МОНГОЛ УЛСЫН ХУУЛЬ

2021 оны 12 сарын 17 өдөр Төрийн ордон, 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 орон зай, кибер орчин дахь мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдлыг хангахтай холбогдсон харилцааг зохицуулахад оршино.

2 дугаар зүйл.Кибер аюулгүй байдлын хууль тогтоомж

2.1.Кибер аюулгүй байдлын 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, Нийтийн мэдээллийн ил тод байдлын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай хууль, Цахим гарын үсгийн 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 холбоотой 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, мэдээллийн сүлжээгээр дамжуулан үйл ажиллагаа явуулж байгаа гадаадын иргэн, харьяалалгүй хүн, гадаадын болон гадаадын хөрөнгө оруулалттай хуулийн этгээдэд энэ хууль нэгэн адил үйлчилнэ.

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 доор дурдсан утгаар ойлгоно:

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

4.1.2."кибер орон зай" гэж интернэт болон бусад мэдээлэл, харилцаа холбооны сүлжээ, тэдгээрийн ажиллагааг хангах мэдээллийн дэд бүтцийн харилцан хамааралтай цогцоос бүрдсэн биет болон биет бус талбар;

4.1.3."кибер орчин" гэж мэдээлэлд хандах, нэвтрэх, цуглуулах, түүнийг боловсруулах, хадгалах, ашиглах боломж олгож байгаа мэдээллийн систем, мэдээллийн сүлжээний орчныг;

4.1.4."бүрэн бүтэн байдал" гэж мэдээллийг зөвшөөрөлгүй устгах, өөрчлөхөөс хамгаалсан байхыг;

4.1.5."нууцлагдсан байдал" гэж мэдээлэлд зөвшөөрөлгүй хандах, нэвтрэх боломжгүй байхыг;

4.1.6."хүртээмжтэй байдал" гэж зөвшөөрөгдсөн хүрээнд мэдээлэлд хандах, нэвтрэх, цуглуулах, ашиглах боломжтой байхыг;

4.1.7."мэдээллийн систем" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.1-д заасныг;

4.1.8."мэдээллийн сүлжээ" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.2-т заасныг;

4.1.9."кибер аюулгүй байдлын эрсдэлийн үнэлгээ" гэж цахим мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдал алдагдах, аюул занал тохиолдох магадлал, эмзэг байдлын түвшин, 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 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."онц чухал мэдээллийн дэд бүтэцтэй байгууллага" гэж кибер аюулгүй байдал алдагдсанаар хэвийн үйл ажиллагаа нь доголдож Монгол Улсын үндэсний аюулгүй байдал, нийгэм, эдийн засагт хохирол учруулж болох мэдээллийн систем, мэдээллийн сүлжээ бүхий байгууллагыг;

4.1.13."кибер аюулгүй байдлын зөрчил" гэж мэдээллийн системийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдалд заналхийлж байгаа аливаа үйлдэл, эс үйлдлийг;

4.1.14."кибер халдлага" гэж мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдлыг алдагдуулах зорилго бүхий үйлдлийг;

4.1.15."үндэсний хэмжээний кибер халдлага" гэж онц чухал мэдээллийн дэд бүтэцтэй байгууллагын мэдээллийн систем, мэдээллийн сүлжээнд халдсаны улмаас тухайн байгууллагын хэвийн үйл ажиллагааг алдагдуулж, Монгол Улсын үндэсний аюулгүй байдал, нийгэм, эдийн засагт хохирол учруулахуйц кибер халдлагыг;

4.1.16."кибер халдлага, зөрчилтэй тэмцэх төв" гэж кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, мэдээллийн системийг нөхөн сэргээх үйл ажиллагааг зохицуулж, мэргэжлийн удирдлагаар хангах үндсэн чиг үүрэг бүхий этгээдийг;

4.1.17."төрийн мэдээллийн нэгдсэн сүлжээ" гэж төрийн байгууллага хоорондын мэдээлэл солилцох, кибер аюулгүй байдлыг хангахад чиглэсэн нэгдсэн дэд бүтэц бүхий төрийн интернэт хэрэглээ, албан болон тусгай хэрэглээний сүлжээний цогцыг;

4.1.18."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-д 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 бодлого, 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, хариу арга хэмжээ авах, нөхөн сэргээх арга хэмжээ.

7 дугаар зүйл.Кибер аюулгүй байдлыг хангах нийтлэг журам

7.1.Кибер аюулгүй байдлыг хангах, урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах нийтлэг журмыг Засгийн газар батална.

7.2.Энэ хуулийн 16.1, 17.1, 19.1-д заасан хуулийн этгээд нь Кибер аюулгүй байдлыг хангах нийтлэг журамд нийцсэн кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журамтай байна.

8 дугаар зүйл.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ

8.1.Кибер аюулгүй байдлын эрсдэлийн үнэлгээг цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагад бүртгүүлсэн хуулийн этгээд хийнэ.

8.2.Энэ хуулийн 8.1-д заасан хуулийн этгээд нь олон улсын мэргэжлийн холбоо, стандартын байгууллага, эсхүл түүнтэй дүйцэхүйц байгууллагаас олгосон хүчин төгөлдөр гэрчилгээ бүхий орон тооны ажилтантай байна.

8.3.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх журам, аргачлалыг цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага тагнуулын байгууллагатай хамтран батална.

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 түүний зөвшөөрснөөр энэ хуулийн 8.1-д заасан хуулийн этгээд хийнэ.

8.5.Энэ хуулийн 8.1-д заасан хуулийн этгээд болон 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 цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагад бүртгүүлсэн хуулийн этгээд хийнэ.

9.2.Мэдээллийн аюулгүй байдлын аудит хийх хуулийн этгээд нь дараах шаардлагыг хангасан байна:

9.2.1.олон улсын мэргэжлийн холбоо, стандартын байгууллага, эсхүл түүнтэй дүйцэхүйц байгууллагаас олгосон мэдээллийн аюулгүй байдлын аудит хийх хүчин төгөлдөр гэрчилгээ бүхий орон тооны ажилтантай байх;

9.2.2.энэ хуулийн 9.2.1-д заасан ажилтан ижил төрлийн аудит хийх эрх бүхий бусад хуулийн этгээдэд зэрэгцсэн гэрээгээр ажилладаггүй байх;

9.2.3.хуульд заасан бусад шаардлага.

9.3.Мэдээллийн аюулгүй байдлын аудит хийх хуулийн этгээд мэдээллийн технологи, мэдээллийн аюулгүй байдлын чиглэлээр үйлчилгээ үзүүлснээс хойш тухайн байгууллагад хоёр жилийн хугацаанд мэдээллийн аюулгүй байдлын аудит хийхийг хориглоно.

9.4.Онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээд тагнуулын байгууллагаар, эсхүл түүний зөвшөөрснөөр энэ хуулийн 9.1-д заасан хуулийн этгээдээр мэдээллийн аюулгүй байдлын аудит хийлгэнэ.

9.5.Мэдээллийн аюулгүй байдлын аудит хийх этгээдийг бүртгэх, аудит хийх журмыг цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага батална.

9.6.Энэ хуулийн 9.1-д заасан хуулийн этгээд болон 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.Үндэсний аюулгүй байдлыг хангах тогтолцооны дагуу Засгийн газар кибер аюулгүй байдлыг хангах талаар дараах бүрэн эрхийг хэрэгжүүлнэ:

10.1.1.кибер аюулгүй байдлын үндэсний стратегийг батлах;

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

10.1.3.үндэсний хэмжээний кибер халдлагаас хамгаалах төлөвлөгөөг батлах;

10.1.4.кибер халдлага, зөрчилтэй тэмцэх үндэсний төв болон нийтийн төвийн дүрэм, зохион байгуулалтын бүтэц, орон тоо, төвүүдийн ажиллах журам, тавигдах шаардлагыг батлах;

10.1.5.онц чухал мэдээллийн дэд бүтэцтэй байгууллагын жагсаалтыг батлах;

10.1.6.төрийн мэдээллийн нэгдсэн сүлжээг байгуулах, ашиглах журам, түүнд холбогдох байгууллагын жагсаалтыг батлах;

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

10.1.8.Кибер аюулгүй байдлын зөвлөлийн Ажлын албаны бүтэц, орон тоо, ажиллах журмыг батлах.

11 дүгээр зүйл.Кибер аюулгүй байдлын зөвлөл

11.1.Кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлагаар хангах, уялдуулан зохицуулах, хэрэгжилтийг зохион байгуулах, мэдээлэл солилцох чиг үүрэг бүхий орон тооны бус Кибер аюулгүй байдлын зөвлөл /цаашид "Зөвлөл" гэх/ ажиллана.

11.2.Зөвлөлийг Ерөнхий сайд тэргүүлж, дэд даргаар цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн Засгийн газрын гишүүн, Тагнуулын ерөнхий газрын дарга нар ажиллах бөгөөд уг Зөвлөл нь Ажлын албатай байна.

11.3.Зөвлөлийн бүрэлдэхүүн, дүрмийг Засгийн газар батална.

11.4.Зөвлөл дараах бүрэн эрхийг хэрэгжүүлнэ:

11.4.1.кибер аюулгүй байдлыг хангах хууль тогтоомжийн хэрэгжилтэд хяналт тавих;

11.4.2.үндэсний хэмжээний кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлага, зохион байгуулалтаар хангах, холбогдох байгууллагын үйл ажиллагааг уялдуулан зохицуулах;

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

11.4.4.кибер аюулгүй байдлыг хангах талаар гадаад улс, олон улсын ижил төстэй байгууллагатай хамтран ажиллах;

11.4.5.хуульд заасан бусад бүрэн эрх.

11.5.Зөвлөл, түүний Ажлын албаны үйл ажиллагаанд шаардагдах зардлыг улсын төсвөөс санхүүжүүлнэ.

11.6.Зөвлөлийн шийдвэр тогтоол, тэмдэглэл хэлбэртэй байх ба тогтоосон журмын дагуу үйлдсэн тамга, тэмдэг, хэвлэмэл хуудас хэрэглэнэ.

11.7.Кибер аюулгүй байдлыг хангах чиглэлээр гаргасан Зөвлөлийн шийдвэрийг холбогдох байгууллага, албан тушаалтан биелүүлж, хэрэгжилтийг тайлагнана.

12 дугаар зүйл.Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага

12.1.Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага кибер аюулгүй байдлыг хангах талаар дараах бүрэн эрхийг хэрэгжүүлнэ:

12.1.1.кибер аюулгүй байдлыг хангах хууль тогтоомж, эрх бүхий байгууллагын шийдвэрийг хэрэгжүүлэх;

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

12.1.3.кибер аюулгүй байдлыг хангах нийтлэг журмыг тагнуулын байгууллага, зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллагатай хамтран боловсруулах;

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

12.1.5.онц чухал мэдээллийн дэд бүтэцтэй байгууллагын жагсаалтыг тагнуулын байгууллага, зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллагатай хамтран боловсруулах;

12.1.6.кибер аюулгүй байдлын эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудит хийх хуулийн этгээдийг бүртгэх;

12.1.7.кибер аюулгүй байдлыг хангах чиглэлээр шинэ техник, технологи, инновац, судалгаа, шинжилгээний үйл ажиллагаа явуулах;

12.1.8.кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, соён гэгээрүүлэх арга хэмжээг хэрэгжүүлэх, холбогдох хууль тогтоомжийг сурталчлах.

13 дугаар зүйл.Тагнуулын байгууллага

13.1.Тагнуулын байгууллага кибер аюулгүй байдлыг хангах талаар дараах бүрэн эрхийг хэрэгжүүлнэ:

13.1.1.төрийн мэдээллийн нэгдсэн сүлжээг зохион байгуулж, түүний кибер аюулгүй байдлыг хангах;

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, холбогдох этгээдэд сургалт зохион байгуулах;

13.1.3.кибер аюулгүй байдлын үндэсний стратегийг цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага, зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллагатай хамтран боловсруулах;

13.1.4.үндэсний хэмжээний кибер халдлагаас хамгаалах төлөвлөгөөг боловсруулах, хэрэгжилтэд хяналт тавьж ажиллах;

13.1.5.үндэсний аюулгүй байдлыг хангах тусгайлсан чиг үүрэг бүхий болон төрийн захиргааны төв байгууллагатай мэдээлэл солилцох, хамтран ажиллах журмыг холбогдох байгууллагатай хамтран батлах;

13.1.6.энэ хуулийн 10.1.6-д заасан журмыг боловсруулах, хэрэгжилтэд хяналт тавих;

13.1.7.энэ хуулийн 13.1.2-т заасан этгээдийн мэдээллийн систем, мэдээллийн сүлжээний аюулгүй байдлыг хангах зориулалт бүхий техник, программ хангамжийг шалган баталгаажуулах, дүгнэлт гаргах;

13.1.8.энэ хуулийн 13.1.2-т заасан этгээдэд гадаад улсын зээл, тусламж, хөрөнгө оруулалтаар хэрэгжих мэдээллийн технологийн төсөл, хөтөлбөрт кибер аюулгүй байдлыг хангах асуудлаар дүгнэлт гаргаж, холбогдох байгууллагад санал, шаардлага хүргүүлэх;

13.1.9.кибер халдлага, зөрчилтэй тэмцэх зорилгоор тоон шинжилгээний лаборатори ажиллуулах;

13.1.10.кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх этгээдийг бүртгэхэд санал өгөх;

13.1.11.кибер аюулгүй байдлыг хангах асуудлаар хүн, хуулийн этгээдэд зөвлөмж, шаардлага хүргүүлэх.

14 дүгээр зүйл.Зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллага

14.1.Зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллага дараах бүрэн эрхийг хэрэгжүүлнэ:

14.1.1.кибер аюулгүй байдлын хууль тогтоомжийн хэрэгжилтийг батлан хамгаалах салбарт зохион байгуулах;

14.1.2.тайван цагт батлан хамгаалах үйл ажиллагааны кибер аюулгүй байдал, зэвсэгт хүчний мэдээллийн систем, мэдээллийн сүлжээний аюулгүй байдлыг хангаж, шаардлагатай үед улсын кибер орон зайн аюулгүй байдлыг хангах үйл ажиллагаанд дэмжлэг үзүүлэх;

14.1.3.хуульд өөрөөр заагаагүй бол зэвсэгт хүчний анги, байгууллагын мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж, программ хангамжийг шалган баталгаажуулах;

14.1.4.кибер аюулгүй байдлыг хангах талаар зэвсэгт хүчний анги, байгууллагад сургалт зохион байгуулах, зөвлөмж хүргүүлэх;

14.1.5.кибер аюулгүй байдлын чадавх, бэлэн байдлыг хангах чиглэлээр гадаад, дотоодын ижил чиг үүрэгтэй байгууллагуудтай мэдээ, мэдээлэл солилцож, хамтран ажиллах.

15 дугаар зүйл.Цагдаагийн байгууллага

15.1.Цагдаагийн байгууллага кибер аюулгүй байдлыг хангах талаар дараах бүрэн эрхийг хэрэгжүүлнэ:

15.1.1.кибер халдлага, зөрчилтэй холбоотой гэмт хэргийн мэдээллийг хүлээн авч, хуульд заасан ажиллагааг явуулах;

15.1.2.энэ хуулийн 15.1.1-д заасан чиг үүргээ хэрэгжүүлэхэд шаардлагатай мэдээллийг холбогдох төрийн байгууллага, албан тушаалтан, хүн, хуулийн этгээдээс гаргуулан авах;

15.1.3.кибер аюулгүй байдлыг хангах асуудлаар хүн, хуулийн этгээдэд зөвлөмж, шаардлага, сэрэмжлүүлэг хүргүүлэх;

15.1.4.кибер халдлага, зөрчилтэй тэмцэх, тоног төхөөрөмж, программ хангамжийг шалгах, судалгаа, шинжилгээ хийх, дүгнэлт гаргах зорилгоор тоон шинжилгээний лаборатори ажиллуулах.

16 дугаар зүйл.Төрийн өмчит хуулийн этгээд

16.1.Төрийн өмчит хуулийн этгээд кибер аюулгүй байдлыг хангах талаар дараах үүргийг хүлээнэ:

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

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

16.1.3.кибер халдлага, зөрчилд өртсөн, өртсөн байж болзошгүй тохиолдолд кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд даруй мэдэгдэх;

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

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

17 дугаар зүйл.Хуулийн этгээд

17.1.Кибер орчинд дундын мэдээллийн системээр дамжуулан мэдээлэл боловсруулах, хадгалах, түгээх, цахим тооцооллын болон түүний хэвийн үйл ажиллагааг хангахад мэдээллийн технологийн чиглэлээр үйлчилгээ үзүүлж байгаа хуулийн этгээд дараах үүргийг хүлээнэ:

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

17.1.2.кибер халдлагын талаар кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд даруй мэдэгдэх, таслан зогсоох боломжгүй бол туслалцаа авах;

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

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

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

17.1.6.кибер аюулгүй байдлын эрсдэлийн үнэлгээг хоёр жил тутамд, холбогдох журамд заасан нөхцөл, байдал үүссэн үед тухай бүр хийлгэж, гарсан дүгнэлт, зөвлөмж, шаардлагын дагуу арга хэмжээг авч хэрэгжүүлэх;

17.1.7.мэдээллийн аюулгүй байдлын аудитыг жил тутамд, холбогдох журамд заасан нөхцөл, байдал үүссэн үед тухай бүр хийлгэж, гарсан дүгнэлт, зөвлөмж, шаардлагын дагуу арга хэмжээг авч хэрэгжүүлэх;

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

17.1.9.кибер халдлага, зөрчилд өртсөн хэрэглэгчид даруй мэдэгдэх.

17.2.Энэ хуульд заасан хугацаанд олон улсын стандартын дагуу мэдээллийн аюулгүй байдлын аудит хийлгэсэн бол тухайн аудитын тайланг үндэслэн энэ хуулийн 17.1.7-д заасан үүргийг хангасанд тооцно.

17.3.Энэ хуулийн 17.1-д зааснаас бусад хуулийн этгээд дараах эрх, үүргийг хэрэгжүүлнэ:

17.3.1.кибер аюулгүй байдлыг хангах нийтлэг журмыг үйл ажиллагаандаа мөрдөх;

17.3.2.кибер халдлага, зөрчлийн талаар кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд мэдэгдэх, шаардлагатай үед туслалцаа авах;

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

17.3.4.хууль тогтоомжид заасан бусад эрх, үүрэг.

18 дугаар зүйл.Иргэн

18.1.Иргэн кибер аюулгүй байдлыг хангах талаар дараах үүргийг хүлээнэ:

18.1.1.өөрийн болон өөрийн асрамжид байгаа хүний кибер аюулгүй байдлыг хариуцах;

18.1.2.холбогдох байгууллагаас гаргасан зөвлөмжийг дагах, шаардлагыг биелүүлэх;

18.1.3.хууль тогтоомжид заасан бусад.

18.2.Кибер халдлага, зөрчил үүссэн, үүссэн байж болзошгүй тохиолдолд Нийтийн төвд даруй мэдэгдэж болно.

19 дүгээр зүйл.Онц чухал мэдээллийн дэд бүтэцтэй байгууллага

19.1.Онц чухал мэдээллийн дэд бүтэцтэй байгууллагад дараах чиглэлээр үйл ажиллагаа эрхэлдэг байгууллага хамаарна:

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

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

19.1.3.хоёр, гуравдугаар шатлалын эрүүл мэндийн байгууллага;

19.1.4.хүн, малын гоц халдварт өвчин судлах лаборатори;

19.1.5.эм, химийн хорт болон аюултай бодис үйлдвэрлэгч;

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

19.1.7.зүй ёсны монополь болон давамгай байдалтай харилцаа холбоо, мэдээллийн технологийн үйлчилгээ эрхлэгч;

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

19.1.9.түлш, шатахуун импортлогч, үйлдвэрлэгч, түгээгч байгууллага;

19.1.10.стратегийн хүнс үйлдвэрлэгч, хадгалагч, түгээгч байгууллага;

19.1.11.мэдээлэл, шуурхай удирдлагын төв;

19.1.12.үндэсний олон нийтийн радио, телевиз;

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

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

19.1.15.хилийн боомтын хяналт удирдлагын систем хариуцсан байгууллага;

19.1.16.стратегийн ач холбогдол бүхий ашигт малтмалын ордыг ашиглах үйл ажиллагаа эрхлэгч;

19.1.17.улсын хилээр нэвтэрч байгаа зорчигч, тээврийн хэрэгслийн бүртгэл, хяналт, мэдээллийн нэгдсэн систем хариуцсан байгууллага.

19.2.Онц чухал мэдээллийн дэд бүтэцтэй байгууллага дараах үүргийг хүлээнэ:

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

19.2.2.кибер халдлага, зөрчлийн үед дагаж мөрдөх төлөвлөгөөг баталж хэрэгжүүлэх;

19.2.3.мэдээллийн аюулгүй байдлыг хангах талаар стандартыг нэвтрүүлэх;

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

19.2.5.кибер аюулгүй байдлын эрсдэлийн үнэлгээг жил тутамд, эсхүл мэдээллийн систем, мэдээллийн сүлжээний өөрчлөлт хийгдэх бүрд хэсэгчлэн, эрх бүхий байгууллагын шаардсанаар тухай бүр хийлгэж, гарсан дүгнэлт, зөвлөмж, шаардлагын дагуу холбогдох арга хэмжээг авч хэрэгжүүлэх;

19.2.6.мэдээллийн аюулгүй байдлын аудитыг хоёр жил тутамд хийлгэх;

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

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

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

19.2.10.кибер аюулгүй байдлын эрсдэлийн үнэлгээний болон мэдээллийн аюулгүй байдлын аудитын тайланг хүлээн авснаас хойш нэг сарын дотор кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд хүргүүлэх;

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

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

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

19.2.14.кибер халдлага, зөрчлийн улмаас мэдээллийн систем, дэд бүтцийн хэвийн үйл ажиллагаа алдагдсан, тасралтгүй үйл ажиллагааг хангах боломжгүй болсон даруйд энэ талаар кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд мэдэгдэх;

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

19.3.Энэ хуульд заасан хугацаанд олон улсын стандартын дагуу мэдээллийн аюулгүй байдлын аудит хийлгэсэн бол тухайн аудитын тайланг үндэслэн энэ хуулийн 19.2.6-д заасан үүргийг хангасанд тооцно.

ДӨРӨВДҮГЭЭР БҮЛЭГ

КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ

20 дугаар зүйл.Кибер халдлага, зөрчилтэй тэмцэх төв

20.1.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:

20.1.1.кибер халдлага, зөрчилтэй тэмцэх үндэсний төв /цаашид "Үндэсний төв" гэх/;

20.1.2.кибер халдлага, зөрчилтэй тэмцэх нийтийн төв /цаашид "Нийтийн төв" гэх/;

20.1.3.кибер халдлага, зөрчилтэй тэмцэх зэвсэгт хүчний төв /цаашид "Зэвсэгт хүчний төв" гэх/.

20.2.Бусад хуулийн этгээд кибер халдлага илрүүлэх, таслан зогсоох үйл ажиллагаа явуулахдаа энэ хуулийн 10.1.4-т заасан холбогдох шаардлагыг хангасан байна.

20.3.Энэ хуулийн 20.1.2, 20.1.3-т заасан төв, 20.2-т заасан хуулийн этгээд нь Үндэсний төвтэй хамтран ажиллаж, кибер халдлага, зөрчлийн талаар харилцан мэдээлэл солилцож ажиллана.

21 дүгээр зүйл.Үндэсний төв

21.1.Үндэсний төв тагнуулын байгууллагын бүтцэд ажиллана.

21.2.Үндэсний төв дараах чиг үүргийг хэрэгжүүлнэ:

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

21.2.2.онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээд болон төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон байгууллагын мэдээллийн системд чиглэсэн кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, кибер халдлага, зөрчилд өртсөн мэдээллийн системийг нөхөн сэргээхэд дэмжлэг үзүүлэх;

21.2.3.улсын хэмжээнд кибер халдлага, зөрчлийн мэдээлэлд дүн шинжилгээ хийх, мэдээллийн сан бүрдүүлэх, статистик мэдээлэл, судалгаа гаргах, анхааруулга, зөвлөмж, мэдээлэл түгээх;

21.2.4.эрхлэх асуудлын хүрээнд Монгол Улсыг төлөөлөн олон улсын болон гадаад улсын ижил төстэй байгууллагатай мэдээ, мэдээлэл солилцох, хамтран ажиллах;

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

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

21.2.7.улсын хэмжээнд бүртгэгдсэн кибер халдлага, зөрчлийн талаарх мэдээллийг ангилах, боловсруулах, хариуцсан байгууллагад шилжүүлэх зорилгоор холбогдох байгууллагын төлөөлөл бүхий багийг ажиллуулах.

22 дугаар зүйл.Нийтийн төв

22.1.Нийтийн төв цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагын дэргэд ажиллана.

22.2.Нийтийн төв дараах чиг үүргийг хэрэгжүүлнэ:

22.2.1.энэ хуулийн 21.2.2-т зааснаас бусад иргэн, хуулийн этгээдийн мэдээллийн систем, мэдээллийн сүлжээнд чиглэсэн кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, кибер халдлага, зөрчилд өртсөн мэдээллийн системийг нөхөн сэргээхэд дэмжлэг үзүүлэх;

22.2.2.кибер халдлага, зөрчлийн талаар судалгаа, дүн шинжилгээ хийх, олон нийтэд зөвлөмж, мэдээлэл түгээх;

22.2.3.энэ хуулийн 20.1.1, 20.1.3-т заасан төв, 20.2-т заасан хуулийн этгээдтэй хамтран ажиллах, мэдээ, мэдээлэл солилцох;

22.2.4.иргэн, хуулийн этгээдэд кибер халдлага, зөрчлийн талаар зөвлөмж, шаардлага хүргүүлэх.

23 дугаар зүйл.Зэвсэгт хүчний төв

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

23.2.Зэвсэгт хүчний төв дараах чиг үүргийг хэрэгжүүлнэ:

23.2.1.батлан хамгаалах салбарын мэдээллийн системд чиглэсэн кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, кибер халдлага, зөрчилд өртсөн мэдээллийн системийг нөхөн сэргээх;

23.2.2.гадны кибер халдлага, түрэмгийллээс хамгаалах үйл ажиллагаанд дэмжлэг үзүүлэх;

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

23.2.4.батлан хамгаалах салбарын кибер аюулгүй байдлыг хангах зориулалттай техник болон программ хангамжийг шалган баталгаажуулах, дүгнэлт гаргах.

ТАВДУГААР БҮЛЭГ

БУСАД ЗҮЙЛ

24 дүгээр зүйл.Кибер аюулгүй байдлын хууль тогтоомж зөрчигчдөд хүлээлгэх хариуцлага

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

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

24.3.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.

25 дугаар зүйл.Хууль хүчин төгөлдөр болох

25.1.Энэ хуулийг 2022 оны 05 дугаар сарын 01-ний өдрөөс эхлэн дагаж мөрдөнө.

МОНГОЛ УЛСЫН ИХ ХУРЛЫН ДАРГА Г.ЗАНДАНШАТАР