МОНГОЛ УЛСЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ

Д.Ариужин
ХСИС-ийн Цагдаагийн сургуулийн ЦЭЗТ-ийн
ахлах багш, цагдаагийн ахлах дэслэгч

Мэдээллийн аюулгүй байдлыг зөвхөн төрийн байгууллага, Монгол Улсын дотоодын асуудлын хэмжээнд ойлгож болохгүй. Манай орны интернэтийн гадаад урсгалын хэмжээ 2010 оноос даруй 80 дахин нэмэгдсэн байна. Энэ нь гадаадаас интернэтээр дамжин ирэх халдлага, хортой код бидэнд нөлөөлөх эрсдэлийг 80 дахин нэмэгдүүлсэн гэж ойлгож болно.

Түүнчлэн Монгол Улсын дотоодын интернэтийн харилцан холболтын дэд бүтцийг байгуулаад нилээн хэдэн жил болж байна. Гэвч сүүлийн 5 жилийн хугацаанд ямар хэмжээний мэдээллийг гадагш алдсан, хортой код, халдлагын уршгаар хэдий хэмжээний хөрөнгийн алдагдал хүлээснийг нарийн тогтоох эрх зүй, технологи, аргачлал бий болоогүй байна.

Технологийн дэвшлээр манай орны хүүхэд залуус Social networking буюу нийгмийн сүлжээний вэб програм хангамжийг (тухайлбал facebook, myspace, biznetwork, twitter) ихээхэн ашиглах болсонтой холбоотой хувийн нууцаа алдах, зүй бус зүйлд уруу татагдах явдал газар авч байна.

Засгийн газар, Харилцаа холбооны зохицуулах хорооноос интернэтийн агуулга, вэб хуудсын агуулгад зохицуулалт, хяналтыг хийж байгаа боловч гадаад улсад байрлах зүй бус агуулгатай тэмцэж чадахгүй байна. Мэдээлэл, шуудан, харилцаа холбоо, технологийн газар, Кибер довтолгоонтой тэмцэх баг хамтран 2008 оноос хойш интернэтийн аюулгүй байдлын судалгааг хийж байна. 2015 оны сүүлийн байдлаар зөвхөн нэг интернэтийн үйлчилгээ үзүүлэгчийн сүлжээгээр 500000 гаруй халдлага, хортой кодын дамжиж байгааг тогтоожээ.

Дээрхи халдлага, хортой кодын 60 гаруй хувийг АНУ, Европын холбооны улсууд, 25 орчим хувийг БНХАУ, 15 орчим хувийг бусад орнуудаас илгээж байна. Энэ нь дан ганц манай улсад мэдээллийн аюулгүй байдлын халдлага, хортой кодын идэвхижил ихсэж байгаа бус дэлхий даяр нэмэгдэж байгаа талаар Олон улсын цахилгаан холбооны байгууллага (ITU) сануулж байна.

Дэлхийн хэмжээнд кибер гэмт хэргийн нөхцөл байдал улам бүр хүнд болж зохион байгуулалт бүхий үндэстэн дамнасан гэмт хэргийн бүлэглэл мэдээлэл, харилцаа холбооны технологийг гэмт үйлдэлдээ ашиглахын зэрэгцээ кибер терроризмын эрсдэл улам бүр нэмэгдсээр байна.

Түүнчлэн томоохон улс орнууд кибер дайн, кибер тагнуулын үйл ажиллагааг идэвхитэй явуулах болсон бөгөөд уг аюул заналаас хамгаалах, дайран довтлох шинэ технологи, хүний нөөцийг бэлтгэхэд их хэмжээний хөрөнгийг зарцуулж байна. Монгол Улсын 2010 оны Улсын төсвийн тухай хуулиар нийт 15 гаруй тэрбум төгрөгийн хөрөнгө оруулалтыг мэдээлэл, харилцаа холбооны чиглэлд хийсэн хэдий ч дээрхи төсвийн 3 хувийг мэдээллийн аюулгүй байдлын хангах ажилд зарцуулсан байгаа нь “Мэдээллийн аюулгүй байдлыг хангах үндэсний хөтөлбөр”-ийн 2010 онд санхүүжүүлэхээр тусгагдсан ажлын 10 хүрэхгүй хувьтай тэнцэж байна. 2015 оны байдлаар мэдээллийн аюулгүй байдлыг хангах

чиглэлээр төсөвт суусан мөнгө 2010 оныхоос 60 хувь буурсан үзүүлэлттэй байгаа нь мэдээллийн аюулгүй байдалд өртөх нөхцөл боломжийг төр засаг, орон нутгийн байгууллагууд олгож байна.

Төрийн байгууллага Улсын нууц, байгууллагын нууц, иргэний хувийн нууцтай холбоотой их хэмжээний мэдээллийн цаасан болон цахим хэлбэрээр хадгалан, боловсруулдаг бөгөөд цаасан мэдээллийн нууцыг хангах асуудлаар хуульд нийцүүлэн боловсруулсан журмыг мөрдөж байна. Харин цахим хэлбэрт буй төрөл бүрийн нууц мэдээллийг хэрхэн боловсруулах, хадгалах, хамгаалах, ашиглах, устгахтай холбоотой эрх зүйн, техникийн шийдлийг өнөөг хүртэл хэрэглээнд нэвтрүүлээгүй байна.

Тухайлбал, Боловсрол соёл шинжлэх ухааны яам, Цагдаагийн ерөнхий газар, Хууль зүй, дотоод хэргийн яам, Шүүхийн шийдвэр гүйцэтгэх ерөнхий газар програм хангамжийг лицензжүүлэх асуудал шийдвэрлэгддэггүй, зориулалтын серверийн өрөөгүй, байгууллагын хэмжээнд мэдээллийн технологи хариуцсан зөвхөн нэг ажилтантай, удирдлага мэдээллийн технологи, мэдээллийн аюулгүй байдалд ач холбогдолгүй ханддаг нь харагдаж байна.

Төрийн 67 байгууллагуудад мэдээллийн аюулгүй байдлын талаар 2010-2017онд хийгдсэн судалгаанаас иш татвал:

- Мэдээллийн системийн тоног төхөөрөмжийн нийт гэмтлийн 35% нь цахилгааны хэлбэлзэл, доголдлоос үүдэлтэй ба систем унах, хатуу диск эвдрэх, тэжээлийн блок болон шилэн кабелийн хөрвүүлэгч шатах хохирол учруулж байна.
- Нийт байгууллагуудын 36% нь вирусны эсрэг програмгүй, 50% нь firewall /галт хана/ ашигладаггүй байна.
- Сүлжээний халдлага эсэргүүцэх системийг нийт байгууллагын 7% нь ашиглаж байна. Үлдсэн 62 төрийн захиргааны байгууллагууд мэдээллийн аюулгүй байдал хэрхэн зөрчигдөж байгаа талаар огт мэдээлэлгүй байна.
- Нийт байгууллагуудын 96% нь сервер, компьютер, сүлжээний төхөөрөмж, бусад техник хэрэгслээ даатгуулаагүй.
- Судалгаанд хамрагдсан байгууллагуудын 75% нь сүлжээ, системийн цоорхойгоо шалгаж скан хийдэггүй, 40% нь зориулалтын серверийн өрөөгүй байна.
- Судалгаанд хамрагдсан байгууллагуудын 98% нь програм хангамжийн албан ёснылицензгүй ашиглагдаж байна. Зөвхөн сервер болон хэрэглээний компьютерийн антивирусны програмууд л лицензтэй байна.
- Судалгаанд хамрагдсан төрийн байгууллагуудын ихэнх хувь нь мэдээллийн аюулгүй байдлын талаар ойлголтгүй, тодорхой ажил эхлүүлээгүй, мэдээллийн системийг онцгой нөхцөлд сэргээх, кибер довтолгоонтой тэмцэх, мэдээллийн аюулгүй байдлын бодлого, стандартыг ажилтнууддаа танилцуулж мөрдүүлэх, сургалт зохион байгуулах зэрэг ажлууд хийдэггүй. Мөн хүний нөөцтэй холбоотой аюулгүй байдлын удирдлага байхгүй.
- Эд хөрөнгийн ангилал хийгдээгүй, хамгаалагдах эд хөрөнгийг нарийн тодруулаагүй. Хандалтын удирдлага сул, мэдээллийн систем суурилуулах, үйлчилгээ хийх удирдлага тодорхой хэмжээнд хэрэгжсэн. Мэдээллийн аюулгүй байдлын будлианы удирдлага байхгүй. Тасралтгүй ажиллагаа, сэргээн босох удирдлага байхгүй байсан нь мэдээллийн аюулгүй байдал хангалтгүй байна.
- Байгууллагуудын тал хувь нь нууцын асуудлыг зөвхөн Төрийн нууцын хуулиар зохицуулдаг, хуулинд заасан нууцлалд хамаарах мэдээллээс бусад мэдээллийг ангилаагүй, үнэлээгүй, үнэ цэнийг тогтоогоогүй, хандах эрхтэй холбоогүй, дийлэнх хувь нь

Засгийн газрын тогтоолд заасан Кирилл ба Монгол үсгийн нэгдсэн кодын стандартыг мөрдөж ажиллаж байна.

- Хууль бус нэвтрэлтийг илрүүлэх бодлого, журам, механизм, техник хангамж, програм хангамж байхгүй учир илрүүлэх боломжгүй. Хууль бус нэвтрэлтийг илрүүлж чадахгүй учир мэдээлэл алдагдах, халдлага үйлдэх эрсдэл өндөр байна.
- Судалгаанд хамрагдсан байгууллагуудын 13 хувьд нь цахим хуудас халдлагад өртөж байсан бөгөөд халдлага хаанаас, хэзээ хийгдсэн талаар ямар ч мэдээлэл байхгүй байна.