



Security  
Solution &  
Service

# Мэдээллийн аюулгүй байдлын удирдлагын ТОГТОЛЦОО



Т.Халтар  
“ЗС” ХХК-ийн зөвлөх  
Доктор, профессор  
[khaltar@sssmn.com](mailto:khaltar@sssmn.com)

## Аюулгүй байдлын талаарх тоо баримтууд

- МАБ-ын эсрэг зөрчлүүдээс учирсан хохирол, 2005 он:  
\$US 17.1 миллиард
- Асуулгад хамрагдсан хүмүүсийн 90% нь 2005 онд халдлагад өртсөн
- Нийтийн түгшүүр дэгдээсэн асуудал нь вирус (хэрэглэгчдийн 85%)
- 5 байгууллагын 2 нь веб сайтыг хууль бусаар ашиглах ажиллагааны хохирогч болсон
- 5 хэрэглэгчийн 3 нь хохирсноо мэддэггүй
- Аюулгүй байдлын халдлагууд 2 жилд 4 дахин нэмэгдэж байна
- МАБ нь мэдээллийн технологийн менежерүүдийн 1-р асуудал

# Мэдээллийн аюулгүй байдал



- Мэдээлэл нь байгууллагын бусад эд хөрөнгийн нэгэн адил үйл ажиллагаа, ажил хэргээ хэвийн явуулахад шаардагдах гол капиталын нэг учраас хамгаалагдсан байх ёстой.
- Мэдээллийн аюулгүй байдал гэдэг нь ажил хэргийн тасралтгүй чанарыг хангах, эрсдэлийг багасгах, хөрөнгө оруулалтын үр ашиг, бизнесийн боломжийг нэмэгдүүлэхийн тулд мэдээллийг олон янзын аюул, заналхийллээс хамгаалах ажиллагаа.

# Аюулгүй байдал гэж юу вэ?



Мэдээллийн технологийн аюулгүй байдлын 3  
бүрдэл хэсэг



# Аюулгүй байдал гэж юу вэ?

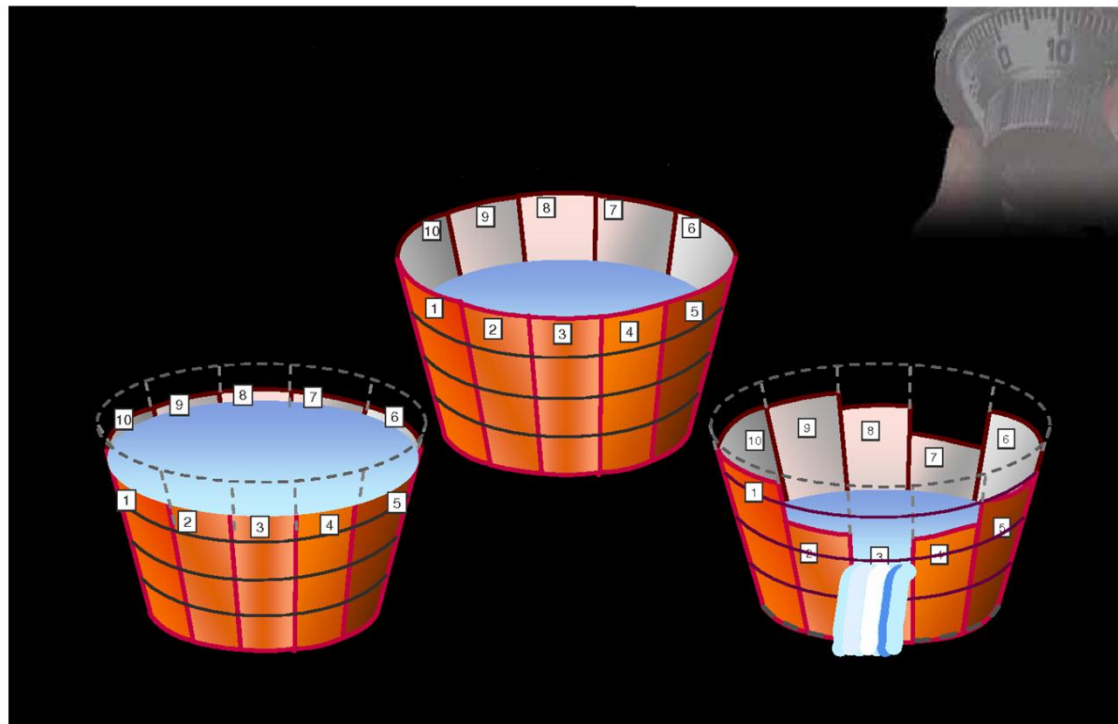


- Адилтгах & Харьцуулан таних-Нөөцөд хандахын тулд хэрэглэгчийг адилтгаж харьцуулан таньсныг батална.
- Хүртээмжтэй, тохиромжтой-Бүрдэл хэсгүүд болон дэд бүтцийн элементүүд сүлжээ бусниулах халдлагаас хамгаалагдсан байх ёстой.
- Нууцлал-Бүрдэл хэсгүүд, үйлчилгээ болон дэд бүтцийн элементүүд хууль бус нэвтрэлтээс хамгаалагдсан байх ёстой.
- Халдашгүй-Бүрдэл хэсгүүд хууль бус өөрчлөхөөс хамгаалагдсан байх ёстой. Өгөгдөл дамжуулахдаа хамгаалах талаар сайн анхаарна.
- Тасалдалгүй – Үйлчилгээг тасралтгүй, гажуудалгүй үзүүлэх, тохиолдол бүр тодорхой бүртгэлтэй хэрэглэгчтэй холбогдсон байх ёстой.

# Аюулгүй байдал гэж юу вэ?



Аюулгүй байдал ямар хэмжээтэй байвал зохих вэ? Торхны загвар



# Аюулгүй байдал гэж юу вэ?



## • Аюулгүй байдлын давхарга



# Мэдээллийн аюулгүй байдлыг хэрхэн хангах вэ?



- Аюулгүй байдлын бодлого, үйл явц, дэг журам, зохион байгуулалтын бүтэц болон програм хангамж, техник хангамжийн чиг үүргүүдийг багтаасан зохих хяналт, удирдлагын багцыг хэрэгжүүлэх замаар мэдээллийн аюулгүй байдлыг хангаж чадна.

# Мэдээллийн аюулгүй байдал яагаад хэрэгтэй вэ?



- Мэдээллийн аюулгүй байдлын тогтолцоог тодорхойлж, бий болгож, дэмжиж, сайжруулах нь өрсөлдөх чадвар, бэлэн мөнгөний урсгал, орлогоо дээшлүүлэх, хууль зүйн нийцлийг бий болгох, бизнесийн нэр төрөө бэхжүүлэх гол хүчин зүйлийн нэг
- Байгууллага болон байгууллагын мэдээллийн систем, сүлжээ олон янзын гарал үүсэлтэй аюул заналхийлэлтэй тулгарч байна.

# Мэдээллийн аюулгүй байдал яагаад хэрэгтэй вэ?



- Хохирлын шалтгаан болж буй нянтай програм, хортой програмууд, компьютер, сүлжээнд хууль бусаар нэвтрэн орох халдлага, үйлчилгээг бусниулсан довтолгоонууд нийтийг хамарсан шинжтэй, илүү шунахай, илүү төвөгтэй, нарийн болж байна.
- Мэдээллийн аюулгүй байдал нь төрийн, төрийн бус байгууллагууд, бизнесийн салбар болон эмзэг чухал дэд бүтцийг хамгаалахад маш чухал, онцгой хэрэгцээтэй болж байна.

# Мэдээллийн аюулгүй байдал яагаад хэрэгтэй вэ?



- Төрийн болон хувийн салбарын харилцаа холбоо нэмэгдэж, мэдээллийн нөөцийг хамтран ашиглаж байгаа нь хандалтын хяналтыг хэрэгжүүлэхэд учирч буй саадыг нэмэгдүүлж байна.
- Компьютер улам бүр олширч, тархан дэлгэрч буй хандлагын улмаас төвлөрсөн, тусгай хяналтын үр дүн буурч байна.
- Мэдээллийн олон систем аюулгүй байдлын шаардлагуудыг хангахааргүй зохион бүтээгджээ.

# Мэдээллийн аюулгүй байдал яагаад хэрэгтэй вэ?



- Техник хэрэгслийн тусламжтайгаар хангаж болох аюулгүй байдлын боломж хязгаарлагдмал учир зохих удирдлага, дэг журам зайлшгүй шаардлагатай.
- Мэдээллийн аюулгүй байдлын удирдлагыг хэрэгжүүлэхэд байгууллагын бүх ажилтнуудын оролцоо шаардагддаг.
- Үүсгэн байгуулагч, хувьцаа эзэмшигчид, гуравдагч тал, хэрэглэгчид, үйлчлүүлэгчид болон бусад талуудын оролцоо шаардагдаж болно.
- Гадны байгууллагын мэргэжилтний зөвлөгөө зайлшгүй шаардлагатай.

# Аюулгүй байдлын шаардлагуудыг хэрхэн ТОГТООХ ВЭ?



- Аюулгүй байдлын шаардлагуудыг тодруулсан байх нь байгууллагын нэг гол асуудал.
- Гурван гол эх сурвалж байдаг.
  - Байгууллагын бизнесийн стратеги, үндсэн зорилгыг үндэслэн тулгарч буй эрсдлүүдийг үнэлсэн үнэлгээ
  - даган мөрдөж байх ёстой хууль, эрх зүйн акт, зохицуулалт, удирдамж, заавар, гэрээнд тусгагдсан шаардлагууд
  - байгууллагаас боловсруулсан мэдээлэл боловсруулах үйл явцын зарчим, зорилго, ажил хэргийн шаардлагуудын нэгдэл

# Аюулгүй байдлын эрсдэлийг үнэлэх.



- Аюулгүй байдлын эрсдэлийн байнгын үнэлгээний үр дүнд аюулгүй байдлын шаардлагуудыг тодруулна.
- Сулхан хамгаалалтын улмаас учирч болох хохирлыг тооцож хяналт, үнэлгээний зардлаа төлөвлөнө.
- Эрсдэлийн үнэлгээний үр дүнд нөлөөлж болох аливаа өөрчлөлтийг мэдрэхийн тулд эрсдэлийн үнэлгээг тодорхой давтамжтайгаар хийж байх (дараа нь тодорхой үзнэ)

# Хяналтыг сонгон авах



- Аюулгүй байдлын шаардлага болон эрсдэлийг тодруулж, эрсдэлийг арилгах шийдвэр гарсны дараа эрсдэлийг зохистой түвшинд хүртэл бууруулахын тулд зохих хяналтыг сонгож хэрэгжүүлнэ.
- Хяналтыг энэ стандартад тусгагдсан юмуу урд нь боловсруулагдсан хяналтын хэлбэрүүдээс сонгож болох ба шаардлагатай бол хяналтын шинэ хэлбэрийг боловсруулж болно.

# Хяналтыг сонгон авах



- Эрсдэлийн үнэлгээ, түүнийг багасгах хувилбар, эрсдлийг удирдах хандлага дээр тулгуурласан байгууллагын шийдвэр, үндэсний болон олон улсын хууль тогтоомж, заавар, удирдамжаас хамаарч хяналтыг сонгоно.
- Энэ хичээлд тусгагдсан зарим хяналтыг мэдээллийн аюулгүй байдлын удирдлагын үндсэн зарчим хэмээн үзэж болох учраас ихэнх байгууллагад хэрэглэхэд тохиромжтой.(цаашид нарийвчлан үзнэ)

# Мэдээллийн аюулгүй байдлын эхлэлийн цэг



- Хяналтын олон хэлбэрийг мэдээллийн аюулгүй байдлын тогтолцоо бий болгох сайн эхлэл гэж /тооцож/ үзэж болно.
- Эрх зүйн үүднээс, түүний дотор хууль тогтоомжийн үүднээс үзвэл хяналт нь байгууллагын үндсэн асуудал гэж тооцогддог.
- Энэ хичээлд тусгагдсан хяналтууд бүгд чухал бөгөөд анхаарлаас гадуур үлдэж болохгүй боловч байгууллагад тулгарч буй өвөрмөц, онцлог эрсдэлээс хамааран ямар хяналт сонгохоо тодруулна.

# Мэдээллийн аюулгүй байдлын эхлэлийн цэг



**Хяналт нь дараах зүйлсийн хамт мэдээллийн аюулгүй байдлын нийтлэг практик гэж тооцогдоно:**

- мэдээллийн аюулгүй байдлын бодлогын баримт бичиг;
- мэдээллийн аюулгүй байдлын талаар хүлээх үүргийн хуваарилалт;
- мэдээллийн аюулгүй байдлын ойлголт, боловсрол, сургалт;
- зөв зүйтэй хэрэглээ;
- техникийн эмзэг байдлын удирдлага;
- бизнесийн тасралтгүй ажиллагааны удирдлага;
- мэдээллийн аюулгүй байдлын будлианы удирдлага болон түүнийг боловсронгуй болгох

# Амжилтад нөлөөлөх гол хүчин зүйлс



## **Туршлагаас харахад байгууллагын хүрээнд мэдээллийн аюулгүй байдлыг амжилттай хэрэгжүүлэхэд дараах хүчин зүйлс ихээхэн нөлөөлдөг:**

- мэдээллийн аюулгүй байдлын бодлого, зорилго, үйл ажиллагаа;
- мэдээллийн хамгаалалтыг хэрэгжүүлэх, дэмжих, хянах болон боловсронгуй болгох байгууллагын дотоод соёлтой нийцсэн хандлага, бүтэц;
- удирдлагын бүх түвшний илт дэмжлэг болон оролцоо;
- мэдээллийн аюулгүй байдлын шаардлага, эрсдэлийн үнэлгээ, эрсдэлийн удирдлагын талаархи сайн ойлголт, мэдлэг;
- бүх менежер, ажилтнууд болон бусад талуудад бүрэн дүүрэн ойлголт бий болгохын тулд үр дүнтэй маркетинг явуулах;



# Амжилтад нөлөөлөх гол хүчин зүйлс

- мэдээллийн аюулгүй байдлын бодлого, стандартын удирдлагыг бүх менежер, ажилтнууд болон гуравдагч талд хуваарилан хэрэгжүүлэх;
- мэдээллийн аюулгүй байдлын удирдлагын үйл ажиллагааны санхүүжилт бий болгох;
- зохих ойлголт, сургалт, боловсролыг бий болгох;
- мэдээллийн аюулгүй байдлын будлиан, учралын үр дүнтэй удирдлагыг бий болгох;
- мэдээллийн аюулгүй байдлын удирдлага дахь ажлын гүйцэтгэл болон буцах холбоог үнэлэхийн тулд хэмжилт, үнэлгээний тогтолцоог бий болгох

# Байгууллагын аюулгүй байдлыг хангах дөрвөн үе шат



- **Байгууллагын аюулгүй байдлын өргөн хөтөлбөрийг хэрэгжүүлэх энгийн дөрвөн үе шат байдаг:**
  - *Ямар ашиг сонирхлыг хамгаалахаа тодорхойлох*
  - *Мэдээллийн эмзэг нөөц бүрийг хэрхэн хамгаалахаа шийдэх*
  - *Ажил хэргийн шаардлагад үндэслэсэн зохих хамгаалалтыг хэрэгжүүлэх*
  - *Сонгосон хамгаалалт үр дүнтэй, үр нөлөөтэй байгаа эсэхийг байнга шалгаж байх*

# Байгууллагын аюулгүй байдлыг хангах дөрвөн үе шат



- **Өмнө дурдсан дөрвөн үе шатыг задлан үзье.**

## Ямар ашиг сонирхлыг хамгаалвал зохих вэ?

- Эмзэг нөөцүүдийг тодруулах
- Нөөцүүдийг ангилах
- Эзэн хариуцагчийг тодруулах, хуваарилах
- Нөөцийн үнэ цэнийг тогтоож ангилах
- Эмзэг нөөцүүдийг хэрхэн ашиглаж буйг тодруулах
- Эрсдэл болон учирч болох аюулыг адилтгах

## Мэдээллийн эмзэг нөөцүүдийг хэрхэн хамгаалсан вэ?

- Аюулгүй байдлын одоогийн бодлого, стандарт, процессийг үнэлэх
- Хэрэглээ, үйлдлийн систем, сүлжээ, өгөгдлийн сангийн хамгаалалтын хэрэгжилтийг үнэлэх
- Хамгаалалтын одоогийн байдлыг шалгаж үзэх /этикийн хакер/

# Байгууллагын аюулгүй байдлыг хангах дөрвөн үе шат



- **Өмнө дурдсан дөрвөн үе шатыг задлан үзье.**

## Эмзэг нөөцүүд хэрхэн хамгаалагдсан байх ёстой вэ?

- Техникийн шаардлагуудыг шинжлэх
- Удирдлагын шаардлагуудыг шинжлэх
- Ялгааны шинжилгээг хөгжүүлэх
- Технологи хөгжүүлэх, зөвлөмж боловсруулах хүрээн дээр үндэслэсэн хэрэглэгчийн аюулгүй байдлын архитектурыг хөгжүүлэх

## Ашиглах нөөцүүдийг хамгаалах:

- Зорилтот орчинд шилжих төлөвлөгөө боловсруулах
- Аюулгүй байдлын бодлого стандарт боловсруулах/боловсронгуй болгох
- Аюулгүй байдлын үйлдлүүдийг боловсруулах
- Түгээлтийн аюулгүй системийн техникийн шийдэл, аюулгүй цахим худалдааны хэрэглээ, криптографийн түлхүүрийн тогтолцоо, смарт картын хэрэглээний шийдлийг боловсруулах.
- Хэрэгжүүлэх төлөвлөгөөг удирдах

# Байгууллагын мэдээллийн аюулгүй байдлын тогтолцоо



<b>ЭРСДЭЛИЙН ЭЦСИЙН ҮНЭЛГЭЭ БОЛОВСРУУЛАЛТ</b>	<b>АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО</b>	<b>М А Б-ЫН ТОГТОЛЦООГ ЗОХИОН БАЙГУУЛАХ</b>
<b>ЭД ХӨРӨНГИЙН УДИРДЛАГА</b>	<b>ХҮНИЙ НӨӨЦТЭЙ ХОЛБООТОЙ АЮУЛГҮЙ БАЙДАЛ</b>	<b>БАЙР, БАЙШИН БОЛОҢ ОРЧНЫ АЮУЛГҮЙ БАЙДАЛ</b>
<b>ХОЛБОЛТ БОЛОН ҮЙЛ АЖИЛЛАГААНЫ УДИРДЛАГА</b>	<b>ХАНДАЛТЫН УДИРДЛАГА</b>	<b>МЭДЭЭЛЛИЙН СИСТЕМ СУУРИЛУУЛАХ, ҮЙЛЧИЛГЭЭ ХИЙХ</b>
<b>МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН БУДЛИАНЫ УДИРДЛАГА</b>	<b>ТАСРАЛТГҮЙ АЖИЛЛАГААНЫ УДИРДЛАГА</b>	<b>НИЙЦЭЛ</b>

# Эрсдэлийн удирдлага



- “Эрсдэл” – энэ бол аюулгүй байдал хэмээх зүйлийн суурийг бүрдүүлж буй үндсэн үзэл баримтлал. Эрсдэл – энэ бол хамгаалалт шаардаж буй хор хохирол учрах магадлал.
- Эрсдэл байхгүй бол хамгаалалт хэрэггүй. Эрсдэл бол аюулгүй байдлын салбарт ажиллагсдын ойлгодог зүйл.
- Эмзэг сул байдал болон аюул заналхийлэл нь эрсдэлийн үндсийг бүрдүүлнэ.
- Аюул заналхийлэл, эмзэг байдал байхгүй бол эрсдэл байхгүй.
- Эмзэг байдал гэдэг нь довтолгоон үйлдэж болох боломжит суваг, зам. Систем, сүлжээ болон захиргааны дэг жаягт байдаг.
- Аюул заналхийлэл гэдэг нь мэдээллийн систем, сүлжээний аюулгүй байдлыг зөрчиж, эвдэж чадах үйлдэл, үйл явдал. Гурван бүрдэл хэсэгтэй:
  - **Бай.** Довтолгоонд өртөж буй бүрдэл хэсэг.
  - **Агентууд.** Аюул, заналхийлэл агуулж, учруулж буй субъект
  - **Үйл явдал.** Аюул агуулж буй үйлдэл.

# Аюул + Эмзэг байдал = Эрсдэл



- Эрсдэл гэдэг нь аюул болон эмзэг байдлын хослол юм.
- Эрсдэлийг үнэлнэ гэдэг нь урьдчилан таах аргагүй үйл явдал бий болох магадлалыг тодорхойлох явдал.
- Эрсдэл гурван түвшинтэй:
  - **Сул.** Аюул бий болох магадлал бага байна. Боломжийн хирээр эмзэг цэгийг илрүүлж арилгах арга хэмжээ авна. Гэхдээ зардал нь бага байна гэсэн үг.
  - **Дунд.** Эмзэг байдал нь мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал, адилтган таних, зөвшөөрөх тогтолцоонд бодитой эрсдэл учруулж байгаа. Ийм үйл явдал бий болох бодит боломж оршиж байгаа. Эмзэг байдлыг арилгах арга хэмжээ авах, үйлдэл хийх нь зохистой.
  - **Хүчтэй.** Эмзэг байдал нь бодитой эрсдэл бий болгож байгаа. Нэн даруй арга хэмжээ авах шаардлагатай.

# Эмзэг, сул байдлыг илрүүлэх



- Эмзэг байдлыг илрүүлэхийн тулд байгууллагад нэвтрэх бүх цэгийг тодруулна. Ө.Х мэдээлэл, систем, сүлжээнд хандах цэгүүдийг (цахим болон биет байдлаар) илрүүлэх, тодруулах. Үүнд:
  - Интернетийн холболт;
  - Алсын зайнаас хандах цэгүүд;
  - Бусад байгууллагатай холбогдсон холболт;
  - Биет байдлаар нэвтрэн орох цэгүүд;
  - Хэрэглэгчийн хандах цэгүүд;
  - Утасгүй холбооны сүлжээний хандалтын цэгүүд.

# Эрсдэлийн шинжилгээ



Эрсдэлийн шинжилгээ хийх үйл явц дараах үе шатуудаас бүрдэнэ.

- Эд хөрөнгийг (мэдээлэл) адилтгах, тодорхойлох, үнэ цэнийг тогтоох
- Аюул заналхийллийг үнэлэх
- Эмзэг байдлыг үнэлэх
- Одоо байгаа болон төлөвлөж буй аюулгүй байдлын арга хэмжээг үнэлэх
- Эрсдэлийн үнэлгээ хийх

# Нэг. ЭРСДЭЛИЙН ЭЦСИЙН ҮНЭЛГЭЭ БОЛОН БОЛОВСРУУЛАЛТ



## Аюулгүй байдлын эрсдэлийг үнэлэх (1/1)

- Эрсдэлийн эцсийн үнэлгээ нь байгууллагын зорилго болон байж болох эрсдэлийн шалгуурын дагуу эрсдэлүүдийг тодруулж, хэмжээг нь тодорхойлж аюулынх нь түвшингээр ангилна.
- Үнэлгээний үр дүн нь мэдээллийн аюулгүй байдлын эрсдэлийг удирдах тэргүүлэх чиглэл болон удирдлагын зохих үйл ажиллагаа, эдгээр эрсдэлээс хамгаалахын тулд сонгож авах хяналтыг тодруулж, чиглүүлэх ёстой.
- Эрсдэлийг үнэлэх, хяналтыг сонгох үйл явц хэд хэдэн удаа давтагдаж болно.
- Эрсдэлийн ач холбогдлыг тодорхойлохын (эрсдэлийн үнэлгээ) тулд эрсдэлийн хэмжээг тогтмол үнэлэх (эрсдэлийн шинжилгээ) ажиллагаа, байж болох эрсдэлийг эрсдэлийн шалгууртай харьцуулах үйл явцыг эрсдэлийн үнэлгээ агуулсан байх ёстой

# ЭРСДЭЛИЙН ЭЦСИЙН ҮНЭЛГЭЭ БОЛОН БОЛОВСРУУЛАЛТ (1/2)



## Аюулгүй байдлын эрсдэлийг үнэлэх

- Аюулгүй байдлын шаардлагуудад өөрчлөлт орсон болон эрсдэлийн тухайн үеийн байдалд, жишээлбэл эд хөрөнгө, аюул, эмзэг байдал, нөлөөлөл, эрсдэлийн үнэлгээнд өөрчлөлт орсон, нөхцөл байдал эрс өөрчлөгдсөн үед эрсдэлийн үнэлгээг үе үе хийж байна.
- Харьцуулж, дахин ашиглаж болохоор үр дүнд хүрэх чадвартай арга зүй ашиглан эрсдэлийн эдгээр үнэлгээг гүйцэтгэнэ
- Үнэлгээ үр дүнтэй байхын тулд нягт тодорхойлогдсон хүрээ хязгаартай байх ёстой бөгөөд бусад салбарын эрсдэлийн үнэлгээтэй холбогдсон байна
- Эрсдэлийн үнэлгээний хүрээ хязгаар нь бүх байгууллага, байгууллагын нэгж, хэсэг, мэдээллийн систем, системийн бүрдэл хэсэг, эсхүл үйлчилгээгээр хязгаарлагдаж болно

# ЭРСДЭЛИЙН ЭЦСИЙН ҮНЭЛГЭЭ БОЛОН БОЛОВСРУУЛАЛТ (1/3)



## Аюулгүй байдлын эрсдэлийг боловсруулах

- Эрсдэлийг боловсруулахын өмнө эрсдэл үнэхээр байгаа эсэхийг тодорхойлох, эрсдэлийг хүлээн авах шалгууруудыг байгууллага бий болгосон байх
- Эрсдэл бага байх юмуу эрсдэлийг боловсруулах үнэ өртөг нь учруулж болох хохирлоосоо их байхад эрсдэл байна гэж хүлээн зөвшөөрч болох юм
- Эрсдэлийг тодруулан гаргаж ирсний дараа эрсдэлийн эцсийн үнэлгээ, эрсдэлийн боловсруулалт хийх шийдвэр гаргах шаардлагатай

# ЭРСДЭЛИЙН ЭЦСИЙН ҮНЭЛГЭЭ БОЛОН БОЛОВСРУУЛАЛТ (1/4)



- **Аюулгүй байдлын эрсдэлийг боловсруулах**

Эрсдэлийг боловсруулах боломжит хувилбарууд дараах зүйлсийг багтаасан байна:

- Эрсдэлийг багасгахын тулд зохих хяналтыг нэвтрүүлэх;*
- Байгууллагын бодлого болон эрсдэл хүлээн авах шалгууруудад уг эрсдэлийг нийцүүлэн ухамсартайгаар, бодитойгоор хүлээн авах;*
- Эрсдэл бий болгож болох үйлдлийг хийлгэлгүйгээр эрсдэлээс зайлсхийх;*
- Холбогдох эрсдэлийг гуравдагч талд, жишээлбэл даатгалын байгууллага, нийлүүлэгчдэд шилжүүлэх.*

# ЭРСДЭЛИЙН ЭЦСИЙН ҮНЭЛГЭЭ БОЛОН БОЛОВСРУУЛАЛТ (1/5)



- **Аюулгүй байдлын эрсдэлийг боловсруулах**

Зохих хяналтыг хэрэгжүүлэх шийдвэр гаргасан тохиолдолд эрсдэлийн үнэлгээний үр дүнд тодруулсан шалгууруудын дагуу тухайн хяналтаа сонгож хэрэгжүүлнэ. Хяналт нь эрсдэлийг зохих түвшинд нь хүртэл бууруулах ёстой. Энэ үед дараах зүйлсийг анхаарч үзнэ:

*-үндэсний болон олон улсын хууль тогтоомж, зохицуулалтын шаардлага, хязгаарлалт;*

*-зохион байгуулалтын зорилгууд;*

*-үйлдэл, ажиллагааны шаардлага, хязгаарлалт;*

*-бууруулж буй эрсдэлтэй холбоотой хэрэгжүүлэх болон үйл ажиллагаа явуулах зардал;*

*-учирч болох гэм хорын эсрэг хяналтыг хэрэгжүүлэх болон түүний хүрээнд явуулах үйл ажиллагааны хөрөнгө оруулалтыг тэнцвэржүүлэх хэрэгцээ, шаардлага.*

# ЭРСДЭЛИЙН ЭЦСИЙН ҮНЭЛГЭЭ БОЛОН БОЛОВСРУУЛАЛТ (1/6)



- **Аюулгүй байдлын эрсдэлийг боловсруулах**

Хяналтыг энэ хичээлээс болон хяналтын бусад хэлбэрээс сонгон авч болохоос гадна байгууллагын өвөрмөц хэрэгцээнд нийцсэн шинэ хяналтыг бий болгож болно. Зарим хяналт мэдээллийн систем бүрт тохирохгүй, бүх байгууллагад бодитой байж чадахгүй гэдгийг хүлээн зөвшөөрөх ёстой. Цөөхөн хүнтэй жижиг байгууллагын хувьд ажлын үүргээ ингэж олон хуваах боломжгүй бөгөөд зохих хяналтыг хэрэгжүүлэх өөр замыг эрж хайхаас өөр аргагүй.

Хяналтын ямар ч сайн багц бүрэн дүүрэн аюулгүй байдлыг хангаж чадахгүй гэдгийг анхаарч аюулгүй байдлын хяналтын үр нөлөө, үр дүнг хянан шалгах, үнэлэх, боловсронгуй болгох удирдлагын нэмэлт үйл ажиллагаа хэрэгжүүлэх шаардлагатай.

# Сөрөг арга хэмжээ



Дараах үндсэн сөрөг арга хэмжээнүүд байдаг:

- Галт хана (сүлжээ хоорондын дэлгэц);
- Вирусын эсрэг ПХ;
- Хандалтын хяналт;
- Хоёр бүрдэлтэй таньж зөвшөөрөх систем;
- Бейж (адилтгах карт);
- Биометр аргууд;
- Ухаалаг (смарт) карт унших систем;
- Харуул;
- Файлд хандах хандалтын хяналт;
- Шифрлэлт;
- Ухамсартай, сайн сургаж бэлтгэсэн ажилтнууд;
- Нэвтрэлтийг илрүүлэх систем;
- ПХ-ыг автоматаар шинэчлэх, сайжруулах, ПХ-ыг удирдах бодлого г.м.

# Хоёр. АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО (2)



- **Мэдээллийн аюулгүй байдлын бодлого**

Зорилго: Ажил хэргийн шаардлага, зохих хууль болон зохицуулалтын дагуу удирдлагын үндсэн чиглэлийг гаргах, мэдээллийн аюулгүй байдлыг дэмжих.

Удирдлагын зүгээс бизнесийн зорилгын дагуу бодлогын чиглэлээ боловсруулах, байгууллагын хэмжээний мэдээллийн аюулгүй байдлын бодлогыг гаргах, хангах замаар мэдээллийн аюулгүй байдлыг дэмжих ёстой.

# Үндсэн агуулга Үндсэн баримт бичиг



# Мэдээллийн аюулгүй байдлын бодлого **(2/1)**



- ***Мэдээллийн аюулгүй байдлын бодлогын баримт бичгүүд.***  
Мэдээллийн аюулгүй байдлын бодлогын баримт бичгүүдийг удирдлага сайшаан баталж, хэвлэн нийтлүүлж, бүх ажилтнууд болон холбогдох талуудад мэдээлсэн байна.  
Мэдээллийн аюулгүй байдлын бодлогын баримт бичиг удирдлагын үүргийг тогтоож, МАБ-ын удирдлагын хандлагыг тодорхойлно. Бодлогын баримт бичигт дараах зүйлсийг оруулсан байна:
  - мэдээллийн аюулгүй байдлын тодорхойлолт, түүний зорилго, хүрээ болон мэдээллийг хамтран ашиглах механизм, аюулгүй байдлын чухал шинж чанар;*
  - мэдээллийн аюулгүй байдлын зорилт, зарчмуудыг дэмжиж буй удирдлагын эрмэлзлэл;*
  - эрсдэлийн эцсийн үнэлгээ болон эрсдэлийн удирдлагын бүтцийг хамруулсан хяналтын зорилгууд болон хяналтыг бий болгох үзэл санаа;*

# Аюулгүй байдлын бодлого (2/2)



- **Мэдээллийн аюулгүй байдлын бодлогын баримт бичгүүд.**

-аюулгүй байдлын бодлого, зарчим, стандарт болон аюулгүй байдлын чухал шинжийг байгууллагад хэвшүүлэх шаардлагуудын тухай товч тайлбар. Энд дараах зүйлс хамаарна:

1. хууль тогтоомж, зохицуулалт болон гэрээний шаардлагуудтай нийцэж буй нийцэл;

2. аюулгүй байдлын боловсрол, сургалт болон ойлголтын шаардлагууд;

3. бизнесийн тасралтгүй ажиллагааны удирдлага;

4. мэдээллийн аюулгүй байдлын бодлогыг зөрчсөний үр дагавар;

-мэдээллийн аюулгүй байдлын будлианы тайланг хамруулсан мэдээллийн аюулгүй байдлын удирдлагын нийтлэг болон өвөрмөц үүргүүдийн тодорхойлолт;

-бодлогыг дэмжих баримт бичгийн лавлагаа, жишээлбэл мэдээллийн тодорхой системд зориулсан аюулгүй байдлын илүү нарийвчилсан бодлого, дэг журам, хэрэглэгчийн даган мөрдөх аюулгүй байдлын удирдамж.

# Аюулгүй байдлын бодлого (2/3)



- *Мэдээллийн аюулгүй байдлын бодлогын баримт бичгүүд.*

*Мэдээллийн аюулгүй байдлын бодлого нь бодлогын ерөнхий баримт бичгийн нэг хэсэг байж болно. Хэрэв мэдээллийн аюулгүй байдлын бодлогыг байгууллагаас гадагш тараасан бол эмзэг, чухал мэдээллүүдийг алдахгүй байх арга хэмжээг авсан байна. Дэлгэрэнгүй мэдээллийг ISO/IEC 13335-1:2004-өөс олж үзэж болно.*

# Аюулгүй байдлын бодлого (2/4)



- *Мэдээллийн аюулгүй байдлын бодлогыг нягтлан шалгах*

-Мэдээллийн аюулгүй байдлын бодлогын бүрэн бүтэн байдал, зохицол, үр нөлөөг хангахын тулд түүнийг төлөвлөсөн цаг хугацаанд юмуу ямар нэг чухал өөрчлөлт гарсан тохиолдолд дахин нягтлан шалгаж байна.

-Аюулгүй байдлын бодлогыг боловсруулах, нягтлан шалгах, үнэлэх үүрэг, хариуцлагыг хүлээсэн хүн байх ёстой

-Удирдлагын хяналт шалгалтын үр дүнг мэдээллийн аюулгүй байдлын бодлогыг нягтлан шалгах үед тооцон үзэх шаардлагатай.

-Нягтлан шалгах мөчлөгийн хуанлийг багтаасан удирдлагын нягтлан шалгах ажиллагааны тодорхой дэгтэй байна.

# Аюулгүй байдлын бодлого (2/5)



- **Мэдээллийн аюулгүй байдлын бодлогыг нягтлан шалгах**  
Удирдлагын нягтлан шалгах ажиллагааны орцод дараах мэдээллүүд багтана:
  - сонирхогч талуудтай тогтоох буцах холбоо;
  - бие даасан нягтлан шалгах ажиллагааны үр дүн (6.1.8-ыг үз);
  - урьдчилан сэргийлэх болон засаж залруулах үйл ажиллагаанууд (6.1.8 болон 15.2.1-ийг үз);
  - удирдлагын урд өмнөх нягтлан шалгах ажиллагааны үр дүн;
  - үйл ажиллагааны гүйцэтгэл болон мэдээллийн аюулгүй байдлын бодлогын нийцэл;
  - мэдээллийн аюулгүй байдлыг удирдах байгууллагын хандлагад (байгууллагын гадаад, дотоод орчин, ажил хэргийн нөхцөл байдал, нөөц, гэрээ, зохицуулалт, эрх зүй, хууль тогтоомжийн орчин, техникийн орчинд орсон өөрчлөлт) нөлөөлж болох өөрчлөлтүүд;
  - аюул заналхийлэл болон эмзэг байдалтай холбоотой чиглэл, хандлагууд;
  - Мэдээ, тайланд тусгагдсан (мэдээлэгдсэн) мэдээллийн аюулгүй байдлын будлиан, зөрчлүүд (13.1-ийг үз);
  - Эрх бүхий байгууллага, этгээдүүдээс гаргасан зөвлөмжүүд (6.1.6-ийг үз).

# Аюулгүй байдлын бодлого (2/6)



- **Мэдээллийн аюулгүй байдлын бодлогыг нягтлан шалгах**

Удирдлагын нягтлан шалгах ажиллагааны гарцад дараах зүйлстэй холбоотой шийдвэр, үйл ажиллагаа багтана:

- мэдээллийн аюулгүй байдлын удирдлага болон үйл явцыг сайжруулах байгууллагын хандлага;
- хяналтын зорилго болон хяналтыг боловсронгуй болгох арга зам;
- нөөц болон хүлээх үүргийн хуваарилалтыг боловсронгуй болгох арга зам.

Удирдлагын нягтлан шалгах ажиллагааны тайланг заавал гаргана. Дахин нягталж хянасан бодлогын талаар удирдлагын дэмжлэг авсан байх ёстой.

# Гурав. Мэдээллийн аюулгүй байдлын ТОГТОЛЦООГ зохион байгуулах



- **Байгууллагын дотоод зохион байгуулалт (3/1)**

Зорилго: Байгууллагын хэмжээнд мэдээллийн аюулгүй байдлыг удирдах.

Байгууллагын хэмжээнд мэдээллийн аюулгүй байдлын хэрэгжилтийг санаачлах, хянах боломжтойгоор удирдлагын бүтцийг тогтооно.

Удирдлагын зүгээс мэдээллийн аюулгүй байдлын бодлогыг сайшаан баталж, аюулгүй байдлын талаар хүлээх, гүйцэтгэх үүргийг хуваарилж, байгууллагын хэмжээнд аюулгүй байдлыг хэрэгжүүлэх ажиллагааг уялдуулж, хянан шалгаж байна.

Хэрэв шаардлагатай бол мэдээллийн аюулгүй байдлын мэргэжилтний зөвлөмж, туслалцаа авах эх сурвалжийг бий болгож, байгууллагын хэмжээнд хүртээмжтэй байлгана.

# Байгууллагын дотоод зохион байгуулалт

(3/2)



- **Мэдээллийн аюулгүй байдлын талаар удирдлагын хүлээх үүрэг**
  - Ил тод чиглэл, удирдамж, илт үзэл баримтлал, тодорхой даалгавар, мэдээллийн аюулгүй байдлын талаар хүлээх үүргийн баталгаажуулалтаар дамжуулан удирдлагаас байгууллагын хэмжээнд аюулгүй байдлыг идэвхтэй дэмжин хөгжүүлнэ.
  - Удирдлага дараах зүйлсийг заавал гүйцэтгэх ёстой:
  - *мэдээллийн аюулгүй байдлын зорилго тодорхойлогдсон, байгууллагын доторхи шаардлагатай тохирч байгаа, зохих үйл явцад нийцэн орсон гэдгийг шалган баталгаажуулсан байх;*
  - *мэдээллийн аюулгүй байдлын бодлогыг томъёолж, хянаж, баталсан байх;*

# Байгууллагын дотоод зохион байгуулалт

(3/3)



- **Мэдээллийн аюулгүй байдлын талаар удирдлагын хүлээх үүрэг**

- мэдээллийн аюулгүй байдлын бодлогын хэрэгжилтийн үр дүнг нягтлан шалгах;
- аюулгүй байдлын санаачлагад зориулсан ил тод чиглэл болон удирдлагын илт дэмжлэгийг бий болгох;
- мэдээллийн аюулгүй байдалд шаардлагатай нөөцөөр хангах;
- байгууллагын хэмжээнд мэдээллийн аюулгүй байдлын талаар гүйцэтгэх үүрэг болон хүлээх үүрэг хариуцлагыг хуваарилж томилох;
- мэдээллийн аюулгүй байдлын мэдлэг, ойлголт бий болгох төлөвлөгөө, хөтөлбөр гаргах;
- мэдээллийн аюулгүй байдлын хяналтуудыг байгууллагын хэмжээнд уялдуулан зохицуулах.

# Байгууллагын дотоод зохион байгуулалт

(3/4)



- **Мэдээллийн аюулгүй байдлын талаар удирдлагын хүлээх үүрэг**

-Гадны болон өөрийн мэргэжилтний мэдээллийн аюулгүй байдлын зөвлөмж, зөвлөгөө хэрэгтэй эсэхийг удирдлагын зүгээс тодруулж үр дүнг нь байгууллагын хэмжээнд хянан шалгаж, уялдуулан зохицуулна.

-Байгууллагын хэмжээнээс хамааран дээрх үүргийг удирдах ажилтнуудын хуралдаан юмуу захирлын зөвлөл гэх мэт удирдлагын байгууллага хэрэгжүүлнэ.

-Илүү тодорхой мэдээллийг ISO/IEC 13335-1:2004 -өөс үзэж болно.

# Байгууллагын дотоод зохион байгуулалт

## (3/5)



- ***Мэдээллийн аюулгүй байдлын уялдаа холбоо***
  - Байгууллагын янз бүрийн үүрэг роль, ажлын чиг үүрэгтэй нэгж, хэсгүүдийн төлөөлөгчид хамтран мэдээллийн аюулгүй байдлын үйл ажиллагааг уялдуулан зохицуулна.
  - Менежерүүд, хэрэглэгчид, удирдах ажилтан, захиргааны ажилтнууд, програм зохиогчид, хянан шалгагч, аюулгүй байдлын ажилтнууд, даатгал, хууль, хүний нөөц, мэдээллийн технологи, эрсдэлийн удирдлагын салбарын мэргэжилтнүүдийн хамтын, харилцан уялдсан ажиллагаа дээр мэдээллийн аюулгүй байдлын уялдаа, зохицол тулгуурлана.
  - Хэрэв бие даасан, чиг үүргийн нэгжийг байгууллага ашигладаггүй, ийм нэгж байгуулсан ч байгууллагын хэмжээнд нийцэхгүй байгаа бол дээр дурдсан үйл ажиллагааг удирдлагын зохих нэгж юмуу аль нэг менежер хэрэгжүүлнэ.

# Байгууллагын дотоод зохион байгуулалт

## (3/6)



- **Мэдээллийн аюулгүй байдлын уялдаа холбоо**

**Дээрх хамтын, харилцан уялдсан ажиллагаагаар:**

*-аюулгүй байдлыг хангах үйл ажиллагааг мэдээллийн аюулгүй байдлын бодлогын дагуу гүйцэтгэж байгаа эсэхийг баталгаажуулна;*

*-үл нийцсэн зүйлсийг (байдлыг) хэрхэн зохицуулахыг тодруулна;*

*-мэдээллийн аюулгүй байдлын аргачлал, үйл явцыг, жишээлбэл эрсдэлийн үнэлгээ, мэдээллийн ангилалыг батална;*

*-мэдээлэлд учирч буй үндсэн аюулуудад орсон өөрчлөлт, мэдээлэл, мэдээлэл боловсруулах аппарат хэрэгслүүдийн аюулд өртөх боломжийг тодруулна;*

*-мэдээллийн аюулгүй байдлын нийцлийг үнэлж, хяналтыг хэрэгжүүлэх ажиллагааг уялдуулна;*

*-мэдээллийн аюулгүй байдлын боловсрол, сургалтыг байгууллагын хэмжээнд үр дүнтэй зохион байгуулж, мэдлэг дэлгэрүүлнэ;*

*-хяналт, мониторинг, мэдээллийн аюулгүй байдлын будлиан, зөрчлийн шалгалтаас олж авсан мэдээллийг үнэлж мэдээллийн аюулгүй байдлын будлиан, зөрчлийн (адилтган тодруулсан) эсрэг авах арга хэмжээг санал болгоно.*

# Байгууллагын дотоод зохион байгуулалт

(3/7)



- **Мэдээллийн аюулгүй байдлын талаар хүлээх үүрэг, хариуцлагыг хуваарилах**
  - Мэдээллийн аюулгүй байдлын талаар хүлээх бүх үүрэг, хариуцлагыг маш сайн тодорхойлсон байх ёстой
  - Мэдээллийн аюулгүй байдлын талаар хүлээх үүрэг хариуцлагыг мэдээллийн аюулгүй байдлын бодлогын дагуу хуваарилна
  - Эд хөрөнгө бүрийг хамгаалах, аюулгүй байдлын үйлдлүүдийг гүйцэтгэх үүрэг маш сайн тодорхойлогдсон байх ёстой.
  - Хэрэв шаардлагатай бол онцлог байр байгууламж, мэдээлэл боловсруулах хэрэгсэлд зориулсан нарийвчилсан удирдамжийг нэмсэн байна.
  - Эд хөрөнгийг хамгаалах болон бизнесийн тасралтгүй ажиллагааны төлөвлөлт хийх гэх мэт аюулгүй байдлын онцлог ажиллагааг гүйцэтгэх үүрэг, хариуцлагыг сайн тодорхойлсон байх ёстой.

# Байгууллагын дотоод зохион байгуулалт

(3/8)



- ***Мэдээллийн аюулгүй байдлын талаар хүлээх үүрэг, хариуцлагыг хуваарилах***

Хэний хариуцах ёстой орон зай, талбар болохыг нарийн тодорхойлсон байна; ялангуяа дараах зүйлсийг илүү анхаарна:

-нэг бүрчилсэн систем бүртэй холбоотой эд хөрөнгө болон аюулгүй байдлын үйл явцыг адилтгаж, тодорхойлсон байх ёстой;

-эд хөрөнгө, үйл явц бүрийг хариуцсан этгээдийг томилсон байх ёстой бөгөөд тэдний хариуцлагыг баримтжуулан баталгаажуулсан байна;

-таньж зөвшөөрөх түвшинг сайн тодорхойлж, баримтаар баталгаажуулсан байх ёстой.

# Байгууллагын дотоод зохион байгуулалт

## (3/9)



- ***Мэдээллийн аюулгүй байдлын талаар хүлээх үүрэг, хариуцлагыг хуваарилах***

-Ихэнх байгууллагад аюулгүй байдлыг хэрэгжүүлэх болон хөгжүүлэх, хяналтыг адилтган тодруулах ажиллагааг зохион байгуулах бүх үүрэг, хариуцлагыг мэдээллийн аюулгүй байдлын менежер хариуцан ажиллана.

-Гэхдээ нөөцөөр хангах, хяналтыг хэрэгжүүлэх үүрэг, хариуцлага ихэвчлэн бусад менежерүүдэд оногддог. Эд хөрөнгийг эзэмшиж буй хүмүүст нь хариуцуулдаг нийтлэг практик хэвшсэн. Энэ тохиолдолд эд хөрөнгийн өдөр тутмын хамгаалалт хангагдана.

# Байгууллагын дотоод зохион байгуулалт

## (3/10)



- ***Мэдээлэл боловсруулах аппарат хэрэгслүүдийг шалган зөвшөөрөх үйл явц.***
  - Мэдээлэл боловсруулах шинэ техник, аппарат хэрэгслүүдийг хянан шалгаж, ашиглаж болох эсэхийг зөвшөөрөх ажиллагааг бүрэн тодорхойлж, хэрэгжүүлсэн байна.

# Байгууллагын дотоод зохион байгуулалт

## (3/11)



- *Мэдээлэл боловсруулах аппарат хэрэгслүүдийг шалган зөвшөөрөх үйл явц.*

**Шалган зөвшөөрөх үйл явцад дараах заавруудыг анхааран үзэх ёстой:**

*-Шинэ хэрэгсэл бүрийн зорилго, ашиглалтыг хүлээн зөвшөөрсөн хэрэглэгчийн зөвшөөрлийг авсан байна. Түүнчлэн аюулгүй байдлын зохих бодлого, шаардлагуудыг хангахын тулд байгууллагын мэдээллийн системийн аюулгүй байдлыг хариуцсан менежерээс зөвшөөрөл авч болно;*

# Байгууллагын дотоод зохион байгуулалт

## (3/12)



- **Мэдээлэл боловсруулах аппарат хэрэгслүүдийг шалган зөвшөөрөх үйл явц.**

**-шаардлагатай бол мэдээллийн системийн бусад бүрдэл хэсгүүдтэй нийцэн ажиллаж чадахыг нь баталгаажуулахын тулд техник хэрэгслүүд болон программ хангамжийг шалгах ёстой (логик бөмбөг суулгасан эсэх, хамгаалалтын шаардлага хангаж байгаа эсэх гэх мэтээр);**

**-зөөврийн компьютер, гэрийн компьютер, зөөврийн бусад гар төхөөрөмж гэх мэт мэдээлэл боловсруулах хувийн хэрэгслүүдийг албаны мэдээлэл боловсруулахад ашиглах нь шинэ эмзэг байдлыг үүсгэж болох тул шаардлагатай хяналтыг тодруулж, хэрэгжүүлсэн байх ёстой.**

# Байгууллагын дотоод зохион байгуулалт

## (3/13)



- **Нууцлалын гэрээ**

-Байгууллагын мэдээлэл хамгаалах хэрэгцээг илэрхийлсэн нууцлалын болон нууцыг хамгаалах, үл задлах тухай гэрээний (холбогдох хүмүүстэй байгуулах) шаардлагуудыг боловсруулж байнга нягтлан шалгаж байх ёстой.

-Нууцлал болон нууцыг хамгаалах, үл задлах гэрээ нь нууц мэдээллийг хамгаалах шаардлагуудтай нийцсэн байх ёстой.

# Байгууллагын дотоод зохион байгуулалт

## (3/14)



- **Нууцлалын гэрээ**

Нууцлал болон нууцыг хамгаалах, үл задлах гэрээний шаардлагуудыг адилтган тодруулахын тулд дараах бүрдэл хэсгүүдийг анхааран үзсэн байх ёстой:

*-хамгаалагдсан байвал зохих мэдээллийн тодорхойлолт (жишээ нь, нууц мэдээлэл);*

*-гэрээний үргэлжилж болох хугацаа, түүний дотор нууцлалын дэглэмийг тодорхойгүй хугацаанд сахих шаардлагатай тохиолдлууд;*

*-гэрээний хугацаа дууссан тохиолдолд хийгдэх ёстой ажлууд;*

*-мэдээллийг хууль бусаар алдах, задлахаас сэргийлэхийн тулд гэрээнд гарын үсэг зурсан талуудын хүлээх үүрэг болон хийх ажиллагаа (“мэдэх шаардлагатай” гэх мэт);*

# Байгууллагын дотоод зохион байгуулалт

## (3/15)



- **Нууцлалын гэрээ**

- мэдээлэл, худалдааны нууц болон оюуны өмчийг эзэмшигчид, тэд нууц мэдээллийг хамгаалахад хэрхэн холбогдож байгааг;
- нууц мэдээллийг зөвшөөрөлтэй ашиглаж буй байдал, гэрээнд гарын үсэг зурсан талуудын мэдээлэл ашиглаж буй байдал;
- нууц мэдээллийг ашиглан хийж буй үйл ажиллагааг хянан шалгах, мониторинг хэрэгжүүлэх бүрэн эрх;
- мэдээллийг хууль бусаар задлах, алдах тохиолдол, нууц мэдээлэлтэй холбоотой зөрчлүүдийг мэдээлэх, тайлагнах үйл явц;
- гэрээний хугацаа дууссан тохиолдолд мэдээллийг буцаан авах болон устгах хугацаа;
- гэрээ зөрчсөн тохиолдолд хийх ёстой ажиллагаа;

Нууцлал болон нууцыг хамгаалах, үл задлах гэрээний шаардлагуудыг тодорхой мөчлөгтэйгээр, эсхүл уг шаардлагад нөлөөлж болох өөрчлөлт орсон тохиолдолд дахин нягтлан шалгаж байх ёстой

# Байгууллагын дотоод зохион байгуулалт

## (3/16)



- ***Эрх бүхий байгууллагуудтай харилцах***

-Эрх бүхий зохих байгууллагуудтай тодорхой харилцаа холбоо тогтоосон байх ёстой.

-Байгууллагууд эрх бүхий байгууллагуудтай (жишээ нь, хууль хамгаалах байгууллагууд, гал түймэртэй тэмцэх байгууллага, хянан шалгах байгууллага г.м) хэзээ, хэн, хэрхэн харилцаж байх, хуулийн заалтуудыг зөрчсөн байж болох аюулгүй байдлын бүртгэгдсэн будлиан, зөрчлийг цаг алдалгүй тайлагнах үйл явцыг тодорхойлсон дэг журамтай байх ёстой.

-Интернетээр дамжин орж ирсэн халдлагад өртсөн байгууллагууд довтолгооны эх сурвалжийг тодруулах, түүний эсрэг арга хэмжээ авахын тулд ямар нэг гуравдагч талын (жишээлбэл, Компьютерийн будлиан зөрчлийн эсрэг хариу үйлдэл хийх баг (CSIRT), Интернетийн үйлчилгээ үзүүлэгч юмуу харилцаа холбооны оператор г.м) тусламж авч болно.

# Байгууллагын дотоод зохион байгуулалт

## (3/17)



- ***Эрх бүхий байгууллагуудтай харилцах***

-Ийм харилцааг хангах нь мэдээллийн аюулгүй байдлын будлиан зөрчлийг удирдах удирдлага (13.2 хэсэг) болон бизнесийн тасралтгүй ажиллагаа, урьдчилан мэдэх боломжгүй зүйлсийг төлөвлөх үйл явцыг дэмжих шаардлагын нэг хэсэг байж болно.

-Байгууллагын заавал даган мөрдөх хууль, зохицуулалтад орж болох өөрчлөлтүүдийг урьдчилан мэдэх, түүнд бэлтгэхэд хууль тогтоох болон зохицуулах байгууллагуудтай тогтоосон харилцаа маш чухал. Эрх бүхий бусад байгууллагуудтай тогтоосон харилцаа мөн чухал ач холбогдолтой.

# Байгууллагын дотоод зохион байгуулалт

## (3/18)



- ***Ашиг сонирхлын бүлгүүдтэй харилцах***
  - Ашиг сонирхлын бүлэг, бусад мэргэжилтнүүд, аюулгүй байдлын форумууд болон мэргэжлийн холбоодтой зохих харилцаа тогтоосон байх ёстой.
  - Аюулгүй байдлын асуудлаар хамтын ажиллагаа, уялдааг сайжруулахын тулд мэдээлэл хамтран ашиглах гэрээг байгуулсан байж болно. Энэ гэрээ нь эмзэг мэдээллийг хамгаалах шаардлагуудыг тодруулсан байх ёстой.

# Байгууллагын дотоод зохион байгуулалт

## (3/19)



- **Ашиг сонирхлын бүлгүүдтэй харилцах**

Ашиг сонирхлын бүлгүүдтэй харилцах болон форум, мэргэжлийн холбооны гишүүн байх нь дараах ач холбогдолтой:

*-мэдээллийн аюулгүй байдлын шилдэг туршлагын (практик) талаар мэдлэгийг дээшлүүлэх, аюулгүй байдлын сүүлийн үеийн мэдээллийг цаг алдалгүй олж авах;*

*-мэдээллийн аюулгүй байдлын ойлголт төлөвшиж байгаа, эсхүл төгс төлөвшсөн гэдгийг баталгаажуулах;*

*-урьдчилсан анхааруулга, зөвлөгөө болон довтолгоо, эмзэг байдалтай холбоотой залруулгыг хүлээн авах;*

*-мэдээллийн аюулгүй байдлын мэргэжилтний зөвлөгөө авах;*

*-шинэ технологи, бүтээгдэхүүн, аюул болон эмзэг байдлын талаар мэдээллийг хамтран ашиглах, солилцох;*

*-мэдээллийн аюулгүй байдлын будлиан, зөрчилтэй тулгарсан тохиолдолд бусадтай харилцах боломжийг хангах*

# Байгууллагын дотоод зохион байгуулалт

## (3/20)



- **Мэдээллийн аюулгүй байдлын бие даасан нягтлан шалгах ажиллагаа**
- Төлөвлөсөн хугацаанд болон том өөрчлөлт орсон тохиолдолд байгууллагын мэдээллийн аюулгүй байдлыг удирдах болон хэрэгжүүлэх хандлагыг шалгах (жишээлбэл, мэдээллийн аюулгүй байдлын хяналтын зорилго, хяналтууд, бодлого, үйл явц болон дэг) бие даасан хөндлөнгийн нягтлан шалгах ажиллагаа хэрэгжүүлж байх ёстой.
- Бие даасан нягтлан шалгах ажиллагааг удирдлага санаачлан хэрэгжүүлнэ. Хөндлөнгийн энэ нягтлан шалгах ажиллагаа нь байгууллагын мэдээллийн аюулгүй байдлын хандлагын хэрэглэхэд тохиромжтой байдал, нийцэл, үр дүнтэй байдлыг тодруулахад зайлшгүй шаардлагатай. Нягтлан шалгах энэ ажиллагаа нь аюулгүй байдлын хандлагыг, үүний дотор бодлого болон хяналтын зорилгыг боловсронгуй болгох боломжийг үнэлсэн байна.

# Байгууллагын дотоод зохион байгуулалт

## (3/21)



- ***Мэдээллийн аюулгүй байдлын бие даасан нягтлан шалгах ажиллагаа***
- Хянагдаж буй нэгжид хамааралгүй хувь хүмүүс, тухайлбал аудитын мэргэжилтэн, бие даасан менежер, эсхүл хөндлөнгийн байгууллагын ажилтнууд нягтлан шалгах энэ ажиллагааг хэрэгжүүлнэ. -зохих дадал, туршлагатай байх.
- Хөндлөнгийн бие даасан нягтлан шалгах ажиллагааны үр дүнг баримтаар бэхжүүлж удирдлагад тайлагнана. Энэ тайланг батлах ёстой.
- Хэрэв мэдээллийн аюулгүй байдлын бодлогын баримт бичигт тусгагдсан мэдээллийн аюулгүй байдлын чиглэлтэй байгууллагын мэдээллийн аюулгүй байдлын удирдлага, хэрэгжүүлэх хандлага зөрчилдсөн, гажсан нь бие даасан нягтлан шалгах ажиллагааны үр дүнд тогтоогдвол удирдлагын зүгээс залруулах арга хэмжээ авч хэрэгжүүлнэ.

# Анхаарал тавьсанд баярлалаа

[www.sssmn.com](http://www.sssmn.com)

[info@sssmn.com](mailto:info@sssmn.com)

70113151