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 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, 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.Монгол Улсын мэдээллийн систем, сүлжээгээр дамжуулан үйл ажиллагаа явуулж байгаа гадаад улсын иргэн, хуулийн этгээд, түүний салбар, төлөөлөгчийн газарт нэгэн адил хамаарна.

3.3.Зэвсэгт хүчний тухай хуулиар тусгайлан зохицуулснаас бусад кибер аюулгүй байдлыг хангах асуудлыг энэ хуулиар зохицуулна.

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 орчны бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдал хангагдсан байхыг;

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

4.1.3.“бүрэн бүтэн байдал” гэж кибер орчин дахь мэдээллийг зөвшөөрөлгүй этгээд устгах, өөрчлөхөөс хамгаалагдсан байхыг;

4.1.4.“нууцлагдсан байдал” гэж кибер орчин дахь мэдээлэлд зөвшөөрөлгүй этгээд нэвтрэх, танилцах, олж авах, ашиглахаас хамгаалагдсан байхыг;

4.1.5.“хүртээмжтэй байдал” гэж кибер орчин дахь мэдээлэлд зөвшөөрөлтэй этгээд мэдээллийн системд хандах, мэдээлэл олж авах, ашиглах боломж бүрдсэн байхыг;

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

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

4.1.8.“кибер аюулгүй байдлын эрсдэлийн үнэлгээ” гэж цахим мэдээлэл, мэдээллийн системийн кибер аюулгүй байдал алдагдаж болох аюул занал, тохиолдох магадлал, эмзэг байдлын түвшинг тогтоох, түүнээс үүсэх үр дагавар, эрсдэлийг бууруулах, урьдчилан сэргийлэх арга хэмжээг тодорхойлох мэргэжлийн үйл ажиллагааг;

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

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

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

4.1.12.“кибер халдлага” гэж мэдээллийн системийн кибер аюулгүй байдлыг алдагдуулах зорилго бүхий бүх төрлийн үйлдлийг;

4.1.13.“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;

4.1.14. “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 дэд бүтэц бүхий байгууллагыг;

4.1.15.“шалгагдагч этгээд” гэж энэ хуулийн үйлчлэлд хамаарах хүн, хуулийн этгээдийг.

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.мэргэжлийн нэгдмэл удирдлагатай байх;

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

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

5.1.4.эрсдлийн үнэлгээнд тулгуурлах;

5.1.5.төр, хувийн хэвшлийн түншлэлд тулгуурлах.

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 байдлын эрсдэлийн үнэлгээ

7.1.Энэ хуулийн үйлчлэх хүрээнд хамаарах хуулийн этгээд нь кибер аюулгүй байдлын эрсдэлийн үнэлгээг жил тутам хийлгэнэ.

7.2.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх журмыг энэ хуулийн 12.1-д заасан байгууллагын саналыг үндэслэн Засгийн газар батална.

7.3.Төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон байгууллага болон онц чухал мэдээллийн дэд бүтэцтэй төрийн байгууллагын кибер аюулгүй байдлын эрсдэлийн үнэлгээг энэ хуулийн 13.1-д заасан байгууллага хийнэ.

7.4.Энэ хуулийн 7.3-д зааснаас бусад хуулийн этгээдийн кибер аюулгүй байдлын эрсдэлийн үнэлгээг энэ хуулийн 12.1-д заасан байгууллагаас эрх олгосон этгээд гүйцэтгэнэ.

8 дугаар зүйл.Мэдээллийн аюулгүй байдлын аудит

8.1.Энэ хуулийн үйлчлэх хүрээнд хамаарах этгээд нь хууль, олон улсын болон үндэсний стандартад нийцүүлэн мэдээллийн аюулгүй байдлын аудитыг хоёр жил тутам хийлгэнэ.

8.2.Мэдээллийн аюулгүй байдлын аудитыг үндэсний аюулгүй байдлыг хангах тусгайлсан чиг үүрэгтэй байгууллага, онц чухал мэдээллийн дэд бүтэцтэй байгууллага 2 жилд нэг удаа, эрх бүхий байгууллагаас шаардсан тохиолдолд төрийн байгууллага тухай бүр хийлгэнэ.

9 дүгээр зүйл.Үйлчилгээний төлбөр

9.1.Кибер аюулгүй байдлын эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудит хийх эрх авсан этгээд үйлчилгээний төлбөр авна.

9.2.Үйлчилгээний төлбөрийг тогтоох аргачлалыг энэ хуулийн 12.1-д заасан байгууллага батална.

9.3.Энэ хуулийн 7.3-д заасан байгууллагын кибер аюулгүй байдлын эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудит хийхэд шаардагдах зардлыг төр хариуцна.

ГУРАВДУГААР БҮЛЭГ
КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ТОГТОЛЦОО

10 дугаар зүйл.Монгол Улсын Их Хурал

10.1.Монгол Улсын Их Хурал кибер аюулгүй байдлыг хангах талаар дараах бүрэн эрхийг хэрэгжүүлнэ:

10.1.1.кибер аюулгүй байдлын талаар төрөөс баримтлах бодлого, хууль тогтоомжийг батлах, тэдгээрийн биелэлтэд хяналт тавих.

11 дүгээр зүйл.Засгийн газар

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

11.1.1.кибер аюулгүй байдлыг хангах талаар хөгжлийн төлөвлөлтийн баримт бичиг батлах, хууль тогтоомжийг хэрэгжүүлэх ажлыг зохион байгуулах, хяналт тавих, биелэлтийг хангах;

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

11.1.3.үндэсний хэмжээний кибер халдлагын үед ажиллах төлөвлөгөө батлах;

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

11.1.5.энэ хуулийн 19.1-д заасан онц чухал мэдээллийн дэд бүтэцтэй байгууллагын жагсаалтыг батлах;

11.1.6.төрийн мэдээллийн нэгдсэн сүлжээг байгуулах, ашиглах журам, түүнд холбогдох байгууллагын жагсаалтыг энэ хуулийн 13.1-д заасан байгууллагын саналыг үндэслэн батлах.

11.1.7.кибер аюулгүй байдлыг хангах чиглэлээр боловсролын тогтолцоог хөгжүүлэх.

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;

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

12.1.3.улсын хэмжээнд 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.кибер аюулгүй байдлыг хангах нийтлэг журам болон бусад холбогдох дүрэм, журам, заавар батлах;

12.1.6.мэдээллийн аюулгүй байдлын аудит хийх этгээдэд тавих шаардлага, эрх олгох журмыг батлах, эрх олгох, журмын хэрэгжилтэд хяналт тавих;

12.1.7.кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх журмын хэрэгжилтэд хяналт тавьж, эрсдлийн үнэлгээ хийх этгээдэд энэ хуулийн 13.1-д заасан байгууллагаас санал авч, эрх олгох;

12.1.8.онц чухал мэдээллийн дэд бүтэцтэй байгууллагын жагсаалтыг энэ хуулийн 13.1-д заасан 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 сурталчилах;

12.1.13.кибер халдлага, зөрчилтэй тэмцэх төвийн үйл ажиллагааг уялдуулан зохицуулах, мэргэжил арга зүйн дэмжлэг үзүүлэх.

13 дугаар зүйл.Тагнуулын байгууллага

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

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

13.1.2. кибер аюулгүй байдлыг хангах нийтлэг журмыг энэ хуулийн 12.1-д заасан байгууллагатай хамтран боловсруулах;

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

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

13.1.5.төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон болон онц чухал мэдээллийн дэд бүтэцтэй төрийн байгууллагын кибер аюулгүй байдлыг хангах зориулалттай техник болон программ хангамжийг шалган баталгаажуулах, дүгнэлт гаргах;

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

13.1.7.төрийн мэдээллийн нэгдсэн сүлжээг зохион байгуулах, ашиглах журмын хэрэгжилтэд хяналт тавих;

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

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

14 дүгээр зүйл.Харилцаа холбооны зохицуулах хороо

14.1.Харилцаа холбооны зохицуулах хороо кибер аюулгүй байдлыг хангах талаар дараах эрх, үүргийг хэрэгжүүлнэ:

14.1.1.үндэсний стандарт боловсронгуй болгох;

14.1.2.эрх бүхий байгууллагын шийдвэрийг үндэслэн цахим орчин дахь контент, хэрэглэгчийг түдгэлзүүлэх, хязгаарлах арга хэмжээ авах;

14.1.3.Энэ хуулийн 14.1.2-д заасан арга хэмжээг хэрэгжүүлэхтэй холбоотой журам батлах.

15 дугаар зүйл.Цагдаагийн байгууллага

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

15.1.1.кибер халдлага, зөрчилтэй холбоотой мэдээллийг харьяаллын дагуу үндэсний болон нэгдсэн төвд мэдэгдэх;

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

15.1.3.кибер гэмт хэргээс урьдчилан сэргийлэх чиглэлээр холбогдох этгээдтэй хамтран арга хэмжээ зохион байгуулах.

16 дугаар зүйл.Төрийн байгууллага

16.1.Төрийн байгууллага кибер аюулгүй байдлыг хангах талаар дараах үүргийг хэрэгжүүлнэ:

16.1.1.кибер аюулгүй байдлын нийтлэг журамд нийцсэн 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 харьяаллын дагуу үндэсний болон нэгдсэн төвд даруй мэдэгдэх;

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

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

16.1.6.энэ хуулийн 11.1.6 дах заалтад заасан жагсаалтад хамрагдсан байгууллагууд төрийн мэдээллийн нэгдсэн сүлжээнд холбогдох;

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

17 дугаар зүйл.Хуулийн этгээд

17.1.Хүний эмзэг мэдээллийг цуглуулж, боловсруулж буй хуулийн этгээдийн кибер аюулгүй байдлыг хангах арга хэмжээг Хүний хувийн мэдээллийг хамгаалах тухай хуулийн 19 дүгээр зүйлээр зохицуулна.

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

17.2.1.кибер аюулгүй байдлын нийтлэг журамд нийцсэн байгууллагын кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам батлаж мөрдөх;

17.2.2.кибер халдлага, зөрчил үүссэн тохиолдолд үндэсний төвд даруй мэдэгдэх;

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

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

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

17.2.6.эрх бүхий байгууллагын шаардсанаар мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийлгэх, гарсан зөвлөмж, дүгнэлтийн дагуу холбогдох арга хэмжээг авч хэрэгжүүлэх, авсан арга хэмжээний талаар хариу мэдэгдэх;

17.2.7.бүтээгдэхүүн үйлчилгээний болон тэдгээрийн шинэчлэл бүрт кибер аюулгүй байдлын холбогдох тест хийсэн байх;

17.2.8.хэрэглэгчид зориулсан хувь хүний мэдээлэл хамгаалах болон мэдээллийн аюулгүй байдлыг хангах журам, нөхцөл, шаардлагыг нийтэд ил байршуулах;

17.2.9.хэрэглэгчийн зүгээс мэдээллийн системийн хэвийн үйл ажиллагаанд нөлөөлөхүйц үйлдэл хийсэн бол тухайн хэрэглэгчийн үйлчилгээг хязгаарлах, хэрэглэгчид мэдэгдэх;

17.2.10.кибер халдлага, зөрчилд өртсөн хэрэглэгчид 24 цагийн дотор мэдэгдэх;

17.2.11.Харилцаа холбооны тухай хуулийн 25.2.11-д заасны дагуу хэрэглэгчийн бүртгэлийг хөтлөх.

18 дугаар зүйл.Иргэн

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

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

18.1.2.холбогдох байгууллагаас гаргасан зөвлөмж, шаардлагыг биелүүлэх;

18.1.3.кибер халдлага, зөрчил үүссэн, үүссэн байж болзошгүй тохиолдолд холбогдох байгууллагад даруй мэдэгдэх, хамтран ажиллах;

18.1.4.хууль тогтоомжид заасан бусад.

19 дүгээр зүйл.Онц чухал мэдээллийн дэд бүтэцтэй байгууллага

19.1.Онц чухал мэдээллийн дэд бүтэцтэй байгууллагад дараах чиглэлийн 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;

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

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

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

19.1.7.түлш, шатахуун имортлогч, үйлдвэрлэгч, түгээгч, стратегийн хүнс үйлвэрлэгч, хадгалагч, түгээгч байгууллага;

19.1.8.мэдээлэл, шуурхай удирдлагын төв;

19.1.9.үндэсний олон нийтийн радио, телевиз;

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

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

19.1.12.хилийн боомтын хяналт удирдлагын систем хариуцсан байгууллага.

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

19.2.1.кибер аюулгүй байдлын нийтлэг журамд нийцсэн байгууллагын кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам баталж мөрдөх;

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

19.2.3.кибер 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, эрх бүхий байгууллагын шаардсанаар тухай бүр хийлгэх;

19.2.6.мэдээллийн аюулгүй байдлын аудитыг хоёр жил тутамд хийлгэх;

19.2.7.мэдээллийн системийн аюулгүй байдлыг хангахад шаардлагатай удирдлага, зохион байгуулалтын болон техникийн арга хэмжээ төлөвлөх, хэрэгжүүлэх;

19.2.8.кибер халдлага, зөрчлийг илрүүлэх, бүртгэх, таслан зогсоох мэдээллийн системтэй байх, эсхүл кибер халдлага, зөрчилтэй тэмцэх төвд холбогдсон байх;

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

19.2.10.кибер халдлага, зөрчлийн үед дагаж мөрдөх төлөвлөгөө, эрсдэлийн үнэлгээний болон аудитын тайланг дараа жилийн нэгдүгээр сард багтаан холбогдох байгууллагад хүргүүлэх;

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

19.2.12.гадаадын иргэн, хуулийн этгээдээр кибер аюулгүй байдлын эрсдэлийн үнэлгээг хийлгэх тохиолдолд энэ хуулийн 13.1-д заасан 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.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 байгууллага, хэрэглэгчид даруй мэдэгдэх.

ГУРАВДУГААР 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 чадавхтай дараах төвүүд ажиллана:

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

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

20.1.3.кибер халдлага, зөрчилтэй тэмцэх зэвсэгт хүчний төв.

20.2.Энэ хуулийн 20.1.1-20.1.3-т заасан төвийг төсөв санхүү, хүний нөөц, техник, технологийн боломжоор хангах үүргийг төр хариуцна.

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

21 дүгээр зүйл.Үндэсний төв

21.1.Үндэсний төв нь энэ хуулийн 12.1-д заасан байгууллагын дэргэд 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.энэ хуулийн 20.1.2, 20.1.3-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;

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

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

21.2.5. энэ хуулийн 20.1.2, 20.1.3-т заасан төв, үндэсний аюулгүй байдлыг хангах тусгайлсан чиг үүрэгтэй байгууллагуудтай мэдээ, мэдээлэл солилцох, хамтран ажиллах;

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

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

22 дугаар зүйл.Төрийн нэгдсэн төв

22.1.Төрийн нэгдсэн төв нь энэ хуулийн 13.1-д заасан байгууллагын дэргэд ажиллана.

22.2.Төрийн нэгдсэн төв нь дараах чиг үүргийг хэрэгжүүлнэ:

22.2.1.онц чухал мэдээллийн дэд бүтэцтэй төрийн байгууллага 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;

22.2.2. энэ хуулийн 20.1.1, 20.1.3-т заасан төв, үндэсний аюулгүй байдлыг хангах тусгайлсан чиг үүрэгтэй байгууллагуудтай мэдээ, мэдээлэл солилцох, хамтран ажиллах;

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

22.2.4.онц чухал мэдээллийн дэд бүтэцтэй төрийн байгууллага, албан тушаалтанд кибер халдлага, зөрчлийн талаар мэдээлэл, зөвлөмж, шаардлага хүргүүлэх;

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

ДӨРӨВДҮГЭЭР БҮЛЭГ
БУСАД ЗҮЙЛ

23 дугаар зүйл.Кибер аюулгүй байдлыг хангах үйл ажиллагаанд тавих хяналт

23.1.Улсын хэмжээнд кибер аюулгүй байдлыг хангах үйл ажиллагаанд энэ хуулийн 12.1-д заасан байгууллага хяналт тавьж, кибер аюулгүй байдлын тухай хууль тогтоомжийн хэрэгжилтийг хянан шалгах ажлыг энэ хууль, холбогдох бусад хуульд заасны дагуу хэрэгжүүлнэ.

23.2.Төрийн мэдээллийн нэгдсэн сүлжээ болон онц чухал мэдээллийн дэд бүтэцтэй төрийн байгууллагын кибер аюулгүй байдлыг хангах үйл ажиллагаанд энэ хуулийн 13.1-д заасан байгууллага хяналт тавина.

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

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

24.2.Энэ хуулийг зөрчсөн хүн, хуулийн этгээдэд Эрүүгийн хууль, 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 2021 оны …. дугаар сарын ….-ны өдрөөс эхлэн дагаж мөрдөнө.

ГАРЫН ҮСЭГ