

УЛСЫН БҮРТГЭЛИЙН БАЙГУУЛЛАГЫН КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ДОТООД ЖУРАМ

Нэг. Зорилго

Монгол Улсын Кибер аюулгүй байдлын тухай хуулийн 7 дугаар зүйлийн 7.2 дахь хэсэг, Кибер аюулгүй байдлыг хангах нийтлэг журмын 1.2 дахь заалтын хэрэгжилтийг хангах, улсын бүртгэлийн байгууллагын кибер аюулгүй байдлыг хангахтай холбоотой харилцааг зохицуулахад оршино. Мөн төрийн болон албаны нууцад хамаарах мэдээллийн кибер аюулгүй байдлыг хангах асуудлыг Төрийн болон албаны нууцын тухай хууль болон түүнд нийцүүлэн гаргасан холбогдох дүрэм, журмаар зохицуулна.

Хоёр. Нэр томьёоны тодорхойлолт

“кибер аюулгүй байдал” гэж Кибер аюулгүй байдлын тухай хуулийн 4.1.1-т заасныг;

“кибер орон зай” гэж Кибер аюулгүй байдлын тухай хуулийн 4.1.2-т заасныг;

“кибер орчин” гэж Кибер аюулгүй байдлын тухай хуулийн 4.1.3-т заасныг;

“мэдээллийн системийн үйлдлийн бүртгэл” Кибер аюулгүй байдлын тухай хуулийн 4.1.11-т заасныг;

“кибер аюулгүй байдлын зөрчил” гэж Кибер аюулгүй байдлын тухай хуулийн 4.1.13-т заасныг;

“кибер халдлага” гэж Кибер аюулгүй байдлын тухай хуулийн 4.1.14-т заасныг;

“мэдээллийн систем” гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.1-т заасныг;

“мэдээллийн сүлжээ” гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.2-т заасныг;

“мэдээлэл солилцох сервис” гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.13-т заасныг;

“мэдээлэл хариуцагч” гэж Хүний хувийн мэдээлэл хамгаалах тухай хуулийн 4.1.8-т заасныг;

“цахим мэдээллийн сан” гэж иргэн, хуулийн этгээд, эд хөрөнгийн эрхийн улсын бүртгэлийн болон бусад мэдээллийн системийг ашиглан хуульд заасны дагуу цуглуулж, боловсруулж, хадгалсан цахим мэдээллийн бүрдлийг;

“давуу эрхтэй хэрэглэгч” гэж улсын бүртгэлийн байгууллагын мэдээллийн систем, мэдээллийн сүлжээ, программ хангамж, сервер, тоног төхөөрөмжид давуу эрхээр нэвтэрч, ашиглаж буй албан хаагчийг;

“хэрэглэгч” гэж улсын бүртгэлийн байгууллагын мэдээллийн систем, мэдээллийн сүлжээ, программ хангамж, сервер, цахим үйлчилгээ болон бусад үйл

ажиллагаанд өөрт олгогдсон эрхийн дагуу хандаж, ашиглаж буй удирдах болон гүйцэтгэх албан тушаалтан, ажилтан;

“бусад хэрэглэгч” гэж гэрээт ажилтан, зөвлөх үйлчилгээ үзүүлэгч, нийлүүлэгч байгууллагын ажилтан, мэдээллийн системд түр эсхүл урт хугацаанд хандах эрх олгогдсон бусад этгээдийг;

“галт хана” гэж кибер халдлага, зөрчлийг илрүүлэх, бүртгэх, таслан зогсоох мэдээллийн системийг;

“серверийн өрөө” гэж байгууллагын мэдээллийн систем, мэдээллийн сүлжээ, дэд бүтэц болон мэдээлэл технологийн тоног төхөөрөмжийг байршуулж, аюулгүй, тасралтгүй ажиллагааг хангах зориулалт бүхий өрөөг;

“техникийн өрөө” гэж байгууллагын харилцаа холбоо, мэдээллийн сүлжээ, цахилгаан болон дэд бүтцийн тоног төхөөрөмжийг байршуулж, ажиллуулах зориулалтын өрөөг;

“сүлжээний тоног төхөөрөмжийн зориулалтын хайрцаг” гэж сүлжээний төхөөрөмж (switch, router, firewall, patch panel, media converter)-ийг суурилуулах зориулалт бүхий төмөр эсвэл тусгай материалаар хийсэн цоожтой хайрцгийг;

“мэдээллийн технологийн тоног төхөөрөмж” гэж байгууллагын үйл ажиллагаанд ашиглагдаж буй сервер, хадгалах төхөөрөмж (сторэйж), сүлжээний тоног төхөөрөмж, суурин болон зөөврийн компьютер, цаг бүртгэлийн төхөөрөмж, хяналтын камер, хурууны хээ унших, царай таних төхөөрөмж болон мэдээлэл цуглуулах, боловсруулах, хадгалах, дамжуулах, хүлээн авахад ашигладаг бүх төрлийн техник хэрэгслийг;

Гурав. Кибер аюулгүй байдлыг хангах

3.1. Улсын бүртгэлийн байгууллагын дарга:

3.1.1. Шаардлагатай удирдлага, санхүү, хүний нөөцийн чадавхыг бүрдүүлж кибер аюулгүй байдлын стратеги төлөвлөгөөг хэрэгжүүлнэ.

3.1.2. Мэдээллийн технологи, кибер аюулгүй байдал хариуцсан албан хаагчийн мэдлэг, ур чадварыг тогтмол дээшлүүлэх арга хэмжээ авна.

3.1.3. Мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээг холбогдох стандарт, эсхүл хуульд заасан хугацаанд хийлгэж, тайланг кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд хүргүүлнэ.

3.1.4. Кибер аюулгүй байдлын удирдах болон гүйцэтгэх чиг үүргийг ажлын байрны, эсхүл албан тушаалын тодорхойлолтод тусгаж, орон тооны, эсхүл хавсран гүйцэтгэх албан хаагчийг томилно.

3.1.5. Улсын бүртгэлийн байгууллагын дарга мэдээллийн систем, сүлжээнд давуу эрхтэй хандах этгээдийг тухай бүр тогтоож, хандах эрхийн ашиглалтад хяналт тавина.

3.2.Кибер аюулгүй байдал хариуцсан нэгж:

3.2.1.Кибер аюулгүй байдлыг хангах стратеги төлөвлөгөөг байгууллагын стратеги төлөвлөгөөтэй уялдуулан боловсруулж, улсын бүртгэлийн байгууллагын даргаар батлуулна.

3.2.2.Аюулгүй байдлын шаардлага хангахгүй компьютер, тоног төхөөрөмж, программ хангамж, лицензийг шинэчлэх, ашиглалтаас хасах тухай саналыг нэгтгэж улсын бүртгэлийн байгууллагын даргад танилцуулна.

3.2.3.Байгууллагын галт хана төхөөрөмж, мэдээллийн систем, мэдээллийн сүлжээ, серверийн лог бүртгэл болон аюулгүй байдлыг хангах үйл ажиллагаанд хяналт тавина.

3.2.4.Байгууллагын кибер аюулгүй байдлыг хангах өдөр тутмын үйл ажиллагааг гүйцэтгэж, шаардлагатай үйл ажиллагааг төлөвлөнө.

3.2.5.Байгууллагын үйл ажиллагаанд ашиглахыг зөвшөөрсөн программ хангамжийн жагсаалтыг боловсруулж, улсын бүртгэлийн байгууллагын даргаар батлуулна.

3.2.6.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудитын үр дүнд үндэслэн эрсдэлийг бууруулахад чиглэсэн арга хэмжээг төлөвлөж, хэрэгжилтэд хяналт тавина.

3.2.7.Байгууллагын албан хаагч, ажилтан, хэрэглэгч талаас кибер халдлага, зөрчил үйлдсэн, эсхүл өртсөн байж болзошгүй тохиолдлыг илрүүлж шаардлагатай арга хэмжээг авна.

3.2.8.Мэдээллийн систем, сүлжээний эмзэг байдлын шалгалтыг хийж, шаардлагатай сайжруулалтыг хариуцсан нэгж, албан тушаалтнаар гүйцэтгүүлж, хяналт тавина.

3.2.9.Байгууллагын мэдээллийн систем, сүлжээнд тохирсон аюулгүй байдлыг хангах систем (IDS/IPS, Firewall, Antivirus, WAF, SIEM гэх мэт) ашиглах.

3.2.10.Кибер халдлага, зөрчлийн үед хариу арга хэмжээ авах төлөвлөгөө боловсруулж улсын бүртгэлийн байгууллагын даргаар батлуулж, хэрэгжилтийг хангах.

3.2.11.Кибер халдлага, зөрчилд өртсөн тохиолдолд мэдээллийн систем, сүлжээний нотлох баримтыг хөндөхөөс сэргийлэх арга хэмжээ авна.

3.2.12.Байгууллага кибер халдлага, зөрчилд өртсөн тохиолдолд холбогдох хууль тогтоомж, дүрэм, журмын дагуу Кибер халдлага, зөрчилтэй тэмцэх үндэсний төвд мэдэгдэж, шаардлагатай мэдээллийг гарган өгч хамтран ажиллах бөгөөд мэдээллийн систем, сүлжээг хэвийн байдалд оруулж, сэргээх хүртэл холболт, ашиглалтыг хязгаарлах, шаардлагатай арга хэмжээг авч хэрэгжүүлнэ.

3.2.13.Албан хаагчдад холбогдох хууль тогтоомж, дүрэм, журам, кибер халдлага, зөрчил, тэдгээрээс урьдчилан сэргийлэх болон кибер аюулгүй байдлыг хангах үйл ажиллагааны талаар мэдлэг олгох сургалтын материалыг боловсруулж, сургалт, мэдээлэл хийх.

3.2.14. Давуу эрхтэй хэрэглэгчдийн бүртгэл, эрхийн мэдээлэлд тогтмол хяналт тавьж, эрхийн хэрэгцээ, шаардлага болон албан үүрэгт өөрчлөлт орсон тохиолдолд холбогдох эрхийг шинэчлэх, хязгаарлах, цуцлах арга хэмжээг тухай бүр авна.

3.2.15. Серверийн өрөөнд нэвтрэх эрх бүхий албан тушаалтнуудыг жагсаалтыг гаргаж, батлуулах.

3.3. Мэдээллийн технологи, сүлжээ хариуцсан нэгж:

3.3.1. Байгууллагын хэмжээнд ашиглагдаж буй мэдээллийн технологийн тоног төхөөрөмжийг (хавсралт маягт-01) бүртгэж, тоног төхөөрөмжийн найдвартай, тасралтгүй, хэвийн ажиллагаанд хяналт тавин, шаардлагатай засвар, үйлчилгээ болон бусад зохион байгуулалтын арга хэмжээг тухай бүр авч, хэрэгжүүлж тэмдэглэл (хавсралт маягт-03) хөтлөн, Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр хүргүүлэх.

3.3.2. Байгууллагын хэмжээнд шаардлагатай мэдээллийн технологийн дэд бүтцийг бий болгох, өөрчлөх, шинэчлэх, засвар үйлчилгээ, холболт, тохиргоо хийх тохиолдолд Кибер аюулгүй байдал хариуцсан нэгжээс санал авч, улсын бүртгэлийн байгууллагын даргад танилцуулан шийдвэрлүүлж, гүйцэтгэх, хэвийн найдвартай, тасралтгүй ажиллагааг хангаж, шаардлагатай зохион байгуулалтын арга хэмжээг тухай бүр авч хэрэгжүүлэн, энэ талаар тэмдэглэл (хавсралт маягт - 02) хөтлөн Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр хүргүүлэх.

3.3.3. Байгууллагын мэдээллийн сүлжээний найдвартай, тасралтгүй, хэвийн ажиллагааг хангах, шаардлагатай зохион байгуулалтын арга хэмжээг тухай бүр авч хэрэгжүүлэх, нэмэлт, засвар, үйлчилгээ, өөрчлөлт, шинэчлэлт, тохиргоо хийсэн талаар тэмдэглэл (хавсралт маягт - 04) хөтлөх, бүтцийн физик, логик зураглал (топологи)-ыг боловсруулах, өргөтгөл, шинэчлэлт, өөрчлөлт хийгдсэн даруй шинэчилж улсын бүртгэлийн байгууллагын даргаар батлуулах, энэ талаар Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр мэдэгдэх.

3.3.4. Байгууллагын хэмжээнд ашиглагдаж байгаа болон шинээр үйл ажиллагаанд нэвтрүүлж буй мэдээллийн системүүдийн бүртгэл, судалгааг хөтөлж, хэвийн найдвартай, тасралтгүй ажиллагааг хангах, шаардлагатай зохион байгуулалтын арга хэмжээг авч хэрэгжүүлэх, нэмэлт, засвар, өөрчлөлт, шинэчлэлт, хөгжүүлэлтийг тухай бүр хийж, тэмдэглэл (хавсралт маягт - 05) хөтлөн Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр хүргүүлэх.

3.3.5. Байгууллагын хэмжээнд ашиглагдаж буй мэдээллийн технологийн тоног төхөөрөмжийн бүртгэл, судалгааг гаргаж, холбогдох мэдээллийг нэгтгэн бүртгэлжүүлж, тогтоосон хугацаанд шинэчлэн хөтөлнө.

3.3.6. Байгууллагын хэмжээнд ашиглагдаж байгаа ашиглалтын хугацаа дууссан, ашиглалтаас хасах мэдээллийн технологийн тоног төхөөрөмжийн судалгааг нэгтгэн, жил бүр бүртгэлээс хасах ажлыг холбогдох нэгжүүдтэй хамтран зохион байгуулж, дүнг Кибер аюулгүй байдал хариуцсан нэгжид хүргүүлэх.

3.3.7. Байгууллагын хэмжээнд мэдээлэл солилцох сервисийн бүртгэл (хавсралт маягт – 06) хөтөлж, нэмэлт, засвар, өөрчлөлт хийгдсэн тухай бүрд Кибер аюулгүй байдал хариуцсан нэгжид мэдэгдэх.

3.3.8.Байгууллагын цахим мэдээллийн сангийн хэвийн найдвартай, тасралтгүй ажиллагааг хангах, шаардлагатай зохион байгуулалтын арга хэмжээг авч хэрэгжүүлэх, нэмэлт, засвар, өөрчлөлт, шинэчлэлт, хөгжүүлэлт хийсэн талаар тэмдэглэл (хавсралт маягт - 07) хөтлөн Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр хүргүүлэх.

3.3.9.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудитын үр дүнд үндэслэн эрсдэлийг бууруулахад чиглэсэн арга хэмжээг холбогдох нэгжүүдтэй хамтран хэрэгжүүлнэ.

3.3.10.Байгууллагын хэмжээнд ашиглагдаж буй мэдээллийн систем, сүлжээг халдлага, зөрчил, саатлын үед сэлгэн ажиллах боломжтой байхаар зохион байгуулна.

3.3.11.Байгууллагын мэдээллийн системийн хөгжүүлэлтийг бусад хэрэглэгчээр гүйцэтгүүлэх тохиолдолд оюуны өмчийн эрхийг хамгаалах, төрийн болон албаны нууцыг хамгаалах, шаардлагатай арга хэмжээг авч хэрэгжүүлэн, Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр мэдэгдэх.

3.3.12.Байгууллагад зохиогчийн эрхийн зөрчилгүй программ хангамж, хөгжүүлэлтийн сан, аюулгүй байдлын шаардлага хангасан тоног төхөөрөмжийг ашиглах, энэ талаар санал боловсруулан, шийдвэрлүүлэх, ашиглалтын талаар бүртгэл, тэмдэглэл хөтлөн Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр хүргүүлэх.

3.3.13.Байгууллагын мэдээллийн систем, мэдээллийн сүлжээнд нэмэлт, засвар, шинэчлэлт, өөрчлөлт хийх, буцаах тохиолдолд холбогдох нэгж, албан тушаалтнаас санал авсны үндсэн дээр өөрчлөлтийг хэрэгжүүлэх, энэ талаар бүртгэл, тэмдэглэл хөтлөн Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр хүргүүлэх.

3.3.14.Мэдээллийн сан, систем, программ хангамж, сүлжээний хандалт, хэрэглэгчийн болон аюулгүй байдлын үйл ажиллагааны талаар дараах үйлдлийн бүртгэлийг хөтөлнө.

- 3.3.11.1.нэвтрэх оролдлого хийсэн, нэвтэрсэн тухай;
- 3.3.11.2.давуу эрхийн хандалт;
- 3.3.11.3.нууц үгийн өөрчлөлт;
- 3.3.11.4.үйлдлийн бүртгэлийг өөрчлөх, устгах;
- 3.3.11.5.мэдээллийн нэгдсэн санд хандах эрх олгох, өөрчлөх, хүчингүй болгох;
- 3.3.11.6.хэрэглэгчийн нэр, системд нэвтрэх нэр буюу ID;
- 3.3.11.7.мэдээллийн нэгдсэн санд нэвтэрсэн, гарсан огноо;
- 3.3.11.8.хандсан хаяг, төхөөрөмжийн мэдээлэл;
- 3.3.11.9.хандалтын үргэлжлэх хугацаа;
- 3.3.11.10.гүйцэтгэсэн үйлдэл, огноо;
- 3.3.11.11.гүйцэтгэсэн үйлдлийн үр дүн.

3.3.15.Байгууллагын цахим мэдээллийн сан, мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлд нэвтрэхэд Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр мэдэгдэж, зөвшөөрөл авах бөгөөд холбогдох хууль, дүрэм, журамд заасан хугацаанд хадгална.

3.3.16.Байгууллагын мэдээллийн систем, мэдээллийн сүлжээнд ашиглагдаж буй үйлдлийн систем, программ хангамжийн шинэчлэлтийг зөвшөөрөгдсөн албан ёсны эх үүсвэрээс авч, суурилуулахаас өмнө тухайн шинэчлэлт нь мэдээллийн систем, мэдээллийн сүлжээний хэвийн ажиллагаа болон байгууллагын кибер аюулгүй байдалд сөргөөр нөлөөлөх эсэхийг шалган, баталгаажуулсны дараа суурилуулж, шинэчлэлт хийнэ.

3.3.17.Кибер аюулгүй байдал хариуцсан нэгжид мэдээллийн систем, цахим мэдээллийн сан, мэдээллийн сүлжээ, галт хана төхөөрөмжийн үйлдлийн бүртгэлийг нэгтгэн цуглуулж, дүн шинжилгээ хийх орчин, нөхцөлийг бүрдүүлэн өгч, цагийн нэгдсэн сервертэй холбосон байна.

3.3.18.Байгууллагын кибер аюулгүй байдал алдагдсаны улмаас хэвийн үйл ажиллагаа доголдсон тохиолдолд тухайн кибер орчныг орлуулан гүйцэтгэх нөөц горим (гар ажиллагаа, механик үйл ажиллагаа), хувилбарыг бүрдүүлсэн байна.

3.3.19.Кибер халдлага, зөрчилд өртсөн цахим мэдээллийн сан, мэдээллийн систем, мэдээллийн сүлжээг боломжит хамгийн бага хугацаанд нөөцлөлтөөс сэргээх орчин, нөхцөлийг бүрдүүлнэ.

3.3.20.Цахим мэдээллийн сан, мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийг нөхөн сэргээх үйл ажиллагааг гүйцэтгэж, хэвийн үйл ажиллагаанд оруулсан талаар тодорхой түвшний баримт нотолгоо, туршилтын үр дүнд үндэслэн кибер халдлага, зөрчилд өртөхөөс өмнөх үеийн хэвийн төлөвт эргэн шилжсэнийг шалган баталгаажуулна.

3.3.21. Кибер халдлага, зөрчил, нөхөн сэргээх үйл ажиллагаа, түүний явц, үр дүнгийн талаарх үнэн зөв мэдээллийг Кибер аюулгүй байдал хариуцсан нэгж болон холбогдох нэгж, албан тушаалтнуудад тухай бүр мэдэгдэж, дүнг Улсын бүртгэлийн байгууллагын даргад танилцуулна.

3.3.22.Мэдээллийн систем, мэдээллийн сүлжээний ачааллыг тогтмол хянаж, шаардлагатай зохион байгуулалтын арга хэмжээг хэрэгжүүлнэ.

3.3.23.Байгууллагын мэдээллийн сүлжээнд холбогдсон болон шинээр холбох компьютер, тоног төхөөрөмжийг MAC хаягаар бүртгэлжүүлэн, IP хаягийг гар аргаар тохируулан холбох, хэрэглэгч тус бүрээр бүртгэл (хавсралт маягт - 09)-ийг хөтлөн Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр хүргүүлэх.

3.3.24.Байгууллагын кибер орчин, цахим мэдээллийн сан, мэдээллийн систем, мэдээллийн сүлжээний эмзэг байдлыг бууруулах, шаардлагатай аюулгүй байдлын арга хэмжээ болон холбогдох хууль, дүрэм, журамд заасан арга хэмжээний хэрэгжилтийг хангаж, Кибер аюулгүй байдал хариуцсан нэгжтэй хамтран ажиллана.

3.3.25.Давуу эрхтэй хэрэглэгчдийн мэдээллийг хянах техникийн боломжийг бүрдүүлэх.

3.4.Сургалт хариуцсан нэгж:

3.4.1.Кибер аюулгүй байдал хариуцсан нэгжийн саналыг үндэслэн кибер аюулгүй байдлын талаар сургалтыг байгууллагын сургалтын төлөвлөгөөнд тусган боловсруулах.

3.4.2.Байгууллагын сургалтын төлөвлөгөөнд батлагдсан хуваарийн дагуу Кибер аюулгүй байдлын талаар сургалтыг нийт ажилтан, албан хаагчдыг хамруулан тухай бүр зохион байгуулж, танхимын болон цахим сургалтын бэлэн байдлыг хангаж, холбогдох байгууллага, нэгж, албан тушаалтанд мэдээлэл хүргүүлэх.

3.4.3.Сургалтын ирцийн бүртгэл хөтөлж, сургалтын тайланд тусгах.

3.5.Төв, орон нутгийн бүтцийн нэгжийн дарга:

3.5.1. Хариуцсан нэгжийн хэмжээнд ашиглаж байгаа мэдээллийн технологийн тоног төхөөрөмжийг бүртгэл (хавсралт маягт - 01), тоног төхөөрөмжийн бүртгэл, хяналтын хуудас (хавсралт маягт - 03)-ийг тогтмол хөтлөнө.

3.5.2.Хариуцсан нэгжийн хэмжээнд ашиглаж байгаа мэдээллийн сүлжээний тоног төхөөрөмж, кабелийг хаягжуулан бүртгэл хөтөлж, техникийн өрөө эсхүл сүлжээний тоног төхөөрөмжийн зориулалтын хайрцагт байршуулан, зөвшөөрөлгүй хандалтаас хамгаалан түгжих, лацдах.

3.5.3.Хариуцсан нэгжийн сүлжээний физик болон логик зураглалыг боловсруулж, нууцлал, аюулгүй байдлыг хангаж, сүлжээний бүтэц, тохиргоонд өөрчлөлт орсон тухай бүр шинэчлэн баталгаажуулах.

3.5.4.Техникийн өрөө нэвтрэх болон сүлжээний тоног төхөөрөмжийн зориулалтын хайрцгийг нээх эрх бүхий албан тушаалтнуудын жагсаалтыг гарган, баталж, хэрэгжилтэд хяналт тавих.

3.5.5.Шинээр томилогдсон болон шилжин ажиллаж буй ажилтан, албан хаагч нарт холбогдох хууль, дүрэм, журам зааврыг танилцуулан, тэмдэглэл хөтөлж, өдөр тутмын үйл ажиллагаанд мөрдлөг болгон, хяналт тавьж ажиллах.

3.5.6.Халагдсан, чөлөөлөгдсөн, шилжин томилогдсон, албан тушаал өөрчлөгдсөн ажилтан, албан хаагч нарын цахим мэдээллийн сан, мэдээллийн систем, мэдээллийн сүлжээнд хандах эрхийг хаалгах арга хэмжээг тухай бүр авах.

3.5.7.Байгууллагаас зохион байгуулж буй мэдээллийн аюулгүй байдлын сургалтад хамрагдах шаардлагатай ажилтан, албан хаагчдыг сургалтад хамрагдах нөхцөл, бололцоогоор тухай бүр хангах.

3.5.8.Хариуцсан нэгжийн хэмжээнд байгууллагын зөвшөөрснөөс бусад төрлийн программ хангамжийг албаны компьютер, техник хэрэгсэлд суулгаж, тохируулахгүй, ашиглахгүй байхад тогтмол хяналт тавьж ажиллах.

3.5.9.Хариуцсан нэгжийн хэмжээнд улсын бүртгэлийн байгууллагын баримталж буй кибер аюулгүй байдлын бодлого, холбогдох хууль, дүрэм, журам, заавар, зөвлөмжийг мөрдөх ажлыг зохион байгуулж, дүнг Кибер аюулгүй байдал хариуцсан нэгжид улирал бүрийн сүүлийн сарын 25-ны өдрийн дотор албан бичгээр хүргүүлэх.

3.6.Хэрэглэгч, бусад хэрэглэгч:

3.6.1.Улсын бүртгэлийн байгууллагын баримталж буй кибер аюулгүй байдлын бодлого, холбогдох хууль, дүрэм, журам, заавар, зөвлөмжийг мөрдөж ажиллах.

3.6.2.Өдөр тутмын үйл ажиллагаатай холбогдуулан үүссэн кибер халдлага, зөрчил, сэжигтэй тохиолдол бүрийг боломжит богино хугацаанд харьяа нэгжийн даргаар дамжуулан, Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр мэдээлэх.

3.6.3.Байгууллагын кибер орчин, цахим мэдээллийн сан, мэдээллийн систем, мэдээллийн сүлжээг зөвхөн албан хэрэгцээнд, холбогдох хууль, дүрэм, журам, заавар, зөвлөмжийн дагуу ашиглах.

3.6.4.Байгууллагаас зохион байгуулж буй мэдээллийн аюулгүй байдлын сургалтад тухай бүр хамрагдах.

3.6.5.Байгууллагын зөвшөөрснөөс бусад төрлийн программ хангамжийг албаны компьютер, техник хэрэгсэлд суулгаж, тохируулахгүй, ашиглахгүй байх.

3.6.6.Байгууллагаас өөрт олгосон мэдээллийн технологийн тоног төхөөрөмж, хандах эрх, нэвтрэх нэр, нууц үгийн аюулгүй байдал, нууцлалыг тогтмол хангаж, хувийн зорилгоор ашиглахгүй, бусдад дамжуулахгүй байх.

3.6.7.Бусдын хандах эрх, нэвтрэх нэр, нууц үгийг ашиглахгүй байх.

3.6.8.Ажлын байрыг түр хугацаагаар орхих үед компьютерыг тухай бүр түгжих, системийн нууцлал, бүрэн бүтэн байдлыг тогтмол хангаж ажиллах.

3.6.9.Цахим шуудан, мессеж болон бусад сувгаар ирсэн сэжигтэй холбоос, хавсралт файлыг нээж харахгүй байх, шууд устгах.

3.6.10.Байгууллагын мэдээллийг хадгалсан баримт бичиг, зөөврийн хадгалах төхөөрөмж, компьютер, техник хэрэгслийг гадагш авч гарах үед хариуцсан бүтцийн нэгжийн даргаас зөвшөөрөл авч, тэмдэглэл (хавсралт маягт - 10)-ийг хөтлөн, Кибер аюулгүй байдал хариуцсан нэгжид тухай бүр мэдэгдэх.

3.7.Давуу эрхтэй хэрэглэгч:

3.7.1.Улсын бүртгэлийн байгууллагын даргын тушаал, шийдвэрийн дагуу олгогдсон мэдээллийн систем, сүлжээ, программ хангамж, цахим мэдээллийн сан, галт хана, байгууллагын бусад үйл ажиллагаанд ашиглагдах давуу эрхтэй хэрэглэгчийн эрхийг зөвхөн холбогдох хууль, дүрэм, журамд заасны дагуу ашиглана.

3.7.2.Хариуцсан мэдээллийн систем, мэдээллийн сүлжээ, сервер, цахим мэдээллийн сан, хамгаалалтын төхөөрөмж болон бусад мэдээллийн технологийн тоног төхөөрөмж, программ хангамжид тохиргоо, засвар, үйлчилгээ хийнэ.

3.7.3.Давуу эрхтэй хэрэглэгчийн эрх болон хэрэглэгчийн эрхийг тусад нь ашиглах бөгөөд өдөр тутмын энгийн үйл ажиллагаанд давуу эрхийг ашиглахгүй.

3.7.4.Давуу эрхтэй хэрэглэгчийн нэвтрэх нэр, нууц үг, баталгаажуулалтын мэдээллийн нууцлал, аюулгүй байдлыг бүрэн хангаж, бусдад дамжуулах, дундын хэрэгцээнд ашиглах болон үүсэж болзошгүй аливаа эрсдэлээс урьдчилан сэргийлнэ.

Дөрөв. Серверийн өрөө

4.1. Байгууллагын мэдээллийн систем, сүлжээ, тоног төхөөрөмж байрлаж буй серверийн өрөөнд нэвтрэхэд кибер аюулгүй байдал хариуцсан нэгжид тухай бүр мэдэгдэж, бүртгэлийн дэвтэр хөтөлнө.

4.2. Серверийн өрөө нь дараах шаардлагыг хангасан байна:

4.2.1. өрөөний хаалга зориулалтын цоож, лацтай байх;

4.2.2. галын дохиоллын системтэй байх;

4.2.3. температур, чийгшил, хяналтын камер зэрэг орчны нөхцөлийг хянах, нэгдсэн өрөө, тасалгаа, хяналт удирдлагатай байх;

4.2.4. орох, гарах хаалганы дэргэд дүрст хяналтын системтэй байх;

4.2.5. галын хор, гал унтраах хэрэгслийг байршуулан ажиллагааг тухай бүр шалгаж тэмдэглэл хөтлөх;

4.2.6. серверийн өрөөнд байршиж буй сүлжээний тоног төхөөрөмжүүдийн порт, кабелийн хоёр талын үзүүрт тэмдэглэгээ хаягжилтыг зайлшгүй хийсэн байх;

4.2.7. серверийн өрөөнд зөвхөн эрх бүхий ажилтан, албан хаагч нэвтрэх бөгөөд нэвтрэх эрх бүхий ажилтан, албан хаагчийн батлагдсан жагсаалтыг үндэслэн бүртгэлийг тухай бүр хөтөлнө. (Хавсралт маягт - 08)

4.2.8. серверийн өрөөг цэвэрлэх хуваарийг боловсруулан батлуулж, тэмдэглэл хөтлөх, шаардлагатай арга хэмжээг Мэдээллийн технологи, сүлжээ хариуцсан нэгж хариуцан гүйцэтгэнэ;

4.2.9. серверийн өрөөнд зориулалтын бус бараа, материал, хувийн эд зүйлс байршуулахыг хориглоно;

4.2.10. серверийн өрөөний тасралтгүй ажиллагааг хангах, тэжээлийн нөөц цахилгаан үүсгүүр (генератор), тог баригч (UPS)-ийн хэвийн, тасралтгүй, найдвартай ажиллагааг хангаж, үзлэг, үйлчилгээг тогтмол хийж тэмдэглэл хөтөлнө.

Тав. Хориглох

5.1. Байгууллагын кибер орон зайд кибер аюулгүй байдал хариуцсан нэгжийн зөвшөөрөлгүйгээр хувийн компьютер, гар утас, таблет болон бусад төхөөрөмж, зөөврийн мэдээлэл тээгч (флаш диск, зөөврийн хатуу диск гэх мэт) төхөөрөмжийг байгууллагын мэдээллийн систем, сүлжээ, цахим мэдээллийн нэгдсэн санд холбох, ашиглах, мэдээлэл хадгалах, боловсруулах, дамжуулахыг хориглоно.

5.2. Байгууллагын зөвшөөрөгдсөнөөс бусад төрлийн болон ажил үүрэгтэй холбоогүй, байгууллагын үйл ажиллагаанд үл хамаарах программ хангамжийг албаны компьютер, техник хэрэгсэлд суулгаж, ашиглах, тоглоом, цахим мөрийтэй тоглоом тоглох.

5.3. Кибер аюулгүй байдлыг хангах, хадлага, зөрчлөөс урьдчилан сэргийлэх аливаа программ хангамжийг давуу эрхтэй хэрэглэгчийн зөвшөөрөлгүйгээр устгах, тохиргоог өөрчлөх.

5.4. Цахим мэдээллийн сан, мэдээллийн сүлжээ, мэдээллийн систем, аюулгүй байдлыг хангах төхөөрөмжөөс аливаа хэлбэрээр өгөгдөл устгах, өөрчлөх, засварлах, хуулбарлах, шилжүүлэх.

5.5. Албан хэрэгцээний компьютер, техник хэрэгсэлд хувийн цахим шуудан, "Cloud", олон нийтийн сүлжээ болон зөвшөөрөгдөөгүй бусад сувгийг ашиглах, албаны болон нууцлалтай мэдээлэл дамжуулах, хадгалах, байршуулах, зөөвөрлөх.

5.6.Бусдын хандах эрх, нэвтрэх нэр, нууц үг, цахим гарын үсэг, цахим гарын үсгийн гэрчилгээ тээгч төхөөрөмж /токен/ болон бусад нэвтрэх хэрэгслийг ашиглах, бусдад дамжуулж, хамтран ашиглах.

5.7.Байгууллагын мэдээллийн систем, сүлжээ, мэдээллийн технологийн тоног төхөөрөмжийн тохиргоо, хамгаалалтын бодлогыг кибер аюулгүй байдал хариуцсан нэгжийн зөвшөөрөлгүйгээр өөрчлөх.

5.8.Байгууллагын дотоод, гадаад сүлжээнд Кибер аюулгүй байдал хариуцсан нэгжээс зөвшөөрөл авалгүйгээр аливаа төхөөрөмж холбох.

5.9.Байгууллагын мэдээллийн аюулгүй байдлын хяналт, мониторинг, аудит, бүртгэл, хамгаалалтын тохиргоо болон бусад хамгаалалтын үйл ажиллагааг зориудаар тойрч гарах (Bypass), идэвхгүй болгох, өөрчлөлт оруулах, хэвийн үйл ажиллагааг алдагдуулах, доголдуулах.

5.10.Цахим мэдээллийн сан дахь өгөгдөл, мэдээлэлд зөвшөөрөлгүйгээр хандах, хуулбарлах, хэвлэх, фото зураг авах, дуу, дүрсний бичлэг хийх, тараах, бусдад дамжуулах.

5.11.Албан хэрэгцээний компьютер, техник хэрэгсэлд үл мэдэх, баталгаагүй эх сурвалжаас цахим хэлбэрээр ирсэн холбоос, хавсралт файл, программ хангамжийг татаж авах, нээх, суулгах, ажиллуулах.

5.12.Лог файл, нөөц хуулбар /Backup/-ыг зөвшөөрөлгүйгээр өөрчлөх, устгах, гэмтээх.

5.13.Давуу эрхтэй хэрэглэгчийн эрх, администраторын эрх болон бусад өндөр түвшний хандалтын эрхийг албан хэрэгцээнээс бусад зорилгоор ашиглах, бусдад дамжуулах, ашиглуулах.

5.14.Өөрт олгогдсон хандалтын эрхийг холбогдох тушаал, шийдвэр, хариуцсан нэгжийн зөвшөөрөлгүйгээр эрхийн түвшинг нэмэгдүүлэх (Privilege escalation), бусад хэрэглэгчийн эрх, бүртгэл, мэдээлэлд зөвшөөрөлгүйгээр хандах, хамгаалалтын хязгаарлалтыг идэвхгүй болгох, тойрч гарах.

Зургаа. Хариуцлага

6.1.Энэхүү журмаар хүлээсэн үүргээ биелүүлээгүй албан хаагчдад холбогдох хууль, дүрэм, журам болон байгууллагын хөдөлмөрийн дотоод журамд заасан хариуцлага хүлээлгэнэ.