КИБЕР АЮУЛГҮЙ БАЙДЛЫН ОЛОН УЛСЫН ЗОХИЦУУЛАЛТ

(Дүн шинжилгээ)

О.Билгүүтэй

АГУУЛГА

УДИРТГАЛ

Судалгааны мэдээллийг дараах 4 бүлэг асуудлын хүрээнд ангилан боловсруулсан:

1. Кибер аюулгүй байдал, халдлагын төрлүүд;
2. Олон улсын стандарт, бодлогын зөвлөмж, Будапештийн конвенц;
3. Кибер аюулгүй байдлын талаарх Монгол Улсад баримталж буй бодлого, зохицуулалтын орчин;
4. Бусад орнуудын туршлага (Солонгос, Малайз)

СУДАЛГААНЫ ХУРААНГУЙ

Кибер аюулгүй байдал өнөө цагт хувийн аж ахуйн нэгжээс эхлээд эдийн засгийн салбар, цаашлаад үндэстний хэмжээнд яригддаг нийтлэг том сэдэв болж хувирсан ба техник технологийн хөгжлөөс үүдэлтэй жам ёсны асуудал юм. Нэг хүнээс нөгөө хүнд очих цахим мэдээ, мэдээлэл анхны агуулга шинжээ гээлгүй үнэн зөв дамжих ёстой. Гэвч мэдээллийн урсгалын зам зуурт хөндлөнгийн хүчин зүйлс нөлөөлснөөр мэдээллийн анхны шинж тэмдэг алдагдаж уг мэдээллийг хүлээн авагч талд сөрөг нөлөө үзүүлэх, нэг ёсны “цахим халдлага үүсэх” боломжтой.

Судалгааны нэгдүгээр бүлэгт, кибер аюулгүй байдлын талаар ерөнхий мэдээллийг тусгасан ба системийн сул талыг ашиглан хувь хүн, аж ахуй нэгж, цаашлаад нууцын зэрэглэлтэй мэдээлэл рүү хэрхэн нэвтэрч халдлага үйлддэг, үүнээс хэрхэн урьдчилан сэргийлж хамгаалдаг талаарх асуудлыг авч үзсэн.

Хоёрдугаар бүлэгт, олон улсад мөрдөж байгаа кибер аюулгүй байдалтай холбоотой стандарт, бодлогын зөвлөмж болон олон улсын гэрээ конвенцийн талаарх мэдээллийг оруулсан. Олон улсад кибер аюулгүй байдалтай холбоотой *ISO/IEC 27032:2012, ISO 27001* стандартуудыг мөрддөг бөгөөд дээрх стандартууд нь мэдээллийн аюулгүй байдлын менежментийн олон улсад хүлээн зөвшөөрөгдсөн стандарт юм. Аливаа улс орны цахим халдлагаас өөрийгөө хамгаалах чадамжийг Олон улсын харилцаа холбооны байгууллагаас *(International Telecommunication Union)* гаргасан кибер аюулгүй байдлын индексээр (The Global Cybersecurity Index) тодорхойлдог байна. Уг индексийг 1) хууль, эрх зүйн арга хэмжээ (Legal), 2) техникийн арга хэмжээ (Technical Measures), 3) байгууллагын зохион байгуулалтын арга хэмжээ (Organization Measures), 4) чадавх хөгжүүлэх арга хэмжээ (Capacity Building Measures), 5) хамтын ажиллагаа (Cooperation Measures) гэсэн үндсэн 5 шалгуур үзүүлэлтээр тодорхойлдог байна.

Мөн Олон улсын Програм хангамжийн холбооноос (BSA) зөвлөж буй кибер аюулгүй байдалтай холбоотой бодлого боловсруулахад засгийн газруудад шаардагдах 6 тулгуур зарчмыг тодорхойлсон. Түүнчлэн 2004 оноос хэрэгжиж эхэлсэн Будапештийн Кибер гэмт хэрэгтэй тэмцэх тухай конвенцийн үзэл баримтлал, зорилго, нэгдэн орсноор үүсэж болох давуу талуудыг мөн энэ бүлэгт тоймлон оруулсан.

Гуравдугаар бүлэгт, Монгол Улс дахь кибер аюулгүй байдлын хууль, эрх зүйн орчин, кибер аюулгүй байдалтай холбоотой үндэсний аюулгүй байдлын стратеги, мэдээллийн аюулгүй байдлыг хариуцсан байгууллага, түүний чиг үүргийн талаарх мэдээллийг оруулсан.

Дөрөвдүгээр бүлэгт, кибер аюулгүй байдлын индексээр тэргүүлэх байр суурь эзэлдэг

сайн туршлагатай орнуудын жишээ болгож Солонгос болон Малайз улсын туршлага, цахим гэмт хэрэгтэй тэмцэх тухай бие даасан хууль болон холбогдох бусад хуулиудын талаарх мэдээллийг оруулсан.

Түлхүүр үг: *Кибер аюулгүй байдал, Мэдээллийн аюулгүй байдал, Кибер аюулгүй байдлын индекс, Будапештийн Кибер гэмт хэрэгтэй тэмцэх тухай конвенц*

Keywords: *Cybersecurity, Information security, Global cyber security index, Budapest cybersecurity convention,*

БҮЛЭГ I. КИБЕР АЮУЛГҮЙ БАЙДАЛ

Мэдээллийн аюулгүй байдал гэдэг нь мэдээлэл болон мэдээллийн системд зөвшөөрөлгүй хандах, мэдээллийг ашиглах, ил болгох, өөрчлөх, хуулах, устгах, мэдээллийн системийн үйл ажиллагааг тасалдуулах, гаднаас хяналт хийхээс хамгаалахыг хэлнэ.[310]

Кибер аюулгүй байдал гэдэг нь кибер гэмт хэргээс систем, сүлжээ, өгөгдлийг хамгаалахад зориулагдсан технологи, үйл явц, арга хэмжээнээс бүрддэг.[311] Кибер аюулгүй байдал нь кибер халдлагын эрсдэлийг бууруулж, систем, сүлжээ, технологийг санаатайгаар ашигласаар байгаа хүмүүсээс аж ахуйн нэгж, байгууллага, хувь хүмүүсийг хамгаалахад чиглэгддэг. Кибер халдлагууд нь олон янзын хэлбэртэй байна. (жишээ нь програмын довтолгоонууд, malware, ransomware, фишинг гэх мэт). Кибер халдлага нь ихэвчлэн хулгайгаар (төлбөрийн картын өгөгдөл, хэрэглэгчийн мэдээлэл, компаний нууцлал, оюуны өмчийн эрхийг зөрчих гэх мэт) сүлжээнд зөвшөөрөлгүй нэвтрэн хохирогч этгээдэд санхүүгийн болон нэр хүндийн хохирол учруулах зорилгоор хийгддэг ажиллагаа юм. Кибер халдлагууд улам бүр боловсронгуй болсоор байгаа ба олон улсад аливаа улсын засгийн газрын мэдээллийн санд халдаж улс орны аюулгүй байдал, батлан хамгаалах, цэрэг, стратеги, улс төрийн салбарт чиглэсэн аюул занал учруулах явдал түгээмэл болж байна. Эдгээрээс зарим нэг нийтлэг аюул заналыг дурдвал:

- **Cyber terrorism** нь террорист бүлэглэлүүдээс засгийн газрын үзэл суртлын болон улс төрийн хөтөлбөрт нэвтрэн орж тодорхой зорилгоор мэдээллийн технологийг ашигладаг хэлбэр юм. Сүлжээнүүд, компьютерийн систем, харилцаа холбооны дэд бүтцэд нэвтэрч халддаг.[312]
- **Cyber warfare** нь улс үндэстний сүлжээнд нэвтэрч, мэдээллийн технологийг доголдуулдаг. Cyber warfare довтолгоонууд нь үндсэн сүлжээг эвдэх ба тухайн сүлжээний хэвийн ажиллагааг тасалдуулах чухал өгөгдлийг боогдуулах замаар халдлага үйлддэг[313].
- **Cyber espionage** нь эзэмшигчийн зөвшөөрөлгүйгээр нууц мэдээллийг олж авах тагнах хэлбэр юм. Cyber espionage нь стратегийн, эдийн засгийн, улс төрийн, цэргийн давуу талыг олж авахад ашиглагддаг.[314]

ХАЛДЛАГЫН АРГА ХЭЛБЭРҮҮД

Кибер гэмт хэрэгтний зүгээс халдлага үйлдэх хэд хэдэн арга хэлбэрүүд байдаг бөгөөд тэдгээр нь хортой програмыг компьютерт оруулах, эсхүл өгөгдлийг хулгайлах зэрэг олон арга замаар хэрэгждэг байна. Үүнд:

- **Social engineering**- Хувь хүний сул талыг ашиглан хортой холбоос дээр даруулах, эсвэл хууран мэхлэх замаар компьютерт нэвтрэх эрх олж авах арга;
- **Phishing /өгөөш хаях замаар хохирогчийг удирдах/**-Хуурамч аж ахуйн нэгж байгуулах, эсхүл тэднийг төлөөлөх замаар хэрэглэгчийн мэдээллийг олж авахыг оролдох үйлдэл;

[310] Мэдээллийн аюулгүй байдлын газар
[311] Төрийн мэдээлэл холбооны газар
[312] https://www.nato.int/cps/en/natohq/topics_140739.htm?
[313] https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf
[314] https://www.vmware.com/topics/glossary/content/cyber-espionage

- **Pharming /Интернэт залилан/-**Вэб сайтын мэдээллийн урсгалыг өөр зүгт чиглүүлэх, хуурамч вэбсайт үйлдэх зэргээр хувь хүний мэдээллийг хулгайлах халдлага;
- **Drive-by /жолоодох/**-Систем доторх тодорхой сул талуудыг ашиглаж халдах;.
- **Man in the middle /зуучлагч/**- Талуудын харилцаанд хөндлөнгөөс оролцож үр дүнд нь хакер хоёр талыг хоёуланг нь удирдах, хохироох боломжтой болох арга.

Malware нь компьютерийн системийг тасалдуулах, гэмтээх, зөвшөөрөлгүй нэвтрэх зорилгоор тусгайлан бүтээсэн програм хангамж бөгөөд эдгээр нь дараах хэлбэртэй байдаг:

- **Ransomware** нь компьютерийн систем дээр хортой программаар кибер халдлагыг эхлүүлсний дараа төлбөр шаарддаг хэлбэр юм. Энэ төрлийн хорт програм нь гэмт хэрэгтнүүдийн дунд түгээмэл болж, жил бүр сая сая байгууллагыг хохироож байна.
- **Viruses** (Вирус) нь нэг компьютерээс нөгөө компьютерт өөрөө өөрийгөө хуулбарлах боломжтой жижиг хэмжээний код юм.
- **Worms** (Өт) нь бусад компьютеруудад тархахын тулд өөрийгөө хуулбарладаг бие даасан хортой програм юм.
- **Trojans** (Троян) вирус нь нэг функц (жишээлбэл, вирус арилгах) мэт харагддаг програм боловч яг үнэндээ үйлдэл хийх үед системийг гэмтээдэг байна.
- **Spyware/adware** төрөл бүрийн файл хавсаргадаг ба үүнийг нээх холбоос дээр дарах эсвэл хортой програмыг татаж авах үед системд нэвтэрч хохирол учруулдаг.

ХАЛДЛАГА ҮЙЛДЭХ СУВГУУД

- Хортой програм (код)-аар дамжин халдаах
- Цахим шуудан, мессежээр дамжин халдаах
- Цахим хуудас, нийтийн сүлжээгээр дамжин халдаах
- Нууц үг тайлах
- Төлбөртэй программыг эвдэж ашиглах

БҮЛЭГ II. КИБЕР АЮУЛГҮЙ БАЙДЛЫН ОЛОН УЛСЫН СТАНДАРТ

Олон улсын стандартчиллын байгууллагаас (ISO) кибер аюулгүй байдлын ойлголт, шалгуур, боловсронгуй болгох зарчмуудыг багтаасан *ISO/IEC 27032:2012 Information technology (Мэдээллийн технологи)* Олон улсын стандартыг 2012 оны 7 дугаар сард тогтоосон байна.[315] Уг стандартад кибер аюулгүй байдал, сүлжээний аюулгүй байдал, хэрэглээний аюулгүй байдал, интернэтийн аюулгүй байдал, дэд бүтцийн аюулгүй байдал гэх мэт нэр томьёонуудыг тодорхойлсон байна. Түүнчлэн ISO 27001 нь мэдээллийн аюулгүй байдлын менежментийн олон улсад хүлээн зөвшөөрөгдсөн стандарт юм. Энэхүү стандартыг хэрэгжүүлснээр мэдээллийг хамгаалах, мэдээллийн аюулгүй байдлыг хангахтай холбоотой арга хэмжээг шалгуур үзүүлэлт болгон талуудад баталгаа өгдөг байна.

ДЭЛХИЙН КИБЕР АЮУЛГҮЙ БАЙДЛЫН ИНДЕКС (GCI)

Америк, Англи, Герман тэргүүтэй өрнөдийн хөгжингүй орнууд кибер аюулгүй байдлаараа дэлхийд тэргүүлж байна. Цахим халдлагаас өөрийгөө хамгаалах чадамжийг Олон улсын харилцаа холбооны байгууллага *(International Telecommunication Union)*-аас гаргасан Дэлхийн кибер аюулгүй байдлын индексээр (The Global Cybersecurity Index) тодорхойлдог. Уг индекс (GCI) нь дэлхийн улс орнуудын кибер аюулгүй байдлын түвшинг тодорхойлсон итгэмжлэгдсэн лавлагаа болдог байна.[316]

Кибер аюулгүй байдал нь олон салбарын огтолцолд оршдог тул улс орнуудын кибер аюулгүй байдлын хөгжлийн түвшинг дараах 5 тулгуур шалгууруар үнэлдэг байна.

- Хууль, эрх зүйн орчин (Legislative environment)
- Техникийн арга хэмжээ (Technical Measures)
- Байгууллагын арга хэмжээ (Organization Measures)
- Чадавх хөгжүүлэх арга хэмжээ (Capacity Building Measures)
- Хамтын ажиллагааны орчин (Cooperation Measures)

Эдгээр шалгуур тус бүрт тухайн орны кибер аюулгүй байдлын түвшинг үнэлэх дараах тодорхой үзүүлэлтүүд багтдаг байна. Үүнд:[317]

Хууль эрх зүйн орчин

- Кибер аюулгүй байдлын тухай хууль
- Кибер аюулгүй байдлыг зохицуулах арга хэмжээ
- Спам, халдлагыг хязгаарлах хууль эрх зүй

Техникийн арга хэмжээ

- CIRT-(Computer Incident Response Team) Компьютерын гэмтлийн хариу арга хэмжээний баг
- CERT-(Computer Emergency Response Team) Компьютерийн түргэн тусламжийн баг
- CSIRT-(Computer Security Incident Response Team) Компьютерийн аюулгүй байдлыг хангах хариу арга хэмжээний баг

[315] https://www.iso.org/standard/44375.html
[316] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[317] https://www.secureworldexpo.com/industry-news/countries-dedicated-to-cybersecurity

- Стандарт хэрэгжүүлэх стратеги
- Стандартчиллын байгууллага
- Спам халдлагыг арилгахад чиглэсэн техникийн механизм, чадавх
- Кибер аюулгүй байдлын зорилгод үүлэн технологи ашиглах
- Хүүхэд багачуудыг онлайнаар хамгаалах механизм

Байгууллагын арга хэмжээ

- Үндэсний кибер аюулгүй байдлын стратеги
- Кибер аюулгүй байдлын агентлаг
- Кибер аюулгүй байдлын хэмжигдэхүүн (Cybersecurity metrics)

Чадавх бэхжүүлэх

- Олон нийтийг мэдээллээр хангах
- Кибер аюулгүй байдлын мэргэжилтнийг гэрчилгээжүүлэх, магадлан итгэмжлэх тогтолцоо
- Кибер аюулгүй байдлын талаар мэргэжилтэн бэлтгэх
- Кибер аюулгүй байдлын боловсролын тухай мэргэжлийн багшийн сургалт
- Кибер аюулгүй байдлын эрдэм шинжилгээ, судалгааны хөтөлбөр (цахим дэд бүтцийг хамгаалах хөтөлбөр)
- Урамшууллын механизм

Хамтын ажиллагаа

- Хоёр тал хүлээн зөвшөөрсөн байх
- Олон тал хүлээн зөвшөөрсөн байх
- Олон улсын оролцогч талуудтай байх
- Олон нийтийн болон хувийн хэвшлийн оролцогч талудтай байх
- Хамтрагч агентлагуудтай байх
- Сайн туршлага, үйл ажиллагаатай байх

Олон улсын харилцаа холбооны байгууллагын дээрх 5 шалгуур үзүүлэлтээр үнэлж, индексийг тодорхойлсноор тухайн улс кибер халдлагаас урьдчилан сэргийлэх чадамжтай эсэхийг тодорхойлох ба бодлогын түвшинд дээрх шалгууруудыг тогтоохыг зөвлөмж болгодог байна.

КИБЕР АЮУЛГҮЙ БАЙДЛЫН ШАЛГУУР ХАНГАСАН ШИЛДЭГ 10 УЛС

Олон улсын харилцаа холбооны байгууллага (ITU)-аас гаргасан судалгаагаар цахим аюулгүй байдлын 5 шалгуурыг хангасан цахим халдлагаас урьдчилан сэргийлэх чадавх өндөр улсуудын индекс[318] ($0 \leq N \leq 1$):

Улс	Индекс GCI score	Хууль Legal	Техник Technical	Байгууллага Organizaional	Чадавх Capacity building	Хамтын ажиллагаа Cooperation
Singapore	0.92	0.95	0.96	0.88	0.97	0.87
USA	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	087	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75

[318] https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/

Estonia	0.84	0.99	0.82	0.85	0.94	0.64
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70
Australia	0.82	0.94	0.96	0.86	0.94	0.44
Georgia	0.81	0.91	0.77	0.82	0.90	0.70
France	0.81	0.94	0.96	0.60	1	0.61
Canada	0.81	0.94	0.93	0.71	0.82	0.70

(Эх сурвалж: International Telecommunication Union 2017)

CyberDB судалгааны платформ нь[319] дэлхий даяар цахим салбарын шинэ технологи шийдлүүдийн талаар мэдээлэл судалгаа, дүн шинжилгээ хийдэг ба уг байгууллагаас кибер аюулгүй байдлаар дээрх жагсаалтад ороогүй орнууд болон тэргүүлэгч улсуудыг дараах байдлаар тодруулсан байна.

Америк: Жил бүр асар их хэмжээний кибер халдлагад өртөж буй орнуудын нэг бол Америкийн Нэгдсэн Улс юм. Тийм ч учраас кибер аюулгүй байдлын компаниудын 58 орчим хувь нь Америкт байрладаг бөгөөд кибер халдлагатай тэмцэх шинэ арга замуудыг судалсаар байна.[320]

Израиль: Кибер аюулгүй байдлын тогтолцоо сайтай улс[321] бөгөөд кибер аюулгүй байдлын чиглэлээр олон шинэ стартап компаниуд үүсч их хэмжээний санхүүжилт татаж байна.[322]

Орос: ОХУ-ыг цахим тагнуул, улс төрийн цахим халдлагад ихээхэн буруутгадаг ба цахим халдлагаас өөрсдийгөө маш сайн хамгаалах чадавх, боловсон хүчин, технологитой байна.

Хятад: 2017 онд Хятад улс Кибер аюулгүй байдлын тухай шинэ хууль баталж, кибер аюулгүй байдал, үндэсний аюулгүй байдлаа хамгаалахыг зорилго тавьсан юм.

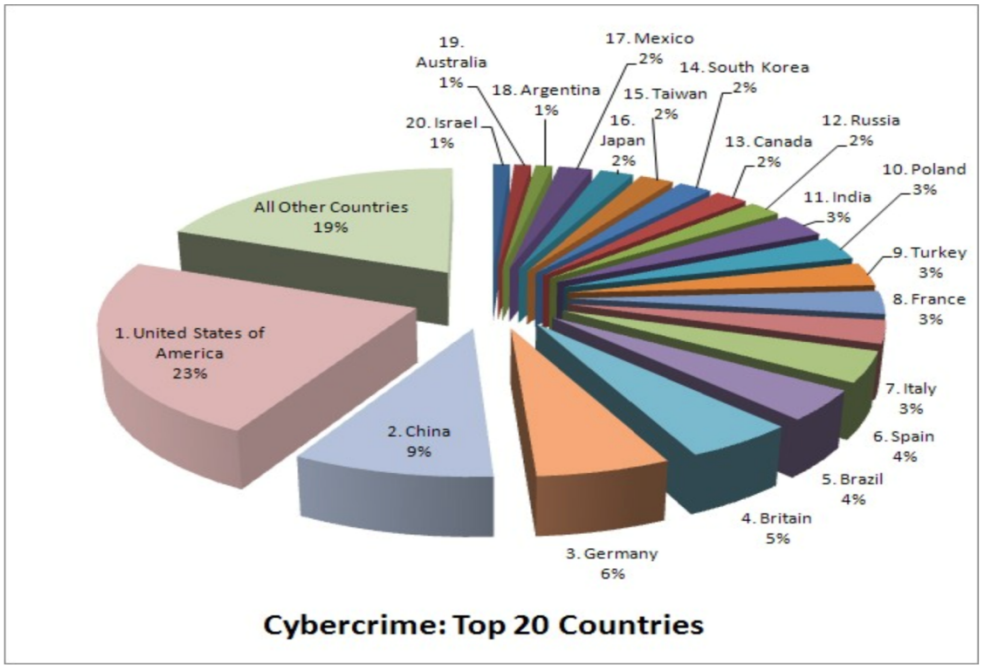
Эстони: Цахим засаглалаараа (e-governance) дэлхийд танигдсан бөгөөд 2007 оноос эхлэн цахим халдлагатай үр дүнтэй тэмцэж кибер аюулгүй байдлын сайн туршлагатай орнуудад тооцогддог.

ЦАХИМ ХАЛДЛАГАД ХАМГИЙН ИХ ӨРТДӨГ УЛСУУД

Symantec (Security research firm) судалгааны байгууллагаас цахим халдлагад хамгийн их өртдөг улсуудыг тодорхойлсон байна. Ингэхдээ дараах 6 түгээмэл халдлагыг шалгуур үзүүлэлт болгон дүн шинжилгээ хийсэн байна.[323]

1. Компьютерийн халдлага (Malicious computer activity)
2. Хортой кодоор халдах (Malicious code)
3. Спам (Spam zombies)
4. Өгөөш хаях замаар халдах (Phishing web site hosts)
5. Бот ашиглах (Bot)
6. Эх үүсвэрт шууд халдах (Attack origin rank)

[319] https://www.cyberdb.co
[320] https://cyberdb1.wpengine.com/database/usa/
[321] https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/
[322] https://cyberdb1.wpengine.com/database/israel/
[323] https://www.broadcom.com/products/cyber-security



BSA: ОЛОН УЛСЫН КИБЕР АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО ҮЙЛ АЖИЛЛАГАА

Сүүлийн жилүүдэд кибер аюулгүй байдлыг хангасан бодлого, эрх зүйн орчныг бүрдүүлэхээр дэлхийн бүх засгийн газрууд хичээн ажиллаж байна. Жил бүр кибер гэмт хэрэг дэлхийн эдийн засгаас хэдэн зуун тэрбум долларыг залилж, бизнесийн үйлчилгээг тасалдуулж, инновацийг саатуулж, ажлын байрны өсөлтийг царцааж байна[324]. Дэлхийн Засгийн газрууд эдгээр аюулыг үр дүнтэй даван туулах нь кибер аюулгүй байдлын талаарх тэнцвэртэй, цогц ухаалаг, үр дүнтэй бодлого боловсруулахаас хамаарна хэмээн үзэж байна.

BSA | Програм хангамжийн холбоо (www.bsa.org) нь дэлхийн засгийн газрууд болон олон улсын зах зээл дээрх програм хангамжийн компаниудыг нэгтгэсэн олон улсын байгууллага юм. Уг байгууллага нь АНУ-ын Вашингтон хотод төвтэй бөгөөд дэлхийн 60 гаруй оронд үйл ажиллагаа явуулдаг ба BSA нь хууль ёсны програм хангамжийг сурталчлах, технологийн шинэчлэлийг дэмжиж төрийн бодлогыг сурталчлах, олон улсын кибер аюулгүй байдлын бодлогын хүрээнд цахим аюулгүй байдлын цогц шийдлүүдийг санал болгодог байна.

BSA-гийн гаргасан бодлогын хүрээнд (Policy framework) засгийн газраас кибер аюулгүй байдлын бодлого явуулахдаа дараах үндсэн 6 зарчимд тулгуурлахыг зөвлөж байна.

- Бодлогыг олон улсын хэмжээнд хүлээн зөвшөөрөгдсөн техникийн стандартад нийцүүлэх;
- Бодлого нь эрсдэлд суурилсан, үр дүнд чиглэсэн, төвийг сахисан технологитой байх;
- Бодлого нь зах зээлийн механизмд суурилах;
- Бодлого нь инновацийг дэмжих уян хатан, дасан зохицох чадвартай байх;
- Төр, хувийн хэвшлийн хосолсон хамтын ажиллагаанд суурилах;
- Бодлого нь хувийн нууцыг хамгаалахад чиглэсэн байх.

[324] BSA International Cybersecurity Policy Framwork 2018

BSA: ҮНДЭСНИЙ КИБЕР АЮУЛГҮЙ БАЙДЛЫН ҮНДСЭН ЭЛЕМЕНТҮҮД:

ЗАСГИЙН ГАЗРЫН ҮЙЛ АЖИЛЛАГААНЫ СТРАТЕГИ

- Кибер аюулгүй байдлын асуудал эрхэлсэн үндэсний байгууллагатай байх;
- Оролцогч талуудын үүрэг, хариуцлагыг тодорхой болгох;
- Байгууллага хоорондын уялдааг бий болгох;
- Үндэсний кибер аюулгүй байдлын стратеги боловсруулах;
- Кибер аюулгүй байдлын дэд бүтцийг бий болгох;
- Үндэсний кибер аюулгүй байдлын төлөвлөгөө, дэд бүтцийг байнга шинэчлэх;
- Салбарын нарийн төлөвлөгөө гаргах;
- Төр болон хувийн хэвшлийн хамтын ажиллагаа оролцоог дэмжсэн бүтэц бий болгох;
- Засгийн газар болон холбогдох байгуулагуудын хамтын ажиллагааны механизмыг бий болгох.

КИБЕР АЮУЛГҮЙ БАЙДАЛ БА ЗАСГИЙН ГАЗАР

- Үндэсний кибер аюулгүй байдлын яаралтай хариу арга хэмжээний баг бий болгох;
- Цаг тухайд мэдээлэл солилцох, түүнийг дэмжих;
- Халдлагын талаарх мэдээллийн дэд бүтэц бий болгох;
- Хувийн мэдээлэлд халдахад мэдэгдэх стандартыг тогтоох;
- Засгийн газрын үйл ажиллагаа ил тод, сул талуудаа засдаг байх.

ЗАСГИЙН ГАЗРЫН ХАНГАМЖ ҮЙЛЧИЛГЭЭ

- Техник төхөөрөмж худалдан авахдаа төвийг сахих;
- Лицензтэй програм хангамж ашиглах;
- Програм хангамжийг борлуулагчаар баталгаажуулсан эсэхийг шалгах;
- Үүлэн үйлчилгээний (Cloud service) аюулгүй байдлын давуу талыг ашиглах;
- Техник, төхөөрөмж худалдан авахдаа аюулгүй байдлыг хангах, шалгах;
- Мэдээллийн технологийн системийг ухаалаг, аюулгүй байдлаар удирдах.

ЭРДЭМ ШИНЖИЛГЭЭ, СУДАЛГАА

- Кибер аюулгүй байдлын технологи, төхөөрөмж хэрэгслийн судалгаа, хөгжүүлэлтийг дэмжих.

КИБЕР АЮУЛГҮЙ БАЙДАЛ БА ХУВИЙН ХЭВШИЛ

- Кибер аюулгүй байдлын үр дүнд төвлөрөх;
- Эрсдэлд суурилсан, уян хатан бодлоготой байх;
- Дотоодын стандартаас гадна кибер аюулгүй байдлын дэд бүтцийг олон улсад хүлээн зөвшөөрөгдсөн стандарттай уялдуулах;
- Тэнцвэртэй, ил тод, олон улсын туршлагад суурилсан байх;
- Эх код, бусад оюуны өмчийг нууцлах;
- Бүтээгдэхүүн сонгохдоо зах зээлд суурилсан шийдлүүдийг ашиглах;
- Олон улсын дата ашиглах;
- Шинээр гарч ирж буй технологийг идэвхжүүлэх бодлогын орчинтой байх;

КИБЕР АЮУЛГҮЙ БАЙДАЛ БА ИРГЭН

- Кибер аюулгүй байдлын талаар олон нийтэд сурталчлах;

- Хэрэглэгчийн сонголтыг бүртгэх, мэдээлэх хэрэгсэл бий болгох;
- Боловсролын бүх түвшинд цахим аюулгүй байдлын мэдлэгийг суулгах;
- Кибер аюулгүй байдлын талаар боловсрол олгох сургалт зохион байгуулах;
- Кибер аюулгүй байдлын мэргэжилтнүүдийг олон талаар дэмжих.

КИБЕР ГЭМТ ХЭРЭГ

- Кибер гэмт хэрэгтэй тэмцэх тухай Будапешт конвенцид нийцсэн цогц хууль эрх зүйн орчинг бий болгох;
- Зөвхөн кибер халдлагад чиглэсэн тусгайлсан хууль эрх зүйн зохицуулалттай байх;
- Хууль сахиулах, хэрэгжүүлэгч байгууллагуудад техникийн сургалт, дэмжлэг үзүүлэх.

ОЛОН УЛСЫН ОРОЛЦОО

1. Кибер аюулгүй байдлын хамтын ажиллагааны гадаад бодлогод нэгдэх;
2. Олон улсын хамтын ажиллагаанд хамрагдах;
3. Экспортын хяналтын бодлогыг кибер аюулгүй байдлын хууль ёсны үйл ажиллагаанаас тусад нь авч үзэх;
4. Өөрийн орны нутаг дэвсгэрийг олон улсын кибер халдлагад ашиглахаас урьдчилан сэргийлэх;
5. Хувийн мэдээллийг хамгаалах, хүний эрхийг хамгаалах.

КИБЕР ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ ТУХАЙ БУДАПЕШТИЙН КОНВЕНЦ

Будапештийн Кибер гэмт хэрэгтэй тэмцэх тухай конвенц нь 2001 оны 11 сарын 23-нд батлагдаж 2004 оны 7-р сарын 1-ний өдрөөс хүчин төгөлдөр болсон. Өнөөдрийг7-р сарын 1-ний өдрөөс хүчин төгөлдөр болсон. 4 улс гарын үсэг зурж, нэгдсэн байна.[325] Гишүүн бус улсууд гарын үсэг зурж нэгдэхэд нээлттэй гэрээ юм.[326] Энэхүү конвенц нь Интернэт болон бусад компьютерийн сүлжээгээр дамжуулан үйлдэгдсэн зөрчил, ялангуяа зохиогчийн эрх, компьютертай холбоотой залилан, хүүхдийн садар самуун, сүлжээний аюулгүй байдлыг зөрчсөн гэмт хэргийн тухай олон улсын анхны гэрээ юм. Энэхүү конвенц нь компьютерийн сүлжээг ашиглан үйлдэгдсэн олон төрлийн зөрчил, гэмт хэргийг зогсоох зорилготой. Түүнчлэн нийгмийг кибер гэмт хэргээс хамгаалахад чиглэсэн нийтлэг хууль эрх зүйн бодлогыг хэрэгжүүлэх, ялангуяа зохих хууль тогтоомжийг баталж, олон улсын хамтын ажиллагааг дэмжихэд чиглэсэн байна.
Уг конвенцийн 2 бүлгийн 1-10 дугаар заалтад голлох 4 төрлийн халдлага зөрчлийг тусгасан байна.[327]

- Компьютерийн мэдээллийн системийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлын эсрэг гэмт хэрэг;
- Компьютертай холбоотой гэмт хэрэг, тухайлбал залилан, хуурамч баримт бичиг үйлдэх;
- Агуулгатай холбоотой зөрчил-хүүхдийн садар самуун бүхий агуулга гэх мэт;

[325] 2020 оны байлдлаар https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/
[326] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[327]https://statesassembly.gov.je/scrutinyreviewresearches/2018/research%20-%20briefing%20paper%20on%20council%20of%20europe%20convention%20on%20cybercrime%20-%2031%20october%202018.pdf

- Зохиогчийн эрхийн зөрчил.

Будапештийн конвенц нь цахим гэмт хэрэгтэй холбоотой хариуцлага хүлээлгэх эрх зүйн орчинг бүрдүүлэхээс гадна олон улсын хамтын ажиллагааны эрх зүйн үндсийг үндэслэсэн хууль эрх зүйн баримт бичиг юм.[328]

Уг конвенцид нэгдэн орсноор тухайн улс конвенцийг дотоодын хууль тогтоомжийн чиглэл болгон ашиглаж болох ба дараах давуу тулууд үүснэ.

- Олон улсын хамтын ажиллагааны хууль эрх зүйн үндэс суурь болно.
- Нэгдэн орсон талууд цаашид конвенцийн хөгжилд нэмэлт санал, протокол оруулж болно.
- Конвенцид гишүүнээр орсон орнууд энэхүү гэрээний дагуу байгуулагдсан цэгүүдэд 24 цаг холбоотой байна.
- Талууд хувийн хэвшилтэй хамтын ажиллагаагаа сайжруулж туршлагажих боломжтой.
- Оролцогч талууд өөрийн хүсэлтээр тэргүүлэгч, чадавхыг бэхжүүлэх төв болж болно.

Будапештийн конвенцитой уялдуулан дотоодын хууль тогтоомжийг бий болгосноор олон улсын цахим гэмт хэрэгтэй тэмцэх шалгуурыг хангах нөхцөл бүрдэх юм. Энэхүү конвенц нь олон улсын хамтын ажиллагааг сайжруулах бөгөөд давхар хууль эрх зүйн шаардлагыг хангахад тусалдаг. Конвенцийн дотоод процедурын зарим эрх мэдэл нь олон улсын хамтын ажиллагааны бүлэгт тусгагдсан байдаг. (Хавсралт 2)

[328] https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac#:~:text=The%20Budapest%20Convention%20requires%20States,cybercrime%20but%20any%20offence%20where

БҮЛЭГ III. МОНГОЛ УЛС ДАХЬ КИБЕР АЮУЛГҮЙ БАЙДАЛ

Монгол Улсын төр, засгаас харилцаа холбооны салбарыг хөгжүүлэх нь улс орны аюулгүй байдлыг хангахад чухал ач холбогдолтой гэдгийг онцгойлон анхаарч 1922 оноос эхлэн Дотоодыг хамгаалах газрын бүтцэд шуудан, телефон, радио, щифр холбооны нэгжийг байгуулж ирсэн нь Мэдээллийн аюулгүй байдлын газрын эх суурь болсон түүхтэй.

Техник технологи хурдтай хөгжиж буй өнөөгийн нийгэмд мэдээллийн аюулгүй байдал хурцаар тавигдаж байна. Монгол Улсын Үндэсний аюулгүй байдлын үзэл баримтлал, Тагнуулын байгууллагын тухай хуулийн 11.1.6, Харилцаа холбооны тухай хуулийн 20.3-т төрийн байгууллагуудыг кибер халдлагаас хамгаалах тогтолцоог бүрдүүлэхийг заасан бөгөөд энэ чиг үүргийг Мэдээллийн аюулгүй байдлын газар хэрэгжүүлэн ажиллаж байна[329].

Тус байгууллага нь төрийн мэдээлэл, харилцаа холбооны аюулгүй байдлыг хангах чиг үүргийн хүрээнд:

1. Төрийн болон онц чухал мэдээллийн сүлжээ, харилцаа холбооны аюулгүй байдлыг хангах, цахим аюул, заналтай тэмцэх;
2. Кибер аюулгүй байдлын талаар баримтлах бодлогын баримт бичгийг боловсруулах;
3. Төрийн байгууллагуудад кибер аюулгүй байдал, мэдээллийн аюулгүй байдалтай холбоотой эрсдэлийн үнэлгээ хийх;
4. Кибер аюулгүй байдлын талаар сургалт сурталчилгаа зохион байгуулах;
5. Төрийн болон нутгийн өөрөө удирдах байгууллагын хэрэгцээнд ашиглагдах тусгай хэрэглээний шуудангийн үйлчилгээ үзүүлэх;
6. Төрийн болон төрийн захиргааны байгууллагуудын хооронд төрийн нууц мэдээ, мэдээлэл дамжуулах, солилцох үеийн нууцлал аюулгүй байдлыг хангах гэсэн чиглэлээр үйл ажиллагаагаа явуулж байна.

МОНГОЛ УЛСЫН ҮНДЭСНИЙ АЮУЛГҮЙ БАЙДЛЫН ҮЗЭЛ БАРИМТЛАЛ

Монгол Улсын Үндэсний Аюулгүй Байдлын Үзэл Баримтлалд мэдээллийн аюулгүй байдлын талаар баримтлах бодлогыг дараах байдлаар тодорхойлсон байдаг.

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.

3.6.1.2.Нийгмийн сэтгэл зүй, тогтвортой байдал, хувь хүний ухамсар, ёс зүйд хөндлөнгөөс нөлөөлөх оролдлогыг хязгаарлана. Дайсагнал, ялгаварлан гадуурхах үзэл, үзэн ядалтыг сурталчилсан, дэмжсэн сурталчилгаа, мэдээллийг таслан зогсоох, саармагжуулах чадавхыг бий болгож, үл зөвшөөрөх сэтгэхүйг нийгэмд төлөвшүүлнэ.

[329] http://isd.gov.mn/

3.6.1.3.Үндэсний мэдээллийн дэд бүтцэд халдах аюулаас хамгаалах, эдийн засаг, нийгмийн чадавхыг сулруулах оролдлоготой тэмцэх чадавхыг бий болгоно.

3.6.1.4.Монгол Улсад гадаадын хөрөнгө оруулалттай хэвлэл мэдээллийн хэрэгсэл үндэсний аюулгүй байдалд харшилсан үйл ажиллагаа явуулбал үйл ажиллагаа явуулах эрхийг нь хязгаарлаж болно. Хэвлэл мэдээллийн хэрэгслийн эзэмшил, харьяалал нь ил тод байх бөгөөд үйл ажиллагаа нь бодитой, тэнцвэртэй, хариуцлагатай байна. Мэдээллийн хэрэгслээр үндэсний үнэт зүйлийг түлхүү нийтлэх, сурталчлахыг дэмжиж, гадны шашин, соёл, төрийн бодлогыг сурталчилсан агуулгатай мэдээллийг зохистой түвшинд хязгаарлана.

3.6.1.5.Мэдээллийн аюулгүй байдлын үндэсний хэмжээний бодлого, эрх зүйн зохицуулалт, стандарт, удирдлага, зохион байгуулалт, сургалтын тогтолцоог бий болгож нийгэм дэх ойлголт, мэдлэгийг төлөвшүүлнэ.

3.6.1.7.Төр, хувийн хэвшлийн байгууллагад мэдээллийн аюулгүй байдлын бодлого, дэг, эрсдэлийн удирдлага, дотоод аудит, үнэлгээний чадавхыг бий болгоно.

3.6.1.8.Мэдээллийн аюулгүй байдлын орчин үеийн дэвшилтэт, өртөг багатай шийдлийг зөвхөн эрсдэлийн үнэлгээний үндсэн дээр сонгон ашиглана. Төрийн байгууллага, онц чухал дэд бүтцийн объектын мэдээллийн аюулгүй байдлыг хангах чиг үүргийг өндөр түвшинд бэлтгэгдэж, итгэмжлэгдсэн үндэсний мэргэжилтнээр гүйцэтгүүлнэ.

3.6.1.9.Өрсөлдөх чадвартай мэдээлэл, харилцаа холбооны систем, техник хэрэгсэл, программ хангамжийн үндэсний үйлдвэрлэл болон мэдээллийн аюулгүй байдлын шийдэл боловсруулах ажиллагааг дэмжин хөгжүүлж технологийн хараат байдлыг бууруулна.

3.6.1.10.Мэдээлэл, харилцаа холбооны технологи, мэдээллийн аюулгүй байдлын чиглэлээр үндэсний суурь болон хавсарга судалгаа, шинжилгээ, сургалтыг онцгойлон дэмжинэ.

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.

ТАГНУУЛЫН БАЙГУУЛЛАГЫН ТУХАЙ ХУУЛЬ

11 дүгээр зүйл.Тагнуулын ерөнхий газрын үүрэг

11.1.Тагнуулын ерөнхий газар дараах үүрэг гүйцэтгэнэ:

11.1.6.Төрийн болон онц чухал мэдээллийн сүлжээ, харилцаа холбооны аюулгүй байдлыг хангах, цахим аюул, заналтай тэмцэх; */Энэ заалтад 2011 оны 6 дугаар сарын 10-ны өдрийн хуулиар өөрчлөлт, 2015 оны 7 дугаар сарын 9-ний өдрийн хуулиар өөрчлөн найруулсан./*

ХАРИЛЦАА ХОЛБООНЫ ТУХАЙ ХУУЛЬ

20 дугаар зүйл.Тусгай хэрэглээний холбооны сүлжээ

20.1.Монгол Улсын батлан хамгаалах, аюулгүй байдлыг хангах, гамшгаас хамгаалах, гэмт хэрэгтэй тэмцэх, нийгмийн хэв журам сахиулах, төрийн болон нутгийн удирдлагын байгууллагын хэрэгцээнд зориулан тусгай хэрэглээний холбооны сүлжээг байгуулан ажиллуулж болно. */Энэ хэсэгт 2019 оны 05 дугаар сарын 30-ны өдрийн хуулиар өөрчлөлт оруулсан./*

20.2.Тусгай хэрэглээний холбооны сүлжээ төрийн хамгаалалтад байна.

20.3.Тусгай хэрэглээний холбооны сүлжээ байгуулах, ашиглах журмыг Засгийн газар тогтооно.

20.4.Тусгай хэрэглээний холбооны сүлжээнд цахилгаан холбооны суваг, тоног төхөөрөмжийг үйлчлэгчтэй байгуулсан гэрээний үндсэн дээр ашиглана.

20.5.Харилцаа холбооны сүлжээгээр дамжуулах тусгай хэрэглээний холбооны мэдээллийн нууцлалт, хамгаалалтыг энэ хуулийн 20.1-д заасан байгууллага хариуцна

БҮЛЭГ IV. ГАДААДЫН ЗАРИМ ОРНЫ ТУРШЛАГА

БНСУ

БНСУ 1980 оноос эхлэн үндэсний мэдээллийн аюулгүй байдал болон нийгмийн сүлжээн дэх асуудлуудыг зохицуулах хууль боловсруулж эхэлсэн ба 1986 онд Харилцаа холбооны сүлжээг сайжруулах тухай хууль (Expansion and promotion of utilization of communications network act) анх баталж байжээ[330]. Одоогоор кибер аюулгүй байдалтай холбоотой асуудлыг хэд хэдэн хуулиар зохицуулж байна. Тухайлбал[331]:

- Сүлжээний тухай хууль (Network act),
- Харилцаа холбооны нууцыг хамгаалах тухай хууль (Protection of communication secret act),
- Мэдээлэл, харилцаа холбооны дэд бүтцийг хамгаалах тухай (The act on protection of information and communication infrastructure),
- Цахим засаглалын тухай хууль (Electronic government act),
- Үндэсний батлан хамгаалахын мэдээллийн дэд бүтцийг бий болгох, мэдээллийн нөөцийг удирдах тухай хууль (Act on Establishment of infrastructure for information of national defence and management of information resources for national defence),
- Зээлийн мэдээллийн ашиглалт, хамгаалалтын тухай хууль (Credit information use and protection act),
- Байршлын мэдээллийг хамгаалах тухай хууль (Act on protection use of location information),
- Үйлдвэрлэлийн технологийг хамгаалах тухай хууль (Act on Prevention of Divulgence and protection of industrial technology),
- Цахилгаан холбооны бизнесийн болон санхүүгийн луйврын тухай хууль (Telecommunication business act and special act on financial fraud) зэрэг хуулиуд багтдаг байна.

Үндэсний хэмжээнд кибер халдлагаас сэргийлэх зорилгоор “Кибер аюулгүй байдлын менежментийн зохицуулалтын (National cyber security management regulation) журам”-ыг Үндэсний Ассамблей баталсан байна. Уг журмаар Засгийн газрын байгууллагуудын

[330] Introduction to Korean cyber security Law
[331] https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/korea

(Үндэсний тагнуулын албаны Үндэсний аюулгүй байдлын төв, Хөх ордон дахь үндэсний аюулгүй байдлын алба) эрх үүрэг, оролцоог тодорхойлсон байна[332]. Кибер халдлагаас хамгаалах мэдээллийн дэд бүтцийн тухай хууль нь үндэсний аюулгүй байдалтай шууд холбогддог ба нийгэмд өдөр бүр тулгардаг эрчим хүч, эрүүл мэнд, банк санхүүгийн цахим үйл ажиллагааг уг хуулиар зохицуулдаг байна. Солонгосын Засгийн газар 2002 онд Мэдээллийн дэд бүтцийг хамгаалах тухай хуулийг (Protecting critical information infrastrucutre act) баталсан байна. Уг хууль нь дараах бүтэцтэй байна.

МЭДЭЭЛЭЛ, ХАРИЛЦАА ХОЛБООНЫ ДЭД БҮТЦИЙГ ХАМГААЛАХ ТУХАЙ ХУУЛЬ

(The Act On Protection Of Information And Communication Infrastructure)

1 дүгээр зүйл. Зорилго
Энэхүү хуулийн зорилго нь харилцаа холбооны нууц, нууцыг хамгаалах, харилцаа холбооны эрх чөлөөг тогтоох, зохих журмын дагуу шийдвэр гаргах замаар харилцаа холбооны эрх чөлөөг зохицуулахад оршино.
2 дугаар зүйл. Нэр томьёоны тайлбар
3 дугаар зүйл. Харилцаа холбооны нууцыг хамгаалах
4 дүгээр зүйл. Хууль бус хяналт шалгалтаар олж авсан мэдээлэл хууль бусаар чагнах, цахилгаан холбооны агуулгыг нотлох баримт болгон ашиглахыг хориглох тухай
5 дугаар зүйл. Эрүүгийн байцаалтын мэдээллийг хязгаарлах зөвшөөрлийн шаадлага
6 дугаар зүйл. Эрүүгийн байцаалтын мэдээллийг хязгаарлах зөвшөөрлийн арга хэмжээ авах эрх олгох журам
7 дугаар зүйл. Үндэсний аюулгүй байдалд нийцүүлэн харилцаа холбооны хяналт
8 дугаар зүйл. Онцгой байдлын үеийн харилцаа холбоог хязгаарлах арга хэмжээ
9 дүгээр зүйл. Харилцаа холбоонд хяналт тавих арга хэмжээний хэрэгжилт
10 дугаар зүйл. Чагнах төхөөрөмжийн зөвшөөрөл олгох журам
11 дүгээр зүйл. Нууцлалын үүрэг
12 дугаар зүйл. Харилцаа холбооны арга хэмжээгээр олж авсан материалыг ашиглахыг хязгаарлах тухай
13 дугаар зүйл. Эрүүгийн байцаан шийтгэх үйл ажиллагаанд мэдээлэл өгөх журам
14 дүгээр зүйл. Бусдын нууцыг задруулах, зөрчих тухай
15 дугаар зүйл. Үндэсний ассамблейн хяналт
16 дугаар зүйл. Торгуулийн заалт
17 дугаар зүйл. Торгууль оногдуулах тухай
18 дугаар зүйл. Гэмт хэрэг үйлдэхийг завдах тухай

МАЛАЙЗ УЛС

Малайз улс кибер аюулгүй байдалтай холбоотой дараах цогц хуулиудыг баталсан байна. Үүнд:

- Зохиогчийн эрхийн тухай хууль (The Copyright (AmendmentAct),
- Тоон гарын үсгийн тухай хууль (The Digital Signature Act),
- Телемедициний тухай хууль (The Telemedicine Act),
- Харилцаа холбоо ба мультимедиан тухай хууль (The Communications and Multimedia Act),

[332] Ibid Page 28

- Цахим худалдааны тухай хууль(Electronic Commerce Act),
- Төрийн цахим үйл ажиллагааны тухай хууль (Electronic Government Activities Act),
- Хувийн мэдээллийг хамгаалах тухай хууль (Personal Data Protection Act), Эрүүгийн хууль (Penal Code),
- Хуурамч мэдээллийн эсрэг хууль (The Anti-Fake News Act) гэх мэт

Малайз улс 1997 онд Компьютерийн гэмт хэрэгтэй тэмцэх тухай хуулийг (The Computer Crimes Act) баталсан ба 2011 оны 12-р сарын 1-нд дахин шинэчилсэн байна. Уг хуулиар зохицуулж буй харилцаа:[333]

КОМПЬЮТЕРИЙН ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ ТУХАЙ ХУУЛЬ, 1997 ("ССА")

Бүлэг 1.

1. Энэ хууль нь 1997 онд батлагдсан Компьютерийн гэмт хэрэгтэй тэмцэх тухай хуулиас эшэлсэн болно. Энэхүү хууль нь Ерөнхий сайдыг томилсон өдрөөс эхлэн хүчин төгөлдөр болно
2. Нэр томьёоны тайлбар

Бүлэг 2.

Компьютерийн мэдээлэл рүү зөвшөөрөлгүй нэвтрэх

Тухайн компьютер болон компьютерийн мэдээлэл (дата)-нд зөвшөөрөлгүй, санаатайгаар нэвтрэх

Энэ хэсэгт заасны дагуу гэм буруутай гэж үзвэл 50 мянган рингитээс ихгүй торгууль ногдуулах буюу таван жилээс дээшгүй хугацаагаар хорих шийтгэл ногдуулна.

Үйл ажиллагаанд нэвтрэх эрхгүйгээр халдах

Эрүүгийн хуулийн 573-р зүйлд зааснаар залилан мэхлэх, хохирол учруулах гэмт хэргийн үйлдэл,

Өөрөө болон бусад хүнээр халдлага үйлдэх,

Энэ хэсэгт заасны дагуу гэмт хэрэг үйлдсэн гэм буруутай этгээдэд 150 мянган рингитээс ихгүй хэмжээний торгууль ногдуулах, эсхүл арван жилээс дээшгүй хугацаагаар хорих ялаар шийтгэнэ.

Аливаа компьютерын өгөгдөл агуулгыг зөвшөөрөлгүй өөрчлөх

Аливаа компьютерийн агуулгыг зөвшөөрөлгүй өөрчлөх үйлдэл хийсэн тохиолдолд гэм буруутайд тооцно.

Энэ хэсэгт заасны дагуу гэмт хэрэг үйлдсэн гэж үзвэл 100-500 мянган рингитээс дээшгүй торгууль ногдуулах, эсхүл долоогоос арван жилийн хорих ялаар шийтгэнэ.

Зөвшөөрөлгүй харилцах

-Компьютерт нэвтрэх дугаар, код, нууц үг эсвэл бусад хэрэгслийг шууд болон дам байдлаар мэдэгдсэн тохиолдолд гэм буруутай гэж үзнэ. Энэ хэсэгт заасны дагуу гэмт хэрэг үйлдсэн тохиолдолд 25 мянган рингитээс дээшгүй торгууль ногдуулах, эсхүл гурван жил хорих ялаар шийтгэнэ.

Гэм буруутанд шийтгэл оногдуулах

Энэхүү хуулийн дагуу гэмт хэрэг үйлдэхийг завдсан эсвэл үйлдсэн тохиолдолд гэм буруутай ба шийтгэлийг оногдуулна.

[333] https://cyrilla.org/ar/entity/xqej2atn2lh?file=1568729651356shamgdeopv.pdf&page=5

Аливаа компьютерт хадгалагдаж байгаа, програм өгөгдөл эсвэл бусад мэдээллийг хууль бусаар зөвшөөрөлгүй нэвтрэх,

Бүлэг 3.

Нэмэлт болон ерөнхий заалтууд[334]

Халдлагын цар хүрээ

Энэхүү хуулийн заалтад гэмт этгээдийн иргэншил болон оршин байгаа харьяаллаас үл хамааран Малайзын нутаг дэвсгэрт хүчин төгөлдөр үйлчлэх бөгөөд энэ хуулийн дагуу гэмт хэрэг үйлдсэн этгээдийг Малайзын Компьютерийн гэмт хэрэгтэй тэмцэх хуулийн дагуу шийтгэдэг байна.

Эрэн сурвалжлах, хураах, баривчлах бүрэн эрх

Энэ хуульд заасны дагуу гэмт хэрэг үйлдсэн болохыг нотлох баримтанд үндэслэх эсвэл шүүгчийн шийдвэр гарвал, байцаагчаас дээш цолтой (above the rank of Inspector) албан хаагч гэмт хэргийн газар хүчээр нэвтрэх, шаардлагатай бол саатуулах, тэнд байгаа нотлох баримтыг хайх, хураах эрхтэй байдаг байна.

Мөрдлөгт саад учруулах

Уг хуульд заасны дагуу албан хаагчийн, эрх үүргийн дагуу мөрдлөг хийх явцад халдах, саад учруулах, байцаалтыг хойшлуулахыг хориглодог байна.

Яллах

Уг хуулийн дагуу яллах ажиллагааг Улсын яллагчийн албан ёсны шийдвэрээр яллахаас бусад тохиолдолд яллахгүй.

[334] https://www.nacsa.gov.my/legal.php

ХАВСРАЛТ

Хавсралт 1. Олон улсын кибер аюулгүй байдлын чиглэлээр үйл ажиллагаа явуулж буй байгууллагууд[335]

Байгууллагын нэр	Холбоос	Хамрах хүрээ
United Nations Internet Governance Forum	https://www.intgovforum.org/multilingual/	Global
United States National Cyber security and Communications Integration Center (NCCIC)	https://www.cisa.gov/about-cisa	National, Global
Messaging and Anti Abuse Working Group (MAAWG)	www.maawg.org	Global
Anti-Abuse Working Group	www.ripe.net	Global
Forum for Incident Response Security Teams (FIRST)	www.firest.org	Global
Asia Pacific Computer Emergency Response Team (AP CERT)	www.apcert.org	Regional
Network Operators Groups (NOGs)	https://en.wikipedia.org/wiki/Internet_network_operators%27_group	Global
Asia Pacific Economic Cooperation (APEC)	www.apec.org	Regional
ICANN Security and Stability Working Group	www.icann.org	Global
Cooperative Cyber Defense and Center of Excellence (CCDCOE)	www,ccdcoe.org	Regional, Global
Council of Europe; Convention on Cybercrime	www.conventions.coe.int	Global
INTERPOL	Interpolnyc.com	Global
Internet Society (ISOC)	www.internetsociety.org	Global

[335] https://www.itic.org/dotAsset/c/c/cc91d83a-e8a9-40ac-8d75-0f544ba41a71.pdf

Хавсралт 2. **Будапештийн конвенцид нэгдсэн орнууд**[336]

(2020 оны 6 сарын байдлаар)

Конвенцид нэгдэн орсон улсууд	
Andorra	Latvia
Argentina	Liechtenstein
Armenia	Lithuania
Australia	Luxembourg
Austria	Malta
Azerbaijan	Mauritius
Belgium	Republic of Moldova
Bosnia and Herzegovina	Monaco
Bulgaria	Montenegro
Cabo Verde	Morocco
Canada	Netherlands
Chile	North Macedonia
Colombia	Norway
Costa Rica	Panama
Croatia	Paraguay
Cyprus	Peru
Czech Republic	Philippines
Denmark	Poland
Dominican Republic	Portugal
Estonia	Romania
Finland	San Marino
France	Senegal
Georgia	Serbia Slovak
Germany	Republic Slovenia
Ghana	Spain
Greece	Sri Lanka
Hungary	Switzerland
Iceland	Tonga
Israel	Turkey
Italy	Ukraine
Japan	United Kingdom
	United States of America

[336] https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac#:~:text=The%20Budapest%20Convention%20requires%20States,cybercrime%20but%20any%20offence%20where

Хавсралт 3. Будапештийн Кибер гэмт хэрэгтэй тэмцэх тухай конвенцийн бүтэц

Бие даасан хууль	Нотлох баримт, мөрдөн байцаахтай холбоотой процедурын хууль	Олон улсын хамтын ажиллагаа
Art. 2 – Illegal access Art. 3 – Illegal interception Art. 4 – Data interference Art. 5 – System interference Art. 6 – Misuse of devices Art. 7 – Computer-related forgery Art. 8 – Computer-related fraud Art. 9 – Child pornography Art. 10 – IPR offences Art. 11 – Attempt, aiding, abetting Art. 12 – Corporate liability	Art. 14 – Scope of procedural provisions Art. 15 – Conditions and safeguards Art. 16 – Expedited preservation Art. 17 – Expedited preservation and partial disclosure of traffic data Art. 18 – Production order Art. 19 – Search and seizure Art. 20 – Real-time collection traffic data Art. 21 – Interception of content data	Art. 23 – General principles Art. 24 – Extradition Art. 25 – General rules Art. 26 – Spontaneous information Art. 27 – MLA in absence of treaty Art. 28 – Confidentiality Art. 29 – Expedited preservation Art. 30 – Partial disclosure traffic data Art. 31 – MLA accessing data Art. 32 – Transborder access Art. 33 – MLA collection traffic data Art. 34 – MLA interception content Art. 35 – 24/7 point of contact

АШИГЛАСАН МАТЕРИАЛ

- Мэдээллийн аюулгүй байдлын газар http://www.isd.gov.mn/?lang=mn&cat=7
- Төрийн мэдээлэл холбооны газар https://www.cita.gov.mn/
- Эрх зүй мэдээллийн систем https://www.legalinfo.mn/
- https://www.nato.int/cps/en/natohq/topics_140739.htm
- https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf
- https://www.vmware.com/topics/glossary/content/cyber-espionage
- https://www.iso.org/standard/44375.html
- https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
- https://www.secureworldexpo.com/industry-news/countries-dedicated-to-cybersecurity
- https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/
- https://www.cyberdb.co
- https://cyberdb1.wpengine.com/database/usa/
- https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/
- https://cyberdb1.wpengine.com/database/israel/
- https://www.broadcom.com/products/cyber-security
- BSA International Cybersecurity Policy Framwork 2018
- https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
- https://statesassembly.gov.je/scrutinyreviewresearches/2018/research%20-%20briefing%20paper%20on%20council%20of%20europe%20convention%20on%20cybercrime%20-%2031%20october%202018.pdf
- https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac#:~:text=The%20Budapest%20Convention%20requires%20States,cybercrime%20but%20any%20offence%20where