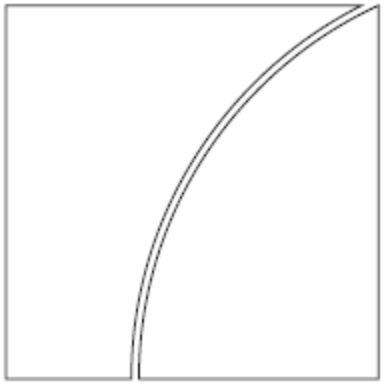
ТӨЛБӨРИЙН БОЛОН
ЗАХ ЗЭЭЛИЙН ДЭД БҮТЦИЙН
ХОРОО



САНХҮҮГИЙН ЗАХ ЗЭЭЛИЙН
ДЭД БҮТЦИЙН
ЦАХИМ АЮУЛГҮЙ БАЙДАЛ

2014 оны 11 дүгээр сар

ОЛОН УЛСЫН ТӨЛБӨР ТООЦООНЫ БАНК

Энэхүү баримт бичгийг ОУТТБ-ны цахим хуудаснаас авч болно (www.bis.org).

ISBN 92-9131-988-6 (хэвлэмэл)

ISBN 92-9131-989-3 (цахим)

Агуулга

1. Оршил

Санхүүгийн системд хийгдэж буй цахим халдлагууд нь байнга давтагдаж, илүү нарийн төвөгтэй болохын зэрэгцээ өргөн хүрээг хамрах болсон. Санхүүгийн зах зээлийн дэд бүтэц (СЗЗДБ) нь санхүүгийн системийн тогтвортой байдлыг дэмжихэд чухал үүрэг гүйцэтгэдэг учраас Төлбөрийн болон зах зээлийн дэд бүтцийн хороо (ТЗЗДБХ) нь СЗЗДБ-д тулгарч буй цахим халдлагын эрсдэл болон халдлага болсон үед үр дүнтэй арга хэмжээ авах бэлэн байдлын түвшинг тогтоохоор ажиллаж байна.

ТЗЗДБХ-ноос СЗЗДБ дэх цахим халдлагын асуудал болон Санхүүгийн зах зээлийн дэд бүтцийн зарчмууд (СЗЗДБЗ)-ын хүрээнд хийгдэх хяналт шалгалтын хоорондын хамаарлыг судлах зорилго бүхий ажлын хэсэг байгуулсан байна.

СЗЗДБ, түүний гишүүд, үйлчилгээ үзүүлэгчид болон бусад холбогдох талуудаас мэдээлэл цуглуулах зорилгоор ажлын хэсгийн гишүүд нь уулзалт, ярилцлагыг зохион байгуулсан. Энэ нь цахим халдлагатай холбоотойгоор СЗЗДБ-ийн чадвар, хэтийн төлвийг илүү сайн ойлгоход чиглэсэн бөгөөд ажлын хэсгээс дараах дүгнэлтийг гаргасан: 1. СЗЗДБ-ийн хувьд цахим аюулгүй байдал нь аажмаар анхаарал татсан томоохон асуудал болж байна. 2. СЗЗДБ нь өөрийн систем дэх цахим халдлагын аюулын улмаас өргөн хүрээг хамарсан санхүүгийн тогтвортой байдалд нөлөөлж болзошгүй эрсдэлүүдэд анхаарлаа хандуулах болсон. 3. СЗЗДБ нь маш том хэмжээний цахим халдлагын үед 2 цагийн дотор системийг хэвийн байдалд оруулах ёстой (2ц-ССЗ) гэсэн зарчмыг хэрэгжүүлэхэд хүндрэлтэй гэж байгаа ч (энэ зорилтод хүрэхийн тулд хэдэн жил ч зарцуулж магадгүй) зарим нь энэ системийг сэргээх цагийг бууруулах хэд хэдэн боломжит шийдэл байх боломжтой гэж үзэж байна. 4. СЗЗДБ нь үр дүнтэй шийдэл олохын тулд зохицуулагч байгууллагатай харилцан уялдаатай ажиллаж, дэмжлэг үзүүлэхэд бэлэн байна.

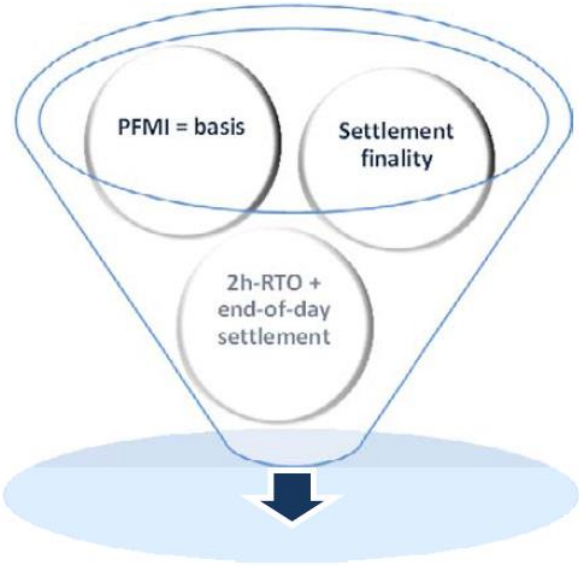
Үүнээс гадна хэдийгээр СЗЗДБ-ийн удирдлагууд цахим аюулгүй байдалд анхаарлаа түлхүү хандуулж байгаа ч ихэнх салбарын манлайлагчдын зүгээс санхүүгийн салбарт тулгарч буй халдлагууд ихсэж байгаа тул богино хугацаанд системийг сэргээхэд илүү анхаарал хандуулах нь зүйтэй гэж үзэж байна. Энэхүү баримт бичиг нь цахим аюулгүй байдлыг хангах зорилгоор СЗЗДБ-ийн авч хэрэгжүүлж буй арга хэмжээ, үзэл баримтлалыг тодорхойлохын зэрэгцээ СЗЗДБ-ийн цахим аюулгүй байдлыг сайжруулах замаар санхүүгийн тогтвортой байдлыг бэхжүүлэхэд шаардлагатай үндэс суурийг бий болгох зорилготой юм.

Энэ тайланд СЗЗДБ нь өөрийн үйл ажиллагааг богино хугацаанд сэргээх ёстой, ноцтой байдал үүссэн үед өдрийн эцэс гэхэд төлбөр тооцоог эцэслэх ёстой гэсэн гол нөхцөлүүдийг удирдлага болгосон. СЗЗДБ-ийн цахим аюулгүй байдлын төлөв, ажлын хэсгээс гаргасан СЗЗДБ-үүдийн салбарын хандлагыг авч үзсэний үндсэн дээр эрх бүхий байгууллагууд нь

харилцан уялдаатай арга хэмжээ, боломжит зөвлөмж зэргийг СЗЗДБЗ-ын Зарчим 17-д нэмж тусгаж болно гэж дүгнэсэн.

2. Ерөнхий ойлголтууд

Энэхүү тайланд дараах 3 үндсэн ойлголтыг ашигласан. 1. СЗЗДБЗ нь уг судалгаа шинжилгээний үндэс болно. 2. Төлбөр тооцоог эцэслэхэд ямар нэг байдлаар нөлөөлөхгүй байна. 3. Зарчим 17-д заасан 2ц-ССЗ болон өдрийн эцэст төлбөр тооцоо бүрэн хийгдэх ёстой гэсэн шаардлагуудыг хангах ёстой.



2.1 СЗЗДБЗ энэ судалгааны үндэс болох нь

СЗЗДБЗ-ыг ТЗЗДБХ болон Үнэт цаасны хороодын олон улсын байгууллагын Техникийн зөвлөлөөс боловсруулсан бөгөөд Системийн хувьд нэн чухал төлбөрийн систем (SIPS), Үнэт цаасны төлбөр тооцооны систем (SSS), Үнэт цаасны төвлөрсөн хадгаламж (CSD), Арилжааны клирингийн төв (CCP) болон Арилжааны мэдээллийн сан (TR) зэрэг санхүүгийн зах зээлийн дэд бүтцүүдэд зориулсан олон улсын стандарт юм. СЗЗДБЗ-ын гол зорилго бол санхүүгийн зах зээлийн дэд бүтцүүд нь санхүүгийн системийн тогтвортой, үр ашигтай байдлыг дэмжиж ажиллах явдал юм. Олон улс орон эдгээр зарчмуудыг хэрэгжүүлж эхлээд байна. Зарчим 3-т хууль, эрх зүйн, зээлийн, төлбөр түргэн гүйцэтгэх чадварын, үйл ажиллагааны болон бусад эрсдэлүүдийг удирдахад зориулсан эрсдэлийн удирдлагын нэгдсэн тогтолцоотой байх талаар тусгасан. Үйл ажиллагааны эрсдэл болон удирдлага, зохион байгуулалтыг харгалзан Зарчим 17 болон Зарчим 2-т илүү тодорхой тусгасан бөгөөд цахим эрсдэл нь энэ хүрээнд хамаарна. СЗЗДБ-ийн цахим аюулгүй байдалтай холбоотой асуудал болон зөвлөмжүүдийг СЗЗДБЗ-ын хүрээнд шийдвэрлэх нь зүйтэй юм.

СЗЗДБЗ-д заасны дагуу цахим эрсдэлийн удирдлагын наад захын шаардлагуудыг СЗЗДБ-ийн төрлөөс хамаарч өөр өөрөөр тогтоох шаардлагагүй юм. Харин СЗЗДБ-ийн тодорхой төрөл

болон/эсвэл цахим халдлагын санхүүгийн системд үзүүлэх нөлөөнөөс хамаарч, дараах хүчин зүйлсийг харгалзан үзсэний үндсэн дээр дээрх шаардлагуудыг биелүүлэх тодорхой арга барил буюу хэрэгслийг сонгож болно. Үүнд:

1. СЗЗДБ нь өөр газраас олох боломжгүй мэдээллийг хадгалж байгаа эсвэл мэдээлэл алдагдсан тохиолдолд эзэмшилтэй холбоотой том хэмжээний асуудал үүсгэж болохуйц эзэмших эрхийг бүртгэдэг эсэх (CSD болон TR г.м);
2. Тухайн СЗЗДБ-ийн гүйлгээний хэмжээ, түүний оролцогчдын тоо болон хэмжээнээс шууд хамааралтайгаар санхүүгийн системд учруулж болох саатал, хямралын цар хүрээ;
3. СЗЗДБ нь өөрийн салбарт (бараг) монополь болж, тухайн үйлчилгээг үзүүлэх цорын ганц сонголт болсон эсэх.

2.2 Төлбөр тооцоог эцэслэх

Төлбөр тооцоог хэзээ эцсийн гэж үзэхийг хуулиар тодорхойлсон байна. Өөрөөр хэлбэл энэ нь гэрээний нөхцөлийн дагуу СЗЗДБ эсвэл түүний оролцогчид нь эргэлт буцалтгүй, маргаангүйгээр хөрөнгө буюу санхүүгийн хэрэгслийг шилжүүлэх, эсвэл үүргээ биелүүлэх явдал юм.

Төлбөр тооцоог эцэслэх нь санхүүгийн системийн тогтвортой байдалд чухал нөлөөтэй. Зээлийн, төлбөр түргэн гүйцэтгэх чадварын болон хууль, эрх зүйн эрсдэлүүд нь төлбөр тооцоог эцэслэх зарчмын дагуу төлбөрийн болон үнэт цаасны гүйлгээнд оролцогч талуудад хамаарна. Эцсийн гэж үзсэн гүйлгээ эцсийн байх болно гэсэн итгэлээс санхүүгийн байгууллагууд болон тэдгээрийн үйлчлүүлэгчдийн төлбөр түргэн гүйцэтгэх чадвар хамаардаг. Том хэмжээний цахим халдлагаас шалтгаалан буруу тоо баримт гарч болох ч тухайн гүйлгээнүүдийн эцсийн байх баталгаа нь санхүүгийн тогтвортой байдлыг хадгалахад чухал үүрэгтэй юм.

Хэрэв хүлээн авагчийн эзэмших эрхгүй нь баталгаатай тогтоогдож, төлбөрийн даалгавар буцаагдан, тухайн хүчингүй болсон эсвэл зөвшөөрөгдөөгүй гүйлгээ нь үр дүнгийн тооцоололд нөлөөлөх тохиолдолд системээр хийгдсэн анхны үр дүнгийн тооцоололд өөрчлөлт оруулалгүй, хэвээрээ үлдэх ёстой гэж ажлын хэсэг шийдвэрлэсэн.

2.3. 2ц-ССЗ зорилт нь цахим аюулгүй байдалд хамааралтай

СЗЗДБ нь дотоодын болон олон улсын санхүүгийн тогтвортой байдалд чухал нөлөө үзүүлдэг тул СЗЗДБЗ нь СЗЗДБ-ээс үйл ажиллагааны тасралтгүй байдлыг ханган ажиллах, өргөн хүрээг хамарсан эсвэл том хэмжээний саатал үүсгэж болох тохиолдлуудыг тусгасан онцгой байдлын төлөвлөгөөтэй байхыг шаарддаг. Хэдийгээр СЗЗДБЗ-ын зарим хэсгүүдэд биет халдлагын үед системийг сэргээх талаар бичсэн байдаг ч цахим халдлага болсон үед гол

үйлчилгээнүүдийг богино хугацаанд сэргээх нь мөн адил чухал юм. Иймээс үйл ажиллагааны эрсдэлийн талаар заасан Зарчим 17 нь цахим аюулгүй байдлыг агуулсан гэж үзэж болно.

СЗЗДБЗ Зарчим 17: СЗЗДБ нь үйл ажиллагааны эрсдэлийн дотоод болон гадаад боломжит хүчин зүйлсийг тодорхойлж, оновчтой бодлого, систем, хяналтын механизмаар дамжуулан тэдгээрийн үйл ажиллагаанд үзүүлж болох үр дагаврыг бууруулах хэрэгтэй. Системүүд нь нууцлал, үйл ажиллагааны найдвартай байдлыг өндөр түвшинд хангахаар төлөвлөгдсөн байхын зэрэгцээ ачаалал даах, өргөтгөх хангалттай хүчин чадалтай байх шаардлагатай. Тасралтгүй ажиллагааг хангах төлөвлөгөө нь үйл ажиллагааг богино хугацаанд сэргээн, өргөн хүрээг хамарсан, том хэмжээний саатал болсон үед ч үүргээ биелүүлэн ажиллахад чиглэгдсэн байх ёстой.
СЗЗДБЗ Зарчим 17, Гол асуудал 6: Тасралтгүй ажиллагааг хангах төлөвлөгөөнд онцгой байдал үүссэн үед мэдээллийн технологийн гол системүүдийн үйл ажиллагааг 2 цагийн дотор хэвийн байдалд оруулах талаар тусгах шаардлагатай. Түүнчлэн уг төлөвлөгөө нь хичнээн ноцтой байдал үүссэн ч төлбөр тооцоог тухайн өдөрт нь багтаан хийх боломжоор хангасан байна.
СЗЗДБЗ Зарчим 17, Тайлбар тэмдэглэгээ 3.17.13: Тасралтгүй ажиллагааг хангах төлөвлөгөөнд гол зорилгуудыг тодорхой тусгахын зэрэгцээ өргөн хүрээг хамарсан, том хэмжээний ослын үед эсвэл онцгой байдал үүсэх үед нэн чухал үйл ажиллагааг цаг алдалгүй сэргээн, хэвийн байдалд оруулах бодлого, журмыг багтаасан байх ёстой.

СЗЗДБ-үүд нь ноцтой цахим халдлагын үед 2ц-ССЗ-д хүрэхэд хүндрэлтэй хэдий ч удирдлагын зүгээс уг зарчмыг ойлгож, дэмжих ёстой. Энэхүү баримт бичгийн 4 дүгээр хэсэгт сэргээх хугацааг богиносгоход нэмэр болох зарим СЗЗДБ-ийн туршлага, дэлгэрэнгүй мэдээллийг тусгасан.

Мөн 2ц-ССЗ нь цахим аюулгүй байдлын бусад хүчин зүйлсэд нөлөөлөх боломжтойг энд тэмдэглэх нь зүйтэй юм. Жишээ нь, зарим тохиолдолд 2ц-ССЗ-д хүрэхийн тулд цуглуулсан нотлох баримтын бүрэн бүтэн байдлыг ханган, хуулийн хүрээнд ашиглах зорилгоор хийдэг шүүхийн шинжилгээ /forensic analysis/-г хялбаршуулж эсвэл иж бүрнээр хийхгүй байж болно. Учир нь уг шинжилгээг хийхийн тулд системийг урт хугацаагаар зогсоох шаардлагатай болдог. Шүүхийн ийм шинжилгээг хойшлуулж болох ч, дараа нь шаардлагатай орчинг бүрдүүлэн, заавал хийх ёстой.

3. Яагаад цахим эрсдэлийг онцгойлон үзэж байна вэ?

СЗЗДБ-д тулгарч буй үндсэн эрсдэлийн нэг тул үйл ажиллагааны эрсдэлийг СЗЗДБЗ-д тодорхойлж өгсөн байдаг. Цахим эрсдэл нь харьцангуй шинэ, нарийн төвөгтэй, маш хурдан өөрчлөгдөн шинэчлэгдэж буй ойлголт учир үүнийг удирдаж, зохицуулахад маш хэцүү. Цахим халдлага нь 3-дагч этгээдээс системд хор хөнөөл учруулан, санхүүгийн алдагдал үүсгэх зорилгоор, санаатайгаар хийх хор хөнөөлтэй үйл ажиллагааны хэлбэртэй байж болно. Энэ тохиолдолд уг халдлагын цар хүрээг тогтоон, засаж залруулан, сэргээхэд маш хэцүү байх магадлалтай. Цахим эрсдэлийн тааварлашгүй байдлаас шалтгаалж, нэн даруй түүнийг удирдан зохицуулах, зохистой шийдэлд хүрэх шаардлагатай болж байна.

Сүүлийн жилүүдэд цахим халдлага нь СЗЗДБ дэх системийн эрсдэлийг хурдацтайгаар ихэсгэж байна. Энэ нь хэд хэдэн шалтгаантай: 1. Санхүүгийн үйлчилгээнд техник технологийн үзүүлэх үүрэг ихэссэн. 2. Санхүүгийн зах зээл дээрх операторуудын харилцаа холбоо, хамаарал маш өндөр болохын зэрэгцээ улам бүр нэмэгдсээр байна. 3. Халдлага үйлдэгч болон тэдгээрийн санаа сэдэл олон төрөл болж, урьдчилан таамаглаагүй эх үүсвэрүүдээс халдлага үйлдэх нь ихсэж байна. Халдлага үйлдэгч гэдэгт үйл ажиллагааг сүйтгэх зорилготой “хактивист”-ууд, санхүүгийн ашиг олох зорилготой цахим гэмт хэрэгтнүүд, улс төрийн болон санхүүгийн тогтворгүй байдал үүсгэх зорилготой террористууд, нууц мэдээллийг өөрчлөх эсвэл олж авах, системийн тогтворгүй байдал үүсгэх зорилготой үндэсний аюулгүй байдалд халдагчдыг хамааруулна. СЗЗДБ-үүдийн цахим аюулгүй байдлыг хангахад тулгарч буй хамгийн том асуудал бол саатлыг арилгах, үр дүнтэй хамгаалалтын арга техникүүдийг нэвтрүүлэх, хамтын ажиллагааны тусламжтайгаар асуудлыг шийдвэрлэх зэргээр халдлагын нарийн төвөгтэй байдал болон харилцан уялдааг удирдан зохицуулах явдал юм.

Түүнээс гадна халдлага үйлдэгчид нь илүү нарийн аргуудыг түлхүү хэрэглэж байна. Жишээ нь, сүүлийн жилүүдэд дэвшилтэт байнгын халдлага (APT-advanced persistent threat) гэх халдлагын шинэ төрлийн арга гарч, шинэчлэгдэж эхэлсэн. Үүний зэрэгцээ бизнесийн хамтрагч нар, нийлүүлж буй бүтээгдэхүүнүүд, ажилтнуудын компьютерууд, ажилтнууд гэх мэт СЗЗДБ рүү довтолж болох эхлэлийн цэгүүд улам ихэссэн. Нийгмийн инженерчлэл (social engineering) ашиглах буюу хүмүүсийг хуурч мэхлэх аргаар Мэдээллийн систем рүү хортой програмуудыг оруулж байна (өөрөөр хэлбэл, чиглэсэн-фишинг).

Цахим халдлагууд нь түвшин, зорилго, хамрах хүрээ зэргээсээ шалтгаалан СЗЗДБ-үүдийн үйл ажиллагааны эрсдэлийн удирдлагын тогтолцоонд томоохон сорилт болж байдаг. Зарим тохиолдолд биет халдлагын үед хэрэглэгдэх эрсдэлийн удирдлага болон үйл ажиллагааны тасралтгүй байдлыг хангах аргачлалууд нь цахим халдлагын үед үр нөлөөгүй эсвэл бүр хүндрүүлэх боломжтой. Жишээ нь, автомат нөөцлөлтийн систем нь төв оффист биет халдлага болсон үед нууц мэдээллийг хадгалж үлдэхэд хэрэгтэй байж болох ч үндсэн системийн нэгэн

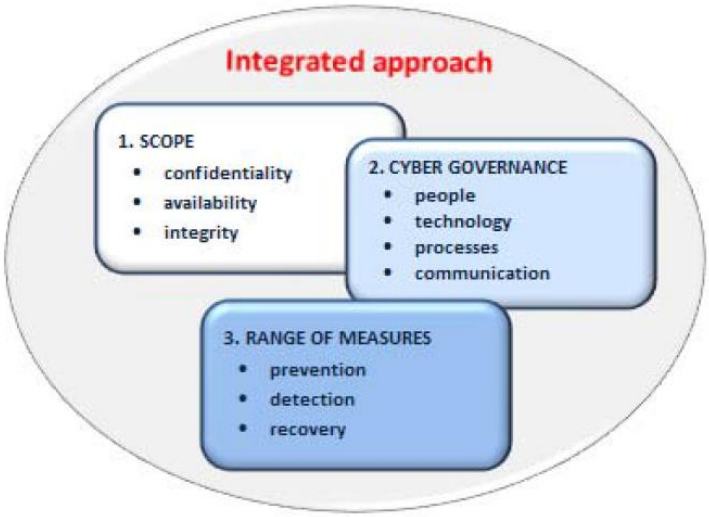
адил цахим халдлагад өртөж болох ба зарим үед хортой програмыг илүү хурдан тархахад дөхөм болж болзошгүй юм.

4. Цахим аюулгүй байдлыг хангах нэгдсэн хандлага

Цахим аюулгүй байдлыг хангах нэгдсэн хандлага гэдэг нь СЗЗДБ-ийн үйлчилгээг доод түвшинд үзүүлэх байсан ч хамаагүй үйл ажиллагааны аюулгүй байдлыг хамгаалан үлдэхийг хэлнэ. Аюулгүй байдлаа хамгаалан үлдэх чадвартай үйл ажиллагаа нь системийг бүрэн унагаалгүйгээр, халдлагын шокыг өөртөө шингээхээр төлөвлөгдсөн байна. Цахим халдлагын онцлогуудыг ойлгон, үйлчилгээг сэргээх боломжтой байхын тулд СЗЗДБ-үүд нь ихэвчлэн өөрийн боловсруулсан цахим аюулгүй байдлын загвар эсвэл илүү ерөнхий загваруудад (жишээ нь: 2014.02 сард хэвлэгдсэн NIST загвар, 2014.01 сард хэвлэгдсэн Дэлхийн эдийн засгийн форумын цахим аюулгүй байдлын хандлага, 2013 онд гарсан MITRE загвар) суурилсан нэгдсэн хандлагыг даган мөрддөг. Цахим аюулгүй байдлын загварыг гаргахад зөвлөгөө авах зорилгоор зарим тохиолдолд гадны зөвлөхүүд эсвэл аудиторуудыг хөлсөлдөг.

Хэдийгээр дээрх загварууд нь бүтэц, ангилал зэргээрээ хоорондоо ялгаатай ч, цахим аюулгүй байдлыг хангах нэгдсэн аргачлал нь дараах өргөн хүрээтэй 3 хэмжигдэхүүнийг хамардаг байна:

1. Хамрах хүрээ: СЗЗДБ-үүдийн цахим аюулгүй байдлын загвар нь нууцлал алдагдах, бүрэн бүтэн байдал алдагдах, бэлэн байдал алдагдах гэх мэт цахим халдлагаас үүсэж болох хэд хэдэн нөхцөлийг авч үздэг.
2. Цахим удирдлага: Энэхүү загвар нь СЗЗДБ-үүдийн мэдээллийн технологийн дэд бүтцээс гадна хүмүүс, процесс болон харилцаа холбоог агуулсан байдаг.
3. Арга хэрэгслүүд: СЗЗДБ нь цахим халдлагаас сэргийлэх, амжилттай болсон халдлага болон халдлага хийх оролдлогуудыг илрүүлэх, халдлага болсон үед урьдчилан тохирсон түвшинд үйлчилгээг сэргээх олон төрлийн аргуудыг үр ашигтай ашиглах нь чухал байдаг.



4.1 Хамрах хүрээ

Ерөнхийдөө, СЗЗДБ-үүдийн цахим аюулгүй байдлын загвар нь дараах 3 асуудлыг шийдвэрлэхэд чиглэдэг байна:

1. Нууцлал алдагдах - нууц мэдээлэл хулгайлагдах
2. Бэлэн байдал алдагдах - систем өөрөө хэвийн байх боловч СЗЗДБ-ийн үзүүлж буй үйлчилгээ рүү зөвшөөрөгдсөн хэрэглэгчид хандах боломжгүй эсвэл ашиглах боломжгүй болох (жишээ нь, СЗЗДБ, түүний оролцогчид болон бусад байгууллагуудын холбогдох суваг ажиллагаагүй болох)
3. Бүрэн бүтэн байдал алдагдах - СЗЗДБ-ийн өгөгдөл буюу системүүд эвдэгдэн, мэдээллийн болон боловсруулалтын аргуудын үнэн зөв байдал эсвэл бүрэн байдалд нөлөөлөх (мөн үйлчилгээний бэлэн байдалд нөлөөлж болно)

Ихэнх цахим халдлагууд нууцад халдах (жишээ нь нууц мэдээлэл хулгайлах) болон системийн бэлэн байдлыг алдагдуулахад (жишээ нь ДДоС халдлага) чиглэдэг. Гэвч сүүлийн үед СЗЗДБ-ийн програм хангамж эсвэл өгөгдлийн (эсвэл аль алины) бүрэн бүтэн байдалд нөлөөлөх халдлагын эрсдэл анхаарал татах нь ихсэж байна. Ерөнхий эрсдэлийн 3 тохиолдлын СЗЗДБ-ийн үйл ажиллагаа болон санхүүгийн системд үзүүлэх нөлөөллийн хэмжээг дараах хүснэгтэд үзүүллээ.

Ингэж үзүүлэхийн гол зорилго нь өөр өөр тохиолдолд СЗЗДБ-ийн аюулгүй байдалд нөлөө үзүүлэх олон төрлийн хүндрэлийг тодорхой болгоход оршино. Биет халдлагаас сэргийлэх аргууд нь цахим халдлагын үед ижил үр дүнтэй биш байж болно. Энэ нь ялангуяа мэдээллийн бүрэн бүтэн байдалтай холбоотой үед тохиолддог.

Тохиолдол 1	Тохиолдол 2	Тохиолдол 3
Нууцлал алдагдах • Цахим халдлагын үед нууц мэдээлэл хулгайлагдана. • Үйлчилгээгээ хэвийн үзүүлж чадна. • Халдлага нь илүү өндөр түвшний дайралтын эхний шат байж болно. • Богино хугацаанд илрүүлэн, арга хэмжээ авахад хэцүү байж болно. • СЗЗДБ-ийн нэр хүндэд муугаар нөлөөлнө.	**Бэлэн байдал алдагдах** • DOS гэх мэт халдлага ашиглан үйлчилгээг ашиглах боломжгүй болгоно. • СЗЗДБ, оролцогч хоорондын харилцаа холбоо, оролцогчдод үзүүлэх тусламж, үйлчилгээний хэвийн ажиллагааны талаар СЗЗДБ-ийн өгдөг мэдээлэл, нийлүүлэгчидтэй холбогдон мэдээлэл авах, бизнесийн хамтрагчтай мэдээлэл солилцох зэрэгт нөлөөлнө. • Систем хэвийн болохгүй цаг алдах тусам оролцогчид болон санхүүгийн зах зээлд үзүүлэх гэмтэл саатлын нөлөө улам даамжирна.	**Бүрэн бүтэн байдал алдагдах** • Цахим халдлагын үед СЗЗДБ-ийн үндсэн мэдээлэл эсвэл системүүд эвдэгдэнэ. • СЗЗДБ-ийн мэдээлэл эсвэл системийн бүрэн бүтэн байдалд итгэх боломжгүй болно. • Нөөц системүүд ч мөн эвдэгдсэн байх магадлалтай. • Эхэн үедээ системүүд хэвийн ажиллаж буй мэт харагдаж болно. • Системийн ажиллагааг хэвийн горимд буцаахын тулд үйлчилгээг зогсоох эсэхийг шийдэх хэрэгтэй. • Асуудлыг илрүүлж, дүн шинжилгээ хийх хугацаа хангалттай байж болно. • Үйлчилгээг хэвийн байдалд оруулахад шаардагдах хугацаа урт байж болно. • СЗЗДБ дэх оролцогчдын байр сууринд хүртэл нөлөөлөх боломжтой тул системийн хэмжээнд сөрөг нөлөө үзүүлэх боломжтой. • Эзэмшигчийн эрх, санхүүгийн позиц зэрэгт маргаан, үл ойлголцол үүссэний улмаас санхүүгийн зах зээлд итгэх итгэлд сөргөөр нөлөөлнө. • Бусад СЗЗДБ-үүд, оролцогчид, тэдгээрийн харилцагчид болон зах зээлд төлбөр түргэн гүйцэтгэх чадварын болон зээлийн нөлөөллийг хамарсан, шаталсан үр дагавар үүсгэж болно.

4.2 Цахим удирдлага

Нэгдсэн цахим удирдлагын загвар ашигладаг СЗЗДБ-үүд цахим аюулгүй байдлыг бодитоор хангаж байна. Тэдгээр нь цахим аюулгүй байдлыг зөвхөн мэдээлэл, харилцаа холбооны технологитой холбоотой биш бөгөөд илүү өргөн хүрээг хамаарсан нөлөөлөл, хамааралтай гэж

үздэг. Удирдлагын загвар нь хүмүүс, технологи, процесс, харилцаа холбоо гэсэн 4 үндсэн хүрээг хамарна.

4.2.1 Хүмүүс

Цахим аюулгүй байдлын нууцлал ба үйл ажиллагааг сэргээх гэсэн 2 гол бүрэлдэхүүн хэсэгт СЗЗДБ-ийн үйл ажиллагааны, удирдах албаны, захирлуудын зөвлөлийн гэсэн бүх шатны ажилтнуудыг татан оролцуулна. Үр дүнтэй цахим аюулгүй байдал нь СЗЗДБ-ээс эрсдэлийн удирдлагын загвартаа цахим эрсдэлийг дэлгэрэнгүй тусгасан байхыг шаарддаг.

СЗЗДБ-ийн удирдлагын авч хэрэгжүүлж буй арга хэмжээ нь байгууллага даяар цахим аюулгүй байдлын талаарх мэдлэг, ойлголтын түвшинг нэмэгдүүлэх чухал хүчин зүйл юм. Ерөнхийдөө СЗЗДБ-үүд нь цахим эрсдэлийг зөвхөн үйл ажиллагаатай холбоотой асуудал биш, тэдний оршин тогтнох чадварт аюул занал учруулж болох бүхэл бүтэн байгууллагын хэмжээний эрсдэл гэдгийг ойлгодог. Ийм ч учраас цахим эрсдэлийн талаар авч буй арга хэмжээ, баримталж буй бодлогын үр нөлөөг тогтоох, мөн СЗЗДБ нь цахим аюулгүй байдалд хэр их анхаарал хандуулж, чухалчилж буйг тодорхойлоход дотоод аудиторууд чухал үүрэг гүйцэтгэдэг.

Зөв, хэрэгжихүйц мэдээллийн нууцлалын бодлого бүхий СЗЗДБ-үүдийн түгээмэл нэг шинж бол бүх үйл ажиллагаандаа мэдээллийн нууцлалыг хангахаас гадна үүнийг чухалчлан авч үздэг удирдлагын тогтолцоотой байх явдал юм. Нэгдсэн хандлага гэж цахим аюулгүй байдлыг ямар нэгэн нэмэлт зүйл бус, үндсэн үйл ажиллагааны нэг хэсэг гэж авч үзэхийг хэлнэ. Ийм байгууллагуудад дээд удирдлагаас эхлээд бүх түвшний ажилтнууд нь ерөнхий мэдлэгийн болон бүхий л төрлийн цахим халдлагын үед хэрхэн ажиллах талаар байнгын сургалтанд хамрагддаг. Байгууллага даяараа мэдлэгтэй, ойлголттой байх нь маш чухал. Бүх ажилтан өндөр түвшний мэдлэгтэй байснаар хохирогч нь цахим халдлага байж болзошгүй сэжигтэй тохиолдлыг мэдэгдэн, цаг тухайд нь ослын үед ажиллах, удирдах тохиромжтой үйл явцыг эхлүүлж, халдлагын хохирлыг багасгах боломжтой болно.

4.2.2 Технологи

Ерөнхийдөө халдлага үйлдэгчид нь халдлага илрүүлэх хэрэгсэлд баригдахгүйн тулд цоорхойнуудыг олж тогтоодог. Тэд цогц орчин дахь нүх сүв эсвэл дэд систем болон үйл ажиллагааны процесс хоорондын үе давхарга руу дайралт хийдэг. Мөн нууцлалын тохиргоо нь хангалттай бус програм хангамж ашиглаж байгаа тохиолдолд тэд ийм нөхцөл байдлыг ашиглана. Мэдээллийн хэрэгслээр мэдээлж байгаагаас харахад цахим халдлага үйлдэгчид нь санхүүгийн систем даяар хохирол учруулахын тулд дан ганц байгууллагын мэдээллийн технологийн дэд бүтэц дэх сул тал руу эхлээд довтолж байна. Ихэнх СЗЗДБ-үүдийн цахим засаглалд мэдээллийн технологи чухал байр суурь эзэлдэг бөгөөд урьдчилан сэргийлэх зорилгоор халдлагатай тэмцэх олон давхарга бүхий цахим аюулгүй байдлын аргуудыг

ашиглан, системээ илүү уян хатан болгохыг хичээдэг. Мэдээллийн технологийн удирдлагын аргын жишээг 4.3 дахь хэсэгт оруулав.

4.2.3 Процессууд

Удирдлагын түвшинд шийдвэр гаргах үед үйл ажиллагааны эрсдэл талаас нь цахим аюулгүй байдлыг үнэлэх хэрэгтэй (шинэ үйлчилгээ, бүтээгдэхүүн, мэдээллийн технологийн хөрөнгө оруулалт болон СЗЗДБ-ийн байгууллагын бүтэц зэргийг хамарна). Зарим СЗЗДБ-үүд үүрэг, хариуцлага зэргийг багтаасан, тодорхой, ойлгомжтой, цахим аюулгүй байдалд хамаарах процессуудыг нэвтрүүлээд байна. Эрсдэлийг хүлээн зөвшөөрөх нь ийм процесуудын нэг жишээ юм. Үйл ажиллагааны эрсдэлийн удирдлагын нэг хэсэг болохын хувьд энэ нь үйл ажиллагааны хэлтэс, дотоод аудит, мэдээллийн аюулгүй байдлын ахлах мэргэжилтэн, зөвлөл зэрэг бүх түвшний ажилтнуудын оролцоо, цахим аюулгүй байдал болон үйл ажиллагааны тасралтгүй байдлын дүн шинжилгээг багтаасан байдаг.

4.2.4 Харилцаа холбоо

СЗЗДБ-үүдийн өөрийн оролцогчид, бусад СЗЗДБ-үүд, үйлчилгээ үзүүлэгчид болон бүтээгдэхүүн нийлүүлэгч 3-дагч этгээдүүдтэй хэрхэн харилцан холбогдсоныг авч үзэхэд тэдгээрийн хоорондын харилцаа холбооны үр ашигтай сувгууд нэн чухал байдаг. Гэвч ихэвчлэн гадны орнуудад төвтэй, өргөн хүрээ хамарсан аюулгүй байдлын багийнхны дунд итгэлцэлд суурилсан харилцаа тогтооход хүндрэлтэй ба энэ нь мэдээлэл солилцоход саад болж болно. СЗЗДБ-ийн аюулгүй байдлын багууд болон түүний зуучлагчдын хоорондох итгэлцэл нь нууц мэдээлэл солилцоход зайлшгүй чухал.

Ихэнх СЗЗДБ-үүд хэвийн болон ачаалалтай үеүдэд мэдээлэл, харилцаа холбооны сувгуудын хэвийн ажиллагааг ханган ажиллахыг хичээдэг. Цахим халдлага болсон үед оролцогч талуудтай цаг алдалгүй харилцаа холбоотой байх нь үйл ажиллагааг хэвийн байдалд оруулах, халдлага цаашид улам тархахаас сэргийлэхэд нэн чухал юм.

4.3 Авах арга хэмжээний төрлүүд

Цахим аюулгүй байдлын нэгдсэн хандлагын 3 дахь хэсэг нь ихэвчлэн мэдээллийн технологийн чиглэлээр авах аюулгүй байдлын олон төрлийн арга хэмжээ байдаг. Бүх төрлийн цахим халдлагаас үр дүнтэй хамгаалах энгийн бөгөөд ид шидтэй шийдэл гэж байхгүй. Харин СЗЗДБ-үүд нь цахим аюулгүй байдлын өөр өөр төрлийн (сэргийлэх, илрүүлэх, сэргээх) арга хэрэгсэл, хэмжигдэхүүнд хөрөнгө оруулалт хийж байна. Аюулгүй байдлын хэмжигдэхүүн, арга хэрэгслүүд нь нэг дор хэд хэдэн зорилгоор ашиглагдаж болдог учир тэдгээрийг сэргийлэх, илрүүлэх, сэргээх гэж нарийн ангилах боломжгүй.

Жишээлбэл, сэргийлэх болон илрүүлэх функцыг нэгтгэх шийдэл их түгээмэл байна (жишээ нь, вирусын эсрэг програм хангамж хортой кодыг илрүүлэх, тусгаарлах үүргийг давхар гүйцэтгэдэг). Үүнтэй нэгэн адилаар сэргээх процессыг сайжруулах алхмууд нь тогтмол хяналт, үнэлэлт, шийдэлтэй (энэ нь илрүүлэх ажиллагааг сайжруулна) хослуулсан үйл явцыг ангилах ажиллагааг (энэ нь сэргийлэх ажиллагааг сайжруулна) багтаасан байж болно.

Өмнө нь цахим аюулгүй байдлын урьдчилан сэргийлэх тал дээр илүү төвлөрч, ашиглаж буй системдээ тааруулж мэдээллийн технологийн нууцлалын шийдэл, арга барилаа сонгодог байсан. Харин одоо илүү анхаарал татаж буй хяналт, илрүүлэлт, сэргээх чадвар руу хөрөнгө оруулалт хийх болж байна.

Энэхүү хөрөнгө оруулалтын шийдвэрүүд нь олон талтай. Цахим халдлагын хамрах хүрээ байнга өөрчлөгдөж байгаа ба байгууллагууд өндөр үнэтэй, нарийн төвөгтэй шийдлүүд, том хэмжээний цахим халдлага хийгдэх давтамж, магадлал өсөж байгааг харгалзан үзэх ёстой болж байна. СЗЗДБ-ийн удирдлагуудын хувьд мэдээллийн нууцлал, аюулгүй байдалд хөрөнгө оруулалт хийх шийдвэр гаргахад зарим тохиолдолд эргэлзээтэй асуудлууд гарч болно.

Зарим СЗЗДБ-үүд том хэмжээний цахим халдлагын үед 2ц-ССЗ болон өдрийн эцэст төлбөр тооцоог хийх зорилгодоо хүрэхийн тулд ойрын хугацаанд хэрэгжүүлж болох ажлууд байгааг мэдэгдсэн. Үүний тулд сэргийлэх, илрүүлэх, сэргээх зэргийг хослуулсан техникт хөрөнгө оруулах шаардлагатай. 2ц-ССЗ-ын хүрээнд эдгээр 3 элементийг нэгдсэн байдлаар авч үзэх шаардлагатай. Дараах хэсэгт цахим аюулгүй байдлыг бэхжүүлж, үйлчилгээний зогсолтын хугацааг багасган, өдрийн эцэст төлбөр тооцоог хийж дуусгах зорилгоор хэд хэдэн СЗЗДБ-үүдийн ашиглаж буй гол туршлага, ойлголтууд болон стратегийн жишээг харуулав.

4.3.1 Сэргийлэх

СЗЗДБ-үүд нь дор дурдсан сэргийлэх арга хэрэгслүүдийг мэдээллийн нууцлалын үндсэн элементүүд болохыг хүлээн зөвшөөрсөн. Тэд мөн эдгээр элемент нь үйл ажиллагааг хурдан хугацаанд сэргээхэд түлхэц болно гэж үздэг. Хэдий тийм ч ямар ч СЗЗДБ цахим халдлагаас сэргийлж болно гэж итгэлтэйгээр хэлж чадахгүй байна. СЗЗДБ-ийн системүүд халдлагад өртсөн бөгөөд СЗЗДБ-үүд халдлагыг илрүүлэх чадвартай байх хэрэгтэй гэсэн аюулгүй байдлын талаарх таамаглал байна (4.3.2-ыг харна уу).

Тодорхойлох нь

СЗЗДБ-үүд бизнесийн нөхцөл байдал, үндсэн үйл ажиллагаанд шаардлагатай нөөц, үүнтэй холбоотой цахим эрсдэлийн талаарх ойлголтоо дээшлүүлснээр өөрсдийн эрсдэлийн удирдлагын стратеги болон бизнесийн хэрэгцээндээ тохируулж хүчин чармайлтаа голлон төвлөрүүлэх юм.

Мэдээлэлтэй байх

Ажилтнуудад сургалт явуулах, халдлагуудын талаар дүн шинжилгээ хийх зэрэг нь байгууллага дахь бүх түвшний цахим аюулгүй байдлын талаарх мэдлэг, мэдээллийг дээшлүүлэх аргууд бөгөөд энэ нь аюулгүй байдлын үр дүнтэй загварчлал гаргах үндэс суурь болж өгдөг.

Гүний хамгаалалт

Гүний хамгаалалт гэж ихэвчлэн нэрлэгддэг аргууд нь сүлжээний нууцлалын удирдлагатай холбоотой байдаг. Энэ нь аль нэг хэсэг халдлагад өртсөн ч бусад руу нэвтрэх боломжийг халдлага үйлдэгчид олгохгүйн тулд систем болон системийн хэсгүүдийг үечлэн давхарлаж, галт хана суурилуулах ажиллагаа юм. И-мэйл гэх мэт интернет рүү холбогддог програмуудыг хамгийн их эрсдэлтэй гэж үзэн, үндсэн суурь системийн хэсгээс тусгаарладаг.

Хортой үйлдлээс сэргийлэх

Вирусын эсрэг шийдлүүдийг ашиглахын зэрэгцээ халдлага үйлдэгчид хортой код ашиглан халдаж болох сул талуудыг тогтоох зорилгоор вэб үйлчилгээ болон дэд бүтцэд дүн шинжилгээ хийх замаар хортой үйлдлээс сэргийлж болно. Дүн шинжилгээ гэдэгт сэжигтэй и-мэйл, хортой код бүхий мэдээллийн урсгал, ДДоС халдлага болон хэрэглэгчдийн мэдээллийг олж авах хакеруудын оролдлого зэргийг хянах, шалгах ажиллагаа хамаарна. Сэжигтэй мэдээллийн урсгалыг тогтоосны дараа, үүнийг блоклож мөн халдлагын эх үүсвэрийг саармагжуулах ажлыг хийж болно.

Халдлага хийж болзошгүй цэгүүдийг багасгах

Халдлагаас сэргийлэх нэг чухал хэсэг бол СЗЗДБ-ийн сүлжээ рүү нэвтрэх боломж олгож болзошгүй цэгүүдийг багасгах явдал юм. Ерөнхийдөө интернет рүү гарах гарцын тоог хязгаарлах, аюулгүй програм хангамжуудыг тодорхойлох, сүлжээний чухал хэсгүүдийг тусгаарлах зэрэг аргуудыг ашиглаж байна.

Програм хангамжийн хөгжүүлэлт

Байгууллагын дотооддоо хөгжүүлж буй програм хангамжуудын хөгжүүлэлтийн явцад мөн урьдчилан сэргийлэлтийг хийж болно. Хөгжүүлэлтийн явцад үндсэн системийн сул талуудын тоог хязгаарлахын тулд програм хангамжийн кодчиллын стандартуудыг ашиглах, турших шаардлагатай.

Тестлэх болон програм хангамжийн удирдлага

Аюулгүй байдлын аудит, пэнтест хийхдээ нууцлал, аюулгүй байдлын стандартуудыг хангаж буй эсэхийг шалгах, ашиглаж буй аюулгүй байдлын зохион байгуулалт дахь сул талуудыг тодорхойлох зорилгоор өндөр түвшний дүгнэлт шинжилгээ, загварчилсан халдлагуудыг

ашигладаг. СЗЗДБ-үүд нь пэнтестийг өөрсдөө болон гадны зөвлөхүүдтэй хамтран тогтмол хийдэг.

Програм хангамжийн удирдлага гэдэгт аюулгүй програм хангамжийг тодорхойлох болон нууцлалтай холбоотой засвар оруулах ажиллагаа хамаарна. Аюулгүй програм хангамжуудийг тодорхойлсноор зөвхөн зөвшөөрөгдсөн програмуудыг сервер болон ажилтнуудын компьютер дээр суулгах, ингэснээр халдлага үйлдэгч үйл ажиллагааны орчинд хортой програм суулгах эрсдэлийг бууруулах юм. Харин жижиг засварууд оруулж, програм хангамж болон үйлдлийн системийн шинэчлэлийг цаг тухайд нь хийснээр системийн сул талуудыг бууруулна. Програм хангамжийн тусламж үйлчилгээг зогсоосноор халдлагад өртөх илүү магадлалтай болдог.

Хандалтын хяналт

Мэдээлэл болон/эсвэл системүүд рүү зөвшөөрөлгүй хандахаас сэргийлэхэд хандалтын хяналт чухал үүрэгтэй. Админ эрхийг зөвхөн зайлшгүй шаардлагатай хэрэглэгчдэд өгөх ба хэрэглэгч ийм эрх авах хүсэлт гаргах бүрт дээд удирдлагад энэ талаар мэдэгдэх шаардлагатай. Админ эрхтэй хэрэглэгчийн тоог багасган, "хамгийн бага эрх"-тэй байх зарчмыг баримталснаар, байгууллага дотроос хийх халдлагын эрсдэл мөн гадны халдлага орох цэгүүдийг хязгаарлах боломжтой. Хандалтын лог болон анхааруулга нь зөвшөөрөгдсөн хандалтуудыг хянах болон сэжигтэй үйлдлүүдийг тодорхойлоход ашиглагдана.

Дэд бүтцийн хяналт ба хөгжүүлэлт

Мэдээллийн технологийн дэд бүтцийн загвар нь нууцлал, аюулгүй байдлын удирдлагад чухал нөлөөтэй. Дэд бүтэц дэх хяналт илүү чанга болсноор урьдчилан сэргийлэх арга хэмжээг авдаг. Виртуал машин (ВМ) эсвэл виртуал дэлгэцийн дүрс (ВДД) нь ажилтнуудыг төвлөрсөн серверт суулгасан компьютер руу хандах боломжоор хангадаг арга юм. Ажлын компьютерын аюулгүй байдал болон мэдээллийн нууцлал нь тухайн серверт төвлөрдөг учир аюулгүй байдлын засваруудыг оруулахад хялбар болгохоос гадна тодорхой хэрэглэгчдэд хандалтын эрх олгох эсвэл хязгаарлах асуудлыг шууд шийдвэрлэх боломж олгодог.

ВМ-уудыг сүлжээ, сервер, ажлын компьютерууд дээр тогтмол мэдээлэл хадгалахгүй горим үүсгэхэд ашиглаж болно. Мөн халдлага үйлдэгчийн суулгасан хортой програмыг үр дүнтэй устгахын тулд ВМ-ыг "алтан горим"-д оруулж, хэвийн болгож болдог. Ингэснээр орчин нь байнга өөрчлөгдөж байх учраас халдлага үйлдэгч СЗЗДБ-ийн сүлжээнд байнгын холболт үүсгэх, тандалт хийх, сүлжээгээр дамжин системийн гүн рүү ороход төвөгтэй болох юм. Уг процесс нь мөн сэргээх явцад нэмэр болдог.

Нууц мэдээллийг шифрлэх зэрэг (энгийн https протоколоос эхлээд илүү өндөр түвшний VPN үйлчилгээ) криптографын хамгаалалтуудыг хэрэглэж интернет гэх мэтийн итгэлтэй бус

орчноор өгөгдөл дамжуулах үед зөвшөөрөлгүй этгээд өөрчлөх эсвэл хандахаас хамгаалдаг учраас ийм хамгаалалтыг үр дүнтэй арга гэж үздэг.

4.3.2 Илрүүлэлт

Урьдчилан сэргийлэх нь чухал боловч дангаараа хангалттай биш. Байгууллагуудын хувьд халдлага үйлдэгч тэдний хамгаалалтыг нэвтрэн, аль хэдийн системд нь орсон гэж бодон бодлогоо боловсруулдаг байна. СЗЗДБ-ийн халдлагыг цаг алдалгүй илрүүлж, хамрах хүрээг тооцоолох чадвар нь сэргээгдэх хугацааг богиносгоход чухал үүрэгтэй. Ихэнх СЗЗДБ нь хэд хэдэн эх үүсвэр болон мэдрэгчүүдээс өгөгдөл цуглуулан, нэгтгэж, харьцуулах замаар богино хугацаанд сэжигтэй үйлдлүүдийг илрүүлэх олон төрлийн хяналтын системийг нэвтрүүлсэн байдаг. Үүнээс гадна, тэд өөрсдийн ашиглаж буй хамгаалалтын аргуудын үр дүнг нягтлах зорилгоор илрүүлэх процесс болон процедуруудыг хянаж, туршдаг.

Хяналт

Халдлага үйлдэгч өгөгдлийг өөрчилсөн тохиолдолд СЗЗДБ тухайн өгөгдлийг хүлээн авч, боловсруулахын өмнө эсвэл дараа тухайн өөрчлөлт хийгдсэн гэдгээс хамаарч илрүүлэх, тохируулах, сэргээх явц өөр өөр байх хандлагатай байна. Дан ганц аюулгүй байдал эсвэл сүлжээний үйл ажиллагааны техникийн хяналт хангалтгүй. Техник талын хамгаалалтаас гадна хяналтын нэмэлт давхарга байдлаар үйлчлүүлэгчдийн дунд ямар нэг хэвийн бус гүйлгээ гарахад (дүн, зуучлагч, гүйлгээ хийсэн хугацаа зэрэг нь хэвийн бус байх) холбогдох талууд нь илрүүлэх боломж бүхий аргуудтай байх шаардлагатай. Үүнээс гадна операторууд нь СЗЗДБ-ийн өдөр тутмын үйл ажиллагаа, нэн чухал болон “энгийн” системүүдийн талаар ойлголттой байх хэрэгтэй. Хяналтын системүүд дэх үйл явцуудыг харьцуулах нь хэвийн бус боловсруулалт хийгдсэн тохиолдлуудыг илрүүлэхэд тусалдаг. Асуудал гарсан үед зохих хэлтэс рүү шилжүүлэх, шийдвэр гаргах процессыг тодорхой болгож өгснөөр СЗЗДБ-ийн хариу үйлдэл үзүүлэх чадварыг сайжруулж, халдлага үйлдэгчийн системд байх хугацааг богиносгоно.

Асуудлыг хурдан ойлгон, авах арга хэмжээг яаралтай эхлүүлэхийн тулд техникийн болон бизнесийн хяналтын шийдлүүд нь ангиллын систем ашиглан хоорондоо холбогддог. Гол үйлчлүүлэгчид нь системийг хянаснаар хэвийн бус нөхцөл бий болох үед хурдацтайгаар мэдээлэх боломжийг ихэсгэнэ. Холбогдогч талуудтай уялдаа холбоотой ажилласнаар цахим халдлага цааш тархахаас сэргийлэхэд туслах юм.

Хяналтын цэг ашиглах

СЗЗДБ-ийн оролцогчдыг хамруулан програм хангамж болон процессыг хуваах (сегментлэх) замаар хяналтын цэг болон баталгаажуулах аргуудыг тогтмол хэрэглэснээр оношилгоо ба ангилал хийхэд шаардагдах хугацааг багасгах боломжтой. Ийм төрлийн бие биенээ

баталгаажуулдаг загварыг бий болгох нь хамгаалалт, илрүүлэлт, мөн СЗЗДБ-ийн сэргээгдэх хурдыг сайжруулах давуу талтай юм.

Бусад туршлагууд

Хэрэглэгч эсвэл бизнесийн хамтрагчийн хувьд програмын ердийн бус хэрэглээ эсвэл ердийн бус гүйлгээ гарах гэх мэт сэжигтэй үйлдлүүдийг илрүүлэх “хьюристик” хяналт түгээмэл болж байна. СЗЗДБ-үүдийн зүгээс мэдээллийн систем рүү нэвтэрсэн халдлага үйлдэгч цааш дамжин, олон системд нөлөөлөх нөлөөллийг багасгахын тулд нэг түвшний сүлжээ болон цогц програм хангамжаас татгалзан, олон тусдаа хэсэгт хуваах (сегментлэх) болсон. Үүний нэг жишээ бол хэдэн жилийн өмнө аюулгүй байдлын компаний хөгжүүлсэн, халдлага үйлдэгчийн хөдөлгөөн бүрийг хянан, сүлжээнээс өгөгдөл гаргахаас сэргийлэн холболт бүр дээр хаалт хийдэг “холболтыг таслах (kill chain)” процесс юм. Энэ аргыг одоо илүү өргөнөөр хэрэглэх болсон.

4.3.3 Сэргээлт

Цахим аюулгүй байдал гэж үйлчилгээнүүдийг доод түвшинд үзүүлэх байсан ч хамаагүй (жишээ нь зөвхөн эрэмбэ өндөртэй гүйлгээнүүдийг дамжуулах) үйл ажиллагааг үргэлжлүүлэх чадварыг хэлнэ. Үйлчилгээ үзүүлэх чадвараа хадгалж үлдэх чадвартай үйл ажиллагаанууд нь системийг бүрэн унагалгүйгээр халдлагын шокыг шингээхээр загварчлагдсан байдаг. Иймд “сэргээлт” гэдэг нь үйлчилгээг бүрэн хэмжээнд үзүүлэх боломжтой болгон, бүрэн сэргээх болон үйл ажиллагааг “тодорхой хугацаанд хангалттай” гэж үзэхүйц түвшинд сэргээхийн аль алиныг нь хамарна. Дараах хэсэгт цахим халдлага амжилттай болсон үед СЗЗДБ-ийн үйл ажиллагааг сэргээх арга техникүүдийн жишээг үзүүллээ. Энд мөн СЗЗДБ нь доорх бүх аргуудыг хэрэглэх шаардлагагүй, хэд хэдэн аргыг хослуулан ашиглах практик байдаг гэдгийг дурдах нь зүйтэй юм.

Үйл ажиллагааг “хэвийн” эсвэл “хангалттай” төлөвт сэргээх

Үйл ажиллагааг богино хугацаанд тогтвортой төлөвт буцаан сэргээх боломжгүйгээс системийн хэмжээнд эрсдэл үүсгэн, илүү өргөн санхүүгийн систем рүү дамжуулах боломжтой учраас халдлагын үе дэх тогтвортой байдал маш чухал. Сэргээх ажиллагааг хурдан гүйцэтгэсэн ч энэ нь цахим аюулгүй байдлыг хангасан гэсэн үг биш. СЗЗДБ нь үйл ажиллагаагаа 2 цагийн дотор сэргээхээр байсан ч анх халдлага амжилттай болоход нөлөөлсөн эмзэг төлөв рүүгээ сэргэх боломжтой юм.

Олон давхарга бүхий технологи ашигладаг бол зарим тохиолдолд үйлчилгээг хэсэгчилэн сэргээх боломжтой байж болно. Өөрөөр хэлбэл, халдлага хийгдсэн системийн хэсгүүдийг засах явцад зарим үйл ажиллагааг сэргээх боломжтой юм. Нэн чухал хэсгүүдийг өдөрт нь багтаан сэргээх боломжгүй тохиолдолд ихэнх СЗЗДБ-үүд нь холбоотой системүүд болон харилцан хамаарлыг харгалзан үзсэний үндсэн дээр ажиллах цагаа уртасгаж болно.

СЗЗДБ-үүд бүтэн өдрийн үйл ажиллагааг харьцангуй богино хугацаанд багтаан гүйцэтгэх боломжтой байхын тулд гол системээ ачаалал даах чадвартай байлгаж болно. Иймээс маш ноцтой цахим халдлага болж нэг өдрөөс илүү үргэлжлэхээс бусад тохиолдолд цагаа уртасгаж, нөөц хүчин чадлаа ашигласнаар өдрийн эцэст төлбөр тооцоог гүйцэтгэх үүргээ биелүүлэх боломжтой юм. Хэрэв осол нэг өдрөөс илүү үргэлжлэх тохиолдолд тохиромжтой гэж үзсэн бол механик аргаар боловсруулалт хийх аргыг сонгож болно.

“Алтан цэг” рүү буцах

Сэргээлт хийх үед авах чухал алхам бол хэзээ халдлага болсныг тодорхойлохоос гадна мэдээллийн технологийн орчин, мэдээлэл болон/эсвэл програм хангамж ямар нэг байдлаар эвдэгдсэн эсэхийг тогтоон, тодорхойлох явдал юм. Энэ нь эвдэгдээгүй “алтан цэг”-ийг тогтоон, халдлага үйлдэгч нэвтрэхээс өмнө ямар байсан тэр төлөв рүү мэдээллийн технологийн орчны хэсгүүд болон өгөгдөл болон/эсвэл програм хангамжийг буцаан сэргээхэд нэн чухал үүрэгтэй.

Гүйлгээ болон холбогдох өгөгдлийг бараг бодит цагийн горимд авч, системээс гадна хадгалах нь алтан цэгийг тодорхойлоход тулгарах саадыг даван туулахад туслах үр дүнтэй арга юм. Уг бичлэгүүдийг тогтмол шалгаж, тулгаснаар цахим халдлагыг илрүүлэх эсвэл эвдэгдсэн буюу хуурамч гүйлгээг тодорхойлоход тусална. Үүний тулд СЗЗДБ-үүд бие даасан 3-дагч этгээд эсвэл оролцогчид буюу тэдгээрийн үйлчлүүлэгчидтэй гүйлгээ тохируулах зохицуулалттай байж болно.

СЗЗДБ-үүд ийм байдлаар бүх боловсруулагдаагүй мессежийн хуулбарыг авах (өгөгдлүүдээс тусдаа), тодорхой давтамжтайгаар оролцогчдын позицыг шалгах, тодорхой давтамжтайгаар өгөгдлийн сангийн хуулбарыг авах зэрэг ажлыг аюулгүй гүйцэтгэж чаддаг. Үүнийг дэмждэг технологи болох “Нэг бичээд, олон уншдаг (WORM)” төхөөрөмж нь нөөцлөлт хийх хугацааны интервалын хооронд алдагдсан гүйлгээнүүдийг тодорхойлоход тусалдаг. СЗЗДБ нь эдгээр гүйлгээг тодорхойлсны дараа тэдгээрийг цаг алдалгүй дахин боловсруулах чадвартай байх хэрэгтэй.

“Халдлага хийгдэхээс өмнөх” сэргээлт эсвэл “Халдлага хийгдсэний дараах” сэргээлт

“Халдлага хийгдэхээс өмнөх” сэргээлт гэж үйл ажиллагааны орчинг хамгийн сүүлийн “итгэлтэй” төлөв рүү өөрөөр хэлбэл халдлага хийгдэхээс өмнөх төлөв рүү шилжүүлэхийг хэлнэ. “Халдлага хийгдсэний дараах” сэргээлт гэдэг нь халдлага хийгдсэн мэдээллийн технологийн орчны хэсгүүдийг итгэлтэй төлөв рүү сэргээх үйл ажиллагааны явцад бүрэн итгэлтэй цэгээс хойших, үйл ажиллагааг үргэлжлүүлэхэд шаардлагатай байгаа төлвийг сонгон сэргээх ажиллагаа юм. “Халдлага хийгдсэний дараах” сэргээлтийг ашигласнаар үйлчилгээний сул зогсолтын хугацааг хязгаарлах боломжтой бөгөөд энэ талаар зарим нэг судалгааны ажлууд хийгдэж байна.

Гэвч олон нийтийн зүгээс “Халдлага хийгдсэний дараах” сэргээлтийг хэрэгжиж боломжтой гэж үзэхгүй байна. “Халдлага хийгдэхээс өмнөх” сэргээлтийг боломжит хугацаанд хийж чадахгүй тохиолдолд л үүнийг хэрэглэж боломжтой гэж үзэж болох юм. Иймээс “Халдлага хийгдсэний дараах” сэргээлтийг ашиглах эсэх нь СЗЗДБ-ийн зүгээс нэн чухал үйл ажиллагааг нь дэмжиж буй мэдээллийн технологийн орчинг итгэлтэй төлөв рүү сэргээхэд шаардлагатай сул зогсолтын хугацааг зөвшөөрөх эсэх эсвэл СЗЗДБ нь бүрэн итгэлтэй бус орчинд нэн чухал үйлчилгээгээ үзүүлсээр байх эсэхээс хамаарна.

Өөр тоног төхөөрөмж

“Өөр тоног төхөөрөмж” (ӨТТ) гэж үндсэн тоног төхөөрөмжөөс өөр технологи ашигласан боловч СЗЗДБ-ийн гол үйл ажиллагааг яг адил гүйцэтгэх чадвартай төхөөрөмжийг хэлнэ. Энэ тохиолдолд үндсэн тоног төхөөрөмж бүхий гол систем рүү цахим халдлага амжилттай хийгдсэн ч СЗЗДБ нь өөр тоног төхөөрөмжүүд ашиглан үйл ажиллагаагаа дахин үргэлжлүүлж чадах юм. Өөр үйл ажиллагаатай өөр системүүд (жишээ нь их дүнтэй болон бага дүнтэй төлбөр тооцооны систем) осол аваарын үед бие биенийхээ нөөц систем болон ажиллахаар зохицсон жишээ байдаг. Ерөнхийдөө ӨТТ нь үндсэн системийн бүх үйл ажиллагааг үзүүлэхгүй ч хамгийн чухал гүйлгээнүүдийг боловсруулах чадвартай байна.

ӨТТ нь СЗЗДБ-ийн үндсэн системээс тусдаа ажиллан, өгөгдөл гэмтсэн үед үйл ажиллагааг нь сэргээх зорилгоор СЗЗДБ-ийн өгөгдлийг нөөцлөн авч болно. Үүнд тусдаа холболтын суваг шаардлагатай байж болох юм. Үүнийг шийдэх нэг боломж бол СЗЗДБ-ийн оролцогчид өгөгдлөө 2 тусдаа тоног төхөөрөмж рүү нэгэн зэрэг шууд илгээснээр “Халдлага хийгдэхээс өмнөх” сэргээлтэнд ашиглаж болно. ӨТТ нь мөн нөөц төв тодорхой цэгээс эхлэн боловсруулалтыг хийж эхлэх гэх мэт “халдлага хийгдсэний дараах” сэргээлтийн сонголттой байж болно.

Гэвч ӨТТ-үүдийн загвараас шалтгаалан эдгээр нь үйл ажиллагааг нарийн төвөгтэй, үнэ өртөг ихтэй болгож магадгүйн зэрэгцээ системийн аюулгүй байдалд нөлөөлж, ажиллагааг нь удаашруулж болно. Түүнчлэн эдгээр нь шинэ төрлийн халдлага нэмэгдэхэд нөлөөлөх боломжтой. Хэдийгээр ӨТТ-үүд төгс байж чадахгүй ч СЗЗДБ-үүдийн тасралтгүй ажиллагааг сайжруулахад хэрэг болж болох юм.

5. Ач холбогдол

Санхүүгийн системийн харилцаа холбоо, харилцан хамаарлыг авч үзвэл СЗЗДБ-ийн түвшин дэх цахим аюулгүй байдал нь түүний үйлчилж буй зах зээлийн цахим аюулгүй байдлыг хангана гэсэн үг биш. Ялангуяа зах зээлийн аюулгүй байдал нь ганц СЗЗДБ-ээс бус харилцан холбогдсон СЗЗДБ-үүд, нэн чухал үйлчилгээ үзүүлэгчид, оролцогчдоос хамаарч байдаг.

Цахим аюулгүй байдлыг хангах хамтарсан буюу нэгдсэн арга зам, ялангуяа халдлагын талаарх болон форензикийн тухай мэдээлэл солилцох зэрэг нь маш чухал.

Ихэнх улс оронд байгууллагууд дотор болон байгууллага хооронд цахим аюулгүй байдлын талаарх идэвхтэй харилцаа байдаг. Дотооддоо ийм харилцаанууд нь ихэвчлэн санхүүгийн болон санхүүгийн бус салбарын, түүнчлэн төрийн болон хувийн секторын СЗЗДБ-үүд, бусад санхүүгийн байгууллагууд, нэн чухал үйлчилгээ үзүүлэгчдийг хамарна. Зарим улс оронд аюулгүй байдлыг хангах туршлага солилцох үүднээс мэдээлэл солилцох зохицуулалт, найдвартай сүлжээг бий болгосон байдаг.

Зах зээлийн хэмжээний үйл ажиллагааг цаг алдалгүй сэргээх нь туршилт хийхэд мөн саад учруулдаг. Уламжлалт, тусгаарласан байдлаар туршилт хийхэд бусад бүх оролцогчдыг хэвийн ажиллагаатай байна гэж үздэг. Энэхүү төсөөллийг авч хаяснаар бусад СЗЗДБ болон оролцогчдыг хамарсан нэгдсэн сургуулилт нь маш цөөхөн СЗЗДБ-үүдэд туршигдсан илүү төвөгтэй түвшинд хийгддэг.

Хэдий тийм боловч нэг этгээдийн бүрэн сэргэлт эсвэл аюулгүй байдлаа хамгаалан үлдэх чадвар нь өөр нэг этгээдийн чадвараас эсвэл бүр оролцогчдын өгөгдлийн санд хадгалагдсан мэдээллээс хамаарч болно. Ийм тохиолдолд өдрийн эцэст төлбөр тооцоог хийж гүйцэтгэх гол зорилгодоо хүрэхийн тулд уялдаа холбоо зайлшгүй шаардлагатай. Түүнчлэн, сэргээлт хийн, өдрийн эцэст төлбөр тооцоог гүйцэтгэж дуусахын тулд ажиллах цагийг уртасгах шаардлагатай байж болно. Цаг уртасгах боломж нь СЗЗДБ бүрт өөр өөр байж болох ч энэ нь бусад дэд бүтэц эсвэл зуучлагчийн товлосон хугацаанд багтах нэг ижил зорилготой байдаг. Гэмтэл саатал болсон өдөр төлбөр тооцоогоо багтаан гүйцэтгэхийн тулд илүү уян хатнаар дээд хязгаарыг хэзээ эсвэл хэрхэн тогтоох талаар шийдвэр гаргахад харилцан уялдаа болон харилцаа холбоо тусалдаг.

Мөн олон СЗЗДБ-үүд хэд хэдэн улс оронд, цагийн зөрүүтэй бүсүүдэд үйл ажиллагаагаа явуулдаг тул харилцан уялдаа, харилцаа холбоог хүндрүүлэх хандлагатай байдаг. Үүнээс үүдэн зохицуулагчид, хяналт тавих эрх бүхий этгээд, хянан шалгагч нар нь дотооддоо болон олон улсын хэмжээнд холбоо тогтоон хамтран ажиллаж, СЗЗДБ-ийн найдвартай, үр ашигтай байдлыг дэмжих шаардлагатай. Гэвч энэ хүрээнд байгууллагын, хууль эрх зүйн, нууцлалын түвшин зэрэгт тулгарч буй хэд хэдэн асуудлыг шийдвэрлэх шаардлагатай болдог.

Тухайлбал олон улсын хэмжээнд үйл ажиллагаа явуулдаг СЗЗДБ-үүд нууцын зэрэглэлтэй мэдээллийг өөрийн байгууллага дотроо түгээх боломжгүй гэдгийг мэдэгдсэн. Хууль, хүчний байгууллагууд эсвэл тагнуулын газрууд СЗЗДБ-ийн удирдлагад нууц мэдээлэл гаргаж өгч болох ч тухайн улсын эрх баригчдаас олгосон нууцлалын зөвшөөрөлгүй этгээдтэй уг мэдээллийг хуваалцах боломжгүй байдаг. Иймд СЗЗДБ-үүд төрийн болон хувийн байгууллагуудын уялдаа холбоо, хичээл зүтгэлээр дээрх асуудлуудыг шийдвэрлэхэд идэвх зүтгэл гаргахыг эрх баригчдаас хүсэж байна.

Хавсралт 1. Нэр томъёоны тодорхойлолт

2ц-ССЗ	2 цагийн дотор систем сэргээгдэх зорилт
Дэвшилтэт байнгын халдлага (advanced persistent threat)	Бизнестэй холбоотой эсхүл улс төрийн зорилго бүхий тодорхой байнд чиглэсэн цахим халдлагын төрөл. Халдлага үйлдэгч нь урт хугацааны туршид өндөр нууцлалтайгаар үйл ажиллагааг нь танддаг. Халдлагын зорилго нь нэн даруй санхүүгийн ашиг олохоор хязгаарлагдахгүй бөгөөд үндсэн систем рүү нэвтрэн анхны зорилгодоо хүрсэн ч халдлагад өртсөн систем хэвийн ажилласан хэвээр байдаг.
Халдлага хийж болзошгүй цэг (attack surface)	Халдлага үйлдэгч систем рүү нэвтрэн СЗЗДБ-д хохирол учруулж болох өргөн хүрээ (програм хангамж, техник хангамж, сүлжээ, хүн)-н дэх эмзэг цэгүүд. Халдлага үйлдэж болзошгүй цөөхөн цэг байна гэдэг нь СЗЗДБ-ийг ашиглах боломж бага буюу халдлага хийх магадлал багатай байна гэсэн үг. Гэвч ийм цэгийг багасгалаа гээд халдлагаас учрах хохирлыг бууруулна гэсэн үг биш.
Базелийн хороо (BCBS)	Банкны хяналт шалгалтын Базелийн хороо
АКТ (CCP)	Арилжааны клирингийн төв
ҮЦТХТ (CSD)	Үнэт цаасны төвлөрсөн хадгаламжийн төв
Цахим халдлага (cyber attack)	Цахим аюулгүй байдалд сөргөөр нөлөөлж болзошгүй нөхцөл эсвэл тохиолдол үүсгэх нэвтрэх оролдлого.
Цахим засаглал (cyber governance)	Хүн, технологи, процесс, харилцаа холбоо гэсэн 4 өргөн хүрээг хамарсан, СЗЗДБ-ийн цахим аюулгүй байдлыг сайжруулах зорилготой аргачлал.
Цахим аюулгүй байдал (cyber resilience)	Цахим халдлагаас үүдсэн тасалдлаас урьдчилан сэргийлэх, нөлөөллийг багасгах, зохицуулах болон/эсхүл богино хугацаанд сэргээх чадвар.
Цахим хамгаалалт (cyber security)	Тогтсон тодорхойлолт байхгүй маш өргөн хүрээг хамарсан ойлголт. Энэ тайланд цахим хамгаалалт гэдэгт СЗЗДБ-ийн үйл ажиллагааны аюулгүй байдалтай холбоотой аюул заналыг бууруулах, сул талыг арилгах, сэргийлэх, олон улсын арга хэмжээ, ослын үед авах арга хэмжээ, аюулгүй байдал, буцаан сэргээх үйл ажиллагаа зэргийг хамарсан стратеги, бодлого, стандартыг хамруулсан.

Цахим аюул занал (cyber threat)	СЗЗДБ-ийн системийн нууцлал, бүрэн бүтэн байдал, бэлэн байдал алдагдахад хүргэх, санаатай болон санамсаргүйгээр нэг болон олон сул талыг ашиглах нөхцөл эсхүл тохиолдол.
ДДоС (DDoS – distributed denial-of-service)	Энэ халдлагын үед халдлага үйлдэгчээс үйлчилгээ авах хуурамч хүсэлтийг маш ихээр илгээн, бай болсон компьютер эсхүл сүлжээний хууль ёсны хэрэглэгчийг ашиглах боломжгүй болгож, хэд хэдэн системийг хортой програмаар хордуулснаар хяналтыг гартаа авдаг.
Халдлага хийгдэхээс өмнөх сэргээлт (failing-backward)	Үйл ажиллагааны орчинг халдлага хийгдэхээс өмнөх хамгийн сүүлийн “итгэлтэй” төлөв рүү сэргээх процесс.
Халдлага хийгдсэний дараах сэргээлт (failing-forward)	Халдлага орсон мэдээллийн технологийн орчны хэсгүүдийг итгэлтэй төлөв рүү сэргээх үйл ажиллагаа хийгдэх явцад үйл ажиллагааг үргэлжлүүлэх шаардлагатай байгаа (хангалттай) төлвийг сонгон сэргээх ажиллагаа.
GCE	G10-ын компьютерийн мэргэжилтнүүд
Алтан цэг (golden point)	Алтан хуулбар ч гэж нэрлэгддэг бөгөөд мэдээллийн технологийн орчны хэсгүүд, өгөгдөл болон програмыг халдлага үйлдэгч халдахаас өмнөх төлөв рүү сэргээж болох цэгийг хэлдэг.
Хьюристик (heuristic)	Алгоритмын аргаар асуудлыг шийдэх боломжгүй үед туршилтын журмаар шийдэх арга. Цахим хамгаалалтын хувьд хортой код болон/эсхүл систем болон үйлчилгээн дэх хэвийн бус тохиолдлыг илрүүлж чадах лог дээр суурилсан мэдээллийн эх сурвалжийг хянах аргачлалыг ашиглах чадвар юм.
Холболтыг таслах (kill chain)	Цэргийн үг хэллэг. Цахим хамгаалалтын хүрээнд энэ нь халдлага үйлдэгч болон халдлагын эргэн тойрон дахь үйл явдлыг холбож үзэх замаар авч болох арга хэмжээг тодорхойлохыг хэлнэ.
Хамгийн бага эрх (least privilege)	Хэвийн ажиллагааг хангахад шаардлагатай хамгийн бага түвшний хандах эрхээр хязгаарлах зарчим. Ажилтнуудын хувьд энэ зарчим нь өөрийн үүргээ гүйцэтгэхэд шаардлагатай хамгийн бага түвшний хэрэглэгчийн эрх өгөхийг хэлнэ.
Хортой програм (malware)	Мэдээллийн системийн нууцлал, бүрэн бүтэн, бэлэн байдалд сөргөөр нөлөөлөх замаар хэвийн ажиллагааг алдагдуулдаг програм хангамж.
MITRE загвар (MITRE framework)	MITRE корпораци, *Цахим аюулгүй байдлын үнэлгээ: бүтцийг сайжруулах нь*. Deborah Bodeau, Richard Graubart, 2013 оны 5 сар

NIST загвар (NIST framework)	Стандарт болон технологийн үндэсний институт, *Нэн чухал дэд бүтцийн цахим аюулгүй байдлыг сайжруулах загвар*, 2014 оны 2 сар
ӨТТ - өөр тоног төхөөрөмж (NSF – non-similar facility)	СЗЗДБ-ийн үндсэн үйл ажиллагааг үндсэн төвийн ашигласнаас өөр технологи ашиглан хуулбарлах.
СЗЗДБЗ (PFMIs)	Санхүүгийн зах зээлийн дэд бүтцийн зарчим
СЗЗДБ Зарчим 2 (PFMI Principle 2)	Удирдлага, зохион байгуулалт: “СЗЗДБ нь үйл ажиллагааныхаа найдвартай, үр ашигтай байдлыг хангаж, санхүүгийн тогтвортой байдлыг дэмжсэн, олон нийтийн эрх ашиг, холбогдох этгээдийн зорилго, зорилтод нийцсэн тодорхой, ил тод удирдлага зохион байгуулалттай байна.”
СхНЧТС (SIPS)	Системийн хувьд нэн чухал төлбөрийн систем
ҮЦТТС (SSS)	Үнэт цаасны төлбөр тооцооны систем
Нийгмийн инженерчлэл (social engineering)	Цахим халдлагын хувьд нийгмийн инженерчлэл гэдэг нь хохирогчийн итгэлийг олж аван, нууц мэдээлэл өгөх, хавсаргасан файлыг татаж авах, мөнгө явуулах болон үүнтэй төстэй зүйл хийхийг ятгах арга.
Чиглэсэн-фишинг (spear-phishing)	Олон тооны цахим шууданг санамсаргүйгээр явуулдаг уламжлалт фишинг аргаас ялгаатай нь хоорондоо ямар нэг зүйлээрээ төстэй хэсэг бүлэг хүн рүү чиглэдэг. Хохирогчид нь цахим шуудан дахь холбоос дээр дарсан үед нууц мэдээлэл эсхүл хувийн мэдээлэл оруулах вэб рүү оруулдаг. Эсвэл холбоосон дээр дарснаар хортой код эсхүл програмыг хохирогчийн компьютерт суулгана.
АМС (TR)	Арилжааны мэдээллийн сан
Гүйлгээний цуваа (transaction chain)	Энэ тайланд гүйлгээний цуваа гэж гүйлгээ эхлүүлснээс эцсийн төлбөр тооцоо хийгдэх хүртэлх санхүүгийн гүйлгээний бүх процессийг хамарсан холбоос болон үйл явдлын цувааг хэлнэ.

Ажиллагааны явцад сэргээх (trust on-the-fly)	Систем ажиллаж байх үед мэдээллийн технологийн орчны бүрэлдэхүүн хэсгүүдийг бүхэлд нь эсвэл зарим хэсгийг нь аюулгүй болгоход чиглэсэн системийн сэргээлтийн арга.
Виртуал дэлгэцийн дүрс /ВДД/ (VDI – virtual desktop image)	Виртуал орчин дахь хэрэглэгч тус бүрийн интерфейсийн дүрс. ВДД нь дотоод сүлжээнд бус гадаад төвлөрсөн серверт ажиллана. Мөн энэ нь хэрэглэгчдийг тусгаарлагдсан үйлдлийн системээр хангахын тулд бодит төхөөрөмжүүдээс салангид байрлана.
Виртуал машин /ВМ/ (VM – virtual machine)	Бодит төхөөрөмжтэй адилаар програмуудыг ажиллуулах боломжтой програм хангамжид суурилсан машин (өөрөөр хэлбэл, компьютер).
Дэлхийн эдийн засгийн форумын цахим аюулгүй байдлын аргачлал (World Economic Forum's cyber resilience approach)	Дэлхийн Эдийн Засгийн Форум, *Хэт-холбогдсон дэлхий дээрх эрсдэл ба хариуцлага*, 2014 оны 1 сар
WORM-нэг бичиж олон удаа унших (WORM – Write Once Read Many times)	Нэгэнт бичигдсэн мэдээллийг өөрчлөх боломжгүй, өгөгдөл хадгалах төхөөрөмж.
WPSI	GCE аюулгүй байдлын ажлын хэсэг.

Хавсралт 2. Ажлын хэсгийн гишүүд

Дарга (Недерландын Төв банк)	Coen Voormeulen
Австралийн Нөөцийн банк	Ashwin Clarke
	Mark Manning
Белгийн Үндэсний банк	Nikolaï Boeckx
	Jorke Kamstra
	Yves Vandenbosch
Канадын Төв банк	Christian Belisle
ECB	Frans Rijkschroeff
Францын Төв банк	Claudine Hurman
	Clement Martin
Германы Бундесбанк	Sylvia Tyroler
BaFin (Германы СЗХ)	Christoph Ruckert (IOSCO-г төлөөлж)
Энэтхэгийн Нөөцийн банк	Kashiap Balakrishnan
Италийн Төв банк	Luigi Sciusco
Японы Төв банк	Mitsu Adachi (BCBS-г төлөөлж)
Солонгосын Төв банк	Heejun Yoo
Мексикийн Төв банк	Victor Manuel De La Luz Puebla
Недерландын Төв банк	Ewoud van Bentem (WPSI дарга)
	Raymond Kleijmeer
	Bram van der Meulen (WPSI гишүүн)
Оросын Төв банк	Nikolay Geronin1
	Dmitry Krutov
	Andrey Kurilo
Шведийн Төв банк	Pär Karlsson
Швейцарийн Үндэсний банк	Frédéric Bos
	Marco Cecchini
Бүгд найрамдах Турк улсын Төв банк	Cemil Ulu
	Özgür Şanlı
Английн Төв банк	Roz Horton
	Freddie Hult
	Ed Kelsey
Англи СЗХ	Farrukh Nazir (BCBS-г төлөөлж)
Холбооны Нөөцийн системийн захирлуудын зөвлөл	Ken Buckley (GCE дарга)
	Jeffrey Marquardt
	Stuart Sperry
Нью-Йоркын Холбооны Нөөцийн банк	Lawrence Sweet
Олон улсын үнэт цаасны хорооны Нарийн бичгийн дарга	Rohini Tendulkar
Олон улсын төлбөр тооцооны банк	Emanuel Di Stefano Bezerra Freire
	Klaus Löber
	Can Bülent Okay

Ажлын хэсгийн үйл ажиллагаанд Peter Kah (Германы Бундесбанк, WPSI гишүүн), Paul Biles (Английн Төв банк), Carlos Conesa, Pan Ng болон Ayn du Bazane нар гүн туслалцаа үзүүлсэн болно.