ХУУЛЬ САХИУЛАХЫН ИХ СУРГУУЛИЙН мэдээллийн АЮУЛГҮЙ БАЙДЛЫН ӨНӨӨГИЙН НӨХЦӨЛ БАЙДАЛ

Г.Лхагвамаа
Хууль сахиулахын удирдлагын академийн Аюулгүй байдлын удирдлага, стратегийн профессорын багийн дэд профессор, доктор /Ph.D/, дэд хурандаа
В.Энхтайван
ХСИС-ийн Мэдээлэл, технологи, аюулгүй байдлын албаны дарга, цагдаагийн дэд хурандаа
Д.Ариужин
Цагдаагийн сургуулийн Цагдаагийн эрх зүйн тэнхимийн ахлах багш, цагдаагийн ахмад

Товч агуулга: Энэхүү илтгэлийн хүрээнд Их сургуулийн мэдээллийн аюулгүй байдлыг хангах үйл ажиллагааны эрх зүйн зохицуулалт, өнөөгийн нөхцөл байдал болон “Check point” ашиглан сүлжээний урсгалд хийсэн судалгааны дүнд дүгнэлт хийж цаашид анхаарах зарим асуудлыг хөндөхийг зорилоо.

Abstract: The purpose of this article is to determine legal regulations of information security in law Enforcement University. Furthermore, it analyzes current conditions of information security based on the findings of check point to identify the way of enhancing information security of LEU.

Түлхүүр үгс: *Хууль сахиулах их сургууль, мэдээллийн аюулгүй байдал, эрх зүйн зохицуулалт, мэдээллийн аюулгүй байдлын алба, өнөөгийн нөхцөл байдал.*

Key words: *Law Enforcement University, information Security, legal environment, information security unit, current conditions*

Удиртгал

Мэдээлэл технологийн хөгжил хувь хүн, байгууллагын хөгжил төдийгүй улс орныг хөгжлийг илэрхийлэх чухал хэмжигдэхүүн болоод байна.

Мэдээлэл харилцаа, холбооны нэгдсэн сүлжээнд холбогдох нь аливаа байгууллагын аюулгүй байдал, түүний дотор мэдээллийн аюулгүй байдалд тодорхой хэмжээгээр нөлөөлж, хууль эрх зүй, энэ талаар хэрэгжүүлэх бодлого зэрэгт харгалзан үзэж, өөрчлөн шинэчлэх шаардлагыг бий болгож байна.

Мэдээлэл технологийн чиглэлээр төрийн болон төрийн бус байгууллага идэвхтэй үйл ажиллагаа явуулж байгаа хэдий ч аюулгүй байдал, хөгжлийн бодлого. эрх зүйн орчин хоцрогдож буй нь ажиглагдаж байна[77].

Нэг. ХСИС-ийн мэдээллийн аюулгүй байдлыг хангах эрх зүйн зохицуулалт

Монгол Улсын Засгийн газрын 2011 оны 7 дугаар сарын 6-ны өдрийн 229 дүгээр тогтоолоор Хууль зүй, дотоод хэргийн салбарын боловсон хүчин бэлтгэх. давтан сургах тогтолцоог боловсронгуй болгох, эрдэм шинжилгээ, судалгааны ажлын уялдааг сайжруулах зорилгоор Цагдаагийн академи, Хилийн цэргийн дээд сургуулийг нэгтгэн Хууль зүй, дотоод хэргийн яамны харьяанд Дотоод хэргийн их сургууль байгуулсан билээ.

Улмаар МУ-ын Засгийн газрын 2012 оны 10 дугаар сарын 13-ны өдрийн 87 дугаар тогтоолоор Дотоод хэргийн их сургуулийг хууль зүйн салбарын шинэчлэлийн хүрээнд “Хууль сахиулахын их сургууль” болгон өөрчлөн зохион байгуулж, Хууль зүйн сайдын 2015 оны 7 дугаар сарын 3-ний өдрийн А/148 дугаар тушаалаар ХСИС-ийн дүрмийг шинэчлэн батлсан байна. Уг дүрэмд зааснаар “Их сургууль нь төрийн өмчид суурилсан, нэгдмэл төвлөрсөн удирдлагатай, эрдэм шинжилгээ-сургалт үйлдвэрлэлийн хэв шинж бүхий дээд боловсролын, төрийн тусгай чиг үүргийн бие даасан байгууллага мөн".

1.1 Их сургуулийн мэдээллийн аюулгүй байдлыг хангах алба нэгж, түүний чиг үүрэг

Их сургууль нь хууль сахиулах, аюулгүй байдлыг хангах байгууллагын мэргэшсэн хүний нөөцийг бэлтгэх чиг үүрэг бүхий бүрэлдэхүүн сургууль болон харьяа сургуультай байхаас гадна мэдээлэл, технологийн аюулгүй байдлыг хангах чиг үүргийг хэрэгжүүлэх цэргийн албаны зохион байгуулалт, аюулгүй байдлын газар, түүний харьяа алба нэгжтэй байна. Энэ талаар ХСИС-ийн дүрмийн 25 дугаар зүйлийн 25.2-д “Цэргийн аюулгүй байдлын газарт Цэргийн зохион байгуулалтын, Мэдээлэл, технологи, аюулгүй байдлын, Соёл, олон нийт, хамтын ажиллагааны алба харьяалагдана” гэж заасан байдаг.

Мөн дүрэмд “Цэргийн албаны зохион байгуулалт, аюулгүй байдлын газрын дарга мэдээллийн технологийн аюулгүй байдлын хүрээнд их сургуулийн мэдээлэл, холбооны найдвартай, гадаад, дотоод сүлжээний аюулгүй байх, хүртээмжтэй байх, тасралтгүй бэлэн байдлыг хангах; их сургуулийн үйл ажиллагааг шуурхай зохион байгуулахад ашиглагдах хэрэглээний программуудыг зохиож, үйл ажиллагаандаа бүрэн ашиглах нөхцлийг бүрдүүлэх, аюулгүй бэлэн байдлыг хангах; мэдээллийн технологи,

[77] Ч.Оргил (2016), Мэдээллийн аюулгүй байдлын хандлага. Стратегийн судалгаа сэтгүүл. 4/2016 №76, 67 дах тал

холбооны дэвшилтэт технологийг ашиглан шуурхай удирдлагын нэгдсэн сүлжээ бий болгох, аюулгүй байдлыг хангах зэрэг чиг үүргийг хэрэгжүүлнэ[78].

Энэ нь их сургуулийн хэмжээнд мэдээллийн аюулгүй байдлыг хангах эрх зүйн үндсийг тодорхойлж, мэдээлэл, холбооны дэвшилтэт технологийг үйл ажиллагаандаа бүрэн ашиглах, аюулгүй байдлыг хангах чиг үүргийг сургуулийн үндсэн бүтцийн нэгж цэргийн албаны зохион байгуулалт, аюулгүй байдлын газрын дарга, түүний харьяа Мэдээлэл, технологи, аюулгүй байдлын алба хэрэгжүүлэхээр тусгагдсан байгаа нь мэдээллийн аюулгүй байдлыг хангах удирдлагын тогтолцоо бүрдсэн болохыг харуулж байна.

Хэрэгжүүлэх чиг үүргийг тогтооосон хэм хэмжээнээс харахад мэдээлэл, холбооны дэвшилтэт технологийг үйл ажиллагаандаа ашиглах, аюулгүй байдлыг хангаж ажиллах талаар зааж өгсөн хэдий ч мэдээллийн орчны хамгаалалт, хэрэглэгчийн хариуцлага, техник болон программ хангамж, ашиглалт, сүлжээний нууцлалыг хэрхэн хангах талаар зааж өгөөгүй байгаа нь энэ талаар бодлогын баримт бичгийг боловсруулж батлан гаргах шаардлагатай болохыг тэмдэглэж байна.

Их сургуулийн холбогдох албанаас ХСИС-ийн Мэдээлэл, Холбоо, Технологийн бодлого, журмыг төслөөр боловсруулсан байна. Уг журмын зорилго нь ХСИС-ийн мэдээлэл, холбоо, технологийн үйл ажиллагааг тасралтгүй, хүртээмжтэй, мэдээллийн аюулгүй байдлын шаардлагад нийцсэн байдлаар явуулахад оршино[78] [79] гэж заасан байна. Бүтцийн хувьд 11 бүлэг, 72 зүйлтэй бөгөөд мэдээллийн аюулгүй байдлыг хангахтай холбоотой дараах харилцааг зохицуулж өгөхөөр тусгажээ. Үүнд:

- Мэдээллийн аюулгүй байдлыг хангах
  Мэдээллийн технологийн техник хэрэгсэл ашиглах
- Сүлжээ, сервер компьютер ашиглах
  Цахим шуудан ашиглах
  Програм хангамжийн систем ашиглах
  Цахим хуудас ажиллуулах, мэдээллийн баяжилт хийх
  Радио болон телефон холбоо ашиглах
  Телехяналтын камерын систем ашиглах
  Сургалт
- Санхүүжилт
  Хариуцлага

Дээрх журмын төсөлд мэдээлэл, мэдээллийн систем гадны халдлагад өртөх, найдвартай байдал алдагдах, ашиглах боломжгүй болохоос үүдэн гарч

[78] Хууль сахиулах их сургууль.(2015) Хууль сахиулахын их сургуулийн дүрмийн 25.6 дах заалт

[79] ХСИС-ийн Мэдээлэл холбоо, технологийн бодлого, журмын төсөл. 2016. 1.1 дэх заалт

болзошгүй эрсдэлийг үндэслэн мэдээллийн нууцлалын ангиллыг дараах 4 түвшинд авч үзэхээр тусгагдсан байна[80].

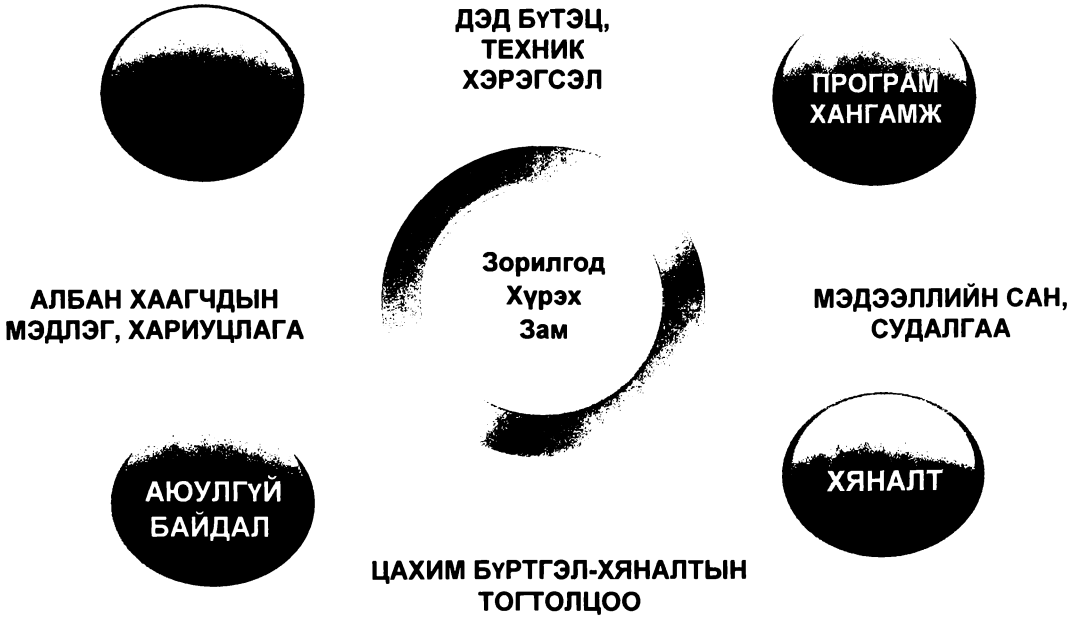
Хүснэгт 1.

Нууцлалын түвшин	Нууцлагдсан байдал	Ашиглах боломж
1	Нийтэд зориулсан /С-1/	Хандах эрхийг хязгаарлаагүй.
2	Албан хэрэгцээнд зориулсан /С-2/	Хандах эрхийг албан тушаалд үндэслэн хязгаарласан.
3	Нууц /С-3/	Эрх бүхий албан хаагчид хамгаалалттай орчинд нэвтэрнэ.
4	Маш нууц /С-4/	Эрх бүхий албан хаагчид нэвтрэх боломжийг хязгаарласан орчинд сайжруулсан хамгаалалттайгаар нэвтэрнэ.

Эх сурвалж: ХСИС-ийн мэдээлэл, холбоо, технологийн бодлого, журмын төслийн үзэл бариmтлалаас. 2016.

Хоёр. ХСИС-ийн мэдээллийн сүлжээний зохион байгуулалт, техник технологийн түвшин, техник хэрэгслийн ашиглалт хамгаалалт

ХСИС нь “Цахим их сургууль” болох зорилгод хүрэх арга замыг дараах байдлаар тодорхойлж байна.



[80] ХСИС-ийн Мэдээлэл холбоо, технологийн бодлого, журмын төсөл. 2016. 3.4 дэх заалт

Цахим их сургууль болно гэдэгт мэдээллийн технологийн дэвшлийг хүртээмжтэй, мэдээллийн сан, судалгааны боловсронгуй програм хангамжтай, бүртгэл-хяналтын тогтолцоотой, аюулгүй байдлыг хангасан байхаар нэвтрүүлж, үр дүнд нь сургалтын орчин цахимжиж, орон зайнаас үл хамаарсан зайны сургалтууд тогтмолжиж, багш, сонсогчдын мэдээллийн технологийн хэрэглээ, мэдлэг ур чадвар нэмэгдэж, сургалтын үйл ажиллагаа цахим хөтчөөр олон нийтэд ил тод мэдээлэгддэг байхыг ойлгож болох юм.

Одоогийн байдлаар их сургууль нэгдсэн интернетийн сүлжээтэй, Сансар кабелийн телевизийн шилэн кабелиуд болон телефон холбооны физик кабелиуд хичээлийн шинэ байранд сувагчлалаар татагдаж, серверийн өрөөнөөс давхар бүрийн хуваарилах самбарууд, албан хаагчийн өрөө, хичээлийн анги, танхимтай холбогдсон, 15 mbps хурд бүхий интернетийн сүлжээнд 650 гаруй хэрэглэгч тогтмол холбогдон ажилладаг.

Түүнчлэн мэдээллийн аюулгүй байдлыг механик байдлаар буюу компьютерийг форматлах, вирусийн програм суулгах замаар аюулгүй байдлыг хангаж байна. Энэ нь их сургуулийн дэд бүтэц, сүлжээ, интернетийн оролт, гаралт дээр хяналтын сүлжээний аюулгүй байдлын төхөөрөмж байрлуулах хэрэгцээ шаардлагыг зайлшгүй бий болгож байна.

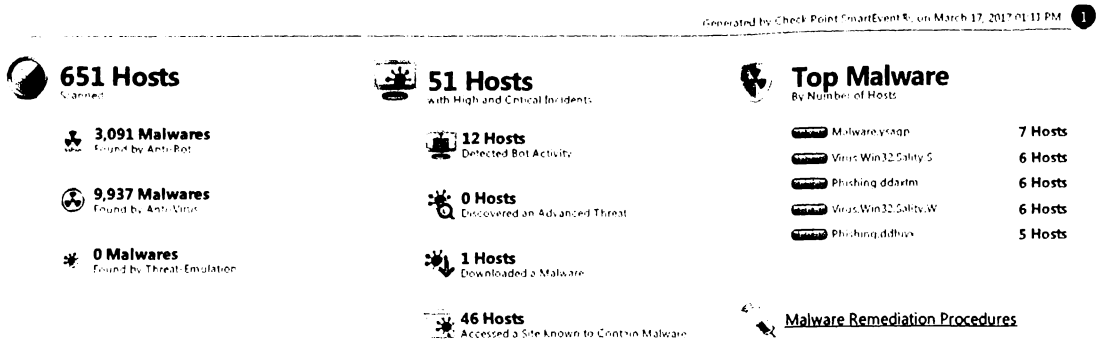
Интернет сүлжээгээр орж ирж байгаа хэдэн мянган халдлага, вирусүүдийг устгах, халдлагыг таслан зогсоох зорилгоор алба хаагчид өөрсдийн хэрэглэж байгаа компьютерт лицензгүй вирусийн програм суулгаж ашигласнаар үр дүнд хүрэхгүй.

Гурав. “Check point” ашиглан сүлжээний урсгалд хийсэн дүн шинжилгээний судалгааны дүн

“Check point” төхөөрөмж нь интернетийн оролт, гаралтын урсгалыг хянаж, сүлжээний аюулгүй байдлыг хангах, аюулаас урьдчилан сэргийлэх, олборлох, мэдээллийг аюулгүй дамжуулах, ялгаатай файлуудыг ангилах, зайлсхийх, дамжуулах боломжгүй файлуудыг саатуулах, үнэлгээ хийх, аюултай файлын аюулыг зогсоож сүлжээнд нэвтрүүлэхгүй шалгаж, кибер халдлагын эсрэг хамгаалах, оролт, гаралтын хяналтыг уян хатан зохицуулах боломжтой учраас төрийн байгууллагууд уг төхөөрөмжийг мэдээллийн аюулгүй байдлыг хангах арга хэрэгсэл болгон ашиглах хандлага нэмэгдэж байна.

Их сургуулийн интернетийн урсгал дээр тухайн төхөөрөмжийг 14 хоног байршуулан хяналт тавьж, дүн шинжилгээ хийхэд дараах нөхцөл байдал тогтоогдлоо.

Зураг 1. Сүлжээний эрсдэлиин статистик дүн



Эх сурвалж: Хууль сахиулах их сургууль (2016) Check point 5200 ашиглан сүлжээний урсгалд хийсэн дүн шинжилгээ, судалгааны тайлан.

Дээрхээс үзэхэд их сургуулийн сүлжээнд чиглэсэн 12,000 гаруй халдлага буюу вирус нэвтрэн орж ирж байна. Мөн 51 компьютер халдлагад өртөж өөрийн мэдээллээ алдах өндөр эрсдэлтэй болсон байгааг харж болно[81].

Зураг 2. Өндөр эрсдэлд өртсөн хэрэглэгч

Host With High or Critical Severity Incidents (1 out of 2)

	Host	Severity	Protection Name	Num. of Incidents	Sent Traffic
Found Bot Activity	10.0.1.23		Trojan-PSW.Win32.Jenxcus.A	6	16.6KB
	10.0.1.23		Backdoor.Win32.VBS.E	6	0B
	10.0.1.223		Virus.Win32.Sality.S	4	0B
	10.0.1.223		Virus.Win32.Sality.CE	4	0B
	10.0.1.23		Virus.Win32.Sality.W	4	10.5KB
	10.0.1.223		Virus.Win32.Sality.CB	4	0B
	10.0.1.23		Virus.Win32.Sality.S	4	2KB
	10.0.1.223		Virus.Win32.Sality.W	4	5.6KB
	10.0.1.20		Virus.Win32.Sality.W	3	816B
	10.0.1.22		Virus.Win32.Sality.CB	3	0B
	10.0.1.22		Virus.Win32.Sality.S	3	1KB
	10.0.1.23		Virus.Win32.Sality.CE	3	0B
	10.0.1.22		Virus.Win32.Sality.W	3	5.2KB
	10.0.1.20		Virus.Win32.Sality.S	3	0B
	10.0.1.23		Virus.Win32.Sality.CB	3	0B
	10.0.1.22		Virus.Win32.Sality.CE	3	0B
	10.0.1.22		Virus.Win32.Sality.Q	2	0B
	10.0.1.17		Virus.Win32.Sality.S	2	0B
	10.0.1.130		Virus.Win32.Sality.S	2	415B
	10.0.1.17		Virus.Win32.Sality.CB	2	0B
	Others (29)			72	147.9KB
	Total (49)			140	190.1KB
Downloaded a Malware	10.0.3.184		Trojan.Win32.Generic.T.brxnp	1	0B
	10.0.1.190		Malware.yrdcz	14	25.3KB
	10.0.3.204		Malware.yrdcz	12	20.2KB
	10.0.3.171		Malware.ysagp	9	3.8KB

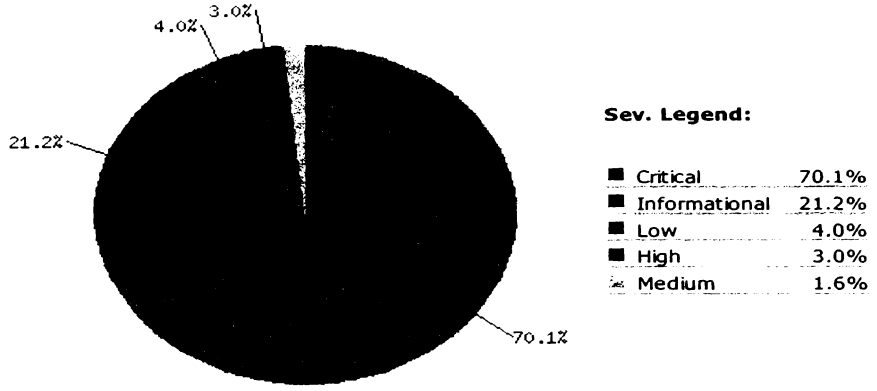
Эх сурвалж: Хууль сахиулах их сургууль (2016) Check point 5200 ашиглан сүлжээний урсгалд хийсэн дүн шинжилгээ, судалгааны тайлан.

[81] Хууль сахиулах их сургууль (2016) Check point 5200 ашиглан сүлжээний урсгалд хийсэн дүн шинжилгээ, судалгааны тайлан.

Нэгэнт вирус тээгч болон бусад серверийн гар хөл болсон дээрх IP хаягтай компьютерүүд нь бусад компьютерүүдэд вирус халдаах, мөн кибер халдлагад өртөгдөх үүд хаалгыг нээж өгч байна гэж үзэж болохоор байна.

Зураг 3. Мэдээллийн аюулгүй байдлын түвшин

Overall Security - % of Total Events by Severity



Эх сурвалж: Хууль сахиулах их сургууль (2016) Check point 5200 ашиглан сүлжээний урсгалд хийсэн дун шинжилгээ, судалгааны тайлан.

Ийнхүү 14 хоногийн хугацаатайгаар Их сургуулийн мэдээллийн сүлжээний урсгалд хийсэн дүн шинжилгээ, судалгааны үр дүн тус их сургуулийн мэдээллийн аюулгүй байдал өндөр эрсдэлтэй түвшинд буюу 70,1 %-ийн мэдээлэл алдагдах, халдлагад өртөх аюултай нөхцөлд байгааг харуулж байна[82].

Дүгнэлт

Их сургуулийн дүрэмд мэдээллийн аюулгүй байдлыг хангах эрх зүйн үндсийг тодорхойлж, аюулгүй байдлыг хангах чиг үүргийг Мэдээлэл, технологи, аюулгүй байдлын алба хэрэгжүүлэхээр тусгасан нь мэдээллийн аюулгүй байдлыг хангах эрх зүйн зохицуулалт болон удирдлагын тогтолцоо үндсэндээ бүрдсэн гэж үзэж байна. Гэвч мэдээллийн орчны хамгаалалт, хэрэглэгчийн хариуцлага, техник болон программ хангамж, ашиглалт, сүлжээний нууцлалыг хэрхэн хангахтай холбоотой харилцаа эрх зүйн зохицуулалтгүй явж ирсэн нь уг харилцааг зохицуулах бодлогын баримт бичгийг батлан, хэрэгжүүлэх шаардлагыг бий болгож байна.

Цаашид Их сургууль мэдээллийн аюулгүй байдлаа хангах, кибер халдлагаас сэргийлэх зорилгоор интернет сүлжээний аюулгүй байдлыг хамгаалах төхөөрөмжтэй болох, төрийн байгууллагуудын нэгдсэн сүлжээнд

[82] Мөн тэнд

өөр өөрсдийн шилэн кабельд сувагчлалаар татаж холбогдох, Их сургууль болон бусад төрийн байгууллагууд Үндэсний Дата Төвийн сүлжээнд холбогдох. интернетийн урсгалыг хяналттай болгох арга хэмжээг авах нь зүйтэй гэж үзэж байна.

Эх сурвалжийн жагсаалт

1. Дотоод хэргийн их сургууль байгуулах тухай. МУ-ын Засгийн газрын 2011 оны 7 дугаар сарын 6-ны өдрийн 229 дүгээр тогтоолын хавсралт.
2. Хууль сахиулахын их сургууль болгон өөрчлөх тухай. МУ-ын Засгийн газрын 2012 оны 10 дугаар сарын 13-ны өдрийн 87 дугаар тогтоолын хавсралт.
3. Хууль сахиулах их сургуулийн дүрэм батлах тухай. Хууль зүйн сайдын 2015 оны 7 дугаар сарын 3-ний өдрийн А/148 дугаар тушаалын хавсралт.
4. Хууль сахиулахын их сургуулийн дүрэм. 2015
5. ХСИС-ийн Мэдээлэл холбоо, технологийн бодлого, журмын төсөл. 2016
6. Хууль сахиулах их сургууль. Check point 5200 ашиглан сүлжээний урсгалд хийсэн дүн шинжилгээ, судалгааны тайлан. 2016
7. Оргил Ч. Мэдээллийн аюулгүй байдлын хандлага. Стратегийн судалгаа сэтгүүл. 4/2016 №76.