

КИБЕР СӨРӨН ТЭСВЭРЛЭХ ТУХАЙ ХУУЛИЙН ТӨСЛИЙНТӨВЧ ТАНИЛЦУУЛГА

Монгол Улсын Их Хурлаас 2021 оны 12 дугаар сарын 17-ны өдөр баталсан Кибер аюулгүй байдлын тухай хуулиар кибер аюулгүй байдлыг хангах төрийн удирдлага, кибер халдлага, зөрчилтэй тэмцэх төвүүд, онц чухал мэдээллийн дэд бүтэцтэй байгууллагын ангилал, эрсдэлийн үнэлгээ, кибер сөрөн тэсвэрлэх чадавхийн аудит, мэдээлэл солилцох суурь зохицуулалтыг бий болгосон. Гэвч хуулийн хэрэгжилтийн явцад байгууллага хоорондын чиг үүргийн зааг, мэдээллийн урсгал, хариу арга хэмжээ авах дараалал, буцаан тайлагнал, аудит болон эрсдэлийн үнэлгээний дараах хяналт, хүний нөөц, санхүүжилт, хувийн мэдээлэл болон нууцын хамгаалалттай уялдах зохицуулалт хангалттай тодорхой бус байгаа нь тогтоогдсон.

Хуулийн хэрэгжилтийн үр дагаврын үнэлгээ, хэрэгцээ шаардлагын тандан судалгаа, бодит стресс тест, хэрэгжүүлэгч байгууллагуудаас ирүүлсэн санал, Монгол Улсын кибер аюулгүй байдлын чадавхын үнэлгээний дүгнэлтэд үндэслэн одоогийн зохицуулалтыг хэсэгчилсэн нэмэлт, өөрчлөлтөөр бус, кибер сөрөн тэсвэрлэх чадавхад суурилсан шинэчилсэн найруулгын хүрээнд боловсронгуй болгох шаардлагатай гэж үзсэн.

Кибер халдлага, зөрчлийн орчин хуулийг анх баталсан үеэс чанарын хувьд өөрчлөгдөж, үйлчилгээ тасалдуулах халдлага, мэдээлэл барьцаалах, өгөгдөл алдагдах, хэрэглэгчийг хууран мэхлэх, нийлүүлэлтийн сүлжээгээр дамжих эрсдэл, үүлэн үйлчилгээ болон дата төвийн хамаарал, олон нийтийн сэтгэл зүй, төрийн үйлчилгээ, эдийн засгийн хэвийн ажиллагаанд зэрэг нөлөөлөх нийлмэл аюул занал нэмэгдэж байна. Ийм нөхцөлд эрх зүйн зохицуулалт нь зөвхөн хамгаалах арга хэмжээг тогтоох бус урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах, хохирлыг хязгаарлах, тасралтгүй ажиллагааг хадгалах, нөхөн сэргээх цогц чадавхад чиглэх шаардлагатай.

Иймд Кибер сөрөн тэсвэрлэх тухай хуулийн төслийг боловсруулсан. Хуулийн төслийн зорилт нь Монгол Улсын кибер сөрөн тэсвэрлэх чадавхийг хангах, кибер орчин дахь онц чухал болон чухал үйлчилгээний тасралтгүй, найдвартай ажиллагааг хамгаалах, кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах, нөхөн сэргээхтэй холбогдсон харилцааг зохицуулахад оршино.

Хуулийн төсөл нь 16 бүлэг, 74 зүйлтэй. Төсөлд нийтлэг үндэслэл, кибер сөрөн тэсвэрлэх чадавхийг хангах төрийн удирдлага, байгууллагын тогтолцоо, кибер халдлага, зөрчилтэй тэмцэх төвүүдийн уялдаа, Кибер аюулгүй байдлын үндэсний төв, Кибер командлал, онц чухал болон чухал мэдээллийн дэд бүтэцтэй этгээдийн ангилал, бүртгэл, үүрэг, салбарын мэдээлэл солилцоо, дүн шинжилгээний төв, байгууллагын дотоод удирдлагын тогтолцоо, кибер халдлага, зөрчлийг мэдээлэх болон хариу арга хэмжээ авах процесс, аудит, эрсдэлийн үнэлгээ, бүртгэл, нийлүүлэлтийн сүлжээ, үүлэн үйлчилгээ, эмзэг байдлыг зохицуулалттай ил болгох, мэдээлэл солилцоо, нууцлал, хүний эрх, кибер хямралын удирдлага, олон улсын хамтын ажиллагаа, хяналт шалгалт, хариуцлага, санхүүжилт, хүний нөөц, шилжилтийн зохицуулалтыг тусгасан.

Төслийн нэг гол зохицуулалт нь Кибер аюулгүй байдлын үндэсний төвийг кибер сөрөн тэсвэрлэх чадавхийг улсын хэмжээнд уялдуулан зохион байгуулах, кибер халдлага, зөрчлийг мэдэгдэх нэг цонхны цахим системийг ажиллуулах, мэдээллийг бүртгэх, ангилах, чиг үүргийн дагуу холбогдох байгууллагад шилжүүлэх, онц чухал болон чухал мэдээллийн дэд бүтэцтэй этгээдийн бүртгэл, хяналт-шинжилгээ, арга зүйн дэмжлэгийг хэрэгжүүлэх чиг үүрэгтэйгээр тодорхойлсон явдал юм. Ингэснээр мэдээлэл хүлээн авах, шилжүүлэх, хариуцах байгууллагыг тогтоох, явцын мэдээлэл өгөх, бүртгэл хаах ажиллагаа нэг мөр болох нөхцөл бүрдэнэ.

Хуулийн төсөлд онц чухал мэдээллийн дэд бүтэцтэй этгээд болон чухал мэдээллийн дэд бүтэцтэй этгээдийг эрсдэлд суурилсан шалгуураар ялган тогтоохоор тусгасан. Ингэснээр байгууллагын нэр, өмчийн хэлбэрээр бус тухайн мэдээллийн систем, сүлжээ, үйлчилгээ, өгөгдлийн бодит ач холбогдол, тасалдах үед үүсэх үр дагавар, хувийн мэдээлэл боловсруулах цар хүрээ, гуравдагч этгээд болон нийлүүлэлтийн сүлжээний хамааралд үндэслэн ялгамжтай үүрэг, хяналт, тайлагнал хэрэгжих боломжтой болно.

Кибер халдлага, зөрчлийг мэдээлэх, бүртгэх, ангилах, шилжүүлэх, баталгаажуулах, үндсэн хариуцагчийг тогтоох, хариу арга хэмжээ авах, таслан зогсоох, нөхөн сэргээх, явцын мэдээлэл өгөх, бүртгэл хаах, үлдэгдэл эрсдэлийг үнэлэх, халдлагын дараах дүн шинжилгээ хийх ажиллагааг нарийвчлан зохицуулсан. Энэ нь мэдээллийн урсгал тасалдах, давхардах, байгууллага хоорондын хариуцлага тодорхойгүй үлдэх, мэдээлэл өгсөн этгээд явцын хариу авахгүй байх эрсдэлийг бууруулахад чиглэнэ.

Аудит, эрсдэлийн үнэлгээний хүрээнд аудит болон үнэлгээ хийх этгээдийн мэргэжлийн шаардлага, хараат бус байдал, ашиг сонирхлын зөрчил, тайлангийн доод агуулга, зөвлөмжийн эрэмбэ, гомдол, мэдээлэл хянан шийдвэрлэх, бүртгэх, бүртгэлийг түдгэлзүүлэх, бүртгэлээс хасах үндэслэл, тайлангийн дараах хяналтыг тусгасан. Ийм зохицуулалт нь аудит, эрсдэлийн үнэлгээг хэлбэр төдий тайлан бус, бодит эрсдэлийг бууруулах хэрэгсэл болгох зорилготой.

Хуулийн төсөлд үүлэн үйлчилгээ, дата төв, домэйн нэр, хостинг, программ хангамж, техник хангамж, туслан гүйцэтгэгч, нээлттэй эхийн бүрэлдэхүүн, нийлүүлэлтийн дараах үйлчилгээтэй холбоотой кибер эрсдэлийг тусгайлан зохицуулсан. Мөн шинэ мэдээллийн систем, программ хангамж, техник хангамж, үүлэн үйлчилгээ, дата төвийн үйлчилгээ ашиглалтад оруулахын өмнө кибер эрсдэлийн үнэлгээ болон кибер сөрөн тэсвэрлэх чадавхийн аудит хийх зохицуулалт тусгагдсан.

Кибер халдлага, зөрчлийн үед техникийн бүртгэлийн мэдээлэл, хортой урсгалтай холбоотой холболтын мэдээлэл, төхөөрөмжийн дүрс хуулбар, халдлагын үзүүлэлт, хэрэглэгчийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууцад хамаарах мэдээлэл боловсруулагдах боломжтой тул төсөлд мэдээллийг тодорхой зорилгоор, шаардлагатай хамгийн бага хэмжээнд боловсруулах, хадгалалтын хугацаа, хандалтын бүртгэл, гуравдагч этгээдэд дамжуулах хязгаар, дахин ашиглах хориг, нийтэд мэдээлэл болон хамгаалах мэдээллийн заагийг тодорхойлохоор тусгасан.

Кибер командлалын эрх зүйн байдлыг Зэвсэгт хүчний кибер аюулгүй байдлын цэргийн удирдлага, төлөвлөлт, бэлэн байдал, хамгаалах болон цэргийн кибер ажиллагааны хэрэгжилтийг зохион байгуулах хүрээнд тогтоож, идэвхтэй цэргийн кибер ажиллагаанд эрх бүхий шийдвэр, хууль зүйн дүгнэлт, эрсдэлийн үнэлгээ, бүртгэл, хяналт, тайлагналын тусгай шаардлага тавьсан. Мөн иргэний мэдээллийн систем, хүний хувийн мэдээлэл, байгууллагын нууц, төрийн болон албаны нууцад хуульд заасан үндэслэлгүйгээр нөлөөлөхийг хориглосон.

Хуулийн төсөл батлагдсанаар төрийн цахим үйлчилгээ, санхүү, эрчим хүч, харилцаа холбоо, эрүүл мэнд, дата төв, төрийн мэдээллийн сан, онц чухал болон чухал үйлчилгээний тасралтгүй, найдвартай ажиллагааг хамгаалах эрх зүйн орчин илүү тодорхой болно. Кибер халдлага, зөрчлийн үед мэдээлэл хүлээн авах, ангилах, шилжүүлэх, хариу арга хэмжээ авах, нөхөн сэргээх дараалал нэг мөр болж, иргэн, хуулийн этгээдийн үйлчилгээ тасалдах, хувийн мэдээлэл алдагдах, санхүүгийн болон шууд бус хохирол амсах эрсдэлийг бууруулах нөхцөл бүрдэнэ.

Төсөл хэрэгжихэд төрийн байгууллага, онц чухал болон чухал мэдээллийн дэд бүтэцтэй этгээд, үйлчилгээ үзүүлэгчид аудит, эрсдэлийн үнэлгээ, хамгаалалтын шийдэл, техникийн бүртгэлийн мэдээлэл, нөөцлөлт, сэргээн ажиллуулах орчин, хүний нөөц, сургалт, сургуулилалттай холбоотой нэмэлт зардал үүснэ. Гэвч эдгээр зардал нь кибер халдлага, үйлчилгээ тасалдах, өгөгдөл алдагдах, олон нийтийн итгэлцэл буурах эрсдэлийг бууруулах урьдчилан сэргийлэх хөрөнгө оруулалтын шинжтэй байна.

Хуулийн төсөлтэй уялдуулан 2021 оны 12 дугаар сарын 17-ны өдөр баталсан Кибер аюулгүй байдлын тухай хуулийг хүчингүй болсонд тооцох асуудлыг дагалдах хуулийн төсөлд тусгана. Мөн хүний хувийн мэдээлэл хамгаалах, нийтийн мэдээллийн ил тод байдал, төрийн болон албаны нууц, эрүүгийн хэрэг, зөрчил шалган шийдвэрлэх ажиллагаа, тагнуул, батлан хамгаалах, зэвсэгт хүчин, гамшгаас хамгаалах, төсөв, төрийн болон орон нутгийн өмчийн хөрөнгөөр бараа, ажил, үйлчилгээ худалдан авах ажиллагааны хууль тогтоомжтой уялдуулах шаардлагатай зохицуулалтыг тусгайлан нягтална.

Иймд Монгол Улсын кибер сөрөн тэсвэрлэх чадавхийг бодит хэрэгжих чадавхтай, байгууллага хоорондын уялдаа бүхий, эрсдэлд суурилсан, хүний эрхийн баталгаатай, тасралтгүй ажиллагаа болон нөхөн сэргээх чадавхад чиглэсэн эрх зүйн орчноор хангах зорилгоор боловсруулсан Кибер сөрөн тэсвэрлэх тухай хуулийн төслийг холбогдох үзэл баримтлал, судалгаа, зардлын тооцоо, дагалдах хуулийн төслийн хамт танилцуулж байна.