АЮУЛГҮЙ БАЙДЛЫН УДИРДЛАГА

КИБЕР АЮУЛГҮЙ БАЙДАЛ, КИБЕР ОРЧИН ДАХЬ МОНГОЛ УЛСЫН ӨНӨӨГИЙН БАЙДАЛД ХИЙСЭН ДҮН ШИНЖИЛГЭЭ

А.Амгаланбаяр
ДХИС-ийн ХАУСПБ-ийн ахлах багш,
цэргийн ухааны магистр, дэд хурандаа

Товч агуулга. Мэдээллийн технологи хурдацтай хөгжиж буй эрин үед мэдээллийн аюулгүй байдлыг хангах явдал нь нэн тэргүүний хэрэгцээ, шаардлага болж байна. Учир нь мэдээллийг цахим хэлбэрээр боловсруулах, хадгалах, дамжуулах нь түгээмэл үзэгдэл болж байгаа бөгөөд цахим хэлбэрт орсон мэдээлэл нь уламжлалт цаасан болон бусад хэлбэрийн мэдээлэлтэй харьцангуй гадны халдлагад (устгах,өөрчлөх,солих г.м.) өртөмтгий шинж чанартай болж эмзэг байдлын түвшин нь нэмэгддэг нь цахим мэдээллийг гадны халдлагаас хамгаалах хамгаалалтын шинэ түвшинг шаардаж байна.

Түлхүүр үгс. Кибер аюулгүй байдал, кибер орчин, өнөөгийн байдал

Оршил. Дэлхийн улс орон бүр засгийн газар, батлан хамгаалах, банк санхүү, тээвэр холбоо гэх мэт амин чухал салбаруудад мэдээллийг цахим хэлбэрээр боловсруулж, хадгалж, ашиглах нь нэмэгдэж тэдгээр дэд бүтцийн удирдлага үйл ажиллагаа нь компьютер, компьютерын сүлжээнээс хамаарах хамаарал нь улам бүр нэмэгдэж байна. Нөгөө талаар мэдээлэл нь эдийн бус баялагт хамаарах хөрөнгө бөгөөд төр засаг, аж ахуйн нэгж, төрийн бус байгууллага, иргэдийн мэдээллийн өмч, хөрөнгийг хамгаалах механизм нь амьдралд төлөвшөөгүйгээс иргэд байгууллагад үлэмж хэмжээний хохирол учирсаар байгаа билээ.

Кибер аюулгүй байдлыг хангах шинэ технологи хөгжихийн хэрээр халдагчид ч мөн адил хөгжиж байдаг. Иймд бид кибер халдлага /цахим халдлага/ гэж юуг ойлгох талаар авч үзэх хэрэгтэй байна. Виртуал ертөнцөд систем, файл, өгөгдөл, дата /мэдээлэл/ гэх зүйлсийн хамгаалалт сул, хангалтгүй тохиолдолд улс үндэстэн, иргэн бүр энэ төрлийн аюул, эрсдэлтэй нүүр тулдаг юм[1].

Үүнтэй холбогдуулан иргэд, аж ахуйн нэгж байгууллагын зүгээс мэдээллийн өмчөө хамгаалах мэдлэг болон механизмыг бий болгох, мэдээллийн аюулгүй байдлын хангах хувь хүний соёлыг бий болгож, төлөвшүүлэх хэрэгцээ, шаардлага амьдралаас урган гарч байна.

Үндсэн хэсэг. Кибер аюулгүй байдлын тухай ойлголт: Компьютер ашиглан үйлдсэн гэмт хэрэг хэдийд анх гарсныг тогтооход хэцүү. “Компьютерийн гэмт хэрэг” гэдэг нэр томъёо 1960-аад оны эхэн үед электрон тооцоолон бодох машин ашиглан үйлдсэн гэмт хэргийн анхны тохиолдлыг АНУ-д илрүүлж, түүний дараа Европын улсуудын хэвлэл мэдээллийн хэрэгслүүдэд өргөн хэрэглэгдэх болжээ[2].

Тухайн үед криминологийн болон эрх зүйн үндэслэл байхгүй байсан хэдий ч уг нэр томъёог хууль

[1] Батболд. Ж, Таны аюулгүй байдал. Уб., 2015.

[2] Цогтбаатар. Б, Мэдээллийн аюулгүй байдал. Уб., 2018.

хамгаалах байгууллагын ажилтнууд болон эрдэмтэн судлаачид өргөн ашиглах болсон байна.

Дэлхийн улс орнуудад Шинжлэх ухаан техникийн үсрэнгүй хөгжил үр өгөөжөө өгөхийн зэрэгцээ шинэ төрлийн аюулуудыг бий болгож байдаг нь сүүлийн үед улам бүр ил тод болох боллоо. Эдгээр аюулуудын нэг нь хакеруудын өдүүлдэг кибер халдлагын учруулж буй хор аюулын асуудал юм. Хакерууд сонирхол татсан улс орны аюулгүй байдалд заналхийлэх, улам бүр өргөжиж буй кибер орон зайд халдах, түүнд агуулагдаж буй мэдээллийг устгах, өөрчлөх, хувиргах замаар улс орнуудын төр, засгийн шийдвэр гаргалтад нөлөөлөх, төрийг чадавхгүйжүүлэх, төрийн үйл ажиллагааг гацаанд оруулах, төрийн нууцад нь нэвтрэх зэрэг тохиолдол ихэсч байна. Мэдээллийн технологийн тэргүүлэх гүрэн болсон хөгжингүй орнуудад ч энэ аюул хор уршиг тулгараад байгаа нь анхаарлыг татаж байна. АНУ-ын Пентагоны дээд зэргийн нууцлалтай гэгдэх сүлжээнд БНХАУ-д төвтэй хакерууд нэвтрэн орж, 300 тэрбум ам. долларын өртөг бүхий F-35 Lightning II гэх шинэ үеийн сөнөөгч онгоцны схем зураг, моделийн мэдээлэл бүхий хэд хэдэн терабайтуудыг татаж авсаныг "The Wall Street Journal" мэдээлсэн[1].

Канад Улсын "Information Warfare Monitoring" байгууллагын шинжээчдийн явуулсан судалгаагаар АНУ дах БНЭУ-ын ЭСЯ-ны копьютерийн сүлжээний кодыг нэвтэн орсон GhostNet хэмээх тагнуул хийх үйлдлийн системтэй програм нь Энэтхэг Улс дах Түвдийн нүүдлийн Засгийн газрын болон Далай ламын цахим шууданг замаас нь хулгайлж байсан гэх мэдээлэл дэлхий нийтийн томооохон хэвлэлүүдэд 2019 онооос нийтлэгдэж эхэлсэн. [2] Түүнчлэн компьютерүүдийн камерийг алсын зайнаас ажиллуулах, дүрс, дуу бичлэгийг хураах, тухайн компьютерүүдээр дамжуулж байгаа бүх мэдээллийг хянадаг байжээ. GhostNet-ийн халдлагад ХБНГУ, БНЭУ, БНСУ, Тайвань, Пакистан, Португаль, Румын зэрэг улс орнууд өртөж байжээ.

НҮБ-аас гаргасан тоо баримтаас харахад кибер гэмт хэргээс учирч буй хохирол, мансууруулах бодисын хууль бус эргэлтээс олдог орлоготой тэнцэх болсон гэж тодорхойлж байна. Зөвхөн АНУ-д кибер гэмт хэргийн улмаас учирч буй хохирол 100 миллиард долларт хүрсэн.Үүний дээр олонхи тохиолдолд учирсан хохирлыг бодитоор тооцож чадахгүй, эдээлэхгүй байгааг дурьдах нь зүйтэй. Сүүлийн үед дэлхийн улс орнуудад бүртгэгдэж байгаа кибер гэмт хэрэг жил бүр өссөөр байна.[3]

Компьютерийн мэдээллийн хүрээн дэх гэмт хэрэгтэй амжилттай тэмцэхэд эдгээр гэмт хэргийн талаархи нэгдсэн ойлголт олон улсын хэмжээнд байх зайлшгүй шаардлагатай хэмээн үзэж Европын холбооноос 1989 оны 9 дүгээр сарын 13-нд №89 тоот зөвлөмж гаргасан байдаг. Энэхүү баримт бичигт үндэсний хууль тогтоох байгууллагуудын удирдлага болговол зохих зарчмууд, түүнчлэн компьютер буруугаар ашиглаж буй тодорхой үйлдлүүдийг гэмт хэрэг гэж үзэн, эрүүгийн хууль тогтоомжид тусгасан байна.

Компьютерийн луйвар: Эдийн засгийн ашиг өөртөө буюу бусдад олох зорилгоор компьютерийн мэдээлэл, программыг оруулах, өөрчлөх, арилгах, мэдээллийн

[1] Anthony. L, The Wall Street Journal. magazine.USA.,2019.

[2] Болд. Д, Safety coach аюулгүй байдлын дасгалжуулагч, Уб., 2022.

[3] Халтар.Т, Компьютерийн мэдээлэл, программыг өөрчлөх, эвдэх, сүйтгэх гэмт хэрэг. Эрдэм судлал. сэтгүүл.Уб., 2002. 107 дах хуудас.

боловсруулалтад өөр байдлаар нэвтрэх замаар эдийн засгийн хохирол учруулан, бусдын эд хөрөнгө алдагдахад хүргэсэн үйлдэл.

Компьютерийн хуурмаглал: Тодорхой халдлагын зүйлийг хуурамчаар үйлдэхийн тулд компьютерийн мэдээлэл, программыг оруулах, арилгах, аль эсвэл мэдээллийн боловсруулалтад өөр байдлаар нэвтэрсэн үйлдэл.

Компьютерийн мэдээлэл, программд хохирол учруулах: Компьютерийн мэдээлэл, программыг хууль бусаар арилгах, хохирол учруулах, чанарыг нь муутгах үйлдэл.

Компьютерийн хорлон саатуулалт: Компьютерийн болон холбоо харилцааны системийн ажиллагаанд саад учруулах зорилгоор компьютерийн мэдээлэл, программыг оруулах, өөрчлөх, арилгах, дарах үйлдэл.

Зөвшөөрөлгүйгээр нэвтрэх: Компьютерийн систем буюу сүлжээнд хамгаалалтыг эвдэн нэвтрэх үйлдэл.

Зөвшөөрөлгүйгээр замаас нь барьж авах: Компьтерийн систем, сүлжээний хэмжээнд дамжуулагдаж буй мэдээллийг техник хэрэгслийн тусламжтайгаар хууль бусаар барьж авах үйлдэл.

Зохиогчийн эрхээр хамгаалагдсан компьютерийн программыг зөвшөөрөлгүй хуулбарлах: Хуулиар хамгаалагдсан компьютерийн программыг хууль бусаар хуулбарлах, тараах, дамжуулах үйлдэл.

Компьютерийн мэдээлэл, программыг өөрчлөх: Компьютерийн мэдээлэл, программыг хууль бусаар өөрчлөх үйлдэл.

Компьютерийн тагнуул: Бусдад эдийн засгийн хохирол учруулах, өөртөө буюу гуравдагч этгээдэд хууль бус ашиг олох зорилгоор бизнес, худалдааны нууцыг ямар нэгэн эрх зүйн үндэслэлгүйгээр хориглогдсон арга хэрэглэн олж авах, задруулах, дамжуулах, ашиглах үйлдэл.

Компьютер зөвшөөрөлгүй ашиглах: Компьютерийн систем, сүлжээг хууль бусаар хэрэглэн түүнийг ашиглах эрх бүхий хүнд хохирол учруулсан буюу учруулахаар байсан, аль эсвэл компьютерийн хэвийн ажиллагааг алдагдуулсан үйлдэл.

Хуулиар хамгаалагдсан компьютерийн программыг зөвшөөрөлгүй ашиглах: Өөртөө болон бусдад хууль бус эдийн засгийн ашиг олох зорилгоор хуулиар хамгаалагдсан компьютерийн программыг хууль бусаар ашиглан эрх эзэмшигчид хохирол учруулсан үйлдэл зэргээр зөвлөмжид тусгажээ.

Анхаарал татвал зохих өөр бас нэг олон улсын эрх зүйн баримт бичиг бол Европын холбооны Кибер гэмт хэргийн тухай 2001 оны Конвенци юм. Уг баримт бичигт дараах ойлголтыг хуульчилсан байдаг.

Кибер орон зай гэдэг нь хоорондоо холбогдсон хэдэн зуун сая компьютер, серверүүд, рүүтэрүүд, свитчүүдээс бүрдэх орон зай юм.

Кибер аюулгүй байдал нь мэдээллийн аюулгүй байдлыг мэдээллийн технологийн түвшинд хангахыг хэлнэ.

Кибер терроризм: Зохион байгуулалттайгаар аливаа улсын компьютер, мэдээлэл, компьютерийн систем, компьютерийн программ , өгөгдөлд халдаж улмаар их хэмжээний хохирол учруулах, мөн үхэл, сүйрэлд хүргэх интернэт ашиглан үйлдсэн террор үйл ажиллагааг хэлнэ.

Кибер дайн: Аливаа улсын төрийн шууд ба шууд бус оролцоотойгоор мэдээллийг өөрчлөх, устгах, мөн компьютер, компьютерийн системийг эвдэх, ажиллагаагүй болгох, удирдлагыг нь хяналтдаа авах зорилгоор өөр улс

үндэстний компьютер, компьютерийн сүлжээнд зөвшөөрөлгүй нэвтрэх, эсвэл компьютерийн системд нөлөөлөх нэг үйл ажиллагааг хэлнэ.

Кибер гэмт хэрэг: Компьютер, мэдээллийн сүлжээ, интернэт ашиглан үйлдэгдсэн бүх төрлийн гэмт хэрэг /хуулинд тусгаснаар/

- Хувь хүний эсрэг
- Өмчийн эсрэг
- Төрийн эсрэг
- Мөнгөний төлөө бус (улс төрийн мессеж өгөх, сорилт, зугаа цэнгэл)
- Мөнгөний зорилгоор
- Зохион байгуулалттай гэмт бүлэглэл, хувь хүн шунахайн сэдэлт, зорилготойгоор
- Кибер дайн зэргээр томьёлсон байдаг.

Кибер гэмт хэргийн ангилал, цар хүрээгээр нь авч үзвэл:

Хүснэгт №1

	Кибер гэмт хэрэг	Кибер, террор	Кибер тагнуул	Кибер дайн
Үйлдэгч	Хувь хүн	Бүлэглэл	Байгууллага	Төр
Зорилго	Эдийн засгийн ашиг сонирхол,хялбар аргаар мөнгө олох	Улс төр, нийгэм, эдийн засгийн шийдвэрт нөлөөлөх	Оюуны өмч, төрийн чухал нууцыг хулгайлах	Цэрэг, улс төрийн давамгай байдал олох
Хохирогч (Бай)	Хувь хүн, компани	Онц чухал дэд бүтэц	Төрийн байгууллага, Компани	Онц чухал дэд бүтэц, төрийн байгууллага
Арга, хэрэгсэл	Phishing, Spamming	DDOS, BotNet	Trojan Horse, Backdoors	Кибер цэрэг, кибер зэвсэг

Олон Улсад 2015-2022 оны байдлаар үйлдэгдсэн хамгийн их хохирол учруулсан кибер гэмт хэрэг:

1.Утасгүй холболтоор хийсэн довтолгоон: Card Systems Solutions Inc компанийн төлбөрийн боловсруулалтын төвийн аюулгүй байдлын системд вирус оруулж эвдэж холбогдох замаар 40 сая гаруй карт эзэмшигчийн нэр, үйлчлүүлдэг банк, дансны дугаарыг гэмт этгээдүүд олж авсны үндсэн дээр 1,8 тэрбум фунт стерлингийг хулгайгаар шилжүүлэн авч чадсан байна. Энэ гэмт хэргийг системийн хамгаалалт эвдэж хувийн мэдээлэл хулгайлсан хамгийн том хэрэг хэмээн тооцож байна.

2.АТМ бэлэн мөнгөний машинд хийсэн халдлага: 1,5 сая цалингийн карт, нийгмийн даатгалын 1,1 сая дугаарыг гэмт этгээдүүд хулгайлсны үндсэн дээр АНУ-ын 49 хотын 130 бэлэн мөнгөний машинаас нэгэн зэрэг 30 минутын хугацаанд 9 сая доллар гаргаж авсан байна. ОХУ, АНУ, Эстони, Украины иргэд энэ хэргийг үйлдсэн байжээ.

3.Гонсалес дахин халдлага: Өмнө нь компьютерийн сүлжээ дэлгүүрүүдэд утасгүй сүлжээгээр халдаж байсан Альберт Гонсалес хэмээх хакер преступлении 7-Eleven болон Hannaford Brothers сүлжээ дэлгүүрүүдийн цахим төлбөр тооцооны Heartland Payment Systems –д 2019 онд халдаж 130 сая кредит картын дугаарыг цуглуулж 8 сая фунт стерлингийг авсан байна. Энэ хакерыг баривчлах үед биед нь 1,65 сая долларыг хурааж авсан байдаг.

4.Ginko виртуаль банкны дампуурал: Ginko виртуаль банкыг байгуулагчид урдаас төлөвлөсний дагуу хуурамчаар дампууруулсны улмаас хадгаламж эзэмшигч 18 мянга орчим хүн хэдэн зуун сая лиднен доллар буюу хагас сая фунт стерлингийн хадгаламжаа алдсан байна.

5.Бразил: 2021 оны 09 сард баривчлагдсан бразилийн фишер Валдир Пауло де Алмейда (Valdir Paulo de Almeida) 18 хакераас бүрдсэн гэмт бүлэглэлийг удирдаж янз бүрийн банкны данснаас 37 сая доллар хулгайлан авсан байна. Тэд фишинг довтолгоон болон Троян кодууд ашигладаг байв. Тэд өдөрт 3 сая хүртэл хордуулсан цахим захиаг хэрэглэгчдэд илгээдэг байжээ.

Кибер орчин дахь Монгол Улсын өнөөгийн байдалд хийсэн дүн шинжилгээ: Монгол Улсад Төрийн холбооны газар 1933 онд ДХГ-ын харъяанд радио холбооны нэгж байгуулагдсанаар үүссэн гэж үздэг. Энэ байгууллага нь төр, засгийн удирдлага болон төрийн байгууллагуудыг нууцлалтай, найдвартай харилцаа холбоо, шуудангаар хангах, төрийн мэдээлэл, харилцаа холбооны аюулгүй байдлыг хангах үүрэгтэй байгууллага юм.[1]

Монгол Улсад анх 1961 онд “Тайблятор” нэртэй компьютерийг ашиглаж байсан. Статистикийн газрын захиалгаар нийлүүлсэн бөгөөд Тайбляторыг анхны программын удирдлагатай компьютер гэж үздэг. Үүний дараа буюу 1986 онд PC /персонал компьютер/-ийг оруулж ирсэн байдаг.Харин 1994 онд манай улс анх интернет хэрэглэгч улсуудын жагсаалтад орж байжээ.[2]

Бусад өндөр хөгжилтэй оронтой харьцуулахад манай улс интернэт хэрэглэгчдийн тоогоор дэлхийн 200 гаруй улсаас 102 дугаарт бичигдэж байгаа хэдий ч хүн амынх нь тоотой харьцуулахад дэлхийд нэгдүгээрт жагсаж байгааг Нийгмийн хамгааллын үйлчилгээний төвийнхөн 2021 онд судалж, тогтоосон байдаг.

Цахим хэрэглээ нэмэгдэхийн хирээр хувь хүн, байгууллага, улс орны мэдээллийн аюулгүй байдлыг хангах хэрэгцээ өсөн нэмэгдэж, эрх зүйн орчинг бий болгох шаардлага тулгарсан. Монгол Улсын хувьд сүүлийн 15 жилийн хугацаанд Кибер аюулгүй байдлыг хангах тухай хуулийн төслийг нийт 7 удаа өргөн барьж, Кибер аюулгүй байдлын тухай хуулийн төслийг Улсын Их Хурлын 2021 оны 12 дугаар сарын 17-ны өдрийн чуулганы нэгдсэн хуралдаанаар хэлэлцэн баталж, кибер аюулгүй байдлыг хангах эрх зүйн үндсийг анх удаа бүрдүүлсэн юм.

Монгол Улсын Кибер аюулгүй байдлын тухай хуулийн 4.1.1."кибер аюулгүй байдал" гэж кибер орчинд мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдал хангагдсан байхыг; мөн хуулийн 4.1.13."кибер аюулгүй байдлын зөрчил" гэж мэдээллийн системийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдалд заналхийлж байгаа аливаа үйлдэл, эс үйлдлийг; 4.1.14."кибер халдлага" гэж мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдлыг алдагдуулах зорилго бүхий үйлдлийг гэж хуульчилж өгсөн байдаг.[3]

Монгол Улсын хувьд кибер аюулгүй байдлаа үндэсний аюулгүй байдлын хэмжээнд тавьсан, кибер дайн, кибер тагнуул идэвхтэй явуулдаг хоёр том кибер гүрний дунд оршиж, энэ хоёр улсаар дайруулан

[1] Эрдэнэ. Ц, Терроризм, түүнтэй тэмцэх асуудал. илтгэлийн эмхтгэл. УБ., 2003. 56 дах тал.

[2] Гантулга. Б, Компьютерийн мэдлэг. Уб., 2012. 13 дах тал.

[3] Монгол Улсын Кибер аюулгүй байдлын тухай хууль. Уб., 2021.

интернетийн урсгалаа авдаг нь өөрөө энэхүү аюулд өртөх магадлалыг өдөр бүр нэмэгдүүлж байна.

ЦЕГ-ын Цахим гэмт хэрэгтэй тэмцэх албаны 2022 онд хийсэн судалгаагаар манай улсад өдөрт 30 мянгаас 100 гаруй мянган кибер довтолгоо, халдлага орж ирдэг. Эдгээр халдлагын 80 гаруй хувийг сонирхогчид компаний мэдээлэл, сервер рүү нэвтрэх оролдлого эзэлдэг бол харин үлдсэн 20 гаруй хувийг өндөр мэргэшсэн, мэргэжлийн хакер, цахим халдлага үйлдэгч хүмүүс аль болохоор мэдэгдэхгүй, ул мөр үлдээхгүйгээр мэдээллүүдийг хуулах оролдлогыг хийдэг.

Ийм төрлийн довтолгоонууд сүүлийн үед Хятад, ОХУ, АНУ, Тайвань, Солонгос, Япон, Бразил, Энэтхэг зэрэг улс орнуудаас ирдэг байна.[1]

Монгол Улсын Засгийн газрын гишүүн, Цахим хөгжил, харилцаа холбооны сайд Н.Учрал нар Зэвсэгт хүчний Жанжин штаб, Зэвсэгт хүчний Кибер аюулгүй байдлын цэргийн командлалд ажиллах үеэр “Миний бие УИХ-ын Инновац, цахим бодлогын байнгын хорооны даргаар ажиллаж байхдаа Кибер аюулгүй байдлын тухай хуулийг батлуулахад ажлын хэсгийг ахалсан. Энэ хууль батлагдсанаар кибер аюулгүй байдлын эрх зүйн орчны үндэс тогтолцоо хуульчлагдсан юм бид үүний эхлэлийг тавьсан, үндэсний аюулгүй байдал гэж Монгол Улсын үндэсний язгуур ашиг сонирхлыг хангах гадаад, дотоод таатай нөхцөл баталгаатай хангагдсан байдлыг хэлдэг бол аюулгүй байдлын бүрэлдэхүүн хэсэг болох мэдээллийн аюулгүй байдлыг хангах хэрэгцээ бидэнд тулгараад байна [2] ” хэмээн кибер аюулгүй байдлын эрх зүйн орчны талаар хэлсэн байдаг.

Мөн Монгол Улсын Засгийн газрын гишүүн, Батлан хамгаалахын сайд Г.Сайханбаяр “Монгол Улсын үндэсний аюулгүй байдлын үндсэн элементийн нэг нь кибер аюулгүй байдлын асуудал. Дэлхийн улс орнуудын өөрчлөлт, шинэчлэлт хамгийн түрүүнд цахим орчинд явагдаж байна. Монгол Улсын Зэвсэгт хүчин Кибер аюулгүй байдлын цэрэгтэй болоод 3 жил болж байгаа. Кибер аюулгүй байдлын хууль эрх зүйн орчин бүрэлдсэн, үндэсний стратегитай болсон, Кибер аюулгүй байдлын цэргийг ашиглах үзэл баримтлал төрөөс батлагдсан. Бидэнд хууль эрх зүйн хувьд бүх үндэс бүрдсэн. Одоо бид кибер аюулгүй байдлын цэргийг жинхэнэ утгаар нь хөгжүүлэх, энэ хүрээнд эхний ээлжид техник, тоног төхөөрөмжийн хангалт хийгдэх шаардлагатай байгаа гэж хэлсэн байдаг. Үүнээс үзэхэд кибер аюулгүй байдлыг улс орны хэмжээнд, иргэний хэмжээнд хангах байгууллага, эрх зүйн орчин бүрдсэн байна. Харин мэргэжлийн боловсон хүчин, өндөр мэдлэгтэй хүний нөөц дутмаг байгаа гэж мэдээлэл өгсөн байдаг.[3]

[1] https://police.gov.mn/as/article/

[2] Монгол Улсын Үндэсний аюулгүй байдлын тухай хууль. Уб., 2001.

[3] http://mod.gov.mn/2023/04/11

Монгол Улсад кибер аюулгүй байдлыг хангаж буй тогтолцоо:
Хүснэгт №2

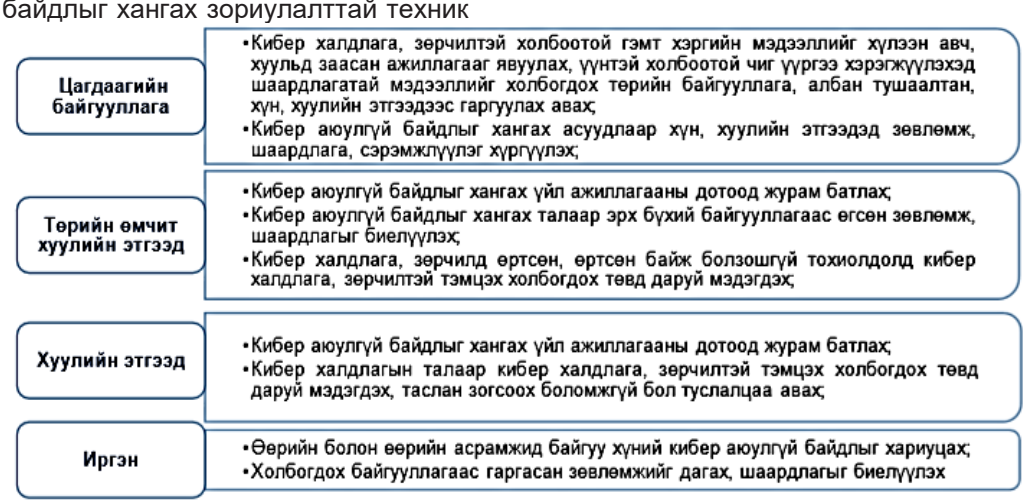
Засгийн газар	•Кибер аюулгүй байдлын үндэсний стратегийг батлах; •Хөгжлийн бодлого, төлөвлөлтийн баримт бичигт кибер аюулгүй байдлыг хангах талаар тусгах, хууль тогтоомжийн биелэлтийг зохион байгуулах; •Онц чухал мэдээллийн дэд бүтэцтэй байгууллагын жагсаалтыг батлах;
Кибер аюулгүй байдлын зөвлөл	•***Зөвлөлийг Ерөнхий сайд тэргүүлж, дэд даргаар цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн Засгийн газрын гишүүн, Тагнуулын ерөнхий газрын дарга нар ажиллана;*** •Кибер аюулгүй байдлыг хангах хууль тогтоомжийн хэрэгжилтэд хяналт тавина; •Үндэсний хэмжээний кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлага, зохион байгуулалтаар хангах, холбогдох байгууллагын үйл ажиллагааг уялдуулан зохицуулах;
Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны байгууллага	•Кибер аюулгүй байдлыг хангах хууль тогтоомж, эрх бүхий байгууллагын шийдвэрийг хэрэгжүүлэх; •Кибер аюулгүй байдлыг талаар хөгжлийн бодлого боловсруулах, хэрэгжилтийг зохион байгуулах; •Кибер аюулгүй байдлыг хангах нийтлэг журмыг тагнуулын байгууллага, зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллагатай хамтран боловруулах;
Тагнуулын байгууллага	•Төрийн мэдээллийн нэгдсэн сүлжээг зохион байгуулж, түүний кибер аюулгүй байдлыг хангах; •Төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон болон онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээдийн кибер аюулгүй байдлыг хангах үйл ажиллагаанд хяналт тавих, холбогдох этгээдэд сургалт зохион байгуулах; •Үндэсний хэмжээний кибер халдлагаас хамгаалах төлөвлөгөөг боловсруулах, хэрэгжилтэд хяналт тавьж ажиллах;
Зэвсэгт хүчний аюулгүй байдлыг хангах байгууллага	•Кибер аюулгүй байдлын хууль тогтоомжийн хэрэгжилтийг батлан хамгаалах салбарт зохион байгуулах; •Тайван цагт батлан хамгаалах үйл ажиллагааны кибер аюулгүй байдал, зэвсэгт хүчний мэдээллийн систем, мэдээллийн сүлжээний аюулгүй байдлыг хангаж, шаардлагатай үед улсын кибер орон зайн аюулгүй байдлыг хангах үйл ажиллагаанд дэмжлэг үзүүлэх;

1. Үндэсний төв: Үндэсний төв нь улсын хэмжээнд кибер халдлага, зөрчилтэй тэмцэх төвүүдийн үйл ажиллагааг уялдуулан зохицуулах, мэргэжил, арга зүйн туслалцаа үзүүлэх, эрхлэх асуудлын хүрээнд Монгол Улсыг төлөөлөн олон улсын болон гадаад улсын ижил төстэй байгууллагатай мэдээ, мэдээлэл солилцох, хамтран ажиллах, кибер халдлага, зөрчлийн талаар мэдээлэл хүлээн авах, холбогдох байгууллагад шилжүүлэх, онц чухал мэдээллийн дэд бүтэцтэй байгууллага, холбогдох бусад байгууллага, албан тушаалтанд кибер халдлага, зөрчлийн талаар зөвлөмж, шаардлага хүргүүлэх, улсын хэмжээнд бүртгэгдсэн кибер халдлага, зөрчлийн талаарх мэдээллийг ангилах үүргийг хүлээж, тагнуулын байгууллагын бүтцэд ажилладаг.

2. Нийтийн төв: Нийтийн төв нь иргэн, хуулийн этгээдийн мэдээллийн систем, мэдээллийн сүлжээнд чиглэсэн кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, кибер халдлага, зөрчилд өртсөн мэдээллийн системийг нөхөн сэргээхэд дэмжлэг үзүүлэх, кибер халдлага, зөрчлийн талаар судалгаа, дүн шинжилгээ хийх, олон нийтэд зөвлөмж, мэдээлэл түгээх, бусад төвүүдтэй хамтран ажиллах, иргэн, хуулийн этгээдэд кибер халдлага, зөрчлийн талаар зөвлөмж, шаардлага хүргүүлэх зэрэг үүргийг хүлээж цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагын дэргэд ажилладаг.

3. Зэвсэгт хүчний төв: Зэвсэгт хүчний төв нь батлан хамгаалах салбарын мэдээллийн системд чиглэсэн кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, кибер халдлага, зөрчилд өртсөн мэдээллийн системийг нөхөн сэргээх, гадны кибер халдлага,

түрэмгийллээс хамгаалах үйл ажиллагаанд дэмжлэг үзүүлэх, гадаад, дотоодын ижил чиг үүрэгтэй байгууллагуудтай мэдээ, мэдээлэл солилцож, хамтран ажиллах, батлан хамгаалах салбарын кибер аюулгүй байдлыг хангах зориулалттай техник болон программ хангамжийг шалган баталгаажуулах, дүгнэлт гаргах үүргийг хүлээж Зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллагын бүтцэд ажилладаг байна.



Энэхүү төвүүд нь өнөөдрийн байдлаар Монгол Улсын кибер аюулгүй байдлыг хангах нэгдсэн үүргийг хүлээж, хамтран ажиллаж байна.

Монгол Улсын Кибер аюулгүй байдалд тулгамдаж буй асуудал:

- Энэ салбарт ажиллах хүний нөөцийн мэдлэг дутмаг, техник, технологийн хүчин чадал муу;
- Олон нийтийн цахим хэрэглээний мэдлэг хомс, ёс зүйгүй хандлага их;
- Кибер довтолгооноос хамгаалах, хариу үйлдэл үзүүлэх чадамж сул;
- Интернэтийн агуулгад хяналт тавьдаггүй, зөвхөн мэдээлэлд үндэслэн ажилладаг;
- Төрийн байгууллагуудын интернэтийн болон дотоод сүлжээ нь хоорондоо холилдсон, интернэтэд олон гарцаар замбараагүй холбогддог;
- Мэдээллийн аюулгүй байдлын бодлого, журам, стандарт мөрдөггүй зэрэг асуудлууд тулгамдаж байна.

Дүгнэлт

Кибер халдлага, цахим гэмт хэрэгтэй тэмцэхэд хамгийн эхний гол асуудал бол хууль, эрх зүйн орчин хийгээд мэргэшсэн боловсон хүчнийг бэлтгэх, техник хэрэгсэл, тоног төхөөрөмжийг шинэчлэн хөгжүүлэх асуудал юм. Монгол Улсад 2022 оноос эхлэн кибер аюулгүй байдлыг хангах эрх зүйн орчин бүрдсэн хэдий ч цаг үеийн хөгжлөөс шалтгаалан энэ төрлийн гэмт хэргийн илрүүлэлт удааширч, ард иргэдээс ирж буй санал, гомдол өдөр ирэх тутамд нэмэгдэх хандлагатай байна.

Энэхүү кибер халдлагад өртөж буй иргэдийн дийлэнх хувийг 12-38 насны эмэгтэйчүүд эзэлж байгаа нь тэдний хууль эрх зүйн мэдлэг, сонор сэрэмжгүй байдал, цахим хэрэглээний мэдлэг хомс, богино хугацаанд ашиг олох хувийн сонирхол, шохоорхол зэрэг байдалтай шууд холбогдож байна.

Цаашид хууль, хүчний болон харилцаа холбоо, банк, санхүүгийн байгууллага, иргэдийн хамтын ажиллагааг нэмэгдүүлж, мэдээлэл солилцох, хамтран ажиллах бололцоог нэмэгдүүлж, энэ чиглэлээр мэргэшсэн байгууллагын туршлагыг нэвтрүүлэх бодит хэрэгцээ тулгараад байна.

Иймд кибер гэмт хэрэгтэй тэмцэх мэргэшсэн алба хаагчдыг буюу кибер-мөрдөгч нарыг цахим хөгжлөөрөө дэлхийд тэргүүлдэг өндөр хөгжилтэй улс оронд бага наснаас эхлэн сургаж, энэ төрлийн гэмт хэрэгт судалгаа шинжилгээ хийх лабораторийг үндэсний төв хэлбэрээр байгуулах шаардлагатай гэж дүгнэж байна.

Санал

1.Кибер гэмт хэрэгтэй тэмцэх мэргэшсэн алба хаагчдыг сурган, дадлагажуулах;

2.Хууль, хүчний болон харилцаа холбоо, банк, санхүүгийн байгууллага, иргэдийн хамтын ажиллагааг нэмэгдүүлэх;

3.Дэвшилтэд технологийн хөгжилтэй хөл нийлүүлэн алхахын тулд кибер аюулгүй байдлыг хангадаг төрийн болон аж ахуй нэгж, байгууллагын тоног төхөөрөмжийг төрийн дэмжлэгтэйгээр шинэчлэх зэрэг болно.

Эх сурвалжийн жагсаалт

1. Монгол Улсын Үндэсний аюулгүй байдлын тухай хууль. Уб., 2001.
2. Монгол Улсын Кибер аюулгүй байдлын тухай хууль. Уб., 2021.
3. Батболд,Ж. Таны аюулгүй байдал. Уб., 2015.
4. Цогтбаатар,Б. Мэдээллийн аюулгүй байдал. Уб., 2018.
5. Болд, Д. Safety coach аюулгүй байдлын дасгалжуулагч, Уб., 2022.
6. Халтар,Т.Компьютерийн мэдээлэл, программыг өөрчлөх, эвдэх, сүйтгэх гэмт хэрэг. Эрдэм судлал. сэтгүүл.Уб., 2002. 107 дах тал.
7. Эрдэнэ,Ц.Терроризм, түүнтэй тэмцэх асуудал.эмхтгэл.УБ.,2003.56 дах тал.
8. Гантулга,Б. Компьютерийн мэдлэг. Уб., 2012. 13 дах тал.
9. Anthony,I.The Wall Street Journal. magazine.USA.,2019
10. https://police.gov.mn/as/article/
11. https://itools.mn/