



Security
Solution &
Service



Үндэсний Аюулгүй Байдлын Үзэл баримтлал болон мэдээллийн аюулгүй байдал

Т.Халтар

“ЗС” ХХК-ийн зөвлөх

Доктор, профессор

khaltar@sssmn.com

Яагаад?



- Анх ҮАБҮБ батлагдаж байх 1994 онд нөхцөл байдал огт өөр байсан
- Өнгөрсөн 16 жилийн дотор нийгмийн бүх амьдралд Мэдээлэл холбооны технологи хүчтэй нэвтэрсэн.
- Түүнийг хууль бус зорилгод ашиглах хэдэн түмэн арга бий болсон
- Цахим засаг, цахим бизнес, цахим худалдаа, цахим боловсрол, цахим эмнэлэг, цахим шүүх, цахим иргэн, цахим байгууллага г.м.
- Монгол улсад мэдээллийн аюулгүй байдлын ойлголт маш муу, төрийн стратеги, бодлого бүрэн боловсруулагдаагүй, ихэнх байгууллагуудад мэдээллийн аюулгүй байдлыг хангах цогц удирдлага байхгүй.
- Энэ бүхэн ҮАБ-д эрсдэл учруулж эхэлсэн

Яагаад?



- Бүх зүйл МХТ-д суурилах болсон
- Онлайн хэлцэл, гүйлгээ, гэрээ олширч, мэдээллийн урсгал эрс нэмэгдсэн.
- Хүн төрөлхтөний хөгжил дэвшил МХТ-оос хамааралтай болсон.
- Эдийн засгийн хөгжлийн хөдөлгүүр нь МХТ
- Мэдээлэл, өгөгдөл, мэдээллийн технологи, мэдээллийн систем, сүлжээ нь аливаа байгууллагын маш чухал, үнэт эд хөрөнгө.
- Гэмт халдлага, үйлдэл, зөрчил эрс нэмэгдэж байна.
- Мэдээллийн аюулгүй байдал нь нэг хувь хүн, нэг байгууллага, нэг улс төдийгүй дэлхийн хамтын нийгэмлэгийн чухал асуудал болон хувирсан.

Яагаад?



- МАБ-ын Мөн чанарыг мэддэггүй,
- Өнгөцхөн ойлголт дээрээ тулгуурладаг,
- Удирдах ажилтнууд болон ихэнх хэрэглэгчид түүний ач холбогдолыг мэдэхгүй,
- Үл тоомсорлодог,
- Хөрөнгө мөнгө зарцуулдаггүй
- МАБ огт хангагдаагүй, мэдээлэл гадагш урсаж байгаа, сүлжээ, вебүүд цоорхой гэсэн магадлалтай
- МАБ-ын довтолгооныг зүгээр нэг танхай хакер төдийгүй өрсөлдөгч байгууллагууд, тусгай албад гүйцэтгэдэг

Яагаад?



- МХТ хүчтэй нэвтэрсний улмаас уламжлалт цаасан баримт бичгийн нууцлал, хамгаалалт шаардлага хангахаа больсон
- Зэвсэгт хүчин, цагдаа, тагнуул, онц байдал, гамшгийн удирдлага, тогтолцоо байдагтай нэгэн адил мэдээллийн аюулгүй байдал, түүнийг хэрэгжүүлдэг тогтолцоо, байгууллагууд байх зайлшгүй шаардлагатай.
- Байгууллага бүр МАБ-ын удирдлагатай болсон.
- МАБ- нь Програм-техникийн асуудал байхаа больж улам бүр нарийн төвөгтэй, **захиргаа-удирдлагын** асуудал болон хувирсан.
- Мэдээллийн нөлөөлөл, хор хөнөөл эрс нэмэгдсэн, Тараах суваг олширсон



Аюулгүй байдалд орж буй өөрчлөлтүүд

- Улсуудын хөгжлийн түвшинд ихээхэн ялгаа гарч байгаагийн улмаас зөрчилдөөн ихсэх хандлагатай болсон.
- Монгол улсад зэс, нүүрс, ураны ордуудад хөрөнгө оруулалт шаардагдаж байгаа, үүний улмаас стратегийн ашиг сонирхолтой улсууд олширсон, ОХУ ураны монополио алдахгүйг хичээж, БНХАУ-ын эрчим хүчний хямд эх үүсвэртэй болох, зэс, зэсийн баяжмалыг хямдаар олж авах, түүхий эдийн ихээхэн нөөцтэй болох, улмаар түүний эдийн үнийг удирдаж байх эрмэлзлэл, Япон, Солонгос улсууд коксжих нүүрс, бусад эрчим хүчний түүхий эд, өнгөт металлыг худалдан авах хямд, олон эх сурвалжтай болох, Канад, Австрали улсууд уул уурхайн их туршлага, хуримтлагдсан капитал дээрээ тулгуурлан стратеги том ордууд олж авч ихээхэн ашиг олох сонирхолтой.
- Хорлон сүйтгэх ажиллагаа, зохион байгуулалттай гэмт хэрэг, мэдээллийн аюулгүй байдлын (кибер) эрсдлүүд гэх мэт шинэ аюулуудын өмнө дэлхийн улсууд бэлэн бус, эмзэг сул байгаа.
- Урд хөршийн эдийн засаг, улс төрийн нөлөөлөл, цэргийн хүчний өсөлт, геополитикийн цоо шинэ нөхцөл байдал үүсэж байгаа, НАТО хүрээгээ өргөжүүлэн тэлсэн, үүний улмаас манай хөрш улсууд шинэ холбоотнуудыг эрж хайх болсон, Шанхайн хамтын ажиллагааны байгууллага нөлөөгөө тэлж байгаа. Хямралт нөхцөл байдлыг цэргийн хүчээр шийдэх хандлага хэвээр байгаа.



Аюулгүй байдалд орж буй өөрчлөлтүүд

- Монголчууд их хэмжээгээр гадагш дүрвэх, гадаад улсуудад хууль бусаар оршин суух явдал ихэссэн, тэдгээр иргэд ихээхэн эмзэг сул байдалтай учир Монгол улсын эсрэг үйл ажиллагаа явуулах, тусгай байгууллагын агентаар элсэх, нөлөөлөлд автах магадлалтай болсон.
- Бүс нутгийн аюулгүй байдлын механизм байхгүй, одоо байгаа Шанхайн хамтын ажиллагааны байгууллага нь манай улсын эрх ашигт бүрэн нийцэж чадахгүй, АНУ, Европ гэх мэт гуравдагч хөршүүдтэйгээ аюулгүй байдлын гэрээ байгуулж чадаагүй, тодорхой механизм, баталгаа байхгүй
- Олон улсын аюулгүй байдлыг хангах (бүс нутгийн хэмжээнд Монгол улсын аюулгүй байдлыг хангах) тогтолцоо сул, олон улсын эрх зүйн хэрэгсэл, механизм боловсронгуй бус.
- Кибер хорлон сүйтгэх ажиллагаа, интернетээр дамжин орж ирэх халдлага, довтолгоон эрс нэмэгдсэн, мэдээллийн дайн улам бүр хүчээ авч байгаа.
- Боловсрол-Хүний хөгжил, эдийн засаг, эрүүл мэнд, байгаль орчин, амьжиргааны түвшин, шинжлэх ухааны салбарын маш олон тулгамдсан асуудлууд (дотоодын) бий болсон.

Мэдээллийн аюулгүй байдал



- 21-р зуунд Мэдээллийн дайн, кибер дайн, кибер арми, цэрэг, кибер зэвсэг
- Мэдээллийн Аюулгүй байдал гэдэг нь өргөн утгаараа **“Нийгэм, институт, байгууллагын мэдээллийн орчны хамгаалагдсан байдал”**
- Мэдээлэл, өгөгдөл, түүнийг дэмжих дэд бүтцийн хамгаалагдсан байдал (байгууллагын аюулгүй байдалтай ижил болж байна)
- “Аюулгүй байдал” гэдэг нь зөвхөн “гадаад, дотоод аюулаас хувь хүн, нийгэм, төр улсын чухал ашиг сонирхлууд хамгаалагдсан байдал” төдийгүй өөрийн үнэт зүйл, зорилго, ашиг сонирхлоос гажсан тохиолдолд хариу үйлдэл хийх тухайн объектийн жам ёсны чадвар. Энэ чадварыг хөгжүүлж чадсанаар Монголын нийгэм, төр, байгууллагууд стратегийн аюулгүй байдлаа хангаж чадна.
- МАБ-нь бүрэн хамгаалалт бий болгохгүй.
- Хамгийн сайн цайз босгосон ч илүү хүчтэй эвдлэгч бүхий хэн нэгэн гарч ирнэ.

Даяаршил болон МАБ



- Монгол улс өөрийн мэдээллийн орон зайг хянах чадваргүй болсон нь геополитикийн эмзэг байдлыг улам ноцтой болгож байна.
- Дэлхий нийтийн мэдээллийн орон зай Монгол улсыг бүхэлд нь залгилаа.
- Дэлхий нийтийн мэдээллийн орон зайд Монгол улс нэгдэн нийлснээр хөрш орнууд болон барууны соёл, олон нийтийн мэдээллийн хэрэгслийн нөлөөллийн хүрээнд бүрэн орж байна.
- Хөрш улсууд Монголыг “дайсан биш гэхдээ найз биш” гэсэн ангилалд оруулаад байгаа нь өөрсдийн ашиг сонирхолд хамруулах, дохио зангаагаараа хөдөлгөдөг улс болгох гэсэн ашиг сонирхлыг нь харуулж байна.
- Энэ бүхний улмаас Монгол улсын хөгжлийн асуудал, үндэсний аюулгүй байдлын үзэл баримтлалыг геополитикийн хүчин зүйлс, даяаршилтай салшгүй холбон авч үзэх шаардлагыг бий болголоо

Аюулууд



- Мэдээллийн салбар дахь Монгол улсын ашиг сонирхлын эсрэг чиглэсэн гадаадын улс төр, эдийн засаг, цэрэг, тагнуулын болон мэдээллийн бүтэц, институтын үйл ажиллагаа;
- Дэлхийн мэдээллийн орон зайд Монгол улсын ашиг сонирхлыг хаах, зөрчих, дарамтлах, мэдээллийн зах зээлээс түрэн гаргах гэсэн зарим улсын эрмэлзэл;
- Мэдээллийн технологи, нөөцийг эзэмших гэсэн олон улсын өрсөлдөөн хурцадсан;
- Олон улсын хорлон сүйтгэх байгууллагуудын үйл ажиллагаа;
- Мэдээллийн хорлон сүйтгэх ажиллагаа (терроризм)-ны идэвхжил;
- Дэлхийн трэгүүлэх улсуудын технологийн давуу байдал болон монголын мэдээллийн дэд бүтцэд сөргөөр нөлөөлөх боломж нь эрс нэмэгдсэн;
- Гадаад улсуудын тагнуулын сансар, агаар, далай, газрын техник, хэрэгслийн хурдтай хөгжил, үйл ажиллагаа;
- Бусад улсын мэдээллийн орон зай, дэд бүтцэд хортойгоор нөлөөлөх, ажиллагааг нь тасалдуулах, мэдээллийн нөөцийг устгах, түүнд зүй бусаад халдах хэрэгслүүдийг бий болгох мэдээллийн дайны үзэл баримтлалыг зарим улс боловсруулсан байдал;

Аюулууд



Хувь хүн, нийгэмд заналхийлж байгаа аюулууд

- кибер хорлон сүйтгэх ажиллагаа;
- нийгмийн ёс суртахуунд заналхийлж буй аюулууд (порнограф тараах, хүчирхийлэл, мансууруулах бодис, гэмт хэргийг сурталчлах, үндэстэн хоорондын дайсагнал, дайн хүчирхийллийг сурталчлах г.м);
- ухамсарт нь үйлчлэн нөлөөлөх (кибер зомби болгох);
- нийгмийн тогтвортой байдлыг алдагдуулах үзэл санааг сурталчлах (арьс өнгөний үзэл, нацизм, шашны сектүүд г.м);
- цахим хэрэгслээр мэдээллийн дайн явуулах;
- залилан мэхлэх, социаль инжиниринг, фишинг, спаминг г.м
- төрийн систем дахь өгөгдөл мэдээллийг өөрчлөх, устгах, хулгайлах г.м;

Эдийн засагт заналхийлж буй аюулууд

- гадаад улс, гадны байгууллагын бизнес тагналт;
- эдийн засгийн алдагдалд хүргэх сөрөг, хуурамч мэдээлэл тараах;
- өрсөлдөгч байгууллага, компанийн сөрөг кибер үйлдэл;
- оюуны өмчийг хууль бусаар ашиглах;

Аюулууд



Батлан хамгаалах чадвар, үндэсний аюулгүй байдалд заналхийлж буй аюулууд

- Гадаад улсын зүгээс Монголын Интернет трафикийг хянах, статистик мэдээлэл цуглуулах, төрийн байгууллагын өгөгдлийн санг шүүж самнах;
- Монгол улсын тооцоолон бодох болон давтамжийн нөөцийг цэргийн зорилгод ашиглах, зомби болгох;
- Монгол улсын сүвгийн нөөцийг хууль бусаар ашиглах;
- Трафикийг зорилго, чиглэлтэйгээр өөрчлөх, гажуудуулах, харилцаа, холбооны системийг сүйтгэх, гажуудуулах;
- Хуурамч мэдээлэл тараах;
- Байлдааны вирус (логик бөмбөг г.м), бусад хэрэгсэл ашиглан тооцоолох, өгөгдөл боловсруулах төв, систем, харилцаа холбооны сүлжээг сүйтгэх;
- тагнуул – хорлон сүйтгэх ажиллагаа г.м.
- botnet технологийг ашиглан аливаа компьютерийг эзэнд нь мэдэгдэлгүй зайнаас удирдах.

Logic bomb буюу үйлдлийн систем, хэрэглээний програмд нууцаар оруулсан код. Тодорхой нөхцөл бүрдэх, тогтоосон цаг хугацаа болох, гаднаас команд өгөхөд идэвхжиж сүйтгэх үйлдэл, нөлөөлөл үзүүлнэ. Зарим үйлдвэрлэгч бүтээгдэхүүнийхээ бүрдэл хэсгүүдэд суулгаж үйлдвэрлэдэг, мэдээллийн дайны зэвсэг болгон ашиглаж байгаа.

Өнөөгийн байдал



- Бүх нийтийн ойлголт мэдлэг үүсээгүй
- Мэдээллийн технологи, мэдээллийн аюулгүй байдлын үйлдвэрлэл хөгжөөгүй, боловсролын тогтолцооны үр нөлөө буурсан, компьютерийн ёс зүйн төлөвшөөгүй, хүний нөөц байхгүй
- Кибер орчны эрүүгийн нөхцөл байдал хүндэрч эхэлж байгаа
- Төрийн байгууллагын уялдаа холбоо сул, эрх зүйн зохицуулалт, нэгдсэн бодлого байхгүй, үл тоомсорлодог
- Байгууллагуудад бодлого, хөтөлбөр, дэг бараг байхгүй
- Иргэний нийгэм энэ чиглэлд ямар ч анхаарал тавьдаггүй, сайн хөгжөөгүй
- Эдийн засгийн хүчин чадал сул
- Санхүүжилт байхгүй
- Аюулгүй байдлыг нь тооцохгүй, хангахгүйгээр МТ-ийг хөгжүүлж байгаа г.м.

Өнөөгийн байдал



- Шеньженд өндөр технологийн тагнуулын төв
- Дамжин өнгөрч буй Интернетийн урсгалыг шүүдэг, хянадаг
- Монголын сүлжээг байнга шүүдэг, самнадаг
- Байнгын халдлага (замаас барих, холбогдох, сонсох, үйлчилгээ бусниулах, нийгмийн боловсруулалт, хуулбарлах, сүлжээ, сайтын хакердах, тагнах, турших г.м)
- Гар утас ашиглах болсон
- Хүмүүсийг элсүүлэх оролдлого

Үндэсний Аюулгүй Байдлын үзэл баримтлал



- Мэдээллийн салбарт үндэсний ашиг сонирхлыг хамгаалах, төр, иргэн, хувийн хэвшлийн мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдлыг баталгаажуулах
- “Мэдээллийн аюулгүй байдал” гэдэгт гадны болон дотоодын сөрөг нөлөөллөөс үл хамааран бүрэн бүтэн байдал, өөрийгөө хөгжүүлэх чадвараа хадгалж буй мэдээллийн орчны тогтвортой байдлыг ойлгож болохоор байна.
- Мэдээллийн аюулгүй байдлыг нэгдүгээрт мэдээллийн орчныг ашиглан хангаж буй объектын аюулгүй байдал, хоёрдугаарт уг мэдээллийн орчны аюулгүй байдал хэмээн үзэж болно.
- Мэдээллийн орчин гэдэгт мэдээллийн харилцан ажиллагаанд оролцож буй субъектуудын нэгдэл, уг харилцан ажиллагааг хангаж буй технологи, төрөл бүрийн нөөцүүдийг ойлгож болно.

Мэдээллийн салбарт үндэсний ашиг сонирхлыг хамгаалах



- Үндэсний аюулгүй байдлыг хангах, улс орны хөгжлийг дэмжих, үндэсний үнэт зүйлийг хэвшүүлэх, нийгмийн оюун санааг төлөвшүүлэх
- Нийгмийн сэтгэл зүй, тогтвортой байдал, хувь хүний ухамсар, ёс зүйд хөндлөнгөөс нөлөөлөх
- Үндэсний мэдээллийн дэд бүтцэд халдах аюулаас хамгаалах, эдийн засаг, нийгмийн чадавхийг сулруулах оролдлоготой тэмцэх
- Хэвлэл мэдээллийн хэрэгсэл үндэсний аюулгүй байдалд харшилсан үйл ажиллагаа явуулахтай тэмцэх
- Мэдээллийн аюулгүй байдлын бодлого, эрх зүйн зохицуулалт, стандарт, удирдлага, зохион байгуулалт, сургалтын тогтолцоог бий болгож нийгэм дэх ойлголт, мэдлэгийг төлөвшүүлэх

Мэдээллийн салбарт үндэсний ашиг сонирхлыг хамгаалах



- Мэдээллийн аюулгүй байдлын бодлого, дэг, эрсдэлийн удирдлага, дотоод аудит, үнэлгээний чадавхийг бий болгох
- Өртөг багатай шийдлийг зөвхөн эрсдэлийн үнэлгээний үндсэн дээр сонгон ашиглах.
- МАБ-ын чиг үүргийг өндөр түвшинд бэлтгэгдэж, итгэмжлэгдсэн үндэсний мэргэжилтнээр гүйцэтгүүлэх
- технологийн хараат байдлыг бууруулах
- суурь болон хавсарга судалгаа, шинжилгээ, сургалт
- Кибер гэмт явдалтай тэмцэх
- Олон улсын хамтын ажиллагааг хөгжүүлэх

Мэдээллийн бүрэн бүтэн байдал



- Мэдээлэл, мэдээллийн орчин, түүний дэд бүтцэд хууль бусаар нөлөөлөх, өөрчлөх үйлчлэлээс хамгаалах
- Шаардлагатай мэдээллийг төрийн мэдээллийн санд төвлөрүүлж, эрх бүхий этгээд хамтран ашиглах, солилцох нөхцөлийг бүрдүүлэх
- Хувь хүний тухай мэдээллийг цуглуулах, хадгалах, ашиглах, бусдад шилжүүлэхийг зохицуулах
- Үндэсний мэдээллийн орчин, дэд бүтцийн эмзэг байдлыг бууруулах
- Үндэсний мэдээллийн дэд бүтэц, харилцаа холбоо, дамжуулалт, хандалтын нууцлал, хамгаалалтыг бүрдүүлэх
- төр-хувийн хэвшлийн түншлэлийн зарчмуудыг ашиглах, мэдээллийн аюулгүй байдлын дотоод аутсорсингийг дэмжих

Мэдээллийн нууцлал



- Мэдээлэл, төхөөрөмж, шугам, түүний бүрдэл хэсэгт хууль бусаар хандах, халдах, задруулахаас хамгаала
- Төрийн мэдээллийн ангилал, нууцын зэрэглэлийг оновчтой болгож, нууц хамгаалалтыг шинэ түвшинд гаргах
- Төрийн өгөгдөл мэдээллийг ангилж, үнэ цэнийг тогтоох, бүртгэх, хадгалах, дамжуулах, шилжүүлэх, хяналт тавих
- Харилцаа холбооны шугам, сувгаас мэдээлэл алдагдах, гадагш урсахаас урьдчилан сэргийлэх, төрийн сүлжээ, өгөгдөл солилцооны хамгаалагдсан дэд бүтцийг байгуулах
- чиг үүрэгт суурилсан хандалтын удирдлага, сүлжээний хяналт-шинжилгээ хийх, халдлагыг илрүүлж таслан зогсоох чадварыг бий болгох.
- шифрлэлт, тоон гарын үсэг, аюулгүй холболт ашиглах

Мэдээллийн хүртээмжтэй байдал



- Хуулиар хориглоогүй мэдээллийг чөлөөтэй хайх, олж авах, үүсгэх, дамжуулах, түгээх эрх, эрх чөлөөг хангах, мэдээллийн дэд бүтэц, түүний бүрдэл хэсэг, үйлчилгээнд чөлөөтэй хандах боломжийг бүрдүүлэх
- Төрийн бодлого боловсруулагчид, нийт иргэн, ард түмэн өргөн мэдээлэл, нэгдмэл ойлголттой байх
- Үндэсний аюулгүй байдалтай холбоотой асуудлуудаар өргөн хүрээтэй мэдээллээр хангах механизмыг бий болгох.
- Төрийн мэдээллийн нээлттэй нөөцийг бүрдүүлэх, тэдгээрийг цахим засгийн үйлчилгээнд үр нөлөөтэй ашиглах боломжийг бүрдүүлэх
- Мэдээллийн хэрэгсэл, дэд бүтцийн хөгжлийг дэмжих
- Хуулиар хориглоогүй мэдээллийг эрэн сурвалжилж олж авах, нийгэмд түгээхэд таатай эрх зүйн орчныг бүрдүүлэх
- Үндэсний мэдээллийн дэд бүтцийн бэлэн байдал, халдлагыг сөрөн зогсох, даван гарах чадварыг бий болгох,
- Тасралтгүй ажиллагааг хангах, сэргээн ажиллуулах төлөвлөлтийг хэвшүүлж, сүлжээний хяналт шинжилгээ, анхааруулгын төв байгуулж, компьютерын онцгой байдлын үед хариу үйлдэл хийх үндэсний тогтолцоог дэмжин хөгжүүлэх

Даяаршил болон МАБ



- Монгол улсын мэдээллийн аюулгүй байдлын геополитикийн шинж чанар,
- Цэрэг – техникийн шинж чанар,
- Соёлын шинж чанар,
- Мэдээлэл – сэтгэл зүйн шинж чанар
- Эрх зүйн шинж чанар - талууд

Байгууллага хэрхэн хангах вэ?



- Удирдлагын ойлголт, манлайлал, дэмжлэг, үүрэг, сэдэл
- МАБ-ын стратеги, бодлого, хөтөлбөр
- МАБ-ын дэг, журам
- Програм техникийн хамгаалалт
- МАБ-ын сургалт, хүний нөөцийг хөгжүүлэх
- Кибер халдлагын мониторинг, будлианы удирдлага
- МАБ-ын аудит, эрсдлийн үнэлгээ
- Мэргэжлийн байгууллагатай хамтран ажиллах
- МАБ-ын ажилтан, систем администраторын орон тоо, тэднийг байнга сурган хөгжүүлэх
- Тасралтгүй ажиллагааны төлөвлөгөө хэрэгжүүлэх, хурдан хугацаанд сэргэн ажиллах чадварыг бий болгох
- Төрийн цахим өгөгдөл, мэдээлэлд хандах хандалтын зэрэглэл, ангилал, удирдлага
- Бүх ажилтны ойлголт, мэдлэг, дэмжлэг, үүрэг хариуцлага
- Тоон гарын үсэг, шифрлэлт ашиглах

Анхаарал тавьсанд баярлалаа

www.sssmn.com

info@sssmn.com

70113151