МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДАЛ, КИБЕР АЮУЛГҮЙ БАЙДАЛ, НУУЦЛАЛЫН ХАМГААЛАЛТ-МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ЭРСДЭЛИЙГ УДИРДАХ АРГА ЗҮЙ

ЗОХИОГЧИЙН ЭРХ НЬ ХАМГААЛАГДСАН БАРИМТ БИЧИГ

©ISO/IEC 2022

Бүх эрх хуулиар хамгаалагдсан. Өөрөөр заагаагүй эсхүл үүнийг хэрэгжүүлэх нөхцөл байдалд шаардаагүй бол энэхүү хэвлэлийн аль ч хэсгийг ямар ч арга хэлбэрээр, цахим болон механик аргаар хуулбарлах, интернет эсвэл дотоод сүлжээнд байршуулах зэргийг бичгээр урьдчилан олгосон зөвшөөрөлгүйгээр хуулбарлахыг хориглоно. Зөвшөөрлийг доорх хаягаар ОУСБ (ISO)-аас эсвэл хүсэлт гаргагчийн улсын ISO-ын гишүүн байгууллагаас авах боломжтой.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org
Published in Switzerland

Агуулга

Өмнөх үг 6
Танилцуулга 8
1 Хамрах хүрээ 9
2 Норматив эшлэл 9
3 Нэр томьёо, тодорхойлолт 9
3.1 Мэдээллийн аюулгүй байдлын эрсдэлтэй холбоотой нэр томъёо 10
3.1.1 гадаад нөхцөл байдал 10
3.1.2 дотоод нөхцөл байдал 10
3.1.3 эрсдэл 10
3.1.4 эрсдэлийн хувилбар 11
3.1.5 эрсдэлийн хариуцагч 11
3.1.6 эрсдэлийн эх үүсвэр 11
3.1.7 эрсдэлийн шалгуур 12
3.1.8 эрсдэлийг бууруулах эрмэлзэл 12
3.1.9 аюул занал 12
3.1.10 эмзэг байдал 12
3.1.11 тохиолдол 12
3.1.12 мэдээллийн аюулгүй байдлын аюултай тохиолдол 13
3.1.13 болзошгүй тохиолдол 13
3.1.14 үр дагавар 13
3.1.15 эрсдэлийн түвшин 13
3.1.16 хяналт 14
3.1.17 үлдэгдэл эрсдэл 14
3.2 Мэдээллийн аюулгүй байдлын эрсдэлийн менежментэд холбоотой нэр томъёо 14
3.2.1 эрсдэлийн менежментийн үйл явц 14
3.2.2 эрсдэлийн талаар мэдээлэх, зөвлөлдөх 14
3.2.3 эрсдэлийн үнэлгээ 15
3.2.4 эрсдэлийг тодорхойлох 15
3.2.5 эрсдэлийн шинжилгээ 15
3.2.6 эрсдэлийн үнэлгээ 15
3.2.7 эрсдэлийн арга хэмжээ 16
3.2.8 эрсдэлийг хүлээн зөвшөөрөх 16
3.2.9 эрсдэлийг хуваалцах 17

3.2.10 эрсдэлийг хадгалах 17
4 Энэхүү баримт бичгийн бүтэц 17
5 Мэдээллийн аюулгүй байдлын эрсдэлийн менежмент 18
5.1 Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явц 18
5.2 Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн мөчлөг 20
6 Нөхцөл байдлыг тодорхойлох 21
6.1 Зохион байгуулалтын асуудал 21
6.2 Сонирхогч талуудын үндсэн шаардлагыг тодорхойлох 22
6.3 эрсдэлийн үнэлгээ хийх 22
6.4 Мэдээллийн аюулгүй байдлын эрсдэлийн шалгуурыг тодорхойлох, хадгалах 23
6.4.1 Ерөнхий 23
6.4.2 Эрсдэлийг хүлээн зөвшөөрөх шалгуур 23
6.4.3 Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээг гүйцэтгэх шалгуур 25
6.5 Тохиромжтой аргыг сонгох 29
7 Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явц 30
7.1 Ерөнхий 30
7.2 Мэдээллийн аюулгүй байдлын эрсдэлийг тодорхойлох 31
7.2.1 Мэдээллийн аюулгүй байдлын эрсдэлийг тодорхойлох, тайлбарлах 31
7.2.2 Эрсдэл хариуцагчдыг тодорхойлох 33
7.3 Мэдээллийн аюулгүй байдлын эрсдэлийг шинжлэх 34
7.3.1 Ерөнхий 34
7.3.2 Болзошгүй үр дагаврыг үнэлэх 35
7.3.3 Болзошгүй тохиолдлыг үнэлэх 36
7.3.4 Эрсдэлийн түвшинг тодорхойлох 38
7.4 Мэдээллийн аюулгүй байдлын эрсдэлийг үнэлэх 39
7.4.1 Эрсдэлийн шинжилгээний үр дүнг эрсдэлийн шалгуур үзүүлэлттэй харьцуулах 39
7.4.2 Шинжилсэн эрсдэлийг эрсдэлийн арга хэмжээнд зориулан эрэмбэлэх 40
8 Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний үйл явц 40
8.1 Ерөнхий 40
8.2 Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний оновчтой хувилбаруудыг сонгох 41
8.3 Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний хувилбаруудыг хэрэгжүүлэхэд шаардлагатай бүх хяналтыг тодорхойлох 42
8.4 ISO/IEC 27001:2022, А хавсралтад заасан хяналттай харьцуулах 46
8.5 Хэрэглэх тухай мэдэгдэл гаргах 47

8.6 Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний төлөвлөгөө 48
8.6.1 Эрсдэлийг арга хэмжээний төлөвлөгөө боловсруулах 48
8.6.2 Эрсдэл хариуцагчийн зөвшөөрөл 49
8.6.3 Мэдээллийн аюулгүй байдлын үлдэгдэл эрсдэлийг хүлээн зөвшөөрөх .. 50
9 Үйл ажиллагаа 51
9.1 Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явцыг гүйцэтгэх . 51
9.2 Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний үйл явцыг гүйцэтгэх 52
10 МАБМТ-тэй холбоотой үйл явцыг ашиглах 53
10.1 Байгууллагын нөхцөл байдал 53
10.2 Манлайлал ба тууштай байдал 54
10.3 Харилцаа холбоо, зөвлөгөө 55
10.4 Баримтжуулсан мэдээлэл 57
10.4.1 Ерөнхий 57
10.4.2 Үйл явцын талаарх баримтжуулсан мэдээлэл 57
10.4.3 Үр дүнгийн талаарх баримтжуулсан мэдээлэл 58
10.5 Мониторинг ба дүн шинжилгээ 59
10.5.1 Ерөнхий 59
10.5.2 Эрсдэлд нөлөөлж буй хүчин зүйлсэд мониторинг, дүн шинжилгээ хийх 60
10.6 Удирдлагын дүн шинжилгээ 61
10.7 Залруулах арга хэмжээ 62
10.8 Байнгын сайжруулалт 63
А хавсралт (мэдээллийн) 65
Эрсдэлийн үнэлгээний үйл явцыг дэмжих аргуудын жишээ 65
А.1 Мэдээллийн аюулгүй байдлын эрсдэлийн шалгуур 65
А.1.1 Эрсдэлийн үнэлгээтэй холбоотой шалгуур 65
А.1.2 Эрсдэлийг хүлээн зөвшөөрөх шалгуур 71
А.2 Хэрэгжүүэх арга 72
А.2.1 Мэдээллийн аюулгүй байдлын эрсдэлийн бүрэлдэхүүн хэсгүүд 72
А.2.4 Тохиолдолд суурилсан арга 79
А.2.5 Өмч хөрөнгө суурилсан арга 81
Ном зүй 93

Өмнөх үг

ОУСБ (Олон улсын стандартчиллын байгууллага) ба ОУЦТК (Олон улсын цахилгаан техникийн комисс) нь дэлхий даяар стандартчиллын мэргэшсэн тогтолцоог бүрдүүлж байна. ОУСБ болон ОУЦТК-ийн гишүүн үндэсний байгууллагууд нь техникийн үйл ажиллагааны тодорхой салбарт эрх бүхий байгууллагаас тодорхой чиглэлийн дагуу байгуулсан техникийн хороодоор дамжуулан, олон улсын стандартыг боловсруулахад оролцдог. ОУСБ болон ОУЦТК-ийн техникийн хороод сонирхсон чиглэлээр хамтран ажилладаг. ОУСБ болон ОУЦТК-тай хамтран ажилладаг төрийн болон төрийн бус бусад олон улсын байгууллагууд уг ажилд оролцдог.

Энэ баримт бичгийг боловсруулахад ашигласан болон цаашид дахин сайжруулж хянах журмыг ОУСБ/ОУЦТК-ийн Удирдамжийн 1-р хэсэгт тайлбарласан болно. Ялангуяа ялгаатай төрлийн баримт бичигт өөр өөр шалгуур шаардлагатайг тэмдэглэвэл зохино. Энэ баримт бичгийн төслийг ОУСБ/ОУЦТК Удирдамжийн 2-р хэсэгт дурдсан хянах засвар оруулах журмын дагуу боловсруулсан болно (www.iso.org/directives -ыг үзнэ үү).

Энэ баримт бичгийн зарим бүрдэл хэсэг нь патентын эрхэд хамаарч болзошгүйд анхаарал хандуулсан. ISO болон IEC нь патентын эрхийг бүхэлд нь эсхүл хэсэгчлэн тодорхойлох талаар аливаа хариуцлага хүлээхгүй. Баримт бичгийг боловсруулах явцад илэрсэн аливаа патентын эрхийн талаарх дэлгэрэнгүй мэдээлэл нь Танилцуулга хэсэг болон/эсвэл ОУСБ-ын хүлээн авсан патентын мэдүүлгийн жагсаалт (www.iso.org/patents) -д байна.

Энэхүү баримт бичигт ашигласан аливаа худалдааны нэрийг хэрэглэгчид тохиромжтой байх зорилгоор оруулсан мэдээлэл бөгөөд мөрдүүлэх зорилго агуулаагүй.

Стандартуудын зөвлөмжийн байдал, тохирлын үнэлгээтэй холбоотой ISO-ийн тусгай нэр томьёо, хэллэгүүдийн утга, түүнчлэн Худалдааны техникийн саад тотгор (TBT) дэх ОУСБ-ын Дэлхийн Худалдааны Байгууллагын (ДХБ) зарчмуудыг дагаж мөрдөж байгаа талаарх мэдээллийг www.iso.org/iso/foreword.html. IEC-д www.iec.ch/understanding-standards сайтаас үзнэ үү.

Энэхүү баримт бичгийг “ISO/IEC JTC 1, Мэдээллийн технологи, Дэд хороо SC 27, Мэдээллийн аюулгүй байдал, кибер аюулгүй байдал ба хувийн нууцыг хамгаалал” хамтарсан техникийн хороо боловсруулсан.

Энэхүү дөрөв дэх хэвлэл нь техникийн хувьд шинэчлэгдсэн бөгөөд өмнөх гурав дахь хэвлэлийг (ISO/IEC 27005:2018) хүчингүйд тооцож, орлоно.

Дараах үндсэн өөрчлөлтүүд орсон байна:

— бүх арга зүйн бичвэрийг ISO/IEC 27001:2022, ISO 31000:2018 стандартад нийцүүлсэн;
— нэр томъёог ISO 31000:2018 стандартын нэр томьёотой нийцүүлсэн;

— заалтуудын бүтцийг ISO/IEC 27001:2022 стандартын загварт тохируулсан;
— эрсдэлийн хувилбаруудын үзэл санааг танилцуулсан;
— тохиолдолд суурилсан арга нь эрсдэлийг тодорхойлох өмч хөрөнгөд суурилсан хандлагаас ялгаатай;
— хавсралтуудын агуулгыг шинэчлэн найруулж, нэг хавсралт болгон өөрчилсөн.

Энэ баримт бичигтэй холбоотой аливаа санал хүсэлт эсвэл асуултыг хэрэглэгчийн хамаарах үндэсний стандартын байгууллагад хандана. Эдгээр байгууллагуудын бүрэн жагсаалтыг www.iso.org/members.html болон www.iec.ch/national-committees вэбсайтаас олж болно.

Энэ стандартыг Монголбанкны хянан шалгагч-мэргэжилтэн М.Саруул орчуулж, Олон улсын цахилгаан техникийн комиссын Хөгжиж буй оронд зориулсан хөтөлбөрийн удирдагч Г.Батцэнгэл хянасан.

Танилцуулга

Энэхүү баримт бичиг нь дараахь хүлээнд арга зүйгээр хангана.

— ISO/IEC 27001-д дурдсан мэдээллийн аюулгүй байдлын эрсдэлийн шаардлагуудыг хэрэгжүүлэх;

— Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл ажиллагааг дэмжихийн зорилгоор ISO/IEC JTC 1/SC 27-оос боловсруулсан стандартуудын үндсэн лавлагаа;

— Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээ (ISO/IEC 27001:2022, 6.1 ба 8-р зүйлийг үзнэ үү);

— Мэдээллийн аюулгүй байдлын хүрээнд ISO 31000 стандартын эрсдэлийн менежментийн удирдамжийг хэрэгжүүлэх.

Энэхүү баримт бичиг нь эрсдэлийн менежментийн талаар дэлгэрэнгүй зааварчилгааг агуулсан бөгөөд ISO/IEC 27003 стандартын удирдамжийг хавсаргасан болно.

Энэхүү баримт бичгийг дараах хүмүүс ашиглахад зориулагдсан:

— ISO/IEC 27001 стандартын дагуу мэдээллийн аюулгүй байдлын менежментийн тогтолцоог бий болгох, хэрэгжүүлэх зорилготой байгууллагууд;

— мэдээллийн аюулгүй байдлын эрсдлийн менежментийг гүйцэтгэдэг эсвэл үүнд оролцдог хүмүүс (жишээ нь, МАБМТ-ны мэргэжилтнүүд, эрсдэл хариуцагчид болон бусад сонирхогч талууд);

— мэдээллийн аюулгүй байдлын эрсдлийн удирдлагын үйл явцыг сайжруулах зорилготой байгууллагууд.

Мэдээллийн аюулгүй байдал, кибер аюулгүй байдал, нууцлалын хамгаалалт — Мэдээллийн аюулгүй байдлын эрсдэлийг удирдах заавар

1 Хамрах хүрээ

Энэхүү баримт бичиг нь байгууллагад туслах арга зүйгээр хангана:

— ISO/IEC 27001 стандартын мэдээллийн аюулгүй байдлын эрсдэлд чиглэсэн шаардлагуудыг хангах;
— Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл ажиллагааг гүйцэтгэх, ялангуяа мэдээллийн аюулгүй байдлын эрсдэлийн үнэлэх, залруулах.

Энэхүү баримт бичиг нь төрөл, хэмжээ, салбараас үл хамааран бүх байгууллагад хэрэглэж болно.

2 Норматив эшлэл

Дараахь баримт бичгүүдийг бичвэрт дурдсан бөгөөд тэдгээрийн хэсэгчилсэн эсхүл нийт агуулга нь энэхүү баримт бичгийн шаардлагад нийцнэ. Огноо бүхий баримт бичгийн хувьд зөвхөн эш татсан хэвлэл хамаарна. Огноо заагаагүй баримт бичгийн хувьд эш татсан баримт бичгийн хамгийн сүүлийн хэвлэл (өөрчлөлтийг оруулаад) хамаарна.

ISO/IEC 27000, Мэдээллийн технологи — Хамгаалалтын арга техник — Мэдээллийн аюулгүй байдлын менежментийн систем - Ерөнхий зүйл ба нэр томьео

3 Нэр томьёо, тодорхойлолт

Энэхүү баримт бичгийн зорилгод ISO/IEC 27000-д дурдсан нэр томьёо, тодорхойлолтууд болон дараах зүйлс хамаарна.

ISO болон IEC нь стандартчилалд ашиглах нэр томъёоны мэдээллийн санг дараах хаягаар бүрдүүлж, хадгалдаг:

— ISO Онлайн хайлтын платформ: https:// www .iso .org/ obp дээрээс авах боломжтой

— IEC Electropedia: https:// www .electropedia .org/ хаягаас авах боломжтой

3.1 Мэдээллийн аюулгүй байдлын эрсдэлтэй холбоотой нэр томъёо

3.1.1 гадаад нөхцөл байдал

зорилтдоо хүрэхийн тулд шаардагдах байгууллагын гадаад орчин

Бичвэрийн 1-р тайлбар: Гадаад нөхцөл байдалд дараахь зүйлс орж болно.

— олон улс, бүс нутаг, үндэсний болон орон нутгийн нийгэм, соёл, улс төр, хууль эрх зүй, зохицуулалт, санхүү, технологи, эдийн засаг, газар зүйн орчин;
— байгууллагын зорилгод нөлөөлж буй гол хүчин зүйлс, хандлага;
— гадаад сонирхогч талуудын харилцаа, ойлголт, үнэ цэнэ, хэрэгцээ, хүлээлт;
— гэрээний харилцаа, үүрэг хариуцлага;
— сүлжээ болон хамаарлын нарийн төвөгтэй байдал.

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.3.1.1, өөрчилсөн — Бичвэрийн 1-р тайлбарыг өөрчилсөн.]

3.1.2 дотоод нөхцөл байдал

зорилтдоо хүрэхийн тулд шаардагдах байгууллагын дотоод орчин

Бичвэрийн 1-р тайлбар: Дотоод нөхцөл байдалд дараахь зүйлийг хамруулж болно.

— алсын хараа, эрхэм зорилго, үнэт зүйлс;
— засаглал, зохион байгуулалтын бүтэц, үүрэг, хариуцлага;
— стратеги, зорилго, бодлого;
— байгууллагын соёл;
— байгууллагын баталсан стандарт, арга зүй, загвар;
— нөөц ба мэдлэгийн чадавхи (хөрөнгө, цаг хугацаа, хүн, үйл явц, тогтолцоо, технологи гэх мэт);
— өгөгдөл, мэдээллийн систем, мэдээллийн урсгал;
— дотоод сонирхогч талуудын ойлголт, үнэ цэнийг харгалзсан тэдэнтэй харилцаа;
— гэрээний харилцаа, үүрэг хариуцлага;
— дотоод харилцан хамаарал, уялдаа.

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.3.1.2, өөрчлөгдсөн — Бичвэрийн 1-р тайлбарыг өөрчилсөн.]

3.1.3 эрсдэл

тодорхойгүй байдал нь зорилгод үзүүлэх нөлөө

Бичвэрийн 1-р тайлбар: Үр нөлөө гэдэг нь хүлээгдэж буй үр дүнгээс эерэг эсвэл сөрөг хазайлт

Бичвэрийн 2-р тайлбар: Зорилтуудын хандлага, ангилал нь ялгаатай байж болох

бөгөөд өөр өөр түвшинд хэрэгжиж болно.

Бичвэрийн 3-р тайлбар: тохиолдол (3.1.11), түүний үр дагавар (3.1.14), болзошгүй тохиолдол (3.1.13)-той холбоотой мэдээлэл хэсэгчлэн болон бүхэлдээ дутмаг төлөвийг тодорхойгүй байдал гэнэ.

Бичвэрийн 4-р тайлбар: Эрсдэлийг ихэвчлэн эрсдэлийн эх сурвалж (3.1.6), тохиолдол, тэдгээрийн үр дагавар, болзошгүй тохиолдлоор илэрхийлдэг .

Бичвэрийн 5-р тайлбар: Мэдээллийн аюулгүй байдлын менежментийн тогтолцооны хүрээнд мэдээллийн аюулгүй байдлын эрсдэлийг мэдээллийн аюулгүй байдлын зорилтод тодорхойгүй байдлын үр нөлөө гэж илэрхийлж болно.

Бичвэрийн 6-р тайлбар: Мэдээллийн аюулгүй байдлын эрсдэл нь ихэвчлэн мэдээллийн аюулгүй байдлын зорилтуудад үзүүлэх тодорхойгүй байдлын сөрөг үр нөлөөтэй холбоотой байдаг.

Бичвэрийн 7-р тайлбар: Мэдээллийн аюулгүй байдлын эрсдэл нь мэдээллийн хөрөнгө эсвэл мэдээллийн өмчийн нэгдлийн эмзэг байдлыг (3.1.10) аюул занал (3.1.9) ашиглан, байгууллагад хохирол учруулах боломжтой холбоотой байж болно.

[ЭХ СУРВАЛЖ: ISO 31000:2018, 3.1, , Бичвэрийн 1-р тайлбарт "Энэ нь эерэг, сөрөг эсвэл хоёулаа байж болох ба боломж, аюул заналыг шийдвэрлэх, бий болгох, үр дүнд хүргэж болно" гэснийг "эерэг эсвэл сөрөг" гэж өөрчилсөн; Бичвэрийн 3-р тайлбарын дугаарыг Бичвэрийн 4-р тайлбар болгон өөрчилсөн; болон Бичвэрийн 3,5,6,7-р тайлбарыг нэмж оруулав.]

3.1.4 эрсдэлийн хувилбар

Анхны шалтгаанаас хүсэгүй үр дагавар (3.1.14)-т хүргэх тохиолдол (3.1.11)-ын дараалал буюу хослол

[ЭХ СУРВАЛЖ: ISO 17666:2016, 3.1.13, өөрчлөлт орсон-Бичвэрийн 1-р тайлбарыг устгасан.]

3.1.5 эрсдэлийн хариуцагч

эрсдэл (3.1.3)-ийг удирдах үүрэг, эрх мэдэл бүхий хүн эсхүл хуулийн этгээд

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.5.1.5]

3.1.6 эрсдэлийн эх үүсвэр

дангаар эсхүл хослон эрсдэл (3.1.3) үүсгэх боломжтой элемент

Бичвэрийн 1-р тайлбар: Эрсдэлийн эх үүсвэр нь дараах гурван төрлийн аль нэг байж болно.

— хүн;

— байгаль орчин;
— техник.

Бичвэрийн 2-р тайлбар: Хүний эрсдэлийн эх үүсвэр нь санаатай болон санамсаргүй байж болно.

[ЭХ СУРВАЛЖ: ISO 31000:2018, 3.4, өөрчлөлт орсон-Бичвэрийн 1,2-р тайлбарыг нэмсэн.]

3.1.7 эрсдэлийн шалгуур

эрсдэл (3.1.3)-ийн ач холбогдлыг үнэлдэг үндэслэл

Бичвэрийн 1-р тайлбар: Эрсдэлийн шалгуур нь байгууллагын зорилт болог гадаад (3.1.1) болон дотоод нөхцөл (3.1.2) байдалд үндэслэдэг.

Бичвэрийн 2-р тайлбар: Эрсдэлийн шалгуур нь стандарт, хууль тогтоомж, бодлого болон бусад шаардлагаас үүсч болно.

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.3.1.3]

3.1.8 эрсдэлийг бууруулах эрмэлзэл

Байгууллага хүлээж авах эсвэл хадгалахад бэлэн байгаа эрсдэл (3.1.3)-ийн хэмжээ ба төрөл

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.7.1.2]

3.1.9 аюул занал

Систем эсхүл байгууллагад хохирол учруулж болзошгүй мэдээллийн аюулгүй байдлын аюултой тохиолдол (3.1.12)-ын болзошгүй шалтгаан

3.1.10 эмзэг байдал

Сөрөг үр дагавар (3.1.14)-тай тохиолдол (3.1.11) үүсгэхэд ашиглаж болох өмч эсхүл хяналт (3.1.16)-ын сул тал

3.1.11 тохиолдол

тодорхой багц нөхцөл байдлын тохиолт эсвэл өөрчлөлт

Бичвэрийн 1-р тайлбар: Тохиолдол нь нэг буюу хэд хэд тохиож болох ба хэд хэдэн шалтгаан, үр дагавартай байж болно (3.1.14).

Бичвэрийн 2-р тайлбар: Тохиолдол нь хүлээгдэж буй ч тохиохгүй, эсхүл хүлээгдэж байгаагүй ч тохиож болно.

[ЭХ СУРВАЛЖ: ISO 31000:2018, 3.5, өөрчлөлт орсон - Бичвэрийн 3-р тайлбарыг хассан.]

3.1.12 мэдээллийн аюулгүй байдлын аюултай тохиолдол

бизнесийн үйл ажиллагааг алдагдуулж, мэдээллийн аюулгүй байдалд заналхийлэх өндөр магадлал бүхий мэдээллийн аюулгүй байдлын нэг эсхүл хэд хэдэн, хүсээгүй эсвэл гэнэтийн мэдээллийн аюулгүй байдлын тохиолдол

3.1.13 болзошгүй тохиолдол

ямар нэг зүйл тохиох боломж

Бичвэрийн 1-р тайлбар: Эрсдэлийн менежментийн нэр томьёоны хувьд “болзошгүй тохиолдол” гэдэг үг нь ямар нэг зүйл тохиох боломжийг объектив эсвэл субъектив болон чанарын эсхүл тоон байдлаар тодорхойлсон эсхүл хэмжиж ерөнхий нэр томьео бөгөөд математик (жишээлбэл, тухайн хугацааны давтамж эсвэл магадлал). байдлаар дүрсэлнэ.

Бичвэрийн 2-р тайлбар: Англи хэлний х "болзошгүй тохиолдол" гэсэн нэр томъёо нь зарим хэл дээр шууд дүйцэхүйц үг байдаггүй; оронд нь "магадлал" гэсэн нэр томъёог ихэвчлэн дүйцүүлж хэрэглэдэг. Гэсэн хэдий ч англи хэлэнд "магадлал" гэдэг нь ихэвчлэн математикийн нэр томъёо гэж явцуу тайлбарладаг. Иймд эрсдэлийн менежментийн нэр томьёонд “болзошгүй тохиолдол” гэдэг үг нь англи хэлнээс бусад олон хэлний “магадлал” гэсэн нэр томьёотой ижил утгаар өргөн хэрэглэгддэг.

[ЭХ СУРВАЛЖ: ISO 31000:2018, 3.7]

3.1.14 үр дагавар

зорилтод нөлөөлөх тохиолдол (3.1.11)-ын үр дүн .

Бичвэрийн 1-р тайлбар: Үр дагавар нь тодорхой эсвэл тодорхойгүй байж болох ба зорилгод эерэг эсвэл сөрөг шууд болон шууд бус нөлөө үзүүлж болно.

Бичвэрийн 2-р тайлбар: Үр дагаврыг чанарын болон тоон хэлбэрээр илэрхийлж болно.

Бичвэрийн 3-р тайлбар: Аливаа үр дагавар нь шаталсан болон хуримтлагдсан нөлөөллөөр даамжирч болно.

[ЭХ СУРВАЛЖ: ISO 31000:2018, 3.6]

3.1.15 эрсдэлийн түвшин

үр дагавар (3.1.14) ба тэдгээрийн болзошгүй тохиолдол (3.1.13)-ын хослолоор илэрхийлэгдсэн эрсдэлийн ач холбогдол

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.6.1.8, өөрчлөлт орсон.-“эрсдэлийн хэмжээ эсхүл эрсдэлийн хослол” гэсэн хэллэгийг “эрсдэлийн ач холбогдол” гэж сольсон]

3.1.16 хяналт

эрсдэл (3.1.3)-ийг хадгалах ба/эсвэл өөрчлөх арга хэмжээ

Бичвэрийн 1-р тайлбар: Хяналт гэж эрсдэлийг хадгалах/өөрчлөх аливаа үйл явц, бодлого, төхөөрөмж, дадал, буюу бусад арга хэмжээг хэлнэ. Гэхдээ үүгээр хязгаарлагдахгүй.

Бичвэрийн 2-р тайлбар: Хяналт нь эрсдэлийн шинж чанарыг үргэлж хүссэн хэмжээнд хүртэл өөрчлөх боломжгүй.

[ЭХ СУРВАЛЖ: ISO 31000:2018, 3.8]

3.1.17 үлдэгдэл эрсдэл

эрсдэлийн арга хэмжээ (3.2.7) авсны дараа үлдсэн эрсдэл (3.1.3)

Бичвэрийн 1-р тайлбар: Үлдэгдэл эрсдэл нь тодорхойлогдоогүй эрсдэл агуулж болно.

Бичвэрийн 2-р тайлбар: Үлдэгдэл эрсдэл нь хадгалагдсан эрсдэлийг агуулж болно.

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.8.1.6, өөрчилсөн — Бичвэрийн 2-р тайлбарыг өөрчилсөн.]

3.2 Мэдээллийн аюулгүй байдлын эрсдэлийн менежментэд холбоотой нэр томъёо

3.2.1 эрсдэлийн менежментийн үйл явц

эрсдэл (3.1.3)-ийг мэдээлэх, зөвлөлдөх, нөхцөл байдлыг тодорхойлох болон тодорхойлох, шинжлэх, үнэлэх, арга хэмжээ авах, мониторинг хийх (3.8.2.1) дүн шинжилгээ хийх менежментийн бодлого, дүрэм, журмыг үйл ажиллагаанд системтэйгээр хэрэглэх

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.1]

3.2.2 эрсдэлийн талаар мэдээлэх, зөвлөлдөх

эрсдэл (3.1.3)-ийн менежментийн талаар мэдээлэл өгөх, хуваалцах, олж авах, сонирхогч талуудтай харилцан яриа өрнүүлэх зорилгоор байгууллагын явуулж буй тасралтгүй, давтагдан хэрэгжүүлдэг үйл явцын багц

Бичвэрийн 1-р тайлбар: Мэдээлэл нь эрсдэл бий эсэх, мөн чанар, хэлбэр, болзошгүй тохиолдол (3.1.13), ач холбогдол, үнэлгээ, хүлээн зөвшөөрөх болон эрсдлийн арга хэмжээтнй холбоотой байж болно.

Бичвэрийн 2-р тайлбар: Зөвлөлдөх гэдэг нь тодорхой асуудлаар шийдвэр гаргах, чиглэлээ тодорхойлохын өмнө тухайн байгууллага болон түүний сонирхогч

талуудын хооронд аливаа асуудлаар мэдээлэлтэй харилцах хоёр талын үйл явц юм. Зөвлөлдөөн нь:

— эрх мэдлийн бус нөлөөлөлөөр шийдвэр гаргахад нөлөөлөх үйл явц;
— шийдвэр гаралтын оролт, үүнд хамтарсан шийдвэр гаргалт хамаарахгүй

3.2.3 эрсдэлийн үнэлгээ

эрсдэлийг тодорхойлох (3.2.4), эрсдэлийн шинжилгээ (3.2.5) ба эрсдэлийн үнэлгээ (3.7.1)-тэй холбоотой бүх үйл явц

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.4.1]

3.2.4 эрсдэлийг тодорхойлох

эрсдэл (3.1.3)-ийг олох, таних, тайлбарлах үйл явц

Бичвэрийн 1-р тайлбар: Эрсдэлийг тодорхойлох гэдэгт эрсдэлийн эх сурвалж (3.1.6), тохиолдол (3.1.11), тэдгээрийн шалтгаан ба болзошгүй үр дагаварыг (3.1.14) тогтоох явдал хамаарна.

Бичвэрийн 2-р тайлбар: Эрсдэлийг тодорхойлох гэдэгт түүхэн баримт, онолын шинжилгээ, шинжээчийн санал болон оролцогч талуудын хэрэгцээ зэрэг багтаж болно.

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.5.1, өөрчлөлт орсон - Бичвэрийн 2-р тайлбарт "сонирхогч тал" гэдгийг "оролцогч талууд" гэж өөрчилсөн]

3.2.5 эрсдэлийн шинжилгээ

эрсдэл (3.1.3)-ийн мөн чанарыг ойлгож, эрсдэлийн төвшин (3.1.15)-г тогтоох үйл явц

Бичвэрийн 1-р тайлбар: Эрсдэлийн шинжилгээний үндсэн дээр эрсдэлийг үнэлэх (3.2.6) ба эрсдэлийн арга хэмжээний (3.2.7) талаар шийдвэрийг гаргах боломжтой.

Бичвэрийн 2-р тайлбар: Эрсдэлийн шинжилгээнд эрсдэлийн тооцоо багтана.

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.6.1]

3.2.6 эрсдэлийн үнэлгээ

Эрсдэл (3.1.3) ба/эсхүл ач холбогдлыг хүлээн зөвшөөрөх буюу хүлцэх боломжтой эсэхийг тогтоох зорилгоор эрсдэлийн үнэлгээ (3.2.5)-ний дүнг эрсдэлийн шалгуур (3.1.7)-тай харьцуулах үйл явц

Бичвэрийн 1-р тайлбар: Эрсдэлийн үнэлгээ нь эрсдэлийн арга хэмжээ (3.2.7)-ний талаар шийдвэр гаргахад тусалдаг.

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.7.1, өөрчлөлт орсон. “хэмжээ” гэсэн үгийг “ач холбогдол” гэж өөрчилсөн.]

3.2.7 эрсдэлийн арга хэмжээ

эрсдэлийг өөрчлөх үйл явц (3.1.3)

Бичвэрийн 1-р тайлбар: Эрсдэлийн арга хэмжээнд дараахь зүйлс орно.

— эрсдэл үүсгэж буй ажиллагааг эхлүүлэхгүй, үргэлжлүүлэхгүй байх шийдвэр гаргаж эрсдэлээс зайлсхийх;
— боломжоо хэрэгжүүлэхийн тулд эрсдэл хүлээж эсвэл нэмэгдүүлэх;
— эрсдэлийн эх үүсвэрийг арилгах (3.1.6);
— болзошгүй тохиолдлыг өөрчлөх (3.1.13);
— үр дагаврыг өөрчлөх (3.1.14);
— эрсдэлийг бусад тал эсвэл талуудтай хуваалцах (үүнд гэрээ, эрсдэлийн санхүүжилт орно); болон
— мэдээлэлтэй шийдвэр гаргаж эрсдэлийг хадгалах.

Бичвэрийн 2-р тайлбар: Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээнд "боломжоо хэрэгжүүлэхийн тулд эрсдэл хүлээх эсвэл нэмэгдүүлэх" гэсэн ойлголт байхгүй бөгөөд энэ сонголт нь эрсдэлийн ерөнхий менежментийн хувьд байгууллагад ийм сонголт байж болно.

Бичвэрийн 3-р тайлбар: Эрсдэлийн сөрөг үр дагаврууудын дагуу авч байгаа арга хэмжээг зарим тохиолдолд “эрсдэлийг бууруулах”, “эрсдэлийг арилгах”, “эрсдэлээс сэргийлэх” болон “эрсдэлийг багасгах” гэж авч үздэг.

Бичвэрийн 4-р тайлбар: Эрсдэлийн арга хэмжээний үр дүнд шинж эрсдэл гарч ирэх эсвэл байгаа эрсдэлийг шинж чанарыг өөрчилж болдог.

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.8.1, өөрчилсөн — Бичвэрийн 1-р тайлбарыг нэмсэн бөгөөд өмнө байсан Бичвэрийн 1 ба 2-р тайлбарын дугаарыг Бичвэрийн 2 ба 3-р тайлбар болгон өөрчилсөн.]

3.2.8 эрсдэлийг хүлээн зөвшөөрөх

тодорхой эрсдэл (3.1.3)-ийг хүлээх тухай мэдээлэлтэй шийдвэр

Бичвэрийн 1-р тайлбар: Эрсдэлийг хүлээн зөвшөөрөх нь эрсдэлийн арга хэмжээгүйгээр (3.2.7) эсвэл эрсдэлийн арга хэмжээний явцад тохиолдож болно.

Бичвэрийн 2-р тайлбар: Хүлээн зөвшөөрөх эрсдэлийг ажиглаж, дүн шинжилгээ хийнэ.

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.7.1.6]

3.2.9 эрсдэлийг хуваалцах

эрсдэлийн арга хэмжээ (3.2.7)-ний хэлбэр бөгөөд бусад талуудтай тохиролцсоны дагуу эрсдэлийг хуваарилах (3.1.3)

Бичвэрийн 1-р тайлбар: Хуулийн болон зохицуулалтын шаардлага нь эрсдэлийг хувалцахыг хязгаарлаж, хориглож эсхүл үүрэг болгож болно.

Бичвэрийн 2-р тайлбар: Эрсдэлийг даатгал эсвэл гэрээний бусад хэлбэрээр хуваалцаж болно.

Бичвэрийн 3-р тайлбар: Эрсдэлийг хуваалцах цар хүрээ нь хуваалцах механизмын найдвартай болон тодорхой байдлаас хамаарна.

Бичвэрийн 4-р тайлбар: Эрсдэлийг шилжүүлэх нь эрсдэлийг хуваалцах хэлбэр юм.

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.8.1.3]

3.2.10 эрсдэлийг хадгалах

тухайн эрсдэл (3.1.3)-ээс олох бодит ашиг, алдагдлаас үүсэх дарамтыг түр зуур хүлээн зөвшөөрөх

Бичвэрийн 1-р тайлбар: Хадгалах хугацааг тодорхой хугацаагаар хязгаарлаж болно.

Бичвэрийн 2-р тайлбар: Хадгалсан эрсдэлийн түвшин (3.1.15) нь эрсдэлийн шалгуур (3.1.7)-аас хамаарч болно .

[ЭХ СУРВАЛЖ: ISO Guide 73:2009, 3.8.1.5, өөрчлөлт орсон - Догол мөрийн эхэнд “түр зуур” гэсэн үгийг нэмсэн; Бичвэрийн 1-р тайлбарт "Үлдэгдэл эрсдэлийг хүлээн зөвшөөрөх нь эрсдэлийг хадгалахад хамаарна." гэснийг "Хадгалах хугацааг тодорхой хугацаагаар хязгаарлаж болно" гэж орлуулсан.]

4 Энэхүү баримт бичгийн бүтэц

Энэхүү баримт бичиг нь дараах бүтэцтэй.

— 5 дугаар зүйл : Мэдээллийн аюулгүй байдлын эрсдэлийн менежмент;
— 6-р зүйл : Контекст байгуулах;
— 7 дугаар зүйл : Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явц;
— 8 дугаар зүйл : Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний үйл явц;
— 9-р зүйл : Үйл ажиллагаа;
— 10-р зүйл : МАБМТ-тэй холбоотой үйл явцыг ашиглах.

Ерөнхий дэд зүйлд өгөгдсөн тайлбараас бусад тохиолдолд 7-р зүйлээс 10-р зүйл дэх эрсдэлийн менежментийн бүх үйл ажиллагааг дараах байдлаар бүтэцлэгдсэн.

Оролт: Үйл ажиллагааг гүйцэтгэхэд шаардлагатай мэдээллийг тодорхойлно.

Ажиллагаа: Үйл ажиллагааг дүрсэлнэ.

Өдөөгч: Үйл ажиллагааг хэзээ эхлүүлэ арга зүгээр хангана. Жишээ нь байгууллагын доторх өөрчлөлт эсхүл төлөвлөгөө эсхүл байгууллагын гадаад нөхцөл байдлын өөрчлөлтөөс шалтгаалж.

Гаралт: Үйл ажиллагааг гүйцэтгэсний дараах бүх мэдээлэл, түүнчлэн гаралтын хангавал зохих шалгуурыг тодорхойлно.

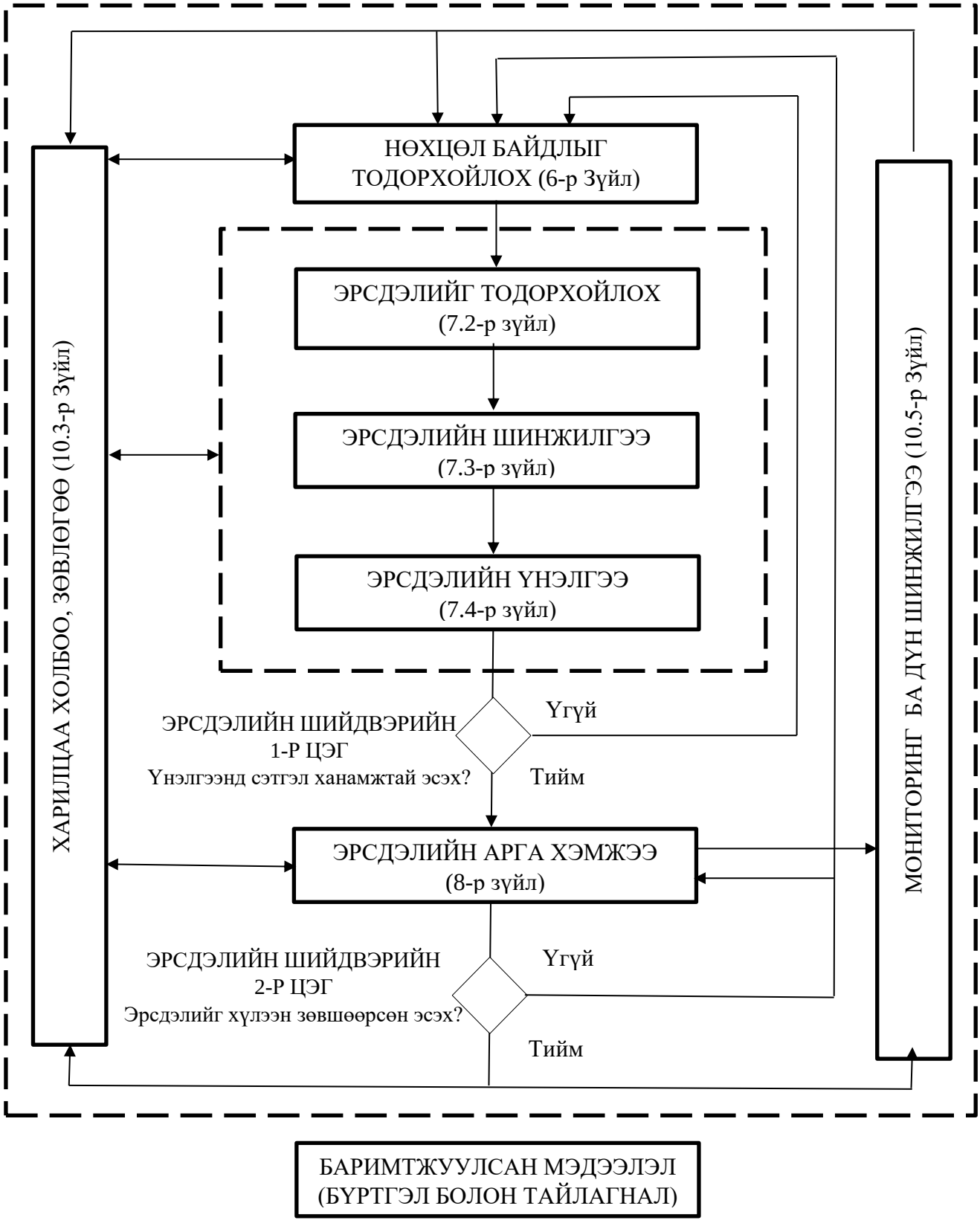
Арга зүй: Үйл ажиллагааг гүйцэтгэх арга зүй, түлхүүр үг, гол ойлголтоор хангана.

5 Мэдээллийн аюулгүй байдлын эрсдэлийн менежмент

5.1 Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явц

Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явцыг 1-р зурагт үзүүлэв .

ТАЙЛБАР: Энэхүү үйл явц нь ISO 31000 стандартад тодорхойлсон эрсдэлийн менежментийн ерөнхий үйл явцад үндэслэнэ.



1-р зураг- Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явц

1-р зургаас харахад мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явц нь эрсдэлийн үнэлгээ ба/буюу эрсдэлийн арга хэмжээ нь давтагдах боломжтой.

Эрсдэлийн үнэлгээний давталтын арга нь давталт бүрт үнэлгээний гүн, нарийвчилсан байдлыг нэмэгдүүлэх боломжтой. Давталтын арга нь хяналтад зарцуулсан цаг хугацаа, хүчин чармайлтыг бууруулахын зэрэгцээ эрсдэлийг зохих ёсоор үнэлж тэнцвэртэй байдлыг сайтар хангадаг.

Нөхцөл байдлыг тодорхойлох гэдэг нь мэдээллийн аюулгүй байдлын эрсдэлийн менежмент эсвэл мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний дотоод болон гадаад нөхцөлийг нэгтгэхийг хэлнэ.

Хэрэв эрсдэлийн үнэлгээ нь эрсдэлийг хүлээн зөвшөөрөгдөх түвшинд хүртэл өөрчлөхөд шаардлагатай үйл ажиллагааг үр дүнтэй тодорхойлох хангалттай мэдээллийг өгсөн бол уг даалгавар бүрэн дуусч, эрсдэлийн арга хэмжээг авна. Хэрэв мэдээлэл хангалтгүй бол эрсдэлийн үнэлгээний давталтыг дахин хийвэл зохино. Үүнд эрсдэлийн үнэлгээний нөхцөл байдлыг өөрчлөх (жишээ нь, хамрах хүрээг шинэчлэх), холбогдох салбарын мэргэжилтнүүдийг татан оролцуулах, эсвэл эрсдэлийг хүлээн зөвшөөрөгдөх хэмжээнд хүртэл өөрчлөхөд шаардлагатай мэдээллийг цуглуулах бусад аргууд орно ("1-р зураг дээр “Эрсдэлийн шийдвэрийн цэг 1" хэсгийг үзнэ үү.).

Эрсдэлийн арга хэмжээнд дор дурсан давтагдах үйл явцыг хамарна:

— эрсдэлийн арга хэмжээний хувилбаруудыг боловсруулах, сонгох;
— эрсдэлийн арга хэмжээг төлөвлөх, хэрэгжүүлэх;
— арга хэмжээний үр ашгийг үнэлэх;
— үлдэгдэл эрсдэлийг хүлээн зөвшөөрөх боломжтой эсэхийг шийдэх;
— хүлээн зөвшөөрөхгүй бол нэмэлт арга хэмжээг хэрэгжүүлэх.

Эрсдэлийн арга хэмжээ нь үлдэгдэл эрсдэлийн хүлээн зөвшөөрөгдөх түвшинд шууд хүргэхгүй байх магадлалтай. Ийм тохиолдолд эрсдэлийн дараагийн арга хэмжээг олох оролдлого хийх эсвэл эрсдэлийн үнэлгээг бүхэлд нь эсвэл хэсэгчлэн дахин хийж болно. Үүнд уг эрсдэлийн үнэлгээний нөхцөлийг өөрчлөх (жишээ нь, харах хүрээг шинэчлэх) болон холбогдох салбарын мэргэжилтнүүдийг оролцуулж болно. Холбогдох аюул занал, эмзэг байдлын талаарх мэдлэг нь эрсдэлийн үнэлгээний дараагийн давталтад тохирсон эрсдэлийн арга хэмжээний талаар илүү сайн шийдвэр гаргахад хүргэнэ. (1-р зураг "эрсдэлийн шийдвэрийн 2-р цэгийг харна уу).

6-р зүйлд эрсдэлийн үнэлгээний нөхцөл байдлыг бүрдүүлэх талаар 7-р зүйлд, эрсдэлийн үнэлгэний үйл ажиллагааг болон 8-р зүйлд эрсдэлийн арга хэмжээний талаар тус тус дэлгэрэнгүй авч үзсэн болно .

Мэдээллийн аюулгүй байдлын эрсдэлийг удирдахад шаардлагатай бусад үйл ажиллагааг 10-р зүйлд авч үзнэ .

5.2 Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн мөчлөг

Эрсдэлийн үнэлгээ, эрсдэлийн арга хэмжээг өөрчлөлтөд тулгуурлан тогтмол

шинэчилж байх ёстой. Энэ нь эрсдэлийн үнэлгээнд бүхэлд нь хамаарах бөгөөд шинэчлэлтүүдийг эрсдэлийн менежментийн хоёр мөчлөгт хуваж болно:

— Стратегийн мөчлөг буюу байгууллагын ерөнхий нөхцөл байдлын өөрчлөлтөөс бизнесийн өмч, эрсдэлийн эх үүсвэр, аюул занал, зорилго эсвэл мэдээллийн аюулгүй байдлын тохиолдлын үр дагавар өөрчлөгдөх. Энэ нь эрсдэлийн үнэлгээний ерөнхий шинэчлэл эсвэл эрсдэлийн үнэлгээ ба эрсдэлийн арга хэмжээний оролт болно. Түүнчлэн шинэ эрсдэлийг тодорхойлох, цоо шинэ эрсдэлийн үнэлгээг эхлүүлэхэд оролт болж чадна;
— үйл ажиллагааны мөчлөг буюу хувилбаруудыг хянаж, шинэчлэх үед дээр дурдсан элементүүд нь эрсдэлийн үнэлгээ, үнэлгээнд нөлөөлөх оролтын мэдээлэл эсвэл өөрчлөгдсөн шалгуур болно. Дүн шинжилгээнд холбогдох эрсдэлийн арга хэмжээний холбогдох шинэчлэлийг оруулбал зохино.

Стратегийн мөчлөгийг урт хугацаанд эсвэл томоохон өөрчлөлт гарсан үед хийх бөгөөд үйл ажиллагааны мөчлөг нь эрсдэлийн арга хэмжээнд хамаарах, тодорхойлогдсон, үнэлгээ хийсэн, дэлгэрэнгүй эрсдэлд илүү богино хугацаанд хийнэ.

Стратегийн мөчлөг нь байгууллага зорилгодоо хүрэхийг эрмэлзэж буй орчинд хамаарах бол үйл ажиллагааны мөчлөг нь эрсдэлийн менежментийн үйл явцын нөхцөл байдлыг харгалзан эрсдэлийн бүх үнэлгээнд хамаарна. Эдгээр хоёр мөчлөгийн хувьд үнэлгээ бүрт өөр өөр нөхцөл байдал, хамрах хүрээ бүхий эрсдэлийн олон үнэлгээ байж болно.

6 Нөхцөл байдлыг тодорхойлох

6.1 Зохион байгуулалтын асуудал

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 4.1-д хамаарна.

Байгууллага гэдэг нь зорилгодоо хүрэхийн тулд үүрэг хариуцлага, эрх мэдэл, харилцаа холбоо бүхий өөрийн чиг үүрэгтэй хүн эсвэл бүлэг хүмүүсийг хэлнэ. Байгууллага нь заавал компани, бусад корпораци эсвэл хуулийн этгээд байх албагүй, энэ нь хуулийн этгээдийн хэсэг (жишээ нь, компанийн мэдээллийн технологийн хэлтэс) байж болох бөгөөд МАБМТ (буюу Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо)-ны хүрээнд "байгууллага" гэж үзэж болно.

Байгууллагын хадгалахыг хүсч байгаа буюу хүлээн зөвшөөрөх эрсдэлийн хэмжээ гэж тодорхойлсон эрсдэлийг бууруулах эрмэлзэл нь байгууллага бүрт өөр өөр байж болохыг ойлгох нь чухал. Жишээ нь, байгууллагын эрсдэлийг бууруулах эрмэлзэлд нөлөөлдөг хүчин зүйлүүд нь хэмжээ, нарийн төвөгтэй байдал, салбар юм. Эрсдэлийг бууруулах эрмэлзлийг дээд удирдлага тогтоож, тогтмол дүн шинжилгээ хийвэл зохино.

Байгууллага нь тодорхойлсон эрсдэлтэй холбоотой менежментийн үйл ажиллагааны хувьд эрсдэл хариуцагчийн үүргийг тодорхойлбол зохино. Эрсдэл хариуцагч нь тодорхойлсон эрсдэлийг удирдах зохих үүрэг, эрх мэдэлтэй байвал зохино.

6.2 Сонирхогч талуудын үндсэн шаардлагыг тодорхойлох

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 4.2-д хамаарна.

Холбогдох сонирхогч талуудын үндсэн шаардлагууд болон эдгээр шаардлагад нийцэж буй байдлыг тодорхойлвол зохино. Үүнд мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний хүрээнд хамаарах аюулгүй байдлын дүрэм, хяналтыг тодорхойлсон лавлаганы бүх баримт бичгийг тодорхойлно.

Эдгээр лавлагааны баримт бичиг нь дараахь зүйлийг агуулж болох боловч үүгээр хязгаарлагдахгүй.

a) ISO/IEC 27001:2022 стандартын А хавсралт;
b) б) МАБМТ-нд хамаарах нэмэлт стандартууд;
c) в) тодорхой салбарт хамаарах нэмэлт стандартууд (жишээ нь, санхүүгийн, эрүүл мэндийн);
d) г) олон улсын болон/эсвэл үндэсний тодорхой зохицуулалтууд;
e) д) байгууллагын аюулгүй байдлын дотоод дүрэм;
f) е) гэрээ, хэлэлцээрт туссан аюулгүй байдлын дүрэм ба хяналт;
g) эрсдэлийн өмнөх арга хэмжээнд үндэслэн хэрэгжүүлсэн аюулгүй байдлын хяналт.

Үндсэн шаардлагын аливаа үл тохирлыг тайлбарлаж, үндэслэлтэй байвал зохино. Эдгээр үндсэн шаардлагууд болон тэдгээрийн нийцэл нь болзошгүй тохиолдлын үнэлгээ болон эрсдэлийн арга хэмжээний оролт байвал зохино.

6.3 эрсдэлийн үнэлгээ хийх

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 4.3-д хамаарна.

Байгууллагууд төслийн менежмент, эмзэг байдлын менежмент, аюултай тохиолдлын менежмент, асуудлын менежмент зэрэг олон янзын үйл явцад агуулагдсан эрсдэлийн эсвэл тодорхой сэдвийн дагуу гэнэтийн үнэлгээг хийж болно. Эрсдэлийн үнэлгээг хэрхэн хийхээс үл хамааран, МАБМТ-ны хүрээнд тухайн байгууллагад хамаарах бүх асуудлыг хамтад нь хамарвал зохино.

Эрсдэлийн үнэлгээ нь тухайн байгууллагад зорилгодоо хүрэхэд нөлөөлж буй эрсдэлийг удирдах шийдвэр гаргахад тусална. Иймд энэ нь хэрэв амжилттай удирдвал байгууллагын зорилгодоо хүрэх болзошгүй тохиолдлыг нэмэгдүүлэх, эрсдэл ба хяналтад чиглэвэл зохино.

МАБМТ-ны нөхцөл байдал, эрсдэлийн үнэлгээний явцад ойлгох асуудлуудын

талаарх дэлгэрэнгүй мэдээллийг ISO/IEC 27003 стандартад дурдсан болно.

6.4 Мэдээллийн аюулгүй байдлын эрсдэлийн шалгуурыг тодорхойлох, хадгалах

6.4.1 Ерөнхий

ISO/IEC 27001:2022, 6.1.2 а) нь байгууллага эрсдэлийн шалгуур үзүүлэлтээ тодорхойлох, өөрөөр хэлбэл эрсдэлийн ач холбогдлыг тодорхойлж, эрсдэлтэй холбоотой шийдвэр гаргах үндэслэлд тавих шаардлагыг тодорхойлдог.

ISO/IEC 27001 стандарт нь байгууллагын мэдээллийн аюулгүй байдлын эрсдэлийн шалгуур үзүүлэлтийг бий болгох, хадгалахад тавих шаардлагыг тодорхойлох бөгөөд үүнд:

а) эрсдэлийг хүлээн зөвшөөрөх шалгуур;

б) мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ хийх шалгуур.

Ерөнхийдөө эрсдэлийн шалгуурыг тогтоохын тулд дараахь зүйлийг анхаарч үзэх хэрэгтэй.

— үр дүн, зорилгод нөлөөлж болох тодорхойгүй байдлын шинж чанар, төрөл (биет болон биет бус);
— үр дагавар, магадлалыг хэрхэн тодорхойлох, урьдчилан таамаглах, хэмжих;
— цаг хугацаатай холбоотой хүчин зүйлүүд;
— хэмжилтийг ашиглахад туушгай байх;
— эрсдэлийн түвшинг хэрхэн тодорхойлох;
— олон эрсдэлийн хослол, дараалыг хэрхэн харгалзан үзэх;
— байгууллагын чадавхи.

хавсралт А- д үзүүлэв .

6.4.2 Эрсдэлийг хүлээн зөвшөөрөх шалгуур

ТАЙЛБАР: Энэ дэд зүйл нь ISO/IEC 27001:2022, 6.1.2 а) 1).

Эрсдэлийг үнэлэхдээ эрсдэлийг хүлээн зөвшөөрөх шалгуурыг ашиглан эрсдэлийг хүлээн зөвшөөрөх боломжтой эсэхийг тодорхойлох шаардлагатай.

Эрсдэлийн арга хэмжээд эрсдэл хүлээн зөвшөөрөх шалгуурыг ашиглан санал болгож буй эрсдэлийн арга хэмжээ нь эрсдэлийн хүлээн зөвшөөрөгдөх түвшинд хүрэхэд хангалттай эсэх, эсвэл цаашид эрсдэлийн арга хэмжээ шаардлагатай эсэхийг тодорхойлох боломжтой.

Байгууллага эрсдэл хүлээн зөвшөөрөх түвшинг тодорхойлох ёстой. Хөгжлийн явцад дараахь зүйлийг анхаарч үзэх хэрэгтэй.

a) мэдээллийн аюулгүй байдлын эрсдэлийг хүлээн зөвшөөрөх шалгуур болон байгууллагын эрсдэлийг хүлээн зөвшөөрөх ерөнхий шалгууруудын нийцтэй байдал;
b) б) эрсдэл хүлээн зөвшөөрөх шийдвэр гаргах эрх бүхий менежментийн түвшинг тодорхойлсон;
c) в) эрсдэлийг хүлээн зөвшөөрөх шалгуур нь олон босго байж болох ба хүлээн зөвшөөрөх эрх мэдлийг менежментийн янз бүрийн түвшинд хуваарилж болно;
d) эрсдэлийг хүлээн зөвшөөрөх шалгуурыг зөвхөн магадлал, үр дагаварт үндэслэх эсвэл хэтийн алдагдал болон хяналтын зардлын хоорондох зардал/үр ашгийн тэнцвэрийг авч үзэх зорилгоор өргөтгөж болно;
e) д) эрсдэлийн өөр өөр ангилалд эрсдэл хүлээн зөвшөөрөх өөр шалгуурыг хэрэглэж болно (жишээ нь, дүрэм журам, хууль тогтоомжийг дагаж мөрдөхгүй байх эрсдэл үргэлж хадгалагдаагүй, харин гэрээний шаардлагын үр дүн бол эрсдэлийг хүлээж авахыг зөвшөөрч болно) ;
f) е) эрсдэлийг хүлээн зөвшөөрөх шалгуур нь ирээдүйн нэмэлт арга хэмжээнд тавигдах шаардлагуудыг багтааж болно (жишээлбэл, сонгосон багцыг хэрэгжүүлэх арга хэмжээ авах зөвшөөрөл, үүрэг хүлээсэн тохиолдолд эрсдэлийн түвшин эрсдэл хүлээн зөвшөөрөх шалгуураас давсан ч эрсдэлийг богино хугацаанд хадгалах боломжтой). тодорхой хугацааны дотор хүлээн зөвшөөрөгдөх түвшинд хүрэх хяналт;
g) эрсдэл хүлээн зөвшөөрөх шалгуурыг тухайн байгууллагын хэрэгжүүлэх, хадгалахыг хүсэж буй эрсдэлийн хэмжээ, төрлийг харуулсан эрсдэлийн дур сонирхолд үндэслэн тодорхойлсон байх;
h) эрсдэлийг хүлээх шалгуур нь нөхцөл байдлаас хамааран үнэмлэхүй эсвэл нөхцөлт байж болно.

Эрсдэлийг хүлээх шалгуурыг дараах нөлөөлөгч хүчин зүйлсийг харгалзан тогтооно.

— байгууллагын зорилго;
— зохион байгуулалтын боломж;
— хууль эрх зүйн болон зохицуулалтын хандлага;
— үйл ажиллагаа;
— технологийн хязгаарлалт;
— санхүүгийн хязгаарлалт;
— үйл явц;
— ханган нийлүүлэгчдийн харилцаа;
— хүний хүчин зүйл (жишээ нь хувийн нууцтай холбоотой).

Нөлөөлөх хүчин зүйлсийн жагсаалт нь үүгээр хязгаарлагдахгүй. Байгууллага тухайн нөхцөл байдалдаа үндэслэн, нөлөөлөх хүчин зүйлсийг харгалзан үзнэ.

Хүлээх энгийн шалгуур (тийм/үгүй) нь практикт үргэлж хангалттай байдаггүй.

Ихэнх тохиолдолд эрсдэлийг хүлээх шийдвэрийг эрсдэлийн тодорхой түвшинд (болзошгүй тохиолдол ба үр дагаврын тодорхой хослол) гаргаж болно. Гэхдээ байгууллагад үзүүлэх нөлөө нь аль нэгээс нь бий болдог тул онцгой үр дагаврыг хүлээн зөвшөөрөх босгыг тэдгээрийн болзошгүй тохиолдлоос үл хамааран тогтоох

эсхүл үр дагавраас үл хамааран маш өндөр болзошгүй тохиолдлыг хүлээн зөвшөөрөх нөхцөл байдал байж болно.

Жишээ нь, компанийн хувьцааны үнэ цэнийг үгүй болгодог цөөн тохиолдлыг хүлээн зөвшөөрөх, эсвэл бодлогын бага зэргийн зөрчлийг тасралтгүй хянах шаардлагаас үүдэн нөөцийг байнга шавхаж байгаа тохиолдол зэрэг хоёр хүчин зүйлийн байгууллагад давамгайлах нөлөөтэйг нь түрүүлж авч үзвэл зохино.

Түүнчлэн эрсдэлийг хүлээх шалгуур нь эрсдэлийн түвшинг болзошгүй тохиолдол, үр дагаврын хослол гэж үзэхээс илүүтэйгээр болзошгүй тохиолдол ба үр дагаврыг бие даан авч үзэж, удирдлагын зардлыг багтаасан байвал зохино.

Эрсдэлийг бууруулах эрмэлзэлтэй байгууллага нь хүлээн зөвшөөрөх өндөр босгыг тогтоодог тул эрсдэл бууруулах эрмэлзэл багатай байгууллагаас илүү эрсдэлийг хүлээн авдаг. Энэ нь байгууллагыг хэт хяналтаас хамгаалж, өөрөөр хэлбэл мэдээллийн аюулгүй байдлын маш олон хяналттай байх нь тухайн байгууллагын зорилгодоо хүрэхэд саад учруулдаг.

Эрсдэл хэр удаан үргэлжлэхээс хамаарч эрсдэл хүлээх шалгуур өөр байж болно (жишээ нь, эрсдэл нь түр зуурын эсвэл богино хугацааны үйл ажиллагаатай холбоотой байж болно).

Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн хүрээнд өөрчлөлтийн үр дүнд бий болсон аливаа эрсдэлийн шалгуур үзүүлэлтүүдийг хянаж, шаардлагатай тохиолдолд шинэчилвэл зохино.

ЖИШЭЭ: Жижиг компани эхэндээ эрсдэлийг бууруулах эрмэлзэлтэй байж болох ч томрох тусам эрсдэлийг бууруулах эрмэлзэлээ бууруулдаг.

Эрсдэлийг хүлээх шалгуурыг эрх бүхий менежментийн түвшинд баталгаа.

6.4.3 Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээг гүйцэтгэх шалгуур

6.4.3.1 Ерөнхий

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 а) 2)-т хамаарна.

Эрсдэлийн үнэлгээний шалгуур нь эрсдэлийн ач холбогдлыг түүний үр дагавар, болзошгүй тохиолдол, эрсдэлийн түвшингээр хэрхэн тодорхойлохыг заана.

Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний шалгуур нь эрсдэлийн менежментийн үйл ажиллагааны зохистой байдлыг харгалзан үзвэл зохино.

Иймд дараахь зүйлсийг анхаарч үзнэ:

a) мэдээллийн ангиллын түвшин;
b) мэдээллийн тоо хэмжээ, аливаа төвлөрөл;

c) мэдээллийг ашигладаг бизнесийн үйл явцын стратегийн үнэ цэнэ;
d) мэдээлэлтэй холбоотой мэдээлэл, өмчийн эгзэгтэй байдал;
e) бэлэн байдал, нууцлал, хүртээмжтэй байдлын үйл ажиллагааны болон бизнесийн ач холбогдол;
f) сонирхогч талуудын хүлээлт, төсөөлөл (жишээ нь , дээд удирдлага);
g) нэр хүндээ алдах зэрэг сөрөг үр дагавар;
h) байгууллагын эрсдэлийн шалгуурт нийцсэн байдал.

Эрсдэлийн үнэлгээний шалгуурууд буюу тэдгээрийг тодорхойлох албан ёсны үндэслэлийг бүх төрлийн эрсдэлийн үнэлгээнд зориулан байгууллагын хэмжээнд стандартчилсан байвал зохино. Учир нь энэ нь бизнесийн олон салбартай холбоотой эрсдэлийн талаар харилцах, харьцуулах, нэгтгэх ажлыг хөнгөвчилнө.

Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний шалгуурууд нь ихэвчлэн:

— үр дагавар;
— болзошгүй тохиолдол;
— эрсдэлийн түвшин.

6.4.3.2 Үр дагаврын шалгуур

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 a) 2)-т хамаарна..

ISO/IEC 27001 нь МАБМТ-ны хамрах хүрээнд мэдээллийн нууцлал, хүртээмжтэй байдал, хүртээмжийг хадгалах, алдахад шууд болон шууд бусаар нөлөөлөх үр дагаврыг авч үзнэ. Мэдээллийн нууцлал, хүртээмжтэй байдал, бэлэн байдал алдагдсаны улмаас байгууллага, хувь хүнд учирсан хохирол, үр дагавар, хохирлын хэмжээг харгалзан, үр дагаврын шалгуур үзүүлэлтийг боловсруулж, тодорхойлсон байвал зохино. Үр дагаврын шалгуур үзүүлэлтийг тодорхойлохдоо дараахь зүйлийг анхаарч үзнэ: .

a) хувь хүн, бүлэг хүмүүсийн амь нас хохирох, гэмтэл учруулах;
b) эрх чөлөө, нэр төр, хувийн нууцыг хамгаалах эрхээ алдах;
c) боловсон хүчин, оюуны өмч (ур чадвар, туршлага)-өө алдагдах;
d) дотоод болон гуравдагч талын үйл ажиллагааны доголдол (жишээ нь бизнесийн үйл ажиллагаа эсвэл үйл явцад гэмтэл учрах);
e) төлөвлөгөө болон дуусах хугацаанд үзүүлэх нөлөө;
f) бизнесийн болон санхүүгийн үнэ цэнээ алдах;
g) бизнесийн давуу тал буюу зах зээлд эзлэх байр сууриа алдах;
h) олон нийтийн итгэл, нэр хүндэд хохирол учруулах;
i) хууль тогтоомж, зохицуулалтын болон дүрэм журмын шаардлагыг зөрчих;
j) гэрээ, үйлчилгээний түвшинг зөрчих;
k) сонирхогч талуудад үзүүлэх сөрөг нөлөө;
l) байгаль орчинд үзүүлэх сөрөг нөлөө, бохирдол.

Үр дагаврын шалгуур нь тухайн байгууллага мэдээллийн аюулгүй байдлын

болзошгүй тохиолдлын ач холбогдлыг тухайн байгууллагад хэрхэн ангилж байгааг тодорхойлдог. Үр дагаврын хэд хэдэн ангиллыг ашиглах, тэдгээрийг хэрхэн тодорхойлсон, ангилал тус бүр ямар үр дагавартай холбоотой болохыг тодорхойлох нь чухал юм. Ихэвчлэн байгууллагын дотоод болон гадаад нөхцөл байдлаас шалтгаалан үр дагаврын шалгуур нь байгууллага өүрт өөр өөр байдаг.

1-Р ЖИШЭЭ: Санхүүгийн жилд байгууллагын данснаас гаргахаар бэлтгэсэн дээд хэмжээ ба үлдээх хамгийн бага хэмжээ нь байгууллагын үр дагаврын хуваарь (scale)-ийн бодит дээд доод хязгаарыг мөнгөн дүнгээр илэрхийлж чадна.

Энэхүү нөхцөл байдлаас хамааралтай хүрээг дараа нь хэд хэдэн үр дагаврын ангилалд хуваж болох бөгөөд тэдгээрийн тоо, тархалт нь байгууллагын эрсдэлийн ойлголт, эрсдлийг бууруулах эрмэлзлээс хамаарна. Мөнгөний үр дагаврын хуваарь(scale)-ийн хэмжээг ихэвчлэн арван жилээр эсвэл 10-ын зэрэгтэй (жишээ нь 100-аас 1000; 1-ээс 10 000 гэх мэт) логарифмын хуваариар илэрхийлдэг боловч тухайн байгууллагын нөхцөл байдалд илүү тохирох өөр тоон схемийг ашиглаж болно.

Байгууллагын өөр өөр салбар эсвэл хэлтэст үр дагаврыг эхлээд мөнгөөр бус янз бүрийн аргаар илэрхийлж болох бөгөөд эдгээр янз бүрийн илэрхийлэлийг ижил төстэй үр дагаврын түвшинг баталгаажуулахын тулд нийтлэг хуваарь(scale)-тай холбон зөв харьцуулж тайлбарлах нь ашигтай байдаг. Энэ нь нийт эрсдэлийг нэгтгэх боломжийг олгоно.

2-Р ЖИШЭЭ: Мэдээллийн зөрчил, түүнчлэн хүний хувийн нууцад нөлөөлж болзошгүй байдал нь МАБМТ-нд хамаарах мэдээллийн нууцлал, хүртээмжтэй байдал, бэлэн байдлыг алдахад хүргэдэг. Энэ нь өгөгдөл хамгаалах талаар хууль тогтоомжийн мөрдөлтөд үл тохиролд хүргэнэ. Болзошгүй үр дагавар нь мэдээлэл алдагдах, мэдээлэлтэй холбоотой өмч, мэдээллийн үйл явц алдагдах, үйл ажиллагааны бизнесийн зорилго, төлөвлөсөн бизнесээ алдах зэрэг болно.

6.4.3.3 Болзошгүй тохиолдлын шалгуур

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 a) 2).

Боллзошгүй тохиолдлын шалгуурыг тодорхойлох нь дараахь зүйлээс хамаарна.

a) санамсаргүй буюу бодит тохиолдол;
b) аюул заналд холбогдох мэдээллийн өмч эсвэл мэдээллийн өртөх зэрэг;
c) байгууллагын эмзэг байдлыг ашигласан байдал;
d) технологийн алдаа;
e) хүний үйлдэл, эс үйлдэхүй.

Болзошгүй тохиодлыг магадлал (тодорхой хугацаанд тохиолдох боломж) эсвэл давтамж (тодорхой хугацаанд тохиолдох дундаж тоо) -аар илэрхийлж болно. Болзошгүй тохиолдлыг ихэвчлэн давтамжаар илэрхийлж, харилцдаг бөгөөд магадлалыг нэгтгэх үед зөвхөн магадлалаар илэрхийлсэн болзошгүй тохиолдлыг ашиглаж болно.

Болзошгүй тохиодлын шалгуур нь хүлээгдэж буй урьдчилан таамаглаж удирдах боломжтой болзошгүй тохиолдлын хүрээг хамарвал зохино.

Удирдах боломжийн хязгаараас гадна эрсдэлийн менежментийн зохих шийдвэр гаргахын тулд (онцгой тохиолдол гэж тодорхойлох) нэг буюу бусад хязгаар хэтэрсэн гэдгийг хүлээн зөвшөөрөх шаардлагатай байдаг. Хэрэв төгсөгөлийн хуваарь(scale)-ууд хэт том бол энэ нь ихэвчлэн хэт тойм тоог гаргадаг бөгөөд үнэлгээнд алдаа гаргахад хүргэдэг. Энэ нь ялангуяа болзошгүй тохиолдолыг экспоненциалаар илэрхийлсэн масштабын дээд төгсгөлд багтах тохиолдолд тохиолддог, учир нь дээд муж дахь өсөлтүүд нь маш өндөр байдаг.

Хэдийгээр бараг бүх зүйл "боломжтой" боловч хамгийн түрүүнд анхаарах ёстой эрсдэлийн эх үүсвэрүүд нь тухайн байгууллагын нөхцөл байдал болон МАБМТ-ны хамрах хүрээнд хамгийн их хамааралтай байх магадлалтай хүмүүс юм.

6.4.3.4 Эрсдэлийн түвшинг тодорхойлох шалгуур

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 a) 2)-т хамаарна..

Эрсдэлийн түвшинг хуваарь(scale)-илах зорилго нь эрсдэл хариуцагч эрсдэлийг хадгалах эсвэл эрсдлийн талаар шийдвэр гаргахад нь туслах, эрсдэлийн арга хэмжээг эрэмбэлэх явдал юм. Тодорхой эрсдэлийн үнэлэгдсэн түвшин нь тухайн эрсдэлийн яаралтай байдлыг тодорхойлоход байгууллагад тусална.

Нөхцөл байдлаас хамааран эрсдэлийн зохих түвшин (ямар ч хяналтыг тооцохгүйгээр) эсвэл одоогийн эрсдэлийн түвшинг (хэрэгжүүлсэн аливаа хяналтын үр нөлөөг харгалзан үзсэн)-г харгалзан үзэх нь зүйтэй. Байгууллага нь дараахь зүйлийг харгалзан эрсдэлийн зэрэглэлийг тогтооно:

a) үр дагаврын шалгуур ба болзошгүй тохиодлын шалгуур;
b) мэдээллийн аюулгүй байдлын тохиолдлууд нв стратегийн, тактикийн болон үйл ажиллагааны түвшин бүхий үр дагавар (үүнийг хамгийн муу тохиолдол гэж тодорхойлж болно, эсвэл ижил үндэслэлийг дараалан ашигласан тохиолдолд);
c) хууль эрх зүйн болон зохицуулалтын шаардлага, гэрээний үүрэг;
d) гуравдагч этгээдэд үзүүлэх урьдчилан таамаглаагүй үр дагаврыг агуулсан байгууллагын хамрах хүрээний хил хязгаараас давсан эрсдэл.

Үнэлэгдсэн эрсдлийг шинжлэхийн тулд эрсдэлийн түвшний шалгуур шаардлагатай.

Эрсдэлийн түвшний шалгуур нь чанарын (жишээ нь, маш их, өндөр, дунд, бага) эсвэл тоон (жишээ нь, тухайн хугацааны мөнгөний алдагдал, хүний амь нас, зах зээлд эзлэх хувь хэмжээгээр илэрхийлэгдэх) байж болно.

ЖИШЭЭ: Эрсдэлийг жилийн хүлээгдэж буй алдагдлын хэмжээ, өөрөөр хэлбэл дараагийн жилийн үр дагаврын дундаж мөнгөн дүнгээр тодорхойлж болно.

Тоон болон чанарын шалгуурыг ашигласан эсэхээс үл хамааран үнэлгээний

хуваарь(scale) нь бүх сонирхогч талуудад ойлгомжтой жишиг хуваарь(scale)-тай байна. Эрсдэлийн шинжилгээ болон эрсдэлийн үнэлгээний хүчин төгөлдөр, тууштай, найдвартай байдлыг хангахын тулд албан ёсны тулгуур хуваарь(scale)-тай шалгалт тохируулгыг тогтмол харьцуулалт хийнэ. .

Хэрэв чанарын аргыг хэрэглэж байгаа бол аливаа чанарын хуваарь(scale)-ийн түвшин нь хоёрдмол утгагүй, түүний өсөлтийг тодорхой зааж, түвшин тус бүрийн чанарын тодорхойлолтыг объектив хэлээр илэрхийлж, түвшин давхцахгүй байна. Өөр өөр хуваарь(scale) ашиглах үед (жишээ нь, өөр өөр бизнесийн хүрээн дэх эрсдэлийг шийдвэрлэхэд) үр дүнг харьцуулж болохуйц байхын тулд ижил тэнцүү (equivalency) байна.

6.5 Тохиромжтой аргыг сонгох

ТАЙЛБАР: Энэ дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 b)-т хамаарна.

Ер нь мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн арга нь байгууллагын бусад эрсдэлийг удирдахад ашигладаг аргуудтай нийцстэй байна.

Сонгосон аргыг баримтжуулна.

ISO/IEC 27001:2022, 6.1.2 б)-ын дагуу Байгууллага МАБМТ-ны хамрах хүрээндээ мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээг давтан хийх шаардлагатай бөгөөд ингэснээр тууштай, үнэн зөв, харьцуулах боломжтой үр дүнг бий болгоно. Сонгосон аргын үр дүн нь дараах шинж чанартай байна:

— тууштай байдал: ижил эрсдэлийг өөр өөр хүмүүс үнэлсэн эсхүл өөр өөр нөхцөлд ижил хүмүүс хийсэн үнэлгээ нь ижил үр дүнг гаргах ёстой;
— харьцуулах боломж: өөр өөр эрсдэлд хийсэн үнэлгээ нь эрсдэлийн түвшин ижил үед харьцуулж боломжтой үр дүнг бий болгохуйцаар эрсдэлийн үнэлгээний шалгуурыг тодорхойлох;
— үнэн зөв байдал: үнэлгээ нь бодит байдалд аль болох ойртсон үр дүнг гаргах ёстой.

Мэдээллийн аюулгүй байдлын эрсдэлийг удирдахад үйл ажиллагааны эрсдэлийн менежментийн аргуудыг ихэвчлэн ашиглана. Сонгосон арга нь үлдэгдэл эрсдэлийг ашиглахтай холбоотой ямар ч тохиромжтой аргыг хэрэглэж болно. Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн хамгийн түгээмэл хэрэглэгддэг аргууд нь эрсдэлийн болзошгүй тохиолдол, үр дагаврыг үнэлэхдээ одоогийн эрсдэлийг ашигладаг.

7 Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явц

7.1 Ерөнхий

Байгууллага нь мэдээллийн эрсдэлийг үнэлэх буюу мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явцыг тодорхойлохын тулд байгууллагын эрсдэлийн үнэлгээний үйл явцыг (хэрэв бий болгосон бол) ашиглана.

Эрсдэлийн үнэлгээ нь үр дагавар, болзошгүй тохиолдол эсвэл бусад тогтоосон шалгуурт үндэслэн, арга хэмжээний хэтийн төлөвт нийцүүлэн, эрсдэлийг эрэмбэлэх боломжийг эрсдэл хариуцагчдад олгодог.

Эрсдэлийн үнэлгээний нөхцөл байдалд хамрах хүрээний тайлбар, зорилго, эрсдэлийн үнэлгээнд нөлөөлж буй дотоод болон гадаад асуудлуудыг оруулж тодорхойлно.

Эрсдэлийн үнэлгээ нь дараахь үйл ажиллагаанаас бүрдэнэ.

a) эрсдэлийг тодорхойлох буюу эрсдэлийг илрүүлэх, таних, тайлбарлах үйл явц (эрсдэлийг тодорхойлох талаар дэлгэрэнгүй мэдээллийг 7.2- т оруулсан болно);
b) эрсдэлийн шинжилгээ буюу эрсдэлийн төрлийг ойлгох, эрсдэлийн түвшинг тодорхойлох үйл явц. Эрсдэлийн шинжилгээ нь эрсдэлийн шалтгаан, эх үүсвэр, тодорхой тохиолдол тохиох болзошгүй тохиолдол, уг тохиолдол нь үр дагавартай байх болзошгүй тохиолдол, эдгээр үр дагаврын ноцтой байдлыг харгалзан үзэх явдал юм. (эрсдэлийн шинжилгээний талаар дэлгэрэнгүйг 7.3-т өгсөн болно) ;
c) эрсдэлийн үнэлгээ нь эрсдэлийн шинжилгээний үр дүнг эрсдэлийн шалгууртай харьцуулах үйл явц бөгөөд эрсдэл ба/эсвэл түүний ач холбогдлыг хүлээн зөвшөөрөх боломжтой эсэхийг тодорхойлох, үнэлэгээ хийгдсэн эрсдэлийг эрэмбэлж, эрсдэлийн арга хэмжээнд зориулах яюдал юм. Энэхүү харьцуулалтад үндэслэн арга хэмжээ хэрэгтэй эсэхийг авч үзнэ. (эрсдэлийн үнэлгээний талаарх дэлгэрэнгүйг 7.4-т өгсөн болно).

Эрсдэлийн үнэлгээний үйл явц нь аль болох тууштай, үнэн зөв, давтагдах боломжтой үр дүнг баталгаажуулахын тулд хангалттай нарийвчилсан арга (6.5-ыг үзнэ үү) болон хэрэгсэлд суурилсан байвал зохино. Цаашилбал, эрсдэлийн түвшин нэмэгдсэн эсвэл буурсан эсэхийг тодорхойлохын тулд үр дүнг харьцуулах боломжтой байх ёстой.

Байгууллагын мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн арга нь байгууллагын эрсдэлийн менежментийн ерөнхий аргатай нийцэх ёстой бөгөөд ингэснээр мэдээллийн аюулгүй байдлын аливаа эрсдэлийг байгууллагын бусад эрсдэлтэй харьцуулж, зөвхөн тусад нь авч үзэхгүй байвал зохино.

ISO/IEC 27001 нь ISO/IEC 27001:2022, 6.1.2-д заасан шаардлагыг биелүүлэхийн тулд тодорхой аргыг ашиглахыг шаарддаггүй. Гэсэн ч үнэлгээний хоёр үндсэн арга

байдаг: тохиолдолд суурилсан арга, өмчид суурилсан арга. Тэдгээрийг 7.2.1-д дэлгэрэнгүй авч үзсэн.

7.2 Мэдээллийн аюулгүй байдлын эрсдэлийг тодорхойлох

7.2.1 Мэдээллийн аюулгүй байдлын эрсдэлийг тодорхойлох, тайлбарлах

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 c) 1)-д хамаарна.

Оролт: Байгууллага болон бусад байгууллагын мэдээллийн аюулгүй байдлын зорилгод хүрэхэд сөргөөр нөлөөлж болзошгүй тохиолдолууд.

Ажиллагаа: Мэдээллийн нууцлал, нэгдмэл байдал, хүртээмжтэй байдлыг алдагдахтай холбоотой эрсдэлийг тодорхойлвол зохино.

Өдөөгч: Эрсдэл хариуцагчид, сонирхогч талууд болон/эсвэл шинжээчид мэдээллийн аюулгүй байдлын зорилгод нөлөөлж болох шинэ эсвэл өөрчлөгдсөн тохиолдлыг илрүүлэх, хайх шаардлагатай байдаг.

Гаралт: Тодорхойлсон эрсдэлүүдийн жагсаалт.

Арга зүй:

Эрсдэлийг тодорхойлох нь эрсдэлийг олох, таних, тайлбарлах үйл явц юм. Энэ нь эрсдэлийн эх үүсвэр, тохиолдлыг тодорхойлоход хүргэнэ.

Эрсдэлийг тодорхойлох зорилго нь мэдээллийн аюулгүй байдлын зорилгод хүрэхийг зогсоох, нөлөөлөх, хойшлуулах боломжтой эдгээр тохиолдлуудад үндэслэн эрсдэлийн жагсаалтыг гаргах явдал юм.

Тодорхойлсон эрсдэлүүд нь хэрэв хэрэгжвэл зорилгодоо хүрэхэд нөлөөлж чадах эрсдэлүүд байвал зохино.

ISO/IEC 27001:2022, 6.1.2 c) нь байгууллага мэдээллийн аюулгүй байдлын эрсдэлийг тодорхойлох мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явцыг бий болгож, хэрэгжүүлэхийг шаардана. Эрсдэлийг тодорхойлоход ихэвчлэн хоёр аргыг хэрэглэдэг.

a) Тохиолдолд суурилсан арга: Эрсдэлийн эх үүсвэрийг авч үзэж, сонирхогч талууд эдгээр эрсдэлийг хүссэн зорилгодоо хүрэхийн тулд хэрхэн ашиглах стратегийн хувилбарыг тодорхойлох,
b) Өмчид суурилсан арга: өмч, аюул занал, эмзэг байдлын талаар дэлгэрэнгүй авч үзэж, үйл ажиллагааны хувилбаруудыг тодорхойлох.

Тохиолдолд суурилсан аргын үндэс нь тохиолдол, үр дагаврыг үнэлэх замаар эрсдэлийг тодорхойлж, үнэлэх боломжтой юм. Тохиолдол, үр дагаврыг ихэвчлэн

дээд удирдлага, эрсдэл хариуцагчийн асуудлыг илрүүлэх болон байгууллагын нөхцөл байдлыг тодорхойлох шаардлагууд (ISO/IEC 27001:2022, 4-р зүйл)-ыг дэлгэрүүлэх үед тодорхойлж болно . Байгууллагын дээд удирдлага болон бизнесийн үйл явцыг хариуцдаг хүмүүстэй ярилцлага хийх нь зөвхөн холбогдох тохиолдол, үр дагаврыг төдийгүй эрсдэл хариуцагчдийг тодорхойлоход тусална.

Тохиолдолд суурилсан арга нь дэлгэрэнгүй түвшинд өмчийг тодорхойлоход их хэмжээний цаг зарцуулахгүйгээр өндөр түвшний буюу стратегийн хувилбаруудыг бий болгож чадна. Энэ нь байгууллага эрсдэлийн арга хэмжээг чухал эрсдэлд чиглүүлэх боломжийг бүрдүүлдэг. Энэхүү аргыг ашиглан тохиолдлыг үнэлэх нь эрсдэл удаан хугацаанд өөрчлөгдөөгүй, түүхэн өгөгдлийг ашиглан, оролцогч сонирхогч талууд зорилгодоо хүрэх боломжийг олгодог. Гэсэн хэдий ч түүхэн өгөгдөл байхгүй эсвэл найдвартай биш эрсдэлтэй тохиолдолд шинжээчийн мэдлэг, туршлагад үндэслэсэн зөвлөгөө эсвэл эрсдэлийн эх үүсвэрийг судлах нь үнэлгээнд тусална.

Өмчид суурилсан аргын үндэс нь хөрөнгө, аюул занал, эмзэг байдлыг шалгах замаар эрсдэлийг тодорхойлж, үнэлэх боломжтой болно. Өмч гэдэг нь байгууллагад үнэ цэнэтэй зүйл бөгөөд хамгаалалт шаарддаг. Мэдээллийн систем нь үйл ажиллагаа, үйл явц, хамгаалах ёстой мэдээллээс бүрддэг гэдгийг харгалзан өмчийг тодорхойлно. Өмчийг төрөл, ач холбогдлоор нь үндсэн болон туслах өмч гэж тодорхойлж, тэдгээрийн хамаарал, эрсдэлийн эх үүсвэр болон байгууллагын сонирхогч талуудтай харьцах харьцаа зэргийг онцолж болно. Аюул занал нь өмчийн эмзэг байдлыг ашиглан холбогдох мэдээллийн нууцлал, хүртээмжтэй байдал болон/эсвэл хүртээмжийг алдагдуулдаг. Хэрэв МАБМТ-ны хүрээнд хөрөнгө, аюул занал, эмзэг байдлын бүх зөв хослолыг дугаарлаж чадвал онолын хувьд бүх эрсдэлийг тодорхойлох болно. Эрсдэлийн үнэлгээний цаашдын үе шатанд мэдээлэлд хамаарах өмч болон мэдээлэл боловсруулах төхөөрөмжид хамаарах өмчийн жагсаалтыг гаргах шаардлагатай.

Өмчид суурилсан арга нь тухайн хөрөнгөд хамаарах аюул, эмзэг байдлыг тодорхойлж, эрсдэлийн тодорхой арга хэмжээг нарийвчилсан түвшинд тодорхойлох боломжийг байгууллагад олгодог.

Аргуудын талаар дэлгэрэнгүйг А хавсралтад өгсөн болно .

Зарчмын хувьд хоёр арга нь зөвхөн тодорхойлсон түвшнээрээ ялгаатай. Хоер арга хоюулаа эрсдлийн ижил хувилбарыг дүрсэлж болно. Жишээ нь, мэдээллийн өмч нь нарийвчилсан түвшинд, бизнесийн үйлчлэл нь ерөнхий түвшинд байна. Тохиолдолд суурилсан үнэлгээг ашиглан эрсдэлийн дагалдах эх үүсвэрийг тодорхойлох нь ерөнхийдөө хувилбарын ерөнхий түвшнээс нарийвчилсан түвшин рүү доош нарийвчлахийг шаардах бөгөөд, харин өмчид суурилсан үнэлгээ нь үр дагавар хэрхэн хуримтлагддагыг харахын тулд дээш нь хайлт хийж хувилбарт хүрдэг.

Эрсдэлийг тодорхойлох нь тун чухал бөгөөд энэ үе шатанд тодорхойлогдоогүй мэдээллийн аюулгүй байдлын эрсдэлийг цаашдын шинжилгээнд оруулахгүй.

Эрсдэлийг тодорхойлохдоо эрсдэлийн эх үүсвэр байгууллагын хяналтанд байгаа эсэхээс үл хамааран, толорхой эрсдэлийн эх үүсвэр тодорхойгүй үед ч эрсдэлийг харгалзан үзэх ёстой. Ялангуяа эрсдэлийн нарийн төвөгтэй хувилбаруудыг үнэлэхийн тулд эрсдэлийн давтан үнэлгээг хийнэ. Эхний ээлжинд өндөр түвшиний ажиглалтад төвлөрч, дараагийн амжилттай үе шатууд нь эрсдэлийн үндсэн шалтгааныг олж тогтоох хүртэл авч үзнэ.

Эрсдэлийг тодорхойлох аливаа аргыг ISO/IEC 27001:2022, 6.1.2 b) стандартын шаардлагыг хангасан тууштай, үнэн зөв, харьцуулж болохуйц үр дүнг гарах хүртэл ашиглана.

Мэдээллийн аюулгүй байдлын эрсдэлийн менежмент нь эрсдэлийг хэрхэн бүтэцлэж, бүлэглэх, нэгтгэх, хуваах, тайлбарлах зэрэг дурын эсвэл хязгаарлалтын аргад захирагдахгүй. Эрсдэл бусад эрсдэлтэй хэсэгчлэн давхцаж, дэд бүлэг үүсгэж эсхүл бусад эрсдэлийн тодорхой тохиолдлыг үүсгэж болно. Эрсдэлийн арга хэмжээний зорилгоор бие даасан эрсдэлийг хянахын тулд илүү өргөн хүрээтэй эсвэл нэгтгэсэн эрсдэлээс тусад нь авч үзнэ.

ЖИШЭЭ 1 Давхардсан хоёр эрсдэлийн жишээ: (1) төв байранд гал гарах эрсдэлтэй; (2) төв байр болон бусад хэд хэдэн барилга байгууламжид гал түймэр гарах нь нягтлан бодох бүртгэлийн хэлтэсийн үйл ажиллагаанд нөлөөлөх эрсдэлтэй.

Эрсдэлийн тодорхой тохиолдлын жишээ: (1) өгөгдөл алдагдах тохиолдол; (2) хувийн мэдээллийн өгөгдөл алдагдах тохиолдол байна.

Хоёрдахь эрсдэл нь эхний эрсдэлийн тодорхой тохиолдол боловч эхний эрсдэлээс өөр шинж чанар, хяналттай байх магадлалтай бөгөөд үүнийг илүү өргөн хүрээтэй эхний эрсдэлээс тусад нь удирдах нь чухал юм.

Тухайн байгууллагын нөхцөл байдлыг авч үзэж буй түвшинд эрсдэлүүд бие биентэйгээ хамааралгүй тохиолдолд тэдгээр эрсдэлийг нэгтгэж болохгүй. Эрсдэлийн удирдлагын төсөв боловсруулах зорилгоор арга хэмжээний хувилбаруудыг төлөвлөхдөө нэгтгэсэн эрсдэлүүдийг тус тусад нь авч үзэх шаардлагатай бөгөөд учир нь тэдгээрийг удирдахад өөр өөр хяналт шаардлагатай байж болно.

ЖИШЭЭ 2 Дата төв нь үер, гал түймэр, цахилгаан эрчим хүчний огцом өсөлт, эвдэн сүйтгэх зэрэг хэд хэдэн бие даасан аюулд өртөж болно.

Нэгтгэсэн эрсдэлийн ерөнхий түвшинг тооцоолохын тулд эдгээр тохиолдлын бие даасан эрсдэлийг эрсдэлийн ерөнхий түвшинд нэгтгэж болох боловч эдгээр тохиолдол тус бүр нь эрсдэлийг удирдахад өөр өөр хяналт шаарддаг тул эрсдэлийн арга хэмжээний зорилгоор тэдгээрийг тус тусад нь авч үзэж, тодорхойлох хэрэгтэй. Эрсдэлийг (болзошгүй тохиолдол ба үр дагаврын хослол) шууд нэгтгэж болохгүй.

7.2.2 Эрсдэл хариуцагчдыг тодорхойлох

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 c) 2).-д

хамаарана.

Оролт: Тодорхойлсон эрсдэлүүдийн жагсаалт.

Ажиллагаа: Эрсдэл нь эрсдэл хариуцагчид хамааралтай байна.

Өдөөгч: Эрсдэл хариуцагчийг тодорхойлох нь дараахь тохиолдолд шаардлагатай:

— өмнө нь хийж байгаагүй;
— эрсдэлтэй холбоотой бизнесийн хэсэгт боловсон хүчний өөрчлөлт гарсан;

Гаралт: Холбогдох эрсдэл болон эрсдэл хариуцагчдын жагсаалт.

Хэрэгжүүлэх арга зүй:

Эрсдэл хариуцагчид нь дээд удирдлага, аюулгүй байдлын хороо, үйл явцыг хариуцагчид, үйл ажиллагааг эзэмшигчид, хэлтсийн менежерүүд болон өмчийн эзэд байж болно.

Байгууллага эрсдэл хариуцагчийг тодорхойлохдоо байгууллагын эрсдэлийн үнэлгээний үйл явцыг (хэрэв тогтоосон бол) ашиглана, эсхүл эрсдэл хариуцагчийг тодорхойлох шалгуурыг тодорхойлбол зохино. Ийм шалгуур нь эрсдэл хариуцагчийн талаар дараахь зүйлсийг анхаарч үзэх хэрэгтэй.

— хариуцаж буй эрсдэлийн талаар үүрэг хүлээсэн, эрсдэлийг удирдах эрх мэдэлтэй байх, өөрөөр хэлбэл тухайн байгууллагад энэ эрх мэдлээ бодитоор хэрэгжүүлэх боломжийг олгосон албан тушаалтай байх;
— тулгамдаж буй асуудлуудыг ойлгож, үндэслэлтэй шийдвэр гаргах боломжтой байх (жишээ нь, эрсдэлийг хэрхэн шийдвэрлэх талаар).

Эрсдэлийн түвшин, эрсдэл ямар өмчид хамаарах нь эрсдэл хариуцагчийг тодорхойлох үндэс болно.

Хуваарилалт нь эрсдэлийн үнэлгээний үйл явцын нэг хэсэг болох ёстой.

7.3 Мэдээллийн аюулгүй байдлын эрсдэлийг шинжлэх

7.3.1 Ерөнхий

Эрсдэлийн шинжилгээний зорилго нь эрсдэлийн түвшинг тодорхойлоход оршино.

ISO/IEC 27001 стандартад ISO 31000 стандартыг ерөнхий загвар болгон эш татсан болно. ISO/IEC 27001:2022 стандартын 6.1.2-д дурдсаны дагуу тодорхойлсон эрсдэл тус бүрийн эрсдэлийн шинжилгээ нь эрсдэлийн түвшинг тодорхойлохын тулд эрсдэлээс үүсэх үр дагавар, эрсдэлийн болзошгүй тохиолдлын үнэлгээнд үндэслэсэн байхыг шаардана.

Үр дагавар, болзошгүй тохиолдолд суурилсан эрсдэлийн шинжилгээ хийх арга техник нь:

a) чанарын, шалгуур үзүүлэлтийн хуваарь(scale)-ийг ашиглан (жишээ нь, өндөр, дунд, бага); эсвэл
b) тоон, тоон утга бүхий хуваарь(scale)-ийг ашиглан (жишээлбэл, мөнгөний зардал, давтамж эсвэл тохиолдох магадлал); эсвэл
c) хагас-тоон, тогтоосон утга бүхий чанарын хуваарь(scale)-ийг ашиглан,

Амжилттай удирдаж чадвал байгууллагын зорилгодоо хүрэх магадлалыг сайжруулах эрсдэл, хяналтад эрсдэлийн шинжилгээг чиглүүлбэл зохино. Эрсдэлийн үнэлгээ, ялангуяа болзошгүй тохиолдол, үр дагаврыг үнэлэхэд ихээхэн цаг зарцуулагддаг. Эрсдэлийн менежментийн талаар үр дүнтэй шийдвэр гаргахын тулд болзошгүй тохиолдол, үр дагаврын анхны, тойм тооцоог ашиглахад хангалттай.

7.3.2 Болзошгүй үр дагаврыг үнэлэх

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 d) 1)-д хамаарна.

Оролт: Тодорхойлсон тохиолдлууд буюу эрсдэлийн хувилбар, үүнд эрсдэлийн эх үүсвэр, бизнесийн үйл явц, бизнесийн зорилго, үр дагаврын шалгуурын жагсаалт. Цаашилбал, одоо байгаа бүх хяналтын жагсаалт, тэдгээрийн үр нөлөө, хэрэгжилт, ашиглалтын байдал.

Ажиллагаа: Мэдээллийн нууцлал, нэгдмэл байдал, хүртээмжтэй байдлыг зохих ёсоор хадгалаагүйгээс үүсэх үр дагаврыг тодорхойлж, үнэлвэл зохино.

Өдөөгч: Үр дагаварыг дараах тохиолдолд үнэлэх шаардлагатай болно:

— өмнө нь хийгээгүй;
— "эрсдэлийн тодорхойлолт"-оор гаргасан жагсаалт өөрчлөгдсөн;
— эрсдэл хариуцагчид эсвэл сонирхогч талууд үр дагаврыг тодорхойлдог нэгжээ өөрчилсөн; эсвэл
— үр дагаварт нөлөөлж буй хамрах хүрээ, нөхцөл байдал өөрчлөгдсөн.

Гаралт: Эрсдэлийн хувилбаруудтай холбоотой болзошгүй үр дагаврын жагсаалт, ашигласан аргаас хамааран хөрөнгө, тохиолдолтой холбоотой үр дагаваруудын хамт.

Хэрэгжүүлэх арга зүй:

Мэдээллийн аюулгүй байдлыг зохих ёсоор хадгалахгүй байх нь түүний нууцлал, нэгдмэл байдал, хүртээмжтэй байдлыг алдагдахад хүргэнэ. Нууцлал, нэгдмэл байдал, хүртээмжтэй байдлыг алдах нь байгууллага болон түүний зорилгын хувьд цаашдын үр дагаварт хүргэж болзошгүй. Мэдээллийн нууцлал, хүртээмжтэй байдал, хүртээмжтэй байдал алдагдах тохиолдолд юу тохиолдохыг харгалзан мэдээллийн аюулгүй байдлын үр дагавраас доошоо чиглэсэн үр дагаврын шинжилгээг хийж болно. Иэхэвчлэн эрсдэл хариуцагч нь тухайн тохиолдол тохиовол үр дагаврыг нь тооцоолж чаддаг. Дараахь элементүүдийг анхаарч үзвэл

зохино.

— үйл ажиллагааг тасалдуулах, саатуулахаас учирсан тохиолдлын улмаас учирсан хохирлыг (цаг хугацаа, өгөгдөл) тооцоо (эсвэл туршлагад үндэслэн хэмжих);
— үр дагаврын ноцтой байдлын тооцоо/төсөөлөл (жишээ нь, мөнгөөр илэрхийлсэн);
— нөхөн сэргээх зардал нь дотооддоо (эрсдэл хариуцагч баг) хийх боломжтой эсэх, эсвэл гадны байгууллагыг дуудах шаардлагатай эсэхээс хамаарна.

7.3.3 Болзошгүй тохиолдлыг үнэлэх

ТАЙЛБАР: Энэ дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 d) 2)-д хамаарна.

Оролт: Тодорхойлсон холбогдох тохиолдол эсвэл эрсдэлийн хувилбаруудын жагсаалт, үүнд эрсдэлийн эх үүсвэр, бизнесийн үйл явц, бизнесийн зорилго, болзошгүй тохиолдлын шалгуурын хамт. Түүнчлэн, одоо байгаа бүх хяналтын жагсаалт, тэдгээрийн үр нөлөө, хэрэгжилт, ашиглалтын байдал.

Ажиллагаа: Боломжит эсвэл бодит хувилбаруудыг үүсэх болзошгүй тохиолдлыг тогтоосон болзошгүй тохиолдлын шалгуурыг ашиглан үнэлж, илэрхийлнэ.

Өдөөгч: Үр дагавартай зэрэгцэн болзошгүй тохиолдлыг үнэлэх нь эрсдэлийн түвшинг тодорхойлох үед эрсдэлийн үнэлгээний үйл явцын гол үйл ажиллагаа юм.

Болзошгүй тохиолдлыг үнэлэх нь дараахь тохиолдолд зайлшгүй шаардлагатай болно.

— өмнө нь хийгдээгүй;
— хамрах хүрээ, нөхцөл байдлын өөрчлөлт нь болзошгүй тохиолдолд нөлөөлж болно гэж тодорхойлсон;
— хэрэгжүүлсэн хяналтад сул талууд илэрсэн;
— Хяналтын үр ашгийн туршилт/аудит нь гэнэтийн үр дүнд хүрсэн;
— аюул заналын орчинд өөрчлөлтүүд илэрсэн (жишээ нь, аюул заналын шинэ оролцогчид/эх сурвалжууд).

Гаралт: Тохиолдол эсвэл эрсдэлийн хувилбаруудын жагсаалт, эдгээрийн тохиолдох болзошгүй тохиолдлын хамт.

Хэрэгжүүлэх арга зүй:

Эрсдэлийн хувилбаруудыг тодорхойлсны дараа чанарын болон тоон шинжилгээний аргуудыг ашиглан нөхцөл байдал, үр дагавар бүрийн болзошгүй тохиолдолд дүн шинжилгээ хийх шаардлагатай. Болзошгүй тохиолдлыг үнэлэх нь үргэлж хялбар байдаггүй бөгөөд үүнийг янз бүрийн аргаар замаар илэрхийлнэ. Эрсдэлийн эх үүсвэрүүд хэр олон удаа тохиолдох эсвэл тэдгээрийн заримыг (жишээлбэл, эмзэг байдал) хэрхэн амархан ашиглаж болохыг харгалзан үзвэл зохино.

— эрсдэлийн эх үүсвэрийн болзошгүй тохиолдлын туршлага, холбогдох статистик;

— зохиомол эрсдэлийн эх үүсвэрийн хувьд: мотивацийн хэмжээ [жишээ нь, халдлагын амьдрах (зардал/ашиг)] болон цаг хугацааны явцад өөрчлөгддөг чадавхи (жишээ нь, боломжит халдагчдын ур чадварын түвшин), боломжит халдлагчдад боломжтой нөөц, ноцтой гэмт хэрэг, террорист байгууллага эсхүл гадаадын тагнуул зэрэгт үзүүлэх нөлөөлөл, түүнчлэн боломжит халдагчдийг татах байдал, эмзэг байдлын талаар ойлголт;
— санамсаргүй эрсдэлийн эх үүсвэрийн хувьд: газарзүйн хүчин зүйл (жишээ нь, аюултай байгууламж эсвэл үйл ажиллагаанд ойрхон), цаг агаарын эрс тэс байдал, галт уулын идэвхжил, газар хөдлөлт, үер, цунами зэрэг байгалийн гамшгийн боломж зэрэг хүний алдаа, тоног төхөөрөмжийн эвдрэлд нөлөөлж болох хүчин зүйлс;
— мэдэгдэж байгаа сул талууд, аливаа саармаг хяналтууд дангаар нь болон нэгтгэсэн;
— одоо байгаа хяналтууд болон тэдгээр нь мэдэгдэж буй сул талуудыг хэр үр дүнтэй бууруулж буй байдал.

Болзошгүй тохиолдлын тооцоо нь хараахан болоогүй, тиймээс бүрэн мэдэгдээгүй зүйлсийг авч үздэг учраас төдийгүй болзошгүй тохиолдол нь статистикийн хэмжигдэхүүн бөгөөд бие даасан тохиолдлуудыг шууд төлөөлахгүй тул угаасаа тодорхой бус байдаг. Үнэлгээний тодорхойгүй байдлын гурван үндсэн эх үүсвэр нь:

— Шийдвэр гаргалтын сэтгэцийн өөрчлөмтгий байдлаас үүдэлтэй үүдэлтэй хувийн тодорхойгүй байдал;
— тохиолдлыг загварчлах энгийнээр арга хэрэгслийг ашиглахаас үүдэлтэй арга зүйн тодорхойгүй байдал;
— хүлээгдэж буй тохиолдлын талаар хангалтгүй мэдлэгтэйгээс үүдсэн системийн тодорхой бус байдал (ялангуяа тохиолдол хязгаарлагдмал эсвэл эрсдэлийн эх үүсвэр цаг хугацааны явцад өөрчлөгддөг бол).

Болзошгүй тохиолдлын тооцооны найдвартай байдлыг нэмэгдүүлэхийн тулд байгууллагууд дараахь зүйлийг ашиглахыг анхаарвал зохино:

a) хувь хүний үнэлгээнээс илүү багийн үнэлгээ;
b) мэдээллийн аюулгүй байдлын зөрчлийн тайлан зэрэг гадаад эх сурвалж;
c) байгууллагын арга барилд тохирсон цар хүрээ, нарийвчлал бүхий хуваарь (scale);
d) "хааяа" гэхийн оронд "жилд нэг удаа" гэх мэт хоёрдмол утгагүй ангилал.

Болзошгүй тохиолдлыг үнэлэхдээ бие даасан болон хамааралтай тохиолдлын ялгааг ойлгох нь чухал. Бие биенээсээ хамааралтай тохиолдлын болзошгүй тохиолдол нь тэдгээрийн хоорондын хамаарлаар (жишээ нь, эхний үйл явдал тохиолдсон тохиолдолд хоёр дахь үйл явдал зайлшгүй байж болно) тодорхойлогддог тул тэдгээрийн болзошгүй тохиолдлыг тусад нь үнэлэх шаардлагагүй болно. Хамааралтай бие даасан тохиолдлуудын болзошгүй тохиолдол нь тэдгээрийн хувь нэмрээ оруулж буй болзошгүй тохиолдлын үр дагаварт хүргэх бүх чухал хувь нэмэр оруулагчид юм.

ЖИШЭЭ: Серверт Denial-of-Service халдлага гарах болзошгүй тохиолдол нь одоогийн аюул занал болон серверийн эмзэг байдал, хүртээмжтэй байдлаас хамаарна. Халдлага эхэлмэгц хорлонтой пакетуудын болзошгүй тохиолдол 100% байж болох ба түүний үнэлгээ нь Denial-of-Service халдлагын болзошгүй тохиолдлыг үнэлэхэд тус болохгүй.

Үнэлгээнд шаардлагагүй төвөг үүсэхээс зайлсхийхийн тулд эрсдэлийн хувилбарт нөлөөлж буй тохиолдлуудын хоорондын хамаарлыг тодорхойлж, эхний ээлжинд бие биенээсээ хамааралгүй тохиолдлын болзошгүй тохиолдлыг үнэлэх нь чухал юм.

Мэдээллийн аюулгүй байдлын тохиолдлын бизнесийн үр дагаврын ерөнхий болзошгүй тохиолдол нь доод түвшний хувь нэмэр оруулах хэд хэдэн тохиолдлын болзошгүй тохиолдол болон тэдгээрийн үр дагавраас хамаардаг. Бизнесийн үр дагаврын болзошгүй тохиолдлыг дээд түвшинд үнэлж тооцоолохыг оронд тус тусад нь үнэлдэг доод түвшний тохиолдлын болзошгүй тохиолдлыг нэгтгэн дүгнэх нь илүү зөв байж болно.

7.3.4 Эрсдэлийн түвшинг тодорхойлох

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 d) 3).-д хамаарна.

<u>Оролт:</u> Өмч, тохиолдолд холбоотой эрсдэлийн хувилбаруудын жагсаалт, тэдгээрийн магадлал (тоон эсвэл чанарын)-ын хамт.

<u>Ажиллагаа:</u> Бүх эрсдэлийн хувилбаруудын үнэлэгдсэн болзошгүй тохиолдол болон үнэлэгдсэн үр дагаврын хослолоор эрсдэлийн түвшинг тодорхойлвол зохино.

<u>Өдөөгч:</u> Мэдээллийн аюулгүй байдлын эрсдэлийг үнэлэх тохиолдолд эрсдэлийн түвшинг тодорхойлох шаардлагатай болно.

<u>Гаралт:</u> Түвшингийн утга бүхий эрсдэлийн жагсаалт.

<u>Хэрэгжүүлэх арга зүй:</u>

Эрсдэлийн түвшинг олон янзаар тодорхойлж болно. Энэ нь ихэвчлэн бүх холбогдох эрсдэлийн хувилбаруудын үнэлэгдсэн болзошгүй тохиолдол болон үнэлэгдсэн үр дагаврын хослолоор тодорхойлогддог. Өөр тооцоонд өмчийн үнэ цэнэ, болзошгүй тохиолдол, үр дагаврыг багтааж болно. Түүнчлэн тооцоолол нь шугаман байх албагүй, жишээ нь, болзошгүй тохиолдлын квадратыг үр дагавартай нэгтгэж болно. Ямар ч тохиолдолд эрсдэлийн түвшинг 6.4.3.4-т заасны дагуу тогтоосон шалгуурыг ашиглан тодорхойлно .

7.4 Мэдээллийн аюулгүй байдлын эрсдэлийг үнэлэх

7.4.1 Эрсдэлийн шинжилгээний үр дүнг эрсдэлийн шалгуур үзүүлэлттэй харьцуулах

ТАЙЛБАР: Энэ дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 е) 1).-д хамаарна

Оролт: Эрсдэлийн шалгуур үзүүлэлт болон түвшингийн утгууд бүхий эрсдэлийн жагсаалт

Ажиллагаа: Эрсдэлийн түвшинг эрсдэлийн үнэлгээний шалгуур, ялангуяа эрсдэлийг хүлээх зөвшөөрөх шалгууртай харьцуулвал зохино.

Өдөөгч: Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээнд зориулан эрэмбэлэхийн тулд эрсдэлийн шинжилгээний үр дүнг эрсдэлийн шалгуур үзүүлэлттэй харьцуулах шаардлагатай болно.

Гаралт: Эрсдэлийн менежменттэй холбоотой нэмэлт арга хэмжээний талаар шийдвэр гаргах саналуудын жагсаалт.

Хэрэгжүүлэх арга зүй:

Эрсдэлийг тодорхойлж, үр дагаврын болзошгүй тохиолдол, ноцтой байдлын утгыг тогтоосны дараа байгууллагууд эрсдэлийг хүлээн зөвшөөрөх шалгуураа ашиглан эрсдэлийг хүлээн зөвшөөрөх боломжтой эсэхийг тодорхойлно. Хэрэв тэдгээрийг хүлээн зөвшөөрөх боломжгүй бол арга хэмжээгээ эрэмбэлвэл зохино.

Байгууллагууд эрсдэлийг үнэлэхийн тулд үнэлэгдсэн эрсдэлийг нөхцөл байдлыг бий болгох явцад тодорхойлсон эрсдэлийн шалгуур үзүүлэлттэй харьцуулна.

Эрсдэлийн үнэлгээний шийдвэр нь үнэлэгдсэн эрсдэл болон тодорхойлсон хүлээн зөвшөөрөх шалгуурыг харьцуулж, үнэлгээнд итгэх итгэлийн түвшинг харгалзана. Харьцангуй бага үр дагавартай байнгын тохиолдолын үед тохиолдол бүрийн эрсдэлийг тус тусад нь авч үзэхээс илүүтэйгээр тодорхой хугацааны туршид хуримтлагдсан үр нөлөөг авч үзэх нь нийт эрсдэлийг илүү бодитой төлөөлнө.

Эрсдэлийн арга хэмжээ шаардлагатай болон шаардлагагүй эрсдэлүүдийн хоорондох заагийг тодорхойлоход тодорхойгүй байдал үүсч болно. Тодорхой нөхцөлд арга хэмжээ шаардлагатай болон шаардлагагүй эрсдэлийг заашлахын тулд хүлээн зөвшөөрөх эрсдэлийн нэг түвшинг ашиглах нь үргэлж тохиромжтой байдаггүй.

Зарим тохиолдолд боломжит хяналтын зардал, үр нөлөө зэрэг нэмэлт параметрүүдийн хамт уян хатан байдлын элементийг шалгуурт оруулах нь илүү үр дүнтэй байдаг.

Эрсдэл хариуцагчид болон бизнесийн болон техникийн мэргэжилтнүүдийн зөвшилцөлд үндэслэн эрсдэлийн түвшинг баталгаажуулж болно. Эрсдэл

хариуцагчид өөрсдийн хариуцлага хүлээх эрсдэлийн талаар сайн ойлголттой байх нь бодитой үнэлгээний үр дүнд нийцнэ. Иймээс үнэлэгдсэн эрсдэл болон эрсдэл хариуцагчийн үзэж буй түвшин хоорондын үл нийцлийг мөшгөж аль нь бодит байдалтай илүү ойр байгааг тодорхойлно.

7.4.2 Шинжилсэн эрсдэлийг эрсдэлийн арга хэмжээнд зориулан эрэмбэлэх

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.2 е) 2)-д хамаарна.

Оролт: Эрсдэлийн шалгуур үзүүлэлттэй харьцуулсан эрсдэлийн үр дүнгийн жагсаалт.

Ажиллагаа: Жагсаалтад орсон эрсдэлийг үнэлэгдсэн түвшинг харгалзан эрсдэлийн арга хэмжээнд зориулан эрэмбэлнэ.

Өдөөгч: Мэдээллийн аюулгүй байдлын эрсдэлийг арилгахын тулд дүн шинжилгээ хийсэн эрсдэлийг эрсдэлийн арга хэмжээнд зориулан эрэмбэлэх шаардлагатай.

Гаралт: Тэргүүлэх ач холбогдол бүхий эрсдэлүүдийн жагсаалт, уг эрсдэлд хүргэдэг эрсдэлийн хувилбаруудын хамт.

Хэрэгжүүлэх арга зүй:

Эрсдэлийн үнэлгээ нь эрсдэлийн шинжилгээгээр олж авсан эрсдэлийн талаарх ойлголтыг ашиглан дараагийн шийдэх алхамыг санал болгодог. Эдгээрт дурдвал зохино:

— эрсдэлийн арга хэмжээ шаардлагатай эсэх;
— үнэлэгдсэн эрсдэлийн түвшинг харгалзан эрсдэлийн арга хэмжээний тэргүүлэх чиглэлүүд.

Эрсдэлийг эрэмбэлэхдээ ашиглах эрсдэлийн шалгуур үзүүлэлтүүд нь байгууллагын зорилго, гэрээ, хууль эрх зүйн болон зохицуулалтын шаардлага, холбогдох сонирхогч талуудын санал бодлыг харгалзана. Эрсдэлийн үнэлгээний үйл ажиллагаанд тэргүүлэх ач холбогдол өгөх нь голчлон хүлээн зөвшөөрөх шалгуурт үндэслэнэ.

8 Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний үйл явц

8.1 Ерөнхий

Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний оролт нь эрсдэлийн үнэлгээний үйл явцын гаралт бөгөөд эрсдэлийн шалгуурын дагуу эрэмбэлэгдсэн, арга хэмжээ шаардлагатай эрсдэлүүд байна.

Энэхүү үйл явцын гаралт нь эрсдэлийн арга хэмжээний төлөвлөгөө [ISO/IEC 27001:2022, 6.1.3 е)]-ний дагуу бие биетэй нь уялдуулах эсвэл сайжруулах шаардлагатай мэдээллийн аюулгүй байдлын хяналт [ISO/IEC 27001:2022, 6.1.3 б)] [үзнэ үү]-ын багц байна.. Ийм байдлаар хэрэгжүүлснээр эрсдэлийн арга хэмжээний төлөвлөгөөний үр нөлөө нь тухайн байгууллагад тулгарч буй мэдээллийн аюулгүй байдлын эрсдэлийг байгууллагын хүлээн зөвшөөрөх шалгуурт нийцүүлэн өөрчлөх явдал юм.

8.2 Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний оновчтой хувилбаруудыг сонгох

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.3 а)-д хамаарна.

Оролт: Тэргүүлэх ач холбогдол бүхий эрсдэлийн жагсаалт, эрсдэлд хүргэж буй тохиолдол эсвэл эрсдэлийн хувилбарын хамт.

Ажиллагаа: Эрсдэлийн арга хэмжээний хувилбаруудыг сонгоно.

Өдөөгч: Хэрэв эрсдэлийн арга хэмжээний төлөвлөгөө байхгүй эсвэл төлөвлөгөө бүрэн бус тохиолдолд мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний зохих хувилбаруудыг сонгох шаардлагатай болно.

Гаралт: Тэргүүлэх ач холбогдол бүхий эрсдэлийн жагсаалт, эрсдэлийн арга хэмжээний сонголтын хамт.

Хэрэгжүүлэх арга зүй:

Эрсдэлийн арга хэмжээний хэд хэдэн сонголтууд нь:

— эрсдэл үүсгэж буй үйл ажиллагааг эхлүүлэхгүй, үргэлжлүүлэхгүй байх шийдвэр гаргах замаар эрсдэлээс зайлсхийх;
— аливаа үйл явдал, үр дагавар гарах магадлалыг өөрчлөх эсвэл үр дагаварын ноцтой байдлыг өөрчлөх замаар эрсдэлийг өөрчлөх;
— мэдээлэл бүхий сонголтыг хийж эрсдэлийг хадгалах;
— бусад талуудтай дотоод болон гадаад үүрэг хариуцлагыг хуваах замаар эрсдэлийг хуваалцах (жишээ нь даатгалаар үр дагаврыг хуваалцах);

ЖИШЭЭ 1 Эрсдэлээс зайлсхийх жишээ бол үерийн бүсэд байрлах оффисын байршил бөгөөд үерийн улмаас оффис эвдэрч гэмтэх, оффис ашиглах боломж болон/эсвэл нэвтрэх эрхийг хязгаарлах явдал юм. Холбогдох физик хяналт нь энэ эрсдэлийг бууруулахад хангалтгүй байж болох бөгөөд энэ тохиолдолд эрсдэлээс зайлсхийх арга хэмжээний сонголт нь хамгийн сайн сонголт байж болно. Энэ нь тухайн оффисын үйл ажиллагааг хаах эсвэл зогсоохтой холбоотой байж болно.

ЖИШЭЭ 2 Эрсдэлээс зайлсхийх өөр нэг жишээ бол тухайн байгууллага өөрийн мэдээллийн систем дэх мэдээллийг удирдах, хадгалах, дамжуулах шаардлага үүсгэхгүйн тулд тодорхой мэдээллийг хувь хүнээс цуглуулахгүй байх сонголт юм.

Эрсдэлийг хуваалцах тохиолдолд магадлал, үр дагаврыг өөрчлөхийн тулд дор хаяж нэг хяналт шаардлагатай бөгөөд байгууллага хяналтыг хэрэгжүүлэх үүрэг хариуцлагыг нөгөө талд шилжүүлдэг.

Эрсдэлийн арга хэмжээний хувилбаруудыг эрсдэлийн үнэлгээний үр дүн, эдгээр хувилбаруудыг хэрэгжүүлэхэд хүлээгдэж буй зардал, эдгээр хувилбаруудаас хүлээгдэж буй үр өгөөжийг тус тусад нь болон бусад хяналтын хүрээнд сонговол зохино. Эрсдэлийн арга хэмжээг тодорхойлсон эрсдэлийн түвшин, хэрэгжүүлэх хугацааны хязгаарлалт ба шаардлагатай дараалал, 7.4-т дурдсан эрсдэлийн үнэлгээний гаралтын дагуу эрэмбэлвэл зохино. Сонголт хийхдээ тухайн эрсдэлийн нөлөөлөлд өртсөн талууд хэрхэн хүлээн зөвшөөрөх , эрсдэлийн талаар эдгээр талуудад мэдээлэх хамгийн тохиромжтой арга замыг авч үзэж болно.

8.3 Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний хувилбаруудыг хэрэгжүүлэхэд шаардлагатай бүх хяналтыг тодорхойлох

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.3 b)-д хамаарна.

Оролт: Тэргүүлэх ач холбогдолтой эрсдэлийн жагсаалт, эрсдэлийн арга хэмжээний сонголтын хамт.

Ажиллагаа: Эрсдэлийг өөрчлөх, хадгалах, зайлсхийх, хуваалцах зэрэг сонгосон эрсдэлийн арга хэмжээнд үндэслэн, уг арга хэмжээнд шаардлагатай зохих эх сурвалжаас бүх хяналтуудыг тодорхойлох.

Өдөөгч: МАБМТ-д нийцэл; мэдээллийн аюулгүй байдлын эрсдэлийг удирдах.

Гаралт: Шаардлагатай бүх хяналтууд.

Хэрэгжүүлэх арга зүй:

Шаардлагатай хяналтыг тодорхойлоход онцгой анхаарал хандуулвал зохино. Хяналт бүрийг дараахь шалгах асуултын дагуу шалгаж, шаардлагатай эсэхийг тодорхойлно:

— энэхүү хяналт нь эрсдэлийн болзошгүй тохиолдол, үр дагаварт ямар нөлөө үзүүлэх вэ;
— хяналт нь эрсдэлийн түвшинг ямар байдлаар хадгалах вэ.

Эрсдэлд маш бага нөлөө үзүүлэх хяналтыг л "шаардлагатай" гэж тодорхойлно. Арга хэмжээ шаардлагатай гэж үнэлэгдсэн эрсдэл бүрт нэг буюу хэд хэдэн хяналтыг хэрэгжүүлнэ.

Хяналтын багцын олон эх сурвалж байдаг. Тэдгээрийг ISO/IEC 27001:2022, А хавсралт, салбарын онцлог дүрэмүүд (жишээ нь ISO/IEC 27017) болон бусад үндэсний, бүс нутгийн, үйлдвэрлэлийн хяналтуудаас олж болно. Байгууллага нэг буюу хэд хэдэн "уламжлалт" хяналтыг тодорхойлж болно (ISO/IEC 27003-ыг үзнэ

үү).

Хэрэв уламжлалт хяналтыг тодорхойлсон бол хяналт гэсэн хэллэгт хяналт юу болох, хэрхэн ажилладаг талаар үнэн зөв, бодитоор тайлбарлавал зохино. Боломжтой бөгөөд тохиромжтой бол энэ хэллэг нь дараахь зүйлийг агуулж болно.

— энэ нь баримтжуулсан хяналт мөн эсэх;
— хяналтыг хэн эзэмшдэг;
— үүнийг хэрхэн хянаж байдаг;
— үүнийг хэрхэн нотлох боломжтой;
— аливаа хамаарахгүй тохиолдол;
— хяналтын үйл ажиллагааны давтамж;
— хяналтын хүлцэл;
— хэрэв энэ нь тодорхойгүй бол хяналт байгаа шалтгаан.

Хэрэв хяналт нь хүлцэх хүрээнээс гадуур байвал хяналт нь тодорхойлсон эрсдэлийг удирдахад хангалттай үр дүнтэй ажиллахгүй.

ЖИШЭЭ 1 “МТ-ийн аюулгүй байдлын менежерийн эзэмшдэг, хортой кодын менежментийн баримтжуулсан үйл ажиллагаа хэрэгждэг. Үүнд Мас компьютерууд хамаарахгүй бөгөөд нийлүүлэгчийн консолоор хянадаг бөгөөд долоо хоног бүр Удирдлагад гүйцэтгэлийн тайланг илгээдэг.

Хэрэв уламжлалт хяналтууд нь хяналт хангалтын тайланг гаргахад тухайн байгууллагыг дэмжих зорилготой бол хяналтын үг хэллэгийн ийм нарийвчилсан арга нь ашигтай байж болно. Гэсэн хэдий ч хяналтын үг хэллэг нь тухайн байгууллагын хүмүүст утга учиртай байх нь илүү чухал бөгөөд тэдгээр хяналт, түүнтэй холбоотой эрсдэлийг удирдах шийдвэр гаргахад нь туслах ёстой.

Хяналтыг тодорхойлох нь хараахан хэрэгжээгүй шинэ хяналтуудыг багтааж болно, эсвэл байгууллагад байгаа хяналтуудыг агуулж болно. Гэхдээ ажиллаж байгаа хяналтыг эрсдэлийн үнэлгээнд шууд оруулахгүй байвал зохино, учир нь:

— мэдээллийн аюулгүй байдлын нэг буюу хэд хэдэн эрсдэлийг удирдахад хяналт шаардлагагүй;
— энэ хяналт нь мэдээллийн аюулгүй байдлын нэг буюу хэд хэдэн эрсдэлийг удирдахад ямар нэгэн байдлаар тусалдаг боловч эрсдэлийн үнэлгээнд оруулахад хангалттай үр дүнтэй биш эсвэл МАБМТ удирддаг, эсвэл;
— энэ нь мэдээллийн аюулгүй байдалтай холбоогүй шалтгаанаар (жишээ нь, чанар, үр ашиг, үр дүнтэй байдал эсвэл нийцэл) одоо ажиллаж болно, эсвэл;
— энэ нь одоогоор ажиллаж байгаа боловч мэдээллийн аюулгүй байдлын үүднээс авч үзвэл энэ нь үндсэн хяналт хэвээр байгаа статусаа зөвтгөх хангалттай нөлөө үзүүлэхгүй тул устгаж болно.

Хэрэв хяналтыг зөвхөн мэдээллийн аюулгүй байдлын эрсдэлийн удирдлагаас өөр зорилгоор ашиглаж байгаа бол хяналтыг мэдээллийн аюулгүй байдлын зорилтууд болон мэдээллийн бус аюулгүй байдлын зорилтуудад хүрэхийн тулд удирдахад

анхаарвал зохино.

ЖИШЭЭ 2: Дотоод хяналтын камер нь үйлдвэрлэлийн үйл явцын чанарыг хянах, мэдээллийн аюулгүй байдлын (хууран мэхлэхээс хамгаалах) зорилготой.

Одоо байгаа хяналтын багцаас (жишээ нь ISO/IEC 27001:2022, А хавсралт, эсвэл салбарын онцлог хяналтын жагсаалт) хяналтыг тодорхойлохдоо хяналт гэсэн үг хэллэг нь эрсдэлийг удирдах шаардлагад нийцэж, хяналт гэж юу болох эсвэл юуг хийх ёстойг нарийн тусгавал зохино. Хэрэв ерөнхий хандлага нь одоо байгаа хяналтын багцыг (жишээ нь ISO/IEC 27001:2022, А хавсралт А эсвэл салбарын онцлог хяналтын жагсаалт) ашиглах бөгөөд уг багц нь нарийвчлан тодорхойлсон шаардлагатай хяналтыг агуулаагүй тохиолдолд уламжлалт хяналтыг хяналтыг нарийвчлан тодорхойлоход анхаарвал зохино.

Хяналтыг урьдчилан сэргийлэх, илрүүлэх, залруулах гэж ангилж болно.

a) урьдчилан сэргийлэх хяналт: нэг буюу хэд хэдэн үр дагаварт хүргэж болзошгүй мэдээллийн аюулгүй байдлын тохиолдолоос урьдчилан сэргийлэх зорилготой хяналт;
b) илрүүлэх хяналт: мэдээллийн аюулгүй байдлын тохиолдлыг илрүүлэх зорилготой хяналт;
c) залруулах хяналт: мэдээллийн аюулгүй байдлын тохиолдлын үр дагаврыг хязгаарлах зорилготой хяналт.

Хяналтын төрөл нь тохиолдол эсхүл түүний үр дагаварыг илрүүлэх, урьдчилан сэргийлэх зорилгоор хяналт хэрэгжиж буй эсэх, хэрэгжих гэж байгаа эсэхийг тодорхойлдог.

ЖИШЭЭ 3: Мэдээллийн аюулгүй байдлын бодлого нь эрсдэлийг хадгалах хяналт боловч бодлогын хэрэгжилт нь эрсдэл үүсэх болзошгүй тохиолдлыг бууруулах зорилготой тул урьдчилан сэргийлэх гэж ангилж болно.

Хяналтыг урьдчилан сэргийлэх, илрүүлэх, залруулах гэж ангилахын ашиг тус нь эрсдэлийн арга хэмжээний төлөвлөгөө нь хяналтын доголдолд уян хатан байх нөхцлийг бүрдүүлэхэд оршино. Урьдчилан сэргийлэх, илрүүлэх, залруулах хяналтын зохих хослолуудын жишээ:

— Урьдчилан сэргийлэх хяналт амжилтгүй тохиолдолд илрүүлэх хяналт эрсдэлийг бууруулах ёстой;
— Илрүүлэх хяналт амжилтгүй тохиолдолд залруулах хяналт эрсдэлийг бууруулах ёстой;
— Урьдчилан сэргийлэх хяналт нь залруулах хяналтыг ашиглах аливаа болзошгүй тохиолдлыг бууруулах ёстой.

Байгууллага хяналтыг ашиглахдаа юуны өмнө аливаа тохиолдлыг илрүүлэх боломжтой эсэхийг шийдвэл зохино. Хэрэв тийм бол илрүүлэх хяналтыг хэрэгжүүлнэ. Хэрэв энэ нь тохиолдлыг илрүүлэх боломжгүй бол илрүүлэх хяналт үр ашиггүй бөгөөд урьдчилан сэргийлэх хяналт ажиллаж байгаа эсэхийг мэдэх

боломжгүй.

ЖИШЭЭ 4: Хэрэв компьютер нь "ботнет (botnet)"-ийн хэсэг болсон эсэх нь тодорхойгүй байгаа бол түүнийг ботнетийн нэг хэсэг болохоос урьдчилан сэргийлэхийн тулд ашиглаж байгаа хяналтууд нь зориулалтын дагуу ажиллаж байгаа эсэхийг мэдэх боломжгүй.

Илрүүлэх хяналт нь зохих ёсоор ажиллах боловч үр дүнгүй хэвээр байж болно.

ЖИШЭЭ 5: Халдлага илрүүлэх/урьдчилан сэргийлэх системийг хэрэгжүүлэх нь сүлжээгээр дамжих хортой программаас урьдчилан сэргийлэх үр дүнтэй арга байж болох ч тархаагүй дэгдэлт гарсан тохиолдолд үйлдлийн системийг хянах систем/дохиолол байхгүй тохиолдолд тэдгээр нь ашиггүй болно.

Илрүүлэгч хяналтыг үл ойшоох эсвэл өгсөн мэдэгдэлийн дагуу зохих арга хэмжээ аваагүй тохиолдолд эцсийн дүндээ үр дүнгүй байдаг. Дараа нь залруулах хяналтыг авч үзвэл зохино. Хэрэв илрүүлэх хяналт амжилтгүй болвол нэг буюу хэд хэдэн хүсэгүй үр дагавар гарах магадлалтай. Залруулах хяналтыг хэрэгжүүлэх нь эдгээр үр дагаврыг хязгаарлахад тусална. Залруулах хяналт нь үр дагавар гарсны дараа хүчин төгөлдөр болдог ч, иэхэвчлэн аливаа тохиолдол гарахаас өмнө тэдгээрийг хэрэгжүүлэх шаардлагатай байдаг.

ЖИШЭЭ 6: Хатуу дискийг шифрлэх нь зөөврийн компьютер хулгайд алдах эсвэл дараа нь өгөгдлийг задлах оролдлогоос сэргийлдэггүй. Гэсэн ч энэ нь мэдээллийг задруулахтай холбоотой үр дагаврын ноцтой байдлыг бууруулдаг. Иймд зөөврийн компьютер хулгайлагдахаас өмнө хяналтыг хэрэгжүүлсэн байвал зохино.

Хяналтыг ангилах нь төгс биш бөгөөд хяналтын тодорхойлсон нөхцөл байдлаас хамаарна.

ЖИШЭЭ 7: Нөөцлөх (backup) нь өгөгдөл алдагдах (жишээ нь дискний толгойн гэмтэл, зөөврийн компьютер алдагдах) тохиолдлоос сэргийлж чадахгүй ч үр дагаврыг бууруулахад тусална. Иймд зарим байгууллага үүнийг урьдчилан сэргийлэх бус залруулах хяналт гэж үзэж болно. Үүний адил, шифрлэлт (encryption) нь мэдээлэл алдагдахаас сэргийлж чадахгүй, гэхдээ энэ тохиолдлыг "халдагчид илрүүлсэн хувийн мэдээлэл" гэж тодорхойлсон бол шифрлэлт нь залруулах биш урьдчилан сэргийлэх хяналт юм.

Эрсдэлд чиглэсэн хяналтыг зохион байгуулах дараалал нь янз бүрийн хүчин зүйлээс хамаарна. Олон арга техникийг ашиглаж болно. Эрсдэл бодитой болсон тохиолдолд хяналтад хөрөнгө оруулах зардал болон үр дагаврыг тооцох хоёрын тэнцвэрийг тогтоох нь тухайн эрсдэл хариуцагчийн үүрэг юм.

Одоо байгаа хяналтуудыг тодорхойлж, эдгээр хяналтууд нь одоогийн хэрэгцээ шаардлагаас давж байгааг тодорхойлох боломжтой. Илүүдэл эсвэл шаардлагагүй хяналтыг (ялангуяа засвар үйлчилгээний зардал өндөртэй бол) арилгахын өмнө зардал-үр ашгийн шинжилгээ хийвэл зохино. Хяналтууд бие биедээ нөлөөлж болох тул илүүдэл хяналтыг арилгах нь нийт аюулгүй байдлыг бууруулна. Тодорхойлсон

нэг буюу хэд хэдэн эрсдэлийг удирдахад шаардлагатай хяналт биш л бол хяналтыг эрсдэлийн арга хэмжээнд оруулгүй. Хяналт нь тодорхойлогдсон мэдээллийн аюулгүй байдлын эрсдэлийн үр дагавар эсвэл магадлалд нөлөө үзүүлнэ. Хяналт нь мэдээллийн аюулгүй байдалд хамаарахгүй тохиолдолд эрсдэлийн арга хэмжээнд хамрагдахгүй.

Хэрэгжиж байгаа боловч сул талтай нь мэдэгдэж байгаа хяналтуудыг анхаарч үзэх хэрэгтэй. Хэрэв сул талтай хяналтын удирдаж буй бүх эрсдэлийн үнэлгээ нь хүлээн зөвшөөрөх шалгуурт багтсан бол хяналтыг сайжруулах шаардлагагүй болно. Хэдийгээр хяналт нь бүрэн үр дүнтэй ажиллахгүй байгаа ч бүрэн үр дүнтэй болгохын тулд үүнийг сайжруулах шаардлагатай байдаггүй. Байгууллага эрсдэлээ амжилттай удирдахын тулд бүх хяналт бүрэн үр дүнтэй байх ёстой гэж үзэж болохгүй. Хяналт бүр нь бүтэлгүйтлийн хүлцлийн түвшинтэй байдаг бөгөөд үүнээс доогуур түвшинд хяналтыг тодорхойлсон эрсдэлийг удирдахад хангалттай үр дүнтэй ажиллахгүй гэж үзэж болно. Хяналт нь хүлцэл дотор ажиллаж байгаа бол түүнийг сайжруулах шаардлагагүй.

8.4 ISO/IEC 27001:2022, А хавсралтад заасан хяналттай харьцуулах

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022, 6.1.3 в).

Оролт: Бүх шаардлагатай хяналтууд (8.3-ыг үзнэ үү).

Ажиллагаа: Шаардлагатай бүх хяналтыг ISO/IEC 27001:2022, Хавсралт А-д заасантай харьцуулна уу.

Өдөөгч: Эрсдэлийн арга хэмжээ төлөвлөгөө боловсруулсан тохиолдолд дутуу хяналтыг тодорхойлох шаардлагатай болно.

Гаралт: Эрсдэлийн арга хэмжээнд хамаарах бүх хяналт.

Хэрэгжүүлэх арга зүй:

ISO/IEC 27001:2022, 6.1.3 с) нь байгууллагаас сонгосон эрсдэлийн арга хэмжээний хувилбаруудыг хэрэгжүүлэхэд шаардлагатай гэж тодорхойлсон хяналтыг ISO/IEC 27001:2022, Хавсралт А-д заасан хяналттай харьцуулахыг шаарддаг. Үүний зорилго нь эрсдэлийн үнэлгээнд шаардлагатай хяналтыг орхигдуулаагүй эсэхийг шалгах аюулгүй байдлын шалгалтын үүрэг гүйцэтгэдэг. Энэхүү аюулгүй байдлын шалгалт нь эрсдэлийн үнэлгээнд ISO/IEC 27001:2022, Хавсралт А-аас орхигдсон хяналтуудыг тодорхойлоход ороогүй болно. Энэ нь хяналтыг бусад стандарт, хяналтын жагсаалттай харьцуулах замаар аливаа эх сурвалжаас дутуу шаардлагатай хяналтыг илрүүлэх аюулгүй байдлын шалгалт юм. Энэхүү шалгалтын явцад илрүүлсэн орхигдуулсан хяналтууд нь салбарын онцлог, захиалгат хяналт эсвэл ISO/IEC 27001:2022, Хавсралт А-аас байж болно. 8.3- т заасан хяналтыг тодорхойлох удирдамжийг эрсдэлийн үнэлгээнд дутуу хяналт нэмэх эсэхийг авч үзэх хэрэгтэй.

ЖИШЭЭ: Байгууллагад аль хэдийн ажиллаж байгаа хяналтыг эрсдэлийн үнэлгээнд нэмэлт анхаарал хандуулахгүйгээр автоматаар оруулахгүй байх нь чухал юм.

Хяналтын энэхүү харьцуулалтыг эрсдэлийн үнэлгээг ашиглан хийдэг бөгөөд хэрэглэх боломжтой байдлын мэдэгдлийг ашиглан хийдэггүй гэдгийг санах нь чухал юм. Энэ зарчим нь эрсдэл бүрийг ээлжлэн харж, эрсдэлд шаардлагатай гэж тодорхойлсон хяналтуудыг ISO/IEC 27001:2022, Хавсралт А-д заасан хяналттай харьцуулж, эрсдэл тус бүрт шаардлагатай хяналт дутуу байгаа эсэхийг тодорхойлоход тусална.

8.5 Хэрэглэх тухай мэдэгдэл гаргах

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022, 6.1.3 d).

Оролт: Эрсдэлд хамаарах бүх хяналт (8.4-ийг үзнэ үү).

Ажиллагаа: Хэрэглэх тухай мэдэгдэл гаргах.

Өдөөгч: Шаардлагатай бүх хяналт, тэдгээрийн үндэслэл, хэрэгжилтийн байдлыг баримтжуулах.

Гаралт: Хэрэглэх тухай мэдэгдэл.

Хэрэгжүүлэх арга зүй:

ISO/IEC 27001:2022, 6.1.3 г-ийн дагуу Хэрэглэх тухай мэдэгдэл (Statement of Applicability буюу SOA) дор хаяж дараахь зүйлийг агуулна.

a) шаардлагатай хяналт;
b) тэдгээрийг оруулах үндэслэл;
c) хэрэгжсэн эсэх;
d) ISO/IEC 27001:2022, А хавсралтаас хяналтыг хассан үндэслэл.

Хэрэгжүүлэхээр төлөвлөж буйг тодорхойлохын тулд шаардлагатай хяналт, эрсдэлийн арга хэмжээний төлөвлөгөөг тодорхойлохын тулд эрсдэлийн үнэлгээг судалж үзэх замаар SOA-г хялбархан гаргаж болно. Зөвхөн эрсдэлийн үнэлгээнд тодорхойлсон хяналтыг SOA-д оруулж болно. Эрсдэлийн үнэлгээнээс хамааралгүй хяналтыг SOA-д нэмж оруулах боломжгүй. Сонгосон эрсдэлийн арга хэмжээний хувилбаруудыг хэрэгжүүлэхэд шаардлагатай хяналтууд болон SOA-ийн хооронд нийцтэй байх ёстой. SOA нь хяналтыг оруулах үндэслэл нь бүх хяналтын хувьд адилхан бөгөөд нэг буюу хэд хэдэн эрсдэлийг хүлээн зөвшөөрөгдөх түвшинд хүргэхийн тулд эрсдэлийн үнэлгээнд шаардлагатай гэж тодорхойлсон гэж хэлж болно. Хяналтын аль нэгэнд хяналтыг оруулах нэмэлт үндэслэл шаардлагагүй. SOA-д багтсан бүх хяналтын хэрэгжилтийн байдлыг "хэрэгжүүлсэн", "хэсэгчилсэн" эсвэл "хэрэглэгдээгүй" гэж тодорхойлж болно. Энэ нь хяналт бүрийн эсрэг тус тусад нь эсвэл ерөнхий мэдэгдэл байж болно.

ЖИШЭЭ: SOA нь "Бүх хяналтыг хэрэгжүүлсэн" гэсэн мэдэгдлийг агуулдаг. SOA-г

бөглөхийн тулд нэмэлт дүн шинжилгээ, мэдээлэл шаардагдахгүй.

8.6 Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний төлөвлөгөө

8.6.1 Эрсдэлийг арга хэмжээний төлөвлөгөө боловсруулах

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.3 е)-д хамаарна.

Оролт: Эрсдэлийн үнэлгээний үр дүн.

Ажиллагаа: Эрсдэлийн арга хэмжээний төлөвлөгөө боловсруулах.

Өдөөгч: Байгууллагын эрсдэлийн арга хэмжээний хэрэгцээ.

Гаралт: Эрсдэлийн арга хэмжээний төлөвлөгөө.

Хэрэгжүүлэх арга зүй:

Энэхүү үйл ажиллагааны зорилго нь тэргүүлэх ач холбогдол бүхий эрсдэлийн жагсаалтад орсон тодорхой эрсдэлүүдийн арга хэмжээний төлөвлөгөө(үүд)-ийг бий болгох явдал юм (7-р зүйлийг үзнэ үү). Эрсдэлийн арга хэмжээний төлөвлөгөө гэдэг нь тухайн байгууллагын эрсдэлийг хүлээн зөвшөөрөх шалгуурт нийцүүлэн эрсдэлийг өөрчлөх төлөвлөгөө юм (6.4.2-ыг үзнэ үү). Эрсдэлийн арга хэмжээний хүрээнд "төлөвлөгөө" гэсэн нэр томъёог хоёр янзаар тайлбарлаж болно. Эхнийх нь төслийн төлөвлөгөө, өөрөөр хэлбэл тухайн байгууллагад шаардлагатай хяналтыг хэрэгжүүлэх төлөвлөгөө юм. Хоёр дахь нь загварын төлөвлөгөө, өөрөөр хэлбэл шаардлагатай хяналтуудыг тодорхойлж, эрсдэлийг өөрчлөхийн тулд хяналтууд нь хүрээлэн буй орчин болон өөр хоорондоо хэрхэн харьцахыг тайлбарлана. Практикт хоёуланг нь ашиглаж болно.

Хяналтыг бий болгосны дараа төслийн төлөвлөгөө нь түүхэнд тэмдэглэгдэхээс өөр үнэ цэнэтэй байхаа больж, дизайны төлөвлөгөө нь ашигтай хэвээр байна.

Арга хэмжээ шаардлагатай эрсдэл бүрийг эрсдэлийн арга хэмжээний төлөвлөгөөний аль нэгэнд нь авч үзвэл зохино. Байгууллага эрсдэлийн арга хэмжээний хэд хэдэн төлөвлөгөөг сонгох боломжтой бөгөөд эдгээр нь хамтдаа эрсдэлийн арга хэмжээний бүх шаардлагатай асуудлыг хэрэгжүүлнэ. Эдгээрийг мэдээллийн хаана байрлаж байгаа (жишээ нь, дата төвийн нэг төлөвлөгөө, гар утасны тооцоололд зориулсан өөр төлөвлөгөө гэх мэт), өмчөөр (жишээ нь, өөр өөр өмчийн ангилалд зориулсан өөр төлөвлөгөө) эсвэл тохиолдлоор (жишээ нь: тохиолдолд суурилсан аргыг ашиглан эрсдэлийг үнэлэх) ангилан, зохион байгуулж болно.

Эрсдэлийн арга хэмжээний төлөвлөгөөг боловсруулахдаа байгууллагууд дараахь зүйлийг анхаарч үзнэ:

— эрсдэлийн түвшин, яаралтай арга хэмжээтэй холбоотой тэргүүлэх байдал;

— хяналтын төрлүүд (урьдчилан сэргийлэх, илрүүлэх, залруулах) эсвэл тэдгээрийн хослолыг хэрэглэх боломжтой эсэх;
— өмчид нэмж шинэ хяналт эхлэхийн өмнө хяналтыг шийдвэрлэхийг хүлээх шаардлагатай эсэх;
— хяналт хэрэгжсэн хугацаа болон бүрэн үр дүнтэй, үйл ажиллагаа явуулах мөчийн хооронд саатал гарсан эсэх.
— Арга хэмжээнд хамрагдсан эрсдэл бүрийн хувьд арга хэмжээний төлөвлөгөөнд дараахь мэдээллийг агуулсан байна:
— Хүлээгдэж буй үр өгөөжийг агуулсан, арга хэмжээний сонголтын үндэслэл;
— төлөвлөгөөг баталж, хэрэгжүүлэх үүрэг, хариуцлагатай хүмүүс;
— санал болгож буй арга хэмжээ;
— шаардлагатай нөөц, түүний дотор болзошгүй нөхцөл байдал;
— гүйцэтгэлийн үзүүлэлтүүд;
— хязгаарлалтууд;
— шаардлагатай тайлагнал, мониторинг;
— үйл ажиллагааг хэрэгжүүлж, дуусгахаар хүлээгдэж буй хугацаа;
— хэрэгжилтийн байдал.

Эрсдэлийн арга хэмжээний төлөвлөгөөний үйл ажиллагаа нь эрсдэлийн түвшин, арга хэмжээний яаралтай байдал зэрэгтэй уялдуулан эрэмбэлнэ. Эрсдэлийн түвшин өндөр, зарим тохиолдолд эрсдэл үүсэх давтамж өндөр байх тусам хяналтыг даруй хэрэгжүүлнэ.

Эрсдэлийн арга хэмжээний төлөвлөгөөнд жагсаасан эрсдэл бүрийн хувьд хэрэгжилтийн нарийвчилсан мэдээллийг хянах ёстой бөгөөд үүнд дараахь зүйлс орно, гэхдээ үүгээр хязгаарлагдахгүй:

— эрсдэлийг хариуцагчид болон хэрэгжилтийг хариуцах хүмүүсийн нэрс;
— хэрэгжүүлэх огноо, цаг хугацаа;
— хэрэгжилтийн үр дүнг туршихаар төлөвлөсөн хяналтын үйл ажиллагаа;
— хэрэгжилтийн байдал;
— зардлын түвшин (хөрөнгө оруулалт, үйл ажиллагаа).

8.6.2 Эрсдэл хариуцагчийн зөвшөөрөл

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.3 f)-д хамаарна.

<u>Оролт:</u> Эрсдэлийн арга хэмжээний төлөвлөгөө(үүд).

<u>Ажиллагаа:</u> Эрсдэл хариуцагчид эрсдэлийн арга хэмжээний төлөвлөгөөг батлах.

<u>Өдөөгч:</u> Эрсдэлийн арга хэмжээний төлөвлөгөөг батлах шаардлага.

<u>Гаралт:</u> Эрсдэлийн арга хэмжээний батлагдсан төлөвлөгөө(үүд).

<u>Хэрэгжүүлэх арга зүй:</u>

Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний төлөвлөгөөг

боловсруулсны дараа эрсдэл хариуцагчаар батлуулна. Эрсдэл хариуцагчид мэдээллийн аюулгүй байдлын үлдэгдэл эрсдэлийг хүлээн зөвшөөрөх эсэхээ шийднэ. Энэхүү шийдвэрийг эрсдэлийг хүлээн зөвшөөрөх тодорхой шалгуурт үндэслэвэл зохино.

Эрсдэлийн үнэлгээний үр дүн, эрсдэлийн арга хэмжээний төлөвлөгөө болон үлэгдэл эрсдэлүүд нь эрсдэл хариуцагчид ойлгомжтой байх ёстой бөгөөд ингэснээр тэд үүргээ зохих ёсоор гүйцэтгэнэ.

8.6.3 Мэдээллийн аюулгүй байдлын үлдэгдэл эрсдэлийг хүлээн зөвшөөрөх

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 6.1.3 f)-д хамаарна.

Оролт: Эрсдэлийн арга хэмжээний батлагдсан төлөвлөгөө(үүд) ба эрсдэлийг хүлээн зөвшөөрөх шалгуур.

Ажиллагаа: Үлдэгдэл эрсдэлийг хүлээн зөвшөөрөх боломжтой эсэхийг тодорхойлох.

Өдөөгч: Байгууллага үлдэгдэл эрсдэлийг хадгалах талаар шийдвэр гаргах хэрэгцээ.

Гаралт: Хүлээн зөвшөөрөх үлдэгдэл эрсдэл.

Хэрэгжүүлэх арга зүй:

Үлдэгдэл эрсдэлийг тодорхойлохын тулд эрсдэлийн арга хэмжээний төлөвлөгөө нь үлдэгдэл болзошгүй тохиолдол, үр дагаврын дараачийн үнэлгээнд тусгагдсан байна. эрсдэлийн арга хэмжээний төлөвлөгөөнд санал болгож буй хяналтууд болон холбогдох үр нөлөөг авч үзэхдээ болзошгүй тохиолдол, үр дагаврыг аль нэгийг нь эсвэл хоёуланг нь бууруулах эсэх, үлдэгдэл эрсдэлийн түвшинг эрсдэлд хуваарилсан эсэхийг харгалзвал зохино. Дараа нь эрсдэл хариуцагч үлдэгдэл эрсдэлийн түвшинг авч үзэхдээ үлдэгдэл эрсдэлийг хүлээн зөвшөөрөх боломжтой эсэхийг тодорхойлно.

Эрсдэлийн арга хэмжээний төлөвлөгөө нь эрсдэлийг хүлээн зөвшөөрөх шалгуурыг хангахын тулд үнэлэгдсэн эрсдэлд хэрхэн арга хэмжээ авах талаар тайлбарлавал зохино.

Зарим тохиолдолд үлдэгдэл эрсдэлийн түвшин нь эрсдэлийг хүлээн зөвшөөрөх шалгуурыг хангадаггүй, учир нь хэрэглэж буй шалгуур нь зонхилох нөхцөл байдлыг харгалздаггүй.

ЖИШЭЭ: Эрсдэлийг дагалдан гарах үр өгөөж нь бизнесийн чухал боломжтой, эсвэл эрсдэлийг өөрчлөх зардал хэт өндөр учраас эрсдэлээ хадгалах шаардлагатай гэж үзэж болно.

Гэсэн ч эрсдэл хүлээн зөвшөөрөх шалгуурыг тэр бүр өөрчлөх боломжгүй байдаг.

Ийм тохиолдолд эрсдэлийг хариуцагчид хүлээн зөвшөөрөх энгийн шалгуурыг хангаагүй эрсдэлийг хадгалж болно. Шаардлагатай бол эрсдэл хариуцагч эрсдэлийн талаар тодорхой тайлбарлаж, эрсдэл хүлээн зөвшөөрөх энгийн шалгуурыг үгүйсгэх шийдвэрийн үндэслэлийг оруулна.

Эрсдэлийг хүлээн зөвшөөрөх нь эрсдэлийг хүлээн зөвшөөрөх талаар эцсийн шийдвэр гаргахаас арга хэмжээг батлах үйл явцыг хамарч болно. Эрсдэл хариуцагчид санал болгож буй эрсдэлийн арга хэмжээний төлөвлөгөө болон үлдэгдэл эрсдэлийг хянаж батлах, ийм зөвшөөрөлтэй холбоотой аливаа нөхцөлийг бүртгэх нь чухал юм. Эрсдэлийн үнэлгээний үйл явц болон эрсдэлийг хүлээн зөвшөөрөх шалгуураас хамаарч эрсдэл хариуцагчаас өндөр түвшний эрх мэдэл бүхий менежерээс эрсдэлийг хүлээн зөвшөөрөх зөвшөөрлийг шаардаж болно.

Үнэлэгдсэн эрсдэлийн арга хэмжээний төлөвлөгөөг хэрэгжүүлэхэд багагүй хугацаа шаардагдаж болно. Эрсдэлийн шалгуур нь эрсдэлийг хүлээн зөвшөөрөгдсөн хугацаанд бууруулахаар төлөвлөсан тохиолдолд эрсдэлийн түвшинг тодорхой хэмжээгээр хүссэн босго хэмжээнээс хэтрүүлж болно. Эрсдэлийг хүлээн зөвшөөрөх шийдвэр гаргахдаа эрсдэлийн арга хэмжээний төлөвлөгөөний хугацаа, эрсдэлийн арга хэмжээний хэрэгжилтийн явц төлөвлөсөнд нийцэж байгаа эсэх зэргийг харгалзан үзнэ.

Зарим эрсдэл нь цаг хугацааны явцад өөрчлөгдөж болно (энэ өөрчлөлт эрсдэлийн арга хэмжээний төлөвлөгөөний хэрэгжилттэй холбоотой эсэхээс үл хамааран). Эрсдэлийг хүлээн зөвшөөрөх шалгуур нь үүнийг харгалзан үзэх бөгөөд байгууллага үнэлэгдсэн эрсдэлд өртөж болох хугацаанаас хамаарч, эрсдэлийг хүлээн зөвшөөрөх босгыг тогтоосон байна.

9 Үйл ажиллагаа

9.1 Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явцыг гүйцэтгэх

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 8.2-д хамаарна.

<u>Оролт:</u> Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явцын талаар баримт бичиг, үүнд эрсдэлийн үнэлгээ, эрсдэлийг хүлээн зөвшөөрөх шалгуурыг агуулсан байна.

<u>Ажиллагаа:</u> Эрсдэлийн үнэлгээний үйл явцыг 7-р зүйлд заасны дагуу гүйцэтгэнэ.

<u>Өдөөгч:</u> Төлөвлөсөн интервалд эсвэл тохиолдолд үндэслэн эрсдэлийг үнэлэх байгууллагын хэрэгцээ.

<u>Гаралт:</u> Үнэлэгдсэн эрсдэлүүд.

<u>Хэрэгжүүлэх арга зүй:</u>

ISO/IEC 27001:2022 стандартын 6.1-д тодорхойлсон мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явцыг байгууллагын үйл ажиллагаанд нэгтгэх ёстой бөгөөд үүнийг төлөвлөсөн интервалаар эсвэл томоохон өөрчлөлт хийх гэж байгаа эсвэл гарсан үед хийвэл зохино. Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явц нь ISO/IEC 27001:2022 стандартын 6.1.2-д заасан шалгуурыг харгалзан үзнэ. Эрсдэлийн үнэлгээг хийх интервалууд нь МАБМТ-д тохирсон байна. МАБМТ (эсвэл түүний нөхцөл байдал) эсвэл аюул заналийн орчинд (жишээ нь, мэдээллийн аюулгүй байдлын шинэ төрлийн халдлага) мэдэгдэхүйц өөрчлөлт гарсан тохиолдолд байгууллага энэ өөрчлөлт нь мэдээллийн аюулгүй байдлын эрсдэлийн нэмэлт үнэлгээ шаардлагатай эсэхийг тодорхойлно.

Байгууллага эрсдэлийн ерөнхий үнэлгээний төлөвлөгөө гаргахдаа бизнесийн ерөнхий үйл явц болон холбогдох төсвийн мөчлөгт хамаарах аливаа хуанлийг харгалзан үзнэ.

ЖИШЭЭ: Хэрэв жилийн мөчлөгтэй төсөвтэй бол тухайн байгууллагаас жилийн тодорхой хугацаанд санхүүжилтийн хүсэлтийг шаардаж болно. Санхүүжилтийг дараа нь олгодог (багасгах эсвэл татгалзах).

Хэрэв худалдан авалтын үйл явцад т холбоотой бол эрсдэлийн арга хэмжээний зөвлөмжийг хэрэгжүүлж, дараагийн ердийн эрсдэлийн үнэлгээний өмнө үр нөлөөг нь үнэлэхээс өмнө төсвийн өөр мөчлөг шаардагдаж болно. Ийм тохиолдолд эрсдэлийн үнэлгээг дараах байдлаар төлөвлөвөл зохино:

a) эрсдэлийн арга хэмжээний зөвлөмжийг санхүүжилтийн өргөдөл гаргах үед гаргах;
b) төсвийн хуваарилалтын үр дүнгийн дагуу дахин үнэлгээ хийх;
c) аливаа худалдан авах ажиллагаа хийж, зөвлөмжийг хэрэгжүүлсний дараа дараагийн ээлжит үнэлгээг хийх.

9.2 Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний үйл явцыг гүйцэтгэх

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 8.3-д хамаарна.

Оролт: Үнэлсэн эрсдэл(үүд).

Ажиллагаа: Эрсдэлийн арга хэмжээний үйл явцыг 8-р зүйлийн дагуу гүйцэтгэнэ.

Өдөөгч: Төлөвлөсөн интервалаар эсвэл тохиолдолд үндэслэн эрсдэлийн арга хэмжээ авах байгууллагын хэрэгцээ.

Гаралт: Хадгалсан эсвэл хүлээн зөвшөөрсөн үлдэгдэл эрсдэл.

Хэрэгжүүлэх арга зүй:

ISO/IEC 27001:2022 стандартын 8.3 нь байгууллага эрсдэлийн арга хэмжээний төлөвлөгөөгөө хэрэгжүүлэхэд тавих шаардлагыг тодорхойлно. 8.6- д дурьдсан

асуудал нь энэхүү дэд зүйлд мөн хамаарна.

10 МАБМТ-тэй холбоотой үйл явцыг ашиглах

10.1 Байгууллагын нөхцөл байдал

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 4-р зүйлд хамаарна.

Оролт: Байгууллага, түүний дотоод болон гадаад нөхцөл байдлын талаар мэдээлэл.

Ажиллагаа: Мэдээллийн аюулгүй байдлын эрсдэлийн менежмент, сонирхогч талуудын шаардлагад нөлөөлж буй дотоод болон гадаад асуудлуудыг тодорхойлж, тайлбарлахын тулд холбогдох бүх мэдээллийг харгалзан үзнэ.

Өдөөгч: ISO/IEC 27001:2022 стандарт нь мэдээллийн аюулгүй байдлын зорилтуудыг бий болгохын тулд энэ төрлийн мэдээлэлд тавигдах шаардлагыг тодорхойлно.

Үр дүн: Мэдээллийн аюулгүй байдлын эрсдэлийн менежментд нөлөөлж буй эрсдэлтэй холбоотой дотоод болон гадаад асуудлууд.

Хэрэгжүүлэх арга зүй:

Байгууллага нь МАБМТ-д эерэг эсвэл сөрөг байдлаар нөлөөлж болох чухал асуудлуудын талаар өндөр түвшний (жишээлбэл, стратегийн) ойлголттой байвал зохино. Энэ нь өөрийн зорилгод нийцэх, МАБМТ-ны төлөвлөсөн үр дүнд хүрэх чадварт нөлөөлөх дотоод болон гадаад нөхцөл байдлыг цаашид мэдэж байх ёстой. Хүлээгдэж буй үр дүн нь эрсдэлийн менежментийн үйл явцыг ашиглах, аль эрсдэлийг зохих ёсоор удирдахыг мэдэх замаар мэдээллийн нууцлал, нэгдмэл байдал, хүртээмжтэй байдлыг хангана.

Эрсдэлийг найдвартай тодорхойлохын тулд байгууллага нь тухайн байгууллагын үйл ажиллагаа явуулж буй нөхцөл байдлыг хангалттай нарийвчлан ойлговол зохино. Энэ нь тухайн байгууллага тухайн байгууллагын дотоод болон гадаад нөхцөл байдал, сонирхогч талууд болон тэдгээрийн шаардлагын талаар мэдээлэл цуглуулна гэсэн үг юм (ISO/IEC 27001:2022, 4.1 ба 4.2-ыг үзнэ үү). Байгууллага МАБМТ-ны төлөвлөсөн үр дүнд нөлөөлж болох аливаа эрсдэлийг үнэлэх оролдлого эсхүл мэдээллийн аюулгүй байдлын эрсдэлээс өмнө эдгээр мэдээллийг цуглуулна. (ISO/IEC 27001:2022, 6.1.1-ийг үзнэ үү).

Байгууллага нь дотоод болон гадаад эрсдэлийн бүх эх үүсвэрийг авч үзнэ. Байгууллагын эсрэг байр суурьтай байгаа сонирхогч талууд, тэдний ашиг сонирхлын талаар ойлголт нь маш их хамааралтай.

ЖИШЭЭ 1: Байгууллагын зорилгод харш ашиг сонирхол бүхий сонирхогч этгээдийн жишээ бол халдагч юм. Халдагч нь аюулгүй байдлын түвшин муутай байгууллагыг сонирхож байдаг. Байгууллага нь энэ талын ашиг сонирхлыг эсрэгээр (хүчтэй

аюулгүй байдлын түвшин) харгалзан үзнэ, өөрөөр хэлбэл байгууллага нь МАБМТ-ны зорилтуудтай зөрчилдөж болзошгүй гэж үзнэ. Байгууллага нь мэдээллийн аюулгүй байдлын үр дүнтэй хяналтыг ашиглан эдгээр ашиг сонирхолд нийцэхгүй байхыг баталгаажуулна.

Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээнд МАБМТ-ны хамрах хүрээг бүрэн оруулаагүй үйлчилгээ, үйл ажиллагаатай харилцах харилцааг анхаарч үзэх хэрэгтэй.

ЖИШЭЭ 2: Ийм нөхцөл байдлын жишээ бол бусад байгууллагатай өмч хуваалцах (жишээ нь: байгууламж, мэдээллийн технологийн систем, мэдээллийн сан) эсвэл бизнесийн чиг үүргийг аутсорсинг хийх явдал юм.

Мэдээллийн аюулгүй байдалд нөлөөлөх бусад холбогдох хүчин зүйлсийг хэрхэн авч үзэх нь тухайн байгууллагын эрсдэлийг тодорхойлох, дүн шинжилгээ хийх аргыг сонгохоос хамаарна.

Байгууллагын мэдээллийн аюулгүй байдлын зорилтууд (ISO/IEC 27001:2022, 6.2-ыг үзнэ үү) эрсдэлийг хүлээн зөвшөөрөх шалгуурыг хязгаарлаж болно (жишээ нь, эрсдэлийг хүлээн зөвшөөрөх түвшин нь бизнесийн янз бүрийн үйл ажиллагаатай холбоотой боломжит ашиг байж болно). Цаашилбал, мэдээллийн аюулгүй байдлын бодлого нь эрсдэлийн арга хэмжээг хязгаарлаж болно (жишээ нь, эрсдэлийн арга хэмжээний тодорхой сонголтуудыг тухайн бодлогод оруулахгүй байж болно).

10.2 Манлайлал ба тууштай байдал

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 5.1-д хамаарна.

<u>Оролт:</u> Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үр дүн эсвэл зөвшөөрөх, батлах шаардлага бүхий мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний үр дүнгийн талаар мэдээлэл.

<u>Ажиллагаа:</u> Зохих түвшний удирдлага нь мэдээллийн аюулгүй байдлын эрсдэлтэй холбоотой үр дүнг авч үзэх, цаашид авах арга хэмжээг шийдвэрлэх эсвэл батвал зохино.

<u>Өдөөгч:</u> ISO/IEC 27001 стандарт нь мэдээллийн аюулгүй байдлын эрсдэлтэй холбоотой бүхий л үйл ажиллагаанд зохих түвшний удирдлага оролцохыг шаардана.

<u>Гаралт:</u> Мэдээллийн аюулгүй байдлын эрсдэлтэй холбоотой шийдвэр эсвэл баталгаа.

<u>Хэрэгжүүлэх арга зүй:</u>

Дээд удирдлага нь эрсдэлийг удирдах үүрэгтэй бөгөөд эрсдэлийн үнэлгээг манлайлж, удирдан чиглүүлнэ. Үүнд:

— эрсдэлийг удирдахад шаардлагатай нөөцийг хуваарилах;
— эрсдэлийн менежментэд холбоотой эрх мэдэл, үүрэг, хариуцлагыг байгууллагын зохих түвшинд хуваарилах;
— зохих сонирхогч талуудтай харилцах.

10.3 Харилцаа холбоо, зөвлөгөө

ТАЙЛБАР 1 Энэ дэд зүйл нь ISO/IEC 27001:2022 стандартын 7.4-д хамаарна.

ТАЙЛБАР 2 ISO/IEC 27001 стандарт нь энэхүү үйл ажиллагааны харилцаа холбооны хэсэгт шууд хамаарна.

Оролт: Эрсдэлийн менежментийн үйл явцаар тодорхойлсон эрсдэл, түүний шалтгаан, үр дагавар болон болзошгүй тохиолдлын талаар мэдээлэл.

Ажиллагаа: Эрсдэл, тэдгээрийн шалтгаан, үр дагавар, тэдгээрийн болзошгүй тохиолдол, тэдгээрийн арга хэмжээнд чиглэсэн хяналтуудын талаарх мэдээллийг гадаад, дотоод сонирхогч талуудад мэдээлэх буюу тэднээс авна.

Өдөөгч: ISO/IEC 27001 стандарт нь ийм харилцаа холбоог шаардана.

Гаралт: Байгууллагын мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явц, үр дүнгийн талаар холбогдох сонирхогчдын төсөөлөл, байнгын ойлголт.

Хэрэгжүүлэх арга зүй:

Харилцаа холбоо, зөвлөлдөх үйл ажиллагаа нь эрсдэл хариуцагчид болон бусад холбогдох сонирхогч талуудтай эрсдэлийн талаарх мэдээллийг солилцох, хуваалцах замаар эрсдэлийг хэрхэн удирдах тохиролцоонд хүрэх зорилготой. Мэдээлэлд эрсдэлийн оршихуй, шинж чанар, хэлбэр, болзошгүй тохиолдол, үр дагавар, ач холбогдол, арга хэмжээ, хүлээн зөвшөөрөх зэрэг орно, гэхдээ үүгээр хязгаарлагдахгүй.

ISO/IEC 27001:2022 стандартын 6.1.2 в) 2)-д мэдээллийн аюулгүй байдлын эрсдэлийн хариуцагчийг тодорхойлохыг шаардана. Эрсдэл хариуцагч зориудаар андуурч эсвэл нуун дарагдуулж болно. Эрсдэл хариуцагчдийг тодорхойлсон ч, тэд өөрсдийгөө эрсдэл хариуцдаг гэдгийг хүлээн зөвшөөрөхөөс татгалзаж, эрсдэлийн менежментийн үйл явцад тэднийг оролцуулахад хүндрэлтэй байж болно. Эрсдэл хариуцах тухай холбогдох хүмүүст мэдээлэх талаар харилцаа холбооны тодорхой журам байвал зохино.

ISO/IEC 27001:2022, 6.1.3 f), эрсдэл хариуцагчдийг эрсдэлийн арга хэмжээний төлөвлөгөө(үүд)-ийг баталж, үлдэгдэл эрсдэлийг хүлээн зөвшөөрөх шийдвэр гаргахыг шаардана. Эрсдэл хариуцагчид болон МАБМТ-г хэрэгжүүлэх үүрэгтэй ажилтнуудын хоорондын харилцаа холбоо нь чухал үйл ажиллагаа юм. Эрсдэл хариуцагчид болон магадгүй бусад сонирхогч талууд, шийдвэр гаргагчидтай эрсдэлийн талаарх мэдээллийг солилцох ба/эсвэл хуваалцах замаар эрсдэлийг хэрхэн удирдах талаар тохиролцсон байна. Мэдээлэлд эрсдэлийн оршихуй, мөн

чанар, хэлбэр, болзошгүй тохиолдол, ач холбогдол, арга хэмжээ, хүлээн зөвшөөрөх зэрэг орно, гэхдээ үүгээр хязгаарлагдахгүй. Харилцаа холбоо нь хоёр чиглэлтэй байна.

Эрсдэлийн шинж чанар, мэдрэмтгий байдлаас шалтгаалан эрсдэл, түүний үнэлгээ, арга хэмжээний талаарх зарим мэдээллийг үнэлэх, арга хэмжээ хэрэгжүүлэх үүрэгтэй хүмүүст “мэдэх шаардлага”-д нийцүүлэн хязгаарлах шаардлага байж болно. Эрсдэлийн харилцаа холбоо нь "мэдэх шаардлага"-ний үндсэн дээр, өөр өөр сонирхогч талуудад шаардлагатай нарийвчилсан түвшинг харгалзан, эрсдэл хариуцагчид эсвэл боломжит хариуцагчидтай зөвлөлдсөний үндсэн дээр илүү мэдрэмтгий эрсдэлүүд болон тэдгээртэй холбоотой сул талуудыг олон нийтэд мэдээлэхээс зайлсхийх зорилгоор хянах ёстой.

Эрсдэлийн талаарх ойлголт нь сонирхогч талуудын таамаглал, үзэл баримтлал, хэрэгцээ, асуудал, холбогдох санаа зовоосон асуудлын ялгаатай байдлаас шалтгаалан өөр өөр байж болно. Сонирхогч талууд эрсдэлийн талаарх ойлголтдоо тулгуурлан эрсдэлийг хүлээн зөвшөөрөх талаар дүгнэлт хийх магадлалтай. Энэ нь сонирхогч талуудын эрсдэлийн талаарх ойлголт, түүнчлэн үр ашгийн талаарх ойлголтыг тодорхойлж, баримтжуулж, үндсэн шалтгааныг тодорхой ойлгож, шийдвэрлэхэд онцгой ач холбогдолтой юм.

Эрсдэлийн талаар мэдээлэл солилцож, зөвлөлдсөнөөр үйл ажиллагаанд сонирхогч талуудын оролцоо нь сайжирч, зохих сонирхогч талууд шийдвэр, үр дүнг хариуцах боломж бүрдэнэ. Шалгууруудыг боловсруулж, эрсдэлийн үнэлгээ хийх аргуудыг сонгох талаар сонирхогч талуудтай харилцах, зөвлөлдөх нь үр дүнг сонирхогч талууд хариуцах байдлыг сайжруулна. Сонирхогч талууд боловсруулахад нь тусалсан үйл явцын үр дүнд эргэлзэх магадлал бага байна. Үүний үр дүнд тэд дүгнэлтийг хүлээн авч, үйл ажиллагааны төлөвлөгөөг дэмжих болзошгүй тохиолдол ихэвчлэн нэмэгдэнэ. Сонирхогч талууд менежер байх тохиолдолд эрсдэлийн менежментийн зорилгод хүрэх, шаардлагатай нөөцөөр хангах үүрэг амлалтыг бий болгож чадна.

Эрсдэлийн харилцаа холбоог дараахь зорилгоор хийнэ:

— байгууллагын эрсдэлийн менежментийн үр дүнг баталгаагаар хангах;
— эрсдэлийн мэдээллийг цуглуулах;
— эрсдэлийн үнэлгээний үр дүнг хуваалцах, арга хэмжээний төлөвлөгөөг танилцуулах;
— эрсдэл хариуцагчид болон сонирхогч талууд харилцан ойлгоогүйгээс мэдээллийн аюулгүй байдлын зөрчил үүсэх болон үр дагавраас зайлсхийх, эсхүл багасгах;
— эрсдэл хариуцагчдийг дэмжих;
— мэдээллийн аюулгүй байдлын шинэ мэдлэг олж авах;
— аливаа ослын үр дагаврыг бууруулахын тулд бусад талуудтай хамтран ажиллах, хариу арга хэмжээг төлөвлөх;
— эрсдэл хариуцагчид болон эрсдэлд байгаа хууль ёсны ашиг сонирхол бүхий бусад талуудад хариуцлагын мэдрэмж төрүүлэх;

— мэдлэг ойлголтыг сайжруулах.

Байгууллага нь ердийн үйл ажиллагаа болон онцгой байдлын үед эрсдэлийн талаар харилцах төлөвлөгөө боловсруулвал зохино. Эрсдэлийн талаар мэдээлэх, зөвлөгөө өгөх үйл ажиллагааг тасралтгүй явуулна.

Томоохон эрсдэл хариуцагчид болон холбогдох сонирхогч талуудын хоорондын уялдааг зохицуулахын тулд эрсдэл, түүнийг эрэмбэлэх, зохих арга хэмжээ авах, хүлээн зөвшөөрөх талаар мэтгэлцэх хороо байгуулж болно.

Эрсдэлийн харилцаа холбоог гадны гуравдагч этгээдэд сайн дураар дамжуулж болох бөгөөд ингэснээр илүү сайн эрсдэлийн менежмент, хариу арга хэмжээний зохицуулалт, мэдлэг ойлголтыг бий болгоно. Түүнчлэн зохицуулагчид эсвэл бизнесийн түншүүдээд шаардлагатай байж болно.

Эрсдэлийн талаар харилцаатай холбооны бүх ажлыг зохицуулахын тулд байгууллагын доторх олон нийттэй харилцах эсвэл харилцааны нэгжтэй хамтран ажиллах нь чухал юм. Энэ нь хямралын үеийн харилцаа холбоо идэвхжсэн тохиолдолд, тухайлбал, тодорхой аюултай тохиолдлуудад хариу үйлдэл үзүүлэхэд маш чухал юм.

10.4 Баримтжуулсан мэдээлэл

10.4.1 Ерөнхий

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 7.5-д хамаарна.

ISO/IEC 27001 стандарт нь эрсдэлийн үнэлгээний үйл явц (ISO/IEC 27001:2022, 6.1.2-ыг үзнэ үү) болон үр дүнгийн талаар (ISO/IEC 27001:2022, 8.2-ыг үзнэ үү); эрсдэлийн арга хэмжээний үйл явц (ISO/IEC 27001:2022, 6.1.3) ба үр дүн (ISO/IEC 27001:2022, 8.3).-ийн талаар баримтжуулсан мэдээллийг байгууллагад хадгалахад тавих шаардлагыг тогтооно.

10.4.2 Үйл явцын талаарх баримтжуулсан мэдээлэл

Оролт: 7, 8-р зүйлд заасны дагуу байгууллагын тодорхойлсон мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ, арга хэмжээний үйл явцын талаар мэдлэг .

Ажиллагаа: Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ, арга хэмжээний үйл явцын талаарх мэдээллийг баримтжуулж, хадгална.

Өдөөгч: ISO/IEC 27001 стандарт нь мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ, эрсдэлийн арга хэмжээний үйл явцын талаар баримтжуулсан мэдээллийг шаардана.

Гаралт: Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үйл явц эсвэл мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний үйл явцын үр дүнтэй байдалд шаардлагатай гэж тухайн байгууллагаас тодорхойлсон, сонирхогч талууд

(жишээ нь, баталгаажуулалтын байгууллага) шаардсан баримтжуулсан мэдээлэл.

Хэрэгжүүлэх арга зүй:

Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний талаарх баримтжуулсан мэдээлэл нь дараахь зүйлсийг агуулна:

a) эрсдэлийн шалгуур үзүүлэлтүүдийн тодорхойлолт (эрсдэлийг хүлээн зөвшөөрөх шалгуур, мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ хийх шалгуурыг агуулна);
b) үр дүнгийн тууштай, үндэслэлтэй, харьцуулагдах үндэслэл;
c) эрсдэлийг тодорхойлох аргын тодорхойлолт (эрсдэл хариуцагчийг тодорхойлох гэх мэт);
d) мэдээллийн аюулгүй байдлын эрсдэлийн шинжилгээний аргын тодорхойлолт (болзошгүй үр дагавар, бодит болзошгүй тохиолдол ба эрсдэлийн түвшингийн үнэлгээ);
e) үр дүнг эрсдэлийн шалгуур үзүүлэлттэй харьцуулах арга, эрсдэлийн арга хэмжээний эрсдэлийг эрэмбэлсэн аргын тодорхойлолт,

Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний үйл явцын талаарх баримтжуулсан мэдээлэл нь дараахь зүйлсийг агуулна:

— Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний оновчтой хувилбаруудыг сонгох арга;
— шаардлагатай хяналтыг тодорхойлох арга;
— шаардлагатай хяналтыг санамсаргүй орхигдуулаагүй гэдгийг тодорхойлоход ISO/IEC 27001:2022 стандартын А хавсралтыг хэрхэн ашиглах;
— эрсдэлийн арга хэмжээний төлөвлөгөөг хэрхэн бий болгох;
— эрсдэл хариуцагчдийн зөвшөөрлийг хэрхэн авах.

10.4.3 Үр дүнгийн талаарх баримтжуулсан мэдээлэл

Оролт: Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ, эрсдэлийн арга хэмжээний үр дүн.

Ажиллагаа: Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ, арга хэмжээний үр дүнгийн талаарх мэдээллийг баримтжуулж, хадгална.

Өдөөгч: ISO/IEC 27001 нь мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ, арга хэмжээний үр дүнгийн талаар баримтжуулсан мэдээллийг шаардана.

Гаралт: Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ, арга хэмжээний үр дүнгийн талаарх баримтжуулсан мэдээлэл.

Хэрэгжүүлэх арга зүй:

Байгууллагууд төлөвлөсөн хугацаанд эрсдэлийн үнэлгээ хийх шаардлагатай, эсвэл томоохон өөрчлөлт хийх санал гаргасан эсвэл өөрчлөлт гарсан тохиолдолд

эрсдэлийн үнэлгээг хуваарийн дагуу хийж байгааг нотлох хуваарь байх ёстой. Хэрэв өөрчлөлтийг санал болгож байгаа эсвэл өөрчлөлт гарсан бол эрсдэлийн үнэлгээний гүйцэтгэлийг нотлох баримт байх ёстой. Үгүй бол байгууллага яагаад өөрчлөлт чухал, үгүйг тайлбарлах ёстой.

Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үр дүнгийн талаарх баримтжуулсан мэдээлэл нь дараахь мэдээллийг ийг агуулна:

a) тодорхойлсон эрсдэл, тэдгээрийн үр дагавар, болзошгүй тохиолдол;
b) эрсдэл хариуцагчийн хувийн мэдээлэл;
c) эрсдэл хүлээн зөвшөөрөх шалгуурыг хэрэглэсний үр дүн;
d) эрсдэлийн арга хэмжээний тэргүүлэх чиглэл.

Алдаанаас суралцаж, байнгын сайжруулалтыг хийхийн тулд эрсдэлийн шийдвэрийн үндэслэлийг бүртгэхийг зөвлөж байна.

Мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний үр дүнгийн талаарх баримтжуулсан мэдээлэл нь дараахь зүйлсийг агуулна.

— шаардлагатай хяналтыг тодорхойлох;
— байгууллагын эрсдэлийг хүлээн зөвшөөрөх шалгуурыг хангахын тулд эдгээр шаардлагатай хяналтууд шаардлагатай болон боломжтой тохиолдолд хэрэгжиж буй нотолгоо.

10.5 Мониторинг ба дүн шинжилгээ

10.5.1 Ерөнхий

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 9.1-д хамаарна.

Байгууллагын мониторингийн үйл явц (ISO/IEC 27001:2022, 9.1-ийг үзнэ үү) нь дараахь зорилгоор эрсдэлийн үнэлгээ болон эрсдэлийн арга хэмжээний үйл явцын бүх талыг хамарвал зохино:

a) эрсдэлийн арга хэмжээний загвар, үйл ажиллагаа нь үр дүнтэй, үр ашигтай, хэмнэлттэй байхыг баталгаажуулах;
b) цаашид эрсдэлийн үнэлгээг сайжруулах мэдээлэл олж авах;
c) аюултай тохиолдлууд (үүнд ойрын алдаанууд), өөрчлөлт, хандлага, амжилт, бүтэлгүйтэлин шинжилгээ ба сурсан зүйлс ;
d) эрсдэлийн арга хэмжээ, тэргүүлэх чиглэлд дүн шинжилгээ шаардлагатай эрсдэлийн шалгуур үзүүлэлт болон эрсдэлийг агуулсан дотоод болон гадаад нөхцөл байдлын өөрчлөлтийг илрүүлэх;
e) шинээр гарч ирж буй эрсдэлийг тодорхойлох.

Эрсдэлийн менежментийн үйл ажиллагааны хадгалагдсан эрсдэлийн хувилбаруудыг үр дүнтэй мониторингийн үйл явцыг хангахын тулд хяналтын хувилбарт шилжүүлж болно. Мониторингийн хувилбаруудын талаарх дэлгэрэнгүй

мэдээллийг А.2.7-д дурьдсан.

10.5.2 Эрсдэлд нөлөөлж буй хүчин зүйлсэд мониторинг, дүн шинжилгээ хийх

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 9.1-д хамаарна.

Оролт: Эрсдэлийн менежментийн үйл ажиллагаанаас олж авсан эрсдэлийн бүх мэдээлэл.

Ажиллагаа: Эрсдэл ба түүний хүчин зүйлс (жишээ нь өмчийн үнэ цэнэ, үр дагавар, аюул занал, эмзэг байдал, болзошгүй тохиолдол) -д мониторинг, дүн шинжилгээ хийж, байгууллагын нөхцөл байдалд гарсан аливаа өөрчлөлтийг эрт үе шатанд тодорхойлж, эрсдэлийн бүрэн дүр зургийг тоймлон авч үзэх.

Өдөөгч: Байгууллагын бодлогод дүн шинжилгээ хийж, одоогийн үйл ажиллагаа эсвэл аюул заналхийллийн орчинд гарсан аливаа өөрчлөлтийг илрүүлэх.

Гаралт: Эрсдэлийн менежментийг байгууллагын бизнесийн зорилго, эрсдэлийг хүлээн зөвшөөрөх шалгууртай тасралтгүй уялдуулах.

Хэрэгжүүлэх арга зүй:

ISO/IEC 27001:2022 стандартын 9.1 нь байгууллагууд мэдээллийн аюулгүй байдлын гүйцэтгэл (болон МАБМТ-ны үр нөлөөг)-ээ үнэлэхийг шаардана. Энэ шаардлагын дагуу байгууллагууд эрсдэлийн арга хэмжээний төлөвлөгөө(үүд)-ээ гүйцэтгэлийн үнэлгээний субьект болговол зохино. Үүний тулд байгууллага эхлээд нэг буюу хэд хэдэн мэдээллийн хэрэгцээг тодорхойлно, тухайлбал, байгууллага өөрийгөө аюул заналаас хамгаалах чадварын талаар Дээд удирдлага юу мэдэхийг хүсч байгааг тайлбарлах хэрэгтэй. Үүнийг дээд түвшний шаардлага болгон ашигласнаар байгууллага мэдээллийн хэрэгцээг хангахад шаардлагатай хэмжилт, хэмжээг хэрхэн хослуулах ёстойг тодорхолйно.

Эрсдэл нь тогтвортой зүйл биш. Тохиолдлын явдлын хувилбарууд, өмчийн үнэ цэнэ, аюул занал, эмзэг байдал, болзошгүй тохиолдол, үр дагавар нь ямар ч заалтгүйгээр гэнэт өөрчлөгдөж болно. Эдгээр өөрчлөлтийг илрүүлэхийн тулд байнгын мониторинг хийх шаардлагатай. Үүнийг шинэ аюул занал, эмзэг байдлын талаарх мэдээллээр хангадаг гадны үйлчилгээгээр дэмжиж болно. Байгууллага дараах хүчин зүйлсийн байнгын мониторингийг хангавал зохино:

a) эрсдэлийн шинэ эх үүсвэрүүд, үүнд шинээр тайлагнасан мэдээллийн технологийн цоорхой;
b) эрсдэлийн менежментийн хамрах хүрээнд шинээр орсон өмч хөрөнгө;
c) өмчийн үнэ цэнийн зайлшгүй өөрчлөлт (жишээ нь бизнесийн шаардлага өөрчлөгдсөнтэй холбоотой);
d) шинээр эсвэл дахин гарч ирж буй аюулд өртөгсдийг тодорхойлохын тулд илрүүлсэн сул талууд;
e) одоо байгаа эсвэл шинэ технологийг ашиглах загварын өөрчлөлт, үүнээс

үүсэх довтолгооны шинэ боломжууд

f) хууль тогтоомжийн өөрчлөлт;
g) эрсдэлийг бууруулах эрмэлзэл, одоо юуг хүлээн зөвшөөрөх, юуг хүлээн зөвшөөрөхгүй талаарх ойлголтын өөрчлөлт;
h) байгууллагын дотор болон гаднах мэдээллийн аюулгүй байдлын аюултай тохиолдол.

Эрсдэлийн шинэ эх үүсвэр эсвэл болзошгүй тохиолдол, үр дагаварт гарсан өөрчлөлтүүд нь өмнө нь үнэлэгдсэн эрсдэлийг нэмэгдүүлэх боломжтой. Бага болон хадгалагдаагүй эрсдэлийг хянан үзэхдээ эрсдэл тус бүрийг тусад нь, мөн эдгээр бүх эрсдэлийг нэгтгэж, тэдгээрийн хуримтлагдсан үр дагаварт дүн шинжилгээ хийнэ. Хэрэв эрсдэл бага буюу хүлээн зөвшөөрөгдөх эрсдэлийн ангилалд хамаарахаа больсон бол 8.2-т заасан нэг буюу хэд хэдэн хувилбарыг ашиглан тэдгээрийг авч үзнэ.

Тохиолдол тохиох болзошгүй тохиолдол болон тэдгээртэй холбоотой үр дагаварт нөлөөлж буй хүчин зүйлс болон эрсдэлиийн янз бүрийн арга хэмжээний сонголтуудын тохиромжтой байдал, өртөгт нөлөөлөх хүчин зүйлс өөрчлөгдөж болно. Байгууллагад нөлөөлж буй томоохон өөрчлөлтүүдэд илүү тодорхой дүн шинжилгээ хийнэ. Эрсдэлийн мониторингийн үйл ажиллагааг тогтмол давтаж, эрсдэлийн арга хэмжээний сонгосон хувилбаруудыг үе үе хянаж байвал зохино.

Шинэ аюул занал, эмзэг байдал эсвэл болзошгүй тохиолдол, үр дагаврыг өөрчлөх нь өмнө нь бага гэж үнэлэгдсэн эрсдэлийг нэмэгдүүлнэ. Бага болон хадгалагдаагүй эрсдэлд дүн шинжилгээ хийхдээ эрсдэл бүрийг тусад нь авч үзэх ба хуримтлагдсан болзошгүй үр дагаврыг үнэлэхийн тулд эдгээр бүх эрсдэлийг нэгтгэн дүгнэнэ. Хэрэв эрсдэл нь бага буюу хүлээн зөвшөөрөгдөх эрсдэлийн ангилалд хамаарахгүй бол тэдгээрийг 8-р зүйлд заасан нэг буюу хэд хэдэн хувилбарыг ашиглан авч үзнэ.

Аюул занал илрэх болзошгүй тохиолдол, тэдгээрийн үр дагаварт нөлөөлөх хүчин зүйлс, болон арга хэмжээний янз бүрийн хувилбаруудын тохиромжтой байдал, өртөгт нөлөөлж буй хүчин зүйлс өөрчлөгдөж болно. Байгууллагад нөлөөлж буй томоохон өөрчлөлтүүдэд илүү тодорхой дүн шинжилгээ хийвэл зохино. Эрсдэлийн мониторингийн үйл ажиллагааг тогтмол давтаж, эрсдэлийн арга хэмжээний сонгосон хувилбаруудыг үе үе дүн шинжилгээ хийнэ.

Эрсдэлийн мониторингийн үйл ажиллагааны үр дүн нь эрсдэлийн дүн шинжилгээний бусад үйл ажиллагааны орц болно. Байгууллага нь ISO/IEC 27001:2022-ын 8-р зүйлийн дагуу томоохон өөрчлөлтүүдийг санал болгосон эсвэл өөрчлөлт гарсан тохиолдолд бүх эрсдэлд тогтмол дүн шинжилгээ хийнэ.

10.6 Удирдлагын дүн шинжилгээ

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 9.3-д хамаарна.

<u>Оролт:</u> Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үр дүн, мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний төлөвлөгөөний байдал.

Ажиллагаа: Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээний үр дүн болон мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний төлөвлөгөөний төлөв байдлыг хянаж, үлдэгдэл эрсдэл нь эрсдэл хүлээн зөвшөөрөх шалгуурт нийцэж байгаа эсэх, эрсдэлийн арга хэмжээний төлөвлөгөө нь холбогдох бүх эрсдэл, тэдгээрийн эрсдэлийн арга хэмжээ хувилбаруудыг тусгасан эсэхийг баталгаажуулна.

Өдөөгч:Төлөвлөгөөт календарьчилсан дүн шинжилгээний хэсэг.

Гаралт: Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ хийх шалгуур, эрсдэлийг хүлээн зөвшөөрөх шалгуурын өөрчлөлт, мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээний шинэчилсэн төлөвлөгөө эсвэл SOA.

10.7 Залруулах арга хэмжээ

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 10.1-д хамаарна.

Оролт: Эрсдэлийн арга хэмжээний төлөвлөгөө үр дүнгүй болсоноор арга хэмжээний төлөвлөгөө дууссаны дараа үлдэгдэл эрсдэл нь хүлээн зөвшөөрөгдөөгүй түвшинд үлдэнэ.

Ажиллагаа: Эрсдэлийн арга хэмжээний төлөвлөгөөг дахин хянаж, үлдэгдэл эрсдэлийг хүлээн зөвшөөрөгдөх хэмжээнд хүртэл өөрчилнө.

Өдөөгч: Эрсдэлийн арга хэмжээний төлөвлөгөөг шинэчлэх шийдвэр.

Гаралт: Эрсдэлийн арга хэмжээний шинэчилсэн төлөвлөгөө ба түүний хэрэгжилт.

Хэрэгжүүлэх арга зүй:

Эрсдэлийн арга хэмжээний төлөвлөгөөний үр ашигтай холбоотой үл тохирлыг дотоод болон хөндлөнгийн аудит, мониторинг, шалгуур үзүүлэлтээр гаргаж болно. Арга хэмжээний төлөвлөгөөг дараахь зүйлсийг тусгаж өөрчлөх шаардлагатай:

— мэдээллийн аюулгүй байдлын эрсдэлийн арга хэмжээ үйл явцын үр дүн;
— төлөвлөгөөний аажим хэрэгжилт (жишээ нь хяналтыг тодорхойлсоны дагуу, загварчилсны дагуу, байгаа байдлаар нь хэрэгжүүлэх);
— хяналтыг хэрэгжүүлэхэд тулгарч буй бэрхшээлүүд (жишээ нь, техникийн болон санхүүгийн асуудал, дотоод болон гадаад хүчин зүйлстэй нийцэхгүй байх, хувийн нууцлал гэх мэт).

Арга хэмжээний төлөвлөгөө дууссаны дараа үлдэгдэл эрсдэл нь хүлээн зөвшөөрөгдөх боломжтой ч хэрэглэгчид ашиглахаас татгалзах, эсвэл ашиглахад хялбар байдлын хувьд эдгээр хяналтыг хэрэглэгчид хүлээн зөвшөөрдөггүй тохиолдол байдаг. (жишээ нь эргономик бус, хэтэрхий төвөгтэй эсвэл хэтэрхий урт).

Байгууллага шинэчилсэн арга хэмжээний төлөвлөгөөний үр нөлөөнд дүн шинжилгээ хийвэл зохино.

10.8 Байнгын сайжруулалт

ТАЙЛБАР: Энэхүү дэд зүйл нь ISO/IEC 27001:2022 стандартын 10.2-д хамаарна.

Оролт: Эрсдэлийн менежментийн үйл ажиллагаанаас олж авсан эрсдэлийн талаар бүх мэдээлэл.

Ажиллагаа: Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явцыг байнга мониторинг, дүн шинжилгээ хийж шаардлагатай бол сайжруулвал зохино.

Өдөөгч: Байгууллага мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явцын явцад олж авсан сургамжаасаа сайжруулж, төлөвшихийг эрмэлздэг.

Гаралт: Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явц нь байгууллагын бизнесийн зорилго эсвэл үйл явцын шинэчлэлд байнга хамааралтай байх

Хэрэгжүүлэх арга зүй:

Нөхцөл байдал, эрсдэлийн үнэлгээний үр дүн, эрсдэлийн арга хэмжээ болон менежментийн төлөвлөгөө нь нөхцөл байдалд тохирсон хэвээр байгаа эсэхэд явцын мониторинг, дүн шинжилгээ хийх нь мэдээллийн аюулгүй байдлын менежментийн үйл явц зөв гэдгийг баталгаажуулахад зайлшгүй шаардлагатай.

Байгууллага нь мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явц болон холбогдох үйл ажиллагаа нь өнөөгийн нөхцөл байдалд тохирсон хэвээр, мөрдөж байгаад шалгах естой. Үйл явц, үйл ажиллагааны аливаа тохиролцсон сайжруулалт эсвэл үйл явцын нийцлийг сайжруулахад шаардлагатай бөгөөд хариуцсан менежерүүдэд мэдэгдвэл зохино. Эдгээр менежерүүдэд аливаа эрсдэл, эрсдэлийн элементийг үл тоомсорлож, дутуу үнэлэхгүй, эрсдэлийг бодитойгоор ойлгож, шаардлагатай хариу арга хэмжээ авах, шийдвэр гаргах баталгааг олгоно.

Өөрчлөлтийн менежментийн үйл явц нь эрсдэлийн менежментийн үйл явцтай байнгын эргэх холбоотой байх ёстой. Ингэснээр эрсдэлийг өөрчлөх боломжтой мэдээллийн системийн өөрчлөлт нь эрсдэлийг нэн даруй анхааралдаа авч, эрсдэлийн үнэлгээний үйл ажиллагааг өөрчилснөөр үнэлгээг зөв хийнэ.

Байгууллага эрсдэлийг хэмжихэд ашигласан шалгуурыг тогтмол шалгаж байвал зохино. Ийнхүү шалгах нь бүх элементүүд бизнесийн зорилго, стратеги, бодлоготой нийцсэн хүчинтэй хэвээр байгаа бөгөөд мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явцын явцад бизнесийн нөхцөл байдалд гарсан өөрчлөлтийг зохих ёсоор харгалзан үзсэнийг эсэхийг баталгаажуулна. Энэхүү мониторинг, дүн шинжилгээний үйл ажиллагаа нь дараахь зүйлд чиглэнэ: (гэхдээ үүгээр хязгаарлагдахгүй):

— хууль эрх зүйн болон байгаль орчны нөхцөл байдал;
— өрсөлдөөний нөхцөл байдал;
— эрсдэлийн үнэлгээний арга;

— өмчийн үнэ цэнэ, ангилал;
— үр дагаврын шалгуур;
— болзошгүй байллын шалгуур;
— эрсдэлийн үнэлгээний шалгуур;
— эрсдэлийг хүлээн зөвшөөрөх шалгуур;
— нийт өмчлөх зардал;
— шаардлагатай нөөц.

Байгууллага шинэ эсвэл өөрчлөгдсөн аюул, эмзэг байдалд анхаарч, удирдлагад зөвлөгөө өгөхийн тулд эрсдэлийн үнэлгээ, эрсдэлийн арга хэмжээний нөөцийн байнгын бэлэн байдлыг хангана.

Эрсдэлийн менежментийн мониторингийн үр дүн нь дараахь зүйлээс хамааран ашигласан арга, аргачлал, арга хэрэгслийг өөрчлөх, нэмэхэд хүргэнэ:

— байгууллагын эрсдэлийн хугацаа;
— илэрсэн өөрчлөлт;
— эрсдэлийн үнэлгээний давталт;
— Мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явцын зорилго (жишээ нь, бизнесийн тасралтгүй байдал, аюултай тохиолдолд тэсвэртэй байдал, нийцэл);
— мэдээллийн аюулгүй байдлын эрсдэлийн менежментийн үйл явцын объект (жишээ нь: байгууллага, бизнесийн нэгж, мэдээллийн үйл явц, түүний техникийн хэрэгжилт, хэрэглээ, интернет холболт).

Эрсдэлийн үнэлгээ, эрсдэлийн арга хэмжээний хамрах хүрээтэй холбоотой эрсдэлийн менежментийн мөчлөгийг 5.2-т үзүүлэв.

А хавсралт (мэдээллийн)
Эрсдэлийн үнэлгээний үйл явцыг дэмжих аргуудын жишээ

А.1 Мэдээллийн аюулгүй байдлын эрсдэлийн шалгуур

А.1.1 Эрсдэлийн үнэлгээтэй холбоотой шалгуур

А.1.1.1 Эрсдэлийн үнэлгээний ерөнхий асуудлууд

Мэдээллийн эрсдэлийн үнэлгээнд хувь хүний тодорхойгүй байдал давамгайлдаг бөгөөд өөр өөр шинжээчид болзошгүй тохиолдол, үр дагаврын хэмжигдэхүүний оноог тайлбарлахдаа тодорхойгүй байдлын өөр өөр хандлагыг харуулдаг. Тулгуур хуваарь(scale) нь үр дагавар, болзошгүй тохиолдол, эрсдэлийн ангиллыг хоёрдмол утгагүй, объектив утгуудтай холбож, боломжтой бол санхүүгийн алдагдалыг мөнгөний нэгжээр, тохиолдох давтамжийг тодорхой хугацаагаар гэх мэтээр тоон аргаар илэрхийлвэл зохино.

Ялангуяа чанарын арыг хэрэглэх тохиолдолд эрсдэлийн шинжээчид өөрсдийн дүгнэлтийн тохиргоог хадгалахын тулд тулгуур хуваарь(scale)-ийн дагуу сургалт, дадлагыг тогтмол хийвэл зохино.

А.1.1.2 Чанарын хандлага

А.1.1.2.1 Үр дагаврын хуваарь(scale)

А.1 хүснэгтэд үр дагаврын хуваарь(scale)-ийн жишээг үзүүлэв.

А.1 хүснэгт- Үр дагаврын хуваарийн жишээ

Үр дагавар	Тайлбар
5-гамшигт (Catastrophic)	**Байгууллагаас гадуур салбарын эсвэл зохицуулалтын үр дагавар** Салбарын экосистемд ихээхэн нөлөөлсөн бөгөөд үр дагавар нь удаан үргэлжлэх боломжтой. ба/эсвэл: улсын хувьд хүндрэлтэй, тэр ч байтугай зохицуулалтын үйл ажиллагааг хангах, эсвэл өөрийн эрхэм зорилтуудыг хангах чадваргүй байдал, ба/эсвэл: хүн болон өмчийн аюулгүй байдалд ноцтой үр дагавар учрах (эрүүл мэндийн хямрал, хүрээлэн буй орчны ихээхэн бохирдол, зайлшгүй шаардлагатай дэд бүтэц сүйрэх гэх мэт).
4- Аюултай (Critical)	**Байгууллагад гамшигт үр дагавар учрах** Байгууллага үйл ажиллагаагаа хэсэгчлэн эсвэл бүхэлд нь хэрэгжүүлэх чадваргүй байдал, хүн болон өмч хөрөнгийн аюулгүй байдалд ноцтой үр дагавар учруулж болзошгүй. Байгууллага нөхцөл байдлыг даван туулахгүй байж болзошгүй (түүний оршин тогтнох байдалд нь аюул занал учирсан), улсын болон салбарын үйл ажиллагаа аажимдаа нөлөөлөх, удаан үргэлжлэх үр дагаваргүй.
3-Ноцтой (Serious)	**Байгууллагын хувьд ноцтой үр дагавар** Хүн, өмч хөрөнгийн аюулгүй байдалд ноцтой үр дагаварт хүргэж болзошгүй үйл ажиллагааны гүйцэтгэлийн иэхээхэн доройтол. Байгууллага нь аливаа салбар, төрд нөлөөлөхгүй, ноцтой хүндрэлтэй (ихээхэн доройтсон байдалд ажиллах) - ээр нөхцөл байдлыг даван туулна.
2-Мэдэгдэхүйц (Significant)	**Байгууллагын хувьд мэдэгдэхүйц боловч хязгаарлагдмал үр дагавар** Хүн, өмч хөрөнгийн аюулгүй байдалд үр дагаваргүйгээр үйл ажиллагааны гүйцэтгэлийн доройтох. Байгууллага нь зарим бэрхшээлийг үл харгалзан нөхцөл байдлыг даван туулна. (доройтсон горимд ажиллах).
1-Бага (Minor)	**Байгууллагын хувьд ялихгүй үр дагавар** Үйл ажиллагаа, үйл ажиллагааны гүйцэтгэл, хүн, өмч хөрөнгийн аюулгүй байдалд ямар нэгэн үр дагавар гарахгүй. Байгууллага нь нөхцөл байдлыг их хүндрэлгүйгээр даван туулна. (хязгааруудыг зарцуулна).

А.1.1.2.2 Болзошгүй тохиолдол (likelihood)-ын хуваарь (scale)

А.2 хүснэгт А.2 болон А.4 хүснэгтэд болзошгүй тохиолдолын хуваарийг илэрхийлэх өөр аргуудын жишээг үзүүлэв. Болзошгүй тохиолдолыг А.2 хүснэгт дахь магадлалын үзүүлэлтээр эсвэл А.4 хүснэгт дэх давтамжтай үзүүлэлтээр илэрхийлж болно.

Магадлалаар илэрхийлэх нь тодорхой хугацааны дотор эрсдэлийн тохиолдол гарах дундаж болзошгүй тохиолдлыг, давтамжаар илэрхийлэх нь тодорхой дундаж

хугацааны дотор эрсдэлийн тохиолдол гарч болох эрсдэлийн тохиолдлын тоог илэрхийлнэ. Эдгээр хоёр арга нь ижил зүйлийг хоёр өөр талаас илэрхийлдэг тул тухайн байгууллага тухайн эрсдэлийн ангилалд хамгийн тохиромжтой гэж үзсэн аргаа хэрэглэнэ.

Хэрэв аргуудыг хоёуланг нь нэг байгууллагад өөр хувилбар болгон ашиглаж байгаа тохиолдолд хуваариудын нөхцөлт тэнцүү заалтууд нь бодит, ижил болзошгүй тохиолдлыг заах нь чухал юм. Үгүй бол, эрсдэлийн үнэлгээний бодит үр дүн нь болзошгүй тохиолдолоос илүүтэйгээр аль хуваарийг ашиглахаас хамаарна. Хэрэв хоёр аргыг аль алиныг нь ашиглавал нөхцөлт зэрэглэл тус бүрийн магадлалын түвшинг тэнцүү зэрэглэлийн давтамжийн утгаас математик аргаар эсхүл эсрэгээрээ анхдагч хуваарийг тодорхойлоход ямар ашиглаж байгаагаас хамаарна.

Хэрэв хоёр аргын аль нэгийг нь дангаар нь ашиглавал хуваарийн өсөлтийг хэт нарийн тодорхойлох шаардлагагүй, учир нь хэрэглэж буй үнэмлэхүй утгуудаас үл хамааран болзошгүй тохиолдлыг эрэмбэлэх боломжтой хэвээр байна. Хэдийгээр А.2 хүснэгт болон А.4 хүснэгт нь болзошгүй тохиолдолын огт өөр өсөлт, зэрэглэлийг ашигладаг боловч, байгууллагын нөхцөл байдал болон үнэлж буй эрсдлийн ангиллаас хамаарч, аль нэгийг нь дангаар нь хэрэглэхэд шинжилгээний үр ашиг адилхан байж болно. Гэсэн хэдий ч тэдгээрийг ижил нөхцөл байдалд өөр хувилбар болгон аюулгүй ашиглах боломжгүй, учир нь тэнцүү зэрэглэлд хамаарах утгууд нь ижил хамааралгүй.

А.2 хүснэгт болон А.4 хүснэгтэд ашигласан ангилал, утгууд нь зөвхөн жишээ юм. Болзошгүй тохиолдолын түвшин бүрт оноох хамгийн тохиромжтой утга нь тухайн байгууллагын эрсдэлийн төлөв байдал, эрсдэлийг бууруулах эрмэлзэлээс хамаарна.

А.2 хүснэгт- Болзошгүй тохиолдолын түвшингийн жишээ

Болзошгүй тохиолдол	Тайлбар
5-Бараг тодорхой	Эрсдэлийн эх үүсвэр нь довтолгооны аргуудын аль нэгийг ашиглан зорилгодоо хүрэх нь гарцаагүй. Эрсдэлийн хувилбарын үүсэх магадлал маш өндөр.
4 - Маш өндөр магадлалтай	Эрсдэлийн эх үүсвэр нь довтолгооны аргуудын аль нэгийг ашиглан зорилгодоо хүрэх магадлалтай. Эрсдэлийн хувилбарын үүсэх магадлал өндөр.
3 - Магадлалтай	Эрсдэлийн эх үүсвэр нь довтолгооны аргуудын аль нэгийг ашиглан зорилгодоо хүрэх боломжтой. Эрсдэлийн хувилбарын үүсэх магадлал маш их байна.
2 - Магадлал багатай	Эрсдэлийн эх үүсвэр нь довтолгооны аргуудын аль нэгийг ашиглан зорилгодоо хүрэх боломж харьцангуй бага байна. Эрсдэлийн хувилбарын үүсэх магадлал бага байна.
1 - Магадлалгүй	Эрсдэлийн эх үүсвэр нь довтолгооны аргуудын аль нэгийг ашиглан зорилгодоо хүрэх магадлал маш бага байна. Эрсдэлийн хувилбарын үүсэх магадлал маш бага.

Болзошгүй тохиолдлын үнэлгээний аль нэг аргыг ашиглахдаа "бага", "дунд", "өндөр" зэрэг хэллэгийг зэрэглэлд хавсаргаж болно. Энэ нь эрсдэлийн мэргэжилтэн биш сонирхогч талуудтай болзошгүй тохиолдлын түвшинг хэлэлцэхэд хэрэг болно. Гэсэн хэдий ч тэдгээр нь субъектив бөгөөд тиймээс зайлшгүй хоёрдмол утгатай. Иймд үнэлгээ хийх эсвэл тайлагнахдаа тэдгээрийг гол тодорхойлох үг болгон ашиглаж болохгүй.

А.1.1.2.3 Эрсдэлийн түвшин

Чанарын хуваарийн ашиг тус, тэдгээрээс үүдэлтэй эрсдлийн үнэлгээний тууштай байдал нь тухайн ангиллын шошгыг бүх сонирхогч талууд хэрхэн тайлбарлахаас бүрэн хамаарна. Аливаа чанарын Түвшин тус бүрийн чанарын тайлбарыг объектив хэлээр илэрхийлэх бөгөөд , ангиллууд нь бие биетэйгээ давхцаж болохгүй.

Иймд болзошгүй тохиолдол, эрсдэлийн үр дагаварын тодорхойлолтыг ярианд ашиглахдаа эдгээр нь тоон (А.4 хүснэгтийн дагуу) эсвэл лавлах оноо (хүснэгтийн дагуу)-г тогтоосон хоёрдмол утгагүй хуваарийг албагггн ёсоор эш татна. Чанарын үнэлгээний өгөгдөл, үр дүнгийн тайлбарын тууштай байдлыг хангахын тулд бүх сонирхогч талууд лавлагаа хуваарийн талаар мэдлэг ойлголттой байвал зохино.

А.3 хүснэгтэд чанарын аргын жишээг үзүүлэв.

А.3 хүснэгт- Эрсдэлийн шалгуурын чанарын аргын жишээ

Болзошгүй тохиолдол	Үр дагавар				
	Гамшигийн	Аюултай	Ноцтой	Мэдэгдэхүйц	Бага
Бараг тодорхой	Маш өндөр	Маш өндөр	Өндөр	Өндөр	Дунд зэрэг
Маш өндөр магадлалтай	Маш өндөр	Өндөр	Өндөр	Дунд	Бага
Магадлалтай	Өндөр	Өндөр	Дунд	Бага	Бага
Магадлал багатай	Дунд	Дунд	Бага	Бага	Маш бага
Магадлалгүй	Бага	Бага	Бага	Маш бага	Маш бага

Чанарын эрсдэлийн матрицын загварыг боловсруулахдаа байгууллагын эрсдэлийг хүлээх шалгуурыг баримтална. (6.4.2 ба А.1.2-ыг үзнэ үү).

ЖИШЭЭ: Байгууллага тохиолдох магадлал багатай ч онцгой үр дагаварт илүү их санаа зовдог, эсвэл бага үр дагавартай өндөр давтамжтай тохиолдлын талаар ихэвчлэн санаа зовдог.

Эрсдэлийн чанарын эсвэл тоон матрицыг боловсруулах үед байгууллагын эрсдэлийн хэмжээ тэгш хэмт бус байдаг. Өчүүхэн тохиолдлууд ихэвчлэн хамгийн их тохиолддог бөгөөд хүлээгдэж буй давтамж нь ихэвчлэн үр дагавар нэмэгдэх тусам буурдаг, туйлын үр дагаварт хүргэх болзошгүй тохиолдол нь маш бага байдаг. Болзошгүй тохиолдол өндөр/бага үр дагавартай тохиолдолоор илэрхийлсэн нь болзошгүй тохиолдол бага/өндөр үр дагавартай тохиолдолтой ижил бөгөөд бизнест үзүүлэх үр нөлөө нь бага тохиолдол хааяа байдаг. Хэдийгээр диагоналийн дагуу бага/бага, өндөр/өндөр тэгш хэмтэй эрсдэлийн матрицыг үүсгэхэд хялбар боловч энэ нь аливаа байгууллагын бодит эрсдлийн хэмжээг үнэн зөв илэрхийлэх магадлал

багатай тул буруу үр дүнд хүргэж болзошгүй юм. Эрсдэлийн матриц нь бодитой бөгөөд байнгын сайжруулах шаардлагыг (ISO/IEC 27001:2022 стандартын 10.2-ыг үзнэ үү) хангах байдлыг баталгаажуулахын тулд ангилал тус бүрийг болзошгүй байдал, үр дагаврын хуваарийн дагуу эрсдэлийн матрицад хуваарилах, түүнчлэн ангилалуудыг байгууллагын эрсдэлийн хэмжээнд харгалзуулах үндэслэлийг хуваарь, матрицыг тодорхойлох эсвэл өөрчлөх үед баримтжуулна. Өндөр хуваарьтай матрицыг ашиглахтай холбоотой тодорхойгүй байдалын талаар хэрэглэгчдэд болгоомжтой тайлбарлана.

Чанарын хуваарийн ашиг тус, тэдгээрээс үүдэлтэй эрсдлийн үнэлгээний тууштай байдал нь тухайн ангиллын шошгыг сонирхогч бүх талууд хэрхэн тайлбарлаж байгаагаас бүрэн хамаарна. Аливаа чанарын хуваарийн түвшин нь хоёрдмол утгагүй, түүний өсөлтийг тодорхой тодорхойлсон, түвшин тус бүрийн чанарын тодорхойлолтыг объектив хэлээр илэрхийлж, ангиллууд нь бие биетэйгээ давхцахгүй байх естой.

А.1.1.3 Тоон арга

А.1.1.3.1 Хуваариуд (scales)-ын хязгаар

Эрсдлийн түвшинг аливаа аргыг ашиглан, холбогдох хүчин зүйлсийг харгалзан тооцоолж болно, болзошгүй тохиолдлыг үр дагавараар үржүүлэх замаар ихэвчлэн гаргадаг. Болзошгүй тохиолдол нь өгөгдсөн хугацаанд тохиох тохиолдлын магадлал эсвэл давтамжийг илэрхийлдэг.

Энэ хугацаа нь ихэвчлэн жил бүр (жилд) эсхүл маш их (жишээ нь зуун жилд) эсвэл байгууллагын хүссэнээр бага (жишээ нь: нэг секундэд) байж болно.

Болзошгүй тохиолдолын хуваарийг байгууллагын нөхцөл байдлыг тусгасан практик үг хэллэгээр тодорхойлох ёстой бөгөөд ингэснээр эрсдэлийг удирдахад энгийн, сонирхогч бүх талууд ойлгоход хялбар байна. Энэ нь илэрхийлэгдэх болзошгүй тохиолдлын хязгаарт бодитой хязгаарлалт хийнэ гэсэн үг юм. Хэрэв хуваарийн хамгийн дээд ба доод хязгаарууд хоорондоо хэт хол байвал түүний доторх ангилал бүр нь хэт өргөн хүрээтэй болзошгүй тохиолдлыг агуулж, үнэлгээг тодорхойгүй болгоно.

ЖИШЭЭ 1: Хуваарийн хамгийн дээд хязгаар болзошгүй тохиолдлын цэгийг байгууллага тохиолдолд хариу үйлдэл үзүүлэх цаг буюу хугацааны хувьд ашигтайгаар тодорхойлдог бол, хамгийн бага эцсийн цэгийг нь ихэвчлэн байгууллагын урт хугацааны стратеги төлөвлөлтийн үргэлжлэх хугацаагаар авдаг.

Хуваарийн тодорхойлсон хязгаараас дээш ба түүнээс доош болзошгүй тохиолдлыг "хуваарийн хамгийн их утгаас их" ба “хуваарийн хамгийн бага утгаас бага” гэж илэрхийлэх ба тодорхойлсон хуваарийн хязгаараас хэтэрсэн хэсэг нь авч үзвэл зохих онцгой тохиолдлууд юм (магадгүй тусгай "хэрээс хэтэрсэн” шалгуур юм). Эдгээр хязгаараас гадуур тодорхой болзошгүй тохиолдол нь тухайн чиглэл дэх үл хамаарах зүйлээс хамаагүй бага ач холбогдолтой.

Хэрэв эрсдэлийн тайланд зөвшөөрөгдсөн бол үр дагаварыг санхүүгийн үзүүлэлтийг ашиглан хэмжих нь ашигтай байдаг, учир нь энэ нь нэгтгэх боломжийг олгоно.

ЖИШЭЭ 2: Мөнгөний үр дагаврын хуваарь нь ихэвчлэн 10 (100-аас 1000; 1000-аас 10000 гэх мэт) байна. хуваарийн ангилалын өргөнийг эдгээрээс хамааруулан сонгох

хэрэгтэй. Ангилал бүрт хамаарах хэт их эрсдэлээс зайлсхийхийн тулд болзошгүй тохиолдлын хуваарийн ангиллын өргөнийг сонгосон үр дагаврын хуваарьтай харьцуулан сонговол зохино.

ЖИШЭЭ 3: Хэрэв болзошгүй тохиолдол ба үр дагаврыг экспоненциал хуваарийн индексээр илэрхийлсэн бол (жишээ нь: хуваарийн утгуудын логарифмууд), эдгээрийг нэгтгэх хэрэгтэй.

Дараа нь эрсдлийн утгыг дараах байдлаар тооцоолж болно: antilog [log (болзошгүй тохиолдлын утга) + log(үр дагаварын утга)].

А.4 хүснэгт- Болзошгүй тохиолдлын логарифм хуваарийн жишээ

дундаж давтамж ойролцоогоор	Log илэрхийлэл	Хуваарийн утга
Цаг тутамд	(Ойролцоогоор 10^5)	5
8 цаг тутамд	(Ойролцоогоор 10^4)	4
Долоо хоногт 2 удаа	(Ойролцоогоор 10^3)	3
Сард 1 удаа	(Ойролцоогоор 10^2)	2
Жилд 1 удаа	(10^1)	1
Арван жилд 1 удаа	(10^0)	0

ЖИШЭЭ 4: А.4 хүснэгтэд өндөр давтамжийн тохиолдлын жишээ нь компьютерийн нууц үгийн тохиолдлын халдлага эсвэл ботнетээс түгээгдсэн “Үйлчилгээнээс татгалзах” халдлага юм. Довтолгооны давтамж үүнээс ч илүү өндөр байж болно.

ЖИШЭЭ 5: А.4 хүснэгтэд бага давтамжтай тохиолдлын жишээ нь галт уулын дэлбэрэлт юм. Хэдийгээр тохиолдол зуунд нэг л тохионо гэж таамаглаж байсан ч энэ нь МАБМТ-ны ашиглалтын хугацаанд тохиолдохгүй гэсэн үг биш юм.

А.5 хүснэгтэд үр дагаврын логарифм хуваарийн жишээг үзүүлэв. Давтамжийг авч үзэх зорилго нь ийм довтолгооны дараалын болзошгүй тохиолдол бага боловч өндөр давтамжийн довтолгооны дараалыг тэсвэрлэх хангалттай хүчтэй хамгаалалтын арга хэмжээгээр хангах явдал юм.

А.5 хүснэгт- Логарифм үр дагаварын хуваарийн жишээ

Үр дагавар (алдагдал)	Log илэрхийлэл	Хуваарийн утга
£1 000 000	(10^6)	6
£100 000	(10^5)	5
£10 000	(10^4)	4
£1 000	(10^3)	3
£100	(10^2)	2
£100-оос бага	(10^1)	1

Хэрэв болзошгүй тохиолдол болон үр дагаврын хуваарь хоёуланд нь түвшин оноохдоо 10 суурьтай логарифмыг ашигласан бол эрсдэлийн шинжилгээ нь эрсдэлийн ижил түвшинд хэт их эрсдэлтэй байж болзошгүй тул зохих байдлаар эрэмбэлж, аюулгүй байдлын хөрөнгө оруулалтын шийдвэр гаргах боломжгүй. Энэ тохиолдолд суурийг багасгаж, тооцсон түвшний тоог нэмэгдүүлэх нь ашигтай байна. Болзошгүй тохиолдол, үр дагавар нь өөр өөр суурьтай тохиолдолд хоёр хүчин зүйлийг нэгтгэн дүгнэх ашигтай томъёог ашиглах боломжгүйг анхаарна уу.

ЖИШЭЭ 6 Хэрэв нэг түвшнээс нөгөөд шилжих үед болзошгүй тохиолдол хоёр дахин нэмэгдэж, үр дагавар нь 10 дахин үнэтэй бол томьёо нь a) ба b) эрсдэлийг үүсгэх бөгөөд эрсдэл b) үр дагаврын түвшин 10 дахин их байх болно. Гэхдээ a) эрсдэлийн болзошгүй тохиолдолын зөвхөн тал хувь нь ижил эрсдэлийн түвшинд байна. Энэ нь эдийн засгийн хувьд буруу юм.

А.4 хүснэгт болон А.5 хүснэгтэд өөр өөр байгууллагуудын түгээмэл тохиолдлуудыг хамарсан болзошгүй тохиолдол, үр дагаврын хүрээг жагсаав. Эдгээр жишээн дэх хуваарийг бүхэлд нь төлөөлсөн эрсдэлийн хүрээтэй ямар ч байгууллага тулгарах магадлал багатай. Болзошгүй тохиолдол, үр дагаврын аль алиных нь дээд ба доод хязгаарыг бодитой тодорхойлоход байгууллагын нөхцөл байдал, МАБМТ-ны хамрах хүрээг ашиглах бөгөөд 1 000-аас 1-ээс хүртэл эрсдэлийн хүрээнд тооцоолох нь практик үнэ цэнэ хязгаарлагдмал байх магадлалтай гэдгийг санаарай.

А.1.2 Эрсдэлийг хүлээн зөвшөөрөх шалгуур

Эрсдэлийг хүлээн зөвшөөрөх шалгуур нь хүлээн зөвшөөрөх боломжгүй утгаас дээш байна.

ЖИШЭЭ 1: хэрэв А.3 хүснэгтэд “дунд зэрэг” утгыг сонгосон тохиолдолд “маш бага”, “бага” эсвэл “дунд зэрэг” утгатай бүх эрсдэлүүдийг байгууллага хүлээн зөвшөөрөх бөгөөд “өндөр” эсвэл “маш өндөр” утгатай бүх эрсдлийг хүлээн зөвшөөрөхгүй.

Байгууллага өнгөөр кодлогдсон эрсдэлийн матрицыг ашиглан үр дагавар, болзошгүй тохиолдлын хуваарийг илэрхийлснээр эрсдэлийн нэг буюу хэд хэдэн үнэлгээний эрсдэлийн тархалтыг гарфик байдлаар харж болно. Эрсдэлийн ийм матриц нь эрсдэлийг хүлээн зөвшөөрөх эсвэл арга хэмжээ шаардлагатай тухай байгууллагын эрсдэлийн хандлагыг мэдээлэхэд ашиглаж болно

ЖИШЭЭ 2: Гурван өнгө ашигласан эрсдэлийн матриц, жишээ нь, эрсдэлийн үнэлгээний гурван түвшинг илэрхийлэхийн тулд улаан, шаргал, ногоон өнгийг хэрэглэсэн.

Эрсдлийн матрицад загварын өөр өнгийг сонгох нь ашигтай байж болно.

ЖИШЭЭ 3: Хэрэв эрсдэлийн матрицыг эрсдлийн үнэлгээний анхны үр дүнг ижил эрсдэлийн дахин үнэлгээний үр дүнтэй харьцуулахдаа ашиглаж байгаа бол одоогийн эрсдэлийн түвшинд илүү олон өнгө хэрэглэвэл эрсдэлийг өөрчлөлтийг илүү хялбар харуулна.

Ийм загварт эрсдэлийн тодорхой утга бүхий эрсдэлийг хүлээн авах удирдлагын түвшний тодорхойлолтыг нэмж оруулах боломжтой.

А.6 хүснэгтэд үнэлгээний хуваарийн жишээг үзүүлэв.

А.6 хүснэгт-Эрсдэлийн матрицийг гурван өнгөөр харуулсан үнэлгээний хуваарийн жишээ

Эрсдэлийн түвшин	Эрсдэлийн үнэлгээ	Тайлбар
Бага (ногоон)	Хүлээн зөвшөөрөх боломжтой	Аливаа арга хэмжээгүйгээр эрсдэлийг шууд хүлээн зөвшөөрнө.

Дунд (шаргал)	Хяналт доор хүлцэх боломжтой	Эрсдэлийн менежментийн дагуу дунд болон урт хугацаанд тасралтгүй сайжруулах ажлын хүрээг тодорхойлж, арга хэмжээ авбал зохино.
Өндөр (улаан)	Хүлээн зөвшөөрөх боломжгүй	Эрсдэлийг бууруулах арга хэмжээг богино хугацаанд зайлшгүй авбал зохино. Аваагүй тохиолдолд үйл ажиллагааг бүхэлд нь эсвэл хэсэгчлэн зогсоовол зохино.

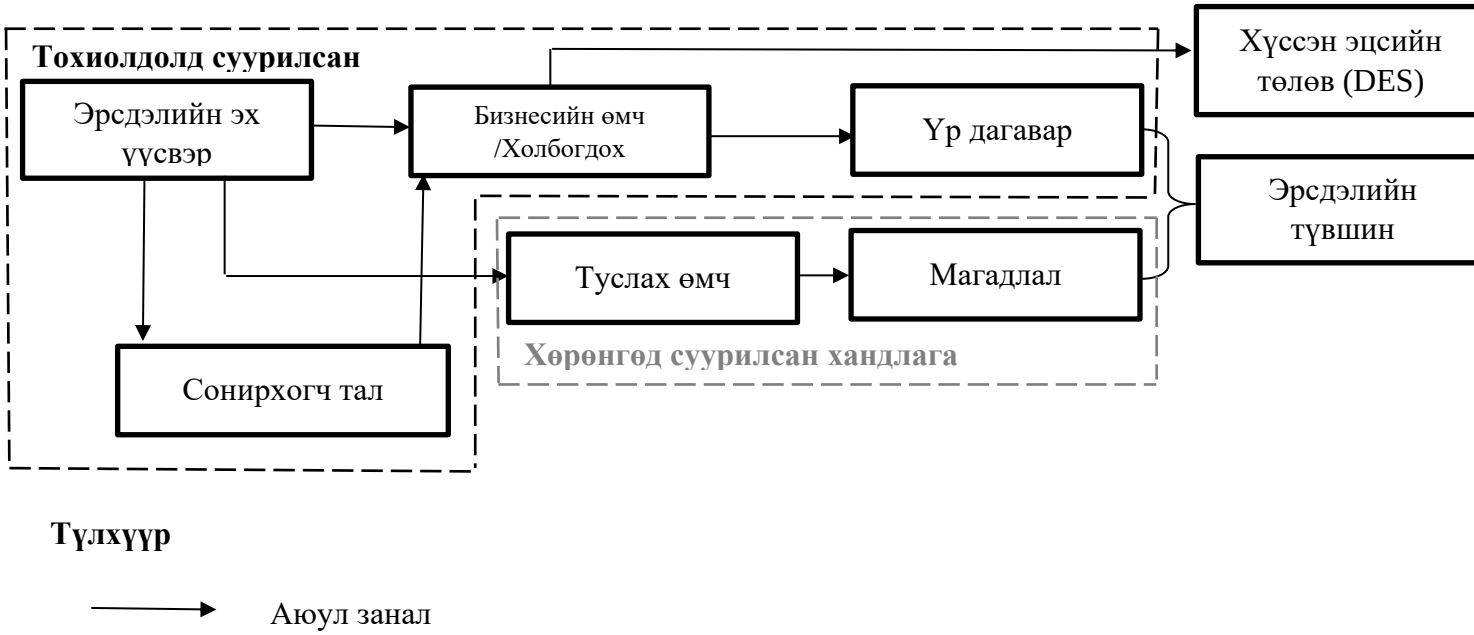
A.2 Хэрэгжүүэх арга

A.2.1 Мэдээллийн аюулгүй байдлын эрсдэлийн бүрэлдэхүүн хэсгүүд

Мэдээллийн аюулгүй байдлын эрсдлийг тодорхойлох, үнэлэхдээ дараахь бүрэлдэхүүн хэсгүүдийг анхаарвал зохино:

— өнгөрсөн хугацаанд холбоотой бүрэлдэхүүн хэсгүүд:
  — аюулгүй байдлын тохиолдол, аюултай тохиолдол (байгууллагын дотор болон гадна талд);
  — эрсдэлийн эх үүсвэр;
  — эмзэг байдалыг ашигласан байдал;
  — хэмжсэн үр дагавар;
— ирээдүйтэй холбоотой бүрэлдэхүүн хэсгүүд:
  — аюул занал;
  — эмзэг байдал;
  — үр дагавар;
  — эрсдэлийн хувилбарууд.

А.2.2-аас А.2.7- зүйлд дурдсан мэдээллийн аюулгүй байдлын эрсдлийн бүрэлдэхүүн хэсгүүдийн хоорондын хамаарлыг бөгөөд А.1 зурагт харуулсан.



А.1 зураг- Мэдээллийн аюулгүй байдлын эрсдлийн үнэлгээний бүрэлдэхүүн хэсэг

"Хүссэн эцсийн төлөв"-ийн талаарх дэлгэрэнгүй мэдээллийг А.2.3 b)-д үзнэ үү.

А.2.2 Өмч хөрөнгө

Эрсдэлийг тодорхойлохдоо өмч хөрөнгөд суурилсан аргыг ашиглахын тулд өмчийг хөрөнгийг тодорхойлно. Эрсдэлийн үнэлгээний үйл явцад эрсдэлийн хувилбаруудыг боловсруулахдаа тохиолдол, үр дагавар, аюул занал, эмзэг байдлыг өмчтэй холбоогдуулан тодорхойлно.

Эрсдэлийн арга хэмжээний үйл явцад хяналт тус бүрийг өмчийн дэд бүлэгт хэрэглэнэ.

Өмчийг хоёр ангилж болно:

— үндсэн/бизнесийн өмч хөрөнгө – байгууллагад үнэ цэнэ бүхий мэдээлэл эсхүл үйл явц

— туслах өмч - бизнесийн нэг буюу хэд хэдэн өмчид суурилсан мэдээллийн системийн бүрэлдэхүүн хэсэг.

үндсэн/бизнесийн өмч – тохиолдолд суурилсан аргад ихэвчлэн хэрэглэнэ. (бизнесийн өмч дэх тохиолдол түүний бизнест үзүүлэх үр дагаварыг тодорхойлно)

Туслах өмч-ихэвчлэн өмчид суурилсан арга (эдгээр өмчийн эмзэг байдал, аюул заналыг тодорхойлж, шинжилнэ) болон эрсдэлийн арга хэмжээ (хяналт тус бүрийг хэрэгжүүлэх өмчийг тодорхойлно)-нд хэрэглэнэ.

Бизнесийн болон туслах өмч нь хоорондоо холбоотой тул туслах өмчид тодорхойлсон эрсдэлийн эх үүсвэрүүд бизнесийн өмчид нөлөөлж болно.

Иймд өмчийн хоорондын хамаарлыг тодорхойлж, байгууллагад тэдгээрийн үнэ цэнийг ойлгох нь чухал юм. Өмчийн үнэ цэнийг буруу үнэлэх нь үр дагаврыг буруу үнэлэхэд хүргэх болох бөгөөд түүнчлэн авч авч үзэж буй болзошгүй тохиолдлын аюул заналын талаар ойлголтод нөлөөлж болно.

ЖИШЭЭ 1: Туслах өмч нь бизнесийн өмч (энэ тохиолдолд мэдээлэл)-ийг агуулж байна

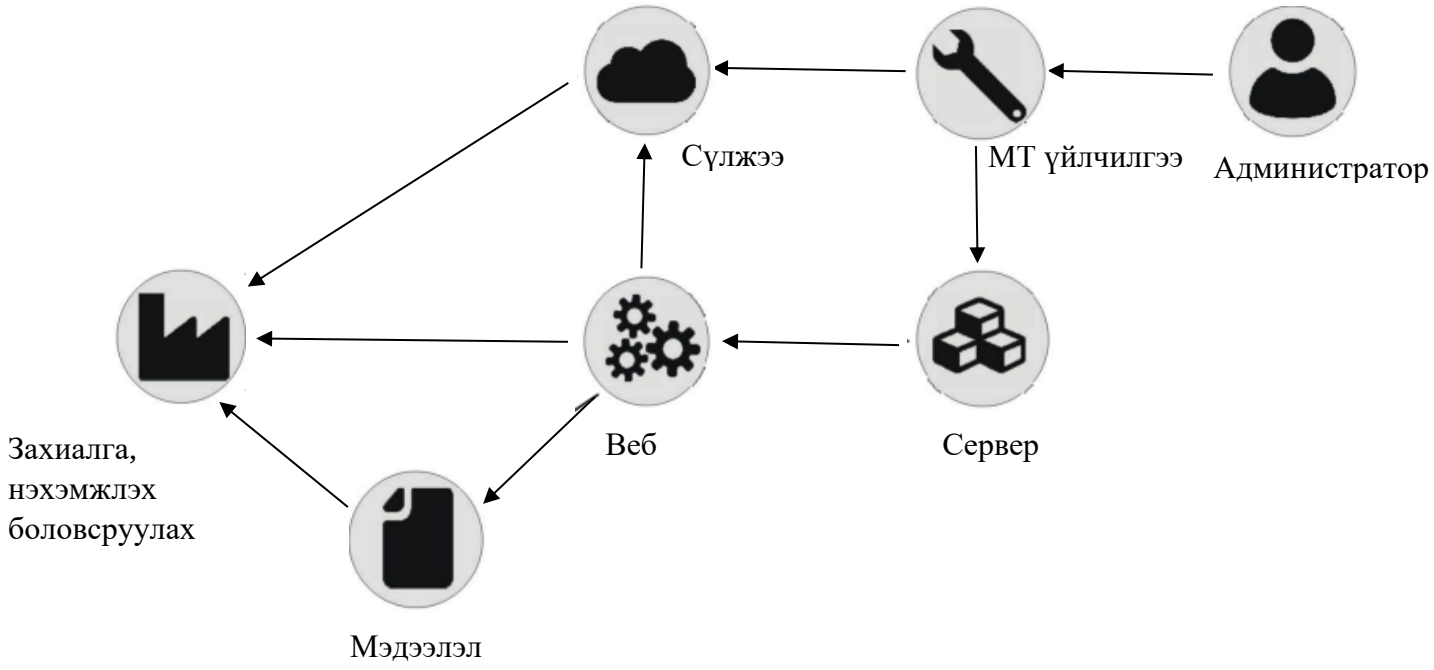
Эрсдлийн эх үүсвэр нь туслах өмчийн эмзэг байдлыг ашиглан зорилгодоо хүрэхээс урьдчилан сэргийлэхийн тулд өгөгдлийг дотоод болон гадаад хяналтаар хамгаална.

Өмчийн төрлүүдийг ялгахдаа хөрөнгийн хоорондын хамаарлыг баримтжуулж, эрсдэлийн тархалтыг үнэлж, туслах өмчид эсхүл туслах өмчид баримтжуулах естой бөгөөд ингэснээр нэг эрсдэлийг хоёр удаа үнэлэхгүй. Өмчийн хамаарлын графикууд нь ийм хамаарлыг харуулах болон бүх хамаарлыг харгалзсан эсэхийг баталгаажуулах үр ашигтай хэсрэгсэл юм.

ЖИШЭЭ 2: А.2 зураг дээрх график нь “захиалга болон нэхэмжлэх боловсруулалт”-д хамаарах бизнесийн өмчийг харуулах бөгөөд дараах байдлаар уншиж болно.

— "Администратор" (төрөл: хүний нөөц), хэрэв зохих сургалтад хамрагдаагүй бол өмчид эрсдэлийг тараана.
— “Мэдээллийн технологийн үйлчилгээ” (төрөл: үйлчилгээ), өмчид эрсдэлийг тараана.
— "Сервер" (төрөл: техник хангамж) эсвэл "Сүлжээ" (төрөл: сүлжээний холболт). Хэрэв сервер ажиллахаа зогсвол эсвэл буруу тохируулсан сүлжээ нь өмчид хөрөнгөд нөлөөлнө.
— "Вэб портал" (төрөл: програм), ажиллахаа болих эсвэл ашиглах боломжгүй болно.

"Вэб портал" байхгүй бол "захиалга, нэхэмжлэх боловсруулах" бизнесийн үйл явц нь үйлчлүүлэгчдэд үйл явцаа нийлүүлэх боломжгүй.



А.2 зураг –Хамаарах өмчийн дүрсийн жишээ

А.2.3 Эрсдлийн эх үүсвэр ба хүсч буй эцсийн төлөв

Энэ төрлийн эрсдэлийн эх үүсвэрийг дараах байдлаар тодорхойлохыг санал болгож байна. Энэхүү дүрслэх аргыг дараах хоёр үндсэн шалгуураар бүтэцлэнэ:

— сэдэл;

— үйлдэл хийх чадвар.

а) А.7 хүснэгтэд эрсдэлийн эх үүсвэрийг тодорхойлох жишээг харуулав.

А.7 хүснэгт-Халдлагын энгийн аргын жишээ

Эрсдэлийн эх үүсвэр	Халдлагын түгээмэл аргуудын жишээ
Төртэй оролцоотой	Улсууд, тагнуулын байгууллагууд Арга: Халдлагуудыг ихэвчлэн мэргэжлийн хүмүүс урьдчилан тодорхойлсон хуанлийн өдөр болон халдлагын аргын дагуу хийдэг. Энэ халдагчийн профайл нь удаан хугацаанд довтолгоо явуулах (тогтвортой нөөц, үйл явц) болон арга хэрэгслээ зорилтот топологитой нийцүүлэх чадвараар тодорхойлогдоно. Өргөтгөлөөр эдгээр субьектууд нь 0-өдрийн эмзэг байдлыг илрүүлэх, худалдан авах арга хэрэгсэлтэй бөгөөд зарим нь тусгаарлагдсан сүлжээнд нэвтэрч, бай (target)-д хүрэхийн тулд дараалсан халдлага хийх чадвартай. (жишээ нь, нийлүүлэлтийн сүлжээнд чиглэсэн халдлага) .
Зохион байгуулалттай гэмт хэрэг	Кибер гэмт хэргийн байгууллагууд (мафи, бүлэглэл, гэмт хэргийн бүлэг)

	Арга: Онлайн эсвэл биечлэн луйвар, барьцаа хүсэх эсхүл ransomware хортой кодоор халдлага хийх, бот-сүлжээ ашиглах гэх мэт. Ялангуяа онлайнаар ашиглах боломжтой халдлагын арга хэрэгсэлүүд олширч байгаатай холбогдуулан, кибер гэмт хэрэгтнүүд улам боловсронгуй, зохион байгуулалттай ажиллагаа явуулж байна. ашиг олох эсвэл залилан мэхлэх зорилготой. Зарим нь 0-өдөрийн эмзэг байдал худалдаж авах эсвэл илрүүлэх хэрэгсэлтэй байдаг.
Террорист	Кибер террористууд, кибер арми Арга: Ихэвчлэн тийм ч нарийн төвөгтэй биш боловч тогтворгүй болгох, сүйтгэх зорилгоор эцсийн байдлаар хийдэг халдлага: интернэт сайтуудын эмзэг сул талуудыг ашиглан эвдрэл учруулах, үйлчилгээ татгалзах (жишээ нь, эмнэлгийн түргэн тусламжийн үйлчилгээг боломжгүй болгох, эрчим хүчний үйлдвэрлэлийн үйлдвэрлэлийн системийг гэнэт зогсоох),
Үзэл суртлын идэвхтэн	Кибер хакерчид, сонирхлын бүлгүүд, сектүүд Арга: Довтолгооны арга, нарийн төвөгтэй байдал нь кибер террористуудынхтай харьцангуй төстэй бөгөөд зорилго нь хор хөнөөл багатай сэдлээс бий болдог. Зарим субьектууд үзэл суртал, мэдээг түгээхийн тулд эдгээр халдлагуудыг хийдэг (жишээлбэл, нийгмийн сүлжээг өргөн хүрээнд дуу хоолой болгон ашиглах).
Сонирхогч	Хакерийн профил нь script-kiddies буюу эсвэл мэдээллийн технологийн талаар сайн мэдлэгтэй хүн; нийгэмд хүлээн зөвшөөрөгдөх, хөгжилтэй, өөрийгөө сорих сэдлээс үүдэлтэй. Арга: онлайнаар ашиглах боломжтой довтолгооны арга хэрэгслийг ашигласан энгийн халдлага
Өшөө авагч	Энэхүү халдагчийн профайлын сэдэл нь хурц өс хонзон эсвэл шударга бус байдлын мэдрэмжээс үүсдэг. (жишээ нь, ноцтой буруугийн улмаас ажлаас халагдсан ажилтан, гэрээ шинэчлэгдээгүй улмаас сэтгэл хангалуун бус үйлчилгээ үзүүлэгч гэх мэт). Арга: Энэхүү халдагчийн профайл нь шийдэмгий байдал, систем, байгууллагын үйл явцын талаарх мэдлэгээр нь тодорхойлогддог. Энэ нь түүнийг аюултай болгож, хор хөнөөл учруулах асар их хүчийг бий болгоно.
Хэвийн бус (pathological) халдагч	Энэхүү халдагчийн профайлын сэдэл нь хэвийн бус эсвэл түрэмгий шинжтэй зарим үед ашиг олох сэдэлээс бий болдог. (шударга бус өрсөлдөгч, шударга бус үйлчлүүлэгч, луйварчин). Арга: Энэ төрлийн халдагчид компьютерийн суурь мэдлэгтэй бөгөөд энэ нь тэднийг халдлагын байны мэдээллийн системийг эвдэх оролдлого хийхэд хүргэдэг, эсвэл тэд онлайнаар ашиглах боломжтой халдлагын арга хэрэгслийг ашигладаг, эсвэл тусгай зориулалтын туслан гүйцэтгэгчийг оролцуулан халдлагыг хийлгэдэг. Зарим тохиолдолд халдагчид анхаарлыг дотоод эх сурвалж руу (сэтгэл ханамжгүй ажилтан, шударга бус үйлчилгээ үйлчилгээ үзүүлэгч) чиглүүлж эвдэх оролдлого хийнэ.

б) Эрсдэлийн эх үүсвэрийн сэдэл - хүссэн эцсийн төлөвийг загварчлах

Маш өргөн хүрээний сэдэл байдаг; үүнд улс төр, санхүү, үзэл суртлын шинжтэй түүнчлэн нийгмийн шинж чанартай эсвэл нэг удаагийн хэвийн бус эсвэл сэтгэлзүйн байдлыг илэрхийлж болно.

Энэ нь сэдлийг шууд илэрхийлэх боломжгүй ч эрсдэлийн эх үүсвэрийн зорилгоор дүрсэлж, хүссэн эцсийн төлөв (DES) буюу Эрсдэлийн эх үүсвэр халдлагын дараа хүсч буй ерөнхий нөхцөлийн хэлбэрээр илэрхийлж болно. Үйл ажиллагааны ерөнхий ангиллын нөхцөл байдлыг системчилж ангилах нь нөхцөл байдлын шинжилгээнд чиглэгдэж болно.

А.8 хүснэгт DES-ийг илэрхийлэх сэдлүүдийн ангиллыг жишээгээр үзүүлэв.

А.8 хүснэгт- DES-ийг илэрхийлэх сэдлүүдийн ангиллын жишээ

Эзлэн түрэмгийлэх	Нөөц ба эдийн засгийн зах зээлийг урт хугацаанд эзлэн авах, улс төрийн эрх мэдлийг олж авах эсвэл үнэт зүйлийг эзэмших
Авах	Нөөц, үр ашигийг булаан авахад чиглэсэн шийдэмгий довтлох, араатан арга
Урьдчилан сэргийлэх	Гуравдагч этгээдийн үйлдлийг хязгаарлах довтолгооны хандлага
Хадгалах	Үзэл суртал, улс төр, эдийн засаг, нийгмийн байдлыг хадгалах хүчин чармайлт
Хамгаалах	Тодорхой өрсөлдөгчийнхөө түрэмгийллээс урьдчилан сэргийлэх эсвэл тэдний үйлдлийг удаашруулах замаар үйлдлээс нь урьдчилан сэргийлэхийн тулд хатуу хамгаалалт хийх, эсвэл илт заналхийлэх арга (жишээ нь, айлган сүрдүүлэх) хэрэглэх.
Даван туулах	Байг ямар ч үнээр хамаагүй хамгаалах, энэ нь хэт түрэмгий үйлдэл хийхэд хүргэдэг

в) Зорилтот бай

DES-д хүрэхийн тулд эрсдлийн эх үүсвэр нь зорилтот системийн бизнесийн өмч хөрөнгөд нөлөөлөх нэг буюу хэд хэдэн обьектод чиглэдэг. Эдгээр нь эрсдэлийн эх үүсвэрийн зорилтот бай юм.

А.9 хүснэгтэд зорилтот байнуудын жишээг үзүүлэв.

А.9 хүснэгт-Зорилтот байнуудын жишээ

Зорилтот бай	Тайлбар
Тагнах (spying)	Тагнуулын ажиллагаа (төртэй холбоотой, эдийн засгийн). Ихэнх тохиолдолд халдагчид мэдээллийн системд удаан хугацаагаар, бүрэн нууцлалтайгаар суулгахыг зорьдог. Зэвсэглэл, сансар огторгуй,агаарын хөлөг, эм үйлдвэрлэл, эрчим хүч болон төрийн зарим үйл ажиллагаа (эдийн засаг, санхүү, гадаад харилцаа) нь тэргүүлэх байнууд байна.
Стратегийн урьдчилан байршуулах	Урьдчилан байршуулах нь эцсийн зорилго нь тодорхойгүй, урт хугацааны халдлагад чиглэгддэг (жишээ нь, харилцаа холбооны операторын сүлжээг эвдэх, улс төр, эдийн засгийн

	хүчтэй нөлөө бүхий үйл ажиллагааг эхлүүлэхийн тулд олон нийтийн мэдээллийн интернет сайтуудад нэвтрэн орох гэх мэт). Ботнет үүсгэх зорилгоор компьютеруудыг гэнэт, асар их хэмжээгээр эвдэх нь энэ ангилалд хамаарч болно.
Нөлөөлөх	Хуурамч мэдээлэл тараах, өөрчлөх, нийгмийн сүлжээн дэх үзэл бодлын удирдагчдыг татан оролцуулах, нэр хүндийг унагах, нууц мэдээллийг задруулах, байгууллага, улсын нэр хүндийг гутаан доромжлох зорилготой ажиллагаа. Эцсийн зорилго нь ойлголтыг тогтворгүй болгох эсвэл өөрчлөх явдал байдаг.
Үйл ажиллагаанд саад учруулах	Жишээ нь, мэдээлэл цуглуулах, цахим нөөцийг ашиглах, физик суурилуулалтыг хийх боломжгүй болгохын тулд интернет сайтыг ашиглах боломжгүй болгох зорилго бүхий хорлон сүйтгэх ажиллагаа. Ялангуяа, үйлдвэрлэлийн системүүд нь хоорондоо холбогдсон мэдээллийн сүлжээнүүдээр дамжуулан өртөх, эмзэг байдалтай байдаг. (жишээ нь: техник хангамжид гэмтэл учруулах эсвэл их хэмжээний засвар үйлчилгээ шаардах эвдрэл үүсгэхийн тулд команд илгээх) . Distributed Deial-of-Service бую (DDoS) халдлага нь цахим нөөцийг саармагжуулахад түгээмэл хэрэглэгддэг арга юм.
Ашиг олох	Шууд болон шууд бусаар санхүүгийн ашиг олох зорилготой үйл ажиллагаа. Ихэвчлэн зохион байгуулалттай гэмт хэрэгтэй холбоотой, интернетээр залилан мэхлэх, мөнгө угаах, завших, шамшигдуулах, санхүүгийн зах зээлийг залилан мэхлэх, захиргааны бичиг баримтыг хуурамчаар үйлдэх, таних таних баримт бичгийг хулгайлах гэх мэтийг дурдаж болно. Ашгийн төлөөх зарим үйл ажиллагаа нь дээр дурдсан халдлагын ангиллын аль нэг аргыг (жишээ нь тагнах, мэдээлэл хулгайлах, үйл ажиллагааг саармагжуулах зорилгоор ransomware хортой код гэх мэт) ашиглаж болох бөгөөд эцсийн зорилго нь санхүүд чиглэсэн хэвээр байна.
Сорих, хөгжилтэй байх	Нийгэмд танигдах, туршилт хийх эсвэл зугаацах зорилгоор давуу талаа ашиглах үйл ажиллагаа. Хэдийгээр ихэвчлэн зугаацах, ямар нэгэн хор хөнөөл учруулах зорилгогүй ч ийм төрлийн ажиллагаа нь хохирогч талд ноцтой үр дагаварт хүргэж болзошгүй.

DES болон зорилтот байны хоорондын ялгааг DES-ийг ялахын тулд өрсөлдөгчийнхөө гэрээний нууц мэдээллийг хулгайлах (стратегийн зорилго) эрсдэлийн эх үүсвэрийн жишээгээр ыг дүрсэлж болно. Зарим тохиолдолд тухайн бай (хүссэн мэдээлэл) нь DES-ийн эцсийн үр дүнд хүргэдэггүй.

Эрсдэлийн эх үүсвэрийн үүднээс авч үзвэл байны үнэ цэнэ нь түүний DES-д оруулах хувь нэмэрт үндэслэнэ гэж үзэж болно.

Эрсдэлийн эх үүсвэрийн байг хоёр том бүлэгт ерөнхийд нь хуваана:

— байны нөөцийг өөрийн ашиг тусын тулд ашиглах, жишээлбэл. тагнуул, хулгай, луйвар, луйвар, наймаа;

— байг нөөцөө ашиглахаас урьдчилан сэргийлэх (сөргөлдөөн нь үргэлж харьцангуй байдаг), жишээ нь: дайн, терроризм, хорлон сүйтгэх, тогтворгүй байдал бий болгох.

A.2.4 Тохиолдолд суурилсан арга

A.2.4.1 Экосистем

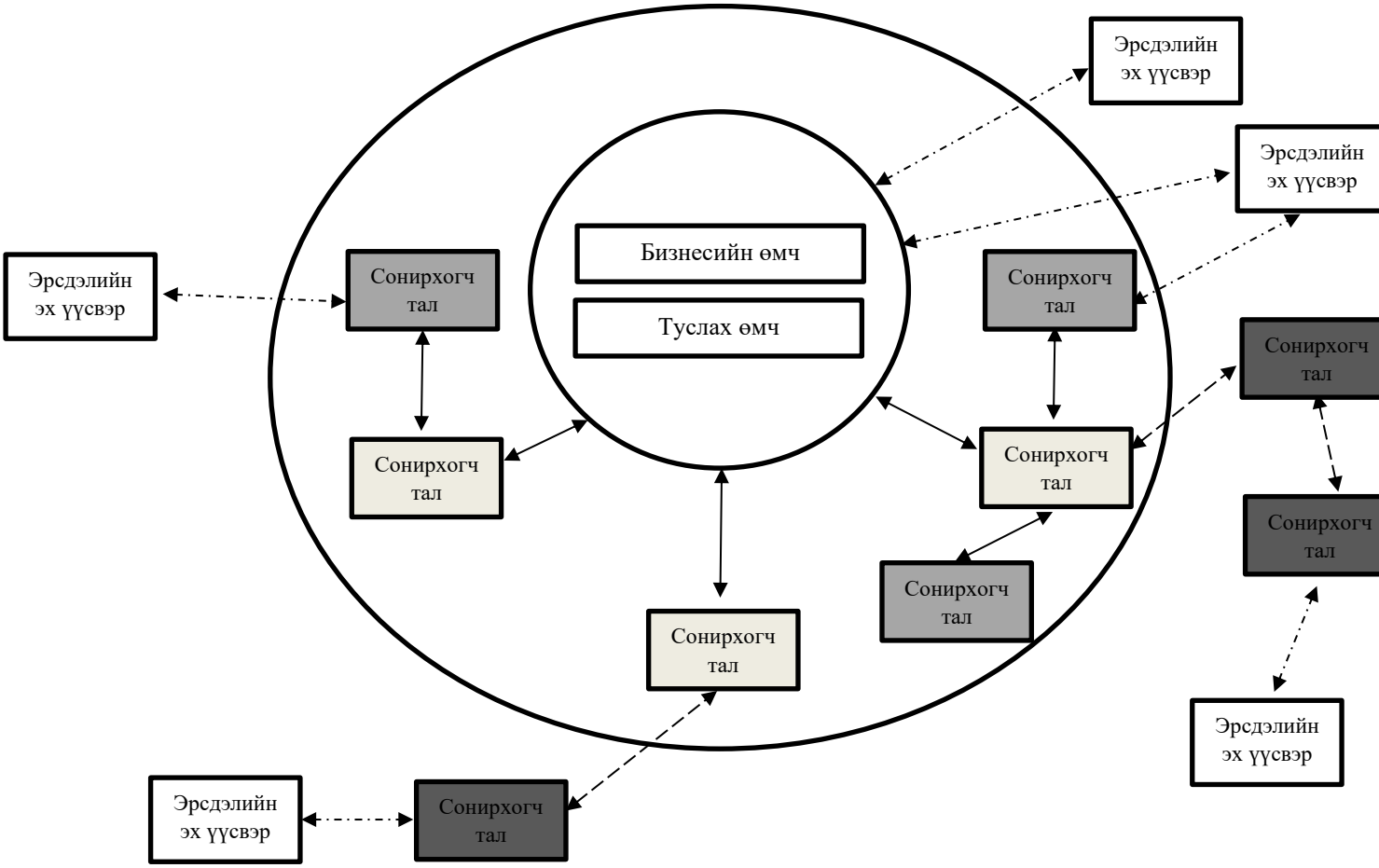
Тохиолдолд суурилсан арга нь байгууллага болон сонирхогч талуудын хоорондын харилцан үйлчлэлийн өөр өөр зам буюу эх үүсвэр бизнесийн өмч хөрөнгө болон тэдгээрийн DES-д хүрэхэд ашиглах бүх экосистемийг шинжлэх замаар хувилбаруудыг бий болгоно.

Зорилгодоо хүрэхийн тулд экосистемийн хамгийн эмзэг холбоосуудыг ашигладаг халдлагын аргууд улам бүр нэмэгдсээр байна.

МАБМТ-ны хүрээнд эрсдэлийн хувилбаруудын шинжилгээнд анхаарвал зохих сонирхогч талууд хоёр төрөл байж болно:

— гадны талууд, үүнд:
  — үйлчлүүлэгчид;
  — түншүүд, хамтран гүйцэтгэгчид;
  — үйлчилгээ үзүүлэгчид (туслан гүйцэтгэгчид, ханган нийлүүлэгчид).
— дотоод талууд, үүнд:
  — техникийн үйлчилгээ үзүүлэгчид (жишээ нь, МТ-ийн удирдлагын санал болгосон дэмжих үйлчилгээ үзүүлэгч);
  — бизнестэй холбоотой үйлчилгээ үзүүлэгчид (жишээ нь, бизнесийн мэдээллийг ашигладаг арилжааны байгууллага);
  — салбар компаниуд (тухайлбал, өөр улс оронд байрладаг).

Сонирхсон талуудыг тодорхойлох зорилго нь экосистемийн талаар тодорхой ойлголттой болж, хамгийн эмзэг бүлгийг тодорхойлох явдал юм. Экосистемийн талаарх мэдлэг ойлголтыг эрсдэлийн урьдчилсан судалгаанд чиглэвэл зохино. А.3 зурагт экосистемийн сонирхогч талуудын тодорхойлолтыг харуулав.



Түлхүүр

Экосистем доторх хамаарал

Экосистемийн зааг хоорондын хамаарал

Эрсдэлийн эх үүсвэр доторх хамаарал

Системд шууд холбогдсон дотоод/гадаад сонирхогч тал

Өөр сонирхогч талтай холбоотой сонирхогч тал

Экосистемийн хүрээнээс гаднах аж ахуйн нэгж

А.3 зураг — Экосистемийн сонирхогч талуудын тодорхойлолт

А.2.4.2 Стратегийн хувилбарууд

Эрсдлийн эх үүсвэр болон холбогдох тохиолдлуудын талаар мэдээлэлд үндэслэн, эрсдэлийн эх үүсвэр өөрийн DES-д хүрэхийн тулд ямар замаар явж болохыг харуулсан өндөр түвшний бодит хувилбарууд (стратегийн хувилбарууд)-ыг төсөөлж болно.

Жишээ нь, экосистемээр дамжих эсвэл бизнесийн зарим үйл явцыг өөрчилж болно. Эдгээр хувилбаруудыг эрсдэлийн эх үүсвэр болон DES-ээс эхлэн тухай бүрт нь эрсдэлийн эх үүсвэрийн талаас нь дараах асуултуудыг тавих замаар тодорхойлж болно:

— Эрсдлийн эх үүсвэрүүд өөрсдийн DES хүрэхийн тулд байгууллагын бизнесийн ямар өмч хөрөнгөд чиглэх вэ?
— Тэд халдлагаа боломжтой болгох эсвэл хөнгөвчлөхийн тулд бизнесийн өмч хөрөнгөд давуу эрх бүхий экосистемд шүүмжтэй ханддаг сонирхогч сонирхогч тал руу довтлох магадлалтай юу?

Хамгийн их өртөж буй элементүүдийг тодорхойлсны дараа эрсдэлийн эх үүсвэрээс DES-д хүрэхийн тулд үүсэх тохиолдлуудын дараалыг тайлбарлах замаар стратегийн хувилбарыг гаргаж, дүрслэх боломжтой. Бизнесийн өмч хөрөнгийг зөрчих нь эцсийн тохиолдолд хамаардаг бол экосистемтэй холбоотой тохиолдол нь завсрын тохиолдол юм. Стратегийн хувилбар нь холбогдох тохиолдлуудын шууд нөлөөлсөн үр дагаврын үнэлгээг илэрхийнэ.

Эдгээр хувилбаруудыг халдлагын дүрс хэлбэрээр эсвэл мэдээллийн системийн зураглалын экосистемийн зураг дээр шууд халдлагын зам(ууд)-ыг давхарлан дүрсэлж болно.

Стратегийн хувилбарууд нь тохиодлын болзошгүй тохиолдлыг нэмж, авч үзэхийг шаардана. Өмч хөрөнгөд дээр суурилсан арга болон холбогдох үйл ажиллагааны хувилбаруудыг тохиодлын болзошгүй тохиолдлыг тодорхойлоход ашиглаж болно. А.2.5.1-д дурдсан аюул заналын жишээг зайлшгүй шаардлагатай үнэлгээг бий болгохын тулд ашиглаж болно.

А.2.5 Өмч хөрөнгө суурилсан арга

А.2.5.1 Аюул заналын жишээ

А.10 хүснэгтэд аюул заналын түгээмэл жишээг үзүүлэв. Жагсаалтыг аюул заналын үнэлгээний үйл явцад ашиглаж болно.

Эрсдлийн эх үүсвэр гэж үзэж буй аюул занал нь санаатай, санамсаргүй эсвэл хүрээлэн буй орчны (байгалийн) байж болох бөгөөд жишээ нь, үндсэн үйлчилгээг гэмтээх, зогсоход хүргэж болно. Жагсаалт нь аюулын төрөл тус бүрд D (санаатай), A (санамсаргүй), E (байгалийн) хамааралтай гэдгийг илэрхийлнэ. D нь мэдээлэлтэй холбоотой мэдээлэл, өмч хөрөнгөд хамаарах бүх төлөвлөсөн үйлдлүүдэд, A нь мэдээлэл, өмч хөрөнгийг санамсаргүйгээр гэмтээж болзошгүй хүний бүх үйлдлүүдэд, E нь хүний үйлдлээс шалтгаалаагүй бүх аюултай тохиолдлуудад ашиглагдана. Аюул заналын бүлгүүдийг эрэмбэлж жагсаагаагүй болно.

Хяналтууд нь аюул занал үйлдэгдэх, үүсэхээс урьдчилан сэргийлэх замаар аюулыг бууруулна. Эрсдэлийг бууруулахын тулд хяналтыг сонгохдоо тохиолдлыг тодорхойлох, хариу үйлдэл үзүүлэх, агуулах (contain), сэргээх чадвартай илрүүлэх, хариу үйлдэл үзүүлэх хяналтыг авч үзвэл зохино. Илрүүлэх, хариу үйлдэл үзүүлэх хяналтууд нь аюул заналд, үр дагавартай хамаарна.

ЖИШЭЭ: Бүртгүүлэх, ажиглах нь аюулгүй байдлын тохиолдлыг тодорхойлох, хариу үйлдэл үзүүлэх боломжийг олгодог.

А.10 хүснэгт – Аюул заналын түгээмэл жишээ

Ангилал	Дугаар	Аюул заналын тайлбар	Эрсдэлийн эх үүсвэрийн төрөл[1]
Физик аюул занал	TP01	Гал	A,D,E
	TP02	Ус	A,D,E
	TP03	Бохирдол, хортой радиаци	A,D,E
	TP04	Том осол	A,D,E
	TP05	Дэлбэрнлт	A,D,E
	TP06	Тоос, коррози, хөлдөлт	A,D,E
Байгалын аюул занал	TN01	Уур амьсгалын үзэгдэл	E
	TN02	Газар хөдлөлтийн үзэгдэл	E
	TN03	Галт уулын үзэгдэл	E
	TN04	Цаг уурын үзэгдэл	E
	TN05	Үер	E
	TN06	Цар тахал/халдварын үзэгдэл	E
Дэд бүтцийн эвдрэл	TI01	Нийлүүлэлтийн системийн эвдрэл	A,D
	TI02	Хөргөлт эсвэл агааржуулалтын системийн эвдрэл	A,D
	TI03	Эрчим хүчний хангамжийн тасалдал	A,D,E
	TI04	Харилцаа холбооны сүлжээний гэмтэл	A,D,E
	TI05	Харилцаа холбооны тоног төхөөрөмжийн гэмтэл	A,D
	TI06	Цахилгаан соронзон радиаци	A,D,E
	TI07	Дулааны радиаци	A,D,E
	TI08	Цахилгаан соронзон импульс	A,D,E
Техникийн гэмтэл	TT01	Төхөөрөмж эсвэл системийн гэмтэл	A
	TT02	Мэдээллийн системийн ханасан байдал	A,D
	TT03	Мэдээллийн системийн засвар авах байдал алдагдах	A,D
Хүний үйлдэл	TH01	Террорист халдлага, хорлон сүйтгэх ажиллагаа	D
	TH02	Нийгмийн инженерчлэл	D
	TH03	Төхөөрөмжийн цацралгалтыг барих	D
	TH04	Зайнаас тагнах	D
	TH05	Чагнах	D
	TH06	Зөөгч эсвэл бичиг баримт хулгайлах	D
	TH07	Төхөөрөмж хулгайлах	D

[1] D=(deliberate буюу санаатай); A=(accidental буюу санамсаргүй); E=(environmental буюу байгалийн);

	TH08	Цахим үнэмлэх, итгэмжлэл хулгайлах	D
	TH09	Дахин боловсруулсан эсвэл хаягдсан зөөвөрлөгчийг олж авах	D
	TH10	Мэдээллийг задруулах	A,D
	TH11	Найдваргүй эх сурвалжаас өгөгдөл оруулах	A,D
	TH12	Техник хангамжид хөндлөнгөөс оролцох	D
	TH13	Програм хангамжид хөндлөнгөөс оролцох	A,D
	TH14	Вэбд суурилсан харилцаа холбоог ашиглан Drive-by-exploits	D
	TH15	Халдлага дахин давтагдах, man-in-the-middle халдлага	D
	TH16	Хувийн мэдээллийг зөвшөөрөлгүй боловсруулах	A,D
	TH17	Байгууламжид зөвшөөрөлгүй нэвтрэх	D
	TH18	Төхөөрөмжийг зөвшөөрөлгүй ашиглах	D
	TH19	Төхөөрөмжийн буруу ашиглах	A,D
	TH20	Төхөөрөмж эсвэл зөөвөрлөгчийг гэмтээх	A,D
	TH21	Програм хангамжийг хуурамчаар хуулах	D
	TH22	Хуурамч эсвэл хуулбарласан програм хангамж ашиглах	A,D
	TH23	Өгөгдөл гэмтэх	D
	TH24	Мэдээллийг хууль бусаар боловсруулах	D
	TH25	Хортой кодыг илгээх эсвэл түгээх	A,D,R
	TH26	Байрлал илрүүлэх	D
Үйл ажиллагаа эсвэл үйлчилгээ алдагдах	TC01	Ашиглалтын алдаа	A
	TC02	Эрх эсвэл зөвшөөрлийг урвуулан ашиглах	A,D
	TC03	Эрх буюу зөвшөөрлийг хуурамчаар үйлдэх	D
	TC04	Үйлдэл татгалзах	D
Зохион байгуулалтын аюул занал	TO01	Боловсон хүчний дутагдал	A,E
	TO02	Нөөцийн хомсдол	A,E
	TO03	Үйлчилгээ үзүүлэгчдийн алдаа	A,E
	TO04	Хууль тогтоомж, дүрэм журмыг зөрчих	A,D

А.2.5.2 Эмзэг байдлын жишээнүүд

А.11 хүснэгтэд аюулгүй байдлын өөр өөр бүс дэх эмзэг байдлын жишээнүүд болон эдгээр эмзэг байдлыг ашиглаж болох аюул заналыг үзүүлэв. Уг жагсаалт нь аюул занал, эмзэг байдлыг үнэлэх явцад холбогдох эрсдэлийн хувилбаруудыг тодорхойлоход тусална. Зарим тохиолдолд бусад аюул занал нь эдгээр эмзэг байдлыг ашиглаж болно.

А.11 хүснэгт-Эмзэг байдлын жишээнүүд

Ангилал	Дугаар	Эмзэг байдлын жишээнүүд
Техник хангамж	VH01	Хадгалах төхөөрөмжийн засвар үйлчилгээ хангалтгүй/алдаатай суурилуулалт
	VH02	Тоног төхөөрөмжийг солих төлөвлөгөөт хуваарь хангалтгүй
	VH03	Чийгшил, тоос, шороонд өртөмтгий
	VH04	Цахилгаан соронзон цацрагт мэдрэмтгий
	VH05	Тохиргооны өөрчлөлтийн хяналт хангалтгүй
	VH06	Хүчдэлийн өөрчлөлтөд мэдрэмтгий
	VH07	Температурын өөрчлөлтөд мэдрэмтгий
	VH08	Хамгаалалтгүй хадгалалт
	VH09	Устгалыг хянахгүй байх
	VH10	Хяналтгүй хуулбарлах
Програм хангамж	VS01	Програм хангамжийн туршилт байхгүй эсвэл хангалтгүй
	VS02	Програм хангамжийн сайтар мэддэг цоорхой
	VS03	Ажлын төхөөхөмжийг орхихдоо “Logout” хийдэггүй
	VS04	Зохих ёсоор мэдээллийг арилгаагүй хадгалах зөөвөрлөгчийг устгах эсвэл дахин ашиглахыг хориглоогүй
	VS05	Аудитын мөрөөр “log”-уудын тохиргоо хангалтгүй.
	VS06	Хандалтын эрхийг буруу хуваарилсан
	VS07	Өргөн тархсан програм хангамж
	VS08	Хэрэглээний программуудыг цаг хугацааны хувьд буруу өгөгдөлд хэрэглэх
	VS09	Хэрэглэгчийн интерфейсийн төвөгтэй байдал
	VS10	Баримт бичиг хангалтгүй эсвэл дутмаг
	VS11	Параметрийг буруу тохируулсан
	VS12	Огноо буруу
	VS13	Таних, баталгаажуулах механизм хангалтгүй (жишээ нь хэрэглэгчийн баталгаажуулалт гэх мэт)
	VS14	Хамгаалалтгүй нууц үгийн хүснэгтүүд
	VS15	Нууц үгийн менежмент муу
	VS16	Шаардлагагүй үйлчилгээг идэвхжүүлсэн
	VS17	Боловсроогүй эсвэл шинэ програм хангамж
	VS18	Хөгжүүлэгчдийн хувьд тодорхойгүй эсвэл бүрэн бус техникийн үзүүлэлтүүд
	VS19	Үр дүнгүй өөрчлөлтийн хяналт
	VS20	Програм хангамжийг хяналтгүй татаж авах, ашиглах
	VS21	Нөөц хуулбар (back up) байхгүй эсвэл бүрэн бус
	VS22	Удирдлагын тайлан гаргахгүй байх
Сүлжээ	VN01	Мессеж илгээх эсвэл хүлээн авахыг баталгаажуулах механизм хангалтгүй
	VN02	Хамгаалалтгүй холбооны шугамууд
	VN03	Хамгаалалтгүй мэдрэмтгий урсгал
	VN04	Холболтын кабель муу
	VN05	Бүтэлгүйтлийн нэг цэг

	VN06	Илгээгч, хүлээн авагчийг таних, баталгаажуулах механизм үр дүнгүй эсвэл дутмаг
	VN07	Аюулгүй бус сүлжээний архитектур
	VN08	Нууц үгүүдийг ил шилжүүлэх
	VN09	Сүлжээний менежмент хангалтгүй (чиглүүлэлтийн уян хатан байдал)
	VN10	Хамгаалалтгүй нийтийн сүлжээний холболтууд
Ажилтан	VP01	Боловсон хүчний хомсдол
	VP02	Ажилд авах журам хангалтгүй
	VP03	Аюулгүй байдлын сургалт хангалтгүй
	VP04	Програм хангамж, техник хангамжийн буруу хэрэглээ
	VP05	Аюулгүй байдлын талаарх мэдлэг ойлголт муу
	VP06	Хяналтын механизм хангалтгүй эсвэл дутмаг
	VP07	Гадны болон цэвэрлэгээний ажилтнуудыг хяналтгүй ажиллуулах
	VP08	Харилцаа холбооны хэрэгсэл, мессежийг зөв ашиглах бодлого үр дүнгүй эсвэл дутмаг
Байгууламж	VS01	Барилга, өрөөнд нэвтрэх физик хяналтыг хангалтгүй эсвэл хайхрамжгүй ашиглах
	VS02	Үерт өртөмтгий бүсэд байрлах
	VS03	Цахилгаан сүлжээ тогтворгүй
	VS04	Барилга, хаалга, цонхны биет хамгаалалт хангалтгүй
Байгууллага	VO01	Хэрэглэгчийг бүртгэх, бүртгэлээс хасах албан ёсны журам боловсруулагдаагүй эсвэл хэрэгжилт нь үр ашиггүй
	VO02	Хандалтын эрхийг хянах албан ёсны үйл явц (хяналт) боловсруулагдаагүй эсвэл хэрэгжилт нь үр дүнгүй
	VO03	Үйлчлүүлэгчид болон/эсвэл гуравдагч этгээдтэй байгуулсан гэрээнд (аюулгүй байдлын тухай) заалт хангалтгүй
	VO04	Мэдээлэл боловсруулах байгууламжид хяналт тавих журам боловсруулаагүй, эсхүл түүний хэрэгжилт үр дүнгүй
	VO05	Аудит (хяналт) тогтмол хийгдээгүй
	VO06	Эрсдэлийг тодорхойлох, үнэлэх журам боловсруулагдаагүй, эсвэл хэрэгжилт нь үр дүнгүй
	VO07	Администратор болон операторын “log”-ийн бүртгэлд бүртгэгдсэн алдааны тайлан хангалтгүй эсвэл дутмаг
	VO08	Үйлчилгээний засвар үйлчилгээний хариу арга хэмжээ хангалтгүй
	VO09	Үйлчилгээний түвшний гэрээ хангалтгүй эсвэл байхгүй
	VO10	Өөрчлөлтийн хяналтын журам боловсруулагдаагүй, эсвэл хэрэгжилт нь үр дүнгүй
	VO11	МАБМТ-ны баримт бичгийн хяналтын албан ёсны журам боловсруулагдаагүй эсвэл хэрэгжилт нь үр дүнгүй байна

	VO12	МАБМТ-ны бүртгэлийн хяналтын албан ёсны журам боловсруулагдаагүй эсвэл хэрэгжилт нь үр дүнгүй байна
	VO13	Таних, баталгаажуулах механизм хангалтгүй (жишээ нь, хэрэглэгчийн баталгаажуулалт гэх мэт)
	VO14	Мэдээллийн аюулгүй байдлын үүрэг хариуцлагыг буруу хуваарилсан
	VO15	Тасралтгүй байдлын төлөвлөгөө байхгүй, эсвэл бүрэн бус эсвэл хуучирсан
	VO16	Цахим шууданг хэрэглэх бодлого боловсруулагдаагүй эсвэл хэрэгжилт нь үр дүнгүй байна
	VO17	Үйлдлийн системд програм хангамжийг нэвтрүүлэх журам боловсруулагдаагүй, эсвэл тэдгээрийн хэрэгжилт үр дүнгүй
	VO18	Нууц мэдээлэлтэй харьцах журам боловсруулагдаагүй, эсвэл тэдгээрийн хэрэгжилт үр дүнгүй
	VO19	Ажлын байрны тодорхойлолтод мэдээллийн аюулгүй байдлын хариуцлагыг заагаагүй
	VO20	Ажилчидтай байгуулсан гэрээнд (мэдээллийн аюулгүй байдлын талаархи) заалт хангалтгүй эсвэл дутмаг
	VO21	Мэдээллийн аюулгүй байдлын аюултай тохиолдлын үеийн сахилгын үйл ажиллагаа тодорхойлогдоогүй, эсвэл зохих ёсоор ажиллахгүй
	VO22	Зөөврийн компьютер хэрэглэх талаар албан ёсны бодлого боловсруулагдаагүй эсвэл хэрэгжилт нь үр дүнгүй
	VO23	Байгууламжаас гадуурх хөрөнгийн хяналт хангалтгүй
	VO24	“Цэвэр ширээ, цэвэр дэлгэц” бодлого хангалтгүй эсвэл дутмаг
	VO25	Мэдээлэл боловсруулах төхөөрөмжийн эрхжүүлэлт (authorization) хэрэгжээгүй эсвэл зохих ёсоор ажиллахгүй
	VO26	Аюулгүй байдлын зөрчлийн мониторингийн механизмыг зохих ёсоор хэрэгжүүлээгүй
	VO27	Аюулгүй байдлын сул талуудын талаар мэдээлэх журам боловсруулагдаагүй эсвэл хэрэгжилт нь үр дүнгүй
	VO28	Оюуны эрхийн заалтуудад нийцэх тухай журам боловсруулагдаагүй, эсвэл хэрэгжилт нь үр дүнгүй

А.2.5.3 Техникийн эмзэг байдлыг үнэлэх аргууд

Мэдээлэл, харилцаа холбооны технологийн систем болон боломжит нөөцүүд (жишээ нь, байршуулсан санхүүжилт, боломжит технологи, туршилт хийх туршлага бүхий ажилтан)-ийн хэрэгцээнээс хамаарч, эмзэг байдлыг тодорхойлоход мэдээллийн системийн туршилт зэрэг идэвхитэй аргыг ашиглаж болно.

Туршилтын аргууд нь дараахь зүйлийг агуулна:

— эмзэг байдлыг сканнердах автомат хэрэгсэл;
— аюулгүй байдлын туршилт, үнэлгээ;
— шургалаа шалгах2 (penetration testing);
— кодын дүн шинжилгээ

Эмзэг байдлыг сканнердах автомат хэрэгсэлийг мэдэгдэж байгаа эмзэг байдал\тай бүлэг хост эсвэл сүлжээний бүлэг [жишээ нь, нэргүй (FTP) файл дамжуулах систем, Sendmail гарц]-ийг сканнердахад ашигладаг.

Гэсэн хэдий ч автоматжуулсан сканнердах хэрэгслээр тодорхойлсон зарим боломжит эмзэг байдал нь системийн орчин нөхцөл дэх эмзэг байдлыг (жишээ нь, эдгээр сканнердах хэрэгслүүд нь байгууламжийн хүрээлэн буй орчин, шаардлагыг харгалзан үздэггүй) бодитоор төлөөлдөггүй. Автоматаар сканнердах програм хангамжаар илрүүлсэн зарим эмзэг байдал нь үнэн хэрэгтээ тэдний хүрээлэн буй орчин нь шаардсан тодорхой сайтанд эмзэг биш байдаг. Иймд туршилтын арга нь хуурамч эерэг хариуг бий болгодог.

Аюулгүй байдлын туршилт, үнэлгээ (STE) нь мэдээллийн системийг тодорхойлоход ашиглаж болох өөр нэг техник бөгөөд эрсдлийн үнэлгээний явцад МХТ-ийн системийн эмзэг байдлыг тодорхойлоход ашиглана. Үүнд туршилтын төлөвлөгөө (жишээ нь, туршилтын арга зүй, туршилтын журам, туршилтын хүлээгдэж буй үр дүн)-г боловсруулах, гүйцэтгэх ажил орно. Системийн аюулгүй байдлын туршилтийн зорилго нь үйл ажиллагааны орчинд МХТ-ийн системийг хэрэглэсэн тохиолдолд мэдээллийн системийн аюулгүй байдлын хяналтын үр нөлөөг шалгах явдал юм. Хэрэглэж буй програм хангамж, техник хангамжийн хяналт нь батлагдсан аюулгүй байдлын шаардлага, байгууллагын аюулгүй байдлын бодлого, үйлдвэрлэлийн стандартын хэрэгжилтийг хангах зорилготой юм.

Шургалгааны шалгалт нь аюулгүй байдлын хяналтын дүн шинжилгээг дэмжих болон МХТ-ын өөр өөр талуудын аюулгүй байдлыг хангахад ашиглаж болно. Эрсдэлийн үнэлгээний үйл явцад шургалааны шалгалтыг МХХТ-ийн системийн аюулгүй байдлыг тойрч гарах санаатай оролдлогыг тэсвэрлэх чадварыг үнэлэхэд ашиглаж болно. Үүний зорилго нь МХХТ-ийн системийг аюул заналын талаас нь турших, МХТ-ийн системийг хамгаалах схемд гарч болзошгүй алдааг илрүүлэх явдал юм.

Кодын дүн шинжилгээ нь эмзэг байдлын үнэлгээний хамгийн нарийн (гэхдээ хамгийн үнэтэй) арга юм.

Аюулгүй байдлын эдгээр төрлийн туршилтын үр дүн нь системийн эмзэг байдлыг тодорхойлоход тусална.

Эмзэг байдлыг амжилттай ашиглахгүй бол шургалааны арга хэрэгсэл нь худал үр дүн гаргаж болзошгүй. Тодорхой эмзэг байдлыг ашиглахын тулд шалгасан систем дээрх яг тэр систем/аппликейшн/засваруудын тохиргоог мэдэх шаардлагатай. Туршилтын үед эдгээр өгөгдөл тодорхойгүй бол тодорхой нэг эмзэг байдлыг амжилттай ашиглах боломжгүй (жишээлбэл, зайнаас эргэх холбоо үүсгэх). Гэсэн

[2] MNS ISO 2382-8:2011 стандартын 08.06.18-д тодорхойлсон.

хэдий ч туршсан үйл явц эсвэл системийг сүйрүүлэх эсвэл дахин эхлүүлэх боломжтой хэвээр байна. Ийм тохиолдолд турш объектыг мөн эмзэг гэж үзвэл зохино.

Аргууд нь дараахь ажиллагааг агуулж болно.

— хүмүүс болон хэрэглэгчидтэй ярилцлага хийх;
— санал асуулга;
— биет үзлэг;
— баримт бичгийн шинжилгээ.

А.2.5.4 Үйл ажиллагааны хувилбарууд

Өмч хөрөнгөд суурилсан аргын хүрээнд эрсдэлийн эх үүсвэрүүд бизнесийн өмч хөрөнгө болон тэдгээрийн хүсч бу эцсийн төлөв (desired end state цаашид “DES” гэх)-д хүрэхийн тулд ашиглаж өөр өөр замдуудад шинжилгээ хийх замаар үйл ажиллагааны хувилбаруудыг гаргана.

Эдгээр хувилбаруудыг шинжлэх нь тохиолдолд суурилсан аргыг нарийвчлан судлахад тусална. хийх нь үйл явдалд суурилсан хандлагыг судлахад тусална.

Амжилттай халдлага нь ихэвчлэн хэд хэдэн цоорхойг ашигласны үр дүн юм. Санаатай халдлага нь ихэвчлэн дараалсан аргыг ашигладаг. Сүүлийнх нь мэдээллийн технологийн хэд хэдэн эмзэг байдлыг уялдуулан ашигладаг. Араас нь МТ, зохион байгуулалт, физик орчны эмзэг байдлыг илрүүлэн ашигладаг. Ашиглагдаж буй цоорхойнуудыг тус тусад нь авч үзэхэд ач холбогдол багатай ийм аргаар хэд хэдэн цоорхойг нэгэн зэрэг ашиглах нь ноцтой үр дагаварт хүргэж болзошгүй юм.

Шинжилсэн хувилбаруудыг ердийн халдлагын дараллын дагуу зохион байгуулж болно. Ашиглах боломжтой хэд хэдэн загвар жишээ нь, кибер алллагын гинжин загвар[3]) байдаг. Энэ арга нь загварчилсан халдлагын нэвтрэх эсхүл илрүүлэх вектор эсхүл тархалтын релей болгон ашиглаж болох чухал туслах өмч хөрөнгийг тодорхойлох боломжийг олгоно.

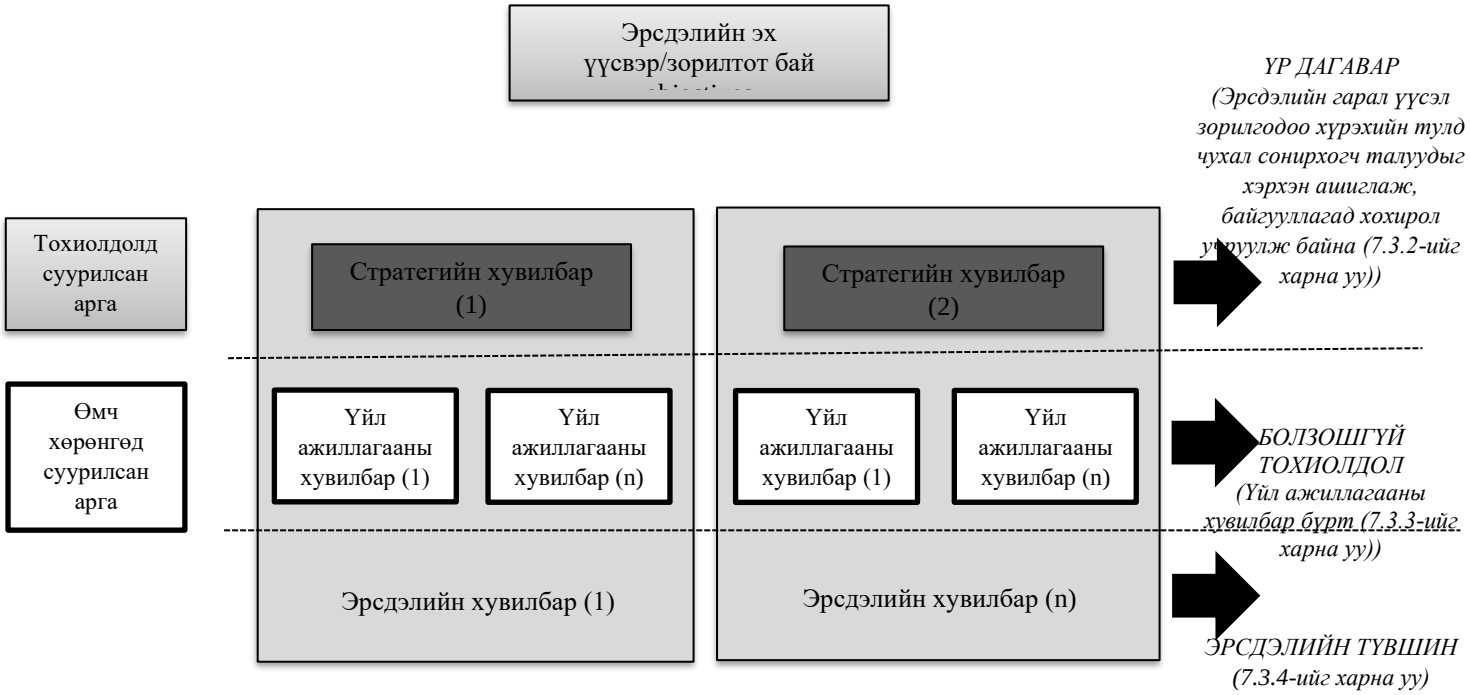
Эдгээр хувилбаруудыг график эсвэл халдлагын диаграм хэлбэрээр дүрсэлж болох бөгөөд энэ нь халдагчийн халдлагын аргыг харуулахад тустай.

А.2.6 Хоёр аргад хамаарах хувилбаруудын жишээ

Эрсдэлийн хувилбаруудыг тохиолдолд суурилсан арга, өмч хөрөнгө суурилсан арга эсвэл хоёуланг нь ашиглан бүтээж болно.

А.4 зурагт эрсдэлийн хувилбарт суурилсан эрсдлийн үнэлгээг үзүүлэв.

[3] Кибер аллагын гинжин загвар нь Lockheed Martin-аас нийлүүлсэн бүтээгдэхүүний худалдааны нэр юм. Уг мэдээлэл нь энэхүү баримт бичгийн хэрэглэгчид ойлголмжтой байдлыг хангах зорилгоор өгөгдсөн бөгөөд нэрлэсэн бүтээгдэхүүнийг ISO-аас баталгаажуулсан баримт биш болно. Ижил үр дүнд хүргэж болох ижил төстэй бүтээгдэхүүнийг ашиглаж болно.



А.4 зураг-Эрсдэлийн хувилбарт суурилсан эрсдлийн үнэлгээ

А.12 хүснэгтэд эрсдэлийн хувилбаруудын жишээ болон өмч хөрөнгө/тохиолдолд суурилсан арга, эрсдэлийн эх үүсвэртэй уялдаа холбоог харуулав.

А.12 хүснэгт-Аргуудад суурилсан эрсдэлийн хувилбаруудын жишээ

Эрсдэлийн эх үүсвэр	Зорилтот бай (DES)	Стратегийн эрсдэлийн хувилбар (Тохиолдолд суурилсан арга)	Үйл ажиллагааны эрсдэлийн хувилбар (Өмч хөрөнгөд суурилсан арга)
Эрх олголтын төлөв	Стратегийн халдлагын векторыг олж авах	Чухал дэд бүтцийг сүйрүүлэх	нийлүүлэлтийн сүлжээнд хортой кодыг далд бөгөөд тогтмол байршуулах
Зохион байгуулалт-тай гэмт хэрэг	Хууль бус үйл ажиллагааг хөгжүүлэх	Портын дэд бүтцийг ашиглах	dockers' union нэвчин орох
			Удирдлагын системийн компьютержсэн урсгалыг хянах
		Татварын сервер (carousel)-ийг луйвардах	Нүүрстөрөгчийн татварын зах зээл дээр хуурамч солилцоо хийх зорилгоор идэвхигүй

			компаниудыг бий болгох
		Мөнгө шаардах	Ransomware хортой кодыг түгээх
Түрэмгий бизнес	Зах зээлийн монополь эрхийг олж авах	Зохицуулагчид нөлөөлөх	Шийдвэр гаргагчийг авилгадах
		Өрсөлдөгчдийг зайлуулах	Нийгмийн сүлжээнд гүтгэлгийн кампанит ажил явуулах

А.2.7 Эрсдэлтэй холбоотой тохиолдлын мониторинг

Эрсдэлтэй холбоотой тохиолдлын монторинг нь 10.5.2-т дурдсанчлан мэдээллийн аюулгүй байдлын эрсдэлийн хувилбарт нөлөөлж болох хүчин зүйлсийг тодорхойлох явдал юм.

Энэ тохиолдолд хүчин зүйлсийг ухайн өмч хөрөнгөд тохиолдсон гэнэтийн үйлдлийг илрүүлэх боломжийг бий болгодог элементүүдийн багц гэж тодорхойлох бөгөөд , мэдээллийн аюулгүй байдлын эрсдлийн хувилбарын өдөөгчийг тодорхойлохын тулд байгууллагын мониторингийн чадавхи, арга хэрэгсэлд нэгтгэх боломжтой. Эрсдэлтэй холбоотой тохиолдлын мониторингийг 7.2.1-д танилцуулсан үйл ажиллагааны хувилбарууд эсвэл стратегийн хувилбаруудаас гарч буй хэд хэдэн үзүүлэлтийг ашиглан тодорхойлж болно. Тэд өөр өөр шинж чанартай байж болно (техникийн, зохион байгуулалтын, зан үйлийн, аудитын үр дүн гэх мэт). Тохиолдлыг үр дагаврын хэмжээ, болзошгүй тохиолдол зэрэг тодорхойлсон тэргүүлэх чиглэлийн дагуу мониторинг хийнэ. А.13 хүснэгтэд мэдээллийн аюулгүй байдлын эрсдэлийн хувилбарын тайлбар жишээг эрсдэлтэй холбоотой тохиолдлын мониторингийн хамт үзүүлэв.

А.13 хүснэгт- эрсдэлийн хувилбарын тайлбар жишээ болон эрсдэлтэй холбоотой тохиолдлын мониторингийн хамаарал

Эрсдэлийн бүрдэл	Жишээ	Мониторинг хийвэл зохих тохиолдолууд
Стратегийн хувилбар (тохиолдолд суурилсан)	Эмзэг баримт бичгүүдийг admin устгадаг	
Холбогдох тохиолдлууд	Чухал баримт бичгүүд устах	
Үр дагаврын ноцтой байдал	Тодорхойлох хэмжигдэхүүн: өндөр	
Үйл ажиллагааны хувилбарууд	Мэдээллийн сан руу шууд нэвтрэх замаар нууц бичиг баримтыг устгах администраторын эрхийг ашиглах	

(өмч хөрөнгөд суурилсан)	Системийн огноо/цагийг өөрчлөхийн тулд root хандалт хийх	Ажлын бус цагаар өгөгдлийн санд хийж буй шууд хандалтыг илрүүлэх
	Өгөгдлийн сан болон администраторын ажлын компвютерт хортой код халдвар тараах	
Болзошгүй тохиолдол	Тодорхойлох хэмжигдэхүүн: дунд	
Эрсдлийн эх үүсвэр	Администратор	
Зорилтот бай	Нууц баримт бичгийн хүртээмжийг алдагдуулах	
DES	Системийн эвдрэл	
Аюулгүй байдлын хяналтууд	Backup стратегийг хэрэгжүүлэх	
	Хортой програмын эсрэг шийдэл	
	NTP хэрэгжүүлэх	Их хэмжээний өгөгдөлд ихээр нөлөөлж буй үйлдлүүдийг илрүүлэх
	OS хамгаалалтыг чангатгах	
	Үйл ажиллагааны өгөгдөлд хандах эрхийг хязгаарлах	

Эх үүсвэр-үйл ажиллагаа-очих газар-өдөөгч (source-function-destination-trigger буюу цаашид “SFDT”) загвар нь эрсдэлтэй холбоотой үйл явдлуудад мониторинг хийх боломжийг бүрдүүлдэг бөгөөд үүнд:

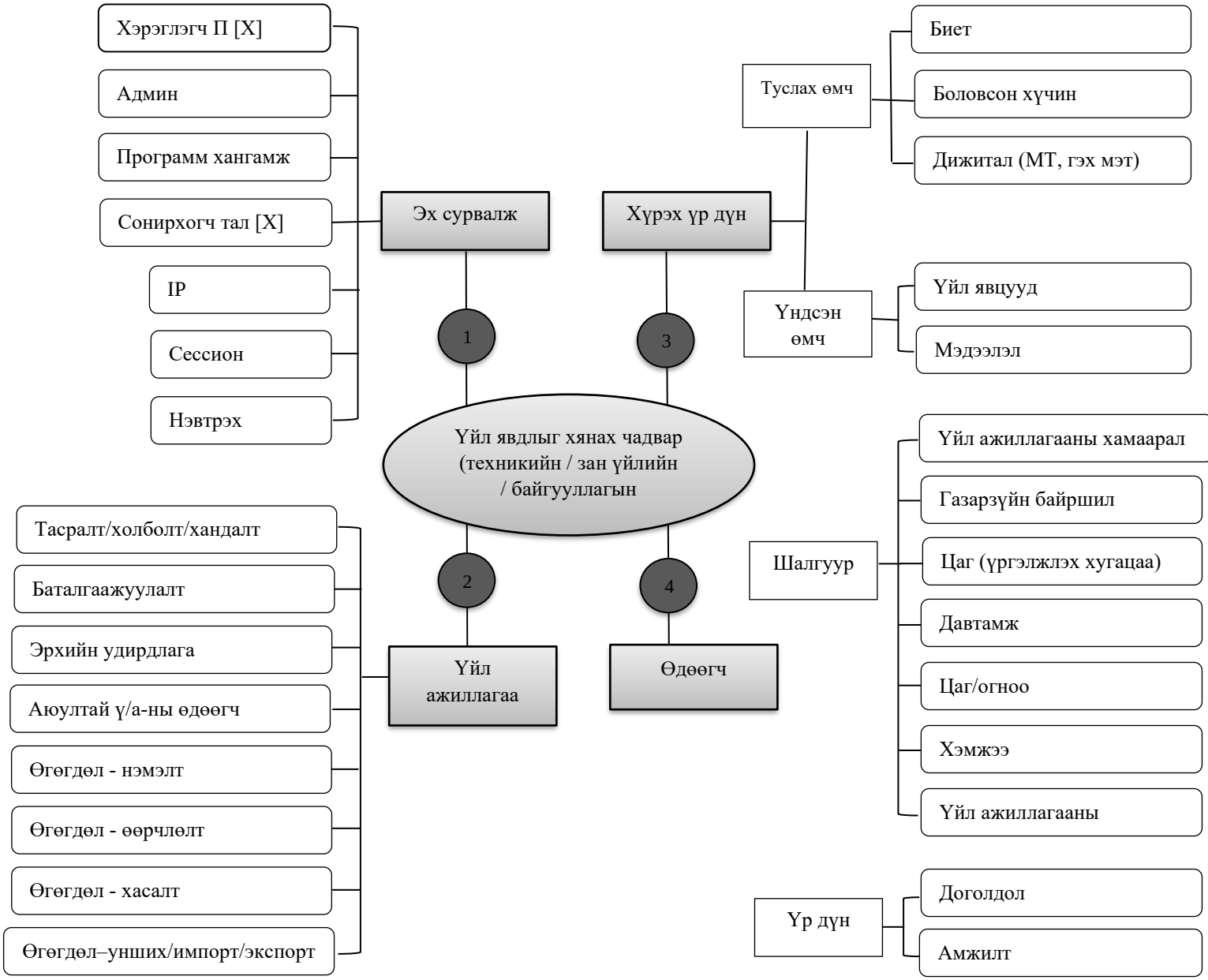
— эх үүсвэр: тохиолдол/техник хаанаас ирж байгааг (хэн, яагаад?) зааж, A.2.3 нөөцөд холбогдох боломжтойг;

— үйл ажиллагаа: халдагч ямар тохиолдол/техникийн төрлийг (юу?) ашигласныг;

— очих газар: ямар арга эсвэл тохиолдол ашиглаж байгааг заана (ямар үндсэн эсвэл туслах хөрөнгө дээр?)

— өдөөгч: ямар нөхцөл нь эрсдэлийн хувилбарыг (халдлагын үр дүн) илрүүлэх, тодорхойлох боломж олгодог.

SFDT загварыг хэрэглэх жишээг А.5 зурагт үзүүлэв.



А.5 зураг- SFDT загварыг хэрэглэх жишээ

Эрсдэлтэй холбоотой тохиолдолын мониторинг үр дүнтэй, үр ашигтай хийж, мэдээллийн аюулгүй байдлын эрсдэлийн хувилбарт мониторинг хийхийн тулд түүний үзүүлэлтүүдийг тодорхойлох шаардлагатай.

Эрсдэлтэй холбоотой тохиолдлуудын мониторингийн үзүүлэлтүүд нь:

— мониторинг хийж буй эрсдэлийн хувилбарын эрсдэлийн түвшин;

— эрсдэлийн хувилбарт мониторинг хийхийн тулд эрсдэлтэй холбоотой тохиолдлын үр нөлөө, чадвар;

— үр ашиг, жинхэнэ эерэг дохио ба худал эерэг дохионы харьцаа, эсвэл үзүүлэлтийн өртөг.

Ном зүй

[1] ISO 17666:2016, *Space systems — Risk management*

[2] ISO/IEC 27001:2022, *Information technology — Security techniques — Information security management systems — Requirements*

[3] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[4] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[5] ISO/IEC 27014, *Information security, cybersecurity and privacy protection — Governance of information security*

[6] ISO/IEC/TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*

[7] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[8] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[9] ISO 31000:2018, *Risk management — Guidelines*

[10] IEC 31010:2019, *Risk management — Risk assessment techniques*

[11] ISO Guide 73:2009, *Risk management — Vocabulary*