НЭЭЛТТЭЙ
НИЙГЭМ
ФОРУМ

# КИБЕР ГЭМТ ХЭРГИЙН ЗОХИЦУУЛАЛТЫН ТАЛААРХ ХАРЬЦУУЛСАН СУДАЛГАА

(Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн үүрэг, үйл ажиллагааны эрсдэлийн хүрээнд)

Улаанбаатар хот
2022 он

ННА 67.408
ДАА 345
К-381

# КИБЕР ГЭМТ ХЭРГИЙН ЗОХИЦУУЛАЛТЫН ТАЛААРХ ХАРЬЦУУЛСАН СУДАЛГАА

(Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн үүрэг, үйл ажиллагааны эрсдэлийн хүрээнд)

**Судалгаа хийсэн: Өмгөөллийн "Фиделитас Партнерс" ХХН**



Хаяг: Монгол Улс,
Улаанбаатар хот-14240,
Сүхбаатар дүүрэг,
Жамьян гүний гудамж-5/1
Утас: 976-76113207
Факс: 976-11-324857
Веб: http://www.forum.mn
И-мэйл: osf@forum.mn

ISBN: 978-9919-9926-6-8

# ӨМНӨХ ҮГ

Монгол Улс Кибер аюулгүй байдлын индекс (Global Cybersecurity Index 2020, ITU)-ээр нийт 184 орноос 120-д эрэмбэлэгдсэн нь энэ чиглэлээрх эрх зүйн орчин, хүний нөөц, техник, технологийн чадавх, дотоодын болон олон улсын хамтын ажиллагааг бэхжүүлэх хэрэгцээ, шаардлага өндөр байгааг илтгэнэ. УИХ цахим хөгжлийн багц хуулийн хүрээнд 2021 онд Кибер аюулгүй байдлын тухай хууль баталж, Эрүүгийн хуулийн 26 дугаар бүлгийг “Кибер аюулгүй байдлын эсрэг гэмт хэрэг” гэж өөрчлөн найруулсан нь энэ чиглэлээр багагүй хүчин чармайлт тавьж буйн илрэл юм. Энэ хүрээнд эрх зүйн зохицуулалт, хэрэгжилтийг бусад улс орны хэм хэмжээтэй харьцуулан судлах хэрэгцээ, шаардлага ч өндөр байгаа билээ.

Тиймээс Нээлттэй Нийгэм Форум нь “кибер аюулгүй байдал”, “виртуал хөрөнгийн үйлчилгээ үзүүлэгч” зэрэг шинэ тутам ойлголт хууль тогтоомжид шинээр туссантай холбогдуулан кибер аюулгүй байдлын эсрэг гэмт хэргийн талаарх улс орнуудын зохицуулалт, түүнийг олон улсад хуульчилсан байдал, виртуал хөрөнгийн биржүүдэд хийгдсэн кибер халдлага, тэдгээрийг шалган тогтоож, шийдвэрлэж буй практик, цаашлаад хэрэглэгч болон виртуал хөрөнгийн биржийн виртуал хөрөнгө алдагдсан тохиолдолд авч буй арга хэмжээ, цахим нотлох баримтыг үнэлж, шалган шийдвэрлэж буй байдал зэргийг Өмгөөллийн Фиделитас Партнерс ХХН-ийн судалснаар Та бүхэнд толилуулж байгаадаа таатай байна.

Бид манай улсад өрнөж буй Эрүүгийн эрх зүйн шинэчлэлийг бодлогын судалгаа, хэрэгжилтийн мониторингоор дэмжихийг зорьж ирсэн бөгөөд энэ хүрээнд 30 орчим судалгаа олны хүртээл болсон билээ. Мөн дээрх судалгааны үр дүнг олон нийтэд танилцуулах, бодлого, шийдвэрт тусгуулах зорилгоор цуврал хэлэлцүүлэг өрнүүлж, хэлэлцүүлгийн видео бичлэгийг олон нийтэд түгээдэг. Та бүхэн манай цахим хуудас, нийгмийн сүлжээнээс эдгээр тайлан, хэлэлцүүлгийг үзэх боломжтойг энэ ташрамд дуулгахад таатай байна. Бидний судалгааны ажилд Таны өгөх санал, шүүмж онцгой үнэ цэнтэй байх болно.

ННФ-ын Гүйцэтгэх захирал П.Эрдэнэжаргал

# АГУУЛГА

# ТОВЧИЛСОН ҮГИЙН ЖАГСААЛТ

| | |
|---|---|
| ВХҮ | Виртуал хөрөнгийн үйлчилгээ |
| ВХҮҮ | Виртуал хөрөнгийн үйлчилгээ үзүүлэгч |
| ВХҮҮтХ | Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн тухай хууль |
| ЭХХШтХ | Эрүүгийн хэрэг хянан шийдвэрлэх тухай хууль |
| Хороо | Санхүүгийн зохицуулах хороо |
| Будапештийн конвенц | Кибер гэмт хэргийн тухай конвенц |
| НҮБ | Нэгдсэн Үндэстний Байгууллага |
| ФАТФ | Мөнгө угаахтай тэмцэх санхүүгийн хориг арга хэмжээ авах байгууллага |
| МҮТС | Мөнгө угаах, терроризмыг санхүүжүүлэх |
| УИХ | Улсын Их Хурал |
| БНСУ | Бүгд Найрамдах Солонгос Улс |
| АНУ | Америкийн Нэгдсэн Улс |
| ОХУ | Оросын Холбооны Улс |
| Швейцар | Швейцарын Холбооны Улс |
| БНЭУ | Бүгд Найрамдах Эстони Улс |
| Сингапур | Бүгд Найрамдах Сингапур Улс |
| Хонконг | Бүгд Найрамдах Хятад Ард Улсын Засаг захиргааны онцгой бүс Хонконг |

# ХҮСНЭГТИЙН ЖАГСААЛТ

# ЗУРГИЙН ЖАГСААЛТ

# ХАВСРАЛТЫН ЖАГСААЛТ

# УДИРТГАЛ

## Судалгааны хэрэгцээ, шаардлага

Нэгдсэн Үндэстний Байгууллагын дэргэдэх мэдээлэл, харилцаа холбооны технологийн асуудал хариуцсан тусгай агентлаг болох Олон улсын харилцаа холбооны нэгдэл (*ITU*)-ээс 2020 онд гаргасан Кибер аюулгүй байдлын индексээр нийт 184 орноос Монгол Улс 120-д эрэмбэлэгджээ.[1] Тус индекс нь кибер аюулгүй байдал, кибер гэмт хэрэгтэй тэмцэх эрх зүйн орчин, технологийн чадавх, кибер аюулгүй байдлыг хангах үндэсний стратеги, чадавх бэхжүүлэх үйл ажиллагаа, хамтын ажиллагаа гэсэн үндсэн таван үзүүлэлтэд тулгуурладаг.[2]

Кибер гэмт хэрэгтэй тэмцэх эрх зүйн орчин бүрдүүлэх нь кибер аюулгүй байдлыг хангасан эсэхийг тодорхойлох эхний үзүүлэлт байх тул кибер гэмт хэргийн дотоодын эрх зүйн зохицуулалтыг бусад улсын хэм хэмжээтэй харьцуулан судлах замаар цаашид сайжруулах арга замыг тодорхойлохыг тэргүүн ээлжид зорьсон болно.

УИХ цахим хөгжлийн багц хууль батлах хүрээнд Кибер аюулгүй байдлын тухай хуулийг 2021 оны 12 дугаар сарын 17-ны өдөр баталж, 2022 оны 5 дугаар сарын 1-ний өдрөөс мөрдөж эхэлсэн. Иймхүү кибер аюулгүй байдлын тухай хуультай болсноор Монгол Улсын Эрүүгийн хуулийн 26 дугаар бүлгийг “Кибер аюулгүй байдлын эсрэг гэмт хэрэг” гэж өөрчлөн найруулж, 26.1 дүгээр зүйл “Кибер орчинд хууль бусаар халдах”, 26.2 дугаар зүйл “Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах” гэх төрлүүдтэй байхаар хуульчилсан.

Кибер аюулгүй байдлын тухай хууль хэрэгжиж эхлэхээс өмнө Эрүүгийн хуулийн 26 дугаар бүлэгт заасан Цахим мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг 2018 онд 53, 2019 онд 67, 2020 онд 164, 2021 онд 160 бүртгэгдсэнээс[3] 2018 онд 3, 2019 онд 9, 2020 онд 11, 2021 онд 6 хэрэг шүүхээр шийдвэрлэсэн[4] тоон үзүүлэлтээс харвал тухайн гэмт хэргийн гаралт 2020 оноос эхлэн хоёр дахин нэмэгджээ.

---

1 Global cybersecurity index 2020, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

2 https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

3 Статистикийн мэдээллийн нэгдсэн сан. Сүүлд хандсан огноо: 2022.08.03, https://1212.mn/tables.aspx?tbl_id=DT_NSO_2300_036V4&13999001_select_all=0&13999001SingleSelect=_t1&CR005_select_all=0&CR005SingleSelect=_217&YearM_select_all=0&YearMSingleSelect=_ 202112_202111_ 202110_202109_202108_202107_202106_202105_ 202104_202103_202102_202101_202012_ 202011_202010_202009_202008_202007_ 202006_202005_202004_202003_202002_202001_ 201912_201911_201910_201909_ 201908_201907_201906_201905_201904_201903_201902_ 201901_201812_201811_201810_201809_201808_201807_201806_201805_201804_201803_ 201802_201801&viewtype=table

4 Статистикийн мэдээллийн нэгдсэн сан. Сүүлд хандсан огноо: 2022.08.03, https://www.1212.mn/tables.aspx?tbl_id=DT_NSO_2300_040V1&CR035_select_all=0&CR035SingleSelect=_1_21&-YearY_select_all=0&YearYSingleSelect=_2018_2019_2020_2021&viewtype=table

Мэдээлэл технологид суурилсан бүтээгдэхүүн, үйлчилгээ тасралтгүй хөгжиж, хэрэглэгчдийн тоо нэмэгдэхийн хирээр кибер гэмт хэргийн хамрах хүрээ өргөжин тэлж байна. Тухайлбал, олон улсад виртуал хөрөнгөд суурилсан гэмт хэргийн тоо 2021 онд дээд хэмжээнд хүрч, хууль бус хаягууд 14 тэрбум ам. доллартой тэнцэх хөрөнгө олж авсан бол энэ тоо 2020 онд 7.8 тэрбум ам. доллар байсныг *Chainalysis* блокчэйн мэдээллийн платформын Крипто гэмт хэргийн тайланд дурджээ.[5]

Виртуал хөрөнгийн үйлчилгээ үзүүлэгч, хөрөнгө оруулагч, виртуал хөрөнгө гаргагчид нь кибер гэмт хэргийн хохирогч болох өндөр эрсдэлтэй бөгөөд виртуал хөрөнгө, түүнд суурилсан үйлчилгээ нь кибер орчинд үйлдэгдэх гэмт хэргийн халдлагын зүйл болж байна. Тухайлбал, хувь хүний данс, цахим хэтэвчид хууль бусаар халдах тохиолдол байх боловч криптобиржийн их хэмжээний криптовалют хадгалах, удирдах зориулалт бүхий цахим хэтэвчүүдэд халдах тохиолдол түгээмэл гарах болсон.

Криптовалютын зах зээлийн хөгжил хурдсахын хэрээр сүүлийн хоёр жилд манай улсад коин, токенууд ихээр гарч, иргэд, олон нийт крипто хөрөнгийн арилжааг сонирхох болж, энэ салбарт хөрөнгө оруулах болсон. Нийгмийн харилцаа цахим хэлбэрт шилжсэнээр түүнийг дагаж их хэмжээний мөнгө эргэлдэх болсон нь тэдгээрийг дагасан гэмт хэргийн гаралтыг нэмэгдүүлсэн. Түүнчлэн судалгаанаас үзэхэд, дэлхийн 43 улсын виртуал хөрөнгийн үйлчилгээ үзүүлэгч, төвлөрсөн бус санхүүгийн платформуудад 2011-2021 онд гарсан кибер аюулгүй байдлын зөрчил болон луйврын нийт 226 тохиолдлын 193 буюу 85.4 хувийг аюулгүй байдал зөрчигдсөн тохиолдол эзэлж байна.[6]

Монгол Улсын хувьд “кибер аюулгүй байдал”, “виртуал хөрөнгийн үйлчилгээ үзүүлэгч” гэх нэр томьёо шинэ ойлголт бөгөөд одоогоор виртуал хөрөнгийн үйлчилгээ үзүүлэгч үүргээ зөрчсөн, эсхүл халдлагад өртсөн гэх асуудлыг шүүхээр шийдвэрлэсэн тохиолдол гараагүй. Гэвч дотоодод тухайн гэмт хэрэг гарсан эсэхээс үл хамаарч виртуал хөрөнгийн үйлчилгээ үзүүлэгч кибер халдлагад өртөж, виртуал хөрөнгө алдагдсан тохиолдолд авах арга хэмжээг судлах, кибер гэмт хэрэг мөрдөн шалгах, гэм буруутай этгээд болон зөрчил гаргасан виртуал хөрөнгийн үйлчилгээ үзүүлэгчид хариуцлага хүлээлгэх хууль тогтоомжийн зохицуулалт тодорхой байх учиртай.

Иймээс судлаачдын баг кибер аюулгүй байдлын эрэг гэмт хэргийн талаарх улс орнуудын зохицуулалт, түүнийг олон улсад хуульчилсан байдал, виртуал хөрөнгийн биржүүдэд хийгдсэн кибер халдлага, тэдгээрийг шалган тогтоож, шийдвэрлэж буй практик, улмаар хэрэглэгч болон виртуал хөрөнгийн биржийн виртуал хөрөнгө алдагдсан тохиолдолд авч буй арга хэмжээг судалсан болно.

---

5 https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/
6 https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/

Судалгааны үр дүнд Монгол Улсын виртуал хөрөнгийн биржид халдлага гарах тохиолдолд дотоодын хуулийн зохицуулалтуудыг оновчтой хэрэглэх зөв практик тогтооход шаардлагатай дүгнэлт, санал боловсруулав.

### Судлагдсан байдал, цаашид судлах асуудал

Кибер гэмт хэрэг буюу цахим орчинд цахим хэрэгсэл ашиглан үйлдэгдэж буй гэмт хэргийн мөн чанар, ойлголт, өнөөгийн байдлын талаар эрдэм шинжилгээний цөөнгүй өгүүлэл нийтлэгджээ. Тухайлбал, Л.Галбаатар "Кибер гэмт хэргийг шүүхэд хянан шийдвэрлэх нь" ном, Д.Булган "Кибер гэмт хэргийн мөн чанар, түүний шинжийг тодорхойлох нь", Б.Өнөрмаа "Цахим хэрэгсэл ашиглан үйлдэгдэж буй гэмт хэргийн шалтгаан нөхцөл, эрх зүйн орчныг боловсронгуй болгох шаардлага", Г.Мөнгөншагай "Цахим гэмт хэрэгтэй тэмцэж буй өнөөгийн байдал, эрх зүйн зохицуулалт", Д.Сумьяацэрэн "Монгол Улс дахь кибер гэмт хэргийн өнөөгийн байдал, дүгнэлт, санал", Б.Цэцэгмаа "Цахим гэмт хэрэгтэй тэмцэж буй өнөөгийн байдал, эрх зүйн зохицуулалт" зэрэг нэг сэдэвт бүтээлүүд гарчээ.

Мөн Хууль зүйн үндэсний хүрээлэнгээс хийж гүйцэтгэсэн "Цахим орчин дахь гэмт хэргээс урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох эрх зүйн зохицуулалт" харьцуулсан судалгаа, Т.Халтар, Т.Баасанжав, Х.Ану нарын "Цахим мэдээллийн аюулгүй байдлын эсрэг (кибер) гэмт хэргийн гүнзгийрүүлсэн судалгаа" болон Б.Солонгын "Кибер гэмт хэргийн эрх зүйн зохицуулалт, өнөөгийн хэрэгжилт" хэмээх эрх зүйн магистрын зэрэг горилсон бүтээл байна.

Дээрх судлаачдын судалгаа, шинжилгээний ажлын агуулгыг ерөнхийлөн нэгтгэвэл тэдгээр нь гагцхүү нэн шинэ төрлийн ойлголтод хамааруулж ерөнхий байдлаар судалжээ. Тодруулбал, ихэнх нь энэ төрлийн гэмт хэргийг тусгайлан хуульчлахаас өмнө судлагдсан тул кибер гэмт хэргийн тухай ойлголт, түүний мөн чанар, төрөл, бүрэлдэхүүний шинж, ижил төрлийн гэмт хэргээс хэрхэн ялгах, Монгол Улсын өнөөгийн байдал хийгээд кибер гэмт хэргээс урьдчилан сэргийлэх нөхцөл боломж, халдлага гарсан тохиолдолд авах арга хэмжээний зохицуулалт байгаа эсэх, нийгмийн хувьсан өөрчлөгдөж буй нөхцөл байдлаас хамаарч хууль, эрх зүйн орчныг цаашид хэрхэн боловсронгуй болгох талаар санал, дүгнэлт гаргасан байна. Тэр ч утгаараа тус сэдвийг судалсан дийлэнх судлаачид судалгааны бүтээлдээ "Кибер гэмт хэргийг тусгайлан хуульчилж, эрх зүйн орчныг боловсронгуй болгох хэрэгцээ, шаардлага зайлшгүй байна" гэсэн дүгнэлтэд хүрчээ.

Цахим гэмт хэрэг, кибер гэмт хэрэг, цахим эрх зүй, цахим мэдээллийн аюулгүй байдлын тухай ном, эрдэм шинжилгээний өгүүллүүд нь өнөөдрийн байдлаар хүчин төгөлдөр даган мөрдөж буй Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн тухай хууль болон 2022 оны 5 дугаар сарын 1-ний өдрөөс мөрдөгдөж эхэлсэн Кибер аюулгүй байдлын тухай, Нийтийн мэдээллийн ил тод байдлын тухай (шинэчилсэн найруулга), Хүний хувийн мэдээлэл

хамгаалах тухай (шинэчилсэн найруулга), Цахим гарын үсгийн тухай (шинэчилсэн найруулга) хуулиуд батлагдахаас өмнө судлагджээ.

Тиймээс энэхүү судалгаа нь Кибер аюулгүй байдлын тухай хууль шинээр батлагдаж, Эрүүгийн хуулиар "Кибер аюулгүй байдлын эсрэг гэмт хэрэг"-ийг зохицуулснаас хойш хийгдэж буй анхны судалгаа болно. Мөн энэ төрлийн гэмт хэргийн зохицуулалтыг хурдацтай хөгжиж буй шинэ салбар болох виртуал хөрөнгийн үйлчилгээний салбарын үйл ажиллагаатай уялдуулан авч үзсэнээрээ шинэлэг юм.

### Судалгааны арга зүй

Судлаачдын багийн зүгээс формал - хууль зүйн үнэлэлт дүгнэлт өгөх болон эрх зүйн харьцуулсан судалгааны аргыг суурь үндэслэл болгосон.

Дараах хүрээнд мэдээлэл цуглуулж, судаллаа. Үүнд:

- Кибер гэмт хэргийг олон улсын баримт бичгүүд болох Кибер гэмт хэргийн тухай конвенц, Дэлхийн Эрүүгийн загвар хуулиар хэрхэн зохицуулсан болох;
- Монгол Улсын Эрүүгийн хууль дахь кибер аюулгүй байдлын эсрэг гэмт хэргийн зохицуулалтыг Кибер гэмт хэргийн тухай конвенц, Дэлхийн Эрүүгийн загвар хууль, судлаачдын байр суурийг судалж, формал-хууль зүйн аргад үндэслэн үнэлэлт дүгнэлт өгөх;
- Кибер аюулгүй байдлын эсрэг гэмт хэргийн зохицуулалтыг ВХҮҮ-ийн үүрэгтэй холбон авч үзэх, кибер аюулгүй байдлыг хамгаалах дотоодын эрх зүйн зохицуулалтыг ВХҮ үзүүлэгчид хэрхэн мөрдөж ажиллах, зөрчсөн тохиолдолд хүлээлгэх хариуцлагыг судалж, анхаарах асуудлыг хууль зүйн үүднээс тодорхойлох;
- Эрүүгийн хэрэг хянан шийдвэрлэх ажиллагаа, кибер гэмт хэрэгтэй тэмцэх олон улсын хамтын ажиллагааны процесст цахим нотлох баримтыг хэрхэн үнэлж, шалган шийдвэрлэж буйд, мөн шүүхийн практикийн судалгаа, мэдээлэл болон Монгол Улсын шүүхийн шийдвэрийн цахим санд буй кибер гэмт хэрэг, цахим нотлох баримт хэрэглэсэнтэй холбоотой тоон мэдээлэл, шийдвэрт дүн шинжилгээ хийж, харьцуулсан дүгнэлт хийх;
- Харьцуулсан судалгааны хүрээнд олон улс дахь виртуал хөрөнгийн биржүүдэд халдсан кибер халдлагуудын жишээ, холбогдох эх сурвалж, материалыг англи, орос, япон, солонгос хэлээр судалж, тэдгээрийг шийдвэрлэж буй практикийг Япон, БНСУ, Сингапур, Хонконг, ОХУ, АНУ, Швейцар, БНЭУ-ын жишээн дээр судална.

# НЭГ. КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЭСРЭГ ГЭМТ ХЭРГИЙН ЗОХИЦУУЛАЛТ БА ВИРТУАЛ ХӨРӨНГИЙН БИРЖИЙН ҮҮРЭГ

## 1.1. Кибер гэмт хэргийн эрх зүйн зохицуулалт, хамрах хүрээ

Мэдээллийн технологийн салбарын хурдацтай хөгжлийн нөлөөгөөр гэмт хэрэг үйлдэх арга, ашиглах зэвсэг, хэрэгсэл болон орчин нөхцөл өөрчлөгдсөөр байна. 1960-аад оны эхээр компьютерыг арилжааны зорилгоор ашиглаж эхэлсэн бөгөөд энэ үеэс компьютерын гэмт хэргийн эхний тохиолдол гарсан гэж үздэг.[7] Улмаар технологийн хөгжлийг дагаж хувь хүн, байгууллагын бүхий л мэдээлэл, баримт бичиг цахим хэлбэрт шилжиж, нийгмийн харилцаа технологиос хамааралтай болсон нь технологи ашиглан үйлдэх гэмт хэрэг нэмэгдэх үндэс болжээ.

“Кибер гэмт хэрэг”[8] гэсэн нэр томьёо нь 1986 онд мэдээллийн системийн хөгжилтэй холбоотой үүссэн[9] ч улс орнуудын эрх зүйн зохицуулалт, эрдэмтэн судлаачдын бүтээлд “Цахим гэмт хэрэг”[10], “Компьютерын гэмт хэрэг”[11], “Кибер аюулгүй байдлын эсрэг гэмт хэрэг”[12] гэх мэт олон нэр томьёо хэрэглэдэг. Компьютерын гэмт хэрэг буюу хууль бус зорилгодоо хүрэхийн тулд компьютер, компьютерын сүлжээ, интернэт ашиглан үйлдэж буй хууль бус үйлдлийг хамтатган “Кибер гэмт хэрэг” гэж нэрлэх болсон.

НҮБ-ын шинжээчид кибер гэмт хэрэгт виртуал орон зай (хүмүүс, баримт, үйл явдлын талаарх мэдээллийг өөр хэлбэрээр агуулсан цахим орчин)-д явагддаг аливаа хууль бус үйлдэл буюу харилцаа холбооны сүлжээ, эсвэл компьютерын систем, сүлжээний эсрэг үйлдэгдсэн бүх гэмт хэргийг хамааруулан авч үздэг.[13] Монгол Улсын Кибер аюулгүй байдлын тухай

---

7 Л.Галбаатар. Кибер гэмт хэргийг шүүхэд хянан шийдвэрлэх нь (Анхны хэвлэл). УБ., 2015, 12 дахь тал., Ian J.Lloyd. 2011. Information Technology Law (Sixth Edition), Oxford University Press. 2011. p.209.

8 Шевченко Елизавета Сергеевна. “Тактика производства следственных действий при расследовании киберпреступлений” диссертация на соискание учебной степени кандитата юридических наук, М., 2016, “Кибер гэмт хэрэг нь кибер орон зайд нийгмийн аюулгүй байдал, өмчид халдсан, хүний эрх болон хуулиар хамгаалагдсан хууль ёсны бусад аших сонирхлыг хөндсөн үйлдлээр илрэх бөгөөд гэмт хэргийн зүйл нь компьютерын мэдээлэл байна”.

9 Бутусова Л.И. Характеристка и сущность киберпреступлений. Журнал “Алтайский юридический вестник”, 2016, №3, с.29.

10 С.Нарангэрэл. Монгол Улсын хууль зүйн нэвтэрхий толь бичиг-2021, УБ., 2021, 639 дэх тал.

11 Bryan A. Garner, Black’s Law Dictionary, 9th edition, 2009, p.455. “Компьютерын гэмт хэрэг гэж хадгалагдсан цахим мэдээллийг устгах болон өөрчлөх зэрэг компьютер ашиглаж үйлдсэн гэмт хэргийг ойлгоно”.

12 Монгол Улсын Эрүүгийн хууль (Шинэчилсэн найруулга). 2015, 26-р бүлэг. https://legalinfo.mn/mn/detail/11634

13 Б.Өнөрмаа. “Цахим хэрэгсэл ашиглан үйлдэгдэж буй гэмт хэргийн шалтгаан нөхцөл, эрх зүйн орчинг боловсронгуй болгох шаардлага” нийтлэл. 2022. https://www.mglbar.mn/news/4065

хуульд виртуал орон зайг “кибер орон зай” гэж тусгасан бөгөөд интернэт болон бусад мэдээлэл, харилцаа холбооны сүлжээ, тэдгээрийн ажиллагааг хангах мэдээллийн дэд бүтцийн хамааралтай цогцоос бүрдсэн биет болон биет бус талбар[14] гэж тодорхойлсон.

Мэдээлэл, харилцаа холбооны сүлжээ “интернэт”-ийн олон талт харилцааг техник, технологи дангаараа зохицуулж чадахгүй нь нэгэнт тодорхой[15] тул тус харилцаанаас үүсэж буй асуудлыг эрх зүйгээр зохицуулах шаардлага гарч байна. Нөгөөтээгүүр кибер гэмт хэргийн онцлогоос хамаарч олон улсын байгууллага, улс орнууд гэмт хэргийн шинэ хэлбэрийг илрүүлэх, таслан зогсоох, урьдчилан сэргийлэхийн тулд түүний эсрэг арга хэмжээ авч, кибер гэмт хэргийн тухай ойлголтыг эрх зүйн үүднээс тодорхойлон, кибер гэмт хэрэгтнүүдийг шийтгэх, хариуцлага тооцох хууль тогтоомж баталж эхэлсэн. Ийнхүү “Кибер аюулгүй байдал” гэх нэр томьёо бий болж, хууль тогтоомжид тусгах, эсхүл тусгайлсан хууль батлан зохицуулж байна.

Монгол Улсын Эрүүгийн хууль (Шинэчилсэн найруулга)-ийн 26 дугаар бүлэгт “Цахим мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг” гэж тусгайлан зохицуулсан. Кибер гэмт хэргийн онцлог нь аливаа улсын нутаг дэвсгэрээр хязгаарлагдахгүй бөгөөд мэдээлэл, харилцаа холбооны сүлжээ “интернэт”-ээр дамжуулан аль ч улс орноос үйлдэх боломжтой тул тухайн гэмт хэрэгтэй тэмцэх, кибер аюулгүй байдлыг хангахад олон улсын хамтын ажиллагаа, нэгдмэл байдал чухал байр суурь эзэлдэг.

Мөн улс орнууд кибер гэмт хэргийн талаарх мэдээлэл солилцох механизм бий болгож байна. Тухайлбал, Шинэ Зеланд Улсад интернэт дэх мэдээллийн аюулгүй байдлын чиглэлээр үйл ажиллагаа явуулдаг *NetSafe* төрийн бус байгууллага нь төрийн байгууллагуудтай хамтран ажилладаг бөгөөд интернэт дэх зохисгүй контентод холбогдох кибер гэмт хэргийн талаарх мэдээлэл үлдээх боломжтой нэгдсэн веб сайт хөгжүүлсэн.[16] Мөн Өмнөд Африкт компьютер болон интернэт ашиглан үйлдсэн гэмт хэргүүдийн талаар иргэдийг мэдээллээр хангах, гэмт хэргийн талаарх гомдол, мэдээлэл тогтмол хүлээн авах *www.Cybercrime.org.za* веб сайт[17] хөгжүүлжээ. АНУ-д интернэт гэмт хэргийн гомдлыг Холбооны мөрдөх товчоо (*FBI*)-ны Хүлээн авах төвд мэдээлэх боломжтой.[18]

Кибер гэмт хэргийг зохицуулж буй эх сурвалжуудыг судалж үзэхэд олон улсад Будапештийн конвенц[19] болон Дэлхийн Эрүүгийн загвар хууль,[20] дотоодод Монгол Улсын Эрүүгийн хууль (Шинэчилсэн найруулга) үндсэн

---

14 Монгол Улсын Кибер аюулгүй байдлын тухай хуулийн 4 дүгээр зүйлийн 4.1.2 дахь хэсэг.

15 МУИС-ийн Хууль зүйн сургуулийн Эрүүгийн эрх зүйн тэнхим. Дэлхийн Эрүүгийн загвар хууль ба орчин үе. УБ., 2013, 7 дахь тал.

16 https://www.netsafe.org.nz/

17 https://cybercrime.org.za/reporting

18 https://www.ic3.gov/Home/ComplaintChoice

19 Convention on Cybercrime (ETS No. 185).

20 Model Criminal Code.

эх сурвалж болж байна. Эдгээр эх сурвалжид кибер гэмт хэргийн онцлог болон төрлүүдийг хэрхэн зохицуулсныг авч үзнэ.

### 1.1.1. Кибер гэмт хэргийн тухай конвенцын зохицуулалт, хамрах хүрээ

Кибер гэмт хэргийн тухай Будапештийн конвенцыг[21] 2001 оны 6 дугаар сарын 22-ны өдөр Европын холбооны Эрүүгийн эрх зүйн хорооноос эцэслэн боловсруулж, 2001 оны 11 дүгээр сарын 8-ны өдөр Европын холбооны төлөөлөгчдийн хорооноос дэмжин, 2001 оны 11 дүгээр сарын 23-ны өдөр Бүгд Найрамдах Унгар Улсын Будапешт хотод гарын үсэг зурах ажиллагаа эхэлсэн.[22]

Будапештийн конвенц нь кибер гэмт хэрэгтэй тэмцэх анхны, хамгийн чухал олон улсын гэрээ бөгөөд компьютерын систем, сүлжээ, өгөгдлийн нууцлал, бүрэн бүтэн байдал, ашиглалтын эсрэг чиглэсэн халдлагыг таслан зогсоох, энэ төрлийн халдлагыг гэмт хэрэг болгон хуульчлах, түүнийг дотоодод болон олон улсын түвшинд илрүүлэх, мөрдөх, яллах, тухайн гэмт хэргээс урьдчилан сэргийлэх үр нөлөөтэй хууль тогтоомж батлах, олон улсын хамтын ажиллагааг шуурхай зохион байгуулах зэрэг асуудлыг зохицуулсан. Мөн Будапештийн конвенцын удиртгал хэсэгт дурдсанаар конвенц нь компьютерын сүлжээ, өгөгдөлтэй холбоотой гэмт хэргийг мөрдөн шалгах, зүйлчлэх, гэмт хэргийн цахим нотлох баримт цуглуулах ажиллагааг зохицуулдаг онцлогтой.

Будапештийн конвенцод компьютерын мэдээлэл, сүлжээний эсрэг гэмт хэрэг (1), компьютерын мэдээлэл, сүлжээний тусламжтай үйлдсэн гэмт хэрэг (2) гэх хоёр шинжийг хамтатган кибер гэмт хэргийг тодорхойлж, түүнийг дөрвөн төрөлд ангилсан.[23] Будапештийн конвенцын хоёрдугаар бүлгийн “Эрүүгийн материаллаг хууль” гэх нэгдүгээр хэсэгт[24] 4 төрөл, нийт 9 гэмт хэргийг дараах байдлаар тусгажээ.

---

[21] Будапештийн конвенцыг тухайн үед 30 улс нэгдэж баталсан ба 2020 оны 9 дүгээр сарын 15-ны өдрийн байдлаар 65 улс нэгдэн орсон байна. Нэгдэн орсон улс орнууд нь өөрийн улсын дотоодын хууль тогтоомждоо тус конвенцын түгээмэл хэм хэмжээг тусгасан. https://www.rm.coe.int/09000016809f44f0 (Сүүлд хандсан: 2022.05.24.)

[22] 정 완 (연구위원, 법학박사), "사이버범죄 방지를 위한 국제공조방안", 형사정책연구, 18권 2호„ (2004), 107 면 https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearch-Bean.artiId=ART001061954, (최종 확인일 2022. 9. 27.)

[23] Л.Галбаатар. Кибер гэмт хэргийг шүүхэд хянан шийдвэрлэх нь (Анхны хэвлэл). УБ., 2015, 12 дахь тал.

[24] https://rm.coe.int/1680081561 Convention on Cybercrime.

| | | |
|---|---|---|
| 1 | Компьютерын өгөгдөл болон системийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлын эсрэг гэмт хэрэг *(Offences against the confidentiality, integrity and availability of computer data and systems)* | 2 дугаар зүйл - Хууль бус нэвтрэлт<br>3 дугаар зүйл - Хууль бусаар саад хийх<br>4 дүгээр зүйл - Өгөгдөлд хөндлөнгөөс оролцох<br>5 дугаар зүйл - Системд хөндлөнгөөс оролцох<br>6 дугаар зүйл - Тоног төхөөрөмж зүй бусаар ашиглах |
| 2 | Компьютер ашигласан гэмт хэрэг *(Computer-related offences)* | 7 дугаар зүйл - Компьютер ашигласан хуурамч баримт<br>8 дугаар зүйл - Компьютер ашигласан залилан |
| 3 | Контент (агуулга)-той холбоотой гэмт хэрэг *(Content-related offences)* | 9 дүгээр зүйл - Хүүхдийн порнографтай холбоотой гэмт хэрэг |
| 4 | Зохиогчийн эрх, түүнд хамаарах эрхийн зөрчилд холбогдох гэмт хэрэг *(Offences related to infringements of copyright and related rights)* | 10 дугаар зүйл - Зохиогчийн эрх болон түүнд хамаарах эрхийн зөрчилд холбогдох гэмт хэрэг |

Кибер гэмт хэрэг нь улсын хилээр хязгаарлагдахгүй[25], үндэстэн дамнаж үйлдэгдэх боломжтой тул улс орнууд дангаар үр дүнтэй урьдчилан сэргийлж, тэмцэх боломжгүй.[26] Тиймээс кибер гэмт хэрэгтэй үр дүнтэй тэмцэх, буруутай этгээдэд хариуцлага ногдуулахад улс орнуудын хамтын ажиллагаа чухал ач холбогдолтой.[27]

Кибер гэмт хэргийн эсрэг үр дүнтэй хариу арга хэмжээ авах систем бүрдээгүй шалтгаан нь улс орнууд кибер гэмт хэргийг дотоодын хууль тогтоомждоо тусгасан боловч үр дүнтэй мөрдөн шалгах, цахим нотлох баримт цуглуулах, эрэн сурвалжлах, яллах, шүүхийн шийдвэр гаргах, гүйцэтгэх олон улсын хамтын ажиллагаа, механизм бүрдээгүйтэй холбоотой.[28]

Мэдээллийн технологи өндөр хөгжсөн улс орнуудын туршлага, үр дүн, дээрх төрлийн харилцааг зохицуулсан хууль тогтоомжийг нягт судалж, үндэсний хууль тогтоомждоо тусгах нь хамгийн оновчтой "гарц"-ын нэг байж болох юм.[29] Судлаачид кибер гэмт хэргийн талаарх олон улсын хамтын ажиллагааг бэхжүүлэхийн тулд Будапештийн конвенцод нэгдэх хэрэгтэй

[25] https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE01572781

[26] 정정일, 사이버범죄에 대한 국제적 대응방안, 343 면

[27] https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE01572781

[28] 한국형사정책연구원, "사이버범죄방지조약에 관한 연구", 2001년, 19 면 https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE01572781

[29] Ц.Хүрэл-Очир. Мэдээллийн технологийн эрх зүйн орчныг бүрдүүлэх асуудалд. "Хууль дээдлэх ёс" сэтгүүл, 2017, №13, 163 дахь тал.

эсэхийг судлах шаардлагатай[30] гэж үзэж, дараах эсрэг тэсрэг байр суурь илэрхийлжээ. Үүнд:

- Улс орнуудын хооронд эрүүгийн хэргийн талаар эрх зүйн харилцан туслалцаа үзүүлэх тухай гэрээ байх боловч бодит байдал дээр тухайн улсын ашиг сонирхол бага тохиолдолд идэвхтэй хамтран ажиллахгүй, цаг хугацаа их зарцуулагддаг тул уг конвенцод нэгдэх шаардлагатай.[31]
- Будапештийн конвенцод нэгдэн орсноор компьютерын өгөгдлийг шуурхай цуглуулах үүрэг хүлээсэн нь хувийн мэдээлэл, Засгийн газрын бүрэн эрхэд халдах эрсдэлтэй,[32] мөн улсын дотоод мэдээлэлд өөр улс нэвтэрч орох нь улсын аюулгүй байдалд нөлөө үзүүлэх тул нэгдэх эсэхийг нухацтай нягтлах шаардлагатай гэж үздэг.[33]

Будапештийн конвенцод анх 30 улс нэгдэж баталснаас хойш 2022 оны байдлаар нийт 67 улс нэгджээ.[34] Харин манай улс уг конвенцод нэгдээгүй бөгөөд нэгдэх эсэхийг шийдэхдээ судлаачдын дээр дурдсан байр суурийг анхаарч үзэхийн зэрэгцээ өөрийн улс орны нөхцөл байдал, эрүүгийн хэрэг хянан шийдвэрлэх ажиллагааны онцлог, энэ чиглэлээр хийгдсэн судалгаануудад үндэслэх нь зүйтэй.

Монгол Улсын Эрүүгийн хуулиар “Кибер аюулгүй байдлын эсрэг гэмт хэрэг”-ийн “кибер орчинд хууль бусаар халдах” болон “кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах” гэсэн хоёр төрлийг тодорхойлсон нь Будапештийн конвенцын Компьютерын өгөгдөл болон системийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлын эсрэг гэмт хэргийн төрөлд хамаарч байна.

Харин цахим хэрэгсэл ашиглан бусдыг залилах гэмт хэргийг өмчийн эсрэг, “кибер орчинд” хүүхэд оролцуулж садар самууныг сурталчилсан гэмт хэргийг хүүхдийн эсрэг, зохиогчийн эрх болон түүнд хамаарах эрхийн зөрчилд холбогдох гэмт хэргийг эдийн засгийн гэмт хэрэгт тус тус хамааруулан зохицуулсан. Эрүүгийн хуулиар зохиогчийн эрх болон түүнд хамаарах эрхийн зөрчилд хамаарах гэмт хэргийн объектив шинжид “цахим орчин”, “цахим хэрэгсэл”, “цахим төхөөрөмж” ашигласан эсэхийг нарийвчилж

30 윤해성·라광현, "주요국의 유럽평의회 사이버범죄방지협약 비준 과정 및 쟁점", 한국경찰학회보 제21권 제3호, (2019.) 123-124면, https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002478962 (최종 확인일 2022. 9. 27.)

31 김만흠 (국회입법조사처장), 국회입법조사처, 제77호, 2020년 12월 1일, 5면

32 박희영·최호진·최성진, 사이버범죄협약 이행입법 연구, 대검찰청 연구 보고서, 2015. 12. 2-3면

33 정태진·이광민, "사이버범죄 대응을 위한 부다페스트협약 가입과 국제공 조 연구", 경찰학논총, 제14권 제2호, (2019). 78면, https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002469538 (최종 확인일 2022. 9. 27.)

34 Будапештийн конвенцод 2022 оны 9 дүгээр сарын 15-ны өдрийн байдлаар 67 улс нэгдээд байгаа бөгөөд гэрээнд гарын үсэг зурсан болон нэгдэн орохыг урьсан нийт 15 орон байна. Нэгдэн орсон улс орнууд нь дотоодын хууль тогтоомждоо тус конвенцын түгээмэл хэм хэмжээг тусгасан. https://www.coe.int/en/web/cybercrime/the-budapest-convention?ref=hackernoon.com

тусгаагүй тул тухайн төрлийн гэмт хэрэг үйлдэхэд эдгээр аргыг ашиглахтай тэмцэх, урьдчилан сэргийлэх арга хэмжээг кибер аюулгүй байдлын эсрэг гэмт хэрэгт хамааруулан үзэх эсэх нь эргэлзээтэй байна.

### 1.1.2. Дэлхийн Эрүүгийн загвар хуулиар тодорхойлсон кибер гэмт хэргийн төрлүүд

Дэлхийн Эрүүгийн загвар хуулийг НҮБ болон Харьцуулсан эрүүгийн эрх зүй судлалын олон улсын хүрээлэн, 80 гаруй орны шинжээч, судлаачдын оролцоотойгоор 2007 онд боловсруулсан.[35]

Дэлхийн Эрүүгийн загвар хууль[36] нь ерөнхий болон тусгай ангиас бүрдэх ба нийт 31 бүлэг, 200 зүйлтэй. Ерөнхий анги нь 14 бүлэг, 1-85 дугаар зүйлийг хамрах бол Тусгай анги нь 17 бүлэг, 86-200 дугаар зүйлийг тус тус хамарна. Тусгай ангийн 16 дугаар бүлэгт "Кибер гэмт хэрэг"-ийг тусгаж, тус гэмт хэргийн таван төрлийг хуульчилсан.

Ийнхүү хуульчлахдаа кибер гэмт хэргийн халдлагын зүйлийг компьютерын систем болон компьютерын өгөгдөл (*data*) гэж хуваан, тэдгээрт зөвшөөрөлгүйгээр нэвтрэх, саад учруулах, устгах, гэмтээх, өөрчлөх, нуух, мөн дээрх гэмт хэргийг үйлдэхдээ тоног төхөөрөмж ашигласан буюу бэлтгэх, худалдах, импортлох зэргээр тоног төхөөрөмж зүй бусаар ашигласан үйлдлийг тус тус гэмт хэрэгт тооцсон.

Дэлхийн Эрүүгийн загвар хуульд заасан кибер гэмт хэргийн төрлүүд, тэдгээрийн объектив шинжийг хүснэгтээр үзүүллээ.[37]

*Хүснэгт 2. Дэлхийн Эрүүгийн загвар хуулиар тодорхойлсон кибер гэмт хэргийн төрөл, объектив шинж*

| № | Гэмт хэрэг | Тухайн гэмт хэрэгт хамаарах хууль бус үйлдэл |
|---|---|---|
| 1 | 184 дүгээр зүйл. Компьютерын системд хууль бусаар нэвтрэх | – Зөвшөөрөлгүйгээр компьютерын системд[38] бүхэлд нь, эсхүл аль нэг хэсэгт нь хууль бусаар нэвтэрсэн гэмт үйлдэл; |
| 2 | 185 дугаар зүйл. Компьютерын мэдээллийн санд хууль бусаар саад хийх | – Зөвшөөрөлгүйгээр, техникийн тусламжтайгаар, компьютерын мэдээллийн санг агуулж буй системээс цахилгаан соронзон долгион илгээх зэргээр компьютерын систем рүү, эсхүл компьютерын мэдээллийг олон нийтэд нээлттэй бус байдлаар дамжуулахад саад учруулах үйлдэл; |

[35] Д.Ренчиндорж. "Дэлхийн Эрүүгийн загвар хууль гаргах болсон шаардлага, үндэслэл, ач холбогдол" эрдэм шинжилгээний өгүүлэл. 2019. https://legaldata.mn/buteel/pdf?id=776

[36] https://www.corteidh.or.cr/tablas/r32562.pdf Model Criminal Code.

[37] Д.Баярсайхан. Дэлхийн Эрүүгийн загвар хууль ба орчин үе. УБ., 2013, 72 дахь тал.

[38] Эрүүгийн загвар хуулийн 184.1 дүгээр зүйлийн 2 дахь хэсэгт "Компьютерын систем" гэдгийг нэг буюу хэд хэдэн программын дагуу мэдээллийг автоматаар боловсруулдаг аливаа төхөөрөмж, эсхүл хоорондоо холбоотой, эсхүл хамааралтай тоног төхөөрөмж гэж тодорхойлсон. https://www.corteidh.or.cr/tablas/r32562.pdf

| | | |
|---|---|---|
| 3 | 186 дугаар зүйл. Компьютерын мэдээллийн санд хөндлөнгөөс орох | – Зөвшөөрөлгүйгээр компьютерын мэдээллийн санг гэмтээх, устгах, өөрчлөх, нуусан бол компьютерын мэдээллийн санд хөндлөнгөөс орсонд тооцно; |
| 4 | 187 дугаар зүйл. Компьютерын системд хөндлөнгөөс оролцох | – Зөвшөөрөлгүйгээр, компьютерын системийг ноцтойгоор саатуулсан, компьютерын мэдээлэл оруулах, дамжуулах, гэмтээх, устгах, эвдэх, өөрчлөх, нуух үйлдлийг ойлгоно. |
| 5 | 188 дугаар зүйл. Тоног төхөөрөмж зүй бусаар ашиглах | – Зөвшөөрөлгүйгээр, компьютерын системд хууль бусаар нэвтрэх; компьютерын мэдээллийн санд хууль бусаар саад хийх, компьютерын мэдээллийн санд хөндлөнгөөс орох, компьютерын системд хөндлөнгөөс орох гэмт хэрэг үйлдэх зорилгоор ямар нэгэн тоног төхөөрөмж ашиглах сэдэл агуулсан байна. Үүнд:<br>– А. Бэлтгэх, худалдах, хэрэглэхээр худалдан авах, импортлох боломж бүрдүүлэх. Үүнд:<br>– А1. Компьютерын системд хууль бусаар нэвтрэх, компьютерын мэдээллийн санд хууль бусаар саад хийх, компьютерын мэдээллийн санд хөндлөнгөөс орох, компьютерын системд хөндлөнгөөс орох гэмт хэрэг үйлдэх зорилгоор боловсруулсан, нийцүүлсэн компьютерын программ зэрэг тоног төхөөрөмж, эсхүл,<br>– А2. Ашиглах нөхцөл бүрдүүлэхийн тулд компьютерын системд нэвтрэхээр компьютерын нууц үг, нэвтрэх код, эсхүл адил төстэй мэдээллийг бүхэлд нь юм уу хэсэгчлэн олж авах,<br>– Б. А.1, А.2 хэсэгт заасны дагуу тоног төхөөрөмж, нууц үг, нэвтрэх код, адил төстэй мэдээлэл эзэмшиж байхыг ойлгоно. |

Дэлхийн Эрүүгийн загвар хуульд тодорхойлж, ангилсан кибер гэмт хэргүүд нь Монгол Улсын Эрүүгийн хуулиар хуульчилсан “Кибер аюулгүй байдлын эсрэг гэмт хэрэг”-ийн агуулгатай төстэй. Тухайлбал, Дэлхийн Эрүүгийн загвар хуулийн 184-187 дугаар зүйлд заасан гэмт хэргүүд нь Монгол Улсын Эрүүгийн хуулийн 26.1. Кибер орчинд хууль бусаар халдах гэмт хэрэгт, 188 дугаар зүйлд заасан гэмт хэрэг нь Эрүүгийн хуулийн 26.2. Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах гэмт хэргийн зохицуулалттай агуулгын хувьд ижил байна.

### 1.1.3. Монгол Улсын Эрүүгийн хууль дахь кибер гэмт хэргийн зохицуулалт

УИХ-аас 2021 оны 12 дугаар сарын 17-ны өдөр Кибер аюулгүй байдлын тухай хууль баталсантай холбогдуулан Эрүүгийн хуульд нэмэлт, өөрчлөлт оруулах тухай хууль баталсан. Тус хуулиар Эрүүгийн хуулийн 26 дугаар бүлэг "Цахим мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэг" гэсэн байсныг "Кибер аюулгүй байдлын эсрэг гэмт хэрэг" болгож өөрчлөн найруулсан. Тодруулбал, Цахим мэдээллийн аюулгүй байдлын эсрэг гэмт хэрэгт (1) Цахим мэдээлэлд хууль бусаар халдах, (2) Цахим мэдээллийн сүлжээнд хууль бусаар халдах программ, техник хэрэгсэл бэлтгэх, борлуулах, (3) Хор хөнөөлт программ хангамж бүтээх, ашиглах, тараах гэсэн гурван төрлийн гэмт хэргийг зүйлчлэн зохицуулж байсныг дараах хоёр төрлийн гэмт хэрэг байхаар өөрчлөн найруулсан:

*Хүснэгт 3. Монгол Улсын Эрүүгийн хуулиар тодорхойлсон кибер аюулгүй байдлын эсрэг гэмт хэрэг*

*26.1 дүгээр зүйл. Кибер орчинд хууль бусаар халдах*

1. Кибер орчинд зөвшөөрөлгүйгээр хандаж мэдээллийн систем, мэдээллийн сүлжээнд нэвтэрсэн, танилцсан;
2. Кибер орчинд хууль бусаар халдаж мэдээллийг устгасан, гэмтээсэн, өөрчилсөн, засварласан, нуусан, нэмж оруулсан, хуулбарлаж авсан, ашиглах боломжгүй болгосон;
3. Кибер орчинд хууль бусаар халдаж мэдээллийн систем, мэдээллийн сүлжээг ашиглах боломжгүй болгосон, хэвийн үйл ажиллагааг алдагдуулсан, хандалтад хязгаарлалт тогтоосон, ноцтой саад учруулсан;
4. Мэдээлэл хадгалагдаж байгаа төхөөрөмжийг устгасан, гэмтээсэн;
5. Гэмт хэргийн улмаас төрийн байгууллагын хэвийн үйл ажиллагаа алдагдсан.

*26.2 дугаар зүйл. Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах*

1. Энэ хуулийн 26.1 дүгээр зүйлд заасан гэмт хэргийг үйлдэх зорилгоор мэдээллийн систем, мэдээллийн сүлжээнд хууль бусаар нэвтрэх тусгай программ, техник хэрэгслийг бэлтгэсэн, борлуулсан, программ хангамжийг тусгайлан зохиосон, зориудаар ашигласан, санаатай тараасан.

Эрүүгийн хуулийн 26 дугаар бүлэгт заасан "цахим мэдээлэл", "цахим мэдээллийн сүлжээнд хууль бусаар халдах" гэснийг "цахим орчинд" гэж Кибер аюулгүй байдлын тухай хуульд нийцүүлэн өөрчилж, "цахим" гэх нэр томьёог цаашид кибер орчинд үйлдэгдсэн гэмт хэрэгт ашиглахаар зохицуулжээ.

Мөн Эрүүгийн хуулийн 17.3 дугаар зүйл. Залилах, 13.10 дугаар зүйл. Хувь хүний нууцад халдах гэмт хэргүүдэд "цахим хэрэгсэл" ашиглаж үйлдэх нөхцөлийг тусгасан байна. Үүнээс гадна Эрүүгийн хуулийн 16.9 дүгээр зүйлийн 2.1 дэх хэсэгт Хүүхэд оролцуулж садар самууныг сурталчлах

гэмт хэргийг “кибер орчныг ашиглаж” үйлдсэн тохиолдолд гэмт хэргийг хүндрүүлэх бүрэлдэхүүнд оруулсан байна.

Монгол Улсын хэмжээнд Эрүүгийн хэргийн анхан шатны шүүхээр 2017 оны 7 дугаар сарын 1-ний өдрөөс 2022 оны 9 дүгээр сарын 1-ний өдөр хүртэлх хугацаанд Монгол Улсын Шүүхийн шийдвэрийн цахим сан *www.shuukh.mn* сайтаас Эрүүгийн хуулийн 26.1 болон 26.2 дугаар зүйлээр зүйлчилж шийдвэрлэсэн, анхан шатны шүүхийн хүчинтэй шийтгэх тогтоолуудыг шүүж үзэхэд шүүхийн нийт 50 шийдвэрийг нээлттэй байршуулжээ.[39] Үүнд:

- Эрүүгийн хуулийн тусгай ангийн 26.1 дүгээр зүйлийн 1 дэх хэсэгт зааснаар ял шийтгэсэн шүүхийн 6 шийдвэр;
- Эрүүгийн хуулийн тусгай ангийн 26.1 дүгээр зүйлийн 2 дахь хэсэгт зааснаар ял шийтгэсэн шүүхийн 22 шийдвэр;
- Эрүүгийн хуулийн тусгай ангийн 26.1 дүгээр зүйл болон 17.1 дүгээр зүйл-Хулгайлах гэмт хэрэгт давхар ял шийтгэсэн шүүхийн 6 шийдвэр;
- Эрүүгийн хуулийн тусгай ангийн 26.1 дүгээр зүйл болон 17.3 дугаар зүйл-Залилах гэмт хэрэгт давхар ял шийтгэсэн шүүхийн 12 шийдвэр;
- Эрүүгийн хуулийн тусгай ангийн 26.1 дүгээр зүйлд зааснаар болон бусад гэмт хэрэгт давхар ял шийтгэсэн шүүхийн 4 шийдвэр.

Дээрх шүүхийн шийдвэрүүдээс үзэхэд кибер орчинд хууль бусаар халдаж мэдээллийг устгасан, гэмтээсэн, өөрчилсөн, засварласан, нуусан, нэмж оруулсан, хуулбарлаж авсан, ашиглах боломжгүй болгосон үйлдэлд ял шийтгэсэн тохиолдол хамгийн их байгаа бол кибер орчинд хууль бусаар халдах гэмт хэргийг бусад гэмт хэрэгтэй буюу хулгайлах, залилах, мөнгө угаах гэмт хэрэгтэй давхар зүйлчлэх тохиолдол мөн цөөнгүй байна. Харин Эрүүгийн хуулийн тусгай ангийн 26.2 дугаар зүйл - кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах гэмт хэрэгт ял шийтгэсэн шүүхийн шийтгэх тогтоол байхгүй.

Эрүүгийн хуулийн 26 дугаар бүлэг Кибер аюулгүй байдлын эсрэг гэмт хэрэг гэх бүлгийг 2021 оны 12 дугаар сарын 17-ны өдрийн хуулиар өөрчлөн найруулсан тул уг хугацаанаас хойш кибер орчинд хууль бусаар халдах гэмт хэрэг үйлдсэнд тооцсон шүүхийн шийтгэх тогтоолуудыг ялган авч үзлээ.

[39] https://shuukh.mn/cases/2/1

*Хүснэгт 4. Кибер орчинд хууль бусаар халдах гэмт хэргээр зүйлчилсэн шүүхийн шийдвэрүүд 2021.12.17-2022.09.01*

| № | Шүүх | Үйл баримт | Шийдвэрлэсэн байдал |
|---|---|---|---|
| 1 | Сонгинохайрхан дүүргийн эрүүгийн хэргийн анхан шатны шүүх[40] Огноо: 2022.07.26 Дугаар: 2022/ШЦТ/962 | Шүүгдэгч Х.А нь бусдын фейсбүүк хаягт хууль бусаар нэвтэрч, тухайн цахим хаягийг ашиглан хохирогч Д.Ц-гээс 700.000 төгрөгийг хуурч, зохиомол байдлыг зориудаар бий болгон залилсан. | Эрүүгийн хуулийн тусгай ангийн 26.1 дүгээр зүйлийн 1 дэх хэсэгт заасан цахим мэдээлэлд хууль бусаар халдах, мөн хуулийн тусгай ангийн 17.3 дугаар зүйлийн 1 дэх хэсэгт заасан залилах гэмт хэрэг үйлдсэн гэм буруутайд тус тус тооцож, ял шийтгэсэн. |
| 2 | Сүхбаатар дүүргийн эрүүгийн хэргийн анхан шатны шүүх[41] Огноо: 2022.06.22 Дугаар: 2022/ШЦТ/662 | Л.Д, Д.Б нар урьдаас тохиролцож үргэлжилсэн үйлдлээр, шунахайн сэдэлтээр, хялбар аргаар мөнгө олох зорилгоор 2018 оны 3-5 дугаар сарын хооронд нэр бүхий хохирогчдын дансны мэдээллийг хууль бусаар тусгайлан бэлтгэсэн төхөөрөмж дээр хуулбарлан бэлтгэж, Малайз Улсын иргэдэд мэдээллийг өгч, хамжигчаар оролцон, арилжааны банкуудын бэлэн мөнгөний машинаас нэр бүхий 42 хохирогчийн данснаас нийт 71.790.800 төгрөгийг хүч хэрэглэхгүйгээр, нууцаар, хууль бусаар хулгайлан авч, их хэмжээний хохирол учруулсан, мөн бүлэглэн нэр бүхий иргэдийн цахим төхөөрөмж, мэдээллийн сүлжээнд хууль бусаар халдаж мэдээллийг хуулбарлан авч Малайз Улсын иргэдэд хууль бусаар дамжуулсан. | Эрүүгийн хуулийн тусгай ангийн 17.3 дугаар зүйлийн 2 дахь хэсгийн 2.2-т заасан бусдыг хуурч, цахим хэрэгсэл ашиглаж, эзэмшигч, өмчлөгчийн эд хөрөнгө, эд хөрөнгийн эрхийг шилжүүлэн авсан гэмт хэрэгт хамжигчаар хамтран оролцож, их хэмжээний хохирол учруулсан гэмт хэрэг үйлдсэн гэм буруутайд, мөн хуулийн тусгай ангийн 26.1 дүгээр зүйлийн 2 дахь хэсэгт заасан цахим мэдээллийн сүлжээнд хууль бусаар халдаж мэдээллийг хуулбарлаж авсан гэмт хэрэг үйлдсэн гэм буруутайд тус тус тооцож, ял шийтгэсэн. |

[40] https://shuukh.mn/single_case/77252?daterange=2021-12-17%20-%202022-10-01&id=1&court_cat=2&bb=1

[41] https://shuukh.mn/single_case/76753?daterange=2021-12-17%20-%202022-10-01&id=1&court_cat=2&bb=1

| | | | |
|---|---|---|---|
| 3 | Баянзүрх дүүргийн эрүүгийн хэргийн анхан шатны шүүх[42] Огноо: 2022.05.03 Дугаар: 2022/ ШЦТ/645 | Шүүгдэгч О.Б нь 2021.11.16-ны өдрөөс 30-ны хооронд хохирогч Т.Т-г гэртээ байхад түүний *DAX* нэртэй криптовалютын биржид бүртгэлтэй хэтэвчид байсан 2.383.710 ширхэг *IHC* коиныг авах зорилгоор хохирогчийн *** гэх мэйл хаягаар дамжин, *DAX* нэртэй криптовалютын биржид бүртгэлтэй хэтэвчид нэвтрэх цахим төхөөрөмж, мэдээлэлд тусгай программ ашиглан хууль бусаар халдаж нэвтэрсэн, улмаар тус бирж дээр гүйлгээ хийх тохиолдолд нэг удаагийн нэвтрэх нэр, нууц үг, хэтэвч эзэмшигчийн гар утсанд суулгасан *Ard* аппликейшнд ирснийг мөн хууль бусаар олж авсан, улмаар мэдээллийг өөрчилсөн, мэдээлэл нэмж оруулсны улмаас хохирогчид 2.383.710 ширхэг *IHC* коин буюу 10.478.147 төгрөгийн хохирол учруулж, бусдын цахим мэдээлэлд хууль бусаар халдаж, мэдээллийг өөрчилсөн, 2021.12.01-ний өдөр хохирогч Т.Т-гийн *DAX* нэртэй криптовалютын биржид бүртгэлтэй хэтэвчид байсан 2.383.710 ширхэг *IHC* коиныг Эрүүгийн хууль-д заасан цахим мэдээлэлд хууль бусаар халдах гэмт хэрэг үйлдэж, өөрийн *Binance* нэртэй криптовалютын бирж дэх хэтэвчдээ шилжүүлж авсан гэдгээ мэдсээр байж, *USDT* коин болгон хувиргаж хэтэвчдээ хадгалан эзэмшсэн. | О.Б-г цахим мэдээлэлд хууль бусаар халдаж, мэдээллийг өөрчилснийулмаас хохирогчийн хууль ёсны ашиг сонирхолд хохирол учирсан буюу Эрүүгийн хуулийн тусгай ангийн 26.1 дүгээр зүйлийн 2 дахь хэсэгт заасан гэмт хэрэг үйлдсэн гэм буруутайд, мөн гэмт хэргийн улмаас олсон мөнгө гэдгийг мэдсээр байж түүнийг эзэмшсэн, ашигласан буюу Эрүүгийн хуулийн тусгай ангийн 18.6 дугаар зүйлийн 1 дэх хэсэгт заасан гэмт хэрэг үйлдсэн гэм буруутайд тус тус тооцож, ял шийтгэсэн. |

[42] https://shuukh.mn/single_case/66652?daterange=2021-12-17%20-%202022-10-01&id=1&court_cat=2&bb=1

| | | | |
|---|---|---|---|
| 4 | Дархан-Уул аймаг дахь сум дундын эрүүгийн хэргийн анхан шатны шүүх[43] Огноо: 2022.04.19 Дугаар: 2022 /ШЦТ/147 | Шүүгдэгч Б.О нь цахим хэрэгсэл ашиглан зохиомол байдлыг зориудаар бий болгож, Ч.Г-гийн фейсбүүк хаягт хууль бусаар халдаж Г.З-д “Ахдаа 300.000 төгрөг зээлээч” гэх мессеж явуулан төөрөгдөлд оруулж, хуурч мэхлэн ХААН банкны 5127150093 дугаарын данс руу 300.000 төгрөг шилжүүлэн авч залилсан. | Эрүүгийн хуулийн тусгай ангийн 17.3 дугаар зүйлийн 1 дэх хэсэгт заасан “Залилах” гэмт хэрэг үйлдсэн гэм буруутайд, мөн цахим мэдээллийн сүлжээнд хууль бусаар халдаж, Эрүүгийн хуулийн тусгай ангийн 26.1 дүгээр зүйлийн 1 дэх хэсэгт заасан гэмт хэрэг үйлдсэн гэм буруутайд тус тус тооцож, ял шийтгэсэн. |
| 5 | Дархан-Уул аймаг дахь сум дундын эрүүгийн хэргийн анхан шатны шүүх[44] Огноо: 2022.01.20 Дугаар: 2022 /ШЦТ/41 | Шүүгдэгч О.И нь З.Л-ийн фейсбүүк хаягт хууль бусаар халдаж, улмаас уг хаягийг ашиглан иргэн З.Л-ийн нэрийн өмнөөс Л.И-д “Хүн рүү мөнгө шилжүүлээд өгөөч” гэж зурвас илгээн хуурч мэхлэн 100,000 төгрөгийг Хаан банкны Ч.М-ийн эзэмшлийн XXXXXXXX дугаартай дансаар шилжүүлэн авч залилсан. | И-г цахим төхөөрөмж, мэдээллийн сүлжээнд хууль бусаар халдсан, Эрүүгийн хуулийн тусгай ангийн 26.1 дүгээр зүйлийн 1 дэх хэсэгт заасан гэмт хэрэг үйлдсэн гэм буруутайд, хуурч, цахим хэрэгсэл ашиглаж зохиомол байдлыг зориудаар бий болгож бодит байдлыг нуух замаар бусдыг төөрөгдөлд оруулж, эзэмшигч, өмчлөгчийн эд хөрөнгө, эд хөрөнгийн эрхийг шилжүүлэн авч бага хэмжээнээс дээш хохирол учруулсан, Эрүүгийн хуулийн тусгай ангийн 17.3 дугаар зүйлийн 1 дэх хэсэгт заасан гэмт хэрэг үйлдсэн гэм буруутайд тус тус тооцож, ял шийтгэсэн. |

[43] https://shuukh.mn/single_case/66740?daterange=2021-12-17%20-%202022-10-01&id=1&court_cat=2&bb=1

[44] https://shuukh.mn/single_case/66975?daterange=2021-12-17%20-%202022-10-01&id=1&court_cat=2&bb=1

Монгол Улсын шүүхийн практикт, Эрүүгийн хуулийн 26.1-д заасан гэмт хэргийг хулгайлах, цахим хэрэгсэл ашиглаж залилах гэмт хэрэгтэй давхар зүйлчилж шийдвэрлэх нь түгээмэл байна. Тухайлбал, бусдын нийгмийн сүлжээ болох *Facebook* хаягт зөвшөөрөлгүйгээр нэвтрэх замаар хохирогчийн хөрөнгийг хууль бусаар олж авч гэмт хэрэг үйлдсэн тохиолдолд кибер орчинд хууль бусаар халдах гэмт хэрэг, залилах гэмт хэргээр давхар зүйлчилж байна. Иймээс хувь хүн өөрийн кибер аюулгүй байдлыг хангах буюу олон нийтийн зориулалттай интернэт, компьютер ашиглахдаа тухайн веб хөтчид мэдээллээ хадгалахгүй байх, нууц үгийн аюулгүй байдлыг хангах зайлшгүй шаардлага үүсэж байна.

Мөн Монгол Улсад виртуал хөрөнгийн биржийн цахим хэтэвчийн нэвтрэх нэр, нууц үгийг олж аван өөрчилж, хэтэвчнээс виртуал хөрөнгийг хууль бусаар авч ашигласан үйлдэлд ял шийтгэжээ. Үүнтэй холбоотойгоор хувь хүн виртуал хөрөнгийн бирж (платформ)-д нэвтрэх харилцагчийн нууц үгийн аюулгүй байдлыг хангах, харин ВХҮҮ нь дээр дурдсан аргаар үйлдэгдэж буй кибер гэмт хэргээс урьдчилан сэргийлэх үүднээс харилцагчийг давхар таньж баталгаажуулах систем нэвтрүүлж, аюулгүй байдлыг хангах шаардлагатай юм.

### 1.2. Виртуал хөрөнгийн үйлчилгээнд ашиглах мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангах виртуал хөрөнгийн биржийн үүрэг

Монгол Улсад ВХҮҮ-ийн кибер халдлагаас сэргийлэх үүрэг хариуцлагыг Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн тухай хууль (ВХҮҮтХ), Кибер аюулгүй байдлын тухай хууль, Зөрчлийн тухай хууль болон Хорооны баталсан Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн үйл ажиллагааны журам, Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журмаар тус тус зохицуулж байна. Энэ хэсэгт ВХҮҮ-д хүлээлгэсэн үүрэг, зөрчсөн тохиолдолд оногдуулах хариуцлагыг хэрхэн зохицуулсныг авч үзэх болно.

#### 1.2.1. ВХҮҮтХ-аар хүлээсэн үүрэг, зөрчилд хүлээлгэх хариуцлага, гадаад орнуудын зохицуулалт

Мөнгө угаах, терроризмыг санхүүжүүлэх (МУТС)-тэй тэмцэхэд хэрэгжүүлэх үйл ажиллагааны шаардлага нь виртуал хөрөнгийн эрх зүйн зохицуулалттай хэрхэн нийцэж байгааг тодорхойлох, тэдгээр шаардлагыг ВХҮҮ-д мөрдүүлэх зорилгоор ФАТФ-ын Зөвлөмж 15-д[45] “виртуал хөрөнгө”, “ВХҮҮ” гэсэн тодорхойлолтууд оруулж, улс орнуудаас ВХҮҮ-дийг бүртгэх, эсхүл тусгай зөвшөөрөл олгох замаар зохицуулалттай болохыг шаардсан.

[45] https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf

Монгол Улс нь ФАТФ-ын зөвлөмжийн хэрэгжилтийг хангах үүднээс[46] 2021 оны 12 дугаар сарын 17-ны өдөр Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн тухай хууль баталж, виртуал хөрөнгийн үйлчилгээ үзүүлэх хуулийн этгээдийг Хорооноос бүртгэж, үйл ажиллагаанд нь хяналт тавихаар хуульчилсан.

Тус хуулиар ВХҮҮ-д харилцагчийн эрх ашгийг хамгаалж, харилцагчтай шударга, ойлгомжтой, төөрөгдөлд оруулахгүйгээр харилцахыг үүрэг болгосны зэрэгцээ кибер аюулгүй байдлыг хангахтай холбоотой дараах үүргүүдийг хүлээлгэсэн. Үүнд:

- Виртуал хөрөнгийн үйлчилгээнд ашиглах мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангасан байх /ВХҮҮтХ 7.1.2/;
- Өөрийн харилцагчийн тухайн үйлчилгээнд хамаарах виртуал хөрөнгө болон мөнгөн хөрөнгийг гүйлгээ хийх, шилжүүлэх, арилжих, хадгалах, удирдах нөхцөл, боломжийг тасралтгүй хангаж ажиллах /ВХҮҮтХ 8.1.4/;
- Үйл ажиллагаагаа эхлүүлэхээс өмнө болон үйл ажиллагаа эрхлэхдээ хуульд заасан болон Хорооноос тогтоосон шаардлагыг бүрэн хангаж ажиллах /ВХҮҮтХ 8.1.1/.

ВХҮҮ хуулиар хүлээсэн дээрх үүргээ зөрчсөн, нэмэлт шаардлагыг хангаж ажиллаагүй бол үйл ажиллагааны онцлог, зөрчлийн шинж байдлыг харгалзан дараах төрлийн хариуцлага хүлээлгэнэ. Үүнд:

- Үүргээ биелүүлээгүйгээс үүдэн гарах хохирлыг төлүүлэх;
- Үйл ажиллагааг нь хязгаарлах;
- Үйл ажиллагааг нь түр зогсоох;
- Бүртгэлээс хасах;
- Зөрчлийн тухай хуульд заасан торгуулийн шийтгэл оногдуулах.

[46] Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн тухай хуулийн төслийн үзэл баримтлал, https://mojha.gov.mn/wp-content/uploads/2021/01/VASP-%D1%82%D0%B0%D0%B-D%D0%B8%D0%BB%D1%86%D1%83%D1%83%D0%BB%D0%B3%D0%B0.pdf

| № | Хүлээлгэсэн үүрэг | Үр дагавар, хариуцлага |
|---|---|---|
| 1 | ВХҮҮ-ийн хангасан байх шаардлага /ВХҮҮтХ 7.1/:<br>– Виртуал хөрөнгийн үйлчилгээнд ашиглах мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангасан байх;<br><br>ВХҮҮ-ийн үүрэг /ВХҮҮтХ 8.1/:<br>– Үйл ажиллагаагаа эхлүүлэхээс өмнө болон үйл ажиллагаа эрхлэхдээ хуульд заасан болон Хорооноос тогтоосон шаардлагыг бүрэн хангаж ажиллах; | Зөрчлийн тухай хуулиар хүлээлгэх хариуцлага:<br>– Виртуал хөрөнгийн үйлчилгээ үзүүлэгч, түүний эрх бүхий албан тушаалтан болон холбогдох этгээд нь хуульд заасан шаардлагыг хангаж ажиллаагүй, эсхүл үүргээ хэрэгжүүлээгүй, түүнийг зөрчсөн бол хүнийг хоёр мянган нэгжтэй тэнцэх хэмжээний төгрөгөөр, хуулийн этгээдийг хорин мянган нэгжтэй тэнцэх хэмжээний төгрөгөөр торгоно /11.33 дугаар зүйлийн 5 дахь хэсэг/.<br><br>ВХҮҮтХ-аар хүлээлгэх хариуцлага:<br>– Виртуал хөрөнгийн үйлчилгээ үзүүлэгч хууль, эсхүл Хорооноос тогтоосон нэмэлт шаардлагыг хангаж ажиллаагүй бол үйл ажиллагааны онцлог, зөрчлийн шинж байдлыг харгалзан үйл ажиллагааг нь хязгаарлах, түр зогсоох, эсхүл бүртгэлээс хасна /ВХҮҮтХ 11.1/.<br>– Виртуал хөрөнгийн үйлчилгээ үзүүлэгч бүртгэлээс хасагдсан бол энэ хуулийн 6.1-д заасан үйл ажиллагаа эрхлэх эрх дуусгавар болно /ВХҮҮтХ 11.2/. |
| 2 | ВХҮҮ-ийн үүрэг /ВХҮҮтХ 8.1/:<br>– Өөрийн харилцагчийн тухайн үйлчилгээнд хамаарах виртуал хөрөнгө болон мөнгөн хөрөнгийг гүйлгээ хийх, шилжүүлэх, арилжих, хадгалах, удирдах нөхцөл, боломжийг тасралтгүй хангаж ажиллах; | Зөрчлийн тухай хуулиар хүлээлгэх хариуцлага:<br>– Виртуал хөрөнгийн үйлчилгээ үзүүлэгч өөрийн харилцагчийн тухайн үйлчилгээнд хамаарах виртуал хөрөнгийг гүйлгээ хийх, шилжүүлэх, арилжих, хадгалах, удирдах нөхцөл, боломжийг тасралтгүй хангаж ажиллаагүй бол хуулийн этгээдийг арван мянган нэгжтэй тэнцэх хэмжээний төгрөгөөр торгоно /11.33 дугаар зүйлийн 2 дахь хэсэг/.<br><br>ВХҮҮтХ-аар хүлээлгэх хариуцлага:<br>– Энэ хуулийн 8.1.4-т заасан үүргийг биелүүлээгүйгээс үүдэн гарах хохирлыг хариуцах /ВХҮҮтХ 8.1.5/;<br>– Виртуал хөрөнгийн үйлчилгээ үзүүлэгч хууль, эсхүл Хорооноос тогтоосон нэмэлт шаардлагыг хангаж ажиллаагүй бол үйл ажиллагааны онцлог, зөрчлийн шинж байдлыг харгалзан үйл ажиллагааг нь хязгаарлах, түр зогсоох, эсхүл бүртгэлээс хасна /ВХҮҮтХ 11.1/.<br>– Виртуал хөрөнгийн үйлчилгээ үзүүлэгч бүртгэлээс хасагдсан бол энэ хуулийн 6.1-д заасан үйл ажиллагаа эрхлэх эрх дуусгавар болно /ВХҮҮтХ 11.2/. |

ВХҮҮ нь мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангасан байх хуульд заасан үүргээ зөрчсөн бол ВХҮҮтХ болон Зөрчлийн тухай хуулиар хариуцлага хүлээх боловч ийнхүү хуульд заасан үүргээ биелүүлэхгүй байгаа эс үйлдэхүй нь Эрүүгийн хуульд хуульчилсан кибер аюулгүй байдлын эсрэг гэмт хэрэгт хамаарахгүй. Иймд ВХҮҮ аливаа халдлагад өртсөн тохиолдолд хуулиар хүлээсэн дээрх үүргээ биелүүлж ажилласан эсэхийг ямар шалгуураар, хэрхэн дүгнэх вэ гэх асуудал хөндөгдөнө.

Хороо нь ВХҮҮтХ-ийн 10 дугаар зүйлийн 10.9.1 дэх заалтад заасан ВХҮҮ-ийн бүртгэл, үйл ажиллагааны шаардлагыг тодорхойлох, журам батлах бүрэн эрхийнхээ хүрээнд 2022 оны 4 дүгээр сарын 6-ны өдрийн 174 дугаартай тогтоолоор Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журмыг баталж, тус журмын гуравдугаар хавсралтаар ВХҮҮ-ийн үйл ажиллагаандаа мөрдөх мэдээллийн технологийн стандартын жагсаалтыг баталсан. Нийт 11 стандарт хангаж ажиллахаар зааснаас MNS ISO/IEC 27001 стандартаас бусдыг нь 2023 оны 3 дугаар сарын 31-ний өдрөөс дагаж мөрдөх юм.

Дээр өгүүснээс дүгнэвэл ВХҮҮ нь Хорооны баталсан журмын хавсралтаар тогтоосон стандартуудыг хангаж, үүнийг хөндлөнгийн эрх бүхий байгууллага баталгаажуулсан бол ВХҮҮтХ-ийн 7 дугаар зүйлийн 7.1.2-т заасан технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлын шаардлагыг хангасан гэж үзэхээр байна.

Мөн кибер халдлагын улмаас виртуал хөрөнгийн биржийн үйл ажиллагаа тасалдсан тохиолдолд ВХҮҮ-ийг ВХҮҮтХ-ийн 8 дугаар зүйлийн 8.1.4-т зааснаар харилцагчийн виртуал хөрөнгө болон мөнгөн хөрөнгийн гүйлгээ хийх, шилжүүлэх, арилжих, хадгалах, удирдах нөхцөл, боломжийг тасралтгүй хангаж ажиллах үүргээ зөрчсөн гэж үзэх эсэх нь эргэлзээтэй. Учир нь хуулийн энэ заалт хэт ерөнхий зохицуулалттай. Өөрөөр хэлбэл, ВХҮҮ нь Хорооноос тогтоосон стандартыг мөрдөж ажиллаагүйн улмаас, эсхүл мөрдөж ажилласан аль ч тохиолдолд кибер халдлагад өртөх эрсдэл бий. Тиймээс мэдээлэл технологийн тасралтгүй, хурдацтай хөгжил, гэм буруугийн хэлбэрийг харгалзсан байдлаар тухайлан зохицуулаагүйгээс цаашид хууль хэрэглээний төвөгтэй байдлыг үүсгэхээр байна.

Иймд ВХҮҮ-ийн виртуал хөрөнгийн үйлчилгээнд ашиглах мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангах үүргийг улс орнууд хууль тогтоомждоо хэрхэн тусгасныг дараах хэсэгт судалж үзлээ.

## БНСУ

БНСУ-ын виртуал хөрөнгийн зах зээлд биржийн кибер халдлага, олон үе шаттай санхүүгийн луйвар, үнийн манипуляц зэргийн улмаас хэрэглэгчид хохирч байгаа тул хэрэглэгчийн эрхийг хамгаалах шаардлага үүссэн,[47] мөн блокчэйн технологийн судалгаа, хөгжлийг хурдасгаж, аж үйлдвэрийн хөгжлийг дэмжих шаардлагатай[48] болсон тул виртуал хөрөнгийн үйлчилгээний талаарх 6 хуулийн төсөл боловсруулсан нь Байнгын хороодын шалгалтын шатанд байна.[49]

Тус хуулийн төслүүдэд биржийн кибер халдлагаас сэргийлэх үүрэг, хариуцлагыг зохицуулахдаа гэм буруугийн зарчмыг ашигласан байна. Энэ асуудлыг Виртуал хөрөнгийн үйлчилгээний хуулийн төсөлд дараах байдлаар тусгасан.[50]

*Хүснэгт 6. БНСУ-ын Виртуал хөрөнгийн үйлчилгээний хуулийн төсөл*

*24 дүгээр зүйл (Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн үүрэг)*
Виртуал хөрөнгийн үйлчилгээ үзүүлэгч нь виртуал хөрөнгө хэрэглэгчийг хамгаалах үүднээс дараах үр дагаврыг гаргахгүйн тулд Ерөнхийлөгчийн шийдвэрээр шаардлагатай арга хэмжээг авна. Үүнд:

1. Виртуал хөрөнгийн арилжаанд “Санхүүгийн цахим гүйлгээний хууль”-ийн 2 дугаар зүйлийн 10 дахь хэсэгт заасан хуурамч хандалт хийх, эсхүл өөрчилсний улмаас гарах үр дагавар;
2. Гэрээ байгуулах, эсхүл арилжааны зааврыг цахимаар дамжуулах, боловсруулах явцад гарах үр дагавар;
3. Виртуал хөрөнгийн арилжааны цахим төхөөрөмж, эсхүл “Мэдээлэл, харилцаа холбооны сүлжээг хурдасгах болон мэдээллийн аюулгүй байдлыг хангах тухай хууль”-ийн 2 дугаар зүйлийн 1 дэх хэсгийн 1 дэх заалтад заасан мэдээлэл, харилцаа холбооны сүлжээнд халдаж, хуурах болон зүй бус бусад аргаар хийсэн хандалт ашигласнаас үүссэн үр дагавар;

*25 дугаар зүйл (Хохирол барагдуулах)*
Энэ хуулийн 24 дүгээр зүйлийг зөрчсөн виртуал хөрөнгийн үйлчилгээ үзүүлэгч нь Ерөнхийлөгчийн шийдвэрийн дагуу хохирлыг барагдуулна. Хэрэв виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн санаатай, эсхүл илт болгоомжгүй гэм буруутай нь тогтоогдоогүй бол хохирлыг барагдуулахгүй.[51]

---

47 [2109935] 가상자산업법안(이용우의원등20인) http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_E2A1O0O5E0K6X1U1B3T2Y5U-0V1T5Z0, (최종 확인일 2022. 9. 27)

48 [2111459] 가상자산 거래 및 이용자 보호 등에 관한 법률안(권은희의원 등 10인) http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_K2T1V0H6U0L9M0X9A4W8A3G-0W7Q6H1, (최종 확인일 2022. 9. 27.)

49 의안정보시스템에서 가상자산으로 총6건이 검색되었습니다, http://likms.assembly.go.kr/bill/BillSearchResult.do , (최종 확인일 2022. 9. 27)

50 [2109935] 가상자산업법안(이용우의원등20인) http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_E2A1O0O5E0K6X1U1B3T2Y5U-0V1T5Z0, (최종 확인일 2022. 9. 27)

51 가상자산업법안, http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_E2A1O0O5E0K6X-1U1B3T2Y5U0V1T5Z0, (최종 확인일 2022. 9. 27)

Дээрх зохицуулалтаас үзвэл ВХҮҮ нь виртуал хөрөнгийн хэвийн үйл ажиллагааг хангах үүднээс Ерөнхийлөгчийн шийдвэрт заасан арга хэмжээг авч хэрэгжүүлэх бөгөөд энэ үүргээ эс биелүүлбэл хохирлыг барагдуулахаар зохицуулжээ. Хохирол барагдуулахын тулд ВХҮҮ-ийн санаатай, эсхүл илт болгоомжгүй үйлдэл байхыг шаардсан.

БНСУ-ын Виртуал хөрөнгийн үйлчилгээний хуулийн төслийн 24, 25 дугаар зүйлийн зохицуулалтыг Монгол Улсын ВХҮҮтХ-ийн 8 дугаар зүйлийн 8.1.4, 8.1.5 дахь заалтын зохицуулалттай харьцуулан үзвэл БНСУ-ын хувьд ВХҮҮ нь гэм буруугүй тохиолдолд хариуцлагаас чөлөөлөгдөхөөр байгаа нь ач холбогдолтой. Харин Монгол Улсын хувьд гэм буруугийн зарчмыг харгалзан үзээгүй бөгөөд виртуал хөрөнгийн биржийн үйл ажиллагаа тасалдсан бүхий л тохиолдолд ВХҮҮ хариуцлага хүлээхээр зохицуулсан нь гэм буруугийн зарчимд нийцэхгүй юм.

### Сингапур Улс

Сингапурын Кибер аюулгүй байдлын тухай хуулийн[52] нэгдүгээр хавсралтаар үндэсний аюулгүй байдал, батлан хамгаалах, гадаад харилцаа, эдийн засаг, нийгмийн эрүүл мэнд, нийтийн аюулгүй байдал, нийтийн хэв журам хамгаалахад зайлшгүй шаардлагатай үйлчилгээнүүдийг баталсан ба энэ хавсралтын 12-т “төлбөрийн үйлчилгээ”-г тусгасан. Тус хуульд зааснаар ВХҮҮ нь төлбөрийн үйлчилгээ үзүүлэгч буюу дижитал төлбөрийн токены үйлчилгээ үзүүлэгч (*Digital Payment Token Services Providers*) юм.

Сингапурын парламентаас 2022 оны 4 дүгээр сарын 5-ны өдөр “Санхүүгийн үйлчилгээ, зах зээлийн тухай хууль”[53] баталж, дижитал токены үйлчилгээг тусгай зөвшөөрөлтэй эрхлэхээр хуульчилсан.

*Хүснэгт 7. Сингапурын Санхүүгийн үйлчилгээ, зах зээлийн тухай хууль*

*2 дугаар зүйл (Нэр томьёоны тайлбар)*

(р) Дижитал төлбөрийн токен үйлчилгээ үзүүлэгч нь энэ хуулиар зохицуулсан “санхүүгийн байгууллага”-д хамаарна.

*29 дүгээр зүйл (Эрх бүхий байгууллагын технологийн эрсдэлийн удирдлагатай холбоотой эрх хэмжээ)*

1. Санхүүгийн байгууллага нь кибер аюулгүй байдлын эрсдэлийн технологийн менежмент, санхүүгийн үйлчилгээг аюулгүй, найдвартай хүргэх, өгөгдөл хамгаалах технологийн аюулгүй байдлыг хангаж ажиллах ба энэ талаар заавар, журам гаргана.
2. (1)-д заасныг хангаж ажиллаагүй, эрх бүхий байгууллагаас өгсөн зааврыг дагаж мөрдөөгүй бол 1 сая ам. доллар хүртэлх дүнгээр торгох ба шийтгэл хүлээснээс хойш энэхүү үйлдлийг үргэлжлүүлсэн бол өдөр тутамд 100,000 ам. долларoор торгоно.

[52] Cybersecurity Act. https://sso.agc.gov.sg/Act/CA2018?ProvIds=Sc1-#Sc1-

[53] Financial services and markets act 2022. https://www.parliament.gov.sg/docs/default-source/default-document-library/financial-services-and-markets-bill-4-2022.pdf

Дээрх зохицуулалтаас үзэхэд Сингапур Улс виртуал хөрөнгийн үйлчилгээнд ашиглах технологийн аюулгүй байдал, тасралтгүй, найдвартай ажиллагааг хангах виртуал хөрөнгийн биржийн үүргийг Монгол Улстай адил хуулиар хүлээлгэжээ.

### Япон Улс

Япон Улсад виртуал хөрөнгийн дотоодын эрх зүйн зохицуулалт 2017 онд бий болсон ч Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн тухай Засгийн газрын тогтоолыг[54] 2017 оны 3 дугаар сарын 24-ний өдөр баталснаар ВХҮҮ-чид, тэдгээрийн харилцааг хууль тогтоомжоор зохицуулж эхэлсэн. Уг тогтоолыг даган хэд хэдэн хуульд нэмэлт өөрчлөлт орсноос гол хуулиуд нь Санхүүгийн төлбөр тооцооны тухай хууль[55] болон Санхүүгийн бүтээгдэхүүн, арилжааны тухай хууль[56] юм.

Токиогийн томоохон криптобирж болох *Mt.Gox*-ыг дампуурлаа зарлахад хүргэсэн гэнэтийн кибер халдлага 2011 онд гарсны дараа Япон Улс энэ салбарт хууль эрх зүйн орчин хэрэгтэй гэж үзсэн бөгөөд Японы тэргүүлэгч криптобирж болох *Coincheck* 2018 онд кибер халдлагад өртсөний дараа хууль эрх зүйн орчноо сайжруулах хэрэгтэй гэсэн дүгнэлтэд хүрчээ.

Улмаар 2018 оны 3 дугаар сард Япон Улсын Санхүүгийн үйлчилгээний агентлагийн[57] дэргэд Криптовалютын үйлчилгээний талаарх судалгааны бүлэг[58] байгуулагдаж, тухайн оны 12 дугаар сар хүртэл нийт 11 удаа хяналт, шалгалт хийж, хэлэлцүүлэг өрнүүлсэн байна. Хэлэлцүүлгийн үр дүнд 2019 оны 5 дугаар сарын 31-ний өдөр Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн тухай Засгийн газрын тогтоол болон Санхүүгийн төлбөр тооцооны тухай хууль, Санхүүгийн бүтээгдэхүүн, арилжааны тухай хуульд тус тус нэмэлт, өөрчлөлт оруулах тухай хууль баталж, 2020 оны 5 дугаар сарын 31-ний өдрөөс мөрдөж эхэлснээр Япон Улсын виртуал хөрөнгийн эрх зүйн орчин бүрджээ.

Дээрх нэмэлт, өөрчлөлтөөр кибер халдлагаас үүдэх виртуал хөрөнгийн гадагш урсгал, виртуал хөрөнгийн биржүүдийн дотоод хяналтын хангалтгүй байдал, хэрэглэгчийн мэдээллийн болон хөрөнгийн аюулгүй байдалд түлхүү анхаарсан дараах зохицуулалтууд нэмэгдсэн. Үүнд:

---

54 暗号資産交換業者に関する内閣府令、平成二十九年三月二十四日（https://bit.ly/3zJL8OP）

55 資金決済に関する法律、平成二十一年六月二十四日（https://bit.ly/3zGNdLt）

56 金融商品取引法、昭和二十三年四月十三日（https://bit.ly/3Ok8D4X）

57 日：金融庁

58 日：仮想通貨交換業等に関する研究会

*"Виртуал хөрөнгийн цйлчилгээ цзцлэгчийн тухай" Засгийн газрын 2017 оны 3 дугаар тогтоол*[59]

*13 дугаар зүйл. Виртуал хөрөнгийн цйл ажиллагаанд холбогдох мэдээллийн аюулгүй байдлын хяналтын арга хэмжээ*

Виртуал хөрөнгийн үйлчилгээ үзүүлэгч нь өөрсдийн үйл ажиллагааны агуулга, арга барилын дагуу виртуал хөрөнгийн үйл ажиллагаанд хамаарах цахим мэдээлэл боловсруулах хяналтын хангалттай арга хэмжээ авах ёстой.

*Санхүүгийн төлбөр тооцооны тухай хууль*[60]

*63.8. Мэдээллийн аюулгүй байдлын хяналт*

Виртуал хөрөнгийн үйлчилгээ үзүүлэгч нь Засгийн газрын тогтоолд заасны дагуу виртуал хөрөнгийн үйлчилгээнд холбогдох мэдээллийн нууц задруулах, устгах, эсхүл халдахаас урьдчилан сэргийлэх, холбогдох бусад мэдээллийн аюулгүй байдлыг хянахад шаардлагатай арга хэмжээг хэрэгжүүлэх ёстой.

*63.16. Үйл ажиллагааг сайжруулах тушаал*

Ерөнхий сайд нь виртуал хөрөнгийн үйл ажиллагааны зөв, баталгаатай гүйцэтгэлийг хангахад хэрэгтэй гэж үзсэн тохиолдолд шаардлагатай хэмжээнд виртуал хөрөнгийн үйлчилгээ үзүүлэгчид үйл ажиллагаа, эсхүл хөрөнгийн нөхцөл байдлыг сайжруулахад шаардлагатай арга хэмжээ болон удирдлагын бусад түвшинд шаардлагатай гэсэн арга хэмжээ авахыг тушааж болно.

*63.17. Бүртгэл цуцлах*

Ерөнхий сайд нь виртуал хөрөнгийн үйлчилгээ үзүүлэгчийг дараах зүйлсийн аль нэгд холбогдсон тохиолдолд 63 дугаар зүйлийн 2-т заасан бүртгэлийг цуцлах, эсхүл 6 сарын дотор хуульд заасан виртуал хөрөнгийн үйлчилгээг бүхэлд нь, эсхүл хэсэгчлэн түдгэлзүүлэхийг тушаана:

(i) 63 дугаар зүйлийн 5.1-ийн заалтуудад холбогдох үед;

(ii) Хууль бус аргаар 63 дугаар зүйлийн 2-т заасан бүртгэлийг хийлгэх үед;

(iii) Энэ хууль, эсхүл энэ хуульд үндэслэсэн шийдвэр, захирамж, тушаал, эсхүл эдгээрт үндэслэсэн арга хэмжээг зөрчсөн үед.

Дээрх заалтуудаас үзвэл Япон Улс ВХҮҮ нь мэдээллийн аюулгүй байдлыг хангах, хянах шаардлагатай арга хэмжээ авахыг хууль, Засгийн газрын тогтоолдоо заасан хэдий ч тэдгээрийг зөрчсөн нь бүртгэлийг цуцлах хүртэлх арга хэмжээ авах үндэслэл болохооргүй байна.

---

59 暗号資産交換業者に関する内閣府令、平成二十九年三月二十四日
https://elaws.e-gov.go.jp/document?lawid=429M60000002007

60 資金決済に関する法律、平成二十一年六月二十四日
https://elaws.e-gov.go.jp/document?lawid=421AC0000000059

## АНУ

АНУ-ын Хууль зүйн яам нь виртуал хөрөнгөтэй холбоотой эрүүгийн болон бусад зохисгүй үйлдэлд хамаарах өргөн хүрээний шүүн таслах ажиллагаа явуулдаг. Мөн зохицуулах үүрэгтэй хэд хэдэн агентлаг виртуал хөрөнгийн үйл ажиллагаанд хамаарах хууль тогтоомжид заасан бүрэн эрхийг хэрэгжүүлдэг ба Хууль зүйн яамтай хамтран криптовалютыг хууль бус зорилгоор урвуулан ашигласан этгээдийг илрүүлж, мөрдөн байцаалтын ажиллагаа явуулж байна.[61] Үүнд Санхүүгийн гэмт хэрэгтэй тэмцэх сүлжээ (*The Financial Crimes Enforcement Network*), Сангийн яамны Гадаад хөрөнгийн хяналтын алба (*Office of Foreign Assets Control*), Валютын хяналтын алба (*Office of the Comptroller of the Currency*), Үнэт цаас ба биржийн хороо (*The Securities and Exchange Commission*), Таваарын фьючерсийн арилжааны комисс (*The Commodity Futures Trading Commission*), Дотоод орлого, татварын хэрэгжилтийн алба (*The Internal Revenue Service and Tax Enforcement*) хамаарна.

АНУ-д ВХҮҮ-ийн тухайлсан хууль батлагдаагүй бөгөөд виртуал хөрөнгийн үйлчилгээнд ашиглах мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангах үүргийг хуулиар хүлээлгээгүй байна.

## Хонконг

Хонконгийн Засгийн газар 2022 оны 6 дугаар сарын 24-ний өдөр Мөнгө угаах, терроризмыг санхүүжүүлэхтэй тэмцэх хуульд нэмэлт өөрчлөлт оруулах тухай хуулийг нийтэлжээ.[62] Энэхүү нэмэлтээр Мөнгө угаах болон терроризмыг санхүүжүүлэхтэй тэмцэх тухай хууль (*Cap. 615*)-д ВХҮҮ-ийн тусгай зөвшөөрлийн дэглэм, ВХҮҮ-д МҮТС-тэй тэмцэх үүрэг хүлээлгэх өөрчлөлтүүд оруулсан.

*Хүснэгт 9. Хонконгийн Мөнгө угаах, терроризмыг санхүүжүүлэхтэй тэмцэх тухай хууль (Cap. 615)*

*2 дугаар хэсэг. Виртуал хөрөнгөд хамаарах үйл ажиллагааны хязгаарлалт*
*53ZRD дугаар зүйл. Виртуал хөрөнгийн үйлчилгээ үзүүлэхэд шаардах тусгай зөвшөөрөл*
*53ZRE дугаар зүйл. Виртуал хөрөнгийн үйлчилгээ үзүүлэх тусгай зөвшөөрөлгүй этгээд үүнтэй холбоотой зар сурталчилгаа гаргах гэмт хэрэг*
*53ZRF дугаар зүйл. Виртуал хөрөнгийн гүйлгээнд залилах, хууран мэхлэх төхөөрөмж зэргийг ашиглах гэмт хэрэг*
*53ZRG дугаар зүйл. Бусдыг залилах зорилгоор, эсхүл болгоомжгүйгээр виртуал хөрөнгөд хөрөнгө оруулахад хүргэх гэмт хэрэг*

[61] https://www.justice.gov/archives/ag/page/file/1326061/download Report of the Attorney General's Cyber digital task force, Cryptocurrency Enforcement framework, 2020.

[62] https://www.gld.gov.hk/egazette/pdf/20222625/es32022262516.pdf Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill, 2022.

*3 дугаар хэсэг. Виртуал хөрөнгийн үйлчилгээний тусгай зөвшөөрөл олгох, эзэмших, бүртгэх*
*53ZRK дугаар зүйл. Тусгай зөвшөөрөл олгох болон эзэмших*
5. *Комисс нь виртуал хөрөнгийн үйлчилгээ үзүүлэх тусгай зөвшөөрөл хүсэгчид кибер аюулгүй байдлын нөхцөл тавина:*
*(р) кибер аюулгүй байдал.*

*6 дугаар хэсэг. Тусгай зөвшөөрөлтэй этгээдийн мэдээлэх болон хураамж төлөх үүрэг*
*53ZRT дугаар зүйл. Тодорхой мэдээлэлд өөрчлөлт орсон тухай мэдэгдэл*
*53ZRU дугаар зүйл. Үйл ажиллагаагаа зогсоох тухай мэдэгдэл*
*53ZRV дугаар зүйл. Холбоо, аж ахуйн нэгж: үйл ажиллагааны мэдэгдэл, хязгаарлалт*
*53ZRW дугаар зүйл. Тусгай зөвшөөрөлтэй*
*53ZRX дугаар зүйл. Жилийн хураамж болон өгөөж*

Дээр өгүүлснээс үзэхэд Хонконгийн Мөнгө угаах, терроризмыг санхүүжүүлэхтэй тэмцэх тухай хуульд виртуал хөрөнгийн үйлчилгээний тусгай зөвшөөрөл авахад кибер аюулгүй байдлын нөхцөл тавихаар хуульчилсан хэдий ч виртуал хөрөнгийн үйлчилгээнд ашиглах мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангах үүргийг хуульчлаагүй байна.

### БНЭУ

БНЭУ нь ВХҮҮ-ийн зохицуулалттай, ФАТФ-ын *Travel Rule*-ийн шаардлагыг дагаж мөрддөг Европын анхны орнуудын нэг юм. БНЭУ-ын Мөнгө угаах, терроризмыг санхүүжүүлэхээс урьдчилан сэргийлэх хууль нь одоогоор хэлэлцүүлгийн шатанд байгаа бөгөөд тус улсад крипто арилжаа явуулж байгаа бүх ВХҮҮ-д хамаарна. Энэ хууль батлагдсанаар төвлөрсөн бус платформ, ICO болон бусад үйлчилгээ үзүүлэгчид ВХҮҮ болно.

БНЭУ-ын Засгийн газар 2021 оны 12 дугаар сарын 23-ны өдөр санхүүгийн гэмт хэргийн эрсдэлийг бууруулахын тулд ВХҮҮ-ийг илүү үр дүнтэй зохицуулах хуулийн төсөл боловсруулсан. Хуулийн шинэчилсэн найруулгын төсөлд ВХҮҮ-д нэрээ нууцалсан виртуал данс нээхийг хориглосон ба хэрэглэгчийг заавал таньж мэдэх үүрэг, ФАТФ-аас тогтоосон ВХҮҮ-ийн шинэчилсэн стандартууд, ВХҮҮ-ийн дүрмийн сангийн хэмжээ зэрэг зохицуулалт тусгасан. Хуулийн төслийг БНЭУ-ын парламентад өргөн мэдүүлсэн ба хууль болж батлагдахын тулд гурван хэлэлцүүлэг хийгдэхээр байна.[63]

БНЭУ-ын Кибер аюулгүй байдлын тухай хуульд[64] системийн аюулгүй байдлын арга хэмжээ авах, кибер ослын талаар мэдээлэх үйлчилгээ үзүүлэгчийн үүргийг хуульчилжээ.

[63] Estonia to tighten regulation of virtual asset service providers | Rahandusministeerium (fin.ee).
[64] Cybersecurity Act of Estonia, https://www.riigiteataja.ee/en/eli/523052018003/consolide.

*7 дугаар зүйл. Үйлчилгээ үзүүлэгчийн системийн аюулгүй байдлын арга хэмжээ*

1. Үйлчилгээ үзүүлэгч нь зохион байгуулалт, үйл ажиллагаа, мэдээллийн технологийн аюулгүй байдлын арга хэмжээг байнга хэрэгжүүлнэ:
   3) кибер ослын улмаас үйлчилгээний тасралтгүй байдал, системийн аюулгүй байдалд үзүүлэх нөлөөллөөс урьдчилан сэргийлэх, бууруулах, эсхүл хамааралтай өөр үйлчилгээний тасралтгүй байдал, системийн аюулгүй байдалд учирч болзошгүй нөлөөллөөс урьдчилан сэргийлэх, багасгах.

*18 дугаар зүйл. Хуульд заасан шаардлагыг зөрчсөн тохиолдолд:*

1. Энэ хуулийн 7 дугаар зүйлийн 1.3-т заасан шаардлагыг үл хангасан үйлчилгээ үзүүлэгчийг 200 хүртэл нэгжтэй тэнцэх хэмжээний мөнгөн дүнгээр торгоно.
2. Энэ үйлдлийг хуулийн этгээд үйлдсэн бол 20,000 евро хүртэлх мөнгөн дүнгээр торгоно.

Иймд ВХҮҮ нь виртуал хөрөнгийн үйлчилгээний тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангах үүргийг БНЭУ-д мөн адил хуулиар хүлээлгэсэн байна.

### Швейцар

Швейцарын парламент 2021 оны 8 дугаар сарын 1-нд Блокчэйны хууль[65] баталснаар энэ салбарын эрх зүйн зохицуулалт хийсэн дэлхийн анхны орнуудын нэг болсон. Виртуал хөрөнгийн биржүүд Швейцарын Санхүүгийн зах зээлийн хяналтын газар (*FINMA*)-т бүртгүүлж, түүний хяналт доор үйл ажиллагаа эрхлэх эрхтэй ба токен техникийн хувьд блокчэйн дэд бүтцэд шилжсэнээр дотоодын МУТС-тэй тэмцэх шаардлагыг дагаж мөрдөхийг шаарддаг.[66] Гэвч виртуал хөрөнгийн үйлчилгээнд ашиглах мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангах виртуал хөрөнгийн биржийн үүргийг хуульчлаагүй байна.

Гадаад орнуудын харьцуулан судалсан зохицуулалтуудаас дүгнэхэд виртуал хөрөнгийн үйлчилгээний аюулгүй байдал, тасралтгүй, найдвартай ажиллагааг хангах виртуал хөрөнгийн биржийн үүргийг Сингапур болон БНЭУ манай улсынхтай адил агуулгаар хуульчилжээ. Харин Хонконгийн хувьд кибер аюулгүй байдлын нөхцөлийг ВХҮҮ-ийн тусгай зөвшөөрөл хүсэгчид тавьж байгаа ч үүнийг үүрэг гэж үзэх боломжгүй бөгөөд АНУ, Швейцар, ОХУ-д мөн виртуал хөрөнгийн биржийн хувьд тусгайлан дээрх агуулгатай үүргийг хуулиар шууд хүлээлгээгүй. Япон, БНСУ-ын хувьд

[65] https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html#:~:text=On%201%20August%202021%2C%20Switzerland,and%20enables%20innovation%20and%20growth

[66] https://complyadvantage.com/insights/crypto-regulations/cryptocurrency-regulations-switzerland/

мэдээллийн аюулгүй байдлыг хангах, үйл ажиллагааны найдвартай байдлыг сайжруулах, хэвийн үйл ажиллагааг хангахын тулд ерөнхийлөгч эсхүл ерөнхий сайдын тушаасан арга хэмжээг хэрэгжүүлэхээр тусгажээ.

### 1.2.2. ВХҮҮ-ээр бүртгүүлэх, хүлээх үүрэг, зөрчилд хүлээлгэх хариуцлага

Хороонд хуулиар олгосон виртуал хөрөнгийн үйлчилгээтэй холбоотой бүрэн эрхийн хүрээнд Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журам болон Виртуал хөрөнгийн үйл ажиллагааны журам батлаж, ВХҮҮ-д үйл ажиллагаа эхлүүлэхээс өмнө болон үйл ажиллагаа эрхлэх хугацаанд тавих нэмэлт шаардлагыг тодорхойлсон.

Тодруулбал, Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журмаар бүртгүүлэх хүсэлт гаргагч, түүний бүтэц, зохион байгуулалт, хүний нөөц, программ хангамж, мэдээллийн технологид тавигдах шаардлагыг тодорхойлж, бүртгэх, бүртгэлээс хасах харилцааг зохицуулсан. Харин Виртуал хөрөнгийн үйл ажиллагааны журмаар ВХҮҮ-ийн зохистой засаглал, үйл ажиллагаа, өөрийн хөрөнгийн хэмжээ, тайлан мэдээнд тавигдах шаардлагыг тодорхойлсон зохицуулалттай. Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журамд кибер аюулгүй байдлыг хангахтай холбоотой дараах нөхцөл, шаардлага тусгагдсан.

*Хүснэгт 11. Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журам*

| |
|---|
| *Гурав. Бүтэц, зохион байгуулалт, хүний нөөцийн шаардлага*<br>3.2. Энэ журмын 3.1-д заасан төлөөлөн удирдах зөвлөл дараах дүрэм, журам, бодлогын баримт бичгийг баталсан байна:<br>*3.2.5. MNS ISO/IEC 27001 стандартын шаардлага, Кибер аюулгүй байдлын тухай хуульд нийцүүлсэн мэдээллийн технологийн аюулгүй байдлыг хангах үйл ажиллагааны журам*;<br>3.5. Хүсэлт гаргагч дараах бүтэц, зохион байгуулалт, тухайн чиглэлээр мэргэшсэн хүний нөөцтэй байна:<br>3.5.2. мэдээллийн технологи, аюулгүй байдал хариуцсан нэгжтэй, эсхүл хариуцсан ажилтантай байх;<br>*Дөрөв. Программ хангамж, мэдээллийн технологид тавигдах шаардлага*<br>4.1. Хүсэлт гаргагч виртуал хөрөнгийн үйлчилгээ үзүүлэхэд шуурхай, тасралтгүй, үйл ажиллагааны онцлогт тохирсон тусгай программ хангамжтай байх бөгөөд уг программ хангамж нь дараах шаардлагыг хангасан байна:<br>4.1.1. арилжаанд оролцогчид нэгнийгээ таньж мэдэх боломжгүй байх;<br>4.1.2. харилцагчийн хувийн мэдээлэл гуравдагч этгээдээс нууц байх;<br>4.1.3. зах зээлийн шаардлагад нийцүүлэн хөгжүүлэх, шинэчлэх боломжтой байх;<br>4.1.4. олон нийтэд мэдээлэл хүргэх хэсэг буюу нээлттэй самбартай байх;<br>4.1.5. арилжааны хяналтын системтэй байх;<br>4.1.6. албан ёсны лицензтэй аюулгүй байдлыг хангах системтэй байх.<br>4.2. *Хүсэлт гаргагч энэ журмын гуравдугаар хавсралтад заасан мэдээллийн технологийн стандартын суцлийн хувилбарыг хангаж, хөндлөнгийн эрх бүхий байгууллагаар баталгаажуулсан байна.* |

ВХҮҮ нь дээрх нөхцөл, шаардлагыг хангаагүй тохиолдолд Хороо ВХҮҮ-ээр бүртгэхээс татгалзана.[67] Хэрэв ВХҮҮ нь Хороонд бүртгүүлэхгүйгээр виртуал хөрөнгийн үйлчилгээ эрхэлсэн бол виртуал хөрөнгийн үйлчилгээнд ашигласан эд зүйлийг хураах, хүнийг 20 сая төгрөгөөр, хуулийн этгээдийг 200 сая төгрөгөөр торгох шийтгэл хүлээнэ.[68] Мөн ВХҮҮ нь үйл ажиллагаандаа ВХҮҮ-ээр бүртгүүлэхэд тавигдах нөхцөл, шаардлагыг бүрэн хангаж ажиллах үүрэгтэй[69] ба энэ үүргээ эс биелүүлбэл 20 сая төгрөгөөр торгох шийтгэл хүлээнэ.[70]

Кибер аюулгүй байдлыг хангахтай холбоотой Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн үйл ажиллагааны журмаар ВХҮҮ дараах мэдээллийг мэдээлэх үүрэг хүлээсэн.

*Хүснэгт 12. Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн үйл ажиллагааны журам*

| |
|---|
| 6.1. ВХҮҮ дараах мэдээллийг өөрийн программ хангамж болон цахим хуудсанд ил тод, нээлттэйгээр байршуулна:<br>6.1.10. үйл ажиллагаанд ашиглах программ хангамж, систем болон мэдээлэл, технологийн өөрчлөлт, шинэчлэлтийн талаар. |
| 7.4. ВХҮҮ дараах мэдээллийг агуулсан үйл ажиллагааны жилийн тайланг дараа оны 3 дугаар сарын 01-ний өдрийн дотор Хороонд тогтмол хүргүүлж, олон нийтэд мэдээлнэ:<br>7.4.5. ашиглаж буй программ хангамж, систем, мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдалд хийлгэсэн эрсдэлийн үнэлгээний дүгнэлт, эрсдэлийг бууруулах, урьдчилан сэргийлэх арга хэмжээ. |

Дээрх байдлаар ВХҮҮ-д журмаар кибер аюулгүй байдлыг хангахтай холбоотой нарийвчилсан үүргүүд хүлээлгэж, үүргээ биелүүлээгүй тохиолдолд хариуцлага хүлээлгэхээр Зөрчлийн тухай хуульд заасан нь ВХҮҮ-д кибер аюулгүй байдал чухал болохыг харуулж байна. Нөгөөтээгүүр виртуал хөрөнгийн үйлчилгээнд кибер аюулгүй байдлын эсрэг гэмт хэрэг гарах, виртуал хөрөнгө ашиглан кибер орчинд гэмт хэрэг үйлдэх замаар мөнгө угаах гэмт хэрэг үйлдэгдэх өндөр эрсдэлтэй салбар гэж үзэж байгаа тул ийнхүү тусгасан гэж дүгнэж болох юм.

### 1.2.3. Кибер аюулгүй байдлын тухай хуулиар хуулийн этгээдийн хүлээсэн үүрэг, зөрчилд хүлээлгэх хариуцлага

НҮБ-ын тусгай агентлаг болох Олон улсын харилцаа холбооны нэгдлээс гишүүн 193 орны хүрээнд 2015, 2017, 2018, 2020 онд Кибер аюулгүй байдлын индексийг үнэлсэн судалгаагаар Монгол Улс 2015 онд 104 дүгээр байранд,

[67] Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журмын 5 дугаар зүйлийн 5.9.3 дахь заалт.

[68] Зөрчлийн тухай хуулийн 11.33 дугаар зүйлийн 1 дэх хэсэг.

[69] Виртуал хөрөнгийнх үйлчилгээ үзүүлэгчийн тухай хуулийн 8 дугаар зүйлийн 8.1.1 дэх заалт.

[70] Зөрчлийн тухай хуулийн 11 дүгээр зүйлийн 5 дахь хэсэг.

2017 онд 103 дугаар байранд, 2018 онд 85 дугаар байранд, 2020 онд 120 дугаар байранд тус тус эрэмбэлэгдсэн.[71]

УИХ-ын 2021 оны 12 дугаар тогтоолоор баталсан "Монгол Улсын хууль тогтоомжийг 2024 он хүртэл боловсронгуй болгох үндсэн чиглэл"-д 2021 онд Кибер аюулгүй байдлын тухай хуулийн төсөл боловсруулж, УИХ-д өргөн барихаар заажээ.[72] Үүний дагуу Кибер аюулгүй байдлын тухай хууль 2021 оны 12 дугаар сарын 17-ны өдөр батлагдаж, 2022 оны 5 дугаар сарын 1-ний өдрөөс хэрэгжиж эхэлснээр Монгол Улсын хэмжээнд нэгдсэн удирдлага, зохион байгуулалттайгаар кибер аюулгүй байдлыг хангах эрх зүйн орчин бүрдсэн.

Тус хуульд зааснаар кибер аюулгүй байдлыг хангах тогтолцоонд "хуулийн этгээд"-ийг хамааруулж, хуулийн 7 дугаар зүйлийн 7.2 дахь хэсэгт зааснаар (1) төрийн өмчит хуулийн этгээд, (2) кибер орчинд дундын мэдээллийн системээр дамжуулан мэдээлэл боловсруулах, хадгалах, түгээх, цахим тооцооллын болон түүний хэвийн үйл ажиллагааг хангахад мэдээллийн технологийн чиглэлээр үйлчилгээ үзүүлж байгаа хуулийн этгээд, (3) онц чухал мэдээллийн дэд бүтэцтэй байгууллага нь Кибер аюулгүй байдлыг хангах нийтлэг журамд нийцсэн кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журамтай байхаар хуульчилсан.

ВХҮҮ нь кибер орчинд дундын мэдээллийн системээр дамжуулан мэдээлэл "боловсруулах", "хадгалах" болон түүний хэвийн үйл ажиллагааг хангах чиглэлээр үйлчилгээ үзүүлж байгаа тул хуулийн 17 дугаар зүйлийн 17.1 дэх хэсэгт заасан хуулийн этгээд гэж үзэж, дараах үүргийг хүлээнэ. Үүнд:

*Хүснэгт 13. Кибер аюулгүй байдлын тухай хууль*

17.1.Кибер орчинд дундын мэдээллийн системээр дамжуулан мэдээлэл боловсруулах, хадгалах, түгээх, цахим тооцооллын болон түүний хэвийн үйл ажиллагааг хангахад мэдээллийн технологийн чиглэлээр үйлчилгээ үзүүлж байгаа хуулийн этгээд дараах үүргийг хүлээнэ:

17.1.1.кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам батлах;

17.1.2.кибер халдлагын талаар кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд даруй мэдэгдэх, таслан зогсоох боломжгүй бол туслалцаа авах;

17.1.3.мэдээллийн системийн үйлдлийн бүртгэлийг кибер аюулгүй байдлын нийтлэг журамд заасан хугацаанд хадгалах;

17.1.4.кибер аюулгүй байдлыг хангах үйл ажиллагааны талаар холбогдох төрийн байгууллагаас мэргэжил, арга зүйн туслалцаа авч, хамтран ажиллах;

[71] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx НҮБ-ын төрөлжсөн агентлаг болох Олон улсын цахилгаан холбооны байгууллагын цахим хуудсанд нийтлэгдсэн судалгаанаас харав.

[72] Монгол Улсын Их Хурлын 2021 оны 1 дүгээр сарын 22-ны өдрийн "Монгол Улсын хууль тогтоомжийг 2024 он хүртэл боловсронгуй болгох үндсэн чиглэл батлах тухай" 12 дугаар тогтоол, https://old.legalinfo.mn/law/details/16009

17.1.5.кибер аюулгүй байдлыг хангах үйл ажиллагаа хариуцсан нэгж, эсхүл албан тушаалтантай байх;

17.1.6.кибер аюулгүй байдлын эрсдэлийн үнэлгээг хоёр жил тутамд, холбогдох журамд заасан нөхцөл, байдал үүссэн үед тухай бүр хийлгэж, гарсан дүгнэлт, зөвлөмж, шаардлагын дагуу арга хэмжээг авч хэрэгжүүлэх;

17.1.7.мэдээллийн аюулгүй байдлын аудитыг жил тутамд, холбогдох журамд заасан нөхцөл, байдал үүссэн үед тухай бүр хийлгэж, гарсан дүгнэлт, зөвлөмж, шаардлагын дагуу арга хэмжээг авч хэрэгжүүлэх;

17.1.8.шинээр нэвтрүүлсэн мэдээллийн технологийн бүтээгдэхүүн, үйлчилгээ болон тэдгээрийн өөрчлөлт, шинэчлэл бүрд кибер аюулгүй байдлын холбогдох шалгалт хийсэн байх;

17.1.9.кибер халдлага, зөрчилд өртсөн хэрэглэгчид даруй мэдэгдэх.

Хуулийн этгээд нь Кибер аюулгүй байдлын тухай хуулийг зөрчсөн бол Эрүүгийн хууль, эсхүл Зөрчлийн тухай хуульд заасан хариуцлага хүлээлгэхээр хуульчилсан[73]. Иймд хуулиар хүлээсэн үүрэг, түүний зөрчилд холбогдох хариуцлагыг хэрхэн зохицуулсныг нарийвчлан авч үзье.

*Хүснэгт 14. Кибер аюулгүй байдлын тухай хуулиар хуулийн этгээдийн хүлээсэн үүрэг, үүргийн зөрчилд хүлээлгэх хариуцлага*

| № | Хүлээлгэсэн үүрэг | Хариуцлагын зохицуулалт |
|---|---|---|
| 1 | Кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам батлах<br>– *7.1.Кибер аюулгүй байдлыг хангах, урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах нийтлэг журмыг Засгийн газар батална.*<br>– *7.2.Энэ хуулийн 16.1, 17.1, 19.1-д заасан хуулийн этгээд нь Кибер аюулгүй байдлыг хангах нийтлэг журамд нийцсэн кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журамтай байна.* | Засгийн газраас нийтлэг журмыг батлаагүй (2022 оны 7 дугаар сарын байдлаар) тул хуулийн этгээдээс энэхүү үүргээ биелүүлэхийг шаардах боломжгүй.<br>Зөрчлийн тухай хуулиар хүлээлгэх хариуцлага:<br>– Энэ үүргийг зөрчсөн тохиолдолд хүлээлгэх хариуцлагыг хуульчлаагүй.<br>Харин ВХҮҮ-ийн хувьд Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журмын 3.2.5-д зааснаар дээрх журмыг баталсан байхыг шаардаж байх тул энэ үүргээ биелүүлээгүй нь Зөрчлийн тухай хуулийн 11 дүгээр зүйлийн 5 дахь хэсэгт зааснаар хуулийн этгээдийг хорин мянган нэгжтэй тэнцэх төгрөгөөр торгох үндэслэл болно. |

[73] Кибер аюулгүй байдлын тухай хуулийн 24 дүгээр зүйлийн 24.2 дахь хэсэг.

| | | |
|---|---|---|
| 2 | Кибер халдлагын талаар кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд даруй мэдэгдэх, кибер халдлага, зөрчилд өртсөн хэрэглэгчид даруй мэдэгдэх<br>– *20.1.Кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, түүнд өртсөн дэд бүтэц, мэдээллийн системийг нөхөн сэргээхэд мэргэжил, арга зүйн туслалцаа, дэмжлэг үзүүлэх үндсэн чиг үүрэг бүхий хүний нөөц, техник, технологийн чадавх, мэдээллийн сантай дараах төвүүд ажиллана.*<br>– *20.1.2.кибер халдлага, зөрчилтэй тэмцэх нийтийн төв /цаашид "Нийтийн төв" гэх/;* | Зөрчлийн тухай хуулиар хүлээлгэх хариуцлага:<br>– 14.13.4.Кибер халдлага, ... кибер халдлага, зөрчилтэй тэмцэх төвд холбогдоогүй бол *хуулийн этгээдийг хоёр мянган нэгжтэй тэнцэх хэмжээний төгрөгөөр торгоно.*<br>– 14.13.2. 2.Кибер халдлага, зөрчилд өртсөн хэрэглэгчид даруй мэдэгдэх үүргээ биелүүлээгүй бол *хуулийн этгээдийг нэг мянган нэгжтэй тэнцэх хэмжээний төгрөгөөр торгоно.* |
| 3 | Мэдээллийн системийн үйлдлийн бүртгэлийг кибер аюулгүй байдлын нийтлэг журамд заасан хугацаанд хадгалах<br>*ВХҮҮтХ-д:*<br>– *12.1.Виртуал хөрөнгийн үйлчилгээ үзүүлэгч тухайн үйл ажиллагааны явцад бий болсон цаасан болон цахим баримт бичгийг хүлээн авсан, эсхүл үүсгэсэн өдрөөс хойш 10-аас доошгүй жил хадгалж, хамгаална.* | Хакерчид ихэвчлэн *TOR*[74]-тэй адил систем ашиглаж, өөрийн *IP* хаягийг нуудаг учраас илрүүлэхэд амаргүй. Мөрдөн шалгах байгууллага хакерын криптовалютын шилжүүлгийн түүхээр мөшгөж, бирж дээр криптовалютыг бэлэн мөнгөөр, эсхүл бусад криптовалютаар солих үед криптовалютыг царцааж, хэрэгтнийг мөрддөг. Виртуал хөрөнгийн шилжүүлэг болон бусад үйлдлийн түүх нь хакерын халдлагыг мөрдөх, олж тогтооход ач холбогдолтой тул "хадгалалт"-ын үүрэгт хариуцлагын механизмыг бүрдүүлэх нь зохимжтой юм. |
| 4 | Кибер аюулгүй байдлыг хангах үйл ажиллагааны талаар холбогдох төрийн байгууллагаас мэргэжил, арга зүйн туслалцаа авч, хамтран ажиллах<br>*Кибер аюулгүй байдлын тухай хуульд:*<br>– *22.2.Нийтийн төв дараах чиг үүргийг хэрэгжүүлнэ:*<br>– *22.2.4.иргэн, хуулийн этгээдэд кибер халдлага, зөрчлийн талаар зөвлөмж, шаардлага хүргүүлэх.* | Кибер халдлагаас урьдчилан сэргийлэх, гарсан тохиолдолд мөрдөн шалгахад хувийн хэвшил, төрийн байгууллагуудын хамтын ажиллагаа чухал нөлөөтэй гэдгийг онцолдог. Монгол Улсын хувьд Кибер аюулгүй байдлын тухай хуулиар төр, хувийн хэвшлийн хамтын ажиллагааг бүрдүүлж өгсөн нь сайшаалтай.<br>Хэдийгээр Кибер аюулгүй байдлын тухай хуулийн 17 дугаар зүйлийн 17.1.2, 17.1.4 дэх заалтад заасан "Туслалцаа авах" үүргээ хуулийн этгээд биелүүлээгүй нь Зөрчлийн тухай хууль болон Эрүүгийн хуульд заасан хариуцлага хүлээлгэх үндэслэл болохгүй ч Монгол Улсын Үндсэн хууль, эрүү, иргэн, захиргааны хэрэг хянан шийдвэрлэх тухай хууль, татварын хууль болон бусад хуульд туслалцаа авах нь иргэн, хуулийн этгээдийн үүрэг бус эрх байхаар хуульчилсан. |

[74] The Onion Routing Network ашиглан нэргүй сүлжээний систем, dark web гэж нэрлэгддэг.

| | | |
|---|---|---|
| 5 | Кибер аюулгүй байдлыг хангах үйл ажиллагаа хариуцсан нэгж, эсхүл албан тушаалтантай байх<br><br>*ВХҮҮтХ-д:*<br>– *7.1.4. ... үйл ажиллагааг явуулах бүтэц, зохион байгуулалт, мэргэшсэн хүний нөөцтэй байх*<br><br>Виртуал хөрөнгийн үйлчилгээ үзүүлэгчээр бүртгүүлэх журам:<br>– *3.5.Хүсэлт гаргагч ... мэргэшсэн хүний нөөцтэй байна:*<br>– *3.5.2.Мэдээллийн технологи, аюулгүй байдал хариуцсан нэгжтэй, эсхүл хариуцсан ажилтантай байх.* | Виртуал хөрөнгийн үйлчилгээ үзүүлэгчээр бүртгүүлэх журмаар хүлээлгэх хариуцлага:<br>– 5.9. ВХҮҮ нь ВХҮҮ-ийн тухай хууль тогтоомж болон энэ журамд заасан нөхцөл, шаардлагыг хангаагүй бол *Хороо хүсэлт гаргагчийг ВХҮҮ-ээр бүртгэхээс татгалзана.*<br>Зөрчлийн тухай хуулиар хүлээлгэх хариуцлага:<br>– 11.33.5.Виртуал хөрөнгийн үйлчилгээ үзүүлэгч, түүний эрх бүхий албан тушаалтан болон холбогдох этгээд нь хуульд заасан шаардлагыг хангаж ажиллаагүй, эсхүл үүргээ хэрэгжүүлээгүй, түүнийг зөрчсөн бол хүнийг хоёр мянган нэгжтэй тэнцэх хэмжээний төгрөгөөр, *хуулийн этгээдийг хорин мянган нэгжтэй тэнцэх хэмжээний төгрөгөөр торгоно.*<br>Өөрөөр хэлбэл, ВХҮҮ-ийг Кибер аюулгүй байдлын тухай хуульд заасан кибер аюулгүй байдлыг хангах үйл ажиллагаа хариуцсан нэгж, эсхүл албан тушаалтантай байх үүргийг зөрчсөн гэх үндэслэлээр шийтгэл оногдуулах, хариуцлага хүлээлгэх үндэслэл Кибер аюулгүй байдлын тухай хууль, Зөрчлийн болон Эрүүгийн хуульд байхгүй ч ВХҮҮтХ-д заасан шаардлагыг хангаж ажиллаагүй, эсхүл үүргээ хэрэгжүүлээгүй, түүнийг зөрчсөн гэх үндэслэлээр дээр дурдсан хариуцлага хүлээлгэх үндэслэл болно. |
| 6 | Кибер аюулгүй байдлын эрсдэлийн үнэлгээг хоёр жил тутамд, холбогдох журамд заасан нөхцөл, байдал үүссэн үед тухай бүр хийлгэж, гарсан дүгнэлт, зөвлөмж, шаардлагын дагуу арга хэмжээг авч хэрэгжүүлэх<br><br>Кибер аюулгүй байдлын тухай хуульд:<br>– 4.1.9. “кибер аюулгүй байдлын эрсдэлийн үнэлгээ” гэж цахим мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээний кибер аюулгүй байдал алдагдах, аюул занал тохиолдох магадлал, эмзэг байдлын түвшин, түүнээс үүсэх үр дагавар, эрсдэлийг бууруулах, урьдчилан сэргийлэх арга хэмжээг тодорхойлох мэргэшсэн үйл ажиллагааг; | – Улс орнуудад бүртгэгдсэн виртуал хөрөнгөтэй холбоотой гэмт хэргийн төрөлд мөнгө угаах, хориотой бодис болон бусад хориотой бараа (галт зэвсэг гэх мэт) худалдах, залилан мэхлэх, татвараас зайлсхийх, компьютерын гэмт хэрэг (жишээ нь, кибер халдлага үйлдэн хулгайлах), хүүхдийн мөлжлөг, хүний наймаа, хориг арга хэмжээнээс зайлсхийх, терроризмыг санхүүжүүлэх зэрэг багтсан байна.[75] |

[75] https://www.mongolbank.mn/documents/cma/guide20220201.pdf ФАТФ-ын тайлан: Виртуал хөрөнгийн мөнгө угаах, терроризмыг санхүүжүүлэхтэй холбоотой байж болох шинж тэмдгүүд. 2020 оны 9 дүгээр сар, 5 дахь тал.

| | | |
|---|---|---|
| | ВХУУтХ-д:<br>– *9.1.Виртуал хөрөнгийн цйлчилгээ цзццлэгч, харилцагчийн хооронд байгуулсан гэрээ, хэлцэлд дараах нөхцөлийг заавал тусгаж, хцлээн зөвшөөрснийг баталгаажуулна:*<br>– *9.1.11.виртуал хөрөнгө, виртуал хөрөнгийн цйлчилгээ нь залилан мэхлэх болон цахим халдлагад өртөх эрсдэлийн талаарх мэдээлэл;* | – ВХУУ нь кибер аюулгүй байдал алдагдах, аюул занал тохиолдох өндөр эрсдэлтэй тул энэхүү эрсдэлийг үнэлж, эрсдэлийг бууруулах, урьдчилан сэргийлэх арга хэмжээг авах нь зүйтэй. Энэ талаар Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн үйл ажиллагааны журмын 7 дугаар зүйлийн 7.4.5-т ВХУУ нь ашиглаж буй программ хангамж, систем, мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдалд хийлгэсэн эрсдэлийн үнэлгээний дүгнэлт, эрсдэлийг бууруулах, урьдчилан сэргийлэх арга хэмжээний талаар мэдээллийг үйл ажиллагааны жилийн тайланд тусгаж, тайланг Хороонд тогтмол хүргүүлж, олон нийтэд мэдээлэхээр заасан.<br>– ВХУУ нь кибер аюулгүй байдлын эрсдэлийн үнэлгээг Цахим хөгжил, харилцаа холбооны яаманд бүртгүүлсэн хуулийн этгээдээр хийлгэх үүрэгтэй.<br>Зөрчлийн тухай хуулиар хүлээлгэх хариуцлага:<br>– 14.13.3.Эрх бүхий байгууллагын шаардсанаар мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийлгээгүй, эсхүл хуульд заасан хугацаанд мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээний тайланг холбогдох байгууллагад ирүүлээгүй бол *хуулийн этгээдийг нэг мянган нэгжтэй тэнцэх хэмжээний төгрөгөөр торгоно.* |
| 7 | Мэдээллийн аюулгүй байдлын аудитыг жил тутамд, холбогдох журамд заасан нөхцөл, байдал үүссэн үед тухай бүр хийлгэж, гарсан дүгнэлт, зөвлөмж, шаардлагын дагуу арга хэмжээг авч хэрэгжүүлэх<br>*Кибер аюулгүй байдлын тухай хуульд:*<br>– *4.1.10.Мэдээллийн аюулгүй байдлын аудит гэж кибер аюулгүй байдлын хуультогтоомж, холбогдох журам, стандартад нийцсэн эсэхэд дүгнэлт гаргах, зөвлөмж өгөх хараат бус хөндлөнгийн мэргэжлийн цйл ажиллагааг хэлнэ.* | Кибер аюулгүй байдлын тухай хуульд зааснаар тус аудитыг 6-д заасан эрсдэлийн үнэлгээний адил, Цахим хөгжил, харилцаа холбооны яаманд бүртгүүлсэн хуулийн этгээд батлагдсан журмын дагуу хийх ба аудит хийлгээгүй бол Зөрчлийн тухай хуулиар:<br>– 14.13.3.Эрх бүхий байгууллагын шаардсанаар мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийлгээгүй, эсхүл хуульд заасан хугацаанд мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээний тайланг холбогдох байгууллагад ирүүлээгүй бол *хуулийн этгээдийг нэг мянган нэгжтэй тэнцэх хэмжээний төгрөгөөр торгоно.* |

| | | |
|---|---|---|
| 8 | Шинээр нэвтрүүлсэн мэдээллийн технологийн бүтээгдэхүүн, үйлчилгээ болон тэдгээрийн өөрчлөлт, шинэчлэл бүрд кибер аюулгүй байдлын холбогдох шалгалт хийсэн байх<br>*ВХҮҮтХ-д:*<br>– *6.1.10.үйл ажиллагаанд ашиглах программ хангамж, систем болон мэдээлэл, технологийн өөрчлөлт, шинэчлэлтийн талаар цахим хуудсанд ил тод, нээлттэйгээр байршуулах.* | Шинэ технологи, бүтээгдэхүүн, үйлчилгээ нь санхүүгийн үр ашиг, хүртээмжийг сайжруулж, инновац бүтээж байдаг ч нөгөө талаас шинэ эрсдэл үүсгэж, хууль бус үйл ажиллагааг санхүүжүүлэх боломж бий болгож байдаг. Иймд шинэ технологитой уялдан гарч ирж буй эрсдэлийг хянаж, урьдчилан сэргийлж байх шаардлагатай.<br>Энэхүү шалгалтыг хэрхэн хийх, шалгалт хийж, хуулиар хүлээсэн үүргээ биелүүлснийг хэрхэн нотлох талаар тодорхой зохицуулалт хуульд тусгагдаагүй.<br>Зөрчлийн тухай хуулиар хүлээлгэх хариуцлага:<br>– 14.13.1.Шинээр нэвтрүүлсэн мэдээллийн технологийн бүтээгдэхүүн, үйлчилгээ болон тэдгээрийн өөрчлөлт, шинэчлэл бүрд кибер аюулгүй байдлын холбогдох шалгалт хийх үүргээ биелүүлээгүй бол *хуулийн этгээдийг гурван зуун нэгжтэй тэнцэх хэмжээний төгрөгөөр торгоно.* |
| 9 | Кибер халдлага, зөрчилд өртсөн хэрэглэгчид даруй мэдэгдэх | Дээр дурдсан 1-8-д заасан үүргүүдийг биелүүлэх нь эцэстээ кибер халдлага, зөрчлөөс сэргийлэх зорилготой. Кибер халдлага, зөрчилд өртсөн тохиолдолд хэрэглэгчид даруй мэдэгдэх нь дараагийн халдлагаас харилцагчийг хамгаалах, харилцагч өөрийн мэдээллийг хамгаалах боломж олгохын зэрэгцээ харилцагчийн итгэлийг нэмэгдүүлдэг.<br>Зөрчлийн тухай хуулиар хүлээлгэх хариуцлага:<br>14.13.2.Кибер халдлага, зөрчилд өртсөн хэрэглэгчид даруй мэдэгдэх үүргээ биелүүлээгүй бол *хуулийн этгээдийг нэг мянган нэгжтэй тэнцэх хэмжээний төгрөгөөр торгоно.* |

## 1.3. Кибер аюулгүй байдлыг хамгаалах дотоодын эрх зүйн баримт бичиг дэх зохицуулалтын анхаарах асуудал

### 1.3.1. Монгол Улсын үндэсний аюулгүй байдлын үзэл баримтлал, хөтөлбөр

Монгол Улсын үндэсний аюулгүй байдлын үзэл баримтлалыг УИХ-ын 2010 оны 7 дугаар сарын 15-ны өдрийн 48 дугаар тогтоолоор баталсан. Энэ үзэл баримтлал нь Монгол Улсын мэдээллийн аюулгүй байдлыг хангах бодлогын үндсэн баримт бичиг болно.[76]

[76] Л.Галбаатар. Монгол Улсын мэдээллийн аюулгүй байдлын эрх зүйн зохицуулалт: Өнөөгийн байдал, тулгамдсан асуудал, шийдвэрлэх арга зам. “Шүүх эрх мэдэл” сэтгүүл, 2018, №4, 112 дахь талаас дам эшлэв.

Энэхүү үзэл баримтлалаар үндэсний аюулгүй байдал баталгаажих цогц бодлогын нэг хэсэг нь “мэдээллийн аюулгүй байдал” болохыг дурдаад мэдээллийн салбарт үндэсний ашиг сонирхлыг хамгаалахад кибер орчин дахь гэмт явдалтай тэмцэх, аливаа гэмт хэргийг илрүүлэх, нотлоход тооцоолох хэрэгслийн криминалистик техникийн шинжилгээ ашиглах үндэсний чадавхыг бий болгон, мэдээллийн аюулгүй байдлыг хангах, мэдээллийн орчинд сөргөлдөх аюулаас сэргийлэх, кибер орчин дахь гэмт явдалтай тэмцэх чиглэлд олон улсын хамтын ажиллагааг өргөжүүлэн хөгжүүлнэ гэж заасан. Үүнд:

*Хүснэгт 15. Монгол Улсын үндэсний аюулгүй байдлын үзэл баримтлал*

*3.6.Мэдээллийн аюулгүй байдал*

Мэдээллийн салбарт үндэсний ашиг сонирхлыг хамгаалах, төр, иргэн, хувийн хэвшлийн мэдээллийн бүрэн бүтэн, нууцлагдсан, хүртээмжтэй байдлыг баталгаажуулах нь мэдээллийн аюулгүй байдлыг хангах үндэс мөн.

3.6.1.Мэдээллийн салбарт үндэсний ашиг сонирхлыг хамгаалах

3.6.1.1.Үндэсний аюулгүй байдлыг хангах, улс орны хөгжлийг дэмжих, үндэсний үнэт зүйлийг хэвшүүлэх, нийгмийн оюун санааг төлөвшүүлэхэд мэдээлэл, мэдээллийн аюулгүй байдал нэн чухал ач холбогдолтой.

3.6.1.11.Кибер орчин дахь гэмт явдалтай тэмцэх, аливаа гэмт хэргийг илрүүлэх, нотлоход тооцоолох хэрэгслийн криминалистик техникийн шинжилгээ ашиглах үндэсний чадавхыг бий болгоно.

3.6.1.12.Мэдээллийн аюулгүй байдлыг хангах, мэдээллийн орчинд сөргөлдөх аюулаас сэргийлэх, кибер орчин дахь гэмт явдалтай тэмцэх чиглэлд олон улсын хамтын ажиллагааг өргөжүүлэн хөгжүүлнэ.

3.6.2.Мэдээллийн бүрэн бүтэн байдал

3.6.2.1.Мэдээлэл, мэдээллийн орчин, түүний дэд бүтцэд хууль бусаар нөлөөлөх, өөрчлөх үйлчлэлээс хамгаалснаар мэдээллийн бүрэн бүтэн байдал хангагдана.

3.6.3.Мэдээллийн нууцлал

3.6.3.1.Мэдээлэл, түүний бүрдэл хэсэгт хууль бусаар хандах, халдах, задрахаас хамгаалагдсанаар нууцлал хангагдана.

Монгол Улсын Засгийн газрын 2010 оны 6 дугаар сарын 2-ны өдрийн 141 дүгээр тогтоолоор Мэдээлэл аюулгүй байдлыг хангах үндэсний хөтөлбөр баталсан. Хөтөлбөрийг 2010-2015 онд хэрэгжүүлж дууссан бөгөөд одоо үндэсний аюулгүй байдлын үзэл баримтлалаас өөр мэдээллийн аюулгүй байдлыг хагахтай холбоотой бодлогын баримт бичиг байхгүй байна.[77] Тус хөтөлбөрт заасан арга хэмжээнүүдийн хэрэгжилтийг хангах зорилгоор “Мэдээллийн аюулгүй байдлыг хангах үндэсний хөтөлбөрийг хэрэгжүүлэх арга хэмжээний төлөвлөгөө”-г Засгийн газрын дээр дурдсан тогтоолоор мөн

[77] Л.Галбаатар. Монгол Улсын мэдээллийн аюулгүй байдлын эрх зүйн зохицуулалт: Өнөөгийн байдал, тулгамдсан асуудал, шийдвэрлэх арга зам, “Шүүх эрх мэдэл” сэтгүүл, 2018, №4, 112 дахь тал.

баталсан. Гэвч үндэсний аюулгүй байдлын үзэл баримтлалын мэдээллийн аюулгүй байдлыг хангах зорилтууд маш хангалтгүй түвшинд хэрэгжиж, тус хөтөлбөрийн биелэлт 45.55 хувийн үзүүлэлттэй гарсан гэж Харилцаа холбоо, мэдээллийн технологийн газар мэдээлсэн.[78]

Энэ нөхцөл байдалд УИХ Кибер аюулгүй байдлын тухай хууль баталж, эрх зүйн орчныг бүрдүүлсэн нь сайшаалтай ч мэдээллийн аюулгүй байдлыг хангах нь нэг удаагийн шинжтэй үйлдэл биш бөгөөд халдлага улам бүр бэлтгэгдсэн, хохирол ихтэй болж байгааг анхаарах шаардлагатай. Улс орнууд мэдээллийн аюулгүй байдлыг хангах ажиллагааг цаг ямагт тасралтгүй, идэвхтэй өрнүүлэх хэрэгтэй[79] болохыг судлаачид ч онцолж байна.

### 1.3.2. Мэдээллийн технологи, кибер аюулгүй байдлыг хангах хүрээнд батлах захиргааны хэм хэмжээний актууд

Кибер аюулгүй байдлын тухай хууль нь Монгол Улсад анхдагч бөгөөд сүүлийн 15 жилийн хугацаанд хэлэлцэж, төсөл нь 7 удаа боловсруулагдсан хууль юм.[80] Тус хууль батлагдсанаар кибер аюулгүй байдлыг хангах тогтолцоо, эрх зүйн орчин бүрдэж, иргэн, хуулийн этгээд, төрийн байгууллагын кибер аюулгүй байдлыг хангах талаарх эрх, үүрэг нь тодорхой болж, кибер аюулгүй байдлыг хангах үйл ажиллагааг хэрэгжүүлэх, кибер аюулгүй байдлын эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудит хийх, хяналт тавих, нэгдсэн удирдлага зохион байгуулалтаар хангах боломж бүрдсэн.[81]

ВХҮҮ нь Кибер аюулгүй байдлын тухай хуульд заасан хуулийн этгээд болохын хувьд тус хуульд заасан кибер аюулгүй байдлыг хангахтай холбоотой баталж, хэрэгжүүлэх журмуудаас өөрт хамаарахыг дагаж мөрдөнө. Үүнд:

---

[78] Кибер аюулгүй байдлын тухай хууль боловсруулах хэрэгцээ, шаардлагыг урьдчилан тандан судалсан үнэлгээний тайлан. 2021.

[79] Л.Галбаатар. Монгол Улсын мэдээллийн аюулгүй байдлын эрх зүйн зохицуулалт: Өнөөгийн байдал, тулгамдсан асуудал, шийдвэрлэх арга зам. “Шүүх эрх мэдэл” сэтгүүл, 2018, №4, 113 дахь талаас дам эшлэв.

[80] http://www.parliament.mn/n/mo3on Кибер аюулгүй байдлын тухай хуулийн танилцуулга.

[81] http://www.parliament.mn/n/mo3on Кибер аюулгүй байдлын тухай хуулийн танилцуулга.

*Хүснэгт 16. Кибер аюулгүй байдлын тухай хуульд үндэслэж батлагдах журмууд*

| Батлах эрх бүхий этгээд | Батлах захиргааны хэм хэмжээний акт буюу журмын нэр | Хуулийн заалт |
|---|---|---|
| Засгийн газар | – Кибер аюулгүй байдлыг хангах, урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах нийтлэг журам[82]<br>– Төрийн мэдээллийн нэгдсэн сүлжээг байгуулах, ашиглах журам[83]<br>– Төрийн мэдээллийн нэгдсэн сүлжээнд холбогдох байгууллагын жагсаалт[84]<br>– Кибер халдлага, зөрчилтэй тэмцэх үндэсний төв болон нийтийн төвийн дүрэм, зохион байгуулалтын бүтэц, орон тоо, төвүүдийн ажиллах журам<br>– Кибер аюулгүй байдлын зөвлөлийн Ажлын албаны бүтэц, орон тоо, ажиллах журам<br>– Онц чухал дэд бүтэцтэй байгууллагын жагсаалт[85] | 7.1<br>10.1.6<br>10.1.4<br>10.1.8<br>10.1.5 |
| Цахим хөгжил, харилцаа холбооны яам | – Мэдээллийн аюулгүй байдлын аудит хийх этгээдийг бүртгэх, аудит хийх журам[86]<br>– Кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх журам, аргачлал (Тагнуулын байгууллагатай хамтран) | 9.5.<br>8.3. |
| Тагнуулын байгууллага | – Үндэсний аюулгүй байдлыг хангах тусгайлсан чиг үүрэг бүхий болон төрийн захиргааны төв байгууллагатай мэдээлэл солилцох, хамтран ажиллах журам | 13.1.5 |

Үүнээс гадна Хорооноос баталсан Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журмын 4 дүгээр зүйлийн 4.2-т зааснаар мэдээллийн технологийн стандартын сүүлийн хувилбарыг хангаж, хөндлөнгийн эрх бүхий байгууллагаар баталгаажуулсан байх шаардлагыг биелүүлэх үүрэгтэй.

Хорооноос тус журмын гуравдугаар хавсралтаар ВХҮҮ-ийн үйл ажиллагаандаа мөрдөх мэдээллийн технологийн стандартын жагсаалт баталсан. Үүнд нийт 11 стандартыг журамласан ба кибер аюулгүй байдлыг хангахад чиглэсэн дараах стандарт байна.

---

82 Тус журмыг Кибер аюулгүй байдлын тухай хуулийн 12 дугаар зүйлийн 12.1.3-т зааснаар Цахим хөгжил, харилцаа холбооны яам Тагнуулын байгууллага, Зэвсэгт хүчний кибер аюулгүй байдлыг хангах байгууллагатай хамтран боловсруулна.

83 Төрийн мэдээллийн нэгдсэн сүлжээг байгуулах, ашиглах журам.

84 Төрийн мэдээллийн нэгдсэн сүлжээнд холбогдох байгууллагын жагсаалт.

85 Онц чухал дэд бүтэцтэй байгууллагын жагсаалт. 20220525-Дугаар-207-1.pdf (mddc.gov.mn)

86 Тус журмын төсөл олон нийтээс санал авах шатанд явж байна. https://mddc.gov.mn/wp-content/uploads/2022/07/%D0%9C%D0%90%D0%91-%D0%A5%D0%A5%D0%9C%D0%A2-%D0%B0%D1%83%D0%B4%D0%B8%D1%82-%D0%B6%D1%83%D1%80%D0%BC%D1%8B%D0%BD-%D1%82%D3%A9%D1%81%D3%A9%D0%BB.pdf

| | |
|---|---|
| MNS 5969 | Мэдээллийн технологи-Аюулгүй байдлын арга техник-Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлага |
| MNS 6197 | Мэдээллийн технологи-Мэдээллийн аюулгүй байдал-Криптографыг хэрэгжүүлэх удирдамж |
| MNS 6242-2 | Мэдээллийн технологи-Аюулгүй байдлын арга-Мэдээллийн технологийн сүлжээний аюулгүй байдал-2-р хэсэг: Сүлжээний аюулгүй байдлын архитектур |
| MNS ISO/IEC 27001 | Мэдээллийн технологи: Аюулгүй байдлын арга техник-Мэдээллийн аюулгүй байдлын удирдлагын тогтолцоо-Шаардлага |
| MNS ISO/IEC 13335-1 | Мэдээллийн технологи-Аюулгүй байдлын арга техник-Мэдээллийн ба холбооны технологийн байдлын удирдлага-1-р хэсэг: Мэдээлэл холбооны технологийн аюулгүй байдлын үндсэн ойлголтууд болон загварууд |
| MNS 6498 | Харилцаа холбооны тоног төхөөрөмжид тавих аюулгүй байдлын шаардлага |

MNS ISO/IEC 27001 стандартын журмыг Стандарт, хэмжил зүйн газар 2021 оны 9 дүгээр сарын 22-ны өдөр баталсан. Бусад 10 стандартын хувьд Хорооны 2022 оны 4 дүгээр сарын 6-ны өдрийн 174 дүгээр тогтоолд[87] зааснаар 2023 оны 3 дугаар сарын 31-ний өдрөөс дагаж мөрдөнө.

Кибер аюулгүй байдлын тухай хууль нь 2022 оны 5 дугаар сарын 1-ний өдрөөс эхлэн дагаж мөрдөгдсөн боловч өнөөдрийн байдлаар хуульд заасан дээрх хэм хэмжээний актуудаас Төрийн мэдээллийн нэгдсэн сүлжээг байгуулах, ашиглах журам, Төрийн мэдээллийн нэгдсэн сүлжээнд холбогдох байгууллагын жагсаалт, Онц чухал дэд бүтэцтэй байгууллагын жагсаалт л батлагдсан байна. Кибер аюулгүй байдлын нийтлэг журамд нийцүүлэн хуулийн этгээдүүд өөрсдийн дотоод журмыг батлах бөгөөд нийтлэг журам батлагдаагүй нь хуулийн этгээдийн хуулиар хүлээсэн үүргийн хэрэгжилтэд нөлөөлөх юм.

Мөн кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлагаар хангах, уялдуулан зохицуулах, хэрэгжилтийг зохион байгуулах, мэдээлэл солилцох чиг үүрэг бүхий орон тооны бус Кибер аюулгүй байдлын зөвлөлтэй байхаар хуульд заасан. Гэвч 2022 оны 7 дугаар сарын байдлаар уг Зөвлөл байгуулагдаагүй бөгөөд Зөвлөлийн бүрэлдэхүүн, дүрэм, бүтэц, орон тоо, ажиллах журмыг Засгийн газар батлаагүй байна.

[87] Санхүүгийн зохицуулах хорооны 2022 оны 4 дүгээр сарын 6-ны өдрийн 174 дугаартай "Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журам батлах тухай" тогтоол.

# ХОЁР. ЭРҮҮГИЙН ХЭРЭГ ХЯНАН ШИЙДВЭРЛЭХ АЖИЛЛАГАА ДАХЬ ЦАХИМ НОТЛОХ БАРИМТЫН ЗОХИЦУУЛАЛТ

## 2.1. Цахим нотлох баримт (дижитал нотлох баримт)-ын төрөл, онцлог

Кибер гэмт хэрэг үйлдэж буй орон зай, тухайн хэрэгт ашиглаж буй төхөөрөмж, хэрэгсэл, халдлагын зүйлээс шалтгаалж зөвхөн уламжлалт нотлох баримт (бичгэн болон эд мөрийн баримт)-уудад тулгуурлан тухайн үйл явдал болсныг нотлох, эсхүл үгүйсгэх боломжгүй тул цахим нотлох баримт цуглуулах, бэхжүүлэх, хадгалах, хамгаалах ажиллагаа чухал байр суурь эзэлдэг. Улс орнуудын эрх зүйн тогтолцооны онцлогтой холбоотойгоор хууль тогтоомж, судлаачдын бүтээлд "цахим нотлох баримт", "дижитал (тоон) нотлох баримт" гэсэн нэр томьёо хэрэглэж байх тул хууль зүйн эдгээр ойлголтын нийтлэг шинж, онцлог, төрлүүдийг энэхүү хэсэгт судалсан болно.

Хэрэгт ач холбогдол бүхий цахим, аналоги, дижитал (тоон) баримтуудыг хамтад нь "Цахим баримт" гэж нэрлэн хэрэг хянан шийдвэрлэх ажиллагаанд нийтлэг байдлаар хэрэглэж байгаа тул энэхүү судалгаанд "цахим нотлох баримт" гэсэн нэр томьёо хэрэглэв.

### 2.1.1. Цахим нотлох баримт ба мэдээлэлд нэвтрэх зарчим

Мэдээлэл (дохио) боловсруулж буй аргад нь үндэслэн цахим нотлох баримтыг "аналоги" болон "дижитал (тоон)" баримт гэж хоёр ангилдаг.[88] Аналоги төхөөрөмж гэдэгт хар цагаан зураг, хальсан дээр буулгасан гэрэл зураг, видео-кассет, дуу хураагуурт хураасан бичлэг зэрэг нотлох баримтын анхдагч шинжийг түлхүү агуулсан, хадгалалтын онцгой нөхцөл шаардах баримтуудыг ойлгох бөгөөд эдгээрийн хэрэглээ өнөөдрийн байдлаар буурсан. Харин дижитал нотлох баримтад "бит"[89] бүр нь 1 эсвэл 0 гэсэн хоёртын хэлбэрээр илэрхийлэгдэж буй баримт мэдээллүүд болох компьютер, гар утас, мессеж, мессенжер зэрэг хадгалагдаж, дамжуулагдаж буй мэдээлэл, зурвасуудыг хамааруулдаг.

Аналоги эсхүл дижитал гэдгээс үл хамаарч цахим нотлох баримт нь хүний хувийн мэдээллийг шууд агуулж байдаг тул "*Мэдээлэлд нэвтрэх үйл ажиллагаа нь тухайн мэдээллийг хайж олох зорилгодоо нийцсэн байх*" зарчим баримтлах шаардлагатай.[90] Уг зарчмын дагуу мөрдөн шалгах

[88] Калитин Сергей Вячеславович. Доказательства электронные и цифровые. Научно-методический электронный журнал "Концепт", 2014, т.20, с.3586-3590. https://e-koncept.ru/2014/54981.htm

[89] Мэдээллийн хэмжих хамгийн жижиг нэгж буюу "Binary digit" нэр томьёоны товчлол.

[90] Data Jurisdiction outcome framing brief in electronic evidence. 2022, May 31, p.1-6. https://www.internetjurisdiction.net/uploads/pdfs/Data-Jurisdiction-Outcome-Framing-Brief-on-Electronic-Evidence.pdf (Сүүлд хандсан 2022.07.27).

ажиллагаанд нэг талаас “хувийн халдашгүй байдлыг хангах” буюу хүний хувийн мэдээллийг, тэр дундаа эмзэг мэдээллийг хамгаалах, нөгөө талаас “нийгмийн аюулгүй байдлыг хангах” буюу гэмт хэргийг илрүүлэх, мөрдөн шалгах, үндэсний аюулгүй байдлыг хангах гэсэн хоёр ашиг сонирхлыг нэгдмэл байдлаар авч үзэж, харилцан тэнцвэртэй байдлыг нь хангах ёстой.[91] Тухайлбал, ВХҮҮ-д хадгалагдаж буй хэрэглэгчийн мэдээлэлд нэвтрэх эрхийг хязгаарлагдмал хүрээнд буюу гэмт хэрэг мөрдөн шалгах зорилгод нийцүүлж, хувийн мэдээлэл цуглуулах, нөгөөтээгүүр бусад этгээдийн хувийн халдашгүй байдлыг хангах ёстой.

“Хувийн халдашгүй байдлыг хангах” болон “нийгмийн аюулгүй байдлыг хангах” ашиг сонирхлыг хооронд нь эрэмбэлэх боломжгүй тул цахим нотлох баримтад нэвтрэх ажиллагаа нь нотлох баримт цуглуулах зорилго, зайлшгүй шаардлага, тэдгээрийн тэнцвэртэй байдлыг хангах зарчимд үндэслэгдэнэ. Уг зарчмыг цахим нотлох баримт буюу цахим захидал, цахим баримт бичиг, дижитал бичлэг, дуу, зураг болон мэдээлэл, харилцаа холбооны сүлжээ интернэт дэх мэдээлэл, нийгмийн сүлжээнд хадгалагдаж буй мэдээллийг олж авах ажиллагаанд баримтлахаар журамлах нь зүйтэй.

Түүнчлэн мэдээлэл технологид суурилсан үйлчилгээ, бүтээгдэхүүнд мэдээлэл хадгалагдаж байгаа тул тухайн мэдээллийг цуглуулах хэмжээ, төрөл бүрийг харгалзан үзэж, мэдээллийг хамгаалах арга хэмжээг тодорхойлох шаардлагатай.[92] Иймд цахим нотлох баримт олж авахад хувийн халдашгүй байдлыг хамгаалах арга хэмжээг үр дүнтэй зохион байгуулах үүднээс цахим нотлох баримтыг төрөлжүүлэх шаардлага үүсдэг.

### 2.1.2. Цахим нотлох баримтын төрлүүд

Цахим нотлох баримт нь кибер гэмт хэрэг төдийгүй уламжлалт гэмт хэргийг мөрдөн шалгахад чухал ач холбогдолтой нотлох баримт юм. Тухайн нотлох баримтад хандах эрхийн зохицуулалт улс орон бүрд харилцан адилгүй байх хэдий ч хүний хувийн халдашгүй байдалд халдах болон түүнийг хамгаалах үйл ажиллагааны түвшинд үндэслэн цахим нотлох баримтыг дараах гурван төрөлд ангилна. Үүнд:[93]

1. Хэрэглэгчийн мэдээлэл (*Subscriber information*)-Тодорхой үйлчилгээ авч буй хэрэглэгчийг тодорхойлоход ач холбогдолтой мэдээллүүд. Хэрэглэгч бүртгүүлэх болон түүнд тодорхой үйлчилгээ үзүүлэх үед цуглуулсан мэдээллүүд байна. Тухайлбал, нэр, гэрийн хаяг, цахим шуудангийн хаяг, утасны дугаар г.м. Эдгээр мэдээлэл гэмт хэргийг мөрдөн шалгах ажиллагаанд нэн тэргүүнд шаардлагатай мэдээллүүд байх тул хуульд зааснаар мэдээлэлд шууд хандаж, хууль сахиулах эрх бүхий ажилтны бүрэн эрхэд хадгалагдана.

---

[91] Data Jurisdiction outcome framing brief in electronic evidence, 2022, May 31, p.1-6. https://www.internetjurisdiction.net/uploads/pdfs/Data-Jurisdiction-Outcome-Framing-Brief-on-Electronic-Evidence.pdf (Сүүлд хандсан 2022.07.27).

[92] Мөн тэнд.

[93] Мөн тэнд.

2. Хандалт/хөдөлгөөн буюу шилжүүлгийн өгөгдөл (*Traffic/Access and Transactional data*)-Хэрэглэгч хоорондын харилцсан мэдээлэл, холбоос, IP хаяг, газар зүйн байршлын мэдээлэл, тодорхой үйлчилгээнд авсан мэдээлэл, харилцааны үүсэл, үргэлжилсэн хугацаа, огнооны талаарх мэдээллүүд. Хууль эрх зүйн зохицуулалтаас хамаарч зарим улс оронд үйлчилгээг эхлүүлэх, зогсоохтой холбоотой мэдээлэл мөн хамаардаг. Тухайн мэдээлэлд нэвтрэх, мэдээлэл цуглуулахад прокурорын зөвшөөрөлтэй байхыг шаардана.
3. Контентын[94] өгөгдөл (*Content data*)-Контент болон цахим шуудан, мессеж, зурган мэдээллүүд. Эдгээр мэдээлэлд нэвтрэх эрхийг зөвхөн шүүгчийн захирамжийн дагуу олгодог.

Хувийн халдашгүй байдалд халдах эрсдэлийн түвшинд үндэслэн нотлох баримтын төрлийг тодорхойлж, мэдээлэлд нэвтрэх эрхийн зохицуулалт хийж байгаа нь хүний хувийн мэдээлэл, эмзэг мэдээлэл алдагдах, гадагш задрах, хувийн аюулгүй байдал алдагдах эрсдэлээс сэргийлэх ач холбогдолтой.

Дээр өгүүлснээс гадна шүүхийн шинжээчдийн "Цахим нотлох баримтын криминалистикийн дэд салбарууд"-аас үзвэл дараах дөрвөн төрлийн цахим нотлох баримтад шинжилгээ хийж байна[95]:

1. Компьютерын шинжилгээ - Системийн бүртгэл (хөтчийн түүх, санах ой)-ээс их хэмжээний цахим мэдээлэл цуглуулах, олж авах ажиллагааг гүйцэтгэнэ. Компьютерын нотлох баримт (цахим нотлох баримт)-ыг дараах тохиолдолд хүлээн зөвшөөрөгдөхүйц шинжээ алдсан гэж үздэг.[96] Үүнд:
   - Компьютерыг зүй бусаар ашиглах замаар үүсгэсэн мэдээлэл;
   - Компьютер зохих ёсоор ажиллаагүй, хүндэтгэн үзэх шалтгааны улмаас, эсхүл тийм шалтгаангүйгээр ажиллаагүй байсантай холбоотойгоор мэдээлэл үүсэх үйл явцад, эсхүл мэдээллийн агуулгад өөрчлөлт орсон, нөлөөлсөн байж болзошгүй.

   Компьютерт хадгалагдаж буй мэдээлэл нь хүлээн зөвшөөрөгдөхүйц шинжийг хадгалж буй эсэхийг тусгай мэргэжлийн шинжээч шинжилгээний үндсэн дээр тогтооно.
2. Өгөгдлийн сангийн шинжилгээ - Өгөгдлийн сан болон мета дата боловсруулах ажиллагааг гүйцэтгэх бөгөөд хэрэгт ач холбогдол

[94] Өргөн нэвтрүүлгийн тухай хуулийн 4 дүгээр зүйлийн 4.1.8 дахь хэсэгт зааснаар "Контент" гэж харилцаа холбооны сүлжээгээр дамжиж байгаа үг, дуу, тэмдэг, дохио, текст, зураг, график, хөдөлгөөнт дүрс бүхий бүх төрлийн мэдээ, мэдээллийн электрон хэлбэрт хувиргасныг" ойлгоно. https://legalinfo.mn/mn/detail/15067

[95] Priyanka V.Kayarkar, Prashant Ricchariya, Anand Motwani. Mining Frequent Sequences for emails in cyber forensics investigation. International Journal of Computer Applications, January 2014, Volume 85, No 17.

[96] Ian J. Lloyd. Information technology law. 9th edition, 2020, p.216.

бүхий мэдээлэл олж авахад өгөгдлийн сан, файлын бүртгэл ашиглана.

3. Сүлжээний шинжилгээ - Хэрэгт ач холбогдол бүхий нотлох баримт цуглуулах зорилгоор компьютерын сүлжээний ачааллыг шинжлэх бөгөөд *LAN* (дотоод сүлжээ) болон *MAN* (орон нутгийн сүлжээ), / *internet* сүлжээгээр дамжин өнгөрөх өгөгдлийг хянадаг.
4. Утасны төхөөрөмжийн шинжилгээ - Утсан төхөөрөмжийн устгагдсан мэдээллийг сэргээхээс илүүтэй дуудлага, мессеж, цахим шуудангийн мэдээллийг шинжилдэг байна.

Криптобиржид халдах буюу кибер орчинд хууль бусаар халдах гэмт хэргийн мөрдөн шалгах ажиллагаанд цахим нотлох баримт олж авах, цуглуулсан баримтад шинжилгээ хийхэд дээр дурдсан криминалистикийн дэд салбаруудаар шинжилгээ хийх шаардлагатай бөгөөд зөвхөн компьютерын шинжилгээнд үндэслэн тухайн нөхцөл байдлыг бүрэн тогтоох боломжгүй юм.

### 2.1.3. Цахим нотлох баримтын онцлог

Цахим нотлох баримт нь өргөн утгаараа “тухайн хэрэгт ач холбогдол бүхий хуульд заасан арга, хэрэгслээр олж авсан цахим төхөөрөмж, хэрэгсэлд хадгалагдаж буй цахим баримт, мэдээллийг” илэрхийлнэ. Харин явцуу утгаараа “зөрчил хэрхэн болсныг компьютер ашиглан батлах, эсвэл няцаах, тухайн зөрчил нь санаатайгаар үйлдэгдсэн, эсвэл хэрэгт холбогдолгүй болохыг батлах хадгалагдаж, эсвэл дамжуулж буй аливаа өгөгдлийг” хэлэх бөгөөд дараах онцлог шинжтэй.[97]

*Хүснэгт 18. Цахим нотлох баримтын онцлог*

| Онцлог | Тайлбар |
|---|---|
| Хэврэг | Компьютерын сүлжээгээр боловсруулсан зарим цахим өгөгдөл маш хэврэг учир амархан устаж, өөрчлөгддөг. Үүнийг цахим нотлох баримт цуглуулах үед онцгой анхаарах нь зүйтэй. Өгөгдөл зөвхөн *RAM* сүлжээний санах ойд хадгалагдах тул урьдчилан сэргийлэх техникийн тусгай арга хэмжээ аваагүй тохиолдолд сүлжээ гэмтэх буюу унтрах аюултай. Сүлжээний санах ойд хадгалагдсан мэдээлэл мөрдөн шалгах үйл ажиллагаанд чухал. Энэхүү нотлох баримтыг цуглуулах технологи нь уламжлалт нотлох баримт цуглуулах ажиллагаанаас ялгаатай. |
| Хувиргахад амархан | Цахим өгөгдлийг хувиргах буюу өөрчлөхөд амархан. Компьютерын шинжилгээний үндсэн суурь зарчмын нэг бол цахим нотлох баримтын бүрэн бүтэн байдлыг хадгалах явдал юм. Компьютерын өгөгдлийг бүрэн бүтэн хадгалах арга хэрэглэх, зохих бичиг баримт бүрдүүлэх нь мөрдөн байцаагчийн хувьд нотлох баримт цуглуулах, бэхжүүлэх талаар хуульд заасан журмыг баримтлаагүй буюу зөрчсөн гэх асуудлаар сэжигтний зүгээс гомдол гаргахаас зайлсхийхэд чухал. |

[97] Л.Галбаатар. Кибер гэмт хэргийг шүүхэд хянан шийдвэрлэх нь. УБ., 2015, 26 дахь тал.

| | |
|---|---|
| Тархан байршсан хадгалалт | Өргөн зурвасын хүртээмж, серверт зайнаас хадгалах боломж нь мэдээлэл хадгалах арга замд нөлөөлдөг. Өмнө нь мөрдөн байцаагчдын хувьд сэжигтний орон байранд төвлөрч компьютерын өгөгдлийг хайж болдог байсан бол одоо цагт тэдний хувьд тоон мэдээллийг хилийн чанадад, шаардлагатай бол сэжигтэй мэдээллийг зөвхөн алсаас хандаж хадгалж болно гэдгийг анхаарах шаардлагатай. |
| Техникийн дэвшлийн хурд | Техникийн дэвшил хурдацтай урагшилж байгаа нь криминалистикийн шинжилгээнд шинэ сорилт бий болгож байна. Ийм хөгжил нь нотлох баримт цуглуулах үүрэгтэй хүмүүсийг сургах, түүнчлэн одоогийн криминалистикийн шинжилгээний багаж, хэрэгслийг шинэчлэхийг шаардана. Үйлдлийн систем болон бусад программ хангамжийн бүтээгдэхүүнүүдийн шинэ хувилбарууд мөрдөн шалгах үйл ажиллагаанд холбоотой янз бүрийн мэдээлэл, өгөгдөл бий болгодог болсон. Ийм дэвшил программ хангамжаас гадна техник хангамжид хамаарах болов. |

## 2.2. Цахим нотлох баримттай ажиллахад баримтлах зарчмууд

### 2.2.1. *ADAM principle*[98]

Австрали Улсын Мюрдок их сургуулийн доктор Ричард Брэйн Адамс нь 2012 онд докторын судалгааны бүтээлдээ *ADAM* зарчмыг тодорхойлж, нийтийн хүртээл болгосон. Уг зарчмыг олон улсын стандартуудаас гадна Их Британи Улсын Цагдаагийн ахлах ажилтнуудын холбооны (*ACPO*) "Компьютерт суурилсан нотлох баримттай ажиллах сайн туршлага" удирдамжид заасан үзэл санаанд тулгуурласан гэж үздэг. Тухайн удирдамжид нотлох баримтын бүрэн бүтэн байдал, үнэн зөвийг тодорхойлоход дараах зарчмуудыг баримтлах талаар тусгажээ. Үүнд[99]:

- Зарчим 1. Шүүхэд хүргүүлж буй дижитал нотлох баримтад хууль сахиулах байгууллага болон албан тушаалтнуудаас ямар нэгэн хэлбэрээр өөрчлөлт оруулахгүй байх;
- Зарчим 2. Хэрэв тухайн нотлох баримтын эх өгөгдөлд нэвтрэх тохиолдолд тухайн мэдээлэлд нэвтрэх зайлшгүй шаардлага, зорилгыг тодорхойлж, нотлох;
- Зарчим 3. Цахим нотлох баримтыг ашиглаж буй явцын талаарх бүрэн тэмдэглэл үйлдэж (хэш[100] болон үйлдлийн мэдээлэл), хяналтын бүртгэл хөтөлж хадгалах бөгөөд тухайн хэрэгт

[98] Advanced Data Acquisition Model.

[99] The ACPO principles of Digital based evidence, https://athenaforensics.co.uk/acpo-guidelines-for-computer-forensics/

[100] Hash буюу хэш нь өгөгдөл болон файлуудыг утга болгон хувиргадаг тодорхой алгоритмд тодорхой оролтыг оруулах үед гаралт хэлбэрээр үүсдэг тоон утга юм.

хамааралгүй гуравдагч этгээд тухайн баримтыг судалж, ижил дүгнэлтэд хүрэх боломжтой байх;

- Зарчим 4. Энэ зарчмууд болон хууль тогтоомжийн биелэлтийг хангах үүргийг хэрэг хянан шийдвэрлэх ажиллагаа хариуцсан эрх бүхий албан тушаалтан хүлээх.

*ADAM principle* буюу Нарийвчилсан мэдээлэл цуглуулах загвар зарчмын дагуу цахим нотлох баримт олж авч, цуглуулж буй мэргэжилтэн (*practitioner*) дараах зарчмуудыг баримтална. Үүнд:[101]

1. Эх өгөгдөлд аливаа өөрчлөлт хийхгүй байх. Хэрэв ажлын зайлшгүй шаардлагаар энэ шаардлагыг биелүүлэх боломжгүй бол нотлох баримтын эх өгөгдөлд нэвтэрсэн мэргэжилтний үйлдлийн эх нотлох баримтад үзүүлэх нөлөөг тодорхойлсноор аливаа өөрчлөлт үүсгэсэн үйл явцыг зөвтгөнө;
2. Анхны өгөгдөл болон түүний хуулбарыг олж авах, тэдгээртэй харилцсан бүх үйл ажиллагааны бүрэн бүртгэл хөтөлнө. Үүнд, хэш функц ашиглан баталгаажуулах процесс, хамгаалалтын гинжин хэлхээ[102]-ний хадгалалт зэрэг хамаарна;
3. Цахим нотлох баримтын эхний хүлээн авагч (*Digital Evidence First Responder*) өөрийн мэдлэг, чадвараас давсан аливаа үйл ажиллагаа явуулахгүй;
4. Цахим нотлох баримтын эхний хүлээн авагч хувийн болон тоног төхөөрөмжийн аюулгүй байдлыг бүх талаар анхаарч үзэх ёстой;
5. Өөрийн үйл ажиллагаанаас болж хохирсон аливаа этгээдийн хууль ёсны эрхийг анхаарч үзэх ёстой;
6. Өөрийн үйл ажиллагаанд хамаарах байгууллагын бүхий л бодлого, дүрэм журмыг анхаарч, энэ талаар мэдлэгтэй байх;
7. Үйлчлүүлэгч, хуулийн мэргэжилтнүүд, багийн ахлагч болон бусад гишүүдтэй зохих ёсоор харилцах.

### 2.2.2. Цахим нотлох баримтыг таньж тодорхойлох, цуглуулах, олж авах, хадгалах *ISO/IEC 27037:2012* стандарт[103]

*ISO/IEC 27037:2012*[104] стандартаар цахим нотлох баримтыг таньж тодорхойлох, цуглуулах, олж авах, хадгалахтай холбоотой харилцааг зохицуулах бөгөөд тухайн баримтад дүгнэлт хийх, танилцуулах, устгах

---

101 https://researchrepository.murdoch.edu.au/id/eprint/14422/2/02Whole.pdf Richard Brian Adams. The Advanced Data Acquisition Model (ADAM): Process model for Digital Forensic practice. 2012.

102 A chain of custody буюу хамгаалалтын гинжин хэлхээ гэдэг нь мэдээлэл, тэмдэглэлийг үүсгэснээс хойш устгах хүртэл хугацаанд байршуулж, хандаж байсан бүхий л үйл ажиллагааг бүрэн, баримтжуулсан, он цагийн дараалал бүхий түүхийг хэлнэ. https://www.ironmountain.com/resources/general-articles/m/maintaining-the-chain-of-custody-at-iron-mountain#:~:text=What%20Is%20It%3F,its%20creation%20through%20its%20destruction.

103 Jaromir Veber and Zdenek Smuthy, July 2015, “Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic”, 14th European Conference on Cyber Warfare and Security, Hatfield, UK.

харилцааг төдий л зохицуулаагүй. Нотлох баримтын эхний хүлээн авагч (*Digital Evidence First Responder*) нь дараах цахим нотлох баримтын бүрэн бүтэн болон найдвартай байдлыг хангахын тулд дараах ерөнхий зарчмуудыг баримтална. Үүнд:

- Цахим хэрэгсэл болон өгөгдлийн нарийн төвөгтэй байдлыг бууруулах;
- Хөндлөнгийн этгээдээр нотлох баримтад хараат бус дүгнэлт гаргуулахын тулд цахим нотлох баримттай холбоотой хийгдэж буй ажиллагаа, өөрчлөлт бүрийг баримтжуулах;
- Тухайн улсын хууль тогтоомжид заасан журмыг баримтлах;
- Нотлох баримтын эхний хүлээн авагч нь өөрийн чадвараас хэтэрсэн үйлдэл гаргахгүй байх.

*ISO/IEC 27037:2012* цахим нотлох баримт боловсруулах үйл ажиллагаа нь дараах үе шатуудаас бүрдэнэ. Үүнд[105]:

1. Таньж тодорхойлох (*Identification*) - Цахим нотлох баримтыг хайх, олж илрүүлэх, баримтжуулах ажиллагаа хамаарна. Материаллаг болон логик хэлбэрээр аль алинаар нь илэрдэг. Тухайн хэрэгт хамааралтай цахим нотлох баримтыг агуулж болзошгүй бүх төхөөрөмжийг тодорхойлно. Нотлох баримтын эхний хүлээн авагч[106] нь гэмт хэрэгт хамааралгүй мэт санагдсан жижиг, нуусан төхөөрөмж, хэрэгслийг анзааралгүй өнгөрөхгүйн тулд системчилсэн хайлт хийх, виртуал хэлбэрээр хадгалагдаж буй нуугдмал нотлох баримт байх боломжтой эсэхийг нягтлах шаардлагатай. Мөн нотлох баримт хүлээн авах явцад төхөөрөмжийн тогтворгүй байдал үүссэн тохиолдолд төхөөрөмжүүдийг эрэмбэлэх, нотлох баримт цуглуулах, боловсруулах ажиллагаа дахь цахим нотлох баримтад учирч болзошгүй хохирлыг бууруулах ёстой.
2. Цуглуулах (*Collection*) - Таньж тодорхойлох ажиллагааны дараа цахим нотлох баримт агуулж буй төхөөрөмж, хэрэгслүүдийг одоогийн байршлаас нь шилжүүлэн лабораторид хүргэж, дүгнэлт гаргах дараагийн шатанд шилжинэ. Төхөөрөмжийг баглах, лабораторид шилжүүлэх зэрэг цуглуулах ажиллагааны бүхий л үйл явцыг баримтжуулдаг. Нотлох баримтын эхний хүлээн авагч нь цахим нотлох баримтад хамаарах материаллаг эд зүйл (нууц үг агуулсан цаасан дээрх тэмдэглэл, төхөөрөмжийн холбогч, тодорхойлогдсон төхөөрөмжүүдээс цахим мэдээлэл олж авахад шаардлагатай техник хангамжууд)-ийг цуглуулна.

---

[104] Jaromir Veber and Zdenek Smuthy, July 2015, "Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic", 14th European Conference on Cyber Warfare and Security, Hatfield, UK.

[105] Jaromir Veber and Zdenek Smuthy, July 2015, "Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic", 14th European Conference on Cyber Warfare and Security, Hatfield, UK.

[106] Эрүүгийн хэрэг хянан шийдвэрлэх ажиллагааг хэрэгжүүлэгч буюу энэ тохиолдолд цахим нотлох баримтын хамгийн түрүүнд олж авах, цуглуулах, бэхжүүлэх ажиллагааг хэрэгжүүлж буй мөрдөгчийг ойлгоно.

3. Мэдээлэл олж авах (*Acquisition*) - Цахим нотлох баримтад холбогдох эхний ажиллагаа нь тэдгээрийг хуулбарлахад (Жишээ нь, хард диск дээр хадгалагдаж байгаа контентуудыг хуулбарлах) ашигласан аргуудыг баримтжуулахад оршино. Шаардлагатай бол устгагдсан файлуудыг олж авах шаардлагатай. Эх хувь болон хуулбар хувь нь ижил гаралтаас үүсгэгдсэн буюу баталгаажсан байх ёстой. Нөхцөл байдлаас (нөхцөл, цаг, үнэ) шалтгаалан нотлох баримтын эхний хүлээн авагч хамгийн тохиромжтой арга, журмыг сонгох ёстой. Хуулбарлах ажиллагааны явцад эх хувь болон хуулбар хувь өөрчлөгдсөн нөхцөлд өөрчлөгдсөн мэдээллийг баримтжуулах шаардлагатай. Баталгаажуулах ажиллагаа хийх боломжгүй нөхцөл (тухайлбал, ажиллаж буй системээс мэдээлэл хүлээн авах явцад мэдээлэл нь муу секторт байрласан, эсхүл мэдээлэл авах хугацаа хязгаарлагдмал үед)-д цахим нотлох баримтын эхний хүлээн авагч нь боломжит сайн хувилбар ашиглаж, дараа нь өөрийн сонгосон аргыг баталгаажуулна. Хэрэв хуулбарыг баталгаажуулах боломжгүй бол баримтжуулсан нь үндэслэлтэй байх ёстой. Цахим нотлох баримт (өгөгдөл) нь хэтэрхий том хэмжээтэй бол нотлох баримтын хүлээн авагч нь зөвхөн хэрэгт хамааралтай файл, фолдерыг хэсэгчлэн авна.
4. Хадгалалт (*Preservation*) - Мөрдөн шалгах ажиллагаанд цахим нотлох баримт хэрэглэх нөхцөл бүрдүүлэх зорилгоор нотлох баримтын бүрэн бүтэн байдлыг хамгаалах арга хэмжээ авна. Цахим нотлох баримтын эхний хүлээн авагч нь нотлох баримтыг анх цуглуулж авснаас нь хойш өөрчлөгдөөгүй болохыг нотлох, өөрчлөгдсөн тохиолдолд үндэслэл, үйлдлийг баримтжуулсан баримт гаргаж өгөх ёстой. Энэхүү ажиллагааг ихэвчлэн цагдаа, шинжээчийн баг хариуцна.

### 2.3. Мөрдөн шалгах явцад цахим нотлох баримт цуглуулах, шалгаж, бэхжүүлэх ажиллагаа

Судалгааны өмнөх хэсэгт дурдсан цахим нотлох баримттай ажиллах зарчмуудад тулгуурлан тухайн нотлох баримтыг цуглуулах, шалгах, бэхжүүлэх процесс ажиллагааг журамладаг байна. Тухайлбал, Олон улсын эрүүгийн цагдаагийн байгууллага (Интерпол)-аас 2021 оны 3 дугаар сард цахим нотлох баримт эрэн хайх, хураан авах ажиллагааны сайн туршлагад үндэслэн зөвлөмж гаргасан. Тус зөвлөмжид *ISO/IEC 27037:2012* стандартаар тогтоосон шаардлагуудыг тусгаж, цахим нотлох баримт эрэн хайх, хураан авах ажиллагааг таван алхамтай байхаар тусгажээ. Үүнд:[107]

1. Хэргийн газрыг аюулгүй болгох

Мэдээлэл алдагдахаас сэргийлж, оролцогчдын мэдээллийн аюулгүй байдлыг хангах зорилгоор тус ажиллагааг тусгай нэгжүүд хариуцан гүйцэтгэдэг. Цахим нотлох баримт цуглуулах явцад аливаа баримт, мэдээлэл, өгөгдөл

[107] https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

устах, өөрчлөгдөхөөс урьдчилан сэргийлэх хүрээнд дараах арга хэмжээг зохион байгуулна:

- Хэргийн газарт зөвшөөрөлгүй хүн нэвтрэх, гадны этгээдийг компьютер, гар утас, цахилгаан хангамж зэрэг бусад төхөөрөмжид ойртохыг хатуу хориглоно.
- Зайнаас мэдээлэл устгагдахаас урьдчилан сэргийлж, холбогдогч нь хэргийн газарт байх хүнтэй холбоо тогтоохгүй байх арга хэмжээг авна.
- Компьютер, гар утас зэрэг төхөөрөмжүүд нь интернэтэд холбогдсон тохиолдолд мэдээлэл алдагдахаас урьдчилан сэргийлж, цахим нотлох баримтыг шалгаж, бэхжүүлэх ажиллагааг гүйцэтгэнэ.
- Төхөөрөмжид хадгалагдаж буй мэдээлэлд зайнаас нэвтрэх, өөрчлөх боломж олгодог утасгүй сүлжээ байгаа эсэхийг шалгана.
- Ажиллагааны явцад бүрэн эрх олгогдоогүй ажилтнуудаас санал болгосон аливаа тусламжаас татгалзана.

Дээрх арга хэмжээг бүрэн зохион байгуулж, хэргийн газрыг аюулгүй болгосны үндсэн дээр цахим нотлох баримтын эхний хүлээн авагч нь ерөнхий үнэлгээ хийж гүйцэтгэнэ.

2. Үнэлгээ хийх

Цахим нотлох баримтын эхний хүлээн авагч буюу хэргийн газарт ажиллаж буй мөрдөгч нь нөхцөл байдлын талаарх ерөнхий үнэлгээг дараах байдлаар гүйцэтгэнэ. Үүнд:

- Боловсруулах боломжтой баримтын тоон утга, цаашид хийж гүйцэтгэх ажиллагаанд шаардагдах төхөөрөмж, зарцуулах хугацаа, гарах зардлыг урьдчилсан байдлаар үнэлж, тодорхойлно.
- Хэргийн газрыг зургаар баримтжуулж, тайлан гаргана.

Ердийн журмаар эд хөрөнгө хураан авах ажиллагааг гүйцэтгэхийн зэрэгцээ цахим нотлох баримт олж авч баримтжуулах, цуглуулах ажиллагааг хамт гүйцэтгэнэ.

3. Нөхцөл байдлыг баримтжуулах

Цахим нотлох баримт цуглуулах, бэхжүүлэх бүх үйл явцыг зохих журам болон хуульд заасан шаардлагын дагуу зохих ёсоор баримтжуулсан байх ёстой. Төхөөрөмжийн анх байсан байршил, төхөөрөмжийн шинж байдлын талаарх дэлгэрэнгүй бүртгэл үйлдэнэ. *Тухайлбал*: "*Зөөврийн компьютер: нотлох бариmтын дугаар EVI 0018, брэнд загвар, ой санамжийн багтаамж, серийн дугаар, төлөв байдал (гэмтсэн, асаалттай, унтраалттай г.м.), нэвтрэх ID, нууц үг болон нэмэлт мэдээлэл (хуцхдуцд ашигладаг, эсхүл интернэтэд холбогдоогүй г.м.)*" мэдээлэл агуулсан байна.

4. Цахим нотлох баримт цуглуулах, боловсруулах

Хэргийн газрыг баримтжуулж дууссаны дараа цахим нотлох баримт цуглуулж, боловсруулах үе шатыг үргэлжлүүлэн гүйцэтгэнэ. Энэ

шатанд нотлох баримттай ажиллах нийтлэг зарчим баримталж, дараах ажиллагаанууд хийгдэнэ. Үүнд:

*Хүснэгт 19. Цахим нотлох баримт цуглуулах, боловсруулах ажиллагаанд анхаарах зүйлс*

| Асаалттай төхөөрөмжийн хувьд | Унтраалттай төхөөрөмжийн хувьд |
|---|---|
| – Асаалттай төхөөрөмжийг унтраахгүй буюу унтрахаас сэргийлж дэлгэцийг амраах, дэлгэц түгжих үйлдлүүдийг идэвхгүй болгох;<br>– Дотоод болон гадаад хандалт байгаа эсэхийг шалгаж, шаардлагатай тохиолдолд сүлжээг тусгаарлах;<br>– Үүлэн хадгалах санд нэвтрэх боломжгүй бол төхөөрөмжийг холбогдсон сүлжээнээс шууд тусгаарлах;<br>– Төхөөрөмжийн шифрлэлтийн систем ажиллаж байгаа эсэхийг шалгах (*Bitlocker, FileVault, VeraCrypt, PGP* диск гэх мэт);<br>– Цахилгааны тэжээлтэй холбоотой эсэхийг шалгах. | – Тухайн улсын хууль тогтоомжоор зөвшөөрсөн бол холбогдогчоос төхөөрөмжид нэвтрэх нууц үг/пин кодыг асууж, зөв эсэхийг шалгах;<br>– Холбогдогч нь холбоотой өөр төхөөрөмж ашигласан байж болзошгүй тул холбоотой байж болох төхөөрөмжүүдийг хайж олох, цуглуулах; |

Төхөөрөмжид хадгалагдаж буй мэдээллийг хуулбарлан авах замаар цахим нотлох баримт цуглуулах ажиллагааг гүйцэтгэдэг. Цахим нотлох баримтын хуулбар үүсгэх үйл явцыг дараах байдлаар баримтжуулна:

- Мэдээллийг (зургаар баталгаажуулсан, эсхүл ашигласан системийн мэдээллийг) хуулбарласан арга;
- Ашигласан цахим хэрэгсэл (техник хангамж, эсхүл программ хангамжийн мэдээлэл);
- Хэрэгт ач холбогдол бүхий мэдээллийн байршил: диск, эсхүл утсан дахь "..." нэртэй файл, "..." кодтой зураг г.м.
- Хэшлэх, түүнд холбогдох мэдээлэл, код;
- Ажиглалтын тэмдэглэл буюу хуулбарлах явцад гарсан асуудлууд (мэдээлэл устсан, өөрчлөгдсөн г.м.).

5. Цахим нотлох баримтыг хураан авах

Цуглуулж, бэхжүүлсэн цахим нотлох баримтыг лацдаж, битүүмжилсний үндсэн дээр хураан авах ажиллагааг гүйцэтгэнэ. Баримтыг битүүмжлэхээс өмнө төхөөрөмжийн шинж байдлыг агуулсан шошго бүхий таних тэмдэг үйлдэж, нотлох баримтыг гадны этгээд ашиглахаас сэргийлж, зориулалтын сав баглаанд хийнэ.

Цахим нотлох баримтаас гадна цахим мэдээллийг олж авахад туслах бусад эд мөрийн болон бичгэн баримтуудыг (нэвтрэх нэр, эсхүл код бичигдсэн тэмдэглэл г.м.) хамт хураан авч, шинжилгээний тусгай байгууллагад хүргүүлнэ.

Дээрх зөвлөмжөөр санал болгож буй алхмуудыг аливаа улс мөрдөн шалгах ажиллагаандаа нийцүүлж, хэрэгжүүлэхийг Олон улсын эрүүгийн цагдаагийн байгууллагаас зөвлөдөг. Эдгээр алхмыг Монгол Улсын хууль тогтоомжтой харьцуулан судалж үзвэл зарим алхамд хамаарах үйл ажиллагааг нь хэрэгжүүлэхээр журамлажээ. Тодруулбал, Монгол Улсын ерөнхий прокурорын 2021 оны 5 дугаар сарын 20-ны өдрийн А/69 дүгээр тушаалын хавсралтаар батлагдсан *Эрүүгийн хэрэгт хөрөнгө, орлого, эд мөрийн баримт, эд зүйлийг хураан авах, бэхжүүлэх, хадгалах, хамгаалах, шилжүүлэх, шийдвэрлэх журам* (Журам)-ын 7.12 дахь хэсэгт цахим баримт хураан авах, бэхжүүлэх, хадгалах, хамгаалах, шилжүүлэх, шийдвэрлэх ажиллагааг дараах байдлаар зохицуулсан байна. Үүнд:

*Хүснэгт 20. Хураан авсан хөрөнгө, орлого, эд мөрийн баримтын талаар авах арга хэмжээний зохицуулалт - Монгол Улс*

| № | Алхам | Эрүүгийн хэрэгт хөрөнгө, орлого, эд мөрийн баримт, эд зүйлийг хураан авах, бэхжүүлэх, хадгалах, хамгаалах, шилжүүлэх, шийдвэрлэх журам (Журам)-ын зохицуулалт |
|---|---|---|
| 1 | Хэргийн газрыг аюулгүй болгох | Журамд эрүүгийн хэрэг хянан шийдвэрлэх ажиллагааг хэрэгжүүлэгч нь мэдээлэл алдагдахаас сэргийлэх зорилгоор хэргийн газарт мэдээллийн аюулгүй байдлыг хангаж, дотоод болон гадаад сүлжээнээс тусгаарлах, төхөөрөмжид хадгалагдаж буй мэдээлэлд гуравдагч этгээд халдахаас урьдчилан сэргийлэх чиглэлээр техникийн хяналт хийх талаар нарийвчлан зохицуулаагүй.<br><br>Харин журамд дараах зохицуулалтыг тусгасан:<br>7.12.6. Компьютер, цахим төхөөрөмжид хадгалагдаж байгаа бүх төрлийн мэдээлэл нь устах, гэмтэх эрсдэлтэй тул үзлэг хийхээс өмнө төхөөрөмжид байгаа мэдээллийг үзэх, агуулгыг хайх, асаах, унтраах зэргээр дур мэдэн оролдохыг хориглоно.<br>7.12.3 дахь хэсэгт цахим төхөөрөмж[108], мэдээлэл хадгалах хэрэгслийг[109] хураан авах шатанд ул мөр үлдсэн, интернэт холболтын модем, кабель шугам, бусад төхөөрөмжтэй холбогдсон эсэхийг шалгана. |
| 2 | Үнэлгээ хийх | Журмаар үнэлгээ хийх тусгайлсан үе шатыг тодорхойлоогүй тул мөрдөгчөөс зардал (боловсруулах боломжтой баримтын тоон утга, цаашид гүйцэтгэх ажиллагаанд шаардагдах төхөөрөмж, зарцуулах хугацаа, гарах зардал)-ын үнэлгээ гаргадаггүй. |

[108] Эрүүгийн хэрэгт хөрөнгө, орлого, эд мөрийн баримт, эд зүйлийг хураан авах, бэхжүүлэх, хадгалах, хамгаалах, шилжүүлэх шийдвэрлэх журмын 7.2.9 дэх хэсэгт зааснаар “Цахим төхөөрөмж” гэж суурин болон гар утас, гэрэл зургийн аппарат, дүрс бичлэгийн камер, таблет, сканер, факсын машин, хэвлэгч, хувилагч, бусад төхөөрөмжийг ойлгоно.

[109] Дээрх журмын 7.2.10 дахь хэсэгт зааснаар “Мэдээлэл хадгалах хэрэгсэл” гэж хард диск, флаш диск, санах ой бүхий картууд, CD, DVD болон бусад хэрэгслийг ойлгоно.

| | | |
|---|---|---|
| 3 | Нөхцөл байдлыг баримтжуулах | Хэргийн газар байгаа цахим төхөөрөмж тус бүрийн төрөл, шинж байдлын талаарх дэлгэрэнгүй бүртгэл үйлдэх ажиллагааг зохицуулаагүй. Хэргийн газарт байгаа цахим төхөөрөмж, мэдээлэл хадгалах хэрэгслүүдийг дугаарлаж, тэдгээр нь бүрэн бүтэн, эсхүл гэмтэлтэй эсэх, брэндийн нэр, ой санамжийн мэдээлэл, серийн дугаар, хэрэглэгчийн мэдээлэл, нэвтрэх нэр, нууц үгийн мэдээлэл агуулсан тухайлсан бүртгэлийн ажиллагааг журамлаагүй байна. |
| 4 | Цахим нотлох баримт цуглуулах, боловсруулах | Өмнөх алхмуудтай харьцуулахад цахим нотлох баримт цуглуулах ажиллагааг журамд дараах байдлаар харьцангуй тодорхой зохицуулсан.<br>7.12.1. Цахим баримтыг мэргэжилтний тусламжтайгаар тусгай техник хэрэгсэл, программ ашиглан хуулбарлан авч, энэ тухай тэмдэглэл[110] үйлдэж, үйл явцыг гэрэл зураг, дуу-дүрсний бичлэгээр бэхжүүлнэ.<br>7.12.2. Мэдээллийг хуулбарлахдаа хөндлөнгийн хоёроос доошгүй гэрчийг байлцуулан, засварлаж өөрчлөх боломжгүйгээр код үүсгэн “хэш” (хэшлэх-тусгай программ ашиглах), тэмдэглэл хөтөлж, түүнд байлцсан хүмүүсээр гарын үсэг зуруулна.<br>7.12.7. Компьютер, цахим төхөөрөмжийн дэлгэц дээрх мэдээлэл, өгөгдлийг устгаж байгаа шинж тэмдэг илэрсэн тохиолдолд шууд унтраана. |
| 5 | Цахим нотлох баримтыг хураан авах | ЭХХШтХ-ийн 24.4 дүгээр зүйлийн 9 дэх хэсэгт хэрэгт ач холбогдолтой цахим баримтыг хуулбарлан авах, эсхүл түүнийг устгах, нэвтрэх боломжийг хязгаарлах боломжгүй бол цахим төхөөрөмжийг хураан авах эрх зүйн үндэслэл бүрдүүлсэн. Хураан авах ажиллагаа нь хууль тогтоомжид үндэслэн хэрэгжих бөгөөд энэхүү ажиллагааг дараах журмаар гүйцэтгэнэ.<br>7.12.3. Цахим төхөөрөмж, мэдээлэл хадгалах хэрэгслийг хураан авахад ул мөр үлдсэн, интернэт холболтын модем, кабель шугам, бусад төхөөрөмжтэй холбогдсон эсэхийг шалгана.<br>7.12.4. Шаардлагатай бол модем, свитч, рүтер зэрэг сүлжээний төхөөрөмжийг хураан авч, тэмдэглэл үйлдэнэ.<br>7.12.8. Хэргийн газраас нууц үг бүхий цаас, программ, техник хангамжийн гарын авлага, компьютероос хэвлэсэн бичвэр болон график материалыг хураан авна.<br>7.12.9. Цахим төхөөрөмж, гар утасны нууц үгийг эд зүйлээ хураалгаж байгаа этгээд буюу өмчлөгч, эзэмшигчээр бичүүлж, эд зүйлийн хамт уут, саванд битүүмжилнэ.<br>7.12.11. Савлахын өмнө шошго тавьж, хоорондоо холбогдсон төхөөрөмжүүдийн холболтуудыг дараа нь угсарч ажиллуулах зорилгоор ойлгомжтой хэлбэрээр хаяглаж, үйл явцыг гэрэл зураг, дуу-дүрсний бичлэгээр бэхжүүлнэ. |

[110] Дээрх журмын 7.12.5 дахь хэсэг зааснаар “Тэмдэглэл”-д цахим төхөөрөмжийг хураан авах үед асаалттай, ажиллагаатай байсан эсэх, тухайн үед хэн, хэрхэн ашиглаж байсан талаарх мэдээллийг тусгана.

| | | |
|---|---|---|
| 6 | Хураан авсан цахим нотлох баримтыг хадгалах | Журам:<br>7.12.12. Соронзон орон бүхий цахилгаан үүсгэх боломжтой аливаа төхөөрөмж, материалаас хол, аюулгүй байдлын хамгаалалттай, температурын хяналт бүхий орчин, чийгшилгүй газарт, зориулалтын хамгаалалтын уут, эсхүл хайрцагт хадгална.<br>7.12.13. Цахим мэдээлэл хадгалах хэрэгслийн мэдээлэл устах, гэмтэхээс сэрэмжилж цахилгаан үүсгүүр, радио дамжуулагч зэрэг соронзон орчин үүсгэх, ердийн дулаанаас хэт өндөр температур, чийгшил, тоосжилт, доргилт ихтэй газарт хадгалахыг хориглоно. |

Монгол Улсын хувьд цахим нотлох баримт хураан авах, бэхжүүлэх, хадгалах, хамгаалах үйл ажиллагааны дараалал, аргачлалыг журамлахдаа цахим баримт хадгалагдаж буй төхөөрөмж бүрд ялгаатай байдлаар бус, нийтлэг байдлаар журамласан. Журмын 7.12-т цахим баримтын талаар дурдахдаа цахим төхөөрөмж, компьютер, гар утас, мэдээлэл хадгалах хэрэгсэл гэх нэр томьёо ашигласан байдаг. Иймд гар утасны төхөөрөмж, компьютер болон мультимедиа дахь цахим нотлох баримтуудтай ажиллах онцлог болон нэвтрүүлсэн сайн туршлагыг дараах дэд хэсгүүдэд авч үзсэн.

### 2.3.1. Гар утасны төхөөрөмжөөс нотлох баримт цуглуулах, бэхжүүлэх

Цахим нотлох баримтын шинжлэх ухааны байгууллага (*SWGDE*)[111]-аас Гар утасны төхөөрөмжөөс нотлох баримт олж авах, цуглуулах, хадгалах, харилцах шилдэг туршлагын талаарх баримт бичгийг 2020 оны 9 дүгээр сарын 17-ны өдөр нийтэлсэн.[112] Тус баримт бичигт зааснаар утасны төхөөрөмж (үүрэн холбооны утас, таблет, ухаалаг гар утас) гэдэгт угсармал системийн бүтэцтэй, боловсруулах чадвартай, утсан харилцаа тогтоох чадвартай, үндсэн санах ойтой зөөврийн төхөөрөмжүүдийг ойлгоно. Гар утасны төхөөрөмжийн үйлдлийн систем нь ямар программ хангамжид суурилснаас шалтгаалж нотлох баримт цуглуулах, бэхжүүлэх, олж авах ажиллагаа нь ялгаатай байх бөгөөд энэ хэсэгт сайн туршлагад дурдсан онцлог талуудыг судалсан болно. Үүнд:

1. Цахим нотлох баримт цуглуулах, бэхжүүлэх

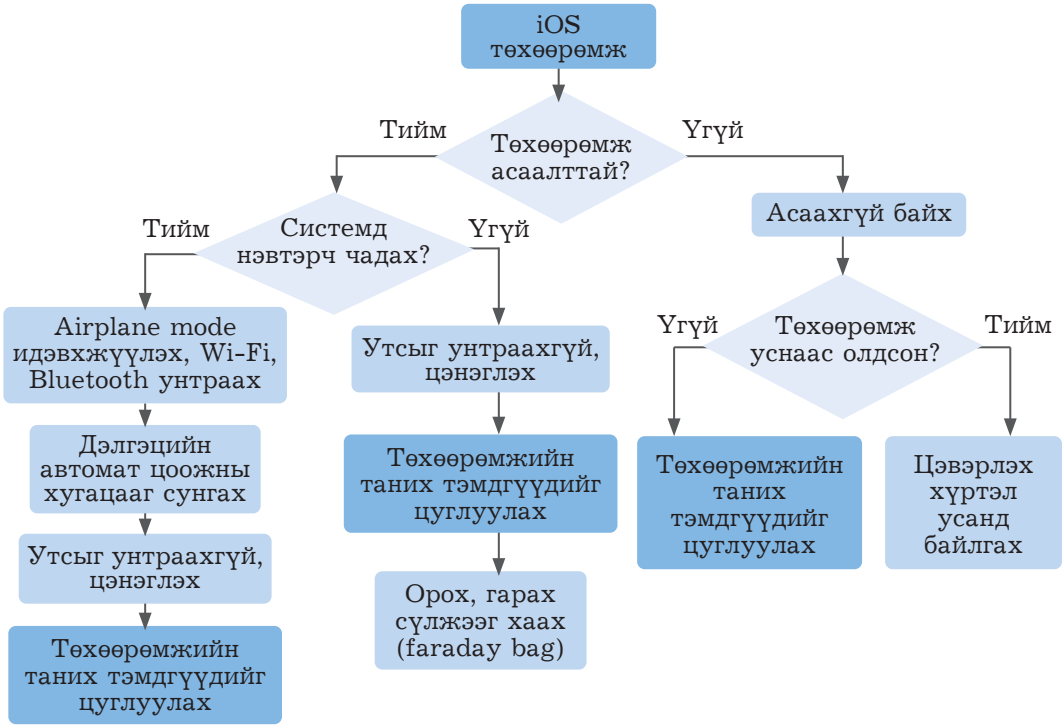
*iOS* нь *iPhone, iPad, iPod Touch* зэрэг гар утасны программ хангамжид зориулан *Apple* компаниас бүтээж, хөгжүүлсэн гар утасны үйлдлийн систем юм. *iOS* үйлдлийн системтэй төхөөрөмжөөс цахим нотлох баримт цуглуулахад дараах дараалал бүхий ажиллагааг гүйцэтгэж байна.

---

[111] Scientific Working Group on Digital Evidence гэх байгууллага нь тухайн салбарт ажилладаг байгууллагуудыг нэгтгэх, шүүх шинжилгээний чанарыг сайжруулах зорилготойгоор дижитал, мультимедиа нотлох баримтуудыг үнэлэх, шинжлэхэд шинжлэх ухааны үүднээс тайлбар хийж, зөвлөмж гаргадаг олон улсын байгууллага.

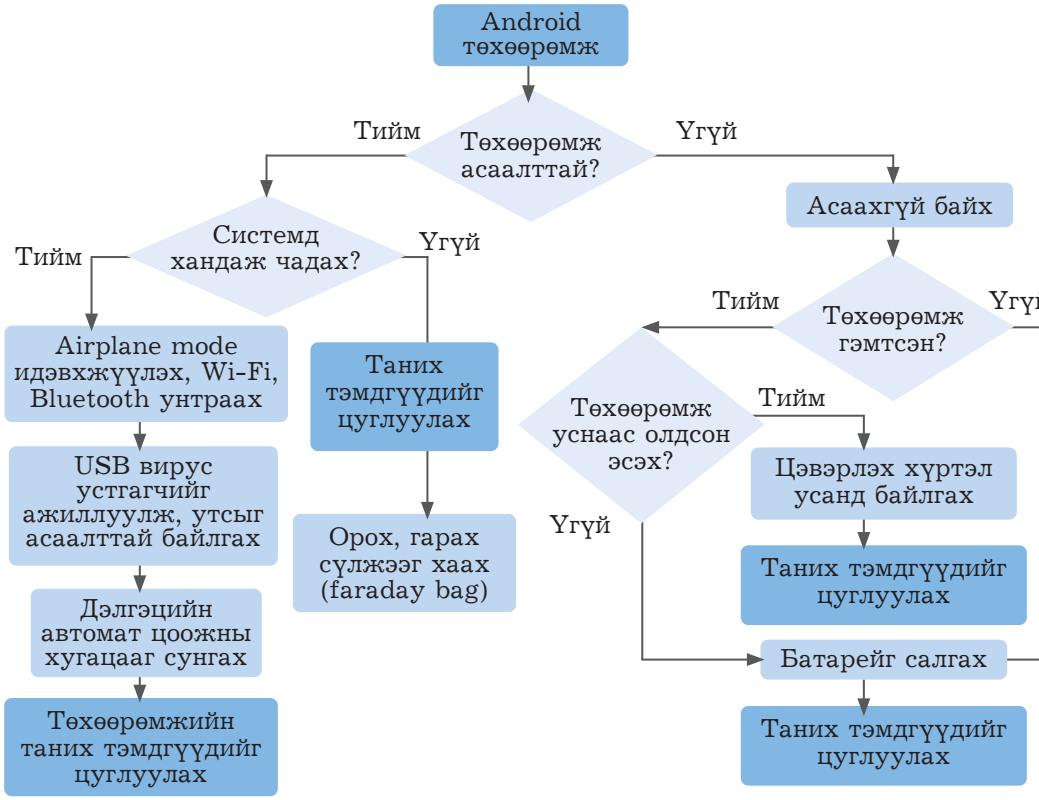
[112] https://athenaforensics.co.uk/wp-content/uploads/2019/01/SWGDE-Best-Practices-for-Mobile-Phone-Forensics-021113.pdf

*Зураг 1. iOS үйлдлийн системтэй төхөөрөмжөөс цахим нотлох баримт цуглуулах дараалал*




Андроид (*Android*) нь *Google*-ийн хөгжүүлсэн, линукс дээр суурилсан гар утасны үйлдлийн систем юм. Андроид олон төрлийн хувилбартай бөгөөд *iOS*-оос ялгаатай нь олон компанийн үйлдвэрлэсэн төхөөрөмж дээр санал болгодог учраас дараах дараалал бүхий ажиллагааг түгээмэл ашигладаг.

*Зураг 2. Андроид системтэй төхөөрөмжөөс нотлох баримт цуглуулах дараалал*




Гар утасны төхөөрөмж асаалттай тохиолдолд унтрааж болохгүй. Үйлдлийн системээс үл хамааран төхөөрөмж асаалттай үед хувирамтгай мэдээлэл[113] (нууцлалын түлхүүр гэх мэт) агуулж байж болзошгүй тул мэдээллийг хуулбарлаж дуусах хүртэл унтраахгүй байх зарчмыг дагаж мөрдөнө. Иймд төхөөрөмж унтрахаас урьдчилан сэргийлж, тэжээлийн эх үүсвэрийг нь аль болох хурдан залгах хэрэгтэй. Автомат түгжээ идэвхжихээс өмнө хугацааг нь уртасгахын тулд дэлгэцийн автомат түгжээний тохиргоог өөрчлөх шаардлагатай. Хэрэв төхөөрөмж цоожлогдоогүй бол мөрдөгч нь цоожлогдохоос сэргийлэхийн тулд цоожлох кодыг идэвхгүй болгох эсвэл мэдрэгчтэй дэлгэцтэй дахин дахин харьцах зэрэг үйлдэл хийх хэрэгтэй.

Утасны төхөөрөмжийг сүлжээнээс тусгаарлах ажиллагаа. Төхөөрөмжийг Нислэгийн горим (*Airplane mode*) дээр тохируулж, *WiFi* болон *Bluetooth* унтраалттай эсэхийг шалгана. Нислэгийн горим байхгүй бол сүлжээнээс хамаарч төхөөрөмж дэх мэдээллийг өөрчлөхөөс сэргийлж, төхөөрөмжид хадгалагдсан мэдээллийг устгах, өөрчлөх, нэмэх зэрэг гаднын нөлөөнөөс хамгаалах (*Faraday bag*) уутанд хийнэ. Төхөөрөмж унтарсан бол унтраалттай чигт нь хадгална.[114]

[113] volatile data.

[114] https://drive.google.com/file/d/1sVko_Uo7o6iootWwn9IoLJ3mrMVXqTDg/view

Дээр дурдсаны адил сүлжээний тусгаарлах ажиллагааг Интерполоос 2021 оны 3 дугаар сард гаргасан электроник болон цахим нотлох баримт эрэн хайх болон хураан авах ажиллагааны шилдэг туршлагад үндэслэсэн зөвлөмжид дараах байдлаар тусгажээ.[115] Тодруулбал, мэдээллийг алсаас өөрчилж, устгуулахгүйн тулд гар утсыг сүлжээнээс нь салгах шаардлагатай. Учир нь гар утасны төхөөрөмж хэрэглэгчийн бүх мэдээллийг устгаж, төхөөрөмжийн санах ойг анхны үйлдвэрийн төлөвт оруулан дахин тохируулах боломжтой. Энэ ажиллагааг биечлэн эсвэл алсаас хийх боломжтой тул нотлох баримт өөрчлөх, устгахгүй байхын тулд нэн даруй урьдчилан сэргийлэх арга хэмжээ авах (жишээлбэл, төхөөрөмжийг хэрэглэгчээс холдуулах, сүлжээнээс тусгаарлах г.м.) шаардлагатай.

Сүлжээнээс тусгаарлахын тулд төхөөрөмжийг унтраах нь хамгаалалтын механизм (жишээ нь, нууц үг, ПИН)-ыг, эсвэл аюулгүй байдлын функцүүдийг идэвхжүүлж, мэдээлэлд нэвтрэх боломжгүй болгох эрсдэлтэй.

Нөхцөл байдлыг баримтжуулах хүрээнд утасны төхөөрөмжтэй холбоотой дараах мэдээллийг судалж, дэлгэрэнгүй бүртгэл үйлдэнэ. Үүнд:

- Утасны төхөөрөмжийн байршил, төхөөрөмжийн төлөв (асаалттай, эсхүл унтраалттай, нууц код байгаа эсэх);
- Төхөөрөмж дээрх үйлдвэрлэгчийн мэдээлэл, гар утасны төхөөрөмжийн марк, загварын дугаар, Харилцаа холбооны хорооны таних дугаар (*FCCID*) болон тоног төхөөрөмжийн таних тэмдэг (Олон улсын хөдөлгөөнт төхөөрөмжийн тэмдэг (*IMEI*), Хөдөлгөөнт төхөөрөмжийн танигч (*MEID*), цахим серийн дугаар (*ESN*) зэрэг танин тодорхойлох бусад мэдээлэл байна.
- Утасны дагалдах хэрэгслүүдийг (кабель, цахилгаан холбогч, сольж, салгаж болох медиа, холбогддог зүйлсийг) зургаар баталгаажуулна. Утасны төхөөрөмж олдсон орчны зургийг авахдаа гар хүрэх, бохирдуулахаас зайлсхийнэ.

### 2.3.2. Компьютероос нотлох баримт цуглуулах, бэхжүүлэх

Интерполоос[116] 2021 оны 3 дугаар сард нийтэлсэн цахим нотлох баримт эрэн хайх, хураан авах ажиллагааны сайн туршлагад үндэслэсэн зөвлөмжид суурин болон зөөврийн компьютероос цахим нотлох баримт цуглуулах, бэхжүүлэх ажиллагааг тухайлсан процедураар гүйцэтгэхээр заасан.

Хамгийн эхний алхам бол компьютер асаалттай эсэхийг тогтооно. Ихэнх суурин компьютер дэлгэц унтарсан хэдий ч асаалттай цахилгаан хэмнэх (*power-saving mode*), эсхүл амрах горим (*state of sleep*)-д шилжсэн байдаг. Иймд дээрх горимд байгаа компьютерыг шууд унтраах товч, эсхүл дахин

[115] https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

[116] https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

тохируулах (*reset*) товч, *Enter* дарахгүйгээр эхлээд хулганыг хөдөлгөх, доош нь гүйлгэх, эсхүл *shift*_товч дарна.

Хэрэв компьютер асаалттай, ажиллагаатай бол дэлгэцийн зураг, огноо, цаг, цагийн бүс, идэвхтэй дүрс, хэрэглэгчийн хийж буй үйлдэл, процесс, программын үйл ажиллагааны үзүүлэлт зэргийг баримтжуулна. Аливаа хортой программ ажиллаж байгаа нь ажиглагдвал цахилгаанаас салгах, өөр бусад сүлжээ, кабель, утасгүй сүлжээнд холбогдсон эсэхийг шалгана. Сүлжээний өөр компьютер дээр хуваалцсан фолдеруудтай холбогдож, шифрлэлт ашиглаж байгаа эсэхийг хайж, тэдгээрийн шинж чанарыг шалгахаас гадна *Dropbox, Google Drive, OneDrive* гэх мэт үүлэн хадгалах сан, веб шуудангийн хуудас, сошиал зэрэг хөтчүүдийн үйл ажиллагааг шалгана.

Хэрэв компьютер унтраалттай бол унтарсан байгааг баримтжуулж, цахилгаан тэжээлээс салгана. Хатуу дискээс гадна бусад санд мэдээлэл хадгалагддаг эсэхийг шууд шалган тогтоох боломжгүй бол компьютерыг бүхэлд нь хураан авна.

### 2.3.3. Виртуал хөрөнгийн төхөөрөмжөөс нотлох баримт цуглуулах, бэхжүүлэх[117]

Эхний хүлээн авагч[118] нь виртуал хөрөнгөд хандах, хадгалах, шилжүүлэх янз бүрийн аргуудыг мэддэг байх ёстой. Криптовалютыг зохих ёсоор хураан авахыг зөвшөөрөхийн тулд холбогдох хууль тогтоомжоор болон шүүхийн, эсхүл бусад (прокурорын) зөвшөөрөл авсан бол хууль сахиулах байгууллага сэжигтний хэтэвчнээс хураан авсан хөрөнгийг агентлагийн хяналтад байдаг албан бөгөөд хамгаалалттай хэтэвч рүү шилжүүлнэ. Хяналтад байдаггүй хэтэвч рүү мөнгө шилжүүлэхэд мэдээллийн хуулбар хамсаатан этгээдэд байж болзошгүй гэдгийг хууль сахиулах байгууллагынхан үргэлж санаж байх хэрэгтэй.

Виртуал хөрөнгийн хэтэвчүүд янз бүрийн хэлбэр, дүрстэй байдаг бөгөөд мөрдөн шалгах ажиллагааны нэгжлэгийн үеэр дараах төрлийн крипто хэтэвчүүд байх боломжтой:

- Дэлгэцийн хэтэвч (*Desktop wallets): Bitcoin Core, Armory, Electrum, Wasabi, Bither* гэх мэт.
- Гар утасны хэтэвч (*Mobile wallets): Mycelium, Edge, BRD, Trust* гэх мэт.
- Онлайн хэтэвч (*Online wallets): BitGo, BTC.com, Coin.Space, Blockchain.com* гэх мэт.
- Техник хангамжийн хэтэвч (*Hardware wallets): BitBox, Coldcard, KeepKey, Ledger, Trezor* гэх мэт.

---

[117] https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf

[118] Нотлох баримтыг хамгийн түрүүнд олсон, танилцаж буй этгээд.

- Цаасан хэтэвч (*Paper wallets*): *bitaddress.org, segwitaddress.org*-аас үүсгэсэн хаягууд гэх мэт.
- Брэйн хэтэвч *(Brain wallets*): Хэтэвчийн хувийн түлхүүр болон хэтэвчийг эргэн сэргээхэд шаардлагатай бүх мэдээллийг цээжилдэг хэтэвчийн төрөл юм.

Хэтэвчийн төрлөөс үл хамааран нотлох баримтын эхний хүлээн авагчдын хамгийн түрүүнд нэвтрэх ёстой чухал мэдээлэл бол шифрлэгдээгүй хувийн түлхүүр *(unencrypted private key*) бөгөөд энэ нь гүйлгээ хийх, мөнгө шилжүүлэх боломж олгодог. Ихэнх тохиолдолд хувийн түлхүүр хамгаалагдсан, эсвэл хадгалагдаагүй байж болно. Тиймээс дараах зүйлсийг эрэлхийлэх ёстой:

- Нууц үг: хувийн түлхүүрийг шифрлэхэд ашигладаг;
- ПИН: техник хангамжийн түрийвч, эсвэл утас руу нэвтрэх код;
- Итгэмжлэл: онлайн хэтэвчийн хэрэглэгчийн нэр, нууц үг;
- *QR* кодууд: эдгээр нь хувийн түлхүүрийг бүрэн хадгалах боломжтой;
- *Seeds*: хувийн түлхүүрийг сэргээхэд ашигладаг үгсийн дараалал (ихэвчлэн 24 ба түүнээс дээш).

Хамгийн алдартай криптовалют болох биткоины хувьд хувийн түлхүүрүүд 256 битийн тоо (*bit number*)-той байдаг бөгөөд тэдгээрийг олон янзаар илэрхийлж болно. Хэтэвч импортлох формат (*WIF*) нь хамгийн түгээмэл төрөл бөгөөд түлхүүр нь '5', 'K' эсвэл 'L' үсгээр эхэлдэг. Шифрлэгдсэн хувийн түлхүүр нь '6P'-ээр эхэлдэг. Жишээлбэл, ижил хувийн түлхүүрийг дараах байдлаар илэрхийлж болно:

- *Base58 Wallet Import Format* (51 тэмдэгт base 58, '5'-ээр эхэлдэг):

· *5JoBSup7GzCohqzfCdU3FQmuQM8KLCu3TTKiTAtbzmWywJfzTni*

- *Base58 Wallet Import Format Prepressed (base58,* 'K', эсвэл 'L' үсгээр эхэлдэг 52 тэмдэгт):

· *L1Yq7N6vhZV79HFVcKxLvbwCJ3qHumWhqmBbxWemTyVLJHfaUjTc*

- *Private Key BIP38 Encrypted Format* (58 тэмдэгт base58, '6P'-ээр эхэлдэг) - нууц үг: 'asdfg':

· *6PYLTEjqt2huN6zgG8Gc2Sdifh33tcDLoJMXXqdK52YrQWXa3fD8az9Za7*

### 2.3.4. Мультимедиа нотлох баримт цуглуулах, бэхжүүлэх

Дижитал нотлох баримтын шинжлэх ухааны байгууллага (*SWGDE*)-аас 2020 оны 9 дүгээр сарын 17-ны өдөр Мультимедиа нотлох баримтыг бэхжүүлэх, шүүхэд гаргаж, танилцуулах практик асуудлын талаар зөвлөмж (Зөвлөмж)[119] гаргасан.

Мультимедиа нотлох баримтыг шүүхийн үйл ажиллагаанд түгээмэл хэрэглэж, хэргийн үйл баримтыг тодорхойлох, хэрэг хянан шийдвэрлэх

[119] https://drive.google.com/file/d/151-yKO_9ZIzpwRgO2CAADsXHMCatKItC/view

ажиллагаанд чухал нөлөө үзүүлэх нотлох баримтын хэлбэр гэж үзэн, шүүхийн үйл ажиллагаанд оролцогчдод мультимедиа нотлох баримтыг оновчтой хэлбэрээр гаргаж өгөх зааварчилгаа, практик зөвлөмж хүргэх зорилгоор тус Зөвлөмжийг нийтэлсэн. Зөвлөмжид шүүх хуралдаанаас өмнө шүүхийн ажилтнууд болон өмгөөлөгчид зөвлөлдсөний үндсэн дээр шүүх танхимд байгаа төхөөрөмж дээр тухайн мультимедиа нотлох баримтыг танилцуулж, туршихын ач холбогдлыг тусгасан. Иймд Зөвлөмжид зааснаар мультимедиа нотлох баримт цуглуулах, бэхжүүлэх ажиллагаа хэрхэн хийгдэхийг Монгол Улсын ЭХХШтХ-д заасантай харьцуулан дараах байдлаар тайлбарлалаа.

“Цахим нотлох баримт” гэдэгт дуу, бичлэг, зураг болон дижитал, эсвэл аналоги форматтай мета өгөгдөл зэргийг хамааруулсан бөгөөд дараах эх сурвалжаас үүсэж болохоор тодорхойлсон. Үүнд:

- Байгууллагын үүсгэсэн эсвэл хадгалсан мультимедиа (ярилцлага, хяналтын камерын болон машины камерын бичлэг, хувцсанд зүүсэн камер, хэргийн газрын бичлэг гэх мэт);
- Гуравдагч этгээдээс ирүүлсэн болон олж авсан мультимедиа (олон нийтийн мэдээллийн хэрэгсэл, видео бичлэгийн төхөөрөмжөөр хийгдсэн бичлэг, гар утас, дрон, *CCTV* камерын бичлэг, зүйлсийн интернэт (*Internet of Things*[120]) гэх мэт).

Технологи, түүний шинж чанарын талаарх мэдлэг дутуугаас түүнийг устгах, буруугаар ашиглах, эсхүл техникийн доголдолтой нотлох баримтыг ойлгохгүйн улмаас хүлээн зөвшөөрөх зэрэг тохиолдол гардаг. Гэвч нотлох баримтыг шүүх хүлээн зөвшөөрөхдөө дараах хууль ёсны, урьдчилсан нөхцөлийг хангасан байхыг шаардана. Үүнд:

- Хамаарал бүхий байх;
- Нотлох баримтыг зохих ёсоор баталгаажуулсан байх;
- Нотлох баримт нь бусдын тайлбар, мэдүүлэгт тулгуурласан бол хүлээн зөвшөөрөгдөх боломжтой байх;
- Нотлох баримт эх хувиар, эсхүл түүнийг хууль ёсоор хуулбарласан хуулбар хувь байх;
- Нотлох баримтыг шударга бусаар олж авсан, асуудлыг будилаантуулах, тангарагтны шүүгчдийг төөрөгдүүлэх болон үндэслэлгүйгээр хугацаа хойшлуулах, цаг үрэх зорилгогүй байх;
- Ямар нэгэн засвар, өөрчлөлт хийх шаардлагагүй байх.

ЭХХШтХ-ийн 16.1 дүгээр зүйлийн 6-д “Нотлох баримтыг хууль бус арга, хэрэгслээр цуглуулж, бэхжүүлэхийг хориглоно” гэж, мөн хуулийн 16.11, 16.12 дугаар зүйлд нотлох баримтаар тооцохгүй байх тохиолдлуудыг хуульчилсан. Шүүхэд ирүүлж буй файлын төрөл нь эх төхөөрөмж дээр бичигдсэн байдлаас өөр байх нь мультимедиа нотлох баримтыг хүлээн зөвшөөрөх эсэхэд эргэлзээ төрүүлж, маргаан үүсгэдэг.

[120] Программ хангамж болон технологийн бусад объектыг интернэт болон холбооны сүлжээгээр дамжуулан бусад төхөөрөмж, системтэй холбож, мэдээлэл солилцдог зүйлс.

1001. (d) цахим хэлбэрээр хадгалагдсан мэдээллийн эх хувьд үнэн зөв мэдээлэл агуулж байгаа аливаа хэвлэмэл материал, нүдээр уншигдах боломжтой бусад материал хамаарна.

1001. (e) хуулбар нь механик, гэрэл зураг, химийн, электрон, бусад ижил төстэй аргаар бий болгох замаар эх хувийг үнэн зөв хуулбарласан хоёр дахь хувь байж болно.

1003. Эх хувь нь баталгаатай эсэх талаар асуулт гараагүй, эсвэл хуулбарыг хүлээн зөвшөөрөх нь шударга бус нөхцөл байдал үүсгэж болзошгүйгээс бусад тохиолдолд эх хувьтай ижил хуулбарыг хүлээн зөвшөөрнө.

Нөгөөтээгүүр эх хувь нь байхгүй болсон, эсвэл шүүхэд танилцуулах боломжгүй (эх хувийг тоглуулах боломжгүй болсон зэрэг) тохиолдолд хуулбарыг зөвшөөрдөг. Хэрэв мультимедиаг эх хувилбараас өөр хэлбэрээр шүүхэд ирүүлэх тохиолдолд урьдчилан шүүхийн мэргэжилтэн, гэрч, эсрэг талын өмгөөлөгч нараар хянуулж, баталгаажуулсан байх шаардлагатай. Улмаар уг хуулбар нь эх хувьтайгаа нийцэж буй эсэхийг гэрчлүүлэх, хуулбар нь ямар нэгэн өөрчлөлтгүй, засвар ороогүй, устгагдаагүй болохыг нотлуулахын тулд цахим нотлох баримт олж авсан, баталгаажуулж, бэхжүүлсэн мэргэжилтнийг шүүхэд дуудаж, хуулбарлаж авсан алхам бүрийг нь тайлбарлуулж болохоор заасан.

Монгол Улсын хувьд ЭХХШтХ-ийн 16.1 дүгээр зүйлийн 4-т “Мөрдөгч энэ хуульд заасан үндэслэл, журмын дагуу нотлох баримт цуглуулж, шалгаж, бэхжүүлнэ” гэж заасны дагуу мөрдөгч нотлох баримтыг бэхжүүлэх ажиллагааг гүйцэтгэнэ.

Мультимедиа нотлох баримт танилцуулахад биет төхөөрөмж (нэг удаагийн зөөвөрлөгч, *USB* флаш, зөөврийн хатуу диск гэх мэт) дээр татан авсан баримт ашиглах боломжтой. Тухайн төхөөрөмжөөс нотлох баримтыг шинжлэн судлах үед гарах алдааг багасгахын тулд мультимедиа нотлох баримт тоглуулах хэрэгслийг оновчтой сонгож, тасалдахаас нь сэргийлэх хэрэгтэй. Хэрэв алдаа гарвал шүүхээс болон эсрэг талын өмгөөлөгчөөс нотлох баримтыг өөр төхөөрөмжөөс (зөөвөрлөгчөөс бус компьютер дээр хадгалагдсан файлаас) түр тоглуулах зөвшөөрөл хүсэх боломжтой.

Нотлох баримтын тухай Холбооны дүрмийн 1006-д шүүх тэр дор нь шалгах боломжгүй их хэмжээний бичвэр, бичлэг, гэрэл зургийн хувьд нотолж чадахуйц хураангуй, график, тооцоолол ашиглахыг зөвшөөрдөг. Мөн өмгөөлөгч, мэргэжилтэн нь шаардлагатай тохиолдолд шүүхийн шийдвэрт нийцүүлэхийн тулд мультимедиагийн форматыг өөрчлөх, засварлахад бэлэн байх хэрэгтэй.

Нотлох баримтаар цуглуулсан гэрэл зураг, видео бичлэгийг бэхжүүлж, тэдгээрийг шүүхэд үзүүлэхэд шаардлагатай бүх тоног төхөөрөмж, программ хангамж бэлэн, зөв тохиргоотой, зөв суурилагдсан эсэхийг сайтар шалгаж, шүүх хуралдааны танхимд урьдчилан туршиж үзэх шаардлагатай. Үүнд дараах хүчин зүйлсийг тооцох бөгөөд тэдгээр нь зөвхөн доор дурдсан үзүүлэлтүүдээр хязгаарлагдахгүй:

- Системийн тохиргоо;
- Зургийн чанар;
- Дуу авианы гаралт;
- Дэлгэцийн хэмжээ ба чанар;
- Проекторын чанар (гэрлийн хэмжээ, дохионы хэлбэр);
- Проекторын тохиргоо (өнгө ялгаралт, цагаан өнгөний тэнцвэр);
- Тохиромжтой аудио, видео кабель, адаптер, дохио хөрвүүлэгч (*HDMI* холболт, *HDMI* хөрвүүлэгч);
- Өрөөний гэрэлтүүлэг;
- Дэлгэцийн өнцөг болон үзэгчид хүртэлх зай.

Аудио нотлох баримтад утасны ярианы бичлэг, дуудлагын бичлэг, хяналтын бичлэг, цагдан хоригдож буй сэжигтнүүдийн ярилцлага зэрэг хамаарна. Аудио бичлэгийг тоглуулах тоног төхөөрөмж нь аудио нотлох баримтын форматыг дэмждэг байх, хурлын өмнө бичлэгийг туршиж үзсэн байх хэрэгтэй. Мөн шүүгчид, шүүхийн ажилтнууд, шүүх хурлын оролцогчдод зориулсан чанар сайтай чихэвч байх, чихэвч байхгүй тохиолдолд сонсогчдод зориулсан чанарын өндөр үзүүлэлттэй дуу өсгөгч ашиглах нь зүйтэй. Компьютер, телевизийн спикер, хөгжим гэх мэт чанарын шаардлага хангахгүй тоглуулагчаар аудио бичлэг тоглуулахаас зайлсхийх шаардлагатай.

# ГУРАВ. ОЛОН УЛС ДАХЬ КИБЕР ГЭМТ ХЭРГИЙН ЗОХИЦУУЛАЛТ, ВИРТУАЛ ХӨРӨНГИЙН БИРЖҮҮДЭД ХИЙГДСЭН КИБЕР ХАЛДЛАГА, ТЭДГЭЭРИЙГ ШИЙДВЭРЛЭЖ БУЙ ПРАКТИК

Монгол Улсын Эрүүгийн хуулиар зохицуулсан кибер гэмт хэргийн зохицуулалтыг Япон, БНСУ, Хонконг, Сингапур, Швейцар, АНУ, БНЭУ, ОХУ-ын эрх зүйн зохицуулалттай харьцуулан судалсан болно. Хууль зүйн харьцуулалтыг дараах агуулгын хүрээнд хийсэн. Үүнд:

1. Кибер гэмт хэргийг хуульчилсан байдал;
2. Кибер орчинд хууль бусаар халдах гэмт хэргийн зохицуулалт;
3. Виртуал хөрөнгийн биржүүдэд хийгдсэн кибер халдлага, тэдгээрийг шийдвэрлэж буй байдал.

Мөн Монгол Улсын Эрүүгийн хуулиар зохицуулсан кибер гэмт хэргийн зохицуулалтаас гадна Кибер гэмт хэргийн олон улсын конвенцоор тодорхойлсон кибер гэмт хэргийн төрлүүдийг хуульчилсан байдлыг харьцуулан авч үзлээ.

### 3.1. Кибер гэмт хэргийг хуульчилсан байдал

Кибер гэмт хэрэг, түүний төрлүүдийг Монгол Улсын Эрүүгийн хуулиар тодорхойлсон бөгөөд тусгайлсан хууль тогтоомжоор тус гэмт хэргийг зохицуулдаггүй. Үүний нэгэн адил Швейцар[121], АНУ[122], ОХУ[123], БНЭУ[124] нь Эрүүгийн хуулиар, эсхүл Гэмт хэргийн тухай хуулиар кибер гэмт хэргийг зохицуулж байна. Харин Япон Улс, БНСУ, Сингапур, Хонконг нь Эрүүгийн хуулиас гадна кибер гэмт хэргийг зохицуулдаг тусгайлсан хууль тогтоомжтой. Үүнд:

- Япон Улс - Эрүүгийн хуулиас[125] гадна Хууль бус хандалтыг хориглох тухай хууль[126];
- БНСУ - Эрүүгийн хуулиас[127] гадна Мэдээллийн харилцаа холбооны сүлжээ ашиглалтыг дэмжих, мэдээллийн аюулгүй байдлыг хангах

[121] https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en

[122] United States Code. Title 18. https://uscode.house.gov/browse/prelim@title1/chapter3&edition=prelim

[123] http://www.consultant.ru/document/cons_doc_LAW_10699/

[124] https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/510052022003/consolide

[125] https://elaws.e-gov.go.jp/document?lawid=140AC0000000045&keyword=%E5%88%91%E6%B3%95

[126] https://elaws.egov.go.jp/document?lawid=411AC0000000128_20150801_000000000000000&keyword=%E4%B8%8D%E6%AD%A3%E3%82%A2%E3%82%AF%E3%82%BB%E3%82%B9

[127] 전기통신금융사기피해방지및피해금환급에관한특별법 (law.go.kr)

тухай хууль[128], Санхүүгийн цахим гүйлгээний тухай хууль[129];

- Сингапур - Компьютерыг урвуулан ашиглах тухай хууль[130];
- Хонконг - Гэмт хэргийн тухай хууль[131], Харилцаа холбооны тухай хууль.[132]

Улс орнуудын эрх зүйн тогтолцооны онцлог, кибер гэмт хэрэгтэй тэмцэх үндэсний бодлого зэрэг хүчин зүйлээс шалтгаалан Эрүүгийн хуулиас гадна тусгайлсан хуульд кибер гэмт хэргийг тодорхойлж, зохицуулж байна. Монгол Улсын Эрүүгийн хуулийн 2.1 дүгээр зүйлийн 1 дэх хэсэгт заасны дагуу зөвхөн Эрүүгийн хуульд заасан нийгэмд аюултай гэм буруутай үйлдэл, эс үйлдэхүйг гэмт хэрэгт тооцдог тул тусгайлсан хуулиар аливаа гэмт хэргийн төрлийг зохицуулдаггүй болно.

Дээрхээс гадна кибер гэмт хэргийн дөрвөн төрлийг тодорхойлсон Будапештийн конвенцод АНУ, Япон, Швейцар, ОХУ, БНЭУ нэгдэн орсон бол Монгол Улс болон Хонконг, Сингапур, БНСУ нэгдэн ороогүй. Будапештийн конвенцоор тодорхойлсон кибер гэмт хэргийн төрлийг дээрх улсууд дараах байдлаар хууль тогтоомждоо тусгажээ. Үүнд:

*Хүснэгт 22. Компьютерын өгөгдөл, системийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлын эсрэг гэмт хэргийн зохицуулалтын харьцуулалт*

| | |
|---|---|
| Монгол Улс | Эрүүгийн хуулийн:<br>26.1 дүгээр зүйл. Кибер орчинд хууль бусаар халдах<br>26.2. дугаар зүйл. Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах гэмт хэрэг нь тухайн бүлэгт хамаарна. |
| Япон Улс | Эрүүгийн хуулийн:<br>168.2. Хууль бусаар электрон, эсхүл цахилгаан соронзон бүртгэл ашиглах, үүсгэх, бэлтгэх<br>168.3. Электрон, эсхүл цахилгаан соронзон бүртгэлийн удирдлагыг хууль бусаар эзэмших<br>Хууль бус хандалтыг хориглох тухай хуулийн:<br>3 дугаар зүйл. Компьютерт зөвшөөрөлгүй нэвтрэх үйлдлийг хориглох<br>4 дүгээр зүйл. Бусдын таних кодыг хууль бусаар олж авахыг хориглох<br>5 дугаар зүйл. Компьютерын зөвшөөрөлгүй хандалтыг дэмжсэн үйлдлийг хориглох<br>6 дугаар зүйл. Бусдын таних кодыг хууль бусаар хадгалахыг хориглох |

[128] https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%EB%B0%8F%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0

[129] https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%84%EC%9E%90%EA%B8%88%EC%9C%B5%EA%B1%B0%EB%9E%98%EB%B2%9

[130] Computer Misuse Act. 1993, https://sso.agc.gov.sg/Act/CMA1993?ProvIds=P12-#pr3-

[131] Crimes Ordinance (Cap. 200), https://www.elegislation.gov.hk/hk/cap200

[132] Telecommunications Ordinance (Cap.106), https://www.elegislation.gov.hk/hk/cap106

| | |
|---|---|
| АНУ | АНУ-ын Холбооны хуулийн 18-р хэсэг, §1030. Компьютерын залилан ба компьютерыг урвуулан ашиглах тухай хуулийн (а):<br>(1) Засгийн газрын цахим орчинд халдах<br>(2) Санхүүгийн байгууллага, АНУ-ын агентлаг, хамгаалагдсан бусад компьютерын мэдээлэлд зөвшөөрөлгүй халдах<br>(3) Компьютерт гэмтэл учруулах<br>(4) Залилан мэхлэх үйлдлээ гүйцэлдүүлэх, үнэ цэн бүхий зүйл олж авах зорилгоор компьютерт нэвтрэх<br>(5) Компьютерын программ, мэдээлэл, кодыг санаатайгаар дамжуулах<br>(6) Компьютерын нэвтрэх нууц үг, түүнтэй адилтгах компьютерт нэвтрэх мэдээллийг худалдах |
| Сингапур | Компьютерыг урвуулан ашиглах тухай хуулийн:<br>3 дугаар зүйл. Компьютерын материалд зөвшөөрөлгүйгээр нэвтрэх.<br>4 дүгээр зүйл. Гэмт хэрэг үйлдэх, үйлдэхэд туслах зорилгоор компьютерт нэвтрэх<br>5 дугаар зүйл. Компьютерын материалыг зөвшөөрөлгүйгээр өөрчлөх<br>6 дугаар зүйл. Компьютерын үйлчилгээг зөвшөөрөлгүйгээр ашиглах, үйлчилгээг зогсоох<br>7 дугаар зүйл. Компьютерыг ашиглахад саад учруулах<br>8 дугаар зүйл. Хандалтын кодыг зөвшөөрөлгүйгээр задруулах |
| Хонконг | Гэмт хэргийн тухай хуулийн:<br>161 дүгээр зүйл. “Гэмт хэргийн болон залилан мэхлэх зорилгоор компьютерт нэвтрэх”<br>Харилцаа холбооны тухай хуулийн:<br>27А хэсэг. “Харилцаа холбооны хэрэгсэл ашиглан компьютерт зөвшөөрөлгүй нэвтрэх” талаар зохицуулсан ба аливаа этгээд харилцаа холбооны хэрэгсэл ашиглан, мэдсээр байж, зөвшөөрөлгүйгээр компьютерт хадгалагдаж буй аливаа программ хангамж, өгөгдлийг олж авахын тулд түүнд хандсан тохиолдолд 4-р түвшний торгууль[133] ногдуулна. |
| БНСУ | Мэдээлэл, харилцаа холбооны сүлжээ ашиглалтыг дэмжих, мэдээллийн аюулгүй байдлыг хангах тухай хуулийн:[134]<br>48 дугаар зүйлийн 1 дэх хэсэгт “*зүй ёсны нэвтрэх эрхгүй, эсхүл зөвшөөрөгдсөн эрхээ хэтрүүлж мэдээлэл, харилцаа холбооны сүлжээнд халдах*” үйлдлийг хориглосон бөгөөд зөрчсөн тохиолдолд “*таван жил хүртэл хорих, эсхүл тавин сая вон хүртэл торгох*” ял ногдуулна. |
| Швейцар | Эрүүгийн хуулийн:<br>143[bis178] дугаар зүйл. Зөвшөөрөлгүйгээр мэдээллийн өгөгдөл олж авах, мэдээлэл дамжуулах системд зөвшөөрөлгүйгээр нэвтрэх<br>144[bis] дүгээр зүйл. Мэдээллийн өгөгдлийг гэмтээх |

[133] Эрүүгийн процессын хууль (Cap 221)-ийн 8-р хэсэгт зааснаар 25,000 ам. доллартой тэнцэх хэмжээ.

[134] 정보통신망 이용촉진 및 정보보호 등에 관한 법률. 2001년.

*Хүснэгт 22-ын үргэлжлэл*

| | |
|---|---|
| БНЭУ | Гэмт хэргийн тухай хуулийн:<br>206 дугаар зүйл. Компьютерын мэдээлэлд халдах<br>207 дугаар зүйл. Компьютерын системийн үйл ажиллагаанд саад учруулах |
| ОХУ | Эрүүгийн хуулийн:<br>272 дугаар зүйл. Компьютерын мэдээлэлд хууль бусаар халдах.<br>273. Компьютерын хортой программ хангамж зохион бүтээх, ашиглах болон түгээх<br>274. Мэдээлэл хадгалах, боловсруулах хэрэгслийн ашиглалт болон компьютерын мэдээлэл, мэдээлэл, харилцаа холбооны сүлжээний дамжуулалтын журам зөрчих<br>274.1. ОХУ-ын мэдээллийн чухал дэд бүтцэд хууль бусаар нөлөөлөх<br>274.2. ОХУ-ын нутаг дэвсгэрт мэдээлэл, харилцаа холбооны сүлжээ Интернэт болон нийтийн хэрэглээний холбооны сүлжээний тогтвортой, бүрэн бүтэн, аюулгүй байдалд заналхийлж буй үйлдэлтэй тэмцэх техник хэрэгслийн төвлөрсөн удирдлагын дүрэм зөрчих |

*Хүснэгт 23. Компьютер ашиглаж үйлддэг гэмт хэргүүдийн зохицуулалтын харьцуулалт*

| | **Компьютер ашиглаж үйлддэг гэмт хэргүүд** |
|---|---|
| Монгол Улс | Эрүүгийн хуулийн:<br>13.10. Хувь хүний нууцад халдах гэмт хэргийг,<br>13.11. Хувь хүний нууцыг задруулах гэмт хэргийг тус тус “***харилцаа холбоо, цахим хэрэгсэл***” ашиглаж үйлдсэн,<br>17.3 зүйлийн 1 дэх хэсэг. Залилах гэмт хэргийг “***цахим хэрэгсэл ашиглаж үйлдсэн***” тохиолдолд хамаарна. |
| Япон Улс | Эрүүгийн хуулийн:<br>246.2. Компьютер ашиглаж хийсэн залилан |
| АНУ | АНУ-ын хуулийн 18-р хэсэг, §1030. Компьютерын залилан ба компьютерыг урвуулан ашиглах тухай хуулийн (а)-д<br>(7) Мөнгө, үнэ бүхий бусад зүйл олж авах зорилгоор хамгаалагдсан компьютерын мэдээллийн нууцлалыг алдагдуулахаар сүрдүүлэх, компьютерт хохирол, гэмтэл учруулахаар сүрдүүлэх |
| Сингапур | Компьютерыг урвуулан ашиглах тухай хуулийн:<br>9 дүгээр зүйл. Хууль зөрчиж олж авсан хувийн мэдээллийг хадгалах, дамжуулах, санал болгох, ашиглах<br>10 дугаар зүйл. Гэмт хэрэгт ашиглах эд зүйл олж авах |
| Хонконг | Гэмт хэргийн тухай хуулийн:<br>60 дугаар зүйлд “Хөрөнгө устгах, гэмтээх” гэж,<br>62 дугаар зүйлд “Хөрөнгө устгах, гэмтээх зорилгоор аливаа зүйлийг эзэмших” гэмт хэргийг хуульчилсан. Мөн хуулийн 59.(1А)-д зааснаар “хөрөнгө устгах, гэмтээх” гэдэгт компьютерыг урвуулан ашиглах буюу хууль бусаар ашиглаж, компьютерын үйлдлийн системд нөлөөлж компьютер, түүнд хадгалагдаж буй өгөгдөл, программыг устгах, өөрчлөх, суулгах зэргийг ойлгохоор заасан. |

| | |
|---|---|
| БНСУ | Эрүүгийн хуулийн:<br>347-2 дугаар зүйл. Компьютер ашиглан залилан үйлдэх[135]<br>Санхүүгийн цахим гүйлгээний тухай хуулийн:<br>49 дүгээр зүйлийн 1.7. Мэдээлэл, харилцаа холбооны сүлжээ ашиглан, өөр цахим дэлгүүрийн нэрээр цахим гүйлгээ хийх<br>49 дүгээр зүйлийн 1.9. Мэдээлэл, харилцааны холбооны сүлжээ ашиглан, цахим дэлгүүр биш этгээд цахим дэлгүүрийн нэрээр цахим мөнгөний гүйлгээ хийх тохиолдол<br>Мэдээлэл, харилцаа холбооны сүлжээ ашиглалтыг дэмжих, мэдээллийн аюулгүй байдлыг хангах тухай хуулийн:<br>74 дүгээр зүйлийн 1.1. Мэдээлэл, харилцааны холбооны сүлжээний баталгааг зөрчих |
| Швейцар | Эрүүгийн хуулийн:<br>147 дугаар зүйл. Компьютерын залилан<br>217 дугаар зүйл. Компьютерын систем хууль бусаар ашиглах |
| БНЭУ | Гэмт хэргийн тухай хуулийн:<br>208 дугаар зүйл. Тагнуулын программ, хортой программ, эсвэл компьютерын вирус тараах<br>$216^{1}$ дугаар зүйл. Компьютертэй холбоотой гэмт хэрэгт бэлтгэх гэмт хэрэг. Энэ зүйлийн 1 дэх хэсэгт:<br>217 дугаар зүйл. Компьютерын системийг хууль бусаар ашиглах гэмт хэрэг. |
| ОХУ | Эрүүгийн хуулийн:<br>159.6. Компьютерын мэдээллийн залилан<br>158 дугаар зүйл. Бусдын эд хөрөнгө хулгайлах (Цахим төлбөр тооцооны системд байгаа мөнгөн хөрөнгө хулгайлах) |

*Хүснэгт 24. Контент агуулгатай холбоотой гэмт хэргийн харьцуулалт*

| | Контент агуулгатай холбоотой гэмт хэргүүд |
|---|---|
| Монгол Улс | Эрүүгийн хуулийн 16.9-д заасан Хүүхэд оролцуулж садар самууныг сурталчлах гэмт хэргийг “***кибер орчныг ашиглаж***” үйлдсэн бол хамаарна. |
| Япон Улс | Эрүүгийн хуулийн 175. Садар самуун материал тараах |
| АНУ | Зохицуулаагүй. |
| Сингапур | Зохицуулаагүй. |
| Хонконг | Зохицуулаагүй. |

[135] https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%ED%98%95%EB%B2%95

| | |
|---|---|
| БНСУ | Мэдээлэл, харилцаа холбооны сүлжээ ашиглалтыг дэмжих, мэдээллийн аюулгүй байдлыг хангах тухай хуулийн:<br>44-7 дугаар зүйлийн 1 дэх хэсэгт порнограф, гүтгэсэн, айдас төрүүлсэн, насанд хүрээгүй хүүхдэд хор хүргэх мэдээллийг мэдээлэл, харилцаа холбооны сүлжээ ашиглан түгээхийг хориглон, зөрчсөн тохиолдолд хүлээлгэх хариуцлагыг мөн хуулийн 70.1.2, 74.1.2, 74.1.3-т, Насанд хүрээгүй хүүхдийг хамгаалах хуульд тус тус заасан байна.[136] |
| ОХУ | Эрүүгийн хуулийн:<br>137 дугаар зүйл. Хувийн халдашгүй байдлыг зөрчих. Интернэт сүлжээгээгээр дамжуулан 16 насанд хүрээгүй хохирогчийн хувийн халдашгүй байдлыг зөрчих<br>242 дугаар зүйл. Порнограф материал болон бусад хэрэгслийг хууль бусаар бэлтгэх<br>282 дугаар зүйл. Хүний нэр төр, алдар хүндийг унагаах |

Зохиогчийн эрх, түүнд хамаарах бусад эрхийг зөрчсөнтэй холбоотой гэмт хэргүүдийн тухайд харьцуулан судалсан улс орнуудад оюуны өмчийн гэмт хэргийг зохицуулсан хэдий ч кибер орчинд, цахим сүлжээнд тараасан, түгээсэн нөхцөлийг тодотгон тайлбарлаагүй, хүндрүүлэх бүрэлдэхүүнд мөн хамааруулаагүй байна.

Харин АНУ-ын Холбооны хуулийн 18-р хэсэг, §1030 (a)(2)-т заасан “хамгаалагдсан бусад компьютерын мэдээлэл”-д зохиогчийн эрхийн хуулиар хамгаалагдсан мэдээллүүдийг хамааруулдаг. Тухайлбал, компьютерын программ хангамжийг зохиогчийн эрхээр бүртгүүлсэн бөгөөд компьютерын мэдээлэлд халдан тухайн программын мэдээллийг авсан бол энэ нь хамгаалагдсан бусад компьютерын мэдээлэл гэх хуулийн зохицуулалтад хамаарна. Мөн АНУ-ын Холбооны хуулийн 18 дугаар хэсэг, §2319. Зохиогчийн эрхийг зөрчсөн гэмт хэргүүдийг хуульчилсан. Үйлдлийн шинж чанар, зохиогчийн эрхийн үнэ цэнээс хамаарч торгох, 1-10 жил хүртэл хугацаагаар хорих ял шийтгэхээр байна. Үүний нэгэн адил БНЭУ-ын Гэмт хэргийн тухай хуульд дараах байдлаар тусгажээ.❑[1]

*Хүснэгт 25. БНЭУ-ын Гэмт хэргийн тухай хууль*

**❑[1] дүгээр зүйл.**
Хууль бусаар хуулбарласан компьютерын программ эзэмших гэмт хэргийг заасан бөгөөд тухайн зүйлийн 1 дэх хэсэгт: “Компьютерын программыг арилжааны зорилгоор хууль бусаар биечлэн ашигласан, эзэмшсэн бол торгууль ногдуулах, эсхүл 3 жил хүртэл хугацаагаар хорих ял шийтгэнэ.

[135] https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EC%A0%95%EB%B3%B4%ED%86%B5%EC%8B%A0%EB%A7%9D%EC%9D%B4%EC%9A%A9%EC%B4%89%EC%A7%84%EB%B0%8F%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%93%B1%EC%97%90%EA%B4%80%ED%95%9C%EB%B2%95%EB%A5%A0

### 3.2. Кибер орчинд хууль бусаар халдах гэмт хэргийн зохицуулалтын харьцуулалт

Судалгаагаар виртуал хөрөнгийн биржийн үйл ажиллагаанд эрсдэл учруулах, биржийн үйл ажиллагааг доголдолд оруулж, хэрэглэгчид их хэмжээний хохирол учруулж буй кибер гэмт хэрэг болох “кибер орчинд хууль бусаар халдах гэмт хэрэг”-ийг улс орнуудад хэрхэн зохицуулж байгааг дараах байдлаар харьцуулан судаллаа. Үүнд:

*Хүснэгт 26. Кибер орчинд хууль бусаар халдах гэмт хэргийн харьцуулалт*

| Улс | Кибер орчинд хууль бусаар халдах гэмт хэрэг | Гэмт хэргийн үндсэн бүрэлдэхүүн | Эрүүгийн хариуцлага |
|---|---|---|---|
| Монгол Улс | Эрүүгийн хуулийн 26.1 дүгээр зүйл. Кибер орчинд хууль бусаар халдах | 1. Кибер орчинд зөвшөөрөлгүйгээр хандаж мэдээллийн систем, мэдээллийн сүлжээнд нэвтэрсэн, танилцсан бол | 2,700 нэгжээс 10,000 нэгжтэй тэнцэх хэмжээний төгрөгөөр торгох, эсхүл 6 сараас 2 жил хүртэл хугацаагаар зорчих эрхийг хязгаарлах, эсхүл 6 сараас 2 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |
| | | 2. Кибер орчинд хууль бусаар халдаж мэдээллийг устгасан, гэмтээсэн, өөрчилсөн, засварласан, нуусан, нэмж оруулсан, хуулбарлаж авсан, ашиглах боломжгүй болгосон бол | 5,400 нэгжээс 27,000 нэгжтэй тэнцэх хэмжээний төгрөгөөр торгох, эсхүл 1 жилээс 5 жил хүртэл хугацаагаар зорчих эрхийг хязгаарлах, эсхүл 1 жилээс 5 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |
| | | 3. Кибер орчинд хууль бусаар халдаж мэдээллийн систем, мэдээллийн сүлжээг ашиглах боломжгүй болгосон, хэвийн үйл ажиллагааг алдагдуулсан, хандалтад хязгаарлалт тогтоосон, ноцтой саад учруулсан бол | 2 жилээс 5 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |
| Япон Улс | Хууль бус хандалтыг хориглох тухай хууль (ХБХХтХ)-ийн 3 дугаар зүйл. Компьютерт зөвшөөрөлгүй нэвтрэх үйлдлийг хориглох | Аливаа этгээд зөвшөөрөлгүйгээр компьютерт нэвтрэх үйлдэл хийхийг хориглоно. | 3 жил хүртэл хугацаагаар хорих ял, эсхүл 1 сая хүртэлх иенээр торгох ял шийтгэнэ. |
| | ХБХХтХ-ийн 4 дүгээр зүйл. Бусдын таних кодыг хууль бусаар олж авахыг хориглох | Аливаа этгээд компьютерт зөвшөөрөлгүйгээр нэвтрэх үйлдэл хийх зорилгоор хандалтын хяналтын чиг үүрэгтэй холбоотой өөр хүний таних кодыг авахыг хориглоно. | 1 жил хүртэл хугацаагаар хорих ял, эсхүл 500 мянга хүртэлх иенээр торгох ял шийтгэнэ. |
| | ХБХХтХ-ийн 5 дугаар зүйл. Компьютерын зөвшөөрөлгүй хандалтыг дэмжсэн үйлдлийг хориглох | Аливаа этгээд ажил мэргэжлийн болон бусад үндэслэлтэй шалтгаанаас бусад тохиолдолд хандалтын хяналтын чиг үүрэгт хамаарах хандалтын администратор болон таних кодтой холбоотой тусгай зөвшөөрөл эзэмшигчээс бусад этгээдэд хандалтын хяналтын чиг үүрэг бүхий өөр этгээдийн таних кодыг өгөхийг хориглоно. | 1 жил хүртэл хугацаагаар хорих ял, эсхүл 500 мянга хүртэлх иенээр торгох ял шийтгэнэ. |

| | | | |
|---|---|---|---|
| АНУ | Компьютерын залилан ба компьютерыг урвуулан ашиглах тухай хууль §1030 (a) | (1) Компьютерт зөвшөөрөлгүйгээр, эсхүл олгосон зөвшөөрлийг хэтрүүлэн нэвтэрч, АНУ-ын Засгийн газраас хамгаалах шаардлагатай гэж үзсэн, гадаад харилцаа, үндэсний аюулгүй байдал, хязгаарлагдмал бүс нутагт хамаарах мэдээллийг олж авсан, тэдгээр мэдээллийг АНУ-д хохирол учруулах, аль нэг гадаад улсын ашиг тусын тулд дамжуулсан, дамжуулахыг оролдсон | торгох,[137] 10 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |
| | | (2) Компьютерт зөвшөөрөлгүйгээр, эсхүл олгосон зөвшөөрлийг хэтрүүлэн нэвтэрч дараах мэдээллийг олж авсан:<br>(A) санхүүгийн байгууллага, карт гаргагч, тэдгээрийн хэрэглэгчийн мэдээлэл;<br>(B) АНУ-ын агентлаг, тэдгээрийн хэлтсийн мэдээлэл; эсхүл<br>(C) хамгаалагдсан бусад компьютерын мэдээллийг олж авсан; | торгох, 1 жил хүртэл хугацаагаар хорих ял, энэ хэргийн улмаас эдийн засгийн хувьд давуу тал, ашиг олсон бол 5 жил хүртэлх хорих ял шийтгэнэ. |
| | | (3) АНУ-ын агентлаг, тэдгээрийн хэлтсийн дотоод үйл ажиллагаанд ашигладаг, нийтийн бус компьютерт зөвшөөрөлгүйгээр хандсан | торгох, 1 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |
| | | (4) Санаатайгаар, зөвшөөрөлгүй, эсхүл олгосон зөвшөөрлийг хэтрүүлэн залилан мэхлэх үйлдлээ гүйцэлдүүлэх, үнэ цэн бүхий зүйл олж авах зорилгоор компьютерт нэвтэрсэн. Энэ тохиолдолд халдлагын зүйл нь зөвхөн компьютер биш бөгөөд 1 жилийн хугацаанд 5,000 ам. доллар хүртэлх үнэ цэн бүхий зүйлс байна. | торгох, 5 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |
| | | (5)(A) программ, мэдээлэл, код, командыг санаатайгаар дамжуулсны улмаас хамгаалагдсан компьютерт гэмт учруулсан<br>(B) хамгаалагдсан компьютерт санаатайгаар, зөвшөөрөлгүйгээр нэвтэрсний улмаас болгоомжгүйгээр хохирол учруулсан<br>(C) хамгаалагдсан компьютерт санаатайгаар, зөвшөөрөлгүйгээр нэвтэрсний улмаас алдагдал, хохирол, учруулсан | торгох, 10 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |

[137] АНУ-ын Холбооны хуулийн 18-р хэсэг, 3571-д зааснаар торгох ялын дэд хэмжээ нь хувь хүн 250,000 ам. доллар, хуулийн этгээд 500,000 ам. доллар, эсхүл гэмт хэргийн улмаас олсон ашиг, шүүгдэгчээс бусдад учруулсан хохирлыг 2 дахин нэмэгдүүлсэнтэй тэнцэх хэмжээтэй байна. https://uscode.house.gov/browse/prelim@title18/part1&edition=prelim

| | | | |
|---|---|---|---|
| Сингапур | Компьютерыг урвуулан ашиглах тухай хууль (КУАтХ)-ийн 3 дугаар зүйл. Компьютерын материалд зөвшөөрөлгүйгээр нэвтрэх | Аливаа этгээд компьютерт хадгалагдаж буй өгөгдөл, программд зөвшөөрөлгүй хандаж, компьютер ямар нэгэн үйлдэл гүйцэтгэхэд хүргэсэн; | 5,000 хүртэл ам. долларoор торгох, 2 жил хүртэлх хугацаагаар хорих ял шийтгэнэ. Энэ хэргийг давтан үйлдсэн бол 10,000 хүртэл ам. долларoор торгох, 3 жил хүртэлх хугацаагаар хорих ял шийтгэнэ. |
| | КУАтХ-ийн 4 дүгээр зүйл. Гэмт хэрэг үйлдэх, үйлдэхэд туслах зорилгоор компьютерт нэвтрэх | Гэмт хэрэг үйлдэх, үйлдэхэд туслах зорилгоор компьютерт нэвтрэх үйлдэл хийсэн гэм буруутай;<br>4.(2) Тухайн этгээдийн үйлдэл нь эд хөрөнгө, залилан мэхлэх, хууль бус үйлдэл хийх, бусдын бие махбодод гэмтэл учруулах зорилготой, ийм төрлийн гэмт хэрэгт хамаарах бол 2 жил хүртэлх хугацаагаар хорих ял шийтгэнэ. | 50,000 хүртэл ам. долларoор торгох, 10 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |
| | КУАтХ-ийн 5 дугаар зүйл. Компьютерын материалыг зөвшөөрөлгүйгээр өөрчлөх | Тухайн үйлдэл нь аливаа компьютерын контентыг зөвшөөрөлгүй өөрчлөхөд хүргэж байгааг мэдсээр байж хийсэн. Энэ гэмт хэргийг үйлдэхэд халдсан программ, эсхүл өгөгдлийн төрөл, хэлбэр, байнгын, эсхүл түр хугацаанд халдах зорилготой байсан эсэх нь чухал биш юм. | 10,000 хүртэл ам. долларoор торгох, 3 жил хүртэл хугацаагаар хорих ялаар, гэмт хэргийг давтан үйлдсэн бол 20,000 хүртэл ам. долларoор торгох, 5 жил хүртэл хугацаагаар хорих ялаар, гэмт хэргийн улмаас хохирол учирсан бол 50,000 хүртэл ам. долларoор торгох, 7 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |
| | КУАтХ-ийн 6 дугаар зүйл. Компьютерын үйлчилгээг зөвшөөрөлгүйгээр ашиглах, үйлчилгээг зогсоох | Аливаа этгээд санаатайгаар компьютерын үйлчилгээг шууд болон шууд бусаар авах зорилгоор компьютерт зөвшөөрөлгүй нэвтрэх эрх олж авсан, цахилгаан соронзон, акустик, механик болон бусад төхөөрөмжөөр компьютерын аливаа үйл ажиллагааг шууд болон шууд бусаар таслан зогсоох, таслан зогсооход хүргэх, эсхүл дээр заасан гэмт хэрэг үйлдэх зорилгоор компьютер, эсхүл бусад төхөөрөмжийг ашигласан, ашиглах шалтгаан болсон бол гэмт хэрэг үйлдсэн гэм буруутайд тооцно. | |
| | КУАтХ-ийн 7 дугаар зүйл. Компьютерыг ашиглахад саад учруулах | Эрх олгогдоогүй аливаа этгээд зөвшөөрөлгүйгээр, санаатайгаар компьютерыг зохих ёсоор ашиглахад саад учруулах, тасалдуулах, компьютерт хадгалагдсан аливаа программ хангамж, өгөгдөлд нэвтрэхэд саад учруулах, үр нөлөө, ашиг тусыг бууруулах аливаа үйлдэл хийсэн бол гэмт хэрэг үйлдсэн гэм буруутайд тооцно. | |

| | | | |
|---|---|---|---|
| Хонконг | Гэмт хэргийн тухай хуулийн 161 дүгээр зүйл. Гэмт хэргийн болон залилан мэхлэх зорилгоор компьютерт нэвтрэх | гэмт хэрэг үйлдэх, хууран мэхлэх, эсхүл өөртөө болон бусдад ашиг олох, бусдад санаатайгаар хохирол учруулах зорилгоор компьютерт нэвтрэх эрх олж авсан, ирээдүйд олж авахаар үйлдэл хийсэн бол | 5 жилийн хорих ял шийтгэнэ. |
| БНСУ | Мэдээлэл, харилцаа холбооны сүлжээ ашиглалтыг дэмжих, мэдээллийн аюулгүй байдлыг хангах тухай хуулийн 48 дугаар зүйлийн 1. Мэдээлэл, харилцаа холбооны сүлжээнд халдах | Хууль ёсны нэвтрэх эрхгүй, эсхүл зөвшөөрөгдсөн эрхээ хэтрүүлж мэдээлэл, харилцаа холбооны сүлжээнд халдах үйлдлийг хориглоно. | 5 жил хүртэл хугацаагаар хорих, эсхүл 50 сая хүртэл воноор торгох ял шийтгэнэ. |
| Швейцар | Эрүүгийн хуулийн 143[bis178] дугаар зүйл. Зөвшөөрөлгүйгээр мэдээлэл олж авах, мэдээлэл дамжуулах системд зөвшөөрөлгүйгээр нэвтрэх | Нэвтрэхээс урьдчилан сэргийлэхийн тулд тусгайлан хамгаалагдсан өгөгдөл боловсруулах системд өгөгдөл дамжуулах төхөөрөмжөөр зөвшөөрөлгүй нэвтэрсэн бол | 3 жилээс илүүгүй хугацаагаар хорих, эсхүл торгох ял шийтгэнэ. |
| | Эрүүгийн хуулийн 144[bis] дүгээр зүйл. Мэдээллийн өгөгдлийг гэмтээх | Зөвшөөрөл олгогдоогүй аливаа этгээд нь цахим хэлбэрээр, эсвэл үүнтэй төстэй хэлбэрээр хадгалагдаж, дамжуулагдсан өгөгдлийг өөрчилсөн, устгасан, ашиглах боломжгүй болгосон бол | 3 жилээс илүүгүй хугацаагаар хорих, эсвэл торгох ял шийтгэнэ. |
| БНЭУ | Гэмт хэргийн тухай хуулийн 206 дугаар зүйл. Компьютерын мэдээлэлд халдах | Компьютерын систем дэх өгөгдөл, программыг хууль бусаар өөрчилсөн, устгасан, гэмтээсэн, блоклосон, компьютерын системд өгөгдөл, программ хууль бусаар байршуулсан | торгууль ногдуулах, эсхүл 3 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |
| | Гэмт хэргийн тухай хуулийн 207 дугаар зүйл. Компьютерын системийн үйл ажиллагаанд саад учруулах | Мэдээлэл байршуулах, дамжуулах, устгах, гэмтээх, өөрчлөх, блоклох замаар компьютерын системийн үйл ажиллагаанд хууль бусаар хөндлөнгөөс оролцсон, саад учруулсан бол | торгууль ногдуулах, эсхүл 3 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |
| | Гэмт хэргийн тухай хуулийн 217 дугаар зүйл. Компьютерын системийг хууль бусаар ашиглах | Код, нууц үг болон хамгаалалтын бусад арга хэмжээг устгах, тойрч гарах замаар компьютерын системд хууль бусаар нэвтэрсэн бол | торгууль ногдуулах, эсхүл 3 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |

| | | | |
|---|---|---|---|
| ОХУ | Эрүүгийн хуулийн 272 дугаар зүйл. Компьютерын мэдээлэлд хууль бусаар халдах. | Компьютерын мэдээллийг устгах, нэвтрэх эрхэд хаалт хийх, өөрчлөх, мэдээллийг хуулбарлаж, хуулиар хамгаалагдсан компьютерын мэдээлэлд хууль бусаар хандсан бол | 200,000 хүртэл рублиэр, эсхүл 18 сар хүртэл хугацааны цалин, түүнтэй адилтгах бусад орлогын мөнгөн дүнгээр торгох, эсхүл 1 жил хүртэл хугацаагаар засан хүмүүжүүлэх тусгай хөдөлмөр эрхлүүлэх, 2 жил хүртэл хугацаагаар эрх чөлөөг хязгаарлах, эсхүл 2 жил хүртэл хугацаагаар албадан хөдөлмөр эрхлүүлэх, эсхүл тухайн хугацаагаар хорих ял шийтгэнэ. |
| | Эрүүгийн хуулийн 274 дүгээр зүйл. Мэдээллийг хадгалах, боловсруулах хэрэгслийн ашиглалт болон компьютерын мэдээлэл, мэдээлэл, харилцаа холбооны сүлжээний дамжуулалтын журам зөрчих | Мэдээлэл хадгалах, боловсруулах хэрэгслийн ашиглалтын журам, эсхүл хамгаалагдсан компьютерын мэдээлэл, мэдээлэл, харилцаа холбооны сүлжээ, түүний ороолт, гаралтын төхөөрөмж дамжуулах журам зөрчиж, их хэмжээний хохирол учруулахуйц компьютерын мэдээллийг хуулбарлах, өөрчлөх, нэвтрэх эрхийг хаах, устгах үр дагавар үүсгэх мэдээллийн харилцаа холбооны сүлжээнд нэвтрэх журам зөрчсөн бол | 500,000 рубль хүртэл, эсхүл 18 сар хүртэл хугацааны цалин, түүнтэй адилтгах бусад орлогын мөнгөн дүнгээр торгох, эсхүл 6 сараас 1 жил хүртэл хугацаагаар засан хүмүүжүүлэх тусгай хөдөлмөр эрхлүүлэх, эсхүл 2 жил хүртэл хугацаагаар эрх чөлөөг хязгаарлах, 2 жил хүртэл хугацаагаар албадан хөдөлмөр эрхлүүлэх, эсхүл тухайн хугацаагаар хорих ял шийтгэнэ. |
| | Эрүүгийн хуулийн 274.1. ОХУ-ын мэдээллийн чухал дэд бүтцэд хууль бусаар нөлөөлөх | ОХУ-ын мэдээллийн чухал дэд бүтцэд хууль бусаар нөлөөлөхийн тулд тухайн мэдээллийг устгах, нэвтрэх эрхэд хаалт хийх, өөрчлөх, хуулбарлах, эсхүл мэдээллийг хамгаалах хэрэгсэлд саад учруулах зорилгоор компьютерын программ, эсхүл компьютерын бусад мэдээлэл зохион бүтээх, тараах, ашиглах үйлдэл хийсэн бол | 2 жил хүртэл хугацаагаар эрх чөлөөг хязгаарлаж (хязгаарлахгүйгээр) 5 жил хүртэл хугацаагаар албадан хөдөлмөрлүүлэх, эсхүл 500,000 рубль, эсхүл 1-3 жил хүртэл хугацааны цалин, түүнд хамаарах бусад орлоготой дүйцэхүйц мөнгөн дүнгээр торгож, 2-5 жил хүртэл хугацаагаар хорих ял шийтгэнэ. |

### 3.3. Виртуал хөрөнгийн биржүүдэд хийгдсэн кибер халдлага, тэдгээрийг шийдвэрлэж буй байдал

Дэлхийн 45 улсын ВХҮҮ, төвлөрсөн бус санхүүгийн платформуудад 2011-2021 онд гарсан кибер аюулгүй байдлын зөрчил болон луйврын нийт 364 тохиолдлоос аюулгүй байдал зөрчигдсөн тохиолдол 290 буюу 79.7 хувийг эзэлж байна.[138]

Судлахаар сонгож авсан улс орнуудын виртуал хөрөнгийн биржүүдэд хийсэн цахим халдлагын төрлүүдийг судалж үзвэл "кибер орчинд хууль бусаар халдах" гэмт хэргийн шинжтэй дараах халдлага үйлдэгдэж, зарим нь шийдвэрлэгджээ. Үүнд:

[138] https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/ Сүүлд хандсан огноо: 2022.08.13.

*Хүснэгт 27. Виртуал хөрөнгийн биржүүдэд хийгдсэн цахим халдлага*

| Улс | Бирж | Огноо[139] | Хэмжээ[140] | Кибер халдлагын төрөл | Шийдвэрлэгдсэн байдал |
|---|---|---|---|---|---|
| Япон Улс | *Mt. Gox* | 2011-2014 | 230,928,049 ам.доллар | Ажилтны компьютерыг хакердаж, системд хууль бусаар нэвтэрч үйлдсэн. | Халдлага үйлдсэн этгээдийг 2020 онд луйвар, мөнгө угаах, хуйвалдаан явуулах болон автомат дата ашиглан системд халдсан үргэлжилсэн үйлдлээр нь буруутгаж Францад ялласан. Харин Бирж дампуурлаа зарлаж, эзэн нь баривчлагдсан. |
| | *Coin-check* | 2018 | 487,387,361 ам.доллар | Ажилтнуудын дотоод сүлжээнд холбогдсон хувийн компьютерт нэвтрэн, хортой программ тарааж үйлдсэн. | Бирж хэрэглэгчдэд хохирлыг нь нөхөн төлөхөө мэдэгдсэн. Харин Биржийг хэрэглэгчдийн виртуал хөрөнгийг найдвартай хадгалах үүргээ зөрчсөн буруутай гэж маргасан ч Дээд шүүхээс уг нэхэмжлэлийг хэрэгсэхгүй болгож шийдвэрлэсэн. Хоёр сэжигтэн илрүүлсэн ба хэтэвчийг царцаах шийдвэр гаргаж, Зохион байгуулалттай гэмт хэргийн ял шийтгэлийн тухай хууль зөрчсөн гэж буруутгасан. |

[139] Анхны халдлага хийсэн болон халдлага үргэлжилсэн хугацаа.
[140] Кибер халдлагын улмаас алдагдсан виртуал хөрөнгийн тухайн үеийн үнэ цэн.

| | | | | | |
|---|---|---|---|---|---|
| Сингапур | *KuCoin* | 2020 | 150,000,000 ам. доллар | *DeFi* протоколууд буюу смарт гэрээгээр баталгаажуулсан блокчейн дээр суурилсан төвлөрсөн бус программууд (*dApps*) ашигласан. | Хулгайлагдсан коинуудын ихэнхийг нь олж авсан ба үлдсэн хэсгийг нь даатгалаас нөхөн төлж, хэрэглэгчдийг хохиролгүй болгосон. |
| | *Exodus & BRD* | 2021 | 7,089,000 ам. доллар | Интернэтэд холбогдсон *hot* хэтэвчнээс виртуал хөрөнгө хулгайлсан. | Халдлага үйлдсэн этгээд тодорхойгүй ч Бүгд Найрамдах Сингапур Улсын шүүхээс дэлхий даяар хөрөнгө битүүмжлэх шийдвэр гаргаж, биржүүдийг нэхэмжлэгчийн хэтэвчээр шилжүүлсэн гүйлгээнүүдэд холбогдох мэдээллийг ил болгох шийдвэр гаргасан. |
| Хонконг | *Bitfinex* | 2016 | 72,200,000 ам. доллар | Хэтэвчүүдийг хакердаж, криптовалютыг хууль бусаар авсан | Халдлага үйлдсэн этгээдүүдийг санхүүгийн хууль бус гүйлгээ хийх, мөнгө угаах гэмт хэрэг бүлэглэн үйлдсэн гэмт хэрэгт ялласан. Шүүх хурал үргэлжилж байгаа. |
| АНУ | *Binance Gemini Poloniex Bittrex* | 2017 | 16,876,000 ам. доллар | Хуурамч веб сайтын тусламжтайгаар хэрэглэгчдийн мэйл хаяг, нууц үгийг олж аван, хэтэвчнээс хөрөнгийг нь хулгайлсан. | Халдлага үйлдсэн этгээдүүдийг санаатайгаар, хуйвалдан Компьютерын залилан ба урвуулан ашиглах хуулийн хэд хэдэн зүйл, заалт зөрчсөн үндэслэлээр ял шийтгэсэн. |

| | | | | | |
|---|---|---|---|---|---|
| БНСУ | Coinrail | 2018 | 383,570,341 вон | Серверийн аюулгүй байдалд халдаж үйлдсэн. | Шүүхээс биржийг үүргээ зөрчсөн гэж үзэж, хохирлыг нөхөн төлүүлэхээр шийдвэрлэсэн. |
| БНЭУ | *TAYLOR* | 2018 | 1,350,000 ам. доллар | Нэг хэтэвч дэх олон эх үүсвэрээс цуглуулж, хууль бусаар авсан | Биржээс хэрэглэгчдээдээ нөхцөл байдлыг даван туулах аян өрнүүлсэн. |
| Швейцар | *Bancor* | 2018 | 23,500,000 ам. доллар | Ухаалаг гэрээг шинэчлэх зориулалттай хэтэвчнээс криптовалютыг хууль бусаар авсан | Шүүхээр шийдвэрлэгдээгүй бөгөөд хэрэглэгчийн хэтэвчид халдаагүй гэж мэдэгдсэн |
| ОХУ | *Live coin* | 2020 | Тодорхой болоогүй, | Биржийн системд халдаж, криптовалютын ханшийг өөрчилсөн. | Шүүхээр шийдвэрлээгүй бөгөөд хэрэглэгчийн хохирлыг Биржээс төлөх ажил зохион байгуулсан. |

Дээр дурдсан кибер халдлагууд, тэдгээрийг шийдвэрлэж буй арга зам, кибер аюулгүй байдлыг хангах ажлын хүрээнд авч буй арга хэмжээг улс орон тус бүрээр нарийвчлан судалсан болно.

### 3.3.1. Япон Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн жишээ

Япон Улс кибер аюулгүй байдлын харилцааг Кибер аюулгүй байдлын суурь хуулиар зохицуулж байна. Тус хууль нь 2014 оны 11 дүгээр сарын 6-ны өдөр батлагдаж, 11 дүгээр сарын 12-ны өдрөөс үйлчилсэн.

Кибер аюулгүй байдлын суурь хуулийн 2 дугаар зүйлд “кибер аюулгүй байдал” гэдгийг электрон, эсхүл цахилгаан соронзонд үүсгэгдсэн мэдээллийг хадгалах мэдээллийн хэрэгсэл, эсхүл мэдээллийн сүлжээгээр дамжуулан электрон компьютер руу чиглэсэн зөвшөөрөлгүй үйл ажиллагаанаас урьдчилан сэргийлэх, мэдээлэл болон харилцаа холбооны сүлжээ, мэдээллийн сүлжээний найдвартай бөгөөд аюулгүй байдлыг хангах, электрон, цахилгаан соронзонд, эсхүл хүний үйл ажиллагаагаар таних боломжгүй бусад төрлийн хэлбэрээр хүлээн авсан, шилжүүлсэн, илгээсэн, эсхүл хадгалсан мэдээлэл устах, алга болох, гэмтэх, нууцлал алдагдахын эрэг, түүнээс урьдчилан сэргийлэх зэргээр мэдээллийг аюулгүй удирдахад

хэрэгжүүлэх шаардлагатай арга хэмжээ, тэдгээрийн найдвартай байдлыг зохих ёсоор хангах болон удирдах”[141] гэж тодорхойлсон байна.

Эдгээр зорилгод хүрэхийн тулд дээрх хуулиар Япон Улсын Засгийн газар, нутгийн удирдлагын байгууллагууд, чухал мэдээллийг хангаж буй дэд бүтцийн 14 салбарын үйлчилгээ эрхлэгч, кибертэй холбоотой бизнес эрхлэгчид, боловсролын болон судалгааны байгууллагуудад тухайлсан үүрэг хүлээлгэсэн.[142]

Энэхүү судалгаагаар Япон Улсын *Mt. Gox, Coincheck* криптобиржүүдэд гарсан кибер халдлага, тэдгээрийг шийдвэрлэсэн байдлыг судалж үзлээ. Халдлага үйлдсэн этгээдүүдийг олж тогтоон, баривчилсан бөгөөд *Mt. Gox* биржид халдлага үйлдсэн этгээд Франц Улсын иргэншилтэй байсан. Япон Улсын дүүргийн шүүхээс түүнийг гэмт хэрэг үйлдсэн гэж үзсэн хэдий ч 2020 оны 1 дүгээр сарын 24-ний өдөр Франц Улс шилжүүлэн авч, луйвар, мөнгө угаах, хуйвалдаан явуулах болон автомат дата ашиглан системд халдсан үргэлжилсэн үйлдлээр нь буруутгаж ялласан. Харин *Coincheck* биржид халдлага үйлдсэн этгээдүүдийг Зохион байгуулалттай гэмт хэргийн ял шийтгэлийн тухай хууль зөрчсөн гэх үндэслэлээр буруутгаж, сэжигтнүүдийн хэтэвчийг царцаах шийдвэрийг Токио хотын шүүх гаргасан байна (Биржүүдэд үйлдэгдсэн халдлагын үйл баримт, шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалтын дэлгэрэнгүйг Хавсралт 1-ээс үзнэ үү).

Дээрх биржийн халдлагын дараа Япон Улсын Санхүүгийн үйлчилгээний агентлагаас биржид газар дээр нь шалгалт хийж, криптовалютын биржийн үйлчилгээ үзүүлэгчид өөрсдийнхөө эрсдэлийн удирдлагын системийн талаарх тайланг Санхүүгийн үйлчилгээний агентлагт хүргүүлж байх шийдвэр гаргасан.

### 3.3.2. Бүгд Найрамдах Сингапур Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн жишээ

Сингапурын хууль сахиулах байгууллага болон хууль тогтоомжийн зохицуулалтын гол чиглэл нь компьютерын тусламжтайгаар үйлдэгдсэн гэмт хэрэг болон контентын гэмт хэрэг байдаг. Компьютерын тусламжтайгаар үйлдэгдэх гэмт хэрэгт хувийн мэдээллийн хулгай, залилан, онлайн мөрийтэй тоглоом зэрэг гэмт хэрэг хамаардаг бол контентын гэмт хэрэгт онлайн орчинд бусдыг доромжлох, үзэн ядах зэрэг хэрэг багтдаг.

Кибер гэмт хэргийн шинжтэй дээрх үйлдлүүдийг Эрүүгийн хууль, Алсын зайн мөрийтэй тоглоомын тухай хууль зэрэг дотоодын хууль тогтоомжоор зохицуулдаг ч үндсэн зохицуулалт нь Компьютерын зүй бус хэрэглээ ба кибер аюулгүй байдлын тухай хууль (*Computer Misuse and Cybersecurity*

[141] サイバーセキュリティ基本法、平成二十六年十一月十二日、第2条（定義）、(https://bit.ly/30mUAvG)

[142] Japan’s National Cybersecurity and Defense Posture, Policy and Organization. Cyber defense Report, September 2020, p.4. (https://bit.ly/3zLRtsX)

*Act*) юм.[143] Сингапур Улсын Кибер аюулгүй байдлын тухай хуулийг[144] 2018 оны 2 дугаар сарын 5-ны өдөр парламент баталж, 2018 оны 3 дугаар сарын 2-ны өдөр Ерөнхийлөгч нь зөвшөөрсөн байдаг.

Кибер аюулгүй байдлын тухай хуулийн 2 дугаар хэсэгт тодорхойлсноор "кибер аюулгүй байдал" гэж компьютер, эсхүл компьютерын систем зөвшөөрөлгүй хандалт, халдлагаас хамгаалагдсан дараах төлөвт байхыг хэлнэ. Үүнд:

a. компьютер, эсхүл компьютерын систем ажиллах боломжтой, бэлэн байх;
b. компьютер, эсхүл компьютерын системийн бүрэн бүтэн байдлыг хангасан байх;
c. компьютер, эсхүл компьютерын системд хадгалагдсан, боловсруулсан, дамжуулж буй мэдээллийн бүрэн бүтэн байдал, нууцлалыг хангасан байх.

Мөн хуульд тодорхойлсноор "кибер аюулгүй байдлын осол" гэдэг нь хууль ёсны зөвшөөрөлгүйгээр компьютер, компьютерын системээр дамжуулан өөр компьютер, компьютерын системийн аюулгүй байдал, кибер аюулгүй байдалд сөргөөр нөлөөлөх, аюул учруулах үйлдэл, үйл ажиллагаа; харин "кибер аюулгүй байдлын заналхийлэл" гэдэг нь хууль ёсны зөвшөөрөлгүйгээр компьютер, компьютерын системээр дамжуулан өөр компьютер, компьютерын системийн аюулгүй байдал, кибер аюулгүй байдалд сөргөөр нөлөөлөх, аюул учруулах мэдэгдсэн болон сэжиглэгдсэн үйлдэл, үйл ажиллагаа гэж тус тус хуульчилсан байна.

Энэхүү судалгаагаар Сингапурт төвтэй *KuCoin, Exodus & BRD, DragonEx* криптобиржүүдэд гарсан кибер халдлага, тэдгээрийг шийдвэрлэсэн байдлыг судалж үзсэн. Биржүүдэд халдлага үйлдсэн этгээдүүдийг олж тогтоон, хариуцлага хүлээлгээгүй байна. Гэхдээ *Exodus & BRD*-д халдлага үйлдсэн этгээдийн эсрэг дэлхий даяар хөрөнгө битүүмжлэх шийдвэрийг Сингапурын Дээд шүүхээс гаргасан бөгөөд халдлага болсон биржүүдийг нэхэмжлэгчийн хэтэвчнээс шилжүүлсэн гүйлгээнүүдтэй холбоотой хэтэвчүүдийн өмчлөгчийн мэдээллийг ил болгох шийдвэр гаргасан. Харин *KuCoin, DragonEx* криптобиржүүд өөрсдийн хэрэглэгчдийн хохирлыг нөхөн төлөхөөр болсон ба *KuCoin* бирж хулгайлагдсан коинуудын олж аваагүй хэсгийг *KuCoin*-ы даатгалаас нөхөн төлсөн бол *DragonEx* бирж 7 сая ам. долларын үнэлгээ бүхий ДрагонХ 1 драгон бонд (Dragon bond) гаргаж, нөхөн төлөхөөр болсон (Биржүүдэд үйлдэгдсэн халдлагын үйл баримт, шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалтын дэлгэрэнгүйг Хавсралт 2-оос үзнэ үү).

[143] https://doj.gov.ph/files/cybercrime_office/Singapore%20Country%20Report.pdf
[144] https://sso.agc.gov.sg/Act/CA2018

### 3.3.3. Хонконгийн кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн жишээ

Хонконгт кибер аюулгүй байдлын тусгайлсан хууль байхгүй ч кибер аюулгүй байдалд хамаарах харилцааг дараах хуулиудын хүрээнд зохицуулж байна. Үүнд:

- Харилцаа холбооны тухай хуулийн[145] 27А. Харилцаа холбооны хэрэгслээр компьютерт зөвшөөрөлгүй нэвтрэх (хакердах);
- Гэмт хэргийн хуулийн[146] 161 дүгээр зүйл. Гэмт хэргийн болон шударга бус зорилгоор компьютерт нэвтрэх, 60 дугаар зүйл. Эд хөрөнгө устгах, гэмтээх;
- Хувийн мэдээлэл хамгаалах тухай хуулийн[147] 64 дүгээр зүйлд Хувийн мэдээллийг зөвшөөрөлгүйгээр тараасан бол гэмт хэрэгт тооцохоор заасан бөгөөд мэдээллийн эзний зөвшөөрөлгүйгээр хувийн мэдээлэл олж авсан, тараасан бол 1,000,000 хонконг долларoор торгох, эсхүл 5 хүртэл жилийн хорих ял шийтгэхээр хуульчилсан.
- Хүсээгүй цахим зурвасын тухай хууль,[148] Садар самуун, зүй бус зүйлд хяналт тавих тухай хууль, Хүүхдийг садар самуунаас урьдчилан сэргийлэх тухай хуулийн холбогдох заалтуудаар зохицуулна.

Хонконгт кибер аюулгүй байдлын хууль тогтоомжийн хэрэгжилтийг цагдаагийн байгууллага, хувийн мэдээллийн нууцлалын комиссар, харилцаа холбоо, хяналтын комиссар хангуулдаг.

2021 онд кибер халдлагын хохирогчид 214,400 хонконг доллар алдсантай холбоотой 496 тохиолдол, 2020 онд 114,400 хонконг доллар алдсантай холбоотой 208 кибер халдлагын тохиолдол цагдаагийн байгууллагад бүртгэгдсэн байна.[149]

Хонконгийн хуулийн шинэчлэлийн хорооны Кибер гэмт хэрэгтэй тэмцэх салбар хороо 2022 оны 6 дугаар сард хуралдан Зөвлөлдөх бичиг гаргасан.[150] Технологийн хөгжил эрчимжиж, интернэт, ухаалаг утас, олон нийтийн сүлжээ хөгжихөөс өмнө 1993 онд батлагдсан Гэмт хэргийн тухай хуулиар кибер гэмт хэргийг бүрэн тодорхойлж, зохицуулж чадахгүй байх тул хууль тогтоомжийн зохицуулалтыг шинэчлэх зайлшгүй шаардлага гарсан гэж үзжээ.

Улмаар НҮБ-ын үзэл баримтлал, Будапештийн конвенц, Дэлхийн Эрүүгийн загвар хуульд туссан гэмт хэргийн төрөл, бусад улс орны туршлагыг судалж кибер гэмт хэрэг нь дараах таван төрөлтэй байх саналыг Зөвлөлдөх бичигт

[145] Telecommunications Ordinance (Cap. 106).
[146] Crimes Ordinance (Cap. 200).
[147] Personal Data (Privacy) Ordinance.
[148] Unsolicited Electronic Messages Ordinance.
[149] https://www.thestar.com.my/tech/tech-news/2021/08/02/cryptocurrency-crime-in-hong-kong-hits-record-levels-with-one-victim-losing-hk124mil-to-fraudsters, хандсан огноо: 2022.04.15.
[150] Consultation Paper https://www.hkreform.gov.hk/en/docs/cybercrime_e.pdf

тусгасан. Зөвлөлдөх бичигт 2022 оны 10 дугаар сарын 19-ний өдөр хүртэл санал авахаар байна. Үүнд:

- Программ, өгөгдөлд хууль бусаар хандах;
- Компьютерын өгөгдлийг хууль бусаар саатуулах;
- Компьютерын өгөгдөлд хөндлөнгөөс оролцох;
- Компьютерын системд хууль бусаар хөндлөнгөөс оролцох;
- Гэмт хэрэг үйлдэх зорилгоор төхөөрөмж, өгөгдөл бэлтгэх, эзэмших.

Энэхүү судалгаагаар Хонконгийн *Bitfinex* криптобиржид гарсан кибер халдлага, түүнийг шийдвэрлэсэн байдлыг судалснаас гадна *Bitfinex & Tether* криптобиржүүдийн хууль тогтоомжоор хүлээсэн үүрэгтэй холбоотой иргэний хэргийн шүүхийн шийдвэрийг тус тус судалж үзсэн. *Bitfinex* биржид халдлага үйлдсэн этгээдүүдийг Манхэттэн дэх гэртээ байхад нь баривчилсан бөгөөд тэдний хөрөнгийг АНУ-ын Засгийн газраас хулгайлсан виртуал хөрөнгийн хэмжээгээр битүүмжилж, хураан авсан ба шүүх хурал үргэлжилж байна. Тэднийг үгсэн хуйвалдаж, бүлэглэн АНУ-ын хуулийн 18-р хэсэг, §1030. Компьютерын залилан ба компьютерыг урвуулан ашиглах тухай хууль зөрчсөн, §1956-г зөрчиж хууль бус үйл ажиллагаа явуулж санхүүгийн гүйлгээ хийсэн, хууль бус үйл ажиллагаанаас олсон хөрөнгө гэдгийг мэдсээр байж хөрөнгийн гарал үүсэл, байршил, эзэмшигчийг нуух, далдлах зэргээр үгсэн хуйвалдсан, хууль бус санхүүгийн гүйлгээ хийхээр завдсан, хууль бус үйл ажиллагааг удирдсан гэмт хэрэгт буруутай гэж үзэн яллаж байна.

Харин *Bitfinex & Tether* биржийн хэрэг нь кибер гэмт хэрэг биш бөгөөд виртуал хөрөнгийн биржийн хууль тогтоомжоор хүлээсэн үүрэгтэй шууд хамааралтай. Тодруулбал, бирж худал мэдээлэл тараахгүй байх, төлбөрийн чадвартай, хангалттай нөөцтэй байх зэрэг үүрэг хүлээсэн ч дээрх үүргийг зөрчиж, улмаар үүргээ биелүүлж байгаа мэт нөхцөлийг хуурамчаар бий болгож, хэрэглэгчдэд худал мэдээлэл тараасан гэж үзсэн. Иймд үүргээ зөрчсөн гэх үндэслэлээр торгуулийн шийтгэл хүлээлгэж, эвлэрлийн гэрээ байгуулан маргааныг дуусгавар болгожээ (Биржүүдэд үйлдэгдсэн халдлагын үйл баримт, шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалтын дэлгэрэнгүйг Хавсралт 3-аас үзнэ үү).

### 3.3.4. Америкийн Нэгдсэн Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн жишээ

Кибер гэмт хэрэг, тэр дундаа хакердах болон хортой программ[151] ашиглан хийгдэж буй гэмт хэргүүд, мэдээллийн систем, бүтэц, харилцаа холбооны сүлжээний аюулгүй байдал, нууцлалд халдсан шинжтэй аливаа үйлдлийг мөрдөн шалгах, хянан шийдвэрлэх гол хууль нь АНУ-ын Холбооны хуулийн §1030. Компьютерын залилан ба компьютерыг урвуулан ашиглах тухай хууль[152] юм.

[151] ransomware, spyware, worms, trojans, viruses.

[152] The Computer Fraud and Abuse Act, 18 U.S.C. 1030. Энэхүү хууль нь АНУ-ын хуулийн 18-р хэсэг. Гэмт хэрэг ба эрүүгийн процесс гэх хэсэгт нэмэлтээр орсон.

Холбооны хуулиас гадна мужууд хакердах, бусад кибер гэмт хэргийг хориглосон хууль тогтоомж баталсан байдаг бөгөөд Холбооны хуулиар тодорхойлсноос өргөн хүрээтэй тодорхойлсон нь ч бий.

Энэхүү судалгаагаар АНУ-ын *Binance, Cryptsy* криптобиржүүдэд гарсан халдлага, тэдгээрийг шийдвэрлэсэн байдлыг судалснаас гадна *Tether* криптобиржийн хуулиар хүлээсэн үүрэгтэй холбоотой маргааныг судалж үзсэн болно.

*Binance, Cryptsy* биржүүдэд халдлага үйлдсэн этгээдүүдийг олж тогтоон яллах дүгнэлт үйлдсэн. Тодруулбал, *Binance* биржид халдлага үйлдсэн этгээдүүдэд АНУ-ын Холбооны хуулийн 18-р хэсэг, Компьютерын залилан ба компьютерыг урвуулан ашиглах тухай хуулийн холбогдох хэсгүүдийг зөрчсөн, хулгайн гэмт хэргийг хүндрүүлэх бүрэлдэхүүнтэйгээр бүлэглэн үйлдсэн, мөнгө угаах гэмт хэрэгт тус тус гэм буруутайд тооцон яллах дүгнэлт үйлдсэн бол *Cryptsy* биржийн хэргийн хувьд АНУ-ын Холбооны хуулийн 18-р хэсэг, сүлжээ ашиглан залилан мэхэлсэн, мөнгө угаах гэмт хэрэг үйлдсэн, мэдээлэл, код ашиглаж хамгаалалттай компьютерт нэвтэрч, залилан мэхэлсэн, Холбооны мөрдөн шалгах ажиллагааны баримт бичгийг устгасан, татвараас зайлсхийхийг оролдсон, мөн тухайн жилүүдэд хувь хүний орлогын албан татварыг тайлагнахдаа дутуу тайлагнаж, хуурамч тайлан гаргасан гэх гэмт хэргийн шинжтэй нийт 17 үйлдэлд буруутгаж, яллах дүгнэлт үйлдэн, хөрөнгийг нь хураахаар шийдвэрлэсэн.

*Tether биржийн хувьд* Таваарын фьючерсийн арилжааны комиссоос Таваарын болон үнэт цаасны арилжааны хууль зөрчиж, худал, төөрөгдүүлсэн мэдэгдэл хийх, эсхүл хийсэн мэдэгдэл нь худал, төөрөгдүүлсэн мэдэгдэл болохыг нотлох шаардлагатай баримт дурдахаас татгалзсан, худал мэдээлэл тараах, манипуляц хийхийг хориглоно гэснийг зөрчсөн гэж үзэж, торгууль ногдуулах шийдвэр гаргасан (Биржүүдэд үйлдэгдсэн халдлагын үйл баримт, шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалтын дэлгэрэнгүйг Хавсралт 4-өөс үзнэ үү).

### 3.3.5. Бүгд Найрамдах Солонгос Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн жишээ

БНСУ-д Кибер аюулгүй байдлыг хангах талаар Мэдээлэл, харилцаа холбооны сүлжээ ашиглалтыг дэмжих, мэдээллийг хамгаалах тухай хууль, Цахилгаан харилцаа холбооны аж ахуйн нэгжийн хууль, Компьютерын программын хамгаалалтын хууль, Харилцаа холбооны нууцын хууль, Үндэсний мэдээлэлжүүлэлтийн суурь хууль, Мэдээлэл, харилцаа холбооны дэд бүтцийг хамгаалах хууль, Зохиогчийн эрхийн хууль, Цахим захиргааны хууль, Цахим захиргааны хэрэгжилтийг хангах үүднээс захиргааны байгууллагуудын үйл ажиллагааны цахимжилтыг дэмжих тухай хууль, Санхүүгийн цахим гүйлгээний тухай хууль, Цахилгаан холбооны санхүүгийн залилангийн хохирлоос сэргийлэх, хохирлыг буцаан олгох тухай тусгай хуулиуд хүчин төгөлдөр үйлчилж байна.

БНСУ-ын Үндэсний ассамблейгаас кибер аюулгүй байдлыг хангах үүднээс дараах хуулийн төслүүдийг боловсруулж, Байнгын хороодын хяналтын шатанд явж байна. Эдгээр төсөлд кибер халдлагын эсрэг хариу арга хэмжээ авах системтэй бодлогыг бүрдүүлж, төр, хувийн хэвшлийн хамтын ажиллагаа, аж үйлдвэр, хүний нөөц, шинжлэх ухааны хөгжлийг дэмжихийг чухалчилж үзжээ. Тухайлбал:

1. Кибер аюулгүй байдлын суурь хуулийн төсөл (2021.12.02-ны өдөр санаачилсан);[153]
2. Үндэсний кибер аюулгүй байдлыг хангах хуулийн төсөл (2021.11.04-ний өдөр санаачилсан);[154]
3. Кибер аюулгүй байдлын суурь хуулийн төсөл (2020.06.30-ны өдөр санаачилсан).[155]

Виртуал хөрөнгийн арилжаа хийгддэг 154 улсаас БНСУ арилжааныхаа хэмжээгээр гуравт ордог бөгөөд ихэнх хэрэглэгчид нь виртуал хөрөнгийг хөрөнгө оруулалтын зорилгоор ашигладаг. Тус улсад виртуал хөрөнгийн арилжаа нэмэгдэхийн зэрэгцээ биржийн кибер халдлага, үнийн манипуляц гэх мэт шударга бус үйлдлийн улмаас хэрэглэгчид хохирох тохиолдол гарч байна. Тодруулбал, 2017-2019 оны хооронд виртуал хөрөнгийн кибер халдлагын улмаас болон зүй бус байдлаар алдагдсан мөнгөнийх нь хэмжээ 178 тэрбум вонд хүрчээ.[156]

БНСУ-ын томоохон дөрвөн платформд хадгалагдах хөрөнгө ойролцоогоор 59,381.4 тэрбум вон, мөн өдөрт хийгдэх арилжааны хэмжээ 10 их наяд вон (2021 оны 8 дугаар сарын 31-ний өдрийн байдлаар) байгааг судлаачид дотоодын санхүүгийн системийн тогтвортой байдалд нөлөөлөхүйц хэмжээний түвшинд хүрсэн гэж үзжээ.[157] Түүнчлэн виртуал хөрөнгө хэрэглэгчийнх нь тоо 5,000,000 давсан[158] байна.

Энэхүү судалгаагаар БНСУ-ын *Coinrail* криптобиржид гарсан халдлагын улмаас хэрэглэгчид учирсан хохирлыг барагдуулахтай холбоотой Сөүл

153 사이버보안 기본법안(윤영찬의원 등 12인)
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_T2B1W1I1M1F7U1Z-8F2R2A4I5D8L6X9

154 국가사이버안보법안(김병기의원 등 13인),
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_P2I1J1H0N0V6U1T8K5N5C5E-2H8A6B0

155 사이버안보 기본법안(조태용의원 등 27인)
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_S2C0I0T6E3Q0C1X-7W4E3I0B7S5Z7Z9

156 가상자산 거래에 관한 법률안(양경숙의원 등 10인)
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_P2Y1J0F5N2C0H1Z4R1S3R3N-3W4H3B0

157 김갑래 · 김준석 (자본시장연구원), 가상자산 거래자 보호를 위한 규제의 기몬 방향, 2021 년, 1면, https://www.kcmi.re.kr/report/report_view?report_no=1470

158 가상자산 거래 및 이용자 보호 등에 관한 법률안(권은희의원 등 10인)
http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_K2T1V0H6U0L9M0X9A4W8A3G-0W7Q6H1

хотын төв дүүргийн шүүхийн шийдвэрлэсэн хэргийг судалсан. Шүүх хэрэглэгчдийн хохирлыг биржээс бүрэн гаргуулахаар шийдвэрлэсэн байна. Шүүхийн дүгнэлтийн үндэслэл болсон Иргэний хуулийн 390,[159] 544,[160] 546[161] дугаар зүйлүүдээс үзвэл бирж кибер халдлагад гэм буруугүй гэдгээ нотолсон тохиолдолд хохирол барагдуулах хариуцлага хүлээхгүй. Энэ хэргийн хувьд *Coinrail* бирж гэм буруугүй гэдгээ нотолж чадаагүй тул шүүх хэрэглэгчдийн хохирлыг биржээс гаргуулахаар шийдвэрлэжээ (Биржүүдэд үйлдэгдсэн халдлагын үйл баримт, шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалтын дэлгэрэнгүйг Хавсралт 5-аас үзнэ үү).

### 3.3.6. Швейцарын Холбооны Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн жишээ

Швейцарт кибер гэмт хэргийг Эрүүгийн хуулиар[162] зохицуулсан байдаг. Эрүүгийн хуулийн тусгай ангийн 143 дугаар зүйлд зөвшөөрөлгүйгээр мэдээллийн өгөгдөл олж авах, мэдээлэл дамжуулах системд зөвшөөрөлгүйгээр нэвтрэх үйлдлийг, 144 дүгээр зүйлд мэдээллийн өгөгдлийг гэмтээх үйлдлийг гэмт хэрэг гэж хуульчилсан. Кибер аюулгүй байдлын тухай бие даасан тусгай хууль байдаггүй боловч[163] Холбооны мэдээлэл хамгаалах тухай ерөнхий хуулиар (*FADP*) хувийн мэдээллийг техникийн болон зохион байгуулалтын зохих арга хэмжээ авах замаар зөвшөөрөлгүй нэвтрэх халдлагаас хамгаалах ёстой гэж үздэг.

Швейцарт кибер аюулгүй байдлыг хамгаалах хүрээнд дараах хуулиудыг хэрэглэдэг. Үүнд:[164]

- Иргэний хууль;
- Үүргийн хууль (*Code of obligations*);
- Будапештийн конвенц;
- Хөдөлмөр эрхлэлтийн тухай хууль;
- Шударга бус өрсөлдөөний тухай хууль;
- Зохиогчийн эрхийн тухай хууль;
- Барааны тэмдгийг хамгаалах тухай хууль.

[159] 390 дүгээр зүйл. Үүрэг гүйцэтгэгч үүргээ үл биелүүлэх ба хохирол барагдуулах). Үүрэг гүйцэтгэгч хүлээсэн үүргээ биелүүлээгүй тохиолдолд үүрэг гүйцэтгүүлэгч хохирлоо шаардаж болно. Гэхдээ үүрэг гүйцэтгэгчийн санаатай, эсхүл болгоомжгүй үйлдэл байхгүй тохиолдолд хохирол шаардаж болохгүй.

[160] 544 дүгээр зүйл. Үүрэг гүйцэтгэлийг хойшлуулах ба цуцлах). Талуудын аль нэг нь үүргээ гүйцэтгээгүй бол боломжит хугацаа тогтоож, үүрэг гүйцэтгэхийг мэдэгдэх ба тухайн хугацаанд үүргээ гүйцэтгээгүй бол гэрээг цуцалж болно. Гэхдээ үүрэг гүйцэтгэгч үүргээ гүйцэтгэхгүй гэдгээ илэрхийлсэн тохиолдолд хугацаа тогтоох шаардлагагүй.

[161] 546 дугаар зүйл. Үүрэг гүйцэтгэх боломжгүй болох ба цуцлах). Үүрэг гүйцэтгэгчээс шалтгаалж үүрэг гүйцэтгэх боломжгүй болсон тохиолдолд үүрэг гүйцэтгүүлэгч гэрээг цуцалж болно.

[162] Swiss criminal Code, https://sherloc.unodc.org/cld/uploads/res/document/che/1937/swiss_criminal_code_en_html/Swiss_Criminal_Code_amJuly2020.pdf

[163] https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/switzerland

[164] https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/switzerland

Швейцарын статистикийн албанаас 2022 оны 3 дугаар сарын 28-ны өдөр мэдээлснээр 2021 онд цахим орчинд үйлдэгдсэн 30,351 кибер гэмт хэрэг цагдаагийн байгууллагад бүртгэгдсэн бөгөөд энэ нь өмнөх оныхтой харьцуулахад 24 хувиар өссөн гэжээ.[165]

Энэхүү судалгаагаар Швейцарын *Trade.io, Bancor* криптобиржид гарсан халдлагын талаар судалсан. Дээрх биржүүдийн халдлагатай холбоотой асуудлыг шүүхээр шийдвэрлээгүй бөгөөд биржүүд хэрэглэгчийн хэтэвч дэх виртуал хөрөнгөд халдаагүй гэж мэдэгдэл хийсэн (Биржүүдэд үйлдэгдсэн халдлагын үйл баримт, шийдвэрлэсэн байдлын дэлгэрэнгүйг Хавсралт 6-гаас үзнэ үү). Мөн виртуал хөрөнгийн биржийн халдлагатай холбоотой шүүхээр шийдвэрлэгдсэн тохиолдлыг Швейцарын Дээд шүүхийн сайтаас хайж үзэхэд нээлттэй байршсан шүүхийн шийдвэр, захирамж байхгүй байна.

### 3.3.7. Бүгд Найрамдах Эстони Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржийн жишээ

БНЭУ нь кибер аюулгүй байдлаа 2018 оны 5 дугаар сарын 23-ны өдрөөс хүчин төгөлдөр мөрдөгдөж эхэлсэн Кибер аюулгүй байдлын тухай хуулиар зохицуулдаг. Тус хууль нь 6 бүлэг, 29 зүйлтэй ба хуулийн 2 дугаар зүйлийн 3-т “Кибер осол гэж системийн аюулгүй байдалд сөргөөр нөлөөлж болзошгүй аливаа үйл явдлыг хэлнэ” хэмээн тодорхойлсон байна.[166]

Энэхүү судалгаагаар БНЭУ-ын *Taylor* криптобиржид гарсан халдлагын талаар судалсан. Дээрх халдлагатай холбоотой асуудлыг шүүхээр шийдвэрлээгүй бөгөөд компани хэрэглэгчдийн хохирлыг нөхөн төлөхийн тулд хэрэглэгчдэд шинэ токен тараах шийдвэр гаргасан ба компанийн үүсгэн байгуулагч, гүйцэтгэх захирал нь болсон явдалд уучлалт гуйж, энэхүү байдлыг даван туулахад туслахыг олон нийт (*community*)-д хандан уриалсан байна (Биржид үйлдэгдсэн халдлагын үйл баримт, шийдвэрлэсэн байдлын дэлгэрэнгүйг Хавсралт 7-гоос үзнэ үү).

Шүүхээс гадуурх Кибер аюулгүй байдлын тухай хуульд заасан хариуцлага оногдуулах этгээд нь БНЭУ-ын Мэдээллийн системийн газар байхаар хуульчилсан. Биржийн халдлагатай холбоотой шүүхээр шийдвэрлэгдсэн тохиолдол, шүүхийн шийдвэр, захирамжийг хайж үзэхэд нээлттэй байршсан шийдвэр, захирамж байхгүй байна.

### 3.3.8. Оросын Холбооны Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржийн жишээ

ОХУ-ын Эрүүгийн хуулиар кибер гэмт хэрэг, түүний төрлүүдийг тодорхой зохицуулсан ба дараах үйлдлийг хийснээр тус хуулийн 272 дугаар зүйлд

---

[165] https://www.swissinfo.ch/eng/swiss-cyber-crime-incidents-increase-by-a-quarter/47469694#:~:text=There%20was%20also%20an%20uptick,the%20virtual%20space%20in%202021.

[166] Cybersecurity Act of Estonia, https://www.riigiteataja.ee/en/eli/523052018003/consolide “Riigi Teataja” нь БНЭУ-ын олон нийтийн сэтгүүл юм.

Компьютерын мэдээлэлд хууль бусаар нэвтрэх гэмт хэрэг үйлдсэнд тооцдог. Үүнд[167]:

- Хууль бусаар компьютерын мэдээлэлд халдах - компьютерын мэдээлэл, эсхүл системд нэвтрэх эрх олгогдоогүй этгээд мэдээлэлд нэвтэрсэн;
- Хэрэглээнд байгаа мэдээллийг бүхэлд нь, эсхүл хэсэгчлэн устгасан;
- Мэдээлэлд нэвтрэх эрхэд хаалт хийсэн;
- Мэдээлэл хадгалах хэрэгсэл дээр хадгалагдаж буй программ, мэдээллийн сан, текстэн мэдээллийг өөрчлөх буюу компьютерын мэдээллийг өөрчилсөн;
- Хууль бусаар компьютерын мэдээллийг бусад төхөөрөмж рүү зөөвөрлөсөн.

Кибер аюулгүй байдлыг хангахтай холбоотой харилцааг ОХУ-ын мэдээллийн технологи, мэдээллийн аюулгүй байдлын тухай хууль[168] болон ОХУ-ын мэдээллийн аюулгүй байдлыг хангах бодлогын баримт бичгээр[169] зохицуулж байна. Тус улс 2020 онд мөнгө угаах гэмт хэрэгтэй тэмцэх зорилгоор Дижитал санхүүгийн хэрэгслийн тухай хууль[170] баталсан бөгөөд энэ хууль 2021 оны 1 дүгээр сарын 1-ний өдрөөс хэрэгжиж эхэлсэн. Уг хуулиар мэдээллийн системийн операторын үйл ажиллагааны онцлог буюу дижитал санхүүгийн хэрэгсэл гаргах журам болон дижитал валют гүйлгээнд гаргахтай холбоотой харилцааг зохицуулна. Криптобиржид тавигдах шаардлага, хуулиар хүлээх үүргийн талаар Дижитал санхүүгийн хэрэгслийн тухай хуулийн 10 дугаар зүйлд "*Санхүүгийн дижитал хөрөнгийн арилжааны оператор*" хэсэгт дараах байдлаар тодорхойлжээ. Үүнд:

- Санхүүгийн дижитал хөрөнгийн арилжааны оператор нь зээл, худалдаа, эсхүл бусад чиглэлээр үйл ажиллагаа явуулдаг хуулийн этгээд байна.
- Хувь нийлүүлсэн хөрөнгийн доод хэмжээг 50 сая рублиэр тогтоосон.
- Хулийн этгээдийн хувьцаа эзэмшигч нь татварын хөнгөлөлт бүхий оффшор бүсэд үйл ажиллагаа явуулдаг хуулийн этгээд байхыг хориглоно.
- Хуулийн этгээдийн дотоод бүтцэд эрсдэл болон дотоод хяналт хариуцсан нэгж байна.
- Хуулийн этгээдийн нэр хүндэд халдахгүй байх үүднээс хүний нөөцийн мэргэшсэн боловсон хүчинтэй байна.

Энэхүү судалгаагаар ОХУ-ын *Live coin* криптобиржид гарсан халдлагыг судалсан бөгөөд бирж үйл ажиллагаагаа хааж, хэрэглэгчдийн хохирлыг барагдуулах талаар мэдэгдэл гаргасан маргаан нь шүүхээр шийдвэрлэгдээгүй байна (Биржид үйлдэгдсэн халдлагын үйл баримт, шийдвэрлэсэн байдлын талаар Хавсралт 8-аас үзнэ үү).

[167] М.Х.Гельдибаев, Е.Н.Рахманова. Уголовное право в схемах и определениях. СПб., 2017, с.521.
[168] http://www.consultant.ru/document/cons_doc_LAW_61798/
[169] https://www.garant.ru/products/ipo/prime/doc/71456224/
[170] http://www.consultant.ru/document/cons_doc_LAW_358753/

# ДҮГНЭЛТ

Кибер гэмт хэргийн зохицуулалтын харьцуулсан судалгаа (Виртуал хөрөнгийн биржийн үүрэг, үйл ажиллагааны эрсдэлийн хүрээнд)-гаар кибер гэмт хэргийн хамрах хүрээ, эрх зүйн эх сурвалж, кибер гэмт хэргийн онцлог, виртуал хөрөнгийн биржийн үүрэг, үүсэж болох хууль зүйн эрсдэл, кибер гэмт хэргийг мөрдөн шалгах явцад цахим нотлох баримттай ажиллах нөхцөл, журмыг судлахын сацуу Япон, БНСУ, Сингапур, Хонконг, Швейцар, ОХУ, АНУ, БНЭУ зэрэг улсын эрх зүйн зохицуулалт болон виртуал хөрөнгийн биржид халдсан кибер халдлага, тэдгээрийг шийдвэрлэсэн байдлыг судалж, дараах нэгдсэн дүгнэлт хийлээ. Үүнд:

1. Будапештийн конвенц болон Дэлхийн Эрүүгийн загвар хууль нь кибер гэмт хэргийн үндсэн шинж, төрлийг тодорхойлж буй эрх зүйн голлох эх сурвалж юм. Унгар Улсын Будапешт хотноо 2001 онд батлагдсан Будапештийн конвенцын хоёрдугаар бүлэгт кибер гэмт хэргийн дөрвөн төрлийг тодорхойлж, есөн гэмт хэргийг хуульчилсан. Будапештийн конвенцод зааснаар кибер гэмт хэрэг нь (1) компьютерын өгөгдөл болон системийн нууцлал, бүрэн бүтэн, хүртээмжтэй байдлын эсрэг гэмт хэрэг, (2) компьютер ашигласан гэмт хэрэг, (3) контент агуулгатай холбоотой гэмт хэрэг, (4) зохиогчийн эрх, түүнд хамаарах эрхийн зөрчилд холбогдох гэмт хэрэг гэсэн дөрвөн төрөлд хуваагдана. Харин Дэлхийн Эрүүгийн загвар хуульд компьютерын системд хууль бусаар нэвтрэх, компьютерын мэдээллийн санд хууль бусаар саад хийх, компьютерын мэдээллийн санд хөндлөнгөөс оролцох, компьютерын системд хөндлөнгөөс оролцох, тоног төхөөрөмж зүй бусаар ашиглах гэмт хэргүүдийг тусгасан байна.

2. Монгол Улсад кибер гэмт хэргийн хамрах хүрээ нь Эрүүгийн хуулийн 26 дугаар бүлэгт заасан “Кибер орчинд хууль бусаар халдах”, “Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах” гэмт хэргээс гадна кибер орчинд цахим хэрэгсэл, дижитал төхөөрөмж ашиглан үйлдэж буй гэмт хэргүүдийг багтаан авч үздэг. Тухайлбал, Эрүүгийн хуулийн 13.10 дугаар зүйлийн 2 дахь хэсэгт заасан Харилцаа холбоо, цахим хэрэгсэл ашиглаж хувь хүний нууцад халдах, 13 дугаар зүйлийн 11 дэх хэсэгт заасан Харилцаа холбоо, цахим сүлжээ ашиглаж хувь хүний нууцыг задруулах, 17.3 дугаар зүйлийн 1 дэх хэсэгт заасан Цахим хэрэгсэл ашиглаж залилах, 16.9 дүгээр зүйлийн 2.1 дэх хэсэгт заасан Кибер орчныг ашиглаж хүүхэд оролцуулж, садар самууныг сурталчлах гэмт хэргүүд нь кибер гэмт хэрэгт хамаарна. Монгол Улсын Эрүүгийн хуулиар тодорхойлсон кибер гэмт хэргийн зохицуулалт Дэлхийн Эрүүгийн загвар хуульд үндэслэсэн байна.

3. Кибер гэмт хэрэг үйлдэх орчин, нөхцөл, ашиглаж буй арга зам, хэрэгсэл нь бусад гэмт хэргүүдтэй харьцуулбал бүх дэлхийг хамарсан, улсын нутаг дэвсгэрээр хязгаарлагдахгүй онцгой шинж агуулсан бөгөөд интернэт сүлжээний тусламжтайгаар дэлхийн аль ч хэсгээс уг гэмт хэргийг үйлдэх боломжтой. Тухайн гэмт хэргээс урьдчилан сэргийлэх болон мөрдөн шалгах ажиллагаанд дотоодод төрийн байгууллага, хувь хүн, хуулийн этгээдийн хамтын ажиллагаа, гадаадад улс хоорондын хамтын ажиллагаа чухал ач холбогдолтой байна. Зарим улс оронд кибер гэмт хэргийн талаарх мэдээлэл солилцох механизм бий болгосон. Тухайлбал, Шинэ Зеланд Улсад интернэт дэх зохисгүй контентын эсрэг кибер гэмт хэргийн талаарх мэдээлэл үлдээх боломжтой веб сайтыг интернэт дэх мэдээллийн аюулгүй байдлын чиглэлээр үйл ажиллагаа явуулдаг *Net-Safe* төрийн бус байгууллагаас хөгжүүлж, төрийн байгууллагуудтай хамтран ажиллаж байна. Мөн Өмнөд Африкт иргэнийг компьютер болон интернэт ашиглан үйлдсэн гэмт хэргүүдийн талаарх мэдээллээр хангах, гэмт хэргийн талаарх гомдол, мэдээллийг тогтмол хүлээн авах веб сайт ажиллуулж байна.

4. Монгол Улсын хэмжээнд Эрүүгийн хэргийн анхан шатны шүүхээр 2017 оны 7 дугаар сарын 1-ний өдрөөс 2022 оны 9 дүгээр сарын 1-ний өдөр хүртэлх хугацаанд Монгол Улсын Шүүхийн шийдвэрийн цахим сан *www.shuukh.mn* сайтаас Эрүүгийн хуулийн 26.1 дүгээр зүйл. Кибер орчинд хууль бусаар халдах болон 26.2 дугаар зүйл. Кибер орчинд хууль бусаар халдах, программ хангамж, техник хэрэгсэл бүтээх, бэлтгэх, борлуулах, ашиглах, тараах гэмт хэргээр зүйлчилж, шийдвэрлэсэн, хүчинтэй, анхан шатны шүүхийн шийтгэх тогтоолуудыг шүүж үзэхэд нийт 50 шүүхийн шийтгэх тогтоолыг нээлттэй байршуулжээ. Шүүхийн шийдвэрүүдийн хууль зүйн дүгнэлтээс үзвэл кибер орчинд хууль бусаар халдаж мэдээллийг устгасан, гэмтээсэн, өөрчилсөн, засварласан, нуусан, нэмж оруулсан, хуулбарлаж авсан, ашиглах боломжгүй болгосон үйлдэлд ял шийтгэсэн тохиолдол дийлэнх нь байгаа бол кибер орчинд хууль бусаар халдах гэмт хэргийг бусад гэмт хэрэгтэй буюу хулгайлах, цахим хэрэгсэл ашиглаж залилах гэмт хэрэгтэй давхар зүйлчлэх тохиолдол цөөнгүй байна. Тухайлбал, бусдын нийгмийн сүлжээ болох *Facebook* хаягт зөвшөөрөлгүйгээр нэвтрэх замаар хохирогчийн хөрөнгийг хууль бусаар олж авах гэмт үйлдэл түгээмэл байна.

5. Монгол Улсад 2022 оны 7 дугаар сарын байдлаар дотоодын криптобиржид гарсан цахим халдлага бүртгэгдээгүй боловч Баянзүрх дүүргийн эрүүгийн хэргийн анхан шатны шүүхээс *DAX* нэртэй криптовалютын биржид бүртгэлтэй хэрэглэгчийн хэтэвчийн нэвтрэх нэр, нууц үгийг олж аван өөрчилж, хэтэвчнээс виртуал хөрөнгийг хууль бусаар авч, түүнийг өөрийн *Binance* нэртэй криптовалютын бирж дэх хэтэвчдээ шилжүүлэн авч, хувиргаж хадгалж эзэмшсэн үйлдэлд гэм буруутайд тооцож, ял шийтгэсэн тохиолдол гарчээ.

6. Иймд хэрэглэгч мэдээллийн аюулгүй байдлын нууцлалаа хадгалаагүйгээс хөрөнгөө алдах эрсдэл байгаагаас гадна ВХҮҮтХ батлагдахаас өмнө үйл ажиллагаа эхэлсэн виртуал хөрөнгийн арилжааны платформууд байгаа тул кибер халдлагад өртөх, хэрэглэгчдийн хөрөнгөд халдах эрсдэл байгааг дурдах нь зүйтэй. Иймээс Монгол Улс нь ФАТФ-ын зөвлөмжийн хэрэгжилтийг хангах үүднээс 2021 оны 12 дугаар сарын 17-ны өдөр ВХҮҮтХ баталсан. Тус хууль болон түүнд үндэслэн батлагдсан Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журам, Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн үйл ажиллагааны журмаар криптобирж буюу ВХҮҮ-д тавигдах хууль зүйн шаардлагыг тодорхойлсон нь кибер гэмт хэргээс урьдчилан сэргийлэх нэг алхам болсон байна. Тухайлбал, Хорооны 2022 оны 4 дүгээр сарын 6-ны өдрийн 174 дүгээр тогтоолоор баталсан Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журмын 3 дугаар хавсралтаар ВХҮҮ-ийн үйл ажиллагаандаа мөрдөх мэдээллийн технологийн нийт 11 стандарт тогтоосон.

7. ВХҮҮ нь журмын хавсралтаар баталсан стандартуудыг хангаж, хөндлөнгийн эрх бүхий байгууллагаар баталгаажуулсан бол кибер халдлагад өртсөн эсэхээс үл хамааран ВХҮҮтХ-ийн 7 дугаар зүйлийн 7.1.2-т заасан технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангасан байх шаардлагыг хангасан гэж үзэхээр байна. Харин кибер халдлагын улмаас виртуал хөрөнгийн биржийн үйл ажиллагаа тасалдсан тохиолдолд ВХҮҮтХ-ийн 8 дугаар зүйлийн 8.1.4-т заасан харилцагчийн тухайн үйлчилгээнд хамаарах виртуал хөрөнгө болон мөнгөн хөрөнгийн гүйлгээ хийх, шилжүүлэх, арилжих, хадгалах, удирдах нөхцөл, боломжийг тасралтгүй хангаж ажиллах үүргээ зөрчсөн эсэхийг тогтоож байж зөрчлийн хариуцлага хүлээлгэхээр зохицуулаагүй. Өөрөөр хэлбэл, ВХҮҮ нь Хорооноос тогтоосон стандартыг мөрдөж ажиллаагүйн улмаас, эсхүл мөрдөж ажилласан хэдий ч кибер халдлагад өртөх боломжтой. Мэдээлэл технологийн тасралтгүй, хурдацтай хөгжил, гэм буруугийн хэлбэрийг харгалзан үзэж, тусгай тохиолдлыг тухайлан зохицуулаагүй нь хууль хэрэглээний төвөгтэй байдал үүсгэхээр байна.

8. ВХҮҮ нь кибер гэмт хэргээс урьдчилан сэргийлэх, түүнтэй тэмцэх хүрээнд ВХҮҮтХ, түүнд үндэслэн батлагдсан журмуудаас гадна Монголын үндэсний аюулгүй байдлын үзэл баримтлал болон Кибер аюулгүй байдлын тухай хуулийг дагаж мөрдөнө. Монгол Улс нь 2021 оны 12 дугаар сарын 17-ны өдөр Кибер аюулгүй байдлын тухай хууль баталсан бөгөөд ВХҮҮ нь тус хуулийн 17.1 дэх хэсэгт заасан үүргийг биелүүлж ажиллахаар байна. Тухайлбал, мэдээллийн эрсдэлийн үнэлгээ, мэдээллийн аудит хийлгэх зэргийг дурдаж болно. Мөн тухайн хуулийг хэрэгжүүлэхтэй холбоотой журмуудыг Засгийн газар болон Цахим хөгжил, харилцаа холбооны яамнаас батлахаар зохицуулсан боловч 2022 оны 7 дугаар сарын байдлаар Засгийн газраас “Кибер

аюулгүй байдлыг хангах, урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах нийтлэг журам”-ыг батлаагүй байна.

9. Кибер халдлагаас урьдчилан сэргийлэх болон мөрдөн шалгах ажиллагаанд хувийн хэвшил, төрийн байгууллагын хамтын ажиллагаа чухал ач холбогдолтой тул Цахим хөгжил, харилцаа холбооны яамны дэргэдэх Нийтийн төв нь кибер халдлага, зөрчлийн талаарх зөвлөмж, шаардлагыг иргэн, хуулийн этгээдэд хүргүүлэхээр тусгасан. ВХҮҮ нь кибер халдлага, зөрчлийн талаарх мэдээллийг тус төвд хүргүүлэх үүргийг мөн хүлээнэ.

10. ВХҮҮ-ийн кибер гэмт хэргээс урьдчилан сэргийлэх, мэдээллийн аюулгүй байдлыг хангах хүрээнд заавал биелүүлэх үүргийг хэрхэн хуульчилсныг харьцуулан судалж үзвэл улс бүрийн онцлогоос хамаарч дараах байдлаар зохицуулж байна. Үүнд:
    - БНСУ-ын Виртуал хөрөнгийн үйлчилгээний тухай хуулийн төслийн 24, 25 дугаар зүйлийн зохицуулалтыг Монгол Улсын ВХҮҮтХ-ийн 8 дугаар зүйлийн 8.1.4, 8.1.5 дахь заалтын зохицуулалттай харьцуулан үзвэл БНСУ-ын хувьд ВХҮҮ-ийн гэм бурууг харгалзан хариуцлагаас чөлөөлөх зарчим баримталж байна.
    - Сингапурын парламентаас 2022 оны 4 дүгээр сарын 5-ны өдөр Санхүүгийн үйлчилгээ, зах зээлийн тухай хууль баталсан бөгөөд тус хуулийн 29 дүгээр зүйлийн 29.(1)-д зааснаар санхүүгийн байгууллага нь кибер аюулгүй байдлын эрсдэлийн технологийн менежмент, санхүүгийн үйлчилгээг аюулгүй, найдвартай хүргэх, өгөгдөл хамгаалах технологийн аюулгүй байдлыг хангаж ажиллах ба энэ талаар заавар, журам гаргахаар заасан. Виртуал хөрөнгийн үйлчилгээнд ашиглах технологийн аюулгүй байдал болон тасралтгүй, найдвартай ажиллагааг хангах виртуал хөрөнгийн биржийн үүргийг Сингапурт мөн адил хуулиар хүлээлгэсэн.
    - Япон Улсад Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн тухай Засгийн газрын 2017 оны 3 дугаар тогтоолын 13 дугаар зүйлд зааснаар ВХҮҮ нь өөрийн үйл ажиллагааны агуулга, арга барилын дагуу виртуал хөрөнгийн үйл ажиллагаанд хамаарах цахим мэдээлэл боловсруулах хяналтын хангалттай арга хэмжээ авах ёстой. Мөн Санхүүгийн төлбөр тооцооны тухай хуулийн 63 дугаар зүйлийн 8 дахь хэсэгт зааснаар ВХҮҮ нь Засгийн газрын тогтоолд заасны дагуу виртуал хөрөнгийн үйлчилгээнд холбогдох мэдээллийн нууц задруулах, мэдээллийг устгах, эсхүл түүнд халдахаас урьдчилан сэргийлэх, холбогдох бусад мэдээллийн аюулгүй байдлыг хянахад шаардлагатай арга хэмжээ авч хэрэгжүүлэх ёстой.
    - АНУ-ын Хууль зүйн яам нь криптовалют болон бусад төрлийн виртуал хөрөнгөтэй холбоотой эрүүгийн болон зохисгүй бусад үйлдэлд хамаарах өргөн хүрээний шүүн таслах ажиллагаа явуулдаг. Хууль зүйн яамнаас гадна АНУ-д зохицуулах үйлчилгээтэй хэд

хэдэн агентлаг виртуал хөрөнгийн үйл ажиллагаанд хамаарах хууль тогтоомжид заасан бүрэн эрхийг хэрэгжүүлдэг ба Хууль зүйн яамтай хамтран криптовалютыг хууль бус зорилгоор урвуулан ашигласан хүмүүсийг илрүүлж, мөрдөн байцаалт явуулж байна.

- БНЭУ нь Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн зохицуулалт бий болгож, ФАТФ-ын *Travel Rule*-ийн шаардлагыг дагаж мөрддөг бөгөөд БНЭУ-д крипто арилжаа явуулж байгаа бүх ВХҮҮ-д энэ нь хамаарах юм.
- Швейцарт виртуал хөрөнгийн биржүүд бүртгүүлснээр үйл ажиллагаа явуулах бөгөөд Швейцарын Санхүүгийн зах зээлийн хяналтын газар (*FINMA*)-т бүртгүүлж, түүний хяналтад үйл ажиллагаа явуулна. Токен техникийн хувьд блокчейн дэд бүтцэд шилжсэнээр дотоодын мөнгө угаах болон терроризмыг санхүүжүүлэхтэй тэмцэх шаардлагыг дагаж мөрдөхийг шаарддаг. Харин виртуал хөрөнгийн үйлчилгээнд ашиглах мэдээлэл, технологийн дэд бүтцийн тасралтгүй, найдвартай ажиллагаа, нууцлал, аюулгүй байдлыг хангах талаарх виртуал хөрөнгийн биржийн үүргийг хуульчлаагүй байна.

11. Кибер гэмт хэрэг үйлдэх орчин, арга, хэрэгслийн онцлогтой холбоотойгоор уг гэмт хэргийг илрүүлэх, мөрдөн шалгахад цахим нотлох баримт чухал байр суурь эзэлдэг. Эрүүгийн хэрэг хянан шийдвэрлэх ажиллагаа дахь цахим нотлох баримттай ажиллах хүрээнд мэдээллийн технологийн шинэ шийдлүүд бий болж байгаа хэдий ч мэдээллийн технологид суурилсан үйлчилгээ, бүтээгдэхүүнээс хэрэгт ач холбогдол бүхий мэдээлэл олж авах, цуглуулах, бэхжүүлэх ажиллагаа нарийн төвөгтэй болсоор байна. Цахим төхөөрөмжид их хэмжээний мэдээлэл хадгалагдаж буйтай холбоотойгоор хэрэгт ач холбогдолгүй, эсвэл заавал олж авах шаардлагагүй хүний хувийн мэдээллийг (эмзэг мэдээллийг) олж авах, цуглуулах, хадгалалтын горим алдагдаж задруулснаар хүний хувийн халдашгүй байдалд халдах эрсдэлтэй тул мэдээлэлд нэвтрэх шатлал бүхий хамгаалалт тогтоосон зохицуулалт бий болгож байна.

12. Харьцуулсан судалгаанаас дүгнэвэл кибер гэмт хэргийг мөрдөн шалгах ажиллагаанд цахим нотлох баримт олж авахаас гадна цуглуулсан баримтын шинжилгээ нь компьютер, өгөгдлийн сан, сүлжээ болон гар утасны төхөөрөмжийн шинжилгээ гэсэн дөрвөн салбарт хуваагдаж байна. Кибер гэмт хэрэгт холбогдох хэрэгт ач холбогдол бүхий баримт олж авах, цуглуулах, үнэлэх ажиллагаанд тусгай шинжилгээ нь өндөр ач холбогдолтой юм.

13. Цахим нотлох баримт нь эмзэг, хувирамтгай, тархан байршиж, техникийн шинэ шийдлүүдтэй салшгүй холбоотой байх тул энэ төрлийн нотлох баримт олж авах, цуглуулах, хураан авах, хадгалах харилцаанд *ACPO, ADAM* зарчмуудыг баримлахаас гадна *ISO/IEC 27037:2012*

стандартаар цахим нотлох баримтыг таньж тодорхойлох, цуглуулах, олж авах, хадгалахад тавигдах шаардлагыг тодорхойлж байна.

14. Цахим нотлох баримттай ажиллах сайн туршлагыг Олон улсын эрүүгийн цагдаагийн байгууллага (Интерпол) болон Цахим нотлох баримтын шинжлэх ухааны байгууллага (*SWGDE*)-аас гаргасан зарим зөвлөмжүүдээс судалж үзэхэд цахим нотлох баримттай ажиллах дарааллыг журамласан байхаас гадна орчин үеийн технологи буюу цахим төхөөрөмж, хэрэгслийн онцлогоос хамаарч хэрхэн ажиллах талаарх тухайлсан зааварчилгаа, журмыг тодорхойлж байна. Тухайлбал, цахим баримт эрэн хайх, хураан авах ажиллагааг хэргийн газрыг аюулгүй болгох, үнэлгээ хийх, нөхцөл байдлыг баримтжуулах, цахим нотлох баримт цуглуулах, боловсруулах, цахим нотлох баримт хураан авах гэсэн таван алхамд хуваарилжээ. Эдгээр алхмыг Монгол Улсын ерөнхий прокурорын 2021 оны 5 дугаар сарын 20-ны өдрийн А/69 дүгээр тушаалын хавсралтаар батлагдсан Эрүүгийн хэрэгт хөрөнгө, орлого, эд мөрийн баримт, эд зүйлийг хураан авах, бэхжүүлэх, хадгалах, хамгаалах, шилжүүлэх, шийдвэрлэх журмын 7.12 дахь хэсэгт заасан цахим баримт хураан авах, бэхжүүлэх, хадгалах, хамгаалах, шилжүүлэх, шийдвэрлэх ажиллагаатай харьцуулбал үнэлгээ хийх, нөхцөл байдлыг баримтжуулах ажиллагаа журамлагдаагүй байна.

15. Монгол Улсад цахим хэрэгсэл, төхөөрөмж бүрд зориулсан цахим нотлох баримт цуглуулах, олж авах, хадгалах, хураан авахтай холбоотой тусгайлсан журам байхгүй. Цахим нотлох баримтын шинжлэх ухааны байгууллага (*SWGDE*)-аас гаргасан зарим зөвлөмжөөс үзвэл гар утасны төхөөрөмж, компьютер, медиа зэрэг төхөөрөмж, хэрэгслээс хэрэгт ач холбогдол бүхий мэдээлэл олж авах, цуглуулах, хадгалах, шинжлэх, хураан авах сайн туршлагыг удирдамж, зөвлөмжид дэлгэрэнгүй дурджээ.

16. Кибер гэмт хэргийн зохицуулалтын харьцуулсан судалгаанаас үзвэл харьцуулсан судалгаагаар сонгон авсан улс орон бүр өөрийн эрх зүйн тогтолцооны онцлогоос шалтгаалан ялгаатай байдлаар зохицуулж байна. Тухайлбал, Монгол Улс, Швейцар, АНУ, ОХУ, БНЭУ нь Эрүүгийн хуулиар, эсхүл Гэмт хэргийн тухай хуулиар кибер гэмт хэргийг зохицуулж байна. Харин Япон, БНСУ, Хонконг, Сингапурын хувьд Эрүүгийн хуулиас гадна тусгайлсан хуулиар кибер гэмт хэргийг зохицуулж байна. Жишээ нь, БНСУ Эрүүгийн хуулиас гадна Мэдээлэл, харилцаа холбооны сүлжээ ашиглалтыг дэмжих, мэдээллийн аюулгүй байдлыг хангах тухай хууль, Санхүүгийн цахим гүйлгээний тухай хуулиар, харин Сингапур Улс Компьютерыг урвуулан ашиглах тухай хуулиар тус тус зохицуулж байна.

17. Будапештийн конвенцод заасан Зохиогчийн эрх, түүнд хамаарах эрхийн зөрчилд хамаарах гэмт хэргийг Монгол Улс болон харьцуулан судалсан

улс орнуудад (АНУ, БНЭУ-ээс бусад) Эрүүгийн хууль (Гэмт хэргийн тухай хууль)-аар зохицуулсан хэдий ч энэ гэмт хэргийн бүрэлдэхүүнд кибер орчин, цахим сүлжээнд тараасан, түгээсэн үйлдлийг хуульчлаагүй. Иймээс энэ төрлийн гэмт хэргийг кибер гэмт хэрэгт шууд хамааруулах боломжгүй юм.

18. Эрүүгийн хууль болон тусгайлсан бусад хуулиар тодорхойлсон кибер орчинд хууль бусаар халдах гэмт хэрэг нь "мэдээлэлд нэвтрэх зөвшөөрөл олгогдоогүй этгээд" хууль бусаар нэвтрэх үйлдлээр илэрдэг. Харин АНУ-ын Компьютерын залилан ба компьютерыг урвуулан ашиглах тухай хуулийн 1030 дугаар зүйлд мэдээлэлд нэвтрэх зөвшөөрөл олгогдоогүй этгээдээс гадна "нэвтрэх зөвшөөрөлтэй этгээд тухайн зөвшөөрлийг хэтрүүлсэн" буюу эрх мэдлээ хэтрүүлж, цахим мэдээлэлд нэвтэрсэн үйлдэл нь кибер орчинд хууль бусаар халдах гэмт хэргийн нэг бүрэлдэхүүн болдог.

19. Харьцуулсан судалгаанаас үзэхэд виртуал хөрөнгийн бирж кибер халдлагад өртөж, хэрэглэгчийн виртуал хөрөнгө алдагдсан тохиолдолд маргааныг дараах байдлаар шийдвэрлэж байна. Үүнд:
    - Бирж кибер халдлагад өртсөнөө хүлээн зөвшөөрч, хэрэглэгчдийн хохирлыг барагдуулан, шүүхийн бус журмаар асуудлыг шийдвэрлэх;
    - Биржийг хууль, журмаар хүлээсэн үүргээ зөрчсөн гэж эрх бүхий зохицуулагч байгууллага (жишээлбэл, АНУ-д *SEC*), эсхүл шүүхээс үзсэн тохиолдолд хариуцлага хүлээлгэх;
    - Бирж хэрэглэгчийн хохирлыг сайн дураар барагдуулаагүй тохиолдолд хэрэглэгч иргэний шүүхийн журмаар биржээс хохирол нэхэмжлэх;
    - Халдлага үйлдсэн буруутай этгээдүүдийг олж тогтоон, холбогдох гэмт хэрэгт эрүүгийн журмаар ял оноох.

# САНАЛ

Судалгааны нэгдсэн дүгнэлтэд үндэслэн кибер гэмт хэргийн зохицуулалтыг боловсронгуй болгох, тэр дундаа виртуал хөрөнгийн үйлчилгээ үзүүлэгч нь кибер гэмт хэргээс урьдчилан сэргийлэх арга хэмжээ авч хэрэгжүүлэхтэй холбогдуулан дараах хэдэн саналыг гаргаж байна. Үүнд:

1. Кибер орчинд, эсхүл цахим хэрэгсэл ашиглаж бусдын оюуны өмчийг зөрчих гэмт үйлдлээс урьдчилан сэргийлэх, зохиогчийн эрх, түүнд хамаарах эрхийн зөрчилд холбогдох гэмт хэрэгтэй тэмцэх зорилгоор Эрүүгийн хуулийн 18.17 дугаар зүйлд заасан Зохиогчийн эрх болон түүнд хамаарах эрхийг зөрчих гэмт хэргийг “кибер орчинд үйлдсэн”, эсхүл “цахим хэрэгсэл, төхөөрөмж ашиглаж үйлдсэн” бол хүндрүүлэх бүрэлдэхүүнд тооцохоор хуульд нэмэлт, өөрчлөлт оруулах;

2. Кибер гэмт хэргийг үйлдэх орчин, нөхцөл аль ч улсын нутаг дэвсгэрээр хязгаарлагдахгүй тул кибер гэмт хэргийн чиглэлээр олон улсын байгууллага, гадаадын бусад оронтой хамтран ажиллах боломж эрэлхийлэх, гэмт хэргээс урьдчилан сэргийлэх, мөрдөн шалгах ажиллагаанд хамтран оролцох туршлага судалж, Будапештийн конвенцод нэгдэх эсэх асуудлыг авч үзэх;

3. Кибер гэмт хэргээс урьдчилан сэргийлэх ажилд төрийн болон төрийн бус байгууллагын хамтын ажиллагааг дэмжиж буй бусад орны сайн туршлагад үндэслэн кибер гэмт хэргийн халдлага, зөрчлийн талаар цаг алдалгүй мэдээлэл солилцох нийтэд нээлттэй цахим платформ хөгжүүлж, кибер гэмт хэрэгт холбогдох мэдээллийн сан бүрдүүлэх;

4. Монгол Улсад түгээмэл үйлдэгдэж буй нийгмийн сүлжээний хаяг болон цахим шууданд зөвшөөрөлгүй нэвтрэх замаар хохирогчийн хөрөнгийг хууль бусаар олж авах гэмт хэргээс урьдчилан сэргийлэх, тэмцэх зорилгоор хувь хүн өөрийн кибер аюулгүй байдлыг хангах буюу олон нийтийн зориулалттай интернэт, компьютер ашиглахдаа тухайн веб хөтчид мэдээллээ хадгалахгүй байх, нууц үгийн аюулгүй байдлыг хангах суурь мэдлэг эзэмшүүлэх;

5. Дээр дурдсан аргаар үйлдэгдэж буй кибер гэмт хэргээс урьдчилан сэргийлэх үүднээс ВХҮҮ нь хэрэглэгчийг давхар таньж баталгаажуулах систем нэвтрүүлж, хэрэглэгчийн аюулгүй байдлыг хангах, ВХҮҮ-ийн хуулиар хүлээсэн үүргийн биелэлтэд Хороо тогтмол хяналт тавих, үр дүнг нь нийтэд тогтмол мэдээлэх;

6. Виртуал хөрөнгийн биржид хууль бусаар халдсан тохиолдолд ВХҮҮ-ийн хууль тогтоомжоор хүлээсэн үүргээ бүрэн биелүүлсэн эсэх буюу халдлагад буруутай эсэхийг шалган тогтоож, гэм буруугүй тохиолдолд

хариуцлагаас чөлөөлөх зарчмыг тусгасан зохицуулалт бий болгох_ эсхүл ийм төрлийн жишиг тогтоох;

7. Кибер аюулгүй байдлыг хангах, урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах нийтлэг журам яаралтай баталж, хэрэгжилтийг нь зохион байгуулах;

8. Кибер гэмт хэргийг мөрдөн шалгах ажлын хүрээнд цахим нотлох баримттай ажиллах тусгайлсан журам баталж мөрдүүлэх. Уг журамд дараах агуулгыг зайлшгүй тусгах. Үүнд:
   - Цахим нотлох баримт нь хүний хувийн мэдээллийг шууд агуулж байдаг тул хувийн халдашгүй байдалд халдах эрсдэлийн түвшинг тогтоох;
   - Мэдээлэлд нэвтрэх үйл ажиллагаа нь тухайн мэдээллийг хайж олох "зорилгодоо нийцсэн байх" зарчим баримтлах үүргийг журамлах;
   - Цахим нотлох баримттай ажиллах *ACPO, ADAM* зарчмуудыг баримтлах.
9. Эрүүгийн хэрэг хянан шийдвэрлэх ажиллагаанд цахим нотлох баримт олж авах, цуглуулах, хадгалах *ISO/IEC 27031:2012* стандарт нэвтрүүлж, цахим баримттай ажиллах процессыг дагаж мөрдөх;

10. Цахим хэрэгсэл, төхөөрөмжийн онцлогоос шалтгаалан цахим нотлох баримттай ажиллах сайн туршлагыг тодорхойлсон Олон улсын эрүүгийн цагдаагийн байгууллага (Интерпол), Цахим нотлох баримтын шинжлэх ухааны байгууллага (*SWGDE)*-аас гаргасан зөвлөмжийг эрүүгийн хэрэг хянан шийдвэрлэх ажиллагаанд нэвтрүүлэх, мөн компьютерын, сүлжээний, өгөгдлийн сангийн, гар утасны төхөөрөмжид хийгдэх шинжилгээ зэрэг криминалистикийн шинжилгээг төрөлжүүлэн хөгжүүлэх.

*Хавсралт 1. Япон Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн кейс, тэдгээрийг шийдвэрлэсэн шүүхийн шийдвэр*

| **Биржийн нэр:** | ***Mt. Gox*** |
|---|---|
| *Үйл баримт* | 2010 онд Токиод үүсгэн байгуулагдсан дэлхийн томоохон криптобиржүүдийн нэг болох *Mt. Gox* дампуурлаа зарласан. Нийтэд ил болгосон баримтуудаар *Mt. Gox* бирж 2011 оны 6 дугаар сард гэнэтийн кибер халдлагад өртөж тус биржийн арилжаалах биткоины нэрлэсэн үнийг ердөө нэг цент хүртэл бууруулан 2000 *BTC* хулгайлсан. Халдагч этгээд нь *Mt. Gox*-ын ажилтны компьютерыг хакердаж энэ хэргийг гүйцэтгэсэн байна. Бирж хэдхэн минутад алдаагаа засаж, эргээд хэвийн ажиллагаандаа орсон ч 8.75 сая гаруй ам. долларын хохирол амссан. Компанийг дампууралд хөтөлсөн гол халдлага үүний дараа, 2014 онд болж тухайн үеийн ханшаар 460 сая ам. доллартой тэнцэх 850,000 биткоин (хэрэглэгчдийн мэдэлд байсан 750,000, компани буюу өөрсдийн мэдэлд байсан 100,000 биткоин) алдсан. Энэ нь тухайн үед дэлхий дээр байсан нийт биткоины 7%-тай тэнцэх хэмжээний биткоин байсан.[171] Энэ хоёр халдлага нь хоорондоо холбоотой бөгөөд халдагчид нийт гурван жилийн хугацаанд энэ хэмжээний биткоин хулгайлсан байсныг 2014 онд олж тогтоон, компани өөрөө олон нийтэд мэдэгдэл хийсэн.[172] |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | 2015 оны 8 дугаар сард *Mt. Gox*-ын эзэн, Франц Улсын иргэншилтэй Марк Карпелес баривчлагдаж, 2016 оны 6 дугаар сард батлан даалтаар суллагдсан. 2019 оны 3 дугаар сард Япон Улсын Дүүргийн шүүхээс Карпелесыг хууль бус бүртгэл хийсэн гэх үндэслэлээр буруутгасан бөгөөд түүнийг өөртөө ашиг олохын тулд эрх мэдлээ урвуулан ашиглаагүй, шамшигдуулалт хийгээгүй гэж дүгнэсэн. *Mt.Gox* биржийн алдагдсан биткоины ихэнхийг ОХУ-ын иргэншилтэй Александр Винник авсан болох нь тогтоогдсон. Түүнийг 2017 оны 1 дүгээр сард АНУ-ын Хууль зүйн албанаас яллаж, үүнээс зургаан сарын дараа Грект байхад нь *Mt. Gox* биржээс хууль бусаар авсан хөрөнгийг нь оролцуулан нийт 4 тэрбум ам. долларын *BTC-е нэртэй* бирж ажиллуулж, мөнгө угаасан хэргээр баривчилсан. Биткоины аюулгүй байдлын мэргэжилтнүүдийн нэгдэл болох *WizSec*-ээс мэдээлснээр *Mt. Gox* биржийн хэтэвчнээс хулгайлагдсан биткоинуудыг Винник өөрийн *BTC*-е нэртэй бирж дэх хэтэвчдээ шилжүүлж худалдсан байна. Винник хоёр жил гаруй хугацаанд Грект саатуулагдан шалгуулж, түүний дараа АНУ, ОХУ болон Францад шилжин шалгагдсан. 2020 оны 1 дүгээр сарын 24-ний өдөр Франц Улс түүнийг шилжүүлэн авч, луйвар, мөнгө угаах, хуйвалдаан явуулах болон автомат дата ашиглан системд халдсан үргэлжилсэн үйлдлээр нь буруутгаж яллаасан.[173] |

[171] Reuters, “Mt. Gox files for bankruptcy, hit with lawsuit”, 2014.02.28, (https://reut.rs/3QzNx4y), нэвтэрсэн 2022.06.10.

[172] Magazine by COINTELEGRAPH, “Report on Crypto Exchange Hacks 2011-2020”, (https://bit.ly/39Ohb5E), нэвтэрсэн огноо: 2022.06.12.

[173] September, 2020, Cyber defense Report, Japan’s National Cybersecurity and Defense Posture, Policy and Organization, p.5, (https://bit.ly/3zLRtsX)

| ***Биржийн нэр:*** | ***Coincheck*** |
|---|---|
| *Үйл баримт* | Япон Улсын тэргүүлэгч криптобиржийн үйлчилгээ үзүүлэгчдийн нэг *Coincheck* 2018 оны 1 дүгээр сарын 26-ны өдөр кибер халдлагад өртөж, нийт 260,000 хэрэглэгчийн хэтэвчнээс 54.7 тэрбум иенээр үнэлэгдэх *NEM* тикертэй токен алдсан. Тус кибер халдлагыг үл мэдэгдэх хакер *Coincheck*-ийн ажилтнуудын дотоод сүлжээнд холбогдсон хувийн компьютерт нэвтрэн, хортой программ тарааж үйлдсэн. Энэ нь 2014 онд болсон *Mt. Gox*-ын дараах, хоёр дахь өндөр дүнтэй халдлага болсон юм. Энэ төрлийн халдлага гарсан нь *Coincheck*-ийн аюулгүй байдлын систем сул байсантай холбоотой бөгөөд тодруулбал, хэрэглэгчийн хөрөнгийг удирдахдаа интернэт салгаж, *"cold wallet"* ашиглаж байгаагүй нь халдлага үйлдэх хамгийн том сул тал болсон гэж үзсэн. |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | 2018 оны 1 дүгээр сарын 27-ны өдөр *Coincheck* хэрэглэгчдийнхээ хохирлыг нөхөн төлөхөө мэдэгдэж, 2018 оны 3 дугаар сарын 12-ны өдөр *NEM* токен хэрэглэгчдэд 46 тэрбум иен төлсөн.<br><br>Энэ хэргийг Токио хотын Цагдаагийн газраас кибер гэмт хэргээр мэргэшсэн 100 орчим тусгай мэргэжилтэн оролцуулан мөрдөж, хоёр сэжигтэн илрүүлсэн бөгөөд тэдгээрийн эрүүгийн хэрэг хянан шийдвэрлэх ажиллагаа үргэлжилж байна. Сэжигтнүүд *Coincheck*-т халдлага гарсан болон түүнээс хойших хугацаанд их хэмжээний *NEM* токеныг бага үнээр, өөр криптовалют болон иенээр арилжих замаар олон тэрбум иений ашиг олсон болох нь тогтоогдсон. Хэрэг шалгах ажиллагааны явцад Токио хотын шүүхээс тус хотын Цагдаагийн газрын хүсэлтээр дээрх сэжигтний нэгнийх нь хэтэвчийг царцаах шийдвэрийг 2020 оны 3 дугаар сарын 30-ны өдөр гаргасан. Энэ нь Япон Улсад Зохион байгуулалттай гэмт хэргийн ял шийтгэлийн тухай хуулийн дагуу анх удаа шүүх хурлаас өмнө гэмт хэрэг үйлдэж олсон хөрөнгийг хураах буюу урьдчилсан хамгаалалтын арга хэмжээ авсан хэрэг болсон. Сэжигтнүүдийг Зохион байгуулалттай гэмт хэргийн ял шийтгэлийн тухай хууль зөрчсөн гэх үндэслэлээр буруутгасан.<br><br>*Coincheck*-ийн халдлагын дараа Япон Улсын Засгийн газар болон санхүүгийн зохицуулагч байгууллагаас криптовалютын биржүүд болон тэдгээрийн аюулгүй байдлын протоколд холбогдох зохицуулалтыг сайжруулах шаардлагатай болсон. Халдлага болох үед Япон Улсад криптовалютын биржийн үйлчилгээ эрхлэгч болон криптовалюттай холбоотой зохицуулалт нэмж оруулсан Төлбөрийн үйлчилгээний тухай хуулийн нэмэлт өөрчлөлт 2017 оны 4 дүгээр сараас эхлэн хэрэгжиж байсан бөгөөд уг хуулийн шилжилтийн үеийн зохицуулалт үйлчилж байсан. |

| | |
|---|---|
| | Японы Санхүүгийн үйлчилгээний агентлагаас халдлагын дараа буюу 2018 оны 2 дугаар сарын 2-ны өдөр *Coincheck*-т газар дээр нь шалгалт хийж, удирдлагын систем болон стратегийн хувьд бүтцээ шинэчлэх, бизнесийн зохистой үйл ажиллагаа явуулах шаардлагууд тавьсан.<br><br>Мөн бусад криптовалютын биржийн үйлчилгээ үзүүлэгчид өөрсдийн эрсдэлийн удирдлагын системийн талаарх тайлангаа Санхүүгийн үйлчилгээний агентлагт хүргүүлж байх шийдвэрийг 2018 оны 2 дугаар сарын 2-ны өдөр гаргасан.<br><br>*Coincheck*-ийн халдлагын улмаас алдсан крипто хөрөнгөө буцаан авах, ханшийн зөрүүнээс үүссэн алдагдлаа нэхэмжилсэн 200 орчим хэрэглэгч иргэний шүүхэд нэхэмжлэл гаргасан байна. Эдгээр нэхэмжлэлийн үндэслэл нь *NEM* токены ханш халдлагад өртөх үе болон *Coincheck*-ээс нөхөн төлсөн үе хоёрын хооронд унасан, мөн халдлага болсны дараа хэсэг хугацаанд бирж дээрх арилжааг зогсоосны үр дагаварт алдагдал хүлээж, хохирол учирсан гэж маргасан. Мөн *Coincheck* биржээс Санхүүгийн үйлчилгээний агентлагт гаргаж өгсөн тайланд дурдсаны дагуу *Coincheck* биржийг нэхэмжлэгчдийн виртуал хөрөнгийг найдвартай хадгалах үүргээ зөрчсөн буруутай гэж маргасан ч энэ маргаанд холбогдох нэхэмжлэлийг Токио хотын Дээд шүүхээс хэрэгсэхгүй болгож шийдвэрлэсэн байна. Хохирол нэхэмжилсэн бусад нэхэмжлэлийг шийдвэрлэхэд хоёр жил гаруй хугацаа өнгөрсөн, мөн *Coincheck* бирж энэ үйлдэлд шууд буруутай гэж шүүхээс шийдвэрлээгүй тул шүүх нэхэмжлэлийг хангахгүй орхих магадлалтай гэж судлаачид үзэж байна.[174] |

[174] Global Report 2021, International Developments and Perspectives on the field of Fraud, Financial Crime and Asset Recovery, pp. 93-96. (https://bit.ly/39HxzFa)

*Хавсралт 2. Сингапур Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн кейс, тэдгээрийг шийдвэрлэсэн шүүхийн шийдвэр*

| ***Биржийн нэр:*** | ***KuCoin*** |
|---|---|
| *Үйл баримт* | 2020 оны 9 дүгээр сард Сингапурт төвтэй *KuCoin* криптобирж халдлагад өртөж, *1,008 BTC, 11,543 ETH, 19,834,042 USDT-ETH, 18,495,798 XRP, 26,733 LTC, 999,160 USDT, 147 сая ERC-20 токен, 87 сая Stellar токен* зэрэг 275 сая ам. долларoос их хэмжээний крипто хөрөнгийг хэтэвчнээс алдсан.[175] Тухайлбал, *KuCoin*-ы *Ethereum* хэтэвчнээс 150 сая гаруй ам. долларын үнэ бүхий *Ethereum* дээр суурилсан жетон шилжүүлсэн болохыг Этэрскан[176]-ын мэдээлэл харуулж байна. Хакерууд интернэтэд холбогдсон (*hot*) хэтэвчүүдийн хувийн нууц үгийг олж аван, крипто хөрөнгүүдийг нь хууль бусаар авсан. Биржээс халдлагад өртсөн хэрэглэгчдийн хохирлыг *KuCoin* болон даатгалын сангаас нөхөн төлөх талаараа мэдэгдсэн.[177]<br><br>Олон улсын блокчейн шинжилгээний *Chainalysis* компани “Хакерууд энэхүү халдлагыг үйлдэхдээ *DeFi* протоколууд буюу ухаалаг гэрээ (*smart contract*)-гээр баталгаажуулсан блокчейн дээр суурилсан төвлөрсөн бус программууд (*dApps*) ашигласан. Эдгээр программ нь ухаалаг гэрээгээр зохицуулагддаг, тодорхой нөхцөл хангагдсан үед арилжаа, зээл гэх мэт гүйлгээг автоматаар гүйцэтгэдэг тул хакерууд *Uniswap, Kyber* зэрэг төвлөрсөн бус бирж гэдгээр нь мэдэх *dApp*-г ашиглаж халдлага үйлдсэн” гэж мэдэгдсэн. Учир нь эдгээр платформ нь стандарт бирж шиг харилцагчийг таньж мэдэх ажиллагаа (*KYC*) хийдэггүй, захиалгын дэвтэрт арилжааны мэдээллийг заавал өгөхгүйгээр валютын своп хийж болдог. |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | Хулгайлагдсан коинуудын 84%-ийг олж авсан бол 16%-тай тэнцэх хэсгийг *KuCoin*-ы даатгалаас нөхөн төлсөн ба хэрэглэгчдийн хохирол бүрэн төлөгдсөн талаар компанийн захирал ярилцлагадаа дурдсан.[178] |

[175] https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap/
[176] https://etherscan.io/address/eb31973e0febf3e3d7058234a5ebbae1ab4b8c23
[177] https://www.kucoin.com/news/en-kucoin-security-incident-update
[178] https://news.bitcoin.com/kucoin-boss-on-strategy-after-hack-we-chose-to-act/

| **Биржийн нэр:** | **Exodus & BRD** |
|---|---|
| Үйл баримт | Нэхэмжлэгч АНУ-ын иргэн 2021 оны 1 дүгээр сарын 8-нд өөрийнх нь хоёр бирж дээрх интернэтэд холбогдсон *hot* хэтэвчнээс *109.83 BTC, 1497.54 ETH* хулгайлагдсаныг мэдсэн. 2021 оны 1 дүгээр сарын 7-ны өдөр нэхэмжлэгч найз нартайгаа амралтын газар байсан бөгөөд мөнгө хэрэгтэй болж, нэг найзтайгаа хамт байхдаа хэтэвчнээсээ зарлага гаргахдаа нууц үгээ хэлсэн. Хэтэвчүүд нь нууц үгээр хамгаалагдсан байсан бөгөөд дээрх үйлдлийн үед нууц үгийг хэн нэгэн этгээд олж авсан байх боломжтой. Нэхэмжлэгчийн хэтэвчнээс гурван өөр хэтэвч рүү гүйлгээ хийгдсэн.<br><br>Нэхэмжлэгч хулгайлагдсан виртуал хөрөнгөтэйгөө холбоотой дээрх үйлдлийг шалгуулахаар шүүхэд хандсан бөгөөд нэг дэх хариуцагч нь хулгайлсан этгээд (хэн гэдэг нь тодорхойгүй), хоёр дахь хариуцагч нь Кайманы арлуудад бүртгэлтэй *Exodus* бирж, гурав дахь хариуцагч нь Сейшелийн арлуудад бүртгэлтэй *BRD* бирж байв. Дээрх хоёр бирж нь Сингапурт үйл ажиллагаа явуулдаг.<br><br>Хэрэг хянан шийдвэрлэх ажиллагааны явцад хулгайлагдсан виртуал хөрөнгийнх нь зарим хэсгийг өөр виртуал хөрөнгийн бирж болон дижитал төлбөрийн үйлчилгээ үзүүлэгч компанид шилжүүлсэн болохыг нэхэмжлэгч мэдсэн тул дөрөв дэх хариуцагчаар АНУ-ын *CQB* криптобиржийг, тав дахь хариуцагчаар АНУ-ын *CQC* санхүүгийн болон дижитал төлбөрийн үйлчилгээ үзүүлдэг компаниудыг нэмэлтээр оруулах хүсэлт гаргасан. |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | Сингапурын Дээд шүүхээс энэ хэргийг дараах байдлаар шийдсэн:[179]<br>– Их Британи, Малайз шиг манай шүүхийн дүрэмд *(Cap 322, R5, 2014 Rev Ed)* хариуцагчийг тусгайлан нэрлэн заасан байхыг шаарддаггүй. Иймд нэхэмжлэгчийн хэтэвчид халдсан этгээд хэдий тодорхойгүй ч 2021 оны 1 дүгээр сарын 8-ны өдөр нэхэмжлэгчийн хэтэвчнээс крипто хөрөнгийг хулгайлсан, түүнд оролцсон, эсхүл тусалсан аливаа хүн, эсхүл хуулийн этгээд байсан бол тэр этгээд хариуцагч болох боломжтой.<br>– Шүүх Сингапурын Олон улсын худалдааны шүүхийн шийдсэн *B2C2 Ltd v Quoine Pte Ltd* болон Шинэ Зеландын шүүхийн *Ruscoe v Cryptopia Ltd* хоорондын маргааны шийдвэрийг иш татан виртуал хөрөнгө бол өөрийн гэсэн үнэ цэнтэй, эдийн бус хөрөнгөд хамаарахыг онцлоод виртуал хөрөнгө нь өмчийн эрхээр хамгаалагдах дөрвөн шаардлага хангана гэж үзсэн. Иймд нэг дэх хариуцагч болох хулгайлсан этгээдийн эсрэг хулгайлагдсан виртуал хөрөнгөтэй харьцах, захиран зарцуулах, үнэ цэнийг нь бууруулахыг хориглосон шийдвэр гаргасан.<br>– Мөн нэг дэх хариуцагчийн эсрэг дэлхий даяар хөрөнгө битүүмжлэх шийдвэр гаргасан.<br>– Гурав болон дөрөв дэх хариуцагчийн эсрэг нэхэмжлэгчийн хэтэвчнээс шилжсэн гүйлгээнүүдтэй холбоотой хэтэвчүүдийн өмчлөгчийн мэдээллийг ил болгох шийдвэр гаргасан. |

[179] In the General division of The High court of The Republic Of Singapore [2022] SGHC 46, https://www.elitigation.sg/gd/s/2022_SGHC_46

*Хавсралт 2-ын үргэлжлэл*

| **Биржийн нэр:** | **DragonEx** |
|---|---|
| *Үйл баримт* | Сингапурын *DragonEx* крипто хөрөнгийн бирж 2019 оны 3 дугаар сард халдлагад өртөж, 7.09 сая ам. долларын үнэлгээ бүхий виртуал хөрөнгө хулгайлагдсан. Хулгайлагдсан хөрөнгөд 135 биткоин, 2738.12 *ETH*, 247,000 *XRP*, 1,464,319.32 *USDT* болон бусад хөрөнгө байсан ба энэхүү халдлагыг Хойд Солонгосын Лазарус бүлэг (*Lazarus group*) үйлдсэн гэж үзэж байгаа.<br><br>Учир нь хакерууд биржийн ажилтнуудыг онилсон бөгөөд *wb-invest.net, wb-bot.org* гэх домайн нэрсээр хортой программыг халхавчлан хэдэн сарын турш хэвийн үйл ажиллагаа явуулсан. *DragonEx*-ийг хакердсан хэргийн мөрдөн байцаалтад тусалж байсан Хятад дахь төв оффисын ажилтан *JohnWick*-ийн мэдээлснээр *DragonEx*-ийн харилцагчийн үйлчилгээний ажилтнуудын нэг нь нэрээ нууцалсан илгээгчээс илгээсэн *wbbot.dmg* хэмээх *install*-ыг нээсэн. Ийнхүү нээхэд хакерууд хэтэвчийн нууц түлхүүрүүдийг олж авсан гэжээ. |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | ДрагонХ 1 драгон бонд (*Dragon bond*) 1 *USD*-той тэнцүү буюу 1:1 харьцаатай, 7 сая ам. долларын үнэлгээ бүхий драгон бонд гаргасан. Хэрэглэгчийн хэтэвчнээс хулгайлагдсан нийт хөрөнгийн 10%-тай тэнцэх хохирлыг анхны валютаар, үлдэх 90%-ыг драгон бондоор нөхөн төлөхөөр болсон.[180] |

*Хавсралт 3. Хонконгийн кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн кейс, тэдгээрийг шийдвэрлэсэн шүүхийн шийдвэр*

| **Биржийн нэр:** | ***Bitfinex*** |
|---|---|
| Үйл баримт | 2016 онд Хонконгийн *Bitfinex* биржээс 119,754 биткоин буюу тухайн үеийн үнэлгээгээр 72 сая ам. доллароор үнэлэгдэх виртуал хөрөнгийг хакерууд хууль бусаар авсан. Хакерууд нийт 2000 хууль бус гүйлгээгээр дамжуулан дээрх хөрөнгийг өөрсдийн хэтэвчид авсан бөгөөд тухайн үед биткоины ханш 20%-аар унасан. Энэхүү халдлагыг 34 настай Илая Личштэйн, түүний эхнэр 31 настай Хитэр Морган нар үйлдсэн бөгөөд 2020 оны 2 дугаар сарын 8-ны өдөр тэднийг Манхэттэн дэх гэртээ байхад нь баривчилсан талаар АНУ-ын Хууль зүйн яам мэдээлсэн.[181] Тэдний 2016 онд хулгайлсан крипто хөрөнгийн ханш одоо ойролцоогоор 4.5 тэрбум ам. долларт хүрсэн. 2016 оноос хойш сүүлийн таван жилийн хугацаанд хулгайлсан биткоиноос ойролцоогоор 25,000 биткоиныг Личштэйн, Морган нарын хяналтад байдаг санхүүгийн дансуудаар мөнгө угаах үйл явцаар дамжуулан хэтэвчнээс гарган авсан. |

[180] https://tokenpost.com/Crypto-exchange-DragonEx-lost-7M-in-hack-announces-compensation-plan-1568

[181] https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency, хандсан огноо: 2022.04.14.

| | |
|---|---|
| Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт | Хулгайлсан биткоины үлдэгдэл 94,636 биткоин болох одоогийн үнэлгээгээр 3.629 тэрбум ам. доллартой тэнцэх виртуал хөрөнгө Личштэйний хэтэвчид байсныг АНУ-ын Засгийн газраас битүүмжлэн, хурааж авсан байна. Личштэйн, Морган нарыг дараах гэмт хэрэгт буруутган, яллах дүгнэлт үйлдсэн.[182] Үүнд:<br>– 18 U.S.C § 1956(*h*)-г зөрчин хууль бус үйл ажиллагаа явуулж санхүүгийн гүйлгээ хийсэн, хууль бус үйл ажиллагаанаас олсон хөрөнгө гэдгийг мэдсээр байж хөрөнгийн гарал үүсэл, байршил, эзэмшигчийг нуух, далдлах зэргээр үгсэн хуйвалдсан, санхүүгийн хууль бус гүйлгээ хийхээр завдсан, хууль бус үйл ажиллагааг удирдсан (олон удаагийн үйлдлээр крипто хөрөнгө угаасан). Дээрх үйлдлийг үйлдэхдээ 18 *U.S.C* § 1343-ыг зөрчиж утас, холбооны хэрэгсэл ашигласан, 18 *U.S.C*. § 1030-ыг зөрчиж компьютер ашигласан болон 18 U.S.C. §371-ийг зөрчиж үгсэн хуйвалдаж гэмт хэрэг үйлдсэн, АНУ-ыг залилан мэхэлсэн гэх гэмт хэрэг.<br>АНУ-д санхүүгийн хууль бус гүйлгээ хийх, мөнгө угаах гэмт хэргийг бүлэглэн үйлдсэн үйлдэлд 20 жил хүртэл хугацаагаар хорих ял, залилан мэхлэх гэмт хэргийг бүлэглэн үйлдсэн бол 5 жил хүртэл хорих ялтай байдаг.[183] 2022 оны 3 дугаар сард Вашингтон DC-д байрлах дүүргийн шүүхэд болсон шүүхийн сонсгол прокурорууудаас гаргасан яллах тогтоолыг хэлэлцэх хүсэлтээр 2022 оны 5 дугаар 4-ний өдөр хүртэл 40 хоногоор хойшилсон. |

| **Биржийн нэр:** | ***Bitfinex & Tether*** |
|---|---|
| Үйл баримт | Нью-Йорк мужийн Ерөнхий прокурорын[184] *Bitfinex* болон *Tether* крипто хөрөнгийн биржүүдийг санхүүгийн буруу менежмент хэрэгжүүлсэн, нөөцөө хэтрүүлэн үнэлж, харилцагч болон зах зээлийг хуурсан, 850 сая ам. долларын алдагдлаа нуун дарагдуулахыг оролдсон гэх үндэслэлээр буруутгасан. Тодруулбал:<br>– Bitfinex болон Tether нь харилцан хамааралтай этгээдүүд (Гүйцэтгэх удирдлага болон хувьцаа эзэмшигчээр хамааралтай) бөгөөд 2017 оны 6-9 дүгээр сарын хооронд Нью-Йоркт байрлах Нобл банканд нээлгэсэн Bitfinex дансаар Tether-ийн орлогыг дамжуулж байсан нь тогтоогдсон бөгөөд энэ нь Bitfinex болон Tether нь зах зээлийг хуурсан гэж үзэх үндэслэл болсон.<br>– 2017-2018 онд Bitfinex бирж хэрэглэгчийн орлого, зарлагын гүйлгээ, төлбөр тооцоог гуравдагч этгээд Криптокапитал корпорацаар гүйцэтгүүлэхээр болсон ба Криптокапитал Bitfinex бирж рүү хэрэглэгч орлого хийхэд зарцуулах 1 тэрбум ам. долларын хөрөнгө эзэмших болсон. Гэтэл 2018 оны дундуур Криптокапиталын банкны дансанд 340 сая ам. долларын битүүмжийг Польшийн Засгийн газраас хийсэн. |

[182] https://www.justice.gov/usao-dc/press-release/file/1470221/download

[183] https://www.cnbc.com/2022/02/08/feds-seize-3point6-billion-stolen-from-bitfinex-hack.html, хандсан огноо: 2022.04.14.

[184] General Attorney.

| | |
|---|---|
| | Криптокапиталын зүгээс энэхүү үйлдлийг түр зуурын гэж хэлж байсан ч 2018 оны 7 дугаар сард Криптокапиталын данс дахь *Bitfinex* биржийн хэрэглэгчдийн 500 сая ам. доллартой тэнцэх хэмжээний мөнгийг мөн битүүмжилсэн. Энэ нь *Bitfinex*-ийн хэрэглэгчдийн орлогын 80 хувьтай тэнцэх мөнгө байсан тул *Bitfinex* түр зуурын хөрвөх чадварын эрсдэлд орсон. Улмаар *Tether*-ээс 400 сая ам. доллар зээлж, буцаан төлсөн. Гэвч дээрх гүйлгээнүүдийг нарийвчлан тайлагнаагүйн дээр 2018 оны 10 дугаар сарын 7-ны өдөр "Төлбөрийн чадваргүй болоогүй, зарим нэг хүндрэлүүд гарсан ч орлого, зарлагын гүйлгээ хэвийн байгаа" гэх мэдэгдэл нь зах зээлийг төөрөгдүүлж, бодит байдлыг гуйвуулсан. Учир нь энэхүү мэдэгдлийг хийхдээ Криптокапиталаас мөнгөө буцаан авах хүсэлтийг удаа дараа гаргасан ч нөгөө тал боломжгүй байсан. Улмаар Криптокапитал 850 сая ам. долларын алдагдлаа төлүүлж чадаагүй, *Tether*-ээс 625 сая ам. доллар зээлж, төлбөр гүйцэтгэж байсан хэдий ч 2019 оны 4 дүгээр сард Криптокапиталын дансанд байгаа мөнгө алдагдаагүй, аюулгүй байгаа гэх мэдэгдлийг дахин хийсэн. Энэ нь алдагдлаа нуун дарагдуулж, хэрэглэгч, зах зээлийг хууран мэхэлж, мөн *Tether*-ээс зээл авсан талаар ямар нэг тайланд тусгаагүй, энэ хугацаанд *Tether* болон *Bitfinex* нь аудит оруулсан ч аудитын дүгнэлтийг бүрэн тайлагнаагүй зэрэг үйлдэл гаргасан.<br><br>Дээрх үйлдлүүд гарах үе буюу 2018 оны эхнээс дунд үе хүртэл *Bitfinex* болон *Tether*-ийн гүйцэтгэх албан тушаалтнууд Нью-Йорк хотод амьдарч, ажиллаж байсан тул энэ хэргийг Нью-Йоркийн Ерөнхий прокурор шалгасан байна. |
| Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт | Нью-Йорк мужийн Ерөнхий прокурор Нью-Йоркийн Бизнесийн ерөнхий хуулийн[185] 352 дугаар зүйл, Гүйцэтгэх хуулийн[86] 63.12 дахь хэсэгт заасан эрхийн хүрээнд хийсэн мөрдөн шалгалтын дүнд үндэслэн 2021 оны 2 дугаар сарын 18-ны өдөр хариуцагч *Bitfinex* болон *Tether*-тэй Эвлэрлийн гэрээ[187] байгуулсан. Энэхүү гэрээгээр дараах үүргийг *Bitfinex*, *Tether* хоёр хүлээсэн. Үүнд:<br>– Дээрх хууль зөрчсөн үйлдэлдээ 18,500,000 ам. долларын торгуулийг гэрээ хүчин төгөлдөр болсноос хойш 5 хоногийн дотор Нью-Йорк мужид төлөх;<br>– Төлсөн торгуультай холбоотойгоор аливаа гомдол, нэхэмжлэл гаргахгүй, татварын маргаан үүсгэхгүй байх;<br>– Нью-Йорк мужид виртуал хөрөнгийн биржийн үйл ажиллагаа явуулж буй хүн, хуулийн этгээдэд хориглосон аливаа үйлдэл гаргахгүй байж, дотоод хяналт, үйл ажиллагаагаа сайжруулах; |

[185] New York General Business Law.

[186] Executive Law.

[187] Settlement Agreement. https://ag.ny.gov/sites/default/files/2021.02.17_-_settlement_agreement_-_execution_version.b-t_signed-c2_oag_signed.pdf, хандсан огноо: 2022.04.15.

| | |
|---|---|
| | – Хариуцагчид нь гэрээ хүчин төгөлдөр болсноос хойш хоёр жилийн хугацаанд улирал бүр дансны хуулга болон гэрээнд зөрчилтэй гэж үзсэн гүйлгээний мэдээллийг илгээнэ. Иймхүү илгээхдээ *Bitfinex* болон *Tether* нь харилцах дансныхаа аливаа гүйлгээг тусад нь бүртгэх ба гүйлгээ, орлогыг хооронд нь холихгүй байх;<br>– Гэрээ хүчин төгөлдөр болсноос хойш хоёр жилийн хугацаанд улирал бүр *Tether* нөөцийн (бэлэн мөнгө, зээл, үнэт цаас гэх мэт) мэдээллээ тайлагнах;<br>– Дээрх хугацаанд орлого, зарлагын төлбөр тооцооны үйлчилгээг гуравдагч этгээдээр гүйцэтгүүлэх бол тухайн этгээдийн хаяг, холбоо барих мэдээлэл, тухайн компанийг сонгохдоо нэмэлтээр хяналт шалгалт (*due diligence*) хийсэн эсэх мэдээллийг Ерөнхий прокурорт ирүүлэх;<br>– Цаашид Нью-Йорк мужид үйл ажиллагаа явуулахдаа хууль тогтоомжийг мөрдөж, холбогдох зөвшөөрөлд заасан шаардлагуудыг хангаж ажиллах;<br>– *Bitfinex болон Tether* нь энэхүү гэрээ болон Ерөнхий прокурорын хяналт шалгалтыг шууд болон шууд бусаар эсэргүүцэж, олон нийтэд чиглэсэн аливаа мэдэгдэл, үйл ажиллагаа хийхгүй болно. |

*Хавсралт 4. Америкийн Нэгдсэн Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн кейс, тэдгээрийг шийдвэрлэсэн шүүхийн шийдвэр*

| ***Биржийн нэр*** | ***Binance*** |
|---|---|
| *Үйл баримт* | ОХУ-ын иргэн Данел Потекин, Дмитрий Красавиди нар (“шүүгдэгчид”) интернэтийн сүлжээ ашиглан *Poloniex, Binance, Gemini* крипто хөрөнгийн биржүүдийн хэрэглэгчид рүү чиглэсэн боловсронгуй фишинг (*phishing*) хийсэн. Ингэхдээ тэд *Poloniex, Binance, Gemini* гэх албан ёсны биржийн сайт шиг харагддаг хуурамч веб сайт худалдан авч байршуулсан бөгөөд хэрэглэгчид эдгээр хуурамч веб сайт руу нэвтрэхэд нь тэдний имэйл хаяг, нууц үгийг хулгайлан, тухайн имэйл хаяг, нууц үгийг ашиглан жинхэнэ биржийн сайт руу нэвтэрч хэрэглэгчийн хэтэвч дэх виртуал хөрөнгийг бүхэлд нь, эсхүл зарим хэсгийг нь зарлага хийн гарган авсан. Шүүгдэгчид гэмт хэргийг 2017 онд үйлдсэн бөгөөд 2017 оны 7 дугаар сарын 17-ны өдрөөс 10 дугаар сарын 29-ний хооронд *Poloniex* бирж дээр 13 хуурамч домайн хаяг ашиглаж, хамгийн багадаа 158 хохирогч (хэрэглэгч)-ийн нэвтрэх нэр, нууц үгийг хулгайлан, тэдгээрийн бүртгэлээр бирж рүү нэвтэрсэн. Шүүгчдэгчид нь 2017 оны 8 дугаар сарын 3-ны өдрөөс 9 дүгээр сарын 27-ны өдрийн хооронд *Poloniex* биржийн 155 хэрэглэгчийн хэтэвчнээс ойролцоогоор 700,000 ам. долларын үнэ бүхий биткоиныг зарлагадаж авсан. Ингэхдээ *Bittrex* бирж дээр зохиомлоор нээсэн таван хэтэвчээр дамжуулан 435 BTC, 8,816 *ETH* зарлагадсан.<br>– 2017 оны 10 дугаар сарын 16-наас 31-ний өдрийн хооронд шүүгдэгчид дээрх аргаар Binance биржийн 142 хэрэглэгчээс ойролцоогоор 566 *BTC* буюу 10 сая ам. доллартой тэнцэх хэмжээний виртуал хөрөнгө хулгайлсан. |

| | |
|---|---|
| | – 2017 оны 10 дугаар сарын 24-ны өдрөөс 11 дүгээр сарын 1-ний өдрийн хоронд *Gemini* бирж дээр дээрх аргаар 45 хэрэглэгчийн хэтэвчид халдаж, ойролцоогоор 1.176 сая ам. доллартой тэнцэх хэмжээний виртуал хөрөнгө хулгайлсан.<br><br>Шүүгчдэгчид нь хохирогчдын хэтэвчид хууль бусаар халдаж, виртуал хөрөнгийг нь хулгайлахаас гадна биржүүд дээр манипуляц (үнэ ханшийг зохиомлоор тогтоох, хуурамч арилжаа хийх) хийж (Калифорнийн хойд мужийн хэрэглэгчдэд) хамгийн багадаа 16,876,000 ам. долларын хохирол учруулсан. |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | АНУ-ын дүүргийн шүүх, Калифорнийн хойд дүүрэг, Сан-Франциско дахь шүүхээс шүүгчдэгчдийг мэдсээр байж, санаатайгаар, хуйвалдан гэмт хэрэг үйлдсэн гэж үзэж, дараах үйлдэлд буруутган, яллах дүгнэлт үйлдсэн:[188]<br>– Залилах, хууран мэхлэх замаар *Poloniex, Binance, Gemini* биржийн хэрэглэгчдийн нэвтрэх нэр, нууц үгийг инженерийн техник ашиглан олж авсан;<br>– Хууль бус аргаар олж авсан мэдээллийг ашиглаж биржүүдийн бүртгэлтэй хаягаар нэвтэрч, залилан мэхлэх гэмт хэргийн схем бий болгосон;<br>– Хэрэглэгчдийн хэтэвч дэх виртуал хөрөнгүүдийг хэрэглэгчийн зөвшөөрөлгүйгээр шилжүүлсэн;<br>– Зөвшөөрөлгүйгээр хэрэглэгчийн бүртгэлээр нэвтэрсэн байхдаа виртуал хөрөнгийн зах зээлд давуу байдал олж авах зорилгоор, арилжааг урвуулан ашигласан (манипуляц хийсэн);<br>– Виртуал хөрөнгийн хэд хэдэн хэтэвч ашиглаж, виртуал хөрөнгийн эх үүсвэр, байршил, эзэмшигчийг өөрчлөх замаар тэдгээрийг зарлагадсан.<br><br>Яллах дүгнэлт үйлдэхдээ АНУ-ын Холбооны хуулийн 18-р хэсэг, Компьютерын залилан ба компьютерыг урвуулан ашиглах тухай хуулийн §1030 (b)-д заасныг зөрчсөн (10 жил хүртэл хорих ял, 3 жил биечлэн эдлэх, 250,000 ам. долларын торгууль, эсхүл олсон ашгийг дахин нугалж хохирлыг нөхөн төлүүлэх), мөн хуулийн §1030 (a)(4), 1030 (c)(3)(A)-д заасан үнэ цэн бүхий зүйл олж авахын тулд хамгаалалттай компьютерт зөвшөөрөлгүй халдсан (5 жил хүртэл хорих ял, 3 жил биечлэн, 250,000 ам. долларын торгууль, эсхүл олсон ашгийг дахин нугалж, хохирлыг нөхөн төлүүлэх), §1349-д заасныг зөрчиж сүлжээ ашиглан залилан үйлдсэн (20 жил хүртэл хорих, 3 жил биечлэн, 250,000 ам. долларын торгууль, эсхүл олсон ашгийг дахин нугалж хохирлыг нөхөн төлүүлэх), §1028 (a)(1)-д зааснаар хулгайн гэмт хэргийг хүндрүүлэх бүрэлдэхүүнтэйгээр бүлэглэн үйлдсэн (2 жил хорих, 3 жил биечлэн, 250,000 ам. долларын торгууль, эсхүл олсон ашгийг дахин нугалж хохирлыг нөхөн төлүүлэх), §1956 (h)-д заасан мөнгө угаах гэмт хэрэг үйлдсэн хэмээн буруутган ял шийтгэж, §982 (a)(2)(B), §1030 (i), (j), §981 (a)(1)(C), АНУ-ын Холбооны хуулийн 28-р хэсэг, §2461 (c)-д зааснаар хөрөнгийг нь хураахаар шийдвэрлэсэн. |

[188] https://www.justice.gov/usao-ndca/press-release/file/1317276/download United States District Court for the Northern District of California, Case No. CR-19-0572-CRB

| ***Биржийн нэр*** | ***Cryptsy*** |
|---|---|
| *Үйл баримт* | *Cryptsy* крипто хөрөнгийн биржийн гүйцэтгэх захирал Паул Вернон 2013 оны 5 дугаар сараас 2015 оны 5 дугаар сар хүртэл өөрийн эрх мэдлийг ашиглан, *Cryptsy* дэх хэтэвчүүдээс нийт 1 сая ам .доллар хулгайлсан. Тэрээр хулгайлсан виртуал хөрөнгүүдийг өөрийн хэтэвчид шилжүүлэн авч, улмаар өөрийн банкны дансанд авсан. Вернон энэхүү үйлдлээ нуусан бөгөөд 2014 оны 7 дугаар сарын 29-ний өдөр ажилтнуудаа "*Cryptsy* бирж тодорхойгүй гуравдагч этгээдийн халдлагад өртөж, 5 сая ам. доллартой тэнцэх хэмжээний биткоин хулгайлагдсан" гэж мэдэгдсэн. Энэхүү мэдэгдлээс хойш 6 сарын хугацаанд Вернон үргэлжлүүлэн биржийн үйл ажиллагаа явуулж, шинэ харилцагч татан, веб сайтын аюулгүй байдал алдагдсаныг хэрэглэгчдэд мэдэгдээгүй. 2015 оны 11 дүгээр сард Вернон гэнэт Хятад руу нүүсэн ба 2016 оны 1 дүгээр сард хэрэглэгчид нь хэтэвчнээсээ алдсан биткоин болон бусад хөрөнгийн талаар блогтоо бичиж, олон нийтэд мэдээлэх болсон. 2016 оны 4 дүгээр сард Вернон *Cryptsy*-гийн серверийг хакердаж, мэдээллийн санг нь устгасан. |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | Энэ хэргийг АНУ-ын Эрүүгийн мөрдөн байцаах алба, Холбооны мөрдөх товчооны Миами дахь алба хамтран шалгаж байгаа. *Cryptsy* крипто хөрөнгийн биржийн гүйцэтгэх захирал Паул Вернон нь компанийн хэрэглэгчдийг залилан мэхэлж, татвараас зайлсхийсэн, сүлжээ ашиглан залилан мэхэлсэн, мөнгө угаасан, компьютер ашиглан залилан мэхэлсэн, баримт бичиг, бүртгэл, нотлох баримтыг устгасан, мөрдөн шалгах ажиллагааны явцад нотлох баримт устгасан гэх үндэслэлээр буруутгагдаж байна. АНУ-ын дүүргийн шүүх, Флоридагийн өмнөд дүүргийн шүүхийн шүүгчийн яллах дүгнэлтэд[189] Верноныг АНУ-ын Холбооны хуулийн 18-р хэсэг[190] §1343 хэсгийн 2-т заасныг зөрчиж, сүлжээ ашиглан залилан мэхэлсэн, §1956 (a)(1)(B)(i) заалтыг зөрчиж мөнгө угаах гэмт хэрэг үйлдсэн, §1030 (a)(5)(A), §1030 (c)(4)(B)(i) заалтыг зөрчин санаатайгаар мэдээлэл, код ашиглаж хамгаалалттай компьютерт нэвтэрч, залилан мэхэлсэн, Прожект Инвестор компани (*Cryptsy*)-ийн 1 болон түүнээс дээш компьютерын серверт халдаж, баримт, мэдээлэл, бүртгэлийг устгасан, §1519-ийг зөрчиж Холбооны мөрдөн шалгах ажиллагааны баримт бичгийг устгасан, АНУ-ын Холбооны хуулийн 26-р хэсэг[191] §7201-д заасныг зөрчиж 2014, 2015 онд татвараас зайлсхийхийг оролдсон, мөн тухайн жилүүдэд хувь хүний орлогын албан татвараа дутуу тайлагнаж, хуурамч тайлан гаргасан гэх гэмт хэргийн шинжтэй нийт 17 үйлдэлд буруутгаж, яллах дүгнэлт үйлдэн, хөрөнгийг нь хураахаар шийдвэрлэсэн. Дээрх гэмт хэргүүд дээд тал нь 5-20 жилийн хорих ялтай. |

[189] https://www.miaminewtimes.com/media/pdf/paulevernonindictment.pdf United States District Court, Southern District of Florida, Case No.19-20509, хандсан огноо: 2022.05.25.

[190] Title 18, United States Code. АНУ-ын Холбооны хуулийн 18-р хэсэг нь АНУ-ын Холбооны Засгийн газрын Эрүүгийн үндсэн хууль юм. Энэ хэсгээр Холбооны гэмт хэргүүд болон эрүүгийн процессыг зохицуулсан. https://uscode.house.gov/browse/prelim@title26&edition=prelim

[191] Title 26, United States Code. АНУ-ын Холбооны хуулийн 26-р хэсэг нь АНУ-ын дотоодын орлого буюу хувь хүн, хуулийн этгээд, айл өрхийн статистик мэдээлэл, Холбооны татвар, татварын буцаалттай холбоотой харилцааг зохицуулсан.
https://www.census.gov/history/www/reference/privacy_confidentiality/title_26_us_code_1.html#:~:text=Title%2026%2C%20U.S.%20Code%20applies,agencies%2C%20including%20the%20Census%20Bureau.

| ***Биржийн нэр*** | ***Tether*** |
|---|---|
| *Үйл баримт* | *Tether* 2014 онд ам. долларын *tether* токен буюу тогтвортой коин (*stable coin*)-ыг танилцуулсан. Энэ хэрэгт Тэтр Холдингс Лимитэд, Тэтр Лимитэд, Тэтр Оперэйшн Лимитэд, Тэтр Интернэшнл Лимитэд[192] гэх дөрвөн компанийг хариуцагчаар (“хариуцагчид”) татсан. Хариуцагчдыг ам. долларын тэтер стэйбл коиныг 2014 онд олон нийтэд танилцуулснаас хойш тэтер коин нь 100% ам. доллар, еврогоор баталгаажсан, тогтвортой зоос хэмээн мэдээлж байсан. Улмаар гүйлгээнд байгаа *USDT* бүрд харгалзах мөнгөн тэмдэгттэй тэнцэх хэмжээний хангалттай ам. долларын нөөцтэй гэж хэрэглэгчид болон зах зээлд мэдэгдсэн хэдий ч ийм хэмжээний хангалттай нөөцтэй байгаагүй болох нь тогтоогдсон. Мөн хариуцагчид дээрх байдлаар 2016 оны 6 дугаар сарын 1-ний өдрөөс 2019 оны 2 дугаар сарын 25-ны өдрийн хооронд бодит байдалд нийцэхгүй, худал, төөрөгдүүлсэн мэдэгдэл хийсэн. Улмаар хариуцагчид энэхүү нөөцдөө баталгаагүй авлага, гуравдагч этгээдийн хөрөнгө болон *Bitfinex*-ийн үйл ажиллагааны болон хэрэглэгчдийн хөрөнгийг багтааж байсныг мэдэгдээгүй, *Bitfinex*-ийн хөрвөх чадварын эрсдэлд ороход энэхүү нөөцөөс *Bitfinex* рүү шилжүүлж байсан болох нь тогтоогдсон. Мөн хариуцагчид өөрсдийн нөөцөд аудит хийлгэж байгаагүй бөгөөд дээрх хугацаанд хамаарах нөөцөд аудитын шалгалт хийхэд *Bitfinex*-ээс *Tether*-ийн шинэхэн нээсэн банкны дансанд 382 сая ам. доллар шилжүүлсэн болох нь илэрсэн. Дээрх үндэслэлүүдээр хариуцагчийг Таваарын арилжааны тухай хууль болон Таваарын фьючерсийн арилжааны комиссын дүрэм зөрчсөн гэж үзэж 41 сая ам. долларын торгууль ногдуулсан. |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | АНУ-ын Таваарын фьючерсийн арилжааны комисс Таваарын арилжааны хуулийн[193] 6(c) (d)-д заасны дагуу хэрэгжүүлсэн ажиллагааныхаа үр дүнд дараах зөрчлийг олж илрүүлэн, торгууль ногдуулах тухай тушаал гаргасан.[194] Тодруулбал, виртуал хөрөнгүүд болох биткоин, тэтер, лайткоин, этер зэрэг токен нь АНУ-ын Холбооны хуулийн 7-р хэсэг, 1a(9)-д тодорхойлсон таваар (*commodity*) гэх тодорхойлолтод хамаарна. Энэ утгаараа виртуал хөрөнгөнд хамаарах таваарыг зохицуулах эрхтэй этгээд нь Комисс бөгөөд хариуцагчдыг Таваарын болон үнэт цаасны арилжааны хуулийн 17-р хэсэг, 180.1(a)(2)(2020)-д бодит нөхцөл байдлын талаар худал, төөрөгдүүлсэн мэдэгдэл хийх, эсхүл хийсэн мэдэгдэл нь худал, төөрөгдүүлсэн зүйл болохыг нотлох шаардлагатай баримт дурдахаас татгалзсан, АНУ-ын Холбооны хуулийн 7-р хэсэг, §9(1)-д худал мэдээлэл тараах, манипуляц хийхийг хориглох, Таваарын фьючерсийн арилжааны комиссын дүрмийн 180.1(a)(2)-т үнэ ханшийг зохиомлоор тогтоох эсэхээс үл хамааран санаатай болон болгоомжгүй байдлаар заль мэх, хууран мэхлэх арга хэрэглэхийг хориглоно гэснийг тус тус зөрчсөн гэж үзсэн. |

[192] Tether Holdings Limited, Tether Limited, Tether Operations Limited, Tether International Limited.

[193] The Commodity Exchange Act.

[194] https://www.cftc.gov/PressRoom/PressReleases/8450-21 Commodity Futures Trading Commission, Order instituting proceedings pursuant to Section 6()c and (d) of the Commodity Exchange Act, making findings, and imposing remedial sanctions, CFTX Docket No.22-04, хандсан огноо: 2022.05.27.

| | |
|---|---|
| | Улмаар энэхүү тушаал гарсан өдрөөс хойш 10 хоногийн дотор хариуцагчид хамтран 41 сая ам. долларын торгууль төлөхийг үүрэг болгосон. Энэхүү торгуулийг төлөх хүртэл хугацаанд хариуцагчид тушаалыг эсэргүүцсэн аливаа мэдэгдэл гаргахгүй бөгөөд комисстой хамтран ажиллаж, хаяг, утасны дугаар өөрчлөгдсөн тохиолдолд бичгээр мэдэгдэх үүрэг хүлээн, эдгээрийг баталгаажуулсан. |

*Хавсралт 5. Бүгд Найрамдах Солонгос Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн кейс, тэдгээрийг шийдвэрлэсэн шүүхийн шийдвэр*

| ***Биржийн нэр*** | ***Coinrail*** |
|---|---|
| *Үйл баримт:* | *Хэрэг №1*[195]<br>2018 оны 6 дугаар сарын 10-ны өдөр БНСУ-ын *Linus* компанийн *Coinrail* хөрөнгийн бирж кибер халдлагад өртөж, нийт 383,570,341 вонтой тэнцэх хэмжээний криптовалют алдагдсан. *Linus* компани халдлага болсны дараа серверийн аюулгүй байдлыг хангахын тулд шалгалт хийсэн ба энэ хугацаанд биржийг хааж, үйл ажиллагааг нь зогсоосон тухай мэдэгдэл гаргасан. Мөн 2018 оны 7 дугаар сарын 15-ны өдөр алдагдсан криптовалютыг үе шаттайгаар худалдан авч, эсхүл өөрийн компанийн *RAIL*-ийг гаргаж, орлуулж өгөх замаар хэрэглэгчдийн хохирлыг барагдуулна гэж мэдэгдсэн боловч хохирлыг барагдуулаагүй.<br>Тиймээс 11 хэрэглэгч *Linus* компани болон ТУЗ-ийг хариуцагчаар татаж, тус бүр өөрт ногдох криптовалюттой тэнцэх хэмжээний хохирол (нийт 383,570,341 вон) болон нэхэмжлэл гардуулсны маргааш өдрөөс буюу 2018 оны 10 дугаар сарын 9-ний өдрөөс эхлэн 2019 оны 5 дугаар сарын 31-ний өдөр хүртэл жилийн 15 хувь, 2019 оны 6 дугаар сарын 1-ний өдрөөс эхлэн хохирол барагдуулж дуусах өдөр хүртэлх хугацаанд жилийн 12 хувийн хүү нэхэмжилсэн. Сөүл хотын төв дүүргийн шүүх 2021 оны 11 дүгээр сарын 5-ны өдөр *Linus* хувьцаат компаниас хохирлыг бүрэн гаргуулж, ТУЗ-ийг хариуцлага хүлээх үндэслэлгүй гэж үзсэн. |
| Шийдвэрлэсэн байдал | Шүүх шийдвэрлэх болсон үндэслэлээ дараах байдлаар тайлбарласан: Нэхэмжлэгчид биржид данс нээснээр бирж ашиглах гэрээ байгуулагдсан ба гэрээний дагуу нэхэмжлэгчид виртуал хөрөнгө, бэлэн мөнгөө гарган авахыг хүсвэл бирж тэр даруй гаргаж өгөх үүрэгтэй. *Linus* компани кибер хадлагад өртсөн өдрөө (2018.06.10) биржийг хааж, үйл ажиллагааг нь зогсоосон. Тиймээс нэхэмжлэгчид тухайн өдрөөс эхлэн өнөөдрийг хүртэл виртуал хөрөнгөө буцаан авч чадахгүй болсон. Үүнийг нэгтгэн дүгнэвэл *Linus* компани кибер халдлагын улмаас биржийн үйл ажиллагааг зогсоож, хаасан явдал нь нэхэмжлэгчдэд виртуал хөрөнгийг нь буцаан өгөх үүргээсээ татгалзсан, мөн кибер халдлагын улмаас цахим хэтэвчид хадгалагдах виртуал хөрөнгийг алдагдуулснаар виртуал хөрөнгийг буцаан өгөх үүргээ биелүүлэх боломжгүй болсон гэж үзэх үндэслэл болох юм. |

[195] 서울중앙지법 2021. 11. 5., 선고, 2018가합567582, 판결 : 항소, https://law.go.kr/LSW/precInfoP.do?mode=0&precSeq=218375#AJAX

| | |
|---|---|
| | *Linus* компани (цаашид хариуцагч гэх)-ийн зүгээс (1) биржийн үйл ажиллагааг зогсоосон нь үүргээ биелүүлэхээс татгалзсан явдал биш, харин халдлагын хохирлыг багасгах зорилготой арга хэмжээ, (2) халдлагад өртсөн явдалд компанийн санаатай болон болгоомжгүй үйлдэл байхгүй, (3) виртуал хөрөнгийг буцаан олгох боломжгүй болсон тул хариуцлага хүлээх үндэслэлгүй гэж маргасан.<br><br>Шүүх үүрэг гүйцэтгэхээс татгалзсан болон үүрэг гүйцэтгэх боломжгүйн улмаас учирсан хохирол шаардсан хэргийн хувьд хариуцагч хариуцлага хүлээх үндэслэлгүй гэдгээ өөрөө нотлох үүрэгтэй (*Дээд шүүхийн 2010 оны 8 дугаар сарын 9-ний өдрийн 26752 дугаар тогтоолыг үндэслэн*) гэж дүгнэсэн. Хариуцагч нь кибер халдлага үйлдэгдсэний дараах мөрдөн шалгах ажиллагааны явцад мэдэгдэл гаргасан боловч өнөөдрийг хүртэл кибер халдлага үйлдсэн арга, биржийн системийн сул тал зэрэг хэргийн нөхцөл байдлын нарийн ширийн зүйлсийг ил болгоогүй. Хариуцагч кибер халдлагаас өмнө мэдээлэл технологийн аюулгүй байдлын зөвлөх компанийн үйлчилгээ авч, мөн БНСУ-ын Интернэт, аюулгүй байдлын агентлагийн аюулгүй байдлын шалгалтад хамрагдсан байна. Үүний дараа ч гэсэн мэдээллийн технологийн аюулгүй байдлын зөвлөх компанитай аюулгүй байдлын үйлчилгээний гэрээ, интернэт сүлжээг тусгаарлах байгууламж нэвтрүүлэх гэрээ байгуулсан баримт байна.<br><br>Гэхдээ (1) хариуцагчийн удирддаг цахим хэтэвчид хадгалагдаж байсан хэрэглэгчдийн виртуал хөрөнгө кибер халдлагад өртөж, алдагдсан явдал нь бүхэлдээ хариуцагчийн ажил үүрэгт хамаарна, (2) хариуцагч цахим хэтэвчид нэвтрэх хэрэглийн аюулгүй байдлын менежментэд хайхрамжгүй хандсан нь дээрх кибер халдлага гарах шалтгаан болсон байж болзошгүй зэргийг харгалзан үзэхэд хариуцагчийн тайлбарыг үндэслэх баримт хангалтгүй тул тайлбарыг хүлээн авах боломжгүй.<br><br>Тиймээс хариуцагч виртуал хөрөнгийг буцаан олгохоос татгалзсан үйлдлээс учруулсан хохиролд нэхэмжлэгч тус бүрд оногдох виртуал хөрөнгийн төлбөрийг кибер халдлага гарах үеийн зах зээлийн ханшаар тооцож (нийт 383,570,341 вон), мөн Хэрэг хянан шийдвэрлэх ажиллагааг хурдасгах тухай тусгай хуулийн дагуу нэхэмжлэл гардуулсны маргааш өдрөөс (2018.10.09) эхлэн 2019 оны 5 дугаар сарын 31-ний өдөр хүртэлх хугацаанд 15 хувиар, 2019 оны 5 дугаар сарын 31-ний өдрөөс эхлэн төлж дуусах хүртэл 12 хувиар тооцон удаашруулсны хохирлыг (алданги) барагдуулах үүрэгтэй.<br><br>Харин *Linus* компани нэхэмжлэгчдийн виртуал хөрөнгийг буцаан өгөхөөс татгалзсан болон буцаан өгөх боломжгүй болсон явдалд ТУЗ-ийн санаатай, эсхүл ноцтой алдаа гаргасан гэх баримт байхгүй тул ТУЗ-д холбогдох нэхэмжлэл үндэслэлгүй гэж дүгнэжээ. |

*Хавсралт 6. Швейцарын Холбооны Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржүүдийн кейс, тэдгээрийг шийдвэрлэсэн байдал*

| ***Биржийн нэр*** | ***Trade.io*** |
|---|---|
| *Үйл баримт* | Швейцарт төвтэй криптовалютын *Trade.io* бирж 7.5 сая доллароор үнэлэгдэх токеноо шилжүүлэг хийх үедээ алдсан. Хакерууд биржийн хэтэвчнээс 50 сая орчим *TIO* буюу *Trade.io token* хулгайлсан. *Trade.io*-гийн мэдээлснээр алдагдсан хөрөнгийн үнэлгээ нь 7.5 сая доллар бөгөөд хэтэвчийг банканд хадгалдаг байжээ. Арилжааны үйл ажиллагаа дээд цэгтээ хүрэх үед нөөцөд байх *TIO*-г хөрвөх чадварын сандаа оруулахаар төлөвлөж байжээ. Гэтэл *Trade.io* нь өөрийн данснаас 50 сая токен татан авч, 1.3 саяыг *Bancor, Kucoin*-д тус тус шилжүүлэх үедээ халдлагад өртсөн. Үүний дараа гурван биржийн *TIO* хадгаламж, мөнгө татах, арилжаа хийх эрхийг хаажээ.[196] |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | Хулгайлагдсан хөрөнгө нь арилжаанд ороогүй байсан тул *Trade.io*-д бүртгэлтэй хэрэглэгчдэд хамаарахгүй аж. Гүйцэтгэх захирал *Preissler* "*TIO*-гийн үнэ цэнийг хамгаалах" зорилгоор хулгайлагдсан токеныг хүчингүй болгохын тулд *TIO* токены кодын сан байгуулахаар төлөвлөж байна гэж мэдэгдэв. |

| ***Биржийн нэр*** | ***Bancor*** |
|---|---|
| *Үйл баримт* | 2018 оны 7 дугаар сарын 9-ний өдөр төвлөрсөн бус бирж болох *Bancor* хакеруудын халдлагад өртсөн. Биржийн хэтэвчнээс 23.5 сая долларын үнэ бүхий хөрөнгө алдагдсан. Бирж дээрх токенуудыг нэн даруй царцаасан бөгөөд энэ нь криптовалютын нийгэмлэгийн зүгээс шүүмжлэл дагуулсан.[197] *Bancor* мэдэгдэлдээ "Зарим ухаалаг гэрээг шинэчлэхэд ашиглагддаг хэтэвч эрсэдсэн" гэв. Үүний үр дүнд хакер 12.5 сая долларын *Ether*, 1 сая долларын *Pundi X*-ийн *NPXS* токен, 10 сая долларын *Bancor*-ын *BNT*-г авсан. |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | Шүүхээр шийдвэрлэгдээгүй бөгөөд хэрэглэгчийн хэтэвчид халдаагүй гэж мэдэгдсэн. |

[196] https://cyware.com/news/tradeio-was-hacked-and-75-million-worth-of-cryptocurrencies-were-stolen-5c7a0c71/

[197] https://cointelegraph.com/magazine/crypto-exchange-hacks/

*Хавсралт 7. Бүгд Найрамдах Эстони Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржийн кейс, тэдгээрийг шийдвэрлэсэн байдал*

| **Биржийн нэр:** | **Taylor** |
|---|---|
| Үйл баримт | Криптовалют арилжааны *TAYLOR* аппликейшн нь кибер халдлагын хохирогч болж, 1.5 сая долларын үнэ бүхий 2,578 *ETH* болон *TAY* токен нийлүүлэлтийн 7 хувийг алдсан байна. Тэдний мэдээлснээр хакерууд нэг хэтэвч дэх хөрөнгийг олон эх үүсвэрээс цуглуулж, дараа нь илүү том руу нь шилжүүлсэн байна. Энэ нь *CypheriumChain* дэх хөрөнгийг үгүй болгосонтой ижил хэтэвч байжээ. *CypheriumChain* нь мөн саяхан хакердуулж, 9.8 сая долларын үнэ бүхий 17 000 *ETH* алдсан. Тиймээс *Taylor*-ын итгэж байгаагаар энэ удаагийн хакерын хэрэг үйлдсэн этгээд нь *CypheriumChain*-ы халдлагыг үйлдсэн этгээд юм. Үүний зэрэгцээ алга болсон *TAY* токенууд нь *IDEX* криптовалют бирж дээр илэрсэн байна. Иймд *TAYLOR* нь *IDEX*-ийн багаас нөхцөл байдал тодорхой болох хүртэл *TAY*-ийг жагсаалтаас хасахыг хүссэн. |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | Тус компани хэрэглэгчдийн хохирлыг нөхөн төлөхийн тулд 5663273 дугаар блок дээр үлдэгдэлтэй хэрэглэгчид шинэ токен тараах шийдвэр гаргасан.[198] Компани хулгайлагдсан токенууд хаана байгааг мэдэж байгаа гэж мэдэгдсэн бөгөөд компанийн үүсгэн байгуулагч, гүйцэтгэх захирал нь болсон явдалд уучлалт гуйж, энэхүү байдлыг даван туулахад туслахыг олон нийт (*community*)-д хандан уриалсан. |

[198] Taylor app loses $1.5M worth of ETH in recent hack - CoinGeek.

*Хавсралт 8. Оросын Холбооны Улсын кибер халдлагад өртсөн виртуал хөрөнгийн биржийн кейс, шийдвэрлэсэн байдал*

| ***Биржийн нэр:*** | ***Live coin***[199] |
|---|---|
| *Үйл баримт* | 2020 оны 12 дугаар сарын 23-наас 24-нд шилжих шөнө *Live coin* биржийн дэд бүтэц, серверт хууль бусаар халдаж, виртуал хөрөнгийн ханшийг их хэмжээгээр бодит бусаар тогтоосон. Криптобиржийн хэрэглэгчийг төөрөгдүүлэх зорилгоор веб сайтын интерфейс дээр виртуал хөрөнгийн ханшийн "бодит бус" үнэлгээ үүсгэсэн. Улмаар хакерчид виртуал хөрөнгийн ханшийг хууль бусаар өөрчилж, арилжаалсан виртуал хөрөнгөө бэлэн мөнгөнд шилжүүлэн авч, их хэмжээний ашиг олсон.<br>Тухайн үед 12 дугаар сарын 24-ний өдөр *Live coin*-ы биткоины үнийг 450,000 ам. доллароос 23,000 ам. доллар хүртэл, *ether*-ийг 600 ам. доллароос 15,000 ам. доллар хүртэл буулгаж, *ripple-ийг* 0.17 ам. долларооc 17 доллар хүртэл өсгөж, дүнг өөрчилсөн байжээ. *Live coin* удирдлагуудаас платформдоо нийтлэхдээ тус үйл явдлыг "сүүлийн хэдэн сарын турш бэлтгэж төлөвлөсөн халдлага" гэж мэдэгдсэн байна. |
| *Шийдвэрлэсэн байдал, хэрэглэсэн хуулийн зохицуулалт* | *Live coin* удирдлагаас 2021 оны 1 дүгээр сарын 16-ны өдөр биржийн үйл ажиллагааг хааж, хохирол барагдуулах талаар мэдэгдэл гаргасан. 2021 оны 3 дугаар сарын 17-ны өдөр хүртэл хэрэглэгчдийн хохирлыг барагдуулах хүсэлт хүлээн авч, барагдуулахаа илэрхийлсэн. Эхний ээлжид 5000 ам. доллар хүртэл хөрөнгөтэй хэрэглэгчийн хөрөнгийг буцаан шилжүүлнэ. Алдагдсан виртуал хөрөнгийг халдлага болох үеийн ханшаар тооцож, стэйбл коиноор шилжүүлэхээ мэдэгдэж, маргааныг шүүхээр шийдвэрлээгүй байна. |

[199] https://www.rbc.ru/crypto/news/5fe4a8c79a79477f19e3a889

# АШИГЛАСАН ЭХ СУРВАЛЖ

**Монгол Улсын хууль тогтоомж:**


- Монгол Улсын Эрүүгийн хууль (Шинэчилсэн найруулга). 2015.
- Зөрчлийн тухай хууль (Шинэчилсэн найруулга). 2017.
- Монгол Улсын Эрүүгийн хэрэг хянан шийдвэрлэх тухай хууль (Шинэчилсэн найруулга). 2017.
- Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн тухай хууль. 2021.
- Кибер аюулгүй байдлын тухай хууль. 2021.
- Өргөн нэвтрүүлгийн тухай хууль. 2019.
- Виртуал хөрөнгийн үйлчилгээ үзүүлэгчийн бүртгэлийн журам. 2022.
- Виртуал хөрөнгийн үйлчилгээний үйл ажиллагааны журам. 2022.
- Монгол Улсын үндэсний аюулгүй байдлын үзэл баримтлал. 2010.
- “Монгол Улсын хууль тогтоомжийг 2024 он хүртэл боловсронгуй болгох үндсэн чиглэл батлах тухай” Монгол Улсын Их Хурлын 2021 оны 1 дүгээр сарын 22-ны өдрийн 12 дугаар тогтоол.


**Ном, өгүүлэл, бусад:**


- С.Нарангэрэл. Монгол Улсын хууль зүйн нэвтэрхий толь бичиг – 2021. УБ., 2021.
- Д.Баярсайхан. Дэлхийн Эрүүгийн загвар хууль ба орчин үе. УБ., 2013.
- Л.Галбаатар. Кибер гэмт хэргийг шүүхэд хянан шийдвэрлэх нь (Анхны хэвлэл). УБ., 2015.
- Б.Өнөрмаа. “Цахим хэрэгсэл ашиглан үйлдэгдэж буй гэмт хэргийн шалтгаан нөхцөл, эрх зүйн орчныг боловсронгуй болгох шаардлага” нийтлэл. 2022.
- Ц.Хүрэл-Очир. Мэдээллийн технологийн эрх зүйн орчныг бүрдүүлэх асуудалд. “Хууль дээдлэх ёс” сэтгүүл, 2017, №13.
- Д.Ренчиндорж. Дэлхийн Эрүүгийн загвар хууль гаргах болсон шаардлага, үндэслэл, ач холбогдол. 2019.
- Л.Галбаатар. Монгол Улсын мэдээллийн аюулгүй байдлын эрх зүйн зохицуулалт: Өнөөгийн байдал, тулгамдсан асуудал, шийдвэрлэх арга зам. “Шүүх эрх мэдэл” сэтгүүл, 2018, №4.
- Кибер аюулгүй байдлын тухай хууль боловсруулах хэрэгцээ, шаардлагыг урьдчилан тандан судалсан үнэлгээний тайлан. 2021.
- Ian J.Lloyd. Information Technology Law (Sixth Edition). Oxford University Press, 2011.

- Convention on Cybercrime (ETS No. 185).
- Model Criminal Code.
- Bryan A. Garner. Black's Law Dictionary. 9th edition, 2009.
- Priyanka V.Kayarkar, Prashant Ricchariya, Anand Motwani "Mining Frequent Sequences for emails in cyber forensics investigation", International Journal of Computer Applications, V85, January 2014, No17.
- 정 완 (연구위원, 법학박사), 사이버범죄 방지를 위한 국제공조방안, 2004.
- 정정일, 사이버범죄에 대한 국제적 대응방안, 343 면
- 윤해성·라광현, 주요국의 유럽평의회 사이버범죄방지협약 비준 과정 및 쟁점, "한국경찰학회보" 제21권 제3호, 2019.
- 김만흠 (국회입법조사처장), 국회입법조사처, 제77호, 2020.
- 박희영·최호진·최성진, "사이버범죄협약 이행입법 연구", 대검찰청 연구보고서, 2015.
- 정태진·이광민, "사이버범죄 대응을 위한 부다페스트협약 가입과 국제공조 연구", "경찰학논총" 제14권 제2호, 2019.
- Шевченко Елизавета Сергеевна. "Тактика производства следственных действий при расследовании киберпреступлений" диссертация на соискание учебной степени кандитата юридических наук, М., 2016.
- Бутусова Л.И. Характеристка и сущность киберпреступлений. Журнал "Алтайский юридический вестник", 2016, №3.
- Калитин Сергей Вячеславович "Доказательства электронные и цифровые". Научно-методический электронный журнал "Концепт", 2014.
- М.Х.Гельдибаев, Е.Н.Рахманова. Уголовное право в схемах и определениях. СПб., 2017.


## Цахим эх сурвалж

**Монгол хэлээр:**


- www.1212.mn
- https://www.mglbar.mn/news/4065
- www.shuukh.mn
- https://mojha.gov.mn/wp-content/uploads/2021/01/VASP-%D1%82%D0%B0%D0%BD%D0%B8%D0%B-B%D1%86%D1%83%D1%83%D0%BB%D0%B3%D0%B0.pdf
- https://www.mongolbank.mn/documents/cma/guide20220201.pdf
- http://www.parliament.mn/n/mo3on
- https://mddc.gov.mn/
- www.legaldata.mn
- www.legalinfo.mn

**Англи хэлээр:**


- https://rm.coe.int/09000016809f44f0
- Global cybersecurity index 2020, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
- https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E
- https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/
- https://crystalblockchain.com/security-breaches-and-fraud-involving-crypto/
- https://www.netsafe.org.nz/
- https://cybercrime.org.za/reporting
- https://www.ic3.gov/Home/ComplaintChoice
- https://www.coe.int/en/web/cybercrime/the-budapest-convention?ref=hackernoon.com
- https://legaldata.mn/buteel/pdf?id=776
- https://www.corteidh.or.cr/tablas/r32562.pdf
- https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf
- https://sso.agc.gov.sg/Act/CA2018?ProvIds=Sc1-#Sc1-
- https://www.parliament.gov.sg/docs/default-source/default-document-library/financial-services-and-markets-bill-4-2022.pdf
- https://www.justice.gov/archives/ag/page/file/1326061/download
- https://www.gld.gov.hk/egazette/pdf/20222625/es32022262516.pdf
- Estonia to tighten regulation of virtual asset service providers | Rahandusministeerium (fin.ee)
- https://www.riigiteataja.ee/en/eli/523052018003/consolide
- https://www.sif.admin.ch/sif/en/home/finanzmarktpolitik/digitalisation-financial-sector/blockchain.html#:~:text=On%201%20August%202021%2C%20Switzerland,and%20enables%20innovation%20and%20growth
- https://complyadvantage.com/insights/crypto-regulations/cryptocurrency-regulations-switzerland/
- https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
- https://www.internetjurisdiction.net/uploads/pdfs/Data-Jurisdiction-Outcome-Framing-Brief-on-Electronic-Evidence.pdf
- https://athenaforensics.co.uk/acpo-guidelines-for-computer-forensics/
- https://researchrepository.murdoch.edu.au/id/

eprint/14422/2/02Whole.pdf
- https://www.interpol.int/content/download/16243/file/Guidelines%20to%20Digital%20Forensics%20First%20Responders_V7.pdf
- https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en
- https://uscode.house.gov/browse/prelim@title1/chapter3&edition=prelim
- https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/510052022003/consolide
- https://sso.agc.gov.sg/Act/CMA1993?ProvIds=P12-#pr3-
- https://www.elegislation.gov.hk/hk/cap200
- https://www.elegislation.gov.hk/hk/cap106
- Cyber defense Report, Japan's National Cybersecurity and Defense Posture, Policy and Organization, September, 2020, p,4, https://bit.ly/3zLRtsX
- https://doj.gov.ph/files/cybercrime_office/Singapore%20Country%20Report.pdf
- https://etherscan.io/address/eb31973e0febf3e3d7058234a5ebbae1ab4b8c23
- https://www.kucoin.com/news/en-kucoin-security-incident-update
- https://news.bitcoin.com/kucoin-boss-on-strategy-after-hack-we-chose-to-act/
- https://www.elitigation.sg/gd/s/2022_SGHC_46
- https://tokenpost.com/Crypto-exchange-DragonEx-lost-7M-in-hack-announces-compensation-plan-1568
- https://www.thestar.com.my/tech/tech-news/2021/08/02/cryptocurrency-crime-in-hong-kong-hits-record-levels-with-one-victim-losing-hk124mil-to-fraudsters
- https://www.hkreform.gov.hk/en/docs/cybercrime_e.pdf
- https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency https://www.justice.gov/usao-dc/press-release/file/1470221/download
- https://www.cnbc.com/2022/02/08/feds-seize-3point6-billion-stolen-from-bitfinex-hack.html
- https://ag.ny.gov/sites/default/files/2021.02.17_-_settlement_agreement_-_execution_version.b-t_signed-c2_oag_signed.pdf
- https://www.justice.gov/usao-ndca/press-release/file/1317276/download
- https://www.miaminewtimes.com/media/pdf/paulevernonindictment.pdf

- https://www.census.gov/history/www/reference/privacy_confidentiality/title_26_us_code_1.html#:~:text=Title%2026%2C%20U.S.%20Code%20applies,agencies%2C%20including%20the%20Census%20Bureau.
- https://www.cftc.gov/PressRoom/PressReleases/8450-21
- https://sherloc.unodc.org/cld/uploads/res/document/che/1937/swiss_criminal_code_en_html/Swiss_Criminal_Code_amJuly2020.pdf
- https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/switzerland
- https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/switzerland
- https://www.swissinfo.ch/eng/swiss-cyber-crime-incidents-increase-by-a-quarter/47469694#:~:text=There%20was%20also%20an%20uptick,the%20virtual%20space%20in%202021.
- https://cyware.com/news/tradeio-was-hacked-and-75-million-worth-of-cryptocurrencies-were-stolen-5c7a0c71/
- https://cointelegraph.com/magazine/crypto-exchange-hacks/


**Бусад хэлээр:**


- https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE01572781
- http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_E2A1O0O5E0K6X1U1B3T2Y5U0V1T5Z0
- http://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_K2T1V0H6U0L9M0X9A4W8A3G0W7Q6H1
- http://likms.assembly.go.kr/bill/BillSearchResult.do
- 暗号資産交換業者に関する内閣府令、平成二十九年三月二十四日 https://bit.ly/3zJL8OP
- 資金決済に関する法律、平成二十一年六月二十四日https://bit.ly/3zGNdLt
- 金融商品取引法、昭和二十三年四月十三日 https://bit.ly/30k8D4X
- 暗号資産交換業者に関する内閣府令、平成二十九年三月二十四日 https://bit.ly/3A1uDh8
- 資金決済に関する法律、平成二十一年六月二十四日（https://bit.ly/30yHxaC）
- http://www.consultant.ru/document/cons_doc_LAW_10699/
- https://www.law.go.kr/
- https://www.garant.ru/products/ipo/prime/doc/71456224/
- http://www.consultant.ru/document/cons_doc_LAW_358753/
- https://www.rbc.ru/crypto/news/5fe4a8c79a79477f19e3a889