Төсөл

МОНГОЛ УЛСЫН ХУУЛЬ

2021 оны ...дугаар сарын ... -ны өдөр

Улаанбаатар хот

КИБЕР АЮУЛГҮЙ БАЙДЛЫН ТУХАЙ

НЭГДҮГЭЭР БҮЛЭГ
НИЙТЛЭГ ҮНДЭСЛЭЛ

1 дүгээр зүйл.Хуулийн зорилт

1.1.Энэ хуулийн зорилт нь кибер аюулгүй байдлыг хангах үйл ажиллагааны тогтолцоо, зарчим, эрх зүйн үндсийг тогтоох, кибер орчин дахь мэдээллийн бүрэн бүтэн, хүртээмжтэй, нууцлагдсан байдлыг хангахтай холбогдсон харилцааг зохицуулахад оршино.

2 дугаар зүйл.Кибер аюулгүй байдлын тухай хууль тогтоомж

2.1.Кибер аюулгүй байдлын тухай хууль тогтоомж нь Монгол Улсын Үндсэн хууль, Үндэсний аюулгүй байдлын тухай хууль, Зэвсэгт хүчний тухай хууль, Төрийн болон албаны нууцын тухай хууль, Харилцаа холбооны тухай хууль, Тагнуулын байгууллагын тухай хууль, Байгууллагын нууцын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай хууль, Нийтийн мэдээллийн тухай хууль, энэ хууль болон эдгээр хуультай нийцүүлэн гаргасан хууль тогтоомжийн бусад актаас бүрдэнэ.

2.2.Монгол Улсын олон улсын гэрээнд энэ хуульд зааснаас өөрөөр заасан бол олон улсын гэрээний заалтыг дагаж мөрдөнө.

3 дугаар зүйл.Хуулийн үйлчлэх хүрээ

3.1.Энэ хууль нь кибер аюулгүй байдлыг хангахтай холбогдон төр, хүн, хуулийн этгээдийн хооронд үүсэх харилцааг уялдуулан зохицуулах, зохион байгуулах, хяналтыг хэрэгжүүлэх харилцаанд үйлчилнэ.

3.2.Хуульд өөрөөр заагаагүй бол Монгол Улсын мэдээллийн систем, сүлжээгээр дамжуулан үйл ажиллагаа явуулж байгаа гадаадын иргэн, харьяалалгүй хүн, гадаадын болон гадаадын хөрөнгө оруулалттай хуулийн этгээд нэгэн адил мөрдөнө.

3.3. Төрийн аудитын байгууллагаас аудит хийхтэй холбогдсон харилцаанд энэ хуулиар зохицуулсан мэдээллийн аюулгүй байдлын аудитын харилцаа хамаарахгүй.

4 дүгээр зүйл.Хуулийн нэр томьёоны тодорхойлолт

4.1.Энэ хуульд хэрэглэсэн дараах нэр томьёог дор дурдсан утгаар ойлгоно:

4.1.1.“кибер аюулгүй байдал” гэж кибер орчинд мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдал хангагдсан байхыг;

4.1.2.“кибер орчин” гэж мэдээлэлд хандах, нэвтрэх, цуглуулах, түүнийг боловсруулах, хадгалах, ашиглах боломж олгож буй мэдээллийн систем, мэдээллийн сүлжээний орчныг;

4.1.3.“бүрэн бүтэн байдал” гэж мэдээллийг устгах, зөвшөөрөлгүй өөрчлөгдөхөөс хамгаалсан байхыг;

4.1.4.“нууцлагдсан байдал” гэж зөвшөөрөгдөөгүй нөхцөлд мэдээлэлд хандах, нэвтрэх боломжгүй байхыг;

4.1.5.“хүртээмжтэй байдал” гэж зөвшөөрөгдсөн хүрээнд мэдээлэлд хандах, нэвтрэх, цуглуулах, ашиглах боломжтой байхыг;

4.1.6.“мэдээллийн систем” гэж Нийтийн мэдээллийн тухай хуулийн 4.1.1-т заасныг;

4.1.7.“мэдээллийн сүлжээ” гэж Нийтийн мэдээллийн тухай хуулийн 4.1.2-т заасныг;

4.1.8. “хүний эмзэг мэдээлэл” гэж Хүний хувийн мэдээлэл хамгаалах тухай хуулийн 4.1.2-т заасныг;

4.1.9 “кибер аюулгүй байдлын эрсдэлийн үнэлгээ” гэж цахим мэдээлэл, мэдээллийн систем, сүлжээний кибер аюулгүй байдал алдагдаж болох аюул занал, тохиолдох магадлал, эмзэг байдлын түвшнийг тогтоох, түүнээс үүсэх үр дагавар, эрсдэлийг бууруулах, урьдчилан сэргийлэх арга хэмжээг тодорхойлох мэргэшсэн үйл ажиллагааг;

4.1.10.“мэдээллийн аюулгүй байдлын аудит” гэж кибер аюулгүй байдлын хууль тогтоомж, холбогдох журам, стандартад нийцсэн эсэхэд шинжилгээ хийж дүгнэлт гаргах, зөвлөмж өгөх хараат бус хөндлөнгийн мэргэжлийн үйл ажиллагааг;

4.1.11.“мэдээллийн системийн үйлдлийн бүртгэл” гэж тухайн мэдээллийн системд хандсан, нэвтэрсэн, боловсруулсан, цуглуулсан, ашигласан үйлдэл, цаг хугацааг тодорхойлох бүртгэлийг;

4.1.12.“кибер аюулгүй байдлын зөрчил” гэж мэдээллийн системийн нууцлагдсан, бүрэн бүтэн, хүртээмжтэй байдалд заналхийлж буй аливаа үйлдэл, эс үйлдлийг;

4.1.13.“кибер халдлага” гэж мэдээллийн систем, сүлжээний кибер аюулгүй байдлыг алдагдуулах зорилго бүхий үйлдлийг;

4.1.14.“үндэсний хэмжээний кибер халдлага” гэж онц чухал мэдээллийн дэд бүтэцтэй байгууллагын эсрэг чиглэсэн кибер халдлагыг;

4.1.15.“кибер халдлага, зөрчилтэй тэмцэх төв” гэж кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу үйлдэл үзүүлэх,

мэдээллийн системийг нөхөн сэргээх үйл ажиллагааг зохицуулж, мэргэжлийн удирдлагаар хангах үндсэн чиг үүрэг бүхий этгээдийг;

4.1.16.“онц чухал мэдээллийн дэд бүтэцтэй байгууллага” гэж кибер аюулгүй байдал нь алдагдсанаар хэвийн үйл ажиллагаа нь доголдож Монгол Улсын үндэсний аюулгүй байдал, нийгэм, эдийн засагт хохирол учруулж болох мэдээллийн систем, мэдээллийн сүлжээ бүхий байгууллагыг;

4.1.17.“төрийн өмчит хуулийн этгээд” гэж Төрийн болон орон нутгийн өмчийн тухай хуулийн 13 дугаар зүйлд заасныг.

5 дугаар зүйл.Кибер аюулгүй байдлыг хангах үйл ажиллагааны зарчим

5.1.Кибер аюулгүй байдлыг хангах үйл ажиллагаанд Үндэсний аюулгүй байдлын тухай хуулийн 4.1-т зааснаас гадна дараах зарчмыг баримтална:

5.1.1.нэгдмэл удирдлагатай байх;

5.1.2.шинжлэх ухаан, дэвшилтэт техник, технологи, инновацад тулгуурласан байх;

5.1.3.үндэсний бүтээгдэхүүн, үйлчилгээ, хүний нөөцийн чадавхыг дэмжих;

5.1.4.эрсдэлийн үнэлгээнд тулгуурлах;

5.1.5.төр, хувийн хэвшлийн түншлэлд тулгуурлах;

5.1.6.олон улсын хамтын ажиллагааг хөгжүүлэх.

ХОЁРДУГААР БҮЛЭГ

КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ҮЙЛ АЖИЛЛАГАА

6 дугаар зүйл.Кибер аюулгүй байдлыг хангах үйл ажиллагааны чиглэл

6.1.Кибер аюулгүй байдлыг хангах үйл ажиллагааг дараах чиглэлээр хэрэгжүүлнэ:

6.1.1.кибер аюулгүй байдлын удирдлага, зохион байгуулалт;

6.1.2.кибер аюулгүй байдлыг хангах техник, технологийн арга хэмжээ;

6.1.3.кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, соён гэгээрүүлэх арга хэмжээ;

6.1.4.кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох арга хэмжээ.

7 дугаар зүйл.Кибер аюулгүй байдлыг хангах нийтлэг журам

7.1.Энэ хуулийн 15.1, 16.2, 18.1-т заасан хуулийн этгээд нь кибер аюулгүй байдлыг хангах нийтлэг журамд нийцсэн кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журамтай байна.

7.2.Кибер аюулгүй байдлыг хангах нийтлэг журмыг харилцаа холбооны асуудал хариуцсан төрийн захиргааны байгууллага баталж, хэрэгжилтэд хяналт тавина.

7.3.Кибер аюулгүй байдлыг хангах нийтлэг журамд дараах асуудлыг тусгана:

7.3.1.кибер аюулгүй байдлыг хангах бүтэц, зохион байгуулалт;

7.3.2.кибер аюулгүй байдлыг хангах талаар хэрэгжүүлэх арга хэмжээ, үйл ажиллагааны болон техник технологийн шаардлага;

7.3.3.кибер аюулгүй байдлыг хангах талаар зохион байгуулах сургалт, мэдээлэл, зөвлөмж түгээх шаардлага;

7.3.4.кибер аюулгүй байдлын эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудит хийлгэх үеийн хэм хэмжээ, тэдгээрийн мөрөөр хэрэгжүүлэх арга хэмжээ;

7.3.5.бусад шаардлага.

8 дугаар зүйл.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ

8.1.Кибер аюулгүй байдлын эрсдэлийн үнэлгээг олон улсын стандартын байгууллага, мэргэжлийн холбоо, эсхүл түүнтэй дүйцэхүйц байгууллагаас олгосон хүчин төгөлдөр гэрчилгээ бүхий ажилтантай хуулийн этгээд харилцаа холбооны асуудал хариуцсан төрийн захиргааны байгууллагад бүртгүүлснээр хийнэ.

8.2.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх журмыг харилцаа холбооны асуудал хариуцсан төрийн захиргааны байгууллага батална.

8.3.Энэ хуулийн 8.2-д заасан журмаар эрсдэлийн үнэлгээ хийх этгээдийг бүртгэх, эрсдэлийн үнэлгээ хийх аргачлалтай холбогдох харилцааг зохицуулна.

8.4.Төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон байгууллага болон онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээдийн кибер аюулгүй байдлын эрсдэлийн үнэлгээг тагнуулын байгууллага эсхүл тагнуулын байгуулагын зөвшөөрснөөр энэ хуулийн 8.1-т заасан хуулийн этгээд хийнэ.

8.5.Энэ хуулийн 8.4-д зааснаас бусад хуулийн этгээдийн кибер аюулгүй байдлын эрсдэлийн үнэлгээг энэ хуулийн 8.1-т заасны дагуу бүртгүүлсэн хуулийн этгээд хийж болно.

8.6.Кибер аюулгүй байдлын эрсдэлийн үнэлгээний тайланг хүлээн авсан холбогдох байгууллага, албан тушаалтан нууцлалыг чандлан хадгалж, задруулахгүй байх үүрэг хүлээнэ.

9 дүгээр зүйл.Мэдээллийн аюулгүй байдлын аудит

9.1.Мэдээллийн аюулгүй байдлын аудитыг үндэсний аюулгүй байдлыг хангах тусгайлсан чиг үүрэгтэй байгууллага, онц чухал мэдээллийн дэд бүтэцтэй байгууллага, төрийн өмчит хуулийн этгээд нь энэ хуульд заасан хугацаанд эсхүл эрх бүхий байгууллагаас шаардсан тохиолдолд хийлгэнэ.

9.2.Мэдээллийн аюулгүй байдлын аудит хийх эрх хүссэн хуулийн этгээд нь дор дурдсан шаардлагыг хангасан байна:

9.2.1.Монгол Улсад бүртгэлтэй хуулийн этгээд байх;

9.2.2.мэдээллийн аюулгүй байдлын аудит хийх эрх бүхий орон тооны ажилтантай байх;

9.2.3.мэдээллийн аюулгүй байдлын аудит хийх эрх бүхий ажилтан нь ижил төрлийн аудит хийх эрх бүхий хуулийн этгээдэд зэрэгцсэн гэрээ буюу контракт байгуулан ажилладаггүй байх;

9.2.4.хуульд заасан бусад.

9.3.Мэдээллийн аюулгүй байдлын аудит хийх эрх хүссэн хуулийн этгээд нь эрх авах тухай хүсэлтийг дараах баримт бичгийн бүрдлийн хамт харилцаа холбооны асуудал хариуцсан төрийн захиргааны байгууллагад хүргүүлнэ.

9.3.1.мэдээллийн аюулгүй байдлын аудит хийх эрх хүссэн тухай хүсэлт;

9.3.2.хуулийн этгээдийн улсын бүртгэлийн гэрчилгээ;

9.3.3. мэдээллийн аюулгүй байдлын аудитын ажилтны мэргэшсэн байдлыг нотлох олон улсын стандартын байгууллага, мэргэжлийн холбоо, эсхүл түүнтэй дүйцэхүйц байгууллагаас олгосон хүчин төгөлдөр гэрчилгээ;

9.3.4.мэдээллийн аюулгүй байдлын аудит хийх эрх бүхий ажилтны хөдөлмөрийн харилцааг нотолсон баримт бичиг.

9.4.Эрх олгох байгууллага нь хүсэлтийг хүлээн авсан өдрөөс хойш ажлын 10 хоногт багтаан шийдвэрлэнэ.

9.5. Мэдээллийн аюулгүй байдлын аудит хийх эрхийг дараах тохиолдолд хүчингүй болгоно:

9.5.1.аудитын үйлчилгээ эрхлэх эрх авахдаа хуурамч баримт бичиг бүрдүүлсэн нь тогтоогдсон;

9.5.2.хуулийн этгээд татан буугдсан;

9.5.3.хуулийн этгээд эрхээ хүчингүй болгуулахаар хүсэлт гаргасан;

9.5.4.аудитын тайланг хуурамчаар үйлдсэн нь тогтоогдсон.

9.6.Мэдээллийн аюулгүй байдлын аудит хийх эрх авсан хуулийн этгээд дараах эрх, үүрэгтэй байна:

9.6.1.аудит хийхэд шаардлагатай үнэн зөв баримт, мэдээллээр хангахыг үйлчлүүлэгчээс шаардах;

9.6.2.үйлчлүүлэгч нь аудитын үйл ажиллагааг гүйцэтгэхэд шаардагдах баримт бичиг, мэдээллээр хангаагүй бол үйлчилгээ үзүүлэхээс татгалзах;

9.6.3.үйлчлүүлэгчийн гомдлыг хянан шийдвэрлэхэд шаардлагатай баримтыг эрх олгосон байгууллагад гарган өгөх;

9.6.4.мэдээллийн аюулгүй байдлын аудит хийх эрх бүхий ажилтан нь ажлаас гарсан, шинээр ажилд орсон тохиолдолд эрх олгосон байгууллагад ажлын таван өдрийн дотор мэдэгдэх.

9.7.Хуулийн этгээд нь мэдээллийн аюулгүй байдлын аудитаас бусад мэдээллийн технологи, мэдээллийн аюулгүй байдлын чиглэлээр үйлчилгээ үзүүлсэн бол тухайн байгууллагад 2 жилийн хугацаанд мэдээллийн аюулгүй байдлын аудит хийхийг хориглоно.

9.8.Эрх авсан этгээдтэй холбоотой үйлчлүүлэгчийн гомдлыг харилцаа холбооны асуудал хариуцсан төрийн захиргааны байгууллага шийдвэрлэнэ.

9.9.Энэ хуулийн 9.8-д заасан шийдвэрийг эс зөвшөөрвөл уг шийдвэрийг хүлээн авснаас хойш 30 хоногийн дотор шүүхэд гомдол гаргана.

9.10.Мэдээллийн аюулгүй байдлын аудитын тайлан мэдээллийг хүлээн авсан холбогдох байгууллага, албан тушаалтан нууцлалыг чандлан хадгалж, задруулахгүй байх үүрэг хүлээнэ.

ГУРАВДУГААР БҮЛЭГ
КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ТОГТОЛЦОО

10 дугаар зүйл.Засгийн газар

10.1.Засгийн газар кибер аюулгүй байдлыг хангах талаар дараах бүрэн эрхийг хэрэгжүүлнэ:

10.1.1.хөгжлийн бодлого төлөвлөлтийн баримт бичигт кибер аюулгүй байдлыг хангах талаар тусгах, хууль тогтоомжийн биелэлтийг зохион байгуулах;

10.1.2.үндэсний хэмжээний кибер халдлагын үед ажиллах төлөвлөгөө батлах;

10.1.3.кибер халдлага, зөрчилтэй тэмцэх үндэсний төв болон төрийн нэгдсэн төвийн дүрэм, зохион байгуулалтын бүтэц, орон тоо, ажиллах журмыг батлах;

10.1.4.онц чухал мэдээллийн дэд бүтэцтэй байгууллагын жагсаалтыг батлах;

10.1.5.төрийн мэдээллийн нэгдсэн сүлжээг байгуулах, ашиглах журам, түүнд холбогдох байгууллагын жагсаалтыг тагнуулын байгууллагын саналыг үндэслэн батлах;

10.1.6.кибер аюулгүй байдлыг хангахад чиглэсэн үйл ажиллагааг хэрэгжүүлэхэд шаардагдах хөрөнгийг улсын төсөвт тусган шийдвэрлүүлэх;

10.1.7.кибер аюулгүй байдлыг хангах чиглэлээр боловсролын тогтолцоог хөгжүүлэх.

11 дүгээр зүйл.Зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллага

11.1.Зэвсэгт хүчний кибер аюулгүй байдлын нэгжийн үйл ажиллагааг Зэвсэгт хүчний тухай хуулиар зохицуулна.

12 дугаар зүйл. Харилцаа холбооны асуудал хариуцсан төрийн захиргааны байгууллага

12.1.Харилцаа холбооны асуудал хариуцсан төрийн захиргааны байгууллага кибер аюулгүй байдлыг хангах талаар дараах эрх, үүргийг хэрэгжүүлнэ:

12.1.1.кибер аюулгүй байдлыг хангах тухай хууль тогтоомж, Засгийн газрын шийдвэрийг хэрэгжүүлэх, хяналт тавих ажлыг энэ хууль, холбогдох бусад хуульд заасны дагуу хэрэгжүүлэх;

12.1.2.кибер аюулгүй байдлын талаар хөгжлийн бодлого боловсруулах, хэрэгжилтийг зохион байгуулах;

12.1.3.кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлага, зохион байгуулалтаар хангах;

12.1.4.кибер аюулгүй байдлыг хангах талаар гадаад улсын болон олон улсын байгууллагатай хамтран ажиллах;

12.1.5.мэдээллийн аюулгүй байдлын аудит хийх эрх олгох;

12.1.6.мэдээллийн аюулгүй байдлын аудит хийх эрхийг олгох, түдгэлзүүлэх, хүчингүй болгох журмыг батлах, журмын хэрэгжилтэд хяналт тавих;

12.1.7.кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх журмын хэрэгжилтэд хяналт тавих, эрсдэлийн үнэлгээ хийх этгээдийг тагнуулын байгууллагаас санал авч, бүртгэх;

12.1.8.онц чухал мэдээллийн дэд бүтэцтэй байгууллагын жагсаалтыг Зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллага, Тагнуулын байгууллагатай хамтран боловсруулах;

12.1.9.кибер аюулгүй байдлыг хангах талаар санал, зөвлөмж өгөх, албан шаардлага хүргүүлэх, хэрэгжилтэд хяналт тавих;

12.1.10.кибер аюулгүй байдлыг хангах талаар шаардлагатай мэдээ, баримт бичгийг холбогдох байгууллагаас гаргуулан авах;

12.1.11.кибер аюулгүй байдлыг хангах чиглэлээр инновац, судалгаа, шинжилгээний үйл ажиллагаа явуулах;

12.1.12.кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, сургалт зохион байгуулах, соён гэгээрүүлэх арга хэмжээг хэрэгжүүлэх, холбогдох хууль тогтоомжийг сурталчлах;

12.1.13.кибер халдлага, зөрчилтэй тэмцэх төвүүдийн үйл ажиллагааг уялдуулан зохицуулах.

13 дугаар зүйл.Тагнуулын байгууллага

13.1.Тагнуулын байгууллага кибер аюулгүй байдлыг хангах талаар дараах эрх, үүргийг хэрэгжүүлнэ:

13.1.1.төрийн мэдээллийн нэгдсэн сүлжээг зохион байгуулж, кибер аюулгүй байдлыг хангах, сүлжээ ашиглах журмын хэрэгжилтэд хяналт тавих;

13.1.2.төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон болон онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээдийн кибер аюулгүй байдлыг хангах үйл ажиллагаанд хяналт тавих, тусгай зориулалттай техник болон программ хангамжийг шалган баталгаажуулах, дүгнэлт гаргах;

13.1.3.кибер аюулгүй байдлыг хангахад ашиглах тоног төхөөрөмж, программ хангамжийг шалган баталгаажуулах, дүгнэлт гаргах, шинжилгээ, судалгаа хийх тоон шинжилгээний лаборатори ажиллуулах;

13.1.4.төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон болон онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээдэд кибер аюулгүй байдлыг хангах талаар сургалт зохион байгуулах;

13.1.5.онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээдэд зээл, тусламж, хөрөнгө оруулалтаар хэрэгжих төсөл, хөтөлбөр, арга хэмжээнд кибер аюулгүй байдлыг хангах асуудлаар дүгнэлт гаргаж холбогдох байгууллагад санал, шаардлага хүргүүлэх;

13.1.6.кибер аюулгүй байдлыг хангах асуудлаар хуулийн этгээдэд зөвлөмж, шаардлага хүргүүлэх;

13.1.7.кибер аюулгүй байдлыг хангах нийтлэг журмыг энэ хуулийн Зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллага, Харилцаа холбооны асуудал хариуцсан төрийн захиргааны байгууллагатай хамтран боловсруулах;

13.1.8.кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх этгээдэд эрх олгоход санал өгөх;

13.1.9.үндэсний хэмжээний кибер халдлагын үед ажиллах төлөвлөгөө боловсруулах, хэрэгжилтэд хяналт тавьж ажиллах.

14 дүгээр зүйл.Цагдаагийн байгууллага

14.1.Цагдаагийн байгууллага кибер аюулгүй байдлыг хангах талаар дараах эрх, үүргийг хэрэгжүүлнэ:

14.1.1.кибер халдлага, зөрчилтэй холбоотой мэдээллийг харьяаллын дагуу холбогдох төвд мэдэгдэх;

14.1.2.кибер аюулгүй байдлыг хангах чиглэлээр үйл ажиллагаа явуулж буй байгууллага, төвтэй мэдээ, мэдээлэл солилцох, хамтран ажиллах;

14.1.3.кибер гэмт хэрэгтэй тэмцэх зорилгоор тоног төхөөрөмж, программ хангамжийг шалгах, шинжилгээ, судалгаа хийх тоон шинжилгээний лаборатори ажиллуулж болно.

15 дугаар зүйл.Төрийн өмчит хуулийн этгээд

15.1.Төрийн өмчит хуулийн этгээд кибер аюулгүй байдлыг хангах талаар дараах үүргийг хэрэгжүүлнэ:

15.1.1. кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам батлах;

15.1.2.кибер аюулгүй байдлыг хангах талаар эрх бүхий байгууллагаас өгсөн зөвлөмж, шаардлагыг биелүүлэх;

15.1.3.кибер халдлага, зөрчилд өртсөн, өртсөн байж болзошгүй тохиолдолд харьяаллын дагуу кибер халдлага, зөрчилтэй тэмцэх төвд даруй мэдэгдэх;

15.1.4.албан хаагчийн сургалт, ажиллах нөхцөл нийгмийн баталгааг хангах хөтөлбөрт кибер аюулгүй байдлыг хангах талаар тусгаж, хэрэгжүүлэх;

15.1.5.кибер аюулгүй байдлыг хангахад шаардагдах хөрөнгө, үйл ажиллагааны зардлыг төсөвт жил бүр тусгах;

15.1.6.мэдээллийн системийн үйлдлийн бүртгэлийг кибер аюулгүй байдлын нийтлэг журамд заасан хугацаанд хадгалах.

16 дугаар зүйл.Хуулийн этгээд

16.1.Хүний эмзэг мэдээллийг цуглуулж, боловсруулж буй хуулийн этгээдийн кибер аюулгүй байдлыг хангах арга хэмжээг Хүний хувийн мэдээллийг хамгаалах тухай хуулийн 20 дугаар зүйлээр зохицуулна.

16.2.Кибер орчинд дундын мэдээллийн систем боловсруулах, хадгалах, түгээх, цахим тооцооллын болон түүний хэвийн үйл ажиллагааг нь хангахад мэдээллийн технологийн чиглэлээр үйлчилгээ үзүүлж буй хуулийн этгээд дараах үүргийг хэрэгжүүлнэ:

16.2.1.кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам батлах;

16.2.2.кибер халдлагыг таслан зогсоох боломжгүй бол үндэсний төвд даруй мэдэгдэж туслалцаа авах;

16.2.3.мэдээллийн системийн үйлдлийн бүртгэлийг кибер аюулгүй байдлын нийтлэг журамд заасан хугацаанд хадгалах;

16.2.4.кибер аюулгүй байдлыг хангах үйл ажиллагааны талаар холбогдох төрийн байгууллагаас мэргэжил, арга зүйн туслалцаа авч хамтран ажиллах;

16.2.5.кибер аюулгүй байдлыг хангах үйл ажиллагаа хариуцсан нэгж, эсхүл албан тушаалтантай байх;

16.2.6.кибер аюулгүй байдлын эрсдэлийн үнэлгээг жил тутамд, эрх бүхий байгууллагын шаардсанаар тухай бүр хийлгэх;

16.2.7.мэдээллийн аюулгүй байдлын аудитыг эрх бүхий байгууллагын шаардсанаар тухай бүр хийлгэх, гарсан зөвлөмж, дүгнэлтийн дагуу холбогдох арга хэмжээг авч хэрэгжүүлэх;

16.2.8.шинээр нэвтрүүлсэн мэдээллийн технологийн бүтээгдэхүүн, үйлчилгээ болон тэдгээрийн өөрчлөлт, шинэчлэл бүрт кибер аюулгүй байдлын холбогдох шалгалт хийсэн байх;

16.2.9.кибер халдлага, зөрчилд өртсөн хэрэглэгчид даруй мэдэгдэх;

16.3.Энэ хуульд заасан хугацаанд олон улсын стандартын дагуу мэдээллийн аюулгүй байдлын аудит хийлгэсэн бол тухайн аудитын тайланг үндэслэн энэ хуулийн 16.2.7-д заасан үүргийг хангасанд тооцно.

16.4.Энэ хуулийн 16.1, 16.2-т зааснаас бусад хуулийн этгээд дараах эрхтэй:

16.4.1.кибер аюулгүй байдлыг хангах нийтлэг журмыг үйл ажиллагаандаа мөрдөх.

16.4.2.кибер халдлага зөрчлийн талаар үндэсний төвд мэдэгдэх, шаардлагатай үед туслалцаа авах;

16.4.3.эрх бүхий байгууллагаас хүргүүлсэн зөвлөмжийг дагах, шаардлагыг биелүүлэх;

16.4.4.хууль тогтоомжид заасан бусад.

17 дугаар зүйл.Иргэн

17.1.Иргэн кибер аюулгүй байдлыг хангах талаар дараах үүргийг хэрэгжүүлнэ:

17.1.1.иргэн өөрийн болон өөрийн асрамжид байгаа хүний кибер аюулгүй байдлыг хариуцах;

17.1.2.холбогдох байгууллагаас гаргасан зөвлөмжийг дагах, шаардлагыг биелүүлэх;

17.1.3.кибер халдлага, зөрчил үүссэн, үүссэн байж болзошгүй тохиолдолд Үндэсний төвд даруй мэдэгдэж болно;

17.1.4.хууль тогтоомжид заасан бусад.

18 дугаар зүйл.Онц чухал мэдээллийн дэд бүтэцтэй байгууллага

18.1.Онц чухал мэдээллийн дэд бүтэцтэй байгууллагад дараах чиглэлийн үйл ажиллагаа эрхэлдэг байгууллага хамаарна:

18.1.1.эрчим хүчний үйлдвэрлэл, дамжуулалт, түгээлт, хяналт удирдлагын систем бүхий байгууллага;

18.1.2.цэвэр, бохир ус, дулааны эх үүсвэр, төвлөрсөн хангамжийн болон түгээлт, хяналт удирдлагын систем бүхий байгууллага;

18.1.3.хоёр, гуравдугаар шатлалын эрүүл мэндийн байгууллага;

18.1.4.хүн, малын гоц халдварт өвчин судлах лаборатори;

18.1.5.эм, химийн хорт болон аюултай бодис үйлдвэрлэгч;

18.1.6.нэгдсэн төлбөр, тооцоо, гүйлгээний цахим систем бүхий банк санхүүгийн байгууллага;

18.1.7.зүй ёсны монопол болон давамгай байдалтай харилцаа холбоо, мэдээллийн технологийн үйлчилгээ эрхлэгч;

18.1.8.агаар, төмөр зам, усан зам, автозамын тээврийн зохицуулалт, хяналт удирдлагын систем бүхий байгууллага;

18.1.9.түлш, шатахуун импортлогч, үйлдвэрлэгч, түгээгч, стратегийн хүнс үйлдвэрлэгч, хадгалагч, түгээгч байгууллага;

18.1.10.мэдээлэл, шуурхай удирдлагын төв;

18.1.11.үндэсний олон нийтийн радио, телевиз;

18.1.12.үндсэн болон дэмжих мэдээллийн систем, суурь мэдээллийн сан хариуцагч байгууллага;

18.1.13.дата төв, түүний салбар болон нөөц төвийн үйл ажиллагаа хариуцсан байгууллага;

18.1.14.хилийн боомтын хяналт удирдлагын систем хариуцсан байгууллага.

18.2.Онц чухал мэдээллийн дэд бүтэцтэй байгууллага нь дараах үүргийг хэрэгжүүлнэ:

18.2.1.кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам батлах;

18.2.2.кибер халдлага, зөрчлийн үед дагаж мөрдөх төлөвлөгөө баталж хэрэгжүүлэх;

18.2.3.мэдээллийн аюулгүй байдлыг хангах талаар стандартыг нэвтрүүлэх;

18.2.4.кибер аюулгүй байдлыг хангах үйл ажиллагаа хариуцсан нэгж, эсхүл албан тушаалтантай байх;

18.2.5.кибер аюулгүй байдлын эрсдэлийн үнэлгээг жил тутамд эсхүл мэдээллийн систем, мэдээллийн сүлжээний өөрчлөлт хийгдэх бүрт хэсэгчлэн, эрх бүхий байгууллагын шаардсанаар тухай бүр хийлгэх;

18.2.6.мэдээллийн аюулгүй байдлын аудитыг дор хаяж хоёр жил тутамд нэг удаа хийлгэх;

18.2.7.мэдээллийн систем, мэдээллийн сүлжээний аюулгүй байдлыг хангахад шаардлагатай удирдлага, зохион байгуулалтын болон техникийн арга хэмжээ төлөвлөх, хэрэгжүүлэх;

18.2.8.кибер халдлага, зөрчлийг илрүүлэх, бүртгэх, таслан зогсоох мэдээллийн системтэй байх;

18.2.9.мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийг кибер аюулгүй байдлын нийтлэг журамд заасан хугацаанд хадгалах;

18.2.10.дараа жилийн нэгдүгээр сард багтаан эрсдэлийн үнэлгээний болон аудитын тайлангийн дараах мэдээллийг хуулийн Харилцаа холбооны асуудал хариуцсан төрийн захиргааны байгууллагад хүргүүлэх:

18.2.10.1.аудит хийсэн эрх бүхий байгууллагын мэдээлэл, цар хүрээ, хамарсан хугацаа;

18.2.10.2.кибер аюулгүй байдлын эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудитын тайлан.

18.2.11.эрх бүхий байгууллагаас хүргүүлсэн зөвлөмж, шаардлагыг биелүүлэх, илэрсэн алдаа, зөрчлийг арилгах арга хэмжээ авах;

18.2.12.гадаадын иргэн, хуулийн этгээдээр кибер аюулгүй байдлын эрсдэлийн үнэлгээг хийлгэх тохиолдолд тагнуулын байгууллагаас санал авах;

18.2.13.хариуцсан мэдээллийн систем, дэд бүтцийн хэвийн, найдвартай, тасралтгүй байдлыг хангах, гэмтэл саатлын үед сэргээн ажиллуулах төлөвлөгөөтэй байх;

18.2.14.кибер халдлага, зөрчлийн улмаас дэд бүтцийн хэвийн, тасралтгүй үйл ажиллагааг хангах боломжгүй бол энэ талаар холбогдох төвд даруй мэдэгдэх;

18.2.15.төлөвлөгөөт үзлэг шалгалт, өөрийн дэд бүтцээс гаднах сүлжээ, системд гарсан гэмтэл, саатал, гэнэтийн буюу давагдашгүй хүчний шинжтэй нөхцөл байдлын улмаас дэд бүтцийн хэвийн, тасралтгүй үйл ажиллагааг хангах боломжгүй бол энэ талаар холбогдох төв, хэрэглэгчид даруй мэдэгдэх.

18.3.Энэ хуульд заасан хугацаанд олон улсын стандартын дагуу мэдээллийн аюулгүй байдлын аудит хийлгэсэн бол тухайн аудитын тайланг үндэслэн энэ хуулийн 18.2.6-д заасан үүргийг хангасанд тооцно.

ДӨРӨВДҮГЭЭР БҮЛЭГ
КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ

19 дүгээр зүйл.Кибер халдлага, зөрчилтэй тэмцэх төв

19.1.Кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, түүнд өртсөн дэд бүтэц, мэдээллийн системийг нөхөн сэргээхэд мэргэжил арга зүйн туслалцаа дэмжлэг үзүүлэх үндсэн чиг үүрэг бүхий, хүний нөөц, техник, технологийн чадавх, мэдээллийн сантай дараах төвүүд ажиллана:

19.1.1.кибер халдлага, зөрчилтэй тэмцэх үндэсний төв /цаашид “Үндэсний төв” гэх/;

19.1.2.кибер халдлага, зөрчилтэй тэмцэх төрийн нэгдсэн төв /цаашид “Төрийн нэгдсэн төв” гэх/;

19.1.3.кибер халдлага, зөрчилтэй тэмцэх зэвсэгт хүчний төв /цаашид “Зэвсэгт хүчний төв” гэх/.

19.2.Энэ хуулийн 19.1.2, 19.1.3-т заасан төв нь үндэсний төвтэй хамтран ажиллаж, кибер халдлага, зөрчлийн талаар харилцан мэдээлэл солилцож ажиллана.

20 дугаар зүйл.Үндэсний төв

20.1.Үндэсний төв нь харилцаа холбооны асуудал хариуцсан төрийн захиргааны байгууллагын дэргэд ажиллана.

20.2.Үндэсний төв дараах чиг үүргийг хэрэгжүүлнэ:

20.2.1.улсын хэмжээнд кибер халдлага зөрчилтэй тэмцэх төвүүдийн үйл ажиллагааг уялдуулан зохицуулах, мэргэжил, арга зүйн туслалцаа үзүүлэх;

20.2.2.энэ хуулийн 19.1.2, 19.1.3-т заасан төвөөс ирүүлсэн мэдээ, тайланд үндэслэн улсын хэмжээнд кибер халдлага зөрчлийн мэдээлэлд дүн шинжилгээ хийх, мэдээллийн сан бүрдүүлэх, статистик, судалгаа хийх, анхааруулга, зөвлөмж, мэдээлэл түгээх;

20.2.3.үндэсний төвийн халдлагаас хамгаалах системд холбогдсон байгууллагад чиглэсэн кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, түүнд өртсөн дэд бүтцийг нөхөн сэргээхэд дэмжлэг үзүүлэх;

20.2.4.эрхлэх асуудлын хүрээнд Монгол Улсыг төлөөлөх, гадаад улсуудын ижил чиг үүрэг бүхий байгууллагатай мэдээ, мэдээлэл солилцох, хамтран ажиллах;

20.2.5. энэ хуулийн 19.1.2, 19.1.3-т заасан төв, үндэсний аюулгүй байдлыг хангах тусгайлсан чиг үүрэгтэй байгууллагуудтай хамтран ажиллах, мэдээ, мэдээлэл солилцох;

20.2.6.кибер халдлага, зөрчлийн мэдээлэл хүлээн авах, холбогдох байгууллагад шилжүүлэх;

20.2.7.онц чухал мэдээллийн дэд бүтэцтэй байгууллага, холбогдох байгууллага, албан тушаалтанд кибер халдлага, зөрчлийн талаар зөвлөмж, шаардлага хүргүүлэх.

21 дүгээр зүйл.Төрийн нэгдсэн төв

21.1.Төрийн нэгдсэн төв нь тагнуулын байгууллагын дэргэд ажиллана.

21.2.Төрийн нэгдсэн төв нь дараах чиг үүргийг хэрэгжүүлнэ:

21.2.1.онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээд болон төрийн мэдээллийн нэгдсэн сүлжээний аюулгүй байдлыг хангах, тус сүлжээнд холбогдсон байгууллага, мэдээллийн системд чиглэсэн кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, кибер халдлага, зөрчилд өртсөн мэдээллийн системийг нөхөн сэргээхэд дэмжлэг үзүүлэх;

21.2.2. энэ хуулийн 19.1.1, 19.1.3-т заасан төв, үндэсний аюулгүй байдлыг хангах тусгайлсан чиг үүрэгтэй байгууллагуудтай хамтран ажиллах, мэдээ, мэдээлэл солилцох;

21.2.3.гадаад улсуудын ижил чиг үүрэг бүхий байгууллагуудтай мэдээ, мэдээлэл солилцох, хамтран ажиллах;

21.2.4.онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээд, албан тушаалтанд кибер халдлага, зөрчлийн талаар мэдээлэл, зөвлөмж, шаардлага хүргүүлэх;

21.2.5.кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, кибер халдлага, зөрчилд дүн шинжилгээ, судалгаа хийх.

22 дугаар зүйл.Зэвсэгт хүчний төв

22.1.Зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллагын бүтцэд Зэвсэгт хүчний төв ажиллана.

22.2.Зэвсэгт хүчний төв нь дараах чиг үүргийг хэрэгжүүлнэ:

22.2.1.батлан хамгаалах салбарын мэдээллийн системд чиглэсэн кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, түүнд өртсөн мэдээллийн системийг нөхөн сэргээх;

22.2.2.гаднын кибер халдлага, түрэмгийллээс хамгаалах үйл ажиллагаанд дэмжлэг үзүүлэх;

22.2.3.гадаад, дотоодын ижил чиг үүрэгтэй байгууллагуудтай мэдээ, мэдээлэл солилцож, хамтран ажиллах.

22.3 Цэргийн байгууллагын кибер аюулгүй байдлыг хангах зориулалттай техник болон програм хангамжийг шалган баталгаажуулах, дүгнэлт гаргах.

ТАВДУГААР БҮЛЭГ
БУСАД ЗҮЙЛ

23 дугаар зүйл.Кибер аюулгүй байдлын тухай хууль тогтоомж зөрчигчдөд хүлээлгэх хариуцлага

23.1.Энэ хуулийг зөрчсөн албан тушаалтны үйлдэл нь гэмт хэргийн шинжгүй бол Төрийн албаны тухай, Хөдөлмөрийн тухай хуульд заасан хариуцлага хүлээлгэнэ.

23.2.Энэ хуулийг зөрчсөн хүн, хуулийн этгээдэд Эрүүгийн хууль, Зөрчлийн тухай хуульд заасан хариуцлага хүлээлгэнэ.

23.3.Байгууллага, хуулийн этгээд нь кибер аюулгүй байдлыг хангах үйл ажиллагаагаа гэрээний үндсэн дээр бусдад хариуцуулсан нь байгууллага, хуулийн этгээдийг энэ хуулийн хариуцлагаас чөлөөлөх үндэслэл болохгүй.

24 дүгээр зүйл. Шилжилтийн үеийн зохицуулалт

24.1.Энэ хуулийн 20-д заасан Үндэсний төвийг 2023 оны 1 дүгээр сарын 01-ний өдрөөс эхлэн харилцаа холбоо, мэдээллийн технологийн асуудал эрхэлсэн төрийн захиргааны байгууллагын дэргэд ажиллуулна.

25 дугаар зүйл. Хууль хүчин төгөлдөр болох

25.1.Энэ хуулийг 2021 оны 11 дүгээр сарын 01-ны өдрөөс эхлэн дагаж мөрдөнө.

ГАРЫН ҮСЭГ