

ОНЦГОЙ БАЙДЛЫН БАЙГУУЛЛАГЫН МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫГ ХАНГАЖ БУЙ УДИРДЛАГА ЗОХИОН БАЙГУУЛАЛТ, ӨНӨӨГИЙН БАЙДАЛ, ТУЛГАМДАЖ БУЙ АСУУДАЛ

Ж.Энхтөр
ДХИС-ийн Удирдлагын академийн
магистрант, ахмад

Товч агуулга: Энэхүү өгүүллэгээр Онцгой байдлын байгууллагын мэдээллийн аюулгүй байдлын өнөөгийн байдлыг судалж, дүн шинжилгээ хийж, тулгамдаж буй асуудлыг тодорхойлж, цаашид сайжруулах арга замыг санал болгоно. Мөн Онцгой байдлын байгууллагын мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааны эрх зүйн зохицуулалт, удирдлага зохион байгуулалт, мэдээллийн аюулгүй байдлыг хангах албаны зохион байгуулалт тогтолцоог бусад хууль сахиулах байгууллагуудтай харьцуулан судалсан.

Түлхүүр үг. Мэдээллийн аюулгүй байдал, мэдээллийн технологи, Онцгой байдлын алба, эрх зүйн орчин,

Оршил

Онцгой байдлын байгууллагын үйл ажиллагаа өргөжихийн хэрээр байгууллагын хэмжээнд мэдээллийн технологийн шинэ системүүд нэвтэрч, түүнийг дагаад сүлжээний бүтэц зохион байгуулалтыг өргөтгөх, мэдээллийн аюулгүй байдлыг хангах, тоног төхөөрөмжийг шинээр суурилуулах, хэвийн ажиллагааг хангах зэрэг ажил зохион байгуулагдаж байна. Мөн төрийн цэргийн болон тусгайлсан чиг үүрэг бүхий байгууллагуудтай тайван цагийн болон гамшгийн үеийн харилцан ажиллагаа, удирдлагын нэгдсэн холбоог хангахад манай байгууллагын холбоо, мэдээллийн чиглэлийн бүтэц, бүрэлдэхүүний тоо харьцангуй цөөн бөгөөд төв, орон нутгийн онцгой байдлын байгууллагын холбоо, зарлан мэдээлэл хариуцсан нэг мэргэжилтний ажлын ачаалал нэмэгдэн ажиллах хүн олдохгүй, албан тушаалаа өөрчлөх, ажлаас гарах зэрэг хүндрэл бэрхшээл гарч байна.

Онцгой байдлын байгууллагын алба хаагчдын мэдээллийн аюулгүй байдлын талаарх мэдлэг хомс, өөрийн болон байгууллагын мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааг хангах хэрэгцээ шаардлага байсаар байна.

Онцгой байдлын байгууллагын Мэдээллийн аюулгүй байдлыг хангаж буй өнөөгийн байдал.

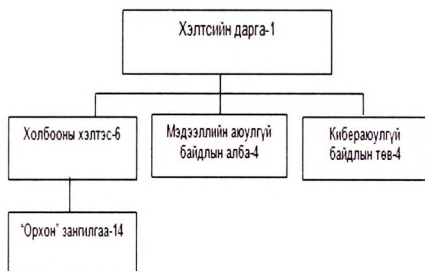
Онцгой байдлын байгууллагт мэдээллийн аюулгүй байдлыг хангахаар ажиллаж байгаа нийт алба хаагчдын 60 хувь нь мэдээллийн технологи, 40 хувь нь радио холбооны инженер мэргэжилтэй ба 19 хувь нь Үндэсний батлан хамгаалахын их сургууль, 31 хувь нь Шинжлэх ухаан технологийн их сургууль, үлдсэн 50 хувь нь мэдээллийн технологийн чиглэлийн бусад сургуулийг төгсчээ.

Онцгой байдлын ерөнхий газрын Холбоо, мэдээллийн технологийн хэлтсийн алба хаагчид нь албаны хэмжээнд холбоо, зарлан мэдээллийн техник хэрэгсэл, тоног төхөөрөмжид засвар үйлчилгээ хийхээс эхлэн энэ чиглэлийн төлөвлөлт, нэггэлийг хөгжүүлэх, мэдээллийн аюулгүй байдлыг хангах, эрх зүйн

баримт бичиг боловсруулах хүртэл өргөн цар хүрээнд ажил үүргээ гүйцэтгэхэд ажлын ачаалал их байна.¹⁸⁰

Төрийн цэргийн болон тусгайлсан чиг үүрэг бүхий байгууллагуудын холбоо, мэдээллийн технологи хариуцсан нэгжийн бүтэц, орон тоог харьцуулан судлахад 22 болон түүнээс дээш алба хаагчтай, 2-4 нэгж, тасаг, хэлтэстэйгээр үйл ажиллагаагаа явуулж байна.

1) ЗЭВСЭГТ ХҮЧНИЙ ЖАНЖИН ШТАБ
УДИРДЛАГА, ХОЛБОО, МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ХЭЛТЭС
/ОФИЦЕР-25, АХЛАГЧ-4, НИЙТ 29/



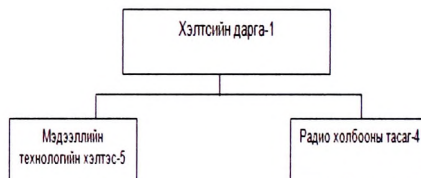
2) ХИЛ ХАМГААЛАХ ЕРӨНХИЙ ГАЗРЫН
ХОЛБОО МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН ХЭЛТЭС
/НИЙТ 9 ОФИЦЕР-9/



3) ЦАГДААГИЙН ЕРӨНХИЙ ГАЗРЫН
МЭДЭЭЛЛИЙН ТЕХНОЛОГИ, ХОЛБООНЫ ТӨВ
/НИЙТ 39 ОФИЦЕР-39/



4) ШҮҮХИЙН ШИЙДВЭР ГҮЙЦЭТГЭХ ЕРӨНХИЙ ГАЗАР
ХОЛБОО, МЭДЭЭЛЛИЙН ТЕХНОЛОГИЙН ХЭЛТЭС
/НИЙТ 10 ОФИЦЕР-10/



“Кибер аюулгүй байдлын тухай хууль”-д төрийн байгууллагуудад кибер аюулгүй байдлыг хангах бүтэц, зохион байгуулалттай байна гэж заасан.

Цаашид “Кибер аюулгүй байдлын тухай хууль”-ийг хэрэгжүүлэх ижил төстэй байгууллагуудын холбоо, мэдээллийн технологийн чиглэлийн бүтэц, орон тоотой уялдуулж, бүтэц, орон тоог нэмэгдүүлэх зайлшгүй шаардлага гарч байна.

Онцгой байдлын ерөнхий газрын Холбоо, зарлан мэдээллийн хэлтсийн зорилго нь Онцгой байдлын байгууллагын холбоо, зарлан мэдээллийн системийн байнгын бэлэн байдлыг хангах арга хэмжээг хэрэгжүүлэхэд мэргэшил-арга зүйн удирдлагаар хангахад оршино.

Онцгой байдлын байгууллагын холбоо, зарлан мэдээллийн системийн төлөвлөлт, нэгтгэлийг хөгжүүлэх, мэдээллийн аюулгүй байдлыг хангах, бодлогын удирдамжаар хангах үндсэн үүрэгтэй.

Нийт 8 журам, 2 заавар боловсруулан мөрдөж байна.

¹⁸⁰ ОБЕГ-ын Холбоо зарлан мэдээллийн хэлтэс.

Цаашид боловсруулах шаардлагатай журам. заавар. стандарт:

1. Онцгой байдлын байгууллагад харилцаа холбоо, мэдээллийн технологийн чиглэлээр баримтлах бодлого
2. Мэдээллийн аюулгүй байдлын зохистой хэрэглээний журам
3. Засвар үйлчилгээний журам
4. Онцгой байдлын байгууллагын холбоо зохион байгуулах заавар
5. Мэдээ, мэдээлэл хүлээн авах, дамжуулах заавар
6. Техник хэрэгсэл, тоног төхөөрөмжийн ашиглалтын заавар
7. Тоон гарын үсэг ашиглах заавар
8. Бүх нийтийн зарлан мэдээлэл дамжуулах стандарт
9. Дотоод зарлан мэдээллийн системийн техникийн шаардлага, стандарт

Холбоо, зарлан мэдээллийн системийн өнөөгийн байдал

Онцгой байдлын албанд ашиглагдаж байгаа холбоо, зарлан мэдээллийн систем, программ болон техник хангамж.

Холбоо, зарлан мэдээллийн зарим техник хэрэгсэл, тоног төхөөрөмжүүд технологийн хувьд хуучирсан, дахин үйлдвэрлэхгүй болж сэлбэг хэрэгсэл олдохгүй болсон зэрэг хүндрэл учирдаг. Тухайлбал, өргөн нэвтрүүлгийн EBS төхөөрөмжийн цахилгаан цэнэг баригч, дуут дохиоллын цамхгийн цахилгаан цэнэг хураагуурын ашиглалтын хугацаа дууссан тул цахилгаан тасарсан үед зарлан мэдээлэл хүргэх боломжгүй болсон байна.

Онцгой байдлын албаны хэмжээнд холбоо, зарлан мэдээллийн техник хэрэгсэл, тоног төхөөрөмжийн нөхөн хангалт, үзлэг, засвар үйлчилгээ, урсгал зардлыг жил бүрийн төсөвт тусгаж хэрэгжүүлэх нь системийн найдвартай ажиллагаа, техник хэрэгслийн насжилт, хэрэглээг уртасгах ач холбогдолтой юм.

Онцгой байдлын байгууллагын цахим мэдээллийн аюулгүй байдлыг хангаж буй эрх зүйн зохицуулалт.

Онцгой байдлын ерөнхий газрын даргын 2020 оны 10 сарын 26-ны өдрийн А/233 тоот тушаалаар батлагдсан “Онцгой байдлын байгууллагын цахим мэдээллийн аюулгүй байдлыг хангах журам”¹⁸¹ нь батлагдсан бөгөөд Энэхүү журам нь Онцгой байдлын байгууллагын цахим мэдээллийн сан, мэдээлэл, түүнийг дэмжих дэд бүтцийн цахим аюулгүй байдлыг хангахтай холбогдсон харилцааг зохицуулдаг.

Онцгой байдлын байгууллагын мэдээллийн аюулгүй байдлын удирдлага, хяналтын тогтолцоог бүрдүүлэх, мэдээллийн аюулгүй байдал, нууцлал, хүртээмжтэй байдлыг дээшлүүлэх, мэдээллийн сүлжээ, системийн найдвартай ажиллагааг хангах, цахим аюул, заналаас урьдчилан сэргийлэх, эрсдэлийг бууруулах, нэн дариу хариу арга хэмжээ авах нь интернэтийн зохистой хэрэглээг бий болгоход энэхүү журмыг дагаж мөрдөнө.

Мэдээллийн аюулгүй байдлыг хангахтай холбоотой эрх зүйн баримт бичиг, арга хэрэгсэл, технологи өөрчлөгдсөн тохиолдолд энэхүү журамд өөрчлөлт оруулж болно.

Энэхүү журам нь Онцгой байдлын байгууллагын мэдээллийн аюулгүй

¹⁸¹Онцгой байдлын байгууллагын мэдээллийн аюулгүй байдлыг хангах журам., 2020., УБ

байдлыг хангах бодлогын нэг хэсэг байна.

Мэдээллийн аюулгүй байдлыг хангах удирдлага, зохион байгуулалт:

Албаны суурин болон зөөврийн компьютерийн нууцлал, аюулгүй байдлыг хангахад дараах арга хэмжээг авч хэрэгжүүлнэ. Үүнд:

Төрийн болон албаны нууцад хамаарах мэдээ, мэдээлэл боловсруулах, хадгалах, хамгаалах зөөврийн болон суурин компьютерийг интернэт сүлжээнд холбохгүй, зөвшөөрөгдсөнөөс бусад эх үүсвэр, оролтуудыг хааж, хатуу диск, компьютерийн гадна хэсэгт лац, тэмдэг тэмдэглэгээ, зориулалтын хамгаалалтыг хийсэн байна.

Ажлын шаардлагаар албаны компьютерийг байгууллагаас гадагш гаргах тохиолдолд Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжээс зөвшөөрөл авах ба нэвтрэх эрх бүхий хамгаалагдсан программ хангамж ашиглан, мэдээлэлд нууцлал хийнэ.

Алба хаагч нь компьютер, бусад техник хэрэгсэл алдагдсан бол системийн зохицуулагч, эд хөрөнгө хариуцсан мэргэжилтэнд яаралтай мэдэгдэнэ. Энэхүү мэдээллийг авснаар хэрэглэгчийн дотоод системд нэвтрэх эрхийг цуцална.

Онцгой байдлын байгууллагын мэдээллийн сан, халдлага илрүүлэх, урьдчилан сэргийлэх хяналтын систем, бусад сервер, хэрэглэгчийн компьютерт албан ёсны эрхтэй үйлдлийн систем, хорт кодын эсрэг, хэрэглээний программ хангамжийг худалдан авах, ашиглах хугацааг сунгах зардлыг жил бүрийн төсөвт тусгана.

Программ хангамж нь нийтэд хүлээн зөвшөөрөгдсөн, холбогдох стандартын шаардлагыг хангасан байх ба албан хэрэглээний программ хангамжийн эх код, технологийн шийдэл, гарал үүсэл нь нууц байна.

Сүлжээний хяналт, зохион байгуулалтад дараах ерөнхий шаардлага тавигдана. Үүнд:

Онцгой байдлын байгууллагын сүлжээний нэгдсэн топологи зурагтай байна.

Аймаг, нийслэлийн Онцгой байдлын байгууллага, түүний салбар, нэгжид харилцаа холбооны үйлчилгээ үзүүлэгч байгууллагатай холбогдож буй шугамын төгсгөл, байгууллагын сүлжээний оролт дээр сүлжээний чиглүүлэгч суурилуулж тохируулсан байна.

Онцгой байдлын байгууллагын сүлжээг гуравдагч талтай холбоход хамтран ажиллах гэрээг Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгж байгуулна.

Онцгой байдлын байгууллагын мэдээллийн сүлжээг Монгол Улсын Засгийн газрын 2012 оны 5 дугаар тогтоолын дагуу зохион байгуулна.

Удирдлага, хяналтын систем, цахим шуудангийн зохион байгуулалтыг хангахад дараах арга хэмжээг авч хэрэгжүүлнэ. Үүнд:

Байгууллагын мэдээллийн системийн тасралтгүй үйл ажиллагааг хангах, мэдээллийн нууцлал, аюулгүй байдлыг дээшлүүлэх зорилгоор компьютер тус бүрийн тохиргоог төвлөрүүлэн зохион байгуулна.

Албаны компьютер нь байгууллагын мэдээллийн нэгдсэн системд нийцсэн Windows үйлдлийн системтэй байх бөгөөд системийн зохицуулагч нь удирдлага,

хяналтын систем ашиглан нэгдсэн удирдлагад оруулна.

Системийн зохицуулагч нь хэрэглэгчийн ажил үүргээс хамааруулан “тусгай”, “онцгой”, “энгийн” гэсэн ангиллаар удирдлага, хяналтын системд домэйнд хандах эрхийн хязгаарлалтыг үүсгэнэ.

Байгууллагын хэмжээнд компьютер ашиглаж буй хэрэглэгч бүр Нэр@nema.gov.mn, Нэр@gmail.com домэйн нэр бүхий албаны цахим шуудангийн хаягтай байна.

Алба хаагч цахим шуудангийн хаяг үүсгэх, устгах, тохиргоо хийх, багтаамжийг нэмэгдүүлэх асуудлыг системийн зохицуулагчид цахим шуудангаар хандан шийдвэрлүүлнэ.

Дараах тохиолдолд мэдээллийн системд хандах эрхийг цуцална.

Үүнд:

Ажлаас чөлөөлөгдсөн;

Урт хугацааны чөлөө авсан;

Жирэмсний амралттай;

Мэдээллийн системд нэвтрэх эрх шаардлагагүй болсон;

Хэрэглэгч өөр ажил, албан тушаалд шилжин томилогдсон;

Хууль, хяналтын байгууллагаас ажиллах эрхийг нь түдгэлзүүлсэн;

Мэдээллийн систем, мэдээллийн санд нэвтрэх эрх бүхий хэрэглэгч мэдээллийн аюулгүй байдлын журмыг зөрчсөн.

Дээрх тохиолдол бүрд байгууллагын хүний нөөцийн мэргэжилтэн нь системийн зохицуулагчид нэн даруй мэдэгдэнэ.

Цахим мэдээллийн санг зохион байгуулахад дараах арга хэмжээг авч хэрэгжүүлнэ. Үүнд:

Их багтаамж бүхий файлыг түргэн шуурхай солилцох зорилгоор дотоод сүлжээнд үүсгэсэн цахим мэдээллийн санг ашиглах ба аймаг, нийслэлийн Онцгой байдлын байгууллага нууцлал, хамгаалалтын шаардлага хангасан төвлөрсөн мэдээллийн сан үүсгэх зориулалтын төхөөрөмжтэй байна.

Мэдээллийн санд хандах хэрэглэгчдийг ажил үүргийн байдлаас хамааруулан системийн зохицуулагчийн, хяналтын, хэрэглэгчийн гэсэн бүлэгт ангилан нэвтрэх эрхийг тогтооно.

Нууцтай танилцах эрх бүхий албан тушаалтан нь тогтоосон эрхийн дагуу төрийн болон албаны нууцад хамаарах мэдээллийн санд ажлын цагаар нэвтэрнэ.

Ажлын байранд шилжилт хөдөлгөөн хийгдсэн тохиолдолд холбогдох баримт, бичгийн цахим хэлбэрийг ажил хүлээлцэх комисст өгч, хүлээлцсэн акт үйлдэж баталгаажуулна.

Төрийн болон албаны нууцад хамаарах мэдээлэлтэй танилцах, түүнийг агуулсан, тээсэн компьютер, техник хэрэгслийг засварлахад нууцын эрхлэгч нь нууцын баталгааг гаргуулж, системийн зохицуулагч нь хяналт тавьж ажиллана.

Системийн зохицуулагч нь цахим мэдээллийн сан устсан тохиолдолд шалтгаан нөхцөлийг тодорхойлох, нөөц архивлалтыг ашиглан мэдээллийн санг сэргээх ба засварлах боломжгүй тохиолдолд системийг нөөц серверт түр хугацаанд үүсгэн хэвийн ажиллагааг хангана.

Сервер компьютерийн нууцлал аюулгүй байдлыг хангахад дараах арга хэмжээг авч хэрэгжүүлнэ. Үүнд:

Системийн зохицуулагч шилжин томилогдох үед сервер компьютерийн тохиргоо, дүрэм, нууц үг, бусад зааврыг Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжийн даргад бичгээр хүлээлгэн өгнө.

Мэдээллийн санг зориулалтын сервер компьютерт үүсгэн, байгууллагын үйл ажиллагаатай холбоотой цахим мэдээллийг байршуулан улирал тутамд шинэчилж, “бүртгэл хөтлөлтийг системийн зохицуулагч, аюулгүй байдлыг хангахыг зохион байгуулалтын бүтцийн нэгж тус бүр хариуцна.

Серверийн өрөөнд нэвтрэх эрх бүхий албан тушаалтны жагсаалтыг Гамшгийн шуурхай удирдлагын асуудал хариуцсан зохион байгуулалтын бүтцийн нэгжийн дарга баталгаажуулна.

Гамшгийн шуурхай удирдлага, зарлан мэдээллийн төвийн техникийн бэлэн байдал хариуцсан инженер эрх бүхий албан тушаалтныг серверийн өрөөнд нэвтрүүлэн бүртгэл хөтөлнө.

Мэдээллийн аюулгүй байдлыг хангахад тоног төхөөрөмж, сүлжээ, программ хангамжийн ашиглалт

Албаны суурин болон зөөврийн компьютерийг ашиглахдаа дараах зүйлсийг анхаарна. Үүнд:

Компьютерт файлыг “С”-ээс бусад дискэнд, шаардлагатай тохиолдолд зөвшөөрөгдсөн нөөц санд хадгална.

Хэрэглэгчийн буруутай үйлдлээс албаны компьютерт гарсан системийн болон техникийн эвдрэл, гэмтлийг тухайн хэрэглэгч өөрөө хариуцан засварлана.

Хэрэглэгч албаны зөөврийн компьютерийг Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжийн зөвшөөрлөөр ашиглана.

Алба хаагч гадаад томилолтоор ажиллахдаа албаны зөөврийн компьютерийг ашигласан бол холбогдох файлыг хуулбарлан авч, тухайн компьютероос устгана.

Хорт кодын эсрэг болон бусад программ хангамжийг ашиглахдаа дараах зүйлсийг анхаарна. Үүнд:

Хэрэглэгч өөрийн компьютерийн хорт кодын эсрэг программ хангамжийг тогтмол хугацаанд уншуулан, хорт код илэрсэн тохиолдолд устгах арга хэмжээг авч, холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгжид мэдэгдэнэ.

Программ, техник хангамжийн туршилтыг Холбоо, техник, цахим мэдээллийн аюулгүй байдал хариуцсан бүтцийн нэгж хийх бөгөөд энэ хугацаанд хорт кодыг дамжуулж болзошгүй хэрэглээний программ хангамжийг ажиллуулж болохгүй.

MNS ISO/IEC 17799 (Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо-шаардлага) стандартад заасны дагуу мэдээллийн системд хууль бусаар нэвтрэх, өөрчлөх эрсдэлийг бууруулахын тулд программ хангамж хөгжүүлэх, турших, түүнд ашиглагдах техник хэрэгсэл, тоног төхөөрөмжийг үндсэн сүлжээнээс тусгаарлана.

Дүрст хурал зохион байгуулахад нууцлал, аюулгүй байдлын шаардлага хангасан албан ёсны эрх бүхий программ хангамж ашиглана.

Интернэт болон дотоод сүлжээг ашиглахдаа дараах арга хэмжээг авч

хэрэгжүүлнэ. Үүнд:

Байгууллагын дотоод сүлжээнд зөвхөн албаны компьютерийг холбох бөгөөд тэдгээрийг физик /MAC/ хаягаар бүртгэнэ.

Нэгдсэн сүлжээг нууцлалын алгоритм, түлхүүр ашиглан зохион байгуулж, сүлжээний хамгаалалт, чиглүүлэгч төхөөрөмжийн тохиргоог хагас жил тутамд шалган бүртгэл хөтөлнө.

Байгууллагын хэмжээнд интернэт сүлжээг дотоод сүлжээнээс тусгаарлаж, нийгмийн сүлжээ болон зүй зохисгүй сайт, холбоосууд (Facebook, Twitter, Wechat, Instagram, Hi5, Youtube, Restricted site гэх мэт)-ыг нэгдсэн удирдлагаар тохируулж хязгаарлана гэж эрх зүйн зохицуулалтуудыг тусгасан байна.

Аймаг, нийслэлийн Онцгой байдлын байгууллагын гамшгаас урьдчилан сэргийлэх асуудал хариуцсан алба хаагчийн компьютерт нийгмийн сүлжээний албан ёсны нэг хаяг бүхий сайтыг ашиглах эрхийг Гамшгийн шуурхай удирдлагын асуудал хариуцсан зохион байгуулалтын бүтцийн нэгжийн даргын зөвшөөрлөөр нээнэ.

Интернэт сүлжээнд төрийн болон албаны нууцад хамаарах мэдээлэл, удирдлагын байранд авахуулсан албаны дүрэмт хувцастай фото зураг, дүрс бичлэгийг байршуулах, цахим шуудангаар бусдад илгээх, интернэт орчны "cloud storage"-д хадгалж болохгүй.

Албан хэрэгцээнд шаардлагагүй веб сайтуудад хандах, их хэмжээтэй файл болон баталгаагүй, сэжигтэй эх сурвалжаас файл татах, байгууллагын сүлжээг ашиглан зүй зохисгүй сэтгэгдэл үлдээж болохгүй.

Компьютерт Dial-up, DSL, модем, гар утас холбох, сүлжээнд утсан болон утасгүй сүлжээний төхөөрөмжийг системийн зохицуулагчийн зөвшөөрлөөр залгаж болно.

Утасгүй сүлжээг зөвхөн утсан сүлжээ татах боломжгүй, алслагдсан газарт ашиглах зайлшгүй нөхцөлд зохион байгуулна.

Дүгнэлт

Онцгой байдлын байгууллагын хэмжээнд холбоо, зарлан мэдээллийн техник хэрэгсэл, тоног төхөөрөмжид засвар үйлчилгээ хийхээс эхлүүлээд энэ чиглэлийн төлөвлөлт, нэгтгэлийг хөгжүүлэх, мэдээллийн аюулгүй байдлыг хангах, эрх зүйн баримт бичиг боловсруулах хүртэл өргөн цар хүрээнд ажил үүргээ гүйцэтгэхэд Холбоо, зарлан мэдээллийн хэлтсийн албан хаагчдын ажлын ачаалал их байна.

Үндэсний аюулгүй байдлыг хангах тусгайлсан чиг үүрэг бүхий байгууллагуудын холбоо, мэдээлэл хариуцсан нэгжийн бүтэц, орон тоог харьцуулан судлахад 9 болон түүнээс дээш алба хаагчтай, 2-4 нэгж, тасаг, хэлтэстэйгээр үйл ажиллагаагаа явуулдаг байна.

Онцгой байдлын байгууллагын холбоо, зарлан мэдээллийн системийг улам бүр өргөтгөн сайжруулахын зэрэгцээ үзлэг, засвар үйлчилгээ нь системийн бэлэн байдлыг хангахад нэн чухал тул энэ чиглэлийн алба хаагчдын ажлын ачаалал, тоног төхөөрөмж, сэлбэг хэрэгслийн нөөц бүрдүүлэлт зэрэг асуудалд анхаарал хандуулах шаардлагатай байна. Өдөр тутмын засвар, үйлчилгээний

ажил их байдаг тул цаашид Онцгой байдлын байгууллагад шинэ техник технологи судалж нэвтрүүлэхэд Холбоо, зарлан мэдээллийн хэлтсийн орон тоо цөөн байна.

Санал:

Онцгой байдлын ерөнхий газрын Гамшгийн шуурхай удирдлагын газрын Холбоо, мэдээллийн технологийн хэлтэст Системийн төлөвлөлт, техник хангамж хариуцсан ахлах мэргэжилтэн, Сервер, системийн эрсдэл хариуцсан мэргэжилтэн, Удирдлага, хяналтын систем хариуцсан мэргэжилтний албан тушаалыгшинээр бий болгож орон тоог нэмэгдүүлэх,

Аймгийн Онцгой байдлын газрын харъяа салбар, нэгжийн зориулалт, бие бүрэлдэхүүний тоо, байршил зэргийг харгалзан Холбоо, зарлан мэдээлэл хариуцсан мэргэжилтний орон тоог нэмэгдүүлэх.

Эх сурвалжийн жагсаалт

- Онцгой байдлын байгууллагын мэдээллийн аюулгүй байдлыг хангах журам
- Т.Халтар Мэдээллийн аюулгүй байдлын гарын авлага. ШУТИС-ийн хэвлэх үйлдвэр. УБ. 2006 он,
 - Nema.gov.mn
 - Кибер аюулгүй байдлын тухай хууль
 - www.google.mn