

КИБЕРТЕРРОРИЗМ ПРОФИЛАКТИКАСИ: МУАММО ВА УЛАРНИНГ ЕЧИМЛАРИ

Эсанов Дилшодбек Илҳомжон ўғли

Ўзбекистон Республикаси ИИВ Академияси магистратураси

“Илмий-педагогик фаолият” мутахассислиги тингловчиси

***Аннотация.** Мақолада кибертерроризм тушунчаси, бугунги кундаги кўринишлари ва жамиятни кибертерроризм хавфидан ҳимоя қилиш зарурияти таҳлил қилиниб, бундай ҳужумларнинг оқибатларини минималлаштириш учун комплекс стратегиялар механизмини ишлаб чиқилиш зарурати таъкидланади.*

***Калим сўзлар:** кибер терроризм, кибермакон, “Dark Web” ноқонуний қурол савдоси, виртуал дунё, ахборот алмашинуви, мафкуравий таъйиқ, мафкуравий иммунитет, Миллий хавфсизлик, ахборот хавфсизлиги, ҳуқуқий механизм, муҳим инфратузилмани муҳофаза қилиш.*

***Abstract.** Article examines the need to protect society from cyberterrorism, and emphasizes the need to develop a mechanism for comprehensive strategies to minimize the consequences of such attacks. By studying the literature, analyzing existing methods and drawing conclusions and suggesting effective measures to protect the population as a solution.*

***Key words:** cyberterrorism, cyberspace, illegal arms trade “Dark Web”, virtual world, information exchange, ideological pressure, ideological immunity, national security, information security, legal mechanism, protection of critical infrastructure.*

***Аннотация.** Статья исследуеть необходимость защиты общества от кибертерроризма, подчеркивается необходимость разработки механизма комплексных стратегий минимизации последствий таких атак. Изучая литературу, анализируя существующие методы и*

делая выводы и предлагая эффективные меры по защите населения в качестве решения.

Ключевые слова: кибертерроризм, киберпространство, незаконная торговля оружием” темная паутина”, виртуальный мир, обмен информацией, идеологическое давление, идеологический иммунитет, национальная безопасность, информационная безопасность, правовой механизм, защита критически важной инфраструктуры.

Бугун дунё бўйлаб ахборот хавфсизлиги билан биргаликда “кибертерроризм” тушунчаси кенг қўлланилиб, унинг аҳамияти борган сари тўлиқроқ эътироф этилмоқда.

Афсуски, геосиёсий кескинлик ва низоларнинг кучайиши, етакчи давлатлар ўртасида ўзаро ишонч тақчиллиги, глобал хавфсизлик институтлари ролининг пасайиши терроризм ва экстремизм таҳдидларига қарши курашишда очиқ ҳамда самарали халқаро ҳамкорликнинг ривожланишига салбий таъсир кўрсатмоқда.

Шу билан бирга, кибермаконда хавф-хатар ва таҳдидлар кучайиб бормоқда. Бунда ноқонуний фаолият, ёллаш ва радикал ғояларни тарғиб этиш бўйича фаол ишлар миллий чегаралар ва қонунчилик нормаларини тан олмайдиган интернет тармоқлари ҳамда каналлари воситасида тобора кўп амалга оширилмоқда.

Бунинг оқибатида бугунги кунда аҳолининг нисбатан заиф қатламлари вакиллари, жумладан, бизнинг ёшларимиз ва меҳнат мигрантлари “онлайн манқуртлаштириш” қурбонига айланмоқда, турли ноқонуний гуруҳларга жалб этилмоқда ва жиноят содир этмоқда. Шу боис қонунчилик базасини янада такомиллаштириш ҳамда ШХТ Минтақавий аксилтеррор тузилмаси ва МДХ Аксилтеррор маркази фаолияти доирасида бундай хавф-хатар ва таҳдидларни бартараф этиш ва уларга тезкорлик билан жавоб қайтариш бўйича халқаро ҳамкорлик самарадорлигини оширишга қаратилган қўшма амалий чора-тадбирларни ўтказиш энг муҳим вазифалар ҳисобланади.

Таъкидлаш лозимки, мамлакатимизнинг Терроризм ва экстремизмга қарши курашиш бўйича миллий стратегияси кенг қамровли, инклюзив ва тизимли ёндашувга асосланган бўлиб, профилактик ва превентив чораларни қўллаш ҳамда вақтида амалий жавоб қайтаришни ўзида мужассам этади. Жамиятда ҳамжихатлик муҳитини мустаҳкамлаш ва очик мулоқотни ривожлантириш, таълим-тарбия соҳасини ҳар томонлама қўллаб-қувватлаш, иш ўринларини яратиш ва аҳолининг ишончли ижтимоий ҳимоясини таъминлаш бу борадаги устувор йўналишлар ҳисобланади.

Шу билан бирга, биз инсон ҳуқуқ ва эркинликларини ҳимоя қилиш ва илгари суриш, қонун устуворлиги тамойилига сўзсиз риоя этишни терроризм ва экстремизмга қарши курашишнинг фундаментал асоси деб ҳисоблаймиз.¹

Кибертерроризм – террористик мақсадлар йўлида компьютер ва телекоммуникация технологиялари (асосан Интернет)дан фойдаланиш. Кибертерроризм, шунингдек, махсус хакер дастурлари орқали компьютер бошқаруви тармоқларини эгаллаб олиш ва компьютер вируслари ёрдамида Интернет тармоғида теракт содир этиш, Интернет тармоғини ишдан чиқаришни кўзда тутди. Ушбу термин биринчи марта 1980-йилларда АҚШдаги Хавфсизлик ва разведка институти (Institute for Security and Intelligence) катта илмий ходими Барри Коллин томонидан ишлатилган.

Кибертерроризм – ахборот технологиялари ички фаолиятига ноқонуний аралаштириш, компьютерда мавжуд дастурлар ёки маълумотларни мақсадли равишда йўқ қилиш, зарар келтириш, давлат органларининг муҳим қисмлари фаолиятини ишдан чиқариш, шу билан бирга, инсонлар ҳаётига хавф солиш, моддий зарар келтириш ёки оммавий қўрқитиш, ноқонуний қурол савдосини амалга ошириш, давлатлар ўртасида ҳарбий

¹ “Кибермаконда хавф-хатар ва таҳдидлар кучайиб бормоқда”. Ўзбекистон Республикаси Президенти Шавкат Мирзиёевнинг Терроризм ва экстремизмга қарши курашиш бўйича халқаро конференция иштирокчиларига мурожаати.

низоларни келтириб чиқариш каби турли зарарли оқибатларга қаратилган хатти-ҳаракатдир.

Террорчилик ҳаракатлари технология билан боғлиқ равишда ривожланиб, ижтимоий ва иқтисодий тузилма даражаларига чиқди. Бугунги кунда интернет, уяли алоқа воситалари, компьютер технологиялари имкониятлари асосида терроризм молиявий ресурсларни қўлга киритиш, маълумотларни ўғирлаш ва ўзгартиришга қаратилган янги ҳаракатлар кўринишини ҳам олган. Террорчилар манфаатларига хизмат қиладиган бу тенденция “Кибер террор” деб номланди. Кибер терроризм тушунчаси доирасига интернет тизимидаги намоёишлар ҳам киради, чунки террорчилар интернет тизимларига йўл очиб, ўз тарафдорлари сонини борган сари оширомоқда. Лекин террор ва терроризм ўртасида нозик бир фарқ бор. Террор зўравонлик асосида одамларга фикрини сингдириш вазиятини билдиради. Терроризм эса таълимот ва кенг тармоқли ҳаракат асосида сиёсий тизимни ўзгартиришга қаратилгани билан фарқланади.

Қайд этиш ўринлики, кибертерроризм янги ва ўрганилмаган жиноий соҳадир. Интернет тармоғидаги очиқ манбалар орқали биологик, кимёвий, ҳаттоки ядро қуролларини тайёрлаш технологияларини ўрганган ҳолда амалга оширилаётган террорчилик ҳаракатлари ҳуқуқни муҳофаза қилувчи органлар эътиборини тортмоқда. Шунини алоҳида қайд этиш керакки, жиноятчилик билан курашиш амалиётининг ривожланиши, хавфсизлик ва жамоат тартибининг таъминлаш – ички ишлар органлари олдида турган вазифаларни муваффақиятли бажариш, аксарият ҳолатларда улар фаолиятининг ахборот ва таҳлилий таъминланганлик даражаси билан белгиланишини кўрсатади.

Фаолиятга автоматлаштиришни жорий қилиш, компьютер технологияларидан фойдаланиш жараёнидаги катта ҳажмдаги маълумотлар билан ишлар юқини енгиллаштиришга ёрдам берган ҳолатларда айниқса асқотади. Бу ўз ўрнида, иш жараёнида вақтнинг тежалишига, вазифаларни бажариш сифати ва тезкорлигининг ошишига олиб келади.

Ички ишлар органлари таркибида ахборот технологияларидан фойдаланиш соҳасида давлат сиёсатини шакллантириш ва амалга ошириш учун масъул бўлган малакали ходимларга эга бўлинмалар ташкил қилинди, ахборот технологияларидан фойдаланиш давлат дастурларини ва лойиҳаларини идоралараро мувофиқлаштириш тизимининг асоси шакллантирилмоқда.

Кибержиноятчилик тушунчаси ахборот-коммуникация технологиялари соҳасидаги кўплаб турдаги жиноятларни ўзида бирлаштирган. Виртуал тармоқда даҳшат солиш, вирус ва бошқа зарарли дастурлар, қонунга зид ахборотлар тайёрлаш ва тарқатиш, электрон хатларни оммавий тарқатиш (спам), хакерлик ҳужуми, веб-сайтларга ноқонуний кириш, фирибгарлик, муаллифлик ҳуқуқини бузиш, кредит карточкалари рақами ва банк реквизитларини ўғирлаш (фишинг ва фарминг) ҳамда бошқа турли ҳуқуқбузарликлар шулар жумласидандир. Бундай ҳолатларда жиноятчилар ўзларини қизиқтирган “объектлар”га моддий ва маънавий зарар етказишни ўз олдига мақсад қилиб қўяди. Кибержиноятчилик ва уни содир этувчи кимсалар доираси эса йилдан-йилга кенгайиб бораётганини ҳаётнинг ўзи кўрсатиб турибди.

Сайтларни ноқонуний йўллар билан бузиш орқали кибертеррорчилар турли махфий маълумотларни олиш имконига ҳам эга бўлаётганини айтиш жоиз. Шунини алоҳида қайд этиш жоизки, инсонларнинг иродавий жиҳатдан сустлиги, етарли ҳуқуқий билим доирасига эга эмасликлари “**виртуал дунё**”²да турли бузғунчи ғоядаги кучлар учун террористик, экстремистик ташвиқотлар ва ғоялар, ўз қарашларини оммага тарғиб қилиш, ҳар хил жиноий тўдалар фаолиятини амалга ошириш йўлида асосий қурол сифатида ҳам қўл келмоқда. Бу эса ўз навбатида глобал ва минтақавий хавфсизликка нисбатан янги таҳдидлар, муаммолар юзага келишига улкан замин яратмоқда. Интернет тармоғи ўзининг очиқлиги, тезкорлиги ва тежамкорлиги, назоратнинг сустлиги ёки умуман йўқлиги,

² Бирлашган Миллатлар ташкилотининг 2022-2023 йиллардаги “World Drug Report” ахборотномаси;

дунё бўйлаб фойдаланувчилари борлиги, ахборотларнинг тез ва арзон йўл билан тўлиқлигича тарқалиши, ҳамфикр гуруҳларни ташкил этиш мумкинлиги, алоқаларнинг аноним экани, асл манбани аниқлаш имкони йўқлиги, стратегик объектлар, ҳарбий ташкилотлар компьютерларига ноқонуний уланиш имкони мавжудлиги, тармоқларнинг яшовчанлиги билан террорчи ташкилотларни ўзига жалб қилиб келмоқда.

Ҳозирда терроризм, жангарилар яшириниб юрган ёки бош қароргоҳлари жойлашган муайян давлат ҳудуди билан чегараланиб қолаётгани йўқ. Улар аллақачон кибермаконга кўчиб улгуришган. Террорчи ташкилотлар ўз сафларини кенгайтириш ҳамда мақсадларига эришиш йўлида турли ҳилдаги интернет сайтлари ҳусусан, “Dark Web”³ нинг қурол олди-сотди саҳифалари, одам савдоси ва гиёҳвандлик моддалар савдоларини амалга оширишда техника ва интернетнинг сўнгги имкониятларидан устомонлик билан фойдаланишмоқда. Шу йўл билан террорчилик ҳаракатлари, мақсад ва вазифалари ҳақида маълумот бериш, ўз ғоя ва мафқурасини омма орасида тарқатиш билан бирга интернет фойдаланувчиларига ахборот-психологик таъсир ўтказиш, одамлар ўртасида ваҳима уйғотиш, террорчилик ҳаракатларини қўллаб-қувватлаш учун маблағ йиғиш, захарли моддалар, портловчи восита ва қурилмалар ҳамда уларни тайёрлаш технологиясини ўргатиш, террорчилик ташкилоти сафига янги аъзоларни қабул қилиш сингари ҳаракатларни амалга оширишмоқда⁴.

Кибертерроризм шиддат билан ўсиб боришининг яна бир сабаби, у қурол-яроғ ёрдамида амалга ошириладиган террорчилик ҳаракатидан арзонга тушади, жанговар ҳаракатлар, хунрезликлар бўлмайди. Бузғунчи ҳаракатлар интернет ва ижтимоий тармоқлардан фойдаланган ҳолда амалга оширилади. Ушбу жиҳат кейинги 5-6 йилда даҳшатли оқибатлар келтирган ИШИД террорчилик ташкилоти фаолиятида яққол кўринди. Улар ўз

^{3 3} <https://www.forbes.ru/tekhnologii/461629-cto-takoe-darknet-i-naskol-ko-on-bezopasen>

⁴ Ўзбекистонда фанлараро инновациялар ва илмий тадқиқотлар журнали 20.01.2024 й, 26-сон;

тизимида ғоя ва мақсадларни тарғиб қилиш билан шуғулланувчи мутахассисларни бирлаштирган алоҳида тузилма ташкил этиб дунёнинг турли манзилларига маълумотларни улашиб инсонларнинг асосан ёшларнинг онгини забт этишмоқда. Интернетда тарқатилаётган бу каби маълумотларнинг 80 фоизи Яқин Шарқ худудларида фаолият юритаётган террорчи ташкилотларга тегишлидир. ОАВ маълумотлари таҳлили ҳамда жабрланувчиларнинг иқроорларига кўра, радикал ғояларнинг тарқатилиши ва ташкилотларга ёллаш ҳаракатларининг аксарияти “Facebook”, “Odnoklassniki”, “Vkontakte”, “Twitter”, “Youtube” каби ижтимоий тармоқларда амалга оширилмоқда. Ҳозир психологик жиҳатдан ишлов берилган, жангариларнинг экстремистик, ақидапарастлик ғоялари билан йўғрилган видеороликлари билан бир қаторда мобил илова-ю, террорчилар белгиси акс эттирилган буюмларни сотиб олиш имконини берувчи электрон дўконлар кўпайиб бораётгани ҳам кибертерроризмнинг таркибий унсурларига айланган. Диний жиҳатдан дунёқараши тор бўлган айрим кишилар ўзларини гўёки ислом динининг жонкуярлари қилиб кўрсатиб, аслида эса, ҳокимиятни эгаллашни мақсад қилиб қўйган турли оқим вакилларининг қуруқ ваъдаларига алданиб қолмоқдалар.

Ҳозирги кунда жаҳон миқёсида айнан ушбу мавзу бўйича тадқиқот олиб бораётган олимлар томонидан террор ва терроризмга қайси томондан қараш ва ёндашишларига қараб, бу тушунчаларга турлича таърифлар бериб келинмоқда. Соҳа тадқиқотчиларидан бири Бешенинг сўзларига кўра, “терроризм давлат ва халқаро ҳамжамиятга таҳдид бўлиб, доимий тарзда кучайиб борадиган, бугуннинг энг таҳликали муаммоларидан бири сифатида қабул қилинган, жуда мураккаб ва кенг тарқалган ҳодисадир”⁵. Юз бераётган иқтисодий қийинчиликлар, оғир шароитлар ва тенг тақсимланмаган ресурслар терроризмни келтириб чиқарадиган энг катта омиллардир.

⁵. Alexander, Y., & Pluchinsky, D. A. (Eds.). (1992). European Terrorism- Today & Tomorrow. New York: Brassey's.

Синклер эса қадимги даврларда террор ҳокимиятни ушлаб қолиш учун ишлатилган куч бўлгани ва унинг юзага чиқишида 10 та тамойил борлигини таъкидлаган. Уларнинг умумий мазмунига кўра террор баъзилар учун қирғин бўлса, бошқалар учун мақсадлар йўлидаги муваффақият ҳисобланган.⁶

Сагыбекова Акмарал Оразбековна террор ва терроризмга оид барча ёндашувларни умумий тарзда ўрганиш ечим бериши мумкинлигини айтади. Лотинчадаги “террере” ўзагидан олинган терроризм умумий олганда кўрқув, даҳшатга солиш, сиёсий луғатларда эса, бошқарувни қулатиш ёки ижтимоий тузилмани ўзгартиришга ҳаракат қилиш мақсадидаги ўлдиришга қаратилган шиддатли ҳаракатлар, деб таърифланади.

Фикримизча, юқорида таҳлил қилинган маълумотлар ҳамда амалий жиҳатларни инобатга олган ҳолда, кибермаконда содир этиладиган жиноятларни олдини олиш ҳамда уларнинг ҳолатини яхшилаш бўйича кўйидаги таклифларни бериш жамиятда юз бериши мумкин бўлган турли хилдаги кўнгилсизликларни олдини олишга улкан замин яратиши мумкин:

Биринчидан, “Хавфсиз кибермакон” тамойили асосида давлат идоралари, хусусий сектор ва манфаатдор томонлар ўртасида киберхавфсизлик таҳдидлари ҳақидаги маълумотларни алмашишни рағбатлантирувчи ва муҳофаза қилувчи ҳуқуқий асосларни яратиш муҳим ҳисобланади. Бундай механизм киберхавфсизлик соҳасида самарали ҳамкорликни таъминлашга хизмат қилади.

Иккинчидан, аҳоли ўртасида ахборотдан самарали ва мақсадли фойдаланиш кўникмаларини ривожлантириш мақсадида, таълим муассасаларида “Ахборот истеъмоли маданияти” фанини жорий этиш таклиф этилмоқда. Бу фан ахборотни бошқариш маданиятини шакллантириш ҳамда маълумотдан оқилона ва масъулиятли фойдаланишни таъминлашга қаратилиши мақсадга мувофиқ.

⁶ Cranston, A. (1986). The Nuclear Terrorist State. Netanyahu, B. (Ed.), Terrorism, How The West Can Win (1st ed.) in (177-181). Toronto: Collins Publishers

Учинчидан, миллий киберхавфсизлик стратегиясини мувофиқлаштириш ва амалга ошириш мақсадида киберхавфсизлик агентлигини ташкил этиш таклиф этилмоқда. Ушбу марказлаштирилган агентлик кибертахдидларни самарали бартараф этиш учун зарур бўлган малакали кадрлар ва етарли ресурслар билан таъминланиши лозим. Бу киберхавфсизликни мустаҳкамлашда муҳим аҳамиятга эга.

Хулоса ўрнида шуни таъкидлаш жоизки, ёшлар орасида интернет орқали тарқалаётган маълумотларни танқидий англаш ва улардан тўғри фойдаланиш бўйича етарли ишларнинг амалга оширилмаётгани интернетдан “ахборот иммунитетининг”нинг йўқлиги натижасида содир бўлмоқда. Бу инсоннинг интернет орқали тарқатиладиган маълумотларни танқидий баҳолаш, уларнинг ҳаққонийлигини аниқлаш ва зарарли ғоявий таъсирларга нисбатан мустаҳкам қаршилик кўрсатиш қобилиятини англатади. Ахборот иммунитетининг ахборот хуружлари ва манипуляцияларга қарши шахснинг фикрий, маънавий ва ахлоқий ҳимояси сифатида намоён бўлади.

Ахборот иммунитетининг асосий элементлари – билим, кадриятлар тизими ва аниқ мақсадлар тизимидан ташкил топган мустаҳкам тузилмага асосланади. Билим ахборотни танқидий таҳлил қилиш ва унинг ҳаққонийлигини баҳолаш учун муҳим бўлса, кадриятлар тизими зарарли ғояларга қарши қалқон вазифасини бажаради. Шу билан бирга, ижтимоий-иқтисодий, сиёсий ва маданий-маърифий соҳалардаги аниқ мақсадлар ахборотга нисбатан онгли ёндашувни шакллантиришда муҳим ўрин тутаяди. Ахборот иммунитетининг инсонни ахборот хуружлари ва манипуляциясидан ҳимоя қилишнинг асосий шартини ҳисобланади.

Бундай мақсадларсиз шахс ва жамият турли мафкуравий таъсирларга учраш хавфи остида қолади. Шу сабабли, ёш авлодда ахборот иммунитетининг шакллантириш, уларни зарарли ғоялардан ҳимоя қилиш жамиятнинг устувор вазифаларидан бири бўлиши лозим.

Фойдаланилган адабиётлар (REFERENCES):

1. Alexander, Y., & Pluchinsky, D. A. (Eds.). (1992). European Terrorism- Today & Tomorrow. New York: Brassey's.
2. Cranston, A. (1986). The Nuclear Terrorist State. Netanyahu, B. (Ed.), Terrorism, How The West Can Win (1st ed.) in (177-181). Toronto: Collins Publishers.
3. Ўзбекистонда фанлараро инновациялар ва илмий тадқиқотлар журналі 20.01.2024 й, 26-сон;
4. Cyberterrorism Defense Initiative , "CDI: Cyberterrorism First Responder (CFR)", Available online at <http://cyberterrorismcenter.org/cfr.html> de Borchgrave, T. Sanderson and J.Harned, "Force multiplier for intelligence," Centre for Strategic and International Studies, 2007.
5. Валихонова, “Фарғона водийси уйғурларида этноинтеграция жараёнлари”. Илмий хабарнома. научный вестник Учредители: Андижанский государственный университет им. ЗМ Бабура 1:45-48

Фойдаланилган интернет сайтлар:

1. <https://www.forbes.ru/tekhnologii/461629-cto-takoe-darknet-i-naskol-ko-on-bezopasen>
2. <https://uz.wikipedia.org/wiki/Kiberterrorchilik>
3. https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=kiber+terrorizm&btnG=
4. <https://oyina.uz/kiril/teahouse/1845>