АРХИВЫН ЕРӨНХИЙ ГАЗРЫН
ДАРГЫН ТУШААЛ

2012 оны 07 сарын 27 өдөр Дугаар А/79 Улаанбаатар хот

"Архивын мэдээллийн аюулгүй байдлыг хангах тухай" гарын авлагыг батлах тухай

Мэдээллийн технологи-Аюулгүй байдлын аргууд-Мэдээллийн аюулгүй байдлын удирдлагын үйл ажиллагааны дүрэм MNS ISO 17799:2007, Мэдээллийн технологи-Аюулгүй байдлын аргууд-Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо-шаардлага MNS ISO/IEC 27001:2009 стандартыг тус тус үндэслэн, Архивын ерөнхий газрын Мэдээллийн аюулгүй байдлын цогц бодлого, дэг, журмыг хэрэгжүүлэх зорилгоор ТУШААХ нь:

1. "Архивын мэдээллийн аюулгүй байдлыг хангах тухай" архивын ажилтнуудад зориулсан гарын авлагыг хавсралт ёсоор баталсугай.

2. Дээрхи гарын авлагыг 2012 оны 10 сарын 1-ний өдрөөс эхлэн өдөр тутмын үйл ажиллагаандаа мөрдөж ажиллахыг нийт төрийн архивын ажилтнуудад үүрэг болгосугай.

3. Гарын авлагыг үйл ажиллагаандаа мөрдүүлэх талаар удирдлага, зохион байгуулалтын арга хэмжээ авч, хэрэгжилтэнд байнгын хяналт тавьж, үр дүнг тооцож ажиллахыг төрийн архивын дарга нарт даалгасугай.

4. Гарын авлагыг хэвлүүлж, төрийн архивуудад шуурхай хүргүүлэхийг Захиргааны удирдлагын хэлтсийн дарга Д.Батхуяг, Мэдээллийн технологийн хэлтсийн дарга Ч.Оюунчимэг нарт тус тус үүрэг болгосугай.

5. Гарын авлагыг хэвлүүлэхэд шаардагдах зардлыг төсвөөс гаргахыг Ерөнхий ня-бо Б.Чинбатад зөвшөөрсүгэй.

ДАРГА Д.ӨЛЗИЙБААТАР

Архивын ерөнхий газрын даргын
2012 оны 07 сарын 27-ны өдрийн
А/79 дугаар тушаалын хавсралт

“Архивын мэдээллийн аюулгүй байдлыг хангах тухай” архивын ажилтнуудад зориулсан гарын авлага

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДАЛ /МАБ/ ГЭЖ ЮУ ВЭ?

MNS ISO/IEC 27001:2009

- “Мэдээ, мэдээлэл боловсруулах хэрэгсэл, холбогдох дэд бүтцийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдал, тасралтгүй ажиллагаа, мөшгөн ашиглагдах шинж, жинхэнэ байх шинж болон найдвартай байдлыг тодорхойлох, бий болгох, хадгалж байхтай холбоотой бүх асуудлууд”

ӨРГӨН УТГААРАА:

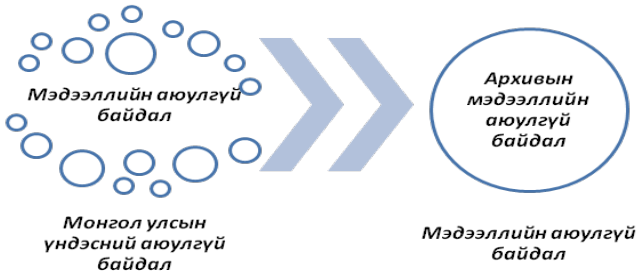
- “Нийгэм, институт, байгууллагын мэдээллийн орчины хамгаалагдсан байдал”
- “Жам ёсны болон зохиомол шинжтэй, санаатай болон санамсаргүй үйлчлэлээс мэдээлэл, түүнийг дэмжих дэд бүтцийн хамгаалагдсан байдал”

ЯВЦУУ УТГААРАА:

- “Өгөгдөл, мэдээ, мэдээлэл, баримт материал, аппарат хэрэгслийг хууль бусаар, зүй бусаар ашиглах, өөрчлөх, устгах гэмтээх, хандах боломжийг хаахаас сэргийлж авсан арга хэмжээ”,
- “Мэдээлэл тоног төхөөрөмжийг аюул заналхийллээс хамгаалах, эмзэг, сул талыг нь буруугаар ашиглахаас хамгаалах боломж олгож буй урьдчилан сэргийлэх үйл ажиллагаа, үйл явц, үйлдлүүд”

МАБ-ыг хангахын тулд хамгаалагдах бүх эд хөрөнгийг тодорхойлох, ангилах, үнэ цэнийг тогтоох, заналхийлж буй аюул, эрсдлийг тодорхойлох, МАБ-ын үзэл баримтлал, бодлого, хөтөлбөр, дэг журам гаргаж, хэрэгжүүлэх, технологийг сайжруулах зэрэг арга хэмжээг авах ёстой.

Мэдээллийн аюулгүй байдал нь Монгол улсын үндэсний аюулгүй байдлын бүрэлдэхүүн хэсэг бөгөөд архивын мэдээлэл нь төрийн мэдээллийн гол тулгуур, нөөц суурь юм.



МАБ-ЫГ ХАНГАХ
/АЮУЛГҮЙ БАЙДЛЫН ДАВХАРГА/

АЮУЛ, ЗАНАЛХИЙЛЭЛ

Өргөн тохиолддог халдлагууд:

- Нянтай програмаар халдварлуулах
- Өгөгдөл хулгайлах
- Өгөгдлийг өөрчлөх, устгах, нэмж хасах, засварлах
- Компьютер, мэдээллийн техник, тоног төхөөрөмжийг хууль бусаар ашиглах
- Сүлжээнд хууль бусаар хандах, нэвтрэх
- Веб сайтыг эвдлэх
- Бусад.....

Довтолгооны аргууд:

- Мэдээллийг дундаас барьж авах
- Дотоод сүлжээний тухай мэдээлэл олж авах
- Програм хангамж болон техник хэрэгслийг хулгайлах, ашиглах, шамшигдуулах
- Цахилгаан соронзон долгионыг барьж авах
- Үйлдлийн систем, програм хангамжийн эмзэг зангилаа уруу довтлох, ачаалах
- Хууль бусаар нэвтрэх
- Байгууллагын хогийн савыг ухах /хаягдсан цаас, диск, дискет олж, ашиглах/
- Ажилтнуудыг худалдаж авах

- Өөрийн биеэр нэвтрэн орох
- Толь сайт бэлтгэж мэдээлэл цуглуулах
- Фишинг
- Бусад.....

Үүсч болох аюул:

- Өгөгдлийн бүрэн бүтэн байдал алдагдах
- Техник хэрэгсэл, тоног төхөөрөмжид эвдрэл гэмтэл гарах
- Нууцлалтай өгөгдлийн нууцлал алдагдах
- Үйлчилгээ тасалдах
- Хяналтаа алдах

АЮУЛУУД БА ХАМГААЛАЛТ

Системийн нийлүүлэгч, үйлдвэрлэгчийн алдаа	•Өөр үйлдвэрлэгчийн төхөөрөмж дээр хуулбар хадгалж байна.
Тээгчийг ашиглах, хулгайлах	•Хоёр дахь тээгч дээр хуулбарыг буулгасан байна.
Үйл ажиллагааны алдаа	•Өөр хэсэг дээр хуулбар хадгалсан байна.
Байгалийн гамшиг	•Газар зүйн хувьд алслагдсан байрлалд хуулбарыг хадгалсан байна.
Кибер халдлага, довтолгоон	•Мэдээллийн аюулгүй байдал, системийн аюулгүй байдлыг хангаж ажиллана, МАБ-ын бодлого, дэг, програм-техникийн арга хэмжээг хэрэгжүүлнэ.
Гэмт санаа бодолтой хэрэглэгч	•Архивчыийн хяналт дор хамгаалагдсан төхөөрөмжид хуулбарыг хадгална.

АЕГ-ЫН МАБ-ЫН ЦОГЦ БОДЛОГО,
ДЭГ, ЖУРАМ

Нийт ажилтнуудын мөрдөж ажиллах бодлого, дэг, журмууд	
1	АЕГ-ын Мэдээллийн аюулгүй байдлын үндсэн бодлого
2	Мэдээллийн нууцлалын бодлого
3	Хортой код, вирусын эсрэг бодлого
4	Цахим шуудан ашиглах бодлого
5	Цахим захидал ашиглах, хадгалах бодлого
6	Цахим захиаг автоматаар дамжуулах бодлого
7	Мэдээллийн аюулгүй байдлын зохистой хэрэглээний бодлого
8	Нууц үгийн журам
9	Зөөврийн тээгчтэй ажиллах журам
10	Байгууллагуудтай цахим бичиг солилцох журам
11	Хортой код, вирусээс хамгаалах дэг
Мэдээллийн технологи хариуцсан ажилтнуудын мөрдөж ажиллах бодлого, дэг, журмууд	
1	АЕГ-ын Мэдээллийн аюулгүй байдлын үндсэн бодлого
2	Шифрлэлтийн бодлого
3	Серверийн аюулгүй байдлын бодлого
4	Серверийг хортой кодоос хамгаалах бодлого
5	Сүлжээний чиглүүлэгчийн аюулгүй байдлын бодлого
6	Өгөгдлийн сангийн нууц үгийн бодлого
7	Зайнаас хандах хандалтын бодлого
8	Интернет холболттой гар утас ашиглан АЕГ-ын сүлжээ, системд хандах /dial-in/ хандалтын бодлого
9	Интернетийн DMZ дахь төхөөрөмжийн бодлого
10	Сүлжээний хамгаалалтын бүсийн /DMZ/ аюулгүй байдлын бодлого
11	АЕГ-ын эмзэг байдлыг шинжлэх, аудит хийх бодлого
12	АЕГ-т програм, тоног төхөөрөмж нийлүүлэгчийн талаар баримтлах бодлого
13	АЕГ-т гаднаас авч буй үйлчилгээний бодлого
14	Эрсдлийн үнэлгээний бодлого

АЕГ-ЫН МАБ-ЫН БОДЛОГЫН ХАМРАХ ХҮРЭЭ

МАБ-ЫН ТАЛААР НИЙТ АЖИЛТНУУДЫН ХҮЛЭЭХ ҮҮРЭГ

НЭГ. ЕРӨНХИЙ ҮҮРЭГ, ХАРИУЦЛАГА

1. Архивын Internet/Intranet/Extranet-тэй хамааралтай систем дээр байгаа бүх мэдээлэлд хууль бусаар хандах аливаа оролдлогоос сэргийлэх, шаардлагатай бүх арга хэмжээг ажилтан бүр авах үүрэгтэй.

2. МАБ-ын бодлого, дэг, журам, зааврууд ыг судалж үйл ажиллагаандаа өдөр тутам дагаж мөрдөнө.

3. Ажил үүргээ гүйцэтгэхдээ зөвхөн зөвшөөрөгдсөн програм хангамжуудыг ашиглана.

4. Сүлжээгээр элдэв тоглоом, видео бичлэг, дуу хөгжим, клип татах, компьютерт суулгах, ашиглах, бусдад дамжуулахыг хориглоно.

5. Өөрийн компьютерт байгаа мэдээллээ ажлын ба хувийн гэж ангилан хадгалах хэрэгтэй.

6. Өөрийн эзэмшилд буй компьютер, бусад техник хэрэгсэл, эд хөрөнгөд хайр гамтай харьцах, ашиглалтын заавар, журмыг хатуу баримтлана.

7. МАБ-тай холбогдох будлиан зөрчил, маргаан, сэжиг бүхий байдал илэрсэн тохоилдолд нэн даруй МАБ хариуцсан ажилтанд мэдэгдэж байна.

8. Бүх компьютер, зөөврийн компьютерийг 10 минутаас доош хугацаанд, эсвэл ажлаа хийхийг больсон үед шууд автоматаар түгждэг дэлгэцийн түгжээгээр (screen saver) хамгаална.

9. Ажилтан компьютерээ ашиглахгүй асаалттай орхих үедээ дэлгэцийг түгжиж байх. Үүний тулд Windows төрлийн үйлдлийн системд цонх+L /цонхны дүрстэй товч/ товчны хослолыг дарна.

10. Архивын ажилтнууд нууцад хамаарах эсвэл хаалттай мэдээллийг зохих ёсоор хамгаалахын тулд өөрсдийн ухамсар, ёс зүй, эрүүл ухаанд тулгуурласан арга хэмжээг авч байна.

ХОЁР. НУУЦ ҮГИЙН БОДЛОГО

Ерөнхий зарчим:

1. Компьютертээ хандах нууц үг, цахим шуудангийн системд хандах эрхийн нууц үг, мэдээллийн сан, сүлжээнд нэвтрэх нууц үг ялгаатай байх.

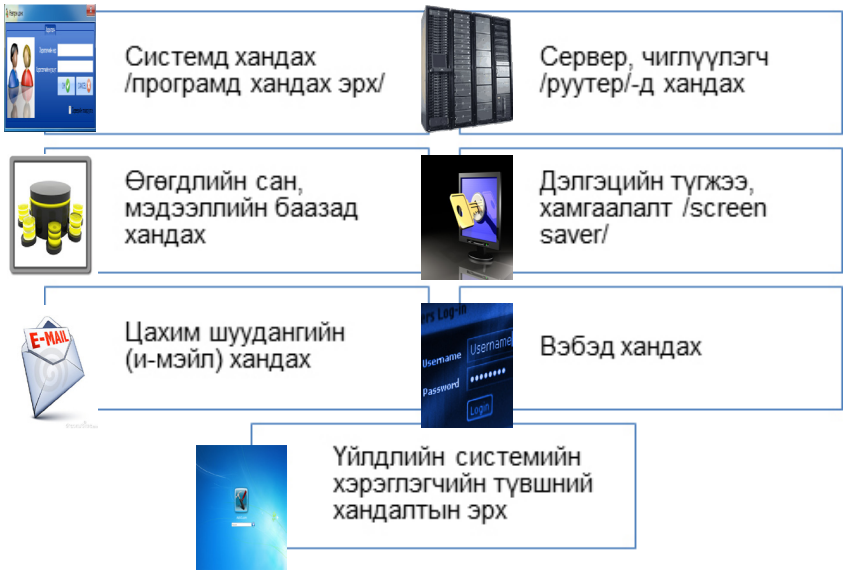
2. Системд нэвтрэх хэрэглэгчдэд шаардлагагүй бол өндөр эрхтэй (administrator төрлийн) хэрэглэгч үүсгэхгүй байх

3. Системийн түвшний бүх нууц үгийг (ж.нь, root, enable, NT admin, application administration accounts) улирал тутамд сольж байх

4. Үндсэн системийн түвшний нууц үг нь тухайн мэдээллийн технологийн ажилтан, МАБ-ын ажилтны удирдлагад байх

5. Давуу эрх бүхий хэрэглэгчдийн хандалтын эрхийн нууц үг нь давтагдашгүй шинжтэй байх

Зорилгоос хамаарч нууц үгийг ялгаатай тогтооно. Үүнд:



Нууц үг бол таны цахим мэдээллийн аюулгүй байдлыг хангах хамгийн анхан шатны, энгийн хамгаалалтын арга юм.

Ямар нууц үг аюулгүй вэ?

- Том болон жижиг үсгүүдийн аль алийг нь хослуулсан,
- Кирил болон латин үсэг оролцуулсан,
- Тоо болон тэмдэгтүүд хавсарсан,
- Аль нэг хэл дээр орчуулагдахааргүй,
- Хувийн мэдээлэл ороогүй, хувийн мэдээлэл дээр тулгуурлаагүй байх (төрсөн он сар өдөр, утасны дугаар, регистр, нас... гм)
- 12-оос дээш үсэг, тоо, тэмдэгт орсон байх.

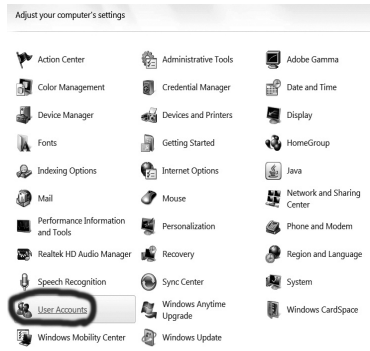
Жишээ нь: KbrАБ2012_Чо

Ингэхдээ та өөрөө амархан санахаар нууц үгийг үүсгэх шаардлагатайг анхааараарай.

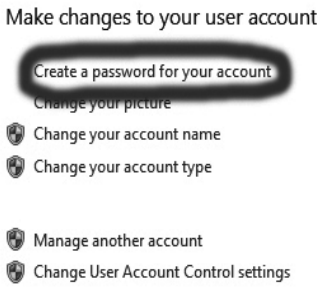
Яаж нууц үгээ үүсгэх вэ?

Нууц үгээ үүсгэхдээ:

Control Panel цэс рүү орох



User account-г сонгоно

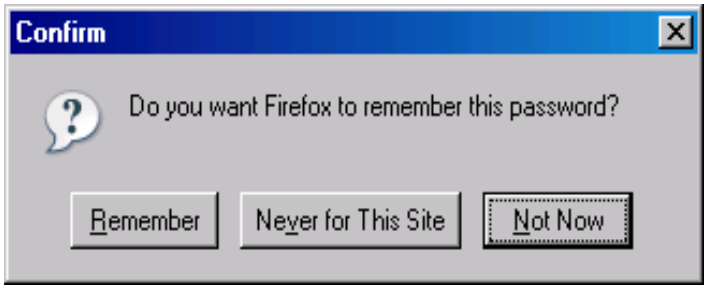


Create a password for your account-г сонгоно

Нууц үгээ бичиж доод талын нүдэнд баталгаажуулсанаар үүснэ

Хэрхэн нууц үгээ хамгаалах вэ?

- Нууц үг нь найдвартай, бусад хүн таахад хялбар биш байх хэрэгтэй.
- Хэрэв ямар нэг програм ашиглах явцад чинь “remember password?” /“нууц үгээ сануулахуу?/ гэсэн асуулт гарч ирвэл нууц үгээ бүү сануул.



- Нууц үгээ цаасан дээр бичиж, ажил дээрээ хадгалж болохгүй.
- Тусгай шифрлэлт ашиглалгүйгээр нууц үгээ компьютерийн файл, систем, зөөврийн тээгчүүдэд хадгалахыг цээрлэ.

- Нууц үгээ алдсан, бусад этгээд мэдсэн, эвдэлсэн сэжиг илрэх тохиолдолд нэн даруй МАБ-ын ажилтанд мэдэгдэж тэр дор нь өөрчилнө.
- Нууц үгийг (email, web, desktop computer гм) 4 сар тутамд өөрчилж байна.
- Нууц үгээ найдвартай хадгалж бусдад бүү дэлгэ. Эрх олгогдсон бүх хэрэглэгчид нууц үг, эрхийнхээ аюулгүй байдлыг хангах үүрэгтэй.

Юуг хориглох вэ?

- Архивын аль нэг хандах эрхэд ашиглаж буй нууц үгийг хамааралгүй хандах эрхэд ашиглах, гадна, дотны хүнд өгөх, задлахыг хориглоно.
- Ашиглаж буй нууц үгийг хэн нэгэнтэй бүү хуваалц (захиргааны ажилтнууд, нарийн бичгийн дарга г.м). Зөвхөн МАБ-ын ажилтны шаардсанаар өгч болох бөгөөд шаардагдах шалгалт, хяналт дууссаны дараа нууц үгээ өөрчилнө.

Хэрэв хэн нэгэн янз бүрийн чухал шаардлага дурдан нууц үгийг тань мэдэхийг хүсвэл яах вэ?

- Зөвхөн МАБ-ын ажилтны шаардсанаар өгч болно. Бусад тохиолдолд МАБ-ын ажилтанд мэдэгдэнэ.
- Холбогдох ажиллагаа, хяналт, шалгалт, дууссаны дараа нууц үгээ өөрчилнө.

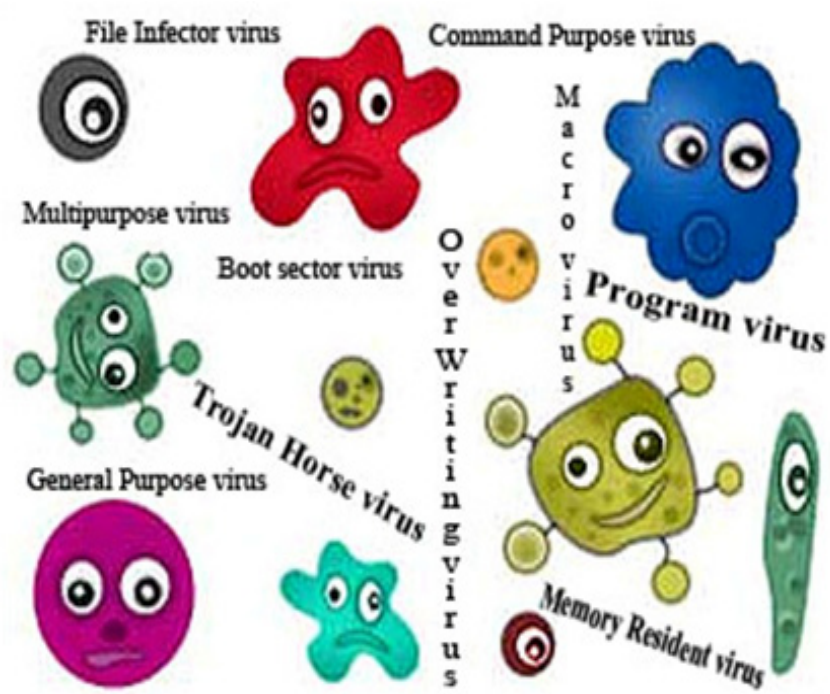
ГУРАВ. ХОРТОЙ КОД, ХУУЛЬ БУС ХӨДӨЛГӨӨНТ КОД, ВИРУСЫН ЭСРЭГ БОДЛОГО

Хортой код, вирус гэж юу вэ?

Компьютерт зөвшөөрөлгүйгээр нэвтрэх чадвартай, тодорхой үүрэг, зорилготой програмыг вирус гэж ойлгож болно. Маш олон төрлийн вирус бий.

Хөдөлгөөнт код гэдэг нь нэг компьютерээс нөгөө компьютерт шилжиж, улмаар хэрэглэгчийн бага зэргийн оролцоотой юмуу огт оролцоогүйгээр тодорхой функцийг автоматаар гүйцэтгэдэг, хэрэгжүүлдэг програм хангамжийн кодыг хэлдэг.

Компьютерийн нянтай програм, сүлжээний өт, трояны морь, логик бөмбөг гэх мэт хортой код, програм болон хөдөлгөөнт кодын нөлөөлөлд програм хангамж, мэдээлэл боловсруулах аппарат хэрэгслүүд өртөмхий, эмзэг байдаг.



Хортой код, хууль бус хөдөлгөөнт код, вирусын уршиг, хор хөнөөл юу вэ?

- Компьютерийн ажиллагааг удаан болгох
- Файл, програм устгах, гэмтээх
- Файл, хавтсыг нуугдмал байдалд оруулах
- Зарим үйлдлүүдийг хаах
- Мэдээлэл хулгайлах
- Үйлдлийн системийг гэмтээх
- Бусад хортой үйлдлүүд

Ямар замаар дамждаг вэ?

Flash disk болон зөөврийн бусад тээгчээр

Интернэт, интранет болон дотоод сүлжээгээр

E-mail-ээр

Хамрах хүрээ: Дотоод, гадаад сүлжээнд холбогдсон ширээний болон зөөврийн компьютерууд, file/ftp/tftp/proxy серверүүд, компьютерт суурилсан

бусад тоног төхөөрөмж, интернетээр дамжуулан архивын сүлжээнд холбогддог гар утас, тооцоолох хэрэгслүүд хамаарна.

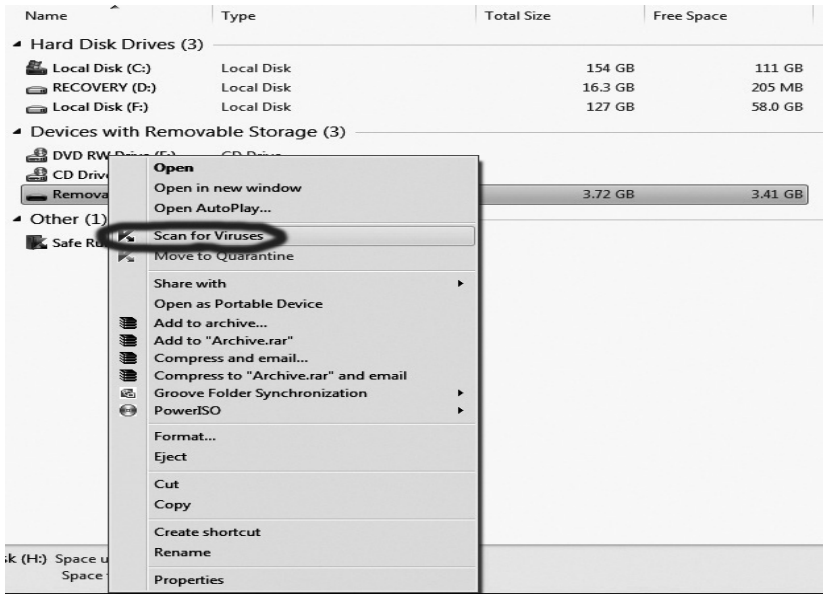
Хортой код, вирусээс хамгаалахад бариmтлах ерөнхий зарчим:

1. Архивын бүх компьютер дээр нэгдсэн нэг стандартын дагуу Интернет аюулгүй байдлын юмуу вирусын эсрэг програм хангамж суулгаж, хортой код, вирусын хайлтыг тогтмол хийн ажиллуулж байна.
2. Бүх сервер дээр хортой код, вирусээс хамгаалах серверийн хувилбарыг заавал суулгаж ажиллуулна.
3. Онц чухал өгөгдөл болон системийн тохируулгыг байнга нөөцлөн хуулж аюулгүй газарт хадгалж байна.
4. Архивын сүлжээнд аливаа нэг хортой код (вирус, өт, троян, цахим зардлын бөмбөг, логик бөмбөг г.м) үүсгэх, оруулах, тараах аливаа санаархал, оролдлогыг хатуу хориглоно.
5. МАБ-ын ажилтан нь Вирус дамжих замуудыг тодорхой хэмжээгээр хаах, хязгаарлах эрхтэй байна.

Хортой код, вирусээс хамгаалахын тулд ажилтан юу хийх ёстой вэ?

- Компьютерт суулгасан вирусын эсрэг програмыг байнга Update хийж шинэчилж байх хэрэгтэй. Антивирусын програмыг түр зогсоосон үед вирус дамжиж болох аливаа хэрэглээний програмыг ажиллуулж болохгүй.
- Зөөврийн дискүүд, тухайлбал флэш, DVD, CD, бусад тээгчийг ашиглахын өмнө заавал шинжилж, гүйлгэн скандаж шалгана.

Скан хийхийн тулд my computer> mouse-ны баруун товч> scan for viruses-ийг сонгоно.



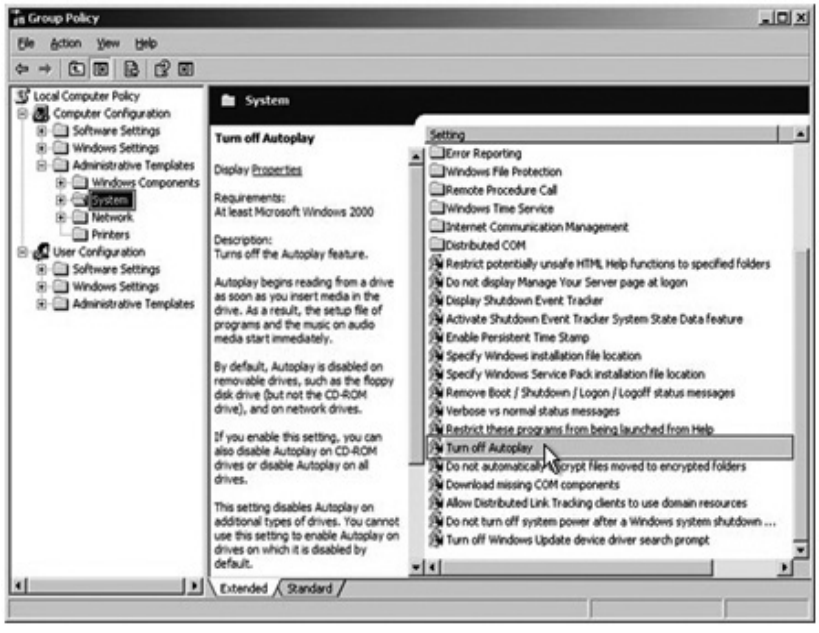
- Мөн цахим болон оптик тээгч дээр байгаа, сүлжээгээр дамжуулан хүлээн авсан аливаа файл, цахим захианы хавсралт, татан авсан зүйлсийг хэрэглэхээсээ өмнө хортой код, вирус агуулсан эсэхийг заавал шалгаж байх хэрэгтэй.
- Майл, мессенжерээр болон үл мэдэх, итгэлгүй, эсвэл сэжигтэй эх сурвалжаас ирсэн цахим захианд хавсаргасан аливаа файл, макросыг хэзээ ч нээж болохгүй бөгөөд нэн даруй устгаж дараа нь хогийн сав (trash)-аас давхар устгана.
- Спам, үргэлжилсэн болон бусад хог захиаг цааш нь илгээлгүй устгаж байна.
- Үл мэдэх, эсхүл сэжигтэй эх сурвалжаас файл, програм хангамж татаж авахыг хориглоно.
- Ажил хэргийн онцгой шаардлага байхгүй бол унших бичих эрхтэйгээр дискийг дундаа хамтран ашиглаж (disk sharing) болохгүй.

Flash дискний вирусээс сэргийлэх арга

Flash, CD, DVD, бусад тээгчийг компьютерт холбох үед autorun команд автоматаар ажиладаг бөгөөд энэ үйлдлээр вирус дамждаг. Иймд shift товчоо дарж байгаад Flash дискээ компьютерт хийж байх эсвэл Autorun командыг зогсоож идэвхгүй болгох шаардлагатай.

Autorun-г идэвхгүй болгохын тулд дараах тохиргоог хийх шаардлагатай.

1. Start - Run ажиллуулаад “gpedit.msc” гэж бичээд OK дарна. Ингэхэд Group Policy цонх гарч ирнэ.
2. Group Policy цонхны Computer Configuration- Administrative Templates - System гэсэн дээр дараад баруун талын хэсэг дэх тохиргоонууд дундаас Turn Off Autoplay гэсэн тохиргоог нээнэ.
3. Тэгээд тохиргоог **Enabled** болгоод **“All Drives”** гэсэн сонголтыг хийнэ.



Хортой код, вирус илэрсэн тохиолдолд юу хийх вэ?

- Хортой код, вирус суусан компьютерийг сүлжээнээс нэн даруй салгана.
- Антивирусын програмын тусламжтайгаар хортой код, вирусыг шалгаж цэвэрлэн, устгаж нягтална.
- Үүний дараа сүлжээнд холбоно.
- Энэ талаар МАБ-ын ажилтанд мэдээлнэ.

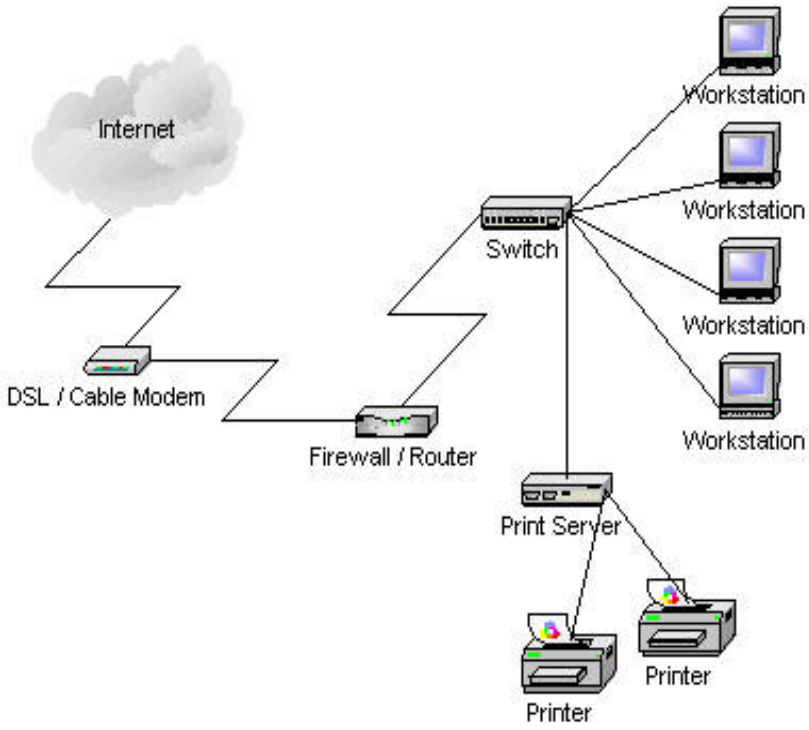
ДӨРӨВ. ЦАХИМ ШУУДАН, СҮЛЖЭЭ АШИГЛАХ БОДЛОГО

Ерөнхий зарчим:

1. Архивын сүлжээний хэрэглэгчдийн үүсгэж буй албаны бүх өгөгдөл нь тухайн архив / байгууллага/-ын өмч мөн.
2. Архивын /холбогдох удирдлагын/ даргын тушаалаар эрх олгогдсон ажилтнууд МАБ-ыг хангах, систем, сүлжээнд үйлчилгээ хийх зорилгоор сүлжээ, систем, тоног төхөөрөмж, мэдээллийн урсгалыг дурын үедээ хянах, нягтлах эрхтэй байна.
3. Архивын ажилтнууд архивын цахим шуудангийн систем ашиглан хадгалсан, явуулсан болон хүлээн авсан цахим захиандаа хувийн халдашгүй байдлын эрх эдлэхгүй.
4. Архив шаардлагатай бол цахим шуудангийн систем дэх захидал, мэдээллийг урьдчилан мэдэгдэлгүйгээр хянан шалгаж болно. Гэхдээ архив бүх цахим захиа, мэдээллийг хянах үүрэггүй.

Архивын цахим шуудангийн системээр ямар мэдээлэл дамжуулахыг хориглох вэ?

- Архивын цахим шуудангийн системийг бусдыг доромжилж гутаах, нэр хүндийг унагаах, бусад зүй бус агуулгатай захидал илгээхэд ашиглах.
- Хуулиар тогтоосон төрийн ба хувийн нууцад хамаарах мэдээ мэдээлэл, мөн архивын байгууллагын нууцад хамаарах мэдээ, мэдээлэл, өгөгдөл, ашиглалтын хязгаартай баримтын талаархи мэдээ, мэдээллийг бусдад дамжуулах.
- Ажилтнууд, архивын нэрийн өмнөөс цахим захиаг нийтэд тараах буюу илгээхдээ хувийн ямар нэг санал дүгнэлт оруулах, мэдээлэл нэмэх, өөрчлөх
- Архивын МАБ-ын ажилтны зөвшөөрөлгүйгээр архивын цахим захиаг гадагш нь автоматаар дахин дамжуулан илгээх



Ажилтан архивын цахим шуудан, сүлжээ ашиглахдаа ямар үүрэг хүлээх вэ?

- Ажилтнууд АЕГ-ын дотоод сүлжээнээс гадны сүлжээ рүү цахим захиа илгээхдээ маш болгоомжтой хандах ёстой.
- Архивын цахим шуудангийн аль нэг хаягаас бусдыг доромжилж гутаах, нэр хүндийг унагаах, бусад зүй бус агуулгатай захидал хүлээн авсан ажилтан энэ тухай шууд удирдсан даргадаа нэн даруй мэдэгдэнэ.
- Ажилтнууд үл таних илгээгчээс ирсэн цахим захиа, түүний хавсралтыг нээхдээ онцгой анхаарч, шаардлагагүй бол ийм захиаг уншилгүй шууд устгаж байна.
- Сүлжээгээр буюу архивын цахим шуудангаар ирсэн архивын үндсэн үйл ажиллагаа, үйлчилгээ, нийтийн санал хүсэлт, гомдол, өргөдлийг хариуцсан ажилтан бүр заавар, журмын дагуу бүртгэн, хадгалж, боловсруулах үүрэгтэй.

Сүлжээ ашиглаж байгаа хэрэглэгчдэд юуг хорих вэ?

- Сүлжээнд байгаа бусдын болон сервер компьютерийн мэдээлэл /file, folder/, програмыг зөөх, устгах түүнд эвдрэл гэмтэл учруулах.
- Сүлжээнд залгагдсан /залгагдаагүй/ компьютер болон төхөөрөмжийг дур мэдэн салгах /залгах/, сервер болон сүлжээний төхөөрөмжүүдийг дур мэдэн асаах, унтраах, оролдох, өөрчлөлт хийх, сүлжээний тохиргоог оролдох, өөрчлөх

Хэрэв сүлжээнд нэмэлт хэрэглэгч холбох, өөрчлөлт оруулах, сервис

хийлгэх шаардлагатай бол сүлжээ хариуцсан мэргэжилтэнд хандана.

ТАВ. ЗӨӨВРИЙН ТЭЭГЧ АШИГЛАХ БОДЛОГО

1. АЕГ-ын ажилтнууд АЕГ-т бүртгэлтэй ажлын зориулалттай зөөврийн тээгчийг зөвхөн албан ажлын компьютерт ашиглана.
2. Дээд шатны байгууллагаас биеэр авчирч өгөхийг хүссэн, эсхүл ажил үүргийн дагуу зайлшгүй шаардлага гарсан тохиолдолд л онц чухал мэдээллийг зөөврийн тээгч дээр хуулбарлаж болно.
3. Хэрэв онц чухал мэдээллийг зөөврийн тээгч дээр хуулбарлан хадгалж байгаа бол АЕГ-ын шифрлэлтийн бодлогод заасны дагуу шифрлэнэ.
4. Архивын МАБ-ын ажилтны зөвшөөрөлгүйгээр архивт бүртгэлтэй зөөврийн тээгчийг байгууллагаас гадуур байгаа өөр бусад компьютерт холбох, түүн дээр ашиглахыг хориглоно.

МАБ-ЫН БОДЛОГО, ДЭГ, ЖУРАМ ЗӨРЧСӨН АЖИЛТНУУДАД ХҮЛЭЭЛГЭХ ХАРИУЦЛАГА

Архивчид, ажилтнууд, гэрээгээр ажиллагсад, гуравдагч талын хэрэглэгчид МАБ-д учирч буй аюул заналхийлэл, эрсдэл болон өөрсдийн хүлээх хариуцлага, гүйцэтгэх үүргээ ухамсарлаж, өдөр тутмын үйл ажиллагааны явцад МАБ-ыг ханган ажиллах үүрэгтэй.

Ажиллагсад архивын өгөгдөл, мэдээлэл үүсгэх, хүлээн авах, боловсруулах, дамжуулах, хадгалах, хамгаалахтай холбоотой хууль бус үйл ажиллагаа үйлдсэн, нууцын зэрэглэлтэй, хаалттай, мэдээ, мэдээлэл, баримт материал, өгөгдлийг санамсаргүй болон санаатайгаар задалсан, МАБ-ын бодлого, дэг, журмуудыг зөрчсөн тохиолдолд зөрчлийн шинжийг харгалзан дараах хариуцлага хүлээлгэнэ:

- Сахилгын арга хэмжээ авах
- Ажлаас халах
- Иргэний хууль, Эрүүгийн хуулийн дагуу хариуцлага хүлээлгэнэ.