Засгийн газрын 2022 оны 493 дугаар

тогтоолын хавсралт

# КИБЕР АЮУЛГҮЙ БАЙДЛЫН ҮНДЭСНИЙ СТРАТЕГИ

## Нэг.Алсын хараа

1.1.Кибер орчинд төр, иргэн, хуулийн этгээдийн мэдээллийн аюулгүй байдал, нууцлал, хүртээмжийг үндэсний хэмжээнд хангана.

## Хоёр.Стратегийн зорилго, зорилт, хугацаа

2.1.Кибер аюулгүй байдлыг хангах эрх зүйн орчныг сайжруулж, удирдлагын нэгдсэн тогтолцоог бүрдүүлэх, онц чухал мэдээллийн дэд бүтцийн кибер аюулгүй байдлыг хангах, уян хатан байдлыг сайжруулах, кибер аюулгүй байдлын талаарх бүх нийтийн мэдлэгийг дээшлүүлж, хүний нөөцийн чадавхыг сайжруулах, гадаад болон дотоод хамтын ажиллагааг хөгжүүлэх замаар кибер орчинд мэдээллийн аюулгүй байдал, нууцлал, хүртээмжийг үндэсний хэмжээнд хангахад энэхүү стратегийн зорилго оршино.

2.2.Стратегийн зорилгыг дараахь зорилтын хүрээнд хэрэгжүүлнэ:

2.2.1.кибер аюулгүй байдлыг хангах эрх зүйн орчин, удирдлагын тогтолцоог бэхжүүлэх;

2.2.2.онц чухал мэдээллийн дэд бүтэцтэй байгууллагын кибер аюулгүй байдлыг хангах;

2.2.3.хүний нөөцийн чадавхыг сайжруулах, шинээр бэлтгэх, давтан сургах;

2.2.4.кибер аюулгүй байдлыг хангах хамтын ажиллагааг өргөжүүлэх;

2.2.5.кибер аюулгүй байдлын уян хатан байдал, халдлагад хариу үйлдэл үзүүлэх чадамжийг бүрдүүлэх.

2.3.Стратегийг 5 жилийн хугацаанд дараахь үе шаттай хэрэгжүүлнэ:

2.3.1.I үе шат: 2022-2025;

2.3.2.II үе шат: 2026-2027.

## Гурав.Кибер аюулгүй байдлын үндэсний стратегийн зорилтыг хэрэгжүүлэх үйл ажиллагаа

3.1.Кибер аюулгүй байдлыг хангах эрх зүйн орчин, удирдлагын тогтолцоог бэхжүүлэх зорилтын хүрээнд дараахь үйл ажиллагааг хэрэгжүүлнэ:

3.1.1.кибер аюулгүй байдлыг хангах эрх зүйн орчныг бэхжүүлэх:

3.1.1.1.кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлагаар хангах, уялдуулан зохицуулах, хэрэгжилтийг зохион байгуулах, мэдээлэл солилцох чиг үүрэг бүхий зөвлөлийг байгуулж, үйл ажиллагааг жигдрүүлэх;

3.1.1.2.кибер халдлага, зөрчлийн талаарх мэдээллийг төр, хувийн хэвшлийн байгууллагууд харилцан солилцох эрх зүйн орчинг бүрдүүлэх;

3.1.1.3.кибер аюулгүй байдлын эрсдэлийн үнэлгээнд үндэслэн кибер халдлагаас хамгаалах төлөвлөгөөг боловсруулж, тасралтгүй сайжруулах хяналтыг хэрэгжүүлэх;

3.1.1.4.кибер аюулгүй байдлыг хангах талаарх олон улсын стандартыг нутагшуулж, түүнд нийцүүлэн дүрэм, журам баталж, хэрэгжүүлэх;

3.1.1.5.кибер аюулгүй байдлын эрсдэлийн үнэлгээнд суурилсан мэдээллийн аюулгүй байдлын хараат бус, хөндлөнгийн, мэргэжлийн үйл ажиллагааг бэхжүүлэх;

3.1.1.6.төрийн байгууллага, төрийн өмчит хуулийн этгээдийн кибер аюулгүй байдлыг хангах тогтолцоог сайжруулахад шаардлагатай хөрөнгө оруулалтыг нэмэгдүүлэхийг бодлогоор дэмжих.

3.1.2.Кибер орчинд хүний эрхийг хамгаалах эрх зүйн орчинг боловсронгуй болгох:

3.1.2.1.кибер орчинд хүний эрхэд халдах, худал мэдээлэл түгээх болон энэ төрлийн зөрчилтэй тэмцэх эрх зүйн орчинг шат дараатай сайжруулах;

3.1.2.2.кибер орчинд хүүхэд хамгаалах эрх зүйн орчинг сайжруулах;

3.1.2.3.кибер терроризм, гэмт хэрэгтэй тэмцэх, хууль эрх зүйн орчинг боловсронгуй болгох.

3.2.Онц чухал мэдээллийн дэд бүтэцтэй байгууллагын кибер аюулгүй байдлыг хангах зорилтын хүрээнд дараахь үйл ажиллагааг хэрэгжүүлнэ:

3.2.1.онц чухал мэдээллийн дэд бүтэцтэй төрийн болон хувийн хэвшлийн байгууллагуудад эрсдэлийн удирдлагын тогтолцоог нэвтрүүлэх;

3.2.2.төрийн болон онц чухал мэдээллийн дэд бүтэцтэй байгууллагад ашиглах мэдээлэл, холбооны тоног төхөөрөмж, мэдээллийн системийг шалган баталгаажуулах лаборатори байгуулах;

3.2.3.Монгол Улсаас хилийн чанадад суугаа дипломат төлөөлөгчийн газар болон төрийн байгууллагын төрийн нууцад хамаарах мэдээ, мэдээлэл солилцох нөхцөлийг бүрдүүлж, хүртээмжийг нэмэгдүүлэх;

3.2.4.онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудад нөхөн сэргээх үйл ажиллагаа, хямралын үеийн удирдлагын

тогтолцоог бүрдүүлэх;

3.2.5.их өгөгдөл, хиймэл оюун ухаан, зүйлсийн интернэт, үүлэн технологи, машин сургалт зэрэг дэвшилтэт технологийн хэрэглээнээс үүдэн гарах эмзэг байдал, аюул заналыг таних, эрсдэлийг бууруулах боломжийг сайжруулах.

3.3.Хүний нөөцийн чадавхыг сайжруулах, шинээр бэлтгэх, давтан сургах зорилтын хүрээнд дараахь үйл ажиллагааг хэрэгжүүлнэ:

3.3.1.Бүх нийтийн кибер аюулгүй байдлын мэдлэг, ойлголтыг дээшлүүлэх:

3.3.1.1.бүх шатны боловсролын байгууллагын сургалтын хөтөлбөрт кибер аюулгүй байдлыг хангах мэдлэг олгох агуулгыг тусгах;

3.3.1.2.кибер аюулгүй байдлыг хангах мэдлэг, ойлголт өгөх үндэсний хэмжээний аян, хөтөлбөрийг тогтмол зохион байгуулах;

3.3.1.3.кибер аюулгүй байдлын чиглэлээр үндэсний болон олон улсын тэмцээн, сургалт, семинар тогтмол зохион байгуулах.

3.3.2.кибер аюулгүй байдлын мэргэшсэн хүний нөөцийг чадавхжуулах:

3.3.2.1.кибер гэмт хэрэг, терроризмтой тэмцэх тусгайлсан чиг үүрэг бүхий байгууллагын хүний нөөцийг бэлтгэх;

3.3.2.2.кибер аюулгүй байдал судлаачдын сургалт, судалгаа, эрдэм шинжилгээний ажлыг дэмжих хөтөлбөр хэрэгжүүлэх;

3.3.2.3.кибер аюулгүй байдлыг хангах хүний нөөцийг чадавхжуулах, мэргэшүүлэх богино, дунд, урт хугацааны сургалтыг нэвтрүүлж, хэрэгжүүлэх;

3.3.2.4.кибер аюулгүй байдлын нийгэмлэгүүдийн үйл ажиллагааг бодлогоор дэмжих.

3.4.Кибер аюулгүй байдлыг хангах хамтын ажиллагааг өргөжүүлэх зорилтын хүрээнд дараахь үйл ажиллагааг хэрэгжүүлнэ:

3.4.1.кибер аюулгүй байдлыг хангах, гэмт хэрэгтэй тэмцэх чиглэлээр Монгол Улсын үндэсний язгуур эрх ашигт харшлахгүй үйл ажиллагаа явуулдаг олон улсын болон бүс нутгийн хэмжээний байгууллагатай хамтран ажиллах, олон улсын байгууллагад гишүүнээр элсэх болон конвенцод нэгдэн орох боломжийг эрэлхийлэх;

3.4.2.кибер аюулгүй байдлыг хангах олон улсын мэргэжлийн холбоонд гишүүнээр элсэх;

3.4.3.кибер аюулгүй байдлыг хангах хүний нөөцийг чадавхжуулах, судалгаа, шинжилгээний ажлыг эрчимжүүлэх чиглэлээр дотоод болон гадаадын байгууллагатай хамтран ажиллах;

3.4.4.төрийн захиргааны байгууллага, хувийн хэвшил, төрийн бус байгууллагын оролцоог хангах, жижиг, дунд, гарааны бизнес эрхлэгч, их сургууль, эрдэм шинжилгээний байгууллагын кибер аюулгүй байдлыг хангах хамтын ажиллагааг өргөжүүлэх;

3.4.5.кибер аюулгүй байдлын өнөөгийн болон зорилтот түвшинг тогтоох, олон улсын стандарт, аргачлалыг нэвтрүүлэхэд олон улсын болон гадаад улсын байгууллагатай хамтран ажиллах;

3.4.6.мэдээлэл, харилцаа холбооны техник хэрэгсэл, программ хангамж, электроникийн үндэсний үйлдвэрлэл, инновац, судалгаа, шинжилгээний хөгжүүлэлтийг дэмжиж, технологийн хараат байдлыг бууруулах.

3.5.Кибер аюулгүй байдлын уян хатан байдал, халдлагад хариу үйлдэл үзүүлэх чадамжийг бүрдүүлэх зорилтын хүрээнд дараахь үйл ажиллагааг хэрэгжүүлнэ:

3.5.1.кибер халдлага, зөрчилтэй тэмцэх Үндэсний төв, Нийтийн төв болон Зэвсэгт хүчний төвийг тус тус байгуулж, кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах үйл ажиллагааг тасралтгүй хэрэгжүүлэх;

3.5.2.кибер халдлага, зөрчилд задлан шинжилгээ хийх тоон шинжилгээний лабораторийг байгуулж, кибер орчин дахь гэмт хэргийг илрүүлэх, нотлох баримт бүрдүүлэх чадавхыг нэмэгдүүлэх;

3.5.3.кибер аюулгүй байдлыг хамгаалахад сүүлийн үеийн дэвшилтэт технологи нэвтрүүлж, шинэ төрлийн арга, техник ашиглахыг дэмжих;

3.5.4.кибер халдлага, зөрчлийн талаарх мэдээлэл солилцох суурь дэд бүтцийг хөгжүүлэх;

3.5.5.кибер халдлага, зөрчилтэй тэмцэх төвүүд хоорондын ажиллагааг идэвхжүүлж, мэдээлэл солилцох технологийн шийдлийг нэвтрүүлэх;

3.5.6.тухайлсан салбар, чиглэлээр кибер халдлага, зөрчилтэй тэмцэх нэгж байгуулахад дэмжлэг үзүүлэх;

3.5.7.үндэсний хэмжээний кибер халдлагаас хамгаалах, зөрчлийн үеийн нөхцөл байдлыг үнэлэх, хариу үйлдэл үзүүлэх, тасралтгүй ажиллах төлөвлөгөөг хэрэгжүүлэх;

3.5.8.кибер гэмт хэрэг, терроризмтой тэмцэх чиглэлээр олон улсын болон бүс нутгийн, мэргэжлийн байгууллагуудтай мэдээлэл солилцох нөхцөлийг бүрдүүлэх;

3.5.9."Үндэсний дата төв" УТҮГ-ын аюулгүй байдлыг хангах чадавхыг нэмэгдүүлэх;

3.5.10.онцгой нөхцөл байдал үүссэн (дайны) үед улсын хэмжээнд кибер орон зайг хамгаалах чадавхыг хөгжүүлэх;

3.5.11.нийтийн түлхүүрийн дэд бүтцийг шинэчилж, олон улсад итгэмжлэгдсэн байх нөхцөлийг хангах;

3.5.12.монголын интернэтийн харилцан холболтын үндсэн сүлжээний өсөн нэмэгдэх хэрэгцээнд тулгуурлан интернэт гарцыг нэмэгдүүлж, аюулгүй байдлыг хангах;

3.5.13.тусгай хэрэглээний радио давтамжийн зурвасын ашиглалт, давтамж хоорондын нөлөөлөлд хяналт тавих техникийн нөхцөл (радио давтамжийн хяналтын эфир)-ийг бүрдүүлэх.

Дөрөв.Стратегийг хэрэгжүүлэх удирдлага,

зохион байгуулалт, хөрөнгө оруулалт

4.1.Үндэсний стратегийг хэрэгжүүлэх үйл ажиллагааг Засгийн газар, Кибер аюулгүй байдлын Үндэсний зөвлөл нэгдсэн удирдлага, зохицуулалтаар хангана.

4.2.Кибер аюулгүй байдлыг хангах үүрэг бүхий байгууллагууд энэхүү стратегийг хэрэгжүүлэх арга хэмжээний төлөвлөгөөг Засгийн газрын үйл ажиллагааны хөтөлбөр, түүнийг хэрэгжүүлэх арга хэмжээний төлөвлөгөөтэй уялдуулан боловсруулж хэрэгжүүлнэ.

4.3.Стратегийг хэрэгжүүлэхэд шаардагдах хөрөнгийн эх үүсвэр нь улсын болон орон нутгийн төсөв, хандивлагч орон, олон улсын банк, санхүүгийн байгууллагын зээл, буцалтгүй тусламж, хувийн хэвшлийн хөрөнгө оруулалт байна.

Тав.Стратегийн зорилтын шалгуур үзүүлэлт,

зорилтот түвшин

5.1.Стратегийн үр дүнг дараахь шалгуур үзүүлэлтээр үнэлнэ:

| № | Шалгуур үзүүлэлт | Хэмжих нэгж | Суурь түвшин | Зорилтот түвшин (2025 он) | Зорилтот түвшин (2027 он) | Мэдээл-лийн эх сурвалж |
|---|---|---|---|---|---|---|
| Зорилт 1. Кибер аюулгүй байдлыг хангах эрх зүйн зохицуулалтыг бэхжүүлэх | | | | | | |
| 1. | Кибер аюулгүй байдлыг хангах хууль, эрх зүйн орчны индекс | индексийн үзүүлэлт | 9.0 (2021оны байдлаар) | 12.6 | 14.4 | ОУЦХБ, Кибер аюулгүй байдлын судалгаа |
| 2. | Кибер аюулгүй байдлыг хангах чиглэлээр баталсан дүрэм, журмын тоо | тоо | 2 (2022 оны байдлаар) | 8 | 12 | ЦХХХЯ |
| Зорилт 2.Онц чухал мэдээллийн дэд бүтэцтэй байгууллагын кибер аюулгүй байдлыг хангах | | | | | | |
| 3. | Кибер аюулгүй байдлын эрсдэлд суурилсан мэргэшсэн үйл ажиллагааг нэвтрүүлсэн онц чухал мэдээллийн дэд бүтэцтэй байгууллагын өсөлтийн хувь | Эрсдэлийн үнэлгээнд хамрагдсан байгууллагын хувь | 2.77 (2022 оны байдлаар) | 50-аас доошгүй | 80-аас доошгүй | ЦХХХЯ Таг.ЕГ |
| | | Эрх бүхий байгууллагаас хүргүүлсэн зөвлөмж, шаардлагыг хэрэгжүүлсэн байгууллагын хувь | 0 (2022 оны байдлаар) | 43-аас доошгүй | 82.4-өөс доошгүй | ЦХХХЯ Таг.ЕГ |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4. | Нөхөн сэргээх үйл ажиллагаа, тасралтгүй ажиллагааны удирдлагын тогтолцоог бүрдүүлсэн байгууллагын өсөлтийн хувь | хувь | 11.5<br>(2022 оны байдлаар) | 80-аас доошгүй | 100 | КХЗТТөвүүд |
| 5. | Тоон шинжилгээний дүгнэлт нотлох баримтын эх сурвалж болох нөхцөлийг бүрдүүлэх | тоон шинжилгээний лабораторийн үйл ажиллагаа жигдэрсэн эсэх | Тоон шинжилгээний лаборатори байгуулах төслийн хэрэгжилт 66%<br>(2021 оны байдлаар) | Лаборатори ашиглалтад орсон байна | Хууль, эрх зүйн орчин бүрдсэн байна. | ТЕГ, ШШҮХ |
| Зорилт 3. Хүний нөөцийн чадавхыг сайжруулах, шинээр бэлтгэх, давтан сургах | | | | | | |
| 6. | Иргэдийн тоон бичиг үсгийн чадавх | хувь | 43.8<br>(2021оны байдлаар) | 47.9 | 50 | ҮСХ, Өрхийн судалгаа |
| 7. | Кибер аюулгүй байдлын судалгааны хүний нөөцийн индекс | индексийн үзүүлэлт | 1.23<br>(2021 оны байдлаар) | 4.53 | 6.73 | ОУЦХБ, Кибер аюулгүй байдлын судалгаа |
| Зорилт 4. Кибер аюулгүй байдлыг хангах хамтын ажиллагааг өргөжүүлэх | | | | | | |
| 8. | Кибер аюулгүй байдлын хамтын ажиллагааны индекс | индексийн үзүүлэлт | 6.82<br>(2021 оны байдлаар) | 8.58 | 9.76 | ОУЦХБ<br>Кибер аюулгүй байдлын судалгаа |
| 9. | Кибер аюулгүй байдлыг хангах олон улсын байгууллагын гишүүнчлэлийн өсөлт | гишүүнчлэлийн тоо | 1<br>(2022 оны байдлаар) | 3 | 6 | FIRST.org<br>APCERT |
| Зорилт 5. Кибер аюулгүй байдлын уян хатан байдал, халдлагад хариу үзүүлэх чадамжийг бүрдүүлэх | | | | | | |
| 10. | Үндэсний тоон гарын үсгийг олон улсад ашиглах нөхцөлийг бүрдүүлэх | Олон улсын итгэмжлэгдсэн жагсаалтад орсон эсэх | Нийтийн түлхүүрийн дэд бүтэц (2014 онд ашиглалтад орсон) | Үндэсний тоон гарын үсгийн үндсэн дэд бүтцийг шинэчилсэн байна. | Олон улсын итгэмжлэгдсэн жагсаалтад орсон байна. | ЦХХХЯ |

| | | | | | | |
|---|---|---|---|---|---|---|
| 11. | Олон улсын интернэтийн гарцын өсөлт | тоо | 2 (2022 оны байдлаар) | 3 | 3-аас доошгүй | ЦХХХЯ, ХХЗХ |
| 12. | Кибер халдлага, зөрчилтэй тэмцэх төв | тоо | 1 (2022 оны байдлаар) | 3 | 3-аас доошгүй | ЦХХХЯ, Таг.ЕГ, КХЗТТөв-үүд |

Зургаа.Стратегийн хэрэгжилтэд хяналт-шинжилгээ,

үнэлгээ хийх

6.1.Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага энэхүү стратегийн зорилт, үйл ажиллагааны хэрэгжилтийн үе шат дуусах бүрд хяналт-шинжилгээ, үнэлгээ хийж, үр дүнг Кибер аюулгүй байдлын зөвлөлд танилцуулна.

---o0o---