Гадаадын иргэн, харьяатын газрын даргын
2025 оны 04 дугаар сарын 07-ны өдрийн
А/116/8 дугаар тушаалын хавсралт

КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ ЖУРАМ

Нэг. Нийтлэг үндэслэл

1.1.Энэ журмын зорилго нь Гадаадын иргэн, харьяатын газар (цаашид “Байгууллага” гэх)-ын мэдээллийн систем, кибер халдлага, кибер аюулгүй байдлын зөрчлийг илрүүлж, сүлжээний аюулгүй байдлыг хангах, хариу арга хэмжээ авах, урьдчилан сэргийлэх, нөхөн сэргээх болон тэдгээртэй холбоотой бусад үйл ажиллагаанд дагаж мөрдөх харилцааг зохицуулахад оршино.

1.2.Байгууллагын газрын төв болон хилийн боомт, орон нутаг дахь газар, хэлтэс (цаашид “Төв, орон нутаг дахь нэгж” гэх)-ийн албан хаагчид болон туршилтын хугацаа, дадлагаар, ажил гүйцэтгэх гэрээгээр ажиллаж буй аж ахуйн нэгж, иргэн нь (цаашид “Албан хаагч” гэх) энэхүү журмыг үйл ажиллагаандаа мөрдөж, цахим мэдээллийн нууцлалыг хамгаална.

1.3.Энэхүү журамд хэрэглэсэн дараах нэр томьёог дор дурдсан утгаар ойлгоно.

1.3.1."кибер аюулгүй байдал" гэж кибер орчинд мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдал хангагдсан байхыг;

1.3.2."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;

1.3.3.”кибер орчин" гэж мэдээлэлд хандах, нэвтрэх, цуглуулах, түүнийг боловсруулах, хадгалах, ашиглах боломж олгож байгаа мэдээллийн систем, мэдээллийн сүлжээний орчныг;

1.3.4."бүрэн бүтэн байдал" гэж мэдээллийг зөвшөөрөлгүй устгах, өөрчлөхөөс хамгаалсан байхыг;

1.3.5."нууцлагдсан байдал" гэж мэдээлэлд зөвшөөрөлгүй хандах, нэвтрэх боломжгүй байхыг;

1.3.6."хүртээмжтэй байдал" гэж зөвшөөрөгдсөн хүрээнд мэдээлэлд хандах, нэвтрэх, цуглуулах, ашиглах боломжтой байхыг;

1.3.7."мэдээллийн систем" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.1-д заасны дагуу мэдээ мэдээллийг боловсруулах, түүний алдааг хянах, найдвартай хадгалах, шаардлагатай мэдээллийг цаг тухайд нь түргэн шуурхай, төрөл бүрийн (дуу авиа, цаасан, хальсан, эд зүйлс, цахилгаан соронзон) байдлаар гаргах, тэдгээрт ашиглагдах техник болон программ хангамжийн бүрдлийг;

1.3.8."мэдээллийн сүлжээ" гэж Нийтийн мэдээллийн ил тод байдлын тухай хуулийн 4.1.2-т заасны дагуу хоёр, түүнээс дээш хэрэглэгчийн хооронд

мэдээлэл илгээх, дамжуулах, хүлээн авах программ хангамж болон техник хэрэгслийн иж бүрдлийг;

1.3.9."кибер аюулгүй байдлын эрсдэлийн үнэлгээ" гэж цахим мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдал алдагдах, аюул занал тохиолдох магадлал, эмзэг байдлын түвшин, түүнээс үүсэх үр дагавар, эрсдэлийг бууруулах, урьдчилан сэргийлэх арга хэмжээг тодорхойлох мэргэшсэн үйл ажиллагааг;

1.3.10."мэдээллийн аюулгүй байдлын аудит" гэж кибер аюулгүй байдлын хууль тогтоомж, холбогдох журам, стандартад нийцсэн эсэхэд дүгнэлт гаргах, зөвлөмж өгөх хараат бус хөндлөнгийн мэргэжлийн үйл ажиллагааг;

1.3.11."хэрэглэгч" гэж байгууллагын мэдээллийн системтэй харьцдаг бүх шатны алба хаагчийг;

1.3.12."мэдээллийн сан" гэж мэдээллийн нэгдсэн ангилал код, индекс, арга зүй, стандартаар ижилсүүлсэн баримт бичгийг шаардлагын дагуу цуглуулж, боловсруулж хадгалсан мэдээлэл, өгөгдлийн бүрдлийг;

1.3.13."мэдээллийн систем" гэж мэдээ мэдээллийг боловсруулах, түүний алдааг хянах, найдвартай хадгалах, шаардлагатай мэдээллийг цаг тухайд нь түргэн шуурхай, төрөл бүрийн (дуу авиа, цаасан, хальсан, эд зүйлс, цахилгаан соронзон) байдлаар гаргах, тэдгээрт ашиглагдах техник болон программ хангамжийн бүрдлийг;

1.3.14."дэд бүтэц" гэж мэдээлэл үүсгэх, хүлээн авах, боловсруулах, хадгалах, дамжуулах, үйл ажиллагааг хангаж буй хоорондоо уялдаа холбоо бүхий холболтын систем, техник хэрэгсэл, тоног төхөөрөмжийн бүрдлийг;

1.3.15."хамгаалалтын төхөөрөмж" гэж мэдээллийн нууцлал хамгаалалтыг сүлжээний түвшинд зохицуулах хэрэгсэл, тоног төхөөрөмжийг;

1.3.16."сүлжээний чиглүүлэгч" гэж байгууллага хоорондын сүлжээг чиглүүлэх, удирдах зориулалтын программ болон техник хангамжийг;

1.3.17."VPN (Virtual Private Network)" гэж нууцлалын алгоритм болон түлхүүрээр үүсгэсэн, мэдээллийг нууцлан дамжуулах сувгийг;

1.3.18."утасгүй сүлжээ" гэж долгионы тархалт ашиглан ойрын зайд мэдээлэл дамжуулах утасгүй холболтын сүлжээг;

1.3.19."нэгдсэн сүлжээ" гэж анги, байгууллага хооронд мэдээлэл солилцох үйл явцыг шуурхай болгох, интернэтийн зохистой хэрэглээг бий болгох зорилгоор үүсгэсэн мэдээллийн аюулгүй байдал хангагдсан нэгдсэн дэд бүтцийг;

1.3.20."хорт код" гэж мэдээлэл устгах, хулгайлах, хуулах, өөрчлөх, эвдэх гэх мэт хорлон сүйтгэх зориулалттай программыг;

1.3.21."зөөврийн мэдээлэл тээгч" гэж флаш диск, зөөврийн хатуу диск, компакт диск, зургийн аппарат болон ухаалаг утасны бичил карт гэх мэт зүйлсийг.

Хоёр. Мэдээллийн сан нөөцлөх, хадгалах

2.1.Байгууллагын төв серверийн цахим мэдээллийн сангийн нөөцлөлт, хадгалалтыг мэдээллийн технологийн чиг үүрэг хариуцсан албан хаагч хариуцна.

2.2.Төв серверийн цахим мэдээллийн сангийн нөөцлөлтийг тусгайлсан хадгалах төхөөрөмжид нөөцөлж, энэ талаар бүртгэл хөтөлнө.

2.3.Мэдээллийн сангийн нөөцлөлтийг нэмэлт хадгалах хэрэгсэлд өдөр бүр хадгалдаг байх арга хэмжээг авна.

2.4.Мэдээллийн сангийн нөөц хувийг "Үндэсний дата төв" УТҮГ-т байршуулж болно.

2.5.Мэдээллийн системийг онцгой нөхцөл байдлын үед сэргээн ажиллуулах төлөвлөгөөтэй байна.

2.6.Мэдээллийн сан нь системийн болон техник хангамжийн үйл ажиллагаанаас үүдэн устах, хэвийн ажиллагаанд доголдол гарсан тохиолдолд түүнийг засах арга хэмжээг мэдээллийн технологийн чиг үүрэг хариуцсан албан хаагч яаралтай авч хэрэгжүүлнэ.

2.7.Кибер аюулгүй байдлын чиг үүрэг хариуцсан албан хаагч 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.

Гурав. Мэдээллийн системийн ашиглалт, нууцлал, хамгаалалт

3.1.Төрийн болон албаны нууцын зэрэглэл бүхий цахим мэдээлэлтэй танилцах, харьцах, мэдээллийн системд хандах албан тушаалтан зохих байгууллага, албан тушаалтны зөвшөөрлийг авна.

3.2.Байгууллагын хамгаалвал зохих мэдээлэл, түүний агуулж байгаа мэдээллийн систем, мэдээллийн сүлжээний нууцлын зэрэглэл, мэдээлэл хариуцагчийг тодорхойлсон жагсаалтыг гаргаж тогтмол шинэчлэнэ.

3.3.Байгууллагын дотоод үйл ажиллагаанд ашиглаж байгаа мэдээллийн системд нэвтрэх эрхийг албан тушаалын тодорхойлолт, ажлын чиг үүргийг харгалзан нэгжийн бичгээр ирүүлсэн саналыг үндэслэн тухайн систем хариуцсан мэдээллийн технологийн чиг үүрэг хариуцсан албан хаагч олгоно.

3.4.Мэдээллийн системд нэвтрэх эрхийг эрх олгогдсон эсхүл шаардлагатай албан хаагчид олгоно.

3.5.Мэдээллийн системд хандах эрх бүхий албан тушаалтны мэдээлэлд хандах, өөрчлөлт оруулах, дуусгавар болгох эрхийн түвшнийг нэгжийн бичгээр ирүүлсэн саналыг үндэслэн мэдээллийн технологийн асуудал хариуцсан нэгжийн холбогдох албан хаагч тохируулж өгнө.

3.6.Мэдээллийн системд нэвтрэх эрх бүхий албан хаагч ажлаас түр чөлөөлөгдсөн, халагдсан, шилжин ажилласан бол холбогдох шийдвэрийг үндэслэн нэвтрэх, хандах эрхийг цуцална.

3.7.Байгууллагын мэдээллийн системийн нууцлал хамгаалал, хэвийн үйл ажиллагаа, нэвтрэлт хандалт, өөрчлөлтийн бүртгэлийг (лог файлын) мэдээллийн технологийн асуудал хариуцсан нэгжийн холбогдох албан хаагч удирдан хянана.

3.8.Мэдээллийн системд нэвтрэх эрх (нууц үг, нэвтрэх нэр)-ийг бусдад шилжүүлэх, зөвшөөрөлгүй нэвтрэх, үзэх, мэдээллийг устгах, дамжуулахыг хориглоно.

3.9.Алба хаагч нь мэдээллийн системд нэвтрэх нууц үгийг хялбар тогтоох, бичигдэх өөрт холбогдол бүхий өгөгдлөөр үүсгэхгүй байхаар тохируулж, 8-аас дээш орон бүхий том жижиг үсэг, тэмдэгт хослуулсан нууц үгийг үүсгэн ашиглана.

Дөрөв. Тоног төхөөрөмжийн аюулгүй байдлыг хангах

4.1.Төрийн болон орон нутаг дахь нэгжид цахим мэдээлэл боловсруулах, хадгалах сервер, сторэйж, нууц мэдээлэл агуулсан компьютер, бусад хадгалах төхөөрөмж нь хууль бусаар хандах, нэвтрэх, гэмтэл учруулах, учирч болох эрсдэл (гал, ус, аянга, цахилгаан тэжээл гэх мэт) хөндлөнгөөс оролцох ажиллагаанаас хамгаалагдсан байна.

4.2.Цахим мэдээлэл боловсруулах, хадгалах үүрэг бүхий сервер, хадгалалт, бусад техник хэрэгслийг байрлуулахдаа цахилгаан тэжээлийн тасалдал үүсэх, хэлбэлзэхээс урьдчилан сэргийлж тог тогтворжуулагч, хамгаалалтын тэжээлийн эх үүсвэрийг суурилуулсан, серверийн өрөөний орчин нөхцөлийн шаардлага хангасан байна.

4.3.Албан хэрэгцээнд хэрэглэгдэж байгаа сүлжээний хамгаалалтын тоног төхөөрөмж, сервер, компьютер, мэдээлэл хадгалагч болон тээгч зөөврийн хэрэгслүүдэд вирус, хортой кодын эсрэг албан ёсны эрх бүхий лицензтэй программ хангамжийг ашиглана.

4.4.Хэрэглэгчийн компьютер болон серверт хортой код илэрсэн тохиолдолд дүн шинжилгээ хийж, яаралтай устгах арга хэмжээг кибер аюулгүй байдлын чиг үүрэг хариуцсан алба хаагч авах бөгөөд холбогдох алба хаагч нь өөрийн хариуцсан компьютер, техник хэрэгслийн аюулгүй байдлыг хангах шаардлагатай арга хэмжээг авна.

Тав. Мэдээллийн сүлжээний аюулгүй байдлыг хангах

5.1.Албан хаагчид үйл ажиллагаандаа “Төрийн мэдээллийн нэгдсэн сүлжээ ашиглах журам”, “Тусгай хэрэглээний мэдээлэл, холбооны сүлжээ байгуулах, ашиглах журам”-ыг мөрдлөг болгон ажиллана.

5.2.Байгууллага нь төрийн мэдээллийн нэгдсэн сүлжээний хамгаалалтад холбогдсон интернэт сүлжээг ашиглана.

5.3.Төрийн мэдээллийн нэгдсэн болон тусгай хэрэглээний сүлжээнд холбох, ашиглалтад хяналт тавих, сүлжээний нууцлалын арга хэрэгсэл, технологийг нэвтрүүлэх ажлыг кибер аюулгүй байдлын чиг үүрэг хариуцсан алба хаагч хэрэгжүүлнэ.

5.4.Төрийн болон албаны нууцад хамаарах цахим мэдээллийг төрийн мэдээллийн нэгдсэн болон тусгай хэрэглээний сүлжээгээр дамжуулна.

5.5.Төрийн нууцад хамаарах мэдээллийг цахим хэлбэрээр дамжуулахдаа сүлжээний нууцлалын арга хэрэгсэл, технологийг ашиглана.

5.6.Байгууллагын мэдээллийн нэгдсэн сүлжээ нь албан ёсны лиценз бүхий галт хана, халдлага илрүүлэх, эсэргүүцэх систем буюу нэгдсэн хяналт, удирдлагын системтэй байна.

5.7.Төв болон орон нутаг дахь нэгж сүлжээний бүтцийн зурагтай байх бөгөөд сүлжээний оролт дээр сүлжээний чиглүүлэгч суурилуулж, тохируулсан байна.

5.8.Төв болон орон нутаг дахь нэгж бусад байгууллагатай нэгдсэн сүлжээ үүсгэн сүлжээг гуравдагч талтай холбоход тухайн байгууллагатай хамтран ажиллах гэрээ байгуулж, мэдээллийн аюулгүй байдлыг хангасны үндсэн дээр холболтыг үүсгэнэ.

5.9.Байгууллагын мэдээллийн нэгдсэн сүлжээнд зөвхөн бүртгэлтэй компьютер, техник хэрэгсэл, телекамерыг холбох ба мэдээллийн сүлжээнд холбогдох эрх бүхий төхөөрөмжийн бүртгэлийг мэдээллийн технологийн чиг үүрэг хариуцсан албан хаагч хяналт тавина.

5.10.Байгууллагын дотоод сүлжээнд албан хэрэгцээний зориулалтаас бусад төрлийн албан хэрэгцээний бус техник хэрэгсэл, компьютер, принтерийг холбохыг хориглох ба тэдгээрт динамик хаяглалт олгохгүй, физик хаягаар холбогддог байх, зөвшөөрөлгүй хандалтуудыг хязгаарлах байдлаар сүлжээний төхөөрөмжүүдийг тохируулна.

5.11.Төрийн нууцад хамаарах цахим мэдээлэл агуулсан, тээсэн компьютер, техник хэрэгслийг интернэт сүлжээнд холбохыг хориглоно.

5.12.Мэдээллийн сүлжээний нууцлал хамгаалалт, хэвийн ажиллагааг мэдээллийн технологийн чиг үүрэг хариуцсан албан хаагч хариуцаж, байгууллагын сүлжээнд ямарваа нэгэн алдаа доголдол гарсан тохиолдолд түүнийг засах арга хэмжээг шуурхай авна.

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

6.1.Нууцын зэрэглэл бүхий мэдээлэл боловсруулах программ хангамж, компьютер, техник хэрэгслийг албан хэрэгцээнд ашиглахдаа кибер аюулгүй байдлын чиг үүрэг хариуцсан албан хаагчийн санал, дүгнэлтийг авч, мэдээллийн технологийн чиг үүрэг хариуцсан албан хаагч (маягт №1)-ийн дагуу бүртгэнэ.

6.2.Кибер аюулгүй байдлын чиг үүрэг хариуцсан албан хаагч компьютер, техник хэрэгсэл, программ хангамжийн мэдээллийн аюулгүй байдлын шаардлага хангасан эсэхийг шалгаж, техникийн үндсэн үзүүлэлт, мэдээллийн системийн нийцэл, ажиллах зарчим зэрэгт үндэслэн туршиж, баталгаажуулна.

6.3.Хувийн хэрэгцээний зөөврийн болон гар төхөөрөмж гэх мэт мэдээлэл боловсруулах хэрэгслүүдийг албаны мэдээлэл боловсруулахад ашиглах шаардлага гарсан тохиолдолд мэдээллийн аюулгүй байдал хариуцсан албан хаагчаар хянуулж, зөвшөөрөл авснаар шинэ эмзэг байдал, эрсдэлийг бууруулна.

6.4.Мэдээллийн системийн зохион байгуулалт, программ хангамжийн

хөгжүүлэлт хийж буй байгууллагатай нууцын гэрээ байгуулна.

6.5.Ашиглалтын явцад дараах арга хэмжээг авч хэрэгжүүлнэ.

6.5.1.цахим мэдээлэл боловсруулах компьютер, техник хэрэгсэл ашиглаж байх явцад сэжигтэй үйлдэл (компьютер, системд нэвтрэх, хортой программ суух, доголдох, мэдээлэл алдсан талаар мэдэх) гарвал кибер аюулгүй байдлын чиг үүрэг хариуцсан албан хаагчид яаралтай мэдэгдэнэ.

6.5.2.компьютер, техник хэрэгсэл эзэмшигч нь зөвхөн албан хэрэгцээнд ашиглах бөгөөд кибер аюулгүй байдал алдагдахаас хамгаалах арга хэмжээг авч хэрэгжүүлж, компьютерынхоо дэлгэц амралт (screen saver and lock)-ыг нууц үгтэй хослуулж хэрэглэнэ.

6.5.3.компьютер, техник хэрэгсэл эзэмшигч албан хэрэгцээнээс бусад зориулалтаар ашиглах, зөвшөөрөлгүй хэрэглээний бус техник хангамж, программ хангамж, дуу, тоглоом гэх мэт шаардлагагүй зүйлсийг нэмж суулгахыг хориглоно.

6.5.4.нууц мэдээлэлтэй харьцдаг алба хаагч ашиглаж байгаа цахим мэдээлэл тээгч компьютер, техник хэрэгслийг мэдээллийн технологийн чиг үүрэг хариуцсан албан хаагч (маягт №2) бүртгэж, нууцлал, хамгааллыг хангана.

6.6.Засварлах үйл ажиллагаанд дараах арга хэмжээг авч хэрэгжүүлнэ.

6.6.1.нууцын зэрэглэл бүхий цахим мэдээлэл тээгч компьютер, техник хэрэгсэл (компьютер, зөөврийн төхөөрөмж, бичлэгийн төхөөрөмж)-ийг засварлахдаа тухайн хариуцсан албан хаагчийг байлцуулж, засвар үйлчилгээг гэрээ болон баталгаат хугацааны дагуу хийж байгаа иргэн, хуулийн этгээд болон мэдээллийн технологийн чиг үүрэг хариуцсан албан хаагч, холбогдох албан хаагчаас “цахим мэдээллийн нууцын баталгаа” авсан байна. (маягт №3)

6.6.2.Засвар үйлчилгээг гэрээний дагуу хийж байгаа иргэн, хуулийн этгээд нь тухайн хадгалагдсан цахим мэдээллийн талаар хариуцсан албан хаагчаас мэдээлэл авсны дараа засвар үйлчилгээг хийнэ.

6.6.3.мэдээлэл технологийн чиг үүрэг хариуцсан албан хаагч төрийн болон албаны нууц мэдээлэл агуулсан, тээсэн программ хангамж, техник хангамжид засвар үйлчилгээ хийсэн талаарх бүртгэлийг тухай бүр хөтөлнө. (маягт №4)

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

6.7.1.албан хаагч өөрийн компьютерын хорт кодын эсрэг программ хангамжийг тогтмол хугацаанд уншуулан, хорт код илэрсэн тохиолдолд устгах арга хэмжээг авч, мэдээллийн технологийн асуудал хариуцсан нэгжид мэдэгдэнэ.

6.7.2.ISOMNS:27001 (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, хэрэгслүүдийг үндсэн сүлжээнээс тусгаарлана.

6.8.Интернэт болон дотоод сүлжээг ашиглахдаа дараах арга хэмжээг авч хэрэгжүүлнэ.

6.8.1.байгууллагын дотоод сүлжээнд зөвхөн албаны компьютерыг холбох бөгөөд тэдгээрийг физик (MAC) хаягаар бүртгэнэ.

6.8.2.байгууллагын хэмжээнд интернэт сүлжээг дотоод сүлжээнээс тусгаарлаж, нийгмийн сүлжээ болон зүй зохисгүй сайт, хаягуудыг (Facebook, Twitter, Wechat, Instagram, Hi5, Youtube, Restricted site гэх мэт)-ыг нэгдсэн удирдлагаар тохируулж хязгаарлана.

6.9.Хэрэглэгч цахим шууданг ашиглахдаа дараах зүйлсийг анхаарна.

6.9.1.цахим шуудангийн хаягт нэвтрэх нэр, нууц үгийн нууцлал, аюулгүй байдлыг хариуцна.

6.9.2.суртал ухуулгын шинжтэй, үргэлжилсэн бичвэртэй, хорт код агуулсан мэдээллийг цахим шуудангаар хүлээн авч, илгээхгүй.

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

6.9.4.ажлын шаардлагаар албаны компьютерыг байгууллагаас гадагш гаргах тохиолдолд мэдээллийн технологийн хэлтсээс зөвшөөрөл авах ба нэвтрэх эрх бүхий хамгаалагдсан программ хангамж ашиглан, мэдээлэлд нууцлал хийнэ.

6.9.5.төрийн болон албаны нууцад хамаарах мэдээллийг нууцлалын программ хангамж ашиглан тусгай зориулалтын төхөөрөмжид улирал тутамд хадгалан нууцын өрөөнд байршуулна.

6.10.Нууц үгийг ашиглахдаа дараах зүйлсийг анхаарна.

6.10.1.нууц үг нь том, жижиг үсэг, тоо, тусгай тэмдэгт (a-z,A-Z, 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./;)-ээс бүрдсэн байна.

6.10.2.нууц үгийг хялбар биш, амархан тогтоож болохоор үүсгэх ба сүлжээ, сервер компьютер, мэдээллийн сан, удирдлагын программ хангамжийн нууц үг 12 тэмдэгтээс багагүй, бусад тоног төхөөрөмжид хандах нууц үг 8 тэмдэгтээс багагүй байна.

6.10.3.удирдлагын системийн нууц үгийг 6 сар, хэрэглэгчийн түвшний нууц үгийг 3 сар тутам солино.

6.10.4.удирдлагын системийн нууц үг, хэрэглэгчийн түвшний нууц үгийг сольсон тухай бүр кибер аюулгүй байдлын чиг үүрэг хариуцсан албан хаагчид хадгалуулна.

Долоо. Кибер аюулгүй байдалд бие даасан болон хөндлөнгийн эрсдэлийн үнэлгээ хийх

7.1.Бие даасан болон хөндлөнгийн эрсдэлийн үнэлгээ нь байгууллагын цахим мэдээллийн аюулгүй байдалд учирч болох эмзэг байдлыг тодорхойлж, эрсдэлийг бууруулах, тодорхой түвшинд байлгах үйл явцыг тодорхойлоход чиглэгдэнэ.

7.2.Энэ журмын 3.2-т заасан жагсаалтад дурдсан мэдээлэлд эрсдлийн үнэлгээ

хийхдээ ISO27005 стандартыг баримтална.

7.3.Байгууллага нь кибер аюулгүй байдлыг хангах зорилгоор бие даасан эрсдэлийн үнэлгээг жил тутам хийж, хөндлөнгийн эрсдэлийн үнэлгээг Кибер аюулгүй байдлын тухай хуульд заасан хугацаанд хийлгэнэ.

7.4.Эрсдэлийн үнэлгээний дүнд үнэлэлт дүгнэлт хийж, зөвлөмжийг хэрэгжүүлж ажиллах бөгөөд шаардлагатай гэж үзвэл мэргэшсэн байгууллага, мэргэжилтний дэмжлэг авч болно.

7.5.Бие даасан эрсдэлийн үнэлгээг мэдээллийн технологийн асуудал хариуцсан нэгж хийж, үнэлгээ дүгнэлтээр илэрсэн зөрчил, дутагдлыг засаж сайжруулах арга хэмжээг холбогдох нэгжтэй хамтран хэрэгжүүлнэ.

7.6.Хөндлөнгийн эрсдэлийн үнэлгээг мэргэшсэн эрх бүхий хуулийн этгээд болон төрийн тусгай байгууллагаар дараах чиглэлээр гүйцэтгүүлнэ.

7.6.1.албанд ашиглаж байгаа мэдээллийн технологийн программ, техник хангамжийг шалгаж, баталгаажуулах;

7.6.2.мэдээллийн аюулгүй байдлыг хангах аудит, кибер аюулгүй байдлыг хангах эрсдэлийн үнэлгээг хуульд заасан хугацаанд эрх бүхий байгууллагаар хийлгэж, тайланг кибер халдлага, зөрчилтэй тэмцэх төвд хүргүүлэх;

7.6.3.мэдээллийн систем, сүлжээнд өөрчлөлт орсон, шинээр нэвтрүүлсэн, эрсдэлтэй нөхцөл байдал үүссэн үед эмзэг байдал болон эрсдэлийн үнэлгээ хийх.

7.7.Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээ хийх байгууллага дараах шаардлагыг хангасан байна.

7.7.1.Кибер аюулгүй байдлын тухай хуульд заасны дагуу зөвшөөрөлтэй хуулийн этгээд байх бөгөөд энэхүү журмыг үндэслэн гэрээ байгуулна.

7.7.2.мэдээллийн систем, сүлжээг мэргэжлийн программ хангамж болон олон улсад хүлээн зөвшөөрөгдсөн аргуудыг ашиглан шинжилнэ.

7.8.Эрсдэлийн үнэлгээ хийхэд дараах арга хэмжээг авч хэрэгжүүлнэ.

7.8.1.байгууллагын мэдээллийн аюулгүй байдлын удирдлага, хяналтын хэрэгжилт, сүлжээний дэд бүтэц, мэдээллийн сангийн бүрэн бүтэн, халдашгүй нууцлагдсан болон хүртээмжтэй байдлыг баталгаажуулах;

7.8.2.мэдээллийн аюулгүй байдлын зөрчил гарч болзошгүй эмзэг байдлыг тодорхойлох;

7.8.3.байгууллагын цахим мэдээллийн дэд бүтцийн зохион байгуулалт мэдээллийн аюулгүй байдлын бодлоготой нийцэж буй эсэхийг тогтоох;

7.8.4.гадны халдлага нэвтрэн орох цоорхой байгаа эсэхийг тодорхойлох;

7.8.5.хэрэглэгч болон мэдээллийн системийн үйл ажиллагааг шалгах.

7.9.Эрсдэлийн үнэлгээ хийх байгууллагад мэдээллийн орчинд хандах дараах эрхийг системийн зохицуулагчийн хяналтан дор олгоно.

7.9.1.хэрэглэгчийн болон үйлдлийн системийн түвшний хандалтын эрх;

7.9.2.байгууллагын цахим мэдээллийн санд хандах эрх;

7.9.3.ажлын талбарт хандах эрх (серверийн өрөө, албаны өрөөнүүд г.м);

7.9.4.шаардлагатай лог (бүртгэл)-ийн файлуудад хандах эрх.

7.10.Мэдээллийн аюулгүй байдлын эрсдэлийн үнэлгээнд үндэслэн эрсдэлийг бууруулах арга хэмжээнд зарцуулах хөрөнгийг жил бүр төсөвт тусгана.

Найм. Кибер аюулгүй байдлыг хангах зохион байгуулалт, албан тушаалтын үүрэг

8.1. Засгийн газрын 2023 оны 224 тогтоолоор баталсан кибер аюулгүй байдлыг хангах нийтлэг журмын 2.1, 2.2-т заасан арга хэмжээг авч хэрэгжүүлнэ.

8.2 Орон нутаг дахь нэгжийн дарга, аймаг дахь төлөөлөл дараах үүрэгтэй.

8.2.1.үндсэн чиг үүргийн хүрээнд Кибер аюулгүй байдлын тухай хууль тогтоомжийн хэрэгжилтийг удирдлага, зохион байгуулалтаар хангах, хяналт тавих;

8.2.2.кибер аюулгүй байдлын чиг үүргийг гүйцэтгэх эсхүл хавсран гүйцэтгэх албан хаагчийг ажиллуулж сургах, бэлтгэх;

8.2.3.кибер аюулгүй байдлыг хангах үйл ажиллагааг боловсронгуй болгоход шаардлагатай санхүүжилтийг төсөвт тусгах, саналаа эрх бүхий албан тушаалтанд танилцуулж, шийдвэрлүүлэх;

8.2.4.кибер аюулгүй байдлыг хангах санал санаачилга, үйл ажиллагааг дэмжин ажиллах.

8.3.Байгууллагын алба хаагч дараах үүрэгтэй байна.

8.3.1.Кибер аюулгүй байдлын тухай болон бусад холбогдох хууль, тогтоомжийг дагаж мөрдөх;

8.3.2.мэдээллийн систем хэрэглэгч нийт алба хаагч Төрийн болон албаны нууцын тухай хууль, Төрийн болон албаны нууцыг хамгаалах нийтлэг журам болон Төрийн албаны тухай хуулийн 37.1.9-д заасныг чанд мөрдөхийн зэрэгцээ “Гадаадын иргэн, харьяатын газрын кибер аюулгүй байдлыг хангах журам”, “Байгууллагын даргын 2018 оны 144 тушаалаар баталсан Мэдээллийн технологийн журам”-ыг дагаж мөрдөх.

8.3.3.илэрсэн халдлага, зөрчил, сэжигтэй тохиолдол бүрийг мэдээллийн технологийн асуудал хариуцсан нэгж, кибер аюулгүй байдлын чиг үүрэг хариуцсан албан хаагчид мэдэгдэх;

8.3.4.байгууллагын мэдээллийн систем, мэдээллийн сүлжээ, зөөврийн болон суурин компьютер, цахим мэдээлэл тээгчийг зөвхөн албан хэрэгцээнд ашиглах, тэдгээрийн аюулгүй байдлыг хангаж ажиллах;

8.3.5.байгууллагаас зохион байгуулж буй кибер аюулгүй байдлын сургалтад хамрагдах, кибер аюулгүй байдлыг хангах талаар өгсөн зөвлөмж, шаардлагыг биелүүлэх;

8.3.6.өөр ажил, албан тушаалд томилогдох, чөлөөлөгдөх тохиолдолд хариуцсан төрийн болон албаны нууцад хамаарах мэдээллийг нууцын эрхлэгчид хүлээлгэн өгч, мэдээллийн системд хандах эрхээ хаалгах.

8.4.Кибер аюулгүй байдлын чиг үүрэг хариуцсан албан хаагч дараах үүрэгтэй.

8.4.1.Кибер аюулгүй байдлын хууль тогтоомжийн хэрэгжилтийг зохион байгуулах;

8.4.2.кибер аюулгүй байдлын хяналт, шалгалт зохион байгуулан үр дүнг тооцож, удирдлагад танилцуулах;

8.4.3.кибер аюулгүй байдлын чиглэлээр бусад байгууллагаас ирүүлсэн зөвлөмж, хяналт шалгалтын акт, эрсдэлийн үнэлгээний дагуу холбогдох арга хэмжээг хэрэгжүүлж, үр дүнг тооцох, танилцуулах;

8.4.4.байгууллагад шинээр нэвтрүүлэх техник технологийн шийдлийг боловсруулах, худалдан авах үйл ажиллагаанд оролцох.

8.5.Мэдээллийн технологийн асуудал хариуцсан нэгж дараах үүрэгтэй.

8.5.1.кибер аюулгүй байдлыг хангах мэргэшүүлэх сургалтанд холбогдох албан хаагчдыг хамруулах;

8.5.2.Засгийн газрын 2022 оны 493 дугаар тогтоолоор батлагдсан "Кибер аюулгүй байдлыг Үндэсний стратеги төлөвлөгөө"-тэй уялдуулан байгууллагын кибер аюулгүй байдлын стратеги төлөвлөгөөг боловсруулж, батлуулах, хэрэгжилтийг хангах, тайлагнах;

8.5.3.байгууллагын хэмжээнд мөрдөгдөх журам, заавар, төлөвлөгөөг боловсруулж, хэрэгжилтэд хяналт тавих, тайлагнах;

8.5.4.кибер орчинд хандаж, мэдээлэлтэй ажиллах ажилтан, албан хаагч, бусад этгээдтэй мэдээллийн нууц хадгалах болон кибер аюулгүй байдлыг хангах чиглэлээр гэрээ байгуулах, нууцын баталгаа гаргуулах.

Ес. Хориглох үйл ажиллагаа

9.1 Дараах үйл ажиллагаа явуулахыг хориглоно.

9.1.1.Албан үүргээ гүйцэтгэх хугацаанд төрийн болон албаны, хувь хүний хуулиар хамгаалагдсан нууцыг чандлан хадгалах, хувийн болон бусдын ашиг сонирхлын төлөө ашиглахгүй, албан ёсны аливаа мэдээллийг эрх бүхий албан тушаалтны зөвшөөрөлгүйгээр тараах.

9.1.2.Интернэт сүлжээнд төрийн болон албаны нууцад хамаарах мэдээллийг байршуулах, цахим шуудангаар бусдад илгээх, интернэт орчны "cloud storage"-д хадгалах.

9.1.3.Албан хэрэгцээнд шаардлагагүй веб сайтуудад хандах, их хэмжээний файл татах, баталгаагүй болон сэжигтэй эх сурвалжаас файл татах, байгууллагын сүлжээг ашиглан зүй зохисгүй сэтгэгдэл үлдээх.

9.1.4.Компьютерт Dial-up, DSL, интернэт token, модем, гар утас холбох, сүлжээнд утсан болон утасгүй сүлжээний төхөөрөмжийг системийн зохицуулагчийн зөвшөөрлөөр залгах.

9.1.5.Албан хэрэгцээнд ашиглагдаж буй компьютерт ёс зүйд үл нийцэх хууль бус материал, бичлэг, зураг, кино, программ тоглоом татаж байршуулах, ашиглах.

9.1.6.Олон нийтийн сүлжээ, чатын программ ашиглаж төрийн болон албаны нууцад хамаарах мэдээлэл дамжуулах, солилцох.

9.1.7.Төрийн болон албаны нууцад хамаарах болон байгууллагын үйл ажиллагаа, нэр хүндэд хор хохирол учруулах, алба хаагчдын нэр хүндэд халдсан цахим мэдээллийг бусдад тараах.

9.1.8.Албан хэрэгцээнээс бусад зориулалтаар зөвшөөрөөгүй программ

хангамжийг суулгаж ажиллуулах.

9.1.9.Бусдын компьютер, техник хэрэгсэлд мэдээллийн санд нэвтрэх эрхийг хадгалж үлдээхгүй.

9.1.10.Хариуцаж буй компьютер, техник хэрэгсэлд засвар, үйлчилгээг гаднын иргэн, хуулийн этгээдээр зөвшөөрөлгүй хийлгэх.

Арав. Хяналт, хариуцлага тооцох

10.1.Энэ журмыг зөрчсөн албан тушаалтанд эрүүгийн хариуцлага хүлээлгэхээргүй бол Төрийн албаны тухай хууль, байгууллагын хөдөлмөрийн дотоод журамд заасны дагуу шийтгэл ногдуулна.

10.2.Нууц мэдээллийг санаатай буюу санамсаргүй байдлаар бусдад задруулснаас үүсэх хохирлыг нөхөн төлүүлэх, буруутай этгээдэд хариуцлага оногдуулах асуудлыг шүүхээр шийдвэрлүүлнэ.

---oOo---