АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШНИНГ ҲАРБИЙ-СИЁСИЙ ЖИҲАТЛАРИ

Батиров Фарход Авазович
Ўзбекистон Республикаси Жамоат хавфсизлиги университети
Ўқув-услубий бошқармаси, ўқув жараёнини режалаштириш
бўлими бошлиғи, доцент

Аннотация: Бугунги дунёда киберхавфсизлик турли хил хавфсизлик таҳдидлари ва киберҳужумлар туфайли жуда муҳимдир. Илгари компютерда фақат антивирусни ўрнатиш керак эди, аммо бугунги ҳужумлар анча мураккаб ва махсус ҳимоя усулларини талаб қилади. Киберхавфсизлик муҳим аҳамиятга эга, чунки у нафақат ахборотни, балки бутун ишчи тизимни вирус ҳужумидан ҳимоя қилади. Кибертаҳдидлар душман давлатлар ва террористик гуруҳлардан тортиб шахсий хакерлар ва ишончли шахслар, жумладан, ўз имтиёзларини ёмон ниятли ҳаракатлар қилиш учун суистеъмол қиладиган ходимлар ёки пудратчилар каби турли манбалардан келиб чиқиши мумкин.

Калит сўзлар: Киберхавфсизлик / хавфсизлик / маълумотлар / ҳимоя / ахборот / хизматлар / бузғунчилар / тармоқ миллий хавфсизлиги / кибер хавфсизлик / ахборот хавфсизлиги.

Аннотация:В современном мире кибербезопасность очень важна из-за различных угроз безопасности и кибератак. Ранее нужно было только установить антивирус на компьютер, но сегодняшние атаки являются куда более сложными и требуют специальных методов защиты. Кибербезопаность важна, потому что она защищает не только информацию, но и всю рабочую систему от вирусной атаки. Киберугрозы могут исходить из самых разных источников: от враждебных государств и террористических групп до отдельных хакеров и доверенных лиц,

таких как сотрудники или подрядчики, которые злоупотребляют своими привилегиями для совершения злонамеренных действий.

Ключевые слова: Кибербезопаность / безопасность / данные / защита / информация / сервисы / злоумышленники / сетьнациональная безопасность / кибербезопасность / информационная безопасность.

Abstract: In today's world, cyber security is very important due to various security threats and cyber attacks. Previously, it was only necessary to install an antivirus on the computer, but today's attacks are much more complex and require special protection methods. Cybersecurity is important because it protects not only information, but the entire working system from a virus attack. Cyber threats can come from a variety of sources, from hostile states and terrorist groups to individual hackers and trusted individuals such as employees or contractors who abuse their privileges to commit malicious acts.

Keywords. Cyber security / security / data / protection / information / services / intruders / network national security / cyber security / information security.

Киберхавфсизлик билан боғлиқ бошқа концепция Ўзбекистонда рақамли кун тартибини (Рақамли Ўзбекистон) амалга ошириш зарурати бўлиб, у Ўзбекистон томонидан қабул қилинган халқаро мажбуриятларга тўғри келади. Ўзбекистонда ижтимоий-иқтисодий, технологик ва миллий киберхавфсизликни ривожлантиришнинг турли даражалари туфайли жиддий муаммолар пайдо бўлиши мумкин. Ўзбекистоннинг Киберстратегияси - бу соҳадаги давлат сиёсатининг асосий йўналишларини ишлаб чиқиш ва амалга оширишни, норматив-ҳуқуқий базани такомиллаштиришни талаб қиладиган давлатнинг ёндашувлари тўпламидир. Мисол учун, Германия иқтисодиёти ҳар хил турдаги киберҳужумлар марказида бўлиб, у сезиларли даражада зарар кўрмоқда, шунинг учун киберхавфсизлик унинг асосий муаммоларидан биридир. Шунга кўра, кибермудофаа тизими ишлаб чиқилди ва доимий равишда такомиллаштирилди.

Германиянинг киберхавфсизликка бўлган ёндашуви ўзининг табиатига кўра мураккаб бўлиб, "Ахборот инфратузилмасини ҳимоя қилиш бўйича Миллий дастур" (2005 йил) ва "Ахборот инфратузилмасини ҳимоя қилиш" га қаратилган меъёрий ҳужжатлар, дастурлар, институтларнинг бутун тизимини ўз ичига олади. Муҳим инфратузилма компонентлари амалга ошириш дастури 2007 йилда қабул қилинган. Ҳукумат, бизнес ва бошқа институтлар иштирокида ишлаб чиқилган ушбу ҳужжатлар IT инқирозларига жавоб беришнинг умумий стратегиясини белгилаб беради ва бизнес ҳамжамиятига йирик киберҳужумларга қарши кўрсатмалар беради. ГФРнинг миллий киберхавфсизлиги учун масъул орган - Ички ишлар вазирлиги. Германия Федерал ахборот хавфсизлиги агентлиги томонидан асос солинган. Ушбу орган ахборот хавфсизлиги сиёсатини шакллантиради ва ҳодиса учун ҳаракатлар режасини тузади: инқирознинг олдини олиш, аниқлаш ва жавоб.

Киберхавфсизлик ва хавфсиз ахборот узатиш жараёнлари соҳасида халқаро ҳамкорлик тузилманинг вазифаларидан бири бўлиши керак. Бу борадаги кейинги ишлар Марказнинг вазифаларини янада ойдинлаштириши аниқ. Шу жихатдан куриш мумкинки, ушбу илгор тажрибадан давлатимизда киберхавфсизликни таъминлашда фойдаланиш мумкин. Муайян йўналишларни тартибга солишга келсак, у норматив соҳада амалга оширилади. Шуни таъкидлаш керакки, мамлакатимизда маълумотларга кириш, маълумотларнинг махфийлиги ва ҳимояси бўйича умумий қоидаларни белгилайдиган умумий, асосий қонун йўқ, аммо маълум даражада Киберстратегия билан алмаштирилади.

Ҳозирги вақтда "ахборот хавфсизлиги" атамаси билан бир қаторда "киберхавфсизлик" атамаси ҳам қўлланилмоқда. Кўпгина ҳолларда, бу ҳодисалар битта деб ҳисобланади, аммо бундай эмас. Икки масала ўртасидаги фарқни кўрсатиш улардан келиб чиқадиган бошқа масалаларнинг моҳиятини тўғри аниқлаш имконини беради. Масалан, ахборот ва киберҳужумлар, ахборот терроризми ва кибертерроризм, ахборот экстремизми ва киберекстремизм. Ғарб олимларининг тадқиқотларида "Кибер хавфсизлик объект" ва "Киберхавфсизлик

объекти", бири "кибер маконда обект хавфсизлиги", иккинчиси эса "объектнинг киберхавфсизлиги (ҳимояланган ҳолати)" деб номланади. Биринчи ҳолда, кибернетик объектнинг хавфсизлиги, яъни кибернетик объект, жумладан, Интернет ва унда қурилган тизимлар атроф-муҳитга қанчалик зарарли эканлиги кўриб чиқилади. Иккинчи ҳолда, кибернетик объектни муҳофаза қилиш ҳолати, яъни ташқи муҳитнинг кибернетик объектларга қанчалик зарар этказиши мумкинлиги кўриб чиқилади. Иккинчи ҳолда, кибержиноят, кибертерроризм, киберекстремизм ва киберҳужумлар ҳақида гапириш мумкин. Чунки уларнинг барчаси ташқи муҳитга таъсир қилади ва кибернетик объектларнинг бир текис ишлашини бузишга қаратилган. Масалан, киберҳужумлар махсус компьютер дастурлари орқали ахборот ва кибермаконда жойлашган обектларга зарар етказувчи мақсадли ҳаракатлар деб қаралади. Бундай киберҳужумлар ҳам ички, ҳам ташқи бўлиши мумкин. Бундай ёндашув жамиятнинг ахборот соҳаси ва ахборот майдонига нисбатан ҳам мақбулдир.

Ахборот хавфсизлиги - мамлакатнинг ахборот манфаатларини (ахборот объектларини) таҳдид ва хавфлардан ҳимоя қилиш ҳолати. Шу билан бирга, ахборот хавфсизлиги деганда ахборот тизимларидан фойдаланиш контекстида ва мақсадли маълумотлар орқали аниқ субъектлар томонидан юзага келадиган хавф ва хавфлар тушунилади. Шуни таъкидлаш керакки, киберхавфсизлик ахборот хавфсизлигининг ажралмас қисмидир. Бошқача қилиб айтганда, ахборот хавфсизлиги киберхавфсизликдан кўра кенгроқ маънога эга. Киберхавфсизлик - бу ахборот тизимларининг ҳолати. Ахборот уруши шароитида мунтазам фаолиятини сақлаб қолишга қодир. Киберхавфсизлик масаласига асосий эътибор техника фанлари соҳасидаги мутахассислар томонидан қаратилади.

Ғарб тадқиқотларида ахборот хавфсизлиги маълумотларнинг махфийлиги, аниқлиги ва фойдаланиш имкониятини ҳимоя қилиш деб қаралади[1]. Ахборот хавфсизлиги концепциясида, шунингдек, ушбу турдаги хавфсизликнинг мақсадлари маълумотларнинг махфийлиги, аниқлиги ва фойдаланиш имкониятига боғлиқлиги таъкидланган.

Ахборотнинг аниқлиги ахборот хавфсизлигининг энг муҳим элементларидан биридир. Шунинг учун ҳам аниқ ахборотни ҳимоя қилиш ва унинг мазмуни ўзгаришининг олдини олиш ахборот хавфсизлигини таъминлашнинг асосий йўналишларидан биридир.

Ахборот хавфсизлигининг учинчи элементи - ҳар қандай субъектнинг самарали фаолияти учун муҳим бўлган ахборотга кириш. Ахборот тизимлари ва сервис веб-сайтларига кириш кўплаб корхоналар учун устувор вазифа ҳисобланади. Веб-сайтларга кириш ҳуқуқини, ҳатто қисқа вақт ичида ҳам бузиш, даромаднинг йўқолишига, мижозларнинг норозилигига ва уларнинг обрўсига путур етказади.

Умуман олганда, сўнгги ўттиз йилликда ахборот ва киберхавфсизлик босқичма-босқич аҳамият касб этиб, бугунги кунда миллий хавфсизлик соҳасидаги устувор йўналишлардан бири ҳисобланади. Чунки интернетдан фойдаланувчилар сони ортиб бориши, компьютер техникасининг турли фаолият соҳаларида кенг қўлланилиши натижасида жамиятнинг ижтимоий-сиёсий ва иқтисодий ривожланишига таъсир кўрсатишнинг янги йўллари ва усуллари вужудга келди. Компьютер технологияларининг ижобий хусусиятлари билан бир қаторда, улар кўпинча салбий оқибатларга ва таҳдидларга эътибор қаратадилар. Интернет ўзига хос тузилишга эга бўлганлиги сабабли у ахборот-коммуникация технологиялари, алоқа тизимлари, ахборот ва Интернет фойдаланувчиларини ўз ичига олади ва шунинг учун миллий ва глобал даражадаги жараёнларни бошқаришга чуқур таъсир кўрсатишга қодир.

Интернет ва ахборот технологияларининг технологик салоҳиятига келсак, Интернетни яратиш лойиҳаси биринчи марта 1961-1962 йилларда АҚШ ҳарбий муҳитида пайдо бўлган ва 1990-йилларнинг бошларига келиб у ҳарбий объектларни бошқариш учун тўлиқ амалга оширилган ва маълумотлар узатишдан фойдаланилган. Яъни, Интернет дастлаб тўлиқ АҚШ армияси эҳтиёжларини қондириш учун яратилган. Бироқ 1994-йилдан бошлаб Қўшма Штатлар Интернетни демократия ривожининг муҳим омили сифатида эътироф

этиб, унинг кейинги ривожланишини хусусий секторга қолдирди. Натижада, интернетни шакллантирадиган ва уни фуқаролик жамиятига тақдим этувчи турли хил хусусий сектор институтлари, жумладан, ахборот технологиялари компаниялари пайдо бўлди[2]. Сўнгги уч ўн йилликда Интернетдан фойдаланувчилар сони тез суръатлар билан ўсиб бормоқда. Мисол учун, Агар 1991-йилда фойдаланувчилар сони 10 минг кишигача бўлган бўлса, 2000-йилда 400 миллиондан ортиқ кишини ташкил этди, 2010-йилда 2,3 миллиарддан ортиқ кишини ташкил этган бўлса, ҳозирда бу кўрсаткич 4 миллиард кишидан ошди[3]. Яъни, ҳозирда дунё аҳолисининг ярми интернетдан фойдаланмоқда, яқин йилларда эса уларнинг сони ортади.

Интернетдан сиёсий мақсадларда фойдаланиш кўплаб олимлар ва тадқиқотчилар томонидан таҳлил қилинган. Интернетнинг иқтисодий ривожланишнинг муҳим элементи сифатидаги аҳамияти ҳамда унинг иқтисодий йўқотишлари ҳақида ҳам кўп гапирилади[4].

Россиялик тадқиқотчи И.Л. Морозов ахборот-технологик инқилоблар натижасида юзага келадиган таҳдид ва хавфларни икки гуруҳга ажратди: тизимли ва ташқи таҳдидлар[5]. Унинг фикрича, биринчи гуруҳ таҳдидлари давлат органлари ва тизимли сиёсий кучлар томонидан мақсадли равишда амалга оширилмоқда. Бундай таҳдидларга алоҳида давлатлар томонидан рақибларнинг сиёсий тизимларига ахборот ва психологик ҳужумлар, мамлакат ичидаги сиёсий кучларнинг тизимга қарши ҳаракатлари ва бошқалар киради. киритилган. Иккинчи гуруҳ таҳдидларининг пайдо бўлиши террористик ва экстремистик ташкилотлар ва кибержиноятчиларнинг фаолиятига боғлиқ. Аниқ тузилма мавжуд эмаслиги сабабли, бундай хатти-ҳаракатларнинг мумкинлиги ва уларнинг ноанъанавийлиги бундай таҳдидларнинг салбий оқибатларини ўз вақтида олдини олишга имкон бермайди.

Шундай қилиб, замонавий шароитда ахборот хавфсизлиги миллий хавфсизлик соҳасидаги устувор йўналишлардан бири бўлиб, миллий манфаатлар ҳимояси даражаси ва сифатини белгилаб беради. Ахборот хавфсизлигини

таъминлаш зарурати ва аҳамияти икки тенденция билан оқланади: биринчидан, ахборот технологиялари, компьютер технологиялари ва Интернет тармоғининг кенгайиши; иккинчидан, жамият ҳаётининг турли соҳаларини ривожлантириш билан боғлиқ.

Ўзбекистоннинг ахборот хавфсизлиги сиёсатининг асосий мақсади шахс, жамият ва давлат манфаатларини мувозанатлаш ва ҳимоя қилишдир. Кибермакондаги мақсадларимизга эришишда биз инсон ҳуқуқ ва эркинликлари, давлат суверенитети тамойилларига таянамиз. Ўзбекистон очиқ, ҳамкорликда ишлайдиган, ишончли ва хавфсиз интернет тарафдоридир.

Ахборот, технология ва киберхавфсизлик соҳасида биз институтларни ривожлантиришга жараёнлар самарадорлигини оширишга инфратузилмани ривожлантиришга ҳаракат қиламиз. Ўзбекистон давлат ахборот, технология, киберхавфсизлик сиёсати, стратегияларини ишлаб чиқиш, шунингдек, секторни бошқаришнинг миллий механизмларини жорий этишни давом эттирмоқда. Биз IT провайдерлари ва рақамли хизматлар провайдерлари ўртасидаги давлатдан-давлат муносабатларининг меъёрий-ҳуқуқий асосларини ишлаб чиқамиз, натижада Миллий киберхавфсизлик маркази ва компьютер бузилишларига жавоб бериш гуруҳларини шакллантириш мумкин бўлади.

ХУЛОСА

Ахборот соҳасида барқарорликни ошириш мақсадида рискларни самарали бошқариш, малакали касбий салоҳиятни ривожлантириш, халқаро стандартларни маҳаллийлаштириш, рақамли саводхонлик даражасини ошириш орқали миллий ахборот кибер имкониятларини ривожлантирамиз. Соҳадаги иштирокчиларнинг хилма-хиллиги, ахборот соҳасида халқаро чегараларнинг йўқлиги, давлат, жамият ва хусусий сектор ўртасидаги имкониятларнинг тақсимланиши ҳисобга олинган ҳолда, давлат ва хусусий ва халқаро секторлар ўртасидаги ҳамкорлик даражасини ошириш зарур калит, давлат бунга интилади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙҲАТИ: (REFERENCES)

1. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века // Вопросы кибербезопасности. – 2013. -№ 1 (1).;

2. История интернета [Электронный ресурс]. ЦКЪ: https://ria.ru/20190902/1558095640.html (дата обращения: 28.09.2020 г.).;

3. Нагирная А.В. География интернета и вопросы информационной безопасности // Геополитика и экогеодинамика регионов. – 2018. -Т.4 (14). -№4.;

4. Акопов Г.Л. Политика и интернет. Монография. -М.: ИНФРА-М, 2020.;

Морозов И.Л. Информационная безопасность политической системы // Полис. Политические исследования. -2002. -№5.;