Мэдээллийн системийн аюулгүй байдлын арга хэмжээний тогтолцоо

2007 оны 12 дугаар сарын 20-ны өдрийн №252 тоот Засгийн газрын тогтоол

RT1. I, 28.12.2007, 71, 440

2008 оны 1 дүгээр сарын 1-нээс хүчин төгөлдөр болсон.

Тус Журмыг Олон нийтийн мэдээллийн тухай хуулийн 43⁹ (1) 4) заалтын үндсэн дээр боловсруулж гаргасан болно.

Бүлэг 1
Нийтлэг үндэслэл

§ 1. Хэрэглэх хүрээ

(1) Төрийн болон орон нутгийн засаг захиргаааны байгууллагын мэдээллийн санд байрласан мэдээллийг боловсруулахад хэрэглэгддэг эсхүл тухайн байгууллагуудад хамаарах мэдээллийн тоног төхөөрөмж, эд хөрөнгийг ашиглахтай холбоотойгоор мэдээллийн системийн аюулгүй байдлын арга хэмжээний тогтолцоог бий болгох үүднээс тус журмыг боловсруулан гаргасан.

(2) Мэдээллийн системийн аюулгүй байдлын арга хэмжээний тогтолцоо нь мэдээллийг хамгаалах зорилготой аюулгүй байдлын арга хэмжээний техникийн үзүүлэлт, зохион байгуулалтын, биет болон мэдээллийн технологийн (IT) аюулгүйн арга хэмжээний тодорхойлолтуудаас бүрдэнэ.

(3) Төрийн нууцтай холбоотой мэдээллийн тогтолцооны аюулгүй байдалд тус Журам хэрэглэгдэхгүй.

§ 2. Аюулгүй байдлын арга хэмжээний тогтолцооны хэрэгжилт

Аюулгүй байдлын арга хэмжээний тогтолцооны хэрэгжилт нь мэдээллийн аюулгүй байдлын зорилгод нийцүүлсэн аюулгүйн ангиллуудын тодорхойлолтоос мөн мэдээллийн системийн аюулгүй байдлын гурван-түвшин бүхий тогтолцооны (үүнээс цааш "ISKE" гэх) хэрэгжилтийн зааварчилгаанд нийцсэн зохих аюулгүйн арга хэмжээг сонгох явдал болон түүний хэрэгжилтээс бүрдэнэ.

§3. Нэр томъёоны тодорхойлолт

(1) Тус Журамд дараах нэр томъёог дор тодорхойлсон байдлаар ойлгоно. Үүнд:

1) "мэдээллийн аюулгүй байдлын талаарх анализ" гэж мэдээллийн ач холбогдолтой, чухал байдалд үнэлгээ хийх болон тухайн мэдээлэл устаж үгүй болсноос үүсэх хохирлоос сэргийлэхийн тулд аюулгүй байдлын ангиллыг тодорхойлох явдлыг хэлнэ.

2) "аюулгүй байдлын арга хэмжээний тулгуур" гэж тухайн мэдээллийн аюулгүй байдлын түвшин болон мэдээллийг хэрэглэх мэдээлийн системээс хамаарч сонголт хийх, сонгосон аргад нийцсэн стандарт каталогид орсон аюулгүйн арга хэмжээг хэлнэ.

3) “аюулгүй байдлын тулгуур” гэж мэдээллийн аюулгүй байдлыг хангах болон түүнийг хангахын тулд гарцаагүй авах аюулгүй байдлын арга хэмжээнүүдийг хэлнэ.
4) “мэдээллийн систем” гэж техникийн системийг ажиллуулах, мэдээллийг ямар нэг аргаар хадгалах, дамжуулах болон түүний хэвийн үйл ажиллагаанд шаардагдах процесс ажиллагаа, нөөцийг хэлнэ.
5) “мэдээллийн аюулгүй байдал” гэж аюулгүйн арга хэмжээг тодорхойлох, сонгох, хэрэглэх зэрэг ажиллагаануудын нийлбэр цогц ажиллагааг хэлнэ.
6) “аюулгүйн арга хэмжээ” гэж мэдээллийг хадгалах, олж авах мөн мэдээллийн систем дэх мэдээллийн аюулгүй байдлыг хангах зохион байгууллалтын арга болон үйл ажиллагаа, техникийн арга хэрэгсэлийг ашиглах болон техникийн процесс ажиллагаануудыг хэлнэ.
7) “аюулгүй байдлын ангилал” гэж гурван бүрэлдхүүн, тэр дундаа аюулгүй байдлын гурван дэд ангиллаас бүрдэх дөрвөн-түвшин бүхий хуваариар илэрхийлэгдэх мэдээллийн чухал, ач холбогдолтой байдлаас үүдсэн мэдээллийн аюулгүйн байдлын шаардлагатай түвшинг хэлнэ.
8) “аюулгүй байдлын дэд ангилал” гэж дөрвөн-түвшин бүхий хуваариар илэрхийлэгдэх мэдээллийн чухал, ач холбогдолтой байдлаас үүдсэн мэдээллийн аюулгүй байдлыг бий болгоход шаардлагатай түвшинг хэлнэ. аюулгүй байдлын гурван дэд ангилал нь мэдээллийн аюулгүй байдлын гурван зорилгоос үүдэлтэй;

(1) Тус Журамд тодорхойлсон нэр томъёоны тайлбар нь EVS/ISO/IEC 2382 (Мэдээллийн технологи, Хэрэглэгдэх үгсийн сан), EVS ISO/IEC 13335 (Мэдээллийн технологи, IT аюулгүй байдлын менежементийн удирдамж)-н Хэсэг 1-5-д заасан стандартууд, EVS ISO/IEC 17799 (Мэдээллийн технологи, Аюулгүйн арга техник, Мэдээллийн аюулгүй байдлын менежементийн журам)-ийн стандартад тодорхойлсон утгаар хэрэглэгдэж байгаа болно.

Бүлэг 2
Аюлгүйн ангилал болон аюулгүйн арга хэмжээ

§ 4. Аюлгүй байдлын арга хэмжээний техник үзүүлэлтүүд

(1) Мэдээллийн аюулгүй байдлын зорилгод нийцүүлэн аюулгүйн ангиллыг тодорхойлох үүднээс мэдээллийн сангийн гол процессор нь мэдээллийн сан дахь мэдээллийн өгөгдөлүүдэд аюулгүй байдлын дүн шинжилгээ хийж зохион байгуулна.

(2) Мэдээллийн сангийн мэдээллийн өгөгдлүүдэд хийсэн аюулгүй байдлын ангилал нь тухайн мэдээллийн сангийн бүртгэл хийхэд эсхүл мэдээллийн санг мэдээллээр баяжуулалт хийхэд бэлтгэж байсан техникийн баримт бичгүүдийн хамтаар Олон нийтийн мэдээллийн тухай хуулийн 43^{9} (1) 6) заалтын үндсэн дээр боловсруулж гаргасан хууль тогтоомжид заасан процесс ажиллагааны дагуу батлагдан, хүлээн зөвшөөрөгдсөн байх ёстой. Аюулгүй байдлын ангилалд нийцэх аюулгүй байдлын арга хэмжээнүүд нь мэдээллийн санг ашиглах үед хэрэглэгдэнэ.

§ 5. Аюулгүй байдлын ангиллын тодорхойлолт

(1) Аюулгүй байдлын дүн шинжилгээний үр дүнд мэдээллийн сангийн гол процессор нь мэдээллийн аюулгүй байдлын зорилгын үндсэн дээр бие биенээс үл хамаарах аюулгүйн дэд ангиллыг тодорхойлон мөн аюулгүй байдлыг хангахын тулд зохион байгуулж ажиллах ёстой.

(2) Аюулгүйн ангиллуудыг мэдээллийн сан дахь мэдээллийн ажиллагаагаар тодорхойлно. Нэг мэдээллийн сан дахь өөр өөр мэдээллүүд нь аюулгүйн өөр өөр ангилалд хамаарч болно. Аюулгүйн ангилалуудтай нийцсэн аюулгүйн арга хэмжээнүүд нь өгөгдөл мэдээллүүд ажиллаж байгаа мэдээллийн систем эсхүл уг ажиллаж байгаа өгөдөл мэдээллийн нэг хэсэгт хамааран үйлчилж болно.

(3) Аюулгүйн ангиллыг хамгаалалтын өндөр түвшин шаардаж байгаа өгөгдөлийн мэдээллийн аюулгүйн түвшингийн үндсэн дээр тодорхойлно.

(4) Мэдээллийн аюулгүйн байдлын холбогдох зорилгыг тодорхойлж байгаа нэрийг илэрхийлсэн үсэг, тоо, тооны түвшинг аюулгүйн ангилалын тэмдэглэлийг хийхэд ашиглана. (Тухайлбал: K2T3S1 гэх мэт)

§ 6. Аюулгүйн түвшин

(1) Аюулгүйн түвшин нь өндөр (H), дундаж (M) эсхүл доод (L) гэж ангилагдана.

(2) Аюулгүйн түвшинг бүрэн бүтэн байдал, нууцлал болон хүртээмжтэй байдлын шалгууруар дүгнэж мэдээллийн аюулгүй байдлын зорилгод нийцүүлэн тогтооно.

(3) Мэдээллийн бүрэн бүтэн байдал гэдэгт үнэн зөв байдал, бүрэн байдал, тодорхой хугацаанд шинэчлэн баяжуулсан байдал, мэдээллийн үнэн зөв, бодитой байдал, хууль бус өөрчлөлтүүд хийгдээгүй байгаа байдлыг бүхэлд нь ойлгоно.

(4) Мэдээллийн нууцлал гэж зөвхөн эрх бүхий этгээд зөвшөөрөгдсөн техникийн хэрэгсэл ашиглан мэдээлэлд нэвтрэхийг хэлнэ.

(5) Мэдээллийн хүртээмжтэй байдал гэж эрх бүхий этгээд зөвшөөрөгдсөн техникийн хэрэгсэл ашиглан урьдаас зохих ёсоор тогтоосон ажлын цагаар (тухайлбал зайлшгүй бөгөөд зохих цаг хугацаанд эсхүл шаардлагатай байсан бөгөөд албаны цагт) тодорхой хугацаагаар эсхүл хялбархан нэвтрэн мэдээллийг ашиглахыг хэлнэ.

§ 7. Аюулгүй байдлын дэд ангилал

(1) Мэдээллийн хүртээмжтэй байдлын үндсэн дээр аюулгүй байдлын дэд ангиллыг доорх заалт хуваариар тодорхойлно. Үүнд:

1) K0 – итгэж болохуйц байдал – чухал биш; гүйцэтгэл – чухал биш;
2) K1 – итгэж болохуйц байдал – 90% (нэг долоо хоногийн хувьд зөвшөөрөгдөхүйц сул зогсолт ~ 24 цаг); хамгийн их ачааллын үед хариу өгөхөд шаардагдах хугацааны өсөлт зөвшөөрөгдөх хэмжээнд байх - цагаар (1÷10)
3) K2 – итгэж болохуйц байдал – 99% (нэг долоо хоногийн хувьд зөвшөөрөгдөхүйц сул зогсолт ~ 2 цаг); хамгийн их ачааллын үед хариу

өгөхөд шаардагдах хугацааны өсөлт зөвшөөрөгдөх хэмжээнд байх – минутаар (1÷10)

4) К3 – итгэж болохуйц байдал – 99.9% (нэг долоо хоногийн хувьд зөвшөөрөгдөхүйц сул зогсолт ~ 10 минут); хамгийн их ачааллын үед хариу өгөхөд шаардагдах хугацааны өсөлт зөвшөөрөгдөх хэмжээнд байх – секундээр (1÷10)

(2) Мэдээллийн бүрэн бүтэн байдлын үндсэн дээр аюулгүй байдлын дэд ангилалыг доорх заалт хуваариар тодорхойлно. Үүнд:

1) Т0 – мэдээллийн эх сурвалж, өөрчлөлт хийгдсэн эсэх болон мэдээлэл сарниж байгаа байдал чухал биш, үнэн зөв байдлыг шалгах, бүрэн бүтэн байдал болон мэдээллийг цаг хугацаанд нь шинэчлэн баяжуулсан байдлыг шалгах шаардлагагүй;

2) Т1 – мэдээллийн эх сурвалж, өөрчлөлт хийгдсэн эсэх болон мэдээлэл сарниж байгаа байдлыг тодорхойлох боломжтой байх; үнэн зөв байдлыг шалгах, бүрэн бүтэн байдал болон мэдээллийг цаг хугацаанд нь шинэчлэн баяжуулсан байдлыг тодорхой нөхцөл тохиолдолд эсхүл шаардлагатай үед шалгах боломжтой;

3) Т2 – мэдээллийн эх сурвалж, өөрчлөлт хийгдсэн эсэх болон мэдээлэл сарниж байгаа байдлыг тодорхойлох боломжтой байх; тодорхой хугацаанд үнэн зөв байдлыг шалгах, бүрэн бүтэн байдал болон мэдээллийг цаг хугацаанд нь шинэчлэн баяжуулсан байдлыг шалгах шаардлагатай;

4) Т3 – мэдээллийн эх сурвалж, өөрчлөлт хийгдсэн эсэх болон мэдээлэл сарниж байгаа байдлыг тодорхойлох нь нотолгооны ач холбогдолтой байх, тодорхой хугацаанд үнэн зөв байдлыг шалгах, бүрэн бүтэн байдал болон мэдээллийг цаг хугацаанд нь шинэчлэн баяжуулсан байдлыг тэр даруй шалгах шаардлагатай;

(3) Мэдээллийн нууцлалын үндсэн дээр аюулгүй байдлын дэд ангиллыг доорх заалт хуваариар тодорхойлно. Үүнд:

1) S0 – олон нийтийн мэдээлэл: мэдээлэлд нэвтрэхийг хязгаарлаагүй (тухайлбал тухайн мэдээллийг сонирхсон хүн бүр унших эрхтэй байх; бүрэн бүтэн байдлыг хадгалах шаардлагад нийцэж байгаа тохиолдолд өөрчлөлт, засвар хийх эрхтэй байх)

2) S1 – дотоод хэрэгцээнд зориулж мэдээллийг ашиглах: тухайн мэдээлэлд нэвтэрч байгаа хүн хууль ёсны ашиг сонирхолынхоо үүднээс нэвтэрч байгааг магадлаж мэдээлэлд нэвтрэхийг зөвшөөрөх;

3) S2 – нууц мэдээлэл: тухайн мэдээллийг ашиглах эрхийг зөвхөн тодорхой бүлэгт олгосон байх; тухайн мэдээлэлд нэвтэрч байгаа хүн хууль ёсны ашиг сонирхолынхоо үүднээс нэвтэрч байгааг магадлаж мэдээлэлд нэвтрэхийг зөвшөөрөх;

4) S3 – маш нууц мэдээлэл: зөвхөн тодорхой хэрэглэгчдэд тухайн мэдээллийг ашиглах эрхийг олгох; тухайн мэдээлэлд нэвтэрч байгаа хүн хууль ёсны ашиг сонирхолынхоо үүднээс нэвтэрч байгааг магадлаж мэдээлэлд нэвтрэхийг зөвшөөрөх;

§ 8. Аюулгүйн ангиллыг тогтоох

KTS-ийн дагуу дэд-ангиллын тэмдэг дээр тулгуурлаж мэдээллийн аюулгүйн ангиллын тэмдэгийг тогтооно. (Тухайлбал: K2T3S1 гэх мэт)

§ 9. Аюулгүйн ангилалд хамаарах аюулгүй байдлын арга хэмжээг сонгох

(1) Мэдээллийг агуулж байгаа мэдээллийн сангийн мэдээллийн аюулгүй байдлын зорилгыг хангах үүднээс аюулгүй байдлын арга хэмжээ нь энэхүү мэдээллийн системд байршиж байгаа мэдээллийн сангийн өгөгдөл мэдээллүүдийн хувьд бий болгосон аюулгүйн ангилалтай нийцсэн байх ёстой.

(2) Аюулгүйн арга хэмжээнүүдийг ISKE-г хэрэгжүүлэх удирдамж зааварчилгаанд нийцүүлэн сонгох ёстой.

(3) ISKE-г хэрэгжүүлэх удирдамж зааварчилгааг Эдийн засгийн сайд болон Харилцаа холбооны сайд баталж, тухайн яамныхаа цахим хуудсанд байршуулсан байна.

Бүлэг 3

Хэрэгжүүлэх үндэслэл

§ 10. Журам хүчин төгөлдөр болох

Тус Журам 2008 оны 1 дүгээр сарын 1-ний өдрөөс эхлэн хүчин төгөлдөр үйлчилнэ.

1 RT = *Riigi Teataja = Төрийн мэдээлэл сэтгүүл*