European Journal of Interdisciplinary Research and Development
Volume-11 Jan. - 2023
Website: www.ejird.journalspark.org ISSN (E): 2720-5746

# КИБЕРТАҲДИД ТУЗУЛМАСИ ВА УНИНГ НАМОЁН БЎЛИШ ШАКЛЛАРИ

Кадиров Мирсултон Батирович
Ўзбекистон Республикаси Жамоат хавфсизлиги университети
Ижтимоий-гуманитар фанлар кафедраси профессори

Батиров Фарход Авазович
Ўзбекистон Республикаси Жамоат хавфсизлиги университети Ўқув-услубий бошқармаси, ўқув жараёнини режалаштириш бўлими бошлиғи
E-mail: Farxod-batirov mail.ru

**АННОТАЦИЯ**
Мазкур мақолада кибертаҳдид тузилмаси ва унинг намоён бўлиш шакллари ҳақида сўз юритилади. Шунингдек, бугунги глобаллашув ва ғоялар таҳдиди авж олган бир пайтда киберхавфсизликни таъминлашнинг муҳим жиҳатлари таҳлил этилган.
Хусусан, кибертаҳдидларнинг давлат сиёсатини амалга оширишда муаммоли вазиятда юзага келтиришнинг олдини олишга доир таклифлар ва хулосалар берилган.

**Калит сўзлар:** Кибержиноят, киберхужум, кибермудофаа, кибертаҳдид, сунъий интеллект, хавфсизлик, маълумотлар, ҳимоя, ахборот, хизматлар, миллий хавфсизлиги, кибер хавфсизлик, ахборот хавфсизлиги.

# СТРУКТУРА КИБЕРУГРОЗЫ И ФОРМЫ ЕЁ ПРОЯВЛЕНИЯ

**АННОТАЦИЯ**:
В данной статье речь идёт о структуре киберугрозы и формах ее проявления. Также анализируются важные аспекты обеспечения кибербезопасности в условиях сегодняшней глобализации и угрозы идей.
В частности, даны предложения и выводы по предупреждению возникновения киберугроз в проблемной ситуации при реализации государственной политики.
**Ключевые слова:** Киберпреступность, кибератака, кибербезопасность, киберугрозы, искусственный интеллект, безопасность, данные, защита,

информация, услуги, национальная безопасность, кибербезопасность, информационная безопасность.

# THE STRUCTURE OF THE CYBER THREAT AND THE FORMS OF ITS MANIFESTATION

**ANNOTATION**

This article focuses on the structure of cyber threat and the forms of its manifestation. The important aspects of cybersecurity in today's globalization and the threat of ideas are analyzed.

In particular, suggestions and conclusions are given to prevent the occurrence of cyber threats in a problematic situation in the implementation of state policy.

**Keywords**: Cybercrime, cyberattack, cybersecurity, cyber threats, artificial intelligence, security, data, protection, information, services, national security, cybersecurity, information security.

**Кириш**

Дунёнинг ривожланган давлатлари тажрибасидан маълум бўладики, бугунги кун миқёсида ахборот технологияларининг ривожланиши ва турли объектлар томонидан фойдаланиш киберхавфсизликни таъминлаш муаммоларни ҳал этиш масалаларини устувор вазифага айлантирмоқда. Чунки кибермаконда турли жиноий гуруҳлар томонидан иқтисодий-ҳарбий жосуслик амалга оширилмоқда. Бу жараёнда дастурий таъминот тизими анъанавий хавфсизлик ечимларини янги усуллар билан жумладан, сунъий интеллект ва таҳлилларни йўқ қилишга интилади. Шу боисдан ҳам бугунги кунда кибертаҳдиддан ташқари, фойдаланувчиларнинг шахсий маълумотларини ноқонуний маълумотлар тўплашдан ҳимоя қилиш ҳам тобора долзарб масалага айланиб бормоқда.

Жаҳоннинг нуфузли университет ва илмий тадқиқот институтларида ахборот-коммуникация технологияларини ривожлантиришнинг юқори суръатларини ҳисобга олган ҳолда, иқтисодиёт, давлат ва ҳаётнинг турли соҳалари учун муҳим аҳамиятга эга бўлган инфратузилмани ҳимоя қилиш, ахборот тизимларига киберҳужумларнинг кўпайишини олдини олиш, кибертаҳдид ва киберхужумларни иқтисодий, молиявий, банк, соғлиқни сақлаш каби инфратузилларманинг асосий соҳаларига таъсирини олдини олиш ва бошқа бир қанча йўналишларда илмий изланишлар олиб борилмоқда. Бу ерда гап ўзаро боғланган тармоқлар ва ахборот инфратузилмасига зарар етказиши мумкин бўлган ҳам фуқаролик, ҳам ҳарбий кибермаконни ҳимоя қилиш ҳақида кетмоқда. Ушбу муаммоларни ҳал қилиш учун концептуал (стратегиялар - тамойиллар) ёндашувларига бўлган эҳтиёж мамлакат инфратузилмасининг мувофиқлаштирилган, ишончли ишлаши

заруратидан келиб чиқади. У давлат, хусусий сектор, жамият ва халқаро ташкилотларнинг кибермакондаги саъй-ҳаракатларини мувофиқлаштиришга қаратилган.

**Мавзуга оид адабиётларнинг таҳлили (Literature review).** "Дунёдаги биринчи киберҳужум" деб ҳисобланган 1988 йилги воқеа сарлавҳаларга айланди. Гарвард битирувчиси Роберт Таппан Моррис томонидан яратилган Моррис вируси, яъни - шахсий зарарли дастур ўша пайтда 60 000 та компьютернинг 10 фоизини юқтирган ва компьютер хавфсизлигида сейсмик силжиш яратган. 30 йил ўтиб, киберхавфсизлик замонамизнинг энг катта муаммоларидан бирига айланди. Кибержиноят илмий тадқиқот лойиҳасидан келиб чиқди ва профессионал кибержиноятчилик хизматларининг жаҳон бозорига тезлик билан кириб келди, натижада геосиёсий босқичда ҳукуматлар кибермаконда бошланиб, рақобатчиларнинг муҳим IT инфратузилмасига зарар етказиши мумкин бўлган гипер илғор киберҳужумларга мурожаат қилишди. Корхоналар, мактаблар, касалхоналар ва жамиятнинг бошқа қисмлари Интернетга тўлиқ уланганидан киберҳужумлар Жаҳон Иқтисодий Форумининг табиий офатлар ва иқлим ўзгариши рўйхатида глобал жамият учун энг катта таҳдидлардан бирига айланади. О.Ғ.Давлатов фикрича, “Ахборот хавфсизлигини таъминлаш энг аввало, турли ахборот манбаларидаги маълумотларни таҳлил этиш, баҳолаш ва зарарли ахборотларни аниқлаш, талабаларни зарарли ахборотлар таҳдидидан ўз-ўзини ва жамият аъзоларини ҳимоя қилиш, уларга қарши курашишга тайёрлашни талаб этади”[1, Б-11].

Йиллар давомида хакерлар эски одатни мустаҳкамлаб борди: “Агар ирода бўлса, унда йўл бор” Ҳимоячи томон хавфсизлик деворларига янги қоидаларни қўллагани ёки ўзлари кўрган ҳужумлар асосида янги аниқлаш сигналларини ишлаб чиққанидек, хакерлар анъанавий ҳимояни олдини олиш учун доимо ўзларининг ҳужум методологиясини қайта ишлаб чиқдилар[2].

Хорижий мамлакатларда Э.Сэрра, Т.Паренти, П.Тронкон, Карл Олбинг, Ю.Диогенес ва бошқа олимлар ушбу муаммонинг турли жиҳатларини ўз соҳалари йўналишларидан келиб чиқиб тадқиқ қилганлар. Жисмоний шахслар, корхоналар ва ҳукуматлар учун киберхавфсизлик хавфининг интернетига тегишли илғор қурилмаларнинг кўпайиши билан ортиб бормоқда. Компьютер хавфсизлиги, киберхавфсизлик ёки ахборот технологиялари хавфсизлиги компьютер тизимлари ва тармоқларини махфий маълумотларнинг чиқиб кетишидан, аппарат, дастурий таъминот ёки электрон маълумотларнинг ўғирланиши ёки шикастланишидан, шунингдек улар тақдим этаётган хизматлардаги носозликлар ва узилишлардан ҳимоя қилиш сифатида яққол намоён бўлади.

Мустақил давлатлар ҳамдўстлиги мамлакатларидан И.Л.Сафронова, Е.А. Соловьева, О.В.Столетов, Е.Н.Молодчая, М.М.Кучерявый, Е.В.Батуева, В.Ф. Джафарли, П.А.Карасев, Е.С.Зиновьева, А.В.Курилкин ва бошқа шу каби олимлар томонидан муаммонинг ҳуқуқий, сиёсий ва ижтимоий-маданий жиҳатлари батафсил ўрганилган. Мазкур тадқиқотлардан маълум бўладики, сунъий интеллект киберхавфсизликда истиқболли ва у асосан таҳдидларни аниқлаш тизимлари билан боғлиқ. Автоматлаштириш нафақат ҳар қандай бузилишлар аниқланишини

таъминлайди, балки заиф бўлимларни ҳам ҳимоя қилиши мумкин. Чуқур ўрганиш имкониятлари энди тармоқ таҳдидларини аниқлаш учун журналлар, транзакциялар (маълумотлар трафиги) ва маълумотларни кузатиш учун фойдаланилмоқда. Машинанинг ўз-ўзини ўрганиш имкониятлари барча мумкин бўлган изларни топиш ва аномалияларни аниқлашни ўз ичига олади. У тузилмани таниб олишни “ўрганиш” ва потенциал ҳужум уринишлари ҳақида огоҳлантириш қобилиятига эга, шунингдек, киберхавфсизлик таҳдидларини олдини олиш учун такрорий хатти-ҳаракатларни мослаштириши ва яшириши мумкин. Бундай инновацион технологиялар кундан-кунга такомиллаштирилмоқда.

Мамлакатимизда М.Х.Рустамбаев, С.Ю.Аҳроров, И.Ю.Иноятов, А.М.Камбаров, С.О.Отамуродов, Р.С.Самаров, А.Сотиволдиев, У.С.Темирова, Н.Ж.Эшнаев, З.Ш.Алимардонов, Б.С.Боймуродов, Э.Ш.Ҳайитов, Р.Самаров ва бошқалар ахборот ва жамоат хавфсизлигини таъминлашнинг турли жиҳатларини ўрганишга алоҳида эътибор қаратганлар.

**Тадқиқот методологияси (Research Methodology).** Парадигма ўзгариши 2017-йилда ҳалокатли тўлов дастури вируслари WannaCry ва NotPetya анъанавий хавфсизлик деворларидан фойдаланган ҳолда 150 та мамлакатдаги минглаб муассасалар, жумладан, қатор соғлиқни сақлаш тизимлари ишини билмаган ҳолда тўхтатиб қўйганида юз берди[3]. Янги ҳужумларнинг олдини олиш учун ишлатилиши мумкин бўлган тобора такомиллаштирилган восита “кечаги ҳужумлар ҳақидаги маълумотлар эртанги таҳдидларни башорат қила олмайди” деган фалсафаси асосида ишлаб чиқилган сунъий интеллект мудофааси эди. Сунъий интеллект рақамли муҳит учун нима "нормал" эканлигини тушуниш ва пайдо бўлган муаммоларни аниқлаш, мудофаага эски ёндашувлардан воз кечиш учун ишора қилиш учун ишлатилган.

Сўнгги йилларда минглаб ташкилотлар тез ҳаракатланувчи киберҳужумларга компьютер тезлигида жавоб бериш учун машина алгоритмларига таянди. Бундай фаол мудофаа функциясида сунъий интеллектдан фойдаланиш хавфсизлик гуруҳлари ролини тубдан ўзгартирди. Ҳужумкор ландшафтнинг кейинги эволюцияси қандай? Хакерлар киберхавфсизлик ландшафтидаги кейинги парадигма ўзгаришини башорат қиладиган, мослашувчи, аниқланмасликни ўрганадиган ва доимий равишда ривожланиб борувчи зарарли алгоритмларни қўллашни ўрганиш учун аллақачон машинани ўрганишдан фойдаланмоқда – булар сунъий интеллектга асосланган ҳужумлардир. Forrester томонидан яқинда ўтказилган тадқиқот шуни кўрсатдики, хавфсизлик бўйича мутахассисларнинг 88 фоизи сунъий интеллект ёрдамида бошқариладиган ҳужумлар киберҳужумлар аллақачон киберҳужумларнинг гипер ўзгаришлар даври эканлигини исботловчи асосий омил бўлишини кутишади – бу вақт масаласидир.

Ҳужумкор интеллект ўзининг (сунъий интеллект) юқори даражада ривожланган ва тақлид қилувчи инсонни ўрганиш ва мослашиш қобилиятидан фойдаланади, аммо янги даврга ўтиши мумкин бўлган машина тезлигидаги ҳужумларни амалга оширади. Attack Сунъий интеллект мақсадли тармоққа кириш имкониятига эга бўлиши ва ҳужумни бошқариш учун кўрган маълумотлардан фойдаланган ҳолда энг қимматли маълумотларнинг жойлашишини автоматик равишда аниқлаши мумкин. Биз аллақачон

бунинг дастлабки белгиларини кўряпмиз - нотўғри маълумот тарқатиш учун мўлжалланган сунъий интеллект томонидан бошқариладиган “dipfey” (чуқур сохта) контент ижтимоий медиа гигантлари учун долзарб муаммодир.

Очиқ манбали AI тадқиқот лойиҳаларида ҳужум даврининг ҳар бир босқичини юклаш учун ишлатилиши мумкин бўлган воситалар ҳали ҳам мавжуд. Тез орада улар, шубҳасиз, норасмий тармоқларда сотиб олинадиган хакерлик хизматлари рўйхатига қўшилади. Darktrace AI interrupts сунъий интеллект лабораториялари ижтимоий тармоқлар таъсиридан келиб чиқиб, ташкилотнинг энг юқори даражадаги мақсадларини автоном тарзда аниқлай оладиган сунъий интеллект прототипларига ҳужум қилади – улар ҳаммасини бир неча сония ичида бажаради. Кейин сунъий интеллект алдаш учун мос платформани танлаб, контекстли фишинг электрон почта хабарларини тайёрлайди. Қабул қилувчи зарарли ҳаволани босиш ёки кейинчалик мақсадли ташкилотга кириш имконини берувчи ҳаволани очиш орқали уларнинг қурбонига айланади.

**Таҳлил ва натижалар (Analysis and results).** Киберхавфсизлик бўйича самарали чора-тадбирларни амалга ошириш жуда қийин жараён. Бугунги кунда ҳужумларни амалга оширадиган қурилмалар сони одамлар сонидан бир неча баравар кўп ва кибер жиноятчилар ҳар куни янги ихтиролардан фойдаланадилар. “Кибержиноятчилар ҳуқуқий нигилизм ва ўзларига юқори баҳо беришлари билан фарқланиб, кўп ҳолатларда ўзларининг жазога тортилмаслиги ва заиф эмаслигини ҳис этган ҳолда қонун нормаларига риоя этмайдилар ва ўзларининг шахсий тушунчаларидан келиб чиқиб, у ёки бу ҳуқуқий нормаларнинг адолатлилиги ва тўғрилигини мустақил аниқлашга ҳақли, деб ҳисоблайдилар. Аксарият ҳолатларда улар инфантилизм, масъулиятсизлик, муросасизлик, ўз ҳаракатларининг оқибатларини тушунмасликни намоён этиб, жамоатчилик фикри ва манфаатларини писанд қилмайдилар”[4, Б-23].

Муваффақиятли киберхавфсизлик ёндашуви ҳимоя қилиниши керак бўлган компьютерлар, тармоқлар, дастурлар ёки маълумотларнинг кўп даражали ҳимояси сифатида характерланади. Ходимлар, бизнес жараёнлари ва технологиялари киберҳужумлардан самарали ҳимояни таъминлаш учун бир-бирини тўлдириши лозим. Ушбу соҳада ишлайдиган ходимлар ахборот хавфсизлигининг асосий тамойилларини тушунишлари, хавфсиз паролларни танлашлари, юборилган ва қабул қилинган электрон почта хабарлари ва бириктирилган файлларга эътибор беришлари ҳамда маълумотларнинг бошқа манбаларда хавфсиз захираланишини таъминлашлари керак. Ҳар бир агентлик давом этаётган ёки муваффақиятли ҳужумларга қарши бир қатор асосий чораларни кўриши муҳим. Ишончли ҳаракатлар режаси ваколатли органлар томонидан бошқарилиши лозим.

2022 йил 15 апрель кунидаги 764-сонли киберхавфсизлик тўғрисида Ўзбекистон Республикасининг Қонуни, “Ўзбекистон Республикаси Давлат хавфсизлик хизмати киберхавфсизлик соҳасидаги ваколатли давлат органидир (бундан буён матнда ваколатли давлат органи деб юритилади).

Ваколатли давлат органининг киберхавфсизлик соҳасидаги ваколатлари жумласига қуйидагилар киради:

киберхавфсизлик соҳасидаги норматив-ҳуқуқий ҳужжатларни ва давлат дастурларини ишлаб чиқиш;
киберхавфсизлик тўғрисидаги қонунчилик ҳужжатларининг ижро этилиши устидан назоратни амалга ошириш;
киберхавфсизлик ҳодисалари юзасидан тезкор-қидирув тадбирларини, терговга қадар текширувларни ва тергов ҳаракатларини амалга ошириш;
киберхавфсизлик ҳодисаларининг олдини олиш, уларни аниқлаш ва бартараф этиш ҳамда уларга нисбатан тегишли чора-тадбирларни, шу жумладан уларнинг оқибатларини тугатиш бўйича ташкилий-техник чора-тадбирларни кўриш;
фавқулодда вазиятларда ахборот тизимлари ва ресурсларини киберҳимоя қилиш ҳамда киберхавфсизлик соҳасидаги бошқа масалалар бўйича чора-тадбирларни ўз ичига олган режаларни ишлаб чиқиш;
киберхавфсизликни таъминлашга доир ишларни, шунингдек муҳим ахборот инфратузилмаси объектларида киберҳужумларнинг олдини олишга, уларни аниқлашга ва уларнинг оқибатларини тугатишга доир ишларни ташкил этиш;
киберхавфсизлик талабларига мувофиқ ахборот тизимлари ва ресурсларидаги аппарат, аппарат-дастурий ҳамда дастурий воситаларни сертификатлаштиришга доир ишларни ташкил этиш;
киберхавфсизлик соҳасида тадқиқотлар ўтказилишини ва мониторингни ташкил этиш;
муҳим ахборот инфратузилмаси объектларининг ягона реестрини шакллантириш, шунингдек ушбу реестрнинг юритилишини ташкил этиш ва таъминлаш;
киберхавфсизлик субъектлари томонидан тақдим этилган маълумотлар асосида объектларни муҳим ахборот инфратузилмаси объектларининг ягона реестрига киритиш тўғрисида қарор қабул қилиш;
муҳим ахборот инфратузилмаси объектларининг киберхавфсизлигини таъминлашга доир талабларни белгилаш;
ахборотлаштириш объектларини ва муҳим ахборот инфратузилмаси объектларини киберхавфсизлик талабларига мувофиқ аттестациядан ўтказиш тартибини белгилаш;
ахборотни криптографик ҳимоя қилиш воситаларини ишлаб чиқишга, ишлаб чиқаришга ва реализация қилишга доир фаолиятни лицензиялаш;
ахборот тизимларидан ҳамда ресурсларидан фойдаланувчиларнинг ҳуқуқлари ва қонуний манфаатларини ҳимоя қилиш чораларини кўриш;
киберхавфсизлик субъектларининг ахборот тизимларини ва ресурсларини ўрганиш ва текширишни, шунингдек муҳим ахборот инфратузилмаси объектларида ўрганишлар ва текширишларни амалга ошириш;
муҳим ахборот инфратузилмаси объектларига бўлган киберҳужумларга уринишларнинг олдини олишга доир режаларни ишлаб чиқиш ва уларни бевосита амалга ошириш;
киберхавфсизлик бўлинмаларининг, мустақил экспертлар хизматлари ва гуруҳларининг фаолиятини тартибга солиш, кибертаҳдидларга қарши курашиш соҳасида ҳуқуқни муҳофаза қилувчи органлар билан ҳамкорлик қилиш;
давлат ва хўжалик бошқаруви органларини, маҳаллий давлат ҳокимияти органларини ахборот тизимлари ҳамда ресурсларида аниқланган заифликлар, кибертаҳдидлар, киберҳужумлар ва бошқа бузғунчи хатти-ҳаракатлар тўғрисида хабардор қилиш;

ҳуқуқни муҳофаза қилувчи органларни ва муҳим ахборот инфратузилмаси субъектларини муҳим ахборот инфратузилмаси объектларида киберхавфсизлик ҳодисаларини биргаликда текширишга жалб этиш;

киберхавфсизлик соҳасида халқаро ҳамкорликни амалга ошириш ва кибертаҳдидларга қарши курашиш бўйича умумий ёндашувларни ишлаб чиқиш, кибержиноятчилик бўйича тергов ҳаракатларини олиб бориш ҳамда кибержиноятчиликнинг олдини олиш борасидаги саъй-ҳаракатларни бирлаштириш, шунингдек Ўзбекистон Республикасининг кибермаконидан террорчилик, экстремистик ва бошқа қонунга хилоф фаолиятда фойдаланилишига йўл қўймаслик чораларини кўриш;

муҳим ахборот инфратузилмаси объектларида киберҳужумларни аниқлаш, уларнинг олдини олиш ва оқибатларини бартараф этиш воситаларини жорий этишга доир ишларни ташкил қилиш, шунингдек киберхавфсизлик ҳодисаларига нисбатан чоралар кўриш;

муҳим ахборот инфратузилмаси объектларидаги мавжуд заифликлар ва эҳтимолдаги таҳдидлар тўғрисидаги маълумотларни аниқлашга, тўплашга ва таҳлил қилишга доир ишларни ташкил этиш;

ахборот тизимлари ва ресурсларида киберхавфсизликнинг таъминланганлик даражаси бўйича таснифлагич яратиш;

киберхавфсизлик объектларини киберхавфсизликни таъминлаш даражасига кўра таснифлаш;

киберхавфсизлик соҳасида кадрлар тайёрлаш бўйича фаолиятни амалга ошириш;

киберхавфсизлик талабларига мувофиқлик юзасидан экспертиза ўтказиш механизмларини белгилаш;

киберхавфсизлик ва муҳим ахборот инфратузилмаси объектларининг киберхавфсизлигини амалга оширишни баҳолаш усулларини белгилаш ва баҳолаш;

муҳим ахборот инфратузилмаси объектларини тоифалаштириш мезонларини белгилаш ва тоифалаштириш;

киберхавфсизлик субъектларининг киберхавфсизлигини таъминлашга жалб этилган ходимларни қонунчиликда белгиланган тартибда аттестациядан ўтказиш.

Ваколатли давлат органининг қонуний талабларини (кўрсатмаларини) бажариш мажбурийдир”[5].

Ушбу комплекс чора-тадбирлар ҳужумларни аниқлаш, тизимларни ҳимоя қилиш, таҳдидларни аниқлаш, уларни йўқ қилиш ва ҳужумлардан кейин қобилиятларни тиклашни тушунтириши долзарб масалалардан ҳисобланади. Шу боисдан ҳам О.Ғ.Давлатов “Ахборот хавфсизлигини таъминлаш, энг аввало, турли ахборот манбаларидаги маълумотларни таҳлил этиш, баҳолаш ва зарарли ахборотларни аниқлаш, талабаларни зарарли ахборотлар таҳдидидан ўз-ўзини ва жамият аъзоларини ҳимоя қилиш, уларга қарши курашишга тайёрлашни талаб этади” деб таъкидлайди[1,Б-24].

Технология ташкилотлар ва индивидуал фойдаланувчиларни киберҳужумлардан ҳимоя қилиш учун зарур воситалар билан таъминлашнинг муҳим элементидир. Ҳимоя қилиниши керак бўлган асосий компонентларга компьютерлар ва ақлли қурилмалар, роутерлар ва модемлар, тармоқ ва булутли муҳит киради. Ушбу компонентларни ҳимоя

қилиш учун ишлатиладиган энг кенг тарқалган технологияларга янги авлод хавфсизлик деворларидан фойдаланиш, DNS фильтрлаш[6], зарарли дастурлардан ҳимоя қилиш, вирусга қарши дастурларни юклаб олиш ва электрон почтани ҳимоя қилиш киради. Бугунги кунда бутун дунё бўйлаб илғор киберҳимоя дастурлари ҳар бир фойдаланувчининг манфаатларини ҳимоя қилади. Индивидуал даражада кибермудофаа ҳужуми шахсий маълумотларнинг ўғирланишига, маблағлар ёки оилавий фотосуратлар каби қимматли маълумотларнинг йўқолишига, давлат ва ҳарбий сирларнинг кенг миқёсда тарқалишига олиб келиши мумкин. Электр станциялари, шифохоналар, молия сектори, банк сектори ва бошқа институтлар каби барча муҳим инфратузилмаларни ҳимоя қилиш жамиятимизнинг омон қолиши ва фаолияти учун жуда муҳимдир.

Ҳар бир тармоқ фойдаланувчиси кибертаҳдидларни ўрганишдан фойда кўради, масалан, 250 кишидан иборат кибермутахассислар жамоаси киберҳужум стратегиялари, янги ва пайдо бўлаётган таҳдидлар ҳақида билиб олади. Улар янги заифликлар ва заифликларни аниқлайди, жамоатчиликни киберхавфсизликнинг аҳамияти ҳақида хабардор қилади ва очиқ кодли дастурий таъминот орқали тизимларнинг ишончлилигини оширади. Давлат хавфсизлик хизмати киберхавфсизлик бўйича соҳа вакилларининг иши ҳар бир фойдаланувчи учун Интернетни хавфсизроқ қилишдир. Масалан, З.Давронов фикрича, «ахборот теварак-атрофдаги турли хил манбалардан тўпланган омиллар бўлиб, бу билимларнинг қайта изҳор қилиш»дир[7].

Ахборот-коммуникация технологияларининг жадал ривожланиши кибержиноятларнинг пайдо бўлиши ва ўсишига олиб келди. Бирлашган Миллатлар Ташкилотининг ҳисоб-китобларига кўра, ҳар йили 2,5 миллиондан ортиқ одам кибержиноят қурбони бўлади ва кибержиноятларнинг умумий зарари 1 миллиард доллардан ошади[8]. Кибержиноятларнинг ўсиши бутун дунё бўйлаб давлат бошқаруви, банк, транспорт, миллий хавфсизлик ва бошқа тизимларни такомиллаштириш кибермудофаа чораларини кенгайтиришни долзарб қилади. 2012-йилда Чикагода бўлиб ўтган НАТО саммитида қабул қилинган якуний декларацияда яна бир бор алянсга аъзо давлатлар, шунингдек, халқаро ташкилотлар (БМТ, Европа Иттифоқи, Европа Кенгаши ва бошқалар) билан киберҳужумлар сони ва сифати ошганлиги қайд этилган.

Ягона кибермудофаани биргаликда ташкил этиш муҳимлиги таъкидланди. АҚШ, Россия, Хитой, Буюк Британия, Франция, Германия ва бошқа бир қатор ривожланган давлатлар аллақачон ўзларининг кибер кучларини яратишган. Гарчи, бу давлатлар ўзларининг асосий мақсади тармоқларини ҳимоя қилиш эканини айтишса-да, ҳужумкор операцияларни ҳам ўтказишни режалаштирмоқда. Кўп йиллар давомида Қўшма Штатлар ва Россия амалдаги президентларга, ҳатто уларнинг энг яқин иттифоқчиларига қарши кенг кўламли электрон жосуслик амалиётларини амалга оширгани ҳақида кўп хабарлар тарқалган. АҚШ ва Мексикада бўлиб ўтган сайловлар глобал ахборот тармоғи бўлган Интернетни глобал кураш майдонига айлантирди[9].

Дунё армияларининг кўпчилиги аллақачон киберҳужумларга амалий жанговар тайёргарликни жанговар тайёргарлик дастурларига киритмоқда. 2008 йилда ташкил этилган НАТО Cyberthreat Experience Center томонидан ташкил этилган тренинглар давомида иштирокчилар ҳатто “ҳаракатланувчи тезюрар поездни тўхтатишга ҳаракат қилишди”. Тренингда қатнашган хакерлар гуруҳи муваффақиятга

эришди: улар поездни тўхтатиб, бошқарув тизимини бузиб, двигателни блокировка қилишга муваффақ бўлишди. Ушбу тренингларда иштирок этувчи хакерлар фақат таклифнома билан келади[10].

Кибермaневрларнинг “сезгир табиати” туфайли ташриф буюрувчиларнинг исм-шарифлари ва рақамлари сир сақланмоқда. Фақатгина “тўқнашув” нинг умумий мақсади маълум: душман тармоғини харитага тушириш, нозик нуқтани топиш ва у ердан тармоққа кириб бориш орқали уни назорат қилиш. Аввалроқ худди шундай машқда АҚШ ва Британия хакерлари бир-бирининг ахборот тизимларига “ҳужум” қилган эди. Собиқ президент Барак Обама ва собиқ бош вазир Девид Кемерон томонидан юқори даражада маъқулланган кибермaневрлар қанчалик муҳим эканидан далолат беради. Ушбу турдаги икки томонлама ёки кўп томонлама тренингнинг турли тегишли идоралар томонидан биргаликда амалга оширилиши киберхавфсизлик бўйича юқори малакали мутахассисларни тайёрлаш ва уларнинг малакасини реал баҳолашда алоҳида рол ўйнаши мумкин.

Хакерлик ҳужумлари - кибержиноят компьютерлар ва смартфонлар учун ҳақиқий таҳдиддир. Хакерлар нафақат компьютерлар, балки смартфонлар ҳам ҳужумга учрамоқда. Ва ниҳоят, одамларнинг шахсий ҳаёти. Ижтимоий тармоқлар кенг тарқалган бир пайтда одамларнинг шахсий ҳаётига ўрин йўқ, уларнинг шахсий маълумотлари кенгроқ веб-сайтларга йўл топади. Шу боисдан ҳам А.К.Расулев таъкидлаганидек, бугунги кунда “Интернет тармоғи фойдаланувчиларининг аксарияти ёшлар эканлигини инобатга олиб, ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятлар учун жиноий жавобгарлик масаласи долзарб ҳисобланади. Ўзбекистон Республикаси ЖКда субъект ёши 13 дан 18 ёшгача бўлиб, умумий субъект ёши 16 ёш белгиланган. Англияда 8, Грецияда 13, Швецияда 15, Финляндияда 16, Миср, Ливан, Ироқ ва АҚШда 7, Исроилда 9, Эрон, Туркияда 11 ёшдан жиноий жавобгарликка тортилиши мумкин”[11, Б-24].

Қуролли можаролар ва ҳарбий стратегияларда ахборот технологияларининг сиёсий ролини ўрганишнинг қуйидаги асосий жиҳатларини ажратиб кўрсатиш зарур. Агар “ахборот технологиялари”ни соф техник маънода (“компьютер технологияси” сифатида) кўриб чиқсак, бу ерда янгилик шубҳасиздир. Аммо, биринчидан, уларнинг сиёсатга таъсирини баҳолаш кўпинча бўрттирилади, чунки компьютер технологиялари соф техник маънода ўз-ўзидан сиёсатни ҳам, халқаро муносабатлар тизимини ҳам тубдан ўзгартирмайди ва агар сиёсатнинг бундай тубдан ўзгариши содир бўлса, унда компьютер технологиясининг роли минималдир. Иккинчидан, компьютер технологияларининг ҳарбий-сиёсий соҳага таъсири бошқа янги, аммо компьютер технологияларининг таъсиридан унчалик фарқ қилмайди. Ва янги ядро технологиялари, компьютер техникасига асосланган юқори аниқликдаги қуроллар эса душман инфратузилмасини жисмоний йўқ қилишга қаратилган бўлиб, шу маънода уларнинг бу ерда таъсири бир хил (ҳаракат кучи жиҳатидан эмас, балки моҳиятан). Шундай қилиб, ядро қуроли бир вақтнинг ўзида ахборот қуроли бўлиши мумкин (душман қуролли кучларининг ахборот ва алоқа тизимларини йўқ қиладиган кучли электромагнит импулснинг генератори сифатида).

**Хулоса ва таклифлар (Conclusion/Recommendations).** Ахборотнинг шахс ва жамиятга таъсири билан боғлиқ бўлган ҳарбий-сиёсий соҳанинг ахборот-психологик томонида бошқача вазиятни кўриш мумкин. Бу ерда психологик соҳага таъсир қилиш Цун Цзи давридан бери ўз моҳиятини деярли ўзгартирмаган тарғибот, дезинформация, онгни манипуляция қилиш усуллари ёрдамида амалга оширилади. Кўриниб турибдики, ўзига хос таъсир ва жисмонийдан ташқарида идеал доирага ўтиш. Бироқ, фундаментал янгилик ҳақида гапириш қийин, чунки бу усулларнинг ўзи инқилобий эмас, балки эволюцион тарзда такомиллаштирилган. Янгилик ахборотга таъсир қилишнинг эски усулларидан фойдаланишда, лекин янги воситалар (биринчи навбатда Интернет) ёрдамида. Агар таъсир даражаси ва қуролли тўқнашувларда фойдаланиш эҳтимоли бўйича ахборот-психологик ва техник жиҳатларни солиштирсак, муҳимлик ва янгилик уйғунлигини қуролли тўқнашувлардаги ахборот инқилоби натижасида юзага келган ташкил этиш ва бошқаришнинг тармоқ шаклларини ўрганишда топиш мумкин. Бу ахборот асридаги қуролли можароларнинг ҳарбий-техник, ташкилий-маъмурий ва ахборот-психологик жиҳатларини комплексда кўриб чиқиш заруратини туғдиради.

## ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. Давлатов О.Ғ. Талабаларда ахборот хавфсизлигини таъминлаш компетентлигини тарихий маданий мерос воситасида ривожлантириш. Педагогика фанлари бўйича фалсафа доктори (PhD) диссертацияси автореферати. –Тошкент, 2018.;
2. Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях: политические аспекты: диссертация ... кандидата политических наук. - Санкт-Петербург, 2011. - 219 с.;
3. https://www.anti-malware.ru/analytics/Threats_Analysis/a-look-at-2017-most dangerous-ransomware-attacks.;
4. Расулев А.К. Ахборот технологиялари ва хавфсизлиги соҳасидаги жиноятларга қарши курашишнинг жиноят-ҳуқуқий ва криминологик чораларини такомиллаштириш. Докторлик (DSc) диссертацияси автореферати. –Тошкент, 2018. –Б.23-24.;
5. Қонунчилик маълумотлари миллий базаси, 16.04.2022 й., 03/22/764/0313-сон.;
6. ДНС-фильтрлаш Интернетнинг домен ўлчамлари сатҳида содир бўлади ва беҳаё ёки зарарли веб-сайтнинг ИП-манзилини топишга имкон бермайди. Бундай ишларни амалга оширадиган бир нечта пуллик маҳсулотлар мавжуд, аммо кўплаб мактаблар хавфсиз бўлмаган сайтларни филтрлаш учун бепул эчимлардан фойдаланмоқдалар.;
7. Давронов З. Илмий ижод методологияси. Т.: Иқтисод-молия, 2007. 180 б.;
8. https://www.cbs.nl/en-gb/news/2022/09/nearly-2-5-million-people-victims-of-cybercrime-in-2021.;
9. https://en.wikipedia.org/wiki/Cyber_force#:~:text=A%20cyber%20force%20is%20a,branch%20or%20a%20combined%20command.;
10. https://www.nato.int/docu/update/2008/05-may/e0514a.html.