Төрийн Албан Хаагчдад Зориулсан МХХТ-ийн
Суурь Мэдлэгийн Академи

МОДУЛЬ 6

Сүлжээ, мэдээллийн аюулгүй байдал, нууцлал

Солонгосын Мэдээллийн
Аюулгүй Байдлын Агентлаг

APCICT ХӨГЖЛИЙН ТӨЛӨӨХ МЭДЭЭЛЭЛ, ХАРИЛЦАА ХОЛБООНЫ
ТЕХНОЛОГИЙН АЗИ, НОМХОН ДАЛАЙН БҮСИЙН СУРГАЛТЫН ТӨВ

Төрийн албан хаагчдад МХХТ-ийн суурь мэдлэг олгох
академийн модулиуд

Модуль 6: Сүлжээ, мэдээллийн аюулгүй байдал, нууцлал хамгаалалт

НҮБ-ын Хөгжлийн Төлөөх Мэдээлэл, Харилцаа Холбооны Технологийн Ази,
Номхон Далайн Бүсийн Сургалтын Төв

Хаяг: Bonbudong, 3rd floor Songdo Techno Park
7-50 Songdo-dong, Yeonsu- gu, Incheon City
Republic of Korea

Утас: +82 32 245 1700002
Факс: +82 32 245 7712
И-мэйл: info@unapcict.org
Веб сайтын хаяг: http://www.unapcict.org

ISBN: 978-89-955886-4-2 [94560]

Хэвлэлийн эхийг Scandinavian Publishing Co Ltd, Studio triangle компани бэлтгэж,
Бүгд Найрамдах Солонгос Улсад хэвлэв.

ӨМНӨХ ҮГ

21 дүгээр зууныг даяаршиж буй дэлхий дээр амьдарч байгаа хүн төрөлхтөний хараат бус, бие даах чадварыг улам бүр нэмэгдүүлсэн гэж тооцдог. 21-р зуун нь шинэ технологийн үр өгөөжийг сая сая хүмүүст амсуулж, ард иргэдийн амьдралыг эрс сайжруулж , ядруурлыг бууруулж чадах мэдээлэл, мэдлэгийн хүртээмжийг өргөжүүлэх боломжоор нээсэн цаг хугацаа билээ. Гэхдээ хараат бус байдал нь дангаараа бус хүн бүрт нээлттэй байх тогтвортой хөгжлийн төлөөх үнэ цэнэ, зорилт, эв нэгдлийн хамт өсөн нэмэгдэх боломжоотой.

Сүүлийн жилүүдэд Ази, Номхон далайн бүс нь мэдээлэл, харилцаа холбооны технологийн хувьд илүү давуу хөгжилтэй бүс нутаг болон хөгжиж байна. ОУЦХБ-ын тооцоолсноор тус бүс нутгийн телефон шугамын тоо хоёр тэрбумаас давж, хөдөлгөөнт холбооны хэрэглэгчийн тоо 1.4 тэрбумд хүрсэн үзүүлэлт гарчээ. 2008 оны хагас жилийн байдлаар дэлхийн нийт хөдөлгөөнт холбооны хэрэглэгчдийн дөрөвний нэг хувийг Хятад болон Энэтхэг улс эзэлсэн тооцоо гарсан. Дэлхийн интернэт хэрэглэгчийн 40 хувийг Ази, Номхон Далайн бүс хамрах бөгөөд интернэтийн өргөн зурвасын дэлхийн зах зээлийн 39 хувийг эзэлж байгаа нь хамгийн том зах зээл гэсэн үг юм.

Технологийн ололт, амжилтуудын үр дүнд тоон хуваагдал арилсан болов уу гэж таамаглахад хараахан арилж амжаагүй байгаа гэсэн хариулт гарч ирж байгаа нь харамсалтай. МНДДУ буюу Мэдээлэлжсэн Нийгмийн Дэлхийн Дээд Уулзалт /МНДДУ/ 2003 онд Женев хотноо зохион байгуулагдснаас хойшхи таван жилийн нөхцөл байдлыг авч үзэхэд тус бүс нутаг технологийн ололт амжилтаар тэргүүлж байсан хэдий ч хүн амын олонх нь ялангуяа ядуу иргэд харилцаа холбооны үндсэн үйлчилгээг авч чадаагүй хэвээр байна.

Тус бүсийн 25 орон буюу голцуу жижиг арлын хөгжиж байгаа орнууд болон далайд гарцгүй орнуудын 100 хүнд ноогдох интернэт хэрэглэгчийн тоо нь 10 хүрэхгүй, эдгээр хэрэглэгчид нь ихэвчлэн томоохон хотод амьдардаг хотын оршин суугчид байхад нөгөө талаас тус бүсийн хөгжингүй орнуудын 100 хүнд ноогдох интернэт хэрэглэгчийн тоо нь 80 гаруй байгаа тооцоо гарчээ. Өргөн зурвасын үйлчилгээний хэрэглээний ялгаа бүр их байна.

Тус бүсийн нийгэм-эдийн засгийн хөгжлийг хангахад МХХТ-ийн чадавхийг ашиглаж, тоон хуваагдлыг арилгахын тулд хөгжиж байгаа орнуудын бодлого боловсруулагчид МХХТ-ийн үйлдвэрлэлийн салбар болон иргэдийн МХХТ-ийн чадварыг хөгжүүлэх түншлэлийг дэмжих, тэргүүлэх ач холбогдол бүхий ажил, арга хэмжээг тодорхойлж, бодлого хэрэгжүүлэх, хууль эрх зүй болон зохицуулалтын орчинг тодорхойлох, төсөв, санхүүг оновчтой хуваарилах шаардлагатай юм.

МНДДУ –ын Үйл ажиллагааны төлөвлөгөөнд “ ....хүн бүр мэдээлэлжсэн нийгэм болон мэдлэгт тулгуурласан эдийн засгийг ойлгох, оролцох, үр өгөөжийг хүртэхийн тулд шаардлагатай мэдлэг, чадвар эзэмших боломжтой байх ёстой....” гэж тусгасан. Уг төлөвлөгөөнд МХХТ-ийн мэргэжлийн боловсон хүчин, шинжээчдийг олноор нь төрүүлэх зорилгоор олон улсын болон бүс нутгийн хамтын ажиллагааг идэвхтэй хөгжүүлэхийг уриалсан байдаг.

Энэхүү уриалгын хүрээнд МХХТ-ийн АНДБ-ийн Сургалтын Төвөөс хөгжлийн зорилтод МХХТ-ийг ашиглах сургалтын хөтөлбөр боловсруулсан. Тус хөтөлбөр нь өөр хоорондоо уялдаа холбоотой 8 модулиас бүрдсэн бөгөөд бодлого боловсруулагчдад МХХТ-ийн санал, санаачилгыг боловсруулж, хэрэгжүүлэхэд дэмжлэг болох мэдлэг, мэдээлэл өгөх зорилготой юм.

Хөгжлийн төлөөх МХХТ-ийн Ази, Номхон далайн бүсийн сургалтын төв нь НҮБ-ын АНДБ-ийн Эдийн Засаг, Нийгмийн Коммисс-/АНДБЭЗНК/-ын бүсийн 5 байгууллагын нэг билээ. АНДБЭЗНК нь Ази, Номхон далайн бүсэд дүн шинжилгээ, норматив үйл ажиллагаа, чадавхийг бэхжүүлэх, бүс нутгийн хамтын ажиллагаа болон мэдлэг хуваалцах замаар тогтвортой, тэгш хамарсан нийгэм, эдийн засгийн хөгжлийг дэмжих зорилготой юм. НҮБ-ын бусад байгууллагууд, олон улсын байгууллагууд, үндэсний хэмжээний түншүүд, оролцогч талуудтай хамтран АНДБЭЗНК нь Хөгжлийн төлөөх МХХТ-ийн Ази, Номхон далайн бүсийн сургалтын төвөөр дамжуулан энэхүү сургалтын модулиудыг ашиглах, нутагшуулах, орчуулах, төрийн байгууллагуудын дээд болон дунд түвшний ажилтнуудад зориулсан бүсийн болон үндэсний хэмжээний семинаруудаар түгээх үйл явцыг хөхүүлэн дэмжиж, энэхүү үйл явцаар дамжуулан бий болсон чадавхи болон олж авсан мэдлэг нь хөгжлийн зорилтуудад нийцэхүйц МХХТ-ийн үр шим болон бодит үйл ажиллагааг бий болгох зорилготой байдаг юм.

Ноелиин Хэйзер

НҮБ-ын Ерөнхий Нарийн Бичгийн Даргын Орлогч Дарга бөгөөд
АНДБ-ийн Эдийн Засаг, Нийгмийн Коммиссын Гүйцэтгэх Нарийн Бичгийн Дарга

УДИРТГАЛ

Төрийн албан хаагчдад зориулсан МХХТ-ийн суурь мэдлэгийн академи хэмээх цуврал модулийг боловсруулах үйл ажиллагаа нь бидэнд ихээхэн урам зориг өгсөн, бидний нүдийг нээн өгсөн үйл ажиллагаа, томоохон аялал байлаа. Академи нь зөвхөн МХХТ-ийн чадавхийг бэхжүүлэх үйл явцад байгаа орхигдсон зүйлсэд бус мөн иргэдийн оролцоо, үйл явцыг өөриймшүүлэн эзэмших замаар сургалтын хөтөлбөр боловсруулах шинэ арга замыг бий болгох зорилготой билээ.

Академи нь Хөгжлийн төлөөх МХХТ-мэдээлэл, харилцаа холбооны технологийн Ази, Номхон далайн бүсийн сургалтын төвийн тэргүүлэх хөтөлбөр бөгөөд бүс нутаг дахь 20 гаруй улсыг хамруулан зохион байгуулсан эрэлт хэрэгцээний үнэлгээний үр дүн, төрийн байгууллагуудын ажилтнууд, олон улсын хөгжлийн нийгэмлэгийн гишүүд, эрдэмтэд болон судлаачидтай хийсэн зөвлөлдөх уулзалтуудын үр дүн; өнөөгийн хэрэглэж буй сургалтын материалын давуу болон сул талуудад хийгдсэн гүнзгийрүүлсэн судалгаа; Хөгжлийн төлөөх МХХТ-мэдээлэл, харилцаа холбооны технологийн Ази, Номхон далайн бүсийн сургалтын төвийн бүсийн болон дэд-бүсийн хүрээнд зохион байгуулсан сургалт, семинаруудад оролцогчдын зүгээс модулийн агуулгын хоорондын хамаарал болон үр ашгийн талаар гаргасан саналууд; МХХТ-ийн салбарын олон тооны экспертүүдийн хийсэн судалгаа зэрэг дээр суурилан боловсруулагдсан билээ. Бүс нутгийн хэмжээнд зохион байгуулагдсан Академийн сургалт/семинарууд нь төрөл бүрийн улс орноос төлөөлөн ирсэн оролцогчдын хооронд мэдлэг, туршлагаа хуваалцах үнэлж баршгүй боломжийг ханган өгсөн бол энэхүү арга хэмжээний хүрээнд Академийн төгсөгчид модулиудыг сайжруулах боломжийг мөн хангаж өгсөн юм.

Академиас гаргасан анхан шатны 8 модулийг үндэсний хэмжээнд түгээн дэлгэрүүлэх, нэвтрүүлэх нь бүсийн хэмжээнд өнөөгийн түншлэлийг бэхжүүлэх, МХХТ-ийн хөгжлийн асуудлаар бодлого боловсруулагч нарын чадавхийг бэхжүүлэх шинэ түншлэлийг бий болгох боломжийг бий болгож байна. Хөгжлийн төлөөх МХХТ-мэдээлэл, харилцаа холбооны технологийн Ази, Номхон далайн бүсийн сургалтын төв нь Үндэсний академиудад бүх бодлого гаргагч нарт хүрч ажиллах гол хандлагаа хэрэгжүүлэх зорилгоор 8 модулийг үндэсний хэмжээнд түгээн дэлгэрүүлэхэд техникийн дэмжлэг үзүүлэх хүсэл эрмэлзлэлтэй байгаа билээ. Хөгжлийн төлөөх МХХТ-мэдээлэл, харилцаа холбооны технологийн Ази, Номхон далайн бүсийн сургалтын төв нь төв болон орон нутгийн засаг захиргаатай нэгэн сүлжээнд ажиллаж буй бүс нутгийн болон үндэсний хэд хэдэн сургалтын байгууллагуудтай хамтран ажиллаж тэдгээр нь өөрсдийн хэрэгцээ болон тэргүүлэх чиглэлд нийцүүлэн Академийн модулиудыг ашиглах, нутагшуулах, орчуулах, түгээх чадавхийг нь бэхжүүлдэг юм. Цаашид ч өнөөгийн модулиудыг өргөжүүлэн гүнзгийрүүлэх болон шинээр боловсруулах төлөвлөгөөтэй байгаа юм.

Түүнчлэн Хөгжлийн төлөөх МХХТ-ийн Ази, Номхон далайн бүсийн сургалтын төв нь Академийн боловсруулан гаргаж буй агуулгыг нь бүс нутгийн хэмжээнд илүү өргөн хүрээнд түгээн дэлгэрүүлэх үйл явцыг баталгаажуулахын тулд олон суваг бүхий хандлагыг ашиглаж байна. Академийн агуулгыг бүс нутгийн болон үндэсний академиар дамжуулан нүүр тулсан байдлаар түгээн дэлгэрүүлэхээс гадна Хөгжлийн төлөөх МХХТ-мэдээлэл, харилцаа холбооны технологийн Ази, Номхон далайн бүсийн сургалтын төвийн Виртуал академийг байгуулан онлайн зайн сургалтыг бий болгон оролцогч нар сургалтын материалыг өөрийн боломжоор судлах бололцоог мөн хангаад байна. Виртуал академи нь бүх модулиуд, тэдгээрийн дагалдах материалууд болох танилцуулгууд, кейсүүдийг агуулж хялбархан нэвтрэн, ашиглах боломжийг хангасны зэрэгцээ татан авах, дахин ашиглах, өөрийн улсад нутагшуулах, нөхцөл байдалд нийцүүлэх боломжийг мөн хангадаг ба мөн виртуал лекцүүд, суралцах аргачлалууд, агуулга хөгжүүлэх аргачлалууд болон гэрчилгээжүүлэлт зэргийг мөн ханган өгсөн.

Анхан шатны цуврал 8 модуль, тэдгээрийг бүс нутгийн болон үндэсний Академийн сургалт/семинаруудаар түгээн дэлгэрүүлэх үйл ажиллагаа нь олон тооны хувьд хүмүүс, байгууллагуудын хичээл зүтгэл, оролцоогүйгээр амжилтад хүрэхгүй байсан юм. Энэхүү боломжийг ашиглан миний бие Академийн төгсөгчид, сургалт/семинаруудад оролцож байсан яамд, сургалтын байгууллагууд, бүс нутгийн болон үндэсний байгууллагуудад талархалаа илэрхийлэхийг хүсэж байна. Эдгээр талууд нь модулиудын агуулгад ихээхэн үнэтэй хувь нэмрийг оруулаад зогсохгүй, хамгийн чухал нь өөрийн улс оронд энэхүү Академийн төлөөлөл болон, энэ талаар нөлөөлөл үзүүлэн өөр өөрийн оронд Академийн курсуудыг нутагшуулахад Ази, Номхон Далайн бүсийн хөгжлийн төлөөх мэдээлэл, харилцаа холбооны технологийн сургалтын төв болон үндэсний болон бүс нутгийн түншлэгч байгууллагуудын хооронд албан ёсны гэрээ байгуулах боломжийг нээн өгсөн билээ.

Түүнчлэн миний бие энэхүү гайхалтай, урам зориг өгсөн аялалд маань өөрийн хувь нэмрийг оруулсан олон тооны хүмүүсийн хүчин чармайлтад талархалаа илэрхийлэхийг хүсэж байна. Тэдний тоонд Академийн төслийн зөвлөх Шахид Ахтар, Редактор Патрисиа Аринто, Хэвлэн нийтлэх менежер Кристин Апикул, бүх зохиогч нар болон Академийн ажилтнууд багтаж буй юм.

Улс орнууд нийгэм- эдийн засгийн хөгжил, Мянганы хөгжлийн зорилтуудад хүрэх, түргэтгэхийн тулд МХХТ-ийн хүний нөөцийн хомсдлыг бууруулах, МХХТ-ийг хэрэгжүүлэхэд тулгарч буй саад тотгорыг бууруулах, МХХТ-ийн хэрэглээг дэмжихэд нь Академи өөр тус дэмийг үзүүлж чадна гэдэгт би бат итгэлтэй байна.

Хьюн-Сук Рии

МХХТХ-ийн АНДБНСТ-ийн захирал
Хөгжлийн төлөөх МХХТ-ийн Ази, Номхон Далайн Бүсийн Сургалтын Төв

ЦУВРАЛ МОДУЛИЙН ТУХАЙ

Өнөөдрийн “мэдээллийн зуунд” бид бүхэн мэдээлэл хүлээн авахад хялбар болсон нь бидний ажиллаж, амьдрах нөхцөл, арга замд ихээхэн өөрчлөлтийг бий болгожээ. “Цахим эдийн засаг” буюу заримдаа “мэдлэгийн эдийн засаг”, “харилцан уялдаатай эдийн засаг” эсвэл “шинэ эдийн засаг” хэмээн нэрлэгдэх эдийн засаг нь бараа бүтээгдэхүүний үйлдвэрлэлээс шинэ санааны үйлдвэрлэлд шилжиж байна. Үүний хүрээнд МХХТ-ийн нийгэм, эдийн засагт үзүүлэх үүрэг нь гол чухал биш ч гэсэн хамрах хүрээгээ ихээхэн нэмэгдүүлсээр байгаа юм.

Үүний үр нөлөөгөөр дэлхийн улс орнуудын Засгийн газрууд хөгжлийн үйл ажиллагаанд МХХТ-ийг ашиглахад ихээхэн анхаарал хандуулах болжээ. Эдгээр улсуудын хувьд хөгжлийн төлөөх МХХТ гэдэг нь зөвхөн МХХТ-ийн салбарыг хөгжүүлэх бус МХХТ-ийг эдийн засаг, нийгэм, улс төрийн хөгжлийн чиглэлд ашиглах үйл явцыг мөн багтааж байна.

Гэхдээ Засгийн газруудад МХХТ-ийн бодлогыг боловсруулахад тулгарч буй хүндрэлүүдийн тоонд бодлого боловсруулагчид үндэсний хөгжлийн хөдөлгөгч болох технологийн талаар мэдлэггүй буй явдал багтаж байна. Хэн нэгэн этгээд өөрийн мэдэхгүй, ойлгохгүй зүйлийг зохицуулах боломжгүй тул олон тооны бодлого боловсруулагч нар МХХТ-ийн салбарын бодлого боловсруулахаас нүүр буруулдаг юм. Үүний зэрэгцээ МХХТ-ийн бодлого боловсруулах үүргийг технологийн мэргэжилтнүүдэд дангаар нь хариуцуулах нь мөн учир дутагдалтай бөгөөд тэд өөрсдийнх нь боловсруулж, ашиглаж буй технологийн бодлогод үзүүлэх нөлөөллийн талаар мэдлэггүй байдаг.

Төрийн албан хаагчдад зориулсан МХХТ-ийн суурь мэдлэгийн академи хэмээх цуврал модулийг Хөгжлийн төлөөх МХХТ-мэдээлэл, харилцаа холбооны технологийн Ази, Номхон далайн бүсийн сургалтын төвөөс:

1. МХХТ-ийн бодлого боловсруулах үүрэг бүхий төв болон орон нутгийн захиргааны бодлого боловсруулагч нар,
2. МХХТ дээр суурилсан хэрэглээг боловсруулах, хэрэгжүүлэх үүрэг бүхий төрийн байгууллагын ажилтнууд,
3. Төслийн удирдлагын үйл ажиллагаандаа МХХТ-ийн аргачлалыг ашиглахаар эрэлхийлж буй менежерүүдэд зориулан боловсруулсан билээ.

Цуврал модуль нь хөгжлийн төлөөх МХХТ-ийн голлох асуудлыг технологийн болон бодлогын үүднээс танилцуулах зорилготой. МХХТ-ийн техникийн зааварчилгааг боловсруулан гаргах бус харин өнөөгийн тоон технологи нь ямар боломж олгож буй, хааш чиглэж буй, бодлого боловсруулахад ямар нөлөө үзүүлж буй талаар сайн ойлголт өгөх зорилготой байлаа. Модулиудын хамрах сэдэв нь сургалтын хэрэгцээний дүн шинжилгээ, дэлхийн хэмжээнд хэрэглэж буй сургалтын материалууд дээр хийсэн судалгааны үр дүн дээр суурилсан билээ.

Модулиудыг хувь хүмүүс бие даан суралцах, эсвэл сургалтын курс, хөтөлбөрт хамрагдан суралцах боломжийг давхар хангахуйц байдлаар боловсруулсан. Модуль тус бүр нь бие даасан сэдэвтэй байгаагийн зэрэгцээ бүгд хоорондоо харилцан хамааралтай, бусад модультай хамаарах хэлэлцүүлэг бүхий байгаа. Үүний урт хугацааны зорилт нь модулиудыг гэрчилгээжүүлэх боломж бүхий уялдаа холбоо бүхий курс болгох явдал билээ.

Модуль бүр нь тухайн модулийн зорилтууд болон уншигчид дараагаар нь өөрсдийн шинээр олж авсан мэдлэгийг тулган шалгах боломжтой зорилтот үр дүнгийн талаар дурдсанаар эхэлсэн. Модулийн агуулга нь бүлэг болон хуваагдсан ба тухайн модулиар олгож буй гол үзэл баримтлалыг гүнзгийрүүлэн ойлгоход нь туслах кейс судалгаа болон дасгалуудыг мөн агуулсан. Дасгалуудыг бүлгээр болон ганцаарчилсан байдлаар хийх зориулалттай. Зураг, хүснэгтүүд нь хэлэлцүүлгийн тодорхой утга санааг тодруулан гаргасан. Эх сурвалжууд болон онлайн эх сурвалж нь уншигчдад нэмэлт мэдээлэл олж авах эх үүсвэр болох байдлаар нэмэгдэж орсон.

МХХТ-ийн хөгжил нь ихээхэн өргөн хүрээнд байх тул зарим тохиолдолд кейс судалгаа болон жишээнүүд нь харилцан зөрчилдөөнтэй байх тохиолдол бий. Ийм учраас л ихээхэн сонирхолтой, шинээр төрөн гарч буй салбар тул бүх улс орнууд МХХТ-ийн аргачлалуудыг хөгжлийн зорилгод ашиглах боломж бүрийг эрэлхийлэх шаардлагыг үүсгэнэ.

Академиас хэвлэн гаргасан Академийн модулийн хэвлэмэл хувилбарт дэмжлэг үзүүлэх зорилгоор онлайн зайн сургалтын Хөгжлийн төлөөх МХХТ-мэдээлэл, харилцаа холбооны технологийн Ази, Номхон далайн бүсийн сургалтын төвийн Виртуал академийг (AVA- http://www.unapcict.org/academy) байгуулсан ба энд танхимын хичээлийг сургагч багш зааж буйг видео форматаар болон ПоверПойнт (PowerPoint) танилцуулга хэлбэрээр үзэн суралцах боломжийг мөн хангана.

Түүнчлэн Хөгжлийн төлөөх МХХТ-мэдээлэл, харилцаа холбооны технологийн Ази, Номхон далайн бүсийн сургалтын төв нь Цахим хамтын ажиллагааны төв (E-collaborative hub- http://www.unapcict.org/ecohub) буюу онлайн сайтыг МХХТ-ын салбарын ажиллагсад, бодлого боловсруулагч нарт зориулан, сургалт, болон суралцах үйл явцад нь дэмжлэг үзүүлэх зорилгоор хийсэн байгаа. Энэхүү цахим хамтын ажиллагааны төв (e-Co hub) нь МХХТ-ийн талаарх олон талын мэдлэг мэдээллийн эх үүсвэр болон, мэдлэг туршлагаа хуваалцах, МХХТ-ын чиглэлд хамтран, үүнд дэвшил гаргах интерактив орон зайн үүргийг гүйцэтгэдэг юм.

МОДУЛЬ 6

Мэдээллийн эринд мэдээлэл нь хамгаалагдах ёстой хөрөнгө бөгөөд бодлого боловсруулагчид мэдээллийн аюулгүй байдал гэж юу болох мэдээллийг задлах, мэдээлэлд халдахын эсрэг арга хэмжээг хэрхэн авах талаар мэддэг байх шаардлагатай. Энэхүү модуль нь мэдээллийн аюулгүй байдлын хэрэгцээ, мэдээллийн аюулгүй байдлын асуудлууд, хандлага болон мэдээллийн аюулгүй байдлын стратегийг боловсруулах үйл явцын талаар товч ойлголтыг өгнө.

МОДУЛИЙН ЗОРИЛГО

Тус модуль нь дараах зорилгуудыг агуулсан болно. Үүнд:

1. Мэдээллийн аюулгүй байдал, нууцлалын талаарх ойлголтууд ба түүнтэй холбоотой ойлголтуудыг тодруулах;

2. Мэдээллийн аюулгүй байдалд тулгарч буй аюулыг тодорхойлох болон тэдгээрийг хэрхэн авч үзэх;

3. Мэдээллийн аюулгүй байдлын талаарх бодлогыг бий болгож хэрэгжүүлэхэд шаардагдах зүйлс болон мэдээллийн аюулгүй байдлын бодлогын хэрэгжилтийн мөчлөгийн талаар хэлэлцэх;

4. Зарим улс орнууд болон олон улсын мэдээллийн аюулгүй байдлын байгууллагуудын хэрэглэдэг мэдээллийн аюулгүй байдал ба нууцлалын стандартуудын талаарх ойлголтыг олгох.

СУРГАЛТААС ГАРАХ ҮР ДҮН

Энэхүү модуль дээр ажилласны дараа уншигчид дараах зүйлсийг хийх чадвартай болно. Үүнд:

1. Мэдээллийн аюулгүй байдал, нууцлал ба тэдгээрт холбогдох ойлголтуудыг тодорхойлох;

2. Мэдээллийн аюулгүй байдалд учирч болох аюулыг таних;

3. Одоо ашиглагдаж буй мэдээллийн аюулгүй байдлын бодлогыг олон улсын мэдээллийн аюулгүй байдал ба нууцлал хамгаалалтын стандартуудын талаас үнэлэх; болон

4. Өөрсдийн нөхцөл байдалд тохирох мэдээллийн аюулгүй байдлын бодлоготой холбоотой зөвлөмжүүдийг боловсруулан гаргах.

АГУУЛГА

КЭЙС СУДАЛГААНЫ ЖАГСААЛТ

ЗУРГИЙН ЖАГСААЛТ

ХҮСНЭГТИЙН ЖАГСААЛТ

ТОВЧИЛСОН ҮГС

APCERT	Team-Ази Номхон далайн бүсийн компьютерийн халдлагад хариу үзүүлэх баг (АНДКХХҮБ)
APCICT	НҮБ-ын хөгжлийн төлөөх мэдээлэл холбооны технологийн Ази Номхон далайн бүсийн сургалтын төв (ХМХХТАНДСТ)
APEC	Ази Номхон далайн эдийн засгийн хамтын ажиллагаа (АНДЭЗХА)
BPM	Manual-Суурь хамгаалалтын гарын авлага (СХГА)
BSI	Британийн стандартын байгууллага
BSI	ХБНГУ-ын мэдээллийн аюулгүй байдлын байгууллага (МАБА)
CC	Нийтлэг шалгуур (НШ)
CCRA	Нийтлэг шалгуурыг хүлээн зөвшөөрөх гэрээ (НШХЗГ)
CECC	Кибер гэмт хэргийн тухай Европын конвенцийн зөвлөл (КГХЕКЗ)
CERT	Компьютерийн халдлагад хариу үзүүлэх баг (КХХҮБ)
CERT/CC	Компьютерийн халдлагын эсрэг багуудыг зохицуулах төв (КХХҮБ/ЗТ)
CIIP	Онц чухал мэдээллийн дэд бүцтийн хамгаалалт (ОЧМДБХ)
CISA	Мэргэшсэн мэдээллийн системийн аудитор (ММСА)
CISSP	Мэргэшсэн мэдээллийн системийн аюулгүй байдлын мэргэжилтэн (ММСАБМ)
CM	Конфигурацийн удирдлага (КУ)
CSEA	Кибер аюулгүй байдлыг бэхжүүлэх тухай хууль (КАББХ)
CSIRT	Компьютерийн аюулгүй байдалд хариу өгөх баг (КАБЗХӨБ)
DoS	Үйлчилгээг бусниулах (ҮБ)
ECPA	Цахим харилцааны нууцлалын тухай хууль (ЦХНХ)
EGC	Европын засгийн газрын компьютерийн халдлагын эсрэг баг (ЕЗГК)
ENISA	Европын мэдээлэл, сүлжээний аюулгүй байдлын агентлаг (ЕМСАБА)
ERM	Байгууллагын эрсдлийн удирдлага (БЭУ)
ESCAP	Ази, Номхон далайн эдийн засаг, нийгмийн зөвлөл (АНДЭЗНЗ)
ESM	Байгууллагын аюулгүй байдлын удирдлага (БАБУ)
FEMA	Холбооны онцгой байдлын удирдлагын агентлаг (ХОБУА)
FIRST	Будлианд хариу өгөх, аюулгүй байдлын багуудын форум (БХӨАБФ)
FISMA	Холбооны мэдээллийн аюулгүй байдлын удирдлагын хууль (ХМАБУХ)
FOI	Мэдээллийн эрх чөлөө (МЭЧ)
ICTD	Хөгжлийн төлөөх мэдээлэл харилцаа, холбооны технологи (ХМХХТ)
IDS	Довтолгоон илрүүлэх систем (ДИС)
IGF	Интернэт засаглалын форум (ИЗФ)
IPS	Довтолгооноос сэргийлэх систем (ДСС)
ISACA	Мэдээллийн системийн хяналт, шалгалтын холбоо (МСХШХ)
ISMS	Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо (МАБУТ)
ISP/NSP	Интернэт, сүлжээний үйлчилгээ эрхлэгч
IT	Мэдээллийн технологи (МТ)
ITU	Олон улсын цахилгаан холбооны байгууллага (ОУЦХБ)
ITU-D	Олон улсын цахилгаан холбооны байгууллагын хөгжлийн хэсэг (ОУЦХБ-Х)
ITU-R	Олон улсын цахилгаан холбооны байгууллагын радио холбооны хэсэг (ОУЦХБ-Р)
ITU-T	Олон улсын цахилгаан холбооны байгууллагын стандартчилалын хэсэг (ОУЦХБ-С)
KISA	Солонгосын мэдээллийн аюулгүй байдлын агентлаг (СМАБА)
MIC	БНСУ-ын Мэдээлэл Холбооны Яам (МХЯ)

NIS	Сүлжээ, мэдээллийн аюулгүй байдал (СМАБ)
NISC	Японы Үндэсний Мэдээллийн Аюулгүй Байдлын Төв (ЯҮМАБТ)
NIST	АНУ-ын Стандарт, технологийн үндэсний төв (СТҮТ)
OECD	Эдийн засгийн хамтын ажиллагаа, хөгжлийн байгууллага (ЭЗХАХБ)
OMB	АНУ-ын Төсөв, Удирдлагын Газар (ТУГ)
OTP	Нэг удаагийн нууц үг
PP	Хамгаалалтын профайл (ХП)
PSG	Байнгын оролцогч талуудын бүлэг (БОТБ)
RFID	Радио давтамжаар таних (РДТ)
SAC	Аюулгүй байдлын баталгаажуулалтын бүрдэл (АБББ)
SFR	Аюулгүй байдлын функцын шаардлага (АБФШ)
SME	Жижиг, дунд үйлдвэрлэл (ЖДҮ)
ST	Аюулгүй байдлын үзүүлэлт (АБҮ)
TEL	Холбоо, мэдээллийн ажлын хэсэг (ХМАХ)
TOE	Үнэлгээний объект (ҮО)
WPISP	Мэдээллийн аюулгүй байдал, нууцлалын ажлын хэсэг (МАБНАХ)
WSIS	Мэдээлэлжсэн нийгмийн дэлхийн дээд хэмжээний чуулга уулзалт (МНДДХЧ)

ТЭМДЭГЛЭГЭЭ

 Кейс судалгаа

 Асуултууд

 Дасгал

 Өөрийгөө шалгах нь

1. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ХЭРЭГЦЭЭ

Энэхүү хэсэг нь дараах зорилготой:
- **Мэдээлэл ба мэдээллийн аюулгүй байдлын тухай ойлголтыг тайлбарлах;**
- **Мэдээллийн аюулгүй байдлын ажиллагаанд ашиглагддаг стандартуудыг тодорхойлох**

Өнөөгийн хүн төрөлхтний амьдрал мэдээлэл, харилцаа холбооны технологи (МХХТ)-оос ихээхэн хамааралтай байна. Энэ нь хувь хүн, байгууллагууд хийгээд улс үндэстэнг цахим халдлага (hacking), кибер терроризм, кибер гэмт хэрэг гэх мэт мэдээллийн системийн халдлагуудад өртөмхий болгож байна. Цөөн хувь хүн, албан байгууллагууд иймэрхүү дайралтыг давах хамгаалалтаар тоноглогдсон байдаг. Засгийн газрууд мэдээлэл, харилцаа холбооны дэд бүтцийг өргөтгөн, мэдээллийн аюулгүй байдлын эсрэг заналхийллээс хамгаалах системүүдийг байгуулах замаар мэдээллийн аюулгүй байдлыг хангахад чухал үүрэг гүйцэтгэнэ.

1.1 Мэдээллийн аюулгүй байдлын тухай үндсэн ойлголт

“Мэдээлэл” гэж юу вэ?

Ерөнхийдөө, мэдээллийг оюун ухааны үйл ажиллагааны үр дүн гэж тодорхойлдог. Энэ нь мэдээллийн хэрэгслээр дамжуулагддаг биет бус бүтээгдэхүүн юм. МХХТ-ийн салбарт мэдээлэл бол өгөгдлийн боловсруулалт, ашиглалт, зохион байгуулалтын үр дүн ба энгийнээр бол баримтын цуглуулга юм.

Мэдээллийн аюулгүй байдлын салбарт мэдээллийг “хөрөнгө” гэж тодорхойлдог. Энэ нь үнэ цэнэ бүхий зүйл учраас хамгаалагдах ёстой зүйл юм. Энэхүү IS/IEC 27001-ын тодорхойлолтыг энэ модулийн хүрээнд ашиглана.

Мэдээлэлд өгч буй ач холбогдол нь өнөөдөр хөдөө аж ахуйн нийгмээс аж үйлдвэрийн нийгэм рүү, эцэст нь мэдээлэлд чиглэсэн нийгэм рүү шилжих шилжилтийг харуулдаг. Хөдөө аж ахуйн нийгэмд газар хамгийн чухал хөрөнгө байсан бөгөөд буудайн хамгийн том үйлдвэрлэлтэй орон өрсөлдөх чадвартай байдаг байв. Аж үйлдвэрийн нийгэмд газрын тосны нөөцтэй байх гэх мэт хөрөнгийн бат бэх байдал өрсөлдөх чадварын гол хүчин зүйл нь байсан. Мэдлэг, мэдээлэлд суурилсан нийгэмд, мэдээлэл нь хамгийн чухал хөрөнгө бөгөөд мэдээлэл цуглуулж, дүн шинжилгээ хийж ашиглах чадвар нь ямар ч улсын өрсөлдөх чадварыг илэрхийлэх давуу тал юм.

Хүмүүсийн үзэл санаа бодит хөрөнгийн үнэ цэнээс мэдээллийн хөрөнгийн үнэлэмж рүү шилжихийн хэрээр мэдээллийг хамгаалах ёстой гэсэн үзэл санаа улам бүр гүнзгийрч байна. Мэдээлэл нь өөрөө түүнийг агуулж буй хэвлэл, мэдээллийн хэрэгслээс илүү үнэлэгддэг. 1-р хүснэгтэд мэдээллийн хөрөнгийг биет хөрөнгөтэй харьцуулсан харьцуулалтыг харууллаа.

Хүснэгт 1. Мэдээллийн хөрөнгө ба биет хөрөнгийн харьцуулалт

Онцлог	Мэдээллийн хөрөнгө	Биет хөрөнгө
Хэлбэр - ашиглалт	Биет хэлбэргүй бөгөөд уян хатан байх чадвартай	Биет хэлбэртэй
Үнэ цэнэ - хувьсах шинж	Нэгтгэж боловсруулагдсан үедээ илүү өндөр үнэ цэнэтэй байна	Нийт үнэ цэнэ нь нэгж үнэ цэнийн нийлбэр
Хамтран ашиглах боломж	Мэдээллийн хөрөнгийг хуулбарлан үйлдвэрлэх боломж хязгааргүй бөгөөд хүмүүс үнэ цэнийг нь хуваалцаж болдог.	Хуулбарлан үйлдвэрлэх боломжгүй; хуулбарлан үйлдвэрлэснээр хөрөнгийн үнэ цэнэ буурдаг
Хэвлэл мэдээллийн хэрэгсэл-хамаарал	Хэвлэл мэдээллийн хэрэгслээр дамжин хүрэх шаардлагатай	Аливаа хамааралгүйгээр хүрэх боломжтой (биет хэлбэрээс шалтгаалан)

Хүснэгт 1-д үзүүлсэнээр мэдээллийн хөрөнгө нь биет хөрөнгөнөөс нилээд ялгаатай байна. Тиймээс мэдээллийн хөрөнгө нь төрөл бүрийн эрсдэлд эмзэг байдаг.

Мэдээллийн хөрөнгөд учрах эрсдэл

Мэдээллийн хөрөнгийн үнэ цэнэ өсөхөд мэдээллийг олж авч, хянах хүсэл сонирхол хүмүүсийн дунд нэмэгддэг. Төрөл бүрийн зорилгоор мэдээллийг ашиглах бүлгүүд бий болж зарим нь мэдээллийн хөрөнгийг ямар ч хамаагүй аргаар олж авахын тулд ихээхэн хүчин чармайлт гаргадаг. Сүүлийн дурдсан зүйлд халдлага, зохиогчийн эрх зөрчих, компьютерийн вирусаар мэдээллийн системийг гэмтээх болон бусад аргууд орно. Мэдээлэлжихтэй холбоотой эдгээр эрсдлүүдийг энэ модулийн 2-р хэсэгт авч үзнэ.

Мэдээлэлд суурилсан орчны сөрөг талд дараах зүйлс орно. Үүнд:

Нэр нууцлалтай байдлаас үүдэн гарах ёс зүйгүй авир ихсэнэ - МХХТ-ийг нэрийн нууцлагдмал байдлыг хадгалахад ашиглаж болох ба ингэснээр тодорхой хувь хүн мэдээллийг хууль бусаар олж авах зэргээр ёс зүйгүй, гэмт хэргийн шинжтэй авир, үйлдэл гаргахад хялбар болдог.

Мэдээллийн эзэмшил ба хяналттай холбоотой зөрчилдөөн - Мэдээллийн эзэмшил ба хяналтаас үүдэн гарсан хүндрэл мэдээлэлжилт өргөжихтэй холбоотойгоор ихэсч байгаа. Жишээлбэл, “цахим - засаглал” гэсэн далбаан дор хувь хүний мэдээллийн сан байгуулах оролдлого хийхтэй зэрэгцэн зарим салбарууд хувь хүний мэдээллийг бусад талуудад задлах зэргээр хувийн нууцад халдаж болох учир, энэ талаар засгийн газар санаа зовниж буйгаа илэрхийлээд байгаа.

Нийгэм, улс орны хоорондох мэдээлэл ба баялгийн зөрүү - Мэдээллийн хөрөнгө эзэмшлийн хэмжээ нь мэдлэг/мэдээлэлд чиглэсэн нийгмийн баялгийг хэмжих хэмжүүр болдог. Хөгжингүй орнууд илүү их мэдээлэл үйлдвэрлэж, мэдээллийг бүтээгдэхүүн хэлбэрээр худалдаалан ашиг олох чадвартай байдаг. Тэгвэл мэдээлэл дутмаг орнуудын хувьд зөвхөн мэдээлэл олж авахын тулд их хэмжээний хөрөнгө оруулалт хэрэгтэй байдаг.

Дэвшилтэт сүлжээнээс үүдэн гарсан өсч буй мэдээллийн хандалт - Мэдлэг/мэдээлэлд суурилсан нийгэм бол сүлжээний нийгэм юм. Дэлхий бүхэлдээ нэг сүлжээ шиг холбогддог. Энэ нь сүлжээний нэг хэсэг дэх сул байдал нь бусад хэсэгтээ сөргөөр нөлөөлнө гэсэн үг юм.

Мэдээллийн ашиглалтын байдал гэж юу вэ?

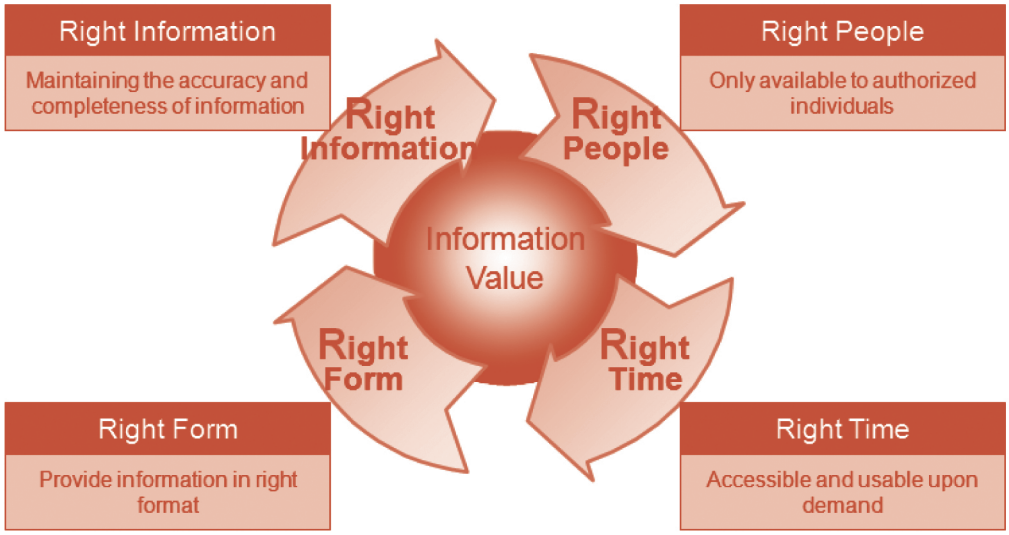
Мэдээллийг хууль бусаар олж авах оролдлогын хариуд хүмүүс мэдээлэлтэй холбоотой гэмт хэргээс сэргийлэх эсвэл ийм төрлийн гэмт хэргийн учруулах хохирлыг багасгахад идэвхи чармайлт гаргаж байна.

Энгийнээр хэлбэл, мэдээллийн ашиглалтын байдал бол мэдээллийн үнэ цэнийг таньж түүнийг хамгаалах явдал юм.

Мэдээллийн ашиглалтын байдлын 4R

Мэдээллийн ашиглалтын байдлын 4R гэдэг бол зөв мэдээлэл (Right information), зөв хүмүүс (Right people), зөв цаг (Right time), зөв хэлбэр (Right form) юм. 4R-ыг хянах нь мэдээллийн үнэ цэнийг хадгалан, хянах хамгийн үр дүнтэй арга юм.

Зураг 1. Мэдээллийн ашиглалтын байдлын 4R



Зөв мэдээлэл гэдэг нь мэдээллийн нэгдмэл байдлыг хангадаг мэдээллийн үнэн зөв, бүрэн байдлыг илэрхийлнэ.

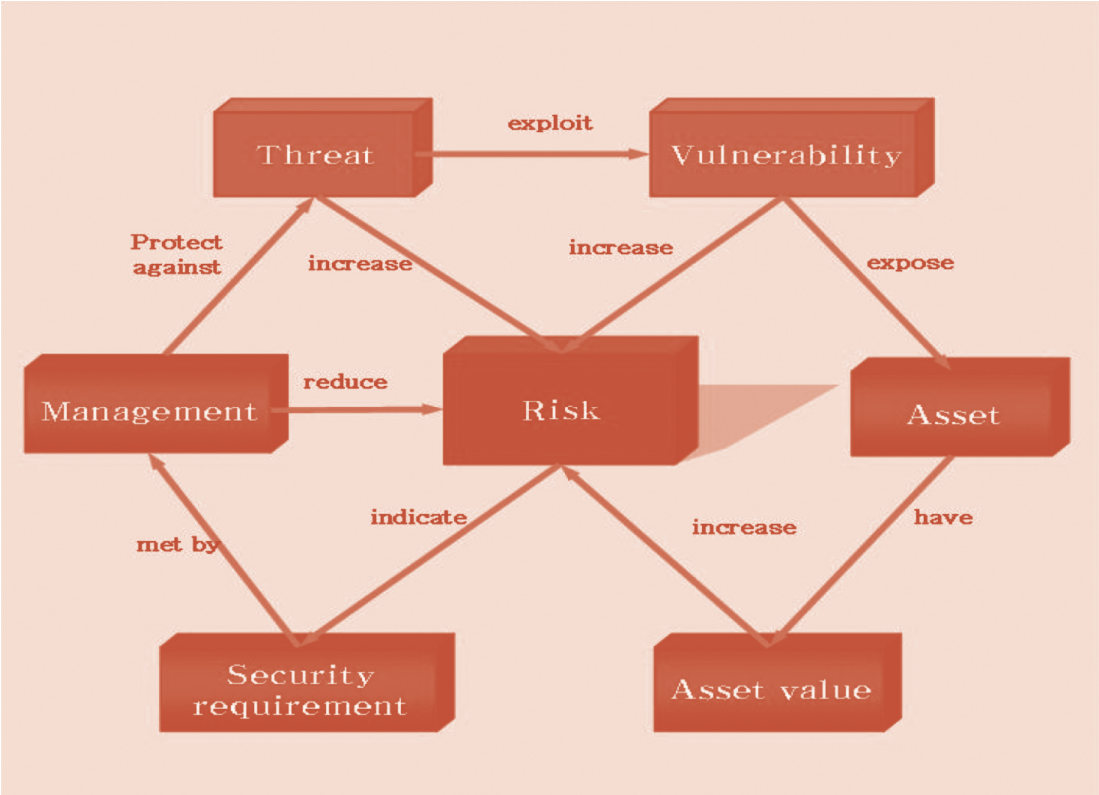
Зөв хүн гэдэг нь нууцлалыг хангахын тулд зөвхөн зөвшөөрөгдсөн хүмүүс мэдээллийг авах боломжтой байх гэсэн үг юм.

Зөв цаг гэдэг нь зөвшөөрөгдсөн этгээд шаардлагатай үедээ мэдээллийг авч ашиглана гэсэн утгыг илтгэнэ.

Зөв хэлбэр гэдэг нь мэдээллийг зөв хэлбэрээр хангах гэсэн үг юм.

Мэдээллийн ашиглалтын байдлыг хамгаалахын тулд 4R-ыг зөв ашиглах ёстой. Энэ нь мэдээлэлтэй харьцах үедээ нууцлал, нэгдмэл болон боломжит байдлыг дагаж мөрдөх ёстой гэсэн үг юм. Мэдээллийн ашиглалтын байдал нь мэдээллийн хөрөнгийн үнэ цэнэ, тэрчлэн тэдгээрийн эрсдэлд эмзэг байдал ба холбогдох аюул заналын талаар тодорхой ойлгосон байхыг шаарддаг. Үүнийг эрдслийн удирдлага гэж нэрлэдэг. Зураг 2-т мэдээллийн хөрөнгө ба эрсдлийн хоорондын харилцан холбоог харуулаа.

Зураг 2. Эрсдэл ба мэдээллийн хөрөнгө хоорондын харилцан холбоо



Эрсдэл нь хөрөнгийн үнэ цэнээр тодорхойлогддог. Томъёолбол:

Эрсдэл=∫(Хөрөнгийн үнэ цэнэ,аюул занал,эмзэг байдал)

Эрсдэл нь хөрөнгийн үнэ цэнэ, аюул занал эмзэг байдалтай шууд хамааралтай. Тиймээс хөрөнгийн үнэ цэнэ, аюул занал эмзэг байдлын хэмжээг удирдан зохицуулах замаар эрсдлийг ихэсгэж, бууруулах боломжтой. Үүнийг эрсдлийн удирдлагаар хийдэг.

Эрсдлийн удирдлагын аргуудад дараах орно:

Эрсдэл бууруулалт (эрсдэл багасгах)-аюул занал/эмзэг байдлын тохиолдох магадлал өндөр ч нөлөө нь бага тохиолдолд үүнийг хийнэ. Үүнд аюул занал, эмзэг байдал гэж юу болох тухай ойлгох, тэдгээрийг хувиргах, бууруулах болон хариу арга хэмжээ авч хэрэгжүүлэх зэрэг багтана. Гэхдээ эрсдлийн бууруулалт эрсдлийн утгыг “0” хүртэл бууруулж чадахгүй.

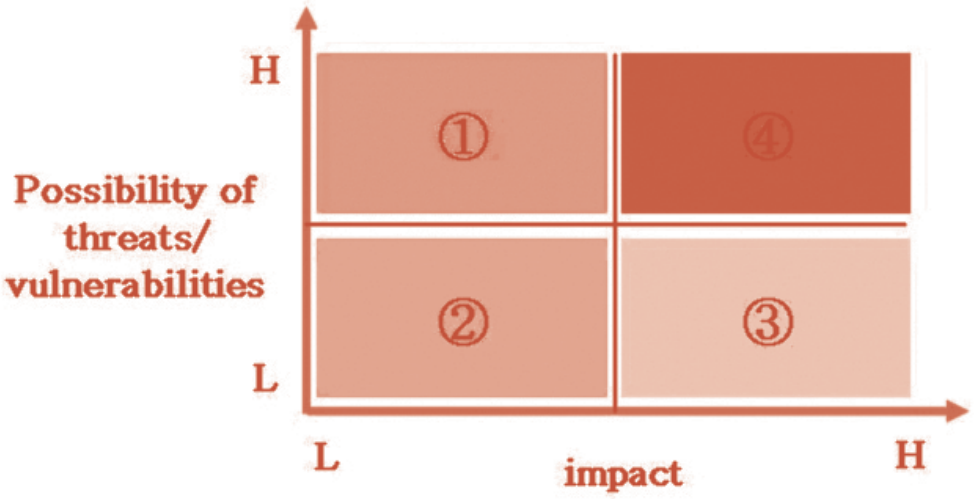
Эрсдэл хүлээн авах- аюул занал/эмзэг байдлын тохиолдох магадлал бага бөгөөд нөлөөлөл нь бага буюу зөвшөөрөх хэмжээнд байгаа үед хийгдэнэ.

Эрсдэл шилжүүлэлт-эрсдэл хэт өндөр боловч тухайн байгууллага шаардлагатай хяналтыг бэлтгэх боломжгүй тохиолдолд эрсдлийг байгууллагаас гадагш шижлүүлж болно. Үүний жишээ нь даатгалын бодлого авч хэрэгжүүлэх юм.

Эрсдлээс зайлсхийх- аюул занал, эмзэг байдал тохиолдох магадлал өндөр бөгөөд нөлөөлөл нь үлэмж их бол жишээ нь өгөгдөл боловсруулах тоног төхөөрөмж, хэрэгслийг гадаад эх үүсвэр рүү илгээх замаар эрсдлээс зайлсхийх нь хамгийн зөв арга юм.

Зураг 3-т эрсдлийн удирдлагын эдгээр дөрвөн аргыг графикаар дүрслэн харууллаа. Энэ зурагт “1” гэж тэмдэглэгдсэн дөрвөлжин бол эрсдлийн бууруулалт,”2” нь эрсдэл хүлээн авах, “3” нь эрсдэл шилжүүлэлт, “4” нь эрсдлээс зайл схийх арга юм.

Зураг 3. Эрсдлийн удирдлагын аргууд



Possibility of threats/vulnerabilities- аюул занал/ эмзэг байдлын магадлал
Impact-нөлөө

Тохирох эрсдлийн удирдлагын аргыг сонгоход анхаарах гол зүйл нь өртөгийн хэмнэлттэй байдал юм. Эрсдэл бууруулах, хүлээн авах, шилжүүлэх, зайлсхийх төлөвлөгөөг гаргахын өмнө өртөгийн хэмнэлттэй байдлын дүн шинжилгээг хийх нь зүйтэй.

1.2 Мэдээллийн аюулгүй байдлын үйл ажиллагааны стандартууд

Нэгдсэн удирдлагын болон техникийн төлөвлөгөөг ашиглалгүйгээр мэдээллийн аюулгүй байдлын үйл ажиллагааг үр дүнтэйгээр явуулж чадахгүй.

Олон байгууллагууд мэдээллийн аюулгүй байдлын үйл ажиллагааны стандартуудыг дэвшүүлээд байгаа. Жишээлбэл Олон улсын Стандартчилалын Байгууллага болон Олон улсын Электротехнкийн Хорооны (ISO/IEC) мэдээллийн аюулгүй байдлын шаардлагууд болон Мэдээллийн Системийн Хяналт, Шалгалтын Холбооны мэргэшсэн мэдээллийн системийн аудитор- MMCA (Certified Information Systems Auditor) болон мэргэшсэн мэдээллийн системийн аюулгүй байдлын мэргэжилтэн- MMCAБМ (Certified Information System Security Professional)-ын үнэлгээний элементүүд зэрэг болно. Эдгээр стандартууд нь мэдээллийн аюулгүй байдлын бодлого, мэдээллийн аюулгүй байдлын байгууллагын байгуулалт ба үйл ажиллагаа, хүний нөөцийн удирдлага, материаллаг аюулгүй байдлын удирдлага, техникийн аюулгүй байдлын удирдлага, аюулгүй байдлын хяналт ба бизнесийн тасралтгүй байдлын удирдлага гэх мэт нэгдмэл мэдээллийн аюулгүй байдлын үйл ажиллагаануудыг дэвшүүлдэг.

Хүснэгт 2-т мэдээллийн аюулгүй байдлын хамрах хүрээтэй холбоотой стандартуудын жагсаалтыг харууллаа.

Хүснэгт 2. Мэдээллийн аюулгүй байдлын хамрах хүрээ ба холбогдох стандартууд

Аюулгүй байдлын хамрах хүрээ	ISO/IEC 27001	ММСА	ММСАБМ
Удирдлагын	• Аюулгүй байдлын бодлого	• МТ-ийн засаглал	• Аюулгүй байдлын удирдлагын туршлагууд • Аюулгүй байдлын архитектур ба загварууд
	• Мэдээллийн аюулгүй байдлын зохион байгуулалт	• МТ-ийн засаглал	
	• Хөрөнгийн удирдлага	• Мэдээллийн хөрөнгийн хамгаалалт	• Аюулгүй байдлын удирдлагын туршлагууд
	• Хүний нөөцийн аюулгүй байдал		
	• Мэдээллийн аюулгүй байдлын ослын удирдлага	• Бизнесийн тасралтгүй байдал ба гамшгийн сэргээлт	• Бизнесийн тасралтгүй байдлын төлөвлөлт ба гамшгийн нөхөн сэргээлтийн төлөвлөлт
	• Бизнесийн тасралтгүй байдлын удирдлага	• Бизнесийн тасралтгүй байдал ба гамшгийн сэргээлт	• Бизнесийн тасралтгүй байдлын төлөвлөлт ба гамшгийн нөхөн сэргээлтийн төлөвлөлт
	• Хууль эрх зүйн биелэлт	• IS аудитын явц	• Хууль, судалгаа, ёс зүй
Материаллаг	• Материаллаг ба байгаль орчны аюулгүй байдал		• Материаллаг аюулгүй байдал
Техникийн	• Харилцаа холбоо, үйл ажиллагааны удирдлага	• Систем, дэд бүтцийн мөчлөгийн удирдлага	• Криптограф • Харилцаа, холбоо ба сүлжээний аюулгүй байдал • Үйл ажиллагааны аюулгүй байдал
	• Хандалт хянах		
	• Мэдээллийн системийг эзэмших, хөгжүүлэх ба ашиглах	• МТ-ийн үйлчилгээг хүргэх ба дэмжлэг үзүүлэх	

ISO/IEC27001[1] нь удирдлагын аюулгүй байдалд төвлөрдөг. Ялангуяа, захиргааны дэг журмын тухайд бичиг баримт болон үйл ажиллагааны хяналт ба бодлого/заавар, хуулийн мөрдөлтийг онцолдог. Удирдах ажилтны тасралтгүй баталгаажуулалт болон хариу арга хэмжээ шаардагддаг. Тийм учраас ISO/IEC27001 нь аюулгүй байдлын систем, тоног төхөөрөмж гэх зэргийг удирдлагын арга байдлаар авч үзэхийг хичээдэг.

Харин эсрэгээрээ, аудитын үйл ажиллагаа, мэдээллийн системийн хяналт дээр төвлөрдөг ММСА[2]-д хүний нөөцийн болон материаллаг аюулгүй байдлын талаар огт дурдагдаагүй. Энэ утгаараа аудиторуудын үүрэг ба аудитын гүйцэтгэл маш чухалд тооцогддог.

ММСАБМ[3] нь техникийн аюулгүй байдалд голчлон анхаардаг. Энэ нь сервер, компьютерүүд гэх мэт тоног төхөөрөмжийн зохион байгуулалт, хяналтыг онцолдог.

ДАСГАЛ

1. Өөрийн байгууллага доторх гишүүдийн дундах мэдээллийн аюулгүй байдлын ойлголтын талаарх төвшнийг үнэл.

2. Танай байгууллага мэдээллийн аюулгүй байдлын ямар арга хэмжээнүүдийг хэрэгжүүлдэг вэ? Тэдгээрийг мэдээллийн аюулгүй байдлын дөрвөн аргын хүрээнд ангил.

3. Өөрийн байгууллага доторх эсвэл өөрийн улс, харьяа нутгийн бусад байгууллагуудын доторх удирдлагын, материаллаг болон техникийн хүрээний мэдээллийн аюулгүй байдлын арга хэмжээнүүдийн жишээг тодорхойл.

Сургалтанд оролцогсод энэхүү дасгалыг багаар хийж болно. Хэрэв оролцогчид өөр өөр улсаас ирсэн бол улсаар нь жижиг бүлэг болгож болно.

ӨӨРИЙГӨӨ ШАЛГАХ НЬ

1. Мэдээлэл бусад хөрөнгөнөөс юугаараа ялгагдаж байна вэ?

2. Мэдээллийн аюулгүй байдал яагаад бодлогын хэмжээний асуудал болж байна вэ

3. Мэдээллийн аюулгүй байдлыг хангах ямар аргууд байдаг? Мэдээллийн аюулгүй байдалд хандсан янз бүрийн аргуудыг ангил.

4. Мэдээллийн аюулгүй байдлын хамрах хүрээ тус бүрээр ялга (удирдлагын, материаллаг ба техникийн)

1. ISO, “ISO/IEC27001:2005” http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm? csnumber=42103.
2. ISACA-г харна уу, “Мэдээллийн системийн аудитын стандартууд” http://www.isaca.org/Template. cfm?Section=CISA_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=19566.
3. (ISC)l-г харна уу. “CISSP® - Мэдээллийн системийн аюулгүй байдлын мэргэшсэн мэргэжилтэн” http://www.isc2.org/cissp.

2. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ХАНДЛАГА БА ЧИГЛЭЛ

Энэхүү хэсэг нь дараах зорилготой:
- **Мэдээллийн аюулгүй байдалд учрах аюул занал; ба**
- **Ийм төрлийн аюул заналын эсрэг авах арга хэмжээг тодорхойлох**

2.1 Мэдээллийн аюулгүй байдалд халдах халдлагын төрлүүд

Халдлага (Hacking)

Халдлага гэж мэдээлэл авах, өөрчлөхийн тулд компьютер болон компьютерийн сүлжээнд албан ёсны зөвшөөрөлгүйгээр нэвтрэхийг хэлнэ.

Халдлагын зорилгоос хамаарч зугаацлын, гэмт хэргийн болон улс төрийн гэж ангилдаг. Зугаацлын шинжтэй халдлага нь тухайн хууль бусаар нэвтрэгч этгээд сониуч зан авирын улмаас програм болон өгөгдлийг зөвшөөрөлгүй өөрчлөх ажиллагаа юм. Гэмт хэргийн шинжтэй халдлагыг залилан болон тагнуулын зорилгоор ашигладаг. Улс төрийн хууль халдлага гэж зөвшөөрөлгүй улс төрийн мэдээ, мэдээллийг цацахын тулд вебсайт руу нэвтрэхийг хэлнэ[4].

Сүүлийн үед халдлага нь кибер заналхийлэл ба кибер дайны нэг хэсэг болох нь улам бүр ихэсч энэ нь үндэсний аюулгүй байдалд ихээхэн аюулыг учруулж байна.

ХЯТАД, АМЕРИКИЙН СҮЛЖЭЭНИЙ ДАЙН

Америкийн Нэгдсэн улсад (АНУ) төвтэй ПойзонБокс гэх хакерын бүлэг Хятадын 350 гаруй сайтуудын үйл ажиллагааг сарын турш доголдуулсан хэргээр буруутгагдсан. Тус бүлэг нь Хятадын төрийн найман байгууллагын вебсайтад 2001 оны 4 сарын 30-нд халдсан гээд хэдийнээ Хятадын 24 вебсайт руу халдчихаад байв. Үүний дараа Хятадын хакерууд Үндэсний батлан хамгаалахын төлөөх зургаа дахь удаагийн сүлжээний дайныг зарлаж 2001 оны 4 сарын 30-наас 5 сарын 1-ны хооронд АНУ-ийн засгийн газрын байгууллагуудын вебсайтууд гэх мэт АНУ-д төвтэй сайтууд руу халдсан байна. Халдлагууд нь Пентагоныг компьютерийн системийн хамгаалалтын төвшнөө INFO-CON NORMAL-аас INFO-CON ALPHA руу өсгөхөд хүргэв.

2001 оны 5 сарын 1-ны өдөр Холбооны мөрдөх товчооны Үндэсний дэд бүтцийн хамгаалалтын төвөөс Хятадын хакерууд АНУ-ын засгийн газрын болон компанийн веб сайтууд руу дайралт хийж буй талаар анхааруулга гаргасан байна.

Сүлжээний дайны дараагаар АНУ цахим заналхийлэл (хууль бус нэвтрэлт зэрэг) нь АНУ-ын засгийн газрын байгууллагуудад маш их хохирол учруулах чадвартай гэдгийг хүлээн зөвшөөрсөн бөгөөд үүний дараагаар мэдээллийн аюулгүй байдлын төсөв болон засгийн газрын байгууллагуудын доторх мэдээллийн бодлогыг сайжруулах зэрээр кибер заналхийлэлийн эсрэг хамгаалалтыг нэмэгдүүлсэн байна.

Эх сурвалж: Attrition.org, “Cyberwar with China: Self

4. Suresh Ramasubramanian, Salman Ansari ба Fuatai Purcell, “Governing Internet Use: Spam, Cybercrime and e-Commerce,” in Danny Butt (ed.), Internet Governance: Asia-Pacific Perspectives (Bangkok: UNDP-APDIP, 2005), 95, http://www.apdip.net/projects/igov/ICT4DSeries-iGov-Ch5.pdf.

Үйлчилгээг бусниулах довтолгоо (Denial-of-Service)

Үйлчилгээг бусниулах довтолгоо- УБ (Denial of Service) зэрэг халдлагууд нь хууль бус нэвтрэгч машин болон өгөгдөл рүү зөвшөөрөлгүйгээр нэвтэрч байхад хууль ёсны хэрэглэгчид үйлчилгээг ашиглах боломжгүй байдаг.

Энэ нь халдлага үйлдэгчид сүлжээг их хэмжээний өгөгдлөөр "ачаалж" эсвэл процесс хяналтын хаалт, хүлээгдэж буй сүлжээний холболт гэх мэт хязгаарлагдмал нөөцийг зориудаар ашиглах зэргээр үйлдэгдэнэ. Эсвэл тэд сүлжээний бүрдэл хэсгийг тасалдуулах болон цоожлогдсон өгөгдөл гэх мэт шилжилтийн шатанд байгаа өгөгдлийг ашигладаг[5].

ЭСТОНИЙН ЭСРЭГ КИБЕР ЗАНАЛХИЙЛЭЛ

2007 оны 5 сарын 4-нд Эстонийн нийслэл хотод, ЗХУ-ын ялалтын хөшөөг хотын төвөөс цэргийн оршуулгын газар луу шилжүүлсэнээс үүдэн Эстоний эсрэг гурван долоо хоног үргэлжилсэн кибер халдлага гарсан бөгөөд сая сая компьютеруудад үйлчилгээг бусниулах довтолгоо (DoS) гэх мэт халдлагуудыг хийсэн байна. Ерөнхийлөгчийн ордон, Эстонийн парламент, эрх баригч нам, хэвлэл мэдээллийнхэн болон банкуудын компьютерийн сүлжээ, вебсайтууд доголдсон байна. Тэр бүү хэл утасгүй сүлжээ хүртэл халдлагад өртсөн байна. Хожим нь халдлага үйлдэгчийн байршил нь Оросын засгийн газрын байгууллага байсныг олж тогтоосон юм. Харин Оросын засгийн газар үүнийг няцаасан байна. Халдлагын эсрэг баг болон мэдээллийн аюулгүй байдлын бодлого дутмагийн улмаас Эстони тэрхүү кибер халдлага гарсан даруйд хариу арга хэмжээ авах боломжгүй байв.

Эх сурвалж: Beatrix Toth, "Estonia under cyber attack" (Hun-CERT, 2007), http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

Хортой код (Malicious code)

Хортой код гэж ажилласан тохиолдолд системд гэмтэл учруулдаг програмыг хэлдэг. Вирус, өт, трояны морь зэрэг нь хортой кодын төрлүүд юм.

Компьютерийн **вирус** гэдэг нь өөр програм, компьютерийн асах хэсэг эсвэл баримт бичигт өөрийн хувилбарыг үүсгэн олширч компьютерийн систем болон өгөгдлийг гэмтээдэг компьютерийн програм болон програмчилалын код юм.

Компьютерийн **өт** нь файлуудыг өөрчилдөггүй боловч автомат бөгөөд ихэнхдээ хэрэглэгчид харагддаггүй үйлдлийн системүүдийг ашиглан идэвхитэй санах ойн хэсэгт суудаг өөрийгөө олшруулдаг вирус юм. Тэдгээрийн хяналтгүй олшролт нь системийн нөөцийг зарцуулж бусад даалгавруудыг удаах болон зогсоодог. Өт байгаа нь илэрсэн тохиолдолд л ихэнхдээ ийм зүйл болдог.

Трояны морь нь хэрэгтэй ба/эсвэл аюулгүй мэт байдаг боловч үнэн хэрэгтээ нуугдсан програмууд эсвэл коммандын скриптыг зогсоож, системийг халдлагад өртөмхий болгох хортой ажиллагаатай юм.

5. ESCAP, "Module 3: Cyber Crime and Security," http://www.unescap.org/icstd/POLICY/publications /internet-use-for-businessdevelopment/module3-sources.asp.

БҮГД НАЙРАМДАХ СОЛОНГОС УЛСЫН 1.25 ИНТЕРНЭТ ХЯМРАЛ

2003 оны 1 сарын 25-нд ‘Slammer worm’ гэх компьютерийн вирус Бүгд Найрамдах Солонгос улсад орон даяар интернэтийн холболт тасалдахад хүргэсэн юм. 9 цаг гаруй үргэлжилсэн энэхүү тасалдал нь өтний улмаас устгагдсан домэйн нэрийн сервер (DNS)-ээс шалтгаалан үүссэн байна.

Энэхүү тасалдалын улмаас онлайн их дэлгүүрүүдийн алдагдал 200,000–500,000 ам.долларааp тоологдож, онлайн худалдааны алдагдал 22.5 тэрбум ам.долларт хүрсэн байна. Хохирогчид нь энгийн хэрэглэгчид байсан учраас Сламмер ворм worm вирусын учруулсан хохирол КодРед болон Нима гэх өтнүүдийн учруулсан хохирлоос илүү их байсан байна.

Тус интернэт хямрал нь Солонгосын засгийн газраас интернэтийн үйлчилгээ эрхлэгчид (ISP) болон мэдээллийн аюулгүй байдлын компаниудад зориулсан иж бүрэн менежментийг авч хэрэгжүүлэхэд нь түхэц өгсөн байна.

Мэдээллийн дэд бүтцийн хамгаалалт ба мэдээллийн аюулгүй байдлын үнэлгээний системүүд бий болсон бөгөөд байгууллага бүрт мэдээллийн аюулгүй байдлын байгууллага болон хороо байгуулагдсан байна.

Хувь хүний мэдээллийг цуглуулж халдлага хийх буюу Social engineering

“Social Engineering” гэх нэр томъёо нь нууц мэдээллийг задлахын тулд хүмүүсийг ашиглахдаа хэрэглэдэг техникийг илэрхийлдэг.

Хэдийгээр энэ нь нууц задруулалт болон залилантай төстэй боловч энэхүү нэр томъёог хууль бусаар мэдээлэл цугуулах болон компьютерийн систем рүү нэвтрэх үйл ажиллагааг тодорхойлоход ашигладаг. Ихэнх тохиолдолд халдагч нь хохирогчтой нүүр тулдаггүй.

Санхүүгийн залилан үйлдэх зорилгоор хувийн мэдээллийг интернэтээр дамжуулан хулгайлах үйлдэл болох фишинг нь үүний жишээ юм. Фишинг нь интернэт дэх ноцтой гэмт хэргийн үйл ажиллагаа болоод байна.

ШВЕДИЙН БАНК “ХАМГИЙН ТОМ” ОНЛАЙН ХУЛГАЙД ӨРТСӨН ТУХАЙ

2007 оны 1 сарын 19-нд Шведийн Норди банк онлайн фишингд өртсөн. Халдлага нь банкны нэрээр зарим үйлчлүүлэгчид рүү нь илгээсэн өөрчлөлт хийсэн Троянаар эхэлсэн байна. Илгээгч нь үйлчлүүлэгчдийг ‘спамтай тэмцэх’ аппликэйшнийг татаж авахыг уриалсан байна. raking.zip’ болон ‘raking.exe’ гэсэн нэртэй хавсаргасан файлыг татаж авсан хэрэглэгчдэд зарим хамгаалалтын компаниудын ‘haxdoor.ki’ гэж нэрлэдэг Троян халдварласан байна.

Хаксдоор нь товчлуурын даралтыг бичихийн тулд килоггерыг суулгаж рүүткит ашиглан өөрийгөө нуудаг. Трояны .ki хувилбарын пэйлоад нь хэрэглэгч Норди онлайн банкны системд холбогдох оролдлого хийхэд идэвхжсэн байна. Хэрэглэгчийг нэвтрэх дугаар гэх мэт нэвтрэх мэдээллээ оруулах хуурамч хуудас руу чиглүүлдэг. Хэрэглэгч мэдээллээ оруулсны дараа алдаа заасан санамж гарч тэдэнд сайт техникийн сааталд орсон тухай мэдээлсэн байна. Дараа нь гэмт этгээдүүд үйлчлүүлэгчдийн данснаас мөнгө авахын тулд цуглуулсан үйлчлүүлэгчийн мэдээллийг жинхэнэ Нордигийн вебсайт дээр ашигласан.

Энэхүү троян агуулсан и-мэйл Нордигийн үйлчлүүлэгчид рүү 15 сарын турш илгээгдсэн байна. Банкны хоёр зуун тавин үйлчлүүлэгч үүнд өртсөн гэж мэдээлж байгаа ба хохирол 7-8 сая Швейцарь кроны (USD 7,300–8,300) хооронд тоологдож байна.

Энэ тохиолдол нь кибер халдлага өндөр төвшний аюулгүй байдлын хамгаалалттай санхүүгийн компаниудад ч нөлөөлөх чадвартай болохыг баталж байна.

Эх сурвалж: Tom Espiner, “Swedish bank hit by ‘biggest ever’ online heist,” ZDNet.co.uk (19 January 2007), http://news.zdnet.co.uk/security/0,1000000 189,39285547,00.htm

2.2 Мэдээллийн аюулгүй байдал дахь аюулын хандлага[6]

Мэдээллийн аюулгүй байдлыг хамгаалах чухал үйл ажиллагаа бол аюулүй байдал дахь аюулын хандлагын дүн шинжилгээ юм. Энэ нь аюулүй байдалд заналхийлж буй аюулын хэлбэрийн өөрчлөгдөх, хөгжих, шинэ чиглэл рүү орох болон шилжих зэрэг арга замуудыг олж мэдэхийн тулд удаан хугацаанд аюулүй байдалд заналхийлж буй хэлбэрүүдийг хайх гэсэн үг юм. Мэдээлэл цуглуулж, уялдуулах болон хэргийн талаарх мэдээллийг сайжруулах давтамжит үйл явцыг болзошгүй аюулыг урьдчилан таамаглах болон тэдгээр аюулуудад тохирох хариу үйлдлийг бэлтгэх боломжтой байхын тулд хийдэг.

Мэдээллийн аюулын байдал дахь аюул заналын хандлагын дүн шинжилгээг гүйцэтгэж энэ талаарх тайлан мэдээг түгээгч байгууллагуудад дараах орно. Үүнд:

- CERT (http://www.cert.org/cert/)
- Symantec (http://www.symantec.com/business/theme.jsp?themeid=threatreport)
- IBM (http://xforce.iss.net/)

Одоогоор мэдээлэгдээд байгаа мэдээллийн аюулын байдал дахь аюул заналын хандлагуудыг дор харууллаа.

6. This section is drawn from Tim Shimeall and Phil Williams, Models of Information Security Trend Analysis (Pittsburgh: CERT Analysis Center, 2002), http://citeseerx.ist.psu.edu/viewdoc /summary?doi=10.1.1.11.8034

Халдлагын хэрэгслийн автоматжилт[7]

Халдагч этгээдүүд одоо мянга мянган интернэт хостуудын мэдээллийг хурдан бөгөөд хялбарханаар цуглуулах боломж олгодог автомат хэрэгслийг ашиглаж байна.

Эдгээр автоматжсан хэрэгслүүдийг ашиглан сүлжээнүүдийг алсын зайнаас судалж тодорхой нэг сул талууд бүхий хостуудыг таних боломжтой. Халдагч этгээдүүд мэдээллийг хожим ашиглах зорилгоор хадгалдаг мөн бусдад ил болгох болон бусад халдагч этгээдүүдэд худалдаалдаг, эсвэл тэр даруй дайралт хийдэг.

Зарим хэрэгслүүд (cain&abel гэх мэт) нэг зорилтын төлөө хэд хэдэн жижиг халдлагуудыг автоматжуулан тохируулдаг. Жишээлбэл, халдагч этгээдүүд багц шинжигчийг ашиглан рутер болон галт ханын (firewall) нууц үгийг олж авах ба шүүлтүүийг идэвхигүйжүүлэхийн тулд нэвтрэн орж дараа нь сервер дээрх өгөгдлийг уншихдаа сүлжээний файл сервисийг ашигладаг.

Илрүүлэхэд бэрхшээлтэй байдаг халдлагын хэрэгслүүд

Зарим халдлагууд орчин үеийн илрүүлэгч багажаар илэрдэггүй халдлагын шинэ хэлбэрийг ашигладаг. Жишээ нь хакерийн нэг арга болох анти-форенсик (anti-forensic) техникүүдийг хадлагын хэрэгслүүдийн бодит шинжийг халхлах болон нуухад ашиглаж байна. Хувьсамтгай хэрэгслүүд ашиглагдах тоолондоо хэлбэрээ өөрчилдөг. Эдгээр хэрэгслийн зарим нь кибер текст дамжуулах протокол (HTTP) гэх мэт түгээмэл протоколыг ашигладаг ба энэ нь тэднийг хууль ёсны сүлжээний хөдөлгөөнөөс ялгахад хэцүү болгодог[8]. MSN мессенжерийн өт үүний тод жишээ юм. MSN Мессенжер Инстант-Мессеж (IM)-ийн клиент дэх компьютерийн өт нь өөрийн харилцагчдаа файл хүлээн авах гэж буй тухай анхааруулгыг эхэлж явуулсныхаа дараа халдвартай хэрэглэгчийн хаягны номноос системд халдварлах зорилго бүхий файлыг илгээдэг. Жинхэнэ IM хэрэглэгчийн төрх байдлыг тэр чигт нь хуулбарладаг ба энэ нь маш ноцтой юм.[9]

Эмзэг талуудын шуурхай илрүүлэлт

Жил бүр Компьютерийн хадлагын эсрэг багуудыг Зохицуулах Төв (Emergency Response Team Coordination Center-CERT/CC) руу өгдөг тайлан мэдээнд ордог програм хангамжийн бүтээгдэхүүний шинээр илрүүлсэн эмзэг талуудын тоо 2 дахин өсч байгаа нь администраторуудад системээ уялдуулан шинэчлэхэд хэцүү болгож байна.

Халдагч этгээдүүд үүнийг мэддэг бөгөөд энэ талыг нь ашигладаг.[10] Зарим халдагч этгээдүүд тэг-өдрийн (эсвэл тэг-цаг) халдлагыг эхлүүлдэг ба энэ нь администраторуудын хараахан олж мэдэж амжаагүй учраас хамгаалалт хийгээгүй байгаа компьютерийн програмын аль нэгэн эмзэг талыг ашигладаг компьютерийн заналхийлэл юм.[11]

Тэгш бус аюул заналын өсөлт ба халдлагын аргуудын нийлэмж

Тэгш бус аюул занал гэдэг нь халдагч этгээд хамгаалагчаас илүү давуу талтай байх нөхцлийг хэлдэг. Аюулын ашиглалт автоматжиж халдах хэрэгсэл боловсронгуй болж байгаа нь тэгш бус аюулын тоог нэмэгдүүлж байна.

---

7. Энэ хэсгийг авсан эх сурвалж, CERT, “Security of the Internet,” Carnegie Mellon University, http://www.cert.org/encyc_article/tocencyc.html
8. Suresh Ramasubrahmanian et al., op. cit., 94.
9. Munir Kotadia, “Email worm graduates to IM,” ZDNet.co.uk (4 April 2005), http://news.zdnet.co.uk /security/0,1000000189,39193674,00.htm.
10. Suresh Ramasubrahmanian et al., op. cit.
11. Wikipedia, “Zero day attack,” Wikimedia Foundation Inc., http://en.wikipedia.org/wiki /Zero_day_attack.
12. Symantec, Symantec Internet Security Threat Report: Trends for January–June 07, Volume XII (September 2007), 13, http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper _internet_security_ threat_report_xii_exec_summary_09_2007.en-us.pdf

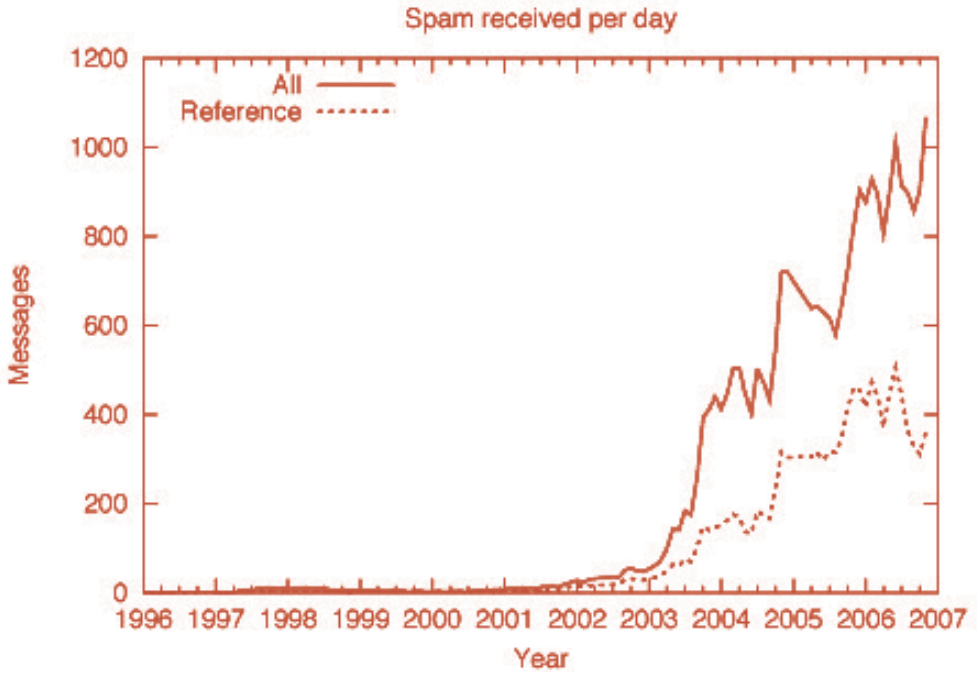
Халдлагын аргуудын нийлэмж гэдэг нь халдагчид зохион байгуулалттай хорлон сүйтгэх ажиллагааг дэмждэг дэлхий нийтийн сүлжээг бий болгохын тулд төрөл бүрийн халдлагын аргуудыг хооронд нь нэгтгэхийг хэлдэг. Үүний жишээ нь MPак серверүүдтэй холбогдож хэрэглэгчийн компьютерт суудаг MPак троян юм. Халдагч нь хууль ёсны сайтууд руу зочилж буй хэрэглэгчдийг аюултай веб сервер рүү чиглүүлэх эсвэл спам мессежүүдээр аюултай веб серверүүд рүү холбоос илгээх замаар тэдгээр серверүүдэд хөдөлгөөн бий болгодог. Эдгээр аюултай серверүүд хэрэглэгчийн хөтөчийг MPак серверүүд[12] рүү чиглүүлдэг.

Дэд бүтцийн халдлагын нэмэгдэж буй аюул

Дэд бүтцийн халдлага нь интернэтийн гол бүрэлдэхүүн хэсгүүдэд нөлөөлөх халдлагууд юм. Интернэт дэх олон тооны байгууллагууд болон хувь хүмүүс, тэдний өдөр тутмын ажил интернэтээс ихээхэн хамааралтай байдаг зэрэг нь эдгээрийг тулгамдсан асуудал болгож байгаа юм. Дэд бүтцийн халдлагууд нь ҮБ, эмзэг мэдээллийн эрсдэл, ташаа мэдээллийн тархалт болон бусад даалгавраас нөөцийн ихээхэн өөрчлөлтийг үүсгэнэ. Ботнет бол дэд бүтцийн халдлагын нэг жишээ юм. “ботнет-botnet” гэдэг нэр томъёо нь “командын хяналтын сервер”-ээр алсын зайнаас удирдагддаг халдвартай компьютерүүдийн бүлгийг хэлдэг. Халдвартай компьютерүүд нийт сүлжээний системд өт, вирусыг тараадаг.

Ботнетийн хэрэглээний улмаас спам хурдацтай өсч байна. Спам нь албан ёсоор илгээгдээгүй и-мэйл, мессенжер, хайлтын хэрэгсэл, блогууд тэр бүү хэл гар утсаар дамжих боломжтой нийтийг хамарсан мессежүүд юм. Зураг 4-т спамын төвшний хандлагыг харууллаа.

Зураг 4. Спамын статистик



Spam received per day-өдөрт хүлээн авдаг спам

БОТНЕТТЭЙ ТЭМЦЭХ НЬ

Ботнетийн уршгийг багасгахын тулд Олон Улсын Цахилгаан Холбооны Байгууллагаас бодлого, технологи ба нийгмийн арга зүйн нэгдлийг санал болгодог.

Бодлогын: Спам ба кибер гэмт хэргийн эсрэг үр дүнтэй бодлого, зохицуулалт

- Бодлого боловсруулалтанд оролцогч талуудын чадавхийг хөгжүүлэх
- Олон улсын харилцаа ба хамтын ажиллагааны цогц үндэс суурь
- Кибер гэмт хэрэг ба нууцлалын хууль эрх зүйн уялдаа холбоо
- Кибер гэмт хэрэг, ботнетийн хор хөнөөлийг бууруулах үндэс суурь

Техникийн: идэвхитэй ботнетийг таньж, тэдгээрийн талаарх мэдээллийг цуглуулах хэрэгсэл, техникүүд

- Ботнетийн хор хөнөөлийг бууруулах ISP-ын шилдэг туршлагууд
- Ботнетийн хор хөнөөлийг бууруулах бүртгэгч ба бүртгэлийн шилдэг туршлагууд
- Цахим-худалдаа болон онлайн гүйлгээний үйлчилгээ үзүүлэгчдэд зориулсан чадавхи хөгжүүлэлт

Нийгмийн: Интернэтийн аюулгүй байдал ба хамгаалалтын талаарх өргөн зурваст-суурилсан боловсролын санал, санаачлагууд

- Хэрэглэгчдийг аюулгүй МХХТ-ийн ашиглалтаар хангах PTF ITU SPAM хэрэгслийн багц нь бодлого төлөвлөгчид, зохицуулагчид болон компаниудад бодлогоо өөрчилж, и-мэйлд итгэх итгэлийн дахин сэргээхэд туслах иж бүрэн багц юм. Энэхүү багц нь олон улсад тулгарч буй асуудлуудаас сэргийлэхийн тулд мэдээллийг дэлхий даяар хуваалцахыг мөн санал болгодог.

Халдлагын зорилгын өөрчлөлт

Компьютер болон сүлжээний халдлагыг сониуч зангийн улмаас эсвэл хувь хүн зугаацах зорилгоор үйлддэг гэж ойлгодог байлаа.

Одоо ихэвчлэн мөнгө, нэр төр гутаах болон хорлон сүйтгэх зорилготой болсон. Түүнчлэн эдгээр төрлийн халдлагууд нь кибер гэмт хэргийн өргөн хүрээний жижигхэн хэсгийг л төлөөлдөг.

Кибер гэмт хэрэг гэдэг нь улс төр, эдийн засаг, шашин эсвэл үзэл суртлын шалтгаанаар дижитал мэдээлэл эсвэл мэдээллийн урсгалыг зориудаар сүйтгэн тасалдуулах ажиллагаа юм.

Хамгийн түгээмэл гэмт хэрэгт хууль бус нэвтрэлт, УБ, хортой код болон Social engineering орно. Сүүлийн үед кибер гэмт хэрэг нь үндэсний аюулгүй байдалд үзүүлэх сөрөг нөлөөгөөрөө кибер халдлага ба кибер дайны нэг хэсэг нь болоод байна.

Хүснэгт 3-т кибер гэмт хэргийн үйлдэгчид хэдий хэмжээний орлого олдог болохыг харууллаа.

Хүснэгт 3. 2007 онд кибер гэмт хэргээс олсон орлого

Орлого	Тухайн-ханш (Ам.долларааp)
Давтагдашгүй аюултай програм (adware) суулгалт бүрт төлөх төлбөр	АНУ-д 30 цент, Канадад 20 цент, Англид 10 цент, бусад газарт 2 цент
Аюултай програмын багц (Malware package), үндсэн хувилбар	$1,000 - $2,000
add-on үйлчилгээ бүхий аюултай програмын багц	$ 20-с эхлээд ханш нь өөр өөр
Ашиглах багцын түрээс – 1 цаг	$ 0.99 - $ 1
Ашиглах багцын түрээс – 2.5 цаг	$ 1.60 - $ 2
Ашиглах багцын түрээс – 5 цаг	$4, өөр байж болно
Мэдээлэл хулгайлах тодорхой нэг Трояны илрээгүй хуулбар	$80, өөр байж болно
Тархсан үйлчилгээг бусниулах довтолгоо (ҮБ)	Өдөрт $100
10,000 халдлагад өртсөн PC	$1,000
Хулгайлагдсан банкны дансны эрх	$50-с эхлээд ханш нь өөр өөр
1 сая цэвэр цуглуулсан (freshly-harvested) и-мэйл (гэрчлэгдээгүй)	Чанараас хамаарч $8 хүртэл

Эх сурвалж:Trend Micro, 2007 Threat Report and Forecast (2007), 41, http://trendmicro.mediaroom.com/file.php/66/2007+Trend+Micro+Report_FINAL.pdf

2.3 Аюулгүй байдлыг сайжруулах

Аюулгүй байдлын заналхийлэл ба халдлагын технологиудын хандлагаар бол бат бэх хамгаалалт нь хувьсан өөрчлөгдөж буй орчинд зохицох уян хатан стратеги, үндэслэл сайтай бодлого, журмууд, тохирох аюулгүй байдлын технологийн хэрэглээ, болон байнгын сонор сэрэмжийг шаардаж байна.

Одоогийн хамгаалалтын байдлыг тодорхойлох замаар аюулгүй байдлыг дээшлүүлэх хөтөлбөрийг эхлэх нь зүйтэй. Аюулгүй байдлыг хангах хөтөлбөрийн салшгүй хэсэг нь баримтжуулсан бодлого ба журмууд мөн тэдгээрийн хэрэгжилтийг дэмжих технологи юм.

Удирдлагын аюулгүй байдал, хамгаалалт

Удирдлагын аюулгүй байдал, хамгаалалт нь мэдээллийн аюулгүй байдлын стратеги, бодлого, чиглэлээс бүрдэнэ. Мэдээллийн аюулгүй байдлын стратеги нь бүх мэдээллийн аюулгүй байдлын үйл ажиллагааны чиглэлийг тогтоодог. Мэдээллийн аюулгүй байдлын бодлого нь байгууллагын хэмжээний мэдээллийн аюулгүй байдлын өндөр төвшний төлөвлөгөө юм. Энэ нь удирдлагын болон материаллаг хамгаалалтын төлөвлөгөө зэрэг тодорхой шийдвэр гаргахад зориулсан хүрээгээр хангадаг. Мэдээллийн аюулгүй байдлын бодлого нь урт хугацааны зорилттой байх хэрэгтэй учраас тодорхой нэг технологи руу чиглэсэн агуулгаас зайлсхийж оновчтой бизнесийн тасралтгүй байдлын төлөвлөгөө боловсруулалтыг багтаасан байх хэрэгтэй.

Мэдээллийн аюулгүй байдлын чиглэлийг мэдээллийн аюулгүй байдлын стратеги ба бодлогын дагуу тогтоох ёстой. Чиглэл нь мэдээллийн аюулгүй байдалтай холбоотой салбар тус бүрийн зохицуулалтыг тодорхойлох ёстой. Чиглэл нь дэлгэрэнгүй, хамрах хүрээний хувьд үндэсний хэмжээнийх байх ёстой, мөн тэдгээрийг байгууллагуудад мөрдлөг болгохын тулд засгийн газраас боловсруулан хэрэгжүүлэх хэрэгтэй.

Мэдээллийн аюулгүй байдлын стандартууд нь аюулгүй байдлыг мэдээллийн бүх салбарт ашиглагдаж болохоор төрөлжсөн бөгөөд нарийвчилсан байх ёстой. Улс орон бүр дэлхий даяар өргөн хэрэглэгддэг удирдлагын, материаллаг болон техникийн аюулгүй байдлын стандартуудыг судлан шинжилснийхээ дараа стандартаа боловсруулах нь зүйтэй.

Стандартууд нь тухайн үед зонхилж буй МХХТ-ийн орчинд тохиромжтой байх хэрэгтэй. Аливаа улсын мэдээллийн аюулгүй байдлын стратеги , бодлого, чиглэл нь холбогдох хуультайгаа нийцэх ёстой. Тэдгээрийн хамрах хүрээ нь үндэсний ба олон улсын хуулийн хүрээнд байх ёстой.

Мэдээллийн аюулгүй байдлын ажиллагаа ба явц

Мэдээллийн аюулгүй байдлын стратеги, бодлого, чиглэлээ нэгэнт тогтоосон бол мэдээллийн аюулгүй байдлын ажиллах журам, явцыг тодорхойлох хэрэгтэй. Хүмүүс мэдээлэл рүү халддаг, дотоодын мэдээллийг задалдаг учраас хүний нөөцийн удирдлага нь мэдээллийн аюулгүй байдлыг удирдах хамгийн чухал хүчин зүйл юм. Тиймээс бидэнд дараах зүйлс шаардлагатай:

1. Мэдээллийн аюулгүй байдлын боловсрол сургалтын хөтөлбөр – Мэдээлэл хамгаалалтын байгууллагын мэдээллийн аюулгүй байдлын төвшинг сайжруулах олон арга байдаг ч үндсэн ажиллагаа нь сургалт юм. Байгууллагын гишүүд мэдээллийн аюулгүй байдлын хэрэгцээг ойлгон хүлээн авч боловсрол сургалтаар дамжуулан холбогдох чадварыг эзэмших ёстой. Гэхдээ стандартчилагдсан мэдээллийн аюулгүй байдлын сургалтын хөтөлбөрүүд нь оролцоо муу бол үр дүнгүй болж болзошгүй учраас гол нь оролцоог нэмэгдүүлэх төрөл бүрийн хөтөлбөрийг боловсруулах нь чухал юм.

2. Төрөл бүрийн арга хэмжээгээр идэвхижүүлэлтийг бэхжүүлэх – Мэдээллийн аюулгүй байдлын стратеги, бодлого, чиглэлийг амжилттай хэрэгжүүлэхэд ажилтнуудын оролцоо чухал. Мэдээллийн аюулгүй байдлыг өдөр тутмын янз бүрийн үйл ажиллагаагаар ажилтнуудын дунд таниулан хэвшүүлэх хэрэгтэй.

3. Дэмжлэг олж авах –Ажилтнууд мэдээллийн аюулгүй байдлын талаар өндөр төвшний ойлголттой бөгөөд тэдэнд мэдээллийн аюулгүй байдлыг сахих хүсэл их байсан ч байгууллагын хамгийн дээд удирдлагуудын дэмжлэггүйгээр мэдээллийн аюулгүй байдлыг хангах хэцүү. Ерөнхий захирал болон мэдээлэл хариуцсан дээд удирдлагын дэмжлэгийг олж авах хэрэгтэй.

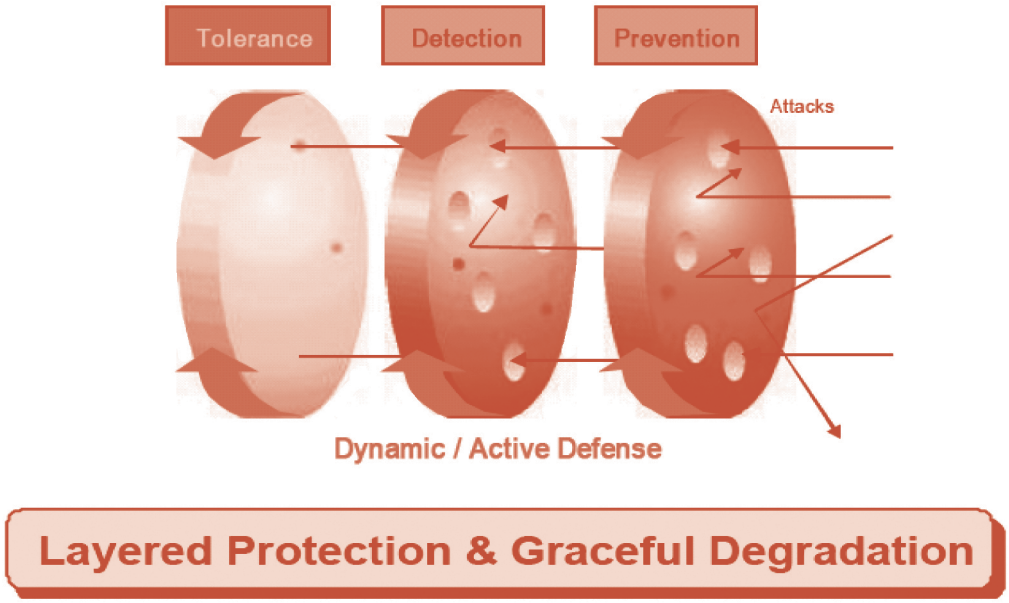
Аюулгүй байдлын технологи

Байгууллагуудад системээс халдлага үйлдэгчдээс хамгаалахад нь туслах зорилгоор төрөл бүрийн технологиудыг хөгжүүлж байгаа. Тэдгээр технологиуд нь систем ба мэдээллийг халдлагаас хамгаалж, хэвийн бус, сэжигтэй ажиллагааг илрүүлэн аюулгүй байдалд нөлөөлөх ажиллагаанд хариу өгөхөд тусалдаг.

Өнөөгийн хамгаалалтын системүүд нь технологиудын нэгдсэн удирдлага руу чиглүүлдэг Defense-In-Depth (DID) буюу гүнзгий төвшний хамгаалалтын загвар дээр тулгуурлан боловсруулагдсан байдаг. Энэхүү загвар нь бүх аюулын эсрэг ганцхан хамгаалалтын давхаргатай байдаг хязгаарт (perimeter) хамгаалалтаас ялгаатай. DID загвар нь сэргийлэлт, илрүүлэлт, тэсвэрлэлтээс бүрдэх ба шат тус бүрт аюулын хэмжээ буурдаг. (Зураг 5).

Зураг 5. Гүнзгий төвшний хамгаалалт

Эх сурвалж: Defense Science Board, Protecting the Homeland: Defensive Information Operations 2000 Summer Study Volume II (Washington, D.C.: Defense Science Board, 2001), 5, http://www.acq.osd.mil/dsb/reports/dio.pdf)



Халдлага эсэргүүцэх технологи

Халдлага эсэргүүцэх технологиуд нь хадгалалт ба системийн төвшний халдлага, аюулаас хамгаалдаг. Энд дараах технологиуд орно. Үүнд:

1. Криптограф (Cryptography) – нууцлал гэж нэрлэгддэг криптограф нь мэдээллийн өөрийн эх хэлбэрээс (ил бичвэр /plaintext/ гэж нэрлэдэг) кодчилсон, ойлгомжгүй хэлбэр (ciphertext гэж нэрлэдэг) лүү буулгах явц юм. Код тайлалт (decryption) нь кодчилсон текстийг авч буцаан үндсэн хэлбэр лүү нь оруулах явцыг хэлдэг. Криптографыг төрөл бүрийн аппликэйшнийг хамгаалахад ашигладаг. Криптограф болон холбогдох технологиудын (IPSec, SSH, SSL, VPN, OTP, г.м.) талаар илүү дэлгэрэнгүй мэдээллийг дараах веб сайтуудаас авах боломжтой:

   - IETF RFC (http://www.ietf.org/rfc.html)
   - RSA – EMC-ын нууцлал хамгаалалтын хэлтсийнхний өнөөдрийн криптографийн талаарх түгээмэл асуултуудад өгсөн хариултуудыг дараах холбоосоор орж үзнэ үү. (http://www.rsa.com /rsalabs/node.asp?id=2152)

2. Нэг-удаагийн нууц үг-ННҮ (One-Time Passport-OTP) – нэрнээс нь харахад, нэг удаагийн нууц үгийг зөвхөн нэг удаа ашиглаж болно гэсэн үг. Тогтмол нууц үгүүд нь алдагдах болон хулгайд өртөхдөө амархан байдаг. Энэ эрсдлийг ННҮ-ээр хийдэг шиг нууц үгээ тогтмол өөрчлөх замаар бууруулах боломжтой. Энэхүү шалтгааны улмаас ННҮ-ийг онлайн банкны үйлчилгээ зэрэг цахим санхүүгийн гүйлгээг хамгаалахад ашигладаг.

3. Галт хана (Firewall) –энэ нь өөр өөр итгэмжлэлийн төвшинтэй компьютерийн сүлжээнүүд хооронд, тухайлбал ямар нэг итгэмжлэлийн бүсгүй интернэт ба хамгийн өндөр төвшний итгэмжлэл бүхий дотоод сүлжээ хоорондын зарим хөдөлгөөний урсгалыг зохицуулдаг. Интернэт ба итгэмжлэгдсэн дотоод сүлжээ хооронд оршдог дундаж итгэмжлэлийн төвшинтэй бүсийг ихэвчлэн “хязгаарт сүлжээ” гэж нэрлэдэг.

4. Эмзэг байдлыг шинжлэх хэрэгсэл –халдлагын аргуудын тооны өсөлт болон түгээмэл хэрэглэгддэг програмуудад байх эмзэг талуудаас шалтгаалан системийн эмзэг байдлыг тодорхой цаг хугацаанд үнэлж байх шаардлагатай. Компьютерийн аюулгүй байдлын хувьд эмзэг байдал бол халдлага үйлдэгчид систем рүү нэвтрэх боломж олгодог сул тал нь юм. Эмзэг байдал нь сул нууц үг, програм хангамжийн халдвар, скрипт кодын тарилга (script code injection), SQL тарилга (SQL injection) болон малвэйр (malware) зэргээс үүдэн гарч болно. Эмзэг байдлыг шинжлэх хэрэгслүүд нь эдгээр эмзэг байдлуудыг илрүүлдэг. Эдгээрийг онлайнаар хялбархан авах боломжтой бөгөөд дүн шинжилгээний үйлчилгээ үзүүлдэг компаниуд ч мөн байдаг.

   Гэхдээ интернэт хэрэглэгчдэд үнэгүй авах боломжтой тэдгээр хэрэгслүүдийг халдлага үйлдэгчид буруугаар ашиглаж болох талтай. Илүү дэлгэрэнгүй мэдээлэл авахыг хүсвэл дараах сайтуудад зочлоорой:

   - INSECURE Security Tool (http://sectools.org)
   - FrSIRT Vulnerability Archive (http://www.frsirt.com/english)
   - Secunia Vulnerability Archive (http://secunia.com)
   - SecurityFocus Vulnerability Archive (http://www.securityfocus.com/bid)

Сүлжээнй эмзэг байдлыг шинжлэх хэрэгсэл нь рутер, галт хана сервер зэрэг сүлжээний нөөцийн эмзэг байдлыг шнжилдэг.

Серверийн эмзэг байдлыг шинжлэх хэрэгсэл нь дотоод систем дэх сул нууц үг, сул тохиргоо болон файлын зөвшөөрлийн алдааг эмзэг байдал гэж үзэн шинжилдэг. Энэхүү хэрэгсэл нь дотоод систем дэх илүү олон эмзэг байдлыг шинжилдэг учраас серверийн эмзэг байдлыг шинжлэх хэрэгсэл нь сүлжээнй эмзэг байдлыг шинжлэх хэрэгсэлтэй харьцуулахад харьцангуй бодит үр дүн өгдөг.

Халдлага илрүүлэх технологи

Илрүүлэх технологийг сүлжээ ба чухал системүүд дэх хэвийн бус байдал болон сэжигтэй нэвтрэлтийг илрүүлэн арилгахад ашигладаг. Илрүүлэлтийн технологид дараах орно:

1. Антивирус –Антивирус програм хангамж бол өт, фишинг халдлагууд, рүүткит, трояны морь болон бусад малвэйр гэх мэт хортой кодыг илрүүлж, арилгах зориулалт бүхий компьютерийн програм юм.[13]

2. Довтолгоон илрүүлэх систем-ДИС (Intrusion Detection System -IDS) – ДИС нь болзошгүй аюулгүй байдлын зөрчлийг илрүүлэхийн тулд компьютер, эсвэл сүлжээн доторх төрөл бүрийн талбараас мэдээлэл цуглуулан шинжилдэг. Халдлага илрүүлэх функцүүдэд хэвийн бус ажиллагааны дүн шинжилгээ ба халдлагын хэлбэрийг таних чадвар зэрэг орно.

3. Довтолгооноос сэргийлэх систем-ДСС (Intrusion prevention system -IPS) – Довтолгооноос сэргийлэх систем нь болзошгүй аюулыг олж илрүүлэн, тэдгээрийг халдлагад ашиглахаас нь өмнө хариу арга хэмжээ авахыг хичээдэг. ДСС нь сүлжээний хөдөлгөөнийг хянаж учирч болох аюулын эсрэг сүлжээний администраторын тогтоосон журмын дагуу шуурхай арга хэмжээ авдаг. Жишээлбэл, ДСС сэжиг бүхий IP хаягнаас ирэх хөдөлгөөнийг хааж болно.[14]

13. Wikipedia, “Antivirus software,” Wikimedia Foundation, Inc., http://en.wikipedia.org/wiki /Antivirus_software.
14. SearchSecurity.com, “Intrusion prevention,” TechTarget, http://searchsecurity.techtarget.com /sDefinition/0,,sid14_gci1032147,00.html.

Систем нэгтгэлийн технологи

Нэгдлийн технологи нь халдлагыг таамаглах, илрүүлэх, устгах зэрэг мэдээллийн аюулгүй байдлын чухал функцуудыг нэгтгэдэг. Нэгдлийн технологид дараах орно:

1. Байгууллагын аюулгүй байдлын удирдлага –БАБУ (Enterprise security management-ESM) - БАБУ систем нь тууштай бодлогод тулгуурлан ДИС, ДСС зэрэг мэдээллийн аюулгүй байдлын шийдлүүдийг удирдан зохицуулж, ажиллуулдаг. Үүнийг мэдээллийн аюулгүй байдлын шийдэл тус бүрийн давуу талыг ашиглаж, тууштай бодлогын дор мэдээллийн аюулгүй байдлын үр дүнг дээшлүүлэх замаар бусад шийдлүүдийн сул талыг нөхөх стратеги хэлбэрээр ашигладаг. Хамгаалалтын технологиудыг ажилуулах хүний нөөцийн хомсдол болон халдлагын аргуудын өөрчлөлт гэх мэт халдлагын шинэчлэл өссөн, мөн илрүүлэхэд хэцүү халдлагын хэрэгслүүд бий болсон зэргээс үүдэн одоогийн хамгаалалтын технологиудыг удирдаж чадах БАБУ-ууд нэгдмэл хэлбэрээр саяхнаас гарч ирсэн. БАБУ-аар удирдлагын үр ашиг дээшилж идэвхитэй хариу арга хэмжээ бий болно.

2. Байгууллагын эрсдлийн удирдлага- БЭУ (Enterprise risk management-ERM) - БЭУ нь мэдээллийн аюулгүй байдлын гадна орших хэсгийг оролцуулан байгууллагатай холбоотой бүх эрсдлүүдийг таамаглахад туслаж хариу арга хэмжээг автоматаар тохируулдаг систем юм. БЭУ-ыг мэдээлэл хамгаалахдаа ашиглахын тулд эрсдлийн удирдлагын зорилго ба системийн хөгжүүлэлтийн загварыг яг таг тодорхойлсон байх шаардлагатай.

Ихэнх байгууллагууд БЭУ-аа өөрсдөө биш мэдээллийн аюулгүй байдлын мэргэжлийн зөвлөх агентлагуудаар боловсруулан хийлгэдэг.

АСУУЛТ

1. Мэдээллийн аюулгүй байдлын ямар аюул заналд танай байгууллага эмзэг, өртөмхий вэ? Яагаад?

2. Мэдээллийн аюулгүй байдлын ямар технологийн шийдлүүд танай байгууллагад байдаг вэ?

3. Танай байгууллага мэдээллийн аюулгүй байдлын бодлого, стратеги, чиглэлтэй юу? Хэрэв байгаа бол, тэдгээр нь танай байгууллагын эмзэг аюул заналуудад хэр хангалттай вэ? Хэрэв байхгүй бол та байгууллагадаа зориулан юуг мэдээллийн аюулгүй байдлын бодлого, стратеги, чиглэлийн арга хэлбэрээр санал болгох вэ?

ӨӨРИЙГӨӨ ШАЛГАХ НЬ

1. Мэдээллийн аюулгүй байдлын аюулын хандлагын шинжилгээг яагаад явуулах хэрэгтэй вэ?

2. Мэдээллийн аюулгүй байдлын ажиллагаанд хүний нөөц яагаад хамгийн чухал хүчин зүйл болдог вэ? Мэдээллийн аюулгүй байдалд зориулсан хүний нөөцийн удирдлагын гол ажилагаанууд юу вэ?

3. Технологийн аюулгүй байдлын DID загварыг тайлбарла. Энэ нь ямар байдлаар ажилладаг вэ?

3. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ҮЙЛ АЖИЛЛАГАА

Энэхүү хэсэг нь дараах зорилготой:
- **Мэдээллийн аюулгүй байдлын бодлого боловсруулалтанд чиглэл өгөх зорилгоор өөр өөр улсын мэдээллийн аюулгүй байдлын ажиллагаануудын жишээг үзүүлэх; ба**
- **Мэдээллийн аюулгүй байдлын бодлогыг хэрэгжүүлэхэд олон улсын хамтын ажиллагааг онцолно.**

3.1 Үндэсний мэдээллийн аюулгүй байдлын үйл ажиллагаанууд

АНУ-ын мэдээллийн аюулгүй байдлын стратеги

2001 оны 9 сарын 11-ний террорист халдлагын дараа АНУ-ын Засгийн Газар биет халдлага төдийгүй кибер заналхийллийн эсрэг үндэсний аюулгүй байдлыг бэхжүүлэхийн тулд Дотоодын Аюулгүй Байдлын Газар (Department of Homeland Security)-ыг байгуулсан. АНУ нь мэдээллийн аюулгүй байдлын ажилтны системээр дамжуулан мэдээллийн аюулгүй байдлын цогц бөгөөд үр дүнтэй ажиллагааг хэрэгжүүлдэг. Мэдээллийн аюулгүй байдлын стратегид Дотоодын аюулгүй байдлын үндсэний стратеги, чухал дэд бүтэц болон хөрөнгийн биет хамгаалалтын үндэсний стратеги ба Кибер орон зайг хамгаалах үндэсний стратеги багтана.

Кибер орон зайг хамгаалах үндэсний стратеги[15] нь кибер аюулгүй байдлын зорилго, чухал дэд бүтэц болон хөрөнгийн хамгаалалтыг тодорхойлохын зэрэгцээ тэдгээрийг кибер халдлагаас сэргийлэх зорилго, үйл ажиллагааг тогтоодог. Кибер орон зайг хамгаалах үндэсний стратегид тодорхойлсон үндэсний таван чухал зорилгод дараах зүйлс багтсан байна:

- Үндэсний кибер орон зайн аюулгүй байдлын хариу өгөх систем
- Үндэсний кибер орон зайн аюулгүй байдал дахь аюул ба эмзэг байдлыг бууруулах хөтөлбөр
- Үндэсний кибер орон зайн аюулгүй байдлын ойлголт ба сургалтын хөтөлбөр
- Засгийн газрын кибер орон зайг хамгаалах тухай
- Үндэсний аюулгүй байдал ба олон улсын кибер орон зайн аюулгүй байдлын хамтын ажиллагаа

Мэдээллийн аюулгүй байдлын хуулийг чангатгах тухай

Кибер аюулгүй байдлыг бэхжүүлэх хууль- КАББХ 2002[16] (Cyber Security Enhancement Act-CSEA) нь Дотоодын аюулгүй байдлын хуулийн хоёрдугаар бүлгийг хамардаг. Энэ нь тодорхой нэг компьютерийн гэмт хэргийг яллах журамд оруулсан нэмэлт өөрчлөлт, онцгой байдлын үед мэдээлэл задлах тухай болон хууль бус нотолгоог итгэл үнэмшлээр хүлээн зөвшөөрөх тухай, хууль бус интернэт зар сурталчилгааг хориглох болон нууцлалыг хамгаалах зэргийг багтаасан.

Онцгой байдлын үед мэдээлэл задлах тухай: 9/11-нээс өмнө, Цахим Холбооны Нууцлалын акт- ЦХНХ (Electronic Communications Privacy Act-ECPA) цахим холбооны үйлчилгээ үзүүлэгчдийг (ISP гэх мэт) хэрэглэгчийн харилцаа холбоог (дуут мэйл, и-мэйл болон хавсралтууд г.м) задруулахыг хориглодог байв. 2001 оны 9 сарын 11-ны

15. The White House, The National Strategy to Secure Cyberspace (Washington, D.C.: The White House, 2003), http://www.whitehouse.gov/pcipb.
16. Computer Crime and Intellectual Property Section, SEC. 225. Cyber Security Enhancement Act of 2002 (Washington, D.C.: Department of Justice, 2002), http://www.usdoj.gov/criminal/cybercrime /homeland_CSEA.htm.

дараагаар батлагдсан АНУ-ын Эх орны тухай хуулийн (USA Patriot Act) дагуу Онцгой байдлын үед мэдээлэл задлах тухай журам нь ISP-уудад и-мэйл болон цахим холбооны агуулга, мэдээллийг хууль хэрэгжүүлэгч агентлагуудад шүүхийн захирамжгүйгээр өгөх боломж олгосон.

Онцгой байдлын үе дэх нээлттэй байдлын тайлбар зохицуулалт КАББХ-д бэхжээд байна. Сэжигтэй агуулга хүлээн авсан Засгийн газрын агентлагууд мэдээллийг задалсан огноо, оролцсон талууд, задалсан мэдээлэл, холбогдох этгээд ба мэдээлэл харилцааны тоо зэргийг мэдээлэл задарснаас хойш 90 хоногийн дотор Ерөнхий прокурорт мэдээлэх ёстой.

Итгэл үнэмшлийн тайлбар: Компьютерийн эзэмшигч болон операторын хүсэлтээр чагнах ажиллагаа явуулсан бол КАББХ нь эрүүгийн болон иргэний хэрэг үүсгэхээс чөлөөлдөг.

Хууль бус төхөөрөмжийн интернэт сурталчилгааны хориг: ЦХНХ нь утсан, аман болон цахилгаан харилцаа холбоог замаас нь сонсох төхөөрөмжүүдийн үйлдвэрлэл, түгээлт, эзэмшил болон онлайн сурталчилгааг хориглодог. Электрон чагнах төхөөрөмжүүдийг сурталчилж болох хэдий ч сурталчлагч нь сурталчилгааныхаа агуулгыг мэддэг байх шаардлагатай.

Компьютерийн гэмт хэргийн шийтгэлийг чангатгах: АНУ-ын компьютерийн залилан ба халдлагын хуулийн дагуу зөвшөөрөлгүйгээр компьютерт нэвтэрч, хохирол учруулах нь хууль бус гэж үздэг. 9/11-нээс өмнө ийм хэрэгт буруутай нь нотлогдсон ямар ч хүн анхны үйлдэл бол 5 жилээс илүүгүй, хоёр дахь үйлдэл бол 10 жилээс илүүгүй шоронд хоригдох ял авдаг байв. 9/11-нээс хойш ийм төрлийн гэмт хэргийн шийтгэлийг дахин авч үзэж анхны үйлдэл бол 10 жилээс илүүгүй, хоёр дахь үйлдэл бол 20 жилээс илүүгүй хорихоор заасан. КАББХ дэх нэмэлт зүйл ангиар гэмт хэрэг үйлдэгч нь бие махбодын ноцтой гэмтэл учруулсан болон учруулах оролдлого хийсэн бол гэмт этгээдийг 20 жилээс илүүгүй хугацаагаар хорихоор заасан; хэрэв үхэлд хүргэсэн, үхэлд хүргэх оролдлого хийсэн бол насаар нь хорих ял оноож болно.

Туслагч этгээдийн хариуцлагыг хөнгөлөх: ЦХНХ нь харилцаа, холбоог дундаас нь чагнахад тусалсан болон хууль сахиулагчдыг мэдээллээр хангасан харилцаа холбооны үйлчилгээ үзүүлэгчийг эрүүгийн шийтгэлээс чөлөөлдөг.

Холбооны мэдээллийн аюулгүй байдлын удирдлагын хууль-ХМАБУХ (Federal Information Security Management Act- FISMA)[17] 2002 оны цахим засаглалын гуравдугаар бүлгийг хамардаг. Энэхүү хууль нь үндэсний сүлжээт дэд бүтцийг хамгаалж мэдээллийн аюулгүй байдлыг хамгаалах үйл хэрэгт бүх иргэд, үндэсний аюулгүй байдлын агентлагууд болон хууль сахиулагч байгууллагууд хүчин зүтгэл гаргахыг уриалдаг. Холбооны мэдээллийн аюулгүй байдлын удирдлагын үндсэн зорилтуудад: (1) үйл ажиллагаа ба хөрөнгөд тавих мэдээллийн аюулгүй байдлын хяналтыг бэхжүүлэх цогц үндсийг хангах; болон (2) мэдээлэл/мэдээллийн системүүдийг хамгаалах тохиромжтой хяналт, үйлчилгээний төлөвлөгөөг боловсруулах, мэдээллийн аюулгүй байдлын хөтөлбөрүүдийн удирдлагыг бэхжүүлэх механизмаар хангах зэрэг орно.

Европын Холбооны мэдээллийн аюулгүй байдлын стратеги

2006 оны 5 сарын мэдэгдлээр[18] Европын Комисс мэдээллийн аюулгүй байдлын талаарх Европын Холбооны сүүлийн үеийн стратегийг тодорхойлсон ба энэ нь оролцогч талуудыг хамарсан хэд хэдэн харилцан хамаарал бүхий арга хэмжээнээс бүрддэг.

Эдгээр арга хэмжээнүүдэд 2002 оны Цахим харилцаа холбооны зохицуулалтын хүрээг бий болгох, Европын мэдээллийн нийгэмлэгийг байгуулах i2010 санаачлагын нэгдэл

17. Office of Management and Budget, Federal Information Security Management Act: 2004 Report to Congress (Washington, D.C.: Executive Office of the President of the United States, 2005), http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf.
18. Europa, “Strategy for a secure information society (2006 communication),” European Commission, http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

болон 2004 оны Европын Сүлжээ ба Мэдээллийн Аюулгүй Байдлын Агентлаг-ЕМСАБА (European Network and Information Security Agency-ENISA)-ийг байгуулах зэрэг багтсан. Энэхүү Мэдэгдлээр бол эдгээр арга хэмжээнүүд нь мэдээллийн нийгэм дэх аюулгүй байдлын асуудлуудыг шийдэх гурван талт аргыг тусгадаг ба тодорхой нэг сүлжээ, мэдээллийн аюулгүй байдлын (NIS) арга хэмжээнүүд, цахим харилцаа холбооны (нууцлал ба өгөгдлийн аюулгүй байдлын асуудлуудыг багтаадаг) болон кибер гэмт хэргийн эсрэг тэмцлийг хамардаг.

Тус Мэдэгдэлд мэдээллийн системийн халдлага, зөөврийн төхөөрөмжийн өсөн нэмэгдэж буй хэрэглээ, “гадаад оюун ухаан”-ны үүсэл болон хэрэглэгчийн ухамсрын төвшинг дээшлүүлэх зэргийг Европын комисс санал солилцоо, хамтын ажиллагаа болон эрх мэдлээр дамжуулан эн тэргүүний анхаарч үзэх аюулгүй байдлын гол асуудлуудаар нэрлэсэн байна. Эдгээр стратегиудыг дараах байдлаар тайлбарлалаа:

Санал солилцоо

Тус комисс нээлттэй, бүгдийг хамарсан олон-талт санал солилцоог тогтоох зорилго бүхий хэд хэдэн арга хэмжээг дэвшүүлэн тавьсан:

- Европын Холбоо даяар хэрэглэж болох хамгийн үр дүнтэй туршлагуудыг тодорхойлоход туслахын тулд сүлжээ ба мэдээллийн аюулгүй байдалтай холбоотой үндэсний бодлогуудын жишиг тогтоох судалгаа. Ялангуяа, энэ судалгаа нь ЖДҮ болон иргэдийн сүлжээ ба мэдээллийн аюулгүй байдалтай холбоотой эрсдлүүд ба бэрхшээлүүдийн талаарх ойлголтыг сайжруулах шилдэг туршлагыг тодорхойлох болно; мөн
- Одоогийн зохицуулалтын хэрэгслүүдийг хэрхэн үр ашигтайгаар ашиглах талаарх оролцогч талуудын хэлэлцүүлэг. Энэхүү хэлэлцүүлгийг бага хурал, семинарын агуулгын хүрээнд зохион байгуулна.

Хамтын ажиллагаа

Үр дүнтэй бодлого боловсруулалт нь шийдвэрлэх асуудлын талаарх тодорхой ойлголт, үнэн зөв, сүүлийн үеийн статистик болон эдийн засгийн мэдээллийг шаарддаг. Тиймээс тус комисс ЕМСАБА- аас дараах зүйлсийг хүснэ:

- Мэдээлэл цуглуулах тохиромжтой хүрээг хөгжүүлэхийн тулд гишүүн орнууд болон оролцогч талуудтай итгэлцэлийг бий болгох; болон
- Аюулд үр дүнтэй хариу үзүүлэх боломжоор хангахын тулд Европчуудын мэдээлэл хамтран ашиглах болон сэргийлэх системийн эдийн засгийн судалгааг нягтлах. Энэхүү систем нь аюул занал, эрсдэл, халдлагын талаарх зохистой мэдээллээр хангах олон хэл дээрх Европын портал сайтыг багтаана.

Үүний зэрэгцээ тус Комисс МХХТ-ийн аюулгүй байдлын салбарт хамаарах мэдээллийг авах боломжийг хангах үүднээс гишүүн орнууд, хувийн хэвшлийнхэн болон судалгааны салбарынхныг хамтран ажиллахыг уриалдаг.

Эрх мэдэл

Аюулгүй байдлын хэрэгцээ ба эрсдлүүдийн талаар ухамсрыг дээшлүүлэхэд оролцогч талуудын эрх мэдэл гол хүчин зүйл нь юм. Тийм учраас гишүүн орнуудыг:

- Үндэсний бодлогын жишиг тогтоох ажиллагаанд идэвхитэй оролцох;
- ЕМСАБА–тай хамтран үр дүнтэй аюулгүй байдлын технологиуд, туршлагууд болон үйл ажиллагааг хэрэгжүүлэхийн үр дүнгийн талаарх ойлголтыг дээшлүүлэх компанит ажлыг дэмжих;
- Аюулгүй байдлын шилдэг туршлагуудыг дэмжихийн тулд цахим засаглалын үйлчилгээнүүдийг дэмжих; болон
- Сүлжээ, мэдээллийн аюулгүй байдлын програмыг дээд боловсролын сургалтын хөтөлбөрийн нэг хэсэг хэлбэрээр хөгжүүлэхэд дэмжлэг үзүүлэхэд уриалсан.

Хувийн хэвшлийнхэн мөн дараах ажлыг хэрэгжүүлэхэд санаачлага гаргах хэрэгтэй. Үүнд:

- Хүртээмжтэй бөгөөд хянах боломжтой аюулгүй байдлаар хангахтай холбоотой програм хангамж үйлдвэрлэгчид болон ISP-уудын хариуцлагыг тодорхойлох;
- Төрөлжилт, нээлттэй байдал, харилцан ажиллах боломж, хэрэгцээт байдал ба өрсөлдөөнийг аюулгүй байдлын гол чиглүүлэгч болгон дэмжих, мөн ID-ын хулгай болон бусад нуущад халдсан халдлагуудтай тэмцэхийн тулд аюулгүй байдлыг бэхжүүлэх бүтээгдэхүүн, үйлчилгээнүүдийн хэрэглээг сайжруулах;
- Сүлжээний операторууд, үйлчилгээ үзүүлэгчид болон ЖДҮ-ийнхэнд аюулгүй байдлын шилдэг туршлагыг дэлгэрүүлэх;
- Ажилтнуудыг аюулгүй байдлын туршлагыг хэрэгжүүлэхэд шаардлагатай мэдлэг чадвараар хангахын тулд хувийн хэвшлийн сургалтын хөтөлбөрүүдийг хөхүүлэн дэмжих;
- Европын Холбоонд хандсан хэрэгцээ шаардлага руу чиглэсэн бүтээгдэхүүн, үйл явц ба үйлчилгээнд зориулсан өртөг багатай аюулгүй байдлын баталгаажуулалтын схемийг бий болгохын төлөө ажиллах; болон
- Эрсдлийн удирдлагын хэрэгсэл болон аргыг хөгжүүлэхэд даатгалын салбарынхныг хамруулах зэрэг болно.

Эх сурвалж: Abridged from Europa, “Strategy for a secure information society (2006 communication),” European Commission, http://europa.eu/scadplus/leg/en /lvb/l24153a.htm.

Кибер гэмт хэргийн тухай Европын Зөвлөлийн конвенци

Европын Холбоо 2001 онд Кибер гэмт хэргийн тухай Европын зөвлөлийн конвенцийг (Council of Europe Convention on Cybercrime-CECC) соёрхон баталсан бөгөөд энэ нь “кибер гэмт хэргийн эсрэг хууль тогтоомж боловсруулах хүсэлтэй засгийн газруудад зориулсан чиглэлийг тогтоож” мөн “энэ салбар дахь олон улсын хамтын ажиллагаагаар хангадаг.” Европын гучин есөн улсаас гадна Канад, Япон, Өмнөд Африк болон АНУ энэхүү гэрээнд гарын үсэг зураад байна.

Энэ нь 2004 оны Долдугаар сараас хүчин төгөлдөр болсон CECC-ыг “энэ асуудлыг хөндсөн олон улсын цорын ганц гэрээ” болгосон юм.[19]

Европын Мэдээлэл, сүлжээний аюулгүй байдлын агентлаг- ЕМСАБА

2004 оны 3 сарын 10-нд Европын парламент болон Европын Холбооны Зөвлөлөөс “Европын Холбооны улсууд дахь сүлжээ ба мэдээллийн аюулгүй байдлыг дээшлүүлэхэд туслах болон иргэд, хэрэглэгчид, бизнесийнхэн болон төрийн байгууллагуудын тусын тулд сүлжээ, мэдээллийн аюулгүй байдлын соёлыг бий болгох явдлыг дэмжих” зорилгоор ЕМСАБА –ийг байгуулсан.

2006 оны 5 сард гарсан байнгын оролцогч талуудын бүлгийн-БОТБ (Permanent Stakeholders Group -PSG) үзэл баримтлалд ЕМСАБА[20]-ийг сүлжээ ба мэдээллийн аюулгүй байдлын төгс чанарын гол төв, СМАБ-ын талуудыг уулзуулах төв мөн Европын Холбооны бүх иргэдийн мэдээллийн аюулгүй байдлын талаарх ойлголт ухамсрын гол чиглүүлэгч гэж үзсэн байна. Үүнтэй холбоотойгоор БОТБ-ийн үзэл баримтлалд ЕМСАБА-ийн урт хугацааны үйл ажиллагааг дараах байдлаар тодорхойлсон байна (Зураг 6):

19. Council of Europe, “Cybercrime: a threat to democracy, human rights and the rule of law,” http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp.
20. Paul Dorey and Simon Perry, ed. The PSG Vision for ENISA (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

Зураг 6. ЕМСАБА-гийн урт хугацааны үйл ажиллагаа

(Эх сурвалж: Paul Dorey and Simon Perry, ed. The PSG Vision for ENISA (Permanent Stakeholders Group, 2006), http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf)

1. Гишүүн орнуудын үндэсний сүлжээ ба мэдээллийн аюулгүй байдлын удирдах газруудтай хамтран ажиллах ба зохицуулах

Үндэсний агентлагуудын хамтын ажиллагаа өнөөгийн нөхцөлд маш чухал. Үндэсний агентлагууд хоорондын, ялангуяа тэргүүний агентлагууд дөнгөж эхэлж буй агентлагуудтай өөрсдийн туршлагаа хуваалцах тал дээр харилцаа, хамтын ажиллагааг дэмжсэнээр илүү ихийг хийх боломжтой.

2. Судалгааны байгууллагуудтай хамтран ажиллах

Бодит ертөнцийн систем дэх аюулгүй байдлын жинхэнэ эрсдлийг удирдахад хамгийн их тустай салбарт анхаарлаа хандуулахын тулд ЕМСАБА үндсэн судалгаа ба зорилтот техникийн хөгжлийг удирдан чиглүүлэхэд зорих ёстой. ЕМСАБА өөрөө судалгааны ажлыг дэмжих ёсгүй бөгөөд харин одоогийн үйл явц, зорилго болон хөтөлбөрүүдийг нэгтгэхэд илүү анхаарч ажиллах хэрэгтэй.

3. Програм хангамж ба техник хангамжийн борлуулагчидтай хамтран ажиллах

Програм хангамж ба техник хангамжийн борлуулагчид хоорондоо өрсөлдөгддөг учраас тэдэнд хоёр талын туршлага дээр нээлттэй санал нэгдэхэд хүндрэлтэй байж болох талтай. Эмзэг хэлэлцүүлгийн уулзалтанд ЕМСАБА нь өрсөлдөөний эсрэг үйл явцын цэвэр байдлыг хангахын зэрэгцээ дундыг сахисан санал хэлж болно. ЕМСАБА-ийн урт хугацааны зорилго нь одоогийн өсч буй аюулгүй байдлын хандлагыг хөгжүүлэхэд бус харин сүлжээний өт, болон бусад төрлийн хүндрэлүүдэд тэсвэртэй сүлжээ ба мэдээллийн найдвартай технологиудыг бий болгоход чиглэх ёстой. Зөв, найдвартай, бат бөх архитектур болон програм хангамж хөгжүүлэх техникийг дэмжсэнээр энэ зорилгодоо хүрэх боломжтой.

4. Стандарт тогтоох ажиллагаанд оролцох

Хамгийн чухал ач холбогдол бүхий санаачлагыг тодорхойлон сурталчлах зорилгоор ЕМСАБА төрөл бүрийн аюулгүй байдлын баталгаажуулалт, магадлан итгэмжлэлийн ажиллагааг сайжруулах зэрэг стандарт тогтоох ажиллагааны NIS-тэй холбоотой сэдвүүдийг хянах хэрэгтэй.

5. Ухуулга, саналаар дамжуулан хууль тогтоох явцад оролцох

ЕМСАБА нь NIS-тэй холбоотой асуудлуудын чиглэл, бусад тогтоомжуудыг боловсруулах болон дэвшүүлэх ажиллагааны эхэн үед саналаа хэлдэг итгэмжлэгдсэн зөвлөх байгууллагын байр суурийг олж авахын төлөө ажиллах хэрэгтэй.

6. Хэрэглэгч байгууллагуудтай ажиллах

Хэрэглэгч байгууллагууд ихэнхдээ хууль тогтоох болон стандарт тогтоох ажиллагаануудад борлуулагчид шиг төлөөлөл сайтай байдаггүй. ЕМСАБА нь хэрэглэгчийн бүлгийг стандартын ажлын ойлголт болон ийм төрлийн ажилд нөлөөлөх боломжоор хангах ёстой.

7. Эцсийн хэрэглэгчийн салбарт гишүүн орнуудын шилдэг туршлагыг дэмжих

ЕМСАБА зөвхөн бизнесийн эрх ашгийг хамгаалаад зогсохгүй мөн интернэт болон дижитал хэрэгслийн хэрэглээний талаарх хэрэглэгчийн итгэлийг бэхжүүлэх ёстой.

8. Хувийн мэдээллийн системийг удирдах техникийн болон улс төрийн шийдлийг олохын төлөө ажиллах

Интернэтэд итгэх хэрэглэгчийн итгэл дутмаг байгаа нь хэрэглэгчид чиглэсэн томоохон цахим бизнесд хамгийн гол саад болж байна. Аливаа сайт, и-мэйл хаяг, эсвэл зарим онлайн үйлчилгээний эзэмшигчийг нарийн шалгаж, мэдэх боломжтой байх нь интернэт дэх байнгын хэрэглэгчдийн итгэлийг нэмэгдүүлэх том ахлам болох юм. Энэ салбар дахь техникийн шийдлийг салбарын удирдах үйл явцаар дамжуулан эрэлхийлэх хэрэгтэй, гэхдээ ЕМСАБА онлайн аж ахуйн нэгжийг баталгаажуулах Европын Холбоог хамарсан бодлогуудад чиглэн ажиллах боломжтой.

9. “Сүлжээ” ба “Мэдээллийн” аюулгүй байдлын асуудлуудад хандсан оролдлогыг тэнцвэртэй байлгах

Европ даяарх бизнесийнхэн болон хэрэглэгчдийн тусын тулд ЕМСАБА нь томоохон интернэт болон сүлжээний үйлчилгээ эрхлэгчдэд (ISP/NSP) шилдэг туршлагын талаар мэдээлэл олж авахад нь туслах зорилгоор тэдэнтэй харилцаа холбоотой байх хэрэгтэй. Интернэт, сүлжээний үйлчилгээ эрхлэгчид нь интернэт дэх аюулгүй байдлыг дээшлүүлэхэд гол үүрэг гүйцэтгэж болох учраас энэ асуудал маш чухал юм. Хамтын ажиллагаа болон ISP-уудын авч буй арга хэмжээний зохицуулалт одоогийн байдлаар дутагдалтай байна.

Эх сурвалж: Abridged from Paul Dorey and Simon Perry, ed. The PSG Vision for ENISA (Permanent Stakeholders Group, 2006),
http://www.enisa.europa.eu/doc/pdf/news/psgvisionforenisafinaladoptedmay2006version.pdf.

БНСУ-ын мэдээллийн аюулгүй байдлын стратеги

Хэдийгээр БНСУ нь интернэтийн технологиороо дэлхийд тэргүүлэгчдийн нэг боловч саяхнаас л мэдээллийн аюулгүй байдлыг хамгаалах хэрэгцээ шаардлагыг анхаарч эхэлсэн. Өргөн зурвасын сүлжээний аюулгүй холбооны орчинг хангах аюулгүй байдлын суурийг байгуулах болон шинэ үеийн зөөврийн төхөөрөмжийн хууль бус хуулбарын эсрэг аюулгүй байдлын технологийг хөгжүүлэх зорилгоор 2004 онд Солонгосын засгийн газар Мэдээлэл, Холбооны Яамаар-МХЯ дамжуулан (MIC) дунд ба урт хугацааны мэдээллийн аюулгүй байдлын төлөвлөгөөг гаргасан. Мөн МХЯ нь оршин суугчийн бүртгэлийн дугаарыг ашиглан нууцлалын нөлөөлөх байдлын үнэлгээг (Privacy Impact Assessment- PIA) нэвтрүүлж насанд хүрэгчдийг бичиг баримтжуулах аргачлалыг тогтоохыг хичээж байна. Түүнчлэн БНСУ нь спам хяналтын систем, технологийн хариу, хэрэглэгчийн сургалт ба ухамсар, улс хооронд мэдээлэл солилцох замаар хувийн болон төрийн байгууллагын хамтын ажиллагааг сайжруулах болон хүний нөөцийн солилцоогоор дамжуулан спамтай тэмцэх Ази Номхон далайн орнуудын хамтын ажиллагааг бий болгох Сөүл Мэлбурны Гэрээнд гарын үсэг зураад байна. Мэдээллийн аюулгүй байдлын төлөвлөгөөний үндсэн зорилго нь: (1) сүлжээний дэд бүцийн аюулгүй байдлыг хангах; (2) шинэ МТ-ийн үйлчилгээ, тоног төхөөрөмжийн найдвартай байдлыг хангах; болон (3) БНСУ-д мэдээллийн аюулгүй байдлын үндсийг дэмжих зэрэг юм. Төлөвлөгөөний хэрэгжилтэнд дөрвөн жилийн хугацаанд 247.89 тэрбум доллар зарцуулахаар төсөвлөсөн. (2005 онд 43 тэрбум, 2006 онд 55.5 тэрбум 2008 онд 80.1 тэрбум ам.доллар).

Сүлжээний дэд бүтцийн аюулгүй байдлыг хангах: Төлөвлөгөөний дагуу сүлжээний дэд бүтцийн аюулгүй байдлыг дараах хэлбэрүүдээр хангах ба үүнд төрөл бүрийн гетероген компьютерийн сүлжээнүүдийг нэгтгэн холбох, мэдээллийн аюулгүй байдлын суурь бүтцийг хөгжүүлэх; шинэ үеийн ДСС аюулгүй байдлын удирдлагыг байгуулах; болон өргөн зурвасын нэгдсэн сүлжээн дэх гэмтэл хувийн сүлжээ рүү тархахаас сэргийлэх зорилгоор сүлжээ тусгаарлах механизмыг хөгжүүлэх зэрэг багтана.

МТ-ийн шинэ үйлчилгээ, тоног төхөөрөмжийн найдвартай байдлыг хангах: МТ-ийн үйлчилгээн дэх мэдээллийн аюулгүй байдлын зөрчлүүдээс үр дүнтэйгээр сэргийлэхийн тулд удирдлагын, техникийн болон материаллаг аюул, эмзэг байдлыг үнэлж чадахуйц мэдээллийн аюулгүй байдлын нөлөөллийн үнэлгээний загварыг боловсруулна.

Мэдээллийн аюулгүй байдлын төвшнийг үнэлэх баталгаажуулалтын явцыг бий болгоно. Шинэ үеийн МТ-ийн үйлчилгээнүүдийн хувьд баталгаажуулалтын системийг хүмүүс, эрх мэдэл, гүйлгээний бичлэгийн баталгаажуулалт гэх мэтийг хамарсан байхаар шинэчлэн сайжруулна. Түүнчлэн, мэдээллийн аюулгүй байдлын технологийн хөгжлийн төлөвлөгөөг өрхийн сүлжээнд тохирсон эрх олголт, халдлагаас сэргийлэх терминал магадлалын технологи, шинэ үеийн үйлчилгээний роботуудын аюулгүй байдлын технологи болон шинэ үеийн агуулгад зориулсан аюулгүй байдлын технологи зэргийг багтаасан байдлаар боловсруулаад байна.

Мэдээллийн аюулгүй байдлын үндсийг бий болгох: Солонгосын мэдээллийн аюулгүй байдлын төлөвлөгөө нь хувьсан өөрчлөгдөж буй мэдээлэл, холбооны орчны шаардлагад нийцэх болон ирээдүйн аюул заналд бэлтгэх зорилго бүхий зохицуулалтыг сайжруулах арга хэмжээнүүдийг багтаадаг. Юуны өмнө, Интернэтийн Будлианд Хариу Үзүүлэх Үйлчилгээний Төв (Internet Incident Response Service Centre) нь боловсронгуй бөгөөд ихээхэн хөгжсөн интернэтийн халдлагын хэргүүдийг зохицуулахын тулд илүү хөгжих ёстой. Дотоодын болон гадаадын мэдээллийн аюулгүй байдлын хамтын ажиллагааны тогтолцоог бэхжүүлж мэдээллийн аюулгүй байдал сул байгаадаа дэмжлэг үзүүлэх хэрэгтэй. Хоёрдугаарт, холбогдох технологиуд болон нууцлал хамгаалах хуулийг боловсруулж Спамд Хариу Үзүүлэх Үйлчилгээний Төвийг ажиллуулах шаардлагатай. Гуравдугаарт, одоогийн мэдээллийн аюулгүй байдлын хуулиудыг компьютержсэн орчны хэрэгцээ шаардлагад нийцүүлэн сайжруулах хэрэгтэй.

Түүнчлэн мэдээллийн аюулгүй байдлын ухамсарыг мэдээллийн аюулгүй байдлын компанит ажил болон мэргэжилтнүүдийн сургалтын програмаар дамжуулан дэмжих нь зүйтэй.

Японы мэдээллийн аюулгүй байдлын стратеги[21]

Япон улс “Мэдээллийн аюулгүй байдал хөгжсөн орон”[22] болох зорилготойгоо уялдуулан нарийвчилсан багц зорилт, үндсэн зарчим болон төслүүдийг мэдээллийн аюулгүй байдлын салбарт боловсруулсан. Мэдээллийн Аюулгүй Байдлын Бодлогын Зөвлөл (Information Security Policy Council) болон Үндэсний Мэдээллийн Аюулгүй Байдлын Төв -ҮМАБТ (National Information Security Center- NISC) нь тус улсын мэдээллийн аюулгүй байдалтай холбоотой бүх ажлыг хянадаг гол байгууллага юм. Кибер заналхийллийн судалгааны салбарт Кибер Цэвэрлэгээний Төв (Cyber Clean Center)-ийг компьютерийн элдэв халдвар, вирусны онцлог шинжийг судлан шинжлэх болон үр дүнтэй, аюулгүй хариу үзүүлэх аргыг боловсруулах зорилгоор байгуулсан.

Японы мэдээллийн аюулгүй байдлын стратегийг хоёр хэсэгт хуваадаг: (1) Түгээмэл хэрэглэгддэг мэдээллийн аюулгүй байдлын талаарх анхны Үндэсний стратеги; болон (2) Аюулгүй Япон YYYY. **Мэдээллийн аюулгүй байдлын талаарх анхны Үндэсний стратеги нь** “МТ-ийн аюулгүй хэрэглээний орчин бүрдүүлэхэд оролцох”-ийн тулд МТ-ийн нийгэм дэх бүх “нэгжүүд”-ийн хэрэгцээ шаардлагыг хүлээн зөвшөөрдөг. Энэхүү стратегиар нэгжүүдийг “чухамдаа МТ-ийн нийгмийн нэг бүрдэл хэсэг хэлбэрээр авч хэрэгжүүлдэг” гэдгийг хүлээн зөвшөөрдөг.[23] “Эдгээр хэрэгжүүлэгч нэгжүүд” –ийг 4 хуваадаг: төвийн ба орон нутгийн захиргаа, онц чухал дэд бүтцүүд, бизнесийнхэн болон хувь хүмүүс. Тус бүр нь өөрийн гэсэн үүрэг, төлөвлөгөөг тодорхойлж тэдгээрийг хэрэгжүүлэх шаардлагатай (Хүснэгт 4).

Хүснэгт 4. Мэдээллийн аюулгүй байдлын талаарх анхны Үндэсний стратегид суурилсан ангилал тус бүрийн үүрэг, төлөвлөгөө

Ангилал	Үүрэг	Төлөвлөгөө
Төвийн ба орон нутгийн захиргаа	Мэдээллийн аюулгүй байдлын арга хэмжээний “тэргүүн туршлага”-аар хангах	Арга хэмжээний стандарт
Чухал дэд бүтцүүд	Тэдгээрийн үйлчилгээний тогтвортой нийлүүлэлтийг хүмүүсийн нийгмийн амьдрал, эдийн засгийн ажиллагааны үндэс болгох явдлыг хангах	Арга хэмжээний төлөвлөгөөн дэх чухал дэд бүтцүүд
Бизнесийнхэн	Зах зээлд өндрөөр үнэлэгдэх мэдээллийн аюулгүй байдлын арга хэмжээг хэрэгжүүлэх	Яам болон агентлагуудыг дэмжих арга хэмжээнүүд
Хувь хүмүүс	МТ-ийн нийгэмд гол үүрэг гүйцэтгэгч гэсэн ухамсрыг дээшлүүлэх	Яам болон агентлагуудыг дэмжих арга хэмжээнүүд

Эх сурвалж: NISC, Japanese Government”s Efforts to Address Information Security Issues (November 2007), http://www.nisc.go.jp/eng/.

Мэдээллийн аюулгүй байдлын талаарх анхны Үндэсний стратегиас гаргасан практик бодлогуудад дараах орно:

- Мэдээллийн аюулгүй байдлын технологийг дэмжих-засгийн газрын хэрэгцээнд зориулагдсан технологиудыг хөгжүүлэх болон урт хугацааны зорилт бүхий технологийн үндсэн санаачлагын “Их Сорилд-д хандсан технологийн хөгжлийг дэмжих;

21. Эх сурвалж: NISC, Japanese Government’s Efforts to Address Information Security Issue (November 2007), http://www.nisc.go.jp/eng/.
22. Information Security Policy Council, The First National Strategy on Information Security (2 February 2006), 5. http://www.nisc.go.jp/eng/pdf/national_strategy _001_eng.pdf.
23. Ibid., 11

- Олон улсын хамтын ажиллагааг дэмжих - мэдээллийн аюулгүй байдал ба сэргийлэлтийн олон улсын суурийг байгуулахад хамтран ажиллаж олон улсын төвшинд Японы тэргүүлэх хувь нэмрийг оруулах.
- Хүний нөөцийг хөгжүүлэх - практик ур чадвар, авъяас болон өргөн хүрээтэй чадамж бүхий хүний нөөцийг хөгжүүлж мэдээллийн аюулгүй байдлын боловсролын системийг зохион байгуулах; болон
- Эрх, ашиг сонирхлын гэмт хэргийн хяналт ба хамгаалах/засах арга хэмжээ - Кибер гэмт хэргийн хяналтыг чангатгах болон холбогдох хуулийн үндсийг хөгжүүлэх, мөн кибер орон зай дахь аюулгүй байдлыг дээшлүүлэх технологийг хөгжүүлэх.

Аюулгүй Япон YYYY нь мэдээллийн аюулгүй байдлын жилийн төлөвлөгөө юм. Аюулгүй Япон 2007 нь 159 мэдээллийн аюулгүй байдлын хэрэгжилтийн арга хэмжээ болон 2007 онд баримтлах 24 тэргүүлэх зорилтуудын төлөвлөгөөний чиглэлийг багтаасан. Эдгээрийг дараах байдлаар хураангуйлж болно:

- Төвийн захиргааны агентлагуудад зориулсан мэдээллийн аюулгүй байдлын арга хэмжээг сайжруулах;
- Мэдээллийн аюулгүй байдлыг хангах арга хэмжээ дутмаг байгууллагууд болон олон нийтэд зориулсан арга хэмжээг хэрэгжүүлэн түгээх; болон
- Мэдээллийн аюулгүй байдлын суурийг бэхжүүлэхэд чиглэсэн эрчимтэй идэвх чармайлт.

АСУУЛТ

1. Танай орны мэдээллийн аюулгүй байдлын үйл ажиллагаанууд дээр дурдсан орнуудынхаас хэр ялгаатай байна вэ?

2. Энэ бүлэгт дурдсан улсуудад хэрэгжүүлж буй мэдээллийн аюулгүй байдлын үйл ажиллагаанд танай оронд ашиглах боломжгүй эсвэл холбоогүй ажиллагаанууд байна уу? Хэрэв байгаа бол аль нь яагаад ашиглах боломжгүй эсвэл холбоогүй вэ?

3.2 Олон улсын мэдээллийн аюулгүй байдлын үйл ажиллагаанууд

НҮБ-ын мэдээллийн аюулгүй байдлын үйл ажиллагаанууд

НҮБ-аас санхүүжүүлдэг Мэдээлэлжсэн Нийгмийн Дэлхийн дээд хэмжээний чуулга уулзалт- МНДДХЧ **(World Summit on the Information Society-МНДДХЧ)**[24] дээр мэдээллийн нийгмийн үр дүнтэй хөгжил ба “мэдээллийн хуваагдлыг” арилгах зарчим, төлөвлөгөөний тунхаглалыг баталсан. Үйл ажиллагааны төлөвлөгөө нь дараах чиглэлийг тодорхойлсон:

- Хөгжлийн төлөөх МХХТ-д засгийн газар, болон бүх талуудын гүйцэтгэх үүрэг
- Мэдээлэлжсэн нийгмийн чухал үндэс болсон мэдээлэл холбооны дэд бүтэц
- Мэдээлэл, мэдлэг авах боломж
- Чадавхи хөгжүүлэлт
- МХХТ-ийн хэрэглээнд итгэл, аюулгүй байдлыг бий болгох
- Боломж олгох орчин [үүсгэх]
- Өдөр тутмын амьдрал дахь МХХТ-ийн хэрэглээ
- Соёлын төрөлжилт ба онцлог, хэл зүйн төрөлжилт болон дотоодын агуулга
- Хэвлэл мэдээлэл
- Мэдээлэлжсэн нйигмийн ёс зүйн хэм хэмжээ
- Олон улсын ба бүс нутгийн хамтын ажиллагаа[25]

24. World Summit on the Information Society, “Basic Information: About МНДДХЧ,” http://www.itu.int/МНДДХЧ/basic/about.html.
25. World Summit on the Information Society, Plan of Action (12 December 2003), http://www.itu.int/МНДДХЧ/docs/geneva/official/poa.htm

Интернэт засаглалын форум (IGF)[26] нь НҮБ-ыг интернэт засаглалын асуудлаар дэмжих байгууллага юм. Энэхүү байгууллагыг интернэт засаглалтай холбоотой асуудлыг тодорхойлж анхаарлаа хандуулах зорилгоор Туннисд болсон 2 дахь удаагийн МНДДХЧ-ын үеэр байгуулсан. 2007 оны 11 сарын 12-15-нд Рио Де Жанеро хотод болсон хоёр дахь IGF форум нь кибер терроризм, кибер гэмт хэрэг болон интернэт дэх хүүхдийн аюулгүй байдал зэрэг мэдээлийн нийгмийн асуудлуудад анхаарсан.

ЭЗХАХБ[27]-ын мэдээллийн аюулгүй байдлын ажиллагаанууд

Эдийн засгийн хамтын ажиллагаа, хөгжлийн байгууллага (ЭЗХАХБ) (Organisation for Economic Co-operation and Development -OECD) нь даяаршиж буй дэлхийн эдийн засагт тулгарч байгаа эдийн засаг, нийгэм, байгаль орчин, засаглалын асуудлуудад анхаарлаа хандуулахын тулд зах зээлийн ардчилсан гучин орны засгийн газар, бизнесийнхэн болон иргэний нийгэмтэй хамтран ажилладаг цорын ганц форум юм. ЭЗХАХБ-ын хүрээнд Мэдээллийн аюулгүй байдал ба нууцлалын ажлын хэсэг- МАБНАХ (Working Party on Information Security and-Privacy WPISP) нь Мэдээлэл, компьютер, холбооны бодлогын зөвлөлийн шууд удирдлаган дор ажилладаг бөгөөд МХХТ-ийн мэдээллийн аюулгүй байдал ба нууцлалд нөлөөлөх нөлөөнд дүн шинжилгээ хийж интернэт эдийн засаг дахь итгэлийг тогтоохын тулд зөвшилцөлөөр бодлогын зөвлөмжүүдийг боловсруулдаг.

МАБНАХ-ийн мэдээллийн аюулгүй байдлын ажиллагаа: 2002 онд ЭЗХАХБ нь “Мэдээллийн систем, сүлжээний хөгжил дэх аюулгүй байдал ба мэдээллийн систем болон сүлжээг ашиглах шинэ арга замыг нэвтрүүлэх”[28] ажлыг дэмжихийн тулд “Аюулгүй байдлын соёлд чиглэсэн мэдээллийн систем, сүлжээний аюулгүй байдлын журам:”[29]-ыг гаргасан.

Мэдээлэлжсэн нийгэм дэх тэргүүн туршлагыг хуваалцахын тулд Мэдээллийн систем ба сүлжээний аюулгүй байдлын дэлхийн форумыг 2003 онд, Мэдээллийн систем, сүлжээний аюулгүй байдлын ЭЗХАХБ-APEC сургалтыг 2005 онд тус тус зохион байгуулсан.

МАБНАХ-ийн нууцлалын талаарх ажиллагаа: 1980 онд гарсан “Нууцлал хамгаалалт ба хувийн мэдээллийн хил дамнасан урсгалын тухай журам” нь төр ба хувийн хэвшил дэх хувийн мэдээлэлтэй харьцах тухай олон улсын зөвшилцөлийг төлөөлдөг. 2002 онд гарсан “Онлайн нууцлал: Бодлого хэрэгжилтийн тухай ЭЗХАХБ үзэл баримтлал” нь нууцлалыг сайжруулах технологиуд, онлайн нууцлалын бодлогууд, цахим худалдаатай холбоотой хэрэгжүүлэлт гэх мэтэд анхаардаг. Одоогоор, МАБНАХ нь Нууцлалын тухай хуулийн хэрэгжилтийн хамтын ажиллагаанд төвлөрч байна.

Бусад ажлууд: 1998 онд ЭЗХАХБ “Криптографын бодлогын чиглэл” –ийг гаргасан бөгөөд Цахим худалдааны Баталгаажуулалтын тухай Оттавагийн Сайд нарын тунхаглалыг боловсруулсан. 2002-2003 онд “ЭЗХАХБ –ын гишүүн орнууд дахь э-баталгаажуулалт болон э-гарын үсгийн хууль зүй, бодлогын хүрээний судалгаа”-г явуулсан. 2005 онд “ЭЗХАХБ орнуудын хил дамнасан баталгаажуулалтын хэрэглээ”-г зарласан.
2004 онд “Биометрт суурилсан технологиуд”-ыг боловсруулж, 2005 онд спамын ажлын хэсгийг байгуулсан. Энэ нь дижитал мэдээлэл бүртгэлийн удирдлага, малвэйр, давамгайлах радио давтамжийн илрүүлэлт (pervasive radio frequency identification-RFID), мэдрэгчид, сүлжээ болон мэдээллийн аюулгүй байдал ба нууцлалыг хэрэгжүүлэх нийтлэг хүрээ зэрэгтэй холбогдож байна.

26. Internet Governance Forum, http://www.intgovforum.org.
27. This section is drawn from WPISP, “Working Party on Information Security and Privacy” (May 2007).
28. OECD, OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Paris: OECD,2002), http://www.oecd.org/dataoecd/16/22/15582260.pdf.
29. Ibid., 8.

АНДЭЗХА[30]-ын мэдээллийн аюулгүй байдлын үйл ажиллагаа

Ази, Номхон Далайн Эдийн Засгийн Хамтын Ажиллагааны-АНДЭЗХА (Asia-Pacific Economic Cooperation-APEC) байгууллага нь Цахилгаан холбоо ба мэдээллийн ажлын хэсгээрээ (Telecommunication and Information Working Group TEL) дамжуулан Ази, Номхон далайн бүсэд мэдээллийн аюулгүй байдлын ажиллагааг хэрэгжүүлж байна. Энэхүү ажлын хэсэг нь: либералчлалын удирдах бүлэг (Liberalization Steering Group), МХХТ-ийн хөгжлийн удирдах бүлэг (ICT Development Steering Group), ба Аюулгүй байдал, хөгжлийн удирдах бүлэг (Security and Prosperity Steering Group) гэсэн гурван удирдах бүлгээс бүрддэг.

Ялангуяа 2005 оны Зургадугаар сард Перугийн Лимад болсон зургаа дахь удаагийн Цахилгаан холбоо ба мэдээллийн салбар сэдэвт АНДЭЗХА Сайд нарын хурлаас хойш Аюулгүй байдал ба хөгжлийн удирдах бүлэг кибер аюулгүй байдал болон кибер гэмт хэргийн талаарх хэлэлцүүлгийг өрнүүлсэн. Цахим-худалдааны хэрэглээнд хэрэглэгчийн итгэлийг бэхжүүлэх зорилтыг багтаадаг АНДЭЗХА Кибер-аюулгүй байдлын стратеги нь төрөл бүрийн эдийн засгийн хүчин чармайлтыг нэгтгэхийн төлөө үйлчилдэг. Эдгээр хүчин чармайлтуудад НҮБ-ын Ерөнхий Ассемблейн 55/63[31]-р тогтоол болон кибер гэмт хэргийн конвенцитой[32] уялдаатай кибер аюулгүй байдлын тухай хуулиудыг баталж хэрэгжүүлэх ажил багтдаг. TEL кибер гэмт хэргийн хууль тогтомжийн санаачлага (Cybercrime Legislation Initiative) болон хэрэгжүүлэлтийн чадавхийг хөгжүүлэх төсөл (Enforcement Capacity Building Project) нь шинэ хуулиудыг хэрэгжүүлэхэд байгууллагуудад дэмжлэг үзүүлдэг.

АНДЭЗХА-ын гишүүд мөн Компьютерийн халдлагын эсрэг багууд-КХХҮБ (Computer Emergency Response Teams- CERTs)-ыг кибер халдлагын эсрэг эрт үеийн анхааруулах хамгаалалтын систем болгон хэрэгжүүлэхэд хамтран ажиллаж байна. БНСУ нь хөгжиж буй гишүүн орнуудад сургалт зохион байгуулж байгаа бөгөөд КХХҮБ байгуулж ажиллуулах удирдамжийг боловсруулаад байна.

ЖДҮ болон өрхийн хэрэглэгчдийг кибер халдлага болон вирусаас хамгаалах ажлыг эн тэргүүний зорилгоо болгоод байгаа ба энэ зорилгын хүрээнд хэд хэдэн хэрэгслийг бүтээгээд байна. Интернэтийг хэрхэн аюулгүй ашиглах болон утасгүй технологи, и-мэйл солилцоотой холбоотой аюулгүй байдлын асуудлуудын талаарх мэдээллээр хангаж байна.

Мэдээлэл солилцоо, журам болловсруулалт болон хоёр талын туслалцааны хуулиудыг гэмт хэргийн зорилгоор буруугаар ашиглах явдлыг бууруулах, бизнесийнхэн болоод иргэдийг хамгаалах бусад арга хэмжээнүүд АНДЭЗХА TEL-ын эн тэргүүний зорилго хэвээр байх болно. Аюулгүй байдлын асуудлын талаарх өөрийн зорилтын нэг хэсэг болгон АНДЭЗХА нь “Ботнетийн эсрэг бодлогын ба техникийн арга замын удирдамж” болон “Кибер аюулгүй байдал ба онц чухал мэдээллийн дэд бүтэц” сэдэвт сургалтыг 2007 онд баталсан.

ОУЦХБ-ын мэдээллийн аюулгүй байдлын ажиллагаа[33]

ОУЦХБ бол МХХТ-ийн чиглэлийн тэргүүлэх НҮБ-ын агентлаг юм. Швейцарийн Женевт төвтэй ОУЦХБ нь 191 гишүүн орон ба 700 гаруй салбарын гишүүд, хамтрагчтай. Дэлхийд харилцаа холбооны дэмжлэг үзүүлэх ОУЦХБ-ын үүрэг нь гурван үндсэн салбарыг хамардаг. Радио холбооны салбар (Radiocommunication Sector ОУЦХБ-Р) нь олон улсын радио давтамжийн спектр болон хиймэл дагуулын тойргийн нөөцийг зохицуулахад анхаардаг. Стандартчилалын салбар (Standardization Sector-ОУЦХБ-С) нь мэдээлэл-холбооны сүлжээ ба үйлчилгээний стандартчилалд анхаардаг. Тэнцүү, найдвартай бөгөөд өртөг багатай МХХТ-ийн үйлчилгээг нийгэм эдийн засгийн өргөн хүрээтэй хөгжлийг дэмжих арга зам болгон түгээхэд туслах зорилгоор хөгжлийн хэсгийг (ОУЦХБ Х) байгуулсан. ОУЦХБ нь мөн TELECOM арга хэмжээнүүдийг зохион байгуулдаг ба

30. Эх сурвалж: APEC, “Telecommunications and Information Working Group,” http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html
31. “Combating the criminal misuse of information”, which recognizes that one of the implications of technological advances is increased criminal activity in the virtual world.
32. An Agreement undertaken in Budapest that aims to uphold the integrity of computer systems by considering as criminal acts any action that violates said integrity. See http://conventions.coe.int /Treaty/EN/Treaties/Html/185.htm.
33. This section is drawn from ITU, “About ITU,” http://www.itu.int/net/about/index.aspx.

МНДДХЧ-ын тэргүүлэх зохион байгуулалтын агентлаг байлаа.
Кибер аюулгүй байдлын салбар дахь ОУЦХБ-ын гол санаачлагуудад МНДДХЧ-ын үйл ажиллагааны чиглэл (МНДДХЧ Action Line C.5), ОУЦХБ-ын дэлхийн кибер аюулгүй байдлын хөтөлбөр (ITU Global Cybersecurity Agenda) болон ОУЦХБ-ын кибер аюулгүй байдлын гарц (ITU Cybersecurity Gateway) багтдаг.

МНДДХЧ үйл ажиллагааны чиглэл C.5 (Action Line C.5)-ын үндсэн зорилтууд нь:

- Онц чухал мэдээллийн дэд бүтцийн хамгаалалт- ОЧМДБХ
- Кибер аюулгүй байдлын дэлхийн соёлыг дэмжих;
- Үндэсний хууль зүйн арга замыг боловсронгуй болгох ба олон улсын хууль зүйн зохицуулалт ба хэрэгжилт;
- Спамтай тэмцэх;
- Хянах, анхааруулах ба гэнэтийн тохиолдолд хариу өгөх чадварыг хөгжүүлэх;
- Үндэсний арга барил, шилдэг туршлага болон үзэл баримтлалын талаарх мэдээллийг хамтран ашиглах; болон
- Нууцлал, өгөгдөл ба хэрэглэгчийн хамгаалалт.

ОУЦХБ-ын дэлхийн кибер аюулгүй байдлын хөтөлбөр (ITU Global Cybersecurity Agenda-GCA) нь мэдээллийн нийгэм дэх итгэл ба аюулгүй байдлыг бэхжүүлэх шийдлүүдийг санал болгох зорилго бүхий ОУЦХБ-ын олон улсын хамтын ажиллагааны хүрээ юм. GCA нь хууль зүйн хүрээ, техникийн арга хэмжээ, байгууллагын бүтэц, чадавхи хөгжүүлэлт ба олон улсын хамтын ажиллагаа гэсэн стратегийн таван баганатай. Эдгээр стратегиудыг доорх зорилгын дагуу боловсруулсан:

- Дэлхий нийтээр хэрэглэхүйц, одоогийн үндэсний/бүсийн хууль тогтоомжийн арга хэмжээ харилцан уялдах боломж бүхий кибер гэмт хэргийн загвар хууль тогтоомжийг боловсруулах;
- Кибер гэмт хэргийн талаарх үндэсний болон бүс нутгийн байгууллагын бүтэц, бодлогыг бий болгох;
- Програм хангамжийн аппликэйшн, системүүдэд зориулсан дэлхий нийтэд хүлээн зөвшөөрөгдсөн аюулгүй байдлын наад захын шалгуур, баталгаажуулалтын тогтолцоог бий болгох;
- Хил дамнасан санаачлагын зохицуулалтыг хангах үүднээс хяналт, анхааруулга ба будлианд хариу өгөх үйл ажиллагааны дэлхий нийтийн хүрээг бий болгох;
- Газар зүйн хил хязгаар дамнан иргэний дижитал үнэмлэхийг хүлээн зөвшөөрөх явдлыг хангах зорилгоор дэлхий нийтээр түгээмэл хэрэглэх, дижитал иргэний мэдээллийн систем болон шаардлагатай байгууллагын бүтцийг боловсруулан батлах;
- Салбар хоорондын болон дээр дурдсан бүх хүрээн дэх мэдлэг, чадавхийг бэхжүүлэх үүднээс хүн ба байгууллагын чадавхи хөгжүүлэлтийг хангах дэлхий нийтийн стратегийг боловсруулах; болон
- Дээр дурдсан бүх хүрээн дэх олон улсын хамтын ажиллагаанд зориулсан олон-оролцоот нийтлэг стратегийн талаар зөвлөмж өгөх.

ОУЦХБ кибер аюулгүй байдлын гарц нь үндэсний болон олон улсын кибер аюулгүй байдалтай холбоотой санаачлагын талаарх хэрэглэхэд хялбар мэдээллийн эх сурвалжаар хангах зорилготой. Эдгээр нь иргэд, төрийн байгууллага, бизнесийнхэн болон олон улсын байгууллагуудад нээлттэй байна. Гарцын үзүүлдэг үйлчилгээнд мэдээлэл хамтран ашиглах, хянах, анхааруулах, болон хууль тогтоомжууд, нууцлал, хамгаалалт мөн салбарын стандартууд, шийдлүүд багтана.

ОУЦХБ-Х нь мөн улс орнуудад кибер орон зайн өндөр төвшний аюулгүй байдлын технологийг хөгжүүлэхэд туслах зорилготой байгуулагдсан ОУЦХБ Кибер аюулгүй байдлын ажлын хөтөлбөр (ITU Cybersecurity Work Programme)-ийг хянадаг. Энэ нь дараах зүйлстэй холбоотой тусламжийг үзүүлдэг:

- Кибер аюулгүй байдал ба ОЧМДБХ-ын үндэсний стратегиуд болон чадавмжуудыг бий болгох
- Кибер гэмт хэргийн зохих хууль тогтоомж ба хэрэгжүүлэлтийн механизмуудыг тогтоох
- Хянах, анхааруулах ба гэнэтийн тохиолдолд хариу өгөх чадварыг бий болгох
- Спам болон холбогдох аюул заналтай тэмцэх
- Хөгжиж буй болон хөгжингүй орнуудын хоорондох аюулгүй байдалтай холбоотой

стандартчилалын ялгааг арилгах гүүр болох
- ОУЦХБ кибер аюулгүй байдал/ ОЧМДБХ лавлах, харилцагчийн мэдээллийн сан болон намтарын мэдээллийн лавлагаа хэвлэлийг бий болгох
- Кибер аюулгүй байдлын үзүүлэлтийг тогтоох
- Бүс нутгийн хамтын ажиллагааны арга хэмжээг дэмжих
- Мэдээлэл хамтран ашиглах ба ОУЦХБ аюулгүй байдлын Гарцыг дэмжих
- Холбогдох үйл ажиллагааг өргөжүүлэн дэмжих

Бусад ОУЦХБ-Х кибер аюулгүй байдалтай холбоотой үйл ажиллагаануудад StopSpamAlliance.org-той хамтарсан ажиллагаанууд, кибер гэмт хэргийн хууль тогтоомж ба хэрэгжүүлэлттэй холбоотой бүс нутгийн чадамж хөгжүүлэх ажиллагаанууд, ботнет устгах хэрэгслийн түгээлт[34], кибер аюулгүй байдал/кибер гэмт хэргийн талаарх хэвлэлүүд[35], хөгжиж буй орнуудад зориулсан кибер гэмт хэргийн загвар хууль тогтоомжийн багц болон үндэсний кибер аюулгүй байдлын өөрийгөө үнэлэх багц хэрэгсэл[36] зэрэг орно.

ISO/IEC-ийн мэдээллийн аюулгүй байдлын ажиллагаа

Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо-МАБУТ (Information Security Management System-ISMS) нь нэрнийх нь илэрхийлж буйгаар мэдээллийн аюулгүй байдлыг удирдах систем юм. Энэ нь аюулгүй байдлын эрсдлийг бууруулах явцдаа мэдээллийн хөрөнгийн найдвартай, нэгдмэл, ашиглах боломжтой байдлыг хангадаг үйл явцууд болон системүүдээс бүрдэнэ. МАБУТ гэрчилгээ нь дэлхий даяар ихээхэн түгээмэл бөгөөд 2005 онд дараах 2 баримт бичгийг гаргаснаар олон улсад стандартчилагдсан МАБУТ-ны түүхэнд эргэлт хийсэн юм. Үүнд: МАБУТ–г бий болгох шаардлагыг дурдсан IS 27001 ба МАБУТ-г хэрэгжүүлэх үндсэн хяналтыг тайлбарласан IS 17799:2005 гэх нэрээр хэвлэгдсэн IS 17799: 2000 орно.

Жинхэнэ МАБУТ стандарт нь BS 7799 байсан ба үүнийг 1995 онд Британийн Стандартын Байгууллага (British Standards Institution -BSI) мэдээлийн аюулгүй байдлын удирдлагыг хэрэглэх хууль хэлбэрээр анх боловсруулсан. 1998 онд энэхүү стандартад тулгуурлан шаардлагын нөхцлийг боловсруулснаар “мэдээлийн аюулгүй байдлын удирдлагыг хэрэглэх хууль” нь 1-р хэсэг, шаардлагын нөхцөл 2-р хэсэг нь болж өөрчлөгдсөн. 1-р хэсэг мэдээлийн аюулгүй байдлын удирдлагын хяналтыг авч үздэг бол 2-р хэсэг МАБУТ-ыг бий болгох шаардлагыг дурдаж, эрсдлийн удирдлагын суурийг тасралтгүй дээшлүүлэх зорилгоор мэдээллийн аюулгүй байдлын үйл явцыг тайлбарладаг (Төлөвлө-Хий-Шалга-Гүйцэтгэ мөчлөг).

1-р хэсгийг 2000 онд ISO/IEC JTC 1/SC27 WG1-ээр IS 17799 гэж тогтоосон. Түүнээс хойш, IS 17799 –ыг хянаж (2,000 гаруй саналаар), дахин засварлан эцсийн хувилбарыг 2005 оны 11 сард олон улсын стандартад бүртгүүлсэн. IS 17799: 2000 нь 10 хяналтын удирдлагын салбар бүхий 126 журмын жагсаалттай. 2005 онд засварласан IS 17799 11 захиргааны хяналтын хүрээ ба 133 журмыг багтаадаг.

1999 онд боловсруулсан BS 7799-ын 2-р хэсгийг МАБУТ гэрчилгээний стандарт болгон ашигладаг байв. Үүнийг 2002 оны 9 сард ISO 9001 болон ISO 14001-тэй нэгтгэн засварласан. ISO нь олон улсын стандартчилагдсан МАБУТ-ны хүсэлтүүдэд нийцүүлэх зорилгоор шуурхай аргачлал ашиглан BS7799 2-р хэсэг: 2002-ыг баталж, богино хугацаанд бага зэрэг засварлан олон улсын ISO27001 стандартаар бүртгэсэн. Хийгдсэн чухал өөрчлөлтүүдэд үр ашигтай байдлын талаарх агуулга нэмэх ба хавсралтыг өөрчлөх зэрэг багтана.

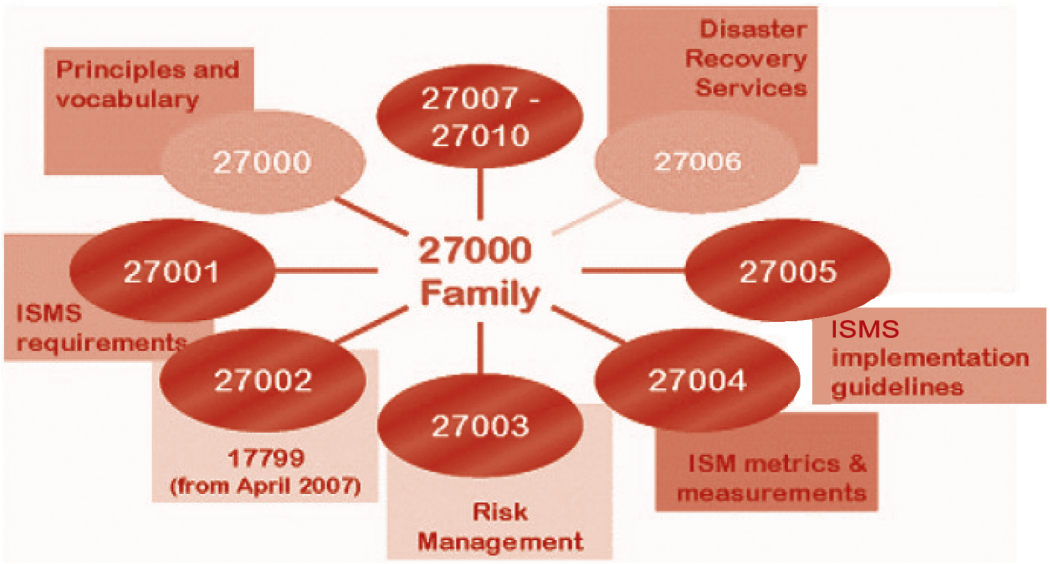
МАБУТ–той холбоотой хоёр чухал бичиг баримт олон улсад стандартчлагдсан учраас олон улсын аюулгүй байдлын стандартуудын бүлэг нь бусад удирдлагын системүүдтэй ижил 27000 гэсэн серийн дугаараар гарч ирсэн (Чанартай бизнес: 9000 сери, байгаль орчны удирдлага: 14000 сери). IS 17799:2005-ын засварласан хувилбар болох IS 27001 нь МАБУТ-г бий болгох шаардлагыг агуулдаг бөгөөд МАБУТ–г хэрэгжүүлэх үндсэн журмыг багтаасан IS17799:2005-ыг 2007 онд IS27002 болгож өөрчилсөн. МАБУТ–г хэрэгжүүлэх удирдамж, мэдээллийн аюулгүй байдлын эрсдлийн удирдлагын стандарт, JTC1SC27-ын боловсруулсан мэдээллийн аюулгүй байдлын удирдлагын хэмжилтийн

34. Suresh Ramasubramanian and Robert Shaw, “ITU Botnet Mitigation Project: Background and Approach” (ITU presentation, September 2007), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit.pdf.
35. ITU-D Applications and Cybersecurity Division, “Publications,” ITU, http://www.itu.int/ITU-D/cyb/publications/.
36. ITU-D Applications and Cybersecurity Division, “ITU National Cybersecurity / CIIP Self-Assessment Tool,” ITU, http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html.

норм ба хэжигдэхүүн зэрэг нь 27000 серид багтдаг.
Зураг 7-д МАБУТ-той холбоотой стандартуудын бүлгийг харууллаа. МАБУТ гэрчилгээ олгох ажиллагаанууд нь эрчимжиж байгаа ба ерөнхий системийн түгээмэл МАБУТ-д тулгуурлан тодорхой нэг салбарт тохирох МАБУТ стандарт болон удирдамжийг боловсруулахаар чармайж байна. Үүний илрэл нь холбооны салбарын онцлогийг тусгасан МАБУТ удирдамжийг хөгжүүлэх оролдлого юм.

Зураг 7. ISO/IEC 27001-ын бүлэг

(ANSIL, Roadmap ISO/IEC 2700x, ISMS, Forum Eurosec 2007,
http://www.ansil.eu/files/pres-eurosec2007-23052007.pdf)



АСУУЛТ

Олон улсын байгууллагуудын санаачилсан мэдээллийн аюулгүй байдлын ямар үйл ажиллагаанууд танай оронд хэрэгжсэн мөн хэрэгжиж байна вэ? Тэдгээрийг хэрхэн хэрэгжүүлж байна вэ?

ӨӨРИЙГӨӨ ШАЛГАХ НЬ

1. Энэ бүлэгт багтсан орнуудын хэрэгжүүлж буй мэдээллийн аюулгүй байдлын үйл ажиллагаануудын төстэй тал нь юу вэ? Ялгаатай нь юу вэ?

2. Энэ бүлэгт багтсан олон улсын байгууллагуудын мэдээллийн аюулгүй байдлын эн тэргүүний зорилтууд нь юу вэ?

4. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН АРГА ЗҮЙ

Энэхүү хэсэг нь олон улсад хэрэглэгддэг удирдлагын, материаллаг болон техникийн мэдээллийн аюулгүй байдлын арга зүйг тодорхойлох зорилготой.

4.1 Мэдээллийн аюулгүй байдлын арга зүй

Мэдээллийн аюулгүй байдлын арга зүй нь мэдээллийн хөрөнгөд хамааралтай байж болох эмзэг байдал, аюул заналыг анхааран үзэж хохирлыг багасгах болон бизнесийн тасралтгүй байдлыг сахих зорилготой. Бизнесийн тасралтгүй байдлыг баталгаажуулахын тулд мэдээллийн аюулгүй байдлын аргачлал нь дотоод мэдээллийн хөрөнгийн найдвартай, нэгдмэл, ашиглах боломжтой байдлыг хангах замыг эрэлхийлдэг. Энэ нь эрсдлийн үнэлгээний арга, хяналтуудын хэрэглээг багтаадаг. Гол нь мэдээллийн аюулгүй байдлын удирдлагын, материаллаг болон техникийн талуудыг хамарсан сайн төлөвлөгөө чухал юм.

Удирдлагын хэсэг

Удирдлагын хэсэгт анхаардаг олон МАБУТ-нууд байдаг. ISO/IEC27001 нь түгээмэл хэрэглэгддэг стандартуудын нэг юм.

Олон улсын МАБУТ стандарт болох ISO/IEC27001 нь BSI –аас гаргасан BS7799 дээр үндэслэсэн. BS7799 нь МАБУТ болон төрөл бүийн байгууллагуудын аюулгүй байдлын стандартууд болон үр дүнтэй аюулгүй байдлын удирдлагад хэрэглэгддэг түгээмэл стандартуудыг хэрэгжүүлэх шаардлагыг нарийвчлан тодорхойлдог. BS7799-ын 1-р хэсэгт байгууллагууд дахь аюулгүй байдлын ажиллагаануудын шилдэг туршлага дээр үндэслэсэн шаардлагатай аюулгүй байдлын ажиллагаануудыг тодорхойлдог.

Одоогийн ISO/IEC27001 болсон 2-р хэсэгт МАБУТ ажиллагаа ба аюулгүй байдлын ажиллагаануудын үнэлгээнд шаардагдах наад захын шаардлагыг дэвшүүлдэг.

ISO/IEC27001-ийн аюулгүй байдлын ажиллагаанууд нь 133 хяналт ба 11 чиглэлээс бүрдэнэ (Хүснэгт 5).

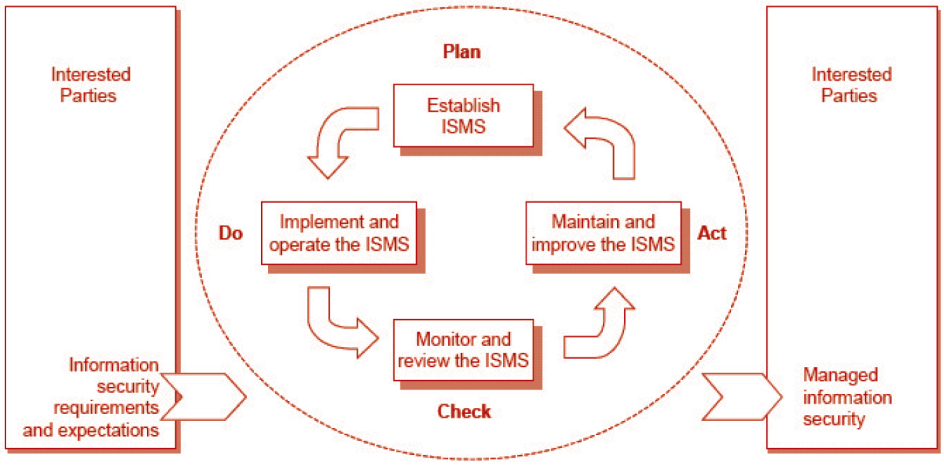
Хүснэгт 5. ISO/IEC27001-ын хяналт

Чиглэл	Элемент
A5.	Аюулгүй байдлын бодлого
A6.	Мэдээллийн аюулгүй байдлын зохион байгуулалт
A7.	Хөрөнгийн удирдлага
A8.	Хүний нөөцийн аюулгүй байдал
A9.	Материллаг болон байгаль орчны аюулгүй байдал
A10.	Холбоо ба үйл ажиллагааны удирдлага
A11.	Хандалтын хяналт
A12.	Мэдээллийн системийн эзэмшил, хөгжүүлэлт ба ашиглалт
A13.	Мэдээллийн аюулгүй байдлын будлианы удирдлага
A14.	Бизнесийн тасралтгүй байдлын удирдлага
A15.	Биелэлт

ISO/IEC27001 нь МАБУТ–ны бүх үйл явцыг бүтэцлэхэд ашиглагдсан Plan-Do-Check-Act үйл явцын загварыг авч хэрэгжүүлсэн. ISO/IEC27001-д МАБУТ үнэлгээний бүх нотолгоог бичиг баримтжуулах ёстой; гэрчигээг 6 сар тутамд хөндлөнгийн хяналтаар шалгуулах ёстой; мөн МАБУТ–ыг тасралтгүй удирдахын тулд нийт үйл явцыг 3 жилийн дараа давтах ёстой.

Зураг 8. МАБУТ явцад хэрэглэгддэг Төлөвлө-Хий-Шалга-Гүйцэтгэ гэсэн аргын загвар

(Source: ISO/IEC JTC 1/SC 27)



Аюулгүй байдлын хяналтуудыг аюулгүй байдлын шаардлагыг тооцож үзсэний үндсэн дээр төлөвлөх хэрэгтэй. Ханган нийлүүлэгч, гэрээлэгчид, үйлчлүүлэгчид болон гадны мэргэжилтнүүд гээд бүх хүний нөөц эдгээр үйл ажиллагаанд оролцох ёстой. Аюулгүй байдлын шаардлагыг тогтоохдоо дараах гурван хүчин зүйлд үндэслэнэ. Үүнд:

- Эрсдлийн үнэлгээ
- Хууль зүйн шаардлага ба гэрээний нөхцөлүүд
- Байгууллагыг ажиллуулах мэдээллийн үйл явц

Завсрын дүн шинжилгээ (Gap analysis) нь одоогийн мэдээллийн аюулгүй байдлын төвшнийг хэмжиж мэдээллийн аюулгүй байдлын ирээдүйн чиглэлийг тогтоох явцыг хэлдэг. Завсрын дүн шинжилгээний үр дүн нь хөрөнгө эзэмшигчийн 133 хяналт ба 11 чиглэлд өгсөн хариултаас үүсэн гарна. Завсрын шинжилгээгээр дутагдалтай хэсгийг нэгэнтээ илрүүлсэн бол тухайн хэсэг бүрт тохирох хяналтыг тогтоох боломжтой.

Эрсдлийн үнэлгээг хөрөнгийн өртөгийн үнэлгээ ба аюул занал, эмзэг байдлын үнэлгээ гэж хуваадаг. Хөрөнгийн өртөгийн үнэлгээ гэдэг нь мэдээллийн хөрөнгийн тоон үнэлгээ юм. Аюул заналын үнэлгээ нь аюулыг найдвартай, нэгдмэл, ашиглах боломжтой байдалтай харьцуулсан үнэлгээ. Доорх жишээнд эрсдлийн үнэлгээнд орсон тооцоололыг харууллаа.

Орлогын нэр	Орлогын өртөг	Аюул занал			Эмзэг байдал			Эрсдэл		
		C	I	A	C	I	A	C	I	A
Хөрөнгийн нэр #1	2	3	3	1	3	1	1	8	6	5

- Хөрөнгийн өртөг + Аюул занал + Эмзэг байдал = Эрсдэл
- Найдвартай байдал: Хөрөнгийн өртөг (2) + Аюул занал (3) + Эмзэг байдал (3) = Эрсдэл (8)
- Нэгдмэл байдал: Хөрөнгийн өртөг (2) + Аюул занал (3) + Эмзэг байдал (1) = Эрсдэл (6)
- Боломжтой байдал: Хөрөнгийн өртөг (2) + Аюул занал (1) + Эмзэг байдал (1) = Эрсдэл (5)

Хяналтын хэрэглээ: Эрсдлийн өртөг тус бүр эрсдлийн үнэлгээний үр дүнгээс хамааран өөр өөр байна. Ялгаатай үнэлэгдсэн хөрөнгөд тохирох хяналтыг хэрэглэхийн тулд шийдвэр гаргах хэрэгтэй болно. Эрсдлүүдийг “Итгэмжлэлийн зэрэг- Degree of Assurance” гэсэн шалгуурын дагуу хүлээн авч болох ба хүлээн авч болохгүй эрсдэл гэж хуваадаг. Хүлээн авч болохгүй эрсдэлтэй мэдээллийн хөрөнгөд хяналтыг хэрэгжүүлэх хэрэгтэй болно. Хяналтыг ISO/IEC хяналтууд дээр үндэслэн хэрэгжүүлэх боловч байгууллагын бодит байдлаас хамаарч хэрэгжүүлэх нь илүү үр дүнтэй.

Улс бүхэн ISO/IEC27001 гэрчилгээний байгууллагатай. Хүснэгт 6*д гэрчилгээний тоог улсаар нь жагсаан харууллаа.

Хүснэгт 6. Гэрчилгээний тоо, улсаар

Япон	2863*	Нидерланд	11	Болгар	2
Энэтхэг	433	Сингапур	11	Канад	2
Нэгдсэн вант улс	368	Филиппин	10	Гибралтар	2
Тайвань	202	Саудын Араб	10	Мэний арал	2
Хятад	174	Пакистан	10	Морокко	2
Герман	108	ОХУ	10	Оман	2
АНУ	82	Франц	9	Катар	2
Унгар	74	Колумб	7	Йемен	2
БНСУ	71	Словен	7	Армани	1
Чех	66	Швед	7	Бангладеш	1
Итали	54	Словак	6	Бельги	1
Хонг Конг	38	Хорват	5	Египет	1
Польш	36	Грек	5	Иран	1
Австрали	28	Өмнөд Африк	5	Казакстан	1
Австри	26	Бахрэйн	4	Киргизстан	1
Ирланд	26	Индонез	4	Лебанон	1
Малайз	26	Кувет	4	Литва	1
Испани	26	Норвег	4	Льюксембург	1
Бразил	20	Шри-Ланк	4	Македон	1
Мексик	20	Швейцарь	4	Молдав	1
Тайланд	17	Чили	3	Шинэ Зеланд	1
Румынь	16	Макао	3	Украйн	1
Турк	15	Перу	3	Уругвай	1
Араб	14	Португал	3	Харьцангуй нийлбэр	4997
Исланд	11	Вьетнам	3	**Үнэмлэхүй нийлбэр**	**4987**

Тэмдэглэл: Энд үзүүлсэн гэрчилгээний тоо 2008 оны 12 сарын 21-ны байдлаар.
Эх сурвалж: International Register of ISMS Certificates, “Number of Certificates per Country,” ISMS International User Group Ltd., http://www.iso27001certificates.com.

Биет буюу материаллаг тал

Одоогоор олон улсын мэдээллийн аюулгүй байдлын биет удирдлагын систем байхгүй. Харин үүний оронд АНУ дахь биет ISMS-ын стандарт болдог, мөн олон улсад аргачлал болгон ашиглагддаг Холбооны Онцгой Байдлын Удирдах Агентлаг - ХОБУА (Federal Emergency Management Agency -FEMA) 426[37]-ыг энд тайлбарлана.

ХОБУА 426 нь барилгыг террорист халдлагаас хамгаалах удирдамжаар хангадаг. Үүнд "Архитектор болон инженерүүдээс бүрдсэн барилгын шинжлэх ухааны бүлэг нь террорист халдлагын улмаас барилга, холбогдох дэд бүтэц болон хүмүүст учирсан хохирлыгбагасгах"-ыг заасан байна.[38] Холбогдох удирдамжийн цувралууд нь ХОБУА 427 ("Террорист халдлагыг сулруулах худалдааны барилгын загварын цагаан толгой - Primer for the Design of Commercial Buildings to Mitigate Terrorist Attacks"), ХОБУА 428 ("Террорист халдлагын үед аюулгүй сургуулийн барилгыг загварчлах цагаан толгой- Primer to Design Safe School Projects in Case of Terrorist Attacks"), ХОБУА 429 ("Барилга дахь терроризмын эрсдлийн удирдлагад зориулсан даатгал, санхүү, ба зохицуулалтын цагаан толгой -Insurance, Finance, and Regulation Primer for Terrorism Risk Management in Buildings"), ХОБУА 430 (архитектор), ба ХОБУА 438 (чиглэл).

ХОБУА 426 нь мэдээллийн аюулгүй байдалтай шууд холбоогүй боловч барилгад халдсан биет халдлагын улмаас мэдээлэл задрах, алдагдах, устахаас сэргийлэх боломжтой. Ялангуяа, ХОБУА 426 нь удирдлагын аюулгүй байдлын бүрдэл хэсэг болох бизнесийн тасралтгүй байдлын төлөвлөгөөтэй нягт холбоотой. ХОБУА 426-ыг ашигласнаар бизнесийн тасралтгүй байдлын төлөвлөгөөний биет талыг хамгаалах боломжтой.

Техникийн тал

Техникийн талын МАБУТ байдаггүй. Нийтлэг Шалгуур - НШ (Common Criteria - CC) гэх мэт олон улсын түгээмэл үнэлгээний стандартуудыг үүний оронд ашиглаж болно.

Нийтлэг Шалгуурын гэрчилгээ[39]

НШ гэрчилгээг өөр өөр улсын МТ-ийн бүтээгдэхүүний аюулгүй байдлын ялгаатай төвшингийн талаарх асуудлыг анхаарч үзэх зорилгоор бий болгосон.

Канад, Франц, Герман, Их Британи болон АНУ зэрэг улсууд МТ-ийн бүтээгдэхүүний үнэлгээний олон улсын стандартыг бий болгосон.

Тодруулбал, НШ нь үйл ажиллагааны болон баталгааны шаардлагуудын тодорхой ангилалд багтах бүтээгдэхүүн, системийн МТ-ийн аюулгүй байдлын шаардлагыг төлөөлдөг.

НШ үйл ажиллагааны шаардлагууд нь аюулгүй байдлын зохих горимыг тодорхойлдог. НШ аюулгүй байдлын функц нь 57 бүлгээс бүтсэн 11 төрлийн 136 бүрдэл хэсгээс тогтдог. Батагааны шаардлагууд нь 40 бүлгийн 9 төрлөөс авсан 86 бүрдэл хэсгээс бүтнэ.

Аюулгүй байдлын функцийн шаардлага-АБФШ: Үнэлгээний объект (Target of Evaluation-TOE)-ын бүх аюулгүй байдлын функцүүдийг тодорхойлдог.
Хүснэгт 7-д SFR-д багтсан аюулгүй байдлын функцүүдийн төрлийг жагсаасан.

37. FEMA, "FEMA 426 - Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings," http://www.fema.gov/plan/ prevent/rms/rmsp426.
38. Ibid.
39. Common Criteria, http://www.commoncriteriaportal.org.

Хүснэгт 7. АБФШ дахь төрлийн бүрэлдэхүүн

Төрлүүд		Дэлгэрэнгүй
FAU	Аюулгүй байдлын аудит	Аудитын мэдээлэл хамгаалалт, бичлэгийн хэлбэр ба үйл явдлын сонголт, мөн дүн шнжилгээний хэрэгсэл, үөрчлийн дохио болон бодит-цагийн дүн шинжилгээ зэргийг багтаасан функцыг илтгэнэ
FCO	Холбоо	Мэдээллийн шилжилтэнд ашиглагддаг YO-ын шалгуурыг тодорхойлно.
FCS	Криптографийн дэмжлэг	Криптографийн түлхүүрийн удирдлага болон болон криптографийн ажиллагааг тодорхойлдог
FDP	Хэрэглэгчийн мэдээлэл хамгаалалт	Хэрэглэгчийн мэдээллийг хамгаалахтай холбоотой шаардлагуудыг заадаг
FIA	Танилт ба	Хүсэлт гаргасан хэрэглэгчийн мэдээллийг бий болгож баталгаажуулах функцын шаардлагыг авч үзнэ
FMT	Аюулгүй байдлын удирдлага	YO Аюулгүй байдлын функцын (АБФ) хэд хэдэн талын удирдлагыг тодорхойлдог: аюулгүй байдлын шинж чанар, АБФ өгөгдөл ба функцууд
FPR	Нууцлал	Системийн ажиллагааг хангалттай хянаж чадах хэмжээний хүрээнд уян хатан байдлыг зөвшөөрөхийн зэрэгцээ хэрэглэгчийн нууцлалын хэрэгцээг хангахын тулд шаардаж болох шаардлагууд
FPT	АБФ-ын хамгаалалт	АБФ ба АБФ өгөгдлийн нийлмэл байдлыг бүрдүүлдэг механизмуудын нэгдэл ба удирдлагатай холбогдох функцын шаардлагуудын бүлгийг багтаана
FRU	Нөөц ашиглалт	Боловсруулах чадамж ба/эсвэл хадгалалтын багтаамж зэрэг шаардлагтай нөөцийн бэлэн байдлыг багтаадаг
FTA	YO хандалт	Хэрэглэгчийн үеийн байгуулалтыг хянах функцийн шаардлагыг тодорхойлдог
FTP	Итгэмжлэгдсэн зам/ суваг	Хэрэглэгч ба АБФ хоорондын итгэмжлэгдсэн холбооны шаардлагаар хангадаг.

Эх сурвалж: Common Criteria, Common Methodology for Information Technology Security Evaluation, September 2007, CCMB-2007-09-004

Аюулгүй байдлын баталгаажуулалтын бүрдлүүд-АББББ: НШ-ын философи нь оновчтой бөгөөд хангалттай аюулгүй байдлын арга хэмжээгээр аюулгүй байдал дахь аюулыг тодорхойлох болон байгууллагын аюулгүй байдлын бодлогод анхаарахыг шаардаж байна. Авч хэрэгжүүлэх арга хэмжээнүүд нь эмзэг байдлыг таньж, түүнийг урвуулан ашиглах магадлалыг бууруулан эмзэг байдлыг ашигласан тохиолдолд учрах хохирлын хэмжээг багасгахад туслах ёстой.[40] Хүснэгт 8-д АББББ-д багтах төрлүүдийг жагсаалаа.

40. Common Criteria, Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements (August 1999, Vesion 2.1), http://www.scribd.com/doc/2091714 /NSA-Common-Critira-Part3.

Хүснэгт 8. АББББ дахь төрлийн бүрэлдэхүүн

Төрлүүд		Дэлгэрэнгүй
APE	Хамгаалалтын профайлын (Protection Profile-PP) үнэлгээ	ХП нь нарийвчилсан бөгөөд дотооддоо тогтвортой гэдгийг, хэрэв ХП нь нэг ба түүнээс дээш ХП эсвэл багц дээр суурилсан бол ХП нь тэдгээр ХП -ууд болон багцуудын зөв жишээ болсон гэдгийг харуулах шаардлагатай
ASE	Аюулгүй байдлын үзүүлэлтийн (Security Target -ST) үнэлгээ	АБҮ нь нарийвчилсан бөгөөд дотооддоо тогтвортой гэдгийг, хэрэв АБҮ нь нэг ба түүнээс дээш ХП эсвэл багц дээр суурилсан бол АБҮ нь тэдгээр ХП-үүд болон багцуудын зөв жишээ болсон гэдгийг харуулах шаардлагатай
ADV	Хөгжүүлэлт	Энэ нь ҮО-ын талаарх мэдээллээр хангадаг. Олж авсан мэдлэгийг ATE болон AVA төрлүүдэд тайлбарласанчлан эмзэг байдлын дүн шинжилгээ явуулах болон ҮО дээр тест хийхэд хэрэглэдэг.
AGD	Удирдамжийн баримт бичиг	ҮО-ын аюулгүй бэлтгэл ба ажиллагааг хангахын тулд ҮО-ын аюулгүй ажиллагаатай холбоотой бүхий л холбогдох талуудыг тайлбарлах шаардлагатай.
ALC	Амьдралын мөчлөгийн дэмжлэг (Life-cycle support)	Конфигурацийн удирдлагын- КУ (Configuration Management) чадамж, КУ хүрээ, нийлүүлэлт, хөгжүүлэлтийн аюулгүй байдал, гэмтэл засах, амьдралын мөчлөг тогтоох, техник, хэрэгсэл, зэргийг багтаасан бүтээгдэхүүний амьдралын мөчлөгт ҮО нь хөгжүүлэгчийн болон хэрэглэгчийн хэнийх нь хариуцлагын дор байгаа гэдгээрээ ялгаатай.
ATE	Тестүүд	Энэ төрлийн онцлох зүйл нь АБФ нь загварын тодорхойлолтынхоо дагуу ажиллаж байгааг баталгаажуулах юм. Энэ төрөл нь нэвтрэлтийн тестийг авч үздэггүй.
AVA	Эмзэг байдлын үнэлгээ	Эмзэг байдлын үнэлгээний үйл ажиллагаа ҮО-ийн хөгжүүлэлт ба ажиллагаан дахь ялгаатай эмзэг байдлуудыг хамардаг.
ACO	Бүрэлдэхүүн	Бүтээсэн ҮО нь өмнө нь үнэлэгдсэн програм хангамж, микропрограм эсвэл техник хангамжийн бүрдэл хэсгийг нийлүүлсэн аюулгүй байдлын функцэд түшиглэх үедээ найдвартай ажиллана гэсэн баталгаагаар хангах зорилготой баталгаажуулалтын шаардлагыг нарийвчлан зааж өгдөг.

Эх сурвалж: Common Criteria, Common Methodology for Information Technology Security Evaluation, September 2007, CCMB-2007-09-004

НШ-ын үнэлгээний арга

1. ХП-ын үнэлгээ: ХП нь ҮО ангилалын хэрэгжилтээс хараат бус аюулгүй байдлын багц шаардлагыг тодорхойлдог ба тохирох бүтээгдэхүүнээр шийдвэрлүүлэх аюулгүй байдлын асуудлын талаарх мэдээллийг агуулдаг. Энэ нь НШ функцын болон баталгааны шаардлагуудыг тодорхойлдог бөгөөд сонгосон функцын болон баталгааны бүрдэл хэсгүүдийн оновчтой байдлаар хангана. Үүнийг МТ-ийн аюулгүй байдлын шаардлагыг хэрэглэгч эсвэл хэрэглэгчийн бүлэг бүтээдэг.

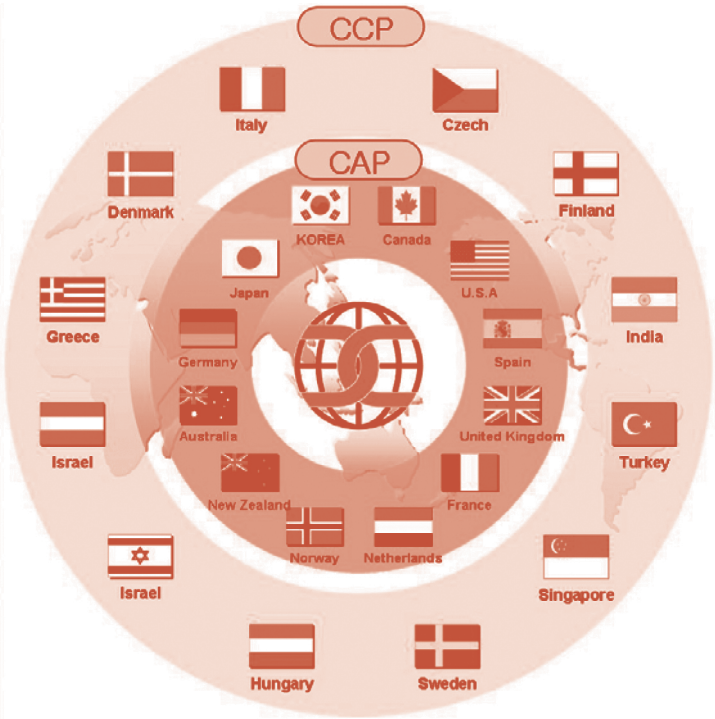
2. АБҮ-ийн үнэлгээ: АБҮ бол ҮО-ын санал болгодог аюулгүй байдал ба үнэлгээний хамрах хүрээний талаас ҮО-ыг хөгжүүлэгч, хэрэглэгч, үнэлгээ хийгч болон үнэлгээний удирдлагын хоорондын хийсэн гэрээний үндэс нь юм. АБҮ–ийн үйлчлүүлэгчдэд ҮО -ыг удирдаж, борлуулж байгаа, худалдан авч байгаа, суурилуулж байгаа, тохируулж байгаа, ажиллуулж байгаа болон ашиглаж байгаа хүмүүс багтана. АБҮ нь зарим бүтээгдэхүүн аюулгүй байдлын шаардлагыг хэрхэн хангаж байгааг харуулах тодорхой нэг хэрэгжилтэнд зориулсан мэдээллийг агуулдаг. Энэ нь нэг ба түүнээс дээш ХП-ыг илтгэж болно. Энэ тохиолдолд АБҮ нь тэдгээр ХП тус бүрд өгөгдсөн аюулгүй байдлын ерөнхий шаардлагуудыг хангах ёстой бөгөөд түүнээс цаашхи шаардлагуудыг тодорхойлж болно.

Нийтлэг шалгуурыг хүлээн зөвшөөрөх гэрээ (Common Criteria Recognition Arrangement)

Нийтлэг шалгуурыг хүлээн зөвшөөрөх гэрээ-НШХЗГ (Common Criteria Recognition Arrangement -CCRA)-ийг үндэстнүүдийн дунд НШ сертификатуудыг зөвшөөрөх зорилгоор зохион байгуулсан. Энэ нь стандартын дагуу НШ үнэлгээ хийгдэж байгааг баталгаажуулах, МТ-ийн бүтээгдэхүүнүүд эсвэл хамгаалалтын мэдээллийн давхардсан үнэлгээг арилгах болон багасгах, мөн гишүүн орнуудын дунд гэрчилгээг батлах замаар МТ-ийн салбар дахь дэлхийн зэх зээлийн боломжуудыг дээшлүүлэх зорилготой.

НШХЗГ нь 24 гишүүн оронтой ба үүний 12 нь Гэрчилгээг Баталгаажуулах Оролцогчид-ГБО (Certificate Authorizing Participants- CAP), 12 нь Гэрчилгээг Ашиглах Оролцогчид-ГАО (Certificate Consuming Participants- CCPs) юм. ГБО нь үнэлгээний гэрчилгээг үйлдвэрлэгчид юм. Тэд өөрсдийн орны гэрчилгээ олгох байгууллагын ивээн тэтгэгч бөгөөд олгогдсон гэрчилгээг баталгаажуулдаг. Тухайн улс ГБО болохоор хүсэлт гаргахаас өмнө хамгийн багадаа 2 жилийн турш ГАО статустай НШХЗГ-ний гишүүн байх ёстой. ГАО нь үнэлгээний гэрчилгээг хэрэглэгчид. Хэдийгээр МТ-ийн аюулгүй байдлын үнэлгээний чадавхийг мөрдөхгүй байж болох ч тэд гэрчилгээтэй/баталгаажсан бүтээгдэхүүн ба хамгаалалтын мэдээллийг ашиглах сонирхолтой байдаг. НШХЗГ-ний гишүүн болохын тулд тухайн орон Удирдлагын хороонд бичгээр хүсэлтээ гаргах ёстой.

Зураг 9. ГБО ба ГАО



4.2 Мэдээллийн аюулгүй байдлын арга зүйн жишээ

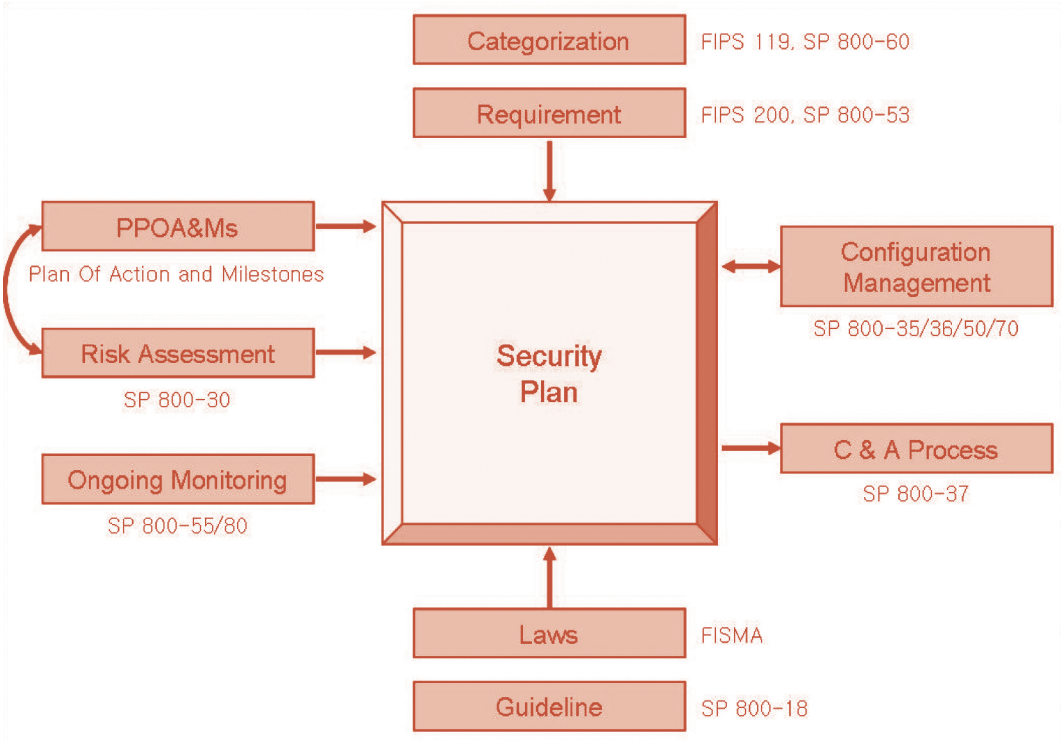
АНУ-ын стандарт, технологийн үндэсний институт

ХМАБУХ-д тулгуурлан, АНУ-ын Стандарт, Технологийн Үндэсний Төв-СТУТ (US National Institute of Standards and Technology-NIST) нь Холбооны байгууллагууд хэрэглэх боломжтой аюулгүй байдлын мэдээлэл ба мэдээллийн системүүдийг бэхжүүлэх журам, стандартуудыг боловсруулаад байна. Журам, стандартууд нь дараах зорилготой:

- Холбооны мэдээлэл ба мэдээллийн системүүдийн ангилалд ашиглаж болох стандартуудыг боловсруулах замаар наад захын аюулгүй байдлын шаардлагыг нарийвчилсан жагсаалтаар хангах;
- Мэдээлэл ба мэдээллийн системүүдийг ангилах боломжтой болгох;
- Холбооны засгийн газрын гүйцэтгэх агентлагуудад үйлчилж буй мэдээллийн системүүдийн аюулгүй байдлын хяналтыг сонгож нарийвчлан зааж өгөх; болон
- Эмзэг байдал дахь аюулгүй байдлын хяналтын ашиг тус, үр дүнг баталгаажуулах.

ХМАБУХ–тай холбоотой журмуудыг тусгай хэвлэл болон Холбооны мэдээллийн боловсруулалтын стандартуудын хэвлэл болгон гаргасан. Үүнд мэдээллийн технологийн 500 цуврал ба компьютерийн аюулгүй байдлын 800 цуврал гэсэн 2 төрлийн цуврал багтана. Зураг 10-т АНУ-ын Засгийн газар аюулгүй байдлын бодлогоо энэхүү стандартад тулгуурлан тогтоохдоо баримталдаг журмыг харууллаа.

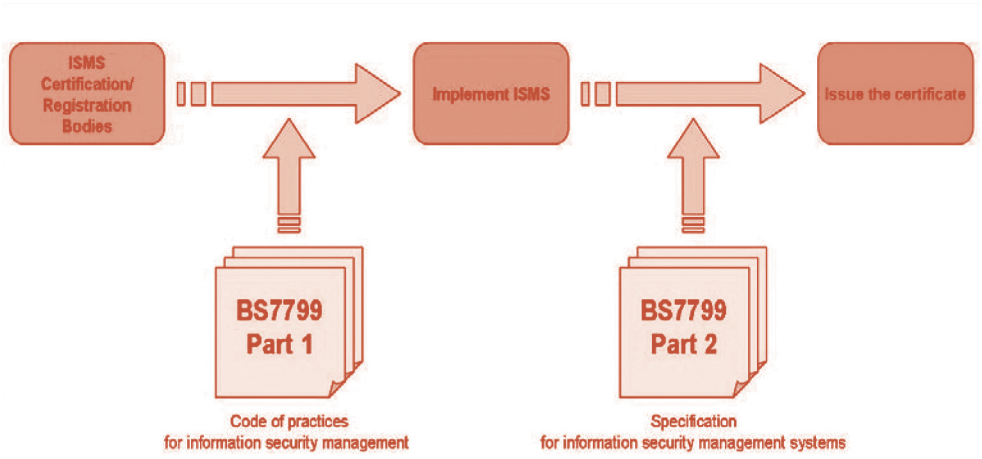
Зураг 10. Аюулгүй байдал төлөвлөлтийн явцын оролт/гаралт



Нэгдсэн Вант Улс (BS7799)

Өмнө нь дурдсанчлан, МАБА нь Англи дахь байгууллагуудын аюулгүй байдлын үйл ажиллагааг шинжилдэг бөгөөд одоогийн ISO27001 (BS7799 2-р хэсэг), ISO27002 (BS7799 1-р хэсэг) болон боловсруулагдсан BS7799 гэрчилгээг олгодог байв.
Зураг 11-т үйл явцыг харууллаа.

Зураг 11. BS7799 гэрчилгээ олгох үйл явц

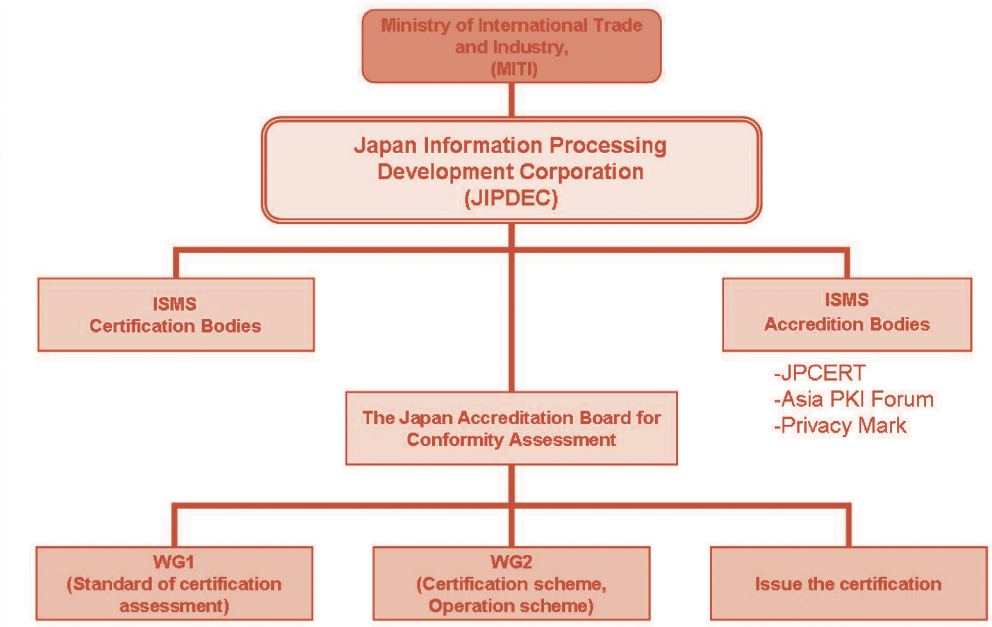


Япон (МАБУТ Хув2.0-оос BS7799 2-р хэсэг: 2002 хүртэл)

Японы мэдээлэл боловсруулалтын хөгжлийн корпорацийн МАБУТ Ver2.0 нь Японд 2002 оны 4 сараас хойш ашиглагдаж байна. Саяхан үүнийг BS7799 2-хэсэг: 2002 орлон гарч ирсэн. Засгийн газар мэдээллийн аюулгүй байдлын төлөвлөлтийг дэмжиж эхэлснээс хойш гэрчилгээ авахаар хүсэлт гаргагчдын тоо нэмэгдсэн. Орон нутгийн захиргааныхан байгууллагуудад МАБУТ гэрчилгээ авахад нь туслах зорилгоор мөнгөн тэтгэмж өгч эхлээд байна. Гэхдээ МАБУТ Ver2.0 удирдлагын талыг бараг онцолж авч үздэггүй мөн мэдээллийн аюулгүй байдлын техникийн талыг агуулаагүй. Түүнчлэн, ихэнх байгууллагууд зөвхөн гэрчилгээ авах сонирхолтой байдгаас бус өөрсдийн мэдээллийн аюулгүй байдлын үйл ажиллагааг сайжруулахад анхаардаггүй.

Зураг 12-т Японы МАБУТ гэрчилгээ олгодог системийг харууллаа.

Зураг 12. Японы МАБУТ гэрчилгээ олголт

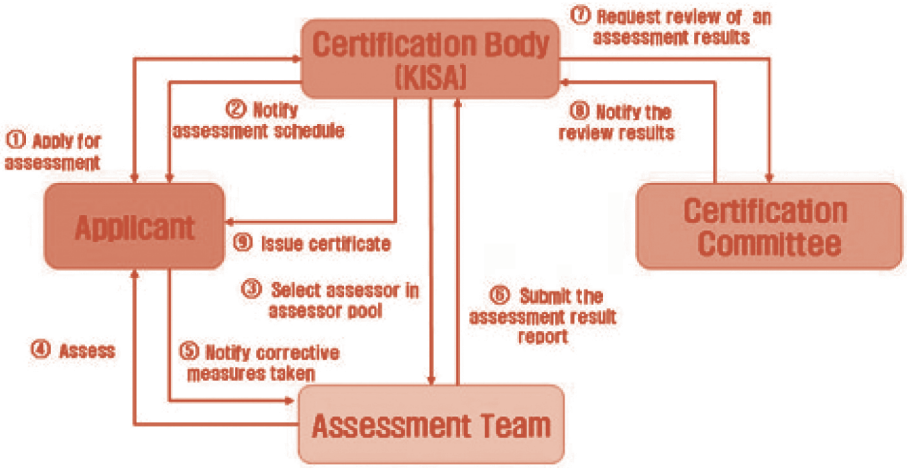


БНСУ (ISO/IEC27001 буюу СМАБА-ийн МАБУТ

Солонгосын мэдээллийн аюулгүй байдлын агентлагаас-СМАБА (Korea Information Security Agency) олгодог, голчлон МХЯ-ны боловсруулсан, МАБУТ гэрчилгээг Солонгосын BSI ISO/IEC 27001 –г нэвтрүүлж байх үед ашиглаж байв. СМАБА-гийн МАБУТ бол техникийн/материаллаг аюулгүй байдлын төлөвлөгөөг багтаадаг нийлмэл удирдлагын систем юм. Тийм учраас СМАБА МАБУТ гэрчилгээний систем нь ISO/IEC27001-д хангалттай байдаггүй мэдээллийн аюулгүй байдлын техникийн хэсгийг бэхжүүлдэг. Ялангуяа “Аюулгүй байдлын журам”-ыг гэрчилгээний шаардлага болгон нэвтрүүлсэн нь техникийн шалгалтыг чангатгасан. Зураг 13-т СМАБА МАБУТ-ын гэрчилгээ олгох үйл явцыг харууллаа.

Зураг 13. СМАБА-ийн МАБУС гэрчилээ

(Эх сурвалж: KISA, “Procedure of Application for ISMS Certification” (2005), http://www.kisa.or.kr/index.jsp)



Герман (МТ-ийн үндсэн хамгаалалтын шаардлага)

Германы МАБА (Bundesamt fur Sicherheit in der Informationstechnik) бол мэдээллийн аюулгүй байдлын үндэсний агентлаг юм. Энэхүү байгууллага нь Германы засгийн газар болоод Германы хотууд, байгууллагууд болон хувь хүмүүст МТ-ийн аюулгүй байдлын үйлчилгээ үзүүлдэг.

МАБА нь Европын МТ-ийн шалгалт ба гэрчилгээний хорооноос хүлээн зөвшөөрөгдсөн олон улсын стандарт болох ISO Guide 25[GUI25] ба Европын стандарт EN45001-д тулгуурлан МТ-ийн үндсэн хамгаалалтын шаардлагыг тогтоосон. Гэрчилгээний төрлүүдэд МТ-ийн үндсэн хамгаалалтын шаардлага, өөрсдийнх нь нэрлэснээр (МТ-ийн үндсэн хамгаалалтын дээд төвшин) болон (МТ-ийн үндсэн хамгаалалтын эхлэл төвшин) багтана.

Түүнчлэн, суурь хамгаалалтын гарын авлага (Baseline protection manual-BPM) болон МАБА стандартын цувралуудын дэд-гарын авлага: 100-Х-ыг боловсруулсан. Тэдгээрт: BSI стандарт 100-1 МАБУТ, МАБА стандарт 100-2, BPM аргачлал болон МАБА стандарт 100-3 Эрсдлийн үнэлгээ[41] зэрэг баримт бичгүүд багтана.

Бусад

Хүснэгт 9-д одоогийн МАБУТ гэрчилгээг жагсаалаа.

Хүснэгт 9. Бусад орнуудын МАБУТ гэрчилгээ

Гэрчилгээний байгууллагууд		Стандартууд
Канад	Холбооны аюулгүй байдлын байгууллага (Communications Security Establishment)	MG-4, Мэдээллийн технологийн системийн гэрчилгээ, баталгаажуулалтын журам
Тайвань	Стандарт, хэмжил зүй, хяналт шалгалтын газар (Bureau of Standards, Meteorology and Inspection)	CNS 17799 & CNS 17800
Сингапур	Мэдээллийн технологийн стандартын хороо (Information Technology Standards Committee)	SS493 : 1-р хэсэг (МТ аюулгүй байдлын стандартын хүрээ) & SS493 : 2-р хэсэг (Боловсруулж буй аюулгүй байдлын үйлчилгээнүүд)

41. Antonius Sommer, “Trends of Security Strategy in Germany as well as Europe” (presentation made at the 2006 Cyber Security Summit, Seoul, Republic of Korea, 10 April 2006), http://www.secure.trusted-site.de/download/newsletter/vortraege/KISA.pdf.

5. МЭДЭЭЛЛИЙН НУУЦЛАЛ ХАМГААЛАЛТ

Энэхүү хэсэг нь дараах зорилготой:
- **Нууцлалын ойлголтод гарсан өөрчлөлтийг тодруулах;**
- **Нууцлалын хамгаалалтын олон улсын хандлагыг тодорхойлох; болон**
- **Нууцлалын нөлөөлөх байдлын үнэлгээний товч ойлголт ба жишээг харуулах.**

5.1 Нууцлалын тухай ойлголт

Хувийн мэдээлэл гэдэг нь тодорхой бус хувь хүн[42] эсвэл тодорхой ба тодорхойлогдох хүнтэй[43] холбоотой аливаа мэдээлэл юм. Үүнд тухайн хүний нэр, утасны дугаар, хаяг, и-мэйл хаяг, машины дугаар, бие махбодын онцлог (нүүрний хэлбэр, гарын хээ, бичгийн хэв), зээлийн картны дуаар болон гэр бүлийн харилцаа зэрэг орно.

Хувийн мэдээлэл рүү зүй бусаар нэвтрэх, цуглуулах, шинжлэх, ашиглах нь тухайн хүнд хандах бусдын хандлагад нөлөөлж эцэст нь түүний нийгмийн байр суурь, өмч хөрөнгө болон аюулгүй байдалд сөрөг нөлөө үзүүлдэг. Тийм учраас хувийн мэдээлэл рүү зүй бусаар нэвтрэх, цуглуулах, хадгалах, шинжлэх болон ашиглахаас хамгаалах хэрэгтэй. Энэ утгаараа хувийн мэдээлэл нь хамгаалалтын субъект болдог.

Хамгаалалтын субъект нь хувийн мэдээлэл өөрөө гэхээсээ илүү хувийн мэдээллийн эрх нь субъект болж байгаа бол энэ нь нууцлалын тухай ойлголт юм. Нууцлалын эрхийг таван аргаар тайлбарладаг:

- Хүсээгүй хандалтаас ангид байх эрх (ж.нь. биет хандалт, богино зурвас илгээх үйлчилгээгээр дамжуулсан хандалт)
- Хувийн мэдээллийг хүсээгүй аргаар ашиглахыг зөвшөөрөхгүй байх эрх (ж.нь. мэдээллийг худалдах, олонд ил болгох)
- Хэн нэгэнд мэдэгдэлгүйгээр, зөвшөөрөлгүйгээр бусад хүмүүс хувийн мэдээлэл цуглуулахыгзөвшөөрөхгүй байх эрх (ж.нь. CCTV болон компьютерийн cookies ашиглах замаар)
- Хувийн мэдээллийг үнэн зөвөөр илэрхийлүүлэх эрх (нэгдмэл байдал)
- Өөрийн мэдээллийн үнэ цэнийн төлөө ашиг олох эрх

Нууцлалын талаарх идэвхигүй ойлголтод оролцохгүй байх эрх болон хүн төрөлхтний нэр төртэй холбоотой угаас заяасан эрх орно. Энэ нь урвуулан ашиглахыг хориглосон хуультай холбогддог.

Нууцлалын талаарх идэвхитэй ойлголтод хувийн мэдээллийн өөрийн хяналт буюу ташаа хувийн мэдээллээс үүдэлтэй нөлөөг засах эрх гэх мэт хувийн мэдээллийг эерэгээр удирдах/хянах эрх орно.

42. Cabinet Office, Privacy and Data-sharing: The way forward for public services (April 2002), http://www.epractice.eu/resource/626.
43. EurLex, “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,” http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg= en&type_doc=Directive&an_doc=1995&nu_doc=46.

5.2 Нууцлалын бодлогын чиг хандлага

Нууцлалын хамгаалалтын тухай ЭЗХАХБ-ын үзэл баримтлал

1980 онд ЭЗХАХБ "Мэдээллийн журмын ЭЗХАХБ" гэж нэрлэгддэг "Нууцлалын хамгаалалт ба Хувийн мэдээллийн хил дамнасан урсгалын тухай журам"-ыг баталсан. 2002 онд "Онлайн нууцлал: Бодлого, журмын тухай ЭЗХАХБ-ын үзэл баримтлал"-ыг зарласан.[44] Энэхүү үзэл баримтлал нь мэдээллийн боловсруулагдсан хэлбэр байдал, мэдээллийн шинж чанар ба доторх агуулгаас шалтгаалан хувь хүний нууц ба эрх чөлөөнд аюул учруулж болох олон нийтийн болон хувийн салбар дахь хувийн мэдээлэлд хамааралтай. Үзэл баримтлалд тодорхойлсон ЭЗХАХБ-ын зарчим нь автоматаар боловсруулагдах хувийн мэдээллийн хүрээн дэх хувь хүний эрх үүрэг болон ийм боловсруулалтанд оролцогчийн эрх үүргийг товч тодорхойлсон. Түүнчлэн Үзэл баримтлалд тусгагдсан үндсэн зарчмуудыг үндэсний болоод олон улсын төвшинд хэрэглэх боломжтой юм.

Нууцлал хамгаалалтын тухай ЭЗХАХБ-ын үзэл баримтлалыг дараах найман зарчим бүрдүүлдэг:

1. **Цуглуулах хязгаарын зарчим**

   Хувийн мэдээллийг цуглуулахад хязгаарлалт байх хэрэгтэй бөгөөд ийм төрлийн мэдээллийг хуулийн дагуу, шударга замаар, боломжтой тохиолдолд тухайн мэдээллийн субъектын зөвшөөрлөөр авах хэрэгтэй.

2. **Мэдээллийн чанарын зарчим**

   Хувийн мэдээлэл нь хэрэглэх зорилго ба тухайн зорилгын хүрээтэй холбоотой байх хэрэгтэй ба үнэн зөв, бүрэн бөгөөд шинэ байх ёстой.

3. **Зорилго тодорхойлох зарчим**

   Хувийн мэдээлэл цуглуулж буй зорилгыг мэдээлэл цуглуулах хугацаанаас хоцролгүй тодорхойлох ёстой бөгөөд дараагийн хэрэглээ нь тэдгээр зорилгын биелэлтээр эсвэл тэдгээр зорилготой нийцэх бусад зорилго болон зорилгын өөрчлөлт бүрт зааснаар хязгаарлагдана.

4. **Ашиглалтыг хязгаарлах зарчим**

   Мэдээллийн субъект өөрөө зөвшөөрсөн болон хуулийн эрх мэдлээс бусад тохиолдолд хувийн мэдээллийг зорилго тодорхойлох зарчимд заасан зорилгоос өөрөөр ашиглах, задруулах болон бусдад нээлтэй болгох ёсгүй.

5. **Аюулгүй байдлыг сахих зарчим**

   Хувийн мэдээллийг зөвшөөрөлгүй нэвтрэх, сүйтгэх, өөрчлөх болон бусдад задруулах зэрэг эрсдлээс тохирох хамгаалалтаар хамгаалах ёстой.

6. **Нээлттэй байдлын зарчим**

   Хувийн мэдээлэлтэй холбоотой хөгжил, журам болон бодлогын талаар нээллтэй байдлын ерөнхий бодлого байх ёстой. Хувийн мэдээллийн оршин байдал, хэв шинж болон тэдгээрийн хэрэглээний гол зорилго түүнчлэн өгөгдөл хянагч этгээдийн мэдээлэл, байнгын байршлыг тогтоох бэлэн аргуудтай байх ёстой.

---

44. OECD, "Privacy Online: OECD Guidance on Policy and Practice," http://www.oecd.org/document /49/0,3343,en_2649_34255_19216241_1_1_1_1,00.html.

7. Хувь хүний оролцооны зарчим

Хувь хүн дараах эрхтэй

a. Мэдээлэлийн операторт өөртэй нь холбоотой мэдээлэл байгаа эсэх талаар баталгааг мэдээллийн операторооос олж авах;
b. Тохирох хугацааны дотор өөртэй нь холбоотой мэдээллийг өөрт шууд ойлгогдох хэлбэрээр зохих төлбөртэйгээр хүлээн авах;
c. (a), (б) хэсгүүдийн дагуу гаргасан хүсэлтэнд татгалзсан шалтгааныг сонсох болон ийнхүү татгалзсаныг эсэргүүцэн гомдол гаргах; болон
d. Өөртэй нь холбоотой гарсан мэдээлэлд гомдол гаргах, гомдол амжилттай болсон тохиолдолд мэдээллийг устгуулах, залруулах, болон өөрчлүүлэх.

5. Хариуцлагын зарчим

Мэдээллийн оператор дээр дурдсан зарчмыг хэрэгжүүлэх арга хэмжээг мөрдөж ажиллах үүрэгтэй.[45]

Нууцлалын хамгаалалттай холбоотой НҮБ-ын үзэл баримтлал

1960-д оны сүүл үеэс хойш, дэлхий ертөнц автомат мэдээлэл боловсруулалтын нууцлалд үзүүлэх нөлөөнд анхаарлаа хандуулж эхэлсэн. Ялангуяа UNESCO 1990 онд Ерөнхий Ассебмлейгаас “Компьютержсэн хувийн мэдээллийг зохицуулах НҮБ-ын журам”-ыг баталснаас хойш нууцлал ба нууцлал хамгаалалтыг сонирхож эхэлсэн. НҮБ-ын журам бичиг баримтуудад болон нийтийн ба хувийн салбарууд дахь компьютержсэн мэдээллийн файлуудад хэрэглэгддэг. Тус журам нь үндэсний хууль тогтоомж эсвэл олон улсын байгууллагуудын дотоод журмуудаар хангаж өгөх наад захын баталгааг хөндсөн хэд хэдэн зарчмыг тогтоосон ба үүнд дараах орно:

1. Хууль ёст байдал ба шударга байдлын зарчим

Аливаа хүний тухай мэдээллийг шударга бус, хуулиас гадуур аргаар цуглуулах, боловсруулах, мөн НҮБ-ын тунхаглалын зорилт, зарчмын эсрэг зорилгоор ашиглах ёсгүй.

2. Үнэн зөв байдлын зарчим

Файлуудыг нэгтгэх эсвэл тэдгээрийг хадгалах үүрэг бүхий хүмүүс нь бичигдсэн мэдээллийн үнэн зөв, уялдаатай байдалд тогтмол шалгалт явуулж байх болон мэдээллийг алдах, орхигдуулахаас зайлсхийхийн тулд тэдгээрийг бүрэн бүтэн хадгалж, тогтмол шинэчилж мөн файл дэх мэдээлэл ашиглагдаж байх явдлыг хангах үүрэгтэй.

3. Зорилгыг тодорхойлох зарчим

Мэдээллийн үйлчлэх зорилго ба тэрхүү зорилгын хүрээн дэх түүний ашиглалт нь нарийн тодорхойлогдсон, хууль ёсных байх хэрэгтэй бөгөөд нэгэнт тодорхойлсон бол олон нийтэд их бага хэмжээгээр таниулах эсвэл хамааралтай хүний анхааралд авчирах хэрэгтэй бөгөөд энэ нь дараах зорилготой:

a. Цуглуулсан, бүртгэгдсэн бүх хувийн мэдээлэл нь тодорхойлсон зорилготойгоо уялдаатай бөгөөд хүрээмжтэй байх;
b. Холбогдох хүн зөвшөөрснөөс бусад тохиолдолд ямар ч хувийн мэдээллийг заасан зорилгоос өөрөө ашиглахгүй байх; болон
c. Хувийн мэдээллийг хадгалах хугацаа нь заасан зорилгын биелэлтийг хангах хугацаанаас хэтрэхгүй байх.

45. To read the entire document where these principles are listed, see the “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

4. Сонирхсон хүн хандах зарчим

Биеийн байцаалтаа үзүүлсэн хэн боловч зүй бус саатал, төрбөргүйгээр өөртэй нь холбоотой мэдээлэл боловсруулагдсан эсэхийг мэдэх, түүнийг ойлгогдох хэлбэрээр олж авах болон хууль бус, хэрэгцээгүй эсвэл үнэн зөв бус зүйл орсон тохиолдолд залруулах, устгуулах, хэрэв цаашид дамжуулагдсан тохиолдолд хаягийн мэдээллийг авах эрхтэй.

5. Ялгаваргүй байх зарчим

6-р зарчимд авч үзсэн хамаарахгүй байх тохиолдолын хувьд, арьс өнгө, гарал үүсэл, бэлгийн чиг хандлага, улс төрийн үзэл бодол, шашин шүтлэг, философийн болон бусад итгэл үнэмшил, түүнчлэн холбоо, үйлдвэрчний эвлэлийн гишүүнчлэлийн талаарх мэдээлэл зэрэг хууль бус ялгаварлалыг нэмэгдүүлж болзошгүй мэдээллийг нэгтгэх, цуглуулах ёсгүй.

6. Хамаарахгүй тохиолдлыг тогтоох эрх мэдэл

1-4-р зарчмуудыг хэрэв тэдгээр нь үндэсний аюулгүй байдал, нийтийн эмх замбараа, эрүүл мэнд ба ёс зүй, түүнчлэн бусдын эрх, чөлөө, ялангуяа мөрдөгдөж буй хүний (хүмүүнлэгийн заалт) эрх чөлөөг хамгаалахад шаардлагатай тохиолдолд тэдгээр зарчмаас гажиж болох бөгөөд, гажилтыг тэдгээрийн хязгаар, тохирох хамгаалалтыг заасан дотоодын хууль зүйн системтэй нийцүүлэн боловсруулсан хууль ба түүнтэй адилтгах тогтоомжуудад тодорхой заасан байх шаардлагатай. Ялгаварлахыг хориглосон 5-р зарчимтай холбоотой хамаарахгүй тохиолдолыг Хүний Эрхийн Олон Улсын Тунхаглал болон хүний эрхийн хамгаалалт ба ялгаварлан гадуурхахаас сэргийлэхтэй хамааралтай бусад холбогдох баримт бичгүүдэд заасан хязгаарын хүрээнд зөвшөөрч болно.

7. Аюулгүй байдлын зарчим

Санамсаргүй алдах, устгах зэрэг байгалийн аюул ба хууль бус хандалт, мэдээллийг луйврын зорилгоор ашиглах, компьютерийн вирусээр халдварлуулах зэрэг хүний аюул заналийн аль алинд тохирох арга хэмжээг авах хэрэгтэй.

8. 8. Хяналт ба шийтгэл

Улс бүрийн хууль өөрийн дотоодын хуулийн системийн дагуу дээр дурдсан зарчмуудын хэрэгжилтийг хянах үүрэг бүхий албан тушаалтныг томилох хэрэгтэй. Энэхүү албан тушаалтан шударга байдал, мэдээлэл боловсруулах, тодруулах болон техникийн чадварыг хариуцсан хүн ба байгууллагуудын хараат бус байдлын баталгааг хангах ёстой. Өмнө дурдсан зарчмуудыг хэрэгжүүлэх үндэсний хуулийн заалтуудыг зөрчсөн тохиолдолд эрүүгийн болон бусад шийтгэлүүдийг оновчтой засах арга хэмжээний хамтаар төлөвлөх ёстой.

9. Хил дамнасан мэдээллийн урсгал

Хоёр ба түүнээс дээш улсын хил дамнасан мэдээллийн урсгалтай холбоотой хууль тогтоомж нь нууцлал хамгаалалтын харьцуулах боломжтой арга хэмжээг санал болгож байгаа тохиолдолд холбогдох орнуудын газар нутаг тус бүрийн хүрээнд мэдээллийг чөлөөтэй солилцох боломжтой байх ёстой. Хэрэв тэнцүү хэмжээний хамгаалалт байхгүй бол, ийм төрлийн солилцоонд хязгаарлалтыг зүй бусаар тавьж болохгүй бөгөөд гагцхүү нууцлалын хамгаалалтын шаардлагын хүрээнд тавина.

10. Ашиглах хүрээ

Энэхүү зарчмуудыг юуны өмнө бүх нийтийн болон хувийн компьютержсэн мэдээлэл болон оновчтой өргөтгөлийн арга замаар мөн өөрчлөлтийн үндсэн дээр гар дээрх мэдээлэлд ашиглаж болохоор болгох хэрэгтэй. Зарчмуудыг бүхэлд нь эсвэл зарим хэсгийг өргөтгөхийн тулд хуулийн этгээд ялангуяа хувь хүний талаар зарим мэдээлэл агуулсан файлуудад Тусгай заалтуудыг оруулж болно.[46]

Европын Холбооны мэдээлэл хамгаалалтын тогтоол

Европын холбооны Сайд нарын зөвлөл Европын холбооны гишүүн орнуудын хилээр хувийн мэдээллийн аюулгүй бөгөөд чөлөөт хөдөлгөөнийг бататгах зохицуулалтын хүрээгээр хангах болон хувийн мэдээллийг хадгалах, дамжуулах ашиглах зэрэг хувийн мэдээллийн эргэн тойрны аюулгүй байдлын үндсийг тогтоох зорилгоор

Хувийн мэдээлэлтэй харьцахтай холбоотой хувь хүний хамгаалалт ба ийм төрлийн мэдээллийн чөлөөт хөдөлгөөний тухай Европын тогтоолыг 1995 оны 10 сарын 24-нд гаргасан. ЕХ-ны мэдээлэл хамгаалалтын тогтоолыг нууцлалын хамгаалалттай холбоотой орон нутгийн хуулиудыг нэгтгэх, тэдгээрийг хооронд нь уялдуулах зорилгоор гаргасан. Европын холбооны тогтоолын 1-р зүйлд “Гишүүн орнууд хүний үндсэн эрх, эрх чөлөөг ялангуяа хувийн мэдээлэлтэй холбоотой тэдний нууцлалын эрхийг хамгаалах ёстой” гэж заасан байдаг.

Европын холбооны тогтоолоор Европын Холбоо, АНУ-ын хооронд зөрчил үүсгэж болох хамгаалалтын төвшин хангалтгүй улсуудад хувийн мэдээлэл дамжуулахыг хориглосон.[47] Европын холбооны гишүүн улс бүр тус тогтоолыг биелүүлэхийн тулд одоогийн хуулиа шинэчлэх эсвэл шинэ нууцлал хамгаалалтын хууль гаргаад байна.

Нууцлал хамгаалалтын тухай Европын холбооны бусад хуулиудад Хүний эрхийн тухай Европын конвенцийн 8-р зүйл, Тогтоол 95/46/EC (Мэдээлэл хамгаалалтын тухай тогтоол), Тогтоол 2002/58/EC (Э-Нууцлалын тогтоол) болон тогтоол 2006/24/EC, 5-р зүйл (Мэдээлэл хадгалах тухай тогтоол) орно.[48]

БНСУ-ын нууцлал хамгаалалт

Бүгд Найрамдах Солонгос улс нь дэлхий дээрх өргөн зурвасын сүлжээ ашиглагчийн ихэнх хувийг эзэлдэг. 2005 оны эхний хагаст, хүн амын 25 хувь, нийт өрхийн 75 хувь нь өргөн зурвасын сүлжээ ашиглаж байв.[49] Өнөөдөр БНСУ-ын утасгүй холбооны сүлжээ болон өргөн зурвасын сүлжээнүүд нь дэлхий дээрх шилдгүүдийн тоонд зүй ёсоор орж байна. Үүнтэй холбоотойгоор тус улсад хувийн мэдээлэл алдагдах тохиолдол ихээхэн газар авсан бөгөөд энэ нь бодлогын болоод технологийн зохицуулалт, шийдлийг шаардаж байна.

Гэхдээ Солонгосын засгийн газар энэ чиглэлд хангалттай хурдан хөдлөхгүй байна. Нууцлал хамгаалалтын хууль Үндэсний Ассемблей дээр гацсан хэвээр байгаа бөгөөд хувийн мэдээллийг хамгаалах бие даасан хууль байхгүй байна.

46. The principles are quoted from the Office of the High Commissioner for Human Rights, “Guidelines for the Regulation of Computerized Personal Data Files,” http://www.unhchr.ch/html/menu3/b/71.htm.
47. Domingo R. Tan, Comment, Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union, 21 LOY. L.A. INT’L & COMP. L.J. 661, 666 (1999).
48. Justice and Home Affairs, “Data Protection” European Commission, http://ec.europa.eu/justice_ home/fsj/privacy/index_en.htm.
49. Internet World Stats, “Korea,” Miniwatts Marketing Group, http://www.internetworldstats. com/asia/kr.htm.

Нөгөө талаар, Солонгосын засгийн газар “u-SafeKorea”-г хэрэгжүүлэх зорилгоор дунд болон урт хугацааны мэдээллийн аюулгүй байдлын чиглэл”-ийг батлан гаргасан бөгөөд 2005 оноос хойшхи тэргүүлэх зэрэглэлийн дөрвөн төсөлд: (1) сүүлийн үеийн дэд бүтцийн аюулгүй байдлыг бататгах; (2) МТ-ийн шинэ үйлчилгээнүүдэд итгэх итгэлийг бий болгох; (3) Өсөлтийн шинэ хөдөлгүүрийн мэдээлэл хамгаалалтын функцыг бэхжүүлэх; болон (4) шинэ кибер орчинд мэдээллийн аюулгүй байдлын үндсийг тавих зэрэг орно. Дөрөв дэх эн тэргүүний зорилтод “Нууцлал хамгаалалтын системийг бэхжүүлэх” гэсэн дэд төсөл орно.

Түүнчлэн, “Төрийн байгууллагууд дахь хувийн мэдээллийг хамгаалах хууль” болон “Телеком сүлжээ ба мэдээллийн хамгаалалтын тухай хууль” зэрэг нууцлал хамгаалалттай холбоотой зарим хуулиуд байдаг.

Төрийн байгууллагууд дахь хувийн мэдээллийг хамгаалах хууль: Энэхүү хууль нь олон нийтийн байгууллагуудын компьютерт буй хувийн мэдээллийг ашиглах, зохицуулах заалтууд болон хүмүүсийн эрх ашгийг хамгаалах заалтуудыг багтаадаг.

Мэдээлэл, холбооны сүлжээний ашиглалт ба мэдээлэл хамгаалалтыг дэмжих тухай хууль: Энэхүү хуулийн зорилго нь хувийн салбарын нууцлал хамгаалах системийг мэдээлэл холбооны сүлжээний өргөжилт болон хувийн мэдээллийг цуглуулах, тараах нь түгээмэл болж байгаатай уялдуулан сайжруулах юм. Тус хууль нь хувийн мэдээллийг цуглуулах, ашиглах, удирдах, устгах зэрэг хувийн мэдээллийн үе шатанд тулгуурлан хувийн мэдээлэл хамгаалалтын үйл явцыг даган мөрддөг. Энэхүү хууль нь мөн хувийн мэдээлэл хэрэглэгчийн эрх, болон нууцлалыг зохицуулах хорооны (privacy mediation committee) байгуулалт ба үйл ажиллагаатай холбоотой заалтуудыг агуулдаг.

Мэдээлэл харилцааны нууцлалыг хамгаалах хууль: Энэхүү хууль нь мэдээлэл харилцааны нууцлал ба эрх чөлөөний зорилтот хүрээ нь мэдээлэл харилцааны нууцлал хамгаалалт болон мэдээлэл харилцааны эрх чөлөөний баталгаажуулалтаар хязгаарлагддаг. Тус хууль нь бичих болон замаас нь чагнах зэргээр нууц ярианд халдахыг хориглодог бөгөөд мэдээлэл харилцааны нууцлалыг хамгаалдаг.

Байршлын мэдээлэл хамгаалах хууль: Энэхүү хууль нь байршилд суурилсан мэдээллийг цуглуулах болон ашиглах ажиллагааг зохицуулахыг эрмэлздэг ба үүнд, ийм төрлийн мэдээллийг задлах, зүй бусаар ашиглахаас сэргийлэх; болон мэдээллийг аюулгүй орчинд ашиглах явдлыг дэмжих ажиллагаанууд ордог. Түүнчлэн хууль нь хүний байршлыг тогтоох (жишээ нь гар утсаар дамжуулан) өнөөгийн харилцаа холбооны технологийн чадвар болон байршлын мэдээллийн алдагдал нь хүний хувийн нууцад ноцтой халдаж, зөрчилд гарахад хүргэж болно гэдгийг хүлээн зөвшөөрдөг. Тиймээс энэхүү хууль нь хуулиар шаардахаас бусад тохиолдолд байршлын мэдээллийг хэзээ ч задлахгүй байхыг журамласан.

АНУ дахь нууцлал хамгаалалт

Засгийн газрын хэт их хязгаарлалтууд цахим худалдааны үйл ажиллагааг боогдуулж байгаа учраас АНУ зах зээлдээ нууцлал хамгаалалтын ажиллагааг анхаарч эхлээд байна. Үүний үр дүнд Траст-е, Беттэр Бизнес Бьюрю Онлайн зэрэг нууцлалын баталгаанууд гарч ирсэн. Хувийн хэвшлийн мэдээллийн нууцлалыг төрөл бүрийн хуулиар хамгаалдаг бол 1974 оны Нууцлалын Хууль нь төрийн хэвшил дэх мэдээллийг нууцлалын хамгаалалтаар хангадаг. Хувийн хэвшлийн нууцлал хамгаалалтын асуудлыг зохицуулдаг байгууллага байдаггүй. Төрийн хэвшилд Удирдлага, Төсвийн Газар (Office of Management and Budget-OMB) нь Нууцлалын хуулийн дагуу холбооны засгийн газрын нууцлалын бодлогыг тогтооход гол үүрэг гүйцэтгэдэг. Хувийн хэвшилд Холбооны Худалдааны Комисс (Federal Trade Commission) нь хүүхдийн онлайн нууцлал, хэрэглэгчийн зээлийн мэдээлэл болон шударга худалдааны ажиллагааг хамгаалах хуулиудыг хэрэгжүүлэх эрхтэй байдаг.

АНУ-ын нууцлал хамгаалалттай холбоотой хуулиудад дараах орно:

- Нууцлалын тухай Хууль (Privacy Act), 1974
- Хэрэглэгчийн зээлийг хамгаалах тухай хууль (Consumer Credit Protection Act), 1984
- Цахилгаан холбооны нууцлалын тухай хууль (Electric Communications Privacy Act), 1986
- Грэм-Лич-Блилийн хууль (Gramm-Leach-Bliley Act), 1999
- Эрүүл мэндийн даатгалын уян хатан, хариуцлагатай байдлын тухай хууль (Health Insurance Portability and Accountability Act), 1996
- Сарбанис-Окслейн хууль (Sarbanes-Oxley Ac)t, 2002
- Хүүхдийн онлайн нууцлал хамгаалалтын тухай хууль (Children"s Online Privacy Protection Act), 1998

Японы нууцлал хамгаалалтын арга хэмжээнүүд

1982 онд ЭЗХАХБ-ын найман үндсэн зарчимд тулгуурлан Япон нууцлал хамгаалалтын арга хэмжээг батлан гаргасан. 1988 онд төрийн хэвшлийн нууцлал хамгаалалтын тухай хуулийг соёрхон баталж хэрэгжүүлж эхэлсэн. Хувийн хэвшлийн тухайд, 1997 онд Нууцлал хамгаалах журмыг Олон улсын худалдаа, үйлдвэрлэлийн яамнаас гаргасан. Нууцлал хамгаалалтын үндэсний хуулиуд ба олон улсын журам, зааврууд хоорондын уялдаа холбоог сайжруулах үүднээс Дэвшилтэт мэдээлэл холбооны нийгмийг дэмжих төв (Advanced Information and Telecommunications Society Promotion Headquarters) нь хувийн мэдээлэл хамгаалах хуулийн хэрэгжилтэнд дэмжлэг үзүүлж байна.

Түүнчлэн Мэдээлэл хамгаалалтын газар (Data Protection Authority)-ыг нууцлал хамгаалалтыг зохих ёсоор дагаж мөрдөх явдлыг хангах болон нууцлалд халдсан тохиолдолд иргэдэд туслах бие даасан агентлагаар баталсан. Мэдээлэл Хамгаалалтын Газар нь мэдээлэл боловсруулалтын ил тод байдлыг дээшлүүлж мэдээллийн субъектын эрх ашгийг хамгаалах болон мэдээлэл боловсруулах агентлаг ба мэдээллийн хэрэглэгчийн аль аль нь өөрсдийн үүргээ биелүүлж байгаа гэдгийг хянан баталгаажуулах эрх бүхий байгууллага юм. Тус Газар нь үндэсний хил дамнуулан мэдээлэл дамжуулсантай холбоотой тохиолдлуудад үндэсний ашиг сонирхлыг хамгаалахад мөн тодорхой үүрэг гүйцэтгэнэ.

Японы нууцлал хамгаалалттай холбоотой хуулиудад дараах орно:

- Төр захиргааны байгууллагын эзэмшдэг компьютерээр боловсруулсан хувийн мэдээллийг хамгаалах тухай хууль (Act for the Protection of Computer Processed Personal Data Held by Administrative Organs), 1988
- Орон нутгийн захиргааны 1529 байгууллагад зориулан 1999 онд баталсан Орон нутгийн захиргааны журам (Regulations of Local Governments enacted in 1999 for 1,529 local governments)
- Хувийн мэдээллийг хамгаалах тухай хууль (Act for the Protection of Personal Information), 2003
- Төр захиргааны байгууллагын эзэмшдэг хувийн мэдээллийг хамгаалах тухай хууль (Act on the Protection of Personal Information Held by Administrative Organs), 2003
- Бие даасан захиргааны байгууллагын хадгалдаг хувийн мэдээллийг хамгаалах тухай хууль (Act for the Protection of Personal Information Retained by Independent Administrative Institutions), 2003
- Аудитын зөвлөлийн тухай хууль (Board of Audit Law), 2003
- RFID тэмдэглэгээтэй холбоотой нууцлал хамгаалалтын удирдамж (Guidelines for Privacy Protection with regard to RFID Tags), 2004

АСУУЛТ

1. Танай оронд мэдээллийн нууцлалыг хамгаалах ямар бодлого, хуулиуд байдаг вэ?

2. Ийм төрлийн бодлого, хуулийг гаргах болон/эсвэл хэрэгжүүлэхэд ямар асуудлууд нөлөөлдөг вэ?

3. Ямар журмууд (ЭЗХАХБ журам болон НҮБ-ын журмуудыг харна уу) танай орны нууцлал хамгаалалттай холбоотой бодлого, хуулиудыг дэмжинэ гэж та бодож байна вэ?

5.3 Нууцлалын нөлөөлөх байдлын үнэлгээ (PIA)

ННБҮ гэж юу вэ?

Нууцлалын нөлөөлөх байдлын үнэлгээ-ННБҮ (Privacy Impact Assessment-PIA) бол шинэ мэдээллийн системийн нэвтрэлт эсвэл одоогийн мэдээллийн системийн өөрчлөлт нь хэрэглэгчийн эсвэл үндэстний нууцлалд хэрхэн нөлөөж буйг судлах, шинжлэх, үнэлэх системтэй үйл явц юм. ННБҮ нь “урьдчилан сэргийлэлтийн зарчим” буюу урьдчилан сэргийлэх нь эмчилгээнээс илүү дээр гэсэн үзэлд суурилдаг. Энэ нь зүгээр нэг системийн үнэлгээ биш, харин шинэ системийг нэвтрүүлэх, өөрчлөхөд нууцлалд нөлөөлөх ноцтой нөлөөг авч үздэг юм. Тиймээс, энэ нь нууцлалын дотоод бодлогын мөрдөлт болон гадаад шаардлагын биелэлтийг хангадаг нууцлал хамгаалалтын хяналтаас өөр юм.

ННБҮ-г шинэ системийг байгуулах үед нууцлалд халдах хүчин зүйлийг судлах зорилгоор хийдэг учраас энэхүү үнэлгээг систем хөгжүүлэх техникийн нөхцөлд өөрчлөлт хийх боломжтой үед буюу хөгжүүлэлтийн эхний шатанд хийх хэрэгтэй. Гэхдээ одоогийн үйлчилгээг ажиллуулах үед хувийн мэдээлэл цуглуулах, ашиглах, зохицуулах ажиллагаанд ноцтой халдлагын эрсдэл тохиолдвол ННБҮ хийж системийг тэр дагуу өөрчлөх нь зүйтэй.

ННБҮ-ний үйл явц[50]

ННБҮ нь ерөнхийдөө гурван хэсгээс бүрдэнэ (Хүснэгт 10).

50. This section is drawn from Information and Privacy Office, Privacy Impact Assessment: A User’s Guide (Ontario: Management Board Secretariat, 2001), http://www.accessandprivacy.gov.on.ca /english/pia/pia1.pdf.

Хүснэгт 10. ННБҮ үйл явц

Ойлголтын дүн шинжилгээ	Мэдээллийн урсгалын дүн шинжилгээ	Бататгах дүн шинжилгээ
Дэвшүүлсэн санаачлагын цар хүрээ болон бизнесийн үндэслэлийн талаар ерөнхий тодорхойлолтыг бэлтгэнэ. Урьдчилсан байдлаар боломжит нууцлалын асуудлууд, эрсдлүүд болон гол оролцогч талуудыг тодорхойлно. Гол асуудлуудын бодлогын дүн шинжилгээ зэрэг төслийн чухал талуудын дэлгэрэнгүй тайбарыг өгнө. Хувийн мэдээллийн гол урсгалуудыг баримтжуулна. Бусад хууль эрзүйд үүнтэй төстэй санаачлагыг хэрхэн зохицуулдагийг нягтлах зорилгоор орчны асуудлын судалгааг эмхтгэнэ. Оролцлогч талуудын асуудлыг тодорхойлох. Олон нийтийн хариу үйлдлийг үнэлэх.	Бизнесийн үйл явцын диаграмаар мэдээллийн урсгалыг шинжилж тодорхой нэг хувийн мэдээллийн элементүүд болон мэдээллийн бүлгийг тодорхойлно. Төслийн мэдээллийн эрх чөлөө -МЭЧ (Freedom of Information FOI), нууцлалын хууль тогтоомж болон холбогдох хөтөлбөрийн тогтоолуудтай хэр нийцэж буйг үнэлнэ. Нууцлалын ерөнхий зарчмуудтай өргөн хүрээнд хэр нийцэж байгааг үнэлнэ. Санаачлагын нууцлалын дүн шинжилгээнд тулгуурлан эрсдлийг шинжилж боломжит шийдлийг тодорхойлно. Дизайны хувилбаруудыг нягталж анхаарлын гадна үлдсэн нууцлалын чухал асуудлуудыг тодорхойлно. Шийдэгдээгүй нууцлалын асуудлуудын хариу арга хэмжээг бэлтгэнэ.	Дэвшүүлсэн санаачлага нь нууцлалын дизайны шаардлагатай нийцэж байгааг бататгаажуулахын тулд биет техник хангамж ба системийн дизайныг хянан шинжилнэ. Дэвшүүлсэн санаачлагын эцсийн хяналтыг хийнэ. МЭЧ, нууцлалын хууль тогтоомж, холбогдох хөтөлбөрийн тогтоолууд, болон нууцлалын ерөнхий зарчмуудтай хэр нийцэж буйг бататгаажуулах зорилгоор дэвшүүлсэн санаачлагад хийсэн техник хангамж ба програм хангамжийн дизайнтай холбоотой аливаа шинэ өөрчлөлтийн нууцлал ба эрсдлийн шинжилгээг явуулна. Харилцаа холбооны төлөвлөгөөг бэлтгэнэ.

Эх сурвалж: Information and Privacy Office, Privacy Impact Assessment: A User"s Guide (Ontario: Management Board Secretariat, 2001), 5, http://www. accessandprivacy.gov.on.ca/english/pia/pia1.pdf.

ННБ-ын үнэлгээний хүрээ

ННБҮ-г дараах тохиолдлуудад хийнэ:

1. Томоохон хэмжээтэй хувийн мэдээллийг агуулж, удирдах шинэ мэдээллийн системийг байгуулахад;
2. Нууцлал зөрчигдөж болох шинэ технологийг ашиглахдаа;
3. Хувийн мэдээллийг агуулж, удирддаг одоогийн мэдээллийн системийг өөрчлөхдөө; болон
4. Нууцлалд халдах эрсдэл тохиолдож болзошгүй үе буюу хувийн мэдээллийг цуглуулах, ашиглах, хадгалах ба/эсвэл устгах үед.

Гэхдээ бүх мэдээллийн системд ННБҮ хийх шаардлагагүй. Одоогийн програм болон системд бага зэргийн өөрчлөлт орсон бол ННБҮ-г хийх шаардлагагүй.

ННБҮ -ний жишээ

Хүснэгт 11-т гурван орны ННБҮ системийг жагсаан харууллаа.

Хүснэгт 11. Үндэсний PIA-ын жишээ

	АНУ	Канад	Австрали/Шинэ Зеланд
Хууль зүйн үндэслэл	2002 оны цахим засаглалын хуулийн 208-р бүлэг OMB нь OMB-M-03-22-тоо ННБҮ шаардлагыг оруулсан байдаг.	2002 оны 5 сард ННБҮ –ний бодлого журмыг нэвтрүүлсэн. Нууцлалын түгээмэл хуулийн үндсэн дээр ННБҮ -г заавал гүйцэтгэнэ.	ННБҮ-г сайн дураар хийнэ (хууль зүйн үндэслэл байхгүй) ННБҮ -г дэмжих ННБҮ гарын авлага (2004, Шинэ Зеланд) ННБҮ -ний журам (2004, Австрали)
Субъект	Бүх гүйцэтгэх салбарын байгууллагууд болон агентлагууд мөн МТ-ийг хэрэглэдэг эсвэл олон нийттэй харилцах зорилгоор веб сайт ажиллуулдаг гэрээлэгчид; Цахим засаглал зэрэг холбогдох агентлаг хоорондын санаачлагууд	Засгийн газрын агентлагуудын явуулдаг бүх хөтөлбөр, үйлчилгээнүүд А	Үүрэг, хязгаар байхгүй
Гүйцэтгэгч	Хувийн мэдээлэлтэй харьцаж буй цахим засаглалын төсөл хэрэгжүүлдэг агентлагууд	Хөтөлбөр, үйлчилгээ боловсруулан ажиллуулж буй засгийн газрын агентлагууд	Холбогдох агентлагууд эсвэл гаднаас зөвлөх агентлагууд авах хүсэлт гаргах замаар
Олон нийтэд дэлгэрүүлэх	Агентлагийн веб сайтаар дамжуулан ННБҮ -г олон нийтэд хүргэх, Холбооны бүртгэлд нийтлэх, эсвэл аюулгүй байдлын шалтгаанаар эсвэл үнэлгээнд агуулагдах нууц, эмзэг болон хувийн мэдээллийг хамгаалах зорилгоор өөрчилж, хүчингүй болгож болох бусад аргууд Агентлагууд санхүүжилт хүссэн систем тус бүрийн PIA-ын хуулбарыг OMB-ын даргад өгнө.	ННБҮ -ний эмхэтгэлийг олон нийтэд ашиглагдахаар болгох Оновчтой хамгаалалтын стратегитай холбоотой тохирох зөвлөгөө, удирдамжийг авахын тулд Нууцлалын бүрэн эрхт төлөөлөгчийн газарт эцсийн ННБҮ ба тайлангийн хуулбарыг өгнө.	ННБҮ-ний дүн ихэнхдээ нийтэд ил байдаггүй (тайлагнах болон олон нийтэд мэдээлэх аливаа үүрэг байхгүй)

ӨӨРИЙГӨӨ ШАЛГАХ НЬ

1. Хувийн мэдээлэл бусад төрлийн мэдээллээс юугаараа ялгаатай вэ?
2. Хувийн мэдээллийг яагаад хамгаалах хэрэгтэй вэ?
3. Нууцлал хамгаалалтын тухай ЭЗХАХБ ба НҮБ-ын зарчмуудын ач холбогдол юу вэ?
4. Нууцлалын нөлөөлөх байдлын үнэлгээг яагаад хийдэг вэ?

6. КОМПЬЮТЕРИЙН АЮУЛГҮЙ БАЙДЛЫН ЗӨРЧИЛД ХАРИУ ӨГӨХ БАГИЙН ҮҮСЭЛ БА ҮЙЛ АЖИЛЛАГАА

Энэхүү бүлэг нь дараах зорилготой:

- **Үндэсний компьютерийн аюулгүй байдлын зөрчилд хариу өгөх баг КАБЗХӨБ (Computer Security Incident Response Team)-ийг хэрхэн байгуулан ажиллуулах талаар тайлбарлах; болон**
- **Өөр бусад улс орнуудын КАБЗХӨБ-ийн загварын талаархи мэдээллээр хангах**

Мэдээллийн аюулгүй байдалд чиглэсэн кибер гэмт хэрэг болон төрөл бүрийн аюул заналын эдийн засагт үзүүлэх нөлөөнөөс шалтгаалан тэдгээрийг ноцтой төвшинд авч үзэх шаардлагатай байна. Жишээлбэл Японы сүлжээний аюулгүй байдлын нийгэмлэг 2006 онд хувийн мэдээллийн урсгалаас учирсан эдийн засгийн хохирол ойролцоогоор 446 сая ам.доллар буюу нэг хүнд 347 м.доллар байна гэж тооцоолсон байна. Феррисын судалгаагаар АНУ дахь спамаас үүдсэн хохирол 2002 онд ойролцоогоор 8,9 тэрбум, 2004 онд 20 тэрбум, 2005 онд 50 тэрбум ам.доллар байсан байна.

КАБЗХӨБ-ийг байгуулах нь мэдээллийн системийн халдлага болон мэдээллийн аюулгүй байдлын зөрчлөөс үүдэн гарах хохирлыг багасгах болон арилгах үр дүнтэй арга юм.

6.1 КАБЗХӨБ-ийн хөгжил ба үйл ажиллагаа

КАБЗХӨБ нь компьютерийн аюулгүй байдлын будлианы тайлан, үйл ажиллагааг хүлээн авах, хянах, хариу өгөх үүрэг бүхий байгууллага юм. КАБЗХӨБ нь хохирлыг багасгах компьютерийн будлианыг зохицуулах үйчилгээгээр хангах ба компьютерийн будлианаас үр дүнтэйгээр гарах боломж олгох зорилготой.[51]

1988 онд Моррис гэх компьютерийн өт анх гарч дэлхий даяар маш хурдацтай тархсан билээ. Үүний дараагаар Батлан Хамгаалах Дээд Судалгааны Төслийн Агентлаг (Defence Advanced Research Projects Agency) програм хангамжийн инженерчлэлийн институтыг байгуулсан бөгөөд дараа нь АНУ-ын Засгийн Газрын гэрээгээр Карниг Меллон Их сургууль дээр КХХҮБ/ЗТ-ыг байгуулсан. Түүнээс хойш Европын улс бүр үүнтэй ижил байгууллагуудыг байгуулаад байна. Өргөн хүрээтэй эмзэг байдлын онцгой тохиолдлыг ганц КАБЗХӨБ дангаар шийдэх боломжгүй учраас 1990 онд Будлианд Хариу Өгөх ба Аюулгүй Байдлын Багуудын Форум-БХӨАБФ (Forum of Incident Response and Security Teams - FIRST) байгуулагдсан. БХӨАБФ-аар дамжуулан мэдээллийн аюулгүй байдлын олон агентлагууд болон КАБЗХӨБ -ууд саналаа солилцож мэдээллээ хамтран ашиглах боломжтой.

Тохирох КАБЗХӨБ загварыг[52] сонгох

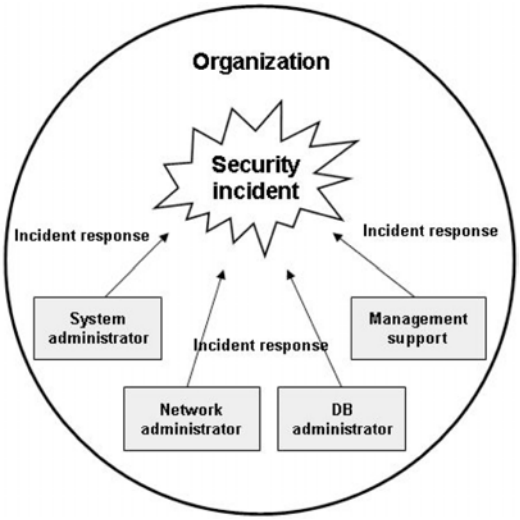
КАБЗХӨБ-ийн зохион байгуулалтын таван ерөнхий загвар байдаг. Орчин, санхүүгийн байдал, хүний нөөц зэрэг төрөл бүрийн нөхцөл байдлыг тооцож үзсэний үндсэн дээр хамгийн тохиромжтойг нь авч ашиглах нь зүйтэй.

1. Аюулгүй байдлын багийн загвар (одоогийн МТ-ийн бүрэлдэхүүнийг ашиглан)
Аюулгүй байдлын багийн загвар нь энгийн КАБЗХӨБ загвар биш юм. Үнэн хэрэгтээ, энэ

51. CERT, “CSIRT FAQ,” Carnegie Mellon University, http://www.cert.org/csirts/csirt_faq.html.
52. This section is drawn from Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek, Organizational Models for Computer Security Incident Response Teams (CSIRTs) (Pittsburgh: Carnegie Mellon University, 2003), http://www.cert.org/archive/pdf/03hb001.pdf.

нь энгийн КАБЗХӨБ-ийнн эсрэг ойлголт юм. Энэхүү загварт, компьютерийн аюулгүй байдлын будлианыг шийдвэрлэх үүрэг бүхий төвийн байгууллага байдаггүй. Харин үүний оронд будлианыг шийдвэрлэх ажлыг систем болон сүлжээний администраторууд эсвэл бусад аюулгүй байдлын системийн мэргэжилтнүүд хэрэгжүүлдэг байна.

Зураг 14. Аюулгүй байдлын багийн загвар



2. Дотоод түгээгдсэн КАБЗХӨБ загвар

Энэхүү загварыг мөн "түгээгдсэн КАБЗХӨБ гэж нэрлэдэг. Энэ загвар дахь баг нь тайлан ба нийт удирдлагыг хариуцсан КАБЗХӨБ администратор ба тухайн хамааралтай байгууллага/агентлагийн бусад хэлтсүүдийн ажилтнуудаас бүрдэнэ. Энэ загварын КАБЗХӨБ нь бүх будлианы хариу өгөх үйл ажиллагааг зохицуулах үүрэг бүхий албан ёсны хүлээн зөвшөөрөгдсөн байгууллага юм. Багийг компани болон агентлаг дотор байгуулдаг учраас тус багийг "дотоодын" гэж үздэг.

Дотоод түгээгдсэн КАБЗХӨБ загвар нь аюулгүй байдлын багийн загвараас дараах байдлаараа ялгарна. Үүнд:

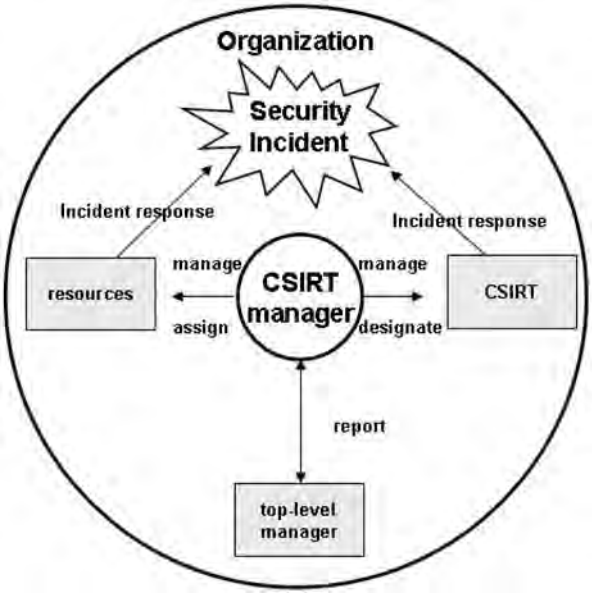
- Илүү албан ёсны болгосон будлианыг шийдвэрлэх бодлого, журам, үйл явцтай;
- Аюулгүй байдлын аюул занал болон хариу өгөх стратегиудтай холбоотой нийт байгууллагатай харилцах харилцааны тогтсон арга; болон
- Будлиан шийдвэрлэх ажлыг хариуцахаар тусгайлан томилогдсон КАБЗХӨБ менежер ба багийн гишүүдтэй.

Зураг 15. Дотоод түгээгдсэн КАБЗХӨБ загвар

3. Дотоод төвлөрсөн КАБЗХӨБ загвар

Дотоод төвлөрсөн КАБЗХӨБ загварын хувьд төвд байршсан баг байгууллагыг хянаж дэмжлэг үзүүлдэг. КАБЗХӨБ нь бүх будлианыг мэдээлэх, шинжлэх болон хариу өгөх үүрэгтэй. Тиймээс багийн гишүүд бусад ажлуудыг гүйцэтгэж чадахгүй, бүх цагаа багийнхаа төлөө ажиллаж будлианыг шийдвэрлэхэд зарцуулдаг. Түүнлчэн КАБЗХӨБ менежер нь мэдээлэл хариуцсан захирал, аюулгүй байдал хариуцсан захирал болон эрсдэл хариуцсан захирал зэрэг дээд төвшний удирдлагуудад тайлагнадаг.

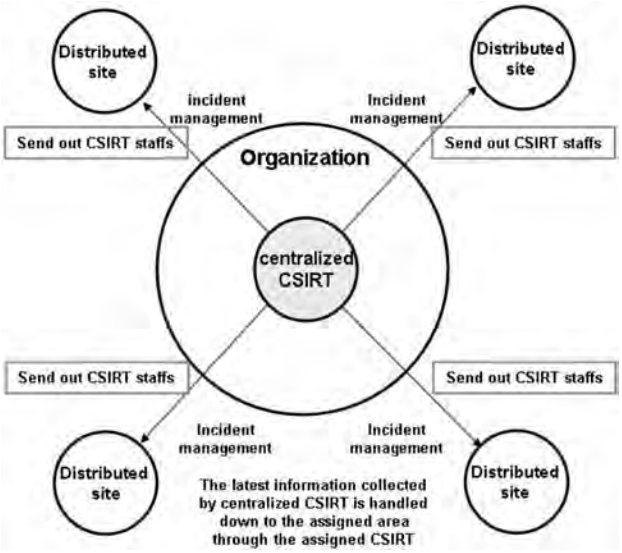
Зураг 16. Дотоод төвлөрсөн КАБЗХӨБ загвар



4. Илгээгдсэн ба төвлөрсөн нэгдмэл КАБЗХӨБ-ийн загвар

Үүнийг мөн “нэгдсэн КАБЗХӨБ” гэж нэрлэдэг. Төвлөрсөн КАБЗХӨБ нь байгууллагыг бүхэлд нь хянаж дэмжлэг үзүүлж чадахгүй үед зарим багийн гишүүдийг байгууллагын хэсэг/хэлтэс/салбар хооронд өөрсдийн үүргийнх нь хүрээнд төвлөрсөн КАБЗХӨБ-ийн үзүүлдэг ижил төвшний үйлчилгээг хүргэх зорилгоор илгээдэг. Төвлөрсөн баг нь тэднийг өндөр төвшний өгөгдлийн дүн шинжилгээ, өгөгдөл сэргээх аргууд болон хохирлыг багасгах стратегиудаар хангадаг. Түүнчлэн энэ нь илгээгдсэн багийн гишүүдэд мэдээллийн аюулгүй байдлын будлиан, эмзэг байдалд хариу өгөх ажиллагаанд нь дэмжлэг үзүүлдэг. Байршил бүр дэх илгээгдсэн багийн гишүүд өөрсдийн тус тусын ажлын хүрээнд стратегиудыг хэрэгжүүлж, дүгнэлт гарган төвлөрсөн баг руу илгээдэг.

Зураг 17. Нэгдсэн КАБЗХӨБ



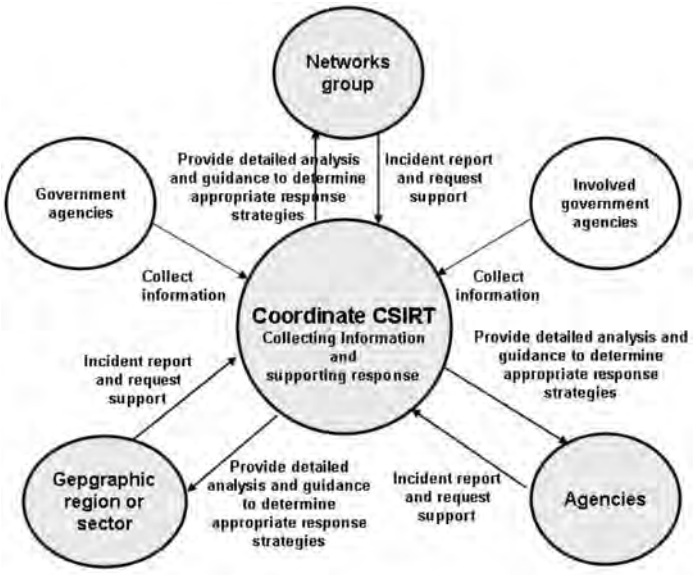
5. Зохицуулах КАБЗХӨБ загвар

Зохицуулах КАБЗХӨБ нь нэгдсэн CSIRT дэх түгээгдсэн багуудын үүргийг бэхжүүлдэг. Зохицуулах КАБЗХӨБ загварт нэгдсэн КАБЗХӨБ дэх багийн гишүүд сүлжээний холболт, газар зүйн хил гэх мэт онцлогуудад үндэслэн бие даасан КАБЗХӨБ-д хуваагдана. Тэдгээрийг төвлөрсөн КАБЗХӨБ нэгтгэдэг.

Зохицуулах КАБЗХӨБ загвар нь үндэсний КАБЗХӨБ системд тохиромжтой. Энэхүү загварыг байгууллага дахь дотоод ажиллагаанд болон гаднын агентлагуудыг дэмжиж нягт нийцүүлэх үүднээс ашиглаж болно.

Зохицуулалтын болон дэмжлэг үзүүлэх үйл ажиллагаануудад мэдээлэл хамтран ашиглах, нөлөөг бууруулах стратегиар хангах, будлианд хариу өгөх, нөхөн сэргээх арга, будлианы хандлага/хэлбэрийн судалгаа/шинжилгээ, эмзэг байдлын өгөгдлийн сан, аюулгүй байдлын багаж хэрэгслийг судлан шинжлэх газар, зөвлөх болон анхааруулах үйлчилгээнүүд орно.

Зураг 18. Зохицуулах КАБЗХӨБ



КАБЗХӨБ-ийг байгуулах: үндэсний КАБЗХӨБ[53] байгуулах үе шатууд

КАБЗХӨБ байгуулах таван үе шат байдаг. КАБЗХӨБ –ийн зорилго, үүрэг нь тэдгээр үе шатаар ахих чиглүүлэгч нь болох ёстой.

1-р шат –Үндэсниы баг хөгжүүлэх талаар оролцогч талуудыг сургах

1-р шат бол ухамсрын шат бөгөөд оролцогч талууд КАБЗХӨБ–ийг байгуулахад юу оролцдог талаар ойлголтоо хөгжүүлнэ. Төрөл бүрийн боловсролын аргаар тэд дараах зүйлсийн талаар суралцана:

a. Үндэсний КАБЗХӨБ–ийн хэрэгцээ шаардлагын ард буй бизнесийг хөтлөгч ба идэвхижүүлэгчид
b. Үндэсний КАБЗХӨБ -ийн будлианд хариу өгөх чадавхийг хөгжүүлэхэд шаардагдах зүйлс
c. Үндэсний баг байгуулах хэлэлцүүлэгт оролцох хүмүүсийг тодорхойлох
d. Тухайн улсын хүрээнд орших гол нөөц ба чухал дэд бүтцүүд
e. КАБЗХӨБ–ийн үйлчлүүлэгчидтэй харилцахын тулд тодорхойлох шаардлагатай харилцааны сувгийн төрлүүд
f. Үндэсний КАБЗХӨБ-ийн хөгжилд нөлөөлөх тодорхой хууль, тогтоомжууд ба бусад бодлогууд
g. Хариу өгөх чадамжийг хөгжүүлэх, төлөвлөх, хэрэгжүүлэх, ажиллуулахад ашиглагдаж болох санхүүжилтийн стратегиуд
h. Үндэсний багийн үйл ажиллагааг дэмжихэд шаардлагатай технологи ба сүлжээний мэдээллийн дэд бүтэц
i. Төрөл бүрийн салбаруудад ашиглагдах учраас үндсэн хариу өгөх төлөвлөгөө
j. Үндэсний КАБЗХӨБ өөрсдийн үйлчлүүлэгчиддээ үзүүлж болох үндсэн үйлчилгээний боломжит багц
k. Тэргүүн туршлагууд ба чиглэлүүд

2-р шат – КАБЗХӨБ-ийг төлөвлөх: 1-р шатанд олж авсан мэдлэг, мэдээлэл дээр тулгуурлана

2-р шат нь 1-р шатанд хуримтлуулсан мэдлэг, мэдээлэлд тулгуурлан КАБЗХӨБ-ийг төлөвлөх ажлыг хамарна. 1-р шатанд хэлэлцсэн асуудлуудыг дахин нягталж, хэлэлцэх бөгөөд дараа нь нарийн зүйлүүдийг тодорхойлж хэрэгжилтийн төлөвлөгөөнд ашиглана. Тус төлөвлөгөөг дараах үйл ажиллагааг тооцож үзсэний үндсэн дээр боловсруулна:

a. Үндэсний КАБЗХӨБ-ийг байгуулах хэрэгцээ шаардлагыг тодорхойлох.
   - Үндэсний багийн үйл ажиллагаанд нөлөөлөх хууль, тогтоомжууд
   - Тодорхойлон хамгаалах шаардлагатай чухал нөөц, баялгууд
   - Одоогоор мэдээлэгдсэн эсвэл мэдээлэгдвэл зохих сүүлийн үеийн будлиан ба хандлагууд
   - Одоогийн будлианд хариу өгөх чадамж ба компьютерийн аюулгүй байдлын магадлагаа
b. Үндэсний КАБЗХӨБ-ийн хэтийн төлвийг тодорхойлох
c. Үндэсний багийн эрхэм зорилгыг тодорхойлох
d. Үйлчилгээ үзүүлэх үйлчлүүлэгчийг (эсвэл үйлчлүүлэгчид) тогтоох
e. Үйлчлүүлэгч ба үндэсний багийн хоорондын харилцааны интерфэйсийг тодорхойлох
f. Үндэсний (засгийн газрын) зөвшөөрөл, удирдлага ба дэмжлэгийн төрлийг тодорхойлох
g. Багийг ажиллуулахад шаардлагатай бие бүрэлдэхүүний ур чадвар, мэдлэгийн төрлүүдийг тогтоох
h. Үндэсний КАБЗХӨБ-ийн үүрэг, хариуцлагыг тодорхойлох

53. This section is drawn from Georgia Killcrece, Steps for Creating National CSIRTs (Pittsburgh: Carnegie Mellon University, 2004), http://www.cert.org/archive/pdf/NationalCSIRTs.pdf.

i. КАБЗХӨБ–ийн будлианыг зохицуулах үйл явцыг нарийвчлан зааж гадны аливаа үйлчлүүлэгч байгууллагын ижил төстэй үйл явцтай ямар холбоотой байгааг тодорхойлох
j. Будлианы үйл ажиллагааг ангилан, тодорхойлох зорилгоор стандартчилагдсан багц шалгуур ба тохирох технологийг хөгжүүлэх
k. Үндэсний КАБЗХӨБ нь үйлчлүүлэгч, мөн дэлхийн бусад КАБЗХӨБ -ууд эсвэл гадны талуудтай хэрхэн харилцан ажиллахыг тодорхойлох

3-р шат – КАБЗХӨБ-ийг хэрэгжүүлэх

3-р шатанд, төслийн баг КАБЗХӨБ-ийг хэрэгжүүлэхдээ 1 ба 2-р шатнаас авсан мэдээллээ ашиглана. Хэрэгжүүлэх үе шат нь дараах дараалаар явагдана:

a. Төлөвлөлтийн шатанд тодорхойлсон сурвалжуудаас санхүүжилт авна
b. Үндэсний КАБЗХӨБ-ийг байгуулаж байгаа тухай болон нэмэлт мэдээллийг (хөгжүүлэлтийн үйл явц ба мэдээлэх шаардлагын тухай) хаанаас авч болох талаар өргөн хүрээтэйгээр зарлана
c. Оролцогч талууд болон бусад тохирох түншийн зохицуулалт болон тэдэнтэй харилцах харилцааны механизмыг албан ёсны болгох
d. Үндэсний КАБЗХӨБ-ийг ажиллуулах аюулгүй мэдээллийн систем ба сүлжээний дэд бүтцийг хэрэгжүүлэх (ж.нь. аюулгүй сервер, аппликэйшн, харилцаа холбооны тоног төхөөрөмж болон бусад дэд бүтцийг дэмжих нөөцүүд)
e. Төлөвлөлтийн шатанд тохиролцсон стандарт болон мэдээлэх удирдамж зэрэг КАБЗХӨБ-ийн бие бүрэлдэхүүний үйл ажиллагаа, явцыг боловсруулах
f. КАБЗХӨБ–ийн тоног төхөөрөмж болон хувийн төхөөрөмжийг авч ашиглах, ажиллуулах дотоод бодлого журам, мөн зохистой хэрэглээний бодлогыг боловсруулах
g. Үндэсний КАБЗХӨБ-ийн үйлчлүүлэгчтэй харилцах харилцааны үйл явцыг хэрэгжүүлэх
h. Бие бүрэлдэхүүнийг тодорхойлж, ажилд авах (эсвэл дахин томилох), КАБЗХӨБ-ийн бүрэлдэхүүнд зориулсан оновчтой сургалт боловсролыг олж авах болон үйлчлүүлэгчийг сургах бусад боломжит өргөн хүрээг хамарсан хүчин чармайлтыг тодорхойлох.

4-р шат – КАБЗХӨБ-ийг ажиллуулах

Үйл ажиллагааны шатанд үндэсний КАБЗХӨБ-ийн үзүүлэх ёстой үндсэн үйлчилгээг тодорхойлж, үйл ажиллагааны хүчин чадал, будлианыг удирдах чадвар зэргийг үнэлнэ. Гарсан үр дүнд тулгуурлан үйл ажиллагааны нарийн зүйлүүдийг тодорхойлон боловсронгуй болгодог. Энэ шатанд дараах үйл ажиллагаа явагдана:

a. Үндэсний КАБЗХӨБ-ийн үзүүлдэг төрөл бүрийн үйлчилгээг идэвхитэй хэрэгжүүлэх
b. Үндэсний КАБЗХӨБ-ийн үйл ажиллагаанны үр өгөөжийг үнэлэх механизмыг боловсруулж хэрэгжүүлэх
c. Үнэлгээний үр дүнгийн дагуу үндэсний КАБЗХӨБ-ийг сайжруулах
d. Үйлчлүүлэгчид хүргэх үйлчилгээг чанаржуулах үүднээс зорилго, үйлчилгээ, бие бүрэлдэхүүнийг оновчтой бөгөөд боломжтой байдлаар өргөтгөх
e. КАБЗХӨБ-ийн бодлого, журмыг үргэлжүүлэн хөгжүүлж бэхжүүлэх

5-р шат – Хамтын ажиллагаа

Үндэсний КАБЗХӨБ нь үр дүнтэй ажиллагаагаар дамжуулан гол оролцогч талуудтай итгэмжит харилцааг хөгжүүлэх боломжтой (4-р шат). Гэхдээ үндэсний КАБЗХӨБ нь хамтрагч байгууллагууд, дотоодын КАБЗХӨБ-ууд, мөн олон улсын КАБЗХӨБ-уудтай урт хугацааны хамтын ажиллагаагаар дамжуулан будлианыг зохицуулах чухал мэдээлэл, туршлагыг солилцож байх шаардлагатай. Энэ шатанд дараах ажиллагаанууд явагдана:

a. Өгөгдөл ба мэдээлэл хамтран ашиглах ажиллагаанд оролцож, хамтрагчид, бусад КАБЗХӨБ-ууд, үйлчлүүлэгчид болон бусад компьютерийн аюулгүй байдлын

мэргэжилтнүүдтэй өгөгдөл, мэдээллийг хамтран ашиглах стандартыг боловсруулахад дэмжлэг үзүүлэх
b. КАБЗХӨБ-уудын бүлгийг дэмжихийн тулд дэлхийн “хяналт ба анхааруулга” функцэд оролцох
c. Довтолгооны чиг хандлага ба хариу өгөх стратегийг хэлэлцэх сургалт, хурал зэргийг зохион байгуулах замаар КАБЗХӨБ-ийн үйл ажиллагааны чанарыг дээшлүүлэх
d. Тэргүүн туршлагын баримт бичиг ба удирдамжийг боловсруулахдаа бүлгийн бусад хүмүүстэй хамтран ажиллах
e. Тасралтгүй дэвших үйл явцын нэг хэсэг болгон будлианыг удирдах үйл явцыг хянаж шинэчлэх.

КАБЗХӨБ-ийн үйлчилгээнүүд[54]

КАБЗХӨБ-уудын үзүүлдэг үйлчилгээнүүдийг реактив үйлчилгээ, проактив үйлчилгээ ба үйлчилгээний чанарын удирдлагын үйлчилгээ гэж ангилж болно.

Реактив үйлчилгээнүүд нь КАБЗХӨБ-ийн үндсэн үйчилгээ юм. Үүнд дараах орно:

1. Сануулга ба анхааруулга – Энэ үйлчилгээнд аюулгүй байдлын эмзэг байдал, халдлагын сануулга, компьютерийн вирус гэх мэт асуудлуудыг шийдвэрлэхэд зориулсан мэдээлэл ба хариу өгөх аргуудаар хангах зэрэг орно.

2. Будлиан шийдвэрлэх – Үүнд хүсэлт ба мэдээллийг хүлээн авах, нөөц хуваарилах болон хариу өгөх, будлиан, халдлагыг шинжилж эрэмбэлэх ажил багтдаг.
Тодорхой хариу өгөх үйл ажиллагаанд дараах орно:

   - Будлианы дүн шинжилгээ –Будлиан, халдлагатай холбоотой боломжит мэдээлэл, туслах нотолгоо баримтуудыг шалгах. Энэхүү дүн шинжилгээ нь будлианы хүрээ, түүний учруулсан хохирлын хэмжээ, будлианы шинж чанар болон хариу өгөх боломжит стратегиуд ба шийдвэрлэх арга замыг тодорхойлох зорилготой.
   - Шүүхийн нотолгоо цуглуулах –Систем гарсан өөрчлөлтийг тодорхойлж, хууль бусаар нэвтрэхэд хүргэсэн ажлуудыг дахин сэргээхэд туслах зорилгоор довтолгоонд өртсөн компьютерийн системээс нотолгоо цуглуулах, хадгалах, баримтжуулах ба шинжлэх ажил.
   - Мөрдөх ба илрүүлэх –Халдагч этгээд систем ба холбогдох сүлжээ рүү хэрхэн нэвтэрсэнийг мөрдөж илрүүлэх ажил багтана.

3. Газар дээр нь будлианд хариу өгөх – КАБЗХӨБ нь үйлчлүүлэгчид будлианаас гарахад нь туслах зорилгоор шууд, газар дээр нь тусламж үзүүлдэг.

4. Будлианд хариу өгөх дэмжлэг – КАБЗХӨБ нь халдлагын хохирогчдод утас, и-мэйл, факс эсвэл бичиг баримтаар дамжуулан будлианаас сэргэн гарахад нь туслаж чиглүүлдэг.

5. Будлианд хариу өгөх зохицуулалт- Будлианд оролцсон талуудын хариу өгөх хүчин чармайлтыг зохицуулна. Үүнд ихэнхдээ халдлагын хохирогч, халдлагад оролцсон бусад газрууд болон халдлагын шинжилгээнд тусламж шаардлагатай аливаа газар багтана. Түүнчлэн ISP-ууд болон бусад КАБЗХӨБ-ууд гээд хохирогчид, МТ-ийн дэмжлэг үзүүлж буй талууд үүнд багтаж болно.

6. Эмзэг байдлыг шийдвэрлэх- Үүнд техник хангамж, програм хангамжийн эмзэг байдлын талаар мэдээ, мэдээлэл хүлээн авах, эмзэг байдлын нөлөөг шинжлэх болон эмзэг байдлыг илрүүлэн засах хариу өгөх стратегийг боловсруулах ажил багтана.

   - Эмзэг байдлын шинжилгээ - Техник хангамж, програм хангамж дахь эмзэг байдлын техникийн шинжилгээ шалгалтыг хэлнэ. Шинжилгээнд эмзэг байдал хаана тохиолдсоныг тогтоох зорилгоор тохируулгын програм буюу дибагер

54. This section is drawn from Carnegie Mellon University, CSIRT Services (2002), http://www.cert.org/archive/pdf/CSIRT-serviceslist.pdf.

(debugger) ашиглах эсвэл туршилтын систем дээр учирсан асуудлыг хуулбарлан үүсгэх оролдлого хийх зэрэг ажил багтана.

- Эмзэг байдлын хариу- Эмзэг байдлыг багасгах, засах оновчтой хариу арга хэмжээг тодорхойлох зэрэг орно. Энэ үйлчилгээнд засварлах код суулгах зэргээр хариу арга хэмжээ хэрэгжүүлэх ажил орж болно.

- Эмзэг байдлын хариу арга хэмжээний зохицуулалт – КАБЗХӨБ нь байгууллага ба үйлчлүүлэгчийн өөр өөр хэсгүүдэд эмзэг байдлын талаар мэдээллийг хүргэж түүнийг хэрхэн багасгаж, засах талаар мэдээллийг хуваалцдаг. КАБЗХӨБ нь мөн амжилттай болсон эмзэг байдлан хариу өгөх стратегиудыг ангилан ялгадаг. Энэхүү үйл ажиллагаанд эмзэг байдал эсвэл эмзэг байдлын тайлан мэдээнд дүн шинжилгээ хийх, өөр өөр талуудын хийсэн техникийн дүн шинжилгээг нэгтгэх зэрэг орно. Энэ үйлчилгээ нь нийтийн эсвэл хувийн архив, болон эмзэг байдлын мэдээлэл, холбогдох хариу өгөх стратегийн мэдлэгийн санг баяжуулах ажиллагааг багтааж болно.

7. Гажуудал (artifact) удирдан зохицуулах – Үүнд компьютерийн вирус, троян морь програмууд, өт, довтолгооны скрипт болон багажуудийг агуулсан гажуудлыг шинжлэх, хариу өгөх, зохицуулах, удирдах зэрэг багтана.

    - Гажуудлын дүн шинжилгээ- КАБЗХӨБ нь системд илэрсэн бүх төрлийн гажуудалд техникийн шалгалт, шинжилгээг хийдэг.

    - Гажуудалд хариу өгөх –Биетийг системээс илрүүлэн устгах оновчтой үйлдлийг тодорхойлох ажил багтана.

    - Гажуудалд өгөх хариуг зохицуулах – Гажуудалтай холбоотой дүн шинжилгээний үр дүн ба хариу өгөх стратегийг бусад судлаачид, КАБЗХӨБ-ууд, борлуулагчид болон аюулгүй байдлын мэргэжилтнүүдтэй хуваалцах, тэдгээрийг нэгтгэх ажил багтана.

Проактив үйлчилгээ нь аливаа будлиан, учрал тохиолдох эсвэл илрэхээс өмнө үйлчлүүлэгчийн дэд бүтэц ба аюулгүй байдлын үйл явцыг дээшлүүлэх зорилготой. Үүнд дараах ажиллагаа орно:

1. Зарлал – Довтолгооны дохиолол, эмзэг байдлын анхааруулга, аюулгүй байдлын мэдээлэл гэх зэрэг орно. Иймэрхүү зарлалууд үйлчлүүлэгчид шинээр илрүүлсэн эмзэг байдал болон довтолгооны хэрэгсэл гэх мэт дунд болон урт-хугацааны нөлөөтэй шинэ зүйлсийн талаар мэдээлдэг. Зарлал нь үйлчлүүлэгчид дөнгөж илэрсэн асуудлуудыг тохиолдохоос өмнө, тэдгээрийн эсрэг өөрсдийн систем, сүлжээг хамгаалах боломж олгодог.

2. Технологийн хяналт – Үүнд ирээдүйн аюул заналыг тодорхойлоход туслах зорилгоор шинэ техникийн хөгжил, довтолгооны үйл ажиллагаа ба холбогдох хандлагыг хянах, ажиглах үйл явц ордог. Энэхүү үйлчилгээний үр дүн нь дунд ба урт хугацааны аюулгүй байдлын асуудлуудад илүү анхаарсан зарим төрлийн удирдамж, зөвлөмж байж болно.

3. Аюулгүй байдлын аудит ба үнэлгээ – Энэхүү үйлчилгээ нь байгууллага эсвэл салбарын бусад стандартуудын тодорхойлсон шаардлагад тулгуурлан байгууллагын аюулгүй байдлын дэд бүтцийн нарийвчилсан шалгалт, дүн шинжилгээг хийдэг.

4. Аюулгүй байдлын багаж хэрэгсэл, програм, дэд бүтэц ба үйлчилгээний тохиргоо, арчлан хамгаалалт – Энэ үйлчилгээ нь багаж хэрэгсэл, програм болон ерөнхий дэд бүтцийг хэрхэн найдвартай тохируулж, үйлчилгээ хийх тухай удирдамжаар хангана.

5. Аюулгүй байдлын багаж хэрэгслийн хөгжил – Энэхүү үйлчилгээ нь аюулгүй байдлын зорилгоор хөгжүүлэн түгээдэг шинэ, үйлчлүүлэгчид тусгайлан зориулсан хэрэгсэл, програм хангамж, plug-in зэргийг хөгжүүлэх ажил багтана.

6. Халдлага илрүүлэх үйлчилгээ – Энэ үйлчилгээг үзүүлдэг КАБЗХӨБ-ууд нь одоогийн ДИС бүртгэлийг нягталж, тэднийг шинжлэн тэдний тогтоосон босгод нийцэх үйл явдлын хариу арга хэмжээг санаачлан эхлүүлдэг.

7. Аюулгүй байдалтай холбоотой мэдээллийг түгээх – Энэ үйлчилгээ нь үйлчлүүлэгчид аюулгүй байдлаа дээшлүүлэхэд нь туслах иж бүрэн, олоход хялбар чухал мэдээллийн цуглуулгаар хангадаг.

Аюулгүй байдлын чанарын удирдлагын үйлчилгээ нь будлиан, эмзэг байдал болон халдлагуудад нэгдсэн байдлаар хариу өгөх замаар олж авсан мэдлэгээр хангах зориулалттай юм. Ийм төрлийн үйлчилгээнд дараах зүйлс агуулагдана:

1. Эрсдлийн дүн шинжилгээ – Үүнд бодит аюул заналыг үнэлэх, мэдээллийн хөрөнгөд учрах эрсдлийн чанарын болон тоон бодит үнэлгээ ба хамгаалалт, хариу өгөх стратегийг үнэлэх КАБЗХӨБ -ийн чадварыг сайжруулах зэрэг орно.

2. Бизнесийн тасралтгүй байдал ба гамшгийг нөхөн сэргээх төлөвлөлт – Бизнесийн тасралтгүй байдал, компьютерийн аюулгүй байдлын довтолгооноос үүдсэн гамшгийн сэргээлтийг оновчтой төлөвлөлтөөр хангадаг.

3. Аюулгүй байдлын зөвлөгөө – КАБЗХӨБ-ууд нь бизнесийн үйл ажиллагааны практик зөвлөгөө, удирдамжаар хангах боломжтой.

4. Ухамсарыг бий болгох – КАБЗХӨБ-ууд нь үйлчлүүлэгчдийн шаарддаг аюулгүй байдлын ажиллагаа, бодлогуудын талаар мэдээлэл, удирдамжийг тодорхойлон, хангах замаар аюулгүй байдлын талаарх ухамсрыг сайжруулах чадвартай байдаг.

5. Боловсрол/сургалт- Энэхүү үйлчилгээнд будлиан мэдээлэх удирдамж, тохирох хариу өгөх арга замууд, будлианд хариу өгөх хэрэгслүүд, будлианаас сэргийлэх аргууд болон компьютерийн аюулгүй байдлын будлианаас хамгаалах, түүнийг илрүүлэх, мэдээлэх, хариу өгөхөд шаардагдах бусад мэдээлэл зэрэг сэдвээр сургалт явуулах үйл ажиллагаа багтана. Сургалт нь семинар, сургалт, практик хичээл хэлбэрээр байж болно.

6. Бүтээгдэхүүний үнэлгээ, гэрчилгээжүүлэлт –Бүтээгдэхүүнүүдийн аюулгүй байдал болон тэдгээр нь КАБЗХӨБ эсвэл бусад байгууллагын аюулгүй байдлын үйл ажиллагаатай нийцэж байгааг баталгаажуулах зорилгоор КАБЗХӨБ нь багаж хэрэгсэл, програм болон бусад үйлчилгээнд үнэлгээ хийж болно.

Хүснэгт 12-т КАБЗХӨБ үйлчилгээ тус бүрийн төвшнийг харууллаа — ж.нь. энэ нь үндсэн, нэмэлт эсвэл онцгой үйлчилгээ эсэхийг КАБЗХӨБ загвар тус бүрт харууллаа.

Хүснэгт 12. КАБЗХӨБ-ийн үйлчилгээнүүд

Үйлчилгээний ангилал	Үйлчилгээ		МАБ-ын баг	Илгээгдсэн	Төвлөрсөн	Нэгдсэн	Зохицуулах
Хариу үзүүлэх (Реактив)	Дохиолол, анхааруулга		Нэмэлт	Үндсэн	Үндсэн	Үндсэн	Үндсэн
	Будлиан шийдвэрлэх	Будлиан шинжлэх	Үндсэн	Үндсэн	Үндсэн	Үндсэн	Үндсэн
		Будлианд газар дээр нь хариу өгөх	Үндсэн	Нэмэлт	Нэмэлт	Нэмэлт	Онцгой
		Будлианд хариу өгөх дэмжлэг	Онцгой	Үндсэн	Үндсэн	Үндсэн	Үндсэн
		Будлианд хариу өгөх зохицуулалт	Үндсэн	Үндсэн	Үндсэн	Үндсэн	Үндсэн
	Гажуудлыг удирдан зохицуулах	Эмзэг байдлын дүн шинжилгээ	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт
		Эмзэг байдлын хариуг зохицуулах	Үндсэн	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт
		Эмзэг байдлын хариу	Нэмэлт	Үндсэн	Үндсэн	Үндсэн	Үндсэн
		Гажуудлын дүн шинжилгээ	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт
		Гажуудалд хариу өгөх	Үндсэн	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт
		Гажуудалд хариу өгөхийг зохицуулах	Нэмэлт	Нэмэлт	Үндсэн	Үндсэн	Үндсэн
Урьдчилан сэргийлэх (Проактив)	Зарлал		Онцгой	Үндсэн	Үндсэн	Үндсэн	Үндсэн
	Технологийн хяналт		Онцгой	Нэмэлт	Үндсэн	Үндсэн	Үндсэн
	Аюулгүй байдлын аудит эсвэл үнэлгээ		Онцгой	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт
	Аюулгүй байдлын багаж хэрэгсэл, аппликэйшн, дэд бүтэц ба үйлчилгээний тохиргоо ба арчлан хамгаалалт		Үндсэн	Нэмэлт	Нэмэлт	Нэмэлт	Онцгой
	Аюулгүй байдлын багаж хэрэгслийн хөгжүүлэлт		Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт
	Халдлага илрүүлэх үйлчилгээ		Үндсэн	Нэмэлт	Нэмэлт	Нэмэлт	Онцгой
	Аюулгүй байдалтай холбоотой мэдээлэл түгээх		Онцгой	Нэмэлт	Үндсэн	Үндсэн	Үндсэн
Аюулгүй байдлын чанарын удирдлага	Эрсдлийн дүн шинжилгээ		Онцгой	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт
	Бизнесийн тасралтгүй байдал ба гамшгаас нөхөн сэргэх төлөвлөлт		Онцгой	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт
	Аюулгүй байдлын зөвлөгөө		Онцгой	Нэмэлт	Нэмэлт	Нэмэлт	Нэмэлт
	Ухамсар бий болгох		Онцгой	Нэмэлт	Нэмэлт	Нэмэлт	Үндсэн
	Боловсрол/сургалт		Онцгой	Нэмэлт	Нэмэлт	Нэмэлт	Үндсэн
	Бүтээгдэхүүний үнэлгээ эсвэл гэрчилгээжүүлэлт		Онцгой	Нэмэлт	Нэмэлт	Нэмэлт	Онцгой

Эх сурвалж: Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek, Organizational Models for Computer Security Incident Response Teams (CSIRTs) (Pittsburgh: Carnegie Mellon University, 2003), http://www.cert.org /archive/pdf/03hb001.pdf.

6.2 Олон улсын КАБЗХӨБ-ууд

Одоогоор, дэлхий даяар компьютерийн аюулгүй байдлын будлианд хариу өгөхөөр байгуулагдсан хэд хэдэн олон улсын мэргэжлийн КАБЗХӨБ-ууд байдаг. Үндэсний КАБЗХӨБ-ууд халдлагуудад хариу өгч, өөрсдийн үүргээ гүйцэтгэж чадах ч олон улсын хэмжээний довтолгоонд олон улсын КАБЗХӨБ анхаарлаа хандуулах шаардлагатай болдог.

Будлианд хариу өгөх аюулгүй байдлын багуудын форум- БХӨАБФ[55]

БХӨАБФ нь 41 орны КХХҮБ-ууд, засгийн газрын агентлагууд болон аюулгүй байдлын компаниудаас бүрдэнэ. Энэ байгууллагын гишүүнчлэлд Компьютерийн халдлагын эсрэг багуудыг зохицуулах төв -КХХҮБ/ЗТ (Computer Emergency Response Team Coordination Center CERT/CC) болон АНУ-КХХҮБ зэрэг 191 байгууллага багтдаг. БХӨАБФ бол будлианд хариу өгөх баг хоорондын мэдээлэл хуваалцах ба хамтран ажиллах ажиллагааны агентлаг юм. Энэ нь будлианд хариу өгөх, хамгаалах ажиллагааг идэвхижүүлэх, гишүүдээ будлианд хариу өгөх технологи, мэдлэг, багаж хэрэгслээр хангах замаар тэдний хоорондын хамтын ажиллагааг дэмжих зорилготой. БХӨАБФ нь дараах үйл ажиллагааг явуулна. Үүнд:

- Будлианд хариу өгөх, хамгаалах шилдэг туршлага, журам, багаж хэрэгсэл, техникийн мэдээлэл болон бусад аргачлалыг хөгжүүлж, хуваалцах;
- Чанартай бодлого, үйлчилгээ, болон аюулгүй байдлын бүтээгдэхүүний хөгжүүлэлтийг дэмжих;
- Оновчтой компьютерийн аюулгүй байдлын удирдамжийг дэмжиж хөгжүүлэх;
- Засгийн газар, аж ахуйн нэгж, боловсролын байгууллагуудад будлианд хариу өгөх багийг байгуулж өргөжүүлэхэд нь туслах; болон
- Аюулгүй цахим орчны төлөө гишүүд хоорондоо технологи, туршлага, мэдлэгээ хуваалцах боломжийг олгох зэрэг орно.

Ази Номхон Далайн КХХҮБ[56]

Ази Номхон Далайн компьютерийн халдлагын эсрэг баг- АНДКХХҮБ (Asia-Pacific Computer Emergency Response Team-APCERT) нь Ази Номхон Далайн бүсэд аюулгүй байдлын мэргэжилтнүүдийн сүлжээний үүрэг гүйцэтгэн будлианд хариу өгөх ажиллагааг бэхжүүлж аюулгүй байдлын ойлголтыг сайжруулах зорилгоор 2003 оны 2 сард байгуулагдсан. Ази Номхон Далайн КХХҮБ-ийн анхны хурал 2002 онд Японд зохион байгуулагдсан. АНДКХХҮБ-ийг Тайпэйд болсон Номхон Далайн 14 КХХҮБ-уудын оролцсон хурлаас хойш нэг жилийн дараа байгуулагдсан. 2007 оны 8 сарын байдлаар АНДКХХҮБ нь 14 жинхэнэ, 6 туслах гишүүнтэй.
АНДКХХҮБ-ийн гишүүд өнөөгийн компьютерийн будлианы тоо хэт ихэсч аливаа байгууллага, улс орон хянахад хэцүү болж байгаа бөгөөд АНДКХХҮБ–ийн гишүүдийн хамтын ажиллагаагаар илүү үр дүнтэй хариу арга хэмжээг авах боломжтой гэдэг дээр санал нэгдэж байна.

БХӨАБФ-ын хувьд мэдээлэл солилцох, нэг нэгэнтэйгээ хамтран ажиллах гишүүд хоорондын харилцан итгэлцэл нь АНДКХХҮБ дэх хамгийн чухал ойлголт юм. Тиймээс АНДКХХҮБ-ийн үйл ажиллагаанууд нь:

- Ази Номхон Далайн бүсийн болоод олон улсын хамтын ажиллагааг бэхжүүлэх;
- Томоохон хэмжээний эсвэл бүсийн хэмжээний сүлжээний аюулгүй байдлын будлианууудыг зохицуулах арга хэмжээг хамтран боловсруулах;
- Компьютерийн вирус, довтолгооны скриптын талаарх мэдээлэл зэрэг аюулгүй байдлын мэдээллийг хамтран ашиглаж, технологи солилцох ажлыг сайжруулах;
- Түгээмэл бэрхшээлүүдийн хамтарсан судалгааг боловсронгуй болгох;

55. FIRST, “About FIRST,” FIRST.org, Inc., http://www.first.org/about/.
56. APCERT, “Background,” http://www.apcert.org/about/background/index.html

- Бүс нутаг дахь бусад КХХҮБ -уудад компьютерийн аюулгүй байдлын будлианд үр дүнтэйгээр хариу өгөхөд нь туслах; болон
- Бүс нутгийн мэдээллийн аюулгүй байдал ба будлианд хариу өгөхтэй холбоотой хууль зүйн асуудлуудад зөвлөгөө өгөх зорилготой.

Европын засгийн газрын КХХҮБ[57]

Европын засгийн газрын халдлагын эсрэг баг-ЕЗГК (European Government CERT) нь Европын улсуудын КХХҮБ-уудтай холбоотой албан бус хороо юм. Гишүүдэд нь Финланд, Франц, Герман, Унгар, Нидерланд, Норвег, Швед, Швейцарь, Англи улсууд багтдаг. Энэ нь дараах үүрэг, хариуцлагатай:

- Томоохон хэмжээний эсвэл бүсийн хэмжээний сүлжээний аюулгүй байдлын будлианууд зохицуулах арга хэмжээг хамтран боловсруулах;
- Аюулгүй байдлын будлиан, хортой кодын аюул ба эмзэг байдалтай холбоотой мэдээлэл хуваалцах, технологи солилцох ажлыг дэмжих;
- Бүлгийн хүрээнд хамтран ашиглаж болох мэдлэг, туршлагын хүрээг тодорхойлох;
- Гишүүдийн сонирхлыг татаж буй сэдвүүдээр хийх хамтарсан судалгаа хөгжлийн чиглэлийг тодорхойлох; болон
- Европын орнуудад засгийн газрын КАБЗХӨБ байгуулах ажлыг дэмжих.

Европын сүлжээ, мэдээллийн аюулгүй байдлын агентлаг- ЕМСАБА[58]

ЕМСАБА-ийн зорилго нь СМАБ-ын соёлыг бий болгох замаар Европын холбооны сүлжээний аюулгүй байдал, ба мэдээллийн аюулгүй байдлыг бэхжүүлэх юм. Тус байгууллагыг Сайд нарын Зөвлөл болон Европын парламент “хай-тех” гэмт хэрэгт хариу өгөх зорилгоор 2004 оны 1 сард байгуулсан. Энэ нь:

- ЕМСАБА–ийн гишүүд болон Европын холбооны орнуудын СМАБ-ыг бэхжүүлэхэд дэмжлэг үзүүлэх;
- Оролцогч талуудын дунд тогтвортой мэдээллийн солилцоог дэмжих; болон
- СМАБ-тай холбоотой үүргийн зохицуулалтыг сайжруулах үүрэгтэй.

ЕМСАБА-ийг вирус, хуурамч нэвтрэлтийг багасгаж аюул заналын онлайн хяналтыг тогтоох олон улсын хүчин чармайлтад хувь нэмрээ оруулна гэж найдаж байна.

6.3 Үндэсний КАБЗХӨБ-ууд

Нилээд хэдэн улс үндэсний КАБЗХӨБ-ийг байгуулаад байна. Хүснэгт 13-т тэдгээр улсуудын КАБЗХӨБ -уудыг вебсайтын хамт жагсаалаа.

57. EGC, http://www.egc-group.org.
58. ENISA, “About ENISA,” http://www.enisa.europa.eu/pages/About_ENISA.htm.

Хүснэгт 13. Үндэсний КАБЗХӨБ-уудын жагсаалт

Улс	Албан ёсны нэр	Веб сайт
Аргентин	Computer Emergency Response Team of the Argentine Public Administration	http://www.arcert.gov.ar
Австрали	Australia Computer Emergency Response Team	http://www.aucert.org.au
Бразил	Computer Emergency Response Team Brazil	http://www.cert.br
Бруней Дарусалам	Brunei Computer Emergency Response Team	http://www.brucert.org.bu
Канад	Public Safety Emergency Preparedness Canada	http://www.psepc-sppcc.gc.ca/prg/em/ccirc/index-en.asp
Чили	Chilean Computer Emergency Response Team	http://www.clcert.cl
Хятад	National Computer Network Emergency Response Technical Ream - Coordination Center of China	http://www.cert.org.cn
Дани	Danish Computer Emergency Response Team	http://www.cert.dk
Эл-Сальвадор	Response Team for Computer Security Incidents	
Финланд	Finnish Communication Regulatory Authority	http://www.cert.fi
Франц	CERT-Administration	http://www.certa.ssi.gouv.fr
Герман	CERT-Bund	http://www.bsi.bund.de/certbund
Хонг Конг	Hong Kong Computer Response Coordination Centre	http://www.hkcert.org
Унгар	CERT-Hungary	http://www.cert-hungary.hu
Энэтхэг	CERT-In	http://www.cert-in.org.in
Индонез	Indonesia Computer Emergency Response Team	http://www.cert.or.id
Япон	JP CERT Coordination Center	http://www.jpcert.or.jp
Литва	LITNET CERT	http://cert.litnet.lt
Малайз	Malaysian Computer Emergency Response Team	http://www.mycert.org.my
Мексик	Universidad Nacional Autonoma de Mexico	http://www.cert.org.mx
Нидерланд	GOVCERT.NL	http://www.govcert.nl
Шинэ Зеланд	Centre for Critical Infrastructure Protection	http://www.ccip.govt.nz
Норвег	Norwegian National Security Authority	http://www.cert.no
Филиппин	Philippines Computer Emergency Response Team	http://www.phcert.org
Польш	Computer Emergency Response Team Polska	http://www.cert.pl

Улс	Албан ёсны нэр	Веб сайт
Катар	Qatar Computer Emergency Response Team	http://www.qcert.org
Саудын Араб	Computer Emergency Response Team - Saudi Arabia	http://www.cert.gov.sa
Сингапур	Singapore Computer Emergency Response Team	http://www.singcert.org.sg
Словени	Slovenia Computer Emergency Response Team	http://www.arnes.si/english/si-cert
Солонгос	CERT Coordination Center Korea	http://www.krcert.or.kr
Испани	IRIS-CERT	http://www.rediris.es/cert
Швед	Swedish IT Incident Centre	http://www.sitic.se
Тайланд	Thai Computer Emergency Response Team	http://www.thaicert.nectec.or.th
Тунис	Computer Emergency Response Team - Tunisian Coordination Center	http://www.ansi.tn/en/about_cert-tcc.htm
Турк	TP-CERT	http://www.uekae.tubitak.gov.tr
Англи	GovCertUK	http://www.govcertuk.gov.uk
АНУ	United States -Computer Emergency Response Team	http://www.us-cert.gov
Вьетнам	Viet Nam Computer Emergency Response Team	http://www.vncert.gov.vn

Эх сурвалж: CERT, “National Computer Security Incident Response Teams,” Carnegie Mellon University, http://www.cert.org/csirts/national/contact.html.

ДАСГАЛ

Танай улсад үндэсний КХЭБ байдаг уу?

1. Хэрэв байдаг бол бүтэцлэгдсэн загварын талаас нь болон ажиллагааны талаас нь тодорхойлно уу.

2. Хэрэв байхгүй бол танай оронд аль КХЭБ загвар тохиромжтой байхыг тодорхойлж танай оронд үндэсний КХЭБ байгуулахад юу шаардлагатай талаар тайлбарлана уу.

ӨӨРИЙГӨӨ ШАЛГАХ НЬ

1. КХЭБ-уудын үндсэн үүрэг нь юу вэ?

2. Олон улсын КХЭБ -ууд үндэсний КХЭБ -уудаас юугаараа ялгаатай вэ?

3. КХЭБ байгуулах ямар шаардлагууд байдаг вэ?

7. МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БОДЛОГЫН МӨЧЛӨГ

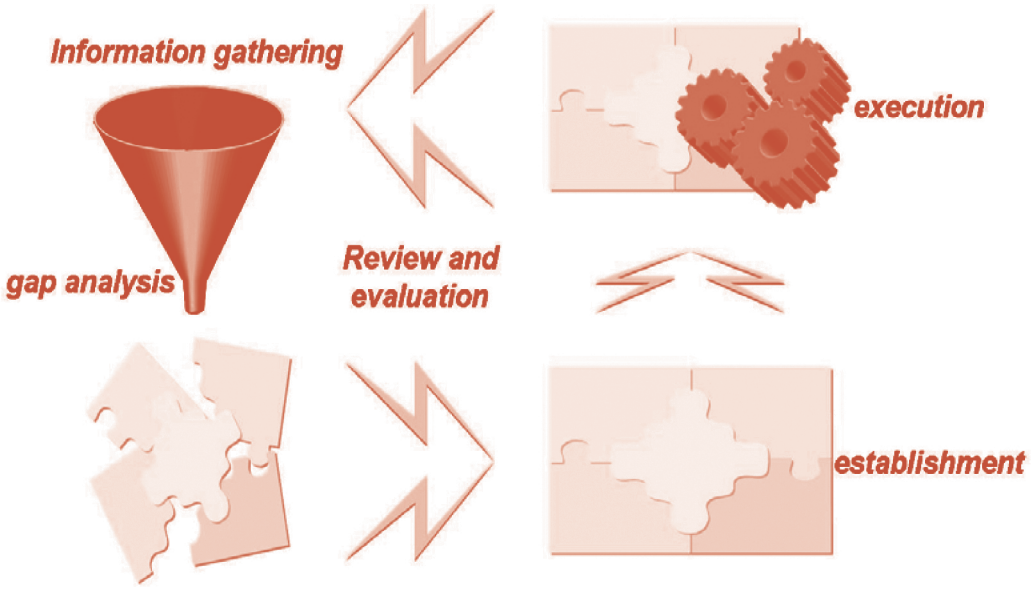
Энэхүү бүлэг нь дараах зорилготой:
- **Мэдээллийн аюулгүй байдлын бодлого боловсруулах үйл явцын тухай товч ойлголт өгөх; болон**
- **Бодлого боловсруулагчид мэдээллийн аюулгүй байдлын бодлого боловсруулахдаа анхаарах асуудлуудыг хэлэлцэх.**

Бодлого боловсруулагчид хэд хэдэн зүйлийг авч үзэх хэрэгтэй бөгөөд үүнд бодлогын үндэслэл, боломжит нөөц, бодлогын чиглэл, төсөв, хууль зүйн шаардлагууд болон бодлогын хүлээгдэж буй үр дүн зэрэг асуудлууд багтана. Энэхүү бүлэгт, эдгээр анхаарах асуудлуудыг мэдээллийн аюулгүй байдлын бодлого боловсруулах өөр өөр шатны хүрээнд авч үзнэ.

Бодлогын асуудал ба хүрээ нь орон бүрт харилцан адилгүй бага зэргийн ялгаатай байна гэдгийг анхаарах хэрэгтэй. Энэ бүлэгт тайлбарлах бодлого боловсруулах үйл явц нь ерөнхий бөгөөд мэдээллийн аюулгүй байдлын бодлого байхгүй гэсэн нөхцөлд суурилсан.

Бусад бодлогуудын адилаар, мэдээллийн аюулгүй байдлын бодлогын мөчлөг 4 шатанд хуваагдаж болно: (1) мэдээлэл цуглуулах ба орон зайн дүн шинжилгээ; (2) бодлого тогтоох; (3) бодлого хэрэгжүүлэх; ба (4) хяналт болон эргэх холбоо (Зураг 19). Түүнчлэн үндэсний мэдээллийн аюулгүй байдлын бодлого нь мэдээллийн аюулгүй байдлын стратеги, хууль зүйн харилцаа, мэдээллийн аюулгүй байдлын байгууллага, мэдээллийн аюулгүй байдлын технологи, болон тэдгээрийн харилцан хамаарлыг багтаасан байвал зохино.

Зураг 19. Мэдээллийн аюулгүй байдлын бодлогын мөчлөг



7.1 Мэдээлэл цуглуулах ба орон зайн дүн шинжилгээ

Мэдээллийн аюулгүй байдлын бодлого боловсруулах эхний алхам бол мэдээлэл цуглуулах ба орон зайн дүн шинжилгээ хийх юм.

Мэдээлэл цуглуулах ажиллагаанд бусад орнуудын мэдээллийн аюулгүй байдлын жишээ болон тухайн орны холбогдох бодлогуудыг мөн нягталж үзэх нь чухал.

Орон зайн дүн шинжилгээнд мэдээллийн аюулгүй байдалтай холбоотой дэд бүтэц тухайлбал одоогийн хуулиуд болон системүүд, түүнчлэн нөхөх хэрэгтэй орон зай, талбарыг ойлгох нь чухал.

Энэ шатанд мэдээллийн аюулгүй байдлын бодлогын чиглэл ба зорилгыг тодорхойлдог учраас маш чухал шат юм.

Мэдээлэл цуглуулах

Гадаад орнуудаас мэдээлэл цуглуулах: Бусад орнууд дахь холбогдох тохиолдлыг тодорхойлохын тулд бодлого боловсруулагчид доорх хэсгүүд дэх ижил төстэй байдлыг авч үзэх хэрэгтэй. Үүнд:

- Үндэсний мэдээллийн аюулгүй байдлын төвшин
- Бодлого тогтоолтын чиглэл
- Сүлжээ ба системийн дэд бүтэц

Эдгээр ижил төстэй байдлыг авч үзсэний үндсэн дээр дараах материалыг цуглуулах хэрэгтэй. Үүнд:

- Мэдээллийн аюулгүй байдалд оролцдог байгууллагуудын зохион байгуулалт ба үйл ажиллагааны талаархи мэдээлэл (Энэ модулийн 3, 6-р бүлгийг харна уу)
- Мэдээллийн аюулгүй байдлын бодлого, хууль, тогтоомжууд (3-р бүлгийг харна уу)
- Олон улсад хэрэглэгддэг мэдээллийн аюулгүй байдлын арга зүй ба бусад орнуудын жишээ (4-р бүлгийг харна уу)
- Аюул заналын хандлага ба түүний эсрэг арга хэмжээ, халдлагын төрлийн дагуу тавих хяналт (2, 6-р бүлгийг харна уу)
- Нууцлал хамгаалалтанд зориулсан арга хэмжээнүүд (5-р бүлгийг харна уу)

Дотоодод мэдээлэл цуглуулах: Хэдийгээр ихэнх бодлого боловсруулагчид мэдээллийн аюулгүй байдлын мэргэжилтнүүд биш боловч тэд мэдээллийн аюулгүй байдалтай холбоотой үйл ажиллагааг гүйцэтгэдэг. Тодруулбал, тэд мэдээллийн аюулгүй байдалтай холбоотой салбаруудад хууль, тогтоомж, бодлого боловсруулдаг. Гэхдээ хууль, тогтоомж, бодлогууд нь тодорхой нэг чиглэлд төвлөрдөг учраас тэдгээрийн хоорондын харилцан холбоо нь бодлого боловсруулагчдад тэр даруй мэдэгдэхгүй байж болох талтай. Тиймээс мэдээллийн аюулгүй байдалтай холбоотой бүх хууль, тогтоомж, бодлогыг цуглуулж дүн шинжилгээ хийх шаардлага гарч байгаа юм.

Орон зайн дүн шинжилгээ

Кунзын Дайтах урлаг номонд “Дайснаа тань” гэсэн байдаг. Энэ нь та өөрийнхөө болоод дайсныхаа хэмжээ хязгаарыг мэдэх хэрэгтэй гэсэн үг юм. Мэдээллийн аюулгүй байдлын бодлого боловсруулах тохиолдолд, энэ нь мэдээллийн аюулгүй байдлын бодлогоор юуг хамгаалах ёстой мөн мэдээллийн аюулгүй байдлын эмзэг байдал ба учрах аюул заналыг мэдэх гэсэн үг юм.

Орон зайн дүн шинжилгээг хоёр үе шатанд хувааж болно:

1. Тухайн улсын чадвар, боломжийг мэдээллийн аюулгүй байдлын ерөнхий хүрээнд ойлгох, ж.нь байгууллага ба хүний нөөц, мөн мэдээлэл, холбооны дэд бүтэц; болон
2. Мэдээллийн аюулгүй байдалд учрах гадаад аюул заналыг таних.

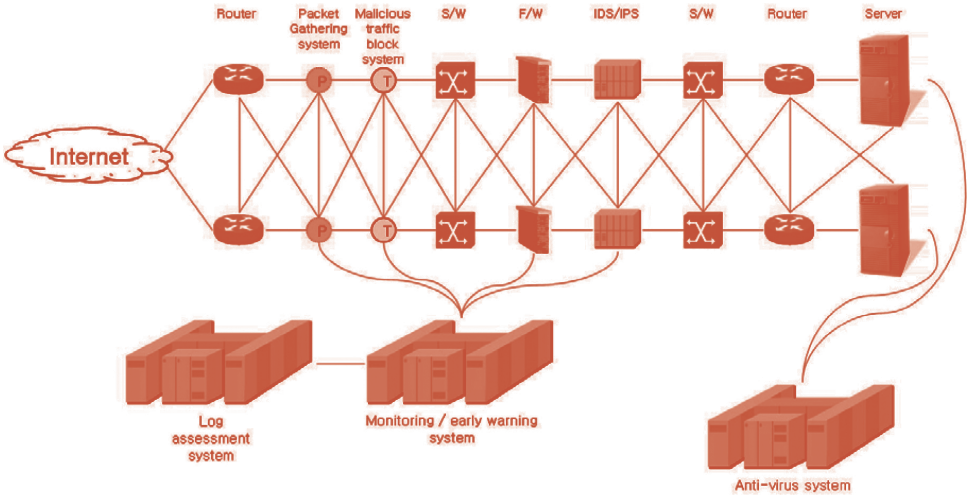
Бодлого боловсруулагчид мэдээллийн аюулгүй байдалтай холбоотой салбарууд дахь төрийн ба хувийн байгууллагууд гээд **мэдээллийн аюулгүй байдлын байгууллага, хүний нөөцийн талаар мэддэг байх шаардлагатай.** Тэд мэдээллийн аюулгүй байдалтай холбоотой ажилд оролцдог байгууллагуудыг мэддэг, тэдгээрийн ажлын хүрээ, үүрэг, хариуцлагыг ойлгодог байх хэрэгтэй. Энэ нь мэдээллийн аюулгүй байдлын одоогийн бүтцийг давхардуулахгүй байхад чухал зүйл юм.

Түүнчлэн мэдээллийн аюулгүй байдлын салбарын мэргэжилтнүүдийг тодорхойлж элсүүлэх нь энэ ажлын хэсэг юм. Ийм мэргэжилтнүүд нь ерөнхийдөө хууль, бодлого, технологи, боловсрол ба холбогдох салбаруудад тодорхой туршлагатай байдаг.

Мэдээлэл холбооны дэд бүтэц гэж цахим хяналтын удирдлагын системүүд болон мэдээллийг цуглуулж, боловсруулж, хадгалж, дамжуулж, хүлээн авдаг МТ-ийн бүтцийг хэлдэг. Товчоор бол мэдээллийн систем, сүлжээ юм.

Мэдээлэл холбооны дэд бүтцийн одоогийн байдлыг ойлгох нь ялангуяа эдийн засгийн зорилгын үүднээс чухал юм. Улсыг бүхэлд нь холбоход томоохон хэмжээний хөрөнгө оруулалт шаардлагатай учраас одоо байгаа мэдээлэл холбооны дэд бүтцээ сайтар хөгжүүлэх нь үр дүнтэй юм. Зураг 20-т мэдээллийн аюулгүй байдалд зориулсан мэдээлэл холбооны дэд бүтцийн жишээг харууллаа. Энэ нь шаардлагатай байж болох бүх элементийг агуулаагүй бөгөөд зөвхөн жишээ болгон харуулах зорилготой юм. Сүлжээний өөр өөр бүрдэл хэсгийн хоорондын харилцан холбоог анхааралаарай.

Зураг 20. Сүлжээ, системийн бүтцийн жишээ



Бодлого боловсруулагчид мэдээллийн аюулгүй байдлын ерөнхий сүлжээ, систем хэрхэн тогтсоныг олж харах чадвартай байх хэрэгтэй.

Орон зайн дүн шинжилгээний хоёр дахь алхам бол **мэдээллийн аюулгүй байдалд учрах гадаад аюул заналыг таних** юм.

2-р бүлэгт дурдсанчлан онц чухал мэдээлэлд заналхийлэх аюул нэмэгдэж байгаа төдийгүй илүү боловсронгуй болж байна. Бодлого боловсруулагчид ямар хариу арга хэмжээ шаардлагатай байгааг шийдэх чадвартай байхын тулд тэдгээр аюул заналыг ойлгодог байх хэрэгтэй. Ялангуяа, бодлого боловсруулагчид дараах зүйлсийг ойлгох ёстой:

- Аюул заналын мэдээллийн аюулгүй байдалд халдаж буй хадлагын хэмжээ
- Хамгийн түгээмэл, хамгийн сүүлийн үеийн довтолгооны төрлүүд
- Аюул заналын төрлүүд ба тэдгээрийн ирээдүйн бат бэх байдлын зэрэглэл

Үндэсний байгууллагууд, хүний нөөц болон мэдээлэл холбооны дэд бүтцийг шинжилж мэдээллийн аюулгүй байдлын салбар дахь аюул заналын бүрдлийг ойлгосныхоо дараа эмзэг байдлын бүрдэл хэсгийг олж авах нь чухал. Энэ нь тухайн улс гадаад аюул заналын бүрдэл хэсгийг эсэргүүцэж чадах хэмжээг тодорхойлох юм. Энэ тодорхойлолтыг дараах зүйлсийг шалгасны үндсэн дээр хийж болно:

- КАБЗХӨБ –ийн одоогийн байдал ба түүний хариу үзүүлэх чадвар
- Мэдээллийн аюулгүй байдлын мэргэжилтнүүдийн одоогийн байдал
- Байгуулалтын төвшин ба мэдээллийн аюулгүй байдлын системийн эрчим
- Мэдээллийн хөрөнгийн халдлагын эсрэг хуулийн хамгаалалт
- Мэдээллийн хөрөнгийг хамгаалах биет орчин

Орон зайн дүн шинжилгээний зорилго болон авч хэрэгжүүлэх шаардлагатай зохимжит хариу арга хэмжээг тодорхойлох чадвартай байх явдал юм. Энэ нь мэдээллийн аюулгүй байдлын бодлого боловсруулалтын хамгийн суурь алхам гэдгийг онцлон тэмдэглэх нь зүйтэй.

7.2 Мэдээллийн аюулгүй байдлын бодлогыг боловсруулах

Үндэсний мэдээллийн аюулгүй байдлын бодлого боловсруулах ажил: (1) бодлогын чиглэлийг тогтоох; (2) мэдээллийн аюулгүй байдлын байгууллагыг байгуулж, үүрэг хариуцлагыг нь тодорхойлох; (3) мэдээллийн аюулгүй байдлын бодлогын хүрээг тодруулах; (4) хуулийг бодлоготой нийцүүлэхийн тулд хууль тогтоох ба/эсвэл шинэчлэх; ба (5) мэдээллийн бодлогын хэрэгжилтэнд төсөв хуваарилах ажиллагааг хамарна.

1. Бодлогын чиглэлийг тогтоож, хэрэгжүүлэх

Ихэнх тохиолдолд, мэдээллийн аюулгүй байдлын бодлогыг баримтлах ажилд хувийн хэвшлийнхнээс илүүтэйгээр төр тэргүүлэн оролцох хэрэгтэй. Ялангуяа засгийн газраас бодлогыг тодорхойлж, шаардлагатай дэд бүтцээр хангахад тэргүүлэх үүрэгтэйгээр оролцож мөн урт хугацааны явцад дэмжиж ажиллах нь зүйтэй юм. Харин хувийн хэвшлийнхэн энэхүү төсөл хэрэгжих явцад зарчмын хүрээнд судалгаа, боловсруулалт болон системийн бүтээн байгуулалт зэрэг ажилд нэгдэн орж хамтран ажиллах шаардлагатай юм.

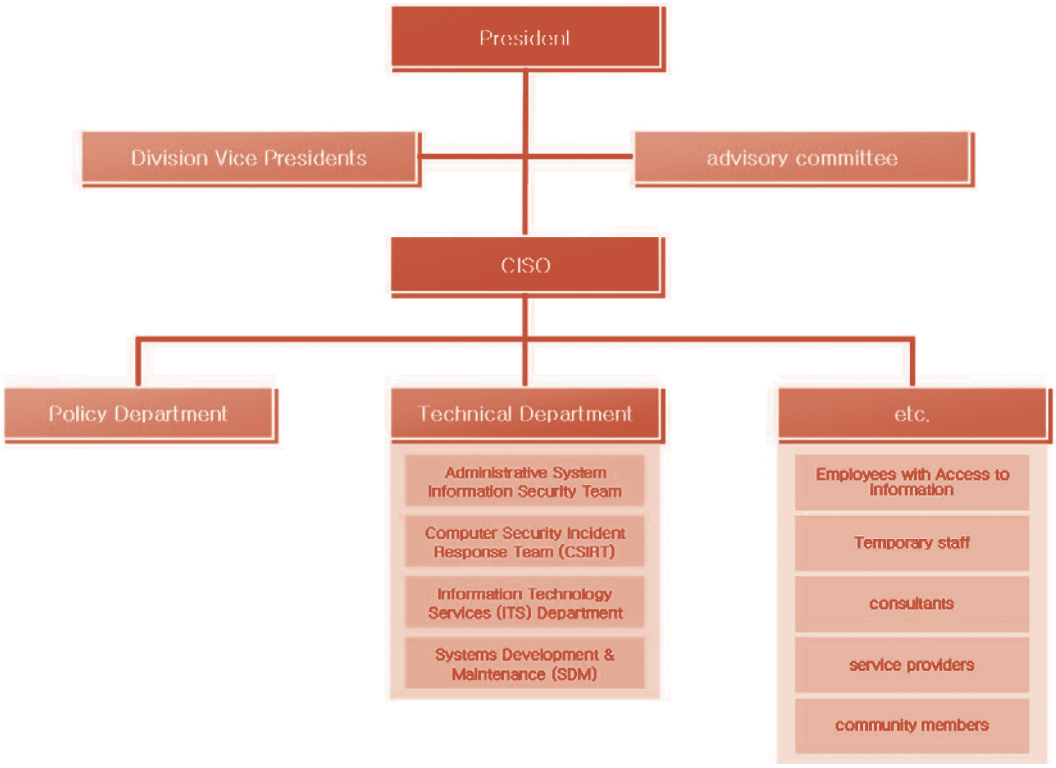
Хувийн хэвшлийн оролцоог төлөвлөх ажилд мэдээлэл холбооны дэд бүтэц байгуулж бэхжүүлэхийн чухал гэдгийг ойлгуулах үйл ажиллагаанууд багтана. Хэрэв засгийн газар мэдээллийн аюулгүй байдлын стратегийг хүлээн зөвшөөрөхөд хувийн хэвшлийг дэмжихээр зорьж буй бол засгийн газар хянах үүргээс илүүтэйгээр дэмжих үүргийг хэрэгжүүлэх хэрэгтэй. Үүнд мэдээллийн аюулгүй байдлын удирдамж түгээх ажил багтана.

2. Мэдээллийн аюулгүй байдлыг хангах байгууллагыг байгуулах ба үүрэг хариуцлагыг тодорхойлох[59]

Мэдээллийн аюулгүй байдлын бодлогын чиглэлийг тогтоосон бол хэрэгжүүлэгч байгууллагыг байгуулах хэрэгтэй. Зураг 21-т үндэсний мэдээллийн аюулгүй байдлын байгууллагын бүтцийг харууллаа.

59. ThissectionisdrawnfromSinclairCommunityCollege,“InformationSecurityOrganization-RolesandResponsibilities,”http://www.sinclair.edu/about/information/usepolicy/pub/infscply/Information_Security_Organization_-_Roles_and_Responsibilities.htm.

Зураг 21. Үндэсний мэдээллийн аюулгүй байдлын байгууллагын жишээ



Үндэсний аюулгүй байдлын байгууллагууд улс бүрийн соёл, онцлогоос шалтгаалан бага зэрэг ялгаатай байна. Хэдий тийм боловч үүрэг хариуцлагын үндсэн зарчим нь ижил байдаг.

Захиргаа, удирдлагын байгууллага

Хэлтсийн дэд ерөнхийлөгчид тус тусын хэлтсүүдийн цуглуулсан мэдээллийг хариуцна. Тэд мэдээллийн аюулгүй байдлын бодлого хэрэгжүүлэхэд туслах, мэдээллийн аюулгүй байдлын ажилтан эсвэл тэдэнд туслах бусад хувь хүмүүсийг томилж болно. Тэдгээр томилогдсон ажилтнууд тэдний хяналтын хүрээнд буй мэдээллийн хөрөнгө нь тодорхой эзэнтэй, эрсдлийн үнэлгээ хийгдсэн, мөн тэдгээр эрсдлүүдэд тулгуурлан аюулгүы байдлын заналхийллийг бууруулах үйл явцыг хэрэгжүүлсэн гэдгийг бататгах ёстой.

Удирдлагууд (Захирал, дарга, менежер г.м.) мэдээлэл ба мэдээллийн системд хандах эрхтэй ажилтнуудыг удирдаж, тэдгээрийн тус тусын салбарт хамаарах мэдээллийн аюулгүй байдлын хяналтыг тодорхойлох, хэрэгжүүлэх, сахиулах ажлыг хийнэ. Мөн тэд бүх ажилагсад мэдээллийн аюулгүй байдалтай холбоотойгоор өөрсдийн үүргээ ухамсарлаж байгаа эсэх болон өөрсдийн ажил үүргээ гүйцэтгэхэд шаардлагатай нөхцөл бололцоогоор хангагдаж байгаа эсэх зэрэг асуудлыг хариуцан ажилладаг. Удирдлагууд мөн ажилтнууд зүй зохистой ажиллаж байгаа эсэх болон аливаа зөрчил, дутагдлаа хэрхэн засч ажиллаж байгааг хянахын тулд хэрэглэгчдийн хандалтын түвшинг үе үе хянаж шалгах хэрэгтэй.

Мэдээллийн аюулгүй байдлын удирдах ажилтан (МАБУА) нь мэдээллийн аюулгүй байдлын бодлогыг зохицуулах, хяналт тавих үүрэгтэй. Өөр өөр хэлтсийн хүмүүстэй ойр ажилладагийн хувьд дарга нь бодлогын тодорхой элементүүдийг зохицуулах, хяналт тавих үүрэг бүхий төлөөлөгчдийг томилох асуудлыг тухайн хэлтсийн удирдлагуудаас шаардаж ажилладаг. Түүнчлэн мэдээлэл эзэмшигчдэд мэдээллийн аюулгүй байдлын талаархи зөвлөмжүүд өгөх маягаар тусалдаг. Үүнд:

- Мэдээллийн эх сурвалжийн хандалт болон боломжит ашиглалттай холбоотой хэрэгжиж болохуйц дүрмийг боловсруулах, түүнийгээ дэлгэрүүлэх
- Мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээ, шинжилгээний ажлыг зохион байгуулах
- Үндэслэл бүхий аюулгүй байдлын удирдамжийг боловсруулах, өгөгдөл болон системийг хамгаалах арга хэмжээ авах
- Системийн аюулгүй байдлын эмзэг байдлын удирдлага болон хяналтын тал дээр туслах
- Мэдээллийн аюулгүй байдлын аудитыг зохицуулах
- Үндэсний мэдээллийн аюулгүй байдлын бодлогын хүрээнд хориг тавих, хяналт шалгалт, шийдвэр гаргахад туслах

Техникийн байгууллага

Мэдээлэлийн аюулгүй байдлын удирдлагын системийн баг нь нууц, хувийн болон эмзэг мэдээллийг үндэсний хууль зүй хийгээд ёс суртахууны хэм хэмжээнд нийцүүлэн хамгаалж, оролцогч талуудад зохистой мэдээллийн хандалт хийх боломжийг олгох маягаар удирдлагын түвшинд аюулгүй байдлын хяналтыг тавьж энэ талын ажлыг боловсруулах үүрэгтэйгээр ажилладаг. Энэхүү баг нь хэрэглэгчид эхний хандалтаар мэдээлэл авах, хандалтын өөрчлөлт, итгэмжлэгдсэн хэрэглэгчдийн мэдээллийн хандалтын талаархи мэдээлэл, түүнчлэн хэрэглэгч болон хянагчдын эрх үүрэг, мэдээллийн аюулгүй байдалтай холбоотой зөрчил маргааныг шийдвэрлэх зэрэг удирдлагын системийн мэдээллийн оновчтой байдал, шударга болон нууц байдлыг хангах үйл ажиллагаа, стандартуудыг боловсруулдаг. Түүнчлэн энэ баг нь Мэдээллийн Аюулгүй Байдлын Ажилтнуудын баг болон Мэдээллийн Аюулгүй Байдлын Удирдах Ажилтны хэлтсүүдийг багтаан ажилладаг бөгөөд Удирдлагын Системийн болон Мэдээллийн Аюулгүй Байдлын Хэлтсийн ажилтнууд тэдэнд зөвлөдөг.

Компьютерийн аюулгүй байдлын зөрчилнд хариу өгөх баг - КАБЗХӨБ нь компьютерийн аюулгүй байдалтай холбоотой асуудлын эрсдлийг бууруулах арга хэмжээ авах, үүний талаар судлах мөн иймэрхүү хэрэг явдал нэгэнт тохиолдвол хор уршгийг нь бууруулахад оролцлогч талуудад тусалж, мэдээллээр хангадаг. Мөн эдгээртэй холбоотойгоор урган гарч болох үйлдлүүдийг тодорхойлж, сануулж ажилладаг. Энэ баг нь асуудлыг эхний үйлдлээр тогтоох, түүнд хариулах, хурцадмал байдлын үеийн шаардлагыг тодорхойлох үүрэг бүхий гүйцэтгэлийн баг, гол чухал будлианд хариу өгөх арга хэмжээг тэргүүлэх үүрэг бүхий удирдлагын баг гэх 2 давхаргаас бүрддэг. Мэдээллийн Аюулгүй Байдлын Удирдах Ажилтан (CISO) болон Мэдээллийн Технологийн Үйлчилгээ, Систем Боловсруулалтын Газрын мэдээллийн технологийн ажилтнуудын төлөөлөгч гишүүд нь гүйцэтгэх багийн нэг хэсэг болдог. Харин удирдлагын багийн хувьд Мэдээллийн Хэлтсийн удирдах ажилтан, Цагдаагийн хэлтсийн дарга, Олон нийтийн мэдээллийн албаны захирал, Мэдээллийн технологийн үйлчилгээний албаны захирал, Систем боловсруулалт хэрэгжилтийн албаны захирал, Мэдээллийн аюулгүй албаны дарга, систем болон сүлжээ хариуцсан менежер, хуулийн зөвлөх, хүний нөөцийн зөвлөх болон дэд ерөнхийлөгчдийн томилсон техникийн судалгааны багийн төлөөлөгчид багтан ажилладаг.

Мэдээллийн Технологийн Үйлчилгээний Хэлтсийн ажилтан гишүүд нь сүлжээ, системийн администраторууд, инженерүүд мөн хэрэглэгчдэд туслах техникийн ажилтнууд болон утсаар холбогдон хэрэглэгчдэд зөвлөгөө өгдөг администраторууд зэрэг техникийн үйлчилгээг үзүүлэгчид байдаг. Мэдээллийн аюулгүй байдлын техникийн тоног төхөөрөмж, сүлжээний орчны хяналт, туршилтыг хариуцан ажиллах үүрэгтэй. Тэд хэрэглэгчдээс мэдээллийн аюулгүй байдал алдагдаж болох сэжигтэй мэдээнүүдийг хүлээн авдаг.

Систем хөгжүүлэлт ба үйлчилгээний хэлтсийн ажилтнууд нь мэдээллийн санг хөгжүүлэгчид болон администраторууд байдаг. Тэд үндэсний мэдээллийн сангийн мэдээллийн аюулгүй байдлыг хангах хамгийн сайн аргуудыг боловсруулж, туршиж, нэгтгэж, хэрэгжүүлж мөн веб програм хөгжүүлэгчдэд програмын аюулгүй байдлын

зарчмын хэрэглээний талаарх сургалтыг явуулдаг.

Бусад

Мэдээлэл ба мэдээллийн системд хандах эрх бүхий ажилтнууд нь үндэсний холбогдох бодлого, дүрэм журам болон удирдах ажилтнуудын тогтоосон дүрэм журамд нийцүүлэн ажиллах ёстой байдаг. Эдгээр нь өөрсдийн дансны нууц үгийг хамгаалах, мэдээллийг буруугаар ашиглаж байгаа болон мэдээллийн аюулгүй байдлын сэжигтэй тохиолдлыг зохих албан тушаалтан (ихэвчлэн удирдлага)-д мэдээлэх ёстой.

Түр ажилтан нь үндсэн болон цагийн ажилтнуудтай ижил үүрэг хүлээнэ.

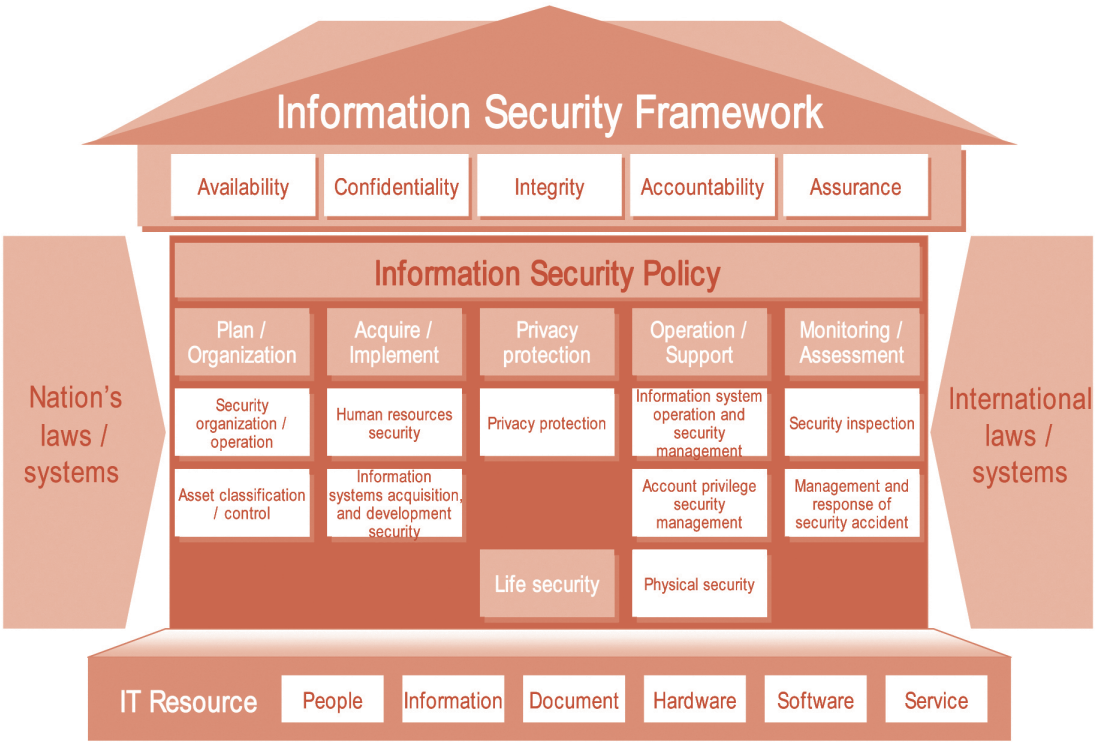
Зөвлөхүүд, үйлчилгээ үзүүлэгчид болон бусад гэрээт гуравдагч талууд нь мэдэх хэрэгтэй гэж үзсэний үндсэн дээр л мэдээллийн хандалт хийдэг. Гуравдагч талын шаардсан сүлжээний мэдээллийг авахад байгууллагын хүрээнд холбогдох дэд ерөнхийлөгч юмуу захирлын зөвшөөрөл, эсвэл сүлжээний мэдээлэлтэй холбоотой хувь хүний хариуцлагыг сайтар ойлгосон гуравдагч талын хэрэглэгч буюу ивээн тэтгэгчийн хүсэлтийн үндсэн дээр мэдээллийг гаргана. Энэхүү хэрэглэгч нь мэдээллийн нууц үгийг задруулахгүй өөрийн ID-г хяналтынхаа хүрээнд байлгах ёстой.

3. Мэдээллийн аюулгүй байдлын бодлогын хүрээг тодорхойлох

Мэдээллийн аюулгүй байдлын хүрээ

Мэдээллийн аюулгүй байдлын хүрээ нь мэдээллийн аюулгүй байдлын бодлогын шалгуурыг тогтоодог. Энэ нь тухайн бодлого мэдээллийн технологийн нөөц (хүмүүс, мэдээлэл, техник хангамж, программ хангамж болон үйлчилгээ)-г харгалзан үзэж, олон улсын хууль тогтоомжуудыг тусгаж, мэдээллийн нууц байдал, аюулгүй байдал, баталгаатай байдлын зарчмуудад нийцсэн эсэхийг бататгадаг. Зураг 22-т мэдээллийн аюулгүй байдлын хүрээг харуулаа.

Зураг 22. Мэдээллийн аюулгүй байдлын хүрээ



Мэдээллийн аюулгүй байдлын бодлого нь мэдээллийн аюулгүй байдлын хүрээний хамгийн чухал хэсэг юм. Энэхүү бодлого нь дараах 5 салбарыг багтаадаг. Үүнд:

А. Төлөвлөгөө ба байгууллага: Энэ нь байгуулалт, үйл ажиллагааны аюулгүй байдал, хөрөнгийн ангилал болон хяналт зэргийг багтаадаг.

Аюулгүй байдлын байгууллага, үйл ажиллагаа нь:

- Үндэсний мэдээллийн аюулгүй байдлын байгууллагын байгуулалт ба систем
- Мэдээллийн аюулгүй байдлын байгууллага бүрийн журам
- Үндэсний мэдээллийн аюулгүй байдлын бүтэц, удирдлага
- Холбогдох олон улсын агентлагуудтай хамтран ажиллах
- Мэргэжилтнүүдийн бүлэгтэй хамтран ажиллах ажиллагааг багтаадаг.

Хөрөнгийн ангилал, хяналт нь:

- Чухал мэдээллийн хөрөнгийг эзэмших эрх ба ангилалын стандарт
- Чухал мэдээллийн хөрөнгийг бүртгэх заавар ба эрсдлийн үнэлгээ
- Чухал мэдээллийн хөрөнгө руу хандах давуу эрхийн зохицуулалт
- Чухал мэдээллийн хөрөнгийг хэвлэх, гадагш гаргах
- Чухал мэдээллийн хөрөнгийг дахин үнэлэх
- Бичиг баримтуудын аюулгүй байдлын удирдлага

Б. Эзэмшилт ба хэрэгжилт: Энэ нь хүний нөөцийн аюулгүй байдал, мэдээллийн системийг эзэмших, аюулгүй байдлыг хөгжүүлэх зэрэг ажлыг багтаадаг.

Хүний нөөцийн аюулгүй байдал гэдэг нь доор дурьдагдах шинэ ажилтнуудыг ажилд авах удирдлагын аргыг тодорхойлох ажил юм:

- Хүний нөөцийн аюулгүй байдлын хариу арга хэмжээ, аюулгүй байдлын сургалт
- Аюулгүй байдлын хууль, тогтоомжуудын зөрчлийг бууруулах
- Гуравдагч талын хандалтын аюулгүй байдлын удирдлага
- Аутсорсингийн ажилтнуудын хандалтын аюулгүй байдлын удирдлага
- Гуравдагч талууд болон аутсорсингийн ажилтнуудын ажил ба удирдлага
- Компьютерийн өрөө, тоног төхөөрөмжийн аюулгүй байдлын удирдлага
- Гол тоног төхөөрөмж ба барилга руу нэвтрэх
- Аюулгүй байдлын ослыг багасгах

Мэдээллийн системийг эзэмших болон аюулгүй байдлыг сайжруулахад дараах зүйлс шаардлагатай. Үүнд:

- Мэдээллийн системийг олж авмагц аюулгүй байдлыг шалгах хэрэгтэй
- Аппликейшн програмыг дотооддоо хөгжүүлэх болон аутсорсинг хийх аюулгүй байдлын удирдлага
- Үндэсний нууцлалын систем (нууцлалын програм, түлхүүр г.м)
- Програм хөгжүүлэлтийн дараах тестүүд
- Аутсорсингоор хөгжүүлэлт хийж буй үеийн боломжит аюулгүй байдлын шаардлага
- Боловсруулалтын аюулгүй байдлын баталгаа

В. Нууцлалын хамгаалалт: Мэдээллийн аюулгүйн бодлогод нууцлал хамгаалалтын асуудлыг оруулах нь зайлшгүй шаардлагатай зүйл биш юм. Хэдий тийм боловч, нууцлалын хамгаалалтын асуудал нь олон улсын асуудал учир хэрэв багтаавал бас давуу талтай. Нууцлалын хамгаалалтын нөхцөлүүд нь дараах зүйлсийг хамардаг. Үүнд:

- Хувийн мэдээллийг цуглуулах, ашиглах
- Хүмүүсийн хувийн мэдээллийг ашиглахдаа урьдчилан зөвшөөрөл авах
- ННБҮ

Г. Үйл ажиллагаа, дэмжлэг: Энэ ажил нь материаллаг болон техникийн аюулгүй байдалтай хамт хийгдэх ёстой. Сүлжээ болон системийн хэрэглээ нь нарийвчлан зохицуулагддаг бөгөөд мэдээллийн материаллаг аюулгүй байдал болон харилцааны дэд бүтцээр мөн тодорхойлогддог.

Мэдээллийн системийн үйл ажиллагаа болон аюулгүй байдлын удирдлага нь дараах зүйлсийг тодорхойлох ажлыг багтаадаг:

- Сервер, сүлжээ, аппликейшн болон мэдээллийн сангийн үйл ажиллагаа, аюулгүй байдлын удирдлага
- Мэдээллийн аюулгүй байдлын систем хөгжүүлэлт
- Хуулийн арга хэмжээний дагуу бүртгэл ба хадгалалт хийх
- Мэдээлэл хадгалалтын удирдлага
- Хөдөлгөөнт тооцоолол
- Хадгалалтын стандарт болон компьютерийн өгөгдлийн аюулгүй байдал
- Цахим худалдааны үйлчилгээ

Дансны давуу эрхийн аюулгүй байдлын удирдлага - Үндэсний мэдээллийн сангийн ашиглалтын нууцлалтай байдлыг баталгаажуулах зорилгоор хандалтын хяналт болон дансны удирдлагыг тодорхойлох ёстой. Үүнд дараах зүйлс багтана. Үүнд:

- Үндэсний мэдээллийн системийн хэрэглэгчийн бүртгэл, устгах, давуу эрхийн удирдлага
- Нууцлагдсан харилцааны давуу эрх ба дансны удирдлага

Материалын аюулгүй байдал: Материалаг аюулгүй байдал нь чухал мэдээллийг хадгалдаг мэдээлэл, холбооны тоног төхөөрөмжийг илтгэдэг. Үүнд дараах ажил орно:

- Аюулгүй байдлын салбарын аргачлалыг тохируулах, удирдах
- Компьютерийн төвийн хандалт, шилжилтийн хяналт
- Байгалийн болон бусад гамшгийн аюулаас урьдчилан сэргийлэх

Д. Хяналт, үнэлгээ: Энэ салбарын мэдээллийн аюулгүй байдлын бодлого нь аюулгүй байдлын будлианаас сэргийлэх болон аюулгүй байдлын будлианыг удирдаж, хариу өгөхөд зориулсан стандарт, үйл явцыг тогтоохыг шаарддаг.

Аюулгүй байдлын шалгалтанд дараах зүйлс багтана:

- Аюулгүй байдлын шалгалтын төлөвлөгөөг бий болгох
- Аюулгүй байдлын хугацаат шалгалтыг хэрэгжүүлэх
- Тайлангийн загварыг зохиох, боловсруулах
- Аюулгүй байдлын шалгалтын субъект, тайланг мэдээлэх ажилтныг тогтоох

Аюулгүй байдлын будлианы удирдлага ба түүнд хариу өгөх ажиллагаа нь дараах зүйлсийг тодорхойлохыг шаарддаг -

- Мэдээллийн аюулгүй байдлын будлианы шийдвэрлэх ажилд байгууллага бүрийн гүйцэтгэх ажил, үүрэг
- Аюулгүй байдлын будлианы шинж тэмдгийг ажиглах, таньж мэдэх журам
- Аюулгүй байдлын будлианыг шийдвэрлэх журам ба хариу арга хэмжээ авах аргачлал
- Аюулгүй байдлын будлианыг шийдвэрлэсний дараагаар хэрэгжүүлэх арга хэмжээ

4. Мэдээллийн аюулгүй байдлын бодлоготой нийцүүлэх зорилгоор хуулиудыг үндэслэх ба/эсвэл шинэчлэх

Хуулиуд нь мэдээллийн аюулгүй байдлын бодлоготой нийцсэн байх ёстой. Төрийн болон хувийн хэвшлийн байгууллагуудыг удирдах хуулиуд байх ёстой. Хүснэгт 14-16-д АНУ, Европын Холбооны Улсууд болон Япон зэрэг орнууд дахь мэдээллийн аюулгүй байдалтай холбоотой хууль тогтоомжуудыг жагсаалтаар харууллаа. Японд төлөөлөх үүрэгтэй мэдээллийн технологийн хууль нь Мэдээлэл Харилцаа Холбооны Сүлжээний Дэвшилтэт Нийгмийг байгуулах тухай үндсэн акт юм. Энэ хууль нь улс орон дахь мэдээллийн аюулгүй байдлын суурь стандарт болдог бөгөөд бусад холбогдох хуулиуд энэхүү хуультай нийцсэн байх ёстой.

Хүснэгт 14. Японы мэдээллийн аюулгүй байдалтай холбоотой хуулиуд

Хуулиуд	Хамрах хүрээ	Зохицуулалтын объект	Шийтгэл
Зөвшөөрөлгүй компьютерийн хандалтын хууль	Бүх салбар	Зөвшөөрөлгүй хандалтыг дэмжсэн үйлдлүүд болон тухайн хүнд мэдэгдэлгүйгээр ID-г нь бусдад өгөх	
Хувийн мэдээллийг хамгаалах тухай хууль	Бизнесийн зорилгоор хувийн мэдээлэл ашигладаг хувийн хэвшлүүд	Хувийн мэдээллийн/ хаяг, утас, й-мэйл хаяг г.м/ удирдлага	Эрүүгийн хариуцлага, шийтгэл
Электрон гарын үсэг, түүний баталгаажилтын тухай акт		Интернэт ашигласан худалдаа болон сүлжээгээр хийгддэг эдийн засгийн үйл ажиллагааг хялбарчлах	

Хүснэгт 15. Мэдээллийн аюулгүй байдалтай холбоотой Европын Холбооны улсуудын хуулиуд

Хуулиуд	Нарийвчлал
Нийтлэг зохицуулалтын хүрээ (Удирдамж 2002/21/EC)	• Цахилгаан холбооны сүлжээ, үйлчилгээг зохицуулах хүрээг танилцуулсан • Аюулгүй холбооны сүлжээгээр дамжуулан нууцлалыг хамгаалах зорилготой
Мэдээллийн хамгаалалтын тухай Европын холбооны удирдамж (1995/46/EC)	• Хувийн мэдээллийг боловсруулах ба чөлөөтэйгээр устгах тухай удирдамж • Гишүүн үндэстнүүдийн үүрэг хариуцлагыг тодорхойлж хувь хүний хувийн мэдээлэлтэй холбоотой эрх мэдлийг хүлээн зөвшөөрөх үндсэн хууль • Америкийн стандартаас илүү чанга
Цахим гарын үсгийн тухай Европын холбооны удирдамж (Удирдамж 2000/31/EC) Цахим худалдааны тухай Европын холбооны удирдамж (2000/31/EC)	• Цахим гарын үсгийн хэрэглээг удирдах • Цахим худалдаа явуулах ажлыг зохицуулах
Кибер гэмт хэргийн тухай гэрээ	• Кибер гэмт хэргийн тухай олон улсын хамгийн цогц гэрээ • Интернэт ашиглан үйлдэгдэж болох бүх эрүүгийн гэмт хэргүүд ба холбогдох ял шийтгэлийг нарийвчлан тогтоодог
Холбоо, сүлжээний тухай мэдээллийн хадгалалтын удирдамж	• Харилцаа холбооны үйлчилээ явуулдаг компаниудаас дуудлагын мэдээллийг 6-24 сар хүртэлх хугацаагаар хадгалахыг шаарддаг (2004, 2005 онуудад Мадрид болон Лондонд гарсан террорист халдлагын дараа батлагдсан)

Хүснэгт 16. Мэдээллийн аюулгүй байдалтай холбоотой АНУ-ын хуулиуд

Хуулиуд	Хамрах хүрээ	Зохицуулалтын хүрээ	Шийтгэл
Холбооны мэдээллийн аюулгүй байдлын удирдлагын тухай хууль 2002	Холбооны удирдах агентлагууд	Засгийн Газрын агентлагууд, мэдээллийн технологийн систем, мэдээллийн аюулгүй байдлын программын мэдээлэл	-
Эрүүл мэндийн даатгалын нууцлал ба хариуцлагатай байдлын тухай хууль	Эрүүл мэндийн байгууллагууд болон эрүүл мэндийн үйлчилгээ үзүүлэгчид	Хувь хүний эрүүл мэндийн талаархи цахим мэдээлэл	Эрүүгийн хариуцлага, мөнгөн торгууль
1999 оны Грэм-Лич-Блилийн хууль	Санхүүгийн байгууллагууд	Үйлчлүүлэгчдийн нууцлал бүхий мэдээлэл	Эрүүгийн хариуцлага, мөнгөн торгууль
2002 оны Сарбанес -Окслейн хууль	Америкийн хөрөнгийн бирж дээрхи компаниуд	Дотоод хяналт болон олон нийтийн санхүүгийн мэдээлэл	Эрүүгийн хариуцлага, мөнгөн торгууль
2003 оны мэдээллийн сангийн аюулгүй байдлын тухай Калифорнийн Акт	Калифорни дахь Засаг захиргааны агентлагууд болон хувийн байгууллагууд	Кодолсон нууцлалтай мэдээллүүд	Мөнгөн торгууль болон хохирогчид мэдэгдэх

5. Мэдээллийн бодлогын хэрэгжилтэнд зориулан төсөв хуваарилах

Аливаа нэгэн бодлогын хэрэгжилт нь төсөв шаарддаг. Хүснэгт 17-д Япон болон АНУ-ын сүүлийн жилүүдийн мэдээллийн аюулгүй байдлыг хангахад зарцуулсан төсвийг харууллаа.

Хүснэгт 17. Япон болон АНУ-ын мэдээлэл хамгаалалтын төсөв

Япон	Япон	2005
Жилийн нийт төсөв	Жилийн нийт төсөв	855,195,000,000,000 иен
Мэдээллийн аюулгүй байдлын төсөв	Мэдээллийн аюулгүй байдлын төсөв	288,000,000,000 иен
Нийт төсвийн хувь	Нийт төсвийн хувь	0.03%
АНУ	**АНУ**	**2007**
Жилийн нийт төсөв	Жилийн нийт төсөв	2,770,000,000,000 ам.дол
Мэдээллийн аюулгүй байдлын төсөв	Мэдээллийн аюулгүй байдлын төсөв	5,759,000,000 ам.дол
Нийт төсвийн хувь	Нийт төсвийн хувь	0.208%

ДАСГАЛ

Хэрвээ танай орон мэдээллийн аюулгүй байдлын бодлоготой бол түүний хөгжлийг дээр тайлбарласан мэдээллийн аюулгүй байдлын бодлого боловсруулалтын таван зүйлээр тодорхойл. Үүнд:

1. Бодлогын чиглэл
2. Мэдээллийн аюулгүй байдлын байгууллага
3. Бодлогын хүрээ
4. Мэдээллийн аюулгүй байдлыг дэмжсэн хуулиуд
5. Мэдээллийн аюулгүй байдлын төсөв хуваарилалт

Хэрэв танай орон мэдээллийн аюулгүй байдлын бодлогоо хараахан тодорхойлж амжаагүй байгаа бол бодлого боловсруулалтын дээрхи 5 зүйлийг бий болгох боломжуудыг авч үзээрэй. Дараах асуултуудыг чиглэл болгон ашиглаарай.

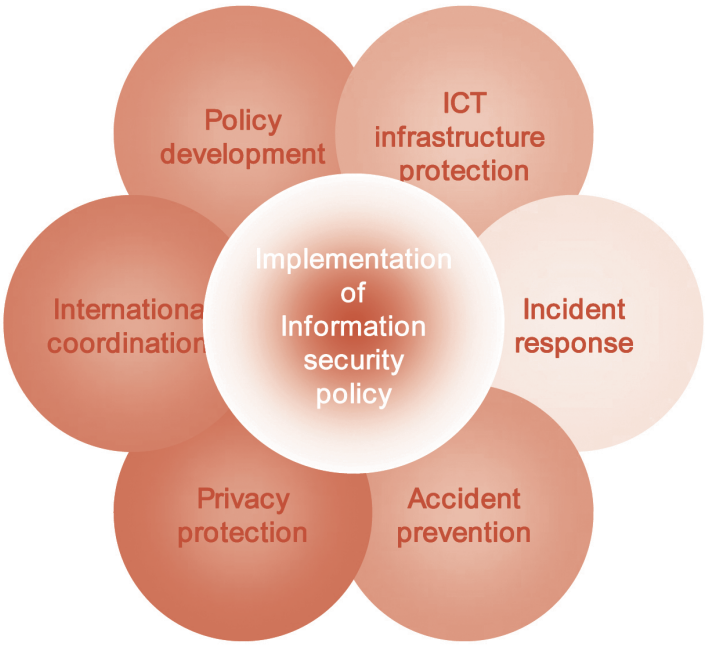
1. Танай оронд мэдээллийн аюулгүй байдлын бодлогын чиглэл ямар байх ёстой вэ?
2. Ямар зохион байгуулалт хэрэгтэй вэ? Мэдээллийн аюулгүй байдлын бодлого боловсруулалт болон хэрэгжилтэд танай орны ямар байгууллагууд оролцох ёстой вэ?
3. Бодлогын хүрээнд ямар асуудлуудыг авч үзэх шаардлагатай вэ?
4. Мэдээллийн аюулгүй байдлын бодлогыг дэмжсэн ямар хуулийг өөрчлилж эсвэл шинээр батлах хэрэгтэй вэ?
5. Хэдий хэмжээний төсөв шаардлагатай вэ? Шаардлагатай төсвийг хаанаас гаргуулах ёстой вэ?

Нэг орноос ирсэн сургалтанд хамрагдагса энэ үйл ажиллагааг хамтран хийж болно.

7.3 Бодлогын гүйцэтгэл, хэрэгжилт

Мэдээллийн аюулгүй байдлын бодлогын шуурхай хэрэгжүүлэхэд засгийн газар, хувийн хэвшлийнхэн болон олон улсын байгууллагын хоорондын хамтын ажиллагааг шаардлагатай. Зураг 23-т хамтын ажиллагаа чухал шаардлагатай байгаа мэдээллийн бодлогын хэрэгжилтийн тодорхой салбаруудыг харууллаа.

Зураг 23. Мэдээллийн аюулгүй байдлын бодлогын хэрэгжилтийн хамтын ажиллагааны салбар



Мэдээллийн аюулгүй байдлын бодлогын боловсруулалт

Хүснэгт 18-д Үндэсний мэдээллийн аюулгүй байдлын бодлогыг боловсруулахад засгийн газар, хувийн хэвшлийнхэн болон олон улсын байгууллагууд хэрхэн хувь нэмрээ оруулж болохыг харууллаа.

Хүснэгт 18.

Салбар	Бодлого боловсруулалтад оруулах хувь нэмэр
Засгийн газар	• Үндэсний стратеги, төлөвлөлтийн байгууллага: Мэдээллийн бодлого болон үндэсний хэмжээний төлөвлөлтийн хоорондын харилцан уялдааг хангах • Мэдээлэл, холбооны технологийн байгууллага: Үндэсний мэдээллийн аюулгүй байдлын технологийн стандартыг тодорхойлох хамтын ажиллагааг бэхжүүлэх • Мэдээллийн аюулгүй байдлын чиг хандлагын судалгааны байгууллага: Дотоодын болон олон улсын мэдээллийн аюулгүй байдлын чиг хандлага болон бодлогын талаархи судалгааг тусгах • Эрхзүйн шинжилгээний байгууллага: Мэдээллийн аюулгүй байдлын бодлого болон одоогийн хуулийн хоорондын зохицлыг хангах • Үндэсний мэдээллийн байгууллага: Чиглэл тогтоох болон стратеги төлөвлөлтөнд хамтран ажиллах • Шинжилгээний агентлагууд: мэдээллийн аюулгүй байдлын хэргүүдийг шийдвэрлэхэд хамтран ажиллах
Хувийн хэвшил	• Мэдээллийн аюулгүй байдлын зөвлөх компаниуд: мэдээллийн аюулгүй байдлын бодлого боловсруулахад мэргэжлийн агентуудыг ашиглах • Мэдээллийн аюулгүй байдлын технологийн хувийн лаборатори: мэдээллийн аюулгүй байдалтай холбоотой технологийн стандартуудыг тогтоох • Их дээд сургууль болон мэргэжил дээшлүүлэх сургуулиудын мэдээллийн аюулгүй байдлын тэнхимүүд: бодлого боловсруулахад мэргэжлийн талаас зөвлөх
Олон улсын байгууллагууд	• Олон улсын мэдээллийн бодлогын стандартуудтай нийцэж буй эсэхийг баталгаажуулах • Олон улсын шинж чанартай аюул заналд хариу өгөх ажиллагааг зохицуулах

Мэдээлэл, холбооны дэд бүтцийн удирдлага, хамгаалалт

Мэдээллийн үр дүнтэй хэрэглээ (цуглуулалт г.м) нь МТ-ийн дэд бүтцийн оновчтой удирдлага, хамгаалалтыг шаарддаг. Мэдээллийн аюулгүй байдлын сайн бодлого нь МТ-ийн бат бэх дэд бүтэцгүйгээр ямар ч хэрэгцээгүй юм. Мэдээлэл, холбооны дэд бүтцийн үр дүнтэй удирдлага, хамгаалалт нь сүлжээ, систем болон мэдээлэлийн технологийн салбарын менежрүүдийн хоорондын хамтын ажиллагааг шаарддаг. Түүнчлэн олон нийтийн болон хувийн байгууллагуудын хоорондын хамтын ажиллагааны үр дүн ч бас нөлөөтэй.

Хүснэгт 19. Мэдээлэл холбооны дэд бүтцийн удирдлага, хамгаалалтын хамтын ажиллагаа

Салбар	Мэдээлэл холбооны дэд бүтцийн удирдлага, хамгаалалтад оруулах хувь нэмэр
Засгийн газар	• Мэдээлэл, холбоны сүлжээтэй хамааралтай байгууллагууд: • үндэсний мэдээлэл, холбооны сүлжээний бүтэц ба аюулгүй • байдлын түвшинг тодорхойлох • Мэдээлэл, холбооны технологийн лаборатори: нийтийн • стандартыг түгээн дэлгэрүүлж, ашиглаж болохуйц технологийг нутагшуулах
Хувийн хэвшлийнхэн	• ISP-ууд: үндэсний мэдээлэл холбооны сүлжээг бий болгоход • хамтрах • Мэдээлэл холбооны технологийн лаборатори: техникийн хөгжлийн үйлчилгээгээр хангах, мэдээлэл харилцааны дэд бүтэц болон аюулгүй байдлын технологийн тогтвортой ажиллагааг хөгжүүлэхэд хамтран ажиллах,
Олон улсын байгууллага	• Олон улсын мэдээлэл харилцаа холбоо болон шинэ мэдээллийн технологийг бэхжүүлэх зорилгоор олон улсын технологийн стандартын байгууллагуудтай хамтран ажиллах

Аюул занал, будлианаас урьдчилан сэргийлэх ба хариу өгөх

Аюул занал, мэдээллийн аюулгүй байдлын будлианд үр дүнтэйгээр хариу өгөх ажил үндэсний мэдээллийн байгууллага, шинжилгээний агентлагууд болон хуулийн байгууллага, түүнчлэн аюулгүй байдлын зөрчлийн хяналтын болон эрсдлийн үнэлгээний байгууллагуудын хамтын ажиллагааг шаарддаг. Мөн техникийн эмзэг байдлыг шалгаж, техникийн хариу арга хэмжээг зөвлөж чадах байгууллагуудтай хамтран ажиллах нь чухал юм.

Хүснэгт 20. Мэдээллийн аюулгүй байдлын осолд хариу өгөх ажиллагаанд хамтран ажиллах (жишээ)

Салбар	Оролцоо
Засгийн газрын байгууллагууд	• Аюулгүй байдлын хариу өгөх байгууллага: бодит байдлын дүн шинжилгээгээр хангах, халдлага, будлианд хариу өгөх болон зөрчил, ослуудад хариу өгөх технологи • Үндэсний мэдээллийн байгууллага: мэдээллийн аюулгүй байдалтай холбоотой зөрчил, ослуудыг шалгах, мөрдөх • Шинжлэн судлах агентлагууд: мэдээллийн аюулгүй байдлын эсрэг хэрэгт өртсөн байгууллагуудтай хамтран ажиллаж зөрчил гаргагчийг мөрдөх, баривчлах • Аюулгүй байдлын үнэлгээ хийх байгууллага: мэдээллийн сүлжээ болон мэдээллийн аюулгүй байдалд суурилсан үйлдвэрлэлийн аюулгүй бөгөөд найдвартай байдлыг баталгаажуулах • Мэдээллийн аюулгүй байдлын боловсролын байгууллага: мэдээллийн аюулгүй байдлын ослын шалтгааныг шинжилж, осол дахин гарахаас сэргийлэхэд хүмүүсийг сургах
Хувийн бүлгүүд	• Будлианд хариу өгөх хувийн байгууллага: хариу арга хэмжээгээр хангаж, техникийн тусламж үзүүлэх • Хувийн шинжлэн шалгах агентлагууд: үндэсний хяналтын агентлагуудтай хамтран ажиллах
Олон улсын байгууллагууд	• Олон улсын аюул занал, будлиан гарсан тохиолдолд Интерпол, КХХҮБ/ЗТ-д мэдэгдэх, тэдэнтэй хамтран ажиллах

Мэдээллийн аюулгүй байдлын будлианаас урьдчилан сэргийлэх

Мэдээллийн аюулгүй байдлын зөрчил, будлианаас урьдчилан сэргийлэх нь хяналт, боловсрол болон өөрчлөлтийн удирдлагын асуудлуудыг багтаадаг. Үндэсний КАБЗХӨБ нь үндсэн хяналтын байгууллага юм. Гол салбар нь мэдээллийн бодлого ба бодит хяналтын өгөгдлийг уялдуулах юм. Иймээс мэдээллийн бодлогын хяналтын хамрах хүрээг авч үзэх нь чухал юм. Мөн түүнчлэн төрийн ба хувийн байгууллагын ажилтнууд, мөн олон нийтэд мэдээллийн аюулгүй байдлын бодлогын талаар боловсрол олгох нь чухал. Түүнчлэн мэдээлэлд хандах хандлага болон аюулгүй байдлын мэдээлэлд нөлөөлдөг үйлдлүүдийг өөрчлөх шаардлагатай байж болох юм. Мэдээллийн аюулгүй байдлын боловсрол болон өөрчлөлтийн удирдлагыг US SP 800-16 (Мэдээллийн технологийн аюулгүй байдлын сургалтын шаардлага) –д тодорхойлсон байдаг.

Хүснэгт 21. Мэдээллийн аюулгүй байдлын зөрчил, ослоос сэргийлэхэд хамтран ажиллах (жишээ)

Салбар	Зохицуулалт
Засгийн газрын байгууллагууд	• Хяналт-шинжилгээний агент: сүлжээний тасралтгүй хяналт ба аюулгүй байдлын аюул заналын дэвшилтэт илрүүлэлт • Цуглуулагч агент: олон усын байгууллагууд болон аюулгүй байдлын сайтуудтай мэдээлэл солилцох • Сургалтын байгууллага: мэдээллийн аюулгүй байдлын зөрчил, осолд хурдан хариу өгөх чадвар, чадамжийг хөгжүүлэх шат дараатай сургалт
Хувийн байгууллагууд	• ISP, аюулгүй байдлын хяналт, вирусын эсрэг хамгаалалтын компаниуд: хөдөлгөөний статистик мэдээ болон халдлагын төрөл, өт/вирусын талаарх мэдээллээр хангах
Олон улсын байгууллагууд	• Халдлагын төрөл, өт/вирусын талаарх мэдээллээр хангах

Нууцлал хамгаалалт

Интернэтийн нууцлал хамгаалалтын арга хэмжээг тогтоох, хувийн мэдээллийн будлианаас урьдчилан сэргийлэх, хувийн мэдээллийн хамгаалалт болон нууцлалын зөрчлийг мэдээлэхэд хамтын ажиллагаа шаардлагатай.

Хүснэгт 22. Нууцлал хамгаалалтын зохицуулалт

Салбар	Зохицуулалт
Засгийн газрын байгууллагууд	• Системийн шинжилгээний байгууллага: хувийн мэдээлэлтэй холбоотой бизнес явуулах болон дотоод, гадаад хувийн мэдээллийн хамгаалалтын чиг хандлагыг судлах • Төлөвлөлтийн байгууллага: хууль/системүүд, техникийн/ удирдлагын арга хэмжээ болон, стандартын удирдлагыг сайжруулах • Техникийн дэмжлэг: бизнесийн зорилгоор кибер хэрэглэгчийн зөвшөөрөл олгох асуудлыг хариуцах • Үйлчилгээний байгууллага: нууцлалын зөрчил болон спамыг шийдвэрлэхэд үзүүлэх дэмжлэгийг зохицуулах
Хувийн байгууллагууд	• Хувийн мэдээллийн аюулгүй байдлын байгууллага: хувийн мэдээллийн аюулгүй байдлыг хангах шаардлагуудыг бүртгүүлэх, хамтарсан холбоо байгуулах, • Хувийн мэдээллийн аюулгүй байдлын талаар зөвлөгөө өгөх
Олон улсын байгууллагууд	• Олон улсын хувийн мэдээллийн аюулгүй байдлын стандартыг хэрэглэхэд хамтран ажиллах

Олон улсын зохицуулалт

Мэдээллийн аюулгүй байдлын зөрчил нь олон улсын шинж чанартай байх хандлагатай учраас мэдээллийн аюулгүй байдлыг хангах асуудал нь нэг улс орон дангаараа хүчин зүтгээд амжилтанд хүрэх боломжгүй зүйл юм. Иймээс засгийн газар болоод хувийн хэвшлийн аль алинынх нь хүрээнд олон улсын зохицуулалт хэрэгтэй. Хувийн хэвшлийн хувьд, мэдээллийн аюулгүй байдлыг дэмжигч, хамгаалагч олон улсын байгууллага нь КХХҮБ/ЗТ юм. Засгийн газрын байгууллагын хувьд ЕМСАБА (Европын Холбооны улсуудын хувьд) болон ОУЦХБ гэх мэт байгууллагууд нь олон улсын мэдээллийн аюулгүй байдлыг хангах харилцааг дэмжин ажиллах зорилго бүхий байгууллагууд юм.

Улс орон бүрт засгийн газрын болон хувийн байгууллагуудыг ижил төстэй олон улсын байгууллагуудтай холбох засгийн газрын байгууллага байх ёстой.

ДАСГАЛ

1. Үндэсний мэдээллийн аюулгүй байдлын бодлогын хэрэгжилтэнд хамтран ажиллах шаардлагатай төрийн болон хувийн байгууллагуудыг тодорхойл. Түүнчлэн тэдгээрийн хамтран ажиллах хэрэгтэй олон улсын байгууллагуудыг тодорхойл.
2. Зураг 23-т үзүүлсэн мэдээллийн аюулгүй байдлын бодлогын хэрэгжилтэнд хамтран ажиллах салбар тус бүрээр тэдгээр агентлагуудын хэрэгжүүлж чадах тодорхой үйл ажиллагаа, арга хэмжээг тодруул.

Нэг улсаас ирсэн оролцогсод энэ дасгалыг хамтдаа хийх боломжтой.

7.4 Мэдээллийн аюулгүй байдлын бодлогын хяналт ба үнэлгээ

Мэдээллийн аюулгүй байдлын бодлого боловсруулалтын эцсийн алхам нь бодлогоо үнэлж, дутагдалтай талаа хөгжүүлэх явдал юм. Бодлогыг ийнхүү хянах нь мэдээллийн аюулгүй байдлын бодлогын үр ашгийг тодорхойлсны дараа маш чухал байдаг. Дотоод бодлогын үнэлгээний аргыг үндэсний мэдээллийн аюулгүй байдлын бодлогын үр ашгийг тодорхойлоход хэрэглэж болно. Энэхүү аргын талаар дор авч хэлэлцсэн байгаа.

Аудитын байгууллагуудын оролцоо

Бодлогын үнэлгээ, шинжилгээ хийх үүрэг бүхий байгууллагууд байдаг. Иймэрхүү байгууллагууд нь үндэсний мэдээллийн аюулгүй байдлын бодлогод тогтмол аудит хийх ёстой байдаг. Мөн түүнчлэн, энэ байгууллага нь мэдээллийн аюулгүй байдлын бодлого боловсруулагч болон хэрэгжүүлэгч байгууллагуудаас тусдаа бие даасан байгууллага байдаг.

Мэдээллийн аюулгүй байдлын бодлогыг хянан засварлах

Асуудалтай байгаа хэсэг ихэвчлэн бодлогын аудитын явцад тогтоогддог. Иймээс илэрсэн алдаа дутагдлыг дахин хянаж ажиллах хэсэг мөн байх ёстой.

Орчны өөрчлөлтүүд

Бодлогын орчны өөрчлөлтүүдэд мэдрэмжтэй хандах нь бас чухал юм. Олон улсын аюул занал (халдлага) болон эмзэг байдлаас үүдсэн өөрчлөлт болон МТ-ийн дэд бүтцийн өөрчлөлтүүд, чухал мэдээллийн зэрэглэлийн өөрчлөлтүүд болон бусад иймэрхүү чухал өөрчлөлтүүд нь үндэсний мэдээллийн аюулгүй байдлын бодлогод тэр даруй тусгагдсан байх ёстой.

ӨӨРИЙГӨӨ ШАЛГАХ НЬ

1. Мэдээллийн аюулгүй байдлын бодлогын мөчлөг тус бүр нэг нэгэндээ хэрхэн нөлөөлж байна вэ? Та энэ үеүүдийг алгасч болох уу? Яагаад болно, яагаад болохгүй?

2. Яагаад мэдээллийн аюулгүй байдлын бодлогын боловсруулалт ба хэрэгжилтэд өөр өөр салбаруудын хамтын ажиллагаа чухал вэ?

ХАВСРАЛТУУД

Нэмэлт материал

Butt, Danny, ed. 2005. Internet Governance: Asia-Pacific Perspectives. Bangkok: UNDPAPDIP. http://www.apdip.net/publications/ict4d/igovperspectives.pdf.

CERT. CSIRT FAQ. Carnegie Mellon University. http://www.cert.org/csirts/csirt _faq.html.

CERT. Security of the Internet. Carnegie Mellon University. http://www.cert. org/encyc_article/tocencyc.html.

Dorey, Paul and Simon Perry, ed. 2006. The PSG Vision for ENISA. Permanent Stakeholders Group. http://www.enisa.europa.eu/doc/pdf/news/psgvisionfor enisafinaladoptedmay2006version.pdf.

ESCAP. Module 3: Cyber Crime and Security. http://www.unescap. org/icstd/POLICY/publications/internet-use-for-business-development/module3-sources.asp.

Europa. Strategy for a secure information society (2006 communication). European Commission. http://europa.eu/scadplus/leg/en/lvb/l24153a.htm.

Information and Privacy Office. 2001. Privacy Impact Assessment: A User"s Guide. Ontario: Management Board Secretariat. http://www.accessandprivacy.gov.on.ca /english/pia/pia1.pdf.

Information Security Policy Council. The First National Strategy on Information Security. 2 February 2006. http://www.nisc.go.jp/eng/pdf/national _strategy_001_eng.pdf.

ISO. ISO/IEC27001:2005. http://www.iso.org/iso/iso_catalogue/catalogue_tc /catalogue_detail.htm?csnumber=42103.

ITU and UNCTAD. 2007. Challenges to building a safe and secure Information Society. In World Information Society Report 2007, 82-101. Geneva: ITU. http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/report.html.

ITU-D Applications and Cybersecurity Division. ITU National Cybersecurity / CIIP Self-Assessment Tool. ITU. http://www.itu.int/ITU-D/cyb/cybersecurity /projects/readiness.html.

Killcrece, Georgia. 2004. Steps for Creating National CSIRTs. Pittsburgh: Carnegie Mellon University. http://www.cert.org/archive/pdf /NationalCSIRTs.pdf.

Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek. 2003. Organizational Models for Computer Security Incident Response Teams (CSIRTs). Pittsburgh: Carnegie Mellon University. http://www.cert.org/archive /pdf/03hb001.pdf.

OECD. 2002. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Paris: OECD. http://www.oecd.org /dataoecd/16/22 /15582260.pdf.

OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186 _1_1_1_1,00.html.

Shimeall, Tim and Phil Williams. 2002. Models of Information Security Trend Analysis. Pittsburgh: CERT Analysis Center. http://citeseerx.ist.psu.edu /viewdoc/summary? doi=10.1.1.11.8034.

The White House. 2003. The National Strategy to Secure Cyberspace. Washington, D.C.: The White House. http://www.whitehouse.gov/pcipb.

СУРГАГЧ БАГШИД ЗОРИУЛСАН ЗӨВЛӨМЖ

“Цуврал модулийн тухай” гэсэн бүлэг дээр дурдсанчлан энэхүү модуль нь олон төрлийн уншигч, суралцагч нарт, өөрчлөгдөж буй өөр өөр нөхцөл байдалд ч өөрийн гэсэн үр дүнгээ өгөхүйц байх зорилготой билээ. Модулийг мөн бүрнээр нь болон хэсэгчлэн, онлайн болон оффлайн байдлаар ч хэрэглэж болохуйцаар бүтээсэн. Сургалтын үргэлжлэх хугацаа нь модулийн агуулгаас хэр хэмжээнд ашиглан, заахыг тодорхойлох юм.

Эдгээр “зөвлөмжүүд” нь сургагч нарт энэхүү модулийг хэрхэн үр дүнтэйгээр цааш заах талаар нь зарим нэгэн санаа, зөвлөмжийг өгч буй.

Сургалтын хандлага, стратегийн талаарх цаашдын зааварчилгааг энэхүү Төрийн албан хаагчдад зориулсан МХХТ-ийн суурь мэдлэгийн академ хэмээх матераилын дагалдах сургалтын гарын авлага дээр илүү тодорхой өгсөн болно. Энэхүү гарын авлагыг доорх хаягаар үзэж болно: http://www.unapcict.org /academy

Хичээлийн бүтэц

90 минутын сургалт

Мэдээллийн аюулгүй байдал болон нууцлал хамгаалалтын талаархи олон улсын стандарт, үзэл баримтлалууд болон үндсэн ойлголтуудыг олгоно. (Модулийн 1 ба 5-р хэсэг). Stress the need for appropriate and effective information security and privacy protection policy.

3 цагийн сургалт

Хоёр хэсгээс бүрдэнэ. Эхний хэсэгт, мэдээллийн аюулгүй байдлын үндсэн ойлголт болон чиг хандлагын талаар заана. Мөн мэдээллийн аюулгүй байдалд учирч болох аюул заналын чиг хандлага орно. (2-р бүлэг). Хоёр дахь хэсэгт, мэдээллийн нууцлал хамгаалалтын тухай ойлголт болон зарчмын талаар, нууцлал хамгаалалтанд нөлөөлөх асуудлуудын талаар, мөн нууцлал хамгаалалтанд нөлөөлөх нөлөөллийн үнэлгээний талаар товчхон тайлбарлах болно.

Бүтэн өдрийн сургалт (6 цаг)

Мэдээллийн аюуогүй байдал болон нууцлал хамгаалалтын гол ойлголтууд болон зарчмын талаар тайлбарласаны дараа МАБ-ын бодлого боловсруулах болон хэрэгжүүлэх асуудалд анхаарлаа хандуулна. (7-р бүлэг)

МАБ болон мэдээллийн нууцлал хамгаалалтын бодлогын учир холбогдлын талаар сургалтанд оролцогчдоос асуулт асуух байдлаар хичээлээ эхлэх нь зүйтэй. Үүний дараа бодлогын нэр томъчонуудыг боловсруулах үйл ажиллагааны талаар хэлэлцэхээсээ өмнө МАБ-ын бодлогын хэрэгжилтийн хугацааны талаар товч танилцуулах хэрэгтэй. МАБ-ын бодлого боловсруулсан орнуудаас оролцож байгаа оролцогчдын хувьд тэднээс зарим нэг бодлогын холбогдолтой зүйлс асууж, түүний хариултыг МАБ-ын бодлогогүй орны оролцогчид сонсох байдлаар ажиллах нь зүйтэй.
(7.2-р хэсгийн төгсгөлд байгаа суралцах үйл ажиллагаа хэсгийг харна уу).

Хоёр өдрийн сургалт

Эхний өдрийн сургалт дээр дурдсан байдлаар хийгдэнэ. Хоёр дахь өдрийн сургалт нь МАБ-ын үйл ажиллагаа болон аргачлал (3 ба 4-р бүлэг), тэр тусмаа КАБЗХҮБ /CSIRT/-ыг байгуулах (6-р бүлэг)-д илүүтэй чиглэгдэх болно. Бусад орны жишээг дурдаж болох ба оролцогчдоос КАБЗХҮБ-ын хамгийн тохиромжтой загварыг тодорхойлох мөн аюулгүй байдлыг хангах тодорхой 1 механизмыг өөрийн орны нөхцөлд нийцүүлэн гаргаж ирэхийг хүсэх нь илүү үр дүнтэй болно.

Хамтран суралцах

Энд оролцогчидтой хамтран ажиллах байдлаар дадлага хийх замаар ажиллах нь зүйтэй. Энэ модулаар маш олон хэрэгцээт мэдээлэл олгох боловч оролцогчид энэ мэдээллээс хаана хэрхэн үр ашигтай ашиглаж чадахыгаа мэдэж авах нь чухал юм. Энэ модулд зарим кейс судалгаанууд орсон ба үүнийг МАБ-ын үзэл баримтлал, зарчим талаас нь судалж үзэх боломжтой. Гэхдээ, оролцогчид өөрийн орны МАБ-ын нөхцөл байдалд илүүтэй тусгаж авч ойлгох нь зүйтэй.

БНСУ-ЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН АГЕНТЛАГ (KISA)-ЫН ТУХАЙ

БНСУ-ын Мэдээллийн Аюулгүй байдлын Агентлаг (KISA) нь мэдээллийн аюулгүй байдлыг сайжруулахад чиглэгдсэн бодлого боловсруулалтыг дэмжих зорилготойгоор Засгийн газрын үндэсний хэмжээний төв хэлбэрээр 1996 онд байгуулагдсан.

Түүний үүрэг нь интернетийн орчин дахь зөрчил, СПАМ, мэдээллийн нууцлал хамгаалалт, цахим гарын үсэг, тусгай дэд бүтцийн хамгаалалт, мэдээллийн аюулгүй байдлын бүтээгдэхүүний үнэлэлт дүгнэлт болон дэмжлэг туслалцаа, бодлого төлөвлөлт болон технологи хөгжүүлэлт, найдвартай бөгөөд аюулгүй мэдээлэлжсэн нийгэм багуулах тухай мэдлэг дээшлүүлэх зэрэг болно.

UN-APCICT- НҮБ-ын Хөгжлийн төлөөх МХХТ-ын Ази, Номхон далайн бүсийн төв

НҮБ-ын Хөгжлийн төлөөх МХХТ-ын Ази, Номхон далайн бүсийн төв нь (UN-APCICT) НҮБ-ын Ази, Номхон далайн бүсийн эдийн засаг, нийгмийн хорооны (ESCAP) салбар юм. UN-APCICT-ийн зорилго нь хүний, институтын чадавхи бүрдүүлэх, улмаар нийгэм эдийн засгийн хөгжилд МХХТ-ыг ашиглах зорилгоор хорооны гишүүн улсуудын хүчин чармайлтыг нэмэгдүүлэхэд оршдог ба дараах гурван гол багана дээр тулгуурладаг:

1. Сургалт. Бодлого боловсруулагч болон МХХТ-ын мэргэжилтнүүдийн МХХТ-ын мэдлэг, ур чадварыг бэхжүүлэх, МХХТ-ын сургагчид, институтуудын чадавхийг сайжруулах;
2. Судалгаа. МХХТ-ын хүний нөөцтэй холбоотой аналитик судалгааг явуулах;
3. Зөвлөгөө. Ази, Номхон далайн бүсийн эдийн засаг, нийгмийн хорооны гишүүн болон холбогдох гишүүдэд хүний нөөцийн хөгжлийн хөтөлбөрт зөвлөгөө өгөх.

UN-APCICT нь БНСУ-ын Инчеон хотод байрладаг.

http://www.unapcict.org

ESCAP- АНДБ-ийн Эдийн засаг, Нийгмийн Хамтын Ажиллагааны байгууллага

ESCAP бол НҮБ-ын бүс нутгийн хөгжлийн төв бөгөөд Ази, Номхон далайн бүсийн НҮБ-ын эдийн засаг, нийгмийн хөгжлийн төв нь болж явдаг. Зорилго нь 53 гишүүн, 9 холбогдох гишүүдийн хоорондын хамтын ажиллагааг нэмэгдүүлэх. Тус байгууллага нь глобал, олон улсын түвшний хөтөлбөрүүд болон асуудлуудын хоорондын стратегийг холбох гүүр болон ажилладаг. Энэ нь бүс нутаг дахь засгийн газруудад глобалчлагдаж буй дэлхийд бүс нутгийн давтагдашгүй нийгэм-эдийн засгийн сорилтуудтай тулгарахад өөрийн байр сууриа хадгалж үлдэх, бүс нутгийн хандлагаар тусламж үзүүлдэхэд оршино.
Төв нь Тайландын Бангкок хотод байрладаг.

http://www.unescap.org

ТӨРИЙН АЛБАН ХААГЧДАД ЗОРИУЛСАН МХТ-ИЙН СУУРЬ МЭДЛЭГИЙН АКАДЕМИ

http://www.unapcict.org/academy

Сургалт нь 8 модультай бөгөөд хөгжлийн төлөөх МХХТ-ын өргөн хүрээний сургалтын хөтөлбөр болж, гол зорилго нь бодлого боловсруулагчдыг чухал шаардлагатай мэдлэг, ур чадвараар хангаснаар үндэсний хөгжлийн зорилгуудад хүрэх, тоон хуваагдлыг арилгахын тулд МХТ-ын боломжуудыг хөшүүрэг болгон ашиглах явдал юм.

Модуль 1- МХХТ-ийн хэрэглээ болон бодит хөгжлийн харилцан хамаарал

МХЗ-уудыг хангахын тулд МХХТ-г хэрэглэхэд бодлогоос хэрэгжүүлэлт хүртэл гол асуудлууд болон шийдвэрийн санаанууудыг онцлон тэмдэглэсэн.

Модуль 2- Хөгжлийн бодлого, үйл явц, засаглалд зориулсан МХХТ

Хөгжлийн төлөөх МХТ-ын бодлого боловсруулах, засаглал дээр төвлөрөн хөгжлийг дэмжих үндэсний бодлого, стратегууд, үндсэн бүтцүүдийн талаар чухал мэдээлэл олгоно.

Модуль 3- Цахим засгийн хэрэглээнүүд

Цахим засгийн ойлголтууд, зарчмууд, хэрэглээний төрлүүдийг тайлбарладаг. Энэ нь мөн хэрхэн засгийн газрын систем бий болсон болон зохиомжийн асуудлуудыг тодорхойлдог.

Модуль 4- Төрийн албан хаагчдад МХХТ-ийн хөгжлийн чиг хандлагуудыг танилцуулах нь

МХХТ-ын одоогийн чиг хандлага, ирээдүйн чиглэлд гүнзгий ойлголт өгөх. Энэ мөн ХМХТ-ын шийдвэр гаргахад гол техникийн болон бодлогын асуудлыг авч үздэг.

Модуль 5- Интернэтийн засаглал

Интернэтийн хэрэглээ, үйл ажиллагааг зохицуулах олон улсын бодлогууд болон процессуудыг одоогийн үргэлжилж буй хөгжлийг авч үздэг.

Модуль 6- Сүлжээ, мэдээллийн аюулгүй байдал, нууцлал

Мэдээллийн аюулгүй байдлын асуудлууд, чиг хандлагууд, мэдээллийн аюулгүй байдлын стратеги боловсруулах процессуудыг авч үзнэ.

Модуль 7- МХХТ-ийн төслийн удирдлагын онол болон практик

Хөгжлийн төлөөх МХХТ-той холбоотой төслийн удирдлагын үзэл баримтлалуудыг тайлбарлах, түүн дотроо аргууд, үйл явцууд, нийтлэг хэрэглэгддэг төслийн удирдлагын зарчмуудыг авч үзнэ.

Модуль 8- Хөгжлийн төлөөх МХХТ-ийн санхүүжилтийн хувилбарууд

Хөгжлийн төлөөх МХХТ-д болон цахим засгийн төслүүдэд зориулсан санхүүжилтийн сонголтуудыг эрж хайх. Төр-хувийн хэвшлийн түншлэл нь хөгжиж буй орнуудын хамгийн хэрэгтэй санхүүжилт гэж онцлон тэмдэглэгддэг.

Эдгээр модулиуд нь Академийн хамтрагчдийн кейс судалгааны дагуу өөр өөр улс орны бодлого боловсруулагчдын шаардлагатай нийцэх, түүнтэй хамааралтай байх зорилгоор шинэчлэн сайжруулагдсан. Модулиуд нь тухайн улс орны хэл дээр орчуулагдана. Цаашлаад, эдгээр модулиуд нь бодлого боловсруулагчидтай тэдний хамааралтай байдлыг хангах зорилгоор тогтмол шинэчлэгдэж, шинэ модулиудыг 21-р зуунд зориулсан МХХТ-иудыг үндэслэн боловсруулна.

Виртуал Академи (AVA – http://ava.unapcict.org)

- Академид зориулсан онлайн зайн сургалтын орчин
- Бүх Академийн модулууд түүн дотроо виртуал лекцүүд, слайдууд болон жишээнүүдэд онлайнаар хандах боломжтой
- Суралцагчдыг өөрсдийн байгаа газраасаа суралцах боломжийг нээж өгсөн

Цахим хамтын ажиллагааны төв (e-Co Hub – http://www.unapcict.org/ecohub)

- Хөгжлийн төлөөх МХХТ-ын мэдлэг хуваалцах, нөөц материалуудын портал
- Модулаар нөөцүүдэд хялбар хандах боломжийг олгодог
- Хэрэглэгчид онлайн хэлэлцүүлэгт оролцож, e-Co Hub-ийн онлайн бүлгийн гишүүн болж, хөгжлийн тлөөх МХХТ-ын мэдлэгээ нэмэгдүүлэх, хуваалцах боломжтой.

AVA болон e-Co Hub-дахь үйлчилгээг авах сонирхолтой байвал доорхи хаягаар бүртгүүлнэ үү.
http://www.unapcict.org/join_form