Төсөл 1.6

КИБЕР СӨРӨН ТЭСВЭРЛЭХ ТУХАЙ

НЭГДҮГЭЭР БҮЛЭГ

НИЙТЛЭГ ҮНДЭСЛЭЛ

1 дүгээр зүйл.Хуулийн зорилт

1.1.Энэ хуулийн зорилт нь Монгол Улсын кибер сөрөн тэсвэрлэх чадавхийг хангах, кибер орчин дахь онц чухал болон чухал мэдээллийн дэд бүтцийн тасралтгүй, найдвартай ажиллагааг хамгаалах, кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, кибер эрсдэлийг удирдах, илрүүлэх, хариу арга хэмжээ авах, нөхөн сэргээхтэй холбогдсон харилцааг зохицуулахад оршино.

2 дугаар зүйл.Кибер сөрөн тэсвэрлэх хууль тогтоомж

2.1.Кибер аюулгүй байдлын хууль тогтоомж нь Монгол Улсын Үндсэн 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 орчин дахь мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийн дэд бүтцийн ашиглалт, хамгаалалт, кибер сөрөн тэсвэрлэх чадавхийг хангах, кибер халдлага, зөрчлийг мэдээлэх, бүртгэх, хариу арга хэмжээ авах, нөхөн сэргээх, мэдээллийн дэд бүтэцтэй этгээдийн үүрэг, хяналт, хариуцлагатай холбогдсон харилцаанд үйлчилнэ.

3.2.Монгол Улсын нутаг дэвсгэрт байгаа эсэхээс үл хамааран Монгол Улсын кибер орчин дахь мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийн дэд бүтцэд чиглэсэн кибер халдлага, зөрчил, түүнд авах хариу арга хэмжээнд болон эдгээртэй холбоотой үйл ажиллагаа явуулж байгаа гадаадын иргэн, харьяалалгүй хүн, гадаад улсын хуулийн этгээдэд энэ хууль үйлчилнэ.

3.3.Энэ хуульд заасан кибер сөрөн тэсвэрлэх чадавхийн аудит, кибер эрсдэлийн үнэлгээний зохицуулалт нь Төрийн аудитын байгууллагаас хуульд заасан бүрэн эрхийн хүрээнд хийх төрийн аудитын харилцаанд хамаарахгүй.

4 дүгээр зүйл.Нэр томьёоны тодорхойлолт

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

4.1.1.“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 талбарыг;

4.1.2.“кибер орчин” гэж мэдээлэл, өгөгдөлд хандах, нэвтрэх, цуглуулах, боловсруулах, хадгалах, ашиглах, дамжуулах боломж олгож байгаа мэдээллийн систем, мэдээллийн сүлжээний орчныг;

4.1.3.“өгөгдөл” гэж мэдээллийн систем, мэдээллийн сүлжээ, төхөөрөмж, программ хангамж, цахим үйлчилгээний ажиллагаанд үүссэн, боловсруулагдсан, хадгалагдсан, дамжуулагдсан, ашиглагдсан цахим буюу машин унших боломжтой хэлбэрээр илэрхийлэгдсэн мэдээллийг;

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

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

4.1.6.“мэдээллийн дэд бүтэц” гэж мэдээлэл, өгөгдөл боловсруулах, хадгалах, дамжуулах, солилцох, хамгаалах, үйлчилгээ үзүүлэх зориулалттай мэдээллийн систем, мэдээллийн сүлжээ, программ хангамж, техник хангамж, мэдээллийн сан, дата төв, үүлэн үйлчилгээ, тэдгээрийн үйл ажиллагааг хангах харилцан хамааралтай техникийн болон зохион байгуулалтын цогцыг;

4.1.7.“мэдээллийн хөрөнгө” гэж байгууллагын үйл ажиллагаа, үйлчилгээ, шийдвэр гаргалт, эрх, үүргийн хэрэгжилтэд үнэ цэн бүхий мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, программ хангамж, техник хангамж, мэдээллийн сан, баримт бичиг, үйлчилгээ болон тэдгээртэй холбоотой эрх, хандалт, тохиргоог;

4.1.8.“үндсэн үйлчилгээ” гэж тасалдах, доголдох, эсхүл ашиглах боломжгүй болох тохиолдолд онц чухал буюу чухал мэдээллийн дэд бүтэцтэй этгээдийн үндсэн чиг үүрэг, хэрэглэгчийн эрх, олон нийтийн үйлчилгээ, нийгэм, эдийн засгийн хэвийн ажиллагаанд шууд нөлөөлөх үйлчилгээг;

4.1.9.“үндсэн өгөгдөл” гэж онц чухал буюу чухал үйлчилгээний тасралтгүй ажиллагаа, хэрэглэгчийн эрх, төрийн мэдээллийн сан, төлбөр тооцоо, бүртгэл, шийдвэр гаргалт, мэдээллийн дэд бүтцийн хэвийн ажиллагаанд зайлшгүй шаардлагатай өгөгдлийг;

4.1.10.“кибер сөрөн тэсвэрлэх чадавх” гэж кибер орчин дахь халдлагыг сөрөн зогсох, даван гарах, хариу арга хэмжээ авах, тасралтгүй ажиллагааг хангах, сэргээн ажиллуулах, мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй болон тасралтгүй байдлыг хангах цогц үйл явцыг;

4.1.11.“кибер занал” гэж мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй болон тасралтгүй байдалд сөрөг нөлөөлөл учруулж болзошгүй нөхцөл, үйлдэл, үйл ажиллагаа, техникийн арга хэрэгсэл, эмзэг байдал ашиглах боломжийг;

4.1.12.“кибер эрсдэл” гэж кибер орчин дахь кибер занал, эмзэг байдал, алдаа, буруу тохиргоо, хүний хүчин зүйл, гуравдагч этгээд, байгалийн болон техникийн шалтгаанаас мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтэц, байгууллага, хүн, үндэсний аюулгүй байдалд сөрөг нөлөөлөл учрах магадлал болон түүнээс үүдэн гарах үр дагаврыг;

4.1.13.“кибер зөрчил” гэж мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдалд зөвшөөрөлгүй хандах, нөлөөлөх, өөрчлөх, устгах, саатуулах, эсхүл уг эрсдэлийг бодитоор үүсгэсэн үйлдэл, эс үйлдэхүйг;

4.1.14.“кибер халдлага” гэж мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдалд зөвшөөрөлгүй нэвтрэх, нөлөөлөх, өөрчлөх, устгах, хуулбарлах, саатуулах, тасалдуулах, хяналт тогтоох зорилготой санаатай үйлдлийг;

4.1.15.“ноцтой кибер халдлага, зөрчил” гэж энэ хуулийн 32 дугаар зүйлд заасан шалгуурыг хангасан кибер халдлага, зөрчлийг;

4.1.16.“онц чухал мэдээллийн дэд бүтэц” гэж тасалдах, алдагдах, гэмтэх, халдлагад өртөх тохиолдолд үндэсний аюулгүй байдал, хүний амь нас, эрүүл мэнд, санхүү, эрчим хүч, харилцаа холбоо, төрийн үйлчилгээ, нийгэм, эдийн засгийн хэвийн ажиллагаанд ноцтой хохирол учруулж болзошгүй мэдээллийн дэд бүтцийг;

4.1.17.“онц чухал мэдээллийн дэд бүтэцтэй этгээд” гэж энэ хуульд заасан шалгуурын дагуу онц чухал мэдээллийн дэд бүтэц ашиглаж, эзэмшиж, эсхүл хариуцаж байгаа хүн, хуулийн этгээдийг;

4.1.18.“чухал мэдээллийн дэд бүтэц” гэж тасалдах, алдагдах, гэмтэх, халдлагад өртөх тохиолдолд олон нийт, эдийн засаг, тодорхой салбар, үйлчилгээний хэвийн ажиллагаанд энэ хуулийн 7.1.4-т заасан журмын босго үзүүлэлтэд хүрэх сөрөг нөлөө үзүүлэх боловч онц чухал мэдээллийн дэд бүтцийн шалгуурт бүрэн хамаарахгүй мэдээллийн дэд бүтцийг;

4.1.19.“чухал мэдээллийн дэд бүтэцтэй этгээд” гэж энэ хуульд заасан шалгуурын дагуу чухал мэдээллийн дэд бүтэц ашиглаж, эзэмшиж, эсхүл хариуцаж байгаа хүн, хуулийн этгээдийг;

4.1.20.“кибер халдлага, зөрчилтэй тэмцэх төв” гэж кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, мэдээллийн системийг нөхөн сэргээх, шинжлэх, сэрэмжлүүлэх үйл ажиллагааг зохицуулж, мэргэжлийн удирдлагаар хангах чиг үүрэг бүхий төв, нэгжийг;

4.1.21.“салбарын эрх бүхий байгууллага” гэж тухайн салбарын бодлого, зохицуулалт, хяналт, бүртгэл, зөвшөөрөл, эсхүл үйл ажиллагааны уялдааг хуульд заасан бүрэн эрхийн хүрээнд хэрэгжүүлэх төрийн байгууллагыг;

4.1.22.“салбарын мэдээлэл солилцоо, дүн шинжилгээний төв” гэж тухайн салбарын байгууллагууд кибер занал, эмзэг байдал, халдлагын үзүүлэлт, сургамж, сайн туршлага, эрсдэлийн мэдээллийг итгэлцэл, нууцлалын дэглэмийн хүрээнд солилцох, нэгтгэн дүн шинжилгээ хийх, түгээх зорилготой төр, хувийн хэвшлийн хамтын ажиллагааны бүтцийг;

4.1.23.“аюулын мэдээлэл” гэж кибер халдлага, кибер занал, эмзэг байдал, халдлагын үзүүлэлт, арга барил, нөлөөлөл, эрсдэлийн түвшин, нөхцөл байдлын үнэлгээ, хамгаалах арга хэмжээний талаарх мэдээллийг;

4.1.24.“халдлагын үзүүлэлт” гэж кибер халдлага, зөрчлийг илрүүлэх, таних, баталгаажуулах, хянах, хариу арга хэмжээ авахад ашиглагдах интернэт протоколын хаяг, домэйн нэр, холбоос, файл, хэш утга, команд удирдлагын хаяг, техникийн бүртгэлийн мэдээлэл, халдлагын арга барил болон бусад техникийн шинж тэмдгийг;

4.1.25.“мэдэгдэл” гэж кибер халдлага, зөрчил гарсан, эсхүл гарах бодит эрсдэл бий болсон талаар энэ хуульд заасан этгээдээс Кибер аюулгүй байдлын үндэсний төв, кибер халдлага, зөрчилтэй тэмцэх холбогдох төв, эсхүл эрх бүхий байгууллагад хүргүүлсэн мэдээллийг;

4.1.26.“интернэт протоколын хаяг” гэж интернэт протоколд суурилсан мэдээллийн сүлжээнд холбогдсон төхөөрөмж, мэдээллийн систем, үйлчилгээний хаягийг танихад ашиглах тоон болон тэмдэгтийн хаягийг;

4.1.27.“техникийн бүртгэлийн мэдээлэл” гэж мэдээллийн систем, мэдээллийн сүлжээ, төхөөрөмж, программ хангамж, үйлчилгээ, хэрэглэгчийн хандалт, холболт, үйлдэл, алдаа, тохиргоо, аюулгүй байдлын үйл явдлын огноо, цаг, эх үүсвэр, чиглэл, төлөв, үйлдлийн төрлийг автоматаар бүртгэсэн мэдээллийг;

4.1.28.“хортой урсгал” гэж мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээний хэвийн ажиллагааг саатуулах, зөвшөөрөлгүй хандах, өгөгдөл өөрчлөх, устгах, дамжуулах, хортой

код ажиллуулах, команд удирдлагын холбоо тогтоох шинж бүхий өгөгдлийн урсгал, холболтын оролдлого, дамжуулалтыг;

4.1.29.“эмзэг байдал” гэж мэдээллийн систем, мэдээллийн сүлжээ, программ хангамж, техник хангамж, үйл ажиллагааны дараалал, хүний хүчин зүйлд байгаа бөгөөд кибер халдлага, зөрчил, доголдол үүсгэхэд ашиглагдаж болзошгүй сул тал, алдаа, буруу тохиргоог;

4.1.30.“техникийн эмзэг мэдээлэл” гэж кибер халдлага үйлдэх, хамгаалалтын арга хэмжээг тойрч гарах, мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцэд зөвшөөрөлгүй хандахад ашиглагдаж болзошгүй эмзэг байдал, тохиргоо, нэвтрэх эрх, түлхүүр, сүлжээний бүтэц, хамгаалалтын арга хэмжээний дэлгэрэнгүй мэдээллийг;

4.1.31.“эмзэг байдлыг зохицуулалттай ил болгох” гэж эмзэг байдлыг олж тогтоосон этгээд түүнийг энэ хуульд заасан сувгаар хариуцсан этгээдэд мэдээлж, засварлах боломж олгох, мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцэд хор хохирол учруулахгүйгээр шийдвэрлэх ажиллагааг;

4.1.32.“кибер эрсдэлийн үнэлгээ” гэж мэдээллийн хөрөнгө, кибер занал, эмзэг байдал, магадлал, нөлөөлөл, эрсдэлийн түвшин, эрсдэлийг бууруулах арга хэмжээг тодорхойлох үйл ажиллагааг;

4.1.33.“кибер сөрөн тэсвэрлэх чадавхийн аудит” гэж байгууллагын мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтэц, үйл ажиллагааны дараалал, удирдлага, хяналт, хамгаалалтын арга хэмжээ хууль, стандарт, гэрээ, дотоод бодлогын шаардлага хангаж байгаа эсэхийг хараат бус байдлаар үнэлэх үйл ажиллагааг;

4.1.34.“нийлүүлэлтийн сүлжээний кибер эрсдэл” гэж нээлттэй эхийн болон хаалттай программ хангамж, техник хангамж, үүлэн үйлчилгээ, гуравдагч этгээд, туслан гүйцэтгэгч, мэдээллийн технологийн үйлчилгээ үзүүлэгч, программ хангамжийн ашиглах эрх, засвар, шинэчлэлт, үйлчилгээтэй холбоотой кибер эрсдэлийг;

4.1.35.“томоохон өөрчлөлт” гэж үндсэн үйлчилгээний тасралтгүй ажиллагаа, өгөгдлийн боловсруулалт, хандалтын удирдлага, мэдээллийн сүлжээний бүтэц, гуравдагч этгээдийн хамааралд нөлөөлөх өөрчлөлтийг;

4.1.36.“кибер хямрал” гэж энэ хуулийн 62 дугаар зүйлд заасан нөхцөл үүссэний улмаас үндэсний хэмжээний кибер сөрөн тэсвэрлэх чадавх, онц чухал болон чухал мэдээллийн дэд бүтцийн тасралтгүй ажиллагаанд ноцтой эрсдэл үүссэн байдлыг;

4.1.37.“идэвхтэй кибер ажиллагаа” гэж Монгол Улсын батлан хамгаалах зорилгоор эрх бүхий удирдлагын бичгээр олгосон шийдвэр, хууль зүйн дүгнэлт, эрсдэлийн үнэлгээ, хяналтын дэглэмийн үндсэн дээр кибер орчинд зорилтот нөлөөлөл үзүүлэх, саармагжуулах, таслан зогсоох, хязгаарлах, хууран саатуулах зорилготой ажиллагааг;

4.1.38.“Кибер командлал” гэж Зэвсэгт хүчний тухай хуулийн 7.3-т заасан кибер аюулгүй байдлын асуудал хариуцсан төрлийн цэргийн командлалыг.

5 дугаар зүйл.Кибер сөрөн тэсвэрлэх чадавхийг хангах зарчим

5.1.Кибер сөрөн тэсвэрлэх чадавхийг хангах үйл ажиллагаанд Үндэсний аюулгүй байдлын тухай хуулийн 4.1-д зааснаас гадна дараах зарчмыг баримтална:

5.1.1.үндэсний аюулгүй байдал, нийтийн ашиг сонирхол, хүний эрх, эрх чөлөөний баталгааны зохистой тэнцвэрийг хангах;

5.1.2.төрийн байгууллага, мэдээллийн дэд бүтэцтэй этгээд, хувийн хэвшил, иргэний нийгмийн хамтын ажиллагаанд тулгуурлах;

5.1.3.эрсдэлд суурилсан, шуурхай, уялдсан удирдлагатай байх;

5.1.4.авах арга хэмжээ нь зайлшгүй, зорилгодоо нийцсэн, зохистой хэмжээтэй байх;

5.1.5.мэдээлэл солилцоо, хариу арга хэмжээ, нөхөн сэргээх ажиллагааны тасралтгүй байдлыг хангах;

5.1.6.үндэсний бүтээгдэхүүн, үйлчилгээ, хүний нөөц, судалгаа, инновацын чадавхыг дэмжих;

5.1.7.олон улсын хамтын ажиллагаа, харилцан мэдээлэл солилцоонд тулгуурлах;

5.1.8.хариуцлагатай, ил тод, хяналттай байх.

5.2.Энэ хуульд заасан арга хэмжээг хэрэгжүүлэхдээ хүний эрх, эрх чөлөө, хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй болон тасралтгүй байдлыг хамгаална.

5.3.Энэ хуулийг хэрэгжүүлэхдээ иргэний үзэл бодлоо илэрхийлэх, хэвлэн нийтлэх, судалгаа шинжилгээ хийх, төрийн болон албаны нууцад хамаарахгүй мэдээлэл хайх, хүлээн авах, хууль ёсны программ хангамж хөгжүүлэх, мэдээллийн технологийн үйлчилгээг ердийн журмаар ашиглах эрхийг үндэслэлгүйгээр хязгаарлахгүй.

ХОЁРДУГААР БҮЛЭГ

КИБЕР СӨРӨН ТЭСВЭРЛЭХ ЧАДАВХИЙГ ХАНГАХ ТОГТОЛЦОО, УДИРДЛАГА, ЧИГ ҮҮРЭГ

6 дугаар зүйл.Монгол Улсын Их Хурлын бүрэн эрх

6.1. Монгол Улсын Их хурал кибер сөрөн тэсвэрлэх чадавхийг хангах талаар дараах бүрэн эрхийг хэрэгжүүлнэ:

6.1.1.кибер аюулгүй байдал, кибер сөрөн тэсвэрлэх чадавхийг хангах хууль тогтоомжийн хэрэгжилтэд хяналт тавьж энэ талаарх Засгийн газрын тайлан, мэдээллийг хэлэлцэх;

6.1.2.кибер аюулгүй байдал, кибер сөрөн тэсвэрлэх чадавхийг хангахтай холбоотой төсөв, эрх зүйн үндсийг батлах.

7 дугаар зүйл.Засгийн газрын бүрэн эрх

7.1.Засгийн газар кибер сөрөн тэсвэрлэх чадавхийг хангах талаар дараах бүрэн эрхийг хэрэгжүүлнэ:

7.1.1.кибер сөрөн тэсвэрлэх чадавхийг хангах үндэсний бодлого, стратеги, төлөвлөгөө, олон улсын хамтын ажиллагааны бодлогыг батлах, хэрэгжилтэд хяналт тавих;

7.1.2.Монгол Улсын Засгийн газрын тухай хуулийн 18^4 дүгээр зүйлд заасны дагуу Кибер аюулгүй байдлын үндэсний төвийн дүрэм, бүтэц, орон тооны дээд хязгаарыг батлах, Кибер аюулгүй байдлын үндэсний төвийн даргыг томилж, чөлөөлөх;

7.1.3.Кибер аюулгүй байдлын үндэсний төвийн саналыг үндэслэн кибер халдлага, зөрчлийг мэдээлэх, хүлээн авах, бүртгэх, ангилах, харилцан мэдээлэл солилцох, шилжүүлэх, давхардлыг арилгах, анхны хариу арга хэмжээ авах, үндсэн хариуцагч, мэдээллийн харьяалал, байгууллага хоорондын чиг үүрэг, хариуцлагын заагийг тогтоох нийтлэг журам болон кибер хямралын үед шуурхай зохион байгуулалт хийх журмыг батлах;

7.1.4.Кибер аюулгүй байдлын үндэсний төвийн саналыг үндэслэн онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийг ангилах, бүртгэх, жагсаалт тогтоох, шинэчлэх журмыг батлах, тэдгээрийн жагсаалтыг батлах, шинэчлэх;

7.1.5.Кибер аюулгүй байдлын үндэсний төвийн саналыг үндэслэн кибер сөрөн тэсвэрлэх чадавхийн аудит, кибер эрсдэлийн үнэлгээ хийх, аудит, үнэлгээ хийх этгээдийг бүртгэх нийтлэг журмыг батлах;

7.1.6.Кибер аюулгүй байдлын үндэсний төвийн саналыг үндэслэн салбарын мэдээлэл солилцоо, дүн шинжилгээний төв байгуулах, бүртгэх, ажиллуулах, мэдээлэл солилцох, шуурхай холбоо барих суваг, байнгын шуурхай холбоо барих горим хэрэгжүүлэх нөхцөл, шаардлагыг тогтоосон нийтлэг журмыг батлах;

7.1.7.Кибер аюулгүй байдлын үндэсний төвийн саналыг үндэслэн онц чухал болон чухал мэдээллийн дэд бүтцийн кибер сөрөн тэсвэрлэх чадавхийг хангах суурь шаардлагыг батлах;

7.1.8.Кибер аюулгүй байдлын үндэсний төв болон Кибер командлалын саналыг үндэслэн идэвхтэй кибер ажиллагааны нарийвчилсан журам, зөвшөөрлийн шатлал, хууль зүйн хяналт, эрсдэлийн үнэлгээ, ажиллагааны бүртгэл, хяналт, тайлагналын дэглэмийг төрийн болон албаны нууцын тухай хууль тогтоомжид нийцүүлэн батлах;

7.1.9.ноцтой кибер халдлага, зөрчил, кибер хямралын үед Засгийн газрын түвшний шуурхай удирдлага, зохион байгуулалтыг хэрэгжүүлэх, үндэсний аюулгүй байдлын түвшинд хамаарах асуудлыг хуульд заасан журмын дагуу Үндэсний аюулгүй байдлын зөвлөлд танилцуулах;

8 дугаар зүйл.Кибер аюулгүй байдлын үндэсний төв

8.1.Кибер аюулгүй байдлын үндэсний төв нь Ерөнхий сайдын эрхлэх асуудлын хүрээнд кибер сөрөн тэсвэрлэх чадавхийг хангах бодлогын хэрэгжилтийг улсын хэмжээнд уялдуулан зохион байгуулах чиг үүрэг бүхий төрийн захиргааны байгууллага байна.

8.2.Кибер аюулгүй байдлын үндэсний төв нь кибер халдлага, зөрчлийг мэдэгдэх нэг цонхны цахим систем ажиллуулах, онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийн бүртгэл хөтлөх, кибер эрсдэлийн үнэлгээ, кибер сөрөн тэсвэрлэх чадавхийн аудитын тайлангийн хэрэгжилтэд хяналт-шинжилгээ хийх, төр, хувийн хэвшлийн мэдээлэл солилцоог зохион байгуулах, кибер сөрөн тэсвэрлэх чадавхийг хангах арга зүйн дэмжлэг үзүүлэх үндсэн чиг үүрэгтэй байна.

8.3.Кибер аюулгүй байдлын үндэсний төв нь байнгын ажиллагаатай кибер халдлага, зөрчлийг мэдэгдэх нэг цонхны цахим систем болон үндэсний кибер нөхцөл байдлын хяналт-шинжилгээний төвтэй байна.

8.4.Энэ хуульд заасан Кибер аюулгүй байдлын үндэсний төвийн чиг үүрэг, эрх нь хууль сахиулах, тагнуул, батлан хамгаалах байгууллагын хуулиар олгосон бүрэн эрхийг орлохгүй бөгөөд тус төвд мөрдөн шалгах ажиллагаа, зөрчил шалган шийлиар олгосон бүрэн эрхийг орлохгүй бөгөөд тус төвд мөрдөн шалгах ажиллагаа, зөрчил шалган шийдвэрлэх ажиллагаа, гүйцэтгэх ажил, тагнуулын ажиллагаа, идэвхтэй кибер ажиллагаа явуулах эрх олгосонд тооцохгүй.

8.5.Кибер аюулгүй байдлын үндэсний төв нь өөрийн чиг үүргийг хэрэгжүүлэх явцдаа гаргасан шийдвэрийг эс зөвшөөрвөл тухайн этгээд Захиргааны ерөнхий хуульд заасан журмаар гомдол гаргах эрхтэй. Гомдол гаргасан нь хүний амь нас, онц чухал мэдээллийн дэд бүтэц, үндэсний аюулгүй байдалд шууд эрсдэл учирсан тохиолдолд яаралтай хэрэгжүүлэх арга хэмжээг түдгэлзүүлэх үндэслэл болохгүй.

9 дүгээр зүйл.Кибер аюулгүй байдлын үндэсний төвийн чиг үүрэг

9.1.Кибер аюулгүй байдлын үндэсний төв кибер сөрөн тэсвэрлэх чадавхийг хангах талаар дараах чиг үүргийг хэрэгжүүлнэ:

9.1.1.кибер сөрөн тэсвэрлэх чадавхийг хангах бодлого, стратеги, төлөвлөгөөний хэрэгжилтийг улсын хэмжээнд уялдуулан зохион байгуулах, хүний нөөц, сургалт, судалгаа, инновацын бодлогын хэрэгжилтийг дэмжих;

9.1.2.кибер халдлага, зөрчлийг мэдэгдэх нэг цонхны цахим системийг байнгын ажиллагаатай ажиллуулж, иргэн, хуулийн этгээд, төрийн байгууллага, онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдээс ирүүлсэн мэдэгдлийг хүлээн авах, бүртгэх, ангилах, техникийн дүн шинжилгээ хийх, шаардлагатай байгууллагад шилжүүлэх, буцаан мэдээлэх ажиллагааг зохион байгуулах;

9.1.3.ноцтой кибер халдлага, зөрчил, кибер хямралын үед мэдээлэл солилцоо, шуурхай хариу арга хэмжээ, хохирлыг бууруулах, тархалтыг хязгаарлах, сэргээн ажиллуулах ажиллагааны уялдааг хангах;

9.1.4.кибер халдлага, зөрчил, кибер занал, эмзэг байдал, халдлагын үзүүлэлтийн талаар холбогдох байгууллага, этгээдэд сэрэмжлүүлэг, техникийн зөвлөмж хүргүүлэх, олон нийтэд кибер сэрэмжлүүлэг мэдээлэх;

9.1.5.онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийн бүртгэл, ангилал, эрсдэлийн түвшинг хөтлөх, жагсаалтыг жил бүр хянан үзэж, шаардлагатай өөрчлөлтийн саналыг Засгийн газарт хүргүүлэх;

9.1.6.кибер эрсдэлийн үнэлгээ, кибер сөрөн тэсвэрлэх чадавхийн аудитын тайланг хүлээн авах, тайланд туссан эрсдэл, зөрчил, зөвлөмжийн хэрэгжилтэд хяналт тавих, аудит, үнэлгээ хийх этгээдийн бүртгэлийн хэрэгжилтэд хяналт тавих;

9.1.7.кибер сөрөн тэсвэрлэх чадавхийг хангах суурь шаардлага, стандарт, аргачлал, зөвлөмжийн төслийг боловсруулах, тэдгээрийн хэрэгжилтэд мэргэжил, арга зүйн дэмжлэг үзүүлэх;

9.1.8.салбарын мэдээлэл солилцоо, дүн шинжилгээний төв байгуулах, бүртгэх, тэдгээрийн үйл ажиллагаанд арга зүйн дэмжлэг үзүүлэх, төр, хувийн хэвшлийн мэдээлэл солилцооны итгэлцлийн орчныг бүрдүүлэх;

9.1.9.төрийн байгууллага, онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийн кибер халдлага, зөрчилд хариу арга хэмжээ авах сургуулилалтыг зохион байгуулах;

9.1.10.эмзэг байдлыг зохицуулалттай ил болгох үндэсний сувгийг ажиллуулах;

9.1.11.улсын хэмжээнд кибер халдлага, зөрчилтэй тэмцэх төв, нэгжийн мэдээлэл солилцоо, мэдэгдэл хүлээн авах, шилжүүлэх, буцаан мэдээлэх ажиллагааг энэ хуульд заасан хүрээнд уялдуулах, мэргэжил, арга зүйн дэмжлэг үзүүлэх;

9.1.12.гадаад улсын болон олон улсын кибер халдлага, зөрчилтэй тэмцэх төв, нэгж, кибер сөрөн тэсвэрлэх чиг үүрэг бүхий байгууллагатай өөрийн бүрэн эрхийн хүрээнд харилцах, хамтран ажиллах, мэдээлэл солилцох;

9.1.13.Засгийн газраас баталсан журмын хүрээнд онц чухал мэдээллийн дэд бүтэц, төрийн болон албаны нууц, төрийн суурь мэдээллийн сан, үндэсний аюулгүй байдалд шууд нөлөөлөх мэдээллийн технологийн төсөл, хөтөлбөрт тагнуулын байгууллагын саналыг үндэслэн кибер аюулгүй байдлын эрсдэлийн дүгнэлт гаргах;

10 дугаар зүйл.Кибер аюулгүй байдлын үндэсний төвийн эрх

10.1.Кибер аюулгүй байдлын үндэсний төв энэ хуульд заасан чиг үүргээ хэрэгжүүлэхдээ дараах эрхтэй:

10.1.1.энэ хуульд хамрагдах этгээдээс кибер халдлага, зөрчлийн мэдэгдэл, бүртгэл, ангилал, техникийн дүн шинжилгээ, кибер эрсдэлийн үнэлгээ, кибер сөрөн тэсвэрлэх чадавхийн аудит, хамгаалалтын арга хэмжээ, тасралтгүй ажиллагаа, сэргээн ажиллуулах ажиллагаанд шууд хамаарах мэдээлэл, тайлан, баримтыг хуульд заасан хүрээнд гаргуулах;

10.1.2.кибер сөрөн тэсвэрлэх чадавхийг хангах, эрсдэл бууруулах, кибер халдлага, зөрчлийн хохирлыг бууруулах, тархалтыг хязгаарлах, сэргээн ажиллуулах, нэмэлт аудит, үнэлгээ хийлгэх, тайлан, зөвлөмжийн хэрэгжилтийг хангах талаар албан шаардлага, зөвлөмж хүргүүлэх;

10.1.3.онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийн суурь шаардлагын хэрэгжилт, кибер халдлага, зөрчилд хариу арга хэмжээ авах төлөвлөгөө, нөөцлөлт, сэргээх чадавх, техникийн бүртгэлийн мэдээлэл хөтлөлт, сургуулилалтын бэлэн байдал, кибер эрсдэлийн үнэлгээ, аудитын зөвлөмжийн биелэлтийг хуульд заасан хүрээнд шалгах;

10.1.4.салбарын эрх бүхий байгууллага, салбарын мэдээлэл солилцоо, дүн шинжилгээний төв, кибер халдлага, зөрчилтэй тэмцэх төв, хууль сахиулах, тагнуул, батлан хамгаалах байгууллага, харилцаа холбоо, интернэт, дата төв, домэйн нэр, хостинг, үүлэн үйлчилгээ үзүүлэгчтэй хуульд заасан хүрээнд мэдээлэл солилцох;

10.1.5.энэ хуулийн 7.1.3-т заасан нийтлэг журмыг хэрэгжүүлэх мэдэгдлийн маягт, техникийн ангиллын аргачлал, мэдээлэл солилцох суваг, нэг цонхны цахим системийн ажиллагааны заавар, кибер халдлага, зөрчлийн тохиолдлын бүртгэл, шилжүүлэг, буцаан мэдээлэх аргачлалыг батлах;

10.1.6.кибер сөрөн тэсвэрлэх чадавхийг хангахтай холбоотой статистик мэдээлэл, хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууцад үл хамаарах нэгтгэсэн тайлан, сэрэмжлүүлэг, зөвлөмжийг нийтлэх;

10.1.7.энэ хуулийн 9.1.13-т заасан кибер аюулгүй байдлын эрсдэлийн дүгнэлт гаргахад шаардлагатай мэдээлэл, баримт бичгийг гаргуулах;

ГУРАВДУГААР БҮЛЭГ
КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ ТОГТОЛЦОО

11 дүгээр зүйл.Кибер халдлага, зөрчилтэй тэмцэх тогтолцоо

11.1.Монгол Улсад кибер халдлага, зөрчилтэй тэмцэх тогтолцоо дараах бүрэлдэхүүнтэй байна:

11.1.1.тагнуулын байгууллагын бүтцэд ажиллах кибер халдлага, зөрчилтэй тэмцэх төв;

11.1.2.Зэвсэгт хүчний Кибер командлалын цэргийн кибер халдлага, зөрчилтэй тэмцэх чиг үүрэг бүхий нэгж;

11.1.3.цагдаагийн байгууллагын кибер гэмт хэрэгтэй тэмцэх нэгж;

11.1.4.салбарын кибер халдлага, зөрчилтэй тэмцэх төв, нэгж;

11.1.5.байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв, нэгж;

11.1.6.салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн шуурхай мэдээлэл солилцооны баг.

11.2.Энэ хуулийн 11.1-д заасан төв, нэгж, баг болон Кибер аюулгүй байдлын үндэсний төв нь кибер халдлага, зөрчлийн талаарх мэдээллийг харилцан солилцох, хүлээн авах, шилжүүлэх, хариу арга хэмжээ авах ажиллагааг энэ хуулийн 7.1.3-т заасан нийтлэг журмын дагуу хэрэгжүүлнэ.

11.3.Энэ хуулийн 11.2-т заасан журмыг хэрэгжүүлэх техникийн аргачлал, мэдээлэл солилцох маягт, шуурхай холбоо барих суваг, кибер халдлага, зөрчлийн тохиолдол шилжүүлэх ажиллагааны зааврыг Кибер аюулгүй байдлын үндэсний төв батална.

12 дугаар зүйл.Тагнуулын байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв

12.1.Тагнуулын байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв нь тагнуулын байгууллагын бүтцэд ажиллаж, гадаад улсын оролцоотой, зохион байгуулалттай, төрийн болон албаны нууц, үндэсний аюулгүй байдал, төрийн мэдээллийн системд шууд нөлөөлөх кибер занал, кибер халдлага, зөрчилтэй тэмцэх чиг үүргийг хуульд заасан хүрээнд хэрэгжүүлнэ.

12.2.Тагнуулын байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв нь төрийн онц чухал мэдээллийн дэд бүтэц, төрийн болон албаны нууц бүхий мэдээллийн систем, төрийн мэдээллийн системд холбогдсон байгууллагад гарсан кибер халдлага, зөрчилд хариу арга хэмжээ авахад хуульд заасан хүрээнд мэргэжил, арга зүйн дэмжлэг үзүүлж, нөхцөл байдлын мэдээлэлд дүн шинжилгээ хийнэ.

12.3.Тагнуулын байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв нь энэ хуулийн 12.1, 12.2-т заасан чиг үүргээ хэрэгжүүлэхдээ төрийн байгууллага, хувийн хэвшил, онц чухал мэдээллийн дэд бүтэцтэй этгээд, чухал мэдээллийн дэд бүтэцтэй этгээдтэй кибер халдлага, зөрчлийн мэдээлэл солилцох, хүлээн авах, шилжүүлэх ажиллагаанд Кибер аюулгүй байдлын үндэсний төвийн нэг цонхны цахим системтэй уялдан ажиллана.

12.4.Тагнуулын байгууллагын кибер халдлага, зөрчилтэй тэмцэх төвийн энэ зүйлд заасан оролцоо нь Кибер аюулгүй байдлын үндэсний төвийн уялдуулан зохицуулах, мэдээлэл солилцох, бүртгэл хөтлөх чиг үүргийг хязгаарлахгүй.

13 дугаар зүйл.Салбарын болон байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв, нэгж

13.1.Онц чухал мэдээллийн дэд бүтэцтэй этгээд кибер халдлага, зөрчилд хариу арга хэмжээ авах чадавхыг өөрийн байгууллагын кибер халдлага, зөрчилтэй тэмцэх нэгжээр хангах, салбарын кибер халдлага, зөрчилтэй тэмцэх төв, нэгжтэй хамтран хэрэгжүүлэх, эсхүл гэрээт мэргэжлийн үйлчилгээ үзүүлэгчээр дамжуулан бүрдүүлсэн байна.

13.2.Энэ хуулийн 13.1-д заасан чадавх нь шуурхай холбоо барих суваг, хариуцсан нэгж буюу гэрээт мэргэжлийн үйлчилгээ үзүүлэгч, кибер халдлага, зөрчилд хариу арга хэмжээ авах төлөвлөгөө, 24 цагийн дотор ажиллуулах боломжтой техникийн багтай байна.

13.3.Чухал мэдээллийн дэд бүтэцтэй этгээд кибер халдлага, зөрчлийг илрүүлэх, мэдэгдэх, тархалтыг хязгаарлах, нотлох баримт хадгалах, үйлчилгээг сэргээх анхан шатны хариу арга хэмжээ авах чадавхтай байна.

13.4.Энэ хуулийн 13.3-т заасан чадавх нь кибер халдлага, зөрчил хариуцах ажилтан, эсхүл дотоод нэгжтэй байх, шуурхай холбоо барих сувагтай байх, хариу арга хэмжээ авах төлөвлөгөөтэй байх, шаардлагатай тохиолдолд салбарын кибер халдлага, зөрчилтэй тэмцэх төв, нэгж, эсхүл гэрээт мэргэжлийн үйлчилгээ үзүүлэгчээс дэмжлэг авах зохицуулалттай байна.

13.5.Салбарын болон байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв, нэгж нь кибер халдлага, зөрчил, кибер занал, эмзэг байдал, хариу арга хэмжээний холбогдох мэдээллийг Кибер аюулгүй байдлын үндэсний төв болон тухайн салбарын мэдээлэл солилцоо, дүн шинжилгээний төвтэй энэ хуулийн 7.1.3-т заасан нийтлэг журамд заасан давтамж, хэлбэрээр солилцоно.

14 дүгээр зүйл.Цагдаагийн байгууллагын кибер гэмт хэрэгтэй тэмцэх нэгж

14.1.Цагдаагийн байгууллагын кибер гэмт хэрэгтэй тэмцэх нэгж нь кибер орчинд үйлдэгдсэн, эсхүл мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцэд халдах замаар үйлдэгдсэн гэмт хэрэгтэй тэмцэх чиг үүргийг холбогдох хуульд заасан хүрээнд хэрэгжүүлнэ.

14.2.Цагдаагийн байгууллагын кибер гэмт хэрэгтэй тэмцэх нэгж нь кибер халдлага, зөрчил нь гэмт хэргийн шинжтэй бол хэрэг бүртгэлт, мөрдөн байцаалт явуулах, нотлох баримт цуглуулах, бэхжүүлэх, шинжилгээ хийлгэх, гэмт хэрэг үйлдсэн этгээдийг тогтоох ажиллагааг хуульд заасан журмын дагуу хэрэгжүүлнэ.

14.3.Цагдаагийн байгууллагын кибер гэмт хэрэгтэй тэмцэх нэгж нь кибер халдлага, зөрчлийн талаарх мэдээллийг Кибер аюулгүй байдлын үндэсний төв, тагнуулын байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв, Кибер командлал, салбарын болон байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв, нэгжтэй энэ хууль болон холбогдох бусад хуульд заасан хүрээнд солилцоно.

14.4.Кибер аюулгүй байдлын үндэсний төвөөс гэмт хэргийн шинжтэй гэж үзэн шилжүүлсэн кибер халдлага, зөрчлийн мэдээллийг цагдаагийн байгууллагын кибер гэмт хэрэгтэй тэмцэх нэгж хүлээн авч, харьяаллын дагуу шийдвэрлэнэ.

14.5.Цагдаагийн байгууллагын кибер гэмт хэрэгтэй тэмцэх нэгжийн энэ зүйлд заасан чиг үүрэг нь Кибер аюулгүй байдлын үндэсний төвийн кибер халдлага, зөрчлийг мэдээлэх, бүртгэх, ангилах, шилжүүлэх, буцаан мэдээлэх, хариу арга хэмжээг уялдуулах чиг үүргийг хязгаарлахгүй.

ДӨРӨВДҮГЭЭР БҮЛЭГ

КИБЕР КОМАНДЛАЛ, ИДЭВХТЭЙ КИБЕР АЖИЛЛАГАА

15 дугаар зүйл.Кибер командлалын чиг үүрэг, хязгаар

15.1.Кибер командлал нь Зэвсэгт хүчний кибер аюулгүй байдлын цэргийн удирдлага, төлөвлөлт, бэлэн байдал, цэргийн мэдээллийн систем, мэдээллийн сүлжээ, командлал, удирдлага, холбооны кибер сөрөн тэсвэрлэх чадавхийг хангах чиг үүрэг бүхий төрлийн цэргийн командлал байна.

15.2.Кибер командлал нь Зэвсэгт хүчний тухай хууль, Батлан хамгаалах тухай хууль болон холбогдох бусад хууль тогтоомжид заасан цэргийн бүтэц, зохион байгуулалтын хүрээнд

ажиллах бөгөөд иргэний мэдээллийн дэд бүтэц, онц чухал мэдээллийн дэд бүтэц, чухал мэдээллийн дэд бүтцэд шууд удирдлага, хяналт хэрэгжүүлэхгүй.

15.3.Кибер командлал нь иргэн, хуулийн этгээд, төрийн бусад байгууллагатай кибер халдлага, зөрчил, кибер хямралтай холбоотой харилцахдаа Кибер аюулгүй байдлын үндэсний төвийн нэг цонхны цахим систем болон энэ хуулийн 7.1.3-т заасан нийтлэг журмыг баримтална.

15.4.Кибер командлал нь Монгол Улсын батлан хамгаалах зорилгоор идэвхтэй кибер ажиллагаа явуулах тохиолдолд уг ажиллагааг эхлүүлэхээс өмнө эрх бүхий шийдвэр, хууль зүйн дүгнэлт, эрсдэлийн үнэлгээ, ажиллагааны бүртгэл, хяналт, тайлагналын дэглэмийг бичгээр бүрдүүлсэн байна.

16 дугаар зүйл.Кибер командлалын үйл ажиллагаанд тавих хориглолт

16.1.Кибер командлал дараах үйл ажиллагаа явуулахыг хориглоно:

16.1.1.хуульд заасан эрх бүхий шийдвэргүйгээр идэвхтэй кибер ажиллагаа явуулах;

16.1.2.дотоодын улс төрийн нам, эвсэл, нэр дэвшигч, хэвлэл мэдээлэл, иргэний нийгэм, иргэн, хуулийн этгээдийн хууль ёсны үйл ажиллагаанд кибер орчинд нөлөөлөх;

16.1.3.иргэний мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцэд хуульд заасан үндэслэлгүйгээр нэвтрэх, саатуулах, өөрчлөх, устгах;

16.1.4.мөрдөн шалгах ажиллагаа, гүйцэтгэх ажил, тагнуулын ажиллагаа явуулах;

16.1.5.хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууцыг зорилгоос гадуур цуглуулах, ашиглах, дамжуулах;

16.1.6.Монгол Улсын олон улсын гэрээ, олон улсын эрх зүйн нийтлэг зарчимд харшлах ажиллагаа явуулах;

16.1.7.сургалт, туршилт нэрээр бодит мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцэд зөвшөөрөлгүй нөлөөлөл үзүүлэх.

ТАВДУГААР БҮЛЭГ
МЭДЭЭЛЛИЙН ДЭД БҮТЭЦ, МЭДЭЭЛЛИЙН ДЭД БҮТЭЦТЭЙ ЭТГЭЭДИЙН АНГИЛАЛ, БҮРТГЭЛ, ҮҮРЭГ

17 дугаар зүйл.Мэдээллийн дэд бүтэц

17.1.Мэдээллийн дэд бүтцийг дараах байдлаар ангилна:

17.1.1.онц чухал мэдээллийн дэд бүтэц;

17.1.2.чухал мэдээллийн дэд бүтэц;

17.1.3.бусад мэдээллийн дэд бүтэц.

17.2.Мэдээллийн дэд бүтцийн ангиллыг тухайн мэдээллийн дэд бүтцийг ашиглан үзүүлж байгаа үйлчилгээ, мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, программ хангамж, техник хангамж, гуравдагч этгээдийн хамаарал нь Монгол Улсын үндэсний аюулгүй байдал, нийгэм, эдийн засаг, хүний амь нас, эрүүл мэнд, төрийн үйлчилгээ, онц чухал үйлчилгээний тасралтгүй ажиллагаанд үзүүлэх бодит болон болзошгүй нөлөөлөлд үндэслэн тогтооно.

17.3.Мэдээллийн дэд бүтцийн ангиллыг тогтоохдоо тухайн мэдээллийн дэд бүтцийг эзэмшиж, ашиглаж байгаа этгээдийн үйл ажиллагааны салбарын нэршил, өмчийн хэлбэр, байгууллагын хэмжээ, улсын болон хувийн хэвшлийн харьяаллыг дангаар үндэслэхгүй.

18 дугаар зүйл.Мэдээллийн дэд бүтэцтэй этгээдийн ангилал

18.1.Мэдээллийн дэд бүтэцтэй этгээдийн ангиллыг тогтоохдоо дараах шалгуурыг харгалзан тогтооно:

18.1.1.үйлчилгээ тасалдах, өгөгдөл алдагдах, мэдээллийн системийн бүрэн бүтэн байдал алдагдах тохиолдолд нийгэм, эдийн засаг, үндэсний аюулгүй байдалд үзүүлэх нөлөөлөл;

18.1.2.хүний амь нас, эрүүл мэнд, олон нийтийн аюулгүй байдалд учрах эрсдэл;

18.1.3.үйлчилгээний хэрэглэгч, хамаарах этгээдийн тоо, газар зүйн хамрах хүрээ;

18.1.4.тухайн үйлчилгээ, мэдээллийн систем, өгөгдлийг орлуулах боломж, орлуулахад шаардагдах хугацаа;

18.1.5.тухайн этгээдийн мэдээллийн систем бусад мэдээллийн систем, үйлчилгээ, мэдээллийн дэд бүтэц, байгууллага, салбартай харилцан хамаарах байдал;

18.1.6.боловсруулж байгаа өгөгдлийн хэмжээ, шинж чанар, мэдрэг байдал, стратегийн ач холбогдол;

18.1.7.тухайн этгээдээс хамаарах нийлүүлэлтийн сүлжээ, гуравдагч этгээдийн үйлчилгээ, үүлэн үйлчилгээ, дата төв, мэдээллийн сүлжээний хамаарал;

18.1.8.өмнө гарсан кибер халдлага, зөрчил, давтагдсан кибер эрсдэл, аудитын дүгнэлт, кибер эрсдэлийн үнэлгээний үр дүн;

18.1.9.үйлчилгээ тасалдах үед иргэн, хуулийн этгээд, төрийн байгууллага, олон нийтэд учрах шууд болон дам хохирлын хэмжээ;

18.1.10.үндэсний хэмжээний өгөгдөл солилцоо, танилт баталгаажуулалт, төлбөр тооцоо, төрийн үйлчилгээ, олон нийтийн үйлчилгээний хэвийн ажиллагаанд үзүүлэх нөлөөлөл.

18.2.Мэдээллийн дэд бүтэцтэй этгээдийн ангиллыг энэ хуулийн 18.1-д заасан шалгуурыг дангаар бус, нийлбэр байдлаар үнэлж тогтоох бөгөөд шалгуур тус бүрийн оноо, жин, босго үзүүлэлт, үнэлгээний аргачлал, дахин үнэлэх хугацааг энэ хуулийн 7.1.4-т заасан журмаар тогтооно.

19 дүгээр зүйл.Бүртгэл, жагсаалт

19.1.Онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийн бүртгэлийг Кибер аюулгүй байдлын үндэсний төв хөтөлнө.

19.2.Онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийн жагсаалтыг Засгийн газар батална.

19.3.Жагсаалтын нээлттэй болон нууц хэсгийг ялган тогтооно.

19.4.Жагсаалтад оруулах, өөрчлөх, хасах шийдвэр гаргахдаа тухайн этгээдэд мэдэгдэх, тайлбар авах, шаардлагатай тохиолдолд нууцлалын дэглэмийн дор сонсох ажиллагаа явуулах боломж олгоно.

19.5.Жагсаалтад орсон этгээд уг шийдвэрийг Захиргааны ерөнхий хуульд заасан журмаар гомдол гаргах эрхтэй.

20 дугаар зүйл.Онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийн нийтлэг үүрэг

20.1.Онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээд дараах нийтлэг үүрэгтэй:

20.1.1.кибер сөрөн тэсвэрлэх чадавхийг хангах дотоод бодлого, журам батлах;

20.1.2.кибер сөрөн тэсвэрлэх чадавхийг хангах асуудал хариуцсан удирдах албан тушаалтан томилох;

20.1.3.мэдээллийн хөрөнгийн бүртгэл хөтлөх;

20.1.4.кибер халдлага, зөрчилд хариу арга хэмжээ авах төлөвлөгөөтэй байх;

20.1.5.тасралтгүй ажиллагаа, гамшгийн нөхөн сэргээх төлөвлөгөөтэй байх;

20.1.6.нөөцлөлт, сэргээх туршилт хийх;

20.1.7.хандалтын удирдлага, олон хүчин зүйлт баталгаажуулалт хэрэгжүүлэх;

20.1.8.техникийн бүртгэлийн мэдээлэл цуглуулах, хадгалах, хянах, сэжигтэй үйл явдлыг илрүүлэх, хариуцсан этгээдэд мэдэгдэх техникийн болон зохион байгуулалтын чадавхтай байх;

20.1.9.эмзэг байдлын удирдлага, засвар, шинэчлэлтийн ажиллагаа хэрэгжүүлэх;

20.1.10.нийлүүлэлтийн сүлжээний кибер эрсдэлийг удирдах;

20.1.11.ажилтанд кибер сөрөн тэсвэрлэх чадавхийг хангах сургалт зохион байгуулах;

20.1.12.энэ хууль болон холбогдох журамд заасан хэлбэрээр салбарын мэдээлэл солилцоо, дүн шинжилгээний төвтэй мэдээлэл солилцох;

20.1.13.ноцтой кибер халдлага, зөрчил гарсан тохиолдолд энэ хуульд заасан хугацаанд мэдэгдэх.

21 дүгээр зүйл.Онц чухал мэдээллийн дэд бүтэцтэй этгээдийн нэмэлт үүрэг

21.1.Онц чухал мэдээллийн дэд бүтэцтэй этгээд дараах нэмэлт үүрэгтэй:

21.1.1.энэ хуулийн 13.1, 13.2-т заасан хэлбэрээр кибер халдлага, зөрчилд хариу арга хэмжээ авах чадавхтай байх;

21.1.2.жил бүр кибер эрсдэлийн үнэлгээ хийх;

21.1.3.хоёр жил тутам хараат бус кибер сөрөн тэсвэрлэх чадавхийн аудит хийлгэх;

21.1.4.томоохон өөрчлөлт, нийлүүлэгчийн өөрчлөлт, ноцтой кибер халдлага, зөрчлийн дараа нэмэлт кибер эрсдэлийн үнэлгээ хийх;

21.1.5.салбарын кибер сургуулилалтад жил бүр оролцох;

21.1.6.холбогдох журамд заасан хугацаа, хэлбэрээр кибер эрсдэлийн үнэлгээ, кибер сөрөн тэсвэрлэх чадавхийн аудит, сургуулилалт, ноцтой кибер халдлага, зөрчлийн тайланг Кибер аюулгүй байдлын үндэсний төвд хүргүүлэх;

21.1.7.үндсэн үйлчилгээ үзүүлэхэд ашиглагдах мэдээллийн системийн сэргээх хугацааны зорилт, сэргээх цэгийн зорилтыг тогтоох;

21.1.8.үйлдвэрлэлийн технологи, үйл ажиллагааны технологи, автоматжуулалтын системд мэдээллийн сүлжээ тусгаарлах, хандалтын хяналт, өөрчлөлтийн бүртгэл, нөөцлөлт, сэргээх, хяналт-шинжилгээний тусгай арга хэмжээ хэрэгжүүлэх;

21.1.9.гуравдагч этгээдийн хандалт, алсын хандалт, үйлчилгээний эрхийг тусгай журмаар удирдах;

21.1.10.тухайн салбарын мэдээлэл солилцоо, дүн шинжилгээний төвд гишүүнээр элсэж, кибер занал, халдлагын үзүүлэлт, эмзэг байдал, кибер халдлага, зөрчлийн сургамжийн мэдээллийг энэ хууль болон холбогдох журмын хүрээнд солилцох.

22 дугаар зүйл.Чухал мэдээллийн дэд бүтэцтэй этгээдийн нэмэлт үүрэг

22.1.Чухал мэдээллийн дэд бүтэцтэй этгээд дараах нэмэлт үүрэгтэй:

22.1.1.хоёр жил тутам кибер эрсдэлийн үнэлгээ хийх;

22.1.2.гурван жил тутам хараат бус кибер сөрөн тэсвэрлэх чадавхийн аудит хийлгэх;

22.1.3.энэ хуулийн 13.3, 13.4-т заасан хэлбэрээр кибер халдлага, зөрчилд анхан шатны хариу арга хэмжээ авах чадавхтай байх;

22.1.4.ноцтой кибер халдлага, зөрчлийн үед хэрэглэгчид мэдээлэх дотоод журамтай байх;

22.1.5.нийлүүлэлтийн сүлжээний кибер шаардлагыг гэрээнд тусгах.

23 дугаар зүйл.Бусад мэдээллийн дэд бүтэцтэй этгээд, иргэний үүрэг

23.1.Энэ хуулийн 17.1.1, 17.1.2-т заасан онц чухал болон чухал мэдээллийн дэд бүтэцтэй этгээдийн шалгуурт хамаарахгүй боловч мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийн сан, өгөгдөл, программ хангамж, цахим үйлчилгээ эзэмшиж, ашиглаж, боловсруулж, эсхүл мэдээллийн технологийн үйлчилгээ авч байгаа иргэн, хуулийн этгээдийг бусад мэдээллийн дэд бүтэцтэй этгээдэд хамааруулна.

23.2.Бусад мэдээллийн дэд бүтэцтэй этгээд кибер аюулгүй байдлыг хангах талаар дараах үүрэгтэй:

23.2.1.мэдээллийн систем, өгөгдөл, хэрэглэгчийн эрх, нууц үг, хандалтын эрхийг хамгаалах;

23.2.2.кибер халдлага, зөрчил, мэдээлэл алдагдах, үйлчилгээ тасалдах эрсдэлийг бууруулах арга хэмжээ авах;

23.2.3.хүний хувийн мэдээлэл, байгууллагын нууц, гэрээний дагуу хамгаалагдах мэдээллийг хамгаалах;

23.2.4.кибер аюулгүй байдлыг хангах нийтлэг журам, эрх бүхий байгууллагаас нийтэд зориулан гаргасан сэрэмжлүүлэг, зөвлөмжийг үйл ажиллагаандаа мөрдөх;

23.2.5.кибер халдлага, зөрчил нь олон хэрэглэгч, гуравдагч этгээд, онц чухал буюу чухал үйлчилгээ, эсхүл хүний хувийн мэдээлэлд ноцтой нөлөөлөхөөр бол кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд мэдэгдэх, шаардлагатай үед туслалцаа авах;

23.2.6.Кибер аюулгүй байдлын үндэсний төв болон хуульд заасан эрх бүхий байгууллагаас хуульд заасан хүрээнд хүргүүлсэн зөвлөмжийг дагах, албан шаардлагыг биелүүлэх;

23.3.Иргэн кибер аюулгүй байдлыг хангах талаар дараах үүрэгтэй:

23.3.1.өөрийн болон өөрийн асрамжид байгаа хүний мэдээллийн систем, цахим хэрэглээ, нэвтрэх эрх, нууц үг, хувийн мэдээллийн аюулгүй байдлыг хангах;

23.3.2.холбогдох байгууллагаас гаргасан сэрэмжлүүлэг, зөвлөмжийг дагах;

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

ЗУРГААДУГААР БҮЛЭГ

САЛБАРЫН МЭДЭЭЛЭЛ СОЛИЛЦОО, ДҮН ШИНЖИЛГЭЭНИЙ ТӨВ

24 дүгээр зүйл.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн эрх зүйн байдал

24.1.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв нь тухайн салбарын кибер занал, эмзэг байдал, халдлагын үзүүлэлт, кибер халдлага, зөрчил, эрсдэлийн мэдээллийг итгэлцэл, нууцлалын дэглэмийн хүрээнд солилцох, нэгтгэн дүн шинжилгээ хийх, түгээх, салбарын кибер сөрөн тэсвэрлэх чадавхийг нэмэгдүүлэх зорилготой төр, хувийн хэвшлийн хамтын ажиллагааны бүтэц байна.

24.2.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв нь ашгийн төлөө бус хуулийн этгээд, мэргэжлийн холбооны дэргэдэх тусгай нэгж, эсхүл салбарын байгууллагуудын хамтарсан гэрээний үндсэн дээр байгуулагдаж болно.

24.3.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв энэ хуулийн 7.1.6-т заасан нийтлэг журмын дагуу Кибер аюулгүй байдлын үндэсний төвд бүртгүүлнэ.

24.4.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв нь хяналт шалгалт, мөрдөн шалгах ажиллагаа, тагнуулын ажиллагаа, гүйцэтгэх ажил, идэвхтэй кибер ажиллагаа явуулахгүй.

25 дугаар зүйл.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв байгуулах салбар

25.1.Онц чухал мэдээллийн дэд бүтцийн салбарт салбарын мэдээлэл солилцоо, дүн шинжилгээний төв байгуулна.

25.2.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв нь тухайн салбарын эрх бүхий байгууллага, Кибер аюулгүй байдлын үндэсний төв, салбарын кибер халдлага, зөрчилтэй тэмцэх төв, нэгжтэй хамтран ажиллана.

25.3.Салбарын онцлогоос хамааран хэд хэдэн салбар хамтарсан салбарын мэдээлэл солилцоо, дүн шинжилгээний төв байгуулж болно.

26 дугаар зүйл.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн чиг үүрэг

26.1.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв дараах чиг үүрэгтэй:

26.1.1.гишүүн байгууллагаас кибер занал, эмзэг байдал, халдлагын үзүүлэлт, кибер халдлага, зөрчлийн сургамж, эрсдэлийн мэдээлэл хүлээн авах;

26.1.2.мэдээллийг нэгтгэх, дүн шинжилгээ хийх, халдлагад өртсөн этгээдийг шууд болон шууд бусаар тодорхойлох боломжгүй болгох, салбарын эрсдэлийн түвшинг тодорхойлох;

26.1.3.гишүүн байгууллагад сэрэмжлүүлэг, зөвлөмж, хамгаалах арга хэмжээний мэдээлэл хүргэх;

26.1.4.Кибер аюулгүй байдлын үндэсний төв, салбарын кибер халдлага, зөрчилтэй тэмцэх төв, нэгжтэй мэдээлэл солилцох;

26.1.5.салбарын кибер сургуулилалт, ширээний дасгал, дуурайлган сургуулилалт зохион байгуулахад оролцох;

26.1.6.салбарын нийлүүлэлтийн сүлжээний кибер эрсдэлийн мэдээлэл солилцох;

26.1.7.салбарын кибер сөрөн тэсвэрлэх чадавхийг хангах сайн туршлага, загвар журам боловсруулах;

26.1.8.гишүүдийн итгэлцлийн дэглэм, мэдээлэл ангилах тэмдэглэгээ, нууцлалын журмыг хэрэгжүүлэх;

26.1.9.салбарын эрсдэлийн нэгтгэсэн тайланг жил бүр Кибер аюулгүй байдлын үндэсний төвд хүргүүлэх;

26.1.10.тухайн салбарын онц чухал мэдээллийн дэд бүтэц, төрийн болон албаны нууц, төрийн суурь мэдээллийн сан, үндэсний аюулгүй байдалд шууд нөлөөлөх мэдээллийн технологийн төсөл, хөтөлбөрт энэ хуулийн 9.1.13-т заасан кибер аюулгүй байдлын эрсдэлийн дүгнэлт гаргуулахад гишүүн байгууллага, салбарын эрх бүхий байгууллагад мэдээлэл, арга зүйн дэмжлэг үзүүлэх;

27 дугаар зүйл.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн бүтэц

27.1.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн дотоод зохион байгуулалт нь гишүүдийн төлөөлөл бүхий удирдлага, гүйцэтгэх нэгж, мэдээлэл, дүн шинжилгээний чиг үүрэг, шуурхай холбоо барих суваг, нууцлал, ёс зүй, ашиг сонирхлын зөрчлийн хяналтыг агуулсан байна.

27.2.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн удирдах бүтцэд гишүүн байгууллага, салбарын эрх бүхий байгууллага, Кибер аюулгүй байдлын үндэсний төвийн төлөөлөл орж болно.

27.3.Кибер аюулгүй байдлын үндэсний төвийн төлөөлөл салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн өдөр тутмын бизнесийн нууц болон гишүүний дотоод мэдээлэлд зөвхөн хууль, гэрээ, нууцлалын журмын хүрээнд хандана.

27.4.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв нь шуурхай холбоо барих сувагтай байна. Салбарын эрсдэлийн түвшин, онцлогийг харгалзан байнгын шуурхай холбоо барих горим хэрэгжүүлэх нөхцөлийг энэ хуулийн 7.1.6-т заасан нийтлэг журмаар тогтооно.

28 дугаар зүйл.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төвд мэдээлэл солилцох хамгаалалт

28.1.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төвд энэ хууль болон холбогдох журамд заасан мэдээлэл солилцооны хүрээнд өгсөн кибер занал, халдлагын үзүүлэлт, эмзэг байдал, кибер халдлага, зөрчлийн урьдчилсан мэдээллийг дангаар нь тухайн мэдээлэл өгсөн этгээдэд хариуцлага хүлээлгэх үндэслэл болгохгүй.

28.2.Энэ хуулийн 28.1 дэх хэсэг нь кибер халдлага, зөрчлийг санаатай нуун дарагдуулсан, худал мэдээлэл өгсөн, хайхрамжгүй хандсан, эсхүл гэмт хэргийн шинжтэй үйлдэл гаргасан этгээдийг хариуцлагаас чөлөөлөх үндэслэл болохгүй.

28.3.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төвд өгсөн мэдээлэл нь байгууллагын нууц, хүний хувийн мэдээлэл, төрийн болон албаны нууцад хамаарах бол холбогдох хуульд заасан хамгаалалт үйлчилнэ.

28.4.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв нь мэдээллийг дараах байдлаар ангилан тэмдэглэнэ:

28.4.1.нийтэд түгээх боломжтой;

28.4.2.гишүүдэд хязгаарлагдсан;

28.4.3.итгэмжлэгдсэн хүлээн авагчид хязгаарлагдсан;

28.4.4.нууцын тусгай дэглэмтэй;

28.4.5.эх сурвалжийн зөвшөөрөлгүй дахин түгээхийг хориглосон.

29 дүгээр зүйл.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн гишүүний үүрэг

29.1.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн гишүүн дараах үүрэгтэй:

29.1.1.кибер занал, халдлагын үзүүлэлт, эмзэг байдал, кибер халдлага, зөрчлийн сургамжийн мэдээллийг өөрт байгаа бөгөөд хууль, гэрээ, нууцлалын дэглэмээр хориглоогүй мэдээллийн хүрээнд хуваалцах;

29.1.2.авсан мэдээллийг зөвхөн хамгаалах, урьдчилан сэргийлэх, эрсдэлийг бууруулах зорилгоор ашиглах;

29.1.3.бусад гишүүний нууц мэдээллийг зөвшөөрөлгүй задруулахгүй байх;

29.1.4.хуурамч, санаатай төөрөгдүүлсэн мэдээлэл түгээхгүй байх;

29.1.5.салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн нууцлал, ёс зүй, мэдээлэл ангилах журмыг мөрдөх;

29.1.6.ноцтой кибер халдлага, зөрчил гарсан тохиолдолд энэ хуульд заасан мэдэгдэх үүргээ салбарын мэдээлэл солилцоо, дүн шинжилгээний төвд мэдээлэл өгсөн эсэхээс үл хамааран биелүүлэх.

ДОЛООДУГААР БҮЛЭГ

КИБЕР СӨРӨН ТЭСВЭРЛЭХ ЧАДАВХИЙГ ХАНГАХ ДОТООД УДИРДЛАГА, СУУРЬ ШААРДЛАГА

30 дугаар зүйл.Удирдлагын хариуцлага

30.1.Онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийн удирдах байгууллага нь кибер эрсдэлийн удирдлагад хяналт тавих үүрэгтэй.

30.2.Энэ хуулийн 30.1-д заасан этгээдийн гүйцэтгэх удирдлага кибер сөрөн тэсвэрлэх чадавхийг хангах бодлого, төсөв, хүний нөөц, хариуцсан нэгж, хэрэгжилтийг хангана.

30.3.Онц чухал мэдээллийн дэд бүтэцтэй этгээд кибер сөрөн тэсвэрлэх чадавхийг хангах асуудал хариуцсан удирдах албан тушаалтныг гүйцэтгэх удирдлагад шууд тайлагнах байдлаар томилно.

31 дүгээр зүйл.Кибер сөрөн тэсвэрлэх чадавхийг хангах суурь шаардлага

31.1.Онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээд мэдээллийн хөрөнгийн бүртгэл, хандалтын удирдлага, техникийн бүртгэлийн мэдээлэл, мэдээллийн сүлжээний хамгаалалт, эмзэг байдлын удирдлага, нөөцлөлт, сэргээх ажиллагаа, кибер халдлага, зөрчилд хариу арга хэмжээ авах төлөвлөгөө, тасралтгүй ажиллагаа, гуравдагч этгээдийн эрсдэл, ажилтны сургалт, дотоод хяналтын суурь шаардлагыг хэрэгжүүлнэ.

31.2.Кибер сөрөн тэсвэрлэх чадавхийг хангах суурь шаардлага, техникийн үзүүлэлт, хэрэгжилтийн аргачлалыг энэ хуулийн 7.1.7-т заасны дагуу батална.

31.3.Кибер аюулгүй байдлын үндэсний төв энэ хуулийн 31.2-т заасан суурь шаардлагыг хэрэгжүүлэх арга зүйн зөвлөмж, техникийн заавар гаргаж болно.

НАЙМДУГААР БҮЛЭГ
КИБЕР ХАЛДЛАГА, ЗӨРЧЛИЙГ МЭДЭЭЛЭХ, БҮРТГЭХ, ШИЛЖҮҮЛЭХ, ХАРИУ АРГА ХЭМЖЭЭ АВАХ

32 дугаар зүйл.Ноцтой кибер халдлага, зөрчлийн шалгуур

32.1.Дараах нөхцөлийн аль нэг үүссэн бол ноцтой кибер халдлага, зөрчил гэж үзнэ:

32.1.1.онц чухал мэдээллийн дэд бүтэц, чухал мэдээллийн дэд бүтэц, эсхүл тэдгээрийн үндсэн үйлчилгээ тасалдсан, доголдсон, ашиглах боломжгүй болсон, эсхүл энэ хуулийн 7.1.3-т заасан нийтлэг журмаар тогтоосон тасалдах эрсдэлийн босго үзүүлэлтэд хүрсэн;

32.1.2.мэдээлэл алдагдсан, өөрчлөгдсөн, устсан, эсхүл ашиглах боломжгүй болсон хэрэглэгч, иргэн, хуулийн этгээдийн тоо, хамрах хүрээ, мэдээллийн төрөл, эрсдэлийн түвшин нь энэ хуулийн 7.1.3-т заасан нийтлэг журмаар тогтоосон ноцтой кибер халдлага, зөрчлийн босго үзүүлэлтэд хүрсэн;

32.1.3.хүний амь нас, эрүүл мэндэд хохирол учирсан, эсхүл хүний амь нас, эрүүл мэндэд хохирол учрах эрсдэл нь энэ хуулийн 7.1.3-т заасан нийтлэг журмаар тогтоосон ноцтой эрсдэлийн шалгуурт хамаарсан;

32.1.4.санхүүгийн систем, төлбөр тооцоо, улсын төсөв, эдийн засагт учирсан буюу учирч болзошгүй хохирлын хэмжээ, хамрах хүрээ, үргэлжлэх хугацаа нь энэ хуулийн 7.1.3-т заасан нийтлэг журмаар тогтоосон босго үзүүлэлтэд хүрсэн;

32.1.5.төрийн суурь мэдээллийн сан, төрөлжсөн мэдээллийн сан, батлан хамгаалах, үндэсний аюулгүй байдал, төрийн үйлчилгээний тасралтгүй ажиллагаанд ашиглагдах мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийн дэд бүтцэд нөлөөлсөн;

32.1.6.кибер халдлага, зөрчилд өртсөн байгууллага, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийн тоо, салбарын хамрах хүрээ, тархалтын түвшин нь энэ хуулийн 7.1.3-т заасан нийтлэг журмаар тогтоосон босго үзүүлэлтэд хүрсэн;

32.1.7.гадаад улсын оролцоо, зохион байгуулалттай бүлэг, барьцаалах төрлийн хортой ажиллагааны шинж илэрсэн бөгөөд тухайн кибер халдлага, зөрчил нь энэ хуулийн 32.1.1-32.1.6-д заасан нөхцөлийн аль нэгийг үүсгэсэн;

32.1.8.энэ хуулийн 7.1.3-т заасан нийтлэг журмын дагуу ноцтой кибер халдлага, зөрчил гэж ангилсан.

33 дугаар зүйл.Кибер халдлага, зөрчлийг мэдэгдэх хугацаа

33.1.Онц чухал мэдээллийн дэд бүтэцтэй этгээд, чухал мэдээллийн дэд бүтэцтэй этгээд болон энэ хуульд мэдэгдэх үүрэг хүлээсэн бусад этгээд ноцтой кибер халдлага, зөрчлийн талаар мэдсэнээс хойш Кибер аюулгүй байдлын үндэсний төвийн нэг цонхны цахим системээр дараах хугацаанд мэдэгдэнэ:

33.1.1.24 цагийн дотор анхны сэрэмжлүүлэг;

33.1.2.72 цагийн дотор анхны тайлан;

33.1.3.нөхцөл байдал өөрчлөгдсөнөөс хойш 24 цагийн дотор завсрын шинэчлэлт;

33.1.4.кибер халдлага, зөрчлийг таслан зогсоож, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийн хэвийн ажиллагааг сэргээснээс хойш 30 хоногийн дотор эцсийн тайлан.

33.2.Кибер халдлага, зөрчил нь хүний амь нас, эрүүл мэнд, үндэсний аюулгүй байдал, онц чухал мэдээллийн дэд бүтцийн тасралтгүй ажиллагаанд шууд эрсдэл үүсгэсэн бол мэдэгдэх үүрэг хүлээсэн этгээд энэ хуулийн 7.1.3-т заасан нийтлэг журмаар тогтоосон богиносгосон хугацаанд мэдэгдэнэ.

33.3.Энэ хуульд заасан хугацаанд мэдэгдэх боломжгүй болсон хүндэтгэн үзэх шалтгаан байсан бол тухайн этгээд мэдэгдэл хүргүүлэхдээ хоцорсон үндэслэл, кибер халдлага, зөрчлийг таслан зогсоох, хохирлыг бууруулах, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийг сэргээх талаар авсан арга хэмжээг тайлбарлана.

34 дүгээр зүйл.Кибер халдлага, зөрчлийн мэдэгдлийн агуулга

34.1.Кибер халдлага, зөрчлийн анхны сэрэмжлүүлэг, анхны тайлан, завсрын шинэчлэлт, эцсийн тайланд тусгах мэдээллийн агуулга, хэлбэр, хавсаргах мэдээлэл, баримтын жагсаалтыг энэ хуулийн 7.1.3-т заасан нийтлэг журам болон Кибер аюулгүй байдлын үндэсний төвөөс баталсан мэдэгдлийн маягтаар тогтооно.

34.2.Кибер халдлага, зөрчлийн мэдэгдэлд тухайн үед тогтоогдсон мэдээллийн хүрээнд кибер халдлага, зөрчлийн шинж, илэрсэн хугацаа, өртсөн мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтэц, өртсөн өгөгдлийн төрөл, хэрэглэгч, иргэн, хуулийн этгээдийн хамрах хүрээ, авсан арга хэмжээ, шаардлагатай дэмжлэгийн талаарх мэдээллийг тусгана.

34.3.Мэдэгдэл гаргасан этгээд тухайн үед бүрэн тогтоогдоогүй мэдээллийг таамаглал байдлаар мэдэгдэх бол уг мэдээллийн эх сурвалж, баталгаажуулах шаардлагатай нөхцөлийг тусад нь тэмдэглэнэ.

35 дугаар зүйл.Кибер халдлага, зөрчлийг бүртгэх, ангилах

35.1.Кибер аюулгүй байдлын үндэсний төв кибер халдлага, зөрчлийн мэдэгдэл хүлээн авсан даруйд тухайн мэдэгдэлд давтагдашгүй бүртгэлийн дугаар олгож, мэдэгдлийг хүлээн авсан огноо, цаг, мэдэгдэл гаргасан этгээд, өртсөн мэдээллийн систем, мэдээллийн сүлжээ,

үйлчилгээ, мэдээллийн дэд бүтэц, урьдчилсан ангилал, авсан арга хэмжээ, шилжүүлсэн эсэх, кибер халдлага, зөрчлийн явцын талаарх мэдээллийг бүртгэнэ.

35.2.Кибер аюулгүй байдлын үндэсний төв кибер халдлага, зөрчлийг шинж, нөлөөлөл, цар хүрээ, өртсөн мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтэц, хүний эрх, үндэсний аюулгүй байдал, эдийн засаг, олон нийтэд үзүүлэх нөлөөлөл, тархалтын түвшин, давтагдах эрсдэлийг харгалзан ангилна.

35.3.Кибер халдлага, зөрчил нь ноцтой эсэхийг энэ хуулийн 32 дугаар зүйл болон энэ хуулийн 7.1.3-т заасан нийтлэг журмын дагуу тогтооно.

35.4.Мэдэгдсэн үйл явдал кибер халдлага, зөрчилд хамаарахгүй гэж үзсэн бол Кибер аюулгүй байдлын үндэсний төв энэ тухай үндэслэл бүхий тэмдэглэл үйлдэж, мэдэгдэл гаргасан этгээдэд энэ хуулийн 7.1.3-т заасан нийтлэг журамд заасан хугацаанд буцаан мэдээлнэ.

35.5.Нэг кибер халдлага, зөрчил хэд хэдэн байгууллага, салбар, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцэд нөлөөлсөн бол Кибер аюулгүй байдлын үндэсний төв тухайн кибер халдлага, зөрчлийг нэгтгэн бүртгэж, мэдээлэл давхардах, хариу арга хэмжээ давхардах, үндсэн хариуцагч тодорхойгүй болохоос сэргийлэх арга хэмжээ авна.

36 дугаар зүйл.Кибер халдлага, зөрчлийн мэдээллийг шилжүүлэх, үндсэн хариуцагчийг тогтоох

36.1.Кибер аюулгүй байдлын үндэсний төв кибер халдлага, зөрчлийн мэдээллийг энэ хууль болон энэ хуулийн 7.1.3-т заасан нийтлэг журмын дагуу тагнуулын байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв, цагдаагийн байгууллага, Кибер командлал, салбарын эрх бүхий байгууллага, салбарын кибер халдлага, зөрчилтэй тэмцэх төв, нэгж, эсхүл холбогдох бусад эрх бүхий байгууллагад шилжүүлнэ.

36.2.Кибер халдлага, зөрчил нь гэмт хэрэг, зөрчлийн шинжтэй бол Кибер аюулгүй байдлын үндэсний төв холбогдох мэдээллийг хууль сахиулах байгууллагад хуульд заасан журмын дагуу шилжүүлнэ.

36.3.Кибер халдлага, зөрчил нь Зэвсэгт хүчний мэдээллийн систем, цэргийн зориулалттай мэдээллийн сүлжээ, командлал, удирдлага, холбооны мэдээллийн дэд бүтцэд нөлөөлсөн бол Кибер командлал хуульд заасан чиг үүргийн хүрээнд хариу арга хэмжээ авна.

36.4.Кибер халдлага, зөрчлийн мэдээллийг шилжүүлэхдээ кибер халдлага, зөрчлийн бүртгэлийн дугаар, урьдчилсан ангилал, шилжүүлсэн үндэслэл, шилжүүлсэн огноо, цаг, хүлээн авсан байгууллага, цаашид хариуцах нэгж, холбоо барих сувгийг бүртгэнэ.

36.5.Кибер халдлага, зөрчлийн үндсэн хариуцагчийг тухайн кибер халдлага, зөрчлийн шинж, өртсөн мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтэц, мэдээллийн ангилал, үйлчилгээний нөлөөлөл, байгууллагын хуульд заасан чиг үүргийг харгалзан энэ хуулийн 7.1.3-т заасан нийтлэг журмын дагуу тогтооно.

36.6.Кибер халдлага, зөрчлийн мэдээллийг өөр байгууллагад шилжүүлсэн нь Кибер аюулгүй байдлын үндэсний төвийн мэдээлэл солилцоо, бүртгэл, уялдуулан зохицуулах чиг үүргийг дуусгавар болгох үндэслэл болохгүй.

36.7.Кибер халдлага, зөрчлийн талаарх мэдэгдэл, мэдээлэл харьяалахгүй байгууллагад ирсэн бол тухайн байгууллага уг мэдээллийг энэ хуулийн 7.1.3-т заасан нийтлэг журмын дагуу харьяалах байгууллагад шилжүүлж, энэ тухай мэдэгдэл гаргасан этгээдэд буцаан мэдээлнэ.

36.8.Кибер халдлага, зөрчлийн мэдээллийг шилжүүлэн авсан байгууллага тухайн кибер халдлага, зөрчилтэй холбоотой авсан арга хэмжээ, явц, үр дүн, бүртгэлийг хаасан эсэх талаарх мэдээллийг хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, мөрдөн шалгах ажиллагааны нууц, техникийн эмзэг мэдээллийн хамгаалалтын шаардлагад нийцүүлэн Кибер аюулгүй байдлын үндэсний төвд буцаан мэдээлнэ.

37 дугаар зүйл.Мэдэгдэл гаргасан этгээдэд буцаан мэдээлэх

37.1.Кибер аюулгүй байдлын үндэсний төв кибер халдлага, зөрчлийн мэдэгдлийг хүлээн авсан тухай мэдэгдэл гаргасан этгээдэд 24 цагийн дотор мэдээлнэ.

37.2.Кибер халдлага, зөрчлийн мэдээллийг өөр байгууллагад шилжүүлсэн бол Кибер аюулгүй байдлын үндэсний төв шилжүүлсэн байгууллага, шилжүүлсэн үндэслэл, цаашид харилцах сувгийн талаарх мэдээллийг энэ хуулийн 7.1.3-т заасан нийтлэг журамд заасан хугацаа, хэлбэрээр мэдэгдэл гаргасан этгээдэд хүргүүлнэ.

37.3.Кибер аюулгүй байдлын үндэсний төв, эсхүл үндсэн хариуцагчаар тогтоогдсон байгууллага кибер халдлага, зөрчлийн явц, авсан арга хэмжээ, нэмэлт мэдээлэл шаардлагатай эсэх, бүртгэлийн төлөвийн талаар мэдэгдэл гаргасан этгээдэд энэ хуулийн 7.1.3-т заасан нийтлэг журамд заасан нөхцөл, хугацаа, хэлбэрээр буцаан мэдээлнэ.

37.4.Буцаан мэдээлэх ажиллагаанд хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, мөрдөн шалгах ажиллагааны нууц, гүйцэтгэх ажил, тагнуулын ажиллагаа, үндэсний аюулгүй байдлын хууль тогтоомжид заасан шаардлагыг баримтална.

37.5.Буцаан мэдээлэх мэдээллийн хэмжээ нь мэдэгдэл гаргасан этгээдэд кибер халдлага, зөрчилд хариу арга хэмжээ авах, хохирол бууруулах, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийг сэргээх, дахин давтагдахаас сэргийлэхэд шаардлагатай хэмжээнээс хэтрэхгүй байна.

38 дугаар зүйл.Кибер халдлага, зөрчилд хариу арга хэмжээ авах, нөхөн сэргээх

38.1.Кибер халдлага, зөрчилд өртсөн этгээд хариу арга хэмжээ авах төлөвлөгөө, тасралтгүй ажиллагаа, нөхөн сэргээх төлөвлөгөөнд заасан хугацаа, дарааллын дагуу хохирлыг бууруулах, тархалтыг хязгаарлах, нотлох баримтыг хадгалах, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийн тасралтгүй ажиллагааг хангах, сэргээн ажиллуулах арга хэмжээг авна.

38.2.Кибер аюулгүй байдлын үндэсний төв кибер халдлага, зөрчлийн шинж, нөлөөлөл, цар хүрээг харгалзан холбогдох байгууллага, салбарын кибер халдлага, зөрчилтэй тэмцэх төв, нэгж, салбарын мэдээлэл солилцоо, дүн шинжилгээний төвтэй хамтран хариу арга хэмжээний уялдааг хангана.

38.3.Кибер аюулгүй байдлын үндэсний төв ноцтой кибер халдлага, зөрчлийн үед хохирлыг бууруулах, тархалтыг хязгаарлах, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийг сэргээх зорилгоор энэ хуульд заасан хүрээнд техникийн болон зохион байгуулалтын арга хэмжээ авах талаар албан шаардлага хүргүүлж болно.

39 дүгээр зүйл.Харилцаа холбоо, интернэт, дата төв, домэйн нэр, хостинг, үүлэн үйлчилгээ үзүүлэгчийн шуурхай хамтын ажиллагаа

39.1.Харилцаа холбоо, интернэт, дата төв, домэйн нэр, хостинг, үүлэн үйлчилгээ үзүүлэгч нь кибер халдлага, зөрчлийг таслан зогсоох, тархалтыг хязгаарлах, хохирлыг бууруулах, нотлох баримтын бүрэн бүтэн байдлыг хадгалах зорилгоор Кибер аюулгүй байдлын үндэсний төв, тагнуулын байгууллагын кибер халдлага, зөрчилтэй тэмцэх төв, хууль сахиулах байгууллага болон хуульд заасан бусад эрх бүхий байгууллагатай хуульд заасан хүрээнд хамтран ажиллана.

39.2.Энэ хуулийн 39.1-д заасан үйлчилгээ үзүүлэгч эрх бүхий байгууллагаас ирүүлсэн хууль ёсны шаардлагыг хүлээн авах, баталгаажуулах, биелүүлэх, хэрэгжилтийн талаар хариу өгөх холбоо барих сувгийг энэ хуулийн 7.1.3-т заасан нийтлэг журамд заасан нөхцөл, шаардлагын дагуу ажиллуулна.

39.3.Эрх бүхий байгууллага энэ хуулийн 39.1-д заасан үйлчилгээ үзүүлэгчид шаардлага хүргүүлэхдээ хууль зүйн үндэслэл, зорилго, авах арга хэмжээ, хамрах хүрээ, хэрэгжүүлэх хугацаа, нууцлалын шаардлагыг тодорхой тусгана.

39.4.Энэ зүйлд заасан хамтын ажиллагаа нь үйлчилгээ үзүүлэгчийн хэрэглэгчийн мэдээлэл, хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, харилцааны нууц, техникийн эмзэг мэдээллийг хуульд заасан үндэслэл, журмаас гадуур гаргуулах үндэслэл болохгүй.

40 дүгээр зүйл.Хортой урсгал, домэйн нэр, хостинг, үүлэн үйлчилгээний ашиглалтыг хязгаарлах

40.1.Кибер халдлага, зөрчилтэй холбоотой хортой урсгал, хортой домэйн нэр, хортой холбоос, хортой хостинг, халдлагын команд, удирдлагын дэд бүтэц, хортой интернэт протоколын хаяг илэрсэн тохиолдолд энэ хуулийн 39.1-д заасан үйлчилгээ үзүүлэгч өөрийн үйлчилгээ, мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийн дэд бүтцэд хамаарах хүрээнд хязгаарлах, тусгаарлах, түр хаах, шүүлтүүр хэрэглэх, чиглүүлэлтийг өөрчлөх зэрэг техникийн арга хэмжээ авна.

40.2.Энэ хуулийн 40.1-д заасан арга хэмжээ нь кибер халдлага, зөрчлийг таслан зогсоох, тархалтыг хязгаарлах зорилгод нийцсэн, тухайн зорилгод хүрэхэд зайлшгүй, зохистой хэмжээтэй байна.

40.3.Домэйн нэр, хостинг, үүлэн үйлчилгээ, мэдээллийн сүлжээний хандалтыг хязгаарлах арга хэмжээ нь хууль ёсны үйлчилгээ, хэрэглэгчийн эрх, мэдээллийн хүртээмжийг үндэслэлгүйгээр хязгаарлахгүй.

40.4.Үйлчилгээ үзүүлэгч энэ зүйлд заасан арга хэмжээг хэрэгжүүлсэн үндэслэл, хугацаа, хамрах хүрээ, авсан арга хэмжээ, үр дүнг техникийн бүртгэлийн мэдээлэл болон дотоод бүртгэлээр баримтжуулна.

41 дүгээр зүйл.Интернэт протоколын хаяг, техникийн бүртгэлийн мэдээлэл хадгалах, гаргуулах

41.1.Энэ хуулийн 39.1-д заасан үйлчилгээ үзүүлэгч кибер халдлага, зөрчилтэй холбоотой хохирогч, халдлагад өртсөн мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтэц, хортой эх үүсвэрийн интернэт протоколын хаягийн хамаарал, холболтын огноо, цаг, техникийн бүртгэлийн мэдээлэл, домэйн нэр, хостинг, үүлэн үйлчилгээний холбогдох бүртгэлийн мэдээллийг хуульд заасан хүрээнд хадгална.

41.2.Эрх бүхий байгууллага кибер халдлага, зөрчлийг таслан зогсоох, хариу арга хэмжээ авах, нотлох баримтын бүрэн бүтэн байдлыг хангах зорилгоор хохирогч, халдлагад өртсөн мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтэц, хортой эх үүсвэртэй холбоотой энэ хуулийн 41.1-д заасан мэдээллийг хуульд заасан үндэслэл, журмын дагуу гаргуулж болно.

41.3.Мэдээлэл гаргуулах шаардлагад мэдээллийн төрөл, хэмжээ, хамрах хугацаа, зорилго, хууль зүйн үндэслэл, хадгалах болон дамжуулах нууцлалын нөхцөлийг тодорхой тусгана.

41.4.Үйлчилгээ үзүүлэгч эрх бүхий байгууллагын хууль ёсны шаардлагад заагаагүй мэдээллийг илүү хэмжээгээр цуглуулах, хадгалах, дамжуулахыг хориглоно.

42 дугаар зүйл.Үйлчилгээ үзүүлэгчийн нотлох баримтын бүрэн бүтэн байдлыг хангах үүрэг

42.1.Энэ хуулийн 39.1-д заасан үйлчилгээ үзүүлэгч кибер халдлага, зөрчилтэй холбоотой техникийн бүртгэлийн мэдээлэл, домэйн нэр, хостинг, үүлэн үйлчилгээний бүртгэл, хортой урсгалтай холбоотой холболтын мэдээллийг өөрчлөх, устгахгүйгээр хуульд заасан хүрээнд хадгална.

42.2.Үйлчилгээ үзүүлэгч нотлох баримт, техникийн бүртгэлийн мэдээлэл, техникийн шинжтэй холбогдох мэдээллийг эрх бүхий байгууллагад шилжүүлэхдээ хүлээлгэн өгсөн болон хүлээн авсан огноо, цаг, мэдээллийн төрөл, хэмжээ, хадгалалтын хэлбэр, шилжүүлсэн үндэслэл, хүлээн авсан этгээдийн мэдээллийг бүртгэнэ.

42.3.Энэ зүйлд заасан мэдээлэл нь хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, харилцааны нууц, мөрдөн шалгах ажиллагааны нууц, техникийн эмзэг мэдээлэл агуулсан бол холбогдох хууль тогтоомжид заасан хамгаалалтын дэглэмийг баримтална.

42.4.Үйлчилгээ үзүүлэгч энэ хуульд заасан хууль ёсны шаардлагыг биелүүлсэн нь тухайн үйлчилгээ үзүүлэгчийг хэрэглэгчтэй байгуулсан гэрээгээр хүлээсэн үүргээ зөрчсөнд тооцох үндэслэл болохгүй.

43 дугаар зүйл.Кибер халдлага, зөрчлийн бүртгэлийг хаах

43.1.Кибер халдлага, зөрчлийн бүртгэлийг Кибер аюулгүй байдлын үндэсний төв, эсхүл үндсэн хариуцагчаар тогтоогдсон байгууллага энэ хуулийн 7.1.3-т заасан нийтлэг журамд заасан нөхцөл, дарааллын дагуу хаана.

43.2.Кибер халдлага, зөрчлийн бүртгэлийг хаасан тухай мэдэгдэл гаргасан этгээдэд энэ хуулийн 7.1.3-т заасан нийтлэг журамд заасан хугацаа, хэлбэрээр буцаан мэдээлнэ.

43.3.Бүртгэлийг хаасан нь тухайн кибер халдлага, зөрчилтэй холбоотой гэмт хэрэг, зөрчил шалган шийдвэрлэх, иргэний, захиргааны, сахилгын болон бусад хуульд заасан хариуцлага хүлээлгэх ажиллагааг дуусгавар болгох үндэслэл болохгүй.

44 дүгээр зүйл.Кибер халдлага, зөрчлийн дүн шинжилгээ хийх

44.1.Ноцтой кибер халдлага, зөрчлийн дараа өртсөн этгээд Кибер аюулгүй байдлын үндэсний төв, үндсэн хариуцагчаар тогтоогдсон байгууллагатай хамтран энэ хуулийн 7.1.3-т заасан нийтлэг журамд заасан хугацаа, аргачлалын дагуу кибер халдлага, зөрчлийн дүн шинжилгээ хийнэ.

44.2.Кибер аюулгүй байдлын үндэсний төв кибер халдлага, зөрчлийн дүн шинжилгээний нууцад үл хамаарах нэгтгэсэн мэдээллийг салбарын мэдээлэл солилцоо, дүн шинжилгээний төв, салбарын эрх бүхий байгууллага, холбогдох этгээдэд сэрэмжлүүлэг, зөвлөмж хэлбэрээр хүргүүлнэ.

44.3.Кибер халдлага, зөрчлийн дүн шинжилгээнд туссан хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, техникийн эмзэг мэдээллийг энэ хууль болон холбогдох хууль тогтоомжид заасны дагуу боловсруулна.

45 дугаар зүйл.Хэрэглэгч, олон нийтэд мэдэгдэх

45.1.Кибер халдлага, зөрчил нь хэрэглэгчийн эрх, хүний хувийн мэдээлэл, үйлчилгээ авах боломж, эд хөрөнгө, эрүүл мэнд, аюулгүй байдалд энэ хуулийн 7.1.3-т заасан нийтлэг

журмаар тогтоосон босго үзүүлэлтэд хүрэх нөлөөлөл үүсгэсэн бол кибер халдлага зөрчилд өртөгч этгээд хэрэглэгчид уг журамд заасан хугацаа, хэлбэрээр мэдээлэл хүргэнэ.

45.2.Хэрэглэгчид мэдэгдэх мэдээлэлд кибер халдлага, зөрчлийн ерөнхий шинж, хэрэглэгчид үүссэн буюу үүсэж болзошгүй эрсдэл, хэрэглэгчийн авах арга хэмжээний зөвлөмж, байгууллагын авсан арга хэмжээ, холбоо барих сувгийн мэдээлэл багтсан байна.

45.3.Олон нийтэд мэдээлэх нь мөрдөн шалгах ажиллагаа, үндэсний аюулгүй байдал, бусад этгээдийн аюулгүй байдалд хохирол учруулах эрсдэлтэй бол холбогдох эрх бүхий байгууллага энэ хуулийн 7.1.3-т заасан нийтлэг журамд заасан үндэслэл, хугацаа, хэлбэрээр мэдээлэх ажиллагааг хойшлуулах, эсхүл мэдээллийн хэмжээг хязгаарлах шийдвэр гаргаж болно.

45.4.Хэрэглэгч, олон нийтэд мэдээлэхдээ кибер халдлага, зөрчлийг давтан үйлдэх, үргэлжлүүлэх, эсхүл эмзэг байдал ашиглах боломж бүрдүүлэх техникийн эмзэг мэдээллийг нийтэд түгээхгүй.

46 дугаар зүйл.Нотлох баримт, техникийн бүртгэлийн мэдээлэл хадгалах

46.1.Кибер халдлага, зөрчилд өртсөн этгээд техникийн бүртгэлийн мэдээлэл, мэдээллийн системийн төлөв байдлын хуулбар, төхөөрөмжийн дүрс хуулбар, холбогдох баримт, халдлагын үзүүлэлт, хортой урсгалтай холбоотой холболтын мэдээллийг хуульд нийцүүлэн хадгална.

46.2.Нотлох баримт хадгалахдаа мэдээллийн бүрэн бүтэн байдал, хадгалалт, шилжүүлгийн бүртгэл, хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, техникийн эмзэг мэдээллийн хамгаалалтыг хангана.

46.3.Нотлох баримт, техникийн бүртгэлийн мэдээллийг эрх бүхий байгууллагад шилжүүлэхдээ хүлээлгэн өгсөн болон хүлээн авсан огноо, цаг, мэдээллийн төрөл, хэмжээ, хадгалалтын хэлбэр, хүлээн авсан этгээд, шилжүүлсэн үндэслэлийг бүртгэнэ.

46.4.Нотлох баримт, техникийн бүртгэлийн мэдээлэл нь гэмт хэрэг, зөрчил шалган шийдвэрлэх ажиллагаанд ашиглагдах бол холбогдох хэрэг хянан шийдвэрлэх ажиллагааны тухай хуульд заасан журмыг баримтална.

47 дугаар зүйл.Кибер халдлага, зөрчлийг сайн дураар мэдэгдсэн этгээдийн хамгаалалт

47.1.Энэ зүйлд заасан хамгаалалт дараах этгээдэд хамаарна:

47.1.1.энэ хуульд заасан мэдэгдэх үүргээ тогтоосон хугацаанд, тухайн үед өөрт байсан бодит мэдээллийн хүрээнд биелүүлсэн этгээд;

47.1.2.энэ хуульд заасан мэдэгдэх үүрэг хүлээгээгүй боловч кибер халдлага, зөрчил, эсхүл кибер халдлага, зөрчил болохоос өмнөх дөхсөн тохиолдлын талаар Кибер аюулгүй байдлын үндэсний төв, эрх бүхий байгууллага, салбарын мэдээлэл солилцоо, дүн шинжилгээний төв, эсхүл холбогдох этгээдэд сайн дураар мэдээлэл өгсөн этгээд.

47.2.Энэ хуулийн 47.1-д заасан этгээд тухайн үед өөрт байсан бодит мэдээлэлд үндэслэн урьдчилсан буюу бүрэн бус мэдээлэл өгсөн бөгөөд уг мэдээлэл техникийн дүн шинжилгээний явцад өөрчлөгдсөн нь дангаараа тухайн этгээдэд хариуцлага хүлээлгэх үндэслэл болохгүй.

47.3.Энэ хуулийн 47.1-д заасан этгээдэд мэдээлэл өгсөн үйлдэлтэй нь холбогдуулан хариуцлага хүлээлгэхгүй. Харин тухайн этгээдийн энэ хууль, бусад хууль, гэрээгээр хүлээсэн үүргээ зөрчсөн эсэх асуудлыг шийдвэрлэхдээ хохирлыг бууруулах арга хэмжээ

авсан, нотлох баримт, техникийн бүртгэлийн мэдээллийг өөрт байгаа мэдээлэл, баримтын хүрээнд хадгалсан, эрх бүхий байгууллагатай хамтран ажилласан байдлыг харгалзана.

47.4.Энэ зүйл нь кибер халдлага, зөрчлийг санаатай нуун дарагдуулсан, худал мэдээлэл өгсөн, нотлох баримтыг устгасан, өөрчилсөн, хуурамчаар бүрдүүлсэн, кибер халдлага, зөрчлийг санаатайгаар үйлдсэн, эсхүл гэмт хэргийн шинжтэй үйлдэл гаргасан этгээдэд хамаарахгүй.

47.5.Энэ хуулийн 47.1-д заасан мэдээлэл өгсөн нь энэ хууль, бусад хууль, гэрээгээр хүлээсэн кибер сөрөн тэсвэрлэх чадавхийг хангах үндсэн үүргээ биелүүлээгүйгээс үүсэх хариуцлагаас тухайн этгээдийг бүрэн чөлөөлөх үндэслэл болохгүй.

47.6.Сайн дураар мэдэгдсэн мэдээлэлд хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, харилцааны нууц, эсхүл техникийн эмзэг мэдээлэл агуулагдсан бол тухайн мэдээллийг энэ хууль болон холбогдох хууль тогтоомжид заасан хамгаалалтын дэглэмийн дагуу хадгалж, ашиглаж, дамжуулна.

ЕСДҮГЭЭР БҮЛЭГ

КИБЕР ЭРСДЭЛИЙН ҮНЭЛГЭЭ, АУДИТ, БҮРТГЭЛ

48 дугаар зүйл.Кибер эрсдэлийн үнэлгээ

48.1.Кибер эрсдэлийн үнэлгээгээр мэдээллийн хөрөнгө, кибер занал, эмзэг байдал, магадлал, нөлөөлөл, эрсдэлийн түвшин, эрсдэлийг бууруулах арга хэмжээг тодорхойлно.
48.2.Ээлжит кибер эрсдэлийн үнэлгээг энэ хуулийн 21.1.2, 22.1.1-т заасан давтамжаар хийнэ.

48.3.Дараах тохиолдолд нэмэлт кибер эрсдэлийн үнэлгээ хийнэ:

48.3.1.мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцэд томоохон өөрчлөлт хийх;

48.3.2.үүлэн үйлчилгээ, дата төв, гуравдагч этгээдийн үндсэн үйлчилгээ, эсхүл нийлүүлэлтийн сүлжээний кибер эрсдэлд нөлөөлөх өөрчлөлт хийх;

48.3.3.ноцтой кибер халдлага, зөрчил гарсны дараа;

48.3.4.байгууллагын үйл ажиллагааны шинж чанар, мэдээллийн хөрөнгө, үндсэн үйлчилгээ, боловсруулж байгаа өгөгдлийн төрөл, хэмжээ, эсхүл кибер эрсдэлийн түвшин нь энэ хуулийн 7.1.5-т заасан нийтлэг журмаар тогтоосон шалгуурт хамаарах хэмжээгээр өөрчлөгдсөн;

48.3.5.Кибер аюулгүй байдлын үндэсний төв хуульд заасан үндэслэлээр нэмэлт кибер эрсдэлийн үнэлгээ хийх албан шаардлага хүргүүлсэн.

48.4.Кибер эрсдэлийн үнэлгээний тайланд үнэлгээний хамрах хүрээ, үнэлсэн мэдээллийн хөрөнгө, кибер занал, эмзэг байдал, эрсдэлийн түвшин, эрсдэлийг бууруулах арга хэмжээ, хариуцах этгээд, хэрэгжүүлэх хугацаа, дахин үнэлэх нөхцөлийг тусгана.

48.5.Кибер эрсдэлийн үнэлгээний тайланг энэ хуулийн 7.1.5-т заасан нийтлэг журамд заасан хугацаа, хэлбэрээр Кибер аюулгүй байдлын үндэсний төвд хүргүүлнэ.

49 дүгээр зүйл.Кибер сөрөн тэсвэрлэх чадавхийн аудит

49.1.Кибер сөрөн тэсвэрлэх чадавхийн аудитаар мэдээлэл, өгөгдөл, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтэц, үйл ажиллагааны дараалал,

удирдлага, хяналт, хамгаалалтын арга хэмжээ нь хууль тогтоомж, стандарт, гэрээ, дотоод бодлогын шаардлага хангаж байгаа эсэхийг хараат бус байдлаар үнэлнэ.
49.2.Ээлжит кибер сөрөн тэсвэрлэх чадавхийн аудитыг энэ хуулийн 21.1.3, 22.1.2-т заасан давтамжаар хийлгэнэ.

49.3.Кибер сөрөн тэсвэрлэх чадавхийн аудитаар аудитын хамрах хугацаанд илэрсэн кибер халдлага, зөрчил, эмзэг байдал, техникийн эмзэг мэдээлэл, халдлагын үзүүлэлт, кибер эрсдэлийн үнэлгээний зөвлөмжийн хэрэгжилт, эдгээрийг Кибер аюулгүй байдлын үндэсний төв, салбарын мэдээлэл солилцоо, дүн шинжилгээний төв болон хуульд заасан эрх бүхий байгууллагад мэдэгдсэн эсэхийг үнэлнэ.

49.4.Аудитын тайланд аудитын хамрах хүрээ, ашигласан стандарт, аргачлал, илэрсэн зөрчил, үл нийцэл, эмзэг байдал, кибер эрсдэл, эрсдэлийн түвшин, хэрэгжүүлэх арга хэмжээ, хариуцах этгээд, хэрэгжүүлэх хугацаа, дахин шалгах нөхцөлийг тусгана.

49.5.Аудитын тайланг энэ хуулийн 7.1.5-т заасан нийтлэг журамд заасан хугацаа, хэлбэрээр Кибер аюулгүй байдлын үндэсний төвд хүргүүлнэ.

49.6.Аудитын тайланд туссан хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, техникийн эмзэг мэдээллийг холбогдох хууль тогтоомжид заасны дагуу хамгаална.

50 дугаар зүйл.Аудит, үнэлгээ хийх этгээдийн бүртгэл

50.1.Кибер сөрөн тэсвэрлэх чадавхийн аудит, кибер эрсдэлийн үнэлгээ хийх этгээдийг Кибер аюулгүй байдлын үндэсний төв энэ хуулийн 7.1.5-т заасан нийтлэг журмын дагуу бүртгэнэ.

50.2.Кибер аюулгүй байдлын үндэсний төв бүртгэгдсэн аудит, үнэлгээ хийх этгээдийн нууцад үл хамаарах мэдээллийг нийтэд мэдээлнэ.

50.3.Аудит, үнэлгээ хийх этгээдийг бүртгэсэн нь тухайн этгээдийн хийсэн аудит, үнэлгээний дүгнэлтийг Кибер аюулгүй байдлын үндэсний төв урьдчилан баталгаажуулсан гэж үзэх үндэслэл болохгүй.

51 дүгээр зүйл.Аудит, үнэлгээ хийх этгээдэд тавих мэргэжлийн шаардлага

51.1.Аудит, үнэлгээ хийх этгээд дараах шаардлагыг хангасан байна:

51.1.1.мэдээллийн аюулгүй байдал, кибер аюулгүй байдал, мэдээллийн технологи, эрсдэлийн удирдлага, аудитын чиглэлээр мэргэшсэн хүний нөөцтэй байх;

51.1.2.аудит, үнэлгээ хийх аргачлал, чанарын хяналтын дотоод журамтай байх;

51.1.3.хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, техникийн эмзэг мэдээлэл хамгаалах журамтай байх;

51.1.4.ашиг сонирхлын зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, мэдэгдэх журамтай байх;

51.1.5.аудит, үнэлгээний баримт материал, нотлох баримт, тайлан, ажлын баримтыг хамгаалах, хадгалах нөхцөлтэй байх;

51.1.6.мэргэжлийн алдаа, буруутай дүгнэлт, мэдээлэл алдагдсанаас үүсэх эрсдэлийг хариуцах санхүүгийн чадавхтай, эсхүл хариуцлагын даатгалтай байх;

51.2.Аудит, үнэлгээ хийх мэргэжилтэнд тавих боловсрол, туршлага, мэргэшлийн гэрчилгээ, сургалт, давтан баталгаажуулалтын шаардлагыг Кибер аюулгүй байдлын үндэсний төв баталж, нийтэд мэдээлнэ.

51.3.Кибер аюулгүй байдлын үндэсний төв энэ хуулийн 51.2-т заасан мэргэшлийн гэрчилгээ, сургалтын жагсаалтыг батлахдаа олон улсын нийтлэг стандарт, мэргэжлийн байгууллагын шаардлага, үндэсний хэрэгцээ, зах зээлийн чадавхыг харгалзана.

51.4.Аудит, үнэлгээ хийх этгээд мэргэжлийн шаардлагыг хангаж байгаа талаарх мэдээллийг энэ хуулийн 7.1.5-т заасан нийтлэг журамд заасан хугацаа, хэлбэрээр Кибер аюулгүй байдлын үндэсний төвд шинэчлэн хүргүүлнэ.

51.5.Онц чухал мэдээллийн дэд бүтэц, төрийн болон албаны нууц, үндэсний аюулгүй байдалтай холбоотой аудит, үнэлгээ хийх этгээдийн эцсийн өмчлөгч, хамаарал бүхий этгээд, гадаадын хөрөнгө оруулалт, ажилтны нууцлалын шаардлагыг Кибер аюулгүй байдлын үндэсний төв тагнуулын байгууллагын саналыг үндэслэн шалгана.

52 дугаар зүйл.Аудит, үнэлгээ хийх этгээдийн хараат бус байдал, ашиг сонирхлын зөрчил

52.1.Аудит хийх этгээд өөрийн хөгжүүлсэн, нийлүүлсэн, эзэмшсэн, ашигласан, удирдсан, эсхүл зөвлөх үйлчилгээ үзүүлсэн мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийн дэд бүтэц, үйлчилгээтэй холбоотой хараат бус аудит хийхийг хориглоно.

52.2.Кибер эрсдэлийн үнэлгээ хийсэн этгээд тухайн үнэлгээг үндэслэн хэрэгжүүлсэн арга хэмжээний үр дүнг хараат бус байдлаар аудитлах тохиолдолд ашиг сонирхлын зөрчил үүсэх эсэхийг урьдчилан мэдэгдэж, Кибер аюулгүй байдлын үндэсний төвөөс зөвшөөрөл авна.

52.3.Аудит, үнэлгээ хийх этгээд дараах нөхцөл үүссэн бол тухайн ажил гүйцэтгэхээс татгалзана:

52.3.1.үнэлүүлэх буюу аудитлуулах этгээдийн хувьцаа эзэмшигч, эрх бүхий албан тушаалтан, ажилтан, эсхүл тэдгээртэй нэгдмэл сонирхолтой этгээд байх;

52.3.2.үнэлүүлэх буюу аудитлуулах этгээдтэй сүүлийн хоёр жилийн хугацаанд аудит, үнэлгээний хараат бус байдалд нөлөөлөхүйц гэрээ, санхүүгийн хамааралтай байсан;

52.3.3.аудит, үнэлгээний дүгнэлтэд нөлөөлөх хувийн, санхүүгийн, гэр бүлийн, эсхүл бусад ашиг сонирхлын зөрчилтэй байх;

52.3.4.хуульд заасан бусад ашиг сонирхлын зөрчил үүссэн.

52.4.Аудит, үнэлгээ хийх этгээд ашиг сонирхлын зөрчил үүссэн, эсхүл үүсэж болзошгүй нөхцөлийг аудит, үнэлгээ эхлэхээс өмнө захиалагч болон Кибер аюулгүй байдлын үндэсний төвд бичгээр мэдэгдэнэ.

52.5.Ашиг сонирхлын зөрчилтэй этгээдийн гаргасан аудит, үнэлгээний тайланг Кибер аюулгүй байдлын үндэсний төв хүлээн авахаас татгалзаж болно.

53 дугаар зүйл.Гомдол, мэдээлэл хянан шийдвэрлэх

53.1.Аудит, үнэлгээ хийх этгээдийн бүртгэл, мэргэжлийн шаардлага, хараат бус байдал, ашиг сонирхлын зөрчил, нууцлалын зөрчил, мэргэжлийн алдаа, аудит, үнэлгээний тайлангийн үндэслэлтэй холбоотой гомдол, мэдээллийг Кибер аюулгүй байдлын үндэсний төв хүлээн авч хянан шийдвэрлэнэ.

53.2.Гомдол, мэдээлэлд гомдол гаргагчийн мэдээлэл, гомдлын үндэслэл, холбогдох аудит, үнэлгээний тайлан, дүгнэлт, зөвлөмж болон нотлох баримтыг тусгана.

53.3.Кибер аюулгүй байдлын үндэсний төв гомдол, мэдээллийг хянан шийдвэрлэхдээ аудит, үнэлгээ хийх этгээдээс тайлбар, холбогдох баримт, мэдээлэл гаргуулж болно.

53.4.Гомдол, мэдээллийг хянан шийдвэрлэсний үндсэн дээр Кибер аюулгүй байдлын үндэсний төв дараах шийдвэрийн аль нэгийг гаргана:

53.4.1.гомдол, мэдээллийг үндэслэлгүй гэж үзэх;

53.4.2.зөрчил, дутагдлыг арилгуулах хугацаатай үүрэг өгөх;

53.4.3.бүртгэлийг түдгэлзүүлэх;

53.4.4.бүртгэлээс хасах;

53.4.5.зөрчил нь гэмт хэрэг, зөрчлийн шинжтэй бол эрх бүхий байгууллагад шилжүүлэх.

53.5.Гомдол, мэдээлэл хянан шийдвэрлэх явцад хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, техникийн эмзэг мэдээллийг холбогдох хууль тогтоомжид заасны дагуу хамгаална.

АРАВДУГААР БҮЛЭГ
НИЙЛҮҮЛЭЛТИЙН СҮЛЖЭЭ, ҮҮЛЭН ҮЙЛЧИЛГЭЭ, ПРОГРАММ ХАНГАМЖИЙН АЮУЛГҮЙ БАЙДАЛ

54 дүгээр зүйл.Нийлүүлэлтийн сүлжээ болон программ хангамжийн кибер эрсдэлийн удирдлага

54.1.Онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээд мэдээллийн технологийн бүтээгдэхүүн, үйлчилгээ, үүлэн үйлчилгээ, дата төвийн үйлчилгээ, туслан гүйцэтгэгч, программ хангамж, техник хангамж сонгох, худалдан авах, ашиглахдаа нийлүүлэлтийн сүлжээний кибер эрсдэлийг үнэлнэ.

54.2.Энэ хуулийн 54.1-д заасан бүтээгдэхүүн, үйлчилгээний гэрээнд кибер сөрөн тэсвэрлэх чадавхийг хангах суурь шаардлага, өгөгдөл хадгалах, байршуулах, шилжүүлэх нөхцөл, туслан гүйцэтгэгч ашиглах нөхцөл, үйлчилгээ дуусахад өгөгдөл буцаан авах, устгах зохицуулалт, тасралтгүй ажиллагаа, нөөцлөлт, сэргээх нөхцөл, техникийн бүртгэлийн мэдээлэл авах боломж, кибер халдлага, зөрчлийг мэдэгдэх үүргийг тусгана.

54.3.Программ хангамжийн нийлүүлэгч, хөгжүүлэгч, үйлчилгээ үзүүлэгч нь энэ хуулийн 54.2-т заасан шаардлагатай холбоотой мэдээлэл, баримт бичиг, баталгааг захиалагчид үнэн зөв гаргаж өгөх үүрэгтэй.

54.4.Энэ хуулийн 54.2-т заасан шаардлагыг хэрэгжүүлэх боломжгүй болсон, эсхүл тухайн бүтээгдэхүүн, үйлчилгээнд ноцтой эмзэг байдал илэрсэн бол нийлүүлэгч, хөгжүүлэгч, үйлчилгээ үзүүлэгч энэ тухай гэрээнд заасан хугацаанд, гэрээнд хугацаа заагаагүй бол мэдсэнээс хойш 72 цагийн дотор захиалагчид мэдэгдэж, эрсдэлийг бууруулах арга хэмжээний санал хүргүүлнэ.

54.5.Кибер аюулгүй байдлын үндэсний төв энэ зүйлд заасан нийлүүлэлтийн сүлжээ болон программ хангамжийн кибер эрсдэлийн удирдлагын талаар арга зүйн зөвлөмж гаргаж болно.

55 дугаар зүйл.Шинэ мэдээллийн систем, үйлчилгээ нэвтрүүлэхийн өмнөх кибер эрсдэлийн үнэлгээ болон кибер сөрөн тэсвэрлэх чадавхийн аудит

55.1.Онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээд шинэ мэдээллийн систем, программ хангамж, техник хангамж, үүлэн үйлчилгээ, дата төвийн үйлчилгээ, эсхүл тэдгээрийн томоохон өөрчлөлт, шинэчлэлийг ашиглалтад оруулахын өмнө кибер эрсдэлийн үнэлгээ хийнэ.

55.2.Энэ хуулийн 55.1-д заасан өөрчлөлт, шинэчлэл нь үндсэн үйлчилгээний тасралтгүй ажиллагаа, үндсэн өгөгдөл, төрийн суурь мэдээллийн сан, төрийн болон албаны нууц, онц чухал мэдээллийн дэд бүтэц, эсхүл чухал мэдээллийн дэд бүтцэд энэ хуулийн 7.1.5-т заасан нийтлэг журмаар тогтоосон босго үзүүлэлтэд хүрэх нөлөөлөл үзүүлэхээр бол кибер сөрөн тэсвэрлэх чадавхийн аудит хийлгэнэ.

55.3.Энэ хуулийн 55.1, 55.2-т заасан кибер эрсдэлийн үнэлгээ болон кибер сөрөн тэсвэрлэх чадавхийн аудитыг энэ хуульд заасны дагуу бүртгэгдсэн аудит, үнэлгээ хийх этгээдээр, эсхүл хуульд заасан эрх бүхий байгууллагаар холбогдох журам, стандарт, аргачлалын дагуу гүйцэтгүүлнэ.

55.4.Кибер эрсдэлийн үнэлгээ, эсхүл кибер сөрөн тэсвэрлэх чадавхийн аудитаар энэ хуулийн 7.1.5-т заасан нийтлэг журмаар тогтоосон ноцтой эрсдэл илэрсэн бол тухайн мэдээллийн систем, мэдээллийн сүлжээ, программ хангамж, техник хангамж, үйлчилгээ, мэдээллийн дэд бүтцийг ашиглалтад оруулах ажиллагааг эрсдэл бууруулах арга хэмжээ авах хүртэл хойшлуулна.

56 дугаар зүйл.Үүлэн үйлчилгээ

56.1.Энэ зүйл нь онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийн үндсэн үйлчилгээний тасралтгүй ажиллагаанд шууд нөлөөлөх, төрийн болон албаны нууц, төрийн суурь мэдээллийн сан, үндсэн өгөгдөл боловсруулах, хадгалах, дамжуулах үүлэн үйлчилгээ ашиглахад хамаарна.

56.2.Энэ хуулийн 56.1-д хамаарах үүлэн үйлчилгээний гэрээнд өгөгдөлд хандах, ашиглах, буцаан авах эрх, өгөгдөл буцаан авах нөхцөл, үйлчилгээ дуусах үед өгөгдөл устгах баталгаа, кибер халдлага, зөрчлийг мэдэгдэх үүрэг, техникийн бүртгэлийн мэдээлэл болон аудитад шаардлагатай мэдээлэл авах боломж, нөөцлөлт, сэргээх хугацаа, туслан гүйцэтгэгчийн хяналт, үйлчилгээний байршил, өгөгдөл дамжуулах нөхцөлийг тусгасан байна.

56.3.Төрийн болон албаны нууц, төрийн суурь мэдээллийн сан, онц чухал мэдээллийн дэд бүтэцтэй этгээдийн үндсэн үйлчилгээний тасралтгүй ажиллагаанд зайлшгүй шаардлагатай үндсэн өгөгдлийг Монгол Улсад байрлах дата төвд хадгална. Гадаад улсад байрлах үүлэн үйлчилгээ ашиглах нөхцөл, кибер эрсдэлийн үнэлгээ, зөвшөөрсөн байршил, хяналтын журмыг Засгийн газар батална.

56.4.Дотоод захиргааны болон өдөр тутмын үйл ажиллагаанд ашиглах үүлэн үйлчилгээний кибер эрсдэлийн үнэлгээ, гэрээний шаардлагыг тухайн үйлчилгээний эрсдэлийн түвшин, боловсруулж байгаа мэдээлэл, өгөгдлийн ангилал, байгууллагын чиг үүрэгт үзүүлэх нөлөөнд нийцүүлэн энэ хуулийн 7.1.7-т заасан суурь шаардлага болон холбогдох журмаар тогтооно.

АРВАН НЭГДҮГЭЭР БҮЛЭГ
ЭМЗЭГ БАЙДЛЫН УДИРДЛАГА БОЛОН САЙН ДУРЫН СУДАЛГАА

57 дугаар зүйл.Эмзэг байдлыг зохицуулалттай ил болгох

57.1.Кибер аюулгүй байдлын үндэсний төв эмзэг байдлыг зохицуулалттай ил болгох үндэсний сувгийг ажиллуулна.

57.2.Онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээд эмзэг байдал мэдээлэх суваг, хариу өгөх хугацаа, эмзэг байдлыг засварлах ажиллагааны журамтай байна.

57.3.Эмзэг байдлыг мэдээлсэн этгээдэд мэдээллийг хүлээн авсан тухай баталгааг ажлын 5 өдрийн дотор хүргүүлнэ.

57.4.Эмзэг байдлыг засварлах хугацааг тухайн эмзэг байдлын эрсдэлийн түвшин, нөлөөллийн цар хүрээ, ашиглагдах боломж, мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцэд үзүүлэх нөлөөллийг харгалзан энэ хуулийн 7.1.7-т заасан суурь шаардлага болон холбогдох аргачлалын дагуу тогтооно.

58 дугаар зүйл.Сайн дурын судлаачийн хамгаалалт

58.1.Дараах нөхцөлийг хангасан этгээдийг зөвхөн эмзэг байдал илрүүлж мэдээлсэн үндэслэлээр кибер халдлага, зөрчил үйлдсэн гэж үзэх үндэслэл болохгүй:

58.1.1.эмзэг байдал мэдээлэх суваг, хариуцсан этгээдийн нийтэд зарласан нөхцөл, эсхүл бичгээр зөвшөөрсөн хүрээнээс хэтрээгүй;

58.1.2.зөвшөөрөгдсөн хүрээнээс илүү мэдээлэл хуулбарлаагүй, мэдээлэл устгаагүй, өөрчлөөгүй;

58.1.3.үйлчилгээ санаатай тасалдуулаагүй;

58.1.4.олж тогтоосон эмзэг байдлыг энэ хуульд заасан сувгаар мэдээлсэн;

58.1.5.засварлах боломж олголгүй нийтэд задруулаагүй;

58.1.6.санхүүгийн болон хууль бус ашиг олох зорилгоор сүрдүүлээгүй;

58.1.7.хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууцыг хууль бусаар цуглуулаагүй, ашиглаагүй, дамжуулаагүй, задруулаагүй.

58.2.Энэ зүйлийн хамгаалалт нь гэмт хэргийн шинжтэй үйлдэл гаргасан, санаатай хохирол учруулсан, мэдээлэл барьцаалсан, зөвшөөрөгдсөн хүрээнээс хэтэрч нэвтэрсэн, эсхүл эмзэг байдлыг хууль бус зорилгоор ашигласан этгээдэд хамаарахгүй.

58.3.Эмзэг байдлыг энэ хуульд заасан сувгаар, зөвшөөрөгдсөн хүрээнд, хохирол учруулахгүйгээр илрүүлж мэдээлсэн этгээдэд тухайн мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцийг хариуцагч этгээд урамшуулал олгож болно. Төсвийн байгууллага урамшуулал олгох нөхцөл, хэмжээ, санхүүжилтийн эх үүсвэрийг төсөв, санхүүгийн холбогдох хууль тогтоомжид нийцүүлэн шийдвэрлэнэ.

АРВАН ХОЁРДУГААР БҮЛЭГ
МЭДЭЭЛЭЛ СОЛИЛЦОО, НУУЦЛАЛ, ХҮНИЙ ЭРХ

59 дүгээр зүйл.Мэдээлэл солилцооны зарчим

59.1.Кибер сөрөн тэсвэрлэх чадавхийг хангахтай холбоотой мэдээлэл солилцоо нь тодорхой зорилготой, шаардлагатай хамгийн бага хэмжээнд хязгаарлагдсан, нууцлалтай, бүртгэлтэй, хяналттай байна.

59.2.Аюулын мэдээллийг кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, хохирлыг бууруулах, тархалтыг хязгаарлах, хамгаалах арга хэмжээ авах зорилгоор энэ хууль болон энэ хуулийн 7.1.3-т заасан нийтлэг журамд заасан нөхцөл, хэлбэрээр солилцож болно.

59.3.Хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, техникийн эмзэг мэдээлэл агуулсан мэдээллийг холбогдох хууль тогтоомжид заасан журмаар боловсруулж, хадгалж, дамжуулна.

60 дугаар зүйл.Мэдээлэл гаргуулах хязгаар

60.1.Кибер аюулгүй байдлын үндэсний төв болон эрх бүхий байгууллага энэ хуульд заасан чиг үүргээ хэрэгжүүлэх зорилгоор мэдээлэл гаргуулахдаа дараах шаардлагыг хангана:

60.1.1.хууль зүйн үндэслэл тодорхой байх;

60.1.2.мэдээлэл гаргуулах зорилго тодорхой байх;

60.1.3.гаргуулах мэдээллийн төрөл, хэмжээ, хамрах хугацаа тодорхой байх;

60.1.4.мэдээлэл гаргуулах хүрээг тухайн зорилгод шаардлагатай хамгийн бага хэмжээгээр хязгаарлах;

60.1.5.мэдээлэл хадгалах хугацаа, устгах нөхцөлийг тогтоох;

60.1.6.нууцлал, мэдээллийн аюулгүй байдлын хамгаалалт хэрэгжүүлэх;

60.1.7.мэдээлэл хүлээн авсан, ашигласан, дамжуулсан бүртгэл хөтлөх.

61 дүгээр зүйл.Хуулийн хэрэгжилтийг хэмжих, үнэлэх, тайлагнах

61.1.Кибер аюулгүй байдлын үндэсний төв энэ хуулийн хэрэгжилтийг жил бүр хэмжиж, үнэлнэ.

61.2.Энэ хуулийн хэрэгжилтийг хэмжих шалгуур үзүүлэлт, үнэлгээний аргачлалыг Кибер аюулгүй байдлын үндэсний төвийн саналыг үндэслэн Засгийн газар батална.

61.3.Кибер аюулгүй байдлын үндэсний төв энэ хуулийн хэрэгжилтийн жилийн үнэлгээний тайланг дараа оны эхний улиралд багтаан Засгийн газарт хүргүүлнэ.

61.4.Засгийн газар энэ хуулийн хэрэгжилтийн талаар жил бүр Монгол Улсын Их Хуралд мэдээлэл танилцуулна.

61.5.Кибер аюулгүй байдлын үндэсний төв энэ хуулийн хэрэгжилтийн жилийн үнэлгээний нууцад үл хамаарах хэсгийг олон нийтэд мэдээлнэ.

61.6.Энэ хуулийн хэрэгжилтийн үнэлгээний тайланд туссан дүгнэлт, зөвлөмжийг үндэслэн Засгийн газар хууль тогтоомж, бодлого, журам, стандарт, төсөв, хүний нөөц, сургалт, техникийн чадавхтай холбоотой арга хэмжээг хуульд заасан бүрэн эрхийн хүрээнд авч хэрэгжүүлнэ.

АРВАН ГУРАВДУГААР БҮЛЭГ
КИБЕР ХЯМРАЛЫН УДИРДЛАГА

62 дугаар зүйл.Кибер хямрал

62.1.Дараах нөхцөлийн аль нэг үүссэн бол кибер хямрал гэж үзнэ:

62.1.1.кибер халдлага, зөрчил хоёр буюу түүнээс дээш онц чухал мэдээллийн дэд бүтцийн салбарт зэрэг нөлөөлсөн;

62.1.2.үндэсний хэмжээнд төрийн үйлчилгээ, санхүү, эрчим хүч, харилцаа холбоо, эрүүл мэнд, тээвэр, эсхүл бусад үндсэн үйлчилгээ тасалдах эрсдэл үүссэн;

62.1.3.гадаад улсын оролцоотой, эсхүл цэргийн шинжтэй кибер занал илэрсэн;

62.1.4.төрийн суурь мэдээллийн сан, үндэсний аюулгүй байдал, батлан хамгаалах, санхүү, эрчим хүч, харилцаа холбоо, эрүүл мэнд, тээврийн мэдээллийн систем, мэдээллийн сүлжээ, үйлчилгээ, мэдээллийн дэд бүтцэд ноцтой нөлөөлөл үүссэн;

62.1.5.нийгэм, эдийн засгийн хэвийн ажиллагаанд энэ хуулийн 7.1.3-т заасан нийтлэг журмаар тогтоосон босго үзүүлэлтэд хүрэх сөрөг нөлөө үүссэн.

62.2.Тагнуулын байгууллага Кибер аюулгүй байдлын үндэсний төвтэй хамтран кибер хямралын үеийн кибер халдлагаас хамгаалах төлөвлөгөөг боловсруулж, Засгийн газарт батлуулахаар хүргүүлнэ.

63 дугаар зүйл.Кибер хямралын зохицуулалт

63.1.Кибер хямралын үед Засгийн газар шуурхай удирдлага, зохион байгуулалтын арга хэмжээг хэрэгжүүлж, шаардлагатай асуудлыг Засгийн газрын хуралдаанаар хэлэлцүүлнэ.

63.2.Кибер аюулгүй байдлын үндэсний төв кибер хямралын үед нэг цонхны цахим системд суурилсан мэдээлэл солилцоо, кибер халдлага, зөрчлийн бүртгэл, шилжүүлэг, буцаан мэдээлэх, хариу арга хэмжээг уялдуулах ажиллагааг зохион байгуулна.

63.3.Тагнуулын байгууллага, цагдаагийн байгууллага, Зэвсэгт хүчин, салбарын эрх бүхий байгууллага, салбарын мэдээлэл солилцоо, дүн шинжилгээний төв, онц чухал мэдээллийн дэд бүтэцтэй этгээд, чухал мэдээллийн дэд бүтэцтэй этгээд кибер хямралын үед хуульд заасан чиг үүргийн хүрээнд хамтран ажиллана.

63.4.Кибер хямралын үед авах арга хэмжээ нь хүний эрх, эрх чөлөө, хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууц, хэвлэлийн эрх чөлөөг хуульд зааснаас бусад үндэслэлээр хязгаарлахгүй.

АРВАН ДӨРӨВДҮГЭЭР БҮЛЭГ
ХЯНАЛТ ШАЛГАЛТ, АЛБАН ШААРДЛАГА, ХАРИУЦЛАГА

64 дүгээр зүйл.Хяналт шалгалт

64.1.Кибер аюулгүй байдлын үндэсний төв энэ хуулийн хэрэгжилтэд эрсдэлд суурилсан хяналт тавина.

64.2.Хяналт шалгалтыг дараах үндэслэлээр хийж болно:

64.2.1.төлөвлөгөөт шалгалт хийх;

64.2.2.ноцтой кибер халдлага, зөрчил гарсан, илэрсэн, эсхүл гарах бодит эрсдэл үүссэн;

64.2.3.кибер сөрөн тэсвэрлэх чадавхийн аудит, кибер эрсдэлийн үнэлгээний тайланд туссан эрсдэл, зөрчил, зөвлөмжийн хэрэгжилтийг шалгах шаардлага үүссэн;

64.2.4.иргэн, хуулийн этгээдээс үндэслэл бүхий гомдол, мэдээлэл ирүүлсэн;

64.2.5.салбарын мэдээлэл солилцоо, дүн шинжилгээний төв, салбарын эрх бүхий байгууллага, кибер халдлага, зөрчилтэй тэмцэх төвөөс ирүүлсэн эрсдэлийн мэдээлэлд үндэслэн шалгалт хийх шаардлага үүссэн;

64.2.6.үндэсний аюулгүй байдал, хүний амь нас, эрүүл мэнд, онц чухал мэдээллийн дэд бүтцийн тасралтгүй ажиллагаанд бодит эрсдэл үүссэн.

65 дугаар зүйл.Албан шаардлага

65.1.Кибер аюулгүй байдлын үндэсний төв энэ хууль, түүнд нийцүүлэн гаргасан журам, суурь шаардлагын зөрчил, эсхүл кибер эрсдэл илэрсэн тохиолдолд дараах албан шаардлага хүргүүлж болно:

65.1.1.зөрчил арилгах;

65.1.2.эрсдэл бууруулах төлөвлөгөө батлуулж, хэрэгжүүлэх;

65.1.3.албан шаардлагад заасан хугацаанд арга хэмжээ авах;

65.1.4.нэмэлт кибер эрсдэлийн үнэлгээ, эсхүл кибер сөрөн тэсвэрлэх чадавхийн аудит хийлгэх;

65.1.5.кибер халдлага, зөрчил мэдэгдэх үүргээ биелүүлэх;

65.1.6.хэрэглэгчид мэдээлэх үүргээ биелүүлэх;

65.1.7.нийлүүлэлтийн сүлжээний кибер эрсдэлийг бууруулах;

65.1.8.нөөцлөлт, сэргээх, тасралтгүй ажиллагааны арга хэмжээ авах.

66 дугаар зүйл.Хариуцлага

66.1.Энэ хуулийг зөрчсөн этгээдэд Зөрчлийн тухай хууль, Эрүүгийн хууль болон холбогдох бусад хуульд заасан хариуцлага хүлээлгэнэ.

66.2.Энэ хуулийг зөрчсөн этгээдэд хариуцлага хүлээлгэх асуудлыг холбогдох хуульд заасан журмаар шийдвэрлэхдээ дараах нөхцөлийг харгалзана:

66.2.1.зөрчлийн шинж, хүндийн хэмжээ;

66.2.2.хохирлын хэмжээ;

66.2.3.хэрэглэгч, иргэн, байгууллагад үзүүлсэн нөлөө;

66.2.4.санаатай буюу хайхрамжгүй үйлдэл, эс үйлдэхүй байсан эсэх;

66.2.5.кибер халдлага, зөрчлийг хуульд заасан хугацаанд мэдэгдсэн эсэх;

66.2.6.эрх бүхий байгууллагатай хамтран ажилласан эсэх;

66.2.7.хохирлыг бууруулах арга хэмжээ авсан эсэх;

66.2.8.давтан зөрчил гаргасан эсэх;

66.2.9.байгууллагын хэмжээ, эрсдэлийн ангилал;

66.2.10.тухайн этгээд энэ хууль, түүнд нийцүүлэн гаргасан журам, суурь шаардлагыг зохих ёсоор биелүүлсэн эсэх;

66.2.11.кибер халдлага нь тухайн үед нийтэд мэдэгдээгүй шинэ арга, хэрэгсэл, эмзэг байдлыг ашиглан үйлдэгдсэн эсэх.

66.3.Байгууллага кибер сөрөн тэсвэрлэх чадавхийг хангах үүргээ гэрээгээр бусдад шилжүүлсэн нь хариуцлагаас чөлөөлөх үндэслэл болохгүй.

66.4.Тухайн этгээд энэ хууль, түүнд нийцүүлэн гаргасан журам, суурь шаардлагыг тухайн үеийн кибер эрсдэлийн түвшинд нийцүүлэн зохих ёсоор хэрэгжүүлсэн бөгөөд тухайн үед нийтэд мэдэгдээгүй шинэ арга, хэрэгсэл, эмзэг байдлыг ашигласан кибер халдлагад өртсөн нь тогтоогдсон, мөн тухайн этгээдээс санаатай буюу хайхрамжгүй үйлдэл, эс үйлдэхүй тогтоогдоогүй бол энэ хуулиар хүлээсэн кибер сөрөн тэсвэрлэх чадавхийг хангах үүргээ биелүүлээгүй үндэслэлээр хариуцлага хүлээлгэхгүй.

66.5.Кибер халдлага, зөрчлийг мэдэгдэх үүргээ биелүүлээгүй, кибер сөрөн тэсвэрлэх чадавхийн аудит, кибер эрсдэлийн үнэлгээ хийлгээгүй, Кибер аюулгүй байдлын үндэсний төвийн албан шаардлагыг биелүүлээгүй, кибер халдлага, зөрчлийн мэдээллийг санаатай нуун дарагдуулсан, нотлох баримт, техникийн бүртгэлийн мэдээллийг устгасан, өөрчилсөн, эсхүл хуурамчаар бүрдүүлсэн үйлдэлд Зөрчлийн тухай хууль, Эрүүгийн хууль болон холбогдох бусад хуульд заасан хариуцлага хүлээлгэнэ.

АРВАН ТАВДУГААР БҮЛЭГ
САНХҮҮЖИЛТ, ХҮНИЙ НӨӨЦ, СУРГАЛТ

67 дугаар зүйл.Санхүүжилт

67.1.Улсын болон орон нутгийн төсөвт кибер сөрөн тэсвэрлэх чадавхийг хангах арга хэмжээ, техник хангамж, программ хангамж, хяналт-шинжилгээ, кибер сөрөн тэсвэрлэх чадавхийн аудит, кибер эрсдэлийн үнэлгээ, сургалт, сургуулилалт, хүний нөөц, тасралтгүй ажиллагаа, нөхөн сэргээх чадавхийг бүрдүүлэх зардлыг хууль тогтоомжид заасан журмын дагуу төлөвлөж тусгана.

67.2.Төсвийн ерөнхийлөн захирагч өөрийн эрхлэх асуудлын хүрээний төрийн байгууллага, төрийн өмчит болон төрийн өмчийн оролцоотой хуулийн этгээдийн кибер сөрөн тэсвэрлэх чадавхийг хангах зардлыг жил бүрийн төсвийн саналд тусгана.

67.3.Онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээд кибер сөрөн тэсвэрлэх чадавхийг хангах үүргээ хэрэгжүүлэх зардлыг жил бүрийн төсөв, бизнес төлөвлөгөөндөө тусгана.

67.4.Энэ хуулийн 67.1, 67.2, 67.3-т заасан төсвийн төлөвлөлт, тайлагналын аргачлал, онц чухал болон чухал мэдээллийн дэд бүтэцтэй этгээдийн эрсдэлийн ангилал, байгууллагын хэмжээ, мэдээллийн дэд бүтцийн ач холбогдолд үндэслэсэн зардлын жишиг, төлөвлөлтийн аргачлалыг төсвийн асуудал эрхэлсэн төрийн захиргааны төв байгууллага Кибер аюулгүй байдлын үндэсний төвтэй хамтран батална.

67.5.Кибер сөрөн тэсвэрлэх чадавхийг хангах зориулалтаар төсөвлөсөн хөрөнгийг зориулалтын бусаар зарцуулахыг хориглоно.

68 дугаар зүйл.Хүний нөөц

68.1.Төрөөс кибер сөрөн тэсвэрлэх чадавхийг хангах хүний нөөцийг бэлтгэх, мэргэшүүлэх, тогтвор суурьшилтай ажиллуулах бодлого хэрэгжүүлнэ.

68.2.Кибер аюулгүй байдлын үндэсний төв, Кибер командлал, кибер халдлага, зөрчилтэй тэмцэх төв, салбарын мэдээлэл солилцоо, дүн шинжилгээний төвийн ажилтан нууцлал, ёс зүй, ашиг сонирхлын зөрчлийн шаардлагыг мөрдөнө.

68.3.Кибер командлалын идэвхтэй кибер ажиллагаанд оролцох алба хаагч тусгай сургалт, хууль зүйн мэдлэг, ёс зүйн шалгуур, нууцлалын шаардлага хангасан байна.

69 дүгээр зүйл.Сургалт, сургуулилалт

69.1.Кибер аюулгүй байдлын үндэсний төв жил бүр үндэсний кибер сургуулилалт зохион байгуулна.

69.2.Онц чухал мэдээллийн дэд бүтэцтэй этгээд жил бүр, чухал мэдээллийн дэд бүтэцтэй этгээд хоёр жил тутам кибер халдлага, зөрчилд хариу арга хэмжээ авах сургуулилалт хийнэ.

69.3.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв нь салбарын сургуулилалтыг Кибер аюулгүй байдлын үндэсний төв, салбарын эрх бүхий байгууллагатай хамтран зохион байгуулж болно.

АРВАН ЗУРГААДУГААР БҮЛЭГ
ШИЛЖИЛТИЙН ЗОХИЦУУЛАЛТ

70 дугаар зүйл.Кибер аюулгүй байдлын үндэсний төв байгуулах

70.1.Энэ хууль хүчин төгөлдөр болсон өдрөөс хойш 90 хоногийн дотор Засгийн газар Кибер аюулгүй байдлын үндэсний төвийг байгуулна.

70.2.Энэ хууль хүчин төгөлдөр болохоос өмнө мөрдөж байсан Кибер аюулгүй байдлын тухай хуульд заасан Кибер халдлага, зөрчилтэй тэмцэх нийтийн төвтэй холбоотой төсөв, орон тоо, эд хөрөнгө, мэдээллийн сан, архив, гэрээ, эрх, үүргийг Кибер аюулгүй байдлын үндэсний төвд шилжүүлнэ.

70.3.Энэ хууль хүчин төгөлдөр болохоос өмнө мөрдөж байсан Кибер аюулгүй байдлын тухай хуульд заасан Кибер халдлага, зөрчилтэй тэмцэх нийтийн төвийн кибер халдлага, зөрчлийг мэдэгдэх, хүлээн авах, бүртгэх, ангилах, мэдээлэл солилцох, хариу арга хэмжээг уялдуулах чиг үүргийг Кибер аюулгүй байдлын үндэсний төв хэрэгжүүлнэ.

70.4.Энэ хууль хүчин төгөлдөр болохоос өмнө мөрдөж байсан Кибер аюулгүй байдлын тухай хуульд заасан Кибер аюулгүй байдлын зөвлөл, түүний ажлын албатай холбоотой төсөв, эд хөрөнгө, архив, мэдээллийн сан, гэрээ, дуусаагүй ажил, эрх, үүргийг Кибер аюулгүй байдлын үндэсний төвд шилжүүлэх асуудлыг Засгийн газар шийдвэрлэнэ.

70.5.Цахим хөгжил, инновац, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагын кибер аюулгүй байдлын бодлого, зохицуулалтын холбогдох чиг үүрэг болон үндэсний кибер халдлага, зөрчилтэй тэмцэх холбогдох төв, нэгжийн төрд хамаарах чиг үүргийн шилжилт, давхардлыг арилгах, хүний нөөц, мэдээллийн сан, архив, гэрээ, эрх, үүргийн шилжилтийн хүрээ, хугацааг Засгийн газар тогтооно.

71 дүгээр зүйл.Журам, заавар батлах хугацаа

71.1.Засгийн газар энэ хууль хүчин төгөлдөр болсон өдрөөс хойш 6 сарын дотор дараах журмыг батална:

71.1.1.Кибер аюулгүй байдлын үндэсний төвийн дүрэм;

71.1.2.онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийг ангилах, бүртгэх, жагсаалт тогтоох, шинэчлэх журам;

71.1.3.кибер халдлага, зөрчлийг мэдээлэх, хүлээн авах, бүртгэх, ангилах, харилцан мэдээлэл солилцох, шилжүүлэх, давхардлыг арилгах, анхны хариу арга хэмжээ авах байгууллага, үндсэн хариуцагч, мэдээллийн харьяалал, чиг үүрэг, хариуцлагын заагийг тогтоох нийтлэг журам;

71.1.4.салбарын мэдээлэл солилцоо, дүн шинжилгээний төв байгуулах, бүртгэх, ажиллуулах, мэдээлэл солилцох, шуурхай холбоо барих суваг, байнгын шуурхай холбоо барих горим хэрэгжүүлэх нөхцөл, шаардлагыг тогтоосон нийтлэг журам;

71.1.5.кибер эрсдэлийн үнэлгээ хийх, кибер сөрөн тэсвэрлэх чадавхийн аудит хийх, аудит, үнэлгээ хийх этгээдийг бүртгэх нийтлэг журам;

71.1.6.идэвхтэй кибер ажиллагааны зөвшөөрөл, хяналт, бүртгэл, тайлагналын тусгай журам;

71.1.7.кибер хямралын үед шуурхай зохион байгуулалт хийх журам;

71.1.8.харилцаа холбоо, интернэт, дата төв, домэйн нэр, хостинг, үүлэн үйлчилгээ үзүүлэгчийн хамтын ажиллагааны журам;

71.1.9.шинэ мэдээллийн систем, программ хангамж, техник хангамж, үүлэн үйлчилгээ, дата төвийн үйлчилгээ нэвтрүүлэхийн өмнөх кибер эрсдэлийн үнэлгээ, кибер сөрөн тэсвэрлэх чадавхийн аудит хийх журам;

71.1.10.үүлэн үйлчилгээ ашиглах, өгөгдлийн байршил, зөвшөөрсөн байршил, кибер эрсдэлийн үнэлгээ, хяналтын журам;

71.1.11.энэ хуулийн хэрэгжилтийг хэмжих шалгуур үзүүлэлт, үнэлгээний аргачлал.

71.2.Кибер аюулгүй байдлын үндэсний төв энэ хууль хүчин төгөлдөр болсон өдрөөс хойш 6 сарын дотор мэдэгдлийн маягт, техникийн ангиллын аргачлал, мэдээлэл солилцох суваг, нэг цонхны цахим системийн ажиллагааны заавар, кибер халдлага, зөрчлийн бүртгэл, шилжүүлэг, буцаан мэдээлэх аргачлал, эмзэг байдлыг зохицуулалттай ил болгох сувгийн ажиллагааны зааврыг батална.

72 дугаар зүйл.Онц чухал болон чухал мэдээллийн дэд бүтэцтэй этгээдийг бүртгэх

72.1.Энэ хууль хүчин төгөлдөр болсон өдрөөс хойш 12 сарын дотор Кибер аюулгүй байдлын үндэсний төв онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийн бүртгэлийг шинэчилнэ.

72.2.Энэ хууль хүчин төгөлдөр болохоос өмнө батлагдсан онц чухал мэдээллийн дэд бүтэцтэй этгээдийн жагсаалт шинэчилсэн жагсаалт батлагдах хүртэл хүчинтэй байна.

73 дугаар зүйл.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв байгуулах шилжилт

73.1.Энэ хууль хүчин төгөлдөр болсон өдрөөс хойш 12 сарын дотор энэ хуулийн 24 дүгээр зүйлд заасан салбарын мэдээлэл солилцоо, дүн шинжилгээний төв байгуулах ажлыг Кибер аюулгүй байдлын үндэсний төв салбарын эрх бүхий байгууллагатай хамтран зохион байгуулна.

73.2.Салбарын мэдээлэл солилцоо, дүн шинжилгээний төв бүрэн байгуулагдах хүртэл тухайн салбарын мэдээлэл солилцоог Кибер аюулгүй байдлын үндэсний төвийн түр зохицуулалтын сувгаар хэрэгжүүлнэ.

74 дүгээр зүйл.Хууль хүчин төгөлдөр болох

74.1.Энэ хуулийг 20... оны ... дугаар сарын ...-ний өдрөөс эхлэн дагаж мөрдөнө.