ЗАМОНАВИЙ ДУНЁДА ГЛОБАЛ ТАҲДИД ВА КИБЕРХАВФСИЗЛИК МУАММОСИ

Батиров Фарход Авазович
Ўзбекистон Республикаси Жамоат хавфсизлиги
Университети Ўқув-услубий бошқармаси, ўқув жараёнини
Режалаштириш бўлими бошлиғи доцент
E-mail: Farxod-batirov@mail.ru

АННОТАЦИЯ

Мазкур мақола замонавий дунёда глобал таҳдид ва киберхавфсизлик муаммоси ҳарбий-сиёсий фанлар контекстида атрофлича ўрганилган. Шунингдек, унда киберхавфсизлик, компьютер хавфсизлиги, транзакция хавфсизлиги, маълумотлар ҳимояси, шахсий маълумотлар хавфсизлиги, интернет тармоғи хавфсизлиги ва ҳаттоки ҳар қандай сигнал узатувчи қурилмалар хавфсизлиги тушунчалари мазмунига аниқлик киритилган. Мақолада муаллиф глобал таҳдидлар контекстида дунёдаги киберхавфсизликнинг замонавий муаммолари, дунёдаги кибермакон ва интернетдаги глобал таҳдидлар элементларини ҳар томонлама ўрганиш бўйича ўз қарашларини таклиф этган ҳамда кибертаҳдидларга қарши курашишнинг энг самарали механизмларини ишлаб чиқиш ва жорий этиш муҳимлигини илмий-амалий жиҳатдан асослаган. Муаллиф кибержиноятлар, кибермакондаги ҳуқуқбузарликлар, компьютер тармоқларини бузиш, зарарли дастурлар ва вируслар тарқалишининг асосий сабабларини ўрганиш, уларнинг таъсирини минималлаштириш бўйича тегишли механизмлар ва давлат сиёсатини янада ривожлантириш муҳим деб ҳисоблайди. Кибержиноятларга қарши курашиш бўйича профилактик ва шошилинч чора-тадбирларни таъминлаш учун кибердавлатлар ўртасида халқаро ҳамкорлик ва ўзаро ҳамкорликни кенгайтириш зарурлиги алоҳида қайд этади. Шунингдек, мақолада муаллиф ҳарбий-сиёсий фанлар контекстида кибержиноятчилар, хакерлар ва кибербузғунчиларга қарши курашишнинг халқаро механизмлари ва мезонларини янгилаш зарурлигини асослайди.

Калит сўзлар: Киберхавфсизлик, киберхавфсизлик тизимини ҳимоя қилиш, киберкосмик тизимнинг ишончлилиги, интернет тармоқ инфратузилмаларининг самарадорлиги, кибержосуслик, ахборот урушлари.

ГЛОБАЛЬНАЯ УГРОЗА И ПРОБЛЕМА КИБЕРБЕЗОПАСНОСТИ В СОВРЕМЕННОМ МИРЕ

АННОТАЦИЯ

Данная статья представляет собой подробное исследование глобальной угрозы и проблемы кибербезопасности в современном мире в контексте военно-политических наук. Он также разъясняет понятия кибербезопасности, компьютерной безопасности, безопасности транзакций, защиты данных, безопасности личных данных, безопасности интернет-сети и даже безопасности любых сигнальных устройств. В статье автор предложил свой взгляд на современные проблемы кибербезопасности в мире в контексте глобальных угроз, комплексного изучения элементов киберпространства и глобальных угроз в сети Интернет, научно и практически обосновал важность разработки внедрение наиболее эффективных механизмов борьбы с киберугрозами. Автор считает важным изучение основных причин распространения киберпреступлений, преступлений в киберпространстве, взломов компьютерных сетей, вредоносных программ и вирусов, а также дальнейшую разработку соответствующих механизмов и государственной политики для минимизации их воздействия. Особо отмечается необходимость расширения международного сотрудничества и взаимного сотрудничества кибергосударств для обеспечения превентивных и неотложных мер по борьбе с киберпреступностью. Также в статье автор обосновывает необходимость обновления международных механизмов и критериев борьбы с киберпреступниками, хакерами и кибервандалами в контексте военной и политической науки.

Ключевые слова. Кибербезопасность, защита системы кибербезопасности, надёжность системы киберпространства, эффективность инфраструктур и интернет-сети, кибершпионаж, информационные войны.

GLOBAL THREAT AND CYBER SECURITY PROBLEM IN THE MODERN WORLD

ABSTRACT

This article is a detailed study of the global threat and the problem of cybersecurity in the modern world in the context of military-political sciences. It also explains the concepts of cyber security, computer security, transaction security, data security, identity security, internet network security, and even the security of any signaling devices. In the article, the author offered his own view on the modern problems of cybersecurity in the world in the context of global threats, a comprehensive study of

the elements of cyberspace and global threats on the Internet, scientifically and practically substantiated the importance of developing the introduction of the most effective mechanisms to combat cyberthreats. The author considers it important to study the main causes of the spread of cybercrimes, crimes in cyberspace, computer network hacks, malware and viruses, as well as the further development of appropriate mechanisms and state policies to minimize their impact. Particularly noted is the need to expand international cooperation and mutual cooperation between cyber states to ensure preventive and urgent measures to combat cybercrime. Also in the article, the author substantiates the need to update international mechanisms and criteria for combating cybercriminals, hackers and cyber vandals in the context of military and political science.

Keywords. Cyber security, protection of the cyber security system, reliability of the cyberspace system, efficiency of infrastructures and the Internet, cyber espionage, information wars.

Ҳозирги замонда инсонпарварлик мафкураси ҳам ўзгарди. Зеро, 18-асрдан бошлаб, яъни маърифатпарварлик даврининг 200 йил давомида сиёсатнинг бош ғояси, ҳаракатлантирувчи кучи адолатли ижтимоий тузилма орқали инсоният нажот топади, деган ишонч эди. У турли шаклларга эга бўлиб, дастлаб Бисмарк давридаги Германияда, кейинроқ Англия, АҚШ ва бошқа мамлакатларда социализм, коммунизм, фашизм ёки «умумий фаровонлик жамияти” ғоялари каби турли сиёсий ҳаракатларни юзага келтирди. Уларнинг орасидаги тафовутларга қарамай, бу оқимларни бирлаштирган мукаммал жамият яратиш имконияти мавжуд эди. Қайд этилган оқимлар вакиллари комил жамиятнинг яратилиши алоҳида олинган шахснинг камолотига олиб келади, деб ҳисоблаганлар.

20-асрнинг бошларида бу мақсадларга эришиш осон деб ҳисобланган. Ўша даврдаги кўпчилик моддий бойлик одамларни озиқ-овқат ва кийим-кечак билан таъминлашдир, деб ўйларди. Аммо аста-секин ҳаёт янада мураккаб эканлигини англаб етди. Маълумки, фаровонлик ошгани сайин одамларнинг эҳтиёжлари ҳам ортиб боради. Постиндустриал жамият назарияси асосчилари ҳақли равишда З.Бжезински, Д.Белл ҳисобланади. Э. Тоффлер ҳисобга олинади. Биринчи марта айнан ана шу олимлар янги типдаги жамиятни “ахборот” ва “ахборот технологиялари” тушунчалари билан бевосита боғладилар[13]. 2021 йил январ ойи ҳолатига кўра, дунёда 4,6 миллиард фаол интернет фойдаланувчиси бор. Келгуси йилга келиб

[13] Алгулиев Р., Салманова П. Информационное общество. Интересные хронологические факты Баку Информационные технологии 2014. – 169 с.

интернетга тахминан 28,5 миллиард қурилма уланади, бу 2017 йилга нисбатан 18 миллиардга кўп. Муаммонинг кўлами халқаро ҳамжамиятдан адекват жавоб беришни талаб қилади. Бугунги кунда рақамли технологиялар ҳуқуқ, ахлоқ, ядро қуролини тарқатмаслик, шунингдек, халқаро барқарорлик соҳасидаги қабул қилинган меъёрларнинг "кучлилигини синовдан ўтказмоқда"[14].

Мамлакатимизда кибертаҳдид ва хатарлардан ҳимояланиш борасида қандай чора-тадбирлар амалга оширилмоқда? Барча мамлакатларда бўлгани каби Ўзбекистонда ҳам киберхавфсизликка давлат даражасида алоҳида эътибор қаратилмоқда. Таъкидлаш жоизки, Ўзбекистон Республикаси Президентининг 2017 йил 30 июндаги "Республикада ахборот технологиялари соҳасини ривожлантириш учун шарт-шароитларни тубдан яхшилаш чора-тадбирлари тўғрисида"ги пф-5099-сон фармони[15] ва Ўзбекистон Республикаси Вазирлар Маҳкамасининг 2012 йил 19 декабрдаги "Ахборот-коммуникация технологияларини ривожлантириш жамғармасини янада ривожлантириш ва унинг маблағларидан самарали фойдаланиш тўғрисида"ги 356-сон қарори[16], шунингдек, 2020–2023 йилларга мўлжалланган киберхавфсизликка доир миллий стратегия ва "Киберхавфсизлик тўғрисида"ги қонунда[17] белгиланган вазифалардан келиб чиқадиган масалаларни ҳал этиш бўйича ишлар давом эттирилмоқда. Қайд этилган ҳужжатларда хусусий ва бошқа муассасаларни киберхавфсизлик соҳасида ўқитиш ва ахборот хавфсизлиги маданиятини шакллантириш, ахборот жараёнларини ҳимоя қилиш, киберхавфсизликни кучайтириш йўналишида тегишли техник ва услубий воситаларни яратиш, ахборот ресурслари ва тизимларини эҳтимолий таҳдидлардан ҳимоя қилиш, киберхавфсизлик соҳасида умуммиллий тайёргарликни ошириш ва ҳ.к. ана шундай асосий мақсадлар белгиланган.

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

[14] https://news.un.org/ru/story/2021/06/1405532
[15] Қонунчилик маълумотлари миллий базаси, 24.07.2021 й., 06/21/6268/0700-сон.
[16] Қонун ҳужжатлари маълумотлари миллий базаси, 24.05.2018 й., 09/18/380/1262-сон, 11.10.2018 й., 09/18/817/2033-сон
[17] Қонунчилик маълумотлари миллий базаси, 16.04.2022 й., 03/22/764/0313-сон

институтлар ва операцион компаниялар ўртасидаги ҳамкорликни мустаҳкамлаш ва уларнинг самарадорлигини оширишдан тобора долзарб аҳамият касб этмоқда.

Киберхавфсизлик одатда компьютер хавфсизлиги, транзаксия хавфсизлиги, маълумотлар ҳимояси, шахсий маълумотлар хавфсизлиги, интернет тармоғи хавфсизлиги ва ҳаттоки ҳар қандай сигнал узатувчи қурилмалар хавфсизлигини ўз ичига олади. Ушбу мавзуларнинг кенг тарқалиши ва муҳим аҳамият касб этиши сабаби киберҳужумлар ва таҳдидлардир. Киберҳужумлар сони ва тури ошгани сайин киберхавфсизлик тармоқлари ҳам ошиб бормоқда. 1980-йиллардан бошлаб “Кибер жиноятчилар”, “Кибер дунёда этика”, “Ахлоқий кибер қароқчилик” каби тушунчалар пайдо бўлди. Киберҳужум турлари орасида пул ювиш ва кибержиноятчиларнинг ўз маҳоратини намойиш қилиш учун қилинган ҳужумлари алоҳида ўрин тутади. Киберхавфсизлик киберҳужумларнинг сезиларли даражада ошиши туфайли давлатлар ва компаниялар учун жуда муҳим бўлиб қолди.

Киберхавфсизлик - бу компьютерлар, серверлар, веб-сайтлар , мобил қурилмалар, электрон тизимлар, тармоқлар ва маълумотларни зарарли ҳужумлардан ҳимоя қилиш амалиётидир. Киберхавфсизлик - бу тизимлар, тармоқлар ва дастурий таъминотни рақамли ҳужумлардан ҳимоя қилиш бўйича чора-тадбирларни амалга оширишдир. Бундай ҳужумлар одатда махфий маълумотларга кириш, уни ўзгартириш, йўқ қилиш, фойдаланувчилардан маблағ олиш, ташкилотлар ёки компанияларнинг нормал фаолиятини бузиш мақсадида амалга оширилади. Киберхавфсизлик бўйича самарали чора-тадбирларни амалга ошириш аллақачон жуда қийин жараён. Чунки бугунги кунда ҳужумлар амалга оширилаётган қурилмалар сони одамлар сонидан бир неча баробар кўп ва кибержиноятчилар ҳар куни янги ихтиролардан фойдаланмоқда.

Кибержиноятларнинг кўпайиши давлат бошқаруви, банк, транспорт, миллий хавфсизлик ва бошқа тизимларни такомиллаштириш ва бутун дунё бўйлаб кибермудофаа чораларини кенгайтиришни долзарб қилади. Киберхавфсизлик энг кенг кўламли, глобал ва деярли бутун дунё бўйлаб муаммолардан биридир. Афсуски, самарали киберхавфсизлик чораларини амалга ошириш аллақачон жуда қийин жараён. Чунки бугунги кунда ҳужумлар амалга оширилаётган қурилмалар сони анчагина кўп ва кибержиноятчилар ҳар куни янги ихтиролардан фойдаланмоқда. Кибертаҳдидлар ва киберҳужумлар биз яшаётган ахборот технологиялари асрининг энг катта муаммоларидан бири десак, хато қилмаган бўламиз. Тизимлар, тармоқлар ва дастурий таъминотни рақамли ҳужумлардан ҳимоя қилиш учун киберхавфсизлик чораларини кўриш керак. Ҳозирги замонда кибер жиноятлар сони ортиб бормоқда. Муваффақиятли киберхавфсизлик ёндашуви ҳимоя қилиш учун муҳим бўлган компьютерлар,

тармоқлар, дастурлар ёки маълумотларнинг кўп қатламли ҳимояси сифатида аниқланади.

Бугунги кунда бутун дунё бўйлаб кенг тарқалган хакерлик тармоқлари молиявий операцияларни амалга оширади, фуқароларнинг шахсий маълумотларига киришга эришади, давлат органларининг расмий рақамларини босим остида ушлаб туради. Сўнгги пайтларда баъзи штатлар сайлов тизимига кириш имконига эга бўлгани ҳақида маълумотлар тарқалмоқда. бу соҳада ташвиқот яратишга уринишлар мавжуд ва шу билан манипуляция имкониятлари кенгаяди. Хакерлар ҳар қандай тизим структурасида тизим хатоларини ёки тизим тешикларини топадилар, улар бу очилиш сабабларини билишади. Афсуски, бир қатор компьютер фойдаланувчилари билимсизлик ва эҳтиёцизлик оқибатида моддий ва маънавий зарар кўрмоқда. Ушбу зарарлардан қочиш учун сиз баъзи асосий мавзуларни билишингиз ва баъзи хавфсизлик чораларини кўришингиз керак.

Киберхавфсизлик бўйича самарали чора-тадбирларни амалга ошириш бугунги кунда жуда қийин, чунки бугунги кунда одамлар кўпроқ қурилмаларга эга бўлишига қарамай, кибержиноятчилар тобора кўпроқ “ихтирочи” ролини ўйнамоқда[18]. Шунингдек, бир қатор компьютер фойдаланувчилари билимсизлик ва эҳтиёцизлик оқибатида моддий ва маънавий зарар кўрмоқда. Ушбу зарарлардан қочиш учун сиз баъзи асосий мавзуларни билишингиз ва баъзи хавфсизлик чораларини кўришингиз керак.

Ходимлар, бизнес жараёнлари ва технологиялари киберҳужумлардан самарали ҳимояланиш учун бир-бирини тўлдириши керак. Ушбу соҳа ходимлари ахборот хавфсизлигининг асосий тамойилларини тушунишлари, кучли паролларни танлашлари, юборилган ва қабул қилинган электрон почта ва унга бириктирилган файлларга эътибор беришлари ва маълумотларнинг бошқа манбаларга хавфсиз захираланишини таъминлашлари керак. Ҳар бир ташкилот давом этаётган ёки муваффақиятли ҳужумларга қарши бир қатор асосий чораларни кўриши керак. Ишончли ҳаракатлар режаси ягона марказдан бошқарилиши керак. Ушбу кенг қамровли чора-тадбирлар ҳужумларни қандай аниқлаш, тизимларни ҳимоя қилиш, таҳдидларни аниқлаш, уларни йўқ қилиш ва ҳужумлардан кейин операцияларни тиклашни тушунтириши керак.

Реал ҳаётда бўлгани каби виртуал дунёда ҳам хавфсизлик муҳим аҳамиятга эга. Дунёда ҳар дақиқада киберкосмосда 500 миллион ҳужум уюштирилади. Киберхавфсизлик стратегиясини тайёрлаган Ўзбекистон ҳам албатта, бу хавф ва хатарлардан хабардор ва бу стратегиядан келиб чиқадиган қоидаларнинг амалга

[18] Курилкин А.В. Информационные и кибернетические операции как инструмент реализации внешней политики : формы, методы, технологии : диссертация ... кандидата политических наук. - Москва, 2021. - 207 с.

оширилиши уларнинг олдини олишда муҳим рол ўйнайди. Ўтган даврда Ўзбекистон ҳам киберхавфсизлик индексини яхшилаган. Global Cybersecurity Index давлатларнинг киберхавфсизлик бўйича рейтингини эълон қилди. Ўзбекистон унда 182 давлат орасида 70-ўринни эгаллади. Индекс бешта асосий йўналишда 82 та саволни жамлаган. Уларнинг ҳар бирига 20 балл берилади. Бунда ҳуқуқий, техник ва ташкилий ҳамда имкониятлар ва ҳамкорликни ривожлантириш бўйича чораларни ўз ичига олади.

Ахборот-коммуникация технологияларининг жадал ривожланиши кибержиноятларнинг пайдо бўлишига ва унинг кундан-кунга ортиб боришига олиб келди. Бирлашган Миллатлар Ташкилоти ҳисоботида айтилишича, ҳар йили 1,5 миллиондан ортиқ одам кибержиноят қурбони бўлади ва кибержиноятларнинг умумий қиймати 1 миллиард доллардан ошади[19]. Бугунги кунда миллий иқтисодиёт ва одамларнинг турмуш тарзи билан боғлиқ бўлган турли хил алоқа, энергетика, транспорт ва бошқа саноат тармоқлари ўз фаолиятини таъминлаш учун компьютер тизимларига таянади ва фуқаролик компьютер тизимлари Интернетга жуда боғлиқ бўлганлиги сабабли, кенг кўламли режалаштирилган тармоқ ҳужумлари кенг қамровли бўлиши мумкин. Чунки бу хужумлар мамлакатнинг нормал иқтисодий фаолиятини фалаж қилади. Бу 20- асрдаги анъанавий электрон ушлаш ва 21- асрдаги кибер уруш ўртасидаги фарқни кўрсатади, чунки у Интернет пассив электрон ушлаш бўлимларига киберҳужумларни амалга ошириш имкониятини беради.

Кибержиноятларнинг кўпайиши давлат бошқаруви, банк, транспорт, миллий хавфсизлик ва бошқа тизимларни такомиллаштириш ва бутун дунё бўйлаб кибермудофаа чораларини кенгайтиришни долзарб қилади. 2012-йилда АҚШнинг Чикаго шаҳрида бўлиб ўтган НАТО саммитида қабул қилинган якуний маъқуллашда киберҳужумлар сони ва сифати ошиши фактлари яна бир бор тилга олинди ва алянсга аъзо давлатлар алоҳида, шунингдек, халқаро ташкилотлар билан (БМТ, Европа Иттифоқи, Европа Кенгаши ва бошқалар) ягона кибермудофаа ташкил этиш муҳимлиги таъкидланди. АҚШ, Россия, Хитой, Англия, Франция, Германия ва бошқа бир қатор ривожланган давлатлар аллақачон ўзларининг махсус киберқўшинларини яратишган. Гарчи бу давлатлар ўзларининг асосий мақсади ўз тармоқларини ҳимоя қилиш эканлигини таъкидлаган бўлсалар-да, бу эрда ҳужум операциялари ҳам кўзда тутилган.

[19] https://rus.lb.ua/economics/2012/01/27/133936_oon_provedet_globalnoe.html

Кўп йиллар давомида Америка Қўшма Штатлари ва Россия сайловолди кампанияларида амалдаги президентларга, ҳатто уларнинг энг яқин иттифоқчиларига қарши кенг кўламли электрон жосуслик амалиётларини ўтказгани ҳақида хабарлар тарқалган. Яқинда АҚШ ва Мексикада бўлиб ўтган сайловлар глобал ахборот тармоғи, Интернетни глобал жанг майдонига айлантирди.

“Harbor Networks” киберхавфсизлик компанияси маълумотларига кўра, 2019-йилда кибержиноятлар сони сўнгги 11 йилга нисбатан 60 баробар кўпдир[20]. Бу жуда жиддий рақам. Айнан шунинг учун киберхавфсизлик давлатлар, компаниялар ва жисмоний шахслар учун жуда муҳим бўлиши керак. Бундай ҳужумлар одатда махфий маълумотларни олиш, уларни ўзгартириш ва йўқ қилиш, фойдаланувчилардан пул ундириш ёки компанияларнинг нормал фаолиятини бузишга қаратилган.

20-асрнинг 60-йилларида ахборот технологияларининг ривожланиши натижасида операцион тизимларни тўлиқ билган, унинг чуқурлигига кирган, компьютерга ҳар томонлама қизиққан, дастурлашни профессионал даражада биладиган компьютер мутахассислари – хакерлар пайдо бўлди.

Қўшма Штатлар 2011 йилда эркин савдо ва ижтимоий-иқтисодий ривожланиш учун ишончли, хавфсиз ва очиқ муҳитни яратиш имконини берувчи киберхавфсизликнинг халқаро асосларини шакллантириш бўйича ҳужжат тайёрлади. Ушбу ҳужжат бир нечта асосий тамойилларни тавсифлайди. Биринчи ўрин - иқтисодий муносабатлар ҳисобланади. Шу боисдан ҳам Қўшма Штатлар шахсий маълумотларни, жумладан, тижорат сирларини ҳимоя қилиш орқали Интернет орқали эркин савдони яратишни таклиф қилмоқда. Яна бир муҳим устувор вазифа – кибермаконда халқаро ахлоқ кодексини яратиш масаласидир. Лойиҳа муаллифларининг фикрича, бундай коднинг мавжудлиги хорижлик хакерлик ҳужумларидан ҳимояланиш имконини беради. Яна бир йўналиш эса кибержиноятчиликка қарши курашга бағишланган[21].

АҚШ эътиборни муайян жиноятларга қаратишга ва интернетга киришни чекламасликка чақиради. Шунингдек, хавфсиз муҳитни яратиш имконияти бўлмаган мамлакатларга ёрдам кўрсатиш кўзда тутилган. Стратегия АҚШнинг барча йирик вазирликларини қамраб олади, уларнинг барчасига хорижий давлатлардаги ўхшаш вазирликлар иштирокида ўзаро ҳамкорлик тамойилларини яратиш вазифаси юклатилган[22].

[20] https://www.harbornetworks.com/blog/topic/mitel-support
[21] Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая : диссертация ... кандидата политических наук. - Москва, 2014. - 207 с.
[22] Виловатых А.В. Информационное противоборство в политическом процессе : тренды цифровой реальности : диссертация ... доктора политических наук. - Москва, 2021. - 347 с.

Кибер уруш икки тоифага бўлинади: кибер жосуслик ва киберҳужумлар. Кибер-жосуслик фаолияти одатда куч билан қасос олишга олиб келмайди; аммо, кибер-жосуслик фаолияти ва киберҳужум фаолияти ўртасида аниқ чегара йўқ ва доимий кибер-жосуслик фаолияти баъзан киберҳужумларга тайёргарлик босқичидир. Агар бирор давлатнинг ҳарбий разведка бошқармаси бошқа давлат интернетини йўқ қилишга ёки миллий иқтисодиёт ва халқ турмуши билан чамбарчас боғлиқ бўлган бошқа давлатларнинг ҳукумати, ҳарбий ёки хусусий корхоналарининг веб-сайтлари ва маълумотлар базаларини йўқ қилишга уринса, одатда бундай киберҳужумлар содир бўлади. Америка Қўшма Штатлари, Буюк Британия, Канада ва бошқа давлатлар кибермудофаа нуқтаи назарини ўзгартирди.Оддий кибермудофаа ўтказишдан ташқари, улар нишоннинг табиати, вазиятнинг таъсири ва самарадорлиги каби мезонларга алоҳида эътибор қаратадилар. Улар хакерлар ва кибержиноятчи ташкилотларга қарши фаол киберҳужумлар уюштирадилар.

АҚШ ҳарбийлари кибермакон ва кибероперацияларда “бурилиш нуқтасида” турибди, бу асосан қуйидаги тўрт жиҳатда акс этади: Биринчидан, киберхуружларнинг олдини олиш нуқтаи назаридан, киберхавфсизлик тизимини ҳисобга олишдан ташқари, у ҳам ходимларнинг омилларини, яъни киберҳужумларнинг олдини олишни кўриб чиқади. Рақибларга таъсир қилиш киберкосмосдаги операциялар қандай амалга оширилаётганини тарозида кўради; иккинчидан, DoDнинг кибер ҳақидаги тушунчаси ривожланмоқда, Америка Қўшма Штатларига қарши зарарли фаолиятни олдини олиш учун ахборот операциялари ва кибероперацияларни янада яқинроқ боғлайди; кенг қамровли тўхтатувчи таъсирга эришиш учун бошқа соҳаларнинг роли; Тўртинчидан, кибермакондаги вазият тез ўзгармоқда, шунинг учун АҚШ ҳарбийлари ушбу соҳада “доимий иштирок этиш” позициясини сақлаб туриши керак.

АҚШ Киберқўмондонлигининг ишчи гуруҳи 2021 йил феврал ва август ойлари орасида биринчи ҳужум кибер операцияларини ўтказди. Операция шу қадар аҳамиятли эдики, АҚШ Мудофаа вазири Лойд Остин уни шахсан кузатиб борди. Операция, шунингдек, рақамли домендаги урушнинг тез ривожланаётган табиати ва ҳужумкор кибер операцияларнинг келажакдаги аҳамиятининг яна бир белгисидир. Операция DoD ахборот тармоғи хавфсизлигини ўз ичига олган “ҳужумкор кибер-таъсир операцияси” эди, бироқ операциянинг аниқ моҳияти ва мақсадлари номаълумлигича қолмоқда. Операцияни амалга оширган ишчи гуруҳ Merilend ҳаво миллий гвардиясининг 175-кибероперация гуруҳи, Delaver ҳаво миллий гвардиясининг 166-кибероперация отряди, АҚШ ҳарбий-денгиз кучларининг 63-киберкомандоси ва АҚШ Ҳарбий ҳаво кучларининг 341-тармоғи Жанговар отрядлар ва Ҳаво кучлари захираси ходимларидан ташкил

топган. АҚШ Киберқўмондонлиги бошқа ҳужумкор кибероперацияларни амалга оширган бўлса-да, бу ишчи гуруҳ томонидан ўтказилган ва тан олинган биринчи ҳужумкор кибероперациядир[23].

Миллий хавфсизлик агентлиги (NSA) ва Киберхавфсизлик ва инфратузилма хавфсизлиги агентлиги (CISA) “5G булутли инфратузилма хавфсизлиги бўйича қўлланма” ҳужжатини эълон қилди. Қўлланма 5G тармоғининг манфаатдор томонларига, шу жумладан хизмат кўрсатувчи провайдерлар ва тизим интеграторларига йўл-йўриқ кўрсатиш учун мўлжалланган тўрт қисмли ҳужжатлардан иборат. Улар орасида китобнинг “Ён ҳаракатнинг олдини олиш ва аниқлаш” номли биринчи қисми сунъий интеллектни кузатиш тизимларидан потентсиал фойдаланишни тақдим этади, шу билан бирга булутли провайдерлар 5G тармоқларида латерал ҳаракатланишнинг олдини олиш ва аниқлаш учун амал қилиши керак бўлган асосий хавфсизлик протоколларини белгилайди; Китобнинг иккинчи қисми, “Тармоқ ресурсларини хавфсиз изолятсия қилиш” 5G булутли инфратузилмасини ҳимоя қилиш учун 5G контейнерга асосланган ёки гибрид контейнер/виртуал тармоқ (шунингдек, Под деб ҳам аталади) таҳдидларига қаратилган; Учинчи қисм, “Транзит, фойдаланишдаги ва дам олишда” “Маълумотлар” 5G асосий булут инфратузилмаси доирасидаги маълумотларнинг махфийлиги, яхлитлиги ва мавжудлигини ҳимоя қилиш учун мўлжалланган; китобнинг “Инфратузилма яхлитлигини таъминлаш” тўртинчи қисми булутли инфратузилма ва ресурсларнинг яхлитлигига қаратилган.

АҚШ Миллий хавфсизлик агентлигининг махфий ҳужжатларидан бирида кибермаконда навбатдаги йирик кенг кўламли можаро бошланиши ҳақидаги маълумотлар мавжуд. АҚШ ҳақиқатда кибер уруш бошлаган ягона давлатдир. Ҳеч кимга сир эмаски, АҚШнинг собиқ президенти Обама Эроннинг минглаб ядро центрифугаларини йўқ қилиш учун киберҳужумга буйруқ берган. Компьютер вируслари билан амалга оширилган кучли технологик ҳужум натижасида америкалик хакерлар Эронга катта моддий зарар етказган ҳолда ядровий дастурни икки йилга орқага қайтаришга муваффақ бўлишди. Энди ҳеч ким бу тезкор маълумотларни, яъни “кибер кучлар” амалиётини аввалгидек қунт билан яширишга уринмаяпти.
2012 йилдан бери Сурияда интернет АҚШ томонидан блокланган. Эслатиб ўтамиз, уч йил аввал АҚШ армиясида мустақил қўшинлар тури сифатида ташкил этилган Кибер-кучлар таркибида 20 мингга яқин ходим мавжуд[24].

[23] https://www.cybercom.mil/Media/News/Tag/47488/cyber/
[24]https://www.thedrive.com/the-war-zone/43776/cyber-command-task-force-conducted-its-first-offensive-operation-as-defense-secretary-watched

Хуллас, биринчидан, бугунги кунда дунёдаги илғор киберҳимоя дастурлари ҳар бир фойдаланувчининг манфаатларини ҳимоя қилади. Индивидуал даражада, кибермудофаа ҳужуми шахсий маълумотларнинг ўғирланиши, пул маблағлари ёки оилавий фотосуратлар каби қимматли маълумотларнинг йўқолиши ва кенг миқёсда давлат ва ҳарбий сирларни ошкор қилиш каби салбий оқибатларга олиб келиши мумкин. Электр станциялари, шифохоналар, молиявий хизматлар кўрсатувчи банк сектори ва бошқа институтлар каби барча муҳим инфратузилмаларни ҳимоя қилиш жамиятимиз ҳаёти ва фаолиятини таъминлаш учун жуда муҳимдир. Иккинчидан, ҳозирда киберхавфсизлик, онлайн хавфсизлик, тармоқлар ишончлилиги учун ҳал қилувчи хавфсизлик масалалари энг муҳим устувор йўналишлардан бири сифатида қаралмоқда. Самарали халқаро ҳамкорлик, кўп томонлама мулоқотга эришиш, ушбу қарорларни муваффақиятли қабул қилиш ва амалга ошириш мақсадида давлат, нодавлат ва халқаро ташкилотлар томонидан ҳар йили минтақавий ва жаҳон миқёсида турли тадбирлар ўтказилмоқда.

ФОЙДАЛАНГАН АДАБИЁТЛАР:

1. Алгулиев Р., Салманова П. Информационное общество. Интересные хронологические факты Баку Информационные технологии 2014. – 169 с.
2. Курилкин А.В. Информационные и кибернетические операции как инструмент реализации внешней политики : формы, методы, технологии : диссертация ... кандидата политических наук. - Москва, 2021. - 207 с.
3. Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая : диссертация ... кандидата политических наук. - Москва, 2014. - 207 с.
4. Виловатых А.В. Информационное противоборство в политическом процессе : тренды цифровой реальности : диссертация ... доктора политических наук. - Москва, 2021. - 347 с.
5. Қонунчилик маълумотлари миллий базаси, 24.07.2021 й., 06/21/6268/0700-сон.
6. Қонун ҳужжатлари маълумотлари миллий базаси, 24.05.2018 й., 09/18/380/1262-сон, 11.10.2018 й., 09/18/817/2033-сон.
7. Қонунчилик маълумотлари миллий базаси, 16.04.2022 й., 03/22/764/0313-сон.
8. https://news.un.org/ru/story/2021/06/1405532
9. https://rus.lb.ua/economics/2012/01/27/133936_oon_provedet_globalnoe.html
10. https://www.harbornetworks.com/blog/topic/mitel-support
11. https://www.cybercom.mil/Media/News/Tag/47488/cyber/
12. https://www.thedrive.com/the-war-zone/43776/cyber-command-task-force-conducted-its-first-offensive-operation-as-defense-secretary-watched