РАҚАМЛИ ТРАНСФОРАМЦИЯЛАШУВ ШАРОИТИДА КИБЕРТАҲДИДЛАРГА ҚАРШИ КУРАШНИНГ ИЖТИМОИЙ ОМИЛЛАРИ

Самижонов Азизбек Исмоилжон ўғли
Фарғона давлат университети тадқиқотчиси
https://doi.org/10.5281/zenodo.13757463

Аннотация: ушбу мақолада киберхавфсизлик тушунчасининг мазмун-моҳияти ва концептуал асослари ҳамда учинчи минг йилликда рақамлаштириш билан боғлиқликда юзага келаётган хавф ва таҳдидлар таҳлил қилинган.

Калит сўзлар: рақамли технологиялар, киберхафсизлик, хавфсизлик, ахборот хавфсизлиги, таҳдид, кибер уруш.

Янги Ўзбекистонда амалга оширилаётган кенг кўламли ислоҳотлар доирасида аҳолининг тинч ҳамда осойишта ҳаётини таъминлаш ва жамиятимизда қонунга итоаткорлик шу билан бирга жамоат хавфсизлиги маданиятини шакллантиришга алоҳида эътибор қаратилиб келинмоқда. Жамоат хавфсизлигини таъминлаш йўналишидаги ишларни “Инсон манфаатларига хизмат қилиш” тамойили асосида ташкил этишнинг янги механизм ва тартиблари жорий этилиб, давлат органларининг жамоатчилик тузилмалари билан ўзаро мақсадли ҳамкорлиги йўлга қўйилди.

Киберхавфсизликни муваффақиятли таъминлаш учун ҳимояланган компьютерлар, тармоқлар, иловалар ёки маълумотларни қамраб олувчи бир нечта ҳимоя қатламларини ташкил қилиш керак. Биз яшаётган “онлайн” дунёда илғор киберҳимоя дастурлари ҳар бир фойдаланувчининг манфаати учун хизмат қилади. Киберхавфсизлик муҳим инфратузилманинг асосий элементларини ўз ичига олади. Бу электр станциялари, шифохоналар ва молиявий хизматлар кўрсатувчи компаниялар учун катта аҳамиятга эга. Шу билан бирга, мамлакатимизда киберхавфсизлик соҳасида маҳаллий ва халқаро экспертлар билан тажриба алмашиш, тегишли соҳадаги сиёсатни ишлаб чиқувчи институтлар ва операцион компаниялар ўртасидаги ҳамкорликни мустаҳкамлаш ва уларнинг самарадорлигини оширишдан тобора долзарб аҳамият касб этмоқда.

Киберхавфсизликни таъминлаш, албатта, муайян меъёрлар тизими билан тартибга солинади. Бу белги аҳолини ноқонуний тажовузлардан, турли таҳдидлардан ҳимоя қилиш қонун устуворлиги асосида амалга оширилаётганидан далолат беради. Шуни таъкидлаш керакки, қонун нормалари фавқулодда вазиятларда киберхавфсизликни таъминлаш соҳасидаги муҳим миқдордаги жамоат муносабатларини тартибга солади, хусусан: инсон ва фуқаронинг ҳуқуқ ва эркинликлари, фуқароларнинг хавфсизлигини таъминлаш соҳасидаги хатти-ҳаракатларининг чегаралари, жисмоний ва юридик шахсларнинг хавфсизлигини таъминлашга қаратилган муайян ҳаракатларни амалга ошириш бўйича вақтинчалик мажбуриятларини белгилайди, ноқонуний хатти-ҳаракатлар турларини белгилайди, яъни фақат қонун нормалари жамоат хавфсизлигига, ҳам оддий ҳаёт шароитида, ҳам фавқулодда вазиятларда хавфсизликка тажовуз қилувчи хатти-ҳаракатларнинг тўлиқ рўйхатини белгилайди. Шахс, жамият ва давлатнинг ҳаётий манфаатларини амалга оширишдан келиб чиқадиган ижтимоий муносабатларнинг мавжудлиги, улар

ижтимоий имтиёзлар, конституциявий тузум, жамоат тартиби, шахсий дахлсизлик, мулк ва бошқаларни ўз ичига олади.

Кибехавфсизликни таъминлаш (давлат томонидан жамиятни таҳдидлардан ҳимоя қилиш учун белгиланадиган ҳамда доимий равишда такомиллаштириб бориладиган сиёсий, ижтимоий-иқтисодий, ҳуқуқий ва бошқа комплекс ташкилий чора-тадбирларни қамраб олувчи яхлит тизим)[1] ҳуқуқий тартибга солишнинг сифат жиҳатидан янги босқичига кўтарилди, яъни у “идоравий ҳуқуқий тартибга солиш” деган қарашда намо ён бўла ётган қобиқдан чиқди, давлат бошқаруви органлари жамоат хавфсизлигини таъминлаш бўйича ваколатли субъектларнинг ҳаракатларини самарали амалга ошириш, муайян ҳудудда жисмоний ва юридик шахсларга нисбатан чеклаш чораларини қўллаш имконини берадиган жамоат хавфсизлигини таъминлаш бўйича махсус чора-тадбирларга “муҳтожлик” сезмоқда, фаолият тегишли даражадаги хавфсизликни, хусусан, жамоат хавфсизлигини таъминлаш зарурлигини белгилайдиган объектлар ва ҳудудлар тобора кўпайиб бормоқда. Аҳоли хавфсизлигининг тегишли даражасини таъминлаш уларнинг барқарор фаолият кўрсатиши учун шарт-шароитларни яратишга ёрдам беради, фавқулодда вазиятларда жамоат хавфсизлигини таъминлаш бўйича ваколатли органлар томонидан қўлланиладиган чора-тадбирлар, бу давлат томонидан қўлланиладиган тегишли маъмурий-ҳуқуқий чора-тадбирлар ҳисобланади.

Интернет кўп жиҳатдан дунёни ривожлантирди, лекин бизга илгари ҳеч қачон маълум бўлмаган турли кўринишдаги ва жуда мураккаб таъсирларга йўл очиб берди. Хавфсизлик истиқболи ўсиши билан бирга хакерлик соҳаси ҳам тез ривожланди. Киберхавфсизликни таъминлаш масаласи ва ечими ҳар бир мамлакатнинг асосий эътиборига айланмоқда ва бу соҳада кескин чора-тадбирларни амалга оширмоқда[2]. Улардан бири, юқори ҳисоблаш ва шифрлаш технология таъминланган компанияларни ташкил этиш ва фаолиятини жорий ривожлантиришдир.

Киберхавфсизлик бу интернетга уланган тизимлар, жумладан аппарат-дастурий, дастурий таъминот воситалар ва маълумотларни кибер ҳужумлардан ҳимоялаш ҳисобланади. Унинг таркиби киберхавфсизлик ва физик хавфсизликдан ташкил топади, ҳамда ташкилотларнинг маълумотлар базасига ва бошқа компютерлаштирилган тизимларга рухсатсиз киришдан ҳимоя қилиш учун қўлланилади ва унда асосий талаблар яни маълумотларнинг махфийлиги, ишончлилиги ва барқарорлигини таъминлаши лозим[3].

Киберхавфсизлик таъминлашнинг асосий йўналишларидан бири ахборот ва тизимларни кибертаҳдидлардан ҳимоя қилиш ҳисобланади. Бу таҳдидлар турли шакл ва кўринишларда бўлиши мумкин[4]. Кибертаҳдидлар асосан инновatсион кўринишларда мамлакат ёки муҳим шахсларнинг махфий, сиёсий ва ҳарбий манбаларини нишонга олади. Бу эса киберхавфсизлик сиёсати, стратегияси ва операtсияларига риоя қилишда турли муаммоларни келтириб чиқаради.

Кибер таҳдидлардан баъзилари қуйидагилар[5]:

Кибертерроризм - бу террористик гуруҳларнинг сиёсий мақсадларига эришиш учун ахборот технологияларидан инновatсион фойдаланиш[6]. У тармоқлар, компютер тизимлари ва телекоммуникатсия инфратузилмаларига ҳужумлар натижасида шакллантирилади. Мисол учун 5-6 йилда даҳшатли оқибатлар келтирган ИШИД террорчилик ташкилоти фаолиятида яққол коъринди. Улар оъз тизимида ғоя ва

мақсадларни тарғиб қилиш билан шуғулланувчи мутахассисларни бирлаштирган алоҳида тузилма ташкил этишди.

Бугунги кунда интернетда тарқатилаётган бу каби маълумотларнинг 80 фоизи Яқин Шарқ ҳудудларида фаолият юритаётган террорчи ташкилотларга тегишлидир. ОАВ маълумотлари таҳлили ҳамда жабрланувчиларнинг иқрорларига коъра, радикал ғояларнинг тарқатилиши ва ташкилотларга ёллаш ҳаракатларининг аксарияти “Фасебоок”, “Телеграм”, “Twиттер”, “Тик-ток”, “YuoTube” каби ижтимоий тармоқларда амалга оширилмоқда[7];

Кибер уруш - бу давлатларнинг ахборот технологияларидан фойдаланиб, ҳар қандай давлатнинг тармоғидан ўтиш орқали маълум бир давлатнинг миллий манфаатларига талофат етказиш мақсадидаги ҳаракатларидир. Кўплаб ривожланган давлатлар томонидан кибер уруш қуролли уришлар таркибига киритилган. Кибер уруш ҳужумлари давлатнинг миллий манфаатларини кўзлаб, давлат назорати асосида яхши тайёрланган хакерлар томонидан компютер тармоқларига амалга оширилади. Кибер уруш ҳужуми қимматли маълумотларни ўз ичига олган алоқа, транспорт, савдо ва тиббий хизматлар каби инфратузилмаларни нишонга олиб, асосий мақсад эса тармоқ калитини олиш ва маълумотлар базасига киридир[8];

Кибер жосуслик - бу ахборот технологияларидаги махфий маълумотларни эгалари орқали ёки эгаларининг рухсатисиз олиш ва фойдаланишдан иборат. У кўпинча жосуслик техникалари ва дастурларидан фойдаланган ҳолда стратегик, иқтисодий, ҳарбий устунликни ошириш учун қўлланилади[9].

Кибер жиноятчилар шахснинг биографик маълумотлари асосида кредит карталари билан фирибгарлик; кибер таъқиб; интернетда бошқаларга туҳмат қилиш; компютер тизимига рухсатсиз киришни қўлга киритиш; дастурий таъминотни литсензиялаш ва савдо белгисининг муаллифлик ҳуқуқини ноқонуний ўзлаштириш, ноқонуний нусхаларни яратиш учун бостирувчи шифрлаш; қароқчи дастурий таъминотни ва жиноят содир этиш учун бировнинг шахсини ўғирлаш каби ишларни амалга оширувчилар ҳисобланади. АҚШ Федерал қидирув бюроси маълумотларига кўра, глобал пандемия даврида АҚШда кибер жиноятлар сони 400 фоизга ошган[10].

Ахборот таҳдидлари ва кибер ҳодисалар сони йилдан-йилга ортиб бормоқда. коронавирус авж олиши 2020-йилда онлайн фаолиятга ўтган компаниялар сонининг сезиларли ўсишига сабаб бўлди, бироқ бузғунчилик, ҳужум ва таҳдидлар шунга мутаносиб равишда ошди. Айниқса ҳозирда хакерлик соҳаси тез суратда ривожланмоқда[11]. Шунингдек, 2022-йилнинг учинчи чорагида Касперский лабораторияси 99 989 нафар фойдаланувчининг компютерларидаги банк ҳисобларидан пул ўғирлаш учун мўлжалланган турли шаклдаги зарарли дастурларни ишга тушишининг олдини олган[12].

Кибер жиноятчилар амалга оширган ҳаракатларидан келиб чиқиб, уч гуруҳга бўлиш мумкин:

1-тоифа кибержиноятчилар – кибер жиноятларни амалга оширишга чанқоқлар: хобби хакерлари; IT мутахассислари (ижтимоий муҳандислик энг катта таҳдидлардан бири); сиёсий мақсадни кўзловчи хакерлар; террор ташкилоти.

2-тоифа кибержиноятчилар – ўзларини кибер жиноятчилар сифатида тан олмайдиганлар: психологик таъсир кўрсатувчи хакерлар; молиявий мақсадни кўзловчи

хакерлар (корпоратив жосуслик); давлат - ҳомийликдаги хакерлик (миллий жосуслик, саботаж); уюшган жиноятчилар.

3-тоифа кибержиноятчилар - инсайдерлар: қасос олмоқчи бўлган собиқ ходимлар; талофат етказиш ёки ўғирлик йўли билан иқтисодий устунликка эришиш учун ходимлардан фойдаланган ҳолда компания рақобати.

Тарихдан ташкилотлар ва ҳукуматлар таҳдидларга қарши курашда аниқ ёндашувни қўллаганлар, ўзларининг тармоқларини ва улардаги қимматли маълумотларни ҳимоя қилиш учун биргаликда индивидуал хавфсизлик технологияларини ишлаб чиқаришган. Бу усул нафақат қиммат ва мураккаб, лекин зарарли кибер бузилишлар ҳақидаги хабарларни ҳозир ҳам эшитмоқдамиз ва бу эса мазкур усулларнисамарасиз эканлигини англатмоқда.

Дарҳақиқат, маълумотларнинг бузилиши бўйича бир гуруҳ экспертлар тармоқни киберхавфсизлик соҳасида устуворликлар масала сифатида белгилади. Ташкилотлар кибер ҳимояни таъминлаш учун махсус ишлаб чиқилган маҳаллий интегратсияланган, автоматлаштирилган янги авлод хавфсизлик платформаларини ишлаб чиқиш ва уни маълумотлар базаси ҳамда тармоқларда қўллаш чора тадбирлар амалга оширилмоқда.

Киберхавфсизликдан фойдаланиш киберҳужумлар, маълумотлар бузилиши ва идентификатор ўғирланишининг олдини олишга ва хавфларни бошқаришда ёрдам беради. Ташкилот тармоқ хавфсизлиги ҳақида аниқ тушунчага эга бўлса ва таҳдидларга қарши самарали чоралар кўриш режасига эга бўлса, бу ҳужумларга йўл қўймаслик яхшироқ эканлигини англаб етамиз. Мисол учун, барча фойдаланувчиларнинг компютерларни зарарли кодларини доимий сканер қилиш ва ҳимоясини таъминлаш умумий ахборотлаштириш обектида маълумотларни ҳимояни таъминлаш мумкин[13].

Хулоса ўрнида шуни таъкидлаш керакки, замонавий виртуал оламда киберхавфсизлик тушунчасига бўлган эътибор кундан-кунга ортиб бормоқда. Бунга нафақат бир фойдаланувчининг кибермакондаги хавфсизлиги, балки бирор -бир корхона ёки ташкилот ва ҳаттоки, бутун давлат миқёсидаги киберхавфсизлик ҳам киради. Интернет оламида хавфсизликни таминлаш фойдаланувчи ва виртуал макон орқасидаги ҳар бир восита билан ўзаро комбинатсион тарзда боғлиқ ҳисобланади. Бу боғлиқликларнинг мукаммал системараммасини ўрганган ҳолда киберхафсизликни таминлаш керакдир.

References:

1. Ўзбекистон Республикаси Президентининг 2021 йил 29 ноябрдаги “Ўзбекистон Республикаси жамоат хавфсизлиги концепциясини тасдиқлаш ва уни амалга ошириш чора-тадбирлари тўғрисида”ги ПФ-27-сон Фармон 1-иловаси.
2. O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi 2018-yil 19-fevraldagi PF-5349-son Farmoni.
3. O‘zbekiston Respublikasi Prezidentining “Axborot texnologiyalari va kommunikatsiyalari sohasini yanada takomillashtirish chora-tadbirlari to‘g‘risida”gi 2018-yil 19-fevraldagi PF-5349-son Farmoni.
4. Scannell, Kara (24 February 2016). «CEO email scam costs companies $2bn». Financial Times (25 Feb 2016). Archived from the original on 23 June 2016. Retrieved 7 May 2016.

5. Marcel, Sébastien; Nixon, Mark; Li, Stan, eds. (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks (PDF). London: Retrieved 8 October 2017.
6. Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr A Dictionary of Computer Science. Oxford Reference. Retrieved 8 October 2017.
7. Nurmatov B. Kiberterrorizm shiddat bilan o‘sib borayotganiga sabab nima. 17.03.2019. https://qashqadaryo.uz/oz/nview/kiberterrorizm-shiddat-bilan-%D0%BEsib-borayotganiga-sabab-nima-17-03.
8. Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr A Dictionary of Computer Science. Oxford Reference. Retrieved 8 October 2017.
9. Andrew Butterfield, Gerard Ekembe Ngondi, and Anne Kerr A Dictionary of Computer Science. Oxford Reference. Retrieved 8 October 2017.
10. Marcel, Sébastien; Nixon, Mark; Li, Stan, eds. (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks (PDF). London: Retrieved 8 October 2017.
11. Федотов Н.Н. ДосАтаки всети. Документальная электро-связь. 2015, №13.
12. Федотов Н.Н. ДосАтаки всети. Документальная электро-связь. 2015, №13.
13. “Milliy axborot resurslarini muhofaza qilishga doir qo‘shimcha chora-tadbirlar to‘g-‘risida” O‘zbekiston Respublikasi Prezidentining 2011-yil 8-iyuldagi PQ-1572-son qarori.