МОНГОЛ УЛСАД ҮЙЛДЭГДЭЖ БАЙГАА КИБЕР ГЭМТ ХЭРГИЙН ШАЛТГААН, НӨХЦӨЛ, ТҮҮНТЭЙ ТЭМЦЭХ АРГА ЗАМ, ҮНДСЭН ЧИГЛЭЛ

СУУРЬ СУДАЛГААНЫ ТАЙЛАН

2015 он

ГАРЧИГ

Европын холбооны Будапештийн конвенци /2001 он/

Монгол, Солонгосын криминологичдын хамтарсан семинар /2013.09.26/

- **Танилцуулга**
- **Илтгэлүүд**

УДИРТГАЛ

Монгол Улсад төдийгүй дэлхийд хурцаар тавигдаж буй асуудлуудын нэг нь мэдээллийн аюулгүй байдал, кибер буюу цахим хил хязгааргүй орчинд үйлдэгдэж буй гэмт хэрэг, түүнийг илрүүлэх, урьдчилан сэргийлэх асуудал юм. Сүүлийн жилүүдэд манай улсын иргэд санаатай болон санаандгүйгээр энэ төрлийн гэмт хэргийг үйлдэх, уг гэмт хэргийн золиос болох, хохирох асуудал нилээдгүй гарч байна. Улс орны хэмжээнд ч мэдээллийн аюулгүй байдалтай холбоотой асуудал хурцаар тавигдаж байна.

Эрх зүйн шинэтгэл, олон улсын харилцаа, хамтын ажиллагааны төлөв байдал, техник-технологи, эрх зүйн хөгжлийн өнөөгийн бодит байдал нь урьд өмнө байгаагүйгээр эрс өөрчлөгдөж улмаар хүний эрх, эрх чөлөөний үнэлэмжээр тодорхойлогддог болсон билээ. Үүний гол хүчин зүйлийн нэг нь хүний эрхийн асуудлыг улс орон бүхэн дотоод, гадаад харилцааны чухал хэмжүүр болгон үнэлэмж тогтоох болсонтой холбоотой.

Энэ нь хүний туйлын эрх буюу бодит үнэнийг мэдэх, мэдээлэл харилцааны эрхтэй шууд холбоотой. Үнэнийг мэдэх эрхийг хангах, хамгаалах, мэдээлэл харилцаа холбооны хөгжлийн гол тулгуур нь компьютер, өндөр хүчин чадалтай техник, ухаалаг технологи бөгөөд даяаршсан мэдээллийн хөдөлгөгч хүч нь кибер буюу цахим орчин юм.

Цахим орчин нь өнөөгийн нийтийн харилцааны чухал хэрэгцээний нэг төдийгүй, нийгмийн хөгжлийг тодорхойлогч болсон компьютер, смарт буюу ухаалаг технологитой салшгүй холбоотой.

Мөн даяаршсан нийгмийн гол мөн чанар, дэлхийн хүн төрөлхтний хоорондын харилцаа холбоо, мэдээллийн үйл ажиллагааны автоматжуулалтын хамгийн гол гүүр нь цхим орчин учир иргэн, аж ахуйн нэгж, байгууллагын мэдээллийн аюулгүй байдлыг хангуулах талаар эрх зүйн орчинг боловсронгуй болгох, мэдээллийн аюулын эрсдлээс урьдчилан сэргийлэх арга хэмжээг боловсронгуй болгох зайлшгүй шаардлага байгааг өнөөгийн хөгжил, дэвшлийн үйл явц илтгэж байна.

Иймд аливаа улс орон, байгууллага, тодорхой бүлэг хамт олон, хувь хүний мэдээлэл, түүний аюулгүй байдлыг баталгаатай хангах, хамгаалах явдал нь нэн чухал ач холбогдолтой бөгөөд тулгамдсан бодит асуудлын нэг болсон мэдээллийн аюулгүй байдал ба кибер орчины өнөөгийн байдал энэ салбарт хэрэглэгдэж байгаа нэр томъёо, кибер орчинд үйлдэгдэж байгаа гэмт хэрэгтэй тэмцэх эрх зүйн тогтолцоо, олон улсын чиг хандлага, тулгамдаж байгаа асуудал, шийдвэрлэх арга замын талаар энэхүү судалгааны ажилд авч үзсэн болно.

Судалгааны ажлын зорилго, зорилт

Энэхүү судалгааны ажлын зорилго нь Монгол Улс дахь цахим гэмт явдлын түвшинг тодорхойлж, түүний шалтгаан нөхцөл, цаашдын чиг хандлага, энэ төрлийн гэмт хэргээс урьдчилан сэргийлэх, түүнтэй тэмцэх эрх зүйн болон үйл ажиллагааг гадаад орнуудын туршлагад үндэслэн, харьцуулан судалж боловсронгуй болгох, санал зөвлөмж боловсруулахад оршино.

Судалгааны ажлын удирдагч:

Ж.Болдбаатар	Доктор (Sc.D), профессор, цагдаагийн бэлтгэл хурандаа

Багийн нарийн бичгийн дарга:

Д.Сумъяацэрэн	Эрдэм шинжилгээ, хөгжлийн хүрээлэнгийн Цагдаа судлалын төвийн эрдэм шинжилгээний ажилтан, докторант, цагдаагийн ахлах дэслэгч

Багийн гишүүд:

Л.Цогтбаяр	Орхон их сургуулийн багш, докторант
Б.Мөнхдорж	Цагдаа судлалын төвийн эрдэм шинжилгээний ахлах ажилтан, докторант, цагдаагийн ахмад
Б.Мөнх-Сэргэлэн	Цагдаа судлалын төвийн эрдэм шинжилгээний ажилтан, цагдаагийн дэслэгч
Л.Одхүү	Докторант, цагдаагийн хошууч
Ч.Цэрэнчимэг	Цагдаагийн сургуулийн Мэдээллийн технологийн тэнхимийн багш, дэслэгч
Б.Баяр	Цагдаагийн сургуулийн криминалистикийн тактикийн тэнхмийн эрхлэгч асан, цагдаагийн бэлтгэл хурандаа

Баянзүрх дүүрэг, 8-р хороо, Хилчний гудамж – 1,
ш/х – 210332, Утас: 976-70155034
Цахим хуудас: www.leu.gov.mn
Э-мэйл: police_study_center@leu.gov.mn

БҮЛЭГ I. КИБЕР ОРЧИНД ҮЙЛДЭГДЭЖ БУЙ ГЭМТ ХЭРЭГ, ТҮҮНИЙ ШАЛТГААН, НӨХЦӨЛ, ЧИГ ХАНДЛАГА

1.1. Кибер орчинд үйлдэгдэж байгаа гэмт хэрэг, хамаарах асуудлууд

Хүн төрөлхтөн өнөөгийн XXI дүгээр зуунд хүртэл хөгжихдөө улс орны дотоодын хийгээд олон улсын хэмжээнд амьдрал, үйл ажиллагааг мэдээллийн ухаалаг технологи, техник хэрэгсэлгүйгээр төсөөлөхийн аргагүй болсон билээ. Тэр бүү хэл, хүн бүрийн өдөр тутмын үйл ажиллагааг мэдээллийн ухаалаг технологи, техник хэрэгсэл, интернет орчингүйгээр төсөөлшгүй. Энэ нь хэдийгээр хүн төрөлхтөний хөгжил тодийгүй, үүнтэй зэрэгцээд гэмт хэрэг үйлдэгдэх талбар болсон байна.

Кибер орчин дахь үйл явцыг судлахын тулд түгээмэл хэрэглэгддэг нэршил, үг зүйг оновчтой тайлбарлаж хэрэглэх нь тухайн салбарыг нарийвчлан судлах алтан үүд хаалга гэж үзэх үндэстэй.

Юуны өмнө “Цахим” болон “Кибер” гэсэн үг өнөөгийн нөхцөл байдалд хэрхэн хэрэглэгдэж байгаа талаар товчхон авч үзье.

“Кибер” гэх үг нь кибернетикийн шинжлэх ухаантай холбоотой бөгөөд анх энэ үгийг 1948 онд америкийн математикч Норберт Винер[1] (1894-1964) болон түүний хамтран зүтгэгчид математикийн шинжлэх ухаантай холбож хэрэглэсэн. Кибернетик гэсэн нэршлийг тэд амьтан болон машин (тоног төхөөрөмж) дахь харилцаа холбооны онол болон удирдлагыг бүхэлд нь хамарсан талбар гэдгээр томьёолсон. Винер грекийн “*kubernetes”* буюу удирдагч гэх үгийн үндэс залуурч гэх утгатай үгийг хэрэглэсэн байдаг. Мөн энэхүү үгийг ашиглахдаа 1830 оны Францад хэрэглэгдэж байсан *“cybernetique”* буюу грек үгтэй үндэс ойр “удирдахуйн урлаг” гэх үл мэдэгдэх Франц нэр томьёонд үндэслэсэн байна.[2] Норберт Винерийн энэхүү онол нь инженерчлэл, системийн удирдлага, компьютер, биологи, философийн шинжлэх ухаануудтай холбоотой юм. Кибернетикийн ухаан нь бүх өөрөө удирдах цогц системүүдийн дотоод харилцаа холбоо болон удирдлага нь хоорондоо ижил төстэй гэж үздэг. Туршилтад суурилсан эмпирик шинжлэх ухаануудтай (физик, биологи гэх мэт) адил материаллаг шинж чанарт анхаарахаасаа илүүтэй нэгж хэсгүүдийн зохион байгуулалт, хэлбэр, хоорондын харилцаа хамаарлыг судалдагаараа ялгаатай. Улам хурдасч буй компьютерийн хөгжил, тэднийг хүнтэй төстэй болгох оролдлогуудаас үүдэн өнөө үед кибернетик нь хиймэл оюун ухаан болон автоматжуулалттай нягт холбогдож, мэдээллийн онолын салбарын санаануудаас олныг өөриймшүүлэн авч байна.[3]

Монгол хэлний тайлбар тольд **“Цахим”** гэдэг нь *нэгдүгээрт,* цахилгаан тооцоолон бодох техник, ийм төрлийн техник ашиглан үйл ажиллагаа явуулах. цахим бараа, цахим тооцоолуур, цахим захиа, цахим шуудан, цахим багаж, цахим тоноглол, цахим карт, цахим хуудас. *Хоёрдугаарт,* маш хурдан. Цахилгаан цахих мэт хурдтай, цахим хурд[4]-ыг ойлгоно гэж заасан байдаг. **Electronic mail** /e-mail/-ийг цахим шуудан гэж бид орчуулж хэрэглэж байна. Тэгэхээр цахим гэдэг үгийн язгуур нь цахих, цахилгаан гэдэг үг болж байна. Бидний өдөр тутам сонсож байдаг, өргөн хэрэглэгдэж байдаг e-game, e-office, e-citizen, e-government гэх зэрэг нэр томьёо нь “e” угтвар авснаар онлайн, дижитал байдлаар буюу интернэт, сүлжээний орчинд энэхүү үйл ажиллагааг явуулж буйг илэрхийлж байдаг.

Аливаа төрлийн үйл ажиллагааг (сургалт, баримт бичиг дамжуулалт г.м) харилцаа холбооны технологи ашиглан үйлдэж байгаа тохиолдолд “цахим” гэдэг үгийг хэрэглэж байна.

---

[1] http://en.wikipedia.org/wiki/Norbert_Wiener

[2] /Oxford English Dictionary, 2nd Edition/ www.wordorigins.org

[3] “Britannica”ширээний нэвтэрхий толь. 1530 дахь тал.

[4] Я.Цэвэл “Монгол хэлний товч тайлбар толь”

Монгол Улсын хуулиудад ч мөн л энэ утгаар нь авч үзсэн байдаг. Тухайлбал, Эрүүгийн хуулийн тусгай ангийн 178[3] дугаар зүйлийн 178[3].2 дахь хэсэгт “Терроризмыг сурталчлах гэмт хэргийг давтан, хэвлэл мэдээллийн хэрэгсэл, холбоо, **цахим сүлжээ** ашиглаж үйлдсэн бол гурваас дээш зургаан сар хүртэл хугацаагаар баривчлах, эсхүл гурван жил хүртэл хугацаагаар хорих ял шийтгэнэ” гэж заасан байдаг.

Цахим гэдэг нь мэдээлэл технологийн орчин дахь үйлчилгээ болон үйл ажиллагааны талаарх ойлголтыг өгч байгаа юм. Харин “кибер” гэсэн үг нь илүү өргөн хүрээний ойлголт бөгөөд эдгээр цахим үйл ажиллагааг явуулж буй дэд бүтэц, орчны үйл ажиллагаа түүний удирдлагын талаарх ойлголтыг агуулж байгаа юм. Монгол Улсын үндэсний аюулгүй байдлын үзэл баримтлалын 3.6.1.11-д “Кибер орчин дахь гэмт явдалтай тэмцэх, аливаа гэмт хэргийг илрүүлэх, нотлоход тооцоолох хэрэгслийн криминалистик техникийн шинжилгээ ашиглах үндэсний чадавхийг бий болгоно”, 3.6.1.1-т. “Мэдээллийн аюулгүй байдлыг хангах, мэдээллийн орчинд сөргөлдөх аюулаас сэргийлэх, кибер орчин дахь гэмт явдалтай тэмцэх чиглэлд олон улсын хамтын ажиллагааг өргөжүүлэн хөгжүүлнэ” гэх зэргээр тусгасан байдаг.

Тиймээс бид цаашид “Цахим гэмт хэрэг” бус **“Кибер гэмт хэрэг”** гэж томьёолж, нэг мөр хэрэглээнд нэвтрүүлэх нь оновчтой гэж үзэв.

Тэгвэл **“Кибер гэмт хэрэг”** гэж чухам юу юм бэ? Энэ талаар дэлхий нийтэд нэгдсэн тодорхойлолт өдийг хүртэл байхгүй. 2001 оны “Кибер гэмт хэргийн тухай” европын /Будапештийн/ конвенцид ч энэ талаар тодохойлолт алга байгаа юм. Энэ нь мэдээж техник, технологийн хэт өсрөнгүй, хурдацтай хөгжилтэй холбоотой юм.

“Britannica” нэвтэрхий тольд дурдсанаар “Кибер гэмт хэрэг” гэж компьютерийг залилан хийх, хүүхдийн порнограф болон оюуны өмч наймаалах, нэрийн хулгай, хувийн нууцад халдах зэрэг хууль бус үйлдэлд ашиглах аливаа үйлдлийг хэлнэ гэж тайлбарласан хэдий ч өнөө үед энэ төрлийн гэмт хэргийг дан ганц компьютер ашиглан үйлдэхээс гадна утас, таблет, хуурамч чип /зээлийн карт/ зэргийг ашиглан үйлдэх болжээ.

Товчхондоо “Компьютер, мэдээллийн сүлжээ, интернет ашиглан үйлдэгдсэн бүх төрлийн гэмт хэрэг” гэж ойлгож болох юм. Кибер гэмт хэрэг нь дараах байдлаар ангилагдана.

- Хувь хүний эсрэг (вирус, залилан,фишинг, спэм г.м)
- Өмчийн эсрэг (бусдын эд хөрөнгийг сүйтгэх, хортой програм тараах г.м)
- Төрийн эсрэг (Кибертерроризм, Мэдээллийн дайн)

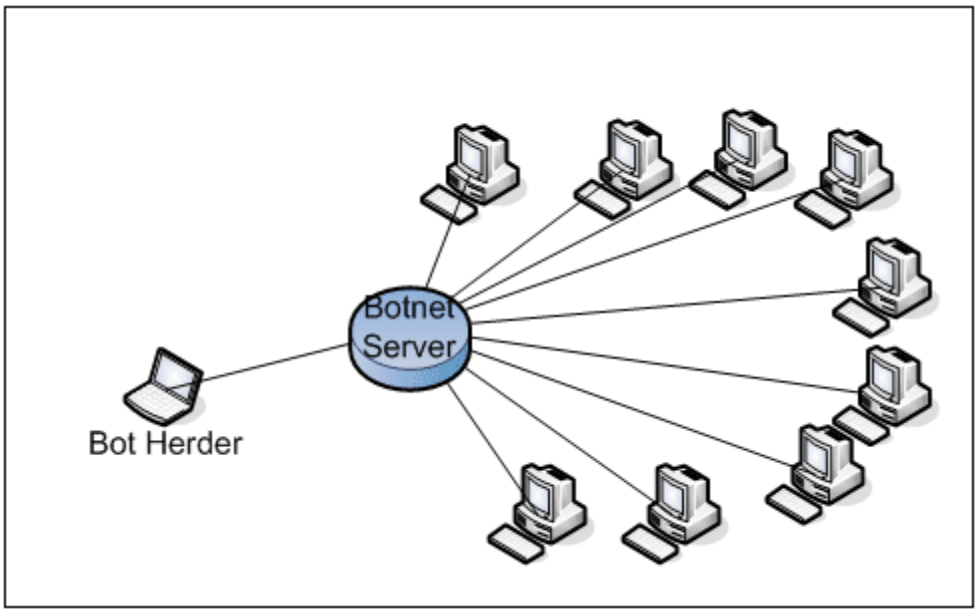
Кибер гэмт хэрэг нь компьютер хэрэглээнд нэвтэрснээс хойш гарах болсон ба компьютер, сүлжээ, Интернэт ашиглан гэмт хэрэг үйлддэг байсан бол одоо үед боловсронгуй болгон, утасгүй сүлжээг өргөн ашиглахаар болжээ. Компьютер, компьютерын сүлжээ ашиглан үйлддэг гэмт хэргийг төрлөөр жагсаан бичвэл:

1. Эвдлэх ажиллагаа /сүлжээнд зөвшөөрөлгүй нэвтрэх, халдах/
2. Тайван байдлыг алдагдуулах буюу кибер мөшгигчид
3. Аж ахуйн /Эдийн зсгийн тагнуул
4. Хүүхдийн порнограф
5. Хулгай, спам
6. Айлган сүрдүүлэх явдал
7. Оюуны өмчид халдах, түүнийг олшруулах, тараах
8. Кибертерроризм
9. Секс сүрдүүлэг
10. Интернет луйвар /э-мэйл лувар/
11. Гутаан доромжлох, гүтгэх, бусдын нэр хүндэд халдах
12. Зээлийн карт хуурамчаар үйлдэх .

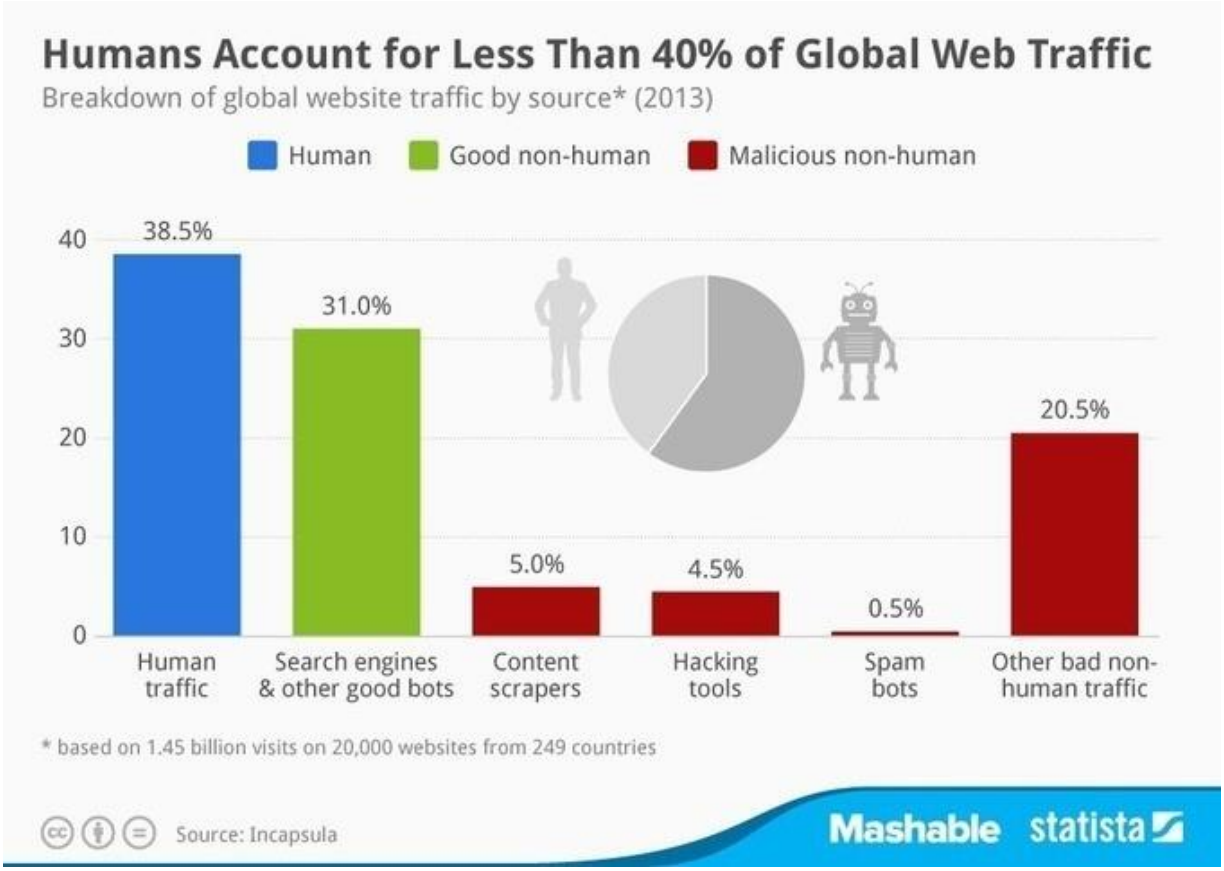
Монголчууд интернэттэй танилцаад 20 орчим жил болж байна. Энэ хугацаанд интернэт нь ус цахилгаан шиг чухал хэрэгцээ болсон гэхэд хилсдэхгүй байх. Тэгвэл интернэтийн “амьгүй албатууд” буюу botnet-ын тухай авч үзье.

Botnet гэж юу вэ?

Энэ нь “robot” болон “internet” гэсэн үгнүүдийн дундаас үүсгэсэн зохиомол үг. Интернэтийн орон зайд тодорхой үүрэг гүйцэтгэхээр програмчлагдсан систем юм. Энэ нь дотроо сайн эсвэл муу зорилготой гэж хуваагдана. **Botnet** гэдэг нь хэдэн арваас авхуулаад хэдэн сая компьютерийг гартаа оруулсан этгээдийн интернетийн сүлжээ юм. Өгөгдсөн тушаалыг үг дуугүй гүйцэтгэдэг.



2013 оны судалгаагаар дэлхийн нийт интернэт урсгалын (traffic) 40 хүрэхгүй хувийг хүмүүсийн үүсгэсэн урсгал эзэлдэг байна. Харин үлдсэн 60 орчим хувийг хүмүүс биш bot-ууд үүсгэж байна. Энэ 60 хувийг дахин нягталж харвал тал нь “сайн”, тал нь “муу” зорилгын үүднээс бий болсон урсгалууд байдаг байна.



Дэлхийн интернэт урсгалын бүтэц (Эх сурвалж: Statista)

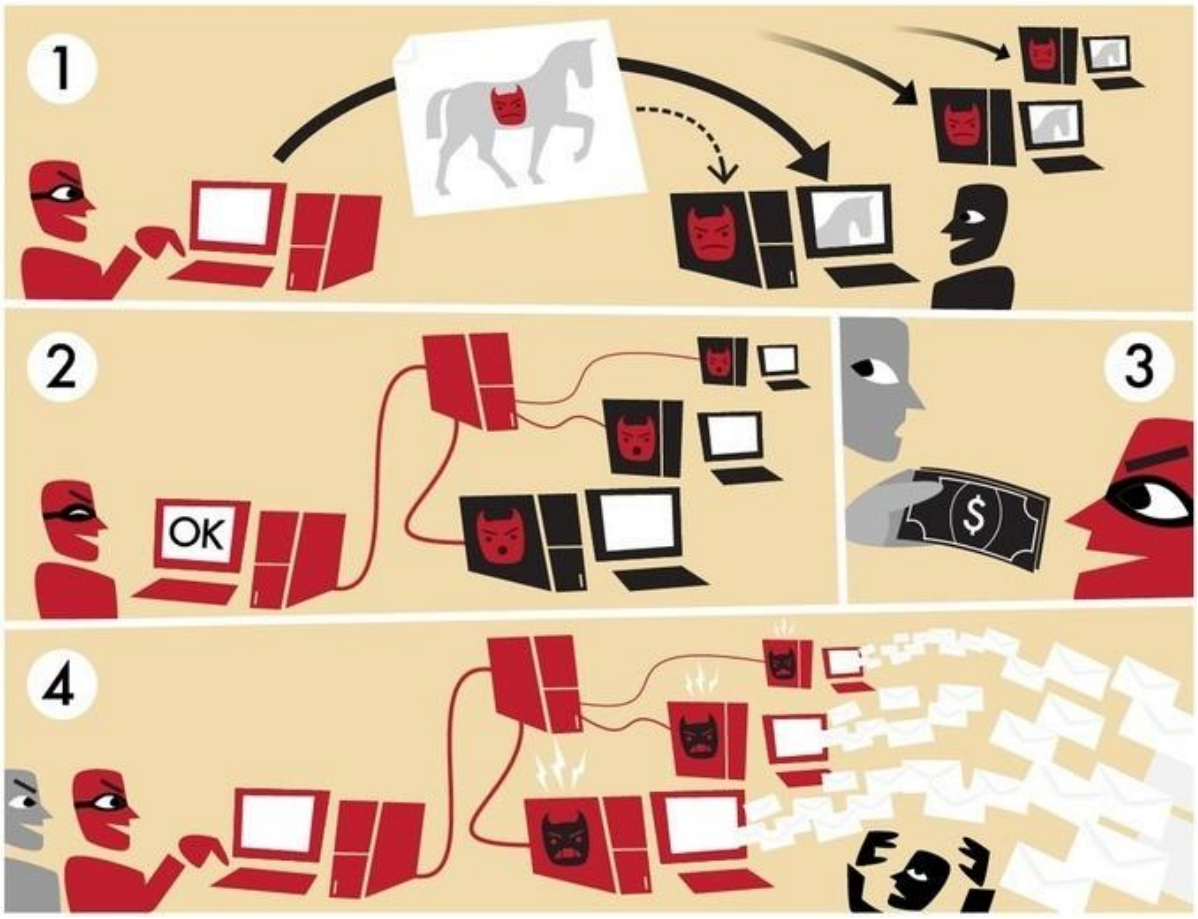
Тэгвэл bot-ын “сайн” урсгал гэж юу вэ?

Үүний ихэнх нь хайлтын систем (search engine) үүсгэж байгаа урсгалууд. Google, Yahoo мэтийн хайлтын системүүд дэлхий даяар ажиллаж байгаа бүх вебсайтуудын контентуудын өөрчлөлтийг шалгаж, индексжүүлэх ажиллагааг тасралтгүй явуулж байдаг. Ингэснээр таны хайлтын үр дүн маш хурдан илэрдэг гэж ойлгож болно.

Энэ бол Google зэрэг хайлтын серверээс бусад вебсайтууд руу хандаж байгаа автомат урсгал.

Харин “муу” буюу сөрөг bot-уудын урсгал гэж юу вэ?

Энэ нь хакеруудын зориуд зохион байгуулсан буруу зорилгоор үүсгэж байгаа урсгал. Энэ үйл явц хэрхэн явагддаг вэ?



Botnet хэрхэн ажилладаг вэ? (Эх сурвалж: Wikipedia)

1. Хакерууд эхлээд вирус хэлбэрээр тусгай программаа хүмүүсийн компьютерт халдаана.

2. Аль болох олон компьютерт халдсанаар хакер нь олон компьютерыг эзэнд нь мэдэгдэлгүй удирдах боломжтой болно гэсэн үг. Ингэсэн компьютеруудыг “зомбинууд” ч гэдэг.

3. Үүний дараа хакер нь хэн нэгнээс мөнгө авч захиалга авна.

1. Ингээд хакер нь захиалгат үйлдлийг эзэнд нь мэдэгдэлгүйгээр “зомби” компьютеруудад комманд өгч гүйцэтгүүлнэ.

Зорилго нь аль нэг сервер руу “зомби”компьютеруудаас довтолгоо үүсгэх, сурталчилгаа спам тараах, хиймэл ачаалал, урсгал үүсгэх зэрэг.

Дэлхий дээр хамгийн том botnet нь 30 сая “зомбитой” байсан тохиолдол ч байдаг.

Өөрийн компьютерээ “зомби” болгохгүйн тулд антивирусны програм суулгаж, байнга шинэчлэлт хийж байх хэрэгтэй.

Нэг жишээ татахад хэн нэгэн өөрийн вебийн хандалтыг өсгөхийн тулд мөнгө төлж bot-уудын урсгалыг өөрийн веб рүү үүсгүүлж болно. Дэлхийн хаа нэгтээ байгаа хэн нэг хүний компьютер эзнээ мэдээгүй байхад уг сайт руу зочилж хандалт үүсгэж байгаа гэсэн үг.

Ийм үйлчилгээ үзүүлдэг botnet-үүд интернэтэд олон бий. Өдөрт хэдэн “зомби” хэрэглэгчээс хандалт үүсгэх вэ? гэдгээсээ хамаараад үнэлгээтэй байдаг.

Ингэж вебсайтаа олон хандалттай болгож харагдуулах замаар үнэ хүргэж зарах, эсвэл сурталчилгааны гэрээ байгуулах зэрэг луйвар хийж болно.

Тэгвэл вебсайтыг юунд нь итгэж үнэлэх вэ?

Энэ бол цэвэр таны хувийн үзэмж, итгэл үнэмшлийн асуудал. Хийц дизайн, өнгө үзэмж, агуулгын чанар, ашигласан технологи, зах зээлд байршсан брэнд, нэр хүнд зэрэг олон үзүүлэлтээр нь үнэлэх нь хамгийн зөв, найдвартай арга болно.[5]

Мэдээлэл, технологийн хөгжлийн өнөө үед манай улсын хүүхэд, залуучууд цахим сүлжээ ашиглан сайт болон онлайн чат, онлайн форумд чөлөөт цагаа өнгөрөөж, гадаад улс орны хүмүүстэй найз болох, таних мэдэхгүй хүнтэй танилцаж, нэр, хаягаа солилцож дотоодын болон гадаад улсын иргэдээс үйлдэх гэмт үйлдлийн хохирогч болох тохиолдол нэмэгдсээр байгаа. Хуурамч хаягаар цахим сүлжээ ашиглан найз нөхөд болон харилцах, цахим хаягаар хуурамч худалдаа, үйлчилгээний вэб хуудас явуулах, хуурах, иргэний нэр хаяг, хэрэглэгчийг төөрөлдүүлж дансны болон хувийн мэдээлэл олж авч, хууль бусаар ашиглан бусдын нэр хүндэд халдах, тухайн мэдээллээр бусдыг сүрдүүлэх, залилан мэхлэх зэрэг хэргүүд шил дараалан гарч байна. Тухайлбал, твиттэр, фэйсбүүк хуудсаар манай улсын иргэдтэй найз болж байнгын харилцаатай байх хэлбэрээр танилцаж улмаар хувийн бичлэг, фото зургийг олж авч олон нийтийн сүлжээ сайтад байршуулан устгуулахыг хүсвэл их хэмжээний мөнгө нэхэмжлэх байдлаар, мөн худалдаа үйлчилгээний төлбөр төлөх явцад хүлээн авагч байгууллагын цахим хуудсын дуурайлган хийж, өөрийн дансанд төлбөр шилжүүлэхийг санал болгох зэргээр иргэдийг төдийгүй аж ахуйн нэгж, байгууллагыг залилах гэмт явдал гарсаар байгаа. Манай улсын эрүүгийн хуулийн тусгай ангид “Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг” гэх бүлгээр зохицуулсан байдаг хэдий ч дийлэнх хэрэг эрүүгийн хуулийн тусгай ангийн 148 дугаар зүйл буюу “бусдын эд хөрөнгийг залилан мэхлэж авах” гэх зүйл заалтад хамааруулж ял шийтгэж байгаа тул цахим гэмт хэргийн хохирлыг тодорхойлоход хүндрэлтэй, энэ талаар хийсэн дорвитой судалгаа ч байдаггүй нь энэ төрлийн гэмт хэргийн өсөлтөд ч нөлөөлж буй.

Өнгөрсөн онд ОХУ-ын ерөнхий сайд Дмитрий Медведевийн орос хэл дээр хөтөлдөг твиттер хаягнаас хакердуулсан байж болзошгүй мэдэгдэл хийсэн. Жиргээний утга нь "Огцорлоо. Засгийн газрын үйлдлээс ичиж байна. Уучлаарай" гэсэн ажээ.[6]

Эндээс үзэхэд, ОХУ-ын засгийн газрын тэргүүн өөрөө ийм мессеж нийтэд өгсөн байх учиргүй бөгөөд анти үзэлтэй хэн нэгний халдлагад өртсөн байх магадлал өндөр байгаа юм. Эсвэл хэн нэгэн зугаагаа гаргаж уг үйлдлийг хийсэн ч байж болох. 2008 онд Польш улсад 14 настай хүү зурагтны удирдлага шиг алсаас удирдах төхөөрөмж угсарч, түүнийгээ ашиглаж шугамын трамвайг замаас нь гаргаж онхолдуулсан хэрэг гарч байсан.[7] Энэ талаар хүү “би зүгээр л тоглосон юм” гэж ярьсан байдаг.

Харин **DDoS** буюу Distributed Denial of Service нь DOS (Denial of Service) нь халдлагын хамгийн шилдэг хувилбар болоод байна. Их хэмжээний мэдээллийг илгээснээр Серверийг зогсоох арга хэлбэр юм. DOS -оос илүү хурдан илүү найдвартай ажиллах бөгөөд ул мөр үлдээдэггүйгээрээ онцлогтой. Энэ чиглэлд БНХАУ-ын Хакерууд сүүлийн үед ихээхэн мэргэшсэн байдаг байна. Хятадын энэхүү халдлага хийдэг төв нь Шанхай хотод байршдаг. DDOS-оор халдлагыг сайтар судалж байж түүнээс хамгаалах шаардлагатай болдог. Энэхүү халдлагаар Аль нэг сервер рүү нэвтрээд, тэр сэрвэр болон түн рүү хандаж байсан бүх компьютеруудын мэдээллийг хуулж авч болдог, түүний мэдээллийг өөрчилж болдгоороо онцлог.

[5] http://www.ikon.mn/n/65b
[6] http://www.businessinsider.com/medvedev-twitter-hacked-2014-8
[7] http://www.securitylab.ru/news/311384.php?pagen=3&el_id=311384

Манай улсын үндэсний хууль тогтоомж /Эрүүгийн хууль/-д тусгай ангийн 25 дугаар бүлэгт “Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг” 226-229 дүгээр зүйлд ингэж хуульчилж өнөөдрийг хүртэл хүчин төгөлдөр мөрдөж байна.

Эрүүгийн хуульд компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг гэж тооцогдсон зарим үйлдлүүд өөр төрлийн гэмт хэргүүдэд /жишээлбэл: өмчийн эсрэг гэмт хэрэг буюу залилан мэхлэх гэх мэт/ хамаарагддаг.

Энэ нь уламжлалт гэмт хэргүүдтэй зарим шинжээрээ төсөөтэй боловч хуульчилсан шинжээрээ өөр учир гэмт хэргийн хуулийн шинэчлэлд анхаарах цаг нэгэнт болсоныг цаг үе шаардаж байна.

Компьютерийн болон кибер орчин дахь мэдээллийн эргэлтийн хүрээ гэмт халдлагад ихээр өртөх болсныг манай улсад анхаарч 1996 оны Монгол Улсын Эрүүгийн хуульд “Мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг”гэсэн 11 дүгээр бүлгийг анх удаа хуульчилсан.[8]

- Компьютерийн мэдээллийг хууль бусаар өөрчлөх гэсэн 153 дугаар зүйл,
- Компьютерийн мэдээлэл программыг эвдэх,сүйтгэх гэсэн 154 дүгээр зүйл,
- Компьютерийн мэдээллийг хууль бусаар олж авах гэсэн 155 дугаар зүйл,
- Компьютерийн мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэх, борлуулах гэсэн 156 дугаар зүйл,
- Нянтай програм зохион бүтээх, ашиглах гэсэн 157 дугаар зүйлүүдийг хуульчилжээ.

Үүний дараа 2002 оны Эрүүгийн хуульд “Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг” гэсэн 25 дугаар бүлгийг хуульчилж[9],

- 226 дугаар зүйлКомпьютерийн мэдээлэл, программыг өөрчлөх, эвдэх, сүйтгэх гэсэн,
- 227 дугаар зүйл Компьютерийн мэдээллийг хууль бусаар олж авах гэсэн,
- 228 дугаар зүйлКомпьютерийн мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэх, борлуулах гэсэн,
- 229 дүгээр зүйл Нянтай программ зохион бүтээх ашиглах гэсэн заалтаар МАБ-ын хүрээнд эрх зүйн хамгаалалттай болсон хэдий ч энэ нь өнөөгийн теник технологийн хөгжил, хүний хэрэглээ болон сэтгэхүйн хөгжлийн шаардлага, агуулгад нэгэнт тохирохгүй болсон.

Мэдээллийн аюулгүй байдал хариуцсан мэргэжилтнүүдийн үзэж байгаагаар компьютерийн мэдээллийн нууцлал алдагдсан, гэмт хэрэг, зөрчилд өртсөн тухай мэдээллийг цагдаа, тагнуул болон Интернэтийн үйлчилгээний байгууллага ISP /**internet service provider**/, вэб сайтийн удирдлагуудын /**administrator**/ хэнд нь ч гэмт хэргийн тохиолдлыг тэр бүр тодорхой мэдээлдэггүй, харилцан мэдээлэл солилцохгүй байгаа нь эрх зүйн тогтолцоо хангагдаагүй гэдгийг онцлон тэмдэглэж ирсэн.

Манай улсад үйлдэгдэж байгаа гэмт хэргийн талаар:

Манай улсад 2006, 2007 онд компьютер, мэдээллийн аюулгүй байдлын эсрэг гэмт тус бүр нэг удаа бүртгэгдсэн нь нэг талаас тухайн гэмт хэрэг тогтвортой байгааг нөгөө талаас халдлагын талаар мэддэггүй, эрх зүйн зохицуулалт хангалтгүй байгааг харуулж байна[10].

ЦЕГ-ын Эрүүгийн цагдаагийн газраас авсан тоо баримт

Д /д	Үйлдэгдсэн он	ГХ-ийн тоо	Үйлдэгсдийн тоо	ЭХҮ	ЭХХ-гүй	ЭХҮ-ээс тат	Шүүх шийдсэн
1	2009	-	-	-	-	-	-
2	2010	3	3	3	3	-	-
3	2011	2	2	2	1	-	1

[8]Монгол Улсын Эрүүгийн хууль 1996 он
[9] Монгол Улсын Эрүүгийн хууль 2002 он
[10]ХЗҮ-ний Хүрээлэнгээс явуулсан судалгааны тайлан 2009 он

4	2012	10	10	7	6	3	1
5	2013	8	8	5	3	3	2

Сүүлийн 5 жилийн байдлаар цахим гэмт хэргийн шинжтэй нийт 23 гэмт хэрэг, үйлдлийг илрүүлснээр 17 материалд эрүүгийн хэрэг үүсгэх шалгаж, 6 материалыг эрүүгийн хэрэг үүсгэхээс татгалзан шийдвэрлэсэн байна.

Мөрдөн шалгах явцад 13 хэргийг хэрэгсэхгүй болгож Шүүхээр 4 хэрэг эцэслэн шийдвэрлэгджээ.

Интерполын үндэсний төв товчооноос Монгол Улсын эзэмшлийн IP хаяг ашиглан гадаад улсад цахим халдлага үйлдсэн гэх асуудлаар 4 үйл ажиллагааг шалган шийдвэрлэсэн[11].

Дээрх тоон мэдээлэл нь кибер орчинд үйлдэгдэх гэмт хэрэг тасралтгүй өсөх хандлагатай байгаа бөгөөд шалган шийдвэрлэх ажиллагаанд эрх зүйн зохицуулалт, салбарын нэгдсэн ойлголт, мэргэжлийн мэдлэг, сургалт, мөрдөх арга барил, ашиглах техник хэрэгсэл, дотоод гадаад хамтын ажиллагаа дутагдал байгааг илэрхийлж байна.

Мөн 2009 – 2012 онд Кибер довтолгооноос хамгаалах төвийн Монгол Улсын интернет сигментэд явуулсан судалгаагаар сард дунджаар 7000-35000 кибер довтолгоо хандаж байгаагаас гадна манайд ботнет суурин хэзээний бий болсон байгааг гадаад улсын Кибер довтолгоотой тэмцэх байгууллагуудаас анхааруулж байна.[12]

1.2. Кибер орчинд үйлдэгдэж байгаа гэмт хэргийн шалтгаан, нөхцөл

Гэмт хэргийн шалтгаан, нөхцөлийг судалж тогтоохгүйгээр криминологийн прогноз боловсруулж чадахгүй. Прогнозгүйгээр гэмт хэргээс урьдчилан сэргийлэх ажлыг амжилттай төлөвлөн хэрэгжүүлж чадахгүйд хүрч болох юм. Өөрөөр хэлбэл, энэ гурван ажиллагаа хоорондоо нягт холбоотой харилцан бие биенээсээ хамааралтай ойлголт юм.

Гэмт хэргийн шалтгаан, нөхцөлийг судлах ажиллагааны эцсийн зорилго нь судалгааны ажлын үр дүнг практик амьдралд хэрэглэж гэмт хэрэг, зөрчлөөс урьдчилан сэргийлэх, нийгмийн сөрөг үзэгдлүүдийг арилгахад чиглэгдсэн арга хэмжээ авах учиртай.

Гэмт хэргээс урьдчилан сэргийлэх ажлыг төлөвлөхдөө дан ганц шалтгаан, нөхцөлийг судалсан судалгааны ажилд тулгуурлах нь учир дутагдалтай. Учир нь гэмт хэргээс урьдчилан сэргийлэх ажлыг төлөвлөхөд маш олон төрлийн тоо, баримт, мэдээ, мэдээллүүдийг цуглуулсан байх шаардлагатай байдаг байна.

Үүнд:

1. Урьдчилан гаргасан криминологийн болон бусад шинжлэх ухааны прогноз,
2. Тухайн нутаг дэвсгэрт үйлчилж байгаа болон үйлчлэх хууль эрхийн актууд,
3. Нийгэм, эдийн засаг, улс төр, эрх зүй, удирдлага зохион байгуулалтын талаарх авах арга хэмжээний төлөвлөлт, тэдгээрийн хэрэгжилт,
4. Төлөвлөлт явуулах нутгийн онцлог, хүн ам зүйн байдал, дэд бүтцийн хөгжил,
5. Оршин суугч иргэдийн ёс заншил,
6. Хууль сахиулах, хэрэгжүүлэх байгууллагуудын үйл ажиллагааны талаарх олон нийтийн санаа бодол,
7. Гэмт хэрэг, зөрчилд холбогдож болзошгүй хүмүүсийн тухай, гэмт хэрэг ихээр үйлдэгддэг газруудын талаарх сүүлийн үеийн тоо баримт, судалгаа,
8. Гэмт хэрэг үйлддэг болон үйлдэж болзошгүй шинэ аргуудын мэдээ,
9. Гэмт хэргээс урьдчилан сэргийлэх талаарх практикийн байгууллагын ажилтан, эрдэмтэн судлаачдын судалгаа, санал бодол, туурвисан ном зохиол,
10. Тухайн нутаг дэвсгэрт зохиогдож байгаа баяр ёслол, уулзалт өдөрлөг гэх мэт олон нийтийг хамарсан арга хэмжээний төлөвлөгөө,

[11]ЦЕГ-ын ЭЦГ-ын гаргасан судалгаа 2014 оны 03 сар
[12] КДХТ-ын судалгаа Т.Халтар 2013

11. Урьд нь гэмт хэргээс урьдчилан сэргийлэх ажил зохион байгуулж үр дүнд хүрээгүй шалтгаан нөхцөлийг судалж дүгнэлт хийх зэрэг бусад шаардлагатай баримт материалууд байна.Энэ талаарх мэдээллийг бид анхаарч үзэх нь зүйтэй юм.

Гэмт хэргийн шалтгааныг төрлийн хувьд тодорхой хэлбэрээр гэмт хэргийн ерөнхий нөхцөл, шууд шалтгаан, гэмт хэрэг үйлдэх шалтаг, гэмт хэрэг үйлдэхэд хөнгөвчилсөн нөхцөл гэж хувааж болно. Гэмт хэргийн шууд шалтгаанд гэм бурууtан этгээдийн нийгмийн эсрэг зан чанар, хувийн байдлаар тодорхойлогддог тийм нөхцөл байдлууд голлон хамаарагдана. Гэмт хэрэг үйлдэх шууд шалтаг нь тодорхой хэлбэрийн нийгэмд аюултай үйл явдлын шууд шалтгаан мэт байх боловч агуулгаар уг шалтгааны хэрэгжихэд гадна талаас нь нөлөөлдөг байна.[13]

Гэмт хэргийн хор уршгийн зайлшгүй болон тохиолдлын аль нь болохыг ялгах нь тухайн үйл явдлын эхлэлээс эцсийн төгсгөл хүртэлх процессуудын шалтгааны хөгжилтөнд дүн шинжилгээ хийж, тодорхой гэмт хэрэг бүрийн бүрэлдэхүүний онцлогоос үндэслэн шийдвэрлэгдэж байх ёстой. Үйл явдлын төгсгөл зайлшгүй ба тохиолдлын байдалтай байдаг нь түүний шалтгаант холбоо нь мөн зайлшгүй ба тохиолдлын байдгаас үндэслэдэг. Иймээс шалтгаант холбоог тохиолдлын ба зайлшгүй гэж ангилах нь бүх төрлийн шинжлэх ухааныг танин мэдэхэд чухал зорилт болдог билээ. Зайлшгүй шалтгаант холбоо гэдэг нь тухайн процессын хөгжилтийн шийдвэрлэгч, тодорхойлогч хүчин зүйл нь бөгөөд гарцаагүй буй болох үр дагаварын тодорхой нөхцөлүүдийг бий болгодог ажээ. Тохиолдлын шалтгаант холбоо нь тухайн үр дагаварын шийдвэрлэх үндэс нь болдоггүй боловч шууд бусаар тэр үр дагаварыг буй болоход нөлөөлсөн байж болох нөхцөл байдлыг бүрдүүлдэг.[14]

Манай улсад үйлдэгдэж байгаа кибер гэмт хэргийн үндсэн шалтгаан нь хувь хүн, байгууллагын мэдээллийн аюулгүй байдлын хамгаалалт сул, дорой байгаатай шууд холбоотой.

Дэлхий хувьсан өөрчлөгдөхийн зэрэгцээ кибер орчны өнөөгийн байдал ч хувьсан өөрчлөгдсөөр байна. Дэлхийн улсуудад Интернетийн хэрэглээ эрс нэмэгдэж, зөвхөн компьютер төдийгүй төрөл бүрийн ухаалаг төхөөрөмж ашиглан сүлжээнд холбогддог болсон, өдөр тутмын амьдралын олон хэрэглээг ухаалаг төхөөрөмж, сүлжээ ашиглан эрхлэн явуулдаг болсон. Үүнтэй зэрэгцэн технологийн ололт амжилтыг зүй бус, гэмт хэрэг үйлдэх зорилгоор ашиглах төрөл, арга хэлбэр, технологи хөгжиж, хүн төрөлхтөний онцгойлон анхаарах, нэг мөр тэмцэх ёстой асуудал болон хувираад байна.

Өнөөдөр мэдээллийн технологийн ололт амжилтыг хууль бус үйлдлүүд төдийгүй гэмт хэрэг үйлдэх, бусад улсын эсрэг хорлон сүйтгэх, устгах, чадварыг бууруулах, тагнан турших зэрэг ноцтой зорилгоор ашигладаг боллоо. Жирийн нэг гэмт этгээд төдийгүй төрийн албан хаагч, тусгайлан бэлтгэгдсэн хүмүүс ч энэ төрлийн үйлдлийг тусгайлан үйлдэх болсон. Энэ төрлийн гэмт хэрэг, тагнан турших үйлдлүүдинн арга, технологи нарийсч илрэх магадлал нь улам багассаар байна. Төрөл бүрийн хортой кодуудыг цахим шуудан, нийгмийн сайтууд, зомби компьютер ашиглан тараах, зөгийн үүр маягийн (botnet) зүй бус сүлжээ үүсгэж бусдын тооцоолох төхөөрөмжийг өөрийн мэдэлд авах (zombie), ухаалаг төхөөрөмжүүдийг хордуулах, зайнаас удирдах, санхүүгийн ашиг олох зорилготой онлайн залилан, сүлжээ, системийн халдлага үйлдэх, зүй бус агуулга бүхий зар сурталчилгааг тараах, хэрэглэгчийн тооцоолох техөөрөмжийг удирдлагадаа авах замаар байгууллагын системд нэвтрэн орж, хортой үйлдлүүд гүйцэтгэх, өгөгдлийг замаас нь барьж авах, нууцаар сонсох зэрэг хэдэн арван мянган аргаар гэмт үйлдлийг үйлдэх боллоо.

Өнөөдөр 15-35 насны дундаж хэрэглэгч өдөр бүр 2,5 цагийг сулжээнд, 4,6 цагийг

[13]Г.Совд. “БНМАУ-ын эрүүгийн эрхийн курс”, УБ., 1973, 146 дахь тал.
[14]Мөн тэнд. 213 дахь тал.

тооцоолох төхөөрөмж дээр ажиллаж өнгөрүүлдэг, 10-20 веб сайт, онлайн хэрэглээнд тогтмол ханддаг болсон талаар судалгаа байна. Оффисын бүх баримт бичгийг тооцоолох төхөөрөмжөөр боловсруулж, албан ажлын 70 гаруй хувийг сүлжээгээр гүйцэтгэдэг болсон. Гэтэл дээр дурдсан хууль бус үйлдэл, халдлага, зөрчил, гэмт хэргийн шинжтэй үйлдлүүд жил бүр 10-аас доошгүй хувиар өсөж хохирол нь жил бүр 20 хувиар өсөж байгаа талаар ЦЕГ-ын Мэдээлэл судалгааны төвөөс эрхлэн гаргадаг гэмт хэргийн мэдээнээс харж болохоор байна. Дэлхийн улс, орнууд үндэсний бодлого, стратеги гаргах, хүний нөөцөө бэлтгэх, хамгаалалтын дэд бүтэц бий болгох, байгууллага бүр бодлого, журам батлан мөрдөж, эрсдлийн үнэлгээ. аудит дээр суурилсан хамгаалалтын шийдлүүд хэрэгжүүлэх, кибер гэмт хэрэгтэй тэмцэх тогтолцоогоо бий болгох, эрх зүйн орчин, хамгаалалтыг бий болгох, бүх нийтийн мэдлэг, ойлголтыг дээшлүүлэх замаар энэ зүй бус үзэгдэлтэй эрчимтэй тэмцэж байна. Харамсалтай нь Монгол Улсад “үндэсний аюулгүй байдлын үзэл баримтлал”-ыг шинэчлэн баталж “Мэдээллийн аюулгүй байдлын үндэсний хөтөлбөр” гаргасан ч хэрэгжилт хангалтгүй, ялангуяа хуулийн салбарын ажилтнуудын ойлголт мэдлэг хомс, кибер гэмт хэрэгтэй тэмцэх туршлага, мэдлэг байхгүй, техникийн хангалт, шинжлэн судлах чадвар бүрэлдээгүй, эрх зүйн зохицуулалт, орчин хоцрогдсон хэвээр, хууль, хяналтын байгууллагууд өөрсдөө кибер халдлага, гэмт хэргийн хохирогч болсоор байна. Эрүүгийн хуулийн хоцрогдсон 4 заалт, Захиргааны хариуцлагын хуулийн 1 заалтаас өөр кибер гэмт үйлдэлтэй тэмцэх зохицуулалт байхгүй, тооцоолох төөхөөрөмжөөс нотлох баримтуудыг гарган авах, баталгаажуулах техник хэрэгсэл, мэргэжилтэн байхгүй, энэ төрлийн гэмт хэргүүдийг зүйлчлэхээс авахуулаад хариуцлага оноох тал дээр учир дутагдалтай байна.

Өсвөр үеийг мэдээллийн технологийн хэрэглээнд сургадаг ч аюулгүй, зохистой хэрэглээнд сургах, кибер орчны төрөл бүрийн аюулаас сэргийлэх мэдлэг, ойлголт өгдөггүй учир кибер гэмт хэргийн хохирогч болох магадлалыг нэмэгдүүлсээр байна. Тиймээс нийгэм даяараа аюулгүй, зохистой хэрэглээний туршлага, ойлголт сул, кибер гэмт хэргийн хохирогч болсон ч тийм байх мэтээр хүлээн авдаг байдал төлөвшиж байна. Их дээд сургуулиудад ч энэ талын мэргэжилтэн бэлтгэх тал дээр сул анхаардаг, бэлтгэж буй мэргэжилтнүүд нь ерөнхий чиглэлийн, орчин үеийн шаардлагаас хоцорсон байдалтай байна. Мэргэжилтнүүдийг цаашид мэргэшүүлэн бэлтгэх үндэсний бололцоо нөөцөө огт ашигладаггүй, хөрөнгө мөнгө хуваарилдаггүй, удирдлага дэмждэггүй зэргээр цааш үргэлжилнэ.

Үндэсний дэд бүтцийг хамгаалах техникийн хамгаалалтууд бий болж байгаа боловч дотроосоо үүсэх аюулуудаас хамгаалагдаагүй, удирдлага, зохион байгуулалт сул, бодлого, журмууд бараг байхгүй, эрсдлийн үнэлгээ, аудит огт хийлгэдэггүй учир гэмт хэрэг байнга үйлдэгдсээр, түүнийг ердийн байдаг л үзэгдэл мэтээр хүлээн авдаг сэтгэхүй төлөвшиж байгаа нь ухаалаг төрийг бий болгох, мэдээллийн технологи хөгжих, төр, бизнесийн онлайн үйлчилгээ нэвтрэхэд ноцтой саад болох, нийгмийн сэтгэл зүйг хордуулах, гаж ойлголт, сэтгэлгээг төлөвшүүлэх, гэмт этгээдүүдэд ял завшуулах, иргэдийн эрх, эрх чөлөөг ноцтой зөрчих боломжийг олгоод зогсохгүй нийгэм, эдийн засаг, улс төрийн ихээхэн хохирол учруулах магадлалтай байна.

Монгол Улсын хувьд орчин үеийн цахим, кибер гэмт хэргийг гэмт хэрэг гэж үзэх үндэслэл, зохицуулалт байхгүй, кибер гэмт хэрэгтнүүд үйлдлээ чөлөөтэй хийж болох талбар болон хувирч байна. Цахим файл, өгөгдлийг нотлох баримт гэж тооцохгүй учир ихэнх кибер гэмт хэргийг мөрдон шалгах ажиллагаа мухардалд орох магадлалтай байна. Тооцоолох хэрэгслийн бүртгэл, аудитын файлуудыг гаргаж авах, шинжлэх, түүнээс нотлох баримтууд олох, бэхжүүлэх талын ямар ч чадвар, тогтолцоо, дэд бүтэц, хүний ноөц байхгүй учир кибер гэмт хэргийг илрүүлэх чадвар маш доогуур түвшинд байна. Хуулийн байгууллагын ажилтнуудын зарим нь өгөгдөл, мэдээлэл, файл, програм гэдгийн ялгааг мэдэхгүй, эрүүгийн хуулийн холбогдох заалтыг зөв ойлгож тайлбарлах чадваргүй байгаа нь энэ төрлийн гэмт хэрэгтэй тэмцэх чадвар маш доогуур байгааг харуулж байна. Олон улсын хамтын ажиллагаа огт хөгжөөгүй учир хил дамжин үйлдэгддэг кибер гэмт хэргийг илрүүлэх боломжийг үгүй

болгож байгаа юм.

1.3. Кибер орчинд үйлдэгдэж байгаа гэмт хэргийн чиг хандлага

Монгол Улсын чиг хандлага, бодлого

Монгол Улсын Их Хурлаас мэдээллийн харилцаа холбоо технологийн талаар баримтлах суурь бодлого боловсруулан батлуулж хэрэгжүүлж байна.

Монгол Улсын Их Хурлын 2008 оны 12 дугаар тогтоолоорМонгол Улсын мянганы хөгжлийн зорилтод суурилсан үндэсний хөгжлийн цогц бодлого /2008-2021/ батлан мөрдүүлж байна. 5.3.4. Мэдээлэл, харилцаа холбооны технологийн хөгжлийн бодлогыг тодорхойлохдоо “Мэдээлэл, харилцааны технологийг Монгол Улсын эдийн засаг, нийгмийн хөгжлийн 21 дүгээр зууны үндсэн хурдасгуур гэж үзнэ”[15] гэж.

Засгийн газрын 2012 оны 101 дүгээр тогтоолын “Цахим засаг” үндэсний хөтөлбөр батлан мөрдүүлж байна:

Төрийн байгууллагын үйл ажиллагааг ил тод, нээлттэй байлгах, төрийн бодлого боловсруулахад иргэдийн оролцоог нэмэгдүүлж, төрөөс үзүүлж байгаа үйлчилгээг хүртээмжтэй, чирэгдэлгүй болгож, цахим засгийн үйлчилгээг хөгжүүлж нэвтрүүлэх зорилгоор “Цахим засаг” үндэсний хөтөлбөрийг 2012-2016 онд хэрэгжүүлж дуусгах зорилготой боловсруулсан[16].

Энэхүү хөтөлбөрийг /цахим засгийг хөгжүүлсэн/АНУ, ХБНГУ, БНСУ, Малайз Улс, Шинэ Зеланд Улс, Япон Улс, БНЭУ зэрэг орны туршлагыг судалсаны үндсэнд хэрэгжүүлсэн.

Энэхүү хөтөлбөртдараах байрыг цахим хэлбэрт зохион байгуулах болсон:

- Арын алба /**back office/** аж ахуй, санхүү, хүний нөөц, архивын үйл ажиллагаа,
- Тоон ялгаа /**digital divide/** телевиз, радио, интернет, холбоо, шуудангын үйл ажиллагааг,
- Цахим үйлчилгээ хүргэх /**electronic service/** цахим хэлбэрээр үйлчилгээ явуулах ажиллагааг,
- Цахим гүйлгээ /**electronictransaction**/ МХХ-ны сүлжээгээр гүйлгээний үйл ажиллагааг,
- Цахим зах зээл /**electronicmarket**/ цахимаар худалдах худалдан авах үйл ажиллагааг,
- Цахим хангамж /**e-procurement/** цахимаар хангамж үйлчилгээг зохион явуулах,
- Мэдээллийн дэд бүтэц /**information infrastructure**/ цахим мэдээллийн ертөнцийг тогтвортой хангах,
- Мэдлэгт суурилсан нийгэм “мэдээлэлжсэн нийгэм” /**know ledge based society/ information society/** мэдлэг бүтээгч, хэрэглэгч нийгэм цогцлуулах, оюуны үйлдвэрлэлийг орон зай цаг хугацаанаас үл хамааралтай зохион байгуулах,
- Шинэ эдийн засаг /**new economy**/ уян хатан эдийн засгийн бүтцийг бий болгох,
- Оюунлаг үйлдвэрлэл /**smart factory**/ программ хангамж нь оюуны багтаамжтай автомат удирдлагатай үйлдвэрлэлийг нэвтрүүлэх зэрэг тодорхой салбарын үйл ажиллагааг цахим нөхцөл байдалд шинээр зохион байгуулах үйл ажиллагаа нэгэнт бодит зүйл болж эхлэсэн нь хууль-эрх зүйн салбарынхан нэн түрүүнд анхаарах асуудал гэж үзэх ёстой.

Өнөө үеийн хөгжлийн тэргүүлэх салбарын нэг нь өндөр хүчин чадалтай техник хэрэгсэл, ухаалаг технологи болж байгаа учир Монгол Улс **2014 оныгмэдээлэл харилцаа холбоо технологийн эрх зүйн шинэчлэлийн жилээр зарласан** нь учиртай.

Салбарын хөгжлийг дэмжсэн эдгээр бодлогын үр дүнд дэлхийн 200 гаруй улсаас мэдээллийн технологийн хөгжлийн түвшинээр манай улс 2013 онд 63 дугаар байрт жагсаж[17], үсрэнгүй хөгжилтэй зарим орны өмнө нэрлэгдэж байгаа нь гар утас, интернэт,

[15]Монгол Улсын Засгийн газрын тогтоол 2012 оны 04.04 дугаар 101 “Цахим засаг” Үндэсний хөтөлбөр /3.3 заалт/
[16]Монгол Улсын Засгийн газрын тогтоол 2012 оны 04.04 дугаар 101 “Цахим засаг” Үндэсний хөтөлбөр
[17]МТШХХ-ны газрын 2013 оны үйл ажиллагааны тайлан

компьютергүйгээр залуу үеийнхний амьдралын хэв маягийг төсөөлөх аргагүй болсонтой холбоотой.

Ухаалаг техник-технологи өдөр өдрөөр улам бүр хөгжиж түүний үр дүнд ухаалаг техник-хэрэгсэл нийт хүн төрөлхтний өдөр тутмын бодит хэрэглээ болсон.

Цахим мэдээ, мэдээлэл, цахим эдийн засаг, цахим ардчилал, цахим засаг, цахим бизнес, цахим банк, цахим эрүүл мэнд, цахим боловсрол, цахим хөдөө аж ахуй,цахим худалдаа, цахим гааль, цахим татвар, цахим гарын үсэг, цахим үнэмлэх /паспорт/ гээд л амьдралын бүхий л хэмнэл гагцхүү мэдээлэлийнхарилцаа холбооны дэвшилтэт технологийн салшгүй бүрэлдэхүүн хэсэг болж байгаа нь маш их давуу талтай байгаа хэдий ч хөгжил дэвшлийн сөрөг үзэгдэл болсон уламжлалт гэмт хэрэг, зөрчил, маргааны бүтэц, шинж өөрчлөгдөж улмаар цахим хэлбэрт хувирч, тодорхой төрлийн гэмт хэргүүд шинээр бий болж, мэдээллийн сүлжээ, систем, мэдээллийн нэгдмэл-бүрэн бүтэн байдал, нууцлал, хамгаалалтад заналхийлэх аюул олширч, эрсдэл урд өмнө байгаагүйгээр эрс нэмэгдэж иргэн, байгууллага, аж ахуйн нэгжийн эрх, ашиг сонирхолд их хэмжээний хор уршиг учруулах түвшинд хүрч байгаа нь нэгэнт бодит зүйл болжээ.

Иймд аливаа шинэ тогтолцоог бүрэлдэж эхлэхтэй зэрэгцүүлэн нэгдсэн ойлголттой болж, бодлого тодорхойлж, нэгдмэл уялдаа холбоо бүхий эрх зүйгээр зохицуулахгүй бол өнөөгийн нийслэлиийн замын хөдөлгөөний сөрөг үзэгдэлбүхэн энгийн зүйл мэт болсонтой адил төсөөлхийн аргагүй сөрөг үр дагавар, хүндрэлийг бий болгох нь ойлгомжтой.

Дэлхийн чиг хандлага

Хүн төрөлхтөн шинжлэх ухаан, технологийн хувьсгалд тулгуурлан аж үйлдвэржсэн нийгмээс мэдээлэлжиж, даяаршиж буй нийгэмд шилжиж байна.

Дэлхий дахинд хүмүүс, эдийн засаг, мэдээлэл, барааны асар өргөн шилжилт хөдөлгөөн, бараа бүтээгдэхүүн, үйлчилгээний хил хязгааргүй урсгал, түүнд суурилсан даяаршилын цоо шинэ нөхцөл байдал бүрдэж байгаагаас улс орон бүр нийгмийн хөгжил, эдийн засгийн өсөлтийн хэтийн бодлогоодаян дэлхийн болон бүс нутгийн хөгжлийн үйл явцтай нягт уялдуулан тодорхойлох болов.

Тооцоолох хэрэгслийн хүчин чадал, өгөгдөл хадгалах техник-технологи өртөг, тоо, чанарын хувьд улам бүр хямд, нийтэд хүртээмжтэй болсоноор ухаалаг гар утас, компьютер, нөүтбүк, таблетийн хэрэглээ эрс өсч байгаа энэ үед дамжуулагдаж буй мэдээлэл нь ямар эрсдлийг үүсгэж байгаа талаар судлан түүнээс хамгаалах ямар боломж байгаа талаар дэлхий нийт анхаарал хандуулж эхэлсэн.

Өндөр хүчин чадалтай ухаалаг технологийн хөгжлийн төсөөлшгүй хурдын хажуугаар мэдээллийн аюулгүй байдлын асуудал зөвхөн програм-техник хангамжийн асуудал байхаа больж улам бүр нарийн төвөгтэй, эрх зүй-удирдлага зохицуулалтын тулгамдсан асуудал болон хувирч байна.

Ийм нөхцөлд Монгол Улсын хөгжилд дэлхийн, ялангуяа Ази тив, Төв болон Зүүн хойд Азийн бүс нутгийн хөгжлийн хандлага, даяаршлын эерэг болон сөрөг хүчин зүйлсийн нөлөөллийн аль алийг нь тооцож, хөгжлөө эрчимтэй бөгөөд тогтвортой явуулахын тулд урт, дунд, богино хугацааны хөгжлийн бодлого, стратеги тодорхойлох шаардлага тулгарч байна.

Хурдацтай хөгжиж буй дэлхийн глобал чиг хандлагаар өнөөдөр мэдээлэлжсэн цоо шинэ нийтийн амьдралд шилжих үйл явц өрнөж, Zettabyte, Big Data-ын эрин үе эхэлсэнээр салбарын мэргэжилтэн нар 2000 оноос эхлэн тусгай хөтөлбөр гарган ажиллаж байна. /вирусын эсрэг болон хамгаалалтын технологи, эрх зүй, хамтын ажиллагаа гэх мэт/

Интернетийн болон бусад ухаалаг технологийн сүлжээг өргөн ашиглаж амьдрах нь гарцаагүй бодит зүйл болсон учир комьютергүйгээр нэг ч өдрийг өнгөрөөх боломжгүй болжээ.

Сүлжээгээр дамжин гаднаас төдийгүй дотроос эх үүсвэртэй халдлага, зөрчил, гэмт хэргүүд ч жил бүр нэмэгдэж, учруулах хохирол нь үлэмж ихсэхийн зэрэгцээ Монгол Улсад

мэдээллийн болон сүлжээний аюулгүй байдлын удирдлагын шинэ тогтолцоо бий болгох зайлшгүй шаардлага тулгарч байгаа байна.

Бодитой болсон энэ хөгжил дэвшил нь хүн төрлхтөнийг хөгжүүлж өөр хооронд нь мэдээллийг шуурхай хүргэж байгаа нь өнөөгийн амьдрал, үйл ажиллагааны чухал хэрэгсэл болсон ч мэдээллийн технологийг ашиглан урд өмнө мэдэгдэж байгаагүй, ойлгох ч боломжгүй байсан гэлтэй төрөл бүрийн халдлага, гэмт хэрэг, зөрчил үйлдэгдэж байгаа билээ.

Тухайлбал, энэ салбарт үйлдэгдэж байгаа гэмт хэрэг, зөрчил нь уламжлалт гэмт хэргээс эрс ялгаатай, гэмт хэрэгтэн зөвхөн комьютерийн ард суугаад тагнах, хулгайлах, дээрэмдэх, залилах, хүчирхийлэх, бусад байдлаар хүний халдашгүй байдалд нь халдах зэргээр гэмт хэрэг үйлддэг болсон нь бодит зүйл болсон. Хакерууд засгийн газрын харьяа байгууллагууд, бизнесийнхэн, батлан хамгаалах цэрэг, хууль сахиулах байгууллага /гааль, татвар, эрчим хүч/ зэрэг байгууллага, хувь хүний мэдээллийн сангаас өдөрт 1ТВ гаруй мэдээлэл хулгайлж байгааг мэргэжилтнүүд тооцоолжээ[18].

Түүнчлэн дэлхийн өндөр хөгжилтэй улс орнуудад онлайн мөрийтэй, бооцоотой тоглоомууд, байгууллага болон хувь хүмүүсийн гэрийн хамгаалалтын систем зэрэгт халдах тохиолдол эрс нэмэгдэж байгаа талаар “McAfee” компаний тайланд дурдсан байна. Манай улсад ч сүүлийн үед баригдаж байгаа орон сууц, оффисын барилгууд цахим цоож, хамгаалалтын систем зэргийг нэвтрүүлж байгаа нь санаа зовох асуудал болон хувирах магадлалтай.

Дэлхий дахинд хурдацтай өсч буй кибер халдлагуудын нэг бол Фишинг /Phishing/ юм. Уг халдлага нь кибер гэмт хэргийн энгийн нэг халдлага боловч асар их хохирол учруулдаг ажээ. Учир нь кибер гэмт хэргийг үйлдэж буй тухайн этгээдээс зөвхөн программын мэдлэг шаардлагагүй бөгөөд цахим хуудас /website/ хийх мэдлэгтэй байхад л хангалттай. Тухайн гэмт үйлдлийн гол зорилго нь тухайн золиосолж буй этгээд нь тухайн цахим хуудсанд зочилсон тохиолдол бүрт түүнийг цахим гэмт хэргийнхээ золиос болгодог ажээ.[19] Энэ нь хэрэглэгчтэй холбоотой чухал мэдээллийн сэжүүрийг илэрхийлэх гол зэвсэг болгон ашиглан, ямар нэгэн тоног төхөөрөмжөөрөө дамжуулан ямар нэгэн зүйл татаж авах болгонд хортой програмыг хэрэглэгчид рүү хайр найргүй явуулдаг байна. Хэрэглэгчийн санхүүгийн өгөгдөл мэдээ мэдээллийг хулгайлахын тулд фишингийн аргыг ашигладаг нь кибер халдлагын талаарх “Kaspersky” компанийн лабораторийн судалгаанаас илэрхий болжээ.[20]

Мөн скимминг /skimming/-ийн талаар дурдахгүй өнгөрч болохгүй. Скимминг гэдэг нь ATM буюу бэлэн мөнгөний автомат машинд суурилуулсан тусгай төхөөрөмжийн туслалцаатай хэрэглэгчийн банкны гүйлгээний картын мэдээллийг хуулбарлан авах гэмт үйлдэл гэж тодорхойлж болох юм. Энэхүү гэмт үйлдэл нь дэлхийн өндөр хөгжилтэй улс орнуудад ихээр үйлдэгдэж байгаа бөгөөд Холливүүдийн луйвар, залилангийн тухай өгүүлэх кинонууд дээр ч ихээр гарах болсон. Манай улсын хувьд энэ төрлийн гэмт хэрэг гарахгүй гэх баталгаагүй. Иймд

[18] "Frequently asked questions and answers Council of Europe Convention on cybercrime", by the United StatesDepartment of Justice 2010
[19] http://www.datacenter.gov.mn/2597.html
[20] https://securelist.com/files/2015/02/KSN_Financial_Threats_Report_2014_eng.pdf

Хууль сахиулах салбарын болон, банк санхүүгийн байгууллагуудын ажилтан, алба хаагчдыг мэдээллээр хангах, урьдчилан сэргийлэх асуудал зүй ёсоор тавигдаж байгаа юм.

“Kaspersky” компанийн лабораторийн өнгөрсөн оны тайланд санхүүгийн халдлага хамгийн ихээр үйлдэгдэж байгаа дэлхийн улс орнуудыг 2013, 2014 оны үзүүлэлтийг дараах байдлаар харьцуулан гаргажээ.[21]

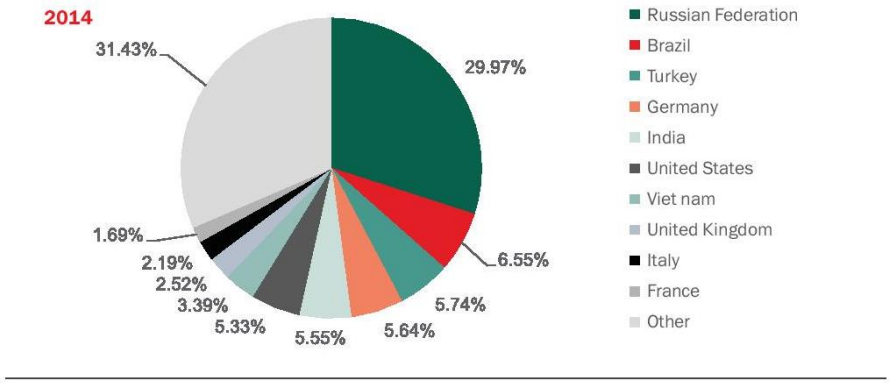


Fig. 20. Geographical distribution of attacks by financial malware in 2014[2]

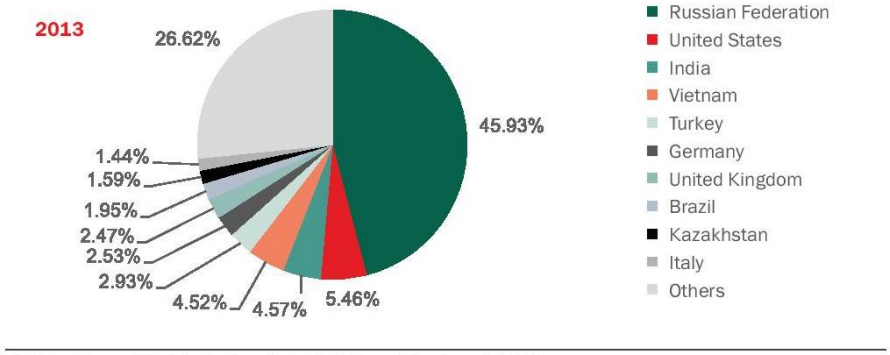


Fig. 21. Geographical distribution of attacks by financial malware in 2013

Хэдхэн жилийн өмнө компьютерийн болон сүлжээний аюулгүй байдал онц чухал асуудал хэмээн тооцогдож байсан бол өнөөдөр нөхцөл байдал бодитойгоор эрс өөрчлөгдөж улмаар мэдээллийн аюулгүй байдлын цогц удирдлага, зохицуулалт бий болгох, нэгдсэн бодлого, хөтөлбөр, эрх зүйн цоо шинэ дэг журам батлан хэрэгжүүлж бодитой бий болж байгаа төрөл бүрийн халдлага, будлиан, санамсаргүй тохиолдол, гэмт хэргийн үйлдэл бүрт эсрэг хариу үйлдэл хийх, түүнийг мэдээллэх, удирдах, сөрөг арга хэмжээ боловсруулах /сургалт, технологи ба ёс зүйтэй хэрэглээ гэх мэт/, мөрдөн шалгах, шинжлэх, баримтжуулах, хуулийн дагуу бодитой шийдвэрлэх шаардлага тулгарч байна.

Кибер орчин дахь мэдээллийн аюулгүй байдлын тухай

Мэдээллийн аюулгүй байдлын хүрээнд Мэдээлэл нь тухайн хувь хүн, байгууллагын үйл ажиллагаа ажил хэргээ хэвийн явуулахад шаардагдах гол хөрөнгө, баялаг учир техникээр, эрх зүйгээр зайлшгүй хамгаалагдсан байх ёстой.

МАБ гэдэг нь ажил хэргийн үйл ажиллагааг тасралтгүй, хэвийн байх нөхцөл байдлыг хангах, эрсдэлийг багасгах, хөрөнгө оруулалтын үр ашиг, бизнесийн боломжийг нэмэгдүүлэхийн тулд мэдээллийг олон янзын аюул, заналаас хамгаалах ажиллагаа. Мэдээлэл цуглуулах, боловсруулах, хадгалах, түгээх, дүн шинжилгээ хийж зохистой ашиглах чадвараар байгууллагын манлайлал үнэлэгдэг учраас МАБ чухал.

Мэдээллийн аюулгүй байдал нь мэдээлэл болон мэдээллийн сүлжээ, системд зөвшөөрөлгүй хууль бусаар нэвтрэх, хандах, мэдээллийг ашиглах, ил болгох, өөрчлөх, хуулах, устгах, мэдээллийн системийн үйл ажиллагааг тасалдуулах, хяналтад байлгах зэрэг хууль бус бүхийл үйл ажиллагаанаас хамгаалах цогц тогтолцоог ойлгоно.

МАБ-ын үндсэн 4-н зарчимыг тодорхойлж болно:

Үнэн зөв, бодитой мэдээллийг Зөв хүнд Зөв цагт Зөв хэлбэр бүтэцтэйбүрэн бүтэн хүргэж байх явдал.

[21] Kaspersky Lab Report “Financial cyberthreats in 2014”

Мэдээлэл харилцааны салбарт үндэсний аюулгүй байдлыг хамгаалах үүднээс Улс, иргэн, хувийн хэвшлийн мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй хэвийн байдлыг баталгаажуулах тухай цогц ойлголт багтана.

МАБ-ыг хангах хууль тогтоомжийн түвшин

Гол хоёр багц арга хэмжээг авах зорилгоор хэрэгжүүлдэг. Үүнд.

• Нийтэд МАБ-ын ойлголт, мэдлэгийн түвшинг дээшлүүлэх, амьдрал үйл ажиллагаанд хэвшүүлэх, сургах арга хэмжээ авах үйл ажиллагааг зохион байгуулах,

• МАБ-ын зөрчил, зөрчил гаргагчдыг нийтийн зүгээс буруутгах, ял шийтгэл оноохыг шаардах зэрэг сэтгэц зүйг төлөвшүүлэх арга хэмжээ авахад чиглэгдэнэ.

МАБ-ын чухал шинж нь аливаа шинжилгээ, судалгаа, бодлогынажилд мэдээллийн нөөцийг төвлөрүүлэх, дээрхи дөрвөн түвшний хандлагыг байгууллага, иргэн бүрт бий болгох, боловсролын үйл ажиллагаанд танин мэдүүлж сургах, зөрчил гаргагчдыг шийтгэх хандлагыг бий болгох, төлөвшүүлэхэд бодлого, хууль тогтоомжуудыг чиглүүлэх онцлогтой.

Үүний тулд энэ салбарт хэрэглэгддэг үйл ажиллагааны дэс дараалал, ашиглагддаг техник-хэрэгсэл, хэрэглэгддэг нэр томъёог нэгдмэл байдлаар танин мэдсэнээр зохицуулах нэгдмэл хууль тогтоомжийг боловсруулах, аливаа сөрөг үзэгдэлтэй тэмцэх арга, арга зүйг богино хугацаанд хэрэгжүүлж чадна гэж үздэг.

МАБ-ыг хамгаалах үйл ажиллагаанд хэрэглэгдэж байгаа нэр томъёо:

МАБ-ыг хангах, хамгаалахын тулд олон улсын хэмжээнд энэ салбарт хэрэглэгдэж байгаа нэр томъёог хэрхэн ойлгох, хууль тогтоомжид хэрхэн тусгах, үйл ажиллагаандаа хэрэглэх нь нэн чухал асуудал бөгөөд энэ салбарт хэрэглэгддэг нэр томъёо бүгд “Англи” хэлээр илэрхийлэгддэг учир судлаачийн хувьд тайлбарлахыг зорилоо.

МАБ-д хэн нэгэн зөрчил гаргач халдахдаа хамгийн эхэнд мэдээллийн сүлжээнд эсвэл системд хууль бусаар нэвтрэх үйлдэл гүйцэтгэхээс эхлэнэ гэж үздэг түүнээс биш шууд мэдээллийн орчинд орж сүйтгэхгүй, энэ нь орон байр, агуулах сав-д нэвтэрч хулгайлах гэмт хэрэг үйлдэж байгаатай адил эхлээд л хууль бусаар нэвтэрнэ гэсэн үг.

Ийм учир мэдээллийн аюулгүй байдал /МАБ/, сүлжээний аюулгүй байдал /САБ/, системийн аюулгүй байдал /СиАБ/, техникийн аюулгүй байдал /ТехАБ/, хүний нөөцийн аюулгүй байдал /ХНАБ/, дэд бүтцийн аюулгүй байдал, орчины аюулгүй байдлын тухай ойлгох хэрэгтэй байх учир эхлээд товч тодорхойлолтыг хүргэж байна.

Эрүүгийн хуулийн 25 дугаар бүлэг[22]-т энэхүү нэр томъёололын ойлголтыг агуулгын хувьд дутагдалтай томъёолсон учир хуулийг хэрэглэх, гэм буруутай нэгэнд хариуцлага тооцоход хүндрэл учирч байна.

Компьютер болон мэдээллийн технологийн сүлжээ:2 буюу хэд хэдэн компьютер, ухаалаг технологи-хэрэгсэл хоорондоо холбогдон мэдээлэл болон эх сурвалжууд, нэмэлт төхөөрөмжүүдийг хамтран ашиглах боломжоор хангагдахыг хэлнэ.

Сүлжээний хэрэглэгчид нь файл, принтер, бусад зүйлээ хамтарч хэрэглэж болохоос кабель утасаар болон утасгүй сүлжээ, Компьютерүүдийг сүлжээнд холбохын тулд тэдгээрийн холболтын техник хангамжийн болон программ хангамжийн орчинг бүрдүүлж өгөх шаардлагатай.

Энд физик холболт хийх болон тэдгээрийг програм хангамжаар /WiFi/ холбох олон боломжууд бий болсон.

Компьютерийн хамгийн том сүлжээ нь Интернет юм.

• Сүлжээний техник хангамжийн орчин: Сүлжээний техник хангамж нь компьютерүүд хоорондоо холбогдоход зориулсан физик компонентууд юм.

Сүлжээний адаптер, сүлжээний кабель,hub, repeater, switch, router, brouter, модем, bridge, wireless гэх мэт физик төхөөрөмжүүдээс гадна кабель утсанд холбодог толгой буюу

[22]Монгол Улсын Эрүүгийн хууль 2002 он

connector, transceiver, vampire tape,сүлжээний бахь, сүлжээний хэвийн ажиллагааг шалгадаг тестер гэх зэргийг мөн авч үзнэ.

Зарим төхөөрөмжүүдийг сүлжээний үйлдлийн системд таниулж өгөх шаардлагатай байдаг.

- Сүлжээний програм хангамжийн орчин: сүлжээний компьютерүүдийг бусад компьютерүүдтэй нь холбох интерфейс болж байдаг сүлжээний үйлдлийн систем, сүлжээний протокол зэргийг ойлгоно. Ажиллуулах програм нь сүлжээний хэрэглэгчийн интерфэйс, мэдээлэл, файл, график, видео, принтер ба дискийн хэрэглэлтийн зөвшөөрөл тогтоох програмаас тогтоно.

Үүний нэг жишээ нь client-server юм.

- Систем: Мэдээллийн техник-хэрэгслийн мэдээлэл боловсруулж хадаглах, санах ой бүхий эд ангийн тогтолцоо,
- “Компьютерийн систем” гэж аль нэг нь эсвэл зарим нь програмтай холбогдож өгөгдлийг автоматаар боловсруулах үйл ажиллагааг хийдэг ямар нэгэн төхөөрөмж эсвэл хоорондоо холбогдсон төхөөрөмжүүдийн бүлэг эсвэл хамааралтай төхөөрөмжүүдийг;
- “Компьютерийн өгөгдөл” гэж компьютерийн системд боловсруулахад тохиромжтой хэлбэрт байгаа бодит байдлын аливаа дүрслэл, мэдээлэл эсвэл концепц, мөн түүн дотроо компьютерийн системийн аливаа функцийг гүйцэтгэх шалтгаан болох программыг агуулна.
- “үйлчилгээ үзүүлэгч” гэж Компьютерийн системийг ашиглан харилцаа холбоо хийх боломжийг үйлчилгээний хэрэглэгчдэд олгодог аливаа төрийн эсвэл хувийн хэвшлийн нэгжийг,

тус харилцаа холбооны үйлчилгээ эсвэл үйлчилгээний хэрэглэгчийн өмнөөс компьютерийн өгөгдлийг боловсруулдаг эсвэл хадгалдаг ямар нэгэн бусад нэгжийг;

- “мэдээллийн урсгалын өгөгдөл” гэж компьютерийн системийн аливаа харилцаа холбоотой хамааралтай, харилцаа холбооны хэлхээний нэг хэсэг болж компьютерийн системээр үүсгэгдсэн, харилцаа холбооны эх үүсвэр, очих газар, чиглэл, хугацаа, он сар өдөр, хэмжээ, үргэлжлэх хугацаа, суурь үйлчилгээний төрлийг тодорхойлох аливаа компьютерийн өгөгдлийг;
- Мэдээллийн техник:Ухаалаг гар утас, компьютер, нөүтбүк, таблет гэх мэт хэрэгсэл,
- Зөвшөөрөлгүйгээр нэвтрэх

Компьютерийн систем буюу сүлжээнд хамгаалалтыг эвдэн нэвтрэх үйлдэл.

- Зөвшөөрөлгүйгээр замаас нь барьж авах

Мэдээллийн технологийн систем, сүлжээний хэмжээнд дамжуулагдаж буй мэдээллийг техник хэрэгслийн тусламжтайгаар хууль бусаар барьж авах үйлдэл.

- Кракер (Cracker): Хакерын мэдлэгээ муу зүйлд хэрэглэж бусдын компьютерийн сүлжээнд нэвтрэх, мэдээллийг устгах эсвэл сүлжээ, системыг хорт муу санааны үүднээс ашигладаг хар хакер хүмүүс юм.
- Хакер /Hacker/: ёс зүйт хакерын тухайд мэдлэгээ ашиглан бусдын мэдээллийн сүлжээнд нэвтэрч аюулаасурьдчилан сэргийлэх зүйлд хэрэглэж ашигладаг цагаан хакер хүмүүс юм. Зарим тохиолдолд ёс зүйгүй хакер бас байна. Энэ талаар дараагийн бүлэгт дэлгэрэнгүй авч үзнэ.
- Компьютерийн луйвар

Эдийн засгийн ашиг өөртөө буюу бусдад олох зорилгоор компьютерийн мэдээлэл, программ-д мэдээлэл оруулах, өөрчлөх, арилгах, мэдээллийн боловсруулалтад өөр байдлаар нэвтэрч эдийн засгийн хохирол учруулан, бусдын эд хөрөнгө алдагдахад хүргэсэн үйлдэл.

- Компьютерийн хуурмаглал

Тодорхой мэдээлэл, бусад халдлагын зүйлийг хуурамчаар үйлдэхийн тулд компьютерийн мэдээлэл, программыг оруулах, арилгах, аль эсвэл мэдээллийн боловсруулалтад өөр байдлаар нэвтэрсэн үйлдэл.

• Компьютерийн мэдээлэл, программд хохирол учруулах

Компьютерийн мэдээлэл, программыг хууль бусаар арилгах, хохирол учруулах, чанарыг нь муутгах үйлдэл.

• Компьютерийн хорлон саатуулалт

Компьютерийн болон холбоо харилцааны системийн ажиллагаанд саад учруулах зорилгоор компьютерийн мэдээлэл, программыг оруулах, өөрчлөх, арилгах, дарах үйлдэл.

• Зохиогчийн эрхээр хамгаалагдсан компьютерийн программыг зөвшөөрөлгүй хуулбарлах.

Хуулиар хамгаалагдсан компьютерийн программыг хууль бусаар хуулбарлах, тараах, дамжуулах үйлдэл.

• Микро схемийг зөвшөөрөлгүй хуулбарлах

Хуулиар хамгаалагдсан хагас дамжуулагчийн микро схемийг хууль бусаар хуулбарлах, ашиглах, импортлох үйлдэл.

Нэмэлт жагсаалтад дараах үйлдлийг хамруулсан байна:

• Компьютерийн мэдээлэл, программыг өөрчлөх

Компьютерийн мэдээлэл, программыг хууль бусаар өөрчлөх үйлдэл.

• Компьютерийн тагнуул

Бусдад эдийн засгийн хохирол учруулах, өөртөө буюу гуравдагч этгээдэд хууль бус ашиг олох зорилгоор бизнес, худалдааны нууцыг ямар нэгэн эрх зүйн үндэслэлгүйгээр хориглогдсон арга хэрэглэн олж авах, задруулах, дамжуулах, ашиглах үйлдэл.

• Компьютер зөвшөөрөлгүй ашиглах

Компьютерийн систем, сүлжээг хууль бусаар хэрэглэн түүнийг ашиглах эрх бүхий хүнд хохирол учруулсан буюу учруулахаар байсан, аль эсвэл компьютерийн хэвийн ажиллагааг алдагдуулсан үйлдэл.

• Хуулиар хамгаалагдсан компьютерийн программыг зөвшөөрөлгүй ашиглах

Өөртөө болон бусдад хууль бусаар эдийн засгийн ашиг олох зорилгоор хуулиар хамгаалагдсан компьютерийн программыг хууль бусаар ашиглан эрх эзэмшигчид хохирол учруулсан үйлдэл.

Европын холбооноос дээрхи хоёр жагсаалтыг гаргахдаа дор дурьдсан зарчмуудыг мөрдөхийг санал болгож байгаа.

Иймд кибер орчинд нийтээр хэрэглэж байгаа нэршилүүдийг нэг мөр болгох, ойлголтоо нэгтгэж байж цаашдын бодлого, суурь бичиг баримт боловсруулах, тодорхойлох, мөрдүүлэх шаардлагатай гэж үзэж байна.

1. Кибер орчинд үйлдэгдэж байгаа гэмт хэрэгтэй тэмцэх эрх зүйн тогтолцоо, олон улсын чиг хандлага

Мэдээллийг тээж байгаа бодит зүйл нь аюулгүй орчинд найдвартай хамгаалагдах учиртай бөгөөд уламжлалт тээгчээс орчин үеийн тээх хэлбэр ялгаатай.

• Кибер орчны сүлжээнд,

• Кибер хэрэгслийн системд,

• Кибер орчны сүлжээний орчинд,

• Кибер техник хэрэгслийн эсрэггсэн хэлбэртэй байна гэж үздэг.

Манай улсын эрүүгийн хуульд компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг гэж тооцогдсон зарим үйлдлүүд өөр төрлийн гэмт хэргүүдэд /жишээлбэл: өмчийн эсрэг гэмт хэрэг буюу залилан мэхлэх гэх мэт/ хамаарагддаг.

Энэ нь уламжлалт гэмт хэргүүдтэй зарим шинжээрээ төсөөтэй боловч хуульчилсан шинжээрээ өөр учир гэмт хэргийн хуулийн шинэчлэлд анхаарах цаг нэгэнт болсоныг цаг үе шаардаж байна.

Компьютерийн болон кибер орчин дахь мэдээллийн эргэлтийн хүрээ гэмт халдлагад ихээр өртөх болсныг манай улсад анхаарч 1996 оны Монгол Улсын Эрүүгийн хуульд “Мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг”гэсэн 11 дүгээр бүлгийг анх удаа хуульчилсан[23]

- Компьютерийн мэдээллийг хууль бусаар өөрчлөх гэсэн 153 дугаар зүйл,
- Компьютерийн мэдээлэл программыг эвдэх,сүйтгэх гэсэн 154 дүгээр зүйл,
- Компьютерийн мэдээллийг хууль бусаар олж авах гэсэн 155 дугаар зүйл,
- Компьютерийн мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэх, борлуулах гэсэн 156 дугаар зүйл,
- Нянтай программ зохион бүтээх, ашиглах гэсэн 157 дугаар зүйлүүдийг хуульчилжээ.

Үүний дараа 2002 оны Эрүүгийн хуульд “Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг” гэсэн 25 дугаар бүлгийг хуульчилж[24],

- 226 дугаар зүйлКомпьютерийн мэдээлэл, программыг өөрчлөх, эвдэх, сүйтгэх гэсэн,
- 227 дугаар зүйл Компьютерийн мэдээллийг хууль бусаар олж авах гэсэн,
- 228 дугаар зүйлКомпьютерийн мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэх, борлуулах гэсэн,
- 229 дүгээр зүйл Нянтай программ зохион бүтээх ашиглах гэсэн заалтаар МАБ-ын хүрээнд эрх зүйн хамгаалалттай болсон хэдий ч энэ нь өнөөгийн теник технологийн хөгжил, хүний хэрэглээ болон сэтгэхүйн хөгжлийн шаардлага, агуулгад нэгэнт тохирохгүй болсон.

Мэдээллийн аюулгүй байдал хариуцсан мэргэжилтнүүдийн үзэж байгаагаар компьютерийн мэдээллийн нууцлал алдагдсан, гэмт хэрэг, зөрчилд өртсөн тухай мэдээллийг цагдаа, тагнуул болон Интернэтийн үйлчилгээний байгууллага ISP /internet service provider/, вэб сайтийн удирдлагуудын /administrator/ хэнд нь ч гэмт хэргийн тохиолдлыг тэр бүр тодорхой мэдээлдэггүй, харилцан мэдээлэл солилцохгүй байгаа нь эрх зүйн тогтолцоо хангагдаагүй гэдгийг онцлон тэмдэглэж ирсэн.

Дараагийн бүлэгт энэ чиглэлийн эрх зүйн зохицуулалт, тогтолцоог авч үзсэн болно.

[23]Монгол Улсын Эрүүгийн хууль 1996 он
[24] Монгол Улсын Эрүүгийн хууль 2002 он

БҮЛЭГ II. КИБЕР ОРЧИНД ҮЙЛДЭГДЭЖ БУЙ ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ ҮНДЭСНИЙ БОЛОН ОЛОН УЛСЫН ЭРХ ЗҮЙН ЗОХИЦУУЛАЛТ

2.1. Кибер орчинд үйлдэгдэж байгаа гэмт хэрэгтэй тэмцэх үндэсний эрх зүйн зохицуулалт, тогтолцоо

Монгол Улсын Эрүүгийн хуулийн “Компьютер, мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг” хэмээх 25-р бүлэг, 226-229-р зүйлд Цахим гэмт хэргийн зарим бүрэлдэхүүнийг хуульчилж, энэ төрлийн гэмт хэрэгтэй тэмцэж байна. Үүнийг хүснэгтээр илэрхийлбэл,

226-р зүйл. Компьютерийн мэдээлэл, програмыг өөрчлөх, эвдэх, сүйтгэх					
№	Халдлагын зүйл	Гэмт үйлдэл	Гэм буруугийн хэлбэр	Материаллаг хохирол	Эрүүгийн хариуцлага
1	226.1. Компьютер, компьютерийн программ, түүний төхөөрөмж (-ийг)	өөрчилсөн, эвдсэн, гэмтээсэн, ашиглах боломжгүй болгосон, мэдээллийн сүлжээг сүйтгэсэн (бол)	Санаатай (-гаар)	-	Хөдөлмөрийн хөлсний доод хэмжээ (цаашид “ХХДХ” гэх)-г 51-200 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох
					3-6 сарын хугацаагаар баривчлах
					2 жил хүртэл хугацаагаар хорих
	226.2.	Урьдчилан үгсэж тохиролцсон бүлэг буюу албан тушаалын байдлаа ашиглаж үйлдсэн	Шунахайн сэдэлт	-	ХХДХ-г 100-250 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох
					-
					3-5 жил хүртэл хугацаагаар хорих
227-р зүйл. Компьютерийн мэдээллийг хууль бусаар олж авах					
№	Халдлагын зүйл	Гэмт үйлдэл	Гэм буруугийн хэлбэр	Материаллаг хохирол	Эрүүгийн хариуцлага
2	227.1. компьютер, мэдээллийн сүлжээнд хадгалагдаж байгаа болон дамжуулж байгаа мэдээлэл	зөвшөөрөлгүйгээр хуулбарласан, бусад аргаар олж авсан	-	Бага бус хэмжээний хохирол	ХХДХ-г 51-100 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох
					3-6 сарын хугацаагаар баривчлах
					2 жил хүртэл хугацаагаар хорих
	227.2.	Урьдчилан үгсэж тохиролцсон бүлэг үйлдсэн	Шунахайн сэдэлт	Их буюу онц их хэмжээний хохирол учирсан	ХХДХ-г 100-25 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох
					-
					2-5 жил хүртэл хугацаагаар хорих
228-р зүйл. Компьютерийн мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэх, борлуулах					
№	Халдлагын зүйл	Гэмт үйлдэл	Гэм буруугийн хэлбэр	Материаллаг хохирол	Эрүүгийн хариуцлага
3	228.1. компьютер, мэдээллийн хамгаалалттай сүлжээ	Хууль бусаар нэвтрэх тусгай программ болон техник хэрэгслийг	-	-	ХХДХ-г 51-150 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох
					3-6 сарын хугацаагаар баривчлах

		бэлтгэсэн буюу борлуулсан			5 жил хүртэл хугацаагаар хорих
229-р зүйл. Нянтай программ зохион бүтээх, ашиглах					
№	Халдлагын зүйл	Гэмт үйлдэл	Гэм буруугийн хэлбэр	Материаллаг хохирол	Эрүүгийн хариуцлага
4	229.1. компьютерийн мэдээлэл	Компьютерийн программ зохион бүтээх, программд өөрчлөлт оруулах, нянтай программыг тусгайлан зохион бүтээх, түүнийг мэдсээр байж ашигласан, тараасан	Зөвшөөрөлгүйгээр устгах, хаах, өөрчлөх болон хуулбарлах зорилго	-	ХХДХ-г 5-50 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох
					100-200 цаг албадан ажил хийлгэх
					1-3 сарын хугацаагаар баривчлах
	229.2.	-	-	Их буюу онц их хэмжээний хохирол	ХХДХ-г 51-250 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох
					3-6 сар
					5 жил хүртэл хугацаагаар хорих

Эндээс харахад, Эрүүгийн хуульд тусгагдсан цахим гэмт хэрэг нь материаллаг болон хэлбэрийн бүрэлдэхүүнтэй, гэм буруугийн санаатай хэлбэртэй, хүндэвтэр болон хүнд гэмт хэрэг байгаа бөгөөд халдлагын зүйлс нь:

1. компьютер, компьютерийн программ, түүний төхөөрөмж
2. компьютер, мэдээллийн сүлжээнд хадгалагдаж байгаа болон дамжуулж байгаа мэдээлэл
3. компьютер, мэдээллийн хамгаалалттай сүлжээ
4. компьютерийн мэдээлэл

Эрүүгийн хуулиар хамгаалж буй эрх ашиг буюу гэмт хэргийн обьект нь иргэн, байгууллагын мэдээллийн аюулгүй байдал байна.[25] Харин эрх зүйн шинэтгэлийн хүрээнд шинэчлэн боловсруулж буй “Гэмт хэргийн тухай” хуулийн төслийн “Мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг” хэмээх бүлгийг Эрүүгийн хуулийн 25 дугаар бүлэгтэй харьцуулан авч үзвэл,

[25] Л.Галбаатар “Цахим эрх зүй”. УБ., 2010 он

№	Эрүүгийн хуульд	Гэмт хэргийн тухай хуулийн төсөлд
1	**226 дугаар зүйл. Компьютерийн мэдээлэл, программыг өөрчлөх, эвдэх, сүйтгэх** **226.1**. Компьютер, компьютерийн программ, түүний төхөөрөмжийг санаатайгаар өөрчилсөн, эвдсэн, гэмтээсэн, ашиглах боломжгүй болгосон, мэдээллийн сүлжээг сүйтгэсэн бол хөдөлмөрийн хөлсний доод хэмжээг тавин нэгээс хоёр зуу дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох, гурваас дээш зургаан сар хүртэл хугацаагаар баривчлах, эсхүл хоёр жил хүртэл хугацаагаар хорих ял шийтгэнэ.	**26.1 Цахим мэдээлэлд хууль бусаар халдах** Цахим төхөөрөмж, мэдээллийн хамгаалалттай сүлжээнд хууль бусаар халдаж мэдээллийг устгасан, гэмтээсэн, өөрчилсөн, хуулбарлаж авсан, мэдээлэл нэмж оруулсан, программ хангамж, сүлжээг ашиглах боломжгүй болгосон, хэвийн үйл ажиллагааг алдагдуулсан, эсхүл мэдээлэл хадгалагдаж байгаа төхөөрөмжийг устгасан, гэмтээсэн бол долоон сая төгрөгөөс гучин зургаан сая төгрөгөөр торгох, эсхүл нэг жилээс таван жил хүртэл хугацаагаар эрх чөлөө хязгаарлах, эсхүл нэг жилээс таван жил хүртэл хугацаагаар хорих ял шийтгэнэ.
	226.2.Энэ хэргийг шунахайн сэдэлтээр, түүнчлэн урьдчилан үгсэж тохиролцсон бүлэг буюу албан тушаалын байдлаа ашиглаж үйлдсэн бол хөдөлмөрийн хөлсний доод хэмжээг нэг зуугаас хоёр зуун тавь дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох, эсхүл гурваас дээш таван жил хүртэл хугацаагаар хорих ял шийтгэнэ.	
2	227. Компьютерийн мэдээллийг хууль бусаар олж авах 227.1.Компьютер, мэдээллийн сүлжээнд хадгалагдаж байгаа болон дамжуулж байгаа мэдээллийг зөвшөөрөлгүйгээр хуулб арласан, бусад аргаар олж авсны улмаас бусдад бага бус хэмжээний хохирол учирсан бол хөдөлмөрийн хөлсний доод хэмжээг тавин нэгээс нэг зуу дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох, гурваас дээш зургаан сар хүртэл хугацаагаар баривчлах, эсхүл хоёр жил хүртэл хугацаагаар хорих ял шийтгэнэ.	**26.2**. **Цахим мэдээллийн сүлжээнд хууль бусаар халдах программ, техник хэрэгсэл бэлтгэх, борлуулах** Цахим төхөөрөмж, мэдээллийн хамгаалалттай сүлжээнд хууль бусаар нэвтрэх тусгай программ, эсхүл техник хэрэгслийг бэлтгэсэн, борлуулсан бол долоон сая төгрөгөөс гучин зургаан сая төгрөгөөр торгох, эсхүл нэг жилээс таван жил хүртэл хугацаагаар эрх чөлөө хязгаарлах, эсхүл нэг жилээс таван жил хүртэл хугацаагаар хорих ял шийтгэнэ.

	227.2.Энэ хэргийг шунахайн сэдэлтээр, түүнчлэн урьдчилан үгсэж тохиролцсон бүлэг үйлдсэн, эсхүл уг хэргийн улмаас их буюу онц их хэмжээний хохирол учирсан бол хөдөлмөрийн хөлсний доод хэмжээг нэг зуугаас хоёр зуун тавь дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох, эсхүл хоёроос дээш таван жил хүртэл хугацаагаар хорих ял шийтгэнэ	
2	227. Компьютерийн мэдээллийг хууль бусаар олж авах 227.1.Компьютер, мэдээллийн сүлжээнд хадгалагдаж байгаа болон дамжуулж байгаа мэдээллийг зөвшөөрөлгүйгээр хуулб арласан, бусад аргаар олж авсны улмаас бусдад бага бус хэмжээний хохирол учирсан бол хөдөлмөрийн хөлсний доод хэмжээг тавин нэгээс нэг зуу дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох, гурваас дээш зургаан сар хүртэл хугацаагаар баривчлах, эсхүл хоёр жил хүртэл хугацаагаар хорих ял шийтгэнэ. 227.2.Энэ хэргийг шунахайн сэдэлтээр, түүнчлэн урьдчилан үгсэж тохиролцсон бүлэг үйлдсэн, эсхүл уг хэргийн улмаас их буюу онц их хэмжээний хохирол учирсан бол хөдөлмөрийн хөлсний доод хэмжээг тавин нэгээс нэг зуугаас хоёр зуун тавь дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох, эсхүл хоёроос дээш таван жил хүртэл хугацаагаар хорих ял шийтгэнэ	**26.2. Цахим мэдээллийн сүлжээнд хууль бусаар халдах программ, техник хэрэгсэл бэлтгэх, борлуулах** Цахим төхөөрөмж, мэдээллийн хамгаалалттай сүлжээнд хууль бусаар нэвтрэх тусгай программ, эсхүл техник хэрэгслийг бэлтгэсэн, борлуулсан бол долоон сая төгрөгөөс гучин зургаан сая төгрөгөөр торгох, эсхүл нэг жилээс таван жил хүртэл хугацаагаар эрх чөлөө хязгаарлах, эсхүл нэг жилээс таван жил хүртэл хугацаагаар хорих ял шийтгэнэ.
3	228. Компьютерийн мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэх, борлуулах 228.1.Компьютер, мэдээллийн хамгаалалттай сүлжээнд хууль бусаар нэвтрэх тусгай программ болон техник хэрэгслийг бэлтгэсэн буюу борлуулсан бол хөдөлмөрийн хөлсний доод хэмжээг тавин нэгээс нэг зуун тавь дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох, гурваас дээш зургаан сар хүртэл хугацаагаар баривчлах, эсхүл таван жил хүртэл хугацаагаар хорих ял шийтгэнэ.	**26.3 дугаар зүйл. Хор хөнөөлт программ хангамж бүтээх, ашиглах, тараах** 1. Цахим төхөөрөмжид хадгалагдаж байгаа мэдээллийг зөвшөөрөлгүйгээр устгах, гэмтээх, өөрчлөх, хуулбарлах, мэдээлэл олж авах, программ хангамж, мэдээлэл хадгалагдаж байгаа төхөөрөмж, сүлжээг ашиглах боломжгүй болгох, хэвийн үйл ажиллагааг алдагдуулах зориулалттай хор хөнөөлт программ хангамжийг тусгайлан зохиосон, зориудаар ашигласан, тараасан бол долоон сая төгрөгөөс гучин зургаан сая төгрөгөөр торгох, эсхүл нэг жилээс таван жил хүртэл хугацаагаар эрх чөлөө

4	229. Нянтай программ зохион бүтээх, ашиглах, тараах 229.1. Компьютерийн мэдээллийг зөвшөөрөлгүйгээр устгах, хаах, өөрчлөх болон хуулбарлах зорилгоор компьютерийн программ зохион бүтээх, программд өөрчлөлт оруулах, нянтай программыг тусгайлан зохион бүтээх, түүнийг мэдсээр байж ашигласан, тараасан бол хөдөлмөрийн хөлсний доод хэмжээг таваас тавь дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох, нэг зуугаас хоёр зуун цаг хүртэл хугацаагаар албадан ажил хийлгэх, эсхүл нэгээс гурван сар хүртэл хугацаагаар баривчлах ял шийтгэнэ.	хязгаарлах, эсхүл нэг жилээс таван жил хүртэл хугацаагаар хорих ял шийтгэнэ.
	229.2.Энэ хэргийн улмаас их буюу онц их хэмжээний хохирол учирсан бол хөдөлмөрийн хөлсний доод хэмжээг тавин нэгээс хоёр зуун тавь дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох, гурваас дээш зургаан сар хүртэл хугацаагаар баривчлах, эсхүл таван жил хүртэл хугацаагаар хорих ял шийтгэнэ.	

ЭХ-ийн 226, 227 дугаар зүйлүүдийг Гэмт хэргийн тухай хуулийн төслийн 26.1 дүгээр зүйлтэй харьцуулахад Мэдээлэлд хууль бусаар халдсан бүх үйлдлийг гэмт хэрэгт тооцохоор одоогийн Эрүүгийн хуульд заасан хоёр зүйлийг нэгтгэн нэг зүйл болгон заасан байна. Өөрөөр хэлбэл цахим төхөөрөмж, мэдээллийн хамгаалалттай сүлжээнд хууль бусаар халдсан тохиолдолд гэмт хэрэгт тооцохоор байна.Бусад зүйл ангийн хэм хэмжээнд агуулгын өөрчлөлт ороогүй байна.

2.2. Кибер орчинд үйлдэгдэж байгаа гэмт хэрэгтэй тэмцэх олон улсын эрх зүйн зохицуулалт, тогтолцоо

1977 онд кибер гэмт хэргийн талаар зохицуулалт бүхий хуулийн төслийг сенатор Рибикофф АНУ-ын Конгресст өргөн барьжээ. Хуулийн төслийг батлаагүй боловч дэлхий нийтийн анхаарлыг энэхүү гэмт хэрэгт хандуулжээ.

1983 онд Франц улсад Эдийн засгийн хамтын ажиллагаа, хөгжлийн байгууллага нь мэргэжлийн экспертүүдийн хороо[26] байгуулж, компьютертэй холбоотой гэмт хэргийн талаар хэлэлцэж, Эрүүгийн хуульд хэрхэн еөрчлөлт талаар ярилцжээ. Хорооны ажлын үр дүнд Эдийн засгийн хамтын ажиллагаа, хөгжлийн байгууллага гишүүн улсуудад эрүүгийн хуулийн зохицуулалтыг сайжруулах, мөн компьютерын гэмт хэргийн талаар тусгахыг зөвлөсөн байна.

Үүнээс гадна Европын зөвлөл мэргэжлийн экспертүүдийн хороо байгуулж, хууль зүйн асуудлыг хэлэлцсэний үр дүнд Зөвлөмж №R(89)9 гаргасан байна. Энэхүү зөвлөмжийг Европын Зөвлөл 1989 оны 9 дүгээр сарын 13-ны өдөр баталжээ. Энэхүү зөвлөмжид компьютертэй холбоотой хууль зөрчсөн үйлдлүүдийн жагсаалтыг гаргасан байжээ.[27]

Мөн 1990 онд энэхүү асуудлыг Монтреал хотод болсон Харьцуулсан эрх зүйн Олон улсын Академийн 13 дугаар Конгресс болон Гавана хотод болсон НҮБ-ын 8 дугаар Эрүүгийн эрх зүйн Конгресс[28], 1992 онд Холбооны бүгд найрамдах Герман улсын Вурцбург хотод Олон улсын конференци[29] дээр хэлэлцжээ.

1995 оны 9 дүгээр сарын 11-ний өдөр Европын Зөвлөл нь Мэдээллийн Технологитой холбоотой процессын хуулийн асуудлын талаар шинэ Зөвлөмж гаргасан байна.

1997 онд Европын Зөвлөл нь Кибер орчны гэмт хэргийн экспертийн хороог шинэ төрлийн гэмт хэрэг, Интернетийн харилцаа холбоон дахь хууль ёсны эрх, гэмт үйлдлийг тодорхойлох зорилгоор байгуулагджээ. Мөн Канад, Япон, Өмнөд Африк, АНУ-ын экспертүүдтэй уулзалт зохион байгуулж, туршлага солилцдог баина. 2001 оны 11 дүгээр сарын 23-ны өдөр Унгар улсын Будапешт хотод олон улсын гэрээ байгуулж, Канад, Япон, Өмнөд Африк, АНУ зэрэг 26 орны төлөөлөгч гэрээнд гарын үсэг зуржээ.

Европын Холбоо нь Интернэтийн орчны хууль бус, хохирол учруулахуйц үйлдлийн эсрэг тэмцэхээр олон төрлийн арга хэмжээ авч байна. 1998 оны 4 дүгээр сард Европын Хороо Зөвлөлд компьютерын гэмт хэргийг судалсан тайлангаа танилцуулжээ. 1999 оны 10 дугаар сард Европын Зөвлөлийн тэргүүний уулзалтаар өндөр технологийн гэмт хэргийн тодорхойлолт, санкцийн ерөнхий ойлголтыг бий болгох хэрэгтэй гэж үзжээ. Европын Парламент өндөр технологитой холбоотой гэмт үйлдлийг эрх зүйн зохицуулалтанд тусгах шаардлагатай гэж үзсэн байна. Европын Холбооны Зөвлөл нь өндөр технологийн гэмт хэрэгтэй тэмцэх стратегийн боловсруулан баталжээ.[30] Мөн Европын Холбооны Зөвлөлөөс 2002 оны 4-р сарын 19-ны өдөр мэдээллийн системийн эсрэг хийх дайралтын тухай шийдвэр гаргасан байна.[31]

---

[26] 1983 оны 5 дугаар сарын 30-ны өдөр Парис хотод хатагтай С.М. Пишра (Франц), М.Массе (Франц), А.Норман (Нэгдсэн вант улс), С.Шойлберг (Норвеги), Б. Де Шуттер (Бельги), У.Сиебер (Герман) нарын бүрэлдэхүүнтэй экспертийн баг ЭЗХАХВайгууллагатай уулзжээ. 1986 оны 9 дүгээр сарын 18-ны өдөр Хороог байгуулжээ.

[27] Компьютертэй холбоотой гэмт хэрэг: Зөвлөмж № R(89) 9 198 9 оны 9 дүгээр сарын 13-ны өдөр Еюропын Зөвлөлийн Сайд нарын Хорооны баталж, Гэмт хэргийн асуудал эрхэлсэн Европын Хороонд илтгэсэн байна

[28] Ulrich Sieber: The International Emergence of Criminal Information Law, 1991, 56 p.

[29] Ulrich Sieber (ed.): Information Technology Crime – National Legislation's and International Initiatives, 1994, 49 p.

[30] http://europa.eu.int/ISPO/elf/InternetPollclesSite/Crime/CrimeCommEN.ht ml

[31] http://europa.eu.int/information society/topics/telecoms/internet/crime /index en.htm

Эрүүгийн хуулийн төсөл ерөнхий 2 хэсэгт хуваагдсан байна. Үүнд:

- Мэдээллийн сүлжээнд хууль бусаар нэвтрэх
- Мэдээллийн сүлжээнд хууль бусаар хөндлөнгөөс оролцох

Үндэстэн дамнасан зохион байгуулалттай , гэмт хэргийн экспертүүдийн Их наймын өндөр технологийн ажлын хэсгийн зүгээс 1997 онд компьютерын гэмт хэрэгтэй тэмцэх 10 зарчмыг боловсруулсан бол 1998 оны 3-р сард 7 өдөр 24 цагийн турш ажиллах экспертүүдийн сүлжээг өндөр технологийн гэмт хэргийг мөрдөхөд туслалцаа үзүүлэхээр байгуулжээ. Аливаа өндөр технологи ашиглах гэмт хэрэгтэнд нуугдах боломж олголгүй, хуулийн дагуу шүүхийн өмнө хариуцлага тооцох зорилготой ажээ. Олон улс орон дээр дурьдсан 10 зарчмыг олон улсын гэрээ, үндэсний хууль тогтоомж, бодлогод тусгасан байдаг. Зарим улс энэхүү экспертийн сүлжээнд холбогдож эхэлжээ.

1999 онд АНУ-ын Калифорни мужийн Стенфордын Их сургуулийн Хүүверын институт Кибер гэмт хэрэг, терроризмтэй тэмцэх олон улсын хамтын ажиллагааны тухай конференци байгуулжээ.[32]

Мөн Олон улсын хүчний байгууллага-Интерпол 1981 онд анхны Интерполын компьютерын гэмт хэргийн мөрдөн байцаагч нарын сургалт семинарыг явуулсан байдаг. 1995, 1996, 1998, 2000 онд Интерпол Компьютерын гэмт хэргийн тухай олон улсын конференци байгуулж, сүүлд 2003 оны 10 дугаар сард Солонгос улсын Сөүл хотод хуралджээ.

Кибер орчны мэдээллийн технологийн хөгжил нь хүмүүсийн нийгэм, худалдаа, амьдралын хэв маяг дахь харилцаа холбоо, ажил төрөл, худалдаа хийх үйл явцыг өөрчилж байна. Энэхүү хөгжилтэй уялдан, олон тооны хүрээнд эрх зүйн асуудлыг бий болгож байна. Кибер гэмт хэргийн хувьд, мэдээлэл, баримтанд хууль бусаар нэвтрэх явдлыг бууруулахын тулд зайлшгүй эрх зүйн зохицуулалт шаардлагатай болсон байна. Иймээс улс орнууд олон улсын гэрээ, хуульд эрх зүйн зохицуулалтыг хийх болжээ.

Стенфордын Их сургуулийн Хүүверын институтийн Кибер гэмт хэрэг, терроризмын тухайн олон улсын гэрээний төслийн 3 дугаар зүйлд ийнхүү тусгажээ:

1. Энэхүү Гэрээний дор дурьдсан гэмт үйлдлийг хууль ёсны бүрэн эрх, зөвшөөрөлгүй аливаа этгээд хууль бусаар, санаатайгаар үйлдсэн бол гэмт хэрэг үйлдсэнд тооцно:

- Гэрээнд хууль бус үйлдэлд тооцсон, эсвэл өмчлөгч этгээдэд мэдэгдэлгүйгээр, мэдэгдэхгүй байх зорилгоор кибер системийг зогсоосон, эсвэл зогсохыг мэдсээр байж, кибер системийн мэдээлэл буюу программыг зохиосон, хадгалсан, өөрчилсөн, устгасан, дамжуулсан, будилуулсан, буруу дамжуулсан, мэхлэсэн, саад хийсэн;
- Хувь хүн болон түүний өмчид бодит хохирол учруулах зорилгоор хуурамч мэдээлэл боловсруулахаар кибер системийн мэдээллийг зохиосон, хадгалсан, өөрчилсөн, устгасан, дамжуулсан, будилуулсан, буруу дамжуулсан, мэхлэсэн, саад хийсэн;
- Нэвтрэхийг хориглосон кибер орчинд тодорхой зорилгоор нэвтэрсэн;
- Хяналтын болон хууль ёсны эсэхийг шалгах механизмд саад болсон;
- Гэрээний 3,4 дүгээр Зүйлд заасан аливаа үйлдлийг хийхээр ямарваа тоног төхөөрөмж буюу программыг үйлдвэрлэсэн, худалдсан, ашигласан, олон нийтэд үзүүлсэн;

[32] http://www.oas.org/juridico/english/conference agenda.htm

- Гэрээнд заасан аливаа хууль бус, хориглосон үйлдлийг хийхэд кибер системийг ашигласан;
- Мужийн нэгжийн дэд бүтцийг хямралд оруулах зорилгоор Гэрээний 3,4 дүгээр Зүйлд заасан аливаа үйлдлийг хийсэн.

Европын Зөвлөлийн Кибер гэмт хэргийн тухай конвенцид:

Хэсэг 1 - Эрүүгийн эрх зүй
Компьютерын мэдээлэл, системийн нууцлал, нэгдмэл байдал,
хууль ёсны байдлын эсрэг гэмт хэрэг
Зүйл 2. Хууль бусаар нэвтрэх
Зүйл 3. Хууль бусаар дамжуулалтыг таслах
Зүйл 4. Мэдээлэлд саад хийх
Зүйл 5. Системд саад хийх
Зүйл б. Хууль бусаар тоног төхөөрөмжийг ашиглах[33] хэмээн заасан байна.

Ялын заалт нь мэдээллийн технологийн гэмт үйлдлээс хамгаалах, бууруулахад чухал нөлөө үзүүлнэ. Гэмт үйлдэл нь гэм буруугүй мэт харагдаж байвч мэдээлэл, баримтад хууль бусаар нэвтэрснээр ноцтой хохирол учруулах боломжтой байдаг. Хууль бусаар системд нэвтэрч, гэмт хэргийг хакерууд үйлдэхээс гадна программ, мэдээллийг хорлон сүйтгэхээр зохион бүтээсэн программ эвддэгийг анхаарах хэрэгтэй.[34]

Мөн “тусгай эрүүгийн эрх зүйн зохицуулалт байхгүй” гэсэн үндэслэлээр хариуцлага тооцохгүй орхиж болохгүй. Эрүүгийн хуульд заагаагүй гэмт үйлдэлд Нууцын тухай хууль, Захиргааны хариуцлагын тухай хууль зэрэг бусад хуулиар хариуцлага тооцох боломжтой байна.

[33] http://conventions.coe.int/treaty/EN/projets/FinalCybercrime.htm
[34] В.Болорсайхан “Төгсөлтийн ажил”

Зарим улсын хууль тогтоомжид кибер гэмт хэргийн талаар хэрхэн туссан, мөн ямар ял шийтгэл оногдуулдаг талаар хүснэгтээр үзүүлбэл,

№	Улс	Ял, шийтгэл
1	**Австри**	Нууцын тухай хууль (Privacy Act; 2000.01.01) Хэсэг 10. Зүйл 52. Захиргааны хариуцлага (1) Тухайн гэмт үйлдэл нь шүүхийн шийдвэрийн хариуцлага тооцох үйлдэлд хамаарахгүй буюу бусад захиргааны хариуцлагын зүйлээр хариуцлага тооцох боломжгүй бол захиргааны буруутай үйлдэлд тооцож, 260,000 хүртэл торгууль оногдуулна. а/ Тухайн этгээд санаатайгаар мэдээллийн санд нэвтэрсэн буюу санаатайгаар хууль бус, шууд, тодорхой нэвтрэх үйлдэл хийсэн б/ Мэдээллийн нууцлал гэсэн 15-р зүйлийг зөрчиж, мэдээллийг дамжуулсан, тус хуулийн 4 6, 4 7-р зүйлийн дагуу тухайн этгээдэд хариуцуулсан мэдээллийг бусад зорилгоор ашигласан в/ хууль ёсны шийдвэрийн эсрэг мэдээллийг ашигласан, мэдээллийг нуун дарагдуулсан, хуурамч мэдээллийг засахгүй орхисон, хуурамч мэдээллийг устгахгүй орхисон г/ Хэсэг 7, Зүйл 27-д заасныг зөрчин, мэдээллийг санаатайгаар устгасан бол хариуцлага тооцно.
2	**Бельги**	Бельгийн Парламент 2000 оны 11 сард Эрүүгийн хуульдаа компьютерын гэмт хэргийн тухай шинэ заалт батлан оруулж, 2001 оны 2 сарын 13-наас хүчин төгөлдөр болжээ. Эрүүгийн гэмт үйлдэлд хамаарах 4 үндсэн асуудлыг хуульчилсан нь компьютерын хуурамч баримт бичиг, компьютерын залилан мэхлэлт, хакерын ажиллагаа, хортой үйл ажиллагаа болно. IV. Компьютерын хакерын ажиллагаа Эрүүгийн хуулийн 3үйл 550(b) 1 Аливаа этгээд зөвшөөрөлгүй гэдгээ мэдсээр байж, компьютерын системд нэвтрэх буюу холбоотой байвал 3 сараас 1 жил хүртэл хугацаагаар хорих, (5,200-5,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ. Хэрэв залилан мэхлэх зорилгоор энэхүү үйлдлийг хийсэн бол 6 сараас 2 жил хүртэл хугацаагаар хорих ял шийтгэнэ. 2 Аливаа этгээд залилан мэхлэх, эсвэл хохирол учруулах зорилгоор компьютерын системд нэвтэрсэн бол 6 сараас 2 жил хүртэл хугацаагаар хорих, (5,200-20,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ. 3 Дээрх 1, 2-р заалтад заасан гэмт хэргийг үйлдэж байгаагаа мэдсэн аливаа этгээд компьютерын системийн хадгалсан, боловсруулсан, дамжуулсан мэдээлэлд нэвтэрсэн, эсвэл мэдээллийг олж авсаар байвал, эсвэл компьютерын системийг хэрэглэсэн, эсвэл санамсаргүйгээр компьютерын системийн хадгалсан, боловсруулсан, дамжуулсан мздээлэлд хохирол учруулсан бол 1-3 жил хоригдох, (5,200-10,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ. 4.Дээрх 1, 2-р заалтад заасан гэмт хэргийг үйлдэхээр завдсан бол тухайн заалтын дагуу хариуцлага хүлээнэ. 5. Дээрх 1-4 заалтад заасан гэмт хэргийг залилан мэхлэх, эсвэл хохирол учруулах зорилгоор үйлдэхэд оролцсон, гүйцэтгэсэн, зуучилсан аливаа этгээд 6 сараас 3 жил хүртэл хугацаагаар хорих, (5,200-20,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ. 6.Дээрх 1-5 заалтад заасан гэмт хэргийг үйлдэхэд зохион байгуулсан, эсвэл хатгасан аливаа этгээд 6 сараас 5 жил хүртэл хугацаагаар хорих, (5,200-40,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ. 7.Дээрх 1-3 заалтад заасан гэмт хэргийн үр дүнд олж авсан мэдээлэл болохыг мэдэж байсан, хадгалсан, бусад этгээдэд задалсан буюу нээлттэй болгосон, тухайн мэдээллийг ашигласан бол б сараас 3 жил хүртэл хугацаагаар хорих, (5,200-20,000,000) торгох ял шийтгэх буюу дээрх ялын нэгээр шийтгэнэ.
3	**Бразил**	2000 оны 7 сарын 14-ны өдөр №9,983 дугаарын хууль дараахь зүйл заалтыг баталжээ: Мэдээллийн системд хуурамч мэдээлэл оруулах 3үйл 313-А. Өөртөө буюу бусад этгээдэд давуу байдал бий болгох, эсвэл хохирол учруулахаар мэдээллийн системийн болон Олон нийтийн мэдээллийн сангийн зөв мэдзээллийг өөрчлөх, ашиглагдахгүй болгох зорилгоор хуурамч мэдээлэл оруулах, хуурамч мэдээлэл оруулахыг зөвшөөрөл бүхий албан тушаалтан хялбар болгох үйлдлийг хэлнэ. Ял: **2-12** жил хорих, торгох ял шийтгэнэ. Мэдээллийн системд зөвшөөрөлгүй өөрчлөлт, сайжруулалт хийх 3үйл 313-Б. Албан тушаалтан зөвшөөрөлгүйгээр мэдээллийн систем буюу компьютерын программд өөрчлөлт, сайжруулалт хийсэн үйлдлийг хэлнэ. Ял: 3 сараас 2 жил хүртэл хугацаагаар баривчлах, торгох ял шийтгэнэ.
4	**Канад**	Канадын Эрүүгийн хууль 342.1 хэсэг: (1) Аливаа этгээд хууль бусаар, ямар ч эрхгүйгээр а/ шууд болон шууд бусаар ямарваа нэгэн компьютерын үйлчилгээг

		b/ электрон-соронзон, дуу авианы, механик болон бусад тоног төхөөрөмж ашиглан, шууд болон шууд бусаар дундаас нь барьж авах, эсвэл дундаас барьж авахад хүргэж байгаа компьютерын системийн аливаа үйлдэл хийсэн c/a болон б хэсэгт заасан гэмт хэргийг үйлдэхэдкомпьютерын системийг шууд болон шууд бусаар ашигласан, эсвэл ашиглахад хүргэж байгаа үйлдэл хийсэн буюу мэдээлэл, компьютерын системтэй холбоотой гэмт хэргийг үйлдсэн d /a, б, с хэсэгт заасан гэмт хэргийг үйлдэхийн тулд бусад этгээдэд компьютерын нууц үгийг хэрэглэх, эзэмших, мөрдөн олоход тусалсан бол гэмт хэрэг үйлдсэн гэм бурууташ этгээдэд тооцож, 10 жилээс хэтрэхгүй хугацаагаар хорих, эсвэл шүүгчийн захирамжаар хариуцлага тооцно.
5	**Чили**	Чили улс 1993 оны 6 сарын 7-нд Автомат мэдээллийг боловсруулсан гэмт хэргийн тухай №19.223 хуулийг хэвлэн нийтэлсэн байна. (Law on Automated Data Processing Crimes no. 19.223) 3үйл 2. Мэдээлэл боловсруулах системд хууль бусаар нэвтэрсэн, эсвэл мэдээлэл боловсруулах системийн мэдээллийг хууль бусаар ашигласан, эсвэл мэдээллийг дамжуулалт дундаас барьж авсан бол ялын бага болон дунд түвшний хэмжээгээр ял шийтгэнэ.
6	**БНХАУ**	1994 оны 2 сарын 18-ны өдрийн БНХАУ-ын Төрийн зөвлөлийн №147 тогтоол. Компьютерын мэдээллийн аюулгүй байдлыг хангах тухай БНХАУ-ын зохицуулалт Бүлэг 4. Хуулийн хариуцлага 3үйл 23'. Олон нийтийн хамгаалалтын байгууллага компьютерын вирус суулгасан, компьютерын мэдээллийн системд аюултай бусад мэдээлэл суулгасан, зөвшөөрөлгүйгээр компьютерын мэдээллийн системийн тусгай хамгаалалтын бүтээгдэхүүнийг худалдсан бол сануулга өгөх, эсвэл хувь хүнд 5,000 хүртэл юан, байгууллагад 15,000 хүртэл юаны торгууль оногдуулна. Хэрэв хууль бус ашиг олсон бол тухайн орлогыг улсын орлого болгож, хууль бус орлогыг 3 дахин нэмэгдүүлсэн хэмжээгээр торгоно. Мөн 1997 оны 12 сарын 11-нд Төрийн Зөвлөл баталж, 1997 оны 12 сарын 30-нд хэвлэн нийтэлсэн Компьютерын мэдээллийн сүлжээ, Интернэт хамгаалалт, Удирдлагын зохицуулалтын тухай тогтоолд хариуцлагыг давхар тусгажээ.
7	**Чехийн Бүгд Найрамдах улс**	Тусгайлсан эрх зүйн зохицуулалт байхгүй боловч Эрүүгийн хуульд зүйлчилж болох заалтууд байна: 182 зүйл. Олон нийтийн хэрэглээний үйлчилгээний нэгжид хохирол учруулах, аюултай байдалд оруулах 249 зүйл. Бусад хүмүүсийн хууль ёсны баримт бичгийг зөвшөөрөлгүй ашиглах 257 зүйл. Мэдээллийн сан дахь мэдээлэлд хохирол учруулах, бууруулгаар ашиглах
8	**Дани**	Эрүүгийн хуулийн 2 63 зүйл: a/ Хууль бусаар бусад этгээдийн мэдээлэл боловсруулах системд ашигладаг мэдээлэл буюу программд нэвтэрсэн бол торгох, 6 сар хүртэл хугацаагаар хорих ял шийтгэнэ. b/ Заалт 1, 2-т заасан гэмт хэргийг бусад этгээдийг хянах, эсвэл компанийн худалдааны нууцыг агуулсан мэдээллийг олох зорилгоор, эсвэл бусад хүндрүүлэх нөхцөлийг агуулсан үйлдэл хийсэн бол 2 жил хүртэл хугацаагаар хорих ял шийтгэнэ.
10	**Финлянд**	Эрүүгийн хуулийн Бүлэг 38 Хэсэг 8: Мэдээллийг хортойгоор ашиглах. Бусдын , хувийн мэдээллийг ашиглан, хамгаалалтын системийг эвдэлж, электрон болон бусад хэлбэрээр мэдээллийг боловсруулж, хадгалж, дамжуулж байгаа компьютерын системийг эвдлэн орсон, эсвэл тухайн системийн тодорхой хэсгийг эвдлэн орсон бол торгох, 1 уил хүртэл хугацаагаар хорих ял шийтгэнэ. Тусгай тоног төхөөрөмж ашиглан, компьютерын систем, эсвэл тухайн системийн тодорхой хэсгийг эвдлэлгүй нэвтэрч, тухайн компьютерын системд хадгалагдах мэдээллмйг авсан бол ял шийтгэнэ. Завдсан тохиолдолд мөн ял шийтгэнэ.
11	**Франц**	Шинэ Эрүүгийн хууль 1993 оны 3 сарын 1-нд хүчин төгөлдөр болжээ. Бүлэг 3. Автомат мэдээлэл боловсруулах систем үрүү дайрах 323-1 зүйл. Хууль бусаар автомат мэдээлэл боловсруулах системд нэвтэрсэн, эсвэл тодорхой хэсэгт хэвтэрсэн бол 1 жил хүртэл хугацаагаар хорих, 100,000 хүртэл торгох ял шийтгэнэ. Гэмт хэрэг үйлдсэний улмаас системийн мэдээллийг устгасан, өөрчилсөн, эсвэл системийн үйлдэл хийх ажиллагаа өөрчлөгдсөн бол 2 жил хүртэл хугацаагаар хорих, 200,000 хүртэл торгох ял шийтгэнэ. 323-2 зүйл. Системийн үйлдэл хийх ажиллагаанд саад болсон, эсвэл гажуудуулсан бол 3 жил хүртэл хугацаагаар хорих, 300,000 хүртэл торгох ял шийтгэнэ.

		323-3 зүйл. Залилан мэхлэх зорилгоор автоматмэдээлэл боловсруулах системд суулгасан, эсвэл автомат мэдээлэл боловсруулах системийн мэдээллийг өөрчилсөн бол 3 жил хүртэл хугацаагаар хорих, 300,000 хүртэл торгох ял шийтгэнэ. 323-4 зүйл. Зохион байгуулагдсан бүлэгт оролцсон, урьдчилан үгсэж тохиролцсон бүлэг 323-1-ээс 323-3 хүртэл заалтад заасан гэмт хэргийг үйлдсэн бол онц ноцтой гэмт хэрэг үйлдсэнд тооцно.
12	**ХБНГУ**	Эрүүгийн хууль Хэсэг 202a. Мэдээллийн тагнуул 1. Зөвшөөрөлгүйгээр өөрийн буюу бусдын төлөө өөрт байхгүй, зөвшөөрөлгүй нэвтрэхээс тусгайлан хамгаалагдсан мэдээлэлд нэвтэрсэн бол 3 жил хүртэл хугацаагаар хорих, торгох ял шийтгэнэ. 2. 1 заалтад заасан мэдээлэлд нүдээр шууд үзэх боломжгүй электрон буюу соронзон хэлбэрээр хадгалагдаж, дамжуулагдаж байгаа мэдээллийг хамруулна. Эрүүгийн хууль Хэсэг 303a. Мэдээллийг өөрчлөх 1.Хууль бусаар мэдээллийг арилгасан, өөрчилсөн, дахин ашиглахгүй болгосон бол 2 жил хүртэл хугацаагаар хорих, торгох ял шийтгэнэ. 2 Завдсан тохиолдолд мөн ял шийтгэнэ. Эрүүгийн хуулийн Хэсэг 303 b. Компьютерын хортой үйл ажиллагаа 1.Бусад этгээдийн бизнес, аж ахуй, захиргааны үйл ажиллагаанд чухал шаардлагатай мэдээлэл боловсруулах үйл ажиллагаанд саад хийсэн бол 5 жил хүртэл хугацаагаар хорих, торгох ял шийтгэнэ: - 300a/1/ хэсэгт заасан гэмт хэрэг үйлдсэн - компьютерын систем буюу мэдээлэл зөөвөрлөгчийг устгасан, хохирол учруулсан, дахин ашиглагдахгүй болгосон, өөрчилсөн 2.Завдсан тохиолдолд мөн ял шийтгэнэ.
13	**Грек**	Эрүүгийн хуулийн 370c2 зүйл: Хууль ёсны эзэмшигчийн хамгаалалт, хязгаарлалтыг эвдлэн, компьютер буюу компьютерын санах ойд хадгалагдсан болон холбоо харилцаагаар дамжуулагдаж ' буй мэдээллийг хууль бусаар олж авсан бол 3 сар хүртэл хугацаагаар хорих, 10,000 драхма хүртэл торгох ял шийтгэнэ. Хэрэв тухайн үйлдэл нь олон улсын асуудал болон Улсын аюулгүй байдалтай холбоотой бол 148 зүйлээр ял шийтгэнэ. Хэрэв гэмт хэргийг мэдээллийг хууль ёсоор эзэмшигчийн туслалцаатай хийсэн бол дээр дурьдсан заалтыг баримтлан, ял шийтгэнэ.
14	**Унгар**	Эрүүгийн хуулийн 300c зүйл: Компьютерын залилан мэхлэлт. 1.Хууль бусаар өөртөө ашиг олохоор хохирол учруулсан, электрон мэдээлэл боловсруулах замаар саад хийсэн, программыг өөрчилсөн, мэдээллийг устгасан, хуурамч буюу бүрэн бус мэдээлэл оруулсан, бусад гэмт хэрэг үйлдэх зорилгоор хууль бус үйлдэл хийсэн бол 3 жил хүртэл хорих ял шийтгэнэ. 2 Хэрэв: а/ их хэмжээний хохирол учирсан бол 5 жил хүртэл хугацаагаар хорих б/ онц их хэмжээний хохирол учирсан бол 2 жилээс 8 жил хүртэл хугацаагаар хорих ял шийтгэнэ. 3. Нийтийн, хөдөлгөөнт гар утасны -электрон карт ашиглаж, гэмт хэрэг үйлдсэн, эсвэл хөдөлгөөнт гар утасны микропрограммыг өөрчилж, мэдээлэлд холбогдсон бол залилан мэхлэлтэд тооцогдоно.
15	**Ирланд**	Эрүүгийн хууль 1991 Хэсэг 5: 1. Хууль бусаар компьютер ашиглаж, а/ Мужийн дотроос Мужийн гадна, дотно хадгалагдах аливаа мэдээлэлд нэвтэрсэн б/Мужийн гаднаас Мужийн дотор хадгалагдах аливаа мэдээлэлд нэвтэрсэн бол 500 хүртэл торгох, 3 **сар** хүртэл хугацаагаар хорих ял дангаар буюу хамт шийтгэнэ. 2. 1 заалт хууль бусаар тодорхой мэдээлэлд нэвтэрсэн, тодорхой мэдээллийн төрөлд нэвтэрсэн, тодорхой этгээдэд хадгалагдах мэдээлэлд нэвтэрсэн бүх этгээдэд хамаарна.
17	**Энэтхэг**	Мэдээллийн технологийн тухай хууль 2000 (2000 оны №20) Бүлэг 11. Компьютерын систем дахь хакерын ажиллагаа

		(1) Санаатайгаар, эсвэл тухайн үйлдэл хор хохирол авчрахыг мэдсээр байж, олон нийт, хувь хүний компьютерын эх сурвалж дээрхи мэдээллийг устгах, арилгах, өөрчлөх, эсвэл мэдээллийн үнэт байдлыг алдуулах, дахин ашиглахгүй болгосон үйлдлийг хакерын ажиллагаанд тооцно. (2) Хакерын ажиллагаа хийсэн бол 3 жил хүртэл хугацаагаар хорих, 200,000 рупигээр торгох йл дангаар буюу хамт шийтгэнэ.
18	**Израиль**	1995 оны Компьютерын тухай хууль 4 хэсэг: Хууль бусаар компьютерын мэдээлэлд нэвтэрсэн бол 3 жил хүртэл хугацаагаар хорих ял шийтгэнэ. Мэдээлэлд нэвтрэх гэдэг нь компьютерт холбогдох хэрэгсэл ашигласан, хэрэгслийн тусламжтай нэвтэрсэн, хууль бусаар нууцаар нэвтэрсэн үйлдлийг ойлгоно.
19	**Итали**	Эрүүгийн хуулийн 615зүйл: Компьютерын болон холбоо харилцааны системд хууль бусаар нэвтрэх. Хамгаалалтын хэрэгслээр хамгаалагдсан компьютерын болон холбоо харилцааны системд хууль бусаар нэвтэрсэн, эсвэл хамгаалалтын албаны ажилтны мэдэгдлийн үл зөвшөөрч, холбогдсон бол 3 жил хүртэл хугацаагаар ял шийтгэнэ. Хэрэв: 1/ Албан тушаалаа урвуулан ашиглаж гэмт хэрэг үйлдсэн бол 2/ Зэвсэглэсэн этгээд хүч хэрэглэн байж, гэмт хэрэг үйлдсэн бол 3/ Системд, мэдээлэлд, мэдээллийт хадгалах программд хохирол учруулсан бол 1 жилээс 5 жил хүртэл хугацаагаар хорих ял шийтгэнэ. Хэрэв компьютерын болон холбоо харилцааны системд хууль бусаар нэвтрэхэд зэвсэгт хүчний ашиг сонирхолд тулгуурлан, олон нийтийн аюулгүй байдалд сөргөөр нөлөөлөх байдал үүссэн бол 1 жилээс 5 жил хүртэл, эсвэл 3 жилээс 8 жил хүртэл ял шийтгэнэ. 615 зүйл. Компьютерын болон холбоо харилцааны системд нэвтрэх кодыг хууль бусаар эзэмших, тараах Өөртөө буюу бусдад ашиг олох, бусдад хохирол учруулах зорилгоор хамгаалалтын хэрэгслээр хамгаалагдсан компьютерын болон холбоо харилцааны системд нэвтрэх код, түлхүүр үгийг эзэмших, хуулбарлах, бусдад дамжуулсан бол 1 жил хүртэл хугацаагаар хорих, 10 сая лир хүртэл хэмжээгээр торгох ял шийтгэнэ. Хэрэв энэ гэмт хэргийг 617 зүйлд заасан гэмт хэргийн хамт үйлдсэн бол 1 жилээс 2 жил хүртэл хугацаагаар хорих, 10 сааяс 20 сая лир хүртэл хэмжээгээр торгох ял шийтгэнэ. 615. Компьютерын системд хохирол учруулах, зогсоох зорилготой программыг тараах. Өөрөө буюу бусдын хийсэн, компьютерын болон холбоо харилцааны системд, системийн мэдээлэл, программыг хэсэгчлэн буюу бүрэн зогсоох, өөрчлөх зорилготой программыг тараасан, дамжуулсан бол 2 жил хүртэл хугацаагаар хорих, 20 сая лир хүртэл хэмжээгээр торгох ял шийтгэнэ.
20	**Япон**	Зөвшөөрөлгүй компьютерт нэвтрэх тухай хууль (Unauthorized Computer Access Law) 1999 оны №128 хууль (2000 оны 2 сарын 3-нд хүчин төгөлдөр болсон) (Зөвшөөрөлгүй компьютерт нэвтрэх үйлдлийг хориглох) Зүйл 3. Зөвшөөрөлгүй компьютерт нэвтрэхийг хориглоно. Зөвшөөрөлгүй компьютерт нэвтрэх гэдэгт дараахь үйлдлийг хамааруулна: 1 тусгай компьютер, харилцаа холбооны шугам, бусад этгээдийн кодыг ашиглан, нэвтрэх хяналтын үйлдлийг хариуцсан компьютерт холбогдож, нэвтрэх хяналтын үйлдлээр хязгаарлагдсан хэрэглээг ашиглах боломжтой болгох үйлдэл, 2 нэвтрэх хяналтын үйлдлийн хязгаарлалтыг бууруулах, хязгаарлагдсан хэрэглээг нэвтрэх хяналтын үйлдэлд мэдэгдэхгүй ашигласан үйлдэл, 3 нэвтрэх хяналтын үйлдэл бүхий компьютерт холбогдсон тусгай компьютер, харилцаа холбооны шугамаар дамжуулан, нэвтрэх хяналтын үйлдлийг суулгаж, хязгаарлалтаас зайлсхийж, мэдээлэл, коммандыг боловсруулах үйлдзл (Зовшөөрөлгүй компьюторт НЭВтрэхийг хялбар болгох үйлдлийг хориглох) Зүйл 4. Бусад этгээдэд нэвтрэх боломж олгох хувийн мэдээлэл, тусгай компьютерыг ашиглах хувийн мэдээллийг дамжуулах, ашиглахыг хориглоно.

		(Эрүүгийн хариуцлага) 3үйл 8. Хэрэв дээр дурьдсан гэмт хэргийг үйлдсэн бол 1 жил хүртэл хугацаагаар хорих, 500,000 иен хүртэл хэмжээгээр торгох ял шийтгэнэ. (1) 3үйл 3-н 1 параграф, 3үйл 4 заасан гэмт хэрэг үйлдсэн бол 300,000 иен хүртэл хэмжээгээр торгох ял шийтгэнэ.
21	**Голланд**	Эрүүгийн хуулийн 138а зүйл: Санаатайгаар, хууль бусаар мэдээлэл хадгалах, боловсруулах автоматжуулсан систем, түүний тодорхой хэсэгт нэвтэрсэн бол компьютерын амгалан тайван байдлыг алдагдуулсан гэмт буруутайд тооцож, 6 сар хүртэл хугацаагаар хорих, 10,000 гилдер хүртэл торгох ял шийтгэнэ. (a) Хамгаалалтын системийг эвдэлсэн бол (b) хуурамч дохио, түлхүүрийн тусламжтайгаар, хуурамчаар чадвартай мэт үйлдэл хийн, техникийн байдлаар саад хийж, нэвтэрсэн бол эрүүгийн хариуцлага хүлээлгэнэ.
23	**Швед**	Эрүүгийн хуулийн Бүлэг 4, Хэсэг 9с: Хэсэг 8, 9 зааснаас бусад тохиолдолд, хууль бусаар автоматжуулсан мэдээлэл боловсруулах ажиллагааны тэмдэглэлд нэвтэрсэн, эсвэл хууль бусаар тэмдэглэлийг өөрчилсөн, устгасан, эсвэл өөрчилсөн, устгасан тэмдэглэлийг бүртгэлд оруулсан бол 2 жил хүртэл хорих, торгох ял шийтгэнэ. Тэмдэглэлд электроник болон автоматжуулсан мэдээлэл боловсруулах ажиллагаанд хэрэглэгдэх бусад мэдээллийг ойлгоно. Завдсан болон бэлдсэн тохиолдолд Эрүүгийн хуулийн Бүлэг 23 заасны дагуу хариуцлага тооцох бөгөөд төгссөн гэмт хэргээс бага шийтгэл онооно.
24	**Швейцарь**	Эрүүгийн хуулийн 14 3 зүйл: Мэдээлэл боловсруулах системд хууль бусаар нэвтрэх Зөвшөөрөлгүйгээр, ашиг олох зорилгагүйгээр электрон тоног төхөөрөмжийн тусламжтайгаар зөвшөөрөлгүй нэвтрэхээс тусгайлан хамгаалагдсан мэдээлэл боловсруулах сйстемд нэвтэрсэн бол торгох, хорих ял шийтгэнэ.
	Латви	Эрүүгийн хуулийн 241 хэсэг: Компьютерын сйстемд дураар нэвтрэх (1) Компьютерын системд дураар нэвтэрч, мэдээлэл авах боломж бүрдүүлсэн бол хорих, сарын орлогыг 80 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээнд хүртэл торгох ял шийтгэнэ. Компьютерын системд дураар нэвтэрч, хамгаалалтын программ хангамжийг эвдсэн, эсвэл харилцаа холбооны шугаманд нэвтэрсэн бол 1 жил хүртэл хугацаагаар хорих, сарын хамгийн бага орлогыг 150 дахин, нэмэгдүүлсэнтэй тэнцэх хэмжээнд хүртэл торгох ял шийтгэнэ.
25	**Нэгдсэн вант улс**	Компьютерыг буруугаар ашиглах тухай хууль 1990 Бүлэг 18. Компьютерын материалд хууль бусаар нэвтрэх (1) Хэрэв дараахь гэмт хэргийг үйлдсэн бол гэм буруутайд тооцно: aаливаа мэдээлэл, программ хадгалах компьютерт нэвтрэх боломжийг хамгаалах зорилгоор компьютерээр төрөл бүрийн үйлдэл хийсэн b/ хамгаалж буй нэвтрэх боломж нь зөвшөөрөлгүй c/ үйлдэл хийж байхдаа тухайн үйлдлээ бүрэн ухамсарласан (2) Гэмт хэрэг үйлдэхдээ дараахь зорилгыг агуулсан байх шаардлагагүй: a/ тодорхой программ, мэдээллийг олохын тулд b/ тодорхой төрлийн программ, мэдээллийн олохын тулд c/ тодорхой компьютерын программ, мэдээллийг олохын тулд (3) Дээр дурьдсан гэмт хэрэг үйлдсэн бол 6 сар хүртэл хугацаагаар хорих, стандарт хэмжээний 5-р түвшин хүртэл хэмжээгээр торгох ял шийтгэнэ.

Интернэт ашиглах хууль бус үйлдлийг зохицуулахад компьютерт шууд холбогдсон болон шууд холбогдолгүй үйл ажиллагаа явуулах технологийн арга барилыг харгалзан үзэх шаардлагатай бөгөөд тухайн арга барилд нууц, иргэний эрх чөлөөний хамгаалалт зэрэг олон чухал нийгмийн сонирхол байгааг анхаарах хэрэгтэй.

Хуулийн байгууллагын хувьд мэдээлийн эх сурвалж, сургалт судалгааны ажил зайлшгүй шаардагдахаас гадна шинэ төрлийн мөрдөн шалгах багаж хэрэгсэл, чадварлаг боловсон хүчин, орон нутгийн нэгж бүрт ажиллах хэсэг, олон улсын нягт хамтын ажиллагаа шаардлагатай байна.

Хэрэглэгчдийн "кибер ёс зүй" хэмээх ойлголтыг төлөвшүүлэх, хууль бус үйлдлийн эрсдлийг бууруулах, хамгаалахад хэрэглэгчдийн мэдлэгийг дээшлүүлэх арга хэмжээ авах хэрэгтэй.[536]

Нууц бол хууль ёсны эрх бөгөөд олон улс орон хуульдаа хүлээн зөвшөөрсөн байдаг боловч хууль зүйн болон соёлын уламжлалын ялгаанаас шалтгаалан, тодорхой ялгаа ажиглагддаг. Ихэнх улс нууцыг хуулиар хамгаалж, олон улсын гэрээ, конвенцид стандарт зарчмыг тусгасан байдаг бол одоо кибер технологийн хүрээнд энэ асуудлыг маш тодорхой болгох шаардлага гарч байна. Зарим судлаачдын дүгнэснээр, дэлхийн түүхэнд анх удаа нууцын асуудлын өргөн хүрээнд авч үзэж байна гэжээ. Кибер орчин дахь нууцыг хамгаалах механизм нь хувийн зохицуулалтанд тулгуурлаж, хувийн үйлдвэр, компани бүр тусгай кодыг зохиож, ашиглаж байна. Олон улс оронд хувийн нууцын эрх зүйн зохицуулалтаар хамгаалалтын механизмыг сайжруулах тал дээр анхаарч байна.

Механизмын тэнцвэрт байдлыг тооцож үзэхдээ Интернэтийн талаар судлах шаардлагатайг мартах ёсгүй. АНУ-ын Дээд шүүхийн 1997 оны б сарын 2 6-ны өдрийн шийдвэрт: "Интернэт үсрэнгүй хөгжиж буй үзэгдэл цаашид үргэлжлэх болно. Нотлох баримтгүй буюу дутмаг байдлаас болж, үндсэн хуульт ёсонд хийдэл үүсэхээс сэргийлж, эрх зүйн зохицуулалтыг улам нарийвчлан боловсронгуй болгож, цаашид гарах сөрөг үзэгдлийн эсрэг бодитой арга хэмжээ авах хэрэгтэй болж байна. Ингэснээр бид бодит бус хэмээх хүмүүсийн сэтгэгдлийг өөрчилж, кибер орчинд ч зохицуулалт үйлчлэх боломжтой харуулах болно." гэжээ.

Гадаад улс орнуудын цаашдын чиг хандлага нь эрүүгийн эрх зүйн зохицуулалтыг улам боловсронгуй болгоход чиглэж байгаа бөгөөд тусгай судалгаа шинжилгээний төвийн үйл ажиллагаа, шинжилгээ, тайлан дээр тулгуурлаж, кибер орчинд үйлдэх гэмт үйлдлийг таслан зогсоох, бууруулах арга хэмжээ авахад чиглэгдэж байна.

[536] http: //www.usdoj .gov/criminal/cybercrime/unlawful..htm

БҮЛЭГ III. КИБЕР ОРЧИНД ҮЙЛДЭГДЭЖ БАЙГАА ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ ОНОЛ, АРГА ЗҮЙН ҮНДЭС

3.1. Кибер орчинд үйлдэгдэж байгаа халдлагатай тэмцэх эрх зүйн онол, арга зүйн үндэс

Судалгааг хэрэгжүүлэх онол, арга зүйн үндсэн тодорхойлолт

Шинжлэх ухааны суурь судалгаа нь аливаа юмс, үзэгдэл, үйл ажиллагааны дотоод хууль, зүй тогтолыг бодит байдлаар нь ямар нэгэн практик хэрэглээний зорилттой холбоогүйгээр судлахад чиглэгдэнэ гэж үздэг.

Харин хавсарга судалгаа нь суурь судалгааны үр дүнг танин мэдэхүйн болон нийтийн амьдралын хэрэгцээнээс үүдэлтэйгээр гарч байгаа зорилтуудыг шийдвэрлэхэд ашиглах, хэрэглэх зэрэг асуудлыг тодорхойлоход чиглэгдэнэ.

Иймд энэ судалгаа нь зарим талаар /энэ бүлэг/ эмпирик түвшингээр бус шинжлэх ухааны мэдлэгийн үндсэн дээр бодит төлөв байдлыг идеалчилсан буюу хийсвэрлэхүйн хэлбэрээр судлан юмс, үзэгдэл үйл явцын үндсэн, гол, ерөнхий хууль, дэс дараалал, зүй тогтолыг тодорхойлоход чиглэгдсэн болно.

Өөрөөр хэлбэл, судалгааны багийн гишүүдийн хувийн бодол, эрэгцүүлэл бус судалгааны зүйлийн өөрийнх нь зүй тогтол, харилцан хамаарал, үүсэл, хөгжлийн хандлагыг харгалзан үнэн зөв танин мэдэхүйн үйл ажиллагааг зохион байгуулах, үйл ажиллагааг хэрэгжүүлэх зарчим, хэм хэмжээг тодорхойлоход чиглэгдсэн.

Судалгааг тодорхой арга зүйг баримтлан хэрэгжүүлэх учиртай бөгөөд шинжлэх ухааны аргууд тэдгээрийн үндэслэл болж байгаа мэдлэгийн хууль, зарчим, мэдлэгийн тухай сургаал, үзэл баримтлалыг судалгааны арга зүйгэж тодорхойлдог.

Арга зүйн мэдлэгийг:

- Философи, социологийн арга зүй,
- Салбар шинжлэх ухааны ерөнхий арга зүй,
- Тодорхой шинжлэх ухааны тусгай арга зүй гэж үзнэ.

Нэг арга зүйг баримтлан тодорхой судалгааг хэрэгжүүлэх нь хангалтгүй байдаг тул эмпиризмын, рационализмын, диалектикийн зэрэг арга зүйн баримтлалаар энэхүү судалгааг гүйцэтгэсэн болно.

Монгол Улсын эрх зүйн шинэтгэл, олон улсын харилцаа, хамтын ажиллагааны төлөв байдал, техник-технологи, эрх зүйн хөгжлийн өнөөгийн бодит байдал нь урд өмнө байгаагүйгээр эрс өөрчлөгдөж улмаар хүний эрх, эрх чөлөөний үнэлэмжээрхөгжил тодорхойлогддог болсон билээ.

Үүний гол хүчин зүйлийн нэг нь хүний эрхийн асуудлыг улс орон бүхэн дотоод, гадаад харилцааны чухал хэмжүүр болгон үнэлэмж тогтоох болсонтой холбоотой.

Энэ нь хүний эрхийг хангах, хамгаалах үйл ажиллагааны хүрээндмэдээллийн аюулгүй байдалтай холбоотой кибер орчин дахь эрх зүйн хамгаалалт буюу компьютерийн /кибер орчин дахь/ сүлжээний хамгаалалт, зохицуулалт юм.

Кибер орчин, орон зайн /компьютерийн сүлжээ/ хөгжлийн нэгэн бодит жишээ бол мэдээж интернет.

Кибер орчин, орон зайн /компьютерийн сүлжээ/нь өнөөгийн нийтийн амьдралын харилцааны чухал хэрэгцээний нэг төдийгүй, нийгмийн хөгжил түүнчлэн нийгмийн сөрөг үзэгдэл болсон гэмт явдлыг тодорхойлогч болсон компьютер болон ухаалаг технологи, хэрэглээтэй салшгүй холбоотой.

Амьдрал үйл ажиллагааны салшгүй хэсэг болсон кибер орон зай, /компьютерийн сүлжээ/орчинд үйлдэгдэж байгаа гэмт халдлагатай тэмцэх эрх зүйн тогтолцоо, өнөөгийн байдлыг эрүүгийн эрх зүйн онол, арга зүйнхамаарах хүрээнд судалж ирээдүйн хандлагыг тодорхойлж, тулгамдсан асуудлыг шийдвэрлэхэд тодорхой хувь нэмэр оруулахад энэхүү судалгааны ач холбогдол чиглэгдэнэ.

Эх газрын эрх зүйн онолын тогтолцоонд “Criminal Law” онолын хүрээнд Франц, ХБНГУ, Европын улсуудад 1986-1988 оны үеэс эхлэн “Computer crimes” гэсэн ойлголт бий болж улмаар Европын улсуудын судлаачдын судалгааны ажлын үр дүнд Эрүүгийн эрхийн онолд “Компьютерийн гэмт хэрэг”, “компьютер ашигласан гэмт хэрэг” гэсэн ойлголтууд бий болж 1990-ээд оны сүүлээс Англо Саксоны эрх зүйн нөлөөгөөр “Кибер гэмт хэрэг” гэсэн ойлголт орж ирсэн.

Одоо Компьютерийн гэмт хэргүүд, Кибер гэмт хэргүүд гэсэн онолын ойлголтыг хөгжүүлж, эрүүгийн хуулиудад зохих бүлгийг оруулж хуульчлан мөрдөж байна. Өндөр хөгжилтэй орнуудын эрүүгийн хуульд 6-13 зүйл заалтын хүрээнд энэ төрлийн гэмт хэргийн диспозицийг тусгасан байна.

Англо Саксоны эрх зүйн онолын тогтолцоонд “TheoryCrime Law”-ийн дотор 1980 оноос эхлэн “Cyber Law” хэмээх онолын ойлголт орж ирсэн. АНУ, Их Британи, Канад, Австралийн судлаачдын 1980-аад оноос хойш хийсэн судалгаа, шинжилгээ, боловсруулалтын үр дүнд онолын зохих тогтолцоо болон хөгжсөн.

Улмаар “Cyber Crime Law”-хуулиудад энэхүү онолын ойлголтыг хуульчлан оруулж тусад нь хуулиуд батлан мөрдөж байна. Кибер гэмт хэргийн тухай хуулиуд ихэвчлэн 18-30 орчим зүйл заалтаар зохицуулах хандлагатай байна.

Кибер орчин дахь өнөөгийн ерөнхий байдал

Дэлхийг бүрхсэн интернэтийн сүлжээнд Монгол Улс анх 1994 оны 01 дүгээр сарын 17-ны өдөр 3 компьютер интернетэд холбон дэлхийн мэдээллийн сүлжээнд /WWW/ холбогджээ. “Мэдээлэл харилцаа” ББХК (Датаком) анх удаа интернэтийн үйлчилгээг явуулж эхэлсэн бөгөөд цорын ганц гарц байсан бол энэ цаг үед цахим орон зайг мэдэхгүй, ашиглахгүй, үр өгөөжийг нь хүртээгүй хүн үгүй болжээ[537].

1996 онд интернэт хэрэглэгчдийн тоо ердөө 500 гаруйхан байсан бол 2007 оноос хойш 25 дахин өсчээ.

2010 оны эцсийн байдлаар гэрээ бүхий интернэт хэрэглэгчийн тоо 199,849 болсон бөгөөд Дэлхийн банкнаас гаргасан судалгаагаар Монгол Улсын интернэт хэрэглэгдэг хүний тоо 2009 оны байдлаар нийт хүн амын 400,000 орчим буюу 13,0 хувийг эзэлж байсан бол ХАОСТ 2010 дүнгээс интернэт хэрэглэдэг хүний тоо 709.625 буюу нийт хүн амын 30.6 хувийг эзэлж байгаа нь дэлхийн дунжаас 0.4 хувиар өндөр үзүүлэлт юм байна.

Өнөөдөр дэлхийн хүн амын 50 хувь нь томоохон хотуудад, 40 орчим хувь нь төв, суурин газарт, үлдсэн хэсэг нь алслагдсан хөдөө амьдарч байна.

Шинэ мянганы нийтлэг хэв шинж, цагийн хуваарь, хүсэл сонирхол, хэрэглээ эрс өөрчлөгдсөн. Энэ нь шинэ мянганы амьдралын дүрэм эрс өөрчлөгдсөн гэсэн үг. Шинэ мянганыхан цаг үргэлж өөр хоорондоо ухаалаг технологи ашиглан холбогдож бүх зүйлээ бусадтай хуваалцах, нээлттэй, эрх чөлөөтэй байх гэсэн нийтлэг дүрэмтэй технологийн мангасууд болсон учир энэ хэв шинжээс хууль сахиулах салбар төдийгүй тээвэр, аялал жуулчлал, үйлчилгээ гэх мэт бүхий л салбар суралцаж байна. Энэ бүх асуудал нь шинэ мянганы амьдралын хэв шинж, үйл ажиллагааг хүлээн авах ажил удаан байж болохгүйгээс гадна түүнтэй хуучины арга баримлаар тэмцэх, хуучин мянганы асьдралаар байлгах гэж захиргааны арга сонгох аваас хэнэг ч алхам амжилтад хүрэхгүй гэдгийг олон улсын судалгааны **EBSCO** байгууллага дүгнэж байна.

Мөн даяаршилсан нийгмийн гол мөн чанар, дэлхийн хүн төрөлхтний хоорондын харилцаа холбоо, мэдээллийн үйл ажиллагааны автоматжуулалтын хамгийн гол гүүр нь компьютерийн сүлжээ учир иргэн, аж ахуйн нэгж, байгууллагын мэдээллийн аюулгүй байдлыг хангуулах талаар эрх зүйн орчинг боловсронгуй болгох, мэдээллийн аюулын эрсдлээс

[537]Л.Цогтбаяр., “Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэргийн эрх зүйн зохицуулалт, өнөөгийн байдал, чиг хандлага” ХСИС ЭШ-ний эмхтгэл, УБ., 2012 он

урьдчилан сэргийлэх арга хэмжээг иж бүрэн боловсронгуй болгох зайлшгүй шаардлагатай инновацид суурилсан шинжлэх ухааны мэдлэгийн тогтолцоогбий болгох асуудал.

Интернэт нь хүн төрөлхтний даяарчлалын салшгүй нэгэн бүхэллэг хэсэг /элемент/ болсон учир интернэтэд суурилж буй орон зай ч өөр хоорондоо харилцан хамааралтай /интеграцлагдах/ болж даяарчлагдахын хэрээр, мэдээ мэдээллийн нэгдмэл байдал, сахилга бат, дэг журмыг шаарддаг цаг үе нэгэнт бүрэлдэн бий болжээ.

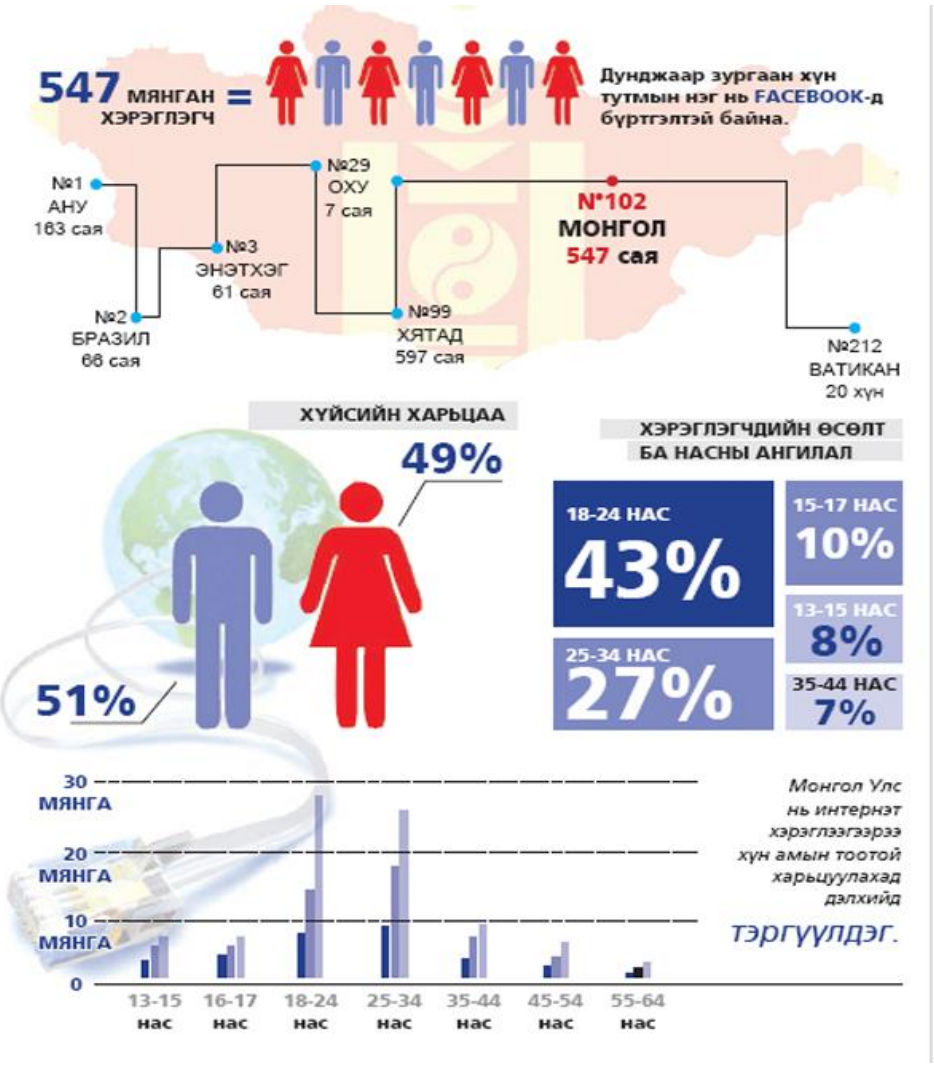
Нийслэлийн хэмжээнд монгол хэлээр нэвтрэх интернэт хэрэглэгчдийн тоо 350 мянга хол давсан гэх статистик мэдээллийг холбогдох албаны хүмүүс өгч байна.

Интернэт хэрэглэгчдийн тоо жилээс жилд өсөж буйг олон эх сурвалжаас харж болно.

Фэйсбүүк цахим хуудас 2006 онд нээгдсэнээс хойш дэлхий нийтээрээ хэрэглэх болсон. Энэ хугацаанд манай улсын 547 мянган хүн дээрх хуудаст бүртгэлтэй болсон байна.

Өөрөөр хэлбэл, зургаан хүн тутмын нэг нь Фэйсбүүк цахим сүлжээг ашигладаг гэсэн үг.

Бусад өндөр хөгжилтэй оронтой харьцуулахад манай улс интернэтийн хэрэглэгчдийн тоогоор 102 дугаарт бичигдэж буй хэдий ч хүн амынх нь тоотой харьцуулахад дэлхийд нэгдүгээрт жагсаж байгааг Нийгмийн хамгааллын үйлчилгээний төвийнхөний судалгаа харуулж байна.



Тухайлбал, 2013 оны 3 сарын байдлаар Фейсбук дээр АНУ-аас 164 сая, Монголоос 547.160 мянган хэрэглэгч, Твиттер дээр АНУ-аас 141,8 сая, Монголоос 50 мянга орчим хэрэглэгч байна.

Эндээс дүгнэхэд, интернэтийн өлгий АНУ-д Фейсбүүкийг нийт хүн амын 52.56 хувь, харин Монголд 17.73 хувь хэрэглэж байна.

Эндээс харахад, дижитал дивайд (digital divide) гэх ойлголтыг ойлгож, төр засгийн хэмжээнд нэгдмэл бодлого болгож гэр хороолол, хөдөө орон нутгийг интернэт сүлжээнд холбох ажлыг иж бүрэн зохицуулах шаардлагатай болжээ.

Цагдаагийн байгууллагад “Цахим гэмт хэргийн хохирогч боллоо” гэсэн гомдол цөөнгүй бүртгэгдэх болсон. 2014 оны 12 сарын байдлаар 64 гэмт хэргийг бүртгэж, мөрдөн байцаалтын ажиллагаа хийж буй юм байна. Үүнээс секс сүрдүүлгийн 39, луйврын дөрөв, гар утасны мессэж ашигласан хоёр, хортой код хэрэглэсэн хоёр, цахим шуудан ашиглаж бусдыг дарамталсан 10, оюуны өмчийг хууль бусаар ашигласан гурав, садар самуун сурталчилсан гурван төрлийн гэмт хэргийг цагдаагийн байгууллага шалгаж байгаа аж. Заримыг нь прокурорын хяналтад шилжүүлжээ.

Цахим шууданг ашиглан иргэдийн хувийн мэдээллийг хууль бусаар олж авч, итгэл үнэмшлийг нь төрүүлж, залилсан тохиолдол ч гарсан байна. Үүний улмаас дээд тал нь 60 гаруй мянган ам.доллараар хохирсон хүн байгаа талаар ЦЕГ-ын Хэвлэл мэдээллийн төвөөс мэдээллэв[538].

Аливаа байгууллага гадаад худалдаа эрхэлдэг, гадны аль нэг байгууллагатай цахим шуудангаар харилцан төлбөр мөнгө шилжүүлдэг бол дараах зүйлсийг анхаарах хэрэгтэй. Үүнд цахим шуудан илгээж буй и-мэйл хаягийг шалгах, цахимаар ирсэн банкны нэр, дансны дугаар байгууллагын нэр зэргийг нягтлах, факс, утсаар нь холбогдож, тулгалт хийх, цахим шууданд хандаж буй ажилчдын бүртгэл хийх шаардлагатай” гэв.

Энэ бүхэн мэдээллийн болон сүлжээний аюулгүй байдалд тулгарч буй эрсдэл, аюулууд улам бүр өсөн нэмэгдэж байгаа, мэдээллийн дайн байнга явагдаж байгааг нотлон харуулж байгаа үзүүлэлт гэж болно. Энэ хандлагыг төр, засгийн болон боловсролын, бусад ААНБ-ын түвшинд ойлгон мэдэрч хүлээн авч, зохих арга хэмжээг хэрэгжүүлж, эрсдлийн үнэлгээ, аудит хэрэгжүүлж, хүний нөөцийг сайтар бэлтгэн хөгжүүлж, МАБ-ын удирдлага, хамгаалалтын арга хэмжээ хэрэгжүүлж чадсанаар улам бүр өсөн нэмэгдэж буй эрсдлээс хамгаалагдах, болзошгүй аюултай тэмцэх бэлэн байдлаа (мэдээллийн аюулгүй байдлыг хангах) бий болгож чадна.

Тухайлбал, 2014 оны 1-р сард явуулсан тандалт судалгаанаас үзэхэд ширээний, зөөврийн, гар утас болон бусад ухаалаг хэрэгсэлийг ашиглан интернетэд байнгын холбогддог хүний тоо /давхардсан/ 2.8 сая давсан тооцоо гарч байна.

Блогчид өөрийн гэсэн уншигчтай болж, өдрөөс өдөрт нэмэгдэж буй сайтууд /сайтын тоо 30000-д хүрч, нэг сайтад хандах хандалтын тоо дунджаар 15000 болсон/ хүмүүсийн анхаарлыг ихээр татах болсон.

Улаанбаатар хотын 12-оос дээш насны нийт хүн амын 60 хувь нь, тэр тусмаа 12-29 насны хүн амын 75-78 хувь нь өдөр бүр интернэтэд холбогдож байна.

Интернэт хэрэглэгчдийн хамгийн их ашигладаг сайтуудыг www.gogo.mn, www.zaluu.com, www.news.mn тэргүүлж, мэдээллийн сайтуудаас мөн www.gogo.mn, www.olloo.mn, www.zaluu.com зэрэг сайтууд хамгийн хүртээмжтэй байсан юм.

Эдгээр мэдээллийн сайтууд руу орохдоо интернэт хэрэглэгч 2 хүн тутмын нэг нь шууд холбогдож, 5 хүн тутмын нэг нь түлхүүр үгээр хайлт хийн google-ээр дамждаг гэжээ. Мөн Facebook-ээр дамждаг гэж судалгаанд оролцогчдын 21 хувь нь хариулсан юм.

Холболтыг насны бүтцээр нь ангилбал шууд холбогддог гэж 20-29 насныхан илүүтэй хариулсан бол 12-19 насныхны түлхүү facebook-ээр дамждаг, 40-өөс дээш насныхны хувьд google-ээр хайлт хийж тухайн мэдээллийн сайтруу холбогддог нь тодорхой байна.

Улаанбаатар хотын 12 ба түүнээс дээш насны нийт хүн амын 84 хувь нь ямар нэгэн байдлаар интернэт ашиглаж байна. Үүнээс 60 гаруй хувь нь өдөр бүр, 16 хувь нь 7 хоногт, 4

[538]ЦЕГ-ын Хэвлэл мэдээллийн төвийн ажилтан, цагдаагийн ахмад Ё.Лхагвасүрэн., УБ., 2015.01.14.

хувь нь 14 хоногт, 3 хувь нь сард, 1 хувь нь улиралд тус бүр нэгээс доошгүй удаа интернэт ашигладаг нь судалгаагаар тогтоогдож байна.

Монгол Улсад одоогийн байдлаар зөвхөн мэдээллийн сайт гэхэд 120 гаруйд хүрч нэлээд нь идэвхтэй үйл ажиллагаа явуулж байна. Монголын сайтуудын холбоо, мэдээллийн сайтуудын нэгдсэн ассоциаци, ҮДТ, КАБГ, Монголын Кибер Довтолгоотой Тэмцэх Төв, MonCIRT /Mongolian Cyber Incident Response Team: кибер довтолгооны эсрэг хариу үйлдэл үзүүлэх үндэсний төв /CSIRT /компьютерийн аюулгүй байдлын будлиантай тэмцэх баг/, Хэвлэлийн хүрээлэн, Глоб интернэшнл төв зэрэг төрийн болон төрөлжсөн төрийн бус байгууллагууд /ТББ/ байгуулагдаж эдгээр судалгааны байгууллагуудад шинэ судлагдахууны судалгааны ажлыг эхлүүлж эрдэм шинжилгээний хэд хэдэн хурал зохион байгуулаад байна.

Гэмт халдлагын тандалт судалгааны түвшин

Кибер орчин дахь гэмт халдлагын өнөөгийн түвшний тандалт судалгааг МКДТТ-тэй хамтран явуулсан.

Монголын Кибер Довтолгоотой Тэмцэх Төв 2008 онд хэрэгжүүлсэн төслийн хүрээнд халдлага илрүүлэх хяналтын (мониторинг) систем байгуулсан бөгөөд энэ систем тогтвортой ажиллаж Интернетийн сегментээр орж ирж буй төрөл бүрийн халдлагыг илрүүлэх боломж бүрдсэн.

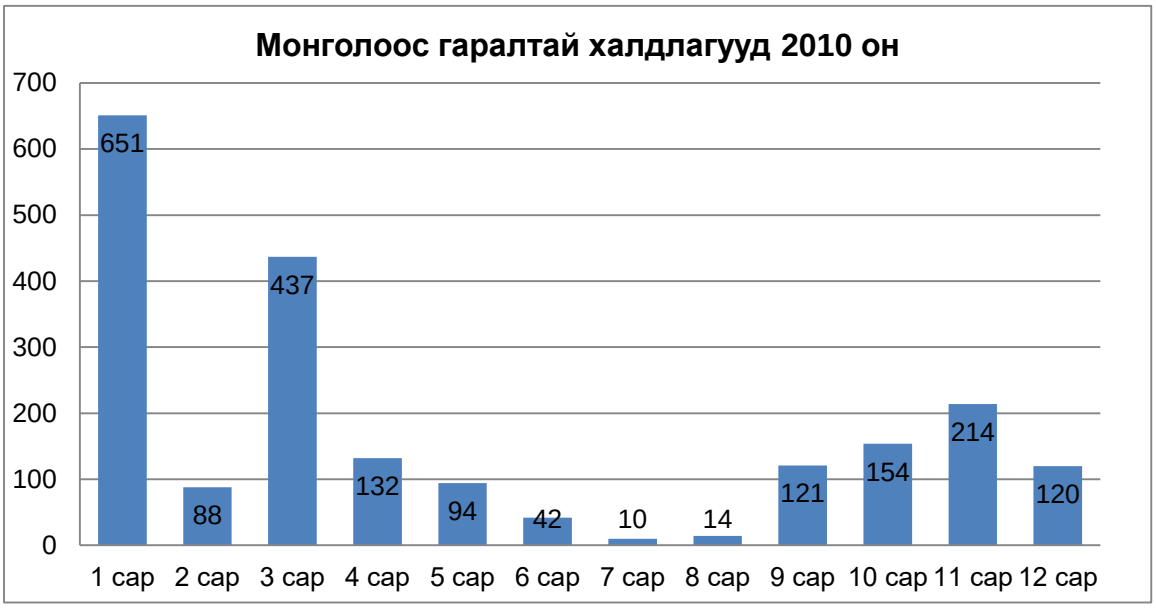
Хяналтын системийг 2008 оны 12-р сараас эхлэн ажиллагаанд оруулж 2009 оны 1-р сараас эхлэн туршилтаар ажиллуулж, тохируулга, сайжруулалт хийсний үр дүнд 2009 оны 06-р сараас эхлэн бүрэн хэмжээгээр тогтвортойгоор ажиллаж байна.

Тиймээс 2009 оны 06-р сараас өмнөх өгөгдлүүд нь бүрэн хэмжээнд шинжлэгдэх боломжгүй, өрөөсгөл шинжтэй байсан болно.

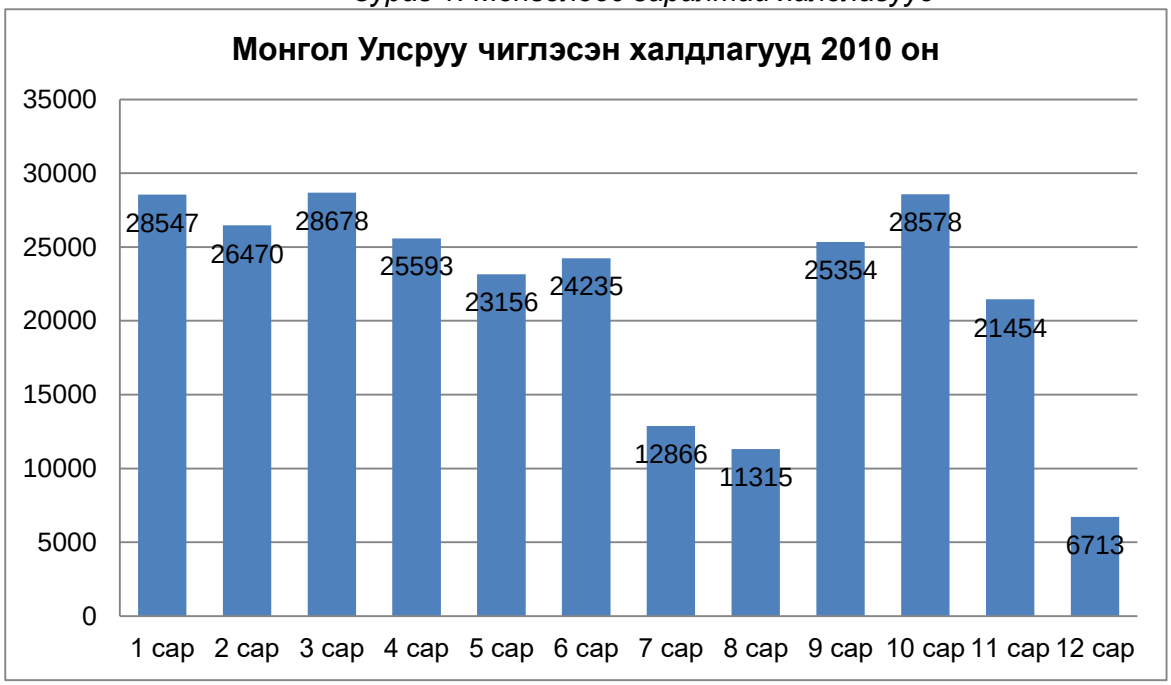
Мониторингийн системийн хүрээнд Интернет гарцууд дээр байрлуулсан мэдрэгч сенсорууд (илрүүлэгч)-ын мэдэрч бүртгэж байгаа халдлагууд (будлиан) сар бүр тогтмол өсөх хандлагатай байна.

Мэдрэгчүүд дээр бүртгэгдсэн халдлагуудыг цугларсан статистик мэдээн дээр тулгуурлан график дүрслэлээр харуулав. Дараах зургуудад 2010-2012 онд мониторингийн системд бүртгэгдсэн халдлагуудын хандлагыг харууллаа.

МОНГОЛ УЛСЫН ИНТЕРНЕТИЙН СЕГМЕНТЭД БҮРТГЭГДЭЖ БУЙ СҮЛЖЭЭНИЙ ХАЛДЛАГУУД



Зураг 1. Монголоос гаралтай халдлагууд

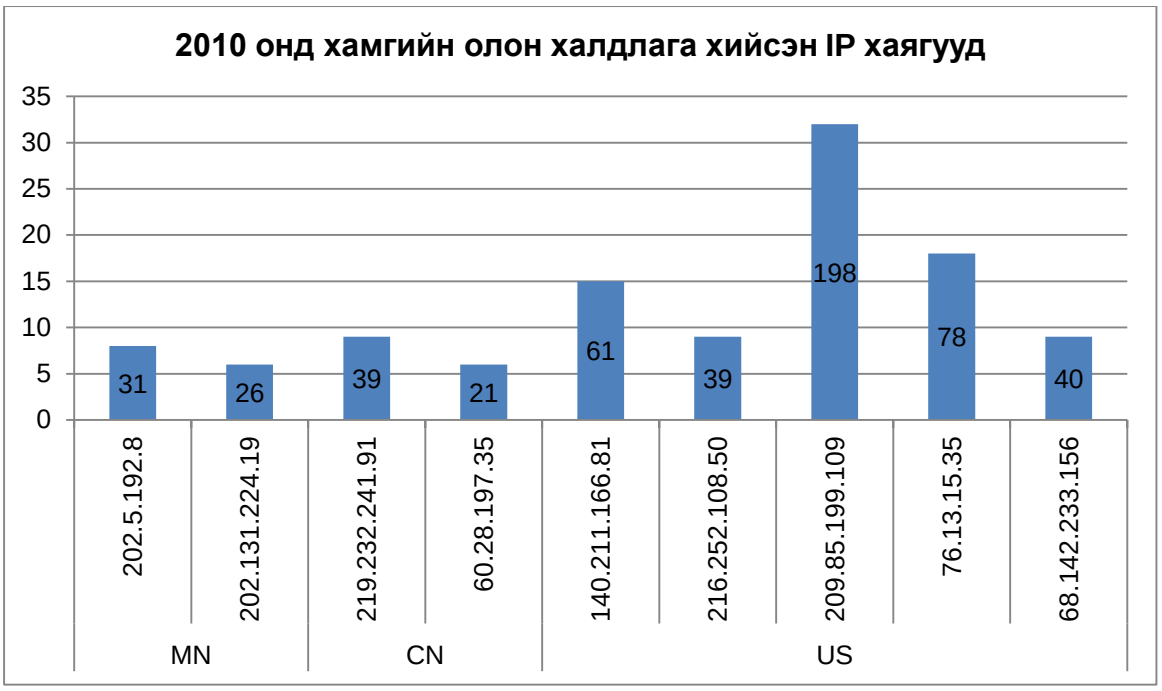


Зураг 2 Монголын Интернет сегментэд гаднаас халдсан халдлагууд

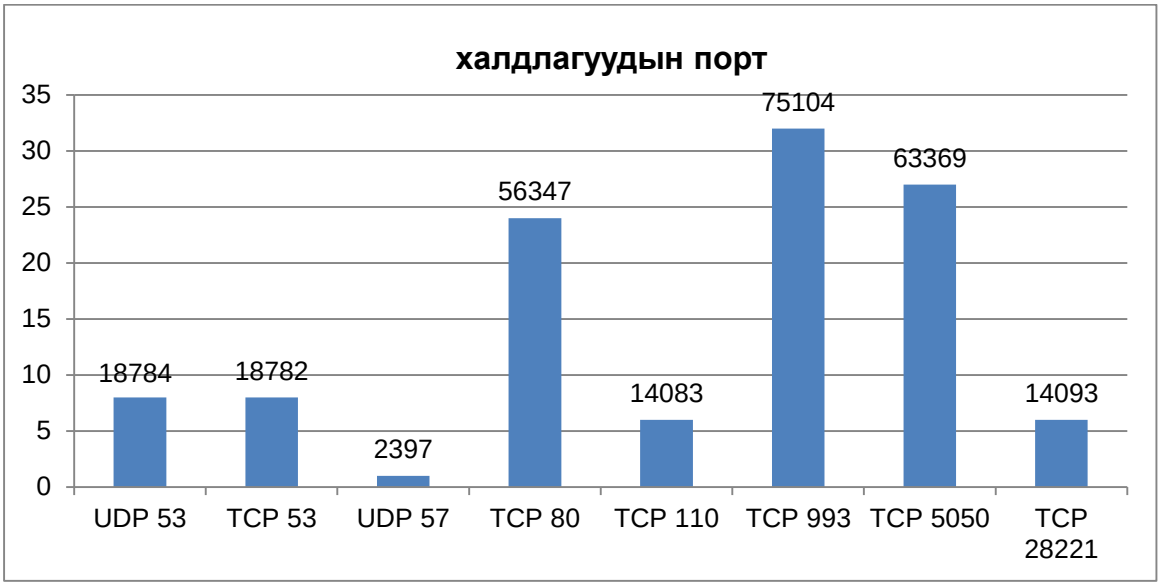
Зураг 1 ба Зураг 2 дээрх графикуудыг харьцуулахад Монгол Улсаас гадагш чиглэсэн халдлагуудын тоо нь харьцангуй бага байгаа бөгөөд гаднаас Монгол Улс руу чиглэгдсэн халдлага үүнээс 20-30 дахин их байна.

Зургаас дүгнэн үзэхэд Монгол Улсын өгөгдөл мэдээлэл, веб хуудсууд болон мэдээллийн технологийн дэд бүтцийг гадны улс орнууд маш ихээр сонирхдог болох нь харагдаж байна.

Дараагийн зургуудад халдлагуудын IP хаяг, порт, улсаар нь сар бүрээр ялган харууллаа.



Зураг 4. 2010 онд бүртгэгдсэн халдлагуудын IP хаягууд.



Зураг 5. Халдлага үйлдэхдээ ашиглаж буй портууд

Монгол Улсын интернетийн дэд бүтэц, сегментэд халдаж буй халдлагууд болон Монголоос гаралтай халдлагын тоог эх үүсвэр (улс)-тэй нь гарган харууллаа.

Графикуудаас харахад, Монгол Улс руу хамгийн ихээр халдлага хийдэг эх сурвалж нь Хятад, Оросын Холбооны улс болон Америкийн нэгдсэн улсуудад байдаг IP хаягууд байна. Тухайлбал 2010 онд:

1. Хятад улсаас 42504
2. Оросын Холбооны улсаас 27791,
3. Америкийн нэгдсэн улсаас 28240,
4. Бразилаас 15355,
5. Тайванаас 14593,
6. Румынаас 9115,
7. Японоос 8417,

8. Италиас 7575,
9. ХБНГУ-аас 7402,
10. Польшоос 6009,
11. Солонгосоос 5404,
12. Унгараас 5575,
13. Энэтхэгээс 4379,
14. Францаас 3814,
15. Канадаас 3430,
16. Мьянмараас 2424,

Монголын IP хаягуудаас 2077 удаа халдлага үйлдсэн тоогоороо эрэмблэгдсэн байна.

Зураг 2-оос харахад, Монгол Улсын интернет сегмент, дэд бүтэц, өгөгдөл мэдээлэлд халдаж буй халдлагууд сар бүр 20000-аас дээш гарч байгаа ба зөвхөн 2010 оны 07, 08, 12-р сард бага зэрэг буурсан байгаа нь зуны амралт, шинэ жил, бусад өвлийн баяруудтай холбоотой байж болох бөгөөд идэвх нь буурахгүй байнга өсөх хандлагатай байгаа бөгөөд сард ойрлцоогоор 30.0-45.0 мянган халдлага хандалттай байна.

Монгол Улсад 1992 оноос эхлэн эрх зүй, эдийн засаг, улс төр, боловсрол зэрэг нийгмийн бүхий л салбарын шинжлэх ухааны мэдлэгийн тогтолцоо болон төрөөс баримтлах суурь бодлогыг шинэчлэх зайлшгүй хэрэгцээ, шаардлагын үүднээс салбар бүрийн шинжлэх ухааны урсгал, чиглэл, эрх зүй, эдийн засгийн дотоод, гадаад хамтын үйл ажиллагаан дахь аюулгүй байдлыг хангах зохицуулалтыг эрс өөрчилсөн олон арга хэмжээ хэрэгжиж байна.

Шинэ мянганы их өөрчлөлтийг нэг хэсэг болсон кибер орчины аюулгүй байдлын эрх зүйн зохицуулалтын өнөөдрийн түшинг авч үзье.

Эрх зүйн орчны хувьд:

1992 оноос хойш УИХ-аас нийт 487 хууль[539], төрөөс баримтлах бодлогын тулгуур баримт бичиг 23 буюу давхардсан тоогоор 50 тогтоол, Олон улсын гэрээ /нэмэлт протоколын хамт/ 319[540] батлан улмаар эдгээр хууль, суурь бодлогын баримт бичгийг хэрэгжүүлэх зорилтын хүрээнд Засгийн газрын тогтоол 1140 орчим батлагдан мөрдөгдөж байна.

Өнөөдөр хүчин төгөлдөр мөрдөж байгаа хуулийн 22 буюу 4,5 хувь (хамааралтай 1-14 заалт бүхий хууль), УИХ-ын тогтоолын 6 буюу 12 хувь, Олон улсын баримт бичгээс байхгүй, Засгийн газрын тогтоолын /хүчинтэй байгаа/ 12 орчим буюу 1 хувь орчим нь кибер орчны аюулгүй байдлыг зохицуулах зорилготой байгаа хэдий ч хоорондын уялдаа, холбоо, нэгдмэл зохицуулалтын зорилго хангалтгүй, хуулийн хэм хэмжээний бүтцийн алдаа ихтэй байна.

1994 онд 9 багц асуудлаар “Үндэсний аюулгүй байдлын үзэл баримтлал”-ыг баталсан бол 2010 оны 07 дугаар сарын 05-ны өдөр шинэчлэн 6 багц асуудлын хүрээг хамааруулан батласан. Аюулгүй байдлыг хангах үйл ажиллагааны хүрээнд Засгийн газрын 2010 оны 06 сарын 02-ны өдөр 141 дүгээр тогтоолоор 4 багц асуудлаар “Мэдээллийн аюулгүй байдлын үндэсний хөтөлбөр” батлагдаж хөтөлбөр хэрэгжүүлэх үйл ажиллагааны нэг хэсэг кибер орчны аюулгүй байдлыг хангах, хамгаалах хүрээнд ТЕГ-ын харъяанд Кибер аюулгүй байдлыг газар байгуулагдсан, мөн "Үндэсний Дата Төв" УТҮГ нь 2009 оны 6 дугаар сарын 24-ны өдөр байгуулагдсан бөгөөд байгуулагдсан цагаасаа эхлэн төрийн цахим дата, мэдээ, мэдээллийг хадгалах, хамгаалах, боловсруулалт хийх болон төр, хувийн хэвшлийн байгууллагуудад мэдээллийн технлогид суурилсан үйлчилгээг үзүүлж байгаа бөгөөд өөр макро түвшинд шийдвэрлэхээр төлөвлөсөн суурь ажил тэр дундаа бодлогын баримт бичиг, суурь хууль батлах ажлын хэрэгжилт хангалтгүй байна.

Харин энэ салбар цаг, минутаар хөгжиж байгаатай холбоотойгоор олон улсын нийтлэг “**стандарт”-**ын талаархи ойлголтыг манай улс нэгэнт бий болгосон нь сайн үзүүлэлт боловч

[539]Legalinfo.mn., 2015 оны 01 дүгээр сарын 08-ны байдлаар.
[540]Мөн тэнд.

органик хууль, тогтоомжуудаар хараахан зохицуулаагүй байгааг дараагийн бүлэг, сэдэвт тоймолж тусгалаа.

Одоогоор Монгол Улсын нөхцөлд Харилцаа холбооны зохицуулах хорооноос 2011.02.27-ны өдөр батлагдсан “Тоон контентийн үйлчилгээний зохицуулалтын ерөнхий нөхцөл шаардлага”, Монголын вэб сайтууд холбооны батлагдсан “Вэб сайт эрхлэгчдэд тавигдах нөхцөл шаардлага” 2011 он зэрэг цөөхөн эрх зүйн дагнасан зохицуулалт байгаа боловч “төрөөс мэдээллийн аюулгүй байдлын талаар баримтлах бодлого”-ын баримт бичиг, “мэдээллийн аюулгүй байдлын ерөнхий хууль”, бусад салбар хууль, “Оюуны өмчийн зохицуулалт”, “Сөрөг контентийн зохицуулалт”, “Мэдээлэл авах эрх, нууцын зохицуулалт” зэрэг олон зохицуулалт шаардлагатай байна.

Тухайлбал: ШУТИС-КТМС-ийн ахлах багш Ч.Эрдэнэбатын 2012-12-14-ний өдрийн “Монголын банкны вэб сайтуудын МАБ-ын зарим судалгаа: SSL, WAF, метадата” илтгэлд дурдсанаар одоогийн хэрэглэж байгаа цахим картны нууцлалд 2015 он гэхэд хакерууд чөлөөтэй нэвтрэх боломжтой аж.

Англиийн “Баркслай” банкны цахим картны нууцлал руу хакерууд дайрч жилд дунджаар 60 мянган еврогийн алдагдалд оруулдаг. Цахим картны системд дайран орж хамгийн дээд тал нь таван сая ам.доллар залилсан байна. Банкны сайтууд хэрэглэгчдийнхээ мэдээллийг найдвартай, сайн хадгалж хамгаалаагүйн улмаас картын мэдээлэл алдагдаж болно. Улмаар картын мэдээллийг олж авсан “хакер” гадны аль нэг оронд карт хэвлүүлэн түүнийг ашиглах явдал ажиглагдаж байна.

Улсын хэмжээнд хамгийн олон салбар нэгжтэй Хаан банкны сүлжээ орон даяар тасарсан тохиолдол гарсан. Нийслэл төдийгүй орон нутаг дахь бүх салбар гүйлгээ хийх боломжгүй болжээ. Мөн АТМ-р үйлчлүүлж болохгүй байв.

2007-2008 онд Засгийн газар түүний харъяа газруудын 66, олон нийтийн байгууллагын 40, боловсролын чиглэлийн 64, банкны 6, компанийн 64, сонин болон мэдээллийн 10, бусад чиглэлийн 80 орчим вэб хуудас хакеруудын дайралтад өртсөн судалгаа гарсан.

Эцэст нь дүгнэхэд Монгол Улсын хувьд Кибер терроризм ба кибер гэмт хэргийн эрх зүйн зохицуулалт, кибер терроризмтой тэмцэх нэгж, байгууллагын бэлэн байдал, ур чадварын түвшинг энэ нийтлэлийн хүрээнд тодорхойлоход бэрхшээлтэй.

Монгол Улсад терроризмын зорилгоор мэдээллийн цахим сүлжээнд халдсан тохиолдол бүртгэгдсэн эсэх талаар нэгдмэл байдлаар судлах шаардлага бий болжээ гэж дүгнэсэн.

Эрүүгийн эрх зүйн ухааны үүднээс авч үзвэл:

Компьютерийн мэдээллийн эргэлтийн хүрээ өргөжиж улмаар гэмт халдлагад өртөх хандлагатай болсныг тусган авчМонгол Улсын 1996 оны Эрүүгийн хуульд “Мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг” гэсэн 11 дүгээр бүлгийг анх удаа оруулж,

- Компьютерийн мэдээллийг хууль бусаар өөрчлөх гэсэн 153 дугаар зүйл,
- Компьютерийн мэдээлэл программыг эвдэх,сүйтгэх гэсэн 154 дүгээр зүйл,
- Компьютерийн мэдээллийг хууль бусаар олж авах гэсэн 155 дугаар зүйл,
- Компьютерийн мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэх, борлуулах гэсэн 156 дугаар зүйл,
- Нянтай программ зохион бүтээх,ашиглахгэсэн 157 дугаар зүйлүүдийг хуульчилсан. Үүний дараа 2002 оны Эрүүгийн хуулийг шинэчлэн найруулахдаа“Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг” гэсэн 25 дугаар бүлгийг оруулж,
- Компьютерийн мэдээлэл, программыг өөрчлөх, эвдэх, сүйтгэх гэсэн 226 дугаар зүйл,
- Компьютерийн мэдээллийг хууль бусаар олж авах гэсэн 227 дугаар зүйл,
- Компьютерийн мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэх, борлуулах гэсэн 228 дугаар зүйл,

- Нянтай программ зохион бүтээх ашиглах гэсэн 229 дүгээр зүйлийг тус тус оруулсан байна.

Хуульчилж байх үед интернет үүсээд дөнгөж 2 жил болж байсан ба энэ салбарын учрыг мэдэх хүн, хэрэглэдэг хүн, ач холбогдолыг нь хүртсэн хүн бараг байхгүй тийм л цаг үеийн эрх зүйн тогтолцоотой байна.

Ийнхүү эрүүгийн эрх зүйгээр кибер орчны аюулгүй байдлыг хүрээ дэх бусдын эрх, ашиг сонирхолыг хамгаалсан хэдий ч өнөөгийн байдлаар гэмт хэргийн бүрэлдэхүүн, нэр томъёолол, үзэгдэл, үйл явцын хоорондын харилцан хамаарал, олон улсын чиг хандлага зэрэгтэй харьцуулан дүгнэх боломж хомс байна. Учир нь 18 жилийн өмнө ерөнхий байдлаар хуульчилсан яг тэр хэвээрээ байна.

Иймд эрүүгийн эрх зүйн асуудлын хүрээнд гипотиз, диспозиц, санкцийг шинжлэх ухааны үндэслэлтэйгээр боловсронгуй болгож, эрс сайжруулах цаг үе нэгэнт болсон.

Хуучин болон одоо хүчин төгөлдөр мөрдөгдөж байгаа эрүүгийн хуульд энэ салбар дахь гэмт хэргийг хэрхэн хуульчилсан нөхцөлийг хууль зүйн шинжлэх ухааны үүднээс тайлбарлах хэрэгтэй.

Хууль тогтоогчийн илэрхийлсэн санаанаас үзэхэд энэ салбарын гэмт хэргүүдийн үндсэн **объект нь** компьютер биш, харин нийгмийн тодорхой харилцаа болногэжээ.

Энэ нь компьютерийн мэдээллийг бий болгох, боловсруулах, хуримтлуулах, хадгалах, эрж хайх, тараах болон хэрэглэгчид гаргаж өгөх явцад үүсэж буй мэдээллийн харилцааны дүнд үүсэх эрх, ашиг сонирхол байх учиртай.

Түүнчлэн мэдээллийн технологи, хангалтын хэрэгсэл бий болгох, ашиглах болон компьютерийн мэдээллийг хамгаалах явцад үүсэх харилцаа үүнд хамаарна.Харин компьютерийн мэдээлэл гэж юу болохыг нэг мөр тодорхойлсон эрх зүйн акт Монгол Улсад хараахан гараагүй байна.

Гэхдээ уг ойлголтыг тодорхойлохгүйгээр энэ төрлийн гэмт хэргийн тодорхойлолтыг гаргах боломжгүй.

Хөгжингүй улс орнуудын “Мэдээллийн болон мэдээлэл хамгаалах” тухай хуулиудад мэдээлэл гэдэг ойлголтыг “хүмүүс, эд зүйлс, факт, үйл явдал, үзэгдэл болон /процесс/ үйл ажиллагааны талаархи /илэрхийлэгдсэн хэлбэрээсээ үл хамаарах/ бүх төрлийн мэдээллүүд” гэж тодорхойлсон байдаг.

Эдгээрээс компьютер болон ухаалаг техник хэрэгсэл, тэдгээрийн систем, сүлжээнд хадгалагдаж байгаа болон дамжуулж байгаа, түүнчлэн энэ салбарт үйлдэгдэж байгаа гэмт хэргийг мөрдөн шалгахад ач холбогдолтой бусад мэдээллүүдийг компьютерийн мэдээлэл гэж үздэг.

Үүнээс гадна, компьютерийн мэдээллийн эсрэг гэмт хэргийг ойлгож зүйлчлэхэд мэдээллийн систем, мэдээллийн сүлжээ, мэдээлэлжүүлэлт, баримт бичиг-мэдээлэл, мэдээллийн ажиллагаа, мэдээллийн нөөц, иргэдийн тухай мэдээлэл, нууц мэдээлэл, мэдээлэл хэрэглэгч, компьютерийн программ, өгөгдлийн бааз болон программыг өөрчлөх, зохицуулан тохируулах, устгах, эвдэх, сүйтгэх гэдэг нэр томъёонуудыг ойлгож мэдэх нь чухал.

МАБ-ыг хангах, хамгаалахын тулд энэ салбарт олон улсын хэмжээнд хэрэглэгдэж байгаа нэр томъёог нэр мөр болгон ойлгох, үйл ажиллагаандаа хэрэглэх нь нэн чухал.

МАБ-д хэн нэгэн зөрчил гаргач халдахдаа хамгийн эхэнд мэдээллийн сүлжээнд нэвтрэх үйлдэл гүйцэтгэхээс эхлэнэ гэж олон улсын эрх зүй үздэг түүнээс биш шууд мэдээлэл дунд нь орж сүйтгэхгүй, энэ нь орон байр агуулах сав-д нэвтэрч хулгайлах гэмт хэрэг үйлдэж байгаатай яг адил эхлээд л хууль бусаар нэвтэрнэ гэсэн үг.

Иймучиронолын үүднээс компьютерийн сүлжээ, систем, кибер орчины тухай эхлээд товч тодорхойлолтыг тайлбарлах хэрэгтэй.

/ЭХ-ийн 25 дугаар бүлэгт энэ ойлголтын агуулгыг дутагдалтай томъёолсон учир хариуцлага тооцоход хүндрэл учирч байгаа гэж үзэх үндэстэй/

Компьютер болон мэдээллийн технологийн сүлжээ[541] **:**Хоёр буюу хэд хэдэн компьютер, ухаалаг технологи-хэрэгсэл хоорондоо холбогдон мэдээлэл болон эх сурвалжууд, нэмэлт төхөөрөмжүүдийг хамтран ашиглах боломжоор хангагдахыг хэлнэ.

Сүлжээний хэрэглэгчид нь файл, принтер, бусад зүйлээ хамтарч хэрэглэж болохоос кабель утсаар болон утасгүй сүлжээ, Компьютерүүдийг сүлжээнд холбохын тулд тэдгээрийн холболтын техник хангамжийн болон програм хангамжийн орчин бүрдсэн байхыг.

Энд физик холболт хийх болон тэдгээрийг програм хангамжаар /**WiFi**/ холбох олон боломжууд байдаг.

Компьютерийн хамгийн том сүлжээ нь **Интернет** юм. Онолын хувьд аливаа юмс, үзэгдэл, үйл явдлыг танин мэдэхэд тухайн зүйлийн илрэх хэлбэр, хамаарал, холбогдол, үүсэн бий болох зүй тогтол, үүсэл, хандлагыг бодитой тогтоох нь чухал.

Иймд кибер орчины аюулгүй байдлыг хангах, хамгаалах үйл ажиллагаанд хэрэглэгдэж байгаа нийтлэг нэршил нэг мөр болоогүй байгаа учир олон улсын хэмжээнд хэрэглэж байгаа нэршлийг цаашид мөрдөх шаардлагатай.

Тухайлбал:

- **Сүлжээний техник хангамжийн орчин**[542] **:** Сүлжээний техник хангамж нь компьютерүүд хоорондоо холбогдоход зориулсан физик компонентууд юм.

Сүлжээний адаптер, сүлжээний кабель**,** **hub, repeater, switch, router, brouter, модем, bridge, wireless** гэх мэт физик төхөөрөмжүүдээс гадна кабель утсанд холбодог толгой буюу **connector, transceiver, vampire tape,сүлжээний бахь,** сүлжээний хэвийн ажиллагааг шалгадаг тестер гэх зэргийг мөн авч үзнэ.

Зарим төхөөрөмжүүдийг сүлжээний үйлдлийн системд таниулж өгөх шаардлагатай байдаг.

- **Сүлжээний програм хангамжийн орчин**[543]: сүлжээний компьютерүүдийг бусад компьютерүүдтэй нь холбох интерфейс болж байдаг сүлжээний үйлдлийн систем, сүлжээний протокол зэргийг ойлгоно. Ажиллуулах програм нь сүлжээний хэрэглэгчийн интерфэйс, мэдээлэл, файл, график, видео, принтер ба дискийн хэрэглэлтийн зөвшөөрөл тогтоох програмаас тогтоно. Үүний нэг жишээ нь **client-server** юм.
- **Систем:** Мэдээллийн техник-хэрэгслийн мэдээлэл боловсруулж хадаглах, санах ой бүхий эд ангийн тогтолцоо,
- **“Компьютерийн систем”** гэж аль нэг нь эсвэл зарим нь програмтай холбогдож өгөгдлийг автоматаар боловсруулах үйл ажиллагааг хийдэг ямар нэгэн төхөөрөмж эсвэл хоорондоо холбогдсон төхөөрөмжүүдийн бүлэг эсвэл хамааралтай төхөөрөмжүүдийг;
- **“Компьютерийн өгөгдөл”** гэж компьютерийн системд боловсруулахад тохиромжтой хэлбэрт байгаа бодит байдлын аливаа дүрслэл, мэдээлэл эсвэл концепц, мөн түүн дотроо компьютерийн системийн аливаа функцийг гүйцэтгэх шалтгаан болох программыг агуулна.
- **“үйлчилгээ үзүүлэгч” гэж** Компьютерийн системийг ашиглан харилцаа холбоо хийх боломжийг үйлчилгээний хэрэглэгчдэд олгодог аливаа төрийн эсвэл хувийн хэвшлийн нэгжийг,

тус харилцаа холбооны үйлчилгээ эсвэл үйлчилгээний хэрэглэгчийн өмнөөс компьютерийн өгөгдлийг боловсруулдаг эсвэл хадгалдаг ямар нэгэн бусад нэгжийг;

- **“мэдээллийн урсгалын өгөгдөл” гэж** компьютерийн системийн аливаа харилцаа холбоотой хамааралтай, харилцаа холбооны хэлхээний нэг хэсэг болж компьютерийн

[541] Л.Цогтбаяр “Кибер орчинд үйлдэгдэж байгаа гэмт хэрэгтэй тэмцэх эрх зүйн тогтолцоо, хандлага” Хууль сахиулахуй сэтгүүл-2, УБ., 2014

[542] Л.Цогтбаяр “Кибер орчинд үйлдэгдэж байгаа гэмт хэрэгтэй тэмцэх эрх зүйн тогтолцоо, хандлага” Хууль сахиулахуй сэтгүүл-2, УБ., 2014

[543] Л.Цогтбаяр “Кибер орчинд үйлдэгдэж байгаа гэмт хэрэгтэй тэмцэх эрх зүйн тогтолцоо, хандлага” Хууль сахиулахуй сэтгүүл-2, УБ., 2014

системээр үүсгэгдсэн, харилцаа холбооны эх үүсвэр, очих газар, чиглэл, хугацаа, он сар өдөр, хэмжээ, үргэлжлэх хугацаа, суурь үйлчилгээний төрлийг тодорхойлох аливаа компьютерийн өгөгдлийг;

- **Мэдээллийн техник:**Ухаалаг гар утас, компьютер, нөөтбүк, таблет гэх мэт хэрэгсэл,
- **Крекер** (**Cracker**): Хакерын мэдлэгээ муу зүйлд хэрэглэж бусдын компьютерийн сүлжээнд нэвтрэх, мэдээллийг устгах эсвэл сүлжээ, системыг хорт муу санааны үүднээс ашигладаг хар хакер хүмүүс юм. **Крекер** бол ямар нэг ашиг сонирхлын дагуу хуулиар хамгаалагдсан програм хангамжийн хамгаалалтыг эвдэлдэг програмист юм.
- **Хакер (Hacker):**Ёс зүйт хакерын тухайд мэдлэгээ ашиглан бусдын мэдээллийн сүлжээнд нэвтэрч аюулаасурьдчилан сэргийлэх зүйлд хэрэглэж ашигладаг цагаан хакер хүмүүс юм. Зарим тохиолдолд ёс зүйгүй хакер бас байна.
- **Хакер** гэдэг нэр томьёо нь анх компьютертай ямар ч хамааралгүй хүмүүсийг хэлдэг байв. “**Хак**” гэдэг нь англи хэлэнд сүхээр мод цавчихад гарах дууг илэрхийлдэг бөгөөд хакер гэдэг нь эрт үед модоор урлагийн хосгүй үнэт бүтээл туурвидаг уран гарт мужаануудыг хэлдэг байжээ[544].

1967 оны 12 дугаар сард Массачусетийн Технологийн Их сургуулийн дэргэдэх “төмөр замын загвар”-ын клубд нэгэн цуглуулагч өөрт байгаа хуучны телефон хэрэгслүүдийг хандивласан байна. Ингээд тус клубийнхэн үүнийг ашиглан замын зангилаануудыг утасны дугаар залган хянах системийг бүтээсэн бөгөөд уг төхөөрөмжийн хэрэглээгээ **“хакинг”**[545] гэж нэрлэж өөрсдийгөө хакерууд гэж нэрлэсэн.

Ер нь заавал компьютерийн програм ч биш харин ямар нэгэн зүйлийг хүний анхаарал татаж чадахуйц хийж бүтээснийг хакинг гэдэг байжээ.Одоо үед хакер гэдэг нэр нь мэдээллийн хулгайч, дээрэмчин, үймүүлэгч, вирус зохиогч, системийн програмист гээд бүх зүйлийг хамрах болсон. Энэ нь хуучны хакеруудад таагүй сэтгэгдэл төрүүлж тэд зарим нэг ялгааг гаргахын тулд крекер гэдэг нэрийг хэрэглэхийг сэтгүүлчдэд санал болгосон ч төдийлөн нийтэд түгээмэл болоогүй билээ.

Иймээс хакинг гэдэг ойлголтыг зөвшөөрөлгүйгээр компьютерийн системд нэвтрэх хэмээн ерөнхий ойлголтоор ашиглаж байна.

Мэдээлэлжүүлэлт гэдэг нь иргэд, байгууллага, албан газрын мэдээллийн нөөцийг бий болгох, ашиглах эрхийг хэрэгжүүлэх, мэдээллийн хэрэгцээг хангах тохиромжтой нөхцөлийг бий болгоход чиглэгдсэн нийгэм-эдийн засаг, шинжлэх ухаан-техник, зохион байгуулалтын ажиллагаа юм[546].

Мэдээллийн аюулгүй байдал нь иргэд, байгууллага, төрийн ашиг сонирхлын тусын тулд мэдээллийн орчныг бий болгох, ашиглах, хөгжүүлэх явдлын хамгаалагдсан байдлыг хэлдэг.

Баримт бичиг-мэдээлэл гэж биет зөөгч дээр бэхжүүлэгдсэн бөгөөд бүрдүүлэгч зүйлүүдийг агуулсан мэдээллийг хэлнэ.

Мэдээллийн ажиллагаа гэдэг нь мэдээллийг цуглуулах, боловсруулах, хуримтлуулах, хадгалах, эрж хайх, тараах ажиллагаа юм.

Мэдээллийн систем гэж баримт бичиг, мэдээллийн технологийн эмхлэгдэн зохион байгуулагдсан нэгдлийг хэлнэ.

Мэдээллийн нөөц гэдэгт мэдээллийн систем дэх баримт бичиг, тэдгээрийн хуримтлал хамаарна.

Иргэдийн тухай мэдээлэл гэдэгт иргэний хувийн байдлыг тогтоох боломж олгож буй түүний амьдралын үйл явдал, баримт, нөхцөл байдлын талаархи мэдээ орно.

---

[544]Л.Цогтбаяр, “гэмт хэргийн нотлох баримтын онол” лекц, УБ., 2012
[545]Мөн тэнд.
[546] Д.Батзориг “Таны зөв сонголт” УБ., 2000, 4 дэх хуудас

Нууц мэдээлэл гэдэгт Монгол Улсын хууль тогтоомжийн дагуу ашиглах зөвшөөрөл олгодог, хамгаалалтын журам, дэглэм тогтоосон баримт бичиг-мэдээллийг оруулна.

Мэдээлэл хэрэглэгч гэж мэдээллийн систем ашиглаж буй субъектуудыг хэлдэг.

Компьютерийн программ гэдэг нь компьютер болон компьютерийн бусад төхөөрөмжийн хэвийн ажиллагааг хангахад зориулагдсан өгөгдөл болон командын нийлбэрийг илэрхийлэх объектив хэлбэр юм[547].

Өгөгдлийн сан гэдэгт компьютерийн тусламжтайгаар олж, боловсруулж болохоор системчлэгдсэн өгөгдлүүдийн нийлбэрийг илэрхийлэх объектив хэлбэрийг ойлгож болно.

Компьютер гэдэгт мэдээллийг автоматаар боловсруулах цахим тооцоолуур машиныг ойлгоно[548].

Компьютерийн систем гэдэг нь нэг буюу нэлээд хэсэг нь программын дагуу ажиллаж, өгөгдлүүдийг автоматаар боловсруулж байгаа ямар нэг төхөөрөмж буюу хоорондоо холбоотой хэсэг төхөөрөмж юм.

Компьютерийн өгөгдөхүүн гэж баримт, мэдээлэл, ойлголтыг компьютерийн системд боловсруулахад тохиромжтой хэлбэрээр оруулсан илэрхийллийг хэлнэ.

Компьютерийн сүлжээ гэдэгт хоёр буюу түүнээс дээш тооны компьютерийн хооронд мэдээлэл солилцох ажиллагааг хангаж буй технологийн системийг ойлгоно.

Мэдээллийн автоматжуулсан систем болон түүний технологийг хангах хэрэгсэл гэдэг нь мэдээллийн системийг зохион бүтээх, ашиглагдах үед бий болсон түүний ашиглалтыг хангаж буй программ, техник, хэл, эрх зүйн болон зохион байгуулалтын хэрэгслүүд /компьютерийн программ, техник хэрэгсэл, толь бичиг, ангилал, аргачлал, дүрэм, заавар, бүдүүвч, тайлбар г.м/ юм.

Компьютерийн вирус /нян/ буюу”**хортой программ**” гэж компьютер, түүний систем, сүлжээний хэвийн ажиллагааг хангахад зориулагдсан компьютерийн программын ажиллагааг алдагдуулахын тулд тусгайлан бүтээгдсэн программыг хэлдэг.

Эрүүгийн хуулийн тайлбар:

Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг гэж

Компьютерийн мэдээлэл, программ, түүний төхөөрөмжийг санаатай өөрчлөх, эвдэх, гэмтээх, ашиглах боломжгүй болгох, мэдээлэл сүлжээг сүйтгэх, компьютерийн мэдээллийг зөвшөөрөлгүй хуулбарлах, бусад хууль бус аргаар олж авах, компьютер, мэдээллийн хамгаалалттай сүлжээнд хууль бусаар нэвтрэх тусгай программ, техник хэрэгсэл бэлтгэх, нянтай программ зохион бүтээх, ашиглах, тараах зэрэг Эрүүгийн хуульд заасан нийгэмд аюултай гэм буруутай үйлдэл, эс үйлдэхүйн цогц бүрдлийг хэлнэ.[549]

Харин эрдэмтэн Ж.Болдбаатар “Хувь хүн, хуулийн этгээд, нийгэм болон төрийн мэдээллийн автоматжуулсан систем дэх эрх, ашиг сонирхлыг гэм буруутайгаар зөрчсөн, эрүүгийн хуульд заасан үйлдэл”[550] гэж тодорхойлжээ.

Нийтлэг бүрэлдэхүүн:

Объект: Монгол Улсын Эрүүгийн хуулиас үзэхэд, компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэргүүдийн нийтлэг объект нь мэдээллийг компьютерээр боловсруулах үед үүсэх нийгмийн харилцаа байна гэжээ.

Эрдэмтэн Г.Совд энэ гэмт хэргийн объектыг түүнийг эзэмшигч буюу гуравдагч этгээдийн мэдээллийн эрх[551] байна гэж тодорхойлсон.

[547] Д.Батзориг “Таны зөв сонголт” Сони сургалтын төв, УБ., 2000, 9 дэх тал
[548] Н.Батцэрэн “Компьютерийн үндсүүд” УБ, 1998., 3 дахь тал
[549]С.Жанцан “Монгол Улсын Эрүүгийн эрх зүй” УБ., 2004, 452 дахь тал
[550]Ж.Болдбаатар “Эрүүгийн эрх зүйн тулгуур ойлголтууд” УБ., 2002, 63 дахь тал
[551]Г.Совд “Монгол Улсын Эрүүгийн хуулийн тайлбар” УБ., 2002, 320-323 дахь тал

Халдлагын зүйл нь компьютерийн тодорхой мэдээлэл, компьютерийн тодорхой систем болон сүлжээний өгөгдлийн сан, түүний файлууд, түүнчлэн хангамжийн тусгай технологи, программ, компьютерийн мэдээллийг хамгаалах хэрэгсэл болон бусад зүйл байна.

Мөнгө, бусад материаллаг үнэт зүйл эсвэл тооцоолон бодох техникийн аппарат, техникийн хэрэгсэл нь энэ хэргийн шууд халдлагын зүйл болохгүй.

Тэрээр бусад гэмт хэргүүдийн халдлагын зүйл болдог. Тэгэхээр компьютерийн мэдээлэл, программыг өөрчилж, эвдэлж, сүйтгэсэн, компьютерийн мэдээллийг хууль бусаар олж авсан, компьютерийн мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэсэн, борлуулсан, нянтай программ зохион бүтээж, ашиглаж, тараасны үр дүнд бусад гэмт хэрэг үйлдэгдсэн бол гэм буруутай этгээд эрүүгийн хуулийн бусад зүйлд зааснаар давхар хариуцлага хүлээнэ.

Үүнд дараахи зүйлийг дурьдаж болно.

- Төрийн эсрэг гэмт хэргийг компьютерийн мэдээлэл ашиглан үйлдсэн бол /Эрүүгийн хуулийн 79,80,87,88 дугаар зүйл/;
- Хүний эрх,эрх чөлөө,алдар хүнд,нэр төрийн эсрэг гэмт хэрэг /110,111 дүгээр зүйл/;
- Иргэдийн улс төрийн,бусад эрх,эрх чөлөөний эсрэг гэмт хэрэг /131,135,136, 140,141,144,145,148,149,150,151,152 дугаар зүйл/;
- Аж ахуйн эсрэг гэмт хэрэг /156,158,159,164,169 дүгээр зүйл/;
- Захиргааны журмын эсрэг гэмт хэрэг /233, 235 дугаар зүйл/;
- Шүүн таслах ажиллагааны эсрэг гэмт хэрэг /246,247,253,257 дугаар зүйл/;
- Албан тушаалын гэмт хэрэг /271 дүгээр зүйл/ - байна.

Иймд компьютерийн гэмт хэргүүдийг өнөөгийн байдлаар:

- Цэвэр компьютерийн гэмт хэрэг /Эрүүгийн хуулийн 25 дугаар бүлэг/
- Компьютер ашиглан үйлдсэн хэрэг гэж ангилж болохоор байна.

Цэвэр компьютерийн гэмт хэрэг гэдэгт компьютерт хадгалагдаж буй мэдээлэл халдлагын зүйл нь болж, түүнд халдаж буй эрүүгийн хуульд заагдсан нийгэмд аюултай, гэм буруутай үйлдлийг ойлгоно.

Ийм мэдээллийг хууль бусаар ашигласны үр дагавар нь янз бүр байж болно.

Тухайлбал, оюуны өмчийн эрх зөрчигдөх, хувийн нууц задрах, эд хөрөнгийн хохирол учрах, байгууллагын ашиг сонирхол зөрчигдөх гэх мэт байж болно.

Тийм ч учраас энэ төрлийн гэмт хэргийг “Нийгмийн аюулгүй байдал, хүн амын эрүүл мэндийн эсрэг гэмт хэрэг” гэсэн наймдугаар хэсэгт оруулжээ.

Тэгэхээр эдгээр гэмт хэргийн төрлийн объект нь нийгмийн аюулгүй байдал болон нийгмийн дэг журам; шууд объект нь компьютерийн мэдээллийг зүй зохистой, аюулгүй ашиглахтай холбогдсон нийгмийн харилцаа байна.

Объектив тал: Гол төлөв материаллаг үр дагавартай байхаар хуульчлагдсан байна.

Өөрөөр хэлбэл, зөвхөн нийгэмд аюултай үйлдэл хийгээд зогсохгүй нийгэмд аюултай үр дагавар учирсан байх, энэ хоёр шинжийн хооронд шалтгаант холбоо байхыг заасан байна.

Тэгэхдээ эдгээр гэмт хэргийг үйлдсэн хугацааг үр дагавар нь хэдийд бий болсоноос үл хамаарч, үйлдэл төгссөн цаг хугацаагаар тооцно.

Нийгэмд аюултай ажиллагаа голчлон үйлдлийн хэлбэрээр илрэх байгаа бөгөөд зөвхөн Эрүүгийн хуулийн 227 дугаар зүйлийн зарим заалтад заасан гэмт хэрэг эс үйлдэхүйгээр хэрэгжиж болно.

Гагцхүү нэг тохиолдолд гэмт хэрэг үйлдэх аргын тухай заалт хүндрүүлэх бүрэлдэхүүний заавал байх шинжээр /226 дугаар зүйлийн 2/ заагджээ.

Эрүүгийн хуулийн 25 дугаар бүлгийн зүйлүүдийн диспозицийг шууд тодорхойлох болон иш татсан байдлаар гаргажээ.Зарим диспозицийг хэрэглэхийн тулд мэдээллийн салбарыг зохицуулж буй хууль, эрх зүйн актууд, компьютер ашиглах заавар, Улсын стандарт болон

бусад тусгай актуудын заалтыг авч үзэх шаардлагатай.Мэдээллийн аюулгүй байдлын тухай бие даасан тусгай хууль манай улсад одоо хэр гараагүй.

Субъектив тал: Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэргийн субъектив талыг хууль тогтоогч зарим тохиолдолд шууд тодорхойлон гаргаагүй боловч зүйлүүдийн утга агуулгаас үзвэл, эдгээр гэмт хэрэг зөвхөн санаатай хэлбэрээр үйлдэгдэхийг заасан байна.

Эрүүгийн хуулийн 226, 229 дүгээр зүйлд заасан гэм хорыг зөвхөн санаатай учруулах талаар шууд заасан.

Эдгээр гэмт хэргийн сэдэлт нь зүйлчлэхэд чухал ач холбогдолгүй бөгөөд ял шийтгэл оногдуулах үед л харгалзан үзнэ.Шунахай, эсвэл танхайн сэдэлттэй байж болохын зэрэгцээ өс хонзон, атаа жөтөө байж болно.

Субъект: Уг төрлийн гэмт хэргийн зарим бүрэлдэхүүн тусгай субъекттэй байж болно.

Тухайлбал, Эрүүгийн хуулийн 226 дугаар зүйлийн 2-т зааснаар өөрийн албан тушаалын хувьд компьютер, компьютерийн систем, сүлжээг ашиглах, нэвтрэн орох эрхтэй хүн тусгай субъект болно.

Эрүүгийн хуулийн 21 дүгээр зүйлийн дагуу 16 насанд хүрсэн хүн уг гэмт хэрэгт эрүүгийн хариуцлага хүлээнэ.

Эрүүгийн хуулийн 226 дугаар зүйлийн 2, 227 дугаар зүйлийн 2-т заасан үйлдлийг урьдчилан үгсэж тохиролцсон бүлэг этгээдийн үйлдсэн гэмт хэрэг гэж тооцохын тулд Эрүүгийн хуулийн 36 дугаар зүйлийн 3-ыг авч үзэх шаардлагатай.нийтийн хэрэглээний сүлжээнд нян тараах зэрэг болно.

Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэргүүд

Компьютерийн мэдээлэл, программыг өөрчлөх, эвдэх, сүйтгэх /ЭХ-ийн 226-р зүйл/

Эрүүгийн хуулийн 226 дугаар зүйлийн 1-д компьютер, компьютерийн программ, түүний төхөөрөмжийг санаатайгаар өөрчлөх, эвдэх, гэмтээх, ашиглах боломжгүй болгох, мэдээллийн сүлжээг сүйтгэх үйлдлүүдэд эрүүгийн хариуцлага хүлээлгэхээр заажээ.

Компьютерийн төхөөрөмж гэдэгт компьютерийн техник хангамж **hardware**-д хамаарах бүх техник хэрэгсэл, тэдгээрийн эд ангиудыг хамааруулан ойлгоно.

Тухайлбал, компьютерийн дэлгэц, системийн блок, гар, хэвлэх хэрэгслүүд.Түүнчлэн, тогтмол болон шуурхай санах байгууламж, дискийн /хатуу, уян/ төхөөрөмж, микропроцессор, микросхем, модем, сүлжээний суурь, эх хавтан гэх мэт эд анги хэрэгсэл хамаарна[552].

Объект: Энэ гэмт хэргийн шууд объект нь компьютерийн мэдээллийн аюулгүй байдлыг болон компьютер,компьютерийн систем,сүлжээний хэвийн ажиллагааг хангах нийгмийн харилцаанууд болон төр, байгууллага, аж ахуйн нэгж,иргэдийн мэдээлэл өмчлөх эрх,ашиг сонирхол байна.[553]

Халдлагын зүйл: нь эрүүгийн эрх зүйн үүднээс дараахи үндсэн шинжээрээ тодорхойлогдох компьютерийн мэдээлэл байна.

- зөвхөн оюуны өмч байна
- эд зүйлсийн шинжийг агуулаагүй байна
- хуулиар хамгаалагдсан байна
- машин зөөгчид /компьютер, компьютерийн систем, түүний сүлжээ/ агуулагдаж байна.

Дээрх шинжийг агуулсан мэдээллүүдэд ашиглахыг нь хязгаарласан баримт бичиг-мэдээллүүд орно.Тэдгээрийг дотор нь төрийн нууцад хамаарах мэдээллүүд, хувь хүний нууцын тухай мэдээллүүд гэж ангилна.Шинэ эрүүгийн хуулийн агуулгаас харахад компьютер, компьютерийн программ, түүний төхөөрөмжийг санаатайгаар өөрчлөх, эвдэх, гэмтээх, ашиглах боломжгүй болгох, мэдээллийн сүлжээг сүйтгэх нь мэдээлэл өмчлөгчийн эрхийг

[552]С.Жанцан “Монгол Улсын Эрүүгийн эрх зүй” УБ., 2004, 455 дахь тал
[553]Ж.Болдбаатар “Эрүүгийн эрх зүйн үндэс” УБ., 2004, 155 дахь тал

түүний дотор төр, төрийн байгууллагууд, бусад хуулийн этгээдүүд, бие хүмүүсийн эрхийг шууд зөрчиж байна.

Амьдрал дээр мэдээлэл хамгаалах дэглэмийг хуулиудаар болон мэдээллийн нөөц өмчлөгчид, төрөөс тусгайлан эрх олгосон байгууллага, албан тушаалтнууд тогтоож байна.

Компьютерийн мэдээллийг хамгаалах хэрэгслүүд ч их олон янз.Энд хамгаалалтын нийтлэг хэрэгслүүд /пропускийн дэглэм, дохиолол, цэрэгжүүлсэн хамгаалалт г.м/; ашиглагчдын боломжийг ялгаатай болгох; компьютерийн мэдээлэлд хууль бусаар нэвтрэн орохыг хүндрүүлсэн оюуны янз бүрийн хэрэгслүүд /нэг бүрийн код, системтэй харьцах адилтгалын төхөөрөмж г.м/ орно.

Объектив тал: Энэ гэмт хэргийн объектив талыг компьютерийн мэдээлэл, компьютерийн программ, мэдээллийн сүлжээг санаатайгаар өөрчлөх, эвдэх, гэмтээх, ашиглах боломжгүй болгох, сүйтгэх идэвхтэй үйлдлүүд бүрдүүлнэ. [554]

Гэхдээ эдгээр үйлдлүүдийг хийхийн тулд компьютерийн мэдээлэлд ямар нэгэн байдлаар нэвтрэн орсон байх шаардлагатай.Тиймээс энэ гэмт хэргийн объектив талын бас нэг шинж нь компьютерийн мэдээлэлд хууль бусаар нэвтрэн орсон идэвхтэй үйлдэл байх ёстой.

Зөвхөн 226 дугаар зүйлийн 2-т заасан албан тушаалын байдлаа ашиглан үйлдэх тохиолдолд компьютерийн мэдээлэлд хууль ёсоор нэвтрэн орсон байх боломжтой юм. Ингэж хууль бусаар нэвтрэн орохдоо:

- суурилуулсан хамгаалалтын системийг давах боломжийг олгодог техникийн болон аппарат-программын тусгай хэрэгслүүдийг ашиглах;
- хүчинтэй нууц үг, кодуудыг хууль бусаар ашиглах юмуу хууль ёсны ашиглагчийн дүрээр систем, сүлжээнд нэвтрэн орох бусад үйлдлүүдийг хийх замыг ашигладаг.

Компьютерийн мэдээлэлд нэвтрэн орох гэдэгт компьютерийн техник, хэрэгсэл ашиглан мэдээллийн эх сурвалжид нэвтрэн орох бүх хэлбэрийг ойлгоно.

Ингэж орсноор компьютерийн мэдээлэл, компьютерийн программ, мэдээллийн сүлжээг өөрчлөх,эвдэх,сүйтгэх үйлдлүүдийг хийж болно.

Компьютер, компьютерийн программ, түүний төхөөрөмжийг санаатайгаар өөрчлөх гэдэг нь компьютерийн холбох байгууламжийн үйл ажиллагааг алдагдуулсан, мэдээлэлд хувьсал, өөр агуулга оруулсан, тэдгээрийг өөр хооронднь хутгасан байх явдал юм.

Ашиглах боломжгүй болгосон гэж сэргээн засварлах ямар ч боломжгүйгээр гэмтээсэн байхыг,

мэдээллийн сүлжээг сүйтгэсэн гэж мэдээлэл дамжих холболтыг эвдсэн, гэмтээсэн, тасалсан, хаасан, ашиглах боломжгүйгээр бүрмөсөн үгүй хийхийг тус тус ойлгоно.

Эвдсэн гэж тэдгээрийн үйл ажиллагааг тасалдуулах, зориулалтаар нь ашиглах боломжгүй болгосныг хэлнэ.

Гэмтээсэн гэдэгт нөхөн засвар үйлчилгээ хийхээс нааш ашиглах боломжгүй, эд ангийг ажиллагаагүй болгосныг ойлгоно.

Энэ гэмт хэргийн улмаас заавал үлэмж хэмжээний хохирол учирсан байхыг шаардах бөгөөд энэ хохирол нь гэмт үйлдэлтэй шалтгаант холбоо нь байж гэмт хэрэг төгсдөг[555].

Энэ гэмт хэргийг бусад гэмт хэргээс ялгах үндсэн гол шинж нь компьютерийг ашиглаж үйлдэгддэг шинж юм.Түүнээс биш компьютер, түүний төхөөрөмж, мэдээллийн сүлжээнд гаднаас халдах нь компьютерийн гэмт хэрэг биш.

Компьютерийг юмуу мэдээлэл тээгчийг /хатуу болон уян диск,CD/ өөрийн эзэмшилд хууль бусаар авах нь компьютерийн мэдээлэлд нэвтрэн орж байна гэж тооцогдохгүй харин өмчийн эсрэг юмуу дураар авирлах үйлдлүүд болно.

[554]Г.Совд “Монгол Улсын Эрүүгийн хуулийн тайлбар” УБ., 2002, 320 дахь тал
[555]С.Жанцан “Монгол Улсын Эрүүгийн эрх зүй” УБ., 2004, 455 дахь тал

Тэгэхээр Эрүүгийн хуулийн 226 дугаар зүйл буюу компьютерийн мэдээлэл, программыг өөрчлөх, эвдэх, сүйтгэх гэсэн томъёолол жинхэнэ компьютерийн гэмт хэргийн тодорхойлолт мөн.

Харин 226 дугаар зүйлийн 1-д заасан компьютер, түүний төхөөрөмжийг санаатайгаар өөрчилсөн, эвдсэн, гэмтээсэн, ашиглах боломжгүй болгосон мэдээллийн сүлжээг сүйтгэсэн хэмээх диспозици нь компьютерийн гэмт хэрэг бус харин эд хөрөнгийг устгасан, гэмтээсэн, эвдсэн, сүйтгэсэн, ашиглах боломжгүй болгосон Эрүүгийн хуулийн 153 дугаар зүйлийн диспозици мэт харагдаж байна.Тийм ч учраас 226 дугаар зүйлийн заалтыг компьютерийн мэдээлэл, программыг компьютер ашиглан өөрчлөх, эвдэх, сүйтгэх гэсэн утгаар ойлгох нь зүйтэй.

Түүнээс гадна компьютер ашиглан компьютер, түүний систем, сүлжээний ажиллагааг алдагдуулах нь энэ хэргийн объектив талын нэг шинж болох ёстой.

Үүнээс үзвэл компьютер юмуу мэдээлэл зөөгчид агуулагдаж байгаа мэдээллийг дулаан, соронзон долгио, механик үйлчлэлээр гаднаас үйлчлэх замаар устгах, өөрчлөх, гэмтээх нь энэ гэмт хэргийн бүрэлдэхүүн болохгүй.

1. Компьютерийн мэдээлэл, программыг өөрчлөх гэдэг нь мэдээлэл тээгч дээр байгаа программ, өгөгдлийн сан, бичвэр болон бусад бүх мэдээлэлд өмчлөгч, эзэмшигчийн зөвшөөрөлгүйгээр өөрчлөлт оруулахыг хэлнэ.

Харин эдгээр мэдээллийг хууль ёсоор эзэмшиж байгаа этгээдүүдийн ил тод хийж буй дараахи өөрчлөлтүүдийг үүнд хамруулан үзэхгүй.

а/ илт алдааг засаж буй өөрчлөлт;

б/хэрэглэгчийн техникийн хэрэгсэл дээр хэвийн ашиглахын тулд программ, өгөгдлийн санд оруулж буй өөрчлөлтүүд ;

в/ бусад программуудтай харилцан ажиллах чадварыг бий болгохын тулд программын объектийн кодыг хэсэгчлэн хувиргах /**декомпиляци**/ өөрчлөлт;

2. Компьютерийн мэдээлэл, программыг эвдэх, сүйтгэх гэдэг нь нэг утгатай бөгөөд ямар нэг тээгчид байгаа мэдээллийг арилгах, буцаан сэргээх боломжгүй болгохыг өөрөөр хэлбэл устгахыг хэлнэ. Учир нь компьютерийн мэдээллийг эвдэх гэсэн утга байхгүй. Зөвхөн устгаж, сүйтгэж болно.

Гэхдээ компьютерийн мэдээллийг арилгах, устгах гэдгийг ойлгоход нилээд түвэгтэй.Жишээлбэл хэн нэгэн MS-DOS үйлдлийн системийн DELETE гэсэн командыг ашиглаад файлыг арилгалаа гэж бодъё.Тэглээ гээд мэдээлэл бодитойгоор алга болж устаагүй байна.Зөвхөн файлын нэрийн эхний үсэг солигдож жирийн аргаар түүнтэй ажиллах боломжгүй болж,уламжлалт командуудыг ашиглах үед хүрэх аргагүй болдог.Тэр ч байтугай компьютер өөрөө хатуу дискийн тэр хэсгийг чөлөөтэй байна гэж үздэг бөгөөд тэнд шинэ мэдээллийг бичиж болно.Гэхдээ л файлыг техникийн утгаар нь устгаагүй ч “DELETE” командыг ашиглан арилгах нь хэрэглэгчийн хэрэглэх боломж, хадгалагдах байдалд ихээхэн аюулд учруулж байна гэсэн үг.

Үүнээс үзвэл устгагдсан мэдээллийг аппарат-программын хэрэгслийн тусламжтайгаар сэргээх юмуу өөр хэрэглэгчээс олж авах хэрэглэгчийн боломж нь гэм буруутай этгээдийг хариуцлагаас чөлөөлөх үндэслэл болдоггүй.

Файлыг өөр нэрээр нэрлэх,түүнчлэн хуучин файлууд шинэ файлуудад автоматаар шахагдах нь мэдээллийг сүйтгэж байгаа явдал биш.

Компьютерийн мэдээллийг устгах сүйтгэх гэсэн нэр томъёонд мэдээллийг хяхан хаахыг мөн оруулан ойлгож болно.Энэ нь хууль ёсны ашиглагчийн компьютерийн мэдээлэлд хүрэхийг зориудаар хүндрүүлэх, компьютерийн систем болон түүний мэдээллийн нөөцөд орохыг хязгаарлан хааж буй үйлдлүүдийг хэлдэг.

Компьютерийн программыг эвдэн сүйтгэх буюу жагсаалаас гаргах нь компьютерийн мэдээллийг устгахаас ялгагдана.Компьютерийн программыг эвдэн сүйтгэснээр программ

файл маягаар зохион байгуулагдсан мэдээлэл болон хувирах ба хэрэглэгчийн ажиллах объект байх чанараа алддаг.

Энэ нь Эрүүгийн хуулийн өөр зүйл ангид заасан гэмт хэрэг болно.Харин компьютерийн мэдээллийг арилган устгасны улмаас компьютерийн программ эвдрэн сүйдсэн бол энэ зүйлээр зүйлчилнэ.

3.Компьютер, түүний систем, сүлжээний ажиллагаа алдагдана гэдэг нь аль нэг программ болон өгөгдлийн сангийн ажиллагаа алдагдах, хувиргасан мэдээллийг өгөх, аппаратын хэрэгсэл болон хэвлэх төхөөрөмжүүд буруу ажиллах, сүлжээний хэвийн ажиллагаа алдагдах, мэдээллийн автомат систем тогтоогдсон горимоороо ажиллахаа болих,компьютерийн мэдээлэл боловсруулалт алдагдахыг хэлдэг. Энэ нь компьютерийн мэдээллийг жинхэнэ утгаар нь устгасан,

- программ хангамж жагсаалаас гарсан,
- тухайн программ хангамжийг суурилуулсан аппаратын хангамжийн бүрэн бүтэн байдал алдагдсан,
- холбооны систем гэмтсэний улмаас үүсдэг. Эдгээр үр дагаврыг компьютер ашиглан бий болгосон бол энэ зүйл ангиар зүйлчлэх үндэслэл гарч ирнэ.

Эрүүгийн хуулийн 226 дугаар зүйлд заасан гэмт хэрэг дээрх үйлдлүүдийн улмаас үлэмж хэмжээний хохирол учирснаар дуусгавар болно.

Гэхдээ компьютерийн мэдээлэлд нэвтрэн орохын тулд түүний хамгаалалтын хэрэгслүүдийг ажиллагаагүй болгох үйлдэл ихэнх тохиолдолд хийгддэг учраас энэ үйлдлийг хийсэн боловч компьютерийн мэдээллийг устгаж арилгаагүй, программыг эвдэн сүйтгээгүй, компьютер, түүний систем, сүлжээний ажиллагааг алдагдуулаагүй, үлэмж хэмжээний хохирол учраагүй байсан ч энэ гэмт хэрэгт завдсан гэж үзэх үндэслэлтэй.

Компьютер, түүний систем, сүлжээ, компьютерийн мэдээлэл, программыг компьютер ашиглан өөрчлөх, эвдэх, сүйтгэх үйлдэл болон учирсан үлэмж хэмжээний хохирлын хоорондох шалтгаант холбоог тогтоох үедээ техникийн эвдрэл, аппарат-программын хэрэгслүүдийн ажиллагааны алдааны улмаас компьютерийн ажиллагаа алдагдсан, мэдээлэл устсан, өөрчлөгдсөний улмаас үлэмж хэмжээний хохирол учирсан байж болохыг сайн анхаарах учиртай.

Мэдээллийн аюулгүй байдал, мэдээллийн үнэ цэнэ гэдэг талаас нь үзэх юм бол компьютер, түүний систем, сүлжээ, компьютерийн мэдээлэл, программыг компьютер ашиглан өөрчлөх, эвдэх, сүйтгэх үйлдэл үйлдэгдэж үлэмж хэмжээний хохирол учрах гэдэг нь маш буруу томъёолол юм.

Зүй нь “компьютер, компьютерийн систем болон сүлжээнд хууль бусаар нэвтрэн орсны улмаас мэдээлэл устсан, хаагдсан, өөрчлөгдсөн эсхүл компьютер, компьютерийн систем, түүний сүлжээний ажиллагааг алдагдуулсан бол” хэмээн тодорхойлох шаардлагатай.

Учир нь иргэд, байгууллага, төрийн мэдээлэл өмчлөх, эзэмших эрхийг зөрчсөн байх нь ямар нэг материаллаг хор уршиг учирсан байхыг шаардахгүйгээр хор уршиг учруулж байгаа тул гэмт хэргийн бүрэлдэхүүн болж байх ёстой.

Үүнийг НҮБ-ын “гэмт явдлаас урьдчилан сэргийлэх болон эрх зүй зөрчигчидтэй харьцах тухай” 10 дугаар конгрессоос гаргасан “компьютерийн сүлжээг ашиглахтай холбогдсон гэмт хэргүүд” гэсэн лавлах баримтад зааж өгсөн байдаг.

Түүнчлэн гэмт явдлын асуудлаарх Европын хороо болон кибер орон зайн гэмт явдлын шинжээчдийн хорооноос бэлтгэж 2001.11.22-нд батлагдсан ”Кибер гэмт явдлын тухай конвенц”-д ч тодорхой материаллаг хохирол учирсан эсэхээс үл хамааран гэмт хэрэг гэж тооцож байхаар заасан байна.

Компьютерийн мэдээллийг хууль бусаар олж авах /ЭХ-ийн 227-р зүйл/

Монгол Улсын Эрүүгийн хуулийн 227 дугаар зүйлд компьютер, компьютерийн систем, сүлжээ буюу машин тээгчид хадгалагдаж буй мэдээллийг хууль бусаар олж авах, аль эсвэл

өөр аргаар мэдээллийг олж авах буюу авах оролдлого хийх тохиолдолд хүлээлгэх хариуцлагыг тусгажээ.

Компьютер, мэдээллийн сүлжээнд хадгалагдаж байгаа мэдээлэл гэж тэдгээрийн санд агуулагдаж байгаа, сүлжээгээр дамжуулагдах, цацагдах үйлдэлд ороогүй мэдээллийг хэлнэ[556].

Дээрхи үйлдлүүдийг компьютерийн мэдээллийн системд нэвтрэхгүйгээр үйлдэх боломжгүй.Энэхүү зүйлээр мэдээллийн халдашгүй байдлын эрх хамгаалагдсан болно.

2 заалт бүхий уг зүйлд гэмт хэргийн бүрэлдэхүүний объект, объектив болон субъектив талын заавал байх шинжүүд тодорхой тусгагдсан.Энэ гэмт хэргийн сэдэлт, зорилго ямар ч байж болно.Тухайлбал, шунахай, өс хонзон, атаархал, мэдээлэл олж авах, хохирол учруулах гэсэн зорилго, өөрийн мэргэжлийн ур чадварыг шалгах гэх мэт.

Объект: энэ гэмт хэргийн объект нь компьютерийн мэдээллийн аюулгүй байдалтай холбогдсон нийгмийн харилцаа бөгөөд халдлагын зүйл нь компьютерийн мэдээлэл байна[557].

Объектив тал: Уг гэмт хэргийн объектив тал дараахи байдлаар компьютерийн системд нэвтэрсэн үйлдлээр тодорхойлогдоно:

- хамгаалалтын системийг эвдэхийн тулд техникийн болон программын тусгай хэрэгсэл ашиглах,
- компьютерт нэвтрэхийн тулд пароль, код хууль бусаар ашиглах, хууль ёсны хэрэглэгчийн нэрээр систем, сүлжээнд нэвтрэх зорилгоор бусад үйлдэл хийж, улмаар мэдээллийг олж авах буюу хуулбарлах, эсвэл бусад аргаар мэдээллийг барьж авах, эсвэл тийнхүү оролцох.

Хууль бус бусад аргаар компьютер дэх мэдээллийг олж авах гэдэг нь компьютерийн систем, сүлжээний дотроос нь буюу гаднаас нь биечлэн болон техник хэрэгслийн тусламжтайгаар мэдээллийг санаатай олж авахыг ойлгоно.

Субъект шууд буюу идэвхитэй аргаар /микрофон, радио хүлээн авагч, модем, хэвлэх төхөөрөмж ашиглан, компьютерийн болон кабель утас цахилгаан соронзон долгионы цацралтаас дуу авиагаар, дүрсээр, ноорог цаас, хальснаас олж авч болдог/ хуулбарласан гэж мэдээллийг эзэмшигчид мэдэгдэхгүйгээр нууц далд аргаар, дур мэдэн мэдээллийн агуулгыг хальс /диск/-нд буулгах, оруулах, гараар болон хэвлэх төхөөрөмж ашиглан хуулж авах, зургийг авах хэлбэртэй байж болно[558].

Энэ гэмт хэрэг хэрхэн үйлдэгдэж болох саяхны жишээг энд сийрүүлье.

Ц.Баасандорж гэгч “Поверсофт системс” ХХК-д ажиллаж байгаад ажлаас гарахдаа уг компаний 4 жилийн турш боловсруулсан “Поверсофт санхүү” программыг хуулбарлан авч, улмаар өөрийн “Динамик системс” компаний нэрээр хувилж борлуулан нийт 45 сая 400 мянган төгрөгийн ашиг олсон болох нь тогтоогджээ[559].

227 дугаар зүйлийн 2 дахь заалтад их хэмжээний хохирлыг хүндрүүлэх бүрэлдэхүүний нэг шинжээр оруулсан болно.

Субъектив тал: Уг гэмт хэргийн субъектив тал нь гэм буруугийн шууд санаатай хэлбэрээр тодорхойлогдоно[560].

Өөрөөр хэлбэл, гэм буруутай этгээд компьютерийн мэдээллийг хууль бусаар олж авах үйлдэл хийж байгаагаа ухамсарлан ойлгож, тийм үйлдэл хийхийг хүссэн байдаг.

227 дугаар зүйлийн 2 дахь заалтад шунахай сэдэлтийг хүндрүүлэх бүрэлдэхүүний шинжээр заасан болно.

Субъект: Уг гэмт хэргийн субъект нь 16 насанд хүрсэн, хэрэг хариуцах чадвартай, бие хүн байна. Гэхдээ ийм гэмт хэргийг компьютерийн техниктэй харьцах туршлагатай, тиймээс ч компьютерийн мэдээллийг хууль бусаар олж авсаны улмаас үүсч болох үр дагаврын талаар

[556]Г.Совд “Монгол Улсын Эрүүгийн хуулийн тайлбар” УБ, 2002, 320 дахь тал
[557]С.Жанцан “Монгол Улсын Эрүүгийн эрх зүй” УБ, 2004, 455 дахь тал
[558]С.Жанцан “Монгол Улсын Эрүүгийн эрх зүй” УБ, 2004, 456 дахь тал
[559]Эрүүгийн 20446114 тоот хэргийн баримт.
[560] Ж.Болдбаатар “Эрүүгийн эрх зүйн үндэс” УБ., 2004, 156 дахь тал

тодорхой мэдлэг бүхий хүмүүс үйлддэгийг анхаарвал зохино.Эрдэмтэн судлаачдын бүтээлд[561] энэ гэмт хэргийн субъектын ангиллын талаар тусгасан байдаг.

Тухайлбал:

Компьютерийн мэдээлэлд хууль бусаар нэвтэрсэн этгээд;

- Урьдчилан үгсэн тохиролцож компьютерийн мэдээлэлд хууль бусаар нэвтэрсэн хүмүүс;
- Албан тушаалын байдлаа ашиглан компьютерийн мэдээлэлд хууль бусаар нэвтэрсэн этгээд;
- Электрон тооцоолон бодох машин түүний систем, сүлжээтэй харьцдаг хүмүүс.

Дээрхээс гадна сэтгэцийн шинэ өвчин болох мэдээллийн өвчтэй хүмүүс уг гэмт хэргийн субъект байж болох магадлалтай[562].

Урьдчилан үгсэж тохиролцсон бүлэг этгээд энэ гэмт хэргийг үйлдсэн бол хүндрүүлж үзнэ.Гэмт хэрэг үйлдэх талаар урьдаас тохиролцсон этгээдүүдийн оролцоотойгоор үйлдсэн гэмт хэргийг урьдаас үгссэн бүлэг этгээдийн үйлдсэн гэмт хэрэг гэнэ[563].

Тийнхүү үгсэн тохиролцох үйлдэл нь гагцхүү гэмт хэрэг үйлдэгдэж эхлэхээс өмнө л байж болно.Тухайн тохиолдолд компьютерийн мэдээллийг хууль бусаар олж авах талаар хамтран гүйцэтгэгчид тохиролцсон байх ёстой.

Харин зохион байгуулагч, захиалагч, хамжигч, хатгагч зэргээр “ажил үүрэг” хуваарилагдсан бол урьдчилан тохиролцсон бүлэг гэж үзэхгүй, Эрүүгийн хуулийн 33 дугаар зүйлийг журамлан зүйлчилнэ.

227 дугаар зүйлийн 1 дүгээр заалт сонгох санкцитай: торгох, баривчлах болон хорих. Торгох ялын хэмжээ нь хөдөлмөрийн хөлсний доод хэмжээг 51-200 дахин нэмэгдүүлсэнтэй тэнцэх үндэсний валют байна.Баривчлах ялын хугацаа 3-6 сар.Хорих ял – 2 жил хүртэл хугацаагаар байна.

Харин 2 дахь заалтын санкци нь чангарч, хөдөлмөрийн хөлсний доод хэмжээг 100-250 дахин нэмэгдүүлсэнтэй тэнцэх төгрөгөөр торгох, 3-5 жил хорих ял болсон байна.

Тухайн гэмт хэргийг зохиогчийн эрхийг зөрчих /Эрүүгийн хуулийн 140 дүгээр зүйл/, иргэний захидал харилцааны нууцын халдашгүй байдлыг зөрчих /Эрүүгийн хуулийн 135 дугаар зүйл/, хувь хүний нууцыг задруулах /Эрүүгийн хуулийн 136 дугаар зүйл/, бусдын эд хөрөнгийг санаатайгаар устгах гэмтээх /Эрүүгийн хуулийн 153 дугаар зүйл/, эх орноосоо урвах /Эрүүгийн хуулийн 79 дүгээр зүйл/, тагнуул хийх /Эрүүгийн хуулийн 80 дугаар зүйл/, төрийн нууц задруулах /Эрүүгийн хуулийн 87 дугаар зүйл/ - зэрэг ижил төсөөтэй хэргээс ялгаж зүйлчлэхэд тухайн гэмт хэргийн төрлийн объектыг харгалзана.

Компьютерийн мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай хэрэгсэл бэлтгэх, борлуулах /ЭХ-ийн 228-р зүйл/

Уг гэмт хэргийн нийгмийн хор аюул нь компьютерийн мэдээллийн эсрэг бусад гэмт хэрэг үйлдэх нөхцөлийг бүрэлдүүлдэгт оршино.

Монгол Улсын Эрүүгийн хуулийн 228 дугаар зүйлд компьютерийн хамгаалагдсан систем буюу сүлжээнд хууль бусаар нэвтрэн ороход зориулагдсан программын болон техникийн тусгай хэрэгслийг борлуулах зорилгоор бэлтгэх юмуу борлуулах үйлдэл хийгдсэн тохиолдолд хүлээлгэх хариуцлагыг тусгасан билээ.Уг хэм хэмжээгээр хүмүүсийн мэдээллийн халдашгүй байдлын эрх хамгаалагдсан болно.

Компьютер, мэдээллийн хамгаалалттай сүлжээ гэж мэдээлэл хамгаалах тусгай техник, хэрэгсэл, программ хангамжаар хангагдсан /хамгаалагдсан/ компьютер, мэдээллийн сүлжээг хэлнэ[564]

[561] В.А.Мазуров “Компьютерные преступления” М, 2002., стр. 119
[562] В.А.Мазуров “Компьютерные преступления” М, 2002., стр.127
[563]Ж.Болдбаатар “Эрүүгийн эрх зүйн үндэс” УБ, 2004., 65 дахь тал

[564]С.Жанцан “Монгол Улсын Эрүүгийн эрх зүй” УБ., 2004, 457 дахь тал

Энэ гэмт хэргийн нэг жишээг энд дурдъя. Д.Баярсайхан гэгч этгээд “Хөдөлмөр хамгаалал, хөдөлгөөн” Төрийн бус байгууллагын компьютерийн нууц үг /код/-ийг ашиглан сүлжээнд нь зөвшөөрөлгүйгээр нэвтрэн орж, 546580 төгрөгийн хохирол учруулжээ[565]

Мэдээллийн системийн эзэмшигч нь тооцоолон бодох системийг өмчлөгч буюу уг системийг хууль ёсны эрхийн дагуу ашиглаж буй аливаа этгээд байна.

Уг зүйлд гэмт хэргийн бүрэлдэхүүний объект, объектив болон субъектив талын олон шинжүүд тусгагджээ.

Энэ гэмт хэргийн сэдэлт, зорилго янз бүр байж болно.

Жишээлбэл, шунахай, өс хонзон, атаархал, мэдээлэл олж авах буюу хохирол учруулах зорилго, мэргэжлийн ур чадвараа шалгах гэх мэт.

Хууль тогтоогч сэдэлт, зорилгыг уг гэмт хэргийн заавал байх шинжээр заагаагүй нь Эрүүгийн хуулийн 228 дугаар зүйлийг компьютерийн элдэв халдлагын үед хэрэглэх боломжийг бүрдүүлсэн гэж үзэж болох талтай.

Объект: Энэхүү гэмт хэргийн объект бол компьютерийн систем, мэдээллийн аюулгүй байдалтай холбогдсон нийгмийн харилцаа бөгөөд халдлагын зүйл нь компьютерийн мэдээлэл юм.

Уг зүйлд заагдсан үйлдэл хийгдсэнээр гэмт хэрэг төгсөнө.Өөрөөр хэлбэл, компьютерийн хамгаалагдсан систем буюу сүлжээнд хууль бусаар нэвтрэн ороход зориулагдсан программын буюу аппаратын тусгай хэрэгслийг борлуулах зорилгоор бэлтгэсэн, аль эсвэл борлуулсан үйлдэл хийгдсэнээр гэмт хэрэг төгсөнө.

Объектив тал: нь компьютер, мэдээллийн хамгаалалттай сүлжээнд хууль бусаар нэвтрэх тусгай программ болон техник хэрэгслийг бэлтгэх буюу борлуулах үйлдлээр тодорхойлогдоно[566].

Энэ нь хэлбэрийн бүрэлдэхүүнтэй гэмт хэрэг.

Субъектив тал: нь гэм буруугийн шууд санаатай хэлбэрээр илэрнэ. Өөрөөр хэлбэл, гэм буруутай этгээд компьютерийн мэдээллийн системд хууль бусаар нэвтрэхэд зориулагдсан тусгай хэрэгсэл бэлтгэж буюу борлуулж байгаагаа ухамсарлан ойлгож, ингэхийг хүсч байдаг болно.

Субъект: нь 16 насанд хүрсэн, хэрэг хариуцах чадвартай, бие хүн байна. Уг гэмт хэргийг гол төлөв компьютерийн техниктэй ажиллах зохих туршлагатай, тиймээс ч компьютерийн мэдээллийн сүлжээнд нэвтрэхэд зориулагдсан тусгай хэрэгсэл бэлтгэсэн буюу борлуулсаны улмаас үүсэх хор уршгийг мэдэх чадвартай хүмүүс үйлддэг онцлогтой.

Энэхүү зүйл нь торгох, баривчлах, хорих – гэсэн сонгох санкцитай.Торгох ялын хэмжээ нь хөдөлмөрийн хөлсний доод хэмжээг 51-150 дахин нэмэгдүүлсэнтэй тэнцэх төгрөг, баривчлах ялын хугацаа 3-6 сар, хорих ял – 5 жил хүртэл.

Нянтай программ зохион бүтээх, ашиглах, тараах /ЭХ-ийн 229-р зүйл/

Нянтай программ зохион бүтээх, ашиглах, тараах гэмт хэргийн улмаас компьютерийн систем гэнэт жагсаалаас гарч таагүй үр дагавар бий болгодогт уг гэмт хэргийн нийгмийн хор аюул оршино.

Программ гэдэг нь тооцоолон бодох машин болон компьютерийн бусад төхөөрөмжийг ашиглан тодорхой үр дүнд хүрэхэд зориулагдсан янз бүрийн мэдээлэл болон командын нийлбэр цогц юм.

Харин **компьютерийн нян гэдэг** бол хэд хэдэн хувь үржин, холбогдсон программыг өөрчлөн, хэвийн үйл ажиллагааг нь алдагдуулах чадвартай программ юм.

[565]Эрүүгийн 330305 тоот хэргийн баримт.

[566]С.Жанцан “Монгол Улсын Эрүүгийн эрх зүй” /схемчилсэн тайлбар, зүйлчлэлийн асуудал/ УБ., 2004, 457 дахь тал

Үүнээс гадна, эдгээр программ нь өөрсдөө бусад программд нэвтрэн орж, тааламжгүй үр дагавар бий болгодог /файл, катологийг гэмтээх, мэдээллийг өөрчлөх, устгах гэх мэт/. Энэ нь компьютерийн гэмт хэрэг үйлдэх нэлээд дэлгэрсэн арга юм.

Одоогоор дэлхийд 100 000 гаруй компьютерийн нян байна гэж үздэг. Хэдий тийм боловч тэдгээрийг дараахи бүлэгт хуваан үзэж болно:

- **Ачааллын нян:** нян тээгчээс мэдээлэл авах үед халдварлалт явагддаг.
- **Файлын нян** EXE, COM, SYS, BAT зэрэг файлыг халдварлуулна. Нян бүхий программыг ашигласнаар эдгээр нян идэвхижинэ.

Тэдгээр нян программаас программ дамжин тархах нь халдварт өвчинтэй төсөөтэй.Эхний үед нянг илрүүлэх боломж туйлын хомс.Учир нь тэрээр энэ үед бүх программыг халдваржуулдаггүй.Цаашлаад ирэхээр компьютерийн үйл ажиллагаа ямар нэгэн хэмжээгээр алдагдана.Сонирхогч программчдын хийсэн нян устгах чадвар багатай байхад мэргэжлийн жинхэнэ программчдын зохион бүтээсэн нь нэн аюултай.

Компьютерийн нян судлал /вирусологи/ гэдэг шинжлэх ухааны бие даасан салбар үүсч хөгжиж байна.

Компьютерийн нянгийн зарим төрлийг[567]энд авч үзье.

- “өт”. Эдгээр нян программын файлыг өөрчилдөггүй бөгөөд компьютерийн санамжид нэвтрэн орж, бусад компьютерүүдийн хаягийг тогтоон, тэдэнд нянгийн хувиудыг илгээнэ.
- “паразит”. Программын файлыг зайлшгүй өөрчилдөг нян.
- “аюултай нян”. Ийм нянг гол төлөв сонирхогчид бий болгодог. Алдаа мадаг ихтэй байдаг тул ийм нянг тусгай программаар илрүүлэхэд хялбар.
- “үл үзэгдэгч”. Тэдгээр нь нэлээд боловсронгуй бөгөөд нянгийн эсрэг программаар илэрдэггүй. Учир нь халдварлагдсан файлыг нээхэд уг нянгууд нэн даруй холдон, хаахад дахин халдваржуулж эхэлдэг байна.
- “хий үзэгдэл”. Уг нянгуудыг илрүүлэх туйлын төвөгтэй. Ийм нянгууд нь программыг халдваржуулах явцдаа кодоо байнга сольж байдаг онцлогтой. Тиймээс дараа дараагийн халдварлагдсан программуудад аливаа шинж байдлыг тогтоож болдоггүй учраас нянгийн эсрэг программ үр дүнгээ өгдөггүй байна.
- “Логик бөмбөг” гэж программын кодыг санаатай өөрчлөх замаар урьдаас тооцоолсон ямар нэгэн нөхцөл бүрэлдэхэд, жишээлбэл, тодорхой хугацаа болоход тооцоолон бодох машины программ буюу системийн заримыг юмуу бүхлээр нь жагсаалаас гаргахыг хэлнэ.

“Логик бөмбөг” бол анхнаасаа программын нэгэн хэсэг бөгөөд өөр программд шилждэггүй онцлогтой.Харин нян бол хөдөлгөөнт программ бөгөөд компьютерийн сүлжээгээр ч дамжих чадвартай.

Объект: Монгол Улсын Эрүүгийн хуулийн 229 дүгээр зүйлд заасан гэмт хэргийн шууд объект нь тооцоолон бодох машин /компьютер/, түүний программ хангалт болон мэдээллийн агуулгыг аюулгүй ашиглахад чиглэгдсэн нийгмийн харилцаа мөн.

Объектив тал: 229.1-д тусгагдсан гэмт хэрэг нь хэлбэрийн бүрэлдэхүүнтэй бөгөөд дараахи үйлдлээр илэрнэ:

- мэдээллийг зөвшөөрөлгүйгээр устгах, түгжих, өөрчлөх буюу хуулбарлах, түүнчлэн, аппаратын хэсгийн ажиллагааг алдагдуулахад илтэд зориулагдсан тооцоолон бодох машины программ зохион бүтээх;
- ийм шинж чанар бүхий өөрчлөлтийг холбогдох программд оруулах, тийм программыг ашиглах;
- тэдгээрийг тараах;
- тийм программ бүхий тээгчийг ашиглах;
- тийм тээгчийг тараах.

[567]Ц.Эрдэнэ “Терроризм, түүнтэй тэмцэх асуудал” илтгэлийн эмхтгэл, УБ., 2003, 56 дахь тал

Программыг зохион бүтээх, өөрчлөх гэж тооцоолон бодох машины хэл болох машинт алгоритмыг бэлтгэх, хувиргахыг хэлнэ.

Программыг ашиглах, тараахгэдэгт түүнийг хэрэглэх, зохион бүтээгчийн ажлын байрнаас хальж хэрэглэхийг ойлгоно.

Нянг зохион бүтээсэн, ашигласан, тарааснаар гэмт хэрэг төгсөнө[568].

Эрүүгийн хуулийн 229 дүгээр зүйлийн 1 дэх заалтад тусгагдсан гэмт хэргийн объектив талын заавал байх шинж нь гэмт хэрэг үйлдэх арга, хэрэгсэл болно.

Энэ нь нэгдүгээрт, үр дагавар нь зөвшөөрөгдөөгүй байвал зохино, хоёрдугаарт, нянтай программ өөрөө байх явдал юм.

Хүндрүүлэх бүрэлдэхүүн: /ЭХ-ийн 229.2/

Эрүүгийн хуулийн 229 дүгээр зүйлийн 2 дугаар заалтад уг гэмт хэргийн хүндрүүлэх бүрэлдэхүүнийг тусгажээ.

Энэ нь материаллаг бүрэлдэхүүнтэй, гэм буруугийн давхардсан хэлбэртэй гэмт хэрэг юм.Үйлдлийн хувьд санаатай, нийгэмд аюултай үр дагаврын хувьд болгоомжгүй.

Нийгмийн аюултай үр дагаврыг санаатай учруулсан тохиолдолд Эрүүгийн хуулийн 229 дүгээр зүйлийн 1 болон холбогдох бусад зүйлээр давхар зүйлчлэн, гэм буруутай этгээдэд нийлмэл гэмт хэрэг үйлдсэнд нь эрүүгийн хариуцлага хүлээлгэнэ.

Эрүүгийн хуулийн 229 дүгээр зүйлийн 2 дахь заалтад заасан гэмт хэргийг үйлдэхдээ гэм буруутай этгээд нянтай программ зохион бүтээж, ашиглаж, тарааж байгаагаа ухамсарлан ойлгож байдаг бөгөөд хүнд хор уршиг учрахыг урьдаас мэдэж байгаа хэрнээ түүнийг зайлуулж чадна хэмээн хангалттай үндэслэлгүйгээр тооцоолдог /хөнгөмсөгөөр найдах/, эсвэл хүнд хор уршиг учирч болохыг урьдаас мэдээгүй боловч зохих анхаарал, болгоомжтой байсан бол мэдэх ёстой байдаг /хайхрамжгүй хандах/.

“Хүнд хор уршиг”-ийг тухайн тохиолдол бүрт үнэлж тогтооно.Хүний амь нас хохирох, хүний бие махбодод хүнд гэмтэл учрах, сүйрэл үүсэх, их хэмжээний материаллаг хохирол зэргийг хүнд хор уршигт тооцно[569].

Гэмт хэргийг субъектив тал нь шууд санаагаар хэрэгжинэ.Гэм буруутай этгээд нянтай программ бүтээж байгаагаа ухамсарлан ойлгож байдаг бөгөөд түүнийг бусад хэрэглэгчид ашиглахад үүсэх үр дагаврыг урьдаас мэдэж, хүсч байдаг болно.Сэдэлт, зорилго зүйлчлэлд нөлөөлөхгүй.

Гэмт хэргийн субъект нь 16 насанд хүрсэн, хэрэг хариуцах чадвартай, бие хүн байна.Монгол Улсын хууль тогтоомжийн дагуу эрүүгийн хариуцлага хүлээх насанд хүрээгүй хүнд захиргааны журмаар хүмүүжлийн чанартай албадлагын арга хэмжээ авч болно.

Эрүүгийн хуулийн 229 дүгээр зүйлийн 1 дэх заалтын санкци нь:

- хөдөлмөрийн хөлсний доод хэмжээг 5-50 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээний төгрөгөөр торгох,
- 100-200 цаг албадан ажил хийлгэх,
- 1-3 сар баривчлах.

Эрүүгийн хуулийн 229 дүгээр зүйлийн 2 дахь заалтын санкци нь:

- хөдөлмөрийн хөлсний доод хэмжээг 51-250 дахин нэмэгдүүлсэнтэй тэнцэх төгрөгөөр торгох,
- 3-6 сар баривчлах,
- 5 жил хүртэл хорих ялаар шийтгэх эрүүгийн эрх зүйн зохицуулалт үйлчилж байна.

Өнөөдөр манай оронд төдийгүй олон улсын хэмжээнд уламжлалт аргаар үйлдэгддэг байсан гэмт халдлага, гэмт хэрэг, зөрчлийн нөхцөл байдал, онцлог шинж, хохирол, орон зай цаг хугацаа, хамаарах хүрээ, үйлдэгчийн бүтэц, сэдэл, зорилго эрс өөрчлөгдөж бараг бүх

[568]Ж.Болдбаатар “Эрүүгийн эрх зүйн үндэс” УБ., 2004, 157 дахь тал
[569]С.Нарангэрэл “Монгол Улсын Эрүүгийн эрх зүй”, УБ., 1999, 143 дахь тал

төрлийн гэмт хэрэг кибер орчинд үйлдэгдэх хандлага ажиглагдаж байгаа нь иргэд, байгууллагын төдийгүй хууль сахиулах байгууллагын анхаарах асуудлын нэг болсон.

Зөвхөн кибер орон зайд ажилладаг хүмүүс, техник хэрэгсэл, хэрэглээний бүтэц төдийгүй олон нийтийн ашигладаг орон зай болох ОНМХ-ийн тоо нэмэгдэж улмаар мэдээллийн цоо шинэ хэрэгслэлүүд болох олон нийтийн сүлжээ, онлайн сэтгүүл зүй, кабелийн телевиз, хэт богино долгионы радио, гар утсаар мэдээлэл дамжуулах, хүлээж авах /мобайл сэтгүүл зүй/ боломж бүрдэхийн зэрэгцээ интернет сэтгүүл зүй, иргэний сэтгүүл зүй, ОНМХ-ийн зар сурталчилгаа, эдийн засгийн сэтгүүл зүй, экологийн сэтгүүл зүй, аналитик сэтгүүл зүй зэрэг мэдээллийн сэтгүүл зүйн цөөнгүй шинэ чиглэлүүд бодит зүйл болж нэвтэрсэн.

Энэ бодит нөхцөл байдал бол кибер орчины мэдээллийг аливаа хүмүүс дэлхийн аль ч өнцгөөс хүлээж авах, бас дамжуулах, өөрийн үзэл бодол, байр сууриа интернетээр илэрхийлэх өргөн боломжийг бүрдүүлсэн.

Товчоор хэлбэл кибер орчин дахь мэдээлэлд орон зай, цаг хугацааны хязгаар, хаалт гэх уламжлалт саад бэрхшээл үгүй болсон.

Монгол Улсын хуулиудад цахим ертөнцийн эрх зүйн зохицуулалт ямар нэг хэмжээгээр байгаа боловч нэгдмэл цогц бодлого, хууль эрх зүйн зохицуулалт, эдийн засгийн хангалттай нөөц бололцоо үгүйлэгдэж байгааг дурдая.

Мэдээллийн технологи хөгжиж буй өнөө цагт мэдээллийн аюулгүй байдлын талаар төрөөс баримтлах нэгдмэл бодлого, ерөнхий хууль, салбарын хуулийнхэрэгцээ шаардлага, ач холбогдолтой дутагдаж байна.

Мэдээллийн салбарт үндэсний аюулгүй байдлыг хамгаалах үүднээс төр, иргэн, хувийн хэвшлийн мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдлыг баталгаажуулах тухай ойлголт багтдаг.

Иймд мэдээллийн аюулгүй байдал гэдэг нь ажил хэргийн тасралтгүй чанарыг хангах, эрсдэлийг багасгах, хөрөнгө оруулалтын үр ашиг, бизнесийн боломжийг нэмэгдүүлэхийн тулд мэдээллийг олон янзын аюул, заналаас хамгаалах ажиллагаатай холбоотой юм.

Дүгнэлт:

Энэ байдлаас үзэхэд өнөөгийн хуулийн дагуу кибер орчинд үйлдэгдэж байгаа гэмт хэрэг, зөрчлийг шийдвэрлэх боломж хомс төдийгүй гэмт хэргийн нэршил, агуулга, зорилго, сэдэл, гэмт хэрэг үйлдсэн арга хэрэгсэл зэргийг үндэслэн хэргийг үнэн зөв шийдвэрлэх, урьдчилан сэргийлэх үйл ажиллагаанд тохирохгүй байх хандлага байгаа тул шинжлэх ухааны үүднээс нэршил, бодлого, арга зүйг бодитой илэрхийлсэн ерөнхий болон салбарын хуулийг яаралтай шинэчлэх шаардлага зүй ёсоор урган гарч байна.

Шинжлэх ухааны мэдлэгийн /онол/ чиглэлийн хувьд:

Өнөөдрийн байдлаар кибер орчины аюулгүй байдлыг хангах, хамгаалах, ёс зүйтэй харилцаа, хандлага, хамтын үйл ажиллагаа бий болгох чиглэлээр тогтсон мэдлэгийн урсгал, чиглэл, тогтолцоог үнэлэх боломжгүй байна.

Кибер орчины аюулгүй байдлыг хангах, хамгаалах, ёс зүйтэй харилцаа, хандлага, хамтын үйл ажиллагаа бий болгох чиглэлээр шинжлэх ухааны судалгааны салбарыг цогцоор нь бий болгох шаардлагатай болжээ.

Хуулийн зүйл, заалтын нэр томъёолол, утга агуулгын хувьд ч нэг мөр тогтсон ойлголт байхгүй байна.

Тухайлбал: Монгол Улсын эрүүгийн хуулийн 25 дугаар бүлэгт “Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг” гэсэн бүлэгт тодорхой үйлдлийг гэмт хэрэг гэж тодорхойлсон боловч нэршил, тодорхойлолт, төрөл гэх мэт тодорхой шинжүүд өнөөгийн цаг үетэй тохирохгүй болсон байна.

Инновацид суурилсан эрх зүйн зохицуулалтыг бүх хүрээнд бий болгох шаардлагатай байна.

3.2. Кибер орчинд үйлдэгдэж байгаа халдлагатай тэмцэх техник зүйн үндэс

Кибер орчинд үйлдэгддэг гэмт халдлагатай тэмцэх үйл ажиллагаа нь гэмт хэрэг, зөрчилтэй тэмцэх уламжлалт арга, техник хэрэгсэлээр тэмцэхээс эрс ялгаатай төдийгүй шинжлэх ухаанд үндэслэсэн цогц үйл яьцыг шаардах боллоо.

Гэмт хэрэг, зөрчилтэй тэмцэх уламжлалт арга, техник хэрэгсэл нь эргүүл, харуул, манаа, хаалт, хашлага, гэрэлтүүлэг, цоож түгжээ, ажиглах, тоолох гэх мэт ихэвчлэн хүний хүчин зүйлийг түлхүү ашиглаж байсан бол өнөөдөр энэ салбарт дээрхи арга, техник хэрэгсэл үндсэндээ хэрэггүй болж шинэ мянганы хэв шинжтэй эрс өөрчлөлтийг шаардаж эхэллээ.

Шинэ мянганы техник хэрэгсэл хаана байна тэнд кибер орон зай оршиж хүн төрөлхтний соёл, шинжлэх ухааны ололтыг хэн хүнгүй ашиглахын зэрэгцээ гэмт халдлага тэнд зэрэгцэн оршино гэж ойлгох хэрэгтэй.

Энэ зуунд цахим мэдээллийн аюулгүй байдлыг хангаж ажиллана гэдэг хамгийн эрсдэлтэй асуудлын нэг болжээ.2015 оны 1-р сарын 15-ны байдлаар манай улсад давхардсан тоогоор 4,3 сая үүрэн холбооны хэрэглэгчтэй бол тэдний 1,5 сая нь ухаалаг гар утас ашигладаг гэсэн тоон мэдээ гарчээ. 2G сүлжээг 430 гаруй сум сууринд хүргэж, хүн амын 98 хувийг хангасан бол 3.5G сүлжээг 260 сум, сууринд хүргэсэн нь хүн амын 90 хувийн хэрэгцээг хангах болжээ. Харин энэ оноос 3.5G сүлжээг 100 хувь нэвтрүүлэх, 4GLTE технологийг нэвтрүүлж эхлэх, үндэсний контент аппликэйшнийг хөгжүүлэлтийг ойрын зорилт болгон дэвшүүлж байгаа юм[570].

Мэдээллийн технологи, шуудан, харилцаа холбооны салбарын ам бүлд хүссэн хүсээгүй багтаахаас аргагүй хэсэг болсон олон нийтийн хэвлэл мэдээллийн хэрэгсэл болох радиогийн тоо 28, 142 телевиз ажиллаж 500 гаруй сонин, сэтгүүл байгаа нь хэтийдсэн тоон үзүүлэлт бөгөөд энэ бүгд цахим болсоныг анхаарах хэрэгтэй.

Ийнхүү бодит тоон үзүүлэлтээр дэлхийд тэргүүлэх хэмжээний нөхцөл байдал нэгэнт бүрэлдэн бий болсон боловч кибер орчны халдлага, довтолгооны гомдол, мэдээлэл байнга хүлээн авах мэргэжлийн буюу иж бүрэн техник хэрэгсэлтэй, тусгай мэргэжилтэний баг бүрдүүлсэн аудит, тандалт, шинжилгээ, судалгааны байгууллага, тэдний хамтын үйл ажиллагаа хангалтгүй байна.

Гадаадын улс орны өнөөгийн байдал

Америкийн “Интернеттэй холбоотой гомдол хүлээн авах төв” (Internet Crime Complaint Center)-ийн мэдээгээр кибер гэмт хэргийн улмаас учирсан хохирлын хэмжээ 2009 оны дүнгээр 560 сая долларт хүрч өмнөх оныхоос хоёр дахин нэмэгдсэн байна.

Тус төвд 2014 онд 336,655 гомдол ирсэн бөгөөд нийт гомдлын 20% нь онлайнаар худалдан авсан бараа ирээгүй, 14.1% нь хувийн нууцад хамаарах мэдээлэл алдагдсан тухай байжээ. Онлайн хохирогчдын дундаж хохирол 575 доллар бөгөөд нийт хохирогчдын 1% нь 100 мянгаас илүү хэмжээний доллар алдсан байна. Мөн хохирогчдын 55 хувь нь 40-өөс дээш насны хүмүүс байжээ.

Энэхүү судалгаа, шинжилгээ, хандлагыг тооцон үнэлж АНУ Засаг захиргаа одоо байгаа засгийн газрын IT системийг клоуд систем рүү шилжүүлэхэд 20 тэрбум долларыг зарцуулахаар өнгөрсөн жилүүдэд шилжүүлсэн байна. Үүний зорилго нь хөрөнгө эзэмшигч хэн нэгнээс үйлчилгээ үзүүлэгч үрүү шилжих явдал болно хэмээн Кундра дурджээ.

Түүнчлэн 2015 он гэхэд их хэмжээний зардал шаардагдсаар байгаа 800 дата төвийн технологийг нь өөрчлөн клоуд системд шилжүүлснээр засгийн газрын агентлагуудын төсвийн дарамтыг бууруулж, их хэмжээний төсвийг хэмнэх бодит боломж бий гэж үзсэн.

Хакерууд засгийн газрын харьяа байгууллагууд, бизнесийнхэн, батлан хамгаалах цэрэг, цагдаагийн зэрэг байгууллагуудын мэдээллийн сангаас өдөрт 1TB гаруй мэдээлэл хулгайлж байна хэмээн тооцоолжээ.

---

[570]“Төр, хувийн хэвшлийн түншлэл-2015” нээлттэй хэлэлцүүлэг, илтгэл,Мэдээллийн технологи, шуудан, харилцаа холбооны салбар., 2015 оны нэгдүгээр сарын 15-ны өдөр Төрийн ордон,

Ийм их хэмжээний мэдээллийг хадгалахын тулд 500 ширхэг толгой компьютер бүхий сүлжээ ашиглах шаардлагатай гэсэн тооцоог ч мөн гаргасан байна.

Дэлхий даяар жил бүр 575 тэрбум долларын цахим гэмт хэрэг үйлдэгддэг болохыг судлаачид тогтоожээ. Зөвхөн хувь хүмүүсийн кредит картны мэдээллийг хулгайлах замаар 150 тэрбум долларыг ашиглаж байгааг судлаачид онцолж байна[571].

Тодруулбал АНУ, Хятад, Япон, Германд нийт 200 тэрбум долларын цахим гэмт хэрэг үйлдэгддэг. Америкийн зургаан хүн тутмын нэг нь буюу 40 орчим сая,Туркийн 54 сая, Германы 16 сая иргэн цахим гэмт хэрэгтнүүдэд мэдээллээ алдаж цахим хэргийн хохирогч болжээ.

Дэлхийн хэмжээнд үйл ажиллагаа явуулдаг корпорацийн цахим аюулгүй байдалдаа зарцуулдаг нэг жилийн дундаж хөрөнгийн хэмжээ 8,9 сая ам.доллар байдаг аж. Сүүлийн үед дэлхий нийтээр цахим ертөнц хурдтайгаар тархахын зэрэгцээ эрсдэл, халдлага хар бараан зүйл түүнийг тойрсонгүй.

Тэдгээрээс тоо баримтаар дурдвал 2013 оны эхний хагасд дэлхийн хэмжээнд 1сая 509 мянга 934 төрлийн шинэ вирус гарсан бөгөөд үүнийг 2012 оны мөн үеийнхтэй харьцуулахад 20% -иар нэмэгдсэн байна[572].

Мөн 2012онд дэлхий нийтийн судалгаагаар цахим гэмт хэргийн улмаас нэг жилд дэлхий нийтээрээ 3 тэрбумаас 1 их наяд ам.долларын хохирол амссан мэдээ байна.

Түүнчлэн 2012 онд цахим гэмт хэргийн хохирогчдын тоо 556 саяд хүрч, хувь хүмүүсийн луйвардуулсан мөнгөний хэмжээ 110 тэрбум ам.доллар болсон нь нэг хүнээс дунджаар 197 ам.долларыг цахим гэмт хэрэгтнүүд луйварджээ.

Ингээд цахим ертөнцийн халдлага, хакердах гэмт хэргүүд дэлхий нийтээр газар авч хичнээн хэмжээний хор хохирол учруулсаныг томоохон кибер халдлагуудын баримтаар сонирхуулая.

- **1983он** -Кевин Митникийг Пентагоны дотоод сүлжээнд нэвтэрсэний төлөө АНУ-ын цагдаа нар баривчилсан. Түүнийг байнгын хяналтад байлгаж, хэд хэдэн удаа Холбооны мөрдөх товчооныхон баривчилж байжээ. Тэрээр товчхондоо хакеруудын бэлгэ тэмдэг юм.
- **1994он** – Оросын математикч Владимир Левин Сити банкны мэдээллийн санд нэвтэрч, хамсаатнуудынхаа хамтаар гадаадын дансруу 10 сая ам.доллар баривчлагдахаасаа өмнө амжиж шилжүүлсэн.
- **2010 оны 6-р сар** – Ираны цөмийн станцын Siemens фермийн тоног төхөөрөмжүүдэд “stux-net” нэртэй шинэ төрлийн вирус нэвтэрчээ.
- **2011 оны 4-р сар**- Sony компанийн “play station”-ий сүлжээ томоохон кибер халдлагад өртөж, хакерчид сүлжээнээс нь нийт 77 сая мэдээллийг хулгайлсан бөгөөд үүний уршигаар компани сар гаруй зогссон байна.
- **2012 оны 5-р сар** –Ерөнхийлөгчийн сонгуулийн хоёр шатны санал хураалтын хооронд Францын ерөнхийлөгчийн оршин суудаг “Элисейн” ордон кибер халдлагад өртжээ. Францын Ерөнхийлөгч Николя Саркозигийн ахлах зөвлөхийн компьютерийг хакердаж стратегийн холбогдолтой нууц баримт бичгүүдийг хулгайлсан байна. Францын тал энэ явдлыг гадаадын засгийн газрын оролцоотой, зохион байгуулалттай хэрэг гэж үзжээ.
- **2012оны 8-р сар** – Газрын тосны “Aromca” группын 30 мянган компьтерт вирус тараажээ.
- **2012 оны 12-р сар** –Францад сайн дурынхан ба шинжээчдээс бүрдсэн 6 ажлын хэсэг бүхий иргэний кибер батлан хамгаалахын сүлжээ байгуулагдаж кибер аюулгүй байдлын талаар зөвлөгөө өгдөг болсон байна.

[571] Internet Crime Complaint Center-ийн мэдээлэл, 2014 оны 6 сарын 10
[572]Internet Crime Complaint Center-ийн мэдээлэл, 2014 он

- **2013 оны 9-р сар** – Германы “Vodafone” гар утасны компанийн 2 сая гаруй хэрэглэгчийн мэдээллийг хулгайлсан.
- **2013 оны 10-р сар** – “Adobe”-ийн серверүүд халдлагад өртөж программ хангамжийн эх код болон 38 сая хэрэглэгчийн мэдээлэл эрсдэлд орсон байна.
- **2014 оны 8-р сар** АНУ-ын 29 мужийн нийт 206 эмнэлгээс 4,5 сая хүний хувийн мэдээлэл алдагдсан бөгөөд үүнд өвчитний овог нэр, төрсөн он сар, гэрийн хаяг утасны дугаар багтжээ.

“Kaspersky Lab" компанийн тооцоогоор хакерууд банк болон компаниудын мэдээлэл рүү шууд халдах болон зохион байгуулалттай гэмт хэрэгтнүүдэд туслах явдал нэмэгджээ.

Тухайлбал кассын машинд вирус суулгаж мөнгийг хулгайлах, хилийн боомт шалганы үйл ажиллагаа, менежментийн системийг хакердаж хар тамхи чөлөөтэй оруулах зэргээр илрэх болсон байна.

“Kaspersky Lab"-ийн Ерөнхий захирал Евгений Касперский "Компаниудын сүлжээнд вирус суулгаж, улмаар тэр нь хэлтсүүд хоорондын файлаар дамжин мөнгө шилжүүлдэг компьютер руу нэвтэрч байна" гэжээ.

Энэ онд үйлдэгдсэн хамгийн аюултай гэмт хэрэг нь “Home Depot" компаниас 53 сая мэйл хаяг, 56 сая төлбөрийн картны мэдээлэл хулгайлсан хэрэг болж байна.

"Бүгдээр бие биеэ тагнан мэдээлэл хулгайлж байна. Янз бүрийн эх сурвалжаас цахим халдлага хийгддэг.Англиас гадна БНХАУ, ОХУ-ын програмистууд ч үүнд хамаатай" гэж Касперский онцолсон байна.

Тухайлбал: Кибер гэмт хэргийн цар хүрээ агуу их, эдгээр нь зүгээр нэг сонгодог дайралтууд биш юм гэж өрсөлдөөний тагнуулын шинжээч Андрей Масалович тэмдэглээд «Сүүлийн хоёр жилийн үйл явдлууд Интернет рүү өөр өнцөгөөс харахыг шаардах болов. “**Арабын хавраас**” эхэлж одоогийн ойрхи дорнодын бүс нутаг дахь үйл явдлаар үргэлжилж байгаа нөхцөл байдлын ихэнх хэсгийг сүлжээнээс удирдан зохион байгуулж байгаа гэж судлаачид тодорхойлж байна. Мөн одоо хакерын талбар нь маш их хэмжээний янз бүрийн гэмт үйлдлийн эздээр дүүрчээ» гэж үзэж байна.

Хакерын заналхийллүүдийг мэргэжилтэнүүд бүхэлдээ гурван хэсэгт хуваадаг.

Эхнийх нь санхүүгийн луйвар хийдэг хувь хүмүүс болон жижигхэн бүлэг, тэдэнтэй үр ашигтай тэмцэж болж байгаа юм.

Хоёрдахь төрөл нь Anonymous маягийн дундаж бүлэглэл бөгөөд тэд үзүүлэлтийн шинжтэй байдаг. Жишээ нь: АНУ-ын баталсан “пиратын эрсэг”хуулийн хариуд тэд дэлхийн Интернет сүлжээг устгана гэж сүрдүүлнэ.

Гуравдахь төрөлкибер террорист-хакерууд. Одоо үед энэ төрөл дэлхийн аюулгүй байдалд хамгийн гол заналхийллүүдийн нэг болоод байна гэж Александр Власов үзэж байна.

«Энэ бол эрчим хүчний системийн ажилд болон усны дамжуулах хоолойн гэмтэл, сүйрэлийг зохион байгуулж чадах нууц байгууллагууд юм.

Жишээ нь тэд Нидерландын усны хамгаалтын системийн удирдлагыг гэмтээхэд хүргэвэл тус улсын тал нь усанд автана» гэж Александр Власов хэллээ.

Гэвч дээрхи тулгамдсан асуудлыг шийдвэрлэхийн тулд техник хэрэгсэлийн агуулгыг хамаарсан цахим орчны зориулалттай ухаалаг техникийн цогц бодлоготой үйл ажиллагааг хэрэгжүүлэх шаардлагатай боллоо.

Үүний тулд дараах үндсэн асуудлыг анхаарах шаардлагатай:

1. Тухайн техник хэрэгсэлтэй ажиллах чадвартай хүний нөөц, сургалтын асуудал,
2. Кибер орчны гэмт халдлагатай тэмцэхэд шаардлагатай техник хэрэгсэл, санхүү, эдийн засгийн асуудал

Кибер орчинд үйлдэгдэж байгаа гэмт халдлагатай тэмцэхэд олон улсын хэмжээнд дараах төрлийн техник хэрэгсэлийг ашиглаж байна.

Үүнд:

А. Гэмт хэргийн шинжтэй үйлдэл, эс үйлдлийг бүртгэх, хянах тоног төхөөрөмж, хэрэгслүүд,

Б. Гэмт хэргийн шинжтэй үйлдэл, эс үйлдлийг илрүүлэх, мөшгөх, эх сурвалжийг олж тогтоох тоног төхөөрөмж, хэрэгслүүд,

В. Гэмт хэргийн шинжтэй үйлдэл, эс үйлдлийн дагуу хариу үйлдэл хийх, эх сурвалжийг дарах, хор хохирлыг бууруулах тоног төхөөрөмж, хэрэгслүүд,

Г. Гэмт хэргийн шинжтэй үйлдэл, эс үйлдлийн нотлох баримтыг илрүүлэх, гарган авах, бэхжүүлэх, задлан шинжлэх, тоног төхөөрөмж, хэрэгслүүд,

Эхний хоёр хэсэг дэх тоног төхөөрөмж, хэрэгслүүд нь “МТ” ашиглаж буй байгууллага, иргэн бүрт байх шаардлагатай.

Гурав, дөрөвдэх хэсэгт заасан тоног төхөөрөмж, хэрэгслүүдийгХууль сахиулах /гэмт хэрэгтэй тэмцэх чиг үүрэг бүхий байгууллага/ байгууллагууд эзэмшиж ашиглах шаардлагатай.

Үүнээс гуравдахь хэсгийн тоног төхөөрөмж, хэрэгслүүд нь цагдаа, тагнуул, зэвсэгт хүчний зэрэг тусгай чиг үүргийн байгууллага, албадуудад түлхүү ашиглагдана. Харин дөрөвдэх хэсгийн тоног төхөөрөмжүүд нь Шүүхийн шинжилгээний болон судалгааны бусад байгууллагуудад ашиглагдаж байна.

Эдгээр техник хэрэгсэлийг үйл ажиллагаандаа нэвтрүүлж, ашиглах шаардлагатай байгаагаас гадна техникийн хурдатай хөгжлийн хандлагаар эдгээр хэрэгсэлүүд бараг улирал бүр ухаалаг болон өөрчлөгдөж, шинэчлэгдэж байгааг анхаарч дэвшилээс хоцрохгүй байхыг эрмэлзэх хэрэгтэй.

Дараагийн нэг асуудал нь техник хэрэгсэлийг дэлхийн улс орнууд нэгэнт бүтээн үйлдвэрлэлд нэвтрүүлсэн байгаа тул манай орны хувьд эдгээр техник хэрэгсэлийг кибер орчны гэмт халдлагатай тэмцэх үйл ажиллагаандаа авч ашиглахаданхаарах нэг асуулдал бол чадвар бүхий баг, хүний нөөц, сургалтын эрх зүй, эдийн засгийн зохицуулалт, тогтолцоо.

Хүний нөөц, сургалтын тогтолцоо, чиг хандлага

Хүний нөөцийн асуудал хийгээд ажлын байрны сургалт өнөөдөр аливаа байгууллагын менежментийн нэн чухал тулгамдсан асуудал боллоо.

Мэдээлэлд дарагдсан мэдлэг минь хаана байна, мэдлэгт дарагдсан ухаан минь хаана байна гэж мэдлэг, боловсролыг ангилж Францийн сэтгэгч, нэрт яруу найрагч нэгэнтээ хэлсэн байдаг.**Томос Элиот /**1888-1965**/**

Энэ XXI зуун бол мэдээлэл хийгээд бодит мэдлэгийн зуун.Мэдээллийн эрин.

Мэдээлэл нь дэлхийн ертөнцийг асар хурдтайгаар нэгтгэн нягтруулж байгаатай адил энэ салбарын хүний нөөцийг боловсролын хүртээмжид анхаарах бусмэргэжлийн хэрэгцээ, боловсролын чанарт гол анхаарал хандуулах шаардлагатай.

Хүний нөөцийг ажлын байрны онцлог, тавигдах тусгай шаардлагын дагуу сонгож, нэгэнт бүрдсэн хүний нөөцийг 5-аас дээш жилийн дараа, урд өмнө эзэмшсэн боловсрол, мэдлэгээр нь ажиллуулах цаг нэгэнт түүх болон үлдсэн учир ажлын байрны дараах чадваржуулах сургалтын явцад сурган энэ салбарт ажиллуулах шаардлагатай.

Жишээ нь 1960 онд ХАААИС төгсчээ гэж бодъё, тэр нөхөр тэтгэвэртээ гаран гартлаа боловсрол, мэдлэгийн талаар санаа амар ажиллаж амьдраад айх аюулгүй өнгөрдөг байж.Энэ нь өөрийгөө хөгжүүлэх онцын шаардлага тулгарахгүй гэсэн үг.

Учир нь мэдлэгийн цар хүрээ урт настай байснаас тэр.1970 онд техникийн их сургууль эсвэл хуулийн сургууль төгссөн хүн мөн нэгэн адил өөрийгөө хөгжүүлэх онцын шаардлага гардаггүй байв.Тэтгэвэртээ гартлаа зовлон багатай ажилланагэсэн үг.

Гэтэл 1980-аад оноос мэдлэгийн нас богиносож эхэлжээ.Амьдралын баталгаа 30-35 нас хүртэл, цаашаа өөрийгөө хөгжүүлэхгүй бол явахгүй болжээ.Их хурдтай хямрал ойртож буйг 1980-аад оны техникийн хөгжил хүмүүст мэдрүүлж өгчээ.

- ✓ 1960 оных 60 хүртлээ,
- ✓ 1970 оных 50 хүртлээ,
- ✓ 1980 оных 45 хүртлээ ажиллаж болдог байсан бол

- ✓ 1990 оны мэргэжилтэн хичнээн онц төгсгөөд, 5 жил ажиллав уу үгүй юү, өөрийгөө хөгжүүлэх ацан шалааны өмнө тулж байна. Олж авсан мэдлэгийнх нь нас огцом богиносчээ гэсэн үг.
- ✓ 2010 оноос хойш мэргэжилтэн жил бүр мэдлэг, харилцаа, хандлага, хамтын ажиллагаагаа шинэчлэх шаардлага гарч байна.

Энэ цаг үед дэлхий даяараа насан туршийн боловсролын бүтэц, тогтолцоонд шилжсэн.Дэлхийн ертөнцийн тогтолцоо даяаршлын дүнд аажмаар бэхжиж, бие даасан хүрээ хязгаар үгүй болж, бүх хүрээ системүүд холбогдож, түүний хараат болох нь батлагдсаар байна.

Мэдлэгийн, чадварын хувьсгал энэ зууныг нөмөрлөө.Ихээхэн хурдтай идэвхтэйгээр эл хувьсгал өрнөж эхэллээ.“Хурдацтай өөрчлөгдөн буй нийгмийн хэрэгцээ шаардлагад өнөөгийн боловсролын, сургалтын систем бүрэн дүүрэн нийцэж байгаа эсэхийг эргэж харах цаг болсон”

Боловсрол, сургалт нь өөрөө хамгийн их үр ашиг өгдөг салбар мөн боловч тухайн зүйлийг яах гэж, юуны тулд эзэмших вэ гэдэг нь тодорхой биш бол ямар ч хэрэггүй хоосон зүйл болж хувирдаг.[573]

Тухайн албa хаагч нарт яагаад үүнийг сурах ёстой, яагаад энэ талын мэдлэгийг авах ёстой вэ гэдэгт ямар ч хариулт өгөлгүйгээр хэн нэгний баталсан дүрмийн дагуу сургаж эхлэвэл нэг ёсны юунд зорьж, хаа хүрэхийг нь хэлэлгүйгээр хаашаа ч хамаагүй алхахыг шууд шаардаж байна гэсэн үг юм.

Өнөөгийн нийгэмд нэг шатны сургуулиас нөгөө шатанд элсэх, сургууль төгсөөд ажилд орох гээд завсрын дамжлага бүрт хүмүүсийг бүрдүүлсэн “профайл”-аар нь үнэлэх болсон.Үүнтэй холбоотойгоор сайтар боловсрох гэхээс илүү, өөрсдийн түүх, намтарыг бусдад тайлагнах, өөрийгөө илэрхийлэх зорилгоор суралцагчид олширсоор байгаа билээ.Түүнчлэн хүмүүсийн сурч боловсрох гэхээс илүү шаталсан тогтолцооны зэрэг дэвийг дүүргэх зорилго нь томоохон асуудал болоод байгаа нь ажиглагдаж байна.

Үүнээс улбаалан боловсролын зэрэг, диплом дээр тулгуурласан статистик үзүүлэлтүүд өссөөр байгаа ч чанарын ахиц дэвшил үүнтэй урвуу хамааралтай болж, “гологдмол”, илүүдэл ажиллах хүч бэлтгэж хаа хаанаа үргүй зардал гаргах явдал газар авсаар байна.

“Хувь хүний болоод үндэсний хөгжлийн чиг хандлагыг хооронд нь нягт зангидаж, боловсрол эзэмшиж буй хүмүүсийн хандлага, сэтгэлгээнд гол анхаарлаа хандуулах хэрэгтэй байна”[574]

Ирээдүйн хандлагаар эдгээр тулгамдсан асуудал бүрийг шийдвэрлэх шаардлагатай. Тухайлбал:

Хүний нөөцийг шилж сонгох хандлага:

Одоогийн бодит байдалд тухайн хүний намтар, түүхийг үндэслэсэнхавтастай бичгээр сонгож байгаа төрх, хандлагыг өөрчлөх цаг болжээ. Өнөөгийн нийгэмд нэг шатны сургуулиас нөгөө шатанд элсэх, сургууль төгсөөд ажилд орох гээд завсрын дамжлага бүрт хүмүүсийн бүрдүүлсэн “профайл”-аар нь үнэлэх болсон.

Үндсэн шаардлага

- ✓ Ярилцлага
- ✓ Тусгай сорил
- ✓ Эрүүл мэнд
- ✓ Сэтгэц, сэтгэл зүйн хамааралаар

Нэмэлт шаардлага

- ✓ Ажлын байрны нэмэгдэл шаардлага /зүс, гадаад төрх, хүйс, нас гэх мэт
- ✓ Тусгай шаардлага /хэл яриа, бие даан ажиллах, тусгай чадварууд гэх мэт/

[573] ЮНЕСКО-гийн боловсролын асуудал эрхэлсэн захирал Чарльз Хопкинс НҮБ-ын нэгдсэн чуулганд хэлсэн үг., 2014,

[574]Л.Цогтбаяр, “Хууль зүйн сэтгэц судлал” лекц, УБ.,2014 он

Хүний нөөцийн сургалтын хандлага

Засгийн газраас боловсруулан УИХ-д өргөн бариад байгаа Төрөөс боловсролын талаар баримтлах бодлого ийм зарчимд тулгуурлажээ./УИХ 1996, 2008 онд Төрөөс боловсролын талаар баримтлах бодлого баталсан/

Иргэн бүрт боловсролын үйлчилгээг тэгш, хүртээмжтэй, чанартай, олон хувилбартай, чөлөөтэй, нээлттэй хүргэхэээс эхлээд боловсролын салбарт сайн засаглал, удирдлагын мэдээллийн нэгдсэн системийг хөгжүүлэх, насан туршдаа боловсрол эзэмших орчин, нөхцөл, боломжийг бүрдүүлэх; боловсролд мэдээллийн технологийг ашиглах, эх хэл, түүх уламжлал, гадаад хэлний сургалтын үндэсний бодлого, хөтөлбөр хэрэгжүүлэх гэх мэт шинэ зарчмууд дээрх баримт бичигт тусгалаа олсон байна.

2015 оноос хойшхи боловсрол ямар байх вэ гэдгийг Дэлхийн боловсролын форум тодорхойлох бөгөөд Ази, Номхон далайн бүсийнхэн бүх нийтийн боловсролын зөвлөлдөх хороо хуралдаж/2014.04.20./ хамтарсан саналд 2030 он гэхэд бүх хүмүүсийг насан туршдаа суралцах, чанартай боловсролыг хүртээмжтэй, тэгш хүртэх боломж, нөхцөлөөр хангах гэсэн ерөнхий зорилго дэвшүүлэн, нийт долоон зорилт тодорхойлжээ.

Хууль цаасан дээр үлдээд эцэст нь амьдрал дээр дураар авирлах явдал гаргуулахгүйн үүднээс энэ салбарын мэргэжилтэн нарыг бэлтгэх, сонгох, хүний нөөц бүрдүүлэх, давтан сургах тогтолцоонд эрс өөрчлөлт оруулах явдал байдаг.

Өнөөдөр сайн чадвартай мэргэжилтэн хэрэгтэй болж байгаа учир үргэлжлүүлсэн буюу ажлын байрны дараах боловсрол, сургалтын тогтолцоог шинэчлэх үндэслэл, шаардлага байгааг авч үзье.

1. Нийтлэг асуудал, өнөөгийн байдал
2. Эрх зүйн боловсролын бүрдэл хэсэг, хөгжил, төлөв
3. Заах арга зүйн төлөв
4. Профессор, багш, дэд бүтэц
5. Асуудал
6. Чиг хандлага

Нэг. Нийтлэг асуудал, өнөөгийн байдал:

1. Олгосон боловсрол, эзэмшсэн мэргэжил, эрэлтийн хоорондын зөрүү буюузавсар гарах учиргүй/энэ нь ажлын байрны онцлог, бусад онцгой шаардлага гэсэн үг/ хэрэв ийм зүйл байгаа бол шүүмжлэл гардаг /муу сурсан байна гэдэг гэх мэт/

Ажил олгогч сургалтын байгууллагын хооронд маргаан, зөрчил үүсдэг гэх мэт.

2. Зах зээлийн буюу чөлөөт өрсөлдөөний эрэлтэд нийцүүлэх. Зай завсар гаргахгүй гэсэн үг. Эрэлт нийлүүлэлтээр шийдвэрлэнэ гэдэг нь асуудал юм. /мөрдөн байцаагч, төлөөлөгч, шинжээч гэж үргэлжилнэ/

3. Универсал буюу тухай чиглэлээр дагнан мэргэших шаардлага гэж байна.

Гадаадын /АНУ, Герман гэх мэт/ улс орнуудад бас л ийм асуудал байгаа боловч тодорхой хэмжээгээр шийдээд л явж байна.

Хоёр. Мэргэшүүлэх боловсролын бүрдэл хэсэг, хөгжил, төлөв:

Тогтолцоо:

Өнөөдөр манай сургуулиуд бүгд адилхан сургалт явуулж байна.

Иргэний ба мэргэжлийн /эрх зүйч эсвэл өөр чиглэлээр бэлтгээд л болж байна/

Иймд эхлээд хүнийг шилж сонгож авна, дараа нь мэргэшсэн /мэргэшүүлнэ/ мэгэжилтэн бэлтгэдэг сургалтад /хөтөлбөрт/ хамруулна, үргэлжилсэн /давтан/ сургалтуудад хамруулна гэсэн тогтолцоо байх хэрэгтэй.

Мэргэшүүлэх боловсролын бүрдэл хэсэг:

Багш, элсэгч, сургалтын орчин, сурах бичиг, хэрэглэгдэхүүн гэх мэт.

Харин манайд сурах тогтолцоо, сургах стандарт хөтөлбөр, сурах бичиг, профессорын баг байна харин багш, эрэлтэд сурагч алга байгаа мэт.

Гурав. Эрх зүйн боловсролын заах арга зүйн төлөв:

Сэтгэгч Аристотел “Полис бол нэгдэл энэ нэгдэл Шударга үнэн бол улс гэрийн салшгүй хэсэг, нийгмийн нэгдлийг цэгцлэн байгуулагч эд юм”[575].

Тэрбээр Уул хад, ой модоор алхаж явах зууpаа байгалийг ажиглан юмс үзэгдлийг танин мэдэж тэрхүү ухаанаар сурагчиддаа лекцээ уншдаг байсан ба энэ арга барил заншлаас нь үүдэн сургуулийг нь **перипатетик сургууль**гэж нэрлэцгээсэн.

Аристотел тухайн үедээ байгалийг ажиглан танин мэдэж сургалтаа явуулж байсан тул өнөө үед түүний заах арга зүйг дэлхийн суралтын байгууллагууд нэвтрүүлж эхлээд байна.

Case study /тохиолдол, бодлого/ ба клиник сургалт /бодит зүйл дээр ажиллаж сурах, дадлагажих/. Эндээс эрх зүйн хэрэглээ өгдөг сургалтын амин сүнс нь бодлого байх учиртай.

Дөрөв. Профессор, багш, дэд бүтэц:

- Багш бэлтгэх тогтолцоо чухал,
- Манайд ийм тогтлолцоо алга байна
- Мэргэжил дээшлүүлэх тогтолцоо
- Номын сан
- Ашигтай талбай, таатай орчин,
- Гадаад ном, сэтгүүл, олон хэлбэртэй байх
- Элсэгчид:
- Элсэгчийн суурь бэлтгэл
- Элсэгчийн нас төлөвшил /туршлага, дадлага, хандлага, харилцаа, хамтын ажиллагаа гэх мэт/
- Хуульчийн ажил мэргэжлийн онцлог
- Боловсрол шаардах,
- Амьдралын туршлага, нас
- Туршлага
- Сургалт

Тав. Асуудал

Мэргэшсэн мэргэжилтэн:Ийм тогтолцоо, ийм үнэлэмж байхгүй учир дүн шинжилгээ хийж боломжгүй байна,

Суралцагч:Суралцагчийг чадваржуулах асуудал хаа хаанаа муу, хангалтгүй байна.

Иймд энэ бүгдийг мэргэшүүлэх, чадваржуулах, үнэ цэнийг бий болгох, үнэлэх, тааламжтай хүрэлцээтэй цалин, таатаай орчин, ухаалаг үйл ажиллагаа байх хэрэгтэй гэж үзэж байна.

Монголын хамгийн чухал баялаг хүн байх юм.

Хүний хамгийн чухал баялаг бол эрдэм мэдлэг байх юм.

Өнөөгийн дэлхий нийтийн сэтгэлгээний чиг хандлага тийм болж байна.

Монголын боловсролын тогтолцооны шинэчлэл үүнийг баримжаалах хэрэгтэй мэт ойлгогдоно.

Эрх зүйн зохицуулалт:

Өнөөдөр мэргэжилтэн бэлтгэж байгаа үндэсний тогтолцоо чамлахааргүй байгаа хэдий ч эрх зүйн зохицуулалтын тухайд:

- Боловсролын тухай хууль 2002.05.03,
- Дээд боловсролын тухай хууль 2002.05.03,
- ШУТех хууль 2006.12.28,
- Инновацийн тухай хууль 2012 он
- Монгол Улсын Их Хурлаас “Төрөөс боловсролын талаар баримтлах бодлого” 1995, 2008 оны бодлогын баримт бичиг,
- Засгийн газраас "Боловсрол" Үндэсний хөтөлбөр (2010-2021 он)

[575]*Great Issues in Western Civilization (volume I) Politics by Aristotle*

2010.02.03 зэрэг хууль, бодлогын суурь тогтолцоо байгаа боловч өөр хоорондын уялдаа байхгүй, эрэлт нийлүүлэлтийн тэгш харьцаа алдагдсан, ихэнх заалт нь тунхаглалын шинжтэй байгаа тул нийтийг хамарсан бүтэц, зохион байгуулалтыннэгдмэл байдлын эрх зүйн зохицуулалт, тогтолцоог яаралтай бий болгох хэрэгтэй.

3.3. Кибер орчинд үйлдэгдэж байгаа халдлагатай тэмцэх бүтэц, зохион байгуулалтын арга зүйн үндэс

Хүн бүр мэдлэгийнхээ хүрээнд сэтгэдэг. Иргэншсэн хүн төрөлхтөн шинжлэх ухааны хүрээнд сэтгэдэг. Шинжлэх ухаанд шинэ үзэл онол гарах бүрт хүн бүрийн сэтгэх хүрээ тэлж аливаа зүйлсийг харах шинэ өнцөг, асуудалд хандах шинэ хандлага, бүтэц, зохион байгуулалт, арга зүйбий болдог.

Харин шинэ бүтэц, зохион байгуулалт, арга зүйнь шинэ технологийншийдлүүдийг бий болгож улмаар шинжлэх ухааны болон салбарын өмнө тулгамдсан олон асуудлуудыг шийдвэрлэн, тухайн орчинд шинэ хэрэглээ эсвэл хэрэглээний шинэ үнэ цэнэ, үнэлэмжийн чиг хандлагуудыг бий болгодог.

Монгол Улсын хувьд кибер орчин дахь гэмт халдлагатай нэгдмэл байдлаар тэмцэхойлголт, эрх зүйн зохицуулалт, тэмцэх нэгж, байгууллагын бэлэн байдал, ур чадварын түвшинг үнэлэх, тодорхойлох шалгуур байхгүй учир нэгтгэн дүгнэхэд бэрхшээлтэй.

Монгол Улсын хувьд кибер орчин дахь мэдээллийн цахим сүлжээнд халдсан гэмт халдлага, довтолгооны тохиолдол нэг бүрийг нарийн бүртгэх бүтэц, зохион байгуулалтын орчин бүрэлдээгүй байгаа учир нэгдмэл статистик мэдээ гаргахад хүндрэлтэй байна.

Мэдээллийн технологи хөгжиж буй өнөө цагт кибер орчины мэдээллийн салбарт хүний эрх, эрх чөлөө, үндэсний аюулгүй байдлыг хамгаалах үүднээс төр, иргэн, хувийн хэвшлийн мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдлыг баталгаажуулах, ажил хэргийн тасралтгүй чанарыг хангах, эрсдэлийг багасгах, хөрөнгө оруулалтын үр ашиг, бизнесийн боломжийг нэмэгдүүлэхийн тулд мэдээллийг олон янзын аюул, заналаас хамгаалах үйл ажиллагааны бүрдэлийг кибер орчин дахь гэмт халдлагатай тэмцэх ойлголт гэж тодорхойлох шаардлага бүрэлдсэн байна.

Кибер орчинд үйлдэгдэж байгаа гэмт халдлагатай тэмцэх асуудал нь:

1. Гэмт халдлагаас урьдчилан сэргийлэхбодлого, үйл ажиллагааны хүрээн дэх цогц асуудал,
2. Гэмт халдлага үйлдэгдэж байгаа болон үйлдэхээр бэлтгэж байх үед нь таслан зогсоохбодлого, үйл ажиллагааны хүрээн дэх цогц асуудал,
3. Нэгэнт гэмт хэрэг үйлдэгдсэн гэх шинж байгаа тохиолдолд мөрдөн шалгах, эцэслэн шийдвэрлэхбодлого, үйл ажиллагааны хүрээн дэх цогц асуудал хамаарна.

Кибер орчны аюулгүй байдлыг хангах, хамгаалах талаар явуулах өөр хоорондоо нягт холбоотой энэхүү бодлого, үйл ажиллагааг хэрэгжүүлэхдээ оролцогч нарыг тодорхой бүтэцэд оруулж сайтар зохион байгуулах эрх зүйн болон эдийн засгийн тогтолцоог үндэсний инновацийн тогтолцоо, судалгаанд үндэслэн бүрдүүлэх нь чухал.

Цогц бодлого, үйл ажиллагааны бүтэц, зохион байгуулалтын хүрээ нь

- Байгууллага, хамт олны
- Үндэсний хэмжээний
- Бүс нутгийн хэмжээний
- Олон улсын хэмжээний гэх мэт хүрээгээр тодорхойлох шаардлага байна.

Ийм учир энэ үйл ажиллагаа нь нийт олны /кибер орчинд ажиллаж үйл ажиллагаагаа хэрэгжүүлэх зорилготой байгууллага, хувь хүн бүр/ өргөн хүрээг хамруулах үүднээс бүх нийтийн оролцоонд тулгуурлаж байж бодит биелэлээ олох нь тодорхой.

1960-аад оны эхээр электрон бүхий хэвлэл мэдээллийн шинэхэрэгсэл нь нийгмийн харилцаа, соёлд нөлөөлөх тухай онол дэвшүүлсэн Маршал Мак Луй хэмээх Канадын эрдэмтэн “шинээр гарч ирж буй хэвлэл мэдээллийн хэрэгсэл нь дамжуулж буй мэдээллээсээ илүүтэйгээр өөрөө аугаа их мэдээллийг агуулна”[576] гэж бичсэн нь өнөөдөр биелэлээ олж байна.

Өөрөөр хэлбэл интернетийн мэдээллийн урсгалд хил хязгаар, хаалт, саад гэж үгүй бөгөөд улс орон төдийгүй дэлхий дахины нийтийн харилцаанд мэдээллийн харилцаа үлэмж их нөлөөтэй болохыг өгүүлсэн хэрэг юм.

Юуны өмнө кибер орон зай нь өөрийн онол, ёс суртахуун, үнэт зүйлс, үнэлэмж, үйл ажиллагааны нэгдмэл дүрэмтэй байх учиртай.

Монголын Улсын хувьд мэдээллийн кибер орон зай, орчинг ёс зүйтэй, ёс суртахуунтай, хариуцлагатай мэдээллийн орчин болгон хувиргах бүтэц, зохион байгуулалтын эрх зүйн орчин үнэхээр дутагдаж байна.

Зүйрлэн хэлбэл орчлонгийн салхи хэдийгээр сайхан ч, аюул дагуулсан хуй салхи хавь ойрын эд зүйлийг бусниулах мэт дур зоргоороо оролцож болохгүй. Түүнчлэн кибер орчины мэдээллийн урсгал дахь үүлэн тооцоолол хүн төрөлхтний дээрээс мөнгөөр бороо оруулах[577]-ын зэрэгцээ хүйтэн хуурай салхиар үлээх нь тодорхой боллоо.

Мэдээллийн кибер орчин түүн дотороос цахим сэтгүүл зүй нь бодит, шуурхай мэдээллийн нэгэн хүчирхэг сүлжээ болон хөгжиж байгаа боловч элдэв хов жив, гүтгэлэг, доромжлол зэрэг ёс зүйгүй, шударга бус мэдээллийн талбар болчих, тэр байтугай улс үндэсний эрхэм ёс уламжлал, ариун суртахууныг толботуулах, улс орны тусгаар тогтнол, аюулгүй байдалд хохирол учруулж болзошгүй мэдээллийн урсгал байгаа хэн бүхэнд илэрхий.

Одоогоор Монголын нөхцөлд Харилцаа холбооны зохицуулах хорооноос 2011.02.27-ны өдөр баталсан “Тоон контентийн үйлчилгээний зохицуулалтын ерөнхий нөхцөл шаардлага”, Монголын вэб сайтууд холбооноос 2011 онд батлагдсан “Вэб сайт эрхлэгчдэд тавигдах нөхцөл шаардлага” зэрэг цөөхөн эрх зүйн дагнасан зохицуулалт байгаа боловч “Оюуны өмчийн зохицуулалт”, “Сөрөг контентийн зохицуулалт”, “Мэдээлэл авах эрх, нууцын зохицуулалт” зэрэг олон зохицуулалтын хэрэгцээ шаардлагатай байна.

Монгол Улсын хуулиудад цахим ертөнцийн эрх зүйн зохицуулалт ямар нэг хэмжээгээр байгаа боловч Кибер орчинд үйлдэгдэж байгаа халдлагатай тэмцэх бүтэц, зохион байгуулалтыг тусгасан нэгдмэл цогц хуулийн зохицуулалт үгүйлэгдэж байна.

Бүх нийтийн оролцоо, нийгэм даяарх ойлголт, мэдлэгтэй тохиолдолд энэ төрлийн гэмт явдалтай тэмцэж чаддаг.Тиймээс иргэн бүрийн оролцоог бий болгох зорилготой нэгдмэл бүтцийг зохицуулсан эрх зүйн зохицуулалт шаардлагатай.

Энэ бүтэц нь:

- ✓ Мэдээллийн аюулгүй байдал, сүлжээ, системийн аюулгүй байдлын чиглэлээр мэргэшин ажилладаг төрийн тусгай байгууллагууд,
- ✓ Хууль сахиулах, хяналтын байгууллага
- ✓ Төрийн байгууллага бүрийн МАБ-ын удирдлагын тогтолцоо;
- ✓ Улсын онцгой байгууллагууд

Тухайлбал: Банк, санхүү, татвар, гааль, зэвсэгт хүчин, онцгой байдал, бусад хууль сахиулах байгууллагууд, даатгал, холбоо, төмөр зам, агаарын тээвэр, эрчим хүч, дулаан, эмнэлэг, боловсрол, бүртгэлийн гэх мэт кибер удирдлагын тогтолцоотой байх шаардлагатай гэх мэт/

- ✓ Мэдээллийн аюулгүй байдал, сүлжээ, системийн аюулгүй байдлын чиглэлээр мэргэшин ажилладаг Хувийн хэвшлийн болон төрийн бус байгууллагууд,

[576]Маршал Мак Луй, "Мэдээллийн хэрэгслийг ойлгох нь", Канад Тр., /1964/

[577]Хятадын “Алибаба” групп тэргүүн **Ма Юнь 2014 оны** есдүгээр сарын 19-ны өдөр Нью Йоркийн Хөрөнгийн бирж дээр25 тэрбум доллараар хувьцааг арилжаалав.

Тухайлбал: Мэргэшсэн компани, MonCIRT,CSIRT (компьютерийн аюулгүй байдлын будлиантай тэмцэх багууд), баталгаажуулж гэрчилгээжүүлдэг байгууллага, мэргэжлийн холбоод, эрдэм шинжилгээний байгууллага, хөндлөнгийн үнэлгээний болон аудитын байгууллага, бүх шатны сургуулиуд г.м.

- ✓ Хувийн хэвшлийн бүх байгууллагын МАБ-ын удирдлагын тогтолцоо

Эдгээр байгууллага бүр кибер орчин дахь гэмт халдлагатай нэгдмэл байдлаар тэмцэхбүтэц, зохион байгуулалтыг бий болгох шаардлагатай.

Энэ бодлого, үйл ажиллагаа нь бие хүнийг, хамт олныг, тодорхой бүлгийг ёс зүй, ёс суртахуун, сэтгэл зүй төлөв байдал, хүсэл эрмэлзлэлийг нийтийн харилцааны зөв чигт чиглүүлэнэ. Ингэснээр нийтлэг ёс журмыг ойлгох, түүнд суралцах, хууль ёсыг хэлбэрэлтгүй хэрэгжүүлэхэд чиглэгдэнэ.

Түүнчлэн нийтийн амьдрал үйл ажиллагааг кибер орчины хөгжлийн чиг хандлагад чиглүүлэх, хууль дэг журмыг хэлбэрэлтгүй сахих, дадал хэвшил сурах, нийтийн өмнө хариуцлага хүлээх үүрэгтэй гэдгийг ойлгуулах явдал байдаг.

Энэ нь кибер орчин дахь гэмт халдлагатай нэгдмэл байдлаар тэмцэхбүтэц, зохион байгуулалтын эрх зүйн зохицуулалтын холбогдолтой олон талын харилцааг хүний ухамсарт суулгахаас гадна зан үйлийг нь сэтгэл зүйн хувьд зохицуулах үйл явц болдог.

Ер нь эрх зүйн нийтлэг зохицуулалт нь нийтийн амьдралын харилцааг журамлах, зохион байгуулах гэсэн 2 хэлбэртэй.

Журамлах гэж хамт олон, бүлэг, бие хүнийг тэдгээрийн зан үйлийг нийтийн харилцааны зөв чигт чиглүүлэх зорилготой.

Харин зохион байгуулах гэж нийтийн амьдрал үйл ажиллагааг олон улсын болон өөрийн улсын хөгжлийн чиг хандлагад чиглүүлэн зохицуулах зорилготой үйл явц.

Иймд шинжлэх ухааны судалгаанд үндэслэсэн бүтэц, зохион байгуулалтын эрх зүйн зохицуулалт нь аливаа хүний хувийн зан байдлыг нийтийн сайн сайхан, тэгш байдлыг хангагч, нийт хүмүүсийн зан төлөвийг өөр хооронд нь тохируулагчийн үүрэг гүйцэтгэх учиртай гэдгийг анхаарах хэрэгтэй.

Ер нь хүн төрөлхтний өв соёл, шинжлэх ухааны ололт амжилт, ёс суртахууны үнэт зүйлийг хадгалах, хамгаалах, хөгжүүлэх зорилгыг заавал биелүүлэх хэм хэмжээнд оруулж, үйл явцыг тэр чигт нь залж байдаг зүйл нь бүтэц, зохион байгуулалтыг зохицуулсан эрх зүйн зохицуулалт гэж үздэг.

Бүтэцэд хамаарч байгаа байгууллага түүний үүрэг бүхий алба хаагчийн ажлын байрны эрх зүйн тодорхойлолт, түүнд тавигдах нийтлэг болон тусгай шалгуур, ажилтны мэдлэг, боловсрол, чадвар, хувийн байдал, хандлага, харилцаа, хамтын ажиллагааны талаар нэгдмэл байдлаар журамласан зохицуулалттай байх шаардлагатай.

Үүний дараа энэ салбарт баримтлаж байгаа бодлого, үйл ажиллагаа нь олон улсын болон өөрийн улсын, тухайн байгууллагын хөгжлийн чиг хандлагад чиглэгдсэн байдлаар зохион байгуулалтад орж, шинжлэх ухааны онол, арга зүйн хийгээд эрх зүй, эдийн засгийн тогтолцоог бий болгох шаардлага бий болсон байна.

Иймээс хууль тогтоох, гүйцэтгэх засаглалын, хууль сахиулах, хуулиар үүрэгжсэн тусгай чиг үүргийн, мэргэжлийн болон төрийн бус, хувийн хэвшлийн бүх байгууллага, иргэдийн кибер аюулгүй байдлыг хангах, хамгаалах салбарт бодлого, үйл ажиллагаа хэрэгжүүлэх бүтэц, зохион байгуулалтыг улам боловсронгуй болгох эдийн засаг, эрх зүйн баталгааг хангах зохицуулалтыг яаралтай бий болгохыг энэ цаг үе шаардаж байна.

Эдгээр байгууллага өөр хоорондоо хамтран ажиллах тогтолцооны талаархи арга зүйн үндэсийг дараагийн бүлэгт илэрхийлнэ.

3.4. Кибер орчинд үйлдэгдэж байгаа гэмт халдлагатай тэмцэх хамтын ажиллагааны үндэс

Дэлхийн улс орнуудад аж үйлдвэржсэн нийгмээс мэдээллэлжсэн эринд шилжих үйл явц улам хурдтай хөгжиж, мэдлэгт тулгуурласан нийгмийг цогцлоон байгуулж, нийгмийн баялаг, үнэт зүйлсийг бүтээх эх сурвалж нь мэдлэг, мэдээлэл гэдгийг дэлхий нийтээр хүлээн зөвшөөрч, улс төр, эдийн засаг, нийгмийн бүхий л хүрээнд мэдээлэл, харилцаа холбооны технологийг өргөнөөр нэвтрүүлэн ашиглаж байна. Дэлхийн олон орон холбоо, мэдээллийн дэд бүтцийг бий болгох үндэсний хөтөлбөрийг дэвшүүлэн хэрэгжүүлж байна.

Тухайлбал өнгөрсөн хугацаанд олон улсад амжилттай хэрэгжсэн Сингапурын “Ухаалаг арал” хөтөлбөр, БНСУ-ын “Мэдээллийн аюулгүй байдлын дэд бүтэц” үндэсний төлөвлөгөө, Малайзын “Мультимедиа супер коридор” хөтөлбөр, Япон улсын “Цахим Япон” зэрэг олон хөтөлбөрийг дурьдаж болно.

Олон улсад “Цахим засаглал” –ыг мэдээлэл, харилцаа холбооны технологийн тэрүүлэх 30 чиглэлийн нэг гэж үздэг бөгөөд төр төвтэй нийгмийг иргэн төвтэй нийгэм бий болгохын тулд төрийн үйлчилгээг иргэд хурдан шуурхай авч, тухайн улсын өнцөг булан бүрт боловсронгуй, үр өгөөжтэй, хүртээмжтэй, ил тод байдлыг хангаж, төрийн үйл ажиллагаанд иргэдийн оролцох бололцоог бүрдүүлэх арга хэрэгсэл гэж үздэг байна.

Ерөнхийдөө олон улс үүнийг нэвтрүүлсэн чиг хандлагаас үзэхэд тухайн мэдээллийг ард иргэдэд **“ТҮГЭЭХ”**, иргэдтэй **“ХАРИЛЦАХ”**, төрөөс **“ЦАХИМ СИСТЕМД СУУРИЛСАН ҮЙЛЧИЛГЭЭ ҮЗҮҮЛЭХ”** гэсэн хэсгүүдэд авч үзэн энэ чиглэлийн дагуу хэрэгжүүлсэн байдаг байна.

Мөн Цахим Засаглал хөтөлбөр хүртээмжтэй байдлын хувьд дараах хэлбэрүүдтэй. Үүнд:

1. C2G (иргэдээс засгийн газар чиглэсэн)
2. G2G (төрөөс төр лүү чиглэсэн)
3. G2C (төрөөс иргэд рүү чиглэсэн)
4. G2E (төрөөс албан хаагчид руу чиглэсэн)
5. G2B (төрөөс бизнесийн байгууллагууд руу чиглэсэн) гэх зэрэг болно.

Олон улсад цахим засаглал

Нэгдсэн Үндэсний Байгууллага болон Дэлхийн Банкнаас жил бүр олон улсын цахим засаглалын хөгжлийн индексийн талаар тайлан гаргадаг бөгөөд уг жагсаалтыг БНСУ тэргүүлэн, Голланд улс удаалж байна. Олон улсын шинжээчид БНСУ-ын хөгжлийг Япон улсын хөгжлийн сайжруулсан хувилбар ч гэж үздэг бөгөөд асар богино хугацаанд мэдээллийн технологийн салбараараа олон улсад яах аргагүй тэргүүлэх байр суурийг эзэлсэн гэж ч сайшаацгаадаг билээ.

2010 оноос хойш тус улс нь 0,9283 индексээр тэргүүлж байгаа бөгөөд, удаах нь 2010 онд 5-р байранд жагсаж байсан Голланд улс 0,9125 индекстэйгээр удаах байрыг тус тус эзэлсэн байна. Харин манай Монгол Улсын хувьд 2010 онд 53-р байранд байсан бол 2012 оны байдлаар 0,5443-ын индекстэйгээр 76-р байранд оржээ. Энэ нь хэдийгээр индексийн хувьд өссөн ч бусад улс орнууд маш эрчимтэй энэ чиглэлээр хөгжиж байгаа гэдгийг харуулж байна.

Уг хөтөлбөрийн хүрээнд дараах үйлчилгээнүүдийг ҮДТ УТҮГ ард иргэдэд хүргээд байна.

Цахим Засаглалын үйлчилгээ

- Замын цагдаагийн бэлэн бус торгуулийн системийн бааз болон холболтууд нь манай байгууллага дээр хийгдсэн бөгөөд уг систем нээгдсэнээр торгуулийн мөнгөн орлого 4 дахин нэмэгдсэн байна. Өмнөх онуудад жилдээ 300 сая төгрөгийн торгуулийн орлого ордог байсан бол энэ торгуулийн систем нэвтэрсэнээр 1.2 тэрбум болж өссөн.

- ТҮЦ машин буюу КИОСК –оор нийтдээ 21 төрлийн үйлчилгээг хүргэж байна. УИХ-тай холбоотой 4 үйлчилгээ, иргэний бүртгэл, гааль, татвар, үл хөдлөх хөрөнгө болон хуулийн этгээдийн лавлагаа, орон сууц захиалах хүсэлт г.м
- Камерийн торгуулийн систем- Замын хөдөлгөөний Удирдлагын төв
- E-immigration–Гадаадын иргэн харъяатын асуудал эрхлэх газар
- Цахим виза- Гадаад харилцааны яам
- Албан журмын даатгал
- Цахим татварын үйлчилгээ –Татварын ерөнхий газар
- Цахим тендер- Худалдан авах ажиллагааны газар

Цахим Засаглалаар тэргүүлэгч эхний 10-н улс орнууд

Country	E-Government 2012	Rank 2012	Rank 2010
Republic of Korea	0.9283	1	1
Netherlands	0.9125	2	5
United Kingdom of Great Britain and Northern Ireland	0.8960	3	4
Denmark	0.8889	4	7
United States of America	0.8687	5	2
France	0.8635	6	10
Sweden	0.8599	7	12
Norway	0.8593	8	6
Finland	0.8505	9	19
Singapore	0.8474	10	11

Монгол Улсын Цахим Засаглалын индекс

Country	E-Government 2012	Rank 2012	Rank 2010
Venezuela	0.5585	71	70
Georgia	0.5563	72	100
Dominica	0.5561	73	105
El Salvador	0.5513	74	73
Grenada	0.5479	75	99
Mongolia	0.5443	76	53
Costa Rica	0.5397	77	71
China	0.5359	78	72
Bosnia and Herzegovina	0.5328	79	74
Turkey	0.5281	80	69

Цаашид үндэсний хэмжээнд кибер орчин, кибер аюулгүй байдлын чиглэлээр үйл ажиллагаа явуулж байгаа төр, хувийн хэвшлийн байгууллагууд хамтран ажиллах эрх зүйн байдал, чиглэлээ нарийн тодорхойлсон цогц төлөвлөгөөтэй батлан хэрэгжүүлэх шаардлага тулгарч байна.

- ✓ Мэдээллийн аюулгүй байдал, сүлжээ, системийн аюулгүй байдлын чиглэлээр мэргэшин ажилладаг төрийн тусгай байгууллагууд,
- ✓ Хууль сахиулах, хяналтын байгууллага
- ✓ Төрийн байгууллага бүрийн МАБ-ын удирдлагын тогтолцоо;
- ✓ Улсын онцгой байгууллагууд

Тухайлбал: Банк, санхүү, татвар, гааль, зэвсэгт хүчин, онцгой байдал, бусад хууль сахиулах байгууллагууд, даатгал, холбоо, төмөр зам, агаарын тээвэр, эрчим хүч, дулаан, эмнэлэг, боловсрол, бүртгэлийн гэх мэт кибер удирдлагын тогтолцоотой байх шаардлагатай гэх мэт/

- ✓ Мэдээллийн аюулгүй байдал, сүлжээ, системийн аюулгүй байдлын чиглэлээр мэргэшин ажилладаг Хувийн хэвшлийн болон төрийн бус байгууллагууд,

Тухайлбал: Мэргэшсэн компани, MonCIRT, CSIRT (компьютерийн аюулгүй байдлын будлиантай тэмцэх багууд), баталгаажуулж гэрчилгээжүүлдэг байгууллага, мэргэжлийн холбоод, эрдэм шинжилгээний байгууллага, хөндлөнгийн үнэлгээний болон аудитын байгууллага, бүх шатны сургуулиуд г.м.

- ✓ Хувийн хэвшлийн бүх байгууллагын МАБ-ын удирдлагын тогтолцооны албадууд зэрэг болно.

Үндэсний байгууллагуудын хамтын ажиллагааны өнөөгийн байдал

Байгууллага, хүний нөөцийн хувьд:

“Мэдээллийн аюулгүй байдлын үндэсний хөтөлбөр”-ийг хэрэгжүүлэх үйл ажиллагааны хүрээнд "Үндэсний Дата Төв" УТҮГ нь 2009 оны 6 дугаар сарын 24-ны өдөр байгуулагдсан, 2011 онд “Кибер аюулгүй байдлын газар” байгуулагдсан, харин ЦЕГ-ын Зохион байгуулалттай

гэмт хэрэгтэй тэмцэх газар /хуучнаар ЭЦГ/ 2 хүний орон тоотой хэсэг /тасаг гэх/, Шүүхийн шинжилгээний хүрээлэнд 2 орон тоо батлан үйл ажиллагаа гүйцэтгэж байна.

Хүний нөөц бэлтгэх, сургалтын хувьд:

Кибер орчны аюулгүй байдлын чиглэлээр хүний нөөц бэлтгэх тогтолцоо, бүтэц, бэлтгэгдсэн багш, сургалтын орчин, суралцагч, сургах хөтөлбөр, дэд бүтэц, хэрэглэгдэхүүн, шинжлэх ухааны чиглэл байхгүй байна.

Хамтын ажиллагааны хувьд:

Улсын хэмжээнд ажиллаж байгаа банк, санхүүгийн байгууллагууд, татвар, гааль, даатгал, интернет үйлчилгээ үзүүлдэг нийт байгууллага, иргэдээс гомдол мэдээлэл хүлээн авч шийдвэрлэж байгаа /Нийслэлийн ЗДТГ гэх мэт/ цөөн байгууллага, КТМС, ХСИС, Үндэсний Дата төв, КАБГ, ХЗҮХ зэрэг байгууллагууд 2009 оноос хойш 8 удаа хамтран ажиллах хүрээнд уулзалт зохион байгуулсан хэдий ч өнөөгийн байдлаар нэгдсэн зохицуулалтгүй, харин ХЗҮХ, ХСИС, Үндэсний Дата төв, КАБГ зэрэг цөөн байгууллага хязгаарлагдмал хүрээнд тус бүр нэг удаа эрдэм шинжилгээний хурал зохион байгуулж, Европын конвенцийн ажлын алба /кибер гэмт хэргийн конвенцийн ажлын алба/, БНСУ-ын криминологийн хүрээлэн зэрэг гадаад улс орны адил чиг үүрэг бүхий байгууллагуудтай хамтран ажиллахаар гэрээ, хэлэлцээр байгуулан ажиллаж байна.

Кибер орчин дахь аюулгүй байдалыг хангах үйл ажиллагаа нь бүх нийтийн оролцоо шаардагддаг учир төр, хувийн хэвшлийн нягт хамтын ажиллагаа, өргөн хэмжээний сургалт, сурталчилгаа, нийтийн ойлголт мэдлэггүйгээр зорилгоо хангаж чадахгүй нь ойлгомжтой.

Мөн “Кибер аюулгүй байдлын 5 дугаар форум” 2014 оны 05 сарын 26-28-нд Улаанбаатар хотноо Кибер орчин дахь аюулгүй байдлыг хангахад тулгамдаж буй асуудал, цаашид кибер аюул заналтай тэмцэх бүс нутгийн хамтын ажиллагааг сайжруулах зорилгоор Мэдээллийн технологи, шуудан харилцаа холбооны газар, Ази номхон далайн бүсийн цахилгаан холбооны байгууллага (АРТ)-тай хамтран уг форумыг зохион байгуулсан.

Форумд Афганистан, Бангладеш, Бутан, БНХАУ, БНАСАУ, БНАЛАУ, Вьетнам, Камбож, Малайз, Малдив, Мянмар зэрэг 20 гаруй орны Мэдээллийн технологи, харилцаа холбооны яамны мэдээллийн аюулгүй байдлын асуудал хариуцсан төлөөлөгч, шинжээчид оролцлоо. Олон улсын байгууллагаас АРТ, Ази номхон далайн бүсийн орнуудын сүлжээ мэдээллийн төв (APNIC), Азийн интернэтийн нийгэмлэг (ISOC), NTT, Хонконгийн Мэдээллийн аюулгүй байдлын мэргэжлийн холбоо (PISA), Токиогийн их сургуулийн төлөөлөгч, эрдэмтэн судлаачид хүрэлцэн иржээ. Манай улсаас Төрийн захиргааны төв байгууллагууд, банк, үүрэн холбооны оператор компаниудын мэдээллийн аюулгүй байдал хариуцсан албан тушаалтан, эрдэмтэн судлаач, инженерүүд оролцлоо.

Боловсролын байгууллагын хувьд:

Их, дээд, МСҮТ, ЕБС-ийн 6 дугаар ангиас эхлэн сургалтын хөтөлбөрт “компьютер” болон “мэдээллийн технологийн”, “Мэдээлэл зүй” сургалт байгаа хэдий ч компьютер техник хэрэгслийн хүрэлцээ муу, хөдөө орон нутгийн хүүхдүүдэд бүр илүү хүндрэлтэй. Оюунтан, сурагчид нь бичвэр шивэх, хүснэгт байгуулах зэрэг алгоритм бичихээс өөр зүйл сургах боломжгүй хөтөлбөрөөр сургалт явуулж байна.

Шинжлэх ухаан мэдлэгийн /онол/ чиглэлийн хувьд:

Өнөөдрийн байдлаар кибер орчины аюулгүй байдлыг хангах, хамгаалах, ёс зүйтэй харилцаа, хандлага, хамтын үйл ажиллагааны чиглэлээр тогтсон мэдлэгийн урсгал, чиглэл, тогтолцоог тодорхой баримтаар үнэлэх боломжгүй байхаас гадна нэр томъёололын хувьд ч тогтсон ойлголт байхгүй байна.

Иймд дээрхи түвшины бүх байгууллага, алба хаагч нарыг энэ салбарын үйл ажиллагаанд нэгдсэн ойлголттой болгон оролцуулах, дотооддоонэгдмэл зохицуулалттайгаар бүгд хамтран ажиллах эрх зүйн зохицуулалтын орчныг бий болгох хэрэгтэй байна.

Кибер орчин дахь гэмт халдлага, довтолгоо нь орон зай, цаг хугацааны хязгааргүй үйлдэгддэг учир олон улсын нягт хамтын ажиллагаа байхгүйгээр тэмцэх боломжгүй.

Энгийн болон тусгай мэргэжлийн сургуулийн чиг хандлага, зорилго нь кибер орчин дахь ёс зүй, сахилга бат, дэг журамыг сургахаар гадна цахим магадлан шинжилгээ, ёс зүйт довтолгоо, хамгаалалт зэрэг цуврал сургалтаар дамжуулан мэдээллийн аюулгүй байдлын ухамсар, ёс зүйг бий болгох, мэдлэг, ойлголтыг нэмэгдүүлэх, улмаар өсвөр залуу үеийнхэнд цахим орчны зөв төлөвшилт бий болгох зорилгоор Мэдээллийн аюулгүй байдлын сургалтыг зохион байгуулах шаардлагатай.

Тухайлбал: Израйл улс өсөн нэмэгдэж буй кибер халдлагуудтай тэмцэх зорилгоор залуучуудыг бэлтгэх “Magshimim Le’umit”үндэсний хөтөлбөр хэрэгжүүл байна[578]. Хөтөлбөр нь 16-18 насны оюуны өндөр чадвартай хүүхдүүдийг элсүүлж, сургах юм байна. Ерөнхий сайд Бинжамин Франклин “Израйл улсад Иран болон бусад улс орнуудаас халдлага ихээр хийгдэж байгаа бөгөөд уг халдлагууд цаашид өсөх хандлагатай байна. Засгийн газрын зүгээс иймэрхүү төрлийн халдлагуудтай тэмцэх чадавхийг Израйлын үндэсний кибер товчоогоороо дамжуулан нэмэгдүүлж байгаа” гэж мэдэгдсэн.

Хэд хэдэн түвшинд нягт хамтран ажиллах шаардлагатай:

- ✓ Эрх зүйн зохицуулалт бүхий заалтуудыг нэг мөр болгох, өөр хооронд нь уялдуулах,
- ✓ Хууль тогтоогчдын түвшний хамтын ажиллагааг идэвхижүүлж, нэг зорилгод чиглүүлэх,
- ✓ Олон улсын гэрээ, конвенцийн түвшинд хамтрах,
- ✓ Гэмт халдлагыгмөрдөн шалгах, эх сурвалжийг олж тогтоох, гэмт этгээдийг илрүүлэх баривчлах чиглэлээр Засгийн Газар хоорондын болон хууль хяналтын байгууллагуудын хамтын ажиллагааг бий болгох
- ✓ Мэдээллийн аюулгүй байдал, сүлжээ, системийн аюулгүй байдлын чиглэлээр мэргэшин ажилладаг Хувийн хэвшлийн болон төрийн бус байгууллагуудын хамтын ажиллагааг идэвхижүүлэх.
- ✓ Сургалтын байгууллагууд болон эрдэмтэд, судлаач нарын судалгаа шинжилгээ, хамтын ажиллагааг дэмжих
- ✓ Хувь хүмүүсийн түвшний харилцаа, хамтын ажиллагаа, ёс зүйн асуудлыг хууль зүйн хүрээнд дэмжин зохион байгуулах, хамтын ажиллагааг улам боловсронгуй болгох шаардлагатай.

[578] The Jerusalem Post-д мэдээлсэн

БҮЛЭГ IV. КИБЕР ОРЧИНД ҮЙЛДЭГДЭЖ БУЙ ГЭМТ ХЭРГИЙГ ШАЛГАН ШИЙДВЭРЛЭХ ТОГТОЛЦООГ БОЛОВСРОНГҮЙ БОЛГОХ АРГА ЗАМ

4.1. Эрх зүйн тогтолцоог боловсронгуй болгох нь

Кибер орчин нь өөрөө олон соёл иргэншилүүд хил дамжин уулзаж улмаар өөр өөр эрх зүйн зохицуулалт дэгүүд хооронд зөрүү гарч олон асуудлыг дагуулж байна. Эдгээр тулгамдсан асуудлыг хөгжлийг чиг хандлагад нийцүүлэн эрх зүйн уламжлалуудыг хооронд нь уялдуулан олон улсын нэгдмэл эрх зүйн зохицуулалтын дагуу чиглүүлэх шийдвэрлэх цаг үе ирлээ.

Монгол Улсад 1992 оноос эхлэн эрх зүй, эдийн засаг, улс төр, боловсролын талаар төрөөс баримтлах суурь бодлогыг шинэчлэх зайлшгүй хэрэгцээ, шаардлагын үүднээс салбар бүрийн шинжлэх ухааны урсгал, чиглэлд эрс өөрчлөлт бий болж хэрэгжиж байгаа ба кибер орчины аюулгүй байдлын чиглэлээр хүчин төгөлдөр мөрдөгдөж байгаа хуулийн 22 /хамааралтай заалт 1-14/ буюу 4,5 хувь, УИХ-ын тогтоолын 6 буюу 12 хувь, Засгийн газрын тогтоолын /хүчинтэй байгаа/ 12 орчим буюу 1 хувь орчим нь кибер орчны харилцааг зохицуулах зорилготой байгаа нь туйлын өсөн нэмэгдэж байгаа харилцааг иж бүрэн зохицуулахад дутагдалтай байна.

“Үндэсний аюулгүй байдлын үзэл баримтлал” 1994 онд 9 багц асуудлаар батлан хэрэгжүүлж байсан бол харин 2010 оны 07 сарын 05-ны өдөр 6 багц асуудлаар шинэчлэгдсэн, мөн Засгийн газрын 2010 оны 06 сарын 02-ны өдөр 141 дүгээр тогтоолоор 4 багц асуудлаар “Мэдээллийн аюулгүй байдлын үндэсний хөтөлбөр” батлагдаж хүчин төгөлдөр мөрдөгдөж байна.

Тиймээс 1994 оноос эхлэн улам хурдацтай өсөж буй киберорчины ирээдүйн орон зай, хэрэглээ, оролцогчдын үйл ажиллагаа, ёс зүйн хандлагыг“Ирээдүй судлал”-ын (**Futurology**) шинжлэх ухааны үүднээс суурь бодлоготой, эрх зүйн зохицуулалттай хөгжүүлбэл тус салбар нь хүн төрөлхтний өв соёл, харилцан ойлголцол, хөгжил дэвшлийн хүч болон урагшилсаар байх болно.

Манай улсын хууль санаачлах, хууль тогтоох байгууллага нь аливаа хууль, тогтоомж боловсруулах, батлах, мөрдүүлэхдээ хэтийн бодлого, үзэл баримтлалын тогтсон чиглэлгүй, инновацийн үйл ажиллагаа-үйл явцад тулгуурлахгүй зөвхөн тоонд анхаарч ирсэн нь харамсалтай.

Өмнөх 3 дугаар бүлэгт дурьдсан асуудлыг шинжлэх ухааны үндэслэлтэйгээр журамлах, зохион байгуулах бодлого, үйл ажиллагааны эрх зүйн зохицуулалтыг дараах чиг хандлагад уялдуулах шаардлага нэгэнт бий болжээ.

Хууль батлан хэрэгжүүлэх үндсэн зарчим нь олон улсын хэмжээнд дараахь байдлаар илэрхийлэгдэх хандлага ажиглагдаж байна.

1. **Nullum crimen sine lege**буюу гэмт хэрэг гэж хуульчлаагүй л бол гэмт хэрэг гэж үзэж болохгүй өөр зохицуулалттай байх зарчим,
2. **Gogitations poenam nemo patitur** буюу аливаа хүн үзэл бодол, итгэл үнэмшилтэй байх жам ёсны эрхтэй бөгөөд түүнийхээ төлөө хариуцлага хүлээхгүй байх зарчим,
3. **Ultima ratio**буюу гарцаагүй онц ноцтой зөрчилд заавал ял, хариуцлага хүлээдэг байх зарчим,
4. **Habeas corpus** буюу аливаа хүн халдашгүй байх бөгөөд хуулиас гадуур хэнийг ч мөрдөн мөшгөж эрх, эрх чөлөөнд нь халдахгүй байхгэсэн олон улсын тулгуур зарчмыг заавал баримтлах шаардлагатай болсон.

2012 онд батлагдсан Инновацийн тухай хуульд “инновацийн үйл ажиллагааны зарчим, удирдлага, зохион байгуулалт, санхүүжилт, төрийн дэмжлэг, оюуны өмчийг эдийн засгийн эргэлтэд оруулан эзэмших, ашиглах, эрх зүйн үндсийг тогтоохтой холбогдсон харилцаагзохицуулахад оршино”[579] гэжээ.

[579]www.Legalinfo.mn., “Инновацийн тухай Монгол Улсын хууль”, 2012.05.22.

Инновацийн тухай хуулийг батлан мөрдөж байгаа нь сайн хэрэг боловч хууль тогтоох, хүний эрүүл мэнд, сэтгэл зүйн цогц судалгаа, шинжилгээний талаар инновацийн үйл ажиллагаа **огт тусгаагүй нь эрх зүйн шинэтгэлийн үйл явц дахь сөрөг хүчин зүйлийг бий болгох магадлал ихэссэн гэж үзэх үндэстэй.**

Эрх зүйн шинэтгэл нь эрх зүйн тогтолцоог улам боловсронгуй болгох, хууль ёс, сахилга батыг бэхжүүлэх, эрх зүйн зохицуулалтын үр нөлөөг сайжруулах, хүний эрх, эрх чөлөө, язгуур ашиг сонирхол, үнэт зүйлийг баталгаатай хангах, хамгаалах, нийтийн амьдралд эрх зүйн сэтгэлгээ, ухамсар, соёл, хэв шинж, уламжлалыг бүрэлдүүлэх, нийт хүмүүст хууль ёсыг ягштал биелүүлэх сэтгэлгээ, уламжлалыг төлөвшүүлэн тогтоох зорилтод чиглэсэн цогц үйл ажиллагаа ажиллагаа байдаг[580].

Энэхүү цогц үйл ажиллагаа нь эрх зүйн шинэтгэлийн зорилтыг хангахад чиглэгдэнэ.

Эрх зүйн соёл, уламжлал төлөвшсөн ихэнх улс оронд ямар салбарт эрх зүйн зохицуулалт шаардлагтай байгааг судалгаа, шинжилгээний /инновацийн тогтолцоонд/ дүнд үндэслэлтэй тогтоох зорилготой цогц үйл ажиллагаа хэрэгжүүлсэний дараа тухайн салбар өөрөө өөрийгөө засан тохинуулах зохицуулалт бүхий иргэншсэн, итгэл үнэмшилтэй хууль хэрэгжүүлдэг.

Энэ үйл ажиллагаа нь тодорхой үе шат дамжин хэрэгждэг.

1. Тухайн салбарт эрх зүйн зохицуулалт шаардлагатай байна гэж үзвэл хараат гарал үүслийн хуулийн дагуу өргөн хүрээнд хамруулан судласны дараа төр-засгаас баримтлах хэтийн бодлогын баримт бичиг боловсруулан баталдаг (40 /50/, 100 жилийн баримжаатай)

(энэ хугацаандаа сургалт, судалгаа, сурталчилгаа, эрдэм шинжилгээний байгууллагатай хамтран ирээдүй судлалын үйл ажиллагаа явуулах),

2. Тухайн салбарын үйл ажиллагааны хэтийн төлөвийг тодорхойлсон ерөнхий болон тусгай хөтөлбөрийг бодлогын баримт бичигт үндэслэн боловсруулан батлан, хэрэгжүүлдэг (4-8 жилийн баримжаатай)

(сургалт, судалгаа, сурталчилгаа, техник-технологид тулгуурлан бодит үйл ажиллагаа эхэлдэг),

3. Салбарын ерөнхий хууль баталдаг. Энэ хуулийг дээрхи бодлогын баримт бичгийн хүрээнд хэрэгжүүлсэн хөтөлбөрийн үр дүнд гарсан үзүүлэлт, хамаарах асуудлыг зохицуулах чадвартай нийтлэг харицааг зохицуулахуйц байхаар батлан хэрэгжүүлдэг. (20-40 жилийн баримжаатай)

(маш сайн судалж, шинжилсэний дүнд судлагдсан нөхцөлийн дагуу тухайн салбарын үйл ажиллагааг хэрэгжүүлэх байгууллага байгуулах, хүний нөөц, технологи, техник гарах үр дүн, өрсөлдөх чадвар зэргийг тооцсон байх),

4. Тухайн салбарт шаардлагатай салбар /органик/ хуулиуд батлах, хэрэгжүүлэх (4-20 жилийн баримжаатай)

(судлагдсан нөхцөлийн дагуу хэрэгжүүлэх байгууллага байгуулах, хүний нөөц, технологи, техник хэрэгслээр хангах, гадаад дотоод хамтын ажиллагаа гэх мэт) гэсэн өөр хоорондоо нягт харилцан хамааралтай, салшгүй нийтлэг шинжтэй, ухаалаг технологитой[581].

Ер нь инновацийн үйл ажиллагаанд тулгуурлан үндэслэлтэй боловсруулагдсан хууль, тогтоомжийн эцсийн зорилго хүмүүсийн хоорондын үйл ажиллагааг зохицуулах, хүн бүрийн эрх, эрх чөлөөг баталгаатай хангах, хамгаалах арга хэрэгсэл учир хууль батлах, мөрдүүлэх технологи үйл ажиллагаа нь маш энгийн, ойлгомжтой, үр дүн сайтай төдийгүй тухайн хуулийн үр дүнг хамгаалах, итгэл үнэмшил эрмэлзлэлийг нийт хүмүүст аяндаа төлөвшүүлэх хандлага байдаг.

---

[580] Л.Цогтбаяр, “Mindset facing problems, discussing ways, and tendencies on the environment of legal reform” ХСИС-ийн ЭШ-ний хурлын илтгэл, 2014., УБ,

[581] **Технологи** гэсэн үг нь эртний Грекийн үр чадвар, арга барил гэсэн үг аж. Монголчууд эрт дээр үеэс аливаа ажил үйл ажиллагааг хэрэгжүүлэх тохирсон арга ухааны цогц ойлголтоор ойлгож ирсэн,Харин өнөөдөр аливаа үйл ажиллагаа хэрэгжүүлэхдээ төлөвлөгөө гаргах, хөтөлбөр боловсруулах, үйл ажиллагааны зорилго, зорилт, чиглэл, оролцогчид, үр дүнг тодорхойлох, сургах, мэдээллэх зэрэг өөр хоорондоо хамаарах үйл явцыг зөв зохион байгуулах арга ажиллагааг багтаасан цогц ойлголт мөн.

Монгол Улсын Үндсэн хууль[582]-ийн 1 дүгээр зүйлийн 2 дахь хэсэгт “Ардчилсан ёс, шударга ёс, эрх чөлөө, тэгш байдал, үндэсний эв нэгдлийг хангах, хууль дээдлэх нь төрийн үйл ажиллагааны үндсэн зарчим мөн”гэж заасан нь засгаас бодлого шийдвэр батлан, хэрэгжүүлэхдээ инновацийн үйл ажиллагаанд тулгуурлах шаардлагатайг илэрхийлсэн ойлголт мөн гэх үндэстэй.

Засгаас хэрэгжүүлж байгаа бүхий л үйл ажиллагаа инновацийн үйл ажиллагаанд тулгуурласан суурь болон салбарын хэрэглээний судалгаа, шинжилгээний үр дүн байх ёстой.

Тухайлбал:

1. Байгаль, нийгмийн талаас үндэслэл сайтай,
2. Шинжлэх ухааны орчин үеийн арга, технологи ашигласан, үндэслэлтэй,
3. Зорилготой, тогтвортой,
4. Үндэсний болон олон улсын эрх зүйд нийцсэн,
5. Бусад хууль, тогтоомжтой уялдаа холбоо сайн, харилцан нөхцөлдсөн,
6. Нийтийн амьдрал үйл ажиллагаанд бүрэн тохирч нөхцөлдсөн,
7. Бодитой, амьдрах чадвартай, алсын хараатай,
8. Нийтийн эрх ашиг, шударга ёсонд үндэслэсэн,
9. Тодорхой, ойлгомжтой, иргэдийн хүсэлд тохирсон итгэл, үнэмшилтэй,
10. Засаглалын болон байгууллага, хамт олон, иргэдийн ашиг сонирхолыг тэгш тэнцвэртэй хослуулж хангасан,
11. Оролцогч нарын сэтгэц зүйд нөлөөлсөн зэрэг орон зай, цаг хугацаа, тоон ба чанар, агуулга ба хэлбэртэй байх үзэл санаанд үндэслэгдсэн байх учиртай.

Эрх зүй, шударга ёс хөгжсөн улс орны иргэдийн ой ухаанд ёс суртахууны /стандарт/ нийтлэг хэм хэмжээ, соёл, хэвшил эцэг эх, хоорондын харилцааны явцад нэгэнт суучихсан байдаг.

Ийм нэгдмэл үйл ажиллагаа байхгүйгээр ямар ч сайн хууль, тогтоомж батлан, хэрэгжүүлж, хатуу чанд дэг журам тогтоолоо ч ёс суртахуунгүй, бусармаг үзэгдэл, үйл ажиллагаа амь бөх оршсоор байдгыг хүн төрөлхтний түүх гэрчилнэ.

Харин эрх зүйн шинэчлэлийг инновацийн үйл ажиллагаанд тулгуурлан үндэслэлтэй зохион байгуулж хэрэгжүүлэхдээ хүмүүсийн ой ухаан, сэтгэл санаанд нөлөөлж, үнэн зөв ухуулан таниулах аваас хууль-эрх зүй муу байсан ч сайн талаас нь хүлээн авч хэрэгжүүлэх хүсэл зориг, сэтгэл санаа, тархи оюуны өгөгдөл аяндаа бий болох зүй тогтолтой.

Монгол Улсын цахим засгийн харилцан нийцэл, мэдээллийг хамтран ашиглах боломжийг бий болгохын тулд хууль зүйн дараах асуудлыг шийдэх шаардлага тулгарна:

- Мэдээллийн аюулгүй байдлын ерөнхий хууль гаргах
- Цахим засгийн хууль боловсруулж батлах
- Цахим гарын үсгийн хууль /бүх салбарт хэрэглэгдэх зориулалттай/ гаргах
- Өгөгдөл хамгаалах тухай хууль гаргах
- Төрийн байгууллагуудын хооронд өгөгдөл, мэдээллийг хамтран ашиглах зохицуулалтын үндсийг бий болгох
- Цахим баримт бичгийг хууль ёсны шинжийг баталгаажуулсан зохицуулалт, хууль ёсны байхад тавигдах шаардлагууд.
- Цахим баримт бичиг хөтлөлт, архивын зохицуулалт
- Цахим халдашгүй байдал, цахим орон зайн аюулгүй байдлыг хангах зохицуулалт
- Цахим төлбөр тооцооны зохицуулалт
- Кибер гэмт хэрэг, цахим өгөгдөл болон сүлжээнд халдсан бусад төрлийн гэмт хэргийг тодорхойлсон эрүүгийн хуулийн зохицуулалт
- Өгөгдөл мэдээлэл солилцох, хамтран ашиглах төрөл бүрийн дэг, журмууд гэх мэт.

[582]Монгол Улсын Үндсэн хууль 1992 он

Дээрх хийгдсэн судалгаа, бусад улсын туршлага, өнөөгийн хэрэгцээ шаардлага, төслийн зорилго, зорилтын дагуу дараах стандарт, журам, дүрэм, зохицуулалтын төслийг боловсруулж батлах шаардлагатай. Үүнд:

- Төрийн өгөгдөл мэдээллийг хамтран ашиглах стратеги
- Төрийн мэдээллийн нэгдсэн санд хандах хандалтын стандарт
- Төрийн мэдээллийн ангилал ба төрөлжүүлэлтийн стандарт
- Төрийн мэдээллийг загварчлалын стандарт
- Платформын дэд бүтцийн стандарт
- Мастер кодын стандарт
- Төрийн мэдээллийн ангилал болон нэгдсэн кодчилолын үндсэн тогтолцооны дүрэм

Дээрх дүрэм, журам, стандартуудыг боловсруулахдаа төрийн өгөгдөл мэдээллийн нэгдмэл санд хандах, хамтран ашиглахад баримтлах дараах зарчмуудыг баримтална:

- Нээлттэй байх
- Уян хатан байх
- Ил тод байх
- Хуульд нийцсэн байх
- Оюуны өмчийг хамгаалах
- Хувийн халдашгүй байдал, өгөгдлийн нууцыг хангах
- Албан ёсны үүрэг, хариуцлага хүлээсэн байх
- Мэргэшсэн байх
- Харилцан уялдаж нийцсэн байх
- Чанартай байх
- Аюулгүй байлдлыг хангасан байх
- Үр нөлөөтэй, үр дүнтэй байх
- Тайлагнадаг байх
- Тогтвортой байх

Төрийн баримт бичгийн нэгдсэн кодчилол, инжинеринг хийх асуудлыг харгалзан үзсэн. Нэгдмэл кодчилолыг хэрэгжүүлэхийн тулд баримт бичгийн инжинеринг хийх шаардлага тулгардаг. Баримт бичгийн инжинеринг нь баримт бичгийг үүсгэж, ашиглаж буй үйл явцыг тодорхойлох, зохиомжлох, хэрэгжүүлэхэд тусална. Энэ хүрээнд бизнес үйл явцын шаардлагын дагуу төрийн баримт бичгийн тодорхойлолт, загварыг тодорхойлох ёстой.

Мөн байгууллагын хоорондын мэдээллийн урсгалыг хөнгөвчлөх үүднээс үйл явцуудыг уялдуулах дүрэм хамрагдана.

Мэдээллийг хамтран ашиглах, харилцан уялдаа, нийцлийг бий болгоход

- Дээд түвшин (бодлого журам)
- Захиргааны түвшин (үйл явц, архитектур)
- Үйлчилгээний түвшин (бүтэц, харьцаа, буцах холбоо)
- Технологийн түвшин (холболт, харилцаа холбоо)
- Бүх шатны сургалтын байгууллагууд болон ажлын байрны үргэлжилсэн сургалтын түвшинд шинжлэх ухааны үндэслэлтэй харилцан нийцэл, уялдааг бий болгох, асуудлыг журмуудад зохих хэмжээнд тусгаж өгөх гэх мэт.

Европын Консулын газар нь 1949 онд байгуулагдаж, дэлхийн 47 орон гишүүнээр элссэн олон улсын томоохон байгууллага бөгөөд тус газраас 2001.11.23-нд батлагдсан, 2004 оны 7-р сарын 1-нд хүчин төгөлдөр болсон Цахим гэмт хэргийн тухай конвенц (Европын зөвлөл, Европын гэрээний цуврал, №185) нь цахим гэмт хэрэгтэй тэмцэх олон улсын эрх зүйн зохицуулалт бөгөөд Будапештийн конвенцид одоогоор дэлхийн интернэтийн хөгжлөөр тэргүүлэгч 55 улс нэгдэн орсон бөгөөд бусад олон орон өөрийн орны хууль тогтоомждоо авч хэрэгжүүлдэг томоохон хэмжээний олон улсын эрх зүйн акт аж.

Монгол Улсын Их Хурлаас 1993 онд батлан, өнөөдөр хүчин төгөлдөр мөрдөж байгаа Монгол Улсын олон улсын гэрээний тухай хуулийн дагуу дээрхи олон улсын эрх зүйн баримт бичиг болох конвенцид нэгдэн орох шаардлагатай.

Мэдээллийн технологийн өндөр хөгжилтэй зарим нэг орны хууль тогтоох байгууллагууд кибер аюулгүй байдлын хуулийн төсөлд дараах зохицуулалтыг хуульчлах гэж байгааг манай улс ч гэсэн тусган авч хууль санаачлахыг санал болгож байна.

Төлөвлөгөө нь дор дурдсан хэсгүүдтэй:

Нийт иргэдийг хамгаалах

1. Үндэсний хэмжээнд мэдээлэл ил болгохыг тайлагнах (National Data Breach Reporting)
2. Компьютерийн гэмт хэрэгтнүүдэд шийтгэл оногдуулах (Penalties for Computer Criminals)

Үндэсний онц чухал дэд бүтцийг хамгаалах

1. Хувийн хэвшил, төр, орон нутгийн засгийн газруудад Засгийн газраас сайн дурын тусламж үзүүлэх (Voluntary Government Assistance to Industry, States, and Local Government)
2. Хувийн хэвшил, төр, орон нутгийн засгийн газруудтай сайн дурын байдлаар мэдээлэл солилцох (Voluntary Information Sharing with Industry, States, and Local Government)
3. Онц чухал дэд бүтцийн кибер аюулгүй байдлын төлөвлөгөөнүүд (Critical Infrastructure Cyber Security Plans)

Засгийн газрын компьютер, сүлжээг хамгаалах

1. Удирдлага (Management)
2. Хүний нөөц (Personnel)
3. Халдлагаас сэргийлэх системүүд (Intrusion Prevention Systems)
4. Дата төвүүд (Data centers)

Хувийн хэвшлийн болон бусад байгууллагуудын мэдээллийн аюулгүй байдлыг хамгаалах

1. *Мэдээллийн аюулгүй байдлын удирдлага*
2. *Хүний нөөцийн бүрэлдэхүүн*
3. *Байгууллагын нууц,*
4. *Байгууллагын мэдээллийн аюулгүй байдал*
5. *Халдлагаас хамгаалах, мэдээллэх*

Хувь хүниймэдээллийн аюулгүй байдлыг хамгаалах

1. *Хувь хүний хувийн нууц, иргэний нэр төрийг хамгаалах*
2. *Кибер орчины ёс зүй, боловсролын талаархи сургалт*
3. *Халдлагаас хамгаалах, мэдээллэх зэрэг шинэ иж бүрэн тогтолцоог боловсронгуй болгох шаардлагатай.*

Кибер орчин дахь гэмт халдлага, гэмт хэргийн бүтцэд нөлөөлж байгаа хоёр өөр хүчин зүйл нь теник технологийн хурдацтай хөгжил, туршлагагүй хэрэглэгч олширч байдаг хил хязгааргүй сүлжээний тархалтыг заавал тооцоолж зэрэглэлийг бий болгох шаардлагатай болжээ.

Кибер орчины өнөөгийн бодит байдал нь хүн төрөлхтний өдөр тутмын амьдрал, үйл ажиллагаанд төдийгүй хууль эрх зүйн орчинд тархсанаар эрх зүйн цоо шинэ салбарыг бий болгох цаг нэгэнт бий болсон учир үндэсний хууль тогтоомж, олон улсын эрх зүйн хэм хэмжээний үндсэн зарчмыг бариmтлан эрх зүйн тогтолцоог боловсронгуй болгох нь чухал.

4.2. Чиг үүрэг бүхий байгууллагын тогтолцоог боловсронгуй болгох нь

Кибер орчин дахь гэмт халдлагатай тэмцэх үүрэгжсэн байгууллагуудын бүтэц, зохион байгуулалт, хүний нөөц, техник хэрэгсэл, арга зүйн тогтолцоо нь мэдээллийн аюулгүй байдлын салбарын хамгийн чухал хэсэг мөн.

Иймд энэ салбарын байгууллагуудын тогтолцоог сайжруулах эдийн засаг, хүний нөөц, эрх зүйн орчны өнөөгийн байдал сул, хангалттай биш байгаа тул цаашид шинээрцогц зохицуулалтыг яаралтай бий болгох шаардлагатай байна.

Чиг үүрэг бүхий байгууллагууд:

- ✓ Цагдаа,
- ✓ Тагнуул,
- ✓ Шүүхийн шинжилгээний байгууллага,
- ✓ Мэргэжлийн бусад байгууллагууд

Тухайлбал: Мэргэшсэн компани, CSIRT компьютерийн аюулгүй байдлын будлиантай тэмцэх багууд, баталгаажуулж гэрчилгээжүүлдэг байгууллага, мэргэжлийн холбоод, эрдэм шинжилгээний байгууллага, хөндлөнгийн үнэлгээний болон аудитын байгууллагууд г.м.

- ✓ Мэдээлэл, шуудан, харилцаа холбооны газар,
- ✓ Харилцаа холбооны зохицуулах хороо,
- ✓ Интернет үйлчилгээ үзүүлдэг байгууллагууд,
- ✓ Их, дээд сургуулиуд /МТ-ийн чиглэлээр сургалтын үйл ажиллагаа эрхэлдэг болон эрх зүйн чиглэлээр сургалтын үйл ажиллагаа эрхэлдэг/

Одоо интернет үйлчилгээ үзүүлдэг тогтолцоо хувийн хэвшилд байгаа тул кибер орчин дахь мэдээлэл хамгаалах, мэдээлэл хуваалцах, эд мөрийн баримт олж авах, мэдээлэл хадгалах зэрэг олон асуудал нь төр хувийн хэвшилийн хамтын ойлголцол, хамтын ажиллагаагүйгээр үр дүнд хүрэхгүй.

Судлаачид “компьютерийн гэмт хэрэг”-ийг олон янзаар тодорхойлдог бөгөөд нэгдсэн ойлголтод хүрч чадахгүй байна. Энэ нь “компьютерийн гэмт хэрэг” гэсэн нэр томъёог “компьютерийн мэдээллийн хүрээн дэх гэмт хэрэг”, “компьютерийн мэдээллийн аюулгүй байдлыг эсрэг гэмт хэрэг”, “компьютер ашиглахтай холбоотой гэмт хэрэг” зэрэг олон янзаар нэрлэж байгаатай холбоотой юм.

Судлаачдын судалгааны үр дүн, “компьютерийн гэмт хэрэг”-тэй тэмцэж буй бусад улсын туршлагыг харгалзаж хууль зүйн онол, практикт ач холбогдолтой криминалистикийн “тусгай” аргачлал боловсруулах, хэрэгжүүлэх үүднээс авч үзвэл “компьютерийн гэмт хэрэг”-т компьютерийн мэдээлэл, түүний орчинд компьютерийн технологийг ашиглан үйлдсэн гэмт хэргийг хамааруулж үзэх нь зүйтэй.

Энэ нь НҮБ-ын шинжээчдээс санал болгож буй жишиг зааварчлагатай нийцсэн байх нь чухал. Үүнд:

1. компьютерийн систем, түүний тусламжтай үйлдэгдэж болох;
2. компьютерийн систем, сүлжээний орчинд гарч болох;
3. компьютерийн систем, сүлжээний мэдээллийн аюулгүй байдлын эсрэг үйлдэж болох бүх төрлийн гэмт хэрэгт хамаарна гэсэн.

Кибер гэмт халдлагыг тодорхойлох шалгуурыг нэг мөр томъёолох шаардлагатай.

Компьютерийн гэмт хэргийн эрүүгийн эрх зүйн ойлголт чухал.

Үүнийг компьютерийн мэдээлэл боловсруулах систем, түүний орчинд улс, нийгэм, иргэн, хуулийн этгээдийн хуулиар хамгаалагдсан эрх, ашиг сонирхлын эсрэг компьютерийн технологийг ашиглан үйлдсэн эрүүгийн хуульд заасан нийгэмд аюултай, гэм буруутай үйлдэл (эс үйлдэхүй) гэж үзэж болох юм.

Компьютерийн гэмт хэргийг криминологийн шинжээр нь эдийн засгийн, хувийн эрх чөлөө, халдашгүй байдлын эсрэг, нийгэм, улс орны ашиг сонирхлын эсрэг гэж ангилж болно.

Орчин үед үзэл бодлоо илэрхийлэх эрх чөлөөний зарчмыг уламжлалт хэвлэл мэдээллийн хэрэгслээс гадна Интернэтэд бас баримтлах ёстой гэсэн хөдөлгөөн дэлхий дахиныг хамарч эхлээд байгаа юм. Интернэт эрчимтэй хөгжин тархаж байгаа өнөө үед «кибер орчин» хэмээх мэдээллийн маш том ертөнц бий болсон.

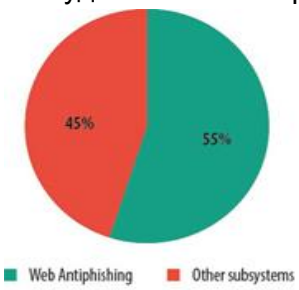
1995 онд дэлхийн хүн амын дөнгөж нэг хувь нь Интернэтэд холбогдсон байсан бол одоо энэ тоо 40 хувь буюу 3 тэрбумд хүрээд байна.

Монгол Улсад Интернэт хэрэглэгчдийн тоо сүүлийн 3 жилд 320 хувь өсч, 2013 оны байдлаар 841 мянгад хүрсэн байна. Энэ бол нийт хүн амын 30 гаруй хувь нь Интернэтэд холбогдсон гэсэн үг. Нөгөө талаар манай оронд Интернэт гэх сая гаруй уншигчтай хэвлэл, мэдээллийн том орон зай болжээ.

Кибер орон зайд дараах халдлага үйлдэгдэх нийтлэг хандлага байгаа тул чиг үүргийн байгууллагууд, хэрэглэгч байгууллага, хувь хүмүүсийн мэдээлэлд хандах хандлага, мэдээллэх тогтолцоог энэ чигт зохион байгуулах хэрэгтэй.

Жишээ нь:

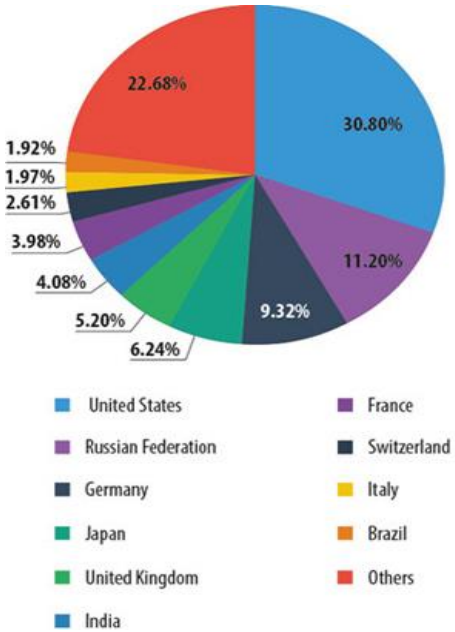
Хэрэглэгчийн санхүүгийн өгөгдөл мэдээ мэдээллийг хулгайлахын тулд фишингийн аргыг ашигладаг нь цахим халдлагын судалгаанаас илэрхий болжээ.



Халдлага ба хэрэглэгчид: Фишингийн өгөгдлийн сан нь тухайн хэрэглэгчийн компьютерт хадгалагддаг бөгөөд энэ нь өгөгдлийн санг идэвхитэй болгох холбоосуудыг агуулдаг байна. 2013 оны байдлаар фишинг халдлага нь дараахь хувьтай байгааг харуулсан бөгөөд нийт халдлагын 55 хувь вэб антифишинг, үлдсэн 45 хувь нь бусад системүүд гэжээ.

Тус лабораторийн судалгаагаар 2013 онд 39,6 сая хэрэглэгчид фишинг халдлагатай нүүр тулсан бөгөөд 2012 оныхоос 2,32 хувиар илэрхий өссөнийг Касберскай лабынхан олж илрүүлсэн байна.

2013 оны байдлаар санхүүгийн чиглэлээр цахим халдлагад өртсөн улс орнууд



Өнгөрөгч 2013 дээрхи байдал нь нилээн өөрчлөлттэй гарсан хэмээн Касперскайгийн шинжээчид үзэж байгаа юм.

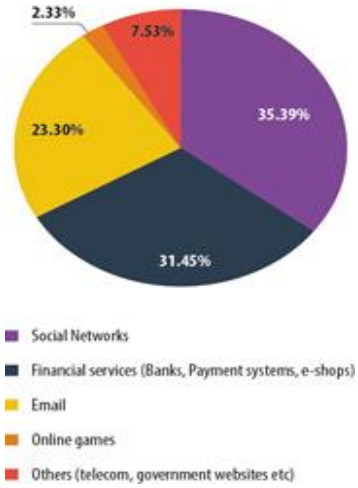
Тухайлбал: ОХУ-ын хэрэглэгчид АНУ-ын цахим хэрэглэгчидтэй харьцуулахад 9,19 хувиар бага байгаа юм.

Харин АНУ-ын уг өөрчлөлт нь 2013 онд 30,8 хувь, 2012 онд 17,56 хувьтайгаар тус тус нэмэгдсэн байна. Харин ХБНГУ-ын статистик үзүүлэлт нь 9,32 хувь, 5,83 хувь зэргээр өмнөх оныхоос бага зэрэг өссөн байна. Дээрхи улс орнуудын статистик мэдээллээс үзэхэд харьцангуй ихэнхи улс орнууд нийтдээ халдлагын тоо хэмжээ буурсан байгаа бөгөөд энэ нь

цогц хэмжээний домэйн нэрийн бүртгэлийн үйл явц, цахим гэмт хэрэгтэй холбоотой хүчин зүлйсийг сайтар судалж дүгнэсний үр дүнд сайн чанарын хамгаалалтын бүтээгдэхүүн ашиглаж, тухай бүрд арга хэмжээ сайн авч байгаад хамаг учир байгаа аж.

Ерөнхийдөө дэлхий даяар интернэт хэрэглэгчидийн тоо өсч байгаа нь төрөл бүрийн цахим хуудас, сошиал сүлжээний сайт, онлайн шоппинг ихэссэнтэй холбоотой. Ихэнхи хүмүүс интернэт орчинд төрөл бүрийн цахим хуудаснаас янз бүрийн файл, аппликейшн суулгаж, татах нь фишинг төрлийн халдлагад өртүүлэх үндсэн гол шалтгаан ч болж байгаа гэж үзэж байна.

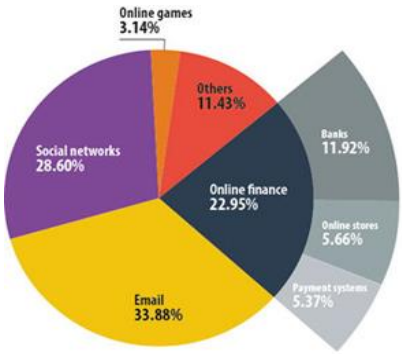
Фишинг юуг онилж байна вэ?



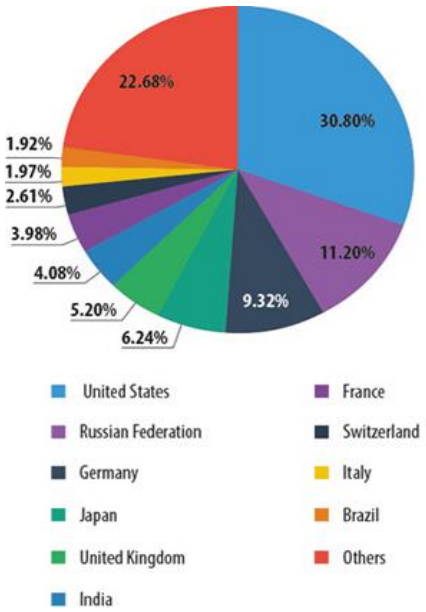
2012 онтой харьцуулахад энэ төрлийн халдлага эрс өссөн бөгөөд графикийн байдлаас үзэхэд хамгийн дээгүүр жагсаж байгаа нь сошиал сүлжээ 35,39 хувь, банк санхүүгийн байгууллагын үйлчилгээ буюу /банк, төлбөр тооцооны бүхий л систем, цахим дэлгүүр/ зэрэг нь 31,45 хувь, дараагаар нь имэйл 23,3 хувь, 2,33 хувьтай буюу хамгийн бага үзүүлэлттэй нь онлайн тоглоом, 7,53 хувь нь харилцаа холбоо, төрийн байгууллагуудын цахим хуудаснууд орсон байна. Ялангуяа онлайн тоглоомын үзүүлэлт нь 2012 оны үзүүлэлтээс 3,14 хувиар, имэйлийн үйлчилгээнээс ирүүлэх хуурамч мэдээлэл, вирус зэргээс үүдэх халдлага 10,5 хувь, мөн цаашлаад 8,5 хувиар тус тус буурсан явдал байлаа.

Санхүүгийн байгууллагуудын санаа зовж буй асуудлууд:

Санхүүгийн байгууллагуудын хувьд хамгийн их санаа зовоож байгаа асуудлууд нь хуурамч банкны төлбөр тооцооны систем, онлайн банкны цахим хуудсууд нь 11,92 хувь, онлайн дэлгүүр 5,66 хувьтай, 5,37 хувьтай гарсан явдал юм.



Төлбөрийн систем Санхүүгийн төрлийн халдлагын бараг 90-ээд хувийг цахим төлбөр тооцооны систем болох Paypal, American Express, Master Card international, Visa or Western Union гэх зэрэг олон улсын төлбөр тооцооны системийг хамардаг байна. **2013 оны төлбөр тооцооны системийн халдлагууд**



Дээрхи графикаас үзэхэд Paypal цахим төлбөр тооцооны хэрэгслүүр хамгийн их халдлагад өртсөн байгаа бөгөөд дараагаар нь American Express 26.26 хувьтай, 11,63 хувь олон улсын мастеркард зэрэг оржээ.

Дэлхий даяар жил бүр 575 тэрбум долларын цахим гэмт хэрэг үйлдэгддэг болохыг судлаачид тогтоожээ. Хувь хүмүүсийн кредит картны мэдээллийг хулгайлах замаар 150 тэрбум долларыг ашиглаж байгааг судлаачид онцолсон байна.

Тодруулбал, АНУ, Хятад, Япон, Германд нийт 200 тэрбум долларын цахим гэмт хэрэг үйлдэгддэг. Америкийн зургаан хүн тутмын нэг нь буюу 40 орчим сая хүн,Туркийн 54 сая, Германы 16 сая иргэн цахим гэмт хэрэгтнүүдэд мэдээллээ алдаж цахим хэргийн хохирогч болжээ үзсэн байдаг.

Тэдгээрээс тоо баримтаар дурдвал 2013 оны эхний хагасд дэлхийн хэмжээнд 1сая 509 мянга 934 төрлийн шинэ вирус гарсан бөгөөд үүнийг 2012 оны мөн үеийнхтэй харьцуулахад 20% -иар нэмэгдсэн байна.

Мөн 2012онд дэлхий нийтийн судалгаагаар цахим гэмт хэргийн улмаас нэг жилд дэлхий нийтээрээ 3 тэрбумаас 1 их наяд ам.долларын хохирол амссан мэдээ байна.

Түүнчлэн 2012 онд цахим гэмт хэргийн хохирогчдын тоо 556 саяд хүрч, хувь хүмүүсийн луйвардуулсан мөнгөний хэмжээ 110 тэрбум ам.доллар болсон нь нэг хүнээс дунджаар 197 ам.долларыг цахим гэмт хэрэгтнүүд луйварджээ.

Цахим ертөнцийн халдлага, хакердах гэмт хэргүүд дэлхий нийтээр газар авч хичнээн хэмжээний хор хохирол учруулсаныг түүхийн томоохон кибер халдлагуудын баримтаар сонирхуулая.

- **1983он** Кевин Митникийг Пентагоны дотоод сүлжээнд нэвтэрсэний төлөө АНУ-ын цагдаа нар баривчилсан. Түүнийг байнгын хяналтад байлгаж, хэд хэдэн удаа Холбооны мөрдөх товчооныхон баривчилж байжээ. Тэрээр товчхондоо хакеруудын бэлгэ тэмдэг юм.
- **1994он** Оросын математикч Владимир Левин Сити банкны мэдээллийн санд нэвтэрч, хамсаатнуудынхаа хамтаар гадаадын дансруу 10 сая ам.доллар баривчлагдахаасаа өмнө амжиж шилжүүлсэн.
- **2010 оны 6-р сар** Ираны цөмийн станцын Siemens фермийн тоног төхөөрөмжүүдэд “stux-net” нэртэй шинэ төрлийн вирус нэвтэрчээ.
- **2011 оны 4-р сар** Sony компанийн “play station”-ий сүлжээ томоохон кибер халдлагад өртөж, хакерчид сүлжээнээс нь нийт 77 сая мэдээллийг хулгайлсан бөгөөд үүний уршигаар компани сар гаруй зогссон байна.

- **2012 оны 5-р сар** Ерөнхийлөгчийн сонгуулийн хоёр шатны санал хураалтын хооронд Францын ерөнхийлөгчийн оршин суудаг “Элисейн” ордон кибер халдлагад өртжээ. Францын Ерөнхийлөгч Николя Саркозигийн ахлах зөвлөхийн компьютерийг хакердаж стратегийн холбогдолтой нууц баримт бичгүүдийг хулгайлсан байна. Францын тал энэ явдлыг гадаадын засгийн газрын оролцоотой, зохион байгуулалттай хэрэг гэж үзжээ.
- **2012оны 8-р сар** Газрын тосны “Aromca” группын 30 мянган компьтерт вирус тараажээ.
- **2012 оны 12-р сар** Францад сайн дурынхан ба шинжээчдээс бүрдсэн 6 ажлын хэсэг бүхийиргэний кибер батлан хамгаалахын сүлжээ байгуулагдаж кибер аюулгүй байдлын талаар зөвлөгөө өгдөг болсон байна.
- **2013 оны 9-р сар** Германы “Vodafone” гар утасны компанийн 2 сая гаруй хэрэглэгчийн мэдээллийг хулгайлсан.
- **2013 оны 10-р сар** “Adobe”-ийн серверүүд халдлагад өртөж программ хангамжийн эх код болон 38 сая хэрэглэгчийн мэдээлэл эрсдэлд орсон байна.
- **2014 оны 8-р сар** АНУ-ын 29 мужийн нийт 206 эмнэлгээс 4,5 сая хүний хувийн мэдээлэл алдагдсан бөгөөд үүнд өвчитний овог нэр, төрсөн он сар, гэрийн хаяг утасны дугаар багтжээ.

Кибер орчинд үйлдэгдэж байгаа гэмт халдлага, гэмт хэрэг зөрчлийг нийтлэг хандлагад үндэслэн цоо шинэ зохицуулалтыг бий болгох хэрэгтэй.

Иймд кибер орчинд үйлдэгдэж байгаа гэмт халдлага, гэмт хэрэг, зөрчилтэй тэмцэх чиг үүрэг бүхий байгууллага, хүний нөөцийн менежмент, сургалт, ажлын байрны тодорхойлолтын талаархи эдийн засаг, эрх зүйн тогтолцоог цогцоор нь боловсронгуй болгох асуудал тулгамдаж байна.

4.3. Үндэсний болон олон улсын байгууллагуудын хамтын ажиллагааг боловсронгуй болгох нь

Манай улсын чиг үүргийн байгууллагын хамтын ажиллагааны өнөөгийн байдал, хандлага

Өгөгдлийн аюулгүй байдлын гэмт халдлага, гэмт хэрэг, зөрчилд дархлаатай байгууллага гэж байдаггүй. Засгийн газар, томоохон корпораци зэрэг нь зөрчил гарах үед тохирох хариу арга хэмжээг авах, сүлжээнд дүн шинжилгээ хийх болзошгүй байдлын төлөвлөгөөтэй байх шаардлагатай.

Улсын хэмжээнд ажиллаж байгаа банк, санхүүгийн байгууллагууд, татвар, гааль, даатгал, интернет үйлчилгээ үзүүлдэг 108 байгууллага, иргэдээс гомдол мэдээлэл хүлээн авч шийдвэрлэж байгаа /Нийслэлийн ЗДТГ гэх мэт/ цөөн байгууллага, КТМС, ХСИС, ҮДТ, КАБГ, ХЗҮХ зэрэг байгууллагууд 2009 оноос хойш 8 удаа хамтран ажиллах хүрээнд уулзалт зохион байгуулсан хэдий ч өнөөгийн байдлаар нэгдсэн зохицуулалтгүй, харин ХЗҮХ, ХСИС, ҮДТ, КАБГ зэрэг цөөн байгууллага хязгаарлагдмал хүрээнд тус бүр нэг удаа эрдэм шинжилгээний хурал зохион байгуулсан төдийгүй Европын конвенцийн ажлын алба, БНСУ-ын Криминологийн хүрээлэн зэрэг гадаад улс орны адил чиг үүргийн байгууллагуудтай хамтран ажиллах хэлэлцээр байгуулан ажиллаж байна.

Мөн “Кибер аюулгүй байдлын 5 дугаар форум” 2014 оны 05 сарын 26-28-нд Улаанбаатар хотноо Кибер орчин дахь аюулгүй байдлыг хангахад тулгамдаж буй асуудал, цаашид кибер аюул заналтай тэмцэх бүс нутгийн хамтын ажиллагааг сайжруулах зорилгоор Мэдээллийн технологи, шуудан харилцаа холбооны газар, Ази номхон далайн бүсийн цахилгаан холбооны байгууллага (АРТ)-тай хамтран уг форумыг зохион байгуулсан.

Форумд Афганистан, Бангладеш, Бутан, БНХАУ, БНАСАУ, БНАЛАУ, Вьетнам, Камбож, Малайз, Малдив, Мянмар зэрэг 20 гаруй орны Мэдээллийн технологи, харилцаа холбооны яамны мэдээллийн аюулгүй байдлын асуудал хариуцсан төлөөлөгч, шинжээчид оролцлоо.

Олон улсын байгууллагаас APT, Ази номхон далайн бүсийн орнуудын сүлжээ мэдээллийн төв (APNIC), Азийн интернэтийн нийгэмлэг (ISOC), NTT, Хонконгийн Мэдээллийн аюулгүй байдлын мэргэжлийн холбоо (PISA), Токиогийн их сургуулийн төлөөлөгч, эрдэмтэн судлаачид хүрэлцэн иржээ. Манай улсаас Төрийн захиргааны төв байгууллагууд, банк, үүрэн холбооны оператор компаниудын мэдээллийн аюулгүй байдал хариуцсан албан тушаалтан, эрдэмтэн судлаач, инженерүүд оролцлоо.

Манай улсын чиг үүргийн байгууллагууд олон улсын адил үйл ажиллагаатай байгууллагатай хамтран ажиллах, үйл ажиллагааны хүрээгээ өргөжүүлэх, мэдээлэл, туршлага солилцох, суралцах ажлуудыг дэс дараатай зохион байгуулж байгаа боловч энэ салбарын хөгжил, хандлагыг гүйцэхгүй байгаа нь эдийн засаг, эрх зүйн зохицуулалт дутагдалтай байгаа илэрхийлэл гэж үзэх үндэслэлтэй.

Энэ нь эдийн засаг, эрх зүйн цогц зохицуулалт дутагдалтай байгааг илэрхийлж байна.

Ер нь олон улсын байгууллагуудын хамтын ажиллагаа энэ салбарт туйлын хэрэгтэй. Учир нь мэдээлэлээ хуваалцах, гэмт халдлагын ул мөр, баримт мэдээллэх, солилцох, нотлох баримт цуглуулах, ажлын туршлага судлах, харилцан суралцах, бүх талаар туслалцах зэрэг маш өргөн хүрээнд ажиллахыг шаарддаг.

Өнөөгийн байдлаар кибер халдлагын төрөл, онцлог, газар зүйн байрлалаас шалтгаалан олон албадтай байх шаардлага гарч байгааг анхаарах хэрэгтэй.

Гадаадын зарим улсын олон улсын хамтын ажиллагааны хандлага

Гадаадын ихэнх улс орнууд кибер орчны гэмт халдлага, гэмт үйл ажиллагаатай тэмцэх, хамтран ажиллахдаа олон улсын конвенци, нутаг дэвсгэрийн зарчмын дагуу салбар бүрт дагнан үйл ажиллагаагаа хэрэгжүүлэх хандлага ажиглагдаж байна.

2013, 2014 онд ухаалаг гар утас, таблет компьютеруудын хэрэглээ ихэссэн нь гэмт хэрэгтнүүдийг үйл ажиллагаа идэвхижсэн гэж үздэг.

Их Британийн ерөнхий сайд Гордон Браун төрийн болон корпорациудын сүлжээг тагнан турших, халдлага үйлдэх гэмт хэрэгтэй тэмцэх зорилго бүхий бие даасан байгууллага бий болгохоор шийдвэрлэжээ. Бодит байдалд энэ шийдвэр нь Кибер аюулгүй байдлыг хариуцсан сайдтай байх шийдвэр юм.

Independent-д бичсэнээр мэдээллийн сүлжээний аюулгүй байдал, электрон тагнуулын эсрэг ажиллах сайдын албан тушаалд иргэний мэргэжлийн хүн томилохоор тооцож байгаа юм байна. Их Британийн ерөнхий сайд өмнө нь нэг биш удаа төр, засгийн болоод бизнесийн байгууллагуудын мэдээллийн системд халдсанаар учирч болзошгүй хор хөнөөлд асар их байж болох тухай санаа зовниж буйгаа илэрхийлж байсан юм.

Орос, Хятадын хакерууд гол аюул заналыг учруулна гэж тэд үзэж байна.

Саяхан Британийн тагнуулын албанаас Британийн Оросын болон Хятадын тусгай албад хоорондын холбоо, мэдээллийн системийг тасалдуулах зорилго бүхий үйл ажиллагаа эрс идэвхижиж буй тухай мэдээлсэн байна.

Аюулгүй байдлын мэргэжилтнүүд ухаалаг гар утастай холбоотой энэ жил өнгөрсөн оныхоос илүү гэмт хэрэг гарах хандлагатай байгааг анхааруулж байна.

Ялангуяа Андройд төхөөрөмжүүд гэмт хэрэгтнүүдийн үндсэн бай болж байгааг аюулгүй байдлын Касперски компани мэдэгджээ.

Тухайлбал уг компани 2012 онд 35000 хортой Андройд програм илрүүлсэн бөгөөд энэ нь өмнөх оныхоос тооны хувьд 6 дахин их үзүүлэлттэй байгаа юм.

Энэ аюулаас хамгаалах нэг арга нь бидний байнга ярьдаг вирусны эсрэг програм суулгаж, мэдээллийн санг нь байнга шинэчилэх, мөн таны хаягаар ирсэн имэйл бүрийг нээхгүй байх явдал юм.

Мэргэжилтнүүдийн хувьд дараах аюул заналуудыг 2015 онд голлоно гэсэн урьдчилсан дүгнэлт гаргасан байна.

Гар утасны хортой код

2012, 2013 онд гэхэд л ухаалаг гар утсанд илэрсэн нийт хортой кодын төрлийн тоо өмнөх 7 жилийн нийлбэрээс илүү байгааг тогтоосон. Хортой кодын 90 хувь нь гар утсанд хандах, утасны системийг тасалдуулах зорилготой бөгөөд Андройд системтэй утасруу чиглэсэн халдлага энэ хэвээр үргэлжлэх өндөр магадлалтай байна.

Жишээлбэл, өөрөө өөрийгөө текст мэссэжээр тараадаг гар утасны өт буюу ворм (worm) өнгөрсөн жил их хэмжээгээр илэрсэн нь энэ жил ч мөн үргэлжлэх төлөвтэй байна. Мөн Аппл (Apple) компаний iOS системтэй гар утаснууд мөн л халдлагад өртөх хандлагатай байна.

Өвчтөний хувийн мэдээллийн хулгай

Эмнэлгийн үйлчилгээ үзүүлдэг байгууллагуудын өөрсдийн бүртгэлийн системийг цахимжуулж байгаагын хажуугаар тухайн системүүдийн цоорхой, зохиомжийн алдаанаас үүдэн мэдээлэл алдагдах явдал зогсохгүй байгааг Identity Theft 911 байгууллагын захирал **Адам Лэвин** мэдэгдсэн байна. Судалгаагаар уг чиглэлийн байгууллагуудын 94 хувь нь өнгөрсөн 2 жилийн хугацаанд ямар нэгэн байдлаар өвчтөний мэдээллээ алдсан гэж мэдүүлжээ.

Төлөвлөсөн халдлага

Голдуу хувь хүмүүс кибер халдлагын бай ихээхэн болдог. Тэгвэл энэ онд тагнуулын зорилготой кибер халдлагууд тодорхой байгууллага эсвэл түүний удирдах ажилтнуудруу өргөнөөр хийгдэх төлөвтэй байна.

Хувийн мэдээлэл хулгайлах зорилготой хортой код

Хэдийгээр гар утаснууд хэрэглэгчийн мэдээллийг дотроо нууцлалтай хадгалдаг ч тухайн шифрийн түлхүүрийн ихэнх нь нийтийн түлхүүрийн криптограф ашигладаг нь гэмт хэрэгтнүүдэд боломж олгосоор байгаа юм. Эцэст нь та өөрөө өөрийнхөө мэдээллийг худалдаж авах хэрэгтэй болно. Энэхүү төрлийн гэмт хэрэг энэ жил мөн л үйлдэгдэх магадлалтай байна.

Мэссэж дундаас нь олзолж авах

Андройд систем дээр ажилладаг утасны мэссэжийг дундаас нь барьж аван өөр дугаар болон сэрвэрлүү дамжуулдаг хортой код байсаар байна. Энэ халдлагад гар утасныхаа мэссэжээрээ дамжуулан интернэт банкны үйлчилгээ ашигладаг хэрэглэгчид ихээхэн өртөж байгаа юм.

Групп халдлага

2008 онд эхэлсэн энэхүү хөдөлгөөнийг ихэнх хүмүүс Anonymous гэдэг бүлгээр мэддэг. Түүнээс хойш ийм төрлийн олон бүлэг хүмүүс улс төрийн болон бусад зорилгоор үндэстэн дамнасан томоохон хэмжээний халдлагуудыг зохион байгуулсаар байна.

Үүлэн халдлага

Сүүлийн үед хүмүүс үүлэн тооцоолол (**cloud computing**) гэгчийг ихээр ашиглах болсон. Үүний хажуугаар бас л эрсдэл байсаар. Хэн нэгэн нь уг үүлэн тооцооллын системд нэвтэрч их хэмжээний мэдээлэлд хандах боломжтой аюул мөн л давтагдахаар байна.

Ашигладаг хэрэгслүүд

- Утасгүй интернэт (wireless) сүлжээний технологи хамгийн том асуудал болж байгаа ба хамгаалагдаагүй сүлжээг хэн нэгэн гаднаас энгийн нэг радио антенн, PDA (бага оврын компьютер) эсвэл гар утас ашиглан хакердаж болдог.
- Пасспорт эвдэгч (пасспорт тайлахад (decrypt) зориулсан програм хангамж бөгөөд тэднийг амжилттай нэвтрэх боломж олгодог)
- Сүлжээ хайх програм хангамж нь нээлттэй байгаа портууд хайж олон сүлжээнд нэвтрэлт хийнэ. (програм хангамж, техник хангамж дээр суурилдаг)
- Хуурамч вебсайтууд (дуурайлган хийсэн URL) таныг веб дээр мэдээллээ оруулах үед системийн програмыг өөрчлөлгүйгээр хакердаж мэдээллийг авдаг. (Үүнд: кредит картны мэдээлэл, и-мейл хаягийн нууц үг, хэрэглэгчийн нэр… гэх мэт)
- СПАМ (и-мейл хаягийн жагсаалт ашиглан ихээхэн хохирол учруулах)

- Эндээс цахим гэмт хэргийг комьютер, мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг ба компьютер, мэдээллийн бусад төхөөрөмжийг ашиглаж үйлдсэн гэмт хэрэг гэж үндсэнд нь хоёр ангилж болохоор байна.

Кибер орон зайн даяаршил, мэдээллийн технологийн хурдтай хөгжил хүн төрөлхтний хянаж чадахааргүй их өөрчлөлтийг авчирлаа. Энэ салбар дахь тулгамдсан асуудлыг аливаа улс дан ганцаараа хянаж чадахааргүй тийм их эрс өөрчлөлтийг авчирлаа. Цаашид ч ойлгогдохооргүй олон олон өөрчлөлтүүд бий болно.

Иймд үүнийг ойлгож, зөв чиглэлээр хөгжүүлэхийн тулд өнгөрсөнийг маш сайн таньж, ойлгож түүнчлэн нийтээрээ нэгдмэл ойлголттой болж, хамтын ажиллагааны зохицуулалт, хяналт, хандлагадаа оруулахөөрчлөлтийг эрс шинэчлэх шаардлагатай болсон байна.

4.4. Кибер орчинд үйлдэгдсэн гэмт хэргийн нотлох баримтыг үнэлэх, шүүхийн шинжилгээний үйл ажиллагааг боловсронгуй болгох нь

Энэ салбарт үйлдэгдэж байгаа гэмт халдлагыг шинжлэх ухааны тодорхой салбарын тусгай мэдлэг, тусгай техник хэрэгсэл, тусгай арга, арга зүйг ашиглан шинжлэн судалж гаргасан баттай дүгнэлтийг үндэслэн болж өнгөрсөн үйл явдлын бодит үнэнийг тогтоохоос өөрөөр уламжлалт аргаар мөрдөн шалгаж шийдвэрлэх ямар ч боломжгүй болсон.

Энэ салбарт үйлдэгдэж байгаа гэмт халдлага бүр орон зай, цаг хугацааны хувьд ямар ч хязгаарлалтгүй төдийгүй үйлдэгч болон хохирогч, хохиролын шинж, онцлог, зорилго, сэдэл, үйлдэлдээ хэрэглэсэн арга, багаж хэрэгсэл зэрэг обьектив, субъектив бүх шинжүүд нь заавал тусгай мэдлэг, арга, технологи шаардах болсонтой холбоотой. Нөгөө талаар маш олон шинжлэх ухааны хүрээг хамарч үүсэн хөгжиж байгаа шинжлэх ухааны цоо шинэ салбарын нэг боллоо.

Компьютерын криминалистикийн шинжилгээ

Компьютерын криминалистик /Англиар “Computer Forensics”, “Digital Forensics”“Electron Forensics” Оросоор “Компьютерная форенсика”/ орчин үед хөгжиж буй криминалистикийн шинжлэх ухааны салбар юм. Компьютерын криминалистик нь криминалистикийн шинжлэх ухааны кибертехнологийн бүлэгт хамаардаг ба үүнд мөн “Мэдээллийн криминалистик” багтдаг байна.

Компьютерын криминалистик нь кибер орчинд үйлдэгдсэн гэх гэмт хэргийн ул мөр үлдсэн мэдээлэл хадгалах төхөөрөмжүүдийг олж илрүүлэх, түүнд шинжилгээ хийх, түүнд агуулагдах баримт болон бусад дижитал нотлох баримтуудын эх сурвалжийг тодруулах зорилготой арга техник юм.

Дээрхээс үзвэл компьютерын үйлдэгдсэн гэх гэмт хэрэг нь зөвхөн нэг компьютер дээр бус хэд хэдэн компьютер хамарсан сүлжээ, цаашлаад интернэтээр дамжин хэд хэдэн улсад байрших компьютерыг хамардаг учир ихэвчлэн хийсвэр кибер орчинд хэргийн газрын үзлэг явагддаг.

Шинжээчийн зүгээс зөвхөн нэг компьютер дээр шинжилгээ хийх бус сүлжээгээр дамжин хийсвэр гэмт хэргийн газарт узлэг хийх, нотлох баримт илрүүлэх, цуглуулах, түүнд шинжилгээ хийх, нотлох баримтыг баталгаажуулах зэрэг ажиллагаануудыг явуулахыг шаарддаг.

Компьютерын криминалистикийн шинжилгээ нь үндсэндээ 2 объект дээр шинжилгээ хийдэг:

1. Сүлжээний бус орчинд байрших компьютер, дижитал нотлох баримтад хийх шинжилгээ
2. Сүлжээний орчин дахь компьютер, дижитал нотлох баримтад хийх шинжилгээ

Сүлжээний бус орчинд байршиж буй компьютер, дижитал нотлох баримтад хийх шинжилгээ нь сүлжээний орчин дахиас илүү хялбар байдаг. Учир нь хэргийн газрын хамрах хүрээ нь зөвхөн тухайн компьютер байдаг ба гаднаас тухайн компьютерт байрлах нотлох

баримтыг устгах, өөрчлөх боломжгүй байдаг юм.

Харин сүлжээний орчин дахь компьютерт хийх шинжилгээ нь төвөгтэй бөгөөд нарийн мэргэшсэн шинжээчийг шаардаж байдаг. Учир нь тухайн компьютерт халдсан этгээд нь дэлхийн аль ч өнцөгт байрших боломжтой ба тухайн компьютерт халдахдаа хэд хэдэн компьютеруудыг дамжин, өөрийн ул мөрийг устгах замаар халдаж, халдлагад өртсөн компьютер дээрх хяналтын файлууд (**лог файлууд**)-ыг устгах, өөрчлөх замаар ул мөрөө устгасан байдаг тул шинжээчийн зүгээс халдагчийн ул мөрийг илрүүлэхийн тулд сүлжээгээр дамжин хэд хэдэн компьютерт үзлэг хийх шаардлагатай үүсдэг ба тухайн компьютер дээрх үлдсэн нотлох баримтуудыг халдагч санаатайгаар өөрчилсөн эсэх, устгасан эсэх зэргийг тогтоох ажиллагаанууд ыг шаарддаг нарийн төвөгтэй ажиллагаа байдаг.

Иймээс компьютерын криминалистикийн шинжээчид тавигдах гол шаардлага нь компьютерын техник эд ангиас гадна, програм хангамж, үйлдлийн систем, сүлжээний орчингийн талаар нарийн мэдлэг байдаг. Тиймдээ зарим улсуудад дээрх чиглэлээр мэргэшсэн байгууллагууд нь цагдаагийн байгууллагад хөндлөнгөөс криминалистикийн шинжилгээ хийхэд туслах зорилготой ажиллаж байдаг.

Электрон буюу цахим нотлох баримтад хийх криминалистикийн шинжилгээ

Электрон нотлох баримтыг хэд хэдэн эх сурвалжаас цуглуулан авах боломжтой байдаг. Нотлох баримт нь янз бүрийн мэдээлэл дамжуулах, хадгалах технологи дээр олддог. Халдагч этгээдийн үлдээсэн ул мөрийг цуглуулахад нотлох баримтыг 3 эх сурвалжаас цуглуулдаг:

1. Халдагчийн компьютер
2. Халдагчийн нэвтэрсэн сервер
3. Халдагч болон халдлагад өртсөн компьютерыг холбосон сүлжээ

Уг гурван эх сурвалжаас нотлох баримтын гарал үүслийг шинжээч нь тогтоох боломжтой болно.

Электрон нотлох баримтыг цуглуулж хураах авахдаа бусад нотлох баримтуудын адил маш хянуур авахыг шаарддаг. Уг электрон нотлох баримт нь нотлох баримтын чанараа алдахгүй байлгахын тулд компьютерын криминалистикт нотлох баримт хураах авах стандартуудыг баримталдаг.

Жишээ нь халдагчийн компьютерын файлуудыг хуулж авахдаа уг файлыг устгах вирус байгаа эсэхийг нягталж үзэх ба тухайн мэдээллийг хадгалж буй хэрэгсэлд соронзон орны нөлөө болон механик гэмтэл учруулахгүй байхыг шаарддаг.

Нотлох баримтыг устах, гэмтэхээс урьдчилан сэргийлэх хэдэн алхмуудыг шинжээчээс шаардаж байдаг:

1. Жинхэнэ нотлох баримтыг хуулбараас ялгаж өгөх
2. Нотлох баримтыг хадгалах төхөөрөмжийг нарийн сонгох
3. Нотлох баримттай холбоотой бүхий л ажиллагаагаа баримтжуулах
4. Хувийн мэдлэгээсээ давсан ажиллагаа явуулахгүй байх

Хэрвээ эдгээр алхмуудыг дагаагүй бол жинхэнэ нотлох баримт өөрчлөгдөх, устах, эвдрэх зэргээр нотлох баримтын чанараа алддаг. Мөн шинжээчийн зүгээс цуглуулж авсан нотлох баримт нь хэрэгт холбогдолгүй, байгууллага хувь хүний нууцад холбогдох мэдээлэл байгаа эсэхийг нягталж үзэхийг шаарддаг.

Зарим тохиолдолд ганцхан компьютерт хадгалагдсан нотлох баримтуудаас гадна тухайн компьютерын хэрэглэгчээс нотлох баримтыг илрүүлэх, цуглуулах, хураах авахад шаардлагатай мэдээллийг олж авч болдог.

Хэрэглэгчийн зүгээс өгч буй мэдүүлгийг ашиглан криминалистикийн шинжээч нь компьютерын тохируулга, програм хангамж, чухал файлуудыг хаана хадгалдаг байсан, тухайн файлд нэвтрэх нууц үг, код зэргийг олж авснаар нотлох баримтад хүрэхэд тун хялбар болж өгдөг. Халдлагад өртсөн компьютерын хэрэглэгч нь туршлагатай хэрэглэгч байсан тохиолдолд түүнээс халдагчийн талаар боломжит таамаглалуудыг цуглуулах замаар халдагчийн үлдээсэн ул мөрийг сүлжээгээр дамжуулан хайхад илүү тус дөхөм болдог.

Нотлох баримтыг цуглуулах - Энэ шатанд шинжээч нь халдлагад өртсөн компьютерын эргэн тойрноос шинжилгээгээ эхэлнэ. Халдлагад өртсөн компьютертой холбоотой мэдээлэл хадгалагч бүхий л биет багаж төхөөрөмжүүдийг хураан авч лабораторийн шинжилгээнд явуулна.

Үүнд:

Компьютерын хатуу диск, уян диск, флэш диск, компакт дискүүд орох ба эдгээрийг лабораторийн шинжилгээнд явуулах боломжгүй тохиолдолд тусгай хуулбарлагч програм хангамжуудыг ашиглан өөр мэдээлэл хадгалагч уруу шилжүүлж авдаг. Жишээ нь компьютерын хатуу дискийг салгаж авахад шууд эвдрэхээр гэмтсэн байвал түүний агуулгыг бүхэлд толин хуулбар хийгч програм ашиглан хуулбарлаж авдаг.

Мөн нэг мэдээлэл хадгалагчаас нөгөө мэдээлэл хадгалагч уруу шилжүүлж цуглуулж авч болох ба энэ тохиолдолд эх мэдээллийг хэзээ хуулбарлаж авсан гэдгийг тэмдэглэлд тодорхой тусгаснаар хуулбарлагдсан файлд үүссэн огноотой таарснаар нотлох баримтын хэмжээнд үнэлэгдэх юм.

Зарим түр зуурын мэдээллийг цуглуулах - Компьютерын зарим мэдээлэл хатуу дискэн дээр хадгалагдалгүй түр зуурын санах ойд хадгалагдаж байгаад өөрөө өөрийгөө устгаж байдаг. Үүний жишээ нь компьютерын шуурхай санах ой, сүүлд компьютерт нэвтэрсэн нэвтрэлтүүдийн бүртгэл зэрэг юм. Хэрэв халдлагад өртсөн компьютер унтраагүй, тэжээлээс салгагдаагүй байгаа тохиолдолд шинжээч шуурхай санах ойд хадгалагдсан мэдээллийг юуны түрүүнд хуулбарлаж авах хэрэгтэй ба ямар нэг байдлаар компьютер тэжээлээс салгагдсан тохиолдолд үнэ цэнэтэй мэдээллийг алдаж болдог.

Нотлох баримтыг баримтжуулах - энэ нь электрон нотлох баримтад хийгдэх криминалистикийн шинжилгээний чухал үе шат юм, Хэн, хэзээ, юуг, хаана, ямар аргаар ажиллагаа явуулсныг шинжилгээний бүх шатанд баримтжуулах нь чухал.

Хэр нарийвчилж шинжилгээг баримтжуулна, тэр хэрээр нотлох баримт үнэ цэнээ хадгалж байдаг. Зарим тохиолдолд компьютерын гэмт хэрэг нь шийдэгдтэл олон жил тойрох тохиолдол гардаг ба энэ тохиолдолд нотлох баримт цуглуулах ажлыг тусгай дэвтэр гарган тэмдэглэж явахыг зөвлөдөг.

Уг дэвтэр наад зах нь дараах зүйлсийг тусгасан байхыг шаарддаг:

- Тухайн хэрэгт хэн шинжээчээр ажиллаж байгаа - Албан ёсны мөрдөн байцаах ажиллагааны үнэлгээ
- Шинжилгээнд оролцож буй хүмүүсийн нэрс
- Хэргийн дугаар
- Шинжилгээ хийх болсон шалтгаан.

Мөн криминалистикийн шинжилгээний доорх мэдээллүүдийг тусгаж өгнө:

- Шинжилж буй компьютерын үйлдлийн систем, түүний үзүүлэлтүүд
- Сүлжээний диаграмм
- Шинжилгээ хийгдэж байхад ажиллаж байсан бүх программууд
- Системд хэн албан ёсоор нэвтэрч орох эрхтэй байсан
- Системийн удирдагчдын нэрс
- Нотлох баримт илрүүлэх, цуглуулах ажиллагааны бүх үе шатыг тэмдэглэсэн тэмдэглэл. Үүнд ажиллагаа явагдсан огноо, хугацаа, хэн явуулсан, ямар ажиллагаа явуулсан, хаана явуулсан, ажиллагааны үр дүнг тус тус тусгана.
- Хэн, хэзээ хураагдаж авсан нотлох баричтуудыг үзсэн, нэвтэрсэн тухай бүртгэл

Эдгээр ажиллагаануудыг бүрэн гүйцэд явуулснаар компьютерын гэмт хэрэгт хийх криминалистикийн шинжилгээ дуусгавар болох хэр алдаагүй, мэргэжлийн төвшинд явуулсан эсэхээс нотлох баримтын чанар нь шалтгаалж байдаг байна.

Мэдээллийн Аюулгүй байдлын тоон шинжилгээ[583]

[583] Ө.Эсболд PhD КТМС Системийн Аюулгүй Байдлын баг УБ., 2013.08.12

• Тоон шинжилгээ гэж юуг ойлгох /тоон нотлох баримт/
• Тоон шинжилгээ болон уламжлалт шинжилгээний харьцуулалт
• Тоон шинжилгээний шаардлага
• Тоон шинжилгээний алхамууд
• Тоон шинжилгээний хэрэгсэл ба харьцуулалт
• Мэдээллийн цуглуулах

Тоон шинжилгээ (Digital forensic)

Аливаа тоон тоног төхөөрөмжтэй хамааралтай материал дээр үндэслэн төрөл бүрийн тусгай арга механизм, техникийг ашиглан дүн шинжилгээ хийх замаар баримт бүрдүүлэх шинжилгээ судалгаа нэг төрөл юм.

Компьютерийн шинжилгээ (Computer forensic)

Компьютер болон хадгалах төхөөрөмжинд хадгалагдсан өгөгдөл дээр үндэслэн төрөл бүрийн тусгай арга механизм, техникийг ашиглан дүн шинжилгээ хийх замаар баримт бүрдүүлэх тоон шинжилгээний нэг төрөл юм.

Тоон нотлох баримт (Digital Evidence)

• Тодорхойлолт

– Компьютер ашиглан зөрчил хэрхэн болсоныг батлах эсвэл няцаах болон тухайн зөрчил нь санаатайгаар эсвэл хэрэгт холбогдолгүй болохыг батлахыг аливаа хадгалагдаж эсвэл дамжуулж буй өгөгдлийг хэлнэ .

• Аудио, видео, текст, зураг, сүлжээний бүртгэл эсвэл бусад тоон хамааралтай өгөгдөл
• Энэ төрлийн баримт нотолгоо нь гол төлөв анзаарагддаггүй

– Мэдээллийг цуглуулахдаа зүй ёсны дагуу хийдэггүй
– Үр дүнтэйгээр шинжилгээ хийдэггүй

Тоон шинжилгээ болон уламжлалт шинжилгээний харьцуулалт

№	Баримтын төрөл	Уламжлалт арга	Тоон арга
1.	Баримт бичгийн нотлох баримт	Зөвшөөрч болох сураг чимээн дээр үндэслэсэн баримт бичиг, зураг, аудио/видео бичлэг гэх мэт	Эмайл
2.	Нарийвчилсан нотлох баримт	Эрэн сурвалжлах явцад олж авсан илрүүлсэн баримт	Бүртгэлийн файл, Файлын цаг хугацааны тамга, үйл явдлыг дахин сэлбэн засах зориулалтай бүх төрлийн мэдээллийн систем
3.	Гэрчийн мэдүүлэг дээр үндэслэсэн нотлох баримт	Албан ёсоор амаар болон бичгээр илэрхийлсэн баримт (тангараг өргөн) эсвэл хуулийн албан ёсны үйл ажиллагааны зорилгоор олж авсан баталгаа	Тоон гарын үсэг ашиглан баталгаажуулсан бичиг баримт (нотариат тоон гарын үсэг ашигласан байх)
4.	Шинжээчийн нотлох баримт	Шинжээч нь өөрийн бодол санааг тусгасан нотлох баримт	Forensic tool ашиглан шинжээчийн гаргасан баримт

Тоон шинжилгээний шаардлага

• Гадны халдагч хэрхэн ажиллаж байгаа процессыг таниж мэдэх.
• Системийн хэрхэн хамгаалах талаар мэдлэгийг нэмэгдүүлэх.
• Мэдээллийн (тоон өгөгдөл) хулгайчийг шийтгэх.
• Хууль санаачлагчидад шинэ бодлогыг боловсруулахад туслах.

Будлианыг илрүүлэх

• Будлианыг бүрэн илрүүлэхэд нилээд хүндрэлтэй.
• Цахим баталгаа нь толгой эргүүлмээр, тодорхой бус байдаг.

• Нотлох баримтыг илрүүлэнгүүт шинжилгээ хийх ёстой.

• Магадгүй нотлох баримтыг баталгаажуулах мэдлэг болон тоног төхөөрөмж, хэрэгсэл дутуу байж болно.

• Баримт нотолгоо нь гол төлөв хугацаатай байдаг тул түүнийг шинжлэх явцад утга нь алдагдах магадлалтай.

• Халдагч гол төлөв баригдахгүй байх арга хэмжээг авдаг.

Халдагчийн зорилго

• Системд нэвтрэх.

• Өгөгдлийг хулгайлан системийг сүйтгэх.

• Арын хаалгыг суулгах эсвэл гэрээр үйлчилдэг утасны үйлчилгээг ашиглах.

• Нотлох баримтыг устгах эсвэл нуух оролдлогыг хийдэг.

Нотлох баримтыг нуун дарагдуулах

• Rootkit – Компьютерийн үйлдлийн системийг өөрчлөх замаар халдлагын үйл ажиллагааг нуух.

• Үндсэн төрлүүд

– Системийн файлыг даран өөрийн файлыг байршуулах (TripWire-аар илэрдэг).– Санах ойд ачаалалгдасан програмыг өөрчлөх (VICE- аар илэрдэг).

– Үйлдлийн системийн цөмд нэмэлт пакет хэлбэртэйгээр суудаг.Илэрүүлэхэд хүндрэлтэй.

• Intel арихтехтур ашигласан компьютерийн үйлдлийн системийн цөмд ихэвчлэн суудаг.

Тоон шинжилгээний алхамууд

- ✓ Аюул заналыг таних
- ✓ Халдлагад өртсөн системийг тусгаарлан хөлдөөх
- ✓ Халдлагад өртсөн гэмтэлд шинжилгээ хийх
- ✓ Хийх үйлдлүүд

• Системийг унтраах, асуудлыг шинжлэх

• Ажиллаж буй системийг засварлах

Шинжилгээнд хаалт үүсэх

• Заримдаа халдлагад өртсөн системийг сүлжээнээс салгах боломжгүй байдаг..– Электрон худалдаа, Банк, Өргөдөл, гомдол хүлээн эвэх, шийдвэрлэх гэх мэт.

• Шинжилгээ хийж буй хэрэгсэл алдаатай байж болно.

– Ашиглаж буй хэрэгсэлүүд хуурамч хувилбар байж болно.

– Албан ёсны бус хэрэгсэл ашиглаж байвал.

– Системээс өгөгдөл дуудахад үйлдлийн системийн цөмөөс худлаа мэдээллийг өгдөг болгон хувиргасан байж болно.

– Covert channel буюу процессуудын хооронд дамжиж буй мэдээллийн олж авах боломжийг хаах.

Хаалтыг даван харах

• Аюулгүй байдлын журмыг нарийвчлан чанд мөрдөх.

• Стандартын дагуу олж авч буй мэдээлэл болон хэрэгслийг сонгон авч ашиглах.

• Нэг төрлийн олон хэрэгсэл ашиглан үр дүнг харьцуулах.

• Digital Forensics-ийн стандартыг дагаж мөрдөх

– IETF RFC 3227: Guidelines for Evidence Collection and Archiving

– Digital Forensics Research Workshop www.dfrws.org

– **ISO/IEC 27037:2012** -Information technology -Security techniques -Guidelines for identification, collection, acquisition, and preservation of digital evidence

Тоон шинжилгээний хэрэгсэл

№	Төрөл	Програм хангамж дээр суурилсан	Техник хангамж дээр суурилсан
1.	Диск хуулбарлах	• ProDiscover	• Data Copy King

		• AccessData • EnCase	• Forensic Imager • Forensic Duplicator
2.	Санах ойг хуулбарлах	• Belkasoft Live RAM Caputer (Windows) • FTK Imager (Windows) • LiME (Linux) • PSXPMem (Mac OS X)	• WindowsSCOPE CaptureGUARD PCIe card (Windows)
3.	Бичилтийг хязгаарлах	• MacForensicsLab Write Controller • SAFE Block	• ICS driver lock • Ultrablock

Тоон шинжилгээний хэрэгслүүдийн харьцуулалт

Үйлдлүүд	**ProDiscover Basic**	**AccessData Ultimate**	**EnCase**
Өгөгдлийн физик хуулалт	+	+	+
Өгөгдлийн логик хуулалт	+	+	+
График интерфейс	+	+	+
Зайнаас ажиллах	*	*	+
Hash үйлдэл	+	+	+
Файлын толгойг шалгах	*	+	+
Түлхүүр үгийг хайх	+	+	+
Шахах	*	+	+
Шифрлэлтийг тайлах	*	+	*

Тоон шинжилгээний хэрэгслүүдийн харьцуулалт

Үйлдлүүд	ProDiscover Investigator	AccessData Ultimate	EnCase
Disk-to-disk хуулбарлалт	+	+	+
Image-to-disk хуулбарлалт	+	+	+
Partition-to-partition хуулбарлалт	+	*	+
Image-to-partition хуулбарлалт	+	*	+
Лог бичих	*	+	+
Тайланг бий болгох	+	+	*
Script дэмжих	*	*	+
Шүүлтүүрийг дэмжих	*	+	+
Command-line дэмжих	*	*	+

Шинжээчдийн зөвлөмж

• Сайн кодуудыг ажиллуулах (binary).

• Бүх нотлох баримтыг **Hash функц** ашиглан хамгаалах, нөөцлөх.

• Эмзэг болон хувирамтгай байдлаар нь зэрэглэлийг тогтоон мэдээллийг цуглуулах.

• Нотлох баримтын эх сурвалжтай ижил сүлжээг бий болгох.

• Бүртгэлийн файлууд бүрэн эсэхийг шалгах (үйл ажиллагаа тасалдахаас сэргийлэх).

Анхааруулга

• Аливаа хэрэглэж буй хэрэгсэлийн жинхэнэ эсэхийг шалгах.

– Ашиглаж буй програм хангамжийн Checksums/hashes-ийг шалгах.

– Хэрэв амьд (ажиллаж) байгаа системд дээр шинжилгээ хийж байгаа бол хэрэгсэлийг CD –нээс шууд ачаалах (F.I.R.E. , Knoppix гэх мэт).

• Процедурыг дуудахдаа систем болон санг ашиглалгүйгээр шууд хэрэглэх.

• Хамгийн сүүлийн үеийн хэрэгсэл ашиглах.

Мэдээллийг цуглуулах

• Программд ашиглаж буй компьютерийн бүх хатуу дискийг хуулбарлан авах

– Файл болгоныг цаг хугацаатай хамт

• Компьютерийн системийг хамгаалах

– Устгах үйлдлээс зайлсхийх, гэмтлээс сэргийлэх

• Файлуудыг эрэн хайх

• Ердийн файл

• Устгагдсан файл

• Нууц үгээр хамгаалагдсан файл

• Нуугдмал файл

• Шифрлэгдсэн файл

• Chain of Custody (мэдээллийг цуглуулах, явцын бүртгэл, дамжуулах, цуглуулах, хянах, шинжлэх):

– Зөвшөөрөлгүйгээр хандах боломжийг хязгаарласан газар өгөгдлийг хадгална.

– Нотлох баримтыг цулуулсан газраас эхлүүлэн мөрийг тэмдэглэн цуглуулна.

– Нотлох баримт болгонд бүртгэлийн файлыг үүсгэнэ.

Тоон шинжилгээний давуу тал

• Их хэмжээний өгөгдөлтэй ажиллах явцад

–Хурдан

–Нэгд нэггүй шалгах боломжтой

–Механик алдаа гарах магадлал бага

Тоон шинжилгээний дутагдалтай тал

• Тоон нотлох баримтыг хүлээн зөвшөөрөлүүхийн тулд:

– Өгөгдлийг дуурайлгаагүй гэдгийг батлах хэрэгтэй

– Бүх нотолгоо нь чухал байдаг

– Шинжээч нь мэргэжлийн хувьд чадварлаг болон баримт бичгийн процедурын бүрэн мэдлэгтэй байх

• Үнийн хувьд өндөр өртөгтэй болдог.

• Оролцогч талууд компьютерийн сайн мэдлэгтэй байхыг шаарддаг.

Тоон шинжилгээний хүндрэлүүд

• Маш их хэмжээний зайг эзэлдэг

• Стеганограф болон шифрлэлт ашигладаг

• Нотлох зүйлсийг утсгадаг хэрэгсэл

• Аливааг өөрчлөх боломж (Файлын он сарыг өөрчлөх)

• Лог болон аудитын файл өөрчлөгдсөн байх

• TOR болон BOTNET сүлжээ

• Anonymizer.com гэх мэт програмууд (Anonymous VoIP дуудлага)

Дүгнэлт

• Тоон шинжилгээний автомат хэрэгсэлүүд тэр бүр үнэн мэдээллийг гаргаж чаддаггүй.

• Мэдээллийн үнэн зөвийг тогтоох хүндрэлтэй байдаг (файлын үүсгэсэн он сар өдөр үнэн эсэх гэх мэт).

• Халдагын төрөл үүсэхтэй хамт үүссэн тул харьцангүй залуу салбар.

• Сүүлийн үеийн програм техник хангамж ашиглах шаардлагатай байдаг тул үнэтэй байдаг.

• Хууль эрх зүйн зохицуулалт чухал үүргийг гүйцэтгэдэг.

Шинэ лаборатори байгуулах шаардлага

Монгол Улсын шүүх шинжилгээний байгууллагад зайлшгүй бий болгох шаардлагатай чиглэл, лабораториуд, хүний нөөц.

• Энэ чиглэлийн бүтцийг хууль сахиулах бүх байгууллагад бий болгох бодлого төлөвлөх,

• Хүрээлэнд төдийгүй шаардлагатай аймаг, дүүргийн цагдаагийн газар, хэлтэст энэ чиглэлээр шинжээчийг тусгайлан бэлтгэх, дахин сургах бодлого төлөвлөх,

• Халдлагын дуудлагаар техник хэрэгсэлд үзлэг хийх зориулалт бүхий шинжээчийн их бүрэн багаж /Лог файл унших зориулалттай/

• Тэсрэх төхөөрөмж, тэсрэх бодисын шинжилгээний лаборатори - Тэсрэх төхөөрөмж, тэсрэх бодисын төрлийг тогтоох, тэсрэлтийн шалтгааныг тогтоох

• Шүүх дижитал судлалын шинжилгээний лаборатори

- Компьютер судлал; Компьютерын техник хангамж, программ хангамжийн бүрэн бүтэн байдлыг тогтоох, устгасан мэдээллийг сэргээх

- Гар утас судлал; Гар утасны эвдрэл гэмтэл, агуулж байгаа болон илгээсэн мэдээллийг судлах,

- Сүлжээ судлал; Дотоод, гадаад сүлжээний аюулгүй байдал, илгээсэн ба хүлээн авсан мэдээллийг тодорхойлох,

- Мэдээллийн сан судлал; Төрөл бүрийн мэдээллийн санд нэвтэрсэн, мэдээлэл алдагдсан эсэхийг тогтоох

• Дүрс бичлэгийн шинжилгээний лаборатори - Дүрс бичлэгийг тодруулах, дүрс бичлэгт бичигдсэн хүнийг адилтгах

• Дуу авианы шинжилгээний лаборатори - Дуу хураагуур, диктофон, дижитал ДУУ хураагч, гар утас зэрэгт бичигдсэн дуу авиаг тодорхой хүний дуу хоолойтой адилтгах

• Хэргийн бодит байдлыг сэргээх лаборатори /нэгж/ - Хэргийн газраас олдсон биет нотлох баримтын байрлал, хэлбэр, хэмжээ, чиглэл зэргээр нөхцөл байдлын шинжилгээ, туршилт хийж тухайн хэргийн болсон байдлыг сэргээх, макет хийх, компьютерын 3D программын аргаар биет байдлаар харуулах

• Галын техникийн шинжилгээний лаборатори - Галын шалтгаан нөхцөлийг тогтоох, галдан шатаасан гэмт үйлдлийг тогтоох

• Бараа судлалын шинжилгээний лаборатори

• Техник инженерийн шинжилгээний лаборатори

• Газрын тосны бүтээгдэхүүний шинжилгээний лаборатори

• Хүнс, тамхи, согтууруулах ундаа, согтууруулах бус ундааны шинжилгээний лаборатори

• Цацраг идэвхт бодисын шинжилгээний лаборатори

• Сэтгэц судлал, сэтгэл судлалын шинжилгээний лаборатори

• Эмнэлэг криминалистикийн шинжилгээний лаборатори

Шүүхийн шинжилгээний үндэсний хүрээлэн өнөөдрийн байдлаар:

Гэрэл зураг, дүрс бичлэг-дүр зургийн шинжилгээний лаборатори

1. Хэргийн газрын үзлэгийн гэрэл зургийн Монгол Улсын хэмжээний нэгдсэн архив
2. Өнгөт гэрэл зургийн лаборатори /Fujifilm digital/
3. Дүрс бичлэгийн шинжилгээ:

дүрсийг сэргээх, тодруулах, томруулах, өргөтгөл сэргээх, харьцуулах, хэмжилт хийх, олон дэлгэцийг ялгах салгах, улсын дугаар, автомашин, хувь хүн эд зүйлийн содон шинжтэмдэг тодруулах, засвар монтаж хийгдсэн эсэх, зураг хэлбэрт хөрвүүлэх, төхөөрөмжийн ажиллагаа тодорхойлох.

4. Гэрэл зураг
5. Аман зураг гаргах
6. Дүр зургийн шинжилгээ
7. Гар утас- тухайн утасны мэдээллийг гаргаж өгөх, дуудлага, мессэж, зураг, интернет түүх, устгагдсан файл сэргээх, сим картнаас дуудлага, мессэж,сэргээх,
8. Компьютер төхөөрөмж:

Тодорхой ажиллагаа шалгах, холбогдсон төхөөрөмжүүд, мэдээллүүдийг үзэх, устсан файл сэргээх, өөрчлөлтийг үзэх, интернет мэдээллүүд, садар самуун дүрс бичлэг, гэрэл зураг илрүүлэх,

9. Мэдээлэл агуулдаг төхөөрөмжүүд:

Флэш, хатуу диск....гэх мэт,

10. Дуу авиа сэргээх, тодруулах, өргөтгөл сэргээх, харьцуулах, засвар монтаж хийгдсэн эсэх, төхөөрөмжийн ажиллагаа тодорхойлох

11. Цахим төхөөрөмжүүд компьютер, дижитал аппарат, видео камер, хяналтын төхөөрөмж, гар утас, смарт, сүлжээний төхөөрөмж зэрэгт магадлах шинжилгээг гүйцэтгэж байна.

Цаашид олон улсын хэмжээнд судалгаа, шинжилгээ явуулах нөхцөл хангах үүднээс дотоод, гадаад хамтын ажиллагааг өргөжүүлэх, бүтэц зохион байгуулалтаа шинэчлэх, бодлогоо шинээр тодорхойлох, хүний нөөцийн сургалтын тогтолцоог хөгжүүлэх шаардлагатай байна.

Шүүх шинжилгээний зарим салбарууд, тухайлбал: Шүүх эмнэлэг, Криминалистикийн шинжилгээ нь хууль зүйн практик шаардлагаар үүсч бие даасан салбар шинжлэх ухаан болтлоо хөгжсөн түүхтэй.

Үүний нэгэн адил энэ салбарын Шүүхийн шинжилгээ мөн л цаг үеийн шаардлагаар нэгэнт салбар шинжлэх ухааны шинжийг нэгэнт олж хөгжиж байгааг анхаарах хэрэгтэй.

Эрүүгийн байцаан шийтгэх тодорхой ажиллагааны нэг болох шүүхийн шинжилгээ гүйцэтгүүлэх нь ЭБША-нд оролцогчдын эрх, хууль ёсны ашиг сонирхолд нийцсэн байхаас гаднаболж өнгөрсөн үйл явдлын бодит үнэнийг тогтооход ихээхэн ач холбогдолтой төдийгүй, энэхүү үйл ажиллагааг шинэ төвшинд гаргах, олон улсын хөгжлийн чиг хандлагад нийцүүлж судлан дүгнэх шаардлага зүй ёсоор тавигдаж байгаа бөгөөд энэхүү шаардлага нь судалгаа гүйцэтгүүлэх хууль ёсны үндэслэл болно.

Гадаадын зарим орны шүүхийн шинжилгээний байгууллагын зохион байгуулалт, үйл ажиллагаа

Гадаадын орнуудын шүүхийн шинжилгээний байгууллагын хууль тогтоомж, бүтэц зохион байгуулалтыг судлах нь судалгааны ажлын зорилго байлаа.

Ингээд гадаадын зарим улсуудын шүүхийн шинжилгээний байгууллагуудын зохион байгуулалт, тогтолцоог авч үзье.

ХБНГУ:

ХБНГУ-ын хууль, хуулийн байгууллагын тогтолцоог манайд авч хэрэглэхэд нэлээд төвөгтэй асуудал гардаг. Энэ нь дараах шалтгаантай:

1. Холбооны улсын системтэй. Тиймээс холбооны улсын хэмжээнд нэг “дээвэр байгууллага” байх, тэгээд 16 муж улс тус бүр тус тусын асуудлыг хариуцсан муж улсын дээд, дунд, доод шатны гэх мэт байгууллагуудтай, эрхлэх асуудлынх нь хүрээ нь ямар хуульд яаж зааснаасаа шалтгаалаад янз бүр байдаг. Манайд бол аль нэг мужаас нь жишээ авахад тохиромжтой.

2. Манай улсад хэрэглэгддэггүй энэ төрлийн салбарын мэргэжлийн үг хэллэг их байдаг.

Эрүүгийн байцаан шийтгэх ажиллагааны чиглэлээр эмнэлгийн болон эмнэлгийн бус шүүхийн /forensic/ шинжилгээ явуулдаг. Эрүүгийн болон криминалистикийн чиглэлээр „эмнэлгийн бус шүүхийн шинжилгээ“-г Холбооны улсын Дотоод хэргийн яамны харъяанд байх Холбооны Эрүүгийн Цагдаагийн өрөнхий газар (ВКА буюу Bundeskriminalamt) болох муж улсуудын Эрүүгийн цагдаагийн газрууд (LKA буюу (Landes Kriminal Amt) өөрсдөө шүүхийн шинжилгээ хийдэг.

ВКА буюу Холбооны эрүүгийн цагдаагийн газар нь 9 хэлтэстэйн нэг нь криминалитикийн техникийн институт (Das Kriminaltechnische Institut гэж байдаг. Энэ институтад

Chemiker/химич/, Physiker /физикч/, Biologen /биологич/, Ingenieure /инженер/, Phonetiker /утасны мэргэжилтэн/, Psychologen /Физиологич/, Linguistik /хэл судлаач/, Pharmakologie /эм зүйч/, Phonetik Kriminalbeamte, Mineralogen, IT- Spezialisten /IT чиглэлийн мэргэжйлтэн/, Elektroniker /электроникч/, Techniker, technische Assistenten 6a Laboranten гэх мэт 60 гаруй мэргэжпийн 300-аад хүн ажилладаг. Эдгээр ажилчид нь дотоод, гадаадад болон муж , дүүргийн эрүүгийн цагдаа нарт сургалт явуулдаг шүүхийн /forensic/ шинжилгээнийхээ чиглэл тус бүрээр хийдэг.

ВКА буюу Холбооны эрүүгийн цагдаагийн газрын хуульд ВКА-ийн бүтцийн талаар байдаггүй. Энэ байгууллагын эрх хэмжээ, үйл ажиллагааны чиглэл, хамрах хүрээ, мужийн Эрүүгийн Цагдаагийн Газартай, Олон улсын адил төстэй байгууллагуудтай хэрхэн хамтран ажиллах, хувь хүнтэм холбоотой мэдээллийн нууц, сан гэх мэтийг зохицуулсан байна. ХБНГУ-д байгууллагын бүтэц зохион байгуулалтыг хуулиар биш журмаар зохицуулдаг.

Эрүүгийн цагдаагийн газрын /ВКА/-ИЙН хариуцсан асуудалд жишээ нь олон улсын зохион байгуулалттай гэмт хэрэг, галт зэвсэг наймаалах, тэсэрч дэлбэрэх бодис, мансууруулах бодис хил давуулан борлуулах, хуурамч мөнгөн дэвсгэрт үйлдэх, төрийн зүтгэлтний амь нас эрүүл мэндэд улс төрийн сэдэлтээр халдсан гэмт хэргүүдэд хэрэг бүртгэлт, мөрдөн байцаалт явуулах, шүүхэд шинжээчээр мэргэжилтнээ явуулах гэх мэт ордог.

Үүнээс гадна дотоод хэргийн сайдын хүсэлт, даалгавраар, аль нэг мужийн дээд байгууллагын хүсэлтээр эсвэл улсын ерөнхий прокурорын хүсэлт болон даалгавраар хуульд заасан бусад гэмт хэрэг гарсан үед мэргэжилтнээ илгээх, оролцох, ихэнхдээ шинжээчээр ажиллах , дүгнэлт гаргаж өгөх эрхтэй байдаг.

Нийт 20 шинжилгээний чиглэл бүхий салбаруудтай (физик химийн лабораторитой, бичиг баримтын үнэн зөвийг шалгах, аюулгүйн техник, дуу авиа таних, бичгийн хэлбэр хэвийн шинжилгээ гэх мэт), жил бүр 14000 гаруй шинжилгээний тайлан, шинжээчийн дүгнэлтийг шүүхэд гаргадаг, ялангуяа дэлхийн бусад орны эрүүгийн цагдаагийн газруудад /энэ нь иргэний цагдаа байж болох/ шинжээчээр ажиллаж, шинжээчийн дүгнэлт гаргаж өгдөг.

ВКА нь эмнэлгийн бус шүүхийн шинжилгээний чиглэлээр (forensic science гэдэг утгаараа) ХБНГУ-даа ганц төв нь төдийгүй, хамгийн том судалгаа, шинжилгээний байгууллага юм байна, Тиймээс ч бусад бүх мужийнхаа орон нутгийн цагдаагийн газрын шинжээчидтэй хамтарч ажилладаг, Мьюнштэр хотод байдаг Германы Цагдаагийн дээд сургуультай нягт хамтын ажиллагаатай. ВКА нь Судалгаа шинжилгээний үр дүн, шүүхээр шийдэгдсэн тодорхой эрүүгийн хэргүүдтэй холбоотой шинжилгээний үр дүн зэргийн зарим хэсгээс олон нийтийн хэвлэл, мэргэжлийн ном, гарын авлага зэрэгт нийтлүүлдэг.

Ялангуяа эдгээр байгууллагатай улсаа төлөөлж харьцдаг. Жишээ нь Baden-brttemberg-хотын эрүүгийн цагдаагийн газрын 6 дугаар хэлтсийн үйл ажиллагааг авч үзье.

1. Чанарын менежмент
2. Криминалистик техникийн институт болон төв албаны мэргэжлийн Coordination
   Доорх нарийн мэргэжлийн салбар хэсгүүдэд
   шинжээчид нь хуваагддаг.

1. Нэгдүгээр хэсэг

- Материалын шинжилгээ буюу сонгодог Криминалистикийн техник (krim.technik.)
- Физик, ерөнхий хими
- Биологи, textile, ул мөр судлал
- Бичгийн хэв, бичиг баримт
- Буу, галт зэвсэг, баллистик шинжилгээ, хэв хэлбэр авах (Form)

2. Химийн болон техникийн шинжилгээний хэсэг

- Гал түймрийн шалтгаан
- Тэсэрч дэлбэрэх бодис
- Хор, хортой зүйлс

3. Гуравдугаар хэсэг. Молекул генетикийн шинжилгээ
- ДНК-цусны
- ДНК-нууц (ялгадас)-ийн ул мөр
- DANN-data-base /өгөгдлийн сан/
4. Дөрөвдүгээр хэсэг
- Танин олуулах шинжилгээ /identification/
- Дактилоскоп /Daktyloskopie/
- Хэргийн газрын мэргэжлийн групп /fototechnik/ манайхаар бол жижүүрийн бүрэлдэхүүн. гэсэн бүтэцтэй юм байна. Бусад мужууд ч гэсэн энэ мужтай адилхан зохицуулалттай.

Эдгээр үйл ажиллагааг тухайн муж улсын хуулиудаар зохицуулсан байдаг ба хуульдаа товч тодорхой эрх зүйн үндсийг тусгаж түүнийгээ тушаал журам хэлбэрээр дэлгэрүүлэн хэрэгжүүлдэг.

Сэтгэц гэм судлалын чиглэлээр муж бүр „эмнэлэг-шорон“-той. Ийм байгууллагад эмч, сэтгэл зүйч, хуульч гэх мэт шаардлагатай мэргэжилтнүүд ажилладаг. Эрүүгийн хэргийн журмаар эрх зүйн бүрэн , бүрэн бус чадамжтай этгээд хэрэг бүртгэл, мөрдөн байцаалт шүүхийн явцад болон шүүхийн дараагийн шатанд ч хүргэгдэн ирж эмчлүүлдэг. Сэтгэц судлалын шинжилгээ энэ байгууллагад хийгддэг, шинжээчийг нь мөн энэ байгууллагаас томилдог гэнэ.

Ерөнхийдөө аль ч мэргэжпээр шинжээч болоход ХБНГУ-д нэг хууль үйлчилдэг, Төрийн байгууллагад ажилладаг нарийн мэргэжлийн албан хаагч нар эрх үүргийнхээ дагуу эсвэл тодорхой мэргэжлийн хүн уг хуульд заасны дагуу төрөөс томилогдсон буюу эрх авсан, тангараг өргөсөн шинжээч гэж 2 янз байдаг.

Тэдгээр нь ихэнхдээ салбарынхаа хамгийн дээд мэргэжлийн нийгэмлэгт шалгалт өгч тангараг өргөн сертификат авдаг. Сертификат өгсөн байгууллагаас эргэж эрхийг нь хасах, түдгэлзүүлэх эрхтэй байна, Эдийн засаг банк санхүү, нягтлан бодох бүртгэл үл хөдлөх хөрөнгийн үнэлгээ, хөдөө аж ахуйн үнэлгээ, гэх мэтчилэн маш олон чиглэлээр шалгалт аван эрхийг нь олгож, нутаг дэвсгэрийн хязгаарлалт, томлигоо хийдэг гэнэ. Дээр дурдсан бүх асуудал салбар тус тусынхаа хуулиар зохицуулагдсан байдаг.

Тухайлбал эрүүгийн байцаан шийтгэх хууль, төрөөс эрх олгосон шинжээчийн тухай хууль /энэ нь бүх төрлийн шинжээчийн/, шүүхийн тухай хууль, насанд хүрээгүй хүмүүсийн шүүхийн тухай хууль, иргэний хэрэг хянан шийдвэрлэх хууль гээд л тус бүрдээ шинжээчийн үйл ажиллагааг зохицуулсан байдаг.

ЯПОН УЛС:

Шүүхийн шинжилгээний үндэсний судалгааны хүрээлэн

Японы Үндэсний цагдаагийн газар нь улс төр болон төвийн гүйцэтгэх засаглалын хяналтаас хараат бус, бие даасан байгууллага юм. Иргэний хяналтыг Ерөнхий сайдын албанд харъяалагдах Олон нийтийн аюулгүй байдлыг хангах Үндэсний Комисс (National Public Safety Commission) -оор дамжуулан хэрэгжүүлдэг. Шүүхийн шинжилгээний үндэсний судалгааны хүрээлэн нь Үндэсний цагдаагийн газрын дэргэдэх байгууллага юм. /National Research Institute of Police Science - An attached National Police Agency in Japan./

Зохион байгуулалт:

Ерөнхийлөгч (Мэргэжлийн хүн) - President (technical officer)

Дэд ерөнхийлөгч (Цагдаагийн ажилтан) - Vice President (Police Officer)

Ерөнхийлөн захирах газар : Ерөнхийлөн захирах хэсэг, Нягтлан бодох хэсэг - Department of General Affairs: General Affairs Section and Accounting Section

Шүүхийн шинжилгээний нэгдүгээр газар: биологийн нэгдүгээр хэсэг, биологийн хоёрдугаар хэсэг, биологийн гуравдугаар хэсэг, биологийн дөрөвдүгээр хэсэг, биологийн тавдугаар хэсэг - First Department of Forensic Science: First Biology Section, Second Biology

Section, Third Biology Section, Fourth Biology Section, Fifth Biology Section

Шүүхийн шинжилгээний хоёрдугаар газар: физикийн хэсэг, гал түймрийн шинжилгээний хэсэг, дэлбэрэлтийг шинжлэх хэсэг, механикын шинжилгээний хэсэг

- Second Department of Forensic Science: Physics Section, Fire Investigation Section, Explosion Investigation Section, Mechanical Investigation Section

- Шүүхийн шинжилгээний гуравдугаар газар: Химийн нэгдүгээр хэсэг, Химийн хоёрдугаар хэсэг, Химийн гуравдугаар хэсэг, Химийн дөрөвдүгээр хэсэг – Third Department of Forensic Science: First Chemistry Section, Second Chemistry Section, Third chemistry Section, Fourth chemistry Section

Шүүхийн шинжилгээнийдөрөвдүгээргазар: Мэдээллийн шинжлэх ухааны нэгдүгээр хэсэг, Мэдээллийн шинжлэх ухааны хоёрдугаар хэсэг, Мэдээллийн шинжпэх ухааны гуравдугаар хэсэг - Fourth Department of Forensic Science: First Information Science Section, Second Information Section, Third Information Section

Криминологи, хүний гэмт зан, үйл судлалын газар: Өсвөр насныхны гэмт хэргийг хариуцсан хэсэг, Гэмт хэргээс урьдчилан сэргийлэх хэсэг, Мөрдөн байцаалтын хэсэг - Department of Criminology and Behavioral Science: Juvenile Section, Crime prevention Section, Investigation Support Section

Замын хөдөлгөөн судлалын газар: Замын хөдөлгөөн судлалын нэгдүгээр хэсэг, Замын хөдөлгөөн судлалын хоёрдугаар, Замын хөдөлгөөн судлалын гуравдугаар хэсэг - Department of Traffic Science:- First Traffic Science Section, Second Traffic Science Section, Third Traffic Science Section

Судалгаа шинжилгээний зохицуулагч - Research Coordinator

Таних, (нэр хаяг) тогтоох төв - Identification Center

Шүүх шинжилгээний сургалтын төв - Training Center of Forensic Science

Шүүх шинжилгээний үндэсний судалгааны хүрээлэнгийн хариуцсан ажил - Activities of National Research Institute of Police’Science

Япон дахь шүүх шинжилгээ хариуцсан гол байгууллагын хувьд, тус хүрээлэнд шүүх шинжилгээнд мэргэшсэн зуу гаруй судлаачид ажилладаг. Тэд биологи, анагаах ухаан, шинжлэх ухаан, хими, эм судлал, физик, газар тариалан, инженер, нийгэм судлал, боловсрол, сэтгэл судлал гэх мэт олон салбарын нарийн мэдлэг ур чадвар шаардсан судалгаа, задлан шинжилгээ, танин тогтоох ажил хариуцан хийдэг. Тус хүрээлэн нь шүүх шинжилгээний салбарт дотооддоо болон олон улсын түвшинд нэр хүндтэй газар мөн.

Судалгаа шинжилгээ, боловсруулан бүтээх ажил

Нийгэм эдийн засгийн олон төрлийн нөхцөл байдлаас үүдэлтэй гэмт хэрэг, осол ихсэж байгаатай холбогдуулан жил бүр олон шинэ судалгааны төсөл хэрэгжүүлдэг. Эдгээр төслийн дагуу гэмт хэргийг илрүүлэх аргачлал техникийг сайжруулах, гэмт хэрэг болон өсвөр насныхны гэмт хэргээс урьдчилан сэргийлэхтэй холбоотой олон төрлийн судалгаа хийгдэж байна. Зам тээврийн осол, бөглөрөл, бохирдлын эсрэг арга хэмжээ авахад мөн эдгээр нь чиглэгдэж байна. Иймээс хүрээлэнгийн үйл ажиллагааны цар хүрээ байнга өргөжсөөр байна.

Задлан шинжлэх, танин тогтоох ажил

Гэмт хэргийг шинжлэх ухааны арга хэрэглэн мөрдөхөд дэмжин тусалдаг тус хүрээлэн нь байгуулагдсан цагаасаа гэмт хэргийн ул мөр, нотолгоог шинжлэн, таних явдлыг үндсэн үүргээ болгон ажиллаж ирсэн билээ. Эдгээр ажлыг бид цагдаагийн газраас, мөн шүүх прокурорын газраас хүлээн авдаг. Хуурамчаар үйлдсэн бүх мөнгөн дэвсгэрт, гэмт хэрэгтэй холбоотой галт зэвсэг, сум зэргийг зөвхөн манай хүрээлэнд нарийвчлан шинжилдэг. Гэмт хэрэгтнүүдийг шүүхээр тогтоох ажилд ийнхүү чухал хувь нэмэр оруулж байна.

Сургалт

Шинжлэх ухаан технологийн салбарт гарч буй хурдацтай хөгжпеөс үүдэн, шинжлэх ухааны аргаар гэмт хэрэг мөрдөх ажиллагааг шинэчлэн сайжруулж стандартчилах шаардлага тулгараад байна. Иймээс орон даяарх мужийн цагдаагийн газрын лабораторид ажилладаг

шинжээчдийг Шүүх шинжилгээний сургалтын төвд урьж, шүүх шинжилгээний гол салбаруудыг хамарсан цуврал сургалтын курс зохион байгуулдаг. Сургалтын төв нь хөгжиж буй орны шинжээчдэд зориулан танин тогтоох арга техникийг сайжруулах хэд хэдэн олон улсын семинар зохион байгуулдаг. Тус төвийн шинжээчид орон нутгийн цагдаа нарт зориулж семинар зохиодгоос гадна хавтаст хэргүүдтэй нь холбоотой асуудлаар зөвлөгөө өгч, аргачлалаа сайжруулахад нь дэмжии ажилладаг.

Их Британийн Умард Ирландын Нэгдсэн Вант Улс:

Шүүхийн шинжилгээний тухай хууль

ИБУИНВУ-ын Гэмт хэргийн /Шүүхийн шинжилгээний / хууль нь 2001 оны 1.1 -нд батлагдан гарсан. Энэхүү хууль нь сэжигтэнд шүүхийн шинжилгээг хийх журмыг хуульчлан тогтоож өгсөн ба ноцтой хэмжээнд авч хэлэлцэгдэх гэмт хэрэгт сэжиглэгдэж байгаа этгээдэд шүүхийн шинжилгээг хийх ба мөн сайн дураар шүүхийн шинжилгээг хийлгэж болох талаар заасан байдаг.

2003 онд энэхүү Шүүхийн шинжилгээний хуульд нэмэлт өөрчлөлт орсон.

Цагдаагийн байцаан шийтгэх ажиллагаанд энэхүү Шүүхийн шинжилгээний хуульд нэмэлт өөрчлөлт оруулсантай давхцан мөн нэмэлт өөрчлөлт орсон байдаг. Энэхүү хууль нь сэжигтэнд шүүхийн шинжилгээ хийх талаар тус хуулийн 3 дугаар зүйлийн 1 дэх хэсэгт тодорхойлохдоо:

гэмт хэрэг үйлдсэн газар дээрэз цагдаагийн ажилтанд сэжиглэгдэн баривчлагдсан этгээд, гэмт хэрэгт ямар нэгэн байдлаар холбогдсон этгээд, хэн нэгэн этгээдийн мэдүүлгээр гэмт хэрэгт холбоотой гэж шалгагдаж байгаа этгээд,

Гэмт хэргийн /Шүүхийн шинжилгээний тухай/ хуулийн 353.А зүйлд хууль ёсоор баривчлагдсан этгээдээс цусны шинжилгээ, шүлс болон үсний дээж авах тухай заасан.

Шүүхийн шинжилгээг явуулах хэлбэр.

Энэ хууль нь сэжигтэнд хийх шүүхийн шинжилгээний ажиллагааг 3 хэлбэрт хувааж үзсэн байдаг.

- Биеийн ил хэсэгт хийх шинжилгээ / хуруу, гарын алганы хээ, биеийн нууц хэсэг хамаарагдахгүй үс, хумснаас авах шинжилгээнүүд байдаг/
- Далд хэсэгт хийх шинжилгээ / цуснаас авах шинжилгээ, шүдний мөр гэх мэт/
- Хөвөн марль зэргээр хийх арчдасын шинжилгээ

Шүүхийн шинжилгээг хийх журам:

Хуулийн дагуу сэжигтэнд шүүхийн шинжилгээг хийлгэх асуудлыг ахлах мөрдөн байцаагчийн тогтоолоор онцгой тохиолдолд шүүхийн зөвшөөрлөөр хийдэг байна. Мөн сэжигтэн этгээдээс зөвшөөрөл авахын өмнө мөрдөн байцаагч дараах зүйлийг тодруулсан байх ёстой байдаг.

1. Сэжигтэн этгээдээс шүүхийн шинжилгээг авахдаа тухайн этгээд гэмт хэрэгт холбогдсон байх ёстой байдаг.
2. Мөн насанд хүрээгүй этгээд болон мөн хэрэг хариуцах чадваргүй этгээд биш гэдгийг нь тодруулах, Хэрвээ ийм этгээдүүд байвал шүүхийн шинжилгээг зөвхөн шүүхийн зөвшөөрлөөр хийдэг байна.
3. Шүүхийн шинжилгээг хийснээр тухайн сэжигтэн гэмт хэрэг үйлдсэн эсвэл гэм буруугүй этгээд юм уу гэдгийг нь нотлох ноцтой учир шалтгаан байгаа бол,
4. Зөвшөөрлийн хүсэлт тавьсан байдал нь бүхий л нөхцөл байдалд шалгагдсан байх,

Бүх шүүхийн шинжилгээг хийх гэж байгаа сэжигтэн этгээдүүдэд шинжилгээний үйл ажиллагаатай холбоотой мэдээллийг өгсөн байх, гэмт хэрэгт хэрэгт холбоотой учраас шалгагдаж байгаа боловч татгалзах эрхтэй гэдгийг нь тайлбарлан өгөх зорилгыг агуулдаг.

Сэжигтэнд хүмүүстэй харилцах болон хувираа ажилладаг хуульчид хандах үндэслэлтэй боломжийг олгох ёстой.

Хэрвээ баривчлагдсан сэжигтэн этгээд зөвшөөрөхгүй байгаа тохиолдолд ахлах мөрдөн

байцаагч биеийн ил хэсэгт хийх шүүхийн шинжилгээг явуулах зөвшөөрөл өгдөг ба харин түүнээс өөр шүүхийн шинжилгээ хийгдэх бол шүүхийн тогтоолыг авах хэрэгтэй болдог.

Ингэхдээ ахлах мөрдөн байцаагч биеийн ил хэсэгт хийх энэхүү шинжилгээний зөвшөөрөл өгөхийн өмнө дараах зүйлийг тогтоосон байх шаардлагатай.

- Сэжигтэн хууль ёсны дагуу баривчлагдсан байх,
- Сэжигтэн нь насанд хүрээгүй болон хэрэг хариуцах чадваргүй этгээд биш байх,
- Тухайн сэжигтэн этгээд гэмт хэрэг үйлдсэн гэж үзэх хангалттай үндэслэл, шалтгаан байгаад итгэлтэй байх,
- Шүүхийн шинжилгээг тухайн этгээдэд хийснээр сэжигтэн этгээд гэм буруутай эсвэл гэм буруугүй гэдгийг тодруулах нотлох баримтыг бий болгох үндэслэлтэй шалтгаан байгаа гэдэгт итгэлтэй байх,
- Шүүхийн шинжилгээг зөвшөөрөлгүйгээр хийж байгаа бүхий л нөхцөл байдлыг баталсан байх хэрэгтэй.
- Зөвхөн шүүхийн тогтоолоор хийгддэг дараах шинжилгээнүүд байдаг. Үүнийг тус хуулийн 8 дугаар зүйл болон 23 дугаар зүйлд заасан байдаг,
- Насанд хүрээгүй этгээд болон хэрэг хариуцах чадваргүй этгээдэд хийх ямар нэгэн шинжилгээ,
- Цагдан хоригдоогүй байгаа сэжигтэн этгээдээс шинжилгээ хийлгэх зөвшөөрөл өгөхгүй байх тохиолдолд хийх ямар нэгэн шинжилгээ,
- Биеийн далд хэсгийн болон арчдасын шинжилгээ хийлгэхийг цагдан хоригдож байгаа этгээд зөвшөөрөхгүй байх үед хийх шинжилгээ.

Шүүхийн тогтоол гаргах шүүгчийн шалгуур нь ахлах мөрдөн байцаагчийн тодруулдаг асуудлууд мөн гарч ирнэ. Тухайлбал, тухайн этгээд нь сэжигтэн байх, шүүхийн шинжилгээ хийх зайлшгүй үл үндэстэй шалтгаан байгаа гэдэгт итгэлтэй байх, шүүхийн шинжилгээг хийснээр тухайн этгээдийг гэм буруутайг нотлох болон гэм буруутайг үгүйсгэх нөхцөл байдлыг бий болгох мөн шүүхийн шинжилгээний үйл ажиллагаа нь бүхий л нөхцөл байдалд шалгагдсан байх ёстой гэх мэтчилэн.

Мөн энэхүү шүүхийн тогтоолыг сэжигтэн давж заалдах гомдол гаргах эрхийг нь хуулийн 115.А-Д заасан байна. Хуулийн 50 дугаар зүйлд зааснаар биеийн далд хэсэгт хийх шинжилгээг сэжигтэн этгээдтэй ижил хүйсийн хүн хийдэг байна.

Австрали:

АХУ-ын Тасмани мужийн Шүүх шинжилгээний байгууллагын бүтэц зохион байгуулалт, тогтолцоо, хууль тогтоомжийн талаар хийсэн тойм судалгаа

Тасмани мужийн шүүхийн шинжилгээний байгууллагын зохион байгуулалт - Тасманий мужийн Шүүх шинжилгээний байгууллага нь Цагдаагийн болон Онцгой байдлын яамны Шүүх шинжилгээний үйлчилгээ үзүүлдэг, уг яамны бүрэлдэхүүнд байдаг. Цагдаагийн болон онцгой байдлын яамны бүрэлдэхүүнд байдаг Шүүх шинжилгээний байгууллага нь хими, биологи зэрэг төрөлжсөн үйлчилгээг төрийн болон орон нутгийн байгууллага, агентлаг, үйлдвэрийн салбар болон нийтэд төлбөртэй үндсэн дээр шинжилгээ хийдэг байна.

Одоогийн байдлаар цагдаагийн болон онцгой байдлын яамны дэргэдэх шүүхмйн шинжилгээний байгууллага нь өөрийн түүхэнд хэд хэдэн удаа бүтцийн өөрчлөлт хийж, 2000 оноос эхлэн тус байгууллага нь Тасманий шүүх шинжилгээний гэсэн нэртэйгээр Цагдаагийн болон онцгой байдлын яаманд харьяанд шилжин ирсэн байна. Уг байгууллага нь Цагдаагийн байгууллагад үндсэн туслалцаа үзүүлдэг байгууллага мөн бөгөөд бусад төрийн болон хувийн, нийтэд үйлчилгээ үзүүлдэг байгууллага юм. Шүүхийн шинжилгээний байгууллагын захирал нь Төрийн нарийн бичгийн дарга, Цагдаагийн болон Онцгой байдлын яаманд тайлангаа танилцуулдаг байна.

Шүүх шинжилгээний байгууллагын дотоод бүтэц:

- Захиргаа
- Хими шинжилгээ
- Биологийн шинжилгээ
- ДНК

Шүүх шинжилгээний байгууллагыг Захирал удирдах бөгөөд уг хэсэг нь гэмт хэрэг гарсан газар дараах чиглэл, төрлийн шинжилгээний ажлыг хийдэг байна. Үүнд:

- Яриа, авиа судлалын
- Баллистик
- Баримт бичгийн
- Уламжпалт гарын

хээ -ДНК-ийн шинжилгээ

- Гэрэл зураг

Хэргийн газарт үзлэг хийх нь гэмт хэргийн илрүүлэх чухал бүрэлдэхүүн хэсэг байдаг бөгөөд үүнд шүүх шинжилгээний байгууллагын хувь нэмэр нэн чухал гэж үздэг байна.

Шүүхийн шинжилгээний журмын хуулийн тойм

Австралийн Холбооны улсын муж бүр шүүхийн шинжилгээний журмын тухай хуультай бөгөөд зарим муж нь шүүхийн шинжилгээний журмын тухай хуулийг бие даасан байдлаар гаргасан байхад зарим муж нь эрүүгийн хуулийн тусгай хэсэг, бүлэг болгон шүүх шинжилгээний журмын ажпыг зохицуулсан байна. Хууль зүй болон Үйлдвэрийн яам нь Цагдаагийн болон онцгой байдал, түүний харьяа шүүхийн шинжилгээний байгууллагыг бодлого, арга зүйн удирдлагаар хангах зэрэг үндсэн чиг үүрэг хэрэгжүүлж байна.

Шүүхийн шинжилгээний журмын тухай хуулийн тухайд,

Ерөнхий зүйл

Тасманы шүүхийн шинжилгээний журмын тухай хууль 2000 онд батлагдсан бөгөөд уг хуулиар гэмт хэрэгт сэжиппэж байгаа этгээд болон хүнд гэмт хэрэг үйлдсэн этгээд, цагдаагийн байгууллагад гэмт хэргийг илрүүлэхэд туслалцаа үзүүлэхэд шүүхийн шинжилгээ хийх үндэслэл, журмыг тодорхойлсон байна. Хуульд зааснаар шүүхийн шинжилгээ нь биед болон биед бус гэсэн төрөлд хуваадаг байна.

Хуулиар тогтоосон хязгаарлалт

Хуульд шүүхийн шинжилгээг гэмт хэргийн хохирогч болон 10 доош настай хүүхдэд шүүхийн шинжилгээ хийхийг хориглосон байдаг. Мөн Цагдаагийн байгууллагын үйл ажиллагааны явцад хийсэн гэрэл зураг болон видео бичлэг хамаарахгүйгээр хуульд заасан байна.

Шүүхийн шинжилгээ хийх нөхцөл

Шүүхийн шинжилгээг 15 ба түүнээс дээш настай сэжигтэн болон сэжиглэгдэж буй этгээдээс албан ёсны зөвшөөрөл авсан үндсэн дээр шинжилгээ хийгдсэн байна. Этгээдэд шүүхийн шинжилгээ хийхийн өмнө шинжилгээний талаар дэлгэрэнгүй тайлбар өгсний түүнээс албан ёсны зөвшөөрөл авсан байна, Хэрвээ сэжиглэгдэж байгаа болон эрүүгийн хэргийн сэжигтэн шүүхийн шинжилгээ явуулах зөвшөөрлөө өгөхгүй байвал цагдаагийн байгууллага нь шүүхэд хандаж шүүхийн шинжилгээ явуулах шийдвэр гаргуулна.

Шүүхийн шинжилгээг 15 ба түүнээс дээш настай сэжигтэн болон сэжиглэгдэж буй этгээдээс албан ёсны зөвшөөрөл авсан үндсэн дээр шинжилгээ хийгдсэн байна. Хэрвээ сэжиглэгдэж байгаа болон эрүүгийн хэргийн сэжигтэн шүүхийн шинжилгээ явуулах зөвшөөрлөө өгөхгүй байвал Цагдаагийн байгууллага нь захирамж зөвшөөрөл авсан байна. шүүхэд хандаж шүүхийн шинжилгээ явуулах шийдвэр гаргуулна.

Хэрвээ сэжиглэгдэж байгаа болон эрүүгийн хэргийн сэжигтэн 15 доош настай байвал шүүхийн шинжилгээ явуулах зөвшөөрлийг түүний эцэг эхээс авсан байна. Хэрвээ хүүхдийн эцэг, эх шинжилгээ явуулах зөвшөөрөл өгөхгүй бол шүүхэд хандаж шүүхээс шинжилгээ явуулах шийдвэр гаргуулсан байна.

Шүүхийн шинжилгээг явуулах журам

Шүүхийн шинжилгээ явуулах ажиллагаа нь этгээдийн нууцлалыг хадгалсан нөхцөл явагдах бөгөөд эмнэлгийн стандартын дагуу явагдана.

Шүүхийн шинжилгээг зөвшөөрөлтэй этгээд явуулна, Хуульд шүүхийн шинжилгээ явуулах жагсаалт, мөн шинжилгээ явуулах эрхтэй бүхий этгээдийн талаар зохицуулсан байна. Үүнд ерөнхийд нь эмнэлгийн ажилтан, шүдний эмч, сувилагч болон зарим тохиолдолд цагдаагийн ажилтан байна.

Шүүхийн шинжилгээнд 15 доош насны хүүхэд орж байгаа бол түүний эцэг, эхийг заавал байлцуулсан байна. Хэрвээ эцэг, эх нь байлцах боломжгүй бол цагдаагийн ажилтан, сэжигтэн биш 18 дээш насны хөндлөнгийн этгээдийг байлцуулан шинжилгээнд оруулсан байна.

Хуульд заасны дагуу шүүхийн шинжилгээний аюулгүй байдал, нууцлал, нотлох баримтыг хамгаалах, мөрдөн шалгалт болон шүүхийн шинжилгээг үр дүнтэй явуулах зорилгоор Цагдаагийн ажилтан шинжилгээний үед байлцаж болно.

Хүч хэрэглэх журам

Хэрвээ хуулиар тухайн төрлийн шүүхийн шинжилгээ авахаар зөвшөөрөгдсөн бол шинжилгээ явуулах эрх бүхий зөвшөөрөлтэй этгээд болон цагдаагийн ажилтан шүүхийн шинжилгээ явуулах тохирсон, боломжит арга хэрэгслээр шинжилгээг явуулж, шинжилгээний дээж устаж алдагдахаас урьдчилан сэргийлсэн байна.

Шүүхийн шийдвэр гаргуулах

Цагдаагийн ажилтан сэжиглэгдэж буй этгээд болон эрүүгийн хэрэгт татагдсан сэжигтний биед үзлэг хийх болон бусад төрлийн шүүхийн шинжилгээ явуулах, зөвшөөрөл олгох асуудлаар шүүхэд хандаж захирамж гаргуулна. Мөн шүүхийн шинжилгээнд орж буй этгээд 15 доош настай байвал мөн шүүхээс шүүхийн шинжилгээ явуулах талаар захирамж гаргуулсан байна. Хуулийн шаардлагыг хангаж байгаа нөхцөлд шүүх захирамж гаргана.

ДҮГНЭЛТ, САНАЛ

Гэмт хэргийн өнөөгийн байдал, шалтгаан, нөхцөлийг харахад үндэсний хэмжээнд тодорхой төрлийн гэмт хэргүүд үйлдэгдэж байгаа бөгөөд өсөх хандлагатай. Олон улсын хэмжээнд энэ төрлийн гэмт хэрэг үндэсний аюулгүй байдлын хэмжээнд хүрч тухайн улс орнууд энэ салбарт анхаарлаа хандуулж, энэ чиглэлийнхээ судалгаа, шинжилгээг төрөлжүүлж, жил бүр судалгаанд хамруулж, чиг хандлагаа тодорхойлж, бодлогыг хэрэгжүүлдэг болсон байна.

Орчин үеийн шинээр үүсч буй технологийн гэмт хэргүүд, түүний дотор кибер гэмт хэрэггэй тэмцэх, түүнээс урьдчилан сэргийлэх эрх зүйн зохицуулалт, чадамжийг Монгол Улсад бий болгохын тулд юуны өмнө Эрүүгийн хуульд гэмт хэргийн шинэ шинж, бүрэлдэхүүнийг нэмэх, “Мэдээллийн технологи, харилцаа холбооны тухаи”, “Мэдээллийн аюулгүй байдлын тухай”, “Өгөгдөл хамгаалах тухай”, “Төрийн өгөгдөл, мэдээлэлд хандах тухай”, “Цахим засгийн тухай” хууль, “Төрийн өгөгдөл мэдээлэл, сүлжээ, системийг хамгаалах тухай” хуулийг шинээр батлан гаргах, Эрүүгийн байцаан шийтгэх хууль, “Иргэний хэрэг хянан шийдвэрлэх тухай”, “Мэдээллийн эрх чөлөөний тухай”, “Оюуны өмчийн тухай” хууль гэх зэрэг 40 орчим хуульд нэмэлт өөрчлөлт оруулж орчин үеийн кибер гэмт хэргийн шинжүүд, санкцийг нэмэх, орчин үеийн мэдээллийн технологийн харилцааны зөв зохистой зохицуулалтыг бий болгох, хамгаалах харилцаануудыг тодорхой болгон зохицуулах, цахим нотлох баримт, түүнийг үнэлэх асуудлыг нэмэх, нийгэмд кибер гэмт явдалтай тэмцэх сэтгэхүйг төлөвшүүлэх, мэдээллийи технологийг зөв зохистой хэрэглэх соёлыг төлөвшүүлэх, өгөгдөл, мэдээллийн үнэ цэнийг бий болгох, хамгаалах сэтгэхүй болон мэдээллийн аюулгүй байдлын үнэ цэнэ, ач холбогдол, түүний тухай ойлголтыг нийгэмд төлөвшүүлэх, кибер гэмт хэргээс урьдчилан сэргийлэх, шалтгаан, нөхцөлийг судлах, тэмцэх зохицуулалтыг бий болгох нь шийдвэрлэх арга замуудын нэг юм.

Монгол Улсын хувьд үндэсний мэдээллийн аюулгүй байдлаа бүрэн хангах, мэдээллийн технологи ашигласан шинэ төрлийн зөрчил, гэмт хэрэгтэй шуурхай, үр бүтээлтэй тэмцэхийн тулд Кибер гэмт хэргийн тухай конвенцид заасан гэмт хэргийн бүрэлдэхүүнийг Эрүүгийн хуульд авч хэрэглэх ч шаардлага бий.

Тодуулбал, Кибер гэмт хэргийн тухай конвенцид нэгдэн орох, соёрхон батлах, эсхүл түүний агуулгыг Эрүүгийн хуульд нэг бүрчлэн хуульчилж одоогийн эрх зүйн зохицуулалтаа сайжруулж, шинэ төрлийн цахим гэмт хэргийн нотлох баримт цуглуулах, бэхжүүлэх, мөрдөн шалгах, хянан шийдвэрлэх, энэ зорилгоор олон улсын болон бүс нутгийн, хоёр талт харилцаатай байх боломж бүрдэнэ. Мөн дараах ойлголтыг хуульчлах нь эрүүгийн хуулийг төсөөтэй хэрэглэхээс урьдчилан сэргийлэх, гэмт этгээд ял завших явдлыг таслан зогсооход чухал үр нөлөөтэй.

Үүнд: компьютерийн сүлжээ, компьютерийн систем, компьютерийн мэдээлэл, интернэтийн үйлчилгээ үзүүлэгч, мэдээллийн урсгал, компьютерийн мэдээлэл, сүлжээний нууцлал, бүрэн бүтэн байдал, ашиглалт гэх мэт байдлаар гэмт хэрэг, зөрчлийн төрөл, онцлогоор нь хуульчлах шаардлагатай.

Түүнээс гадна мэдээлэлтэй холбоотой эрх зүйн актууд, төрийн бодлогын баримт бичгүүдэд энэ төрлийн гэмт үйлдэл, зөрчлөөс сэргийлэх, хүүхэд залуус, нийгмийн гишүүдийг зөв, соёлтой, аюулгүй зан үйлд сургах, төлөвшүүлэх талаар тусгаж өгөх шаардлагатай нь харагдаж байна. Цэцэрлэг, дунд сургуулиас нъ эхлэн хүүхэд, өсвөр үеийнхэнд аюулгүй зохистой хэрэглээ, соёлтой зөв зан үйлийг төлөвшүүлэхэд чиглэсэн сургалтын агуулга, хөтөлбөрийг бий болгох, мэдээлэл зүйл хичээлийг агуулгад нэмж оруулах шаардлага харагдаж байна. Их дээд сургуулийн мэргэжлийн оюутнуудад “Кибер орчинд ажиллах ёс зүй, соёл” хичээлийг ордог болгох хэрэгцээтэй байна.

Төрөөс батлан гаргасан бодлогын баримт бичгүүд, тухайлбал, “Үндэсний аюулгүй байдлын үзэл баримтлал”, Мэдээллийн аюулгүй байдлын үндэсний хөтөлбөрт тусгагдсан

мэдээллийн аюулгүй байдлыг хангах, кибер гэмт хэрэг, явдалтай тэмцэх заалтуудын биелэлтийг бодитой болгох, ялангуяа сэтгэлгээний өөрчлөлт хийхэд онцгойлон анхаарах цаг болжээ.

Түүнчлэн энэ чиглэлээр ажиллаж буй үндэсний аж ахуйн нэгж, ТББ-ыг дэмжих бодлогыг ч хэрэгжүүлэх шаардлагатай байна. Кибер гэмт хэргийн талаар хамтран ажиллах, харилцах туслалцах гэрээг бүс нутгийн болон халдлагын эх үүсвэр болж буй улсуудтай байгуулах нь олон улсын хамтын ажиллагааг хөгжүүлэх нэг арга зам мөн. Төрийн байгууллагуудаас гадна Компьютерийн халдлагатай тэмцэх баг, мэдээллийн аюулгүй байдал, кибер гэмт хэргийн чиглэлд ажилладаг. судалгаа хийдэг, шийдэл боловсруулдаг хувийн, төрийн бус байгууллагуудыг төрийн бодлогоор. дэмжих, тусламж, дэмжлэг үзүүлэх, олон улсын хамтын ажиллагаа хөгжүүлэхэд нь туслах нь олон талын ач холбогдолтой.

Хуулийн байгууллагуудын гэмт хэрэгтэй тэмцэх, илрүүлэх, таслан зогсоох, урьдчилан сэргийлэх чиг үүргээ хэрэгжүүлэх үүднээс шинэлэг үзэл баримтлалаар эрх зүйн зохицуулалт хийх шаардлага зүй ёсоор тавигдаж байна. Өөрөөр хэлбэл, шүүхийн шинжилгээний байгууллагын тогтолцоо, үйл ажиллагаа, шинжээчийн эрх зүйн байдлыг “хараат бус” байдлаар хуульчлах шаардлагатай гэсэн дүгнэлтэд хүрлээ. Үүнд:

1. Шүүхийн шинжилгээний тухай хуулийг батлан гаргах;
2. Шүүхийн шинжилгээний тухай хуульд шинжилгээний байгууллагын эрх зүйн байдал, бүтэц зохион байгуулалтыг бруулж өгөх;
3. Шинжилгээний байгууллагын хийх шинжилгээний төрлийг заах;
4. Шинжээч гэдэг ойлголтыг хуульд зааснаар биш илүү өргөн практик үйл ажиллагааны хүрээнд тодорхойлж өгөх;

Хохирлын хэмжээг тогтоох, үнэлэх талаар

Судалгаагаар байцаан шийтгэх ажиллагааны явцад гэмт хэргийн улмаас учирсан хохирлын хэмжээг тогтоох буюу үнэлэх ажиллагаа зохих журмын дагуу хийгддэггүй, хамгийн төлөвшсөн гэж үзэх боломжтой эд хөрөнгийн үнэлгээ хийх аргачлал, журам байдаггүй, эрх зүйн зохицуулалт нь боловсронгуй биш учраас хохирлын хэмжээг тогтоох, үнэлэх ажиллагаа бэрхшээлтэй, шийдвэрлэхэд төвөгтэй тулгамдсан асуудлын нэг болох нь тодорхойлогдсон. Ялангуяа Шүүхийн шинжилгээний тухай хуулийг батлан гаргах шаардлагатай байгаа нь судалгаанаас харагдаж байна.

Зохион байгуулалтын хүрээнд:

1. Гэмт хэргийн улмаас учирсан хохирлын зэрэг, шинж байдлыг иж бүрэн тогтоох шинжилгээний байгууллага бий болгох, энэ чиг үүргийг Шүүхийн шинжилгээний үндэсний төвд хариуцуулах;
2. Гадаадын орнуудын шүүхийн шинжилгээ явуулж жишгийг шүүхийн шинжилгээний хууль батлахдаа харгалзан үзэх жишээ нь зарим оронд цагдаагийн байгууллагын харьяанд байхад зарим оронд хараат бус бие даасан хэлбэртэй байдаг. Түүнчлэн хууль тогтоомжоор үйл ажиллагаагаа зохицуулдаг байхад нөгөө хэсэг нь журмаар үйл ажиллагаа зохицуулдаг юм байна.
3. Шинжээчийг илүү олон төрлийн салбарын мэргэжилтнүүдээс бүрдүүлэх, шинжилгээ хийх төрлийг олшруулах, албан хаагчдыг бэлтгэх, сургах, дадлагажуулахад анхаарах.
4. Шинжилгээ хийж байгаа албан хаагч нь цагдаагийн алба хаагчийн нэгэн адил захирах, захирагдах үүрэг хүлээх нь шинжээчийн дүгнэлт гаргахад нөлөөлж болох эсэхийг харгалзах, өөрөөр хэлбэл шүүхийн шинжилгээний байгууллагыг цагдаагийн байгууллагын бүтцэд оруулах нь тэдгээрийн шийдвэр, өдөр тутмын үйл ажиллагаанд нөлөөлж болох юм.

Гадаадын зарим орнуудын шүүхийн шинжилгээний байгууллагуудын хууль тогтоомж, бүтэц зохион байгуулалтын ололттой талуудыг нэвтрүүлж ажиллах нь манай улсын шүүхийн шинжилгээний байгууллагын хөгжилд зохих хувь нэмэр оруулах нэг “түлхүүр” юм.

Энд кибер аюулгүй байдлыг хангах эрх зүйн зохицуулалтын арга хэмжээний үндсэн чиглэлийг танилцуулъя:

- Олон улсын болон дотоодын түвшинд кибер гэмт хэргээс урьдчилан сэргийлэх, кибер халдлагыг саатуулах, түүнд хариу үйлдэл үзүүлэх чадавхийг бэхжүүлэх, цахим нотлох баримт цуглуулах, үнэлэх, дүгнэх үе шатыг боловсронгуй болгох чиглэлээр Эрүүгийн хууль, Эрүүгийн байцаан шийтгэх хуулийн холбогдох зүйл, заалтыг шинэчлэх
- Нутаг дэвсгэрийн болон улсын бүрэн эрхт байдлын зарчмаар кибер гэмт хэргийг илрүүлэх, түүнийг мөрдөх эрх зүйн хэм хэмжээ бий болгох
- Кибер гэмт хэрэгтэй тэмцэх, тоон мэдээллийн шинжилгээ хийх алба байгуулах, тийм албыг давтан сургах, кибер халдлагад хариу үзүүлэх чиглэлээр зохион байгуулах, шүүх эрх мэдэл болон хувийн сектор кибер гэмт хэргийг шийдвэрлэх чадавхийг бэхжүүлэх
- Өгөгдөл хамгаалах, нууцлал, тоон гарын үсэг, худалдааны эрх зүй, цахим засаг, шифрлэлттэй холбоотой эрх зүйн тогтолцоог хянаж шинэтгэх
- Кибер аюулгүй байдлыг хангах чиглэлээр хууль тогтоомжийг уялдуулан өөрчлөх, бусад улс орны эрх зүйн ололтоос туршлага судлах
- Олон улсын түншлэгчидтэй кибер халдлагыг мөрдөн шалгах асуудлаар мэдээлэл солилцох, хамтран ажиллах механизмыг боловсронгуй болгох
- Кибер аюулгүй байдлыг хангах чиглэлээр стратегийн түвшинд ажилладаг олон улсын байгууллагуудтай хамтран ажиллах арга замыг Засгийн газрын бүхэл түвшинд тодорхойлж хэрэгжүүлэх. Тухайлбал, бусад улс орнуудын кибер аюулгүй байдлыг хангах, хууль сахиулах байгууллагуудын хоорондын хамтын ажиллагааг эхлүүлэх, хөгжүүлэх, аюулгүй байдлын стандартуудыг боловсруулах, мэдээлэл солилцоход аюулгүй байдлыг хангахад чиглэсэн олон улсын гэрээ, хэлэлцээр байгуулах
- Олон улсын шинжтэй кибер халдлагад хариу үйлдэл үзүүлэх үйл ажиллагааг зохицуулахад бусад улсын төрийн байгууллагуудтай хамтран хэлэлцээ хийх, харилцан үүрэг хүлээх
- Мэдээлэл цуглуулах, нотлох баримтыг бэхжүүлэх үйл ажиллагааны эрх зүйн зохицуулалтыг тодорхой болгох. Тухайлбал, халдлага, хакерийн үйл ажиллагааг шийдвэрлэхтэй холбоотой шүүх эрх мэдлийн байгууллагад учрах бэрхшээлийг шийдвэрлэх.

2010 оноос хойш зохион байгуулагдаж байгаа “Cyber Olymp” хэмээх дэлхийн ёс зүйт буюу “White Hat” хакерийн дэлхийн хэмжээний тэмцээнд Монголын үндэсний дата төвийн программист, мэдээллийн технологийн инженерүүдээс бүрдсэн баг 2013 онд амжилттай оролцож дөвөрдүгээр байранд шалгарсан байдаг. Дэлхийн өндөр хөгжилтэй орнуудын хакеруудтай өрсөлдөж энэ хэмжээний амжилт үзүүлнэ гэдэг бол манай улс дотооддоо мэдээллийн аюулгүй байдлын боловсон хүчнээ богино хугацаанд хэр үр дүнтэй бэлдсэний илрэл. Энэ мэт залуучуудыг дэмжихийн зэрэгцээ цаашлаад дараа дараагийн үеийг бодлогоор дэмжин бэлтгэж гаргаж ирэх, тэднийг мэдээллийн аюулгүй байдлын салбарт үр өгөөжтэй ажиллуулах нь зүйтэй.

Тооцоолох хэрэгслүүдийн хатуу диск, санах ой, тээгч дээрх өгөгдлийн дүр файлыг бүрэн хуулж авах, лог бүртгэлийн болон аудитын файлуудыг гарган авах, задлан шинжлэх техник, тоног төхөөрөмж, програм хангамж бүхий лаборатори байгуулах, хэргийн газарт үзлэг хийхэд шаардагдах төхөөрөмжүүд худалдан авч мэргэжилтнүүдийг бэдтгэх, шинжээч нарыг сурган хөгжүүлэх, ажилтнуудыг төхөөрөмжтэй ажиллаж сургах, гаргасан өгөгдлийг тайлан унших чадварт сургах хэрэгцээ нэгэнт бий болжээ. Энэ чадварыг бий болгосноор зөвхөн кибер гэмт хэрэг төдийгүй тооцоолох хэрэгсэл ашигласан аливаа гэмт хэргийг нотлох баримтуудыг гарган авах, ашиглах, гэмт хэргийг мөрдөхөд орчин үеийн технологийн ололт, чадамжийг ашиглах өргөн боломж нээгдэнэ.

АШИГЛАСАН МАТЕРИАЛ

1. Монгол Улсын Үндсэн хууль 1992 он
2. Монгол Улсын Эрүүгийн хууль 1996 он
3. Монгол Улсын Эрүүгийн хууль 2002 он
4. Г.Совд. “БНМАУ-ын эрүүгийн эрхийн курс”, УБ., 1973 он.
5. Г.Совд “Монгол Улсын Эрүүгийн хуулийн тайлбар” УБ., 2002
6. С.Жанцан “Монгол Улсын Эрүүгийн эрх зүй” УБ., 2004
7. С.Жанцан “Монгол Улсын Эрүүгийн эрх зүй” /схемчилсэн тайлбар, зүйлчлэлийн асуудал/ УБ., 2004
8. С.Нарангэрэл “Монгол Улсын Эрүүгийн эрх зүй”, УБ., 1999
9. Ж.Болдбаатар “Эрүүгийн эрх зүйн тулгуур ойлголтууд” УБ., 2002
10. Ж.Болдбаатар “Эрүүгийн эрх зүйн үндэс” УБ., 2004
11. “Britannica”ширээний нэвтэрхий толь..
12. Я.Цэвэл “Монгол хэлний товч тайлбар толь”
13. ХЗҮ-ний Хүрээлэнгээс явуулсан судалгааны тайлан 2009 он
14. ЦЕГ-ын ЭЦГ-ын гаргасан судалгаа 2014 оны 03 сар
15. Т.Халтар “КДХТ-ын судалгаа” 2013
16. Монгол Улсын Засгийн газрын тогтоол 2012 оны 04.04 дугаар 101 “Цахим засаг” Үндэсний хөтөлбөр
17. МТШХХ-ны газрын 2013 оны үйл ажиллагааны тайлан
18. Л.Галбаатар “Цахим эрх зүй”. УБ., 2010 он
19. В.Болорсайхан “Төгсөлтийн ажил”
20. Л.Цогтбаяр., “Компьютерийн мэдээллийн аюулгүй байдлын эсрэг гэмт хэргийн эрх зүйн зохицуулалт, өнөөгийн байдал, чиг хандлага” ХСИС ЭШ-ний эмхтгэл, УБ., 2012 он
21. ЦЕГ-ын Хэвлэл мэдээллийн төвийн ажилтан, цагдаагийн ахмад Ё.Лхагвасүрэн., УБ., 2015.01.14.
22. Л.Цогтбаяр “Кибер орчинд үйлдэгдэж байгаа гэмт хэрэгтэй тэмцэх эрх зүйн тогтолцоо, хандлага” Хууль сахиулахуй сэтгүүл-2, УБ., 2014
23. Л.Цогтбаяр, “гэмт хэргийн нотлох баримтын онол” лекц, УБ., 2012
24. Д.Батзориг “Таны зөв сонголт” УБ., 2000
25. Н.Батцэрэн “Компьютерийн үндсүүд” УБ, 1998
26. Ц.Эрдэнэ “Терроризм, түүнтэй тэмцэх асуудал” илтгэлийн эмхтгэл, УБ., 2003
27. “Төр, хувийн хэвшлийн түншлэл-2015” нээлттэй хэлэлцүүлэг
28. Л.Цогтбаяр, “Хууль зүйн сэтгэц судлал” лекц, УБ.,2014 он
29. Ө.Эсболд PhD КТМС Системийн Аюулгүй Байдлын баг УБ., 2013.08.12
30. Л.Цогтбаяр, “Mindset facing problems, discussing ways, and tendencies on the environment of legal reform” ХСИС-ийн ЭШ-ний хурлын илтгэл, УБ, 2014.
31. Ulrich Sieber: The International Emergence of Criminal Information Law, 1991
32. Ulrich Sieber (ed.): Information Technology Crime – National Legislation's and International Initiatives, 1994
33. В.А.Мазуров “Компьютерные преступления” М, 2002
34. Internet Crime Complaint Center-ийн мэдээлэл, 2014 оны 6 сарын 10
35. *Great Issues in Western Civilization (volume I) Politics by Aristotle*
36. Маршал Мак Луй, "Мэдээллийн хэрэгслийг ойлгох нь", Канад Тр., /1964/

ЦАХИМ ЭХ СУРВАЛЖ

1. www.Legalinfo.mn.
2. http://en.wikipedia.org/wiki/Norbert_Wiener
3. /Oxford English Dictionary, 2nd Edition/
4. www.wordorigins.org
5. http://www.ikon.mn/n/65b
6. http://www.businessinsider.com/medvedev-twitter-hacked-2014-8
7. http://www.securitylab.ru/news/311384.php?pagen=3&el_id=311384

8. "Frequently asked questions and answers Council of Europe Convention on cybercrime", by the United StatesDepartment of Justice 2010
9. http://europa.eu.int/ISPO/elf/InternetPollclesSite/Crime/CrimeCommEN.ht ml
10. http://europa.eu.int/information society/topics/telecoms/internet/crime /index en.htm
11. http://www.oas.org/juridico/english/conference agenda.htm
12. http://conventions.coe.int/treaty/EN/projets/FinalCybercrime.htm
13. http://www.usdoj .gov/criminal/cybercrime/unlawful..