқув марказлари негизида ёшларни киберхавфсизлик асослари бўйича ўқитилишини таъминлаш ҳамда ҳар йили талаба ва ўқувчилар орасида киберхужумлар аниқлаш бўйича республика миқёсида конкурслар ўтказиш назарда тутилган⁵.

Бугунги глобаллашув даврида интернет тармоғидан фойдаланишда киберхавфсизлик ҳамда киберқуролнинг нечоғлик зарурлиги, турли хил ёт ахборотлар кириб келишини, жумладан мумкин бўлмаган маълумотларни

⁴ Ўзбекистон Республикасининг «Киберхавфсизлик тўғрисида»ги қонуни. <https://lex.uz/uz/docs/5960604>

⁵ Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги «2022-2026 йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида»ги ПФ-60-сонли Фармони. <https://lex.uz/docs/5841063>

ноқонуний олиш хавфсизлигини таъминлаш муҳимлигича қолмоқда. Буни амалга ошириш учун эса киберхавфсизлик бўйича мутахассислар, шунингдек, ахборот хавфсизлиги бўйича таҳлилчилар жуда зарур. Шу мақсадда мамлакатимизда замонавий дастурлаш технологияларини ўзлаштирган кадрларни тайёрлашга алоҳида эътибор қаратилмоқда. Айтиш пайтда юртимизда “Бир миллион дастурчи” лойиҳаси амалга оширилмоқда. Бугун дунёда рақамлашув, мобиллашув, сунъий интеллектни жорий эта оладиган кадрлар - дастурчиларга талаб юқори. Боиси рақамли иқтисодий таъминловчи инфраструктура, АКТ соҳасига киритилган катта миқдордаги инвестиция ҳам электрон имкониятлардан самарали фойдалана олувчи дастурчилар орқалигина киберхавфсизликни таъминлай олиш мумкин.

Хулоса ўрнида айтиш жоизки, киберхавфсизликни таъминлашга фақат тегишли давлат идоралари ва мутасаддилар зиммасидаги вазифа эмас, балки бугунги кунда ахборот технологиялари билан ишлайдиган, компьютер ёки уяли алоқа воситаларига эга бўлган ҳар бир инсон ҳисса қўшиши лозим. Бунинг учун ушбу йўналишда қабул қилинаётган янги меъёрлар, тартиблар, жорий этилаётган янгиликлардан мунтазам хабардор бўлиш талаб қилинади.

Фойдаланилган адабиётлар:

1. Васенин В.А. Информационная безопасность и компьютерный терроризм. <https://www.crime-research.ru>
2. Ибрагимов В. Кибертерроризм в Интернете до и после 11 сентября 2001: угрозы и нейтрализация. <http://www.crimeresearch.ru/articles/vagif>
3. Голубев В.А. Кибертерроризм – угроза национальной безопасности. <https://www.crive-research.ru>
4. Ўзбекистон Республикасининг “Киберхавфсизлик тўғрисида”ги қонуни. <https://lex.uz/uz/docs/5960604>
5. Ўзбекистон Республикаси Президентининг 2022 йил 28 январдаги “2022-2026 йилларга мўлжалланган Янги Ўзбекистоннинг тараққиёт стратегияси тўғрисида”ги ПФ-60-сонли Фармони. <https://lex.uz/docs/5841063>