“МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ҮНДЭСНИЙ ХӨТӨЛБӨР” БОЛОВСРУУЛАХ НӨХЦӨЛ БАЙДЛЫН ДҮН ШИНЖИЛГЭЭ

I. МУ-ын Мэдээллийн аюулгүй байдлын өнөөгийн байдал

Дэлхий нийтэд мэдээллийн технологийн хөгжил нь бусад салбарын хөгжилтэй харьцуулахад асар хурдтай хөгжиж байна. Өнөөдөр дэлхийн бүх улс орон, эдийн засаг, нийгмийн хамгааллыг сайжруулах боломжтой мэдээлэл, харилцаа холбооны дэд бүтцийн шинэ эко-системийг бий болгохыг зорьж байна. Өнгөрсөн 10 жилийн хугацаанд Мэдээлэл, харилцаа холбооны технологи нь МТ-ын үйлчилгээ болон мэдээллийн урсгалыг нэмэгдүүлэх замаар эдийн засгийн хөгжилд туйлын ач холбогдолтой эерэг нөлөө үзүүлж буй хэдий ч ямар ч улс орны хувьд мэдээллийн аюулгүй байдлыг хангах асуудал хурцаар тавигдах болсон. Дэлхийн улсууд цахим халдлага, цахим гэмт хэргээс үүдэн өнгөрсөн 2017 онд 600 тэрбум америк долларын хохирол амссан бөгөөд энэ нь дэлхийн нийт эдийн засгийн 1 хувьтайтэнцэх хэмжээний дүн юм.[1] Түүнчлэн АНУ-д байрлах *Ponemon* хүрээлэнгийн судалгаагаар амжилттай үйлдэгдсэн цахим халдлага, цахим гэмт хэргээс үүдэн нэг байгууллага 2017 онд дунджаар 130 цахим халдлагад өртөж 11.7 сая америк долларын алдагдал хүлээлээ.[2] Иймд гадаад орнууд цахим мэдээллийн аюулгүй байдлын асуудлыг үндэсний аюулгүй байдлынхаа тэргүүлэх зорилтуудын нэг хэмээн зарлаж, хөрөнгө оруулалт хийх, үндэсний хэмжээнд стратеги, хөтөлбөр боловсруулж хэрэгжүүлэх, хууль, эрх зүйн орчноо боловсронгуй болгох, техник технологи, хүний нөөцөө бэхжүүлэх зэрэг арга хэмжээг хэрэгжүүлж байна. Тухайлбал АНУ 2017 онд цахим мэдээллийн аюулгүй байдлыг хангах чиглэлээр нийт 60.4 тэрбум америк доллар зарцуулсан бол 2018 онд 66 тэрбум долларыг зарцуулахаар төлөвлөсөн.[3]

Монгол Улсын хувьд Улсын их хурлаар 2010 оны 7 дугаар сарын 15-ны өдөр батлагдсан Үндэсний аюулгүй байдлын үзэл баримтлалын 3.6 дугаар зүйлд Үндэсний аюулгүй байдлыг хангах, улс орны хөгжлийг дэмжих, үндэсний үнэт зүйлийг хэвшүүлэх, нийгмийн оюун санааг төлөвшүүлэхэд мэдээлэл, мэдээллийн аюулгүй байдал нэн чухал ач холбогдолтой гэж заасан байдаг. Мөн Засгийн газрын 2017 оны 47 дугаар тогтоолоор батлагдсан “Төрөөс мэдээлэл харилцаа холбооны хөгжлийн талаар баримтлах бодлого 2017-2025” баримт бичгийн 2.3.7 дугаар заалтад “Үндэсний ашиг сонирхлыг хамгаалах, төр, иргэн, байгууллагын мэдээллийн бүрэн бүтэн байдал, үнэн зөв, хамгаалалттай, хүртээмжтэй байдлыг баталгаажуулах замаар мэдээллийн аюулгүй байдлыг хангана” гэж тусгасан ба “Төрөөс мэдээлэл, харилцаа холбооны хөгжлийн талаар баримтлах бодлого 2017-

---

[1] АНУ-ын Стратеги, олон улс судлалын хүрээлэнгийн мэдээлснээр

[2] Судалгаанд 7 улс /АНУ, Их британи, ХБНГУ, Франц, Итали, Авсрали, Япон/-ын 1000 ба түүнээс дээш тооны ажилтантай 254 компани хамрагдсан. /https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf/

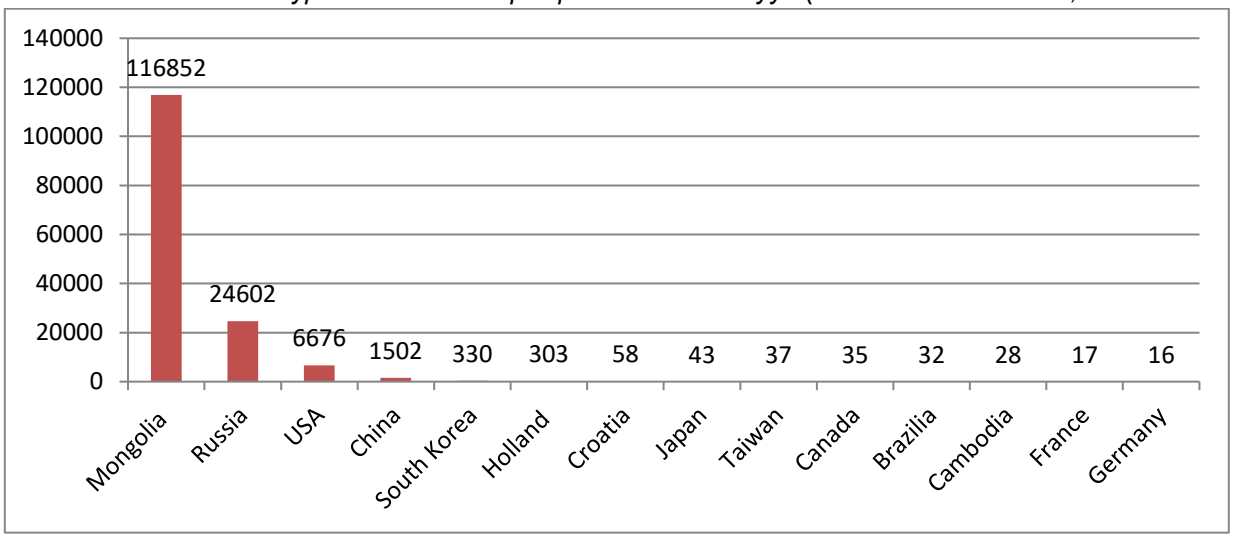
[3] © Statista 2018

2025”-ыг хэрэгжүүлэх арга хэмжээний төлөвлөгөөний мэдээлэл, харилцаа холбооны салбарын эрх зүйн тогтолцоо, зохион байгуулалтыг оновчтой болгох замаар салбарын хөгжлийн таатай орчинг бүрдүүлэх тухай 1 дүгээр зорилтын хүрээнд хэрэгжүүлэх арга хэмжээний 2 дугаарт Мэдээллийн аюулгүй байдлын тухай үндэсний хөтөлбөр шинээр боловсруулж батлуулна гэж тус тус тусгасан байдаг.

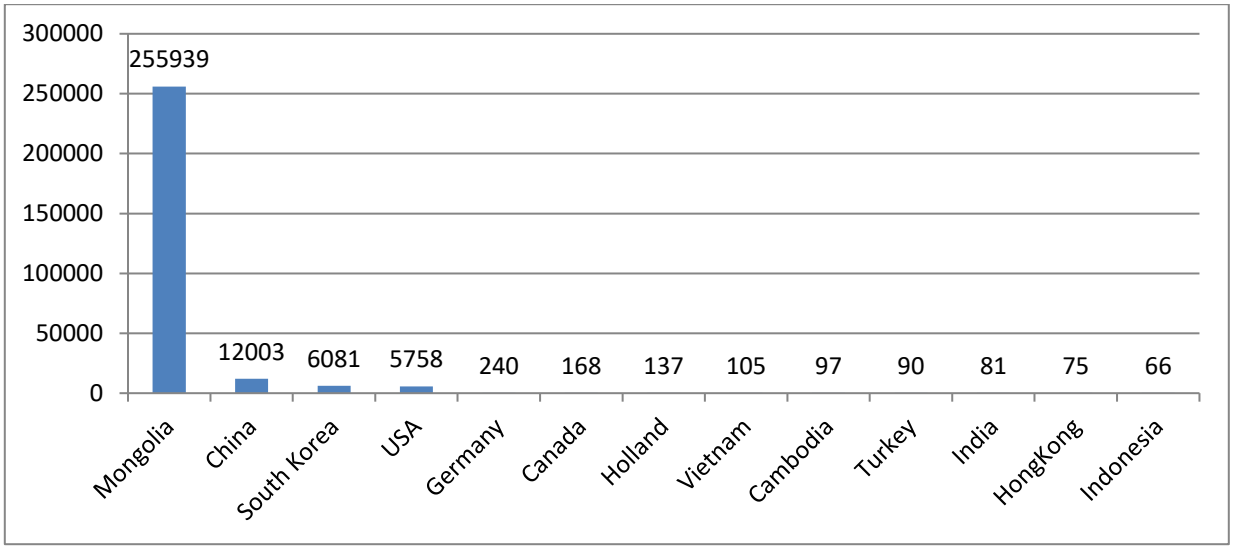
Эрх зүйн асуудлын хувьд Монгол улсад мэдээллийн аюулгүй байдлыг хангахтай холбоотой тусгайлсан хууль хараахан батлагдаагүй байгаагаас энэ чиглэлийн асуудал нь УИХ-ын болон Засгийн газрын тогтоолоор батлагдсан баримт бичгүүдэд тусгасан зүйл, заалтуудын хүрээнд хангагдаж байна гэж хэлж болно. Тухайлбал ЗГ-ын 312, 05, 159-р дугаар тогтоолуудаар мэдээллийн аюулгүй байдлыг хангахтай холбоотой асуудлуудыг журмаар болон тогтоолын заалтаар зохицуулсан байдалтай байна.

Монгол Улсын хэмжээнд кибер халдлагыг илрүүлэх, хариу арга хэмжээ авах чиг үүрэг бүхий ажлыг ТЕГ-ын Төрийн мэдээлэл холбооны газар, Үндэсний дата төв УТҮГ, MON-CERT ТББ, MN-CERT ТББ зэрэг хэд хэдэн байгууллагууд хариуцан ажиллаж байна. Эдгээр байгууллагуудын мэдээллээс үзэхэд Төрийн байгууллагуудын цахим хуудасны сервер рүү халдсан хамгийн сэжигтэй хандалтууд нь Монгол, Хятад, ОХУ, АНУ, Герман улсад бүртгэлтэй хостуудаас хандсан халдлагууд бүртгэгдэж байна. Мөн төрийн мэдээллийн нэгдсэн сүлжээнд халдсан халдлагуудыг харахад гадаадын 40 орчим улсаас зөвхөн 1 хоногт дунджаар 9900 тооны маш өндөр түвшний, 8000 орчим тооны өндөр түвшний цахим халдлага бүртгэгдэж байна. Маш өндөр түвшний халдлагад мэдээлэл хулгайлах зорилготой халдлагууд дийлэнх хувийг эзэлж байна. Үүнээс дүгнэхэд ойролцоо улс орнуудаас халдаж байгаа кибер халдлага хийх байдал өсөн нэмэгдэх хандлагатай байна.

Зураг 1. Маш өндөр түвшний халдлагууд (7 хоногт нийт 150,699 халдлага)



Зураг 2. Өндөр түвшний халдлагууд (7 хоногт нийт 283,628 халдлага)



Эх сурвалж: ТЕГ-ийн Мэдээллийн аюулгүй байдлын газар

Хүснэгт 1. Үндэсний дата төвд халдсан халдлага:

Сар	Халдлагын хандалт (2018 оны 1-р улирлын байдлаар)		
	Нийт	Blocked	Халдсан
1-р сар	1,554,871,515	288,061,785	6,040,464
2-р сар	1,153,032,474	205,384,566	8,499,178
3-р сар	872,177,062	170,229,196	5,068,749
Нийт	3,580,081,051	663,675,547	19,558,391

Хүснэгт 2. Top 10 Email addresses received spam email

№	Spam email хүлээж авсан и-мэйл хаяг	Нийт
1	…@aaib.gov.mn (Нислэг техникийн осол, зөрчлийг шинжлэн шалгах алба)	25,509
2	…@mne.gov.mn (Байгал орчин, аялал жуулчлалын яам)	21,017
3	…@mofa.gov.mn (ХХААХҮЯ)	11,559
4	…@gsmi.mn (Global strategic management institute)	9692
5	…@nso.mn (Үндэсний статистикийн газар)	7041
6	…@audit.gov.mn (Үндэсний аудитын газар)	6305
7	…@procurement.gov.mn (цахим худалдан авах ажиллагааны систем)	4299
8	…@investmongolia.com (Үндэсний хөгжлийн газар)	4006
9	…@khural.uv.gov.mn (Увс аймгийн иргэдийн төлөөлөгчдийн хурал)	3185
10	...@mta.gov.mn (Монголын татварын алба)	3164

Хүснэгт 3. Цахим шуудангийн хаягт халдсан халдлагын төрлүүд

Хувь	Вирус	Тайлбар
49%	*BZ.ZeroHour	Вирусны эсрэг програм хангамжгүй хэрэглэгчдэд ихэвчлэн халдварладаг хортой код
20%	SFP.Rogue.0hr.20170302-1500.Pdflmg	Хуурамч аппликешн
8%	SFP.Malware.25738.AceHeur.Exe	Хортой код
5%	SFP.Malware.25815.ZipHeur.BadExt	Хортой код
5%	SFP.Malware.26959.PdfHeur.DocmJS	Хортой код
4%	SFP.Malware.26959.JsHeur	Хортой код
3%	Win.Trojan.AutoIT-6333854-0	Хэрэглэгчийн өгөгдлийг татаж авдаг хортой код
2%	SFP.Rogue.0hr.20170214-1029.Pdflmg	Хортой код
2%	BN.ZeroHour-fb3c3fea351b537	Вирусны эсрэг програм хангамжгүй хэрэглэгчдэд ихэвчлэн халдварладаг хортой код
2%	Win.Trojan.Agent-6423146-0	Хэрэглэгчийн өгөгдлийг татаж авдаг хортой код

Эх сурвалж: Үндэсний дата төв УТҮГ-ын 2018 оны тайлан

Монгол улсын засгийн газраас 2011 оны 312 дугаар тогтоолын хүрээнд болон МАБ-ын үндэсний хөтөлбөрийн хүрээнд Төрийн байгууллагуудын мэдээллийн системд 2013, 2015 онуудад тус тус мэдээллийн системийн эрсдлийн үнэлгээ хийсэн. Энэхүү ажиллагааг МТШХХГ, ЗГХЭГ, ҮДТ УТҮГ, КАБГ байгууллагууд хамтран 2013 онд 22, 2015 онд 61 төрийн захиргааны байгууллагуудын мэдээллийн системд эрсдэлийн үнэлгээ хийв. Ингэхдээ Мэдээллийн аюулгүй байдлын бодлого, дүрэм, журам, стандарт, хөрөнгө оруулалт, Хүний нөөцийн мэдээллийн аюулгүй байдлын мэдлэг чадвар, Програм хангамжийн эрсдэл, Өгөгдлийн сан, мэдээлэл солилцох эрсдэл, Техник хангамжийн эрсдэл, Сүлжээний эрсдэл, Орчны эрсдэл, Цахим хуудас, цахим шуудангийн аюулгүй байдлын эрсдэл гэсэн 8 шалгуур үзүүлэлтийн 95 асуулгаар үнэлгээг тооцсон. Тагнуулын байгууллагаас 2013-2017 онуудад төрийн байгууллагууд, эрчим хүчний салбарын онц чухал дэд бүтэцтэй байгууллагуудад мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээ хийсэн. Эдгээр эрсдлийн үнэлгээний дүгнэлтүүдээс харахад тус байгууллагуудын удирдлагын цахим мэдээллийн аюулгүй байдлын талаарх ойлголт, дэмжлэг сул, энэхүү чиглэлээр ажилладаг хүний нөөцийн чадвар дутмаг, мэдээллийн технологийн хэрэглээ өндөр ч энэ чиглэлд хэрэгжүүлсэн төсөв, хөтөлбөрүүдэд аюулгүй байдлын асуудлыг орхигдуулсан, мэдээллийн аюулгүй байдлын үндэсний стандартуудыг мөрддөггүй, цахим мэдээллийн аюулгүй байдлын чиглэлээр сургалт, сурталчилгаа хийгддэггүй, цахим халдлагад өртөх өндөр магадлалтай нийтлэг дүр зурагтай байгаа нь тогтоогдсон.

Монгол Улсын Засгийн газрын 2010 оны 141 дүгээр тогтоолоор батлагдаж 2010-2015 оны хооронд хэрэгжсэн “Мэдээллийн аюулгүй байдлыг хангах” үндэсний хөтөлбөрийн хэрэгжилтэд хийсэн дүгнэлтээс үзэхэд тус хөтөлбөрийн хүрээнд нийт 66 арга хэмжээ хэрэгжүүлэхээр төлөвлөгдсөнөөс 12 нь 100%, 12 нь 60-90%, 22 нь 30-50%, үлдсэн 20 арга хэмжээ нь 0-20%-ийн биелэлттэй гарч хөтөлбөрийн нийт үнэлгээ 45,55%-ийн үзүүлэлттэй байна. Энэхүү хөтөлбөрийн хүрээнд хэрэгжүүлсэн ололттой талууд байгаа хэдий ч хэд хэдэн шалтгааны улмаас уг хөтөлбөрийн биелэлт хангалттай үр дүнд хүрээгүй гэж дүгнэгдэж байна. Үүний шалтгаан нь хэрэгжүүлэгч байгууллагуудын хамтын ажиллагаа сул, уялдаа холбоо хангалтгүй, Монгол улсад кибер аюулгүй байдлын хариу арга хэмжээ авах, мэдээллийн аюулгүй байдлыг хангах тогтолцоо байхгүй, Монгол Улс үндэсний аюулгүй байдлыг хангахад чиглэгдсэн зохицуулалт сул зэрэг дутагдлууд байгаа нь манай улсын мэдээллийн систем, мэдээллийн технологийн дэд бүтэц бүхий байгууллагууд кибер халдлагад өртөж болзошгүй эмзэг байдалтай байгаа юм. Түүнчлэн Монгол улс кибер аюулгүй байдлыг хангах тал дээр доогуур эрэмблэгддэг цөөхөн орнуудын нэгт орж байгаа бөгөөд Олон улсын цахилгаан холбооны байгууллагаас гаргадаг дэлхийн кибер аюулгүй байдлын индексээр 2017 оны байдлаар 164 орнуудаас 104-р байранд эрэмбэлэгдэж байна.

Эдгээр асуудлуудыг дүгнэхэд Монгол улсад мэдээллийн аюулгүй байдлыг хангах хууль эрх зүй, бодлого зохицуулалтын орчинг бий болгох, мэдээллийн аюулгүй байдлын эмзэг байдлыг бууруулах, урьчилан сэргийлэх, халдлагад хариу үйлдэл үзүүлэх тогтолцоог сайжруулах, мэдээллийн аюулгүй байдлыг хангах чиглэлээр үйл ажиллагаа явуулдаг дотоод гадаадын төрийн болон төрийн бус байгууллага, иргэний нийгмийн байгууллагуудтай хамтын ажиллагааг өргөжүүлэх болон мэдээллийн аюулгүй байдлын мэргэшсэн мэргэжилтэн бэлтгэж хүний нөөцийг чадавхижуулах, иргэдийн мэдлэгийг дээшлүүлэх, интернетийн зохистой хэрэглээг төлөвшүүлэх зэрэг асуудлуудыг шийдвэрлэх зайлшгүй шаардлагууд бий болоод байгаа юм.

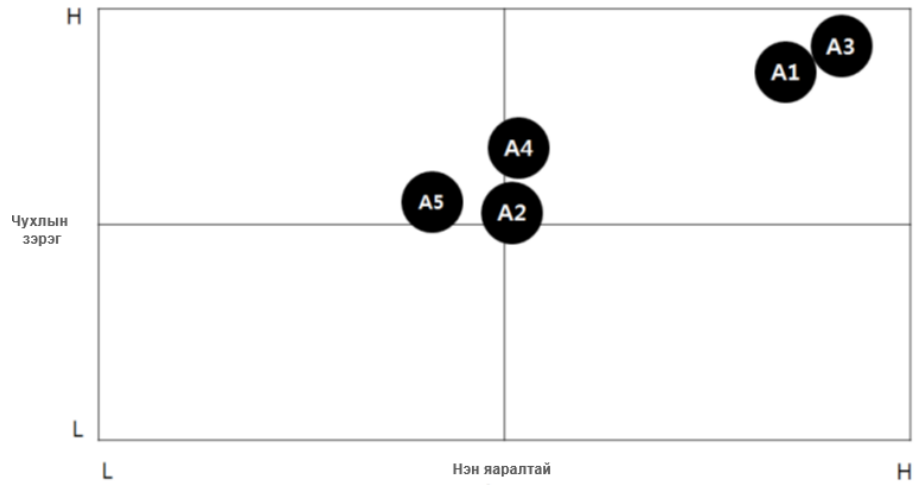
II. Монгол Улсын мэдээллийн аюулгүй байдлын тогтолцоог боловсронгуй болгоход шаардлагатай хүчин зүйлсийг тодорхойлох судалгаа

Харилцаа холбоо мэдээллийн технологийн газар нь үйл ажиллагааныхаа чиг үүргийн хүрээнд мэдээллийн аюулгүй байдлыг хангах чиглэлээр бодлого боловсруулж, түүний хэрэгжилтийг ханган ажиллаж байна. Тус газраас 2017 онд Цахим мэдээллийн аюулгүй байдлын тухай хуулийн төсөл боловсруулах ажлын хүрээнд үндэсний мэдээллийн аюулгүй байдлын тогтолцоог бий болгож, халдлагад хариу үйлдэл үзүүлэх чадавхийг бэхжүүлэх зорилго бүхий судалгааны төсөл хэрэгжүүлсэн.

Уг төслийн хүрээнд бид үндэсний хэмжээнд мэдээллийн аюулгүй байдлыг хангах, Монгол улсын мэдээллийн аюулгүй байдлын тогтолцоог боловсронгуй болгоход чухал ач холбогдолтой болон яаралтай хэрэгжүүлэх шаардлагатай хүчин зүйлсийг тодорхойлох зорилгоор энэ чиглэлд шийдвэр гаргагчид, асуудал гардан хариуцсан инженер, мэргэжилтэн, эрдэмтэн судлаачдын дунд судалгаа явуулсан. Ингэхдээ судалгааны асуулгыг Бүтэц/ Хүний нөөц, МХХ-ны дэд бүтэц, Хууль эрх зүйн орчин ба стандарт, болон МТ-ийн аюулгүй байдал ба аудит гэсэн 4 үндсэн чиглэлд ангилж, чиглэл бүрт нарийвчилсан үнэлгээний асуултууд дэвшүүлэн эдгээр үнэлгээний асуултуудаар асуудлын яаралтай байдал болон ач холбогдлыг 5-1 хүртэлх (“5”чухал биш – “1” чухал) эрэмбээр дүгнэх байдлаар тооцсон.

Мэдээллийн аюулгүй байдлын тогтолцоонд чухал ач холбогдолтой ба яаралтай байдлын шаардлагуудыг тодорхойлох үнэлгээний асуудлуудыг дараах байдлаар шинжилсэн болно:

2.1 Бүтэц/хүний нөөц



Зураг 3. Бүтэц/Хүний нөөц - Шаардлагатай хүчин зүйлсын судалгааны үр дүн

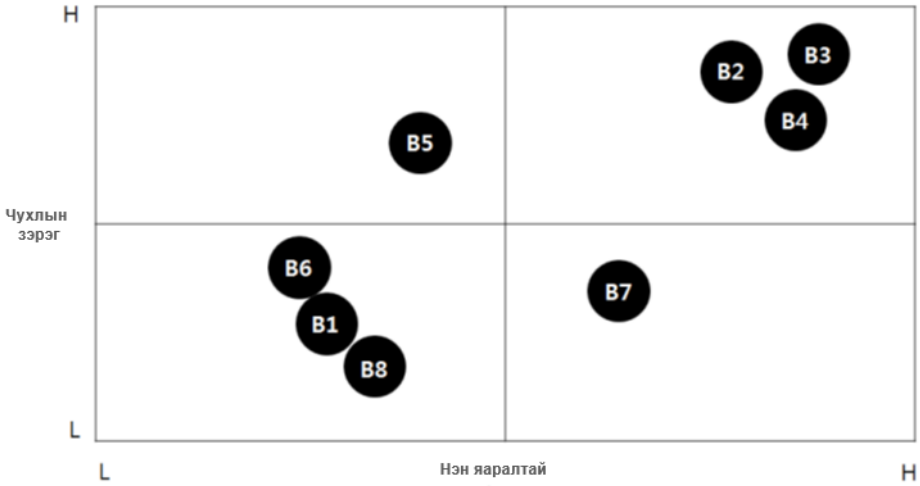
A1 : МАБ-ын үндэсний төв (CERT) бий болгох
A2 : Шинжээч ажилд авах,
A3 : Боловсрол, сургалт
A4 : Төр, хувийн хэвшлийн түншлэл
A5 : Үйл ажиллагааны гарын авлага гаргах

Цахим мэдээллийн аюулгүй байдлыг хангах тогтолцооны“Бүтэц, хүний нөөц”-ийн чиглэлд шаардлагатай хүчин зүйлсийн анализ үр дүнг Зураг 1-ээр харуулж байна. Судалгаанд оролцогчид энэ чиглэлд “Боловсол, сургалт” болон “Мэдээллийн аюулгүй байдлын үндэсний төв (CERT) бий болгох” хүчин зүйлсийг нэн чухал бөгөөд яаралтай гэж тодорхойлж байна. Уг судалгааны үр дүнгээс үзэхэд Монгол улсын

мэдээллийн аюулгүй байдлыг хангах чиг үүрэгбүхий оролцогчид МУ-д Кибер аюулгүй байдлын асуудлаар мэргэшсэн шинжээчдийг сургах боловсролын болон сургалтын хөтөлбөрүүдийг зохион байгуулах, мөн кибер халдлага, аюул заналд хариу үйлдэл үзүүлэх хяналтын цамхаг буюу үндэсний хэмжээний CERT байгуулах нь нэн чухал юм гэж үзэж байна.

Үүнээс гадна бусад үнэлгээний үзүүлэлтүүд болох “Шинжээч ажилд авах”, “Төр, хувийн хэвшлийн түншлэл” болон “Үйл ажиллагааны гарын авлага гаргах” зэргийг чухалд тооцсон боловч “Боловсрол, сургалт” ба “МАБ-ын үндэсний төв (CERT) бий болгох” үзүүлэлттэй харьцуулахад яаралтай байдал нь харьцангүй бага байна.

2.2 Мэдээлэл харилцаа холбооны дэд бүтэц



Зураг 4. МХХ-ны дэд бүтэц - Шаардлагатай хүчин зүйлсын судалгааны үр дүн

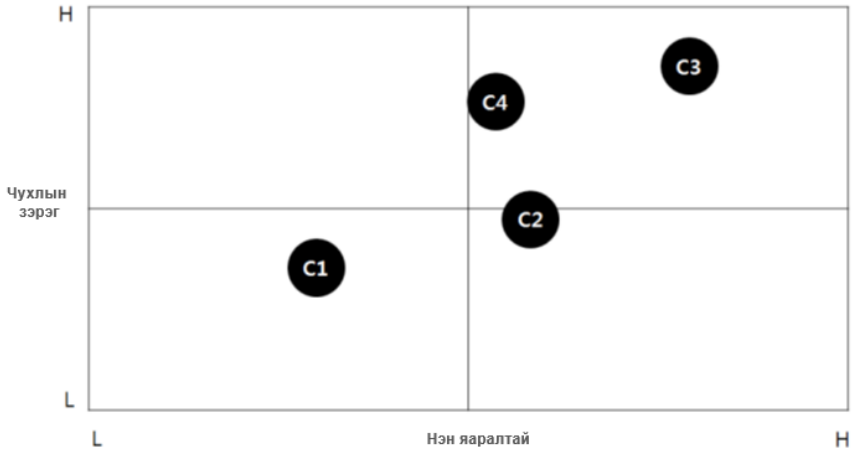
B1 :Үндэсний (CERT) төвд зориулсан барилга шинээр барих
B2 :Хяналтын болон мэдээллэх хэрэгсэл
B3 :Үндэсний хэмжээнд кибер халдлагыг илрүүлэх систем
B4 :Мэдээллийн аюулгүй байдлын тоног төхөөрөмж нэвтрүүлэх
B5 : Анализ хийх систем
B6 :Мобайл/веб хөгжүүлэлт
B7 :Төрийн мэдээллийн аюулгүй байдлын ПХ
B8 :Сүлжээний утастай/утасгүй дэд бүтэц

Цахим мэдээллийн аюулгүй байдлыг хангах тогтолцооны “Мэдээлэл харилцаа холбооны дэд бүтэц”-ийн чиглэлд шаардлагатай хүчин зүйлсийн анализ үр дүнг Зураг 2 дээр харуулж байна. “Мэдээлэл харилцаа холбооны дэд бүтэц”-ийн хувьд “Үндэсний хэмжээний кибер халдлагыг илрүүлэх систем”, “Хяналтын болон мэдээллэх хэрэгсэл”, мөн “Мэдээллийн аюулгүй байдлын тоног төхөөрөмж нэвтрүүлэх” асуудлууд нэн чухал бөгөөд яаралтайд тооцогдсон байна. Үүнээс үзэхэд

судалгаанд оролцогч талууд “Бүтэц/хүний нөөц”-ийн чиглэлд хийсэн судалгаа дээр авч үзсэн шиг үндэсний хэмжээнд кибер халдлага илрүүлэх систем хэрэгтэй гэж үзсэн бөгөөд үүнтэй зэрэгцэн кибер халдлагын хяналтын болон мэдээллэх хэрэгсэл, мэдээллйн аюулгүй байдлын тоног төхөөрөмж яаралтай бөгөөд нэн чухал гэж дүгнэж байна.

Кибер халдлагад анализ хийх систем чухал боловч яаралтай нэвтрүүлэх хүчин зүйлд тооцогдоогүй байна. “Төрийн мэдээллийн аюулгүй байдлын ПХ”-ын хувьд чухал шаардлагатай гэхээс илүү нэн яаралтай хүчин зүйл гэж үзсэн байна. Үүнээс гадна “Мобайл/вэб хөгжүүлэлт”, “Үндэсний (CERT) төвд зориулсан барилга шинээр барих” болон “Сүлжээний утастай/утасгүй дэд бүтэц” –ийн асуудлуудын чухал шаардлагатай бөгөөд яаралтай байдал бусад хүчин зүйлстэй харьцуулахад харьцангуй багаар дүгнэгдсэн байна.

2.3 Хууль эрх зүйн орчин ба стандарт



Зураг 5. Хууль эрх зүйн орчин ба стандарт - Шаардлагатай хүчин зүйлсын судалгааны үр дүн.

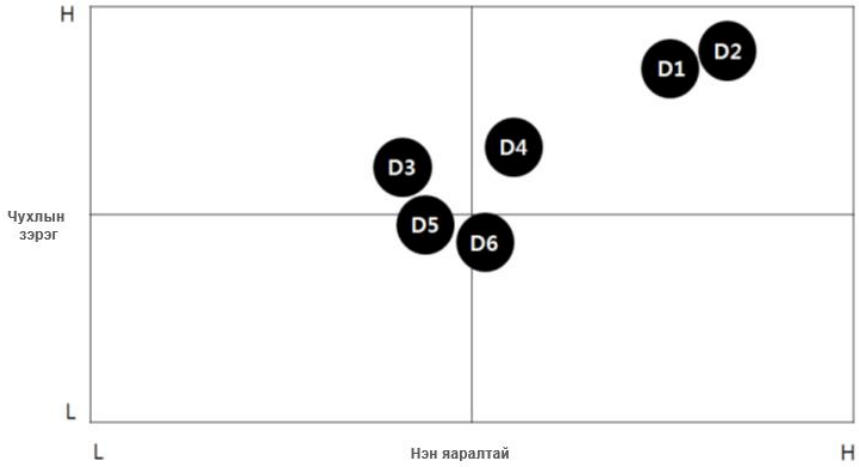
C1 : Тэргүүлэгч орны сайн жишиг
C2 :Мэдээллийн аюулгүй байдлын стандартынудирдамж
C3 : Хууль боловсруулж, батлуулах
C4 : Гадны тэргүүлэгч байгууллагатай хамтран ажиллах

Зураг 3 дээр Цахим мэдээллийн аюулгүй байдлыг хангах тогтолцооны “Хууль эрх зүйн орчин ба стандарт”-ийн чиглэлд хэрэгжүүлэх шаардлагатай хүчин зүйлсийн анализ үр дүнг харуулж байна. Эндээс үзэхэд судалгаанд оролцогчид кибер аюулгүй байдлыг хангах тухай хууль боловсруулж батлуулах асуудал нэн чухал бөгөөд яаралтай хэрэгжүүлэх хүчин зүйл гэж дүгнэсэн байна.

Үүний дараагаар “Гадны тэргүүлэгч байгууллагатай хамтран ажиллах” явдлыг чухалд тооцож байна. Мөн “мэдээллийн аюулгүй байдлын стандартын удирдамж”-ийн хувьд чухал хүчин зүйлд тооцогдсон боловч “гадны тэргүүлэгч байгууллагатай

хамтран ажиллах” асуудлыг бодвол харьцангуй доогуур үзүүлэлттэй дүгнэгдсэн байна. Энэ хэсэгт “Тэргүүлэгч орны сайн жишиг” нэвтрүүлэх асуудал бусад үзүүлэлттэй харьцуулахад хамгийн багаар үнэлэгдсэн байна.

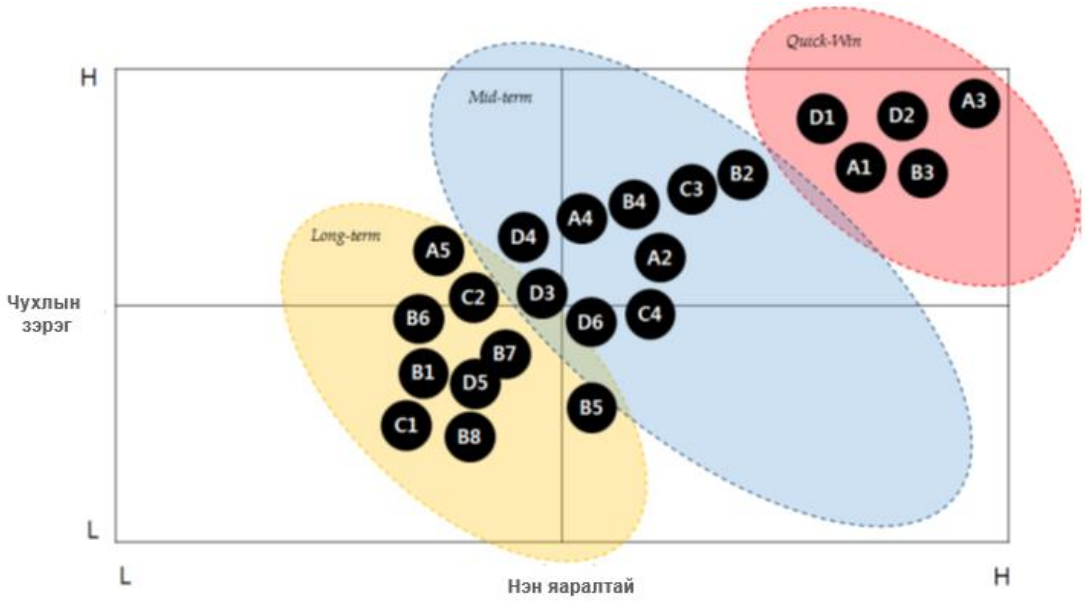
2.4 **МТ-ын аюулгүй байдал ба аудит**



Зураг 6. МТ-ын аюулгүй байдал ба аудит - Шаардлагатай хүчин зүйлсын судалгааны үр дүн.

D1 :Кибер халдлагын мэдээлэл хуваалцах систем
D2 :Үндэсний суурь сүлжээний аюулгүй байдлын хяналтын систем
D3 : IT аудит нэвтрүүлэх
D4 : Эрсдлийн үнэлгээний системийн сайжруулалт
D5 : SLA удирдамж
D6 :Хувийн хэвшил дэх сургалтын хөтөлбөр

Цахим мэдээллийн аюулгүй байдлыг хангах тогтолцооны “МТ-ын аюулгүй байдал/аудит”-ийн чиглэлд хэрэгжүүлэх шаардлагатай хүчин зүйлсийн анализ үр дүнг Зураг 4 дээр харуулж байна.“МТ-ын аюулгүй байдал/аудит”-ийн хувьд “Кибер халдлагын мэдээлэл хуваалцах систем” болон “Үндэсний суурь сүлжээний аюулгүй байдлын хяналтын систем”-ийн яаралтай ба чухал байдлын үнэлгээ хамгийн өндөр дүгнэгдсэн байна. Эндээс дүгнэхэд судалгаанд хамрагдсан хүмүүс үндэсний суурь сүлжээний аюулгүй, найдвартай байдлыг хангах болон кибер халдлагын талаарх мэдээлэл солилцооны систем бий болгох явдал нь нэн чухал шаардлагатай хүчин зүйлс гэж үзэж байна. Үүний дараагаар “Эрсдлийн үнэлгээний системд сайжруулалт хийх” явдал нь чухал бөгөөд яаралтай хүчин зүйлд тооцогдож байгаа бол “IT аудит нэвтрүүлэх” болон “SLA удирдамж” хэрэгжүүлэх явдал чухалд тооцогдож байгаа боловч яаралтай хэрэгжүүлэх шаардлагатай гэж үзээгүй байна. Харин “хувийн хэвшилд зориулсан боловсролын хөтөлбөр, сургалт зохион байгуулах асуудал дундаж үзүүлэлттэй байна.



Зураг 7. Шаардлагатай хүчин зүйлсийн нэгдсэн судалгааны үр дүн

Үндэсний хэмжээнд мэдээллийн аюулгүй байдлыг хангах, Монгол улсын мэдээллийн аюулгүй байдлын тогтолцоог боловсронгуй болгоход чухал ач холбогдолтой болон нэн яаралтай хэрэгжүүлэх шаардлагатай хүчин зүйлсийг тодорхойлох судалгаанд оролцсон хүмүүсийн нэгдсэн дүн шинжилгээний үр дүнг зураг 5 дээр үзүүлэв.

Нийт 23 хүчин зүйлсийн нэн чухал болон яаралтайг тодорхойлох нэгдсэн графикаас харахад “МАБ-ын үндэсний төв (CERT) бий болгох” (A1), “Боловсрол, сургалт” (A3),“Үндэсний хэмжээнд кибер халдлагыг илрүүлэх систем” (B3),“Кибер халдлагын мэдээлэл хуваалцах систем” (D1),“Үндэсний суурь сүлжээний аюулгүй байдлын хяналтын систем” (D2) хүчин зүйлсийн хэрэгцээ шаардлага хамгийн өндөр буюу эдгээр асуудлыг богино хугацаанд хэрэгжүүлэх шаардлагатай болох нь харагдаж байна.

Үүний дараагаар Мэдээллийн аюулгүй байдлын тоног төхөөрөмж (B4), Төр, хувийн хэвшлийн түншлэл (A4), Шинжээч ажилд авах (A2), Эрсдлийн үнэлгээний системийн сайжруулалт (D4), Гадны тэргүүлэгч байгууллагатай хамтран ажиллах (C4), IT аудит нэвтрүүлэх (D3),Хувийн хэвшил дэх сургалтын хөтөлбөр (D6) хүчин зүйлсийн нэн чухал болон яаралтай байдал нь дундаж хэмжээнд дүгнэгдсэн буюу эдгээр үйл ажиллагааг дунд хугацаанд хэрэгжүүлж болохоор байна.

Эцэст нь Үйл ажиллагааны гарын авлага гаргах(A5), Мэдээллийн аюулгүй байдлын стандартынудирдамж (C2), Анализ хийх систем (B5), Төрийн мэдээллийн аюулгүй байдлын ПХ (B7), SLA удирдамж (D5), Мобайл/веб хөгжүүлэлт (B6), Үндэсний (CERT) төвд зориулсан барилга шинээр барих (B1), Сүлжээний утастай/утасгүй дэд бүтэц(B8), Тэргүүлэгч орны сайн жишиг (C1) гэх хүчин зүйлсийн нэн чухал болон яаралтай байдал нь хамгийн багаар дүгнэгдэж байгаа бөгөөд эдгээр үйл ажиллагааг урт хугацаанд хэрэгжүүлэхээр харагдаж байна.

МУ-ын кибер аюулгүй байдлыг хангах чиг үүрэг бүхий талуудын дүгнэсэн

кибер аюулгүй байдлыг хангахад нэн чухал бөгөөд яаралтай хэрэгжүүлэх шаардлагатай хүчин зүйлсийг тодорхойлох судалгааны үр дүнд ерөнхийдөө мэдээллийн аюулгүй байдлыг хангах тогтолцоог бий болгож цахим мэдээллийн аюулгүй байдлыг үндэсний хэмжээнд хангах төв бий болгох, түүнийг ажиллуулах мэргэжлийн боловсон хүчинг бэлтгэх талаар арга хэмжээ авах явдал нэн чухал шаардлагатай гэж дүгнэгдэж байна.

III. Дүгнэлт

Монгол улсад мэдээллийн аюулгүй байдлын тогтолцоог бий болгож, халдлагад хариу үйлдэл үзүүлэх чадавхийг бэхжүүлэх зорилго бүхий судалгааны төслийн үр дүнг дараах байдлаар дүгнэж байна.

Нэгдүгээрт, Монгол улс кибер аюулгүй байдлыг хангах чиглэлээр хүчин чармайлт гаргаж буй хэдий ч дотоодоос болон гадаад улс орноос (БНХАУ, ОХУ, БНСУ г.м.) Монгол руу чиглэсэн кибер халдлагын тоо өсөн нэмэгдэх чиг хандлагатай байна. Үүний зэрэгцээ кибер орон зайд үүсэх үндэстэн хоорондын зөрчилдөөний улмаас кибер тэмцэл гүнзгийрч байна. Монгол улсын хувьд кибер халдлагад хариу арга хэмжээ авах чиг үүргийг хэд хэдэн субьектууд хариуцан ажиллаж байгаа боловч хоорондын уялдаа холбоо сул, хамтран ажиллах ажлын процесс тодорхой бус, мөн Монгол Улсын олон улс дахь кибер аюулгүй байдлын индекс (GCI) 2017 оны байдлаар 0.228 буюу 164 орноос 103 дугаарт эрэмблэгдэж байгаа зэргээс харахад энэ нөхцөлийг өөрчилж шинэчлэх хэрэгтэй. Тиймээс Монгол улсад кибер аюулгүй байдлыг хангах чиг үүрэг бүхий үндэсний хэмжээний төв (CERT) байгуулж кибер халдлагап хариу үйлдэл үзүүлэх чадавхийг бэхжүүлэх зайлшгүй шаардлага бий болоод байна.

Хоёрдугаарт, дэлхий дахинд кибер халдлагын төрлүүд улам боловсронгуй, ухаалаг болохын зэрэгцээ зорилтотхалдлагын тоо нэмэгдэж кибер аюул заналын хүрээ өргөжин тэлж байна. Мөн түүнчлэн Монгол Улсын мэдээлэл харилцаа холбооны үйлчилгээ хэрэглэгчдийн тоо жил ирэх тусам нэмэгдэхийн хирээр кибер аюул заналд өртөх эрсдэл үүсч, түүнээс үүдэх хор хохирол өсөн нэмэгдэх магадлалтай байна. Тиймээс учирч болзошгүй халдлагын эрсдлээс урьдчилан сэргийлэх, аюулгүй байдлыг хангах програм, техник хангамж нэвтрүүлэх, түүнийг ажиллуулах кибер аюулгүй байдлын нарын мэргэжлийн боловсон хүчинг бэлтгэх арга хэмжээ авах шаардлагатай байна.

Гуравдугаарт, цахим мэдээллийн аюулгүй байдлыг хангах чиг үүрэг бүхий төрийн болон төрийн бус байгууллага, аж ахуй нэгжүүд кибер халдлагын талаарх мэдээллийг холбогдох субьектууд хооронд түргэн шуурхай хуваалцаж, хамтран хариу арга хэмжээг авах зорилго бүхий кибер халдлагын мэдээлэл хуваалцах системийг нэвтрүүлэх шаардлагатай бөгөөд цахим мэдээллийн аюулгүй байдлыг хангах чиглэлээр бүс нутгийн болон олон улсын хэмжээнд хамтын ажиллагааг

хөгжүүлэх шаардлагатай.

Эцэст нь, Монгол Улсад үндэсний мэдээллийн аюулгүй байдлыг хангах тогтолцоог бий болгож, үүнд оролцогч талуудыг бүрэн эрх, чиг үүргийг тодорхойлон хуульчилж өгөх зүй ёсны шаардлага бий болоод байна.

Иймд дээрх асуудлуудыг шийдвэрлэхийн тулд Монгол улсад мэдээллийн аюулгүй байдлыг хангах хууль эрх зүй, бодлого зохицуулалтын орчинг бий болгох, мэдээллийн аюулгүй байдлын эмзэг байдлыг бууруулах, урьчилан сэргийлэх, халдлагад хариу үйлдэл үзүүлэх тогтолцоог сайжруулах, мэдээллийн аюулгүй байдлыг хангах чиглэлээр үйл ажиллагаа явуулдаг дотоод гадаадын төрийн болон төрийн бус байгууллага, иргэний нийгмийн байгууллагуудтай хамтын ажиллагааг өргөжүүлэх болон мэдээллийн аюулгүй байдлын мэргэшсэн мэргэжилтэн бэлтгэж хүний нөөцийг чадавхижуулах, иргэдийн мэдлэгийг дээшлүүлэх, зохистой хэрэглээг төлөвшүүлэх чиглэлүүдээр тодорхой төсөл, арга хэмжээг хэрэгжүүлэхээр Мэдээллийн аюулгүй байдлыг хангах үндэсний хөтөлбөрийн төсөлд тусгахыг зорилоо.

Ашигласан материалын жагсаалт:

- “Монгол улсад CERT-ийн шинэчлэл хийх болон МТ-ийн аудитын тогтолцоог нэвтрүүлэх ТЭЗҮ” төслийн тайлан
- “Мэдээллийн аюулгүй байдлын үндэсний хөтөлбөр 2010-2015” дүгнэлт тайлан
- “ДЦХБ, Олон Улсын кибер аюулгүй байдлын индекс - 2017”
- Үндэсний дата төв УТҮГ-ын 2017 оны үйл ажиллагааны жилийн эцсийн тайлан
- ХХМТ-ийн салбарын “Цагаан ном - 2017”,ХХМТГ.
- http://legalinfo.mn
- http://cita.gov.mn
- http://crc.gov.mn

~~oOo~~