МОНГОЛ УЛСЫН
БАТЛАН ХАМГААЛАХЫН САЙДЫН
ТУШААЛ

2023 оны 12 сарын 27 өдөр Дугаар А/425 Улаанбаатар хот

Журам батлах тухай

Монгол Улсын Засгийн газрын тухай хуулийн 24 дүгээр зүйлийн 2, Монгол Улсын яамны эрх зүйн байдлын тухай хуулийн 8.2 дахь хэсэг, Монгол Улсын батлан хамгаалах тухай хуулийн 14 дүгээр зүйлийн 14.1.14, Кибер аюулгүй байдлын тухай хуулийн 14 дүгээр зүйлийн 14.1.1, 14.1.2 дахь заалт, Засгийн газрын 2023 оны 224 дүгээр тогтоолын хавсралтаар батлагдсан "Кибер аюулгүй байдлыг хангах нийтлэг журам"-ын 1.2 дахь хэсэг, Батлан хамгаалахын сайдын зөвлөлийн 2023 оны 11 дүгээр хуралдааны шийдвэрийг тус тус үндэслэн ТУШААХ нь:

1. "Батлан хамгаалахын кибер аюулгүй байдлыг хангах журам"-ыг хавсралтаар баталж, 2024 оны 01 дүгээр сарын 01-ний өдрөөс мөрдсүгэй.

2. Журмын хэрэгжилтийг ханган, холбогдох зардлыг шийдвэрлэж ажиллахыг Батлан хамгаалах яам (бригадын генерал Д.Ганхуяг), Зэвсэгт хүчний Жанжин штаб (хошууч генерал С.Ганбямба), Төрлийн цэргийн командлагч (дарга), цэргийн нэгтгэл, анги, байгууллагын захирагч (дарга) нарт үүрэг болгосугай.

3. Тушаалын хэрэгжилтэд хяналт тавьж ажиллахыг яамны Хяналт-шинжилгээ, үнэлгээ, дотоод аудитын газар (хурандаа Н.Пүрэвдорж)-т даалгасугай.

САЙД Г.САЙХАНБАЯР

323100799

Батлан хамгаалахын сайдын 2023 оны
12..дугаар сарын 07-ны өдрийн
... дугаар тушаалын хавсралт
04/425

БАТЛАН ХАМГААЛАХЫН КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1. Батлан хамгаалахын кибер аюулгүй байдлыг хангахтай холбогдсон харилцааг энэхүү журмаар зохицуулна.

1.2. Зэвсэгт хүчний тухай, Кибер аюулгүй байдлын тухай хууль, Монгол Улсын Засгийн газар, Кибер аюулгүй байдлын зөвлөл, батлан хамгаалахын болон цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллагаас гаргасан холбогдох хууль, дүрэм, журам, стандарт нь энэхүү журмын эрх зүйн үндэслэл болно.

1.3. Батлан хамгаалах яам, түүний харьяа байгууллага, Зэвсэгт хүчний тухай хуулийн шинэчилсэн найруулгын 7.3-т заасан нэгжүүд, мөн гадаад улсад үүрэг гүйцэтгэж байгаа Зэвсэгт хүчний цэргийн баг (цаашид "байгууллага" гэх), бие бүрэлдэхүүн (цэргийн ажиглагч болон штабын офицерууд) энэхүү журмыг дагаж мөрдөнө.

1.4. Энэ журамд хэрэглэсэн нэр томъёог дор дурдсан утгаар ойлгоно:

1.4.1."Батлан хамгаалахын кибер аюулгүй байдал" гэж (цаашид "КАБ" гэх) кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, хамгаалах, хариу арга хэмжээ авах, эрсдлийн үнэлгээ хийх, программын болон техникийн шалган баталгаажуулалт, сургалт, соён гэгээрүүлэх ажил, кибер технологийн ашиглалт, хөгжүүлэлт, хамтын ажиллагааг;

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

1.4.3."Мэдээллийн сүлжээ" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.2-д заасныг;

1.4.4."Нөөц" гэж болзошгүй эрсдэлээс урьдчилан сэргийлэх зорилгоор хуулбарлан хадгалсан өгөгдлийг;

1.4.5."Халдлагаас урьдчилан сэргийлэх систем" (IPS-Intrusion Prevention System) гэж сүлжээн дэх мэдээллийн пакетын агуулгад үндэслэн хортой пакетуудыг сүлжээнд нэвтрэхээс сэргийлдэг системийг;

1.4.6."Халдлагыг илрүүлэх систем (IDS-Intrusion Detection System) гэж сүлжээний урсгалыг хянаж халдлагын шинж тэмдгийг илрүүлэх, дүн шинжилгээ хийх, халдлага илэрсэн тохиолдолд анхааруулга /alert/ илгээдэг системийг;

1.4.7.Вебэд суурилсан галт хана (WAF-Web Application Firewall) гэж Вебэд суурилсан программ хангамжуудын хоорондох "HTTP" урсгалыг шүүх, хянах замаар нэвтрүүлдэг программ хангамжийг;

1.4.8.Имэйл шүүлтүүр (Email Filter) гэж цахим шууданг тодорхой шалгуурын дагуу (спам эсвэл фишингээс хамгаалах, дүн шинжилгээ хийх) эмх цэгцэнд оруулах үйл ажиллагааг;

1.4.9.Аюулгүй байдлын мэдээлэл, үйл ажиллагааны менежмент (SIEM-Security information and event management) гэж кибер халдлага, зөрчил илрэхээс өмнө аюулгүй байдлын хувьд болзошгүй халдлага, эмзэг байдлыг урьдчилан таньж илрүүлэх, хэрэгжүүлэх ажлыг тодорхойлдог программ хангамж болон үйлчилгээг;

1.4.10.Нөхөөс (Patch) гэж программын эмзэг байдал мэдэгдсэн даруйд үйлдвэрлэгч эсвэл хөгжүүлэгчээс гаргасан сайжруулалт хийгдсэн программ хангамжийг;

1.4.11.энэ журамд тусгагдаагүй КАБ-ын талаар бусад нэр томъёог Кибер аюулгүй байдлын тухай хуульд зааснаар ойлгоно.

Хоёр. Кибер халдлага, зөрчлөөс урьдчилан сэргийлэх

2.1. Энэхүү журмын 1.3-д заасан байгууллага нь кибер халдлага, зөрчлөөс урьдчилан сэргийлэх чиглэлээр дараах арга хэмжээг авч хэрэгжүүлнэ:

2.1.1. кибер аюулгүй байдлын сургалт, сурталчилгаа, соён гэгээрүүлэх ажлыг өөрийн бие бүрэлдэхүүнтэй тогтмол явуулахын зэрэгцээ, хамтран ажиллагч байгууллагуудад дэмжлэг үзүүлэх;

2.1.2.байгууллагын чухал мэдээллийн сан, өгөгдөлийн хувилсан нөөцийг үүсгэх, нууцлалын горимыг холбогдох журмын дагуу чанд мөрдүүлэх;

2.1.3.байгууллагад ашиглагдаж байгаа мэдээллийн систем, программ хангамжид хийгдэх хугацаат шинэчлэлийг тухай бүрд хойшлуулалгүй хийх.

2.2. Алба хаагч нь кибер халдлага, зөрчлөөс урьдчилан сэргийлэх чиглэлээр дараах ажлыг гүйцэтгэнэ:

2.2.1.кибер аюулгүй байдлыг хангахтай холбоотой хууль, эрх зүйн мэдлэгээ байнга нэмэгдүүлэх, үйл ажиллагаанд нэвтэрч буй мэдээллийн технологийн зохистой хэрэглээг судалж, мэдэх;

2.2.2.өөрийн аюулгүй байдлыг хангахаас гадна хамтран ажиллагч нөхрийнхөө ойрын зөвлөх нь байж, зөрчил гаргахаас сэргийлэх;

2.2.3.журмын хэрэгжилтийг хангахад холбогдох байгууллага, албан тушаалтанд дэмжлэг үзүүлэх, хуулийн хүрээнд кибер аюулгүй байдлыг сайжруулах талаар санал, санаачилга гаргах, хамтран ажиллах.

Гурав. Кибер халдлага, зөрчлийг илрүүлэх

3.1. Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээний хэвийн бус үйл ажиллагааг илрүүлэхэд дараах арга хэмжээг авч хэрэгжүүлнэ:

3.1.1.мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийг тогтмол цуглуулж, тайлан гаргах;

3.1.2.мэдээллийн систем, мэдээллийн сүлжээний хэвийн бус үйл ажиллагаа, үйлдлийг ноцтой байдлаар нь эрэмбэлж, эрэмбийн дарааллаар эрх бүхий албан тушаалтан, хуулийн этгээдэд мэдээлэх нөхцөлийг бүрдүүлэх;

3.1.3.мэдээллийн систем, мэдээллийн сүлжээ, аюулгүй байдлын тоног төхөөрөмжийн үйлдлийн бүртгэлийг нэгтгэн цуглуулж, дүн шинжилгээ хийх боломжийг бүрдүүлэх;

3.1.4.кибер халдлага, зөрчилтэй холбоотой нотлох баримтыг цуглуулж, баримтын хуулбарыг эх хувиас зөрүүгүй байлгах.

3.2. Мэдээллийн систем, мэдээллийн сүлжээг хянахад байгууллага нь дараах арга хэмжээг хэрэгжүүлнэ:

3.2.1.мэдээллийн сүлжээний урсгалд тасралтгүй хяналт тавих;

3.2.2.биет орчныг хянах;

3.2.3.мэдээллийн систем, мэдээллийн сүлжээнд үйлчилгээ авах тохиолдолд тухайн үйлчилгээ үзүүлэгчийн үйл ажиллагаанд хяналт тавих;

3.2.4.мэдээллийн системийн эмзэг байдлын шалгалтыг тогтмол хийх.

3.3. Байгууллага нь кибер халдлага, зөрчлийг илрүүлэх ажиллагааг байнга туршин шалгаж, илрүүлэх ажиллагааны арга хэлбэрт тогтмол сайжруулалт хийнэ.

3.4. Байгууллага нь журмын 1.4.6-1.4.11-д тусгасан өөрийн мэдээллийн системд тохирсон кибер аюулгүй байдлыг хангах үүрэг бүхий цогц технологи, техник, программ хангамжийг хэрэглэнэ.

Дөрөв. Кибер халдлага, зөрчлөөс хамгаалах

4.1. Байгууллага нь мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээнд хандах эрхийг тодорхойлж, энэ талаар бүртгэл хөтөлнө.

4.2. Кибер аюулгүй байдлын цэргийн командлал (цаашид “КАБЦК” гэх)-аас мэдээллийн систем, мэдээллийн сүлжээнд давуу эрхтэй (admin) хандах албан тушаалтныг тогтоож, хандах эрхийн ашиглалтыг хянана.

4.3. Байгууллагын мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байрлаж байгаа зориулалтын өрөөнд зөвшөөрөлгүй нэвтрэхийг хориглох бөгөөд өрөө нь дараах шаардлагыг хангасан байна:

4.3.1.өрөөний хаалга байнга цоожтой байх;

4.3.2.цонхны хамгаалалттай байх;

4.3.3.дотор болон гадна дүрст хяналтын системтэй байх;

4.3.4.температур, чийгшил зэрэг орчны нөхцөлийг хянах боломжтой техник болон программ хангамжаар тоноглогдсон байх.

4.4. Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээний техник, тоног төхөөрөмжийг байршуулах зориулалтын өрөөгүй бол энэ журмын 3.3-т заасан шаардлагад дүйцэх, тоног төхөөрөмжид зөвшөөрөлгүй этгээд хандахаас сэргийлсэн зориулалтын зогсуур /Rack/-т байршуулж болно.

4.5. Байгууллагын алба хаагч бүр хэрэглэгчийн эцсийн төхөөрөмж (компьютер гэх мэт)-тэй ажиллахад аюулгүй байдлыг хангах талаар дараах арга хэмжээг хэрэгжүүлнэ:

4.5.1.байгууллага зөвшөөрснөөс бусад төрлийн программ хангамжийг ашиглахгүй байх;

4.5.2.төхөөрөмжид нэвтрэхэд нууц үгийг "Зэвсэгт хүчний мэдээллийн аюулгүй байдлыг хангах журам"-ын 5.5.6.2.3-д заасны дагуу ашигладаг байх;

4.5.3.хувийн хэрэгцээнд ашиглахгүй байх;

4.5.4.нууцын зэрэглэлтэй мэдээлэл агуулсан төхөөрөмжийг зөвшөөрсөн бүсээс зөвшөөрөлгүйгээр гадагш гаргахгүй байх;

4.5.5.байгууллагаас өөрт олгосон төхөөрөмж, нэвтрэх нэр, нууц үгийг ашиглах ба бусдад дамжуулж, ашиглуулахгүй байх;

4.5.6.засвар үйлчилгээг зөвхөн байгууллагын мэдээллийн технологи хариуцсан нэгж, ажилтнаар оношлуулах, засварлуулах.

4.6. Байгууллага нь мэдээлэл, түүнийг агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээний техник хэрэгсэлд хортой кодоос хамгаалах лицензтэй программ хангамж ашиглана.

4.7. Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээнээс мэдээлэл алдагдахаас сэргийлэх талаар дараах арга хэмжээг авч хэрэгжүүлнэ:

4.7.1.алдагдах эрсдэлтэй мэдээллийг тодорхойлох;

4.7.2.мэдээлэл алдагдаж болзошгүй мэдээллийн систем, мэдээллийн сүлжээ, төхөөрөмж, зөөврийн хэрэгслүүдийг тогтмол хянах;

4.7.3.мэдээллийг холбогдолгүй этгээдэд дамжуулахаас сэргийлэх, дамжуулсан тохиолдолд холбогдох албан тушаалтанд нэн даруй мэдэгдэх;

4.7.4.мэдээлэлд зөвшөөрөлгүй хандаж, ашиглах, устгах, өөрчлөх үйлдэл хийж байгаа этгээдийн үйлдлийг таслан зогсоох;

4.7.5.мэдээллийн систем, мэдээллийн сүлжээний, өгөгдөл, тохиргоог нөөцлөх хуваарь гаргаж, хуваарийн дагуу тогтмол нөөцлөж байгууллагын нууцад хадгалах.

4.8. Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээнд дараах үйлдлийн бүртгэлийг /log file/ хөтөлнө:

4.8.1.нэвтрэх оролдлого болон нэвтэрсэн тухай;

4.8.2.давуу эрхийн хандалт;

4.8.3.нууц үгийн өөрчлөлт;

4.8.4.үйлдлийн бүртгэлийг өөрчлөх, устгах;

4.8.5.хандах эрх олгох, өөрчлөх, хүчингүй болгох.

4.9. Үйлдлийн бүртгэлд дараах мэдээллийг тодорхойлно.

4.9.1.хэрэглэгчийн нэр, системд нэвтрэх нэр буюу ID;

4.9.2.огноо;

4.9.3.хандсан хаяг, төхөөрөмжийн мэдээлэл;

4.9.4.хандалтын үргэлжлэх хугацаа;

4.9.5.гүйцэтгэсэн үйлдэл;

4.9.6.гүйцэтгэсэн үйлдлийн үр дүн.

4.10. Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийг нэг жилийн хугацаатай хадгална.

4.11. Сэжигтэй үйлдлийн бүртгэл илэрвэл КАБЦК-д тухай бүрд нь хүргүүлнэ.

4.12. Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээнд ашиглагдаж байгаа үйлдлийн систем, программ хангамжийг шинэчлэхэд дараах арга хэмжээг авч хэрэгжүүлнэ.

4.12.1.шинэчлэл /patch, update/ гарах бүрт суулгах;

4.12.2.зөвшөөрөгдсөн, албан ёсны эх үүсвэрээс шинэчлэх.

Тав. Кибер халдлага, зөрчилд хариу арга хэмжээ авах

5.1. Байгууллага нь “Зэвсэгт хүчний кибер аюулгүй байдлын заавар”-ын дагуу кибер халдлага, зөрчлийн үед хариу арга хэмжээ авах төлөвлөгөөг баталж, хэрэгжүүлэх бөгөөд төлөвлөгөөнд дараах мэдээллийг тусгана.

5.1.1.байгууллага дотор кибер халдлага, зөрчлийг мэдэгдэх албан тушаалтан;

5.1.2.тохиолдлыг шинжилж, кибер халдлага, зөрчилд тооцох шалгуур үзүүлэлт;

5.1.3.халдлага, зөрчлийн талаарх мэдээллийг илгээх, хүлээн авах суваг.

5.2. Кибер аюулгүй байдал хариуцсан ажилтан энэ журмын 5.1.2-т заасан шалгуур үзүүлэлтийн дагуу кибер халдлага, зөрчлийн тохиолдол бүрт үнэлгээ хийж халдлага, зөрчлийг тодорхойлно.

5.3. Байгууллага кибер халдлага, зөрчилд өртсөн тохиолдолд төлөвлөгөөний дагуу хариу арга хэмжээг хэрэгжүүлж, шаардлагатай тохиолдолд КАБЦК-д мэдэгдэнэ.

Зургаа. Мэдээллийн систем, мэдээллийн сүлжээг нөхөн сэргээх

6.1. Байгууллага нь нөхөн сэргээх ажиллагааг энэ журмын 6.2, 6.3-т заасныг баримтлан шат дараалсан арга хэмжээг авч хэрэгжүүлнэ.

6.2. Кибер халдлага, зөрчлийн хор уршгийг арилгахад дараах арга хэмжээг авч хэрэгжүүлнэ:

6.2.1.кибер халдлага, зөрчилд өртсөн мэдээллийн систем, мэдээллийн сүлжээний нотлох баримтыг хөндөхөөс сэргийлэх;

6.2.2.мэдээллийн систем, мэдээллийн сүлжээ хэвийн байдалд орж сэргэх хүртэл холболт, ашиглалтыг хязгаарлах;

6.2.3.байгууллагын үйл ажиллагаа хэвийн байдалд шилжих хүртэл кибер халдлага, зөрчил илэрсэн үндсэн шалтгаан болсон мэдээллийн системийн үйл ажиллагааг зогсоох.

6.3. Мэдээллийн систем, мэдээллийн сүлжээний хэвийн үйл ажиллагааг нөхөн сэргээхэд дараах арга хэмжээг авч хэрэгжүүлнэ:

6.3.1.кибер халдлага, зөрчилд өртсөн мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийг боломжит хамгийн бага хугацаанд нөөцлөлтөөс сэргээх;

6.3.2.нөхөн сэргээгдсэн мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийг кибер халдлага, зөрчилд өртөхөөс өмнөх үеийн хэвийн төлөвт эргэн шилжсэнийг шалгасны дараа системийн хэвийн үйл ажиллагаанд оруулна;

6.3.3.нөхөн сэргээх үйл ажиллагааны хүрээнд авсан арга хэмжээ, үр дүнг баримтжуулан холбогдох эрх бүхий албан тушаалтанд танилцуулах;

6.3.4.мэдээллийн систем, мэдээллийн сүлжээ, мэдээллийг нөхөн сэргээж, хэвийн үйл ажиллагаанд оруулсан талаар тодорхой түвшний нотолгоо, үр дүнд үндэслэн нөхөн сэргээх үйл ажиллагааг дуусгах.

Долоо. Кибер аюулгүй байдлыг хангах удирдлага, зохион байгуулалт

7.1. КАБЦК нь холбогдох хууль тогтоомжийн хүрээнд Зэвсэгт хүчний кибер орон зайг хамгаалах, байгууллагын мэдээллийн систем, мэдээллийн сүлжээний эрсдлийг үнэлэх, техник хангамж, программ хангамжид шалган баталгаажуулалт хийх, сургалт, сурталчилгааны ажлыг зохион байгуулна.

7.2. КАБЦК-аас томилогдсон бүрэлдэхүүн 2-3 жилд 1 удаа эсвэл эрсдэлтэй нөхцөл байдал үүссэн үед байгууллагын эрсдлийн үнэлгээг “КАБ-ын эрсдэлийн үнэлгээний заавар”-ын дагуу хийж гүйцэтгэнэ.

7.3. КАБЦК нь байгууллагуудад ашиглагдаж байгаа мэдээллийн технологийн техник, программ хангамжийг шалган баталгаажуулна. Шалган баталгаажуулалтыг хийхдээ “Зэвсэгт хүчний кибер аюулгүй байдлын заавар”-ыг мөрдлөг болгоно.

7.4. Байгууллага нь КАБ хариуцсан орон тооны албан тушаалтантай байна.

7.5. Байгууллага нь КАБ-ыг хангахад зохион байгуулалтын чиглэлээр дараах арга хэмжээг авч хэрэгжүүлнэ:

7.5.1.байгууллагын аюулгүй байдлыг хангах төлөвлөгөөнд Кибер аюулгүй байдлын тухай хууль тогтоомжийг хэрэгжүүлэх арга хэмжээ, байгууллагын сүлжээний зураглал /топологи/-ыг тусгаж, гүйцэтгэлд нь хяналт тавих;

7.5.2.байгууллага нь халдлага, зөрчил илэрсэн тохиолдолд авч хэрэгжүүлэх хариу арга хэмжээ авах төлөвлөгөө гаргаж, жилд нэгээс доошгүй удаа төлөвлөгөөний дагуу дадлага хийж тайланг КАБЦК-д хүргүүлэх;

7.5.3.КАБ-ыг хангах чиглэлээр зохион байгуулж байгаа сургалт, судалгаа, шалган баталгаажуулалт, эрсдэлийн үнэлгээний ажилд дэмжлэг үзүүлэх;

7.5.4.КАБ-ыг хангах чиглэлээр хүргүүлсэн заавар, зөвлөмж, шаардлагыг тогтоосон хугацаанд хэрэгжүүлж хариу мэдэгдэх;

7.5.5.эрсдэлийн үнэлгээний үр дүнг үндэслэн эрсдэлийг бууруулахад чиглэсэн арга хэмжээг төлөвлөж, төлөвлөгөөний хэрэгжилтийн тайланг КАБЦК-д хүргүүлэх;

7.5.6.байгууллага нь КАБЦК-ын шалган баталгаажуулсан техник болон программ хангамжийг ашиглах.

Найм. Албан тушаалтны нийтлэг үүрэг, хариуцлага

8.1. Байгууллагын удирдах албан тушаалтан кибер аюулгүй байдлыг хангах чиглэлээр дараах нийтлэг үүрэг хүлээнэ:

8.1.1.кибер аюулгүй байдлыг хангах үйл ажиллагааг зохион байгуулах, байгууллагыг төлөөлөх;

8.1.2.кибер аюулгүй байдлыг хангах бодлого, дүрэм, журмыг мөрдүүлэх;

8.1.3.кибер аюулгүй байдлыг хангах төлөвлөгөө гаргах, хэрэгжүүлэхэд шаардагдах зардлыг байгууллагын жил бүрийн төсөв, төлөвлөгөөнд тусгах.

8.2. Байгууллагын кибер аюулгүй байдал хариуцсан албан тушаалтан дараах нийтлэг үүрэг хүлээнэ.

8.2.1.байгууллагын кибер аюулгүй байдлыг хангах өдөр тутмын үйл ажиллагааг хариуцан гүйцэтгэх;

8.2.2.холбогдох дүрэм, журмыг шинэчлэх санал боловсруулах;

8.2.3.кибер аюулгүй байдлыг хангахад шаардлагатай үйл ажиллагаа, нөөцийг төлөвлөх.

8.3. Байгууллагын нийт алба хаагч кибер аюулгүй байдлыг хангах чиглэлээр дараах нийтлэг үүрэг хүлээнэ:

8.3.1.энэ журам болон кибер аюулгүй байдлын тухай хууль, кибер аюулгүй байдлыг хангахтай холбоотой бусад дүрэм, журмыг дагаж мөрдөх;

8.3.2.илэрсэн халдлага, зөрчил, сэжигтэй тохиолдол бүрийг КАБ хариуцсан албан тушаалтанд тухай бүрд нь шуухай мэдэгдэх;

8.3.3.байгууллагын мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээг зөвхөн албан хэрэгцээнд, заасан журам, зааврын дагуу хэрэглэх;

8.3.4.байгууллагаас зохион байгуулж байгаа кибер аюулгүй байдлын мэдлэг олгох сургалтад хамрагдах;

8.3.5.компьютерт техникийн болон программ хангамжийн алдаа гарсан, цахим мэдээлэлд хандах боломжгүй болсон тохиолдолд КАБ хариуцсан албан тушаалтанд нэн даруй мэдэгдэх.

8.4. Энэ журмыг зөрчсөн албан тушаалтанд холбогдох хууль тогтоомжийн дагуу хариуцлага ногдуулна.

---oOo---