ХАЛДВАРТ ОВЧИН
СУДЛАЛЫН ҮНДЭСНИЙ ТӨВИЙН
ЕРӨНХИЙ ЗАХИРЛЫН
ТУШААЛ

2022 оны 07 сарын 11 өдөр Дугаар А/199 Улаанбаатар хот

Журам батлах тухай

Төрийн болон албаны нууцын тухай хууль, Кибер аюулгүй байдлын тухай хуулийн 10 дугаар зүйлийн 10.1.5 дахь хэсэг, 19 дүгээр зүйлийн 19.2 дах хэсэг, Засгийн газрын 2022 оны 05 дугаар сарын 25-ны өдрийн 207 дугаар тогтоол, Хүний хүвийн мэдээлэл хамгаалах тухай хуулийн 6 дугаар зүйл, Эрүүл мэндийн сайдын 2019 оны А/396 дүгээр тушаал, Халдварт өвчин судлалын үндэсний төвийн дүрмийн 5.3 дахь заалтыг тус тус үндэслэн ТУШААХ нь:

1. Халдварт өвчин судлалын үндэсний төвийн "Кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам"-ыг хавсралтаар тус батлалсугай.
2. Журмыг нийт алкилтнуудад танилцуулж, хэрэгжилтийг хангах ажлыг зохион байгуулж ажиллахыг Мэдээлэл технологийн албаны дарга (Д.Доржпалам)-д даалгасугай.
3. "Кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам"-ыг мөрдөж ажиллахыг нийт алкилтнуудад үүрэг болгосугай.
4. Энэхүү тушаалын хэрэгжилтэнд хяналт тавьж ажиллахыг Стратеги төлөвлөлт, гадаад харилцаа зохицуулах газар захиргаа (Д.Баярсайхан)-д даалгасугай.

ЕРӨНХИЙ ЗАХИРЛЫН АЛБАН
ҮҮРГИЙГ ХАВСРАН ГҮЙЦЭТГЭГЧ Ж.БАЙГАЛМАА

ХӨСҮТ-ийн Ерөнхий захиргаан
2023 оны 07 дугаар сарын 27-ны өдрийн
А/154 дугаар тушаалын хавсралт

КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ҮЙЛ АЖИЛЛАГААНЫ ДОТООД ЖУРАМ

Нэг.Нийтлэг үндэслэл

1.1.Энэхүү журмын зорилго нь Кибер аюулгүй байдлын тухай хуулийн 16.1, 18.1-д заасан хуулийн этгээд (цаашид "байгууллага" гэх)-ийн мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдлыг хангах, кибер халдлага, кибер аюулгүй байдлын зөрчлийг илрүүлэх, хариу арга хэмжээ авах, урьдчилан сэргийлэх, нөхөн сэргээх болон тэдгээртэй холбоотой бусад үйл ажиллагаанд дагаж мөрдөх нийтлэг харилцаог зохицуулахад оршино.

1.2.Байгууллага нь кибер аюулгүй байдлын хууль тогтоомж, энэ журам, олон улсын стандартад нийцүүлэн, өөрийн үйл ажиллагааны онцлог, цар хүрээг харгалзан кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журмыг батлан, мөрдөнө.

1.3.Байгууллагын нэвтрүүлсэн олон улсын стандарт, холбогдох хууль, дүрэм, журмын хүрээнд тавигдах шаардлага нь хоорондоо давхацсан тохиолдолд өндөр шаардлага тогтоосон шаардлагыг дагаж мөрдөнө.

1.4.Энэ журмын 1.2-т заасан дотоод журмыг жил бүр тогтмол хугацаанд, эсхүл холбогдох хууль тогтоомж, байгууллагын дотоод бүтэц, мэдээллийн систем, мэдээллийн сүлжээнд өөрчлөлт орсон тухай бүр шаардлагатай өөрчлөлтийг оруулна.

1.5.Төрийн болон албаны нууцад хамаарах мэдээллийн кибер аюулгүй байдлыг хангахад Төрийн болон албаны нууцын тухай хууль, журмыг дагаж мөрдөнө.

Хоёр.Кибер аюулгүй байдлыг хангах зохион байгуулалтын арга хэмжээ

2.1.Байгууллага кибер аюулгүй байдлыг хангах чиглэлээр дараах зохион байгуулалтын арга хэмжээг авч хэрэгжүүлнэ.

2.1.1.кибер аюулгүй байдлыг хангах стратеги төлөвлөгөөг байгууллагын стратеги төлөвлөгөөтэй уялдуулан боловсруулах;

2.1.2.шаардлагатай удирдлага, санхүү, хүний нөөцийн чадавхыг бүрдүүлж кибер аюулгүй байдлын стратеги төлөвлөгөөг хэрэгжүүлэх;

2.1.3.мэдээллийн технологи, кибер аюулгүй байдал хариуцсан эжилтэн, албан хаагчийн мэдлэг, ур чадварыг тогтмол дээшлүүлэх арга хэмжээг авах;

2.1.4.мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээг холбогдох стандарт, эсхүл хуульд заасан хугацаанд хийлгэх, тайланг кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд хүргүүлэх;

2.1.5.эрсдэлийн үнэлгээний үр дүнд үндэслэн эрсдэлийг бууруулахад чиглэсэн арга хэмжээг төлөвлөх, хэрэгжүүлэх;

2.1.6.кибер халдлага, зөрчилтэй тэмцэх төвөөс хүргүүлсэн зөвлөмж, шаардлагыг тогтоосон хугацаанд, эсхүл ажлын 10 өдрийн дотор хэрэгжүүлж хариу мэдээлэх;

2.1.7.кибер аюулгүй байдлыг хангахтай холбоотой энэ журмын 1.2-т заасан журам болон холбогдох баримт бичгийг боловсруулж, байгууллагын холбогдох ажилтан, албан тушаалтанд тухай бүр танилцуулах;

2.2.Байгууллага нь кибер аюулгүй байдлыг хангах чиглэлээр дараах хүний нөөцийн арга хэмжээг авч хэрэгжүүлнэ.

2.2.1.кибер аюулгүй байдлын удирдах болон гүйцэтгэх чиг үүргийг ажлын байрны, эсхүл албан тушаалын тодорхойлолтод тусгаж, орон тооны, эсхүл хавсран гүйцэтгэх ажилтныг томилох;

2.2.2.кибер аюулгүй байдлын мэдлэг олгох дараах сургалтыг зохион байгуулах:

2.2.2.1.жил бүр тогтмол хугацаанд, нийт ажилтнуудыг хамруулах;

2.2.2.2.ажилтныг томилогдсоноос хойш 1 сарын дотор;

2.2.2.3.гэрээгээр хамтран ажиллаж байгаа гуравдагч талын ажилтныг тухай бүр.

2.2.3.кибер орчинд хандаж, мэдээлэлтэй ажиллах ажилтан, албан хаагч, бусад этгээдтэй мэдээллийн нууц хадгалах болон кибер аюулгүй байдлыг хангах талаар үүрэг, хариуцлагыг тусгасан гэрээ байгуулах, эсхүл нууцын баталгаа үйлдэх;

2.2.4.албан хаагч бүрд кибер халдлага, зөрчилтэй тэмцэх, кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журмын зөрчлийн үед авах арга хэмжээний талаар мэдлэг олгох.

Гурав.Мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээг тодорхойлох

3.1.Байгууллага хамгаалбал зохих мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээний нууцын зэрэглэл, мэдээлэл хариуцагчийг тодорхойлсон жагсаалтыг гаргаж, тогтмол шинэчилнэ.

3.2.Байгууллага нь энэ журмын 3.1-д заасан мэдээллийн нууцын зэрэглэлийг холбогдох хууль, журамд нийцүүлж тогтооно.

3.3.Байгууллага нь энэ журмын 3.1-д заасан жагсаалтад дурдсан мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээнд учирч болзошгүй аюул занал, үр дагавар, нөлөөллийг үнэлэх зорилгоор эрсдэлийн үнэлгээг хийхдээ ISO 27005 стандартыг баримтална.

3.4.Байгууллага нь мэдээллийн нууцын зэрэглэлээс хамаарч, танилцах, ашиглах, дамжуулах, хадгалахтай холбоотой үйл ажиллагааг зохицуулсан тусгайлсан журмыг батлан, мөрдөж болно.

Дөрөв.Кибер халдлага, зөрчлөөс хамгаалах арга хэмжээ

4.1.Байгууллага нь мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээнд зөвшөөрөлгүй хандах, дамжуулах, өөрчлөх, устгахаас хамгаалж хандалтын удирдлагыг тодорхойлно.

4.2.Байгууллага нь хандалтын удирдлагад тодорхойлсны дагуу мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээнд хандах эрхийг өгөөж, энэ талаар бүртгэл хөтлөх, хяналт тавьж ажиллах бөгөөд тухай бүр шаардлагатай өөрчлөлтийг оруулна.

4.3.Байгууллагын удирдлага мэдээллийн систем, мэдээллийн сүлжээнд дээгүү эрхтэй (admin, root) хандах эгээдийг тухай бүр тогтоож, хандах эрхийн ашиглалтад хяналт тавина.

4.4.Байгууллагын мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байрлаж байгаа зориулалтын өрөөнд зөвшөөрөлгүй нэвтрэхийг хориглох бөгөөд өрөө нь дараах шаардлагыг хангасан байна:

4.4.1.өрөөний хаалга цоожтой байх;

4.4.2.дохиоллын системтэй байх;

4.4.3.цонхны хамгаалалттай байх;

4.4.4.орох хаалганы дээгүд дүрст хяналтын системтэй байх;

4.4.5.температур, чийгшил зэрэг орчны нөхцөлийг хянах, бүрдүүлэх хэрэгсэлтэй байх;

4.4.6.хаалганы түлхүүр, эрхийг зөвхөн эрх бүхий ажилтан хадгалах.

4.5.Байгууллага мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байршуулах зориулалтын өрөөгүй бол энэ журмын 4.4-т заасан шаардлагад дүйцэх, тоног төхөөрөмжид зөвшөөрөлгүй этгээд хандахаас сэргийлсэн цоож, шүүгээ бүхий өрөөнд байршуулж болно.

4.6.Байгууллагын ажилтан, албан хаагч бүр хэрэглэгчийн эцсийн төхөөрөмж (компьютер зэрэг)-тэй ажиллахад аюулгүй байдлыг хангах талаар дараах арга хэмжээг авч хэрэгжүүлнэ:

4.6.1.байгууллага зөвшөөрснөөс бусад төрлийн программ хангамжийг ашиглахгүй байх;

4.6.2.төхөөрөмжид нэвтрэхэд нууц үг ашигладаг байх;

4.6.3.хувийн хэрэгцээнд ашиглахгүй байх;

4.6.4.нууцын зэрэглэлтэй мэдээлэл агуулсан төхөөрөмжийг зөвшөөрсөн бусдаас зөвшөөрөлгүйгээр гадагш гаргахгүй байх;

4.6.5.байгууллагаас өөрт олгосон төхөөрөмж, нэвтрэх нэр, нууц үгийг ашиглах ба бусдад дамжуулж, ашиглуулахгүй байх;

4.6.6.засвар үйлчилгээг зөвхөн байгууллагын мэдээллийн технологи хариуцсан нэгж, ажилтнаар хийлгэх, оношлуулах;

4.7.Байгууллага үүлэн технологид суурилсан үйлчилгээ (цаашид "үйлчилгээ" гэх) ашиглах бол энэ журмын 1.2-т заасан журамд, эсхүл тусгайлсан журам баталж, дараах мэдээллийг тусгана.

4.7.1.үйлчилгээг ашиглахад тавигдах хөвөр аюулгүй байдлын шаардлага;

4.7.2.үйлчилгээг сонгох шалгуур үзүүлэлт, харилцааний хамрах хүрээ;

4.7.3.байгууллагын албан хаагчийн үүрэг, хариуцлага;

4.7.4.үүлэн технологид суурилсан үйлчилгээ үзүүлэгч этгээдийн хэрэгжүүлж буйаас өөр аюулгүй байдлыг хангах үйл ажиллагаа;
4.7.5.үйлчилгээтэй холбоотой байгууллагын хэрэгжүүлж болох өөр аюулгүй байдлын арга хэмжээ;
4.7.6.байгууллага олон үйлчилгээг зэрэг ашиглах үед тодорхойлсон аюулгүй байдлыг үнэлэхэд зохион байгуулах арга хэмжээ;
4.7.7.үйлчилгээ ашиглах үед тохиолдсон халдлага, зөрчлийн эрэг авах харуу арга хэмжээ;
4.7.8.эрсдэлийг бууруулах арга хэмжээ;
4.7.9.үйлчилгээнд өөрчлөлт орсон эсэхүл зогсоох үед хэрэгжүүлэх аюулгүй байдлын арга хэмжээ;
4.8.Байгууллага үүлэн технологид суурилсан үйлчилгээ авах бол холбогдох хууль тогтоомжид нийцүүлэн ажил гүйцэтгэгчтэй байгуулах гэрээнд дараах шаардлагыг тусгана.
4.8.1.үйлдвэрлэгчээс тогтоосон стандартын дагуу технологийн шийдэл хэрэгжүүлэх талаар;
4.8.2.байгууллагын аюулгүй байдлын шаардлагад нийцсэн хандалтын удирдлага хэрэгжүүлэх талаар;
4.8.3.хортой кодын хяналт болон хамгаалалтын шийдлийг хэрэгжүүлэх талаар;
4.8.4.харилцан зөвшөөрсөн байршилд мэдээллийг хадгалах, боловсруулах талаар;
4.8.5.халдлага зөрчлийн үед эсэхүл гүйцэтгэгч, эсэхүл үйлдвэрлэгчээс техникийн туслалцаа үзүүлэх талаар;
4.8.6.ажил гүйцэтгэгч нь үйлчилгээтэй холбоотой туслан гүйцэтгэх гэрээ байгуулахад байгууллагын өөр аюулгүй байдлын шаардлагыг хангуулах талаар;
4.8.7.өөр халдлага, зөрчлийн дараа нөхөн сэргээхэд техникийн туслалцаа үзүүлэх талаар;
4.8.8.үйлчилгээг зогсоох үед ажил гүйцэтгэгчийн эзэмшсэн хэсэгт үйлчилгээний хүртээмжтэй байдлыг баталгаажуулах талаар;
4.8.9.нөөц өгөгдөл, тохиргооны файл, эх код, байгууллагын эзэмшлийн өгөгдлийг шаардлагатай үед гаргаж өгөх талаар;
4.9.Үйлчилгээтэй холбоотой дараах өөрчлөлтийн үед ажил гүйцэтгэгч байгууллагад урьдчилан мэдэгдэл хүргэнэ.
4.9.1.үйлчилгээний тасралтгүй ажиллагаа, аюулгүй байдалд нөлөөлөл үзүүлэх хэмжээний техникийн өөрчлөлт орсон;
4.9.2.мэдээллийг хадгалах, боловсруулах газар зүйн байршил өөрчлөгдсөн;
4.9.3.гэрээ байгуулсан туслан гүйцэтгэгчийн үйлчилгээнд өөрчлөлт орсон;
4.10.Байгууллага мэдээлэл, түүнийг агуулах байгаа мэдээллийн систем, мэдээллийн сүлжээг хортой кодоос хамгаалах програмыг ханган ажиллана.
4.11.Байгууллага мэдээллийн систем, мэдээллийн сүлжээнээс мэдээлэл алдагдахаас урьдчилан сэргийлэх талаар дараах арга хэмжээг авч хэрэгжүүлнэ:
4.11.1.алдагдах эрсдэлтэй мэдээллийг тодорхойлох;

4.11.2.мэдээлэл алдагдах болзошгүй мэдээллийн систем, мэдээллийн сүлжээ теххэрэмж, зөөвөрийн хэрэгслүүдийг тогтмол хянах;
4.11.3.мэдээллийг бусад этгээдэд дамжуулахаас сэргийлэх, дамжуулсан бол холбогдох арга хэмжээг шуурхай авах;
4.11.4.мэдээлэлд зөвшөөрөлгүй хандах, ашиглах, устгах, өөрчлөх үйлдэл хийж байгаа этгээдийн үйлдлийг таслан зогсоох;
4.11.5.мэдээлэл боловсруулж байгаа мэдээллийн систем, мэдээллийн сүлжээг халдлага, зөрчил, саатлын үед сэргээн ажиллах боломжтой байхаар зохион байгуулах;
4.12.Байгууллага өөрийн мэдээллийн системийн хөгжүүлэлтийг бусдаар гүйцэтгүүлэх тохиолдолд оюуны өмчийн эрхийг хамгаалах талаар арга хэмжээг авч хэрэгжүүлнэ.
4.13.Байгууллага зохиогчийн эрхийн зөрчилгүй программ хангамж, хөгжүүлэлтийн сан, худалдан авч, ашиглана.
4.14.Мэдээллийн систем, мэдээллийн сүлжээнд өөрчлөлт оруулахдаа өөрчлөлтийн удирдлагыг хэрэгжүүлж холбогдох талуудад мэдэгдэж, зөвшөөрөлийг үндэслэн дээр өөрчлөлтийг хэрэгжүүлж, эсхүл өөрчлөлтийг буцаах бөгөөд энэ талаар бүртгэл хөтөлнө.
4.15.Энэ журмын 3.1-д заасан мэдээллийн систем, мэдээллийн сүлжээний, өгөгдөл, тохиргоог нөөцлөх хуваарь гаргаж, хуваарийн дагуу тогтмол нөөцлөнө. Нөөцийн бүрэн бүтэн байдлыг шалгаж баталгаажуулна.
4.16.Байгууллага мэдээллийн систем, мэдээллийн сүлжээнд даралт үйлдлийн бүртгэлийг хөтөлнө.
4.16.1.нэвтрэх оролдлого болон нэвтэрсэн тухай;
4.16.2.давуу эрхийн хандалт;
4.16.3.нууц үгийн өөрчлөлт;
4.16.4.үйлдлийн бүртгэлийг өөрчлөх, устгах;
4.16.5.хандах эрх олгох, өөрчлөх, хүчингүй болгох.
4.17.Үйлдлийн бүртгэлд дараах мэдээллийг тодорхойлно:
4.17.1.хэрэглэгчийн нэр, системд нэвтрэх нэр буюу ID;
4.17.2.огноо;
4.17.3.хандсан хаяг, төхөөрөмжийн мэдээлэл;
4.17.4.хандалтын үргэлжлэх хугацаа;
4.17.5.гүйцэтгэсэн үйлдэл;
4.17.6.гүйцэтгэсэн үйлдлийн үр дүн;
4.18.Байгууллага нь мэдээллийн системийн үйлдлийн бүртгэлд эрх олгогдсон этгээд зөвшөөрлөөр хандах нөхцөлийг бүрдүүлнэ.
4.19.Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийг доор дурдсан хугацаанд хадгална.
4.19.1.кибер аюулгүй байдлын тухай хуулийн 19.1-д заасан байгууллага 1 жил буюу түүнээс дээш хугацаагаар;
4.20.Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээнд зөвшөөрөгдөөгүй байгаа үйлдлийн систем, программ хангамжийг шинэчлэхэд дараах арга хэмжээг авч хэрэгжүүлнэ.

4.20.1.шинэчлэл гарах бүрд суулгах;
4.20.2.зөвшөөрөгдсөн албан ёсны эх үүсвэрээс шинэчлэх;
4.20.3.шинэчлэлийг суулгахаас өмнө эмзэг байдал үүсгэх эсэхийг шалгах, баталгаажуулах.

Тав.Кибер халдлага, зөрчлийг илрүүлэх арга хэмжээ

5.1.Мэдээллийн систем, мэдээллийн сүлжээний хэвийн бус үйл ажиллагааг илрүүлэхэд дараах арга хэмжээг авч хэрэгжүүлнэ.
5.1.1.мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийг тогтмол цуглуулж, тайлан гаргах;
5.1.2.мэдээллийн систем, мэдээллийн сүлжээний хэвийн бус үйл ажиллагаа, үйлдлийг нөөцтэй байдлаар нь эрэмбэлж, эрэмбийн дарааллаар эрх бүхий ажилтан, албан хаагч, этгээдэд мэдээлэх нөхцөлийг бүрдүүлэх;
5.1.3.мэдээллийн систем, мэдээллийн сүлжээ, аюулгүй байдлын тоног төхөөрөмжийн үйлдлийн бүртгэлийг нэгтгэн цуглуулж, дүн шинжилгээ хийх боломжийг бүрдүүлэх;
5.1.4.байгууллагын ажилтан, албан хаагч, нийлүүлэгч, хэрэглэгч талаас кибер халдлага, зөрчил үйлдсэн, эсхүл ертөнц байж болзошгүй тохиолдлыг илрүүлэх;
5.1.5.кибер халдлага, зөрчилтэй холбоотой нотлох баримтыг цуглуулж, баримтын хүлээлгэх эх хувилах зөрүүгүй байлгах.
5.2.Мэдээллийн систем, мэдээллийн сүлжээг хөнгөвд дараах арга хэмжээг авч хэрэгжүүлнэ.
5.2.1.мэдээллийн систем, мэдээллийн сүлжээний ачаалалыг тогтмол, эсхүл 24/7 горимоор хянах;
5.2.2.бичиг орчныг хянах;
5.2.3.мэдээллийн систем, мэдээллийн сүлжээнд үйлчилгээ авах тохиолдолд тухайн үйлчилгээ үзүүлэгчийн үйл ажиллагаанд хяналт тавих;
5.2.4.мэдээллийн систем, мэдээллийн сүлжээний эмзэг байдлын шалгалтыг тогтмол хийх;
5.3.Кибер халдлага, зөрчлийг илрүүлэх ажиллагаат туршин шалгах, тогтмол сайжруулалт хийнэ.
5.4.Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээнд тохирсон аюулгүй байдлыг хангах систем (IDS/IPS, antimalware, WAF, Email filter, SIEM)-ийг хэрэглэнэ.

Зургаа.Кибер халдлага, зөрчилд хариу арга хэмжээ авах

6.1.Байгууллага нь «кибер халдлага, зөрчлийн үед хариу арга хэмжээ авах төлөвлөгөө» батлах, хэрэгжүүлэх бөгөөд төлөвлөгөөнд дараах мэдээллийг тусгана.
6.1.1.байгууллага дотор «кибер халдлага, зөрчлийг мэдэгдэх албан тушаалтан;
6.1.2.тохиолдлыг шинжилж, кибер халдлага, зөрчилд тооцох шалгуур үзүүлэлт;
6.1.3.халдлага, зөрчлийн талаарх мэдээллийг илгээх, хүлээн авах суваг;

6.2.Кибер аюулгүй байдал хариуцсан ажилтан энэ журмын 6.1.2-т заасан шалгуур үзүүлэлтийн дагуу кибер халдлага, зөрчлийн тохиолдол бүрд үнэлгээ хийж халдлага, зөрчлийг тодорхойлно.
6.3.Байгууллага жилд нэгээс доошгүй удаа кибер халдлага, зөрчилд хариу арга хэмжээ авах төлөвлөгөөний дагуу дадлага, туршилт хийж, төлөвлөгөөг тогтмол шинэчилж сайжруулна.
6.4.Байгууллага кибер халдлага, зөрчилд өртсөн тохиолдолд төлөвлөгөөний дагуу кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд мэдэгдэж, шаардлагатай мэдээллийг гарган өгч хамтран ажиллана.

Долоо Мэдээллийн систем, мэдээллийн сүлжээг нөхөн сэргээх арга хэмжээ

7.1.Байгууллага кибер халдлага, зөрчилд өртсөн мэдээллийн систем, мэдээллийн сүлжээг нөхөн сэргээх үйл ажиллагааг хариуцах албан тушаалтан, үйл ажиллагааны дарааллыг тодорхойлсон нөхөн сэргээх төлөвлөгөөг баталж, хэрэгжүүлнэ.
7.2.Байгууллага энэ журмын 7.1-д заасан төлөвлөгөөнд тусгагдсан үйл ажиллагааг жилд нэгээс доошгүй удаа шалган туршиж, шаардлагатай өөрчлөлтийг оруулж сайжруулалт хийнэ.
7.3.Кибер халдлага, зөрчлийн хор уршгийг арилгахад дараах арга хэмжээг авч хэрэгжүүлнэ.
7.3.1.кибер халдлага, зөрчилд өртсөн мэдээллийн систем, мэдээллийн сүлжээний нотлох баримтыг хөндөхөөс сэргийлэх;
7.3.2.мэдээллийн систем, мэдээллийн сүлжээ хэвийн байдалд орж сэргэх хүртэл холболт, ашиглалтыг хязгаарлах;
7.3.3.байгууллагын үйл ажиллагааны хэвийн байдал сэргэх хүртэл кибер халдлага, зөрчил илэрсэн үндсэн шалтгаан болсон мэдээллийн системийн үйл ажиллагааг зогсоох;
7.3.4.мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдал алдагдсаны улмаас хэвийн үйл ажиллагаа доголдсон тохиолдолд тухайн мэдээллийн систем, мэдээллийн сүлжээний үйл ажиллагааг орлуулан гүйцэтгэх нөөц горим (гар ажиллагаа, механик үйл ажиллагаа)-той байх;
7.4.Мэдээллийн систем, мэдээллийн сүлжээний хэвийн үйл ажиллагааг нөхөн сэргээхэд дараах арга хэмжээг авч хэрэгжүүлнэ.
7.4.1.кибер халдлага, зөрчилд өртсөн мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийг боломжит хамгийн бага хугацаанд нөөцлөлтөөс сэргээх;
7.4.2.нөхөн сэргээгдсэн мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийг кибер халдлага, зөрчилд өртөхөөс өмнөх үеийн хэвийн төлөвт эргэн шилжсэнийг шалган баталгаажуулах;
7.4.3.нөхөн сэргээх үйл ажиллагааны хүрээнд авсан арга хэмжээ, үр дүнг баримтжуулан холбогдох эрх бүхий албан тушаалтанд танилцуулах;
7.4.4.мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийг нөхөн сэргээж, хэвийн үйл ажиллагаанд оруулсан талаар тодорхой түвшний баримт нотолгоо, туршилтын үр дүнд үндэслэн нөхөн сэргээх үйл ажиллагааг дуусгах;

7.5.Кибер халдлага, зөрчил, нөхөн сэргээх үйл ажиллагаа, түүний явц, үр дүнгийн талаарх үнэн зөв мэдээллийг мэдээллийн систем, мэдээллийн сүлжээнд холбогдсон талуудад тухай бүр мэдэгдэнэ.

Найм.Үүрэг, хариуцлага

8.1.Байгууллагын удирдах албан тушаалтан кибер аюулгүй байдлыг хангах чиглэлээр дараах үүрэгтэй:

8.1.1.байгууллагын кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлагаар хангах, уялдуулан зохион байгуулах, байгууллагыг төлөөлөх;

8.1.2.кибер аюулгүй байдлыг хангах бодлого, дүрэм, журам батлах;

8.1.3.кибер аюулгүй байдлыг хангах төлөвлөгөө гаргах, хэрэгжүүлэхэд шаардагдах нөөцийг байгууллагын жил бүрийн төсөв, төлөвлөгөөнд тусгах.

8.2.Байгууллагын кибер аюулгүй байдал хариуцсан ажилтан дараах үүрэгтэй:

8.2.1.байгууллагын кибер аюулгүй байдлыг хангах өдөр тутмын үйл ажиллагааг хариуцан гүйцэтгэх;

8.2.2.холбогдох дүрэм, журмыг боловсруулах, шинэчлэх санал боловсруулах;

8.2.3.кибер аюулгүй байдлыг хангахад шаардлагатай үйл ажиллагаа, нөөцийг төлөвлөх;

8.2.4.кибер аюулгүй байдлыг хангах мэргэшүүлэх сургалтад хамрагдах;

8.3.Байгууллагын нийт ажилтан кибер аюулгүй байдлыг хангах чиглэлээр дараах үүрэгтэй:

8.3.1.энэ журам болон мэдээллийн аюулгүй байдлыг хангахтай холбоотой бусад дүрэм, журмыг дагаж мөрдөх;

8.3.2.илэрсэн халдлага, зөрчил, сэжигтэй тохиолдол бүрийг аюулгүй байдал хариуцсан ажилтанд мэдэгдэх;

8.3.3.байгууллагын мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээг зөвхөн албан хэрэгцээнд заасан журам, зааврын дагуу хэрэглэх;

8.3.4.байгууллагаас зохион байгуулж буй кибер аюулгүй байдлын мэдлэг олгох сургалтад хамрагдах;

8.4.Энэхүү журмыг зөрчсөн албан тушаалтан, байгууллагад холбогдох хууль тогтоомжид заасан хариуцлага хүлээлгэнэ.

----оОо----