КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЧАДАВХЫН ҮНЭЛГЭЭ

Монгол Улс

2025 оны 2 сар

(ЯПОНЫ ОЛОН УЛСЫН ХАМТЫН АЖИЛЛАГААНЫ БАЙГУУЛЛАГА (ЖАЙКА)-ЫН ЗАХИАЛГААР ИНФО СЕК ПЛАС ХХК ОРЧУУЛАВ.)

Global Cyber Security Capacity Centre
OXFORD MARTIN SCHOOL
UNIVERSITY OF OXFORD
DEPARTMENT OF COMPUTER SCIENCE

АГУУЛГА

Баримт бичгийн удирдлага 4
Товчилсон үгсийн тайлбар 5
ОРШИЛ 6
ТАНИЛЦУУЛГА 22
Кибер аюулгүй байдлын чадавхын хэмжээс 22
Кибер аюулгүй байдлын чадавхын төлөвшлийн үе шат 24
МОНГОЛЫН КИБЕР АЮУЛГҮЙ БАЙДЛЫН НӨХЦӨЛ БАЙДАЛ 25
ҮНЭЛГЭЭНИЙ ТАЙЛАН 27
Хураангуй 27
ХЭМЖЭЭС 1 28
КИБЕР АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО БОЛОН СТРАТЕГИ 28
ҮР ДҮНГИЙН ТОЙМ 29
D 1.1 КИБЕР АЮУЛГҮЙ БАЙДЛЫН ҮНДЭСНИЙ СТРАТЕГИ 29
D 1.2 ЗӨРЧИЛД ХАРИУ ҮЗҮҮЛЭХ БОЛОН ОНЦГОЙ БАЙДЛЫН МЕНЕЖМЕНТ 34
D 1.3 ОНЦ ЧУХАЛ БҮТЦИЙН ХАМГААЛАЛТ 40
D 1.4 БАТЛАН ХАМГААЛАХ БОЛОН ҮНДЭСНИЙ АЮУЛГҮЙ БАЙДАЛД КИБЕР АЮУЛГҮЙ БАЙДЛЫН ОРОЛЦОО 46
ЗӨВЛӨМЖ 48
ХЭМЖЭЭС 2 53
КИБЕР АЮУЛГҮЙ БАЙДЛЫН СОЁЛ БОЛОН НИЙГЭМ 53
ҮР ДҮНГИЙН ТОЙМ 54
D 2.1 КИБЕР АЮУЛГҮЙ БАЙДЛЫН СЭТГЭЛГЭЭ 54
D 2.2 ОНЛАЙН ҮЙЛЧИЛГЭЭНД ИТГЭХ ИТГЭЛ 57
D2.3 ХУВИЙН МЭДЭЭЛЛИЙГ ОНЛАЙН ОРЧИНД ХАМГААЛАХ ТАЛААР ХЭРЭГЛЭГЧДИЙН ОЙЛГОЛТ 59
D 2.4 ТАЙЛАГНАХ МЕХАНИЗМ 60
D 2.5 ХЭВЛЭЛ МЭДЭЭЛЭЛ БОЛОН ОНЛАЙН ПЛАТФОРМУУД 61
ЗӨВЛӨМЖ 63
ХЭМЖЭЭС 3 66
КИБЕР АЮУЛГҮЙ БАЙДЛЫН МЭДЛЭГ БОЛОН ЧАДАМЖ БИЙ БОЛГОХ 66
ҮР ДҮНГИЙН ТОЙМ 67
D 3.1 КИБЕР АЮУЛГҮЙ БАЙДЛЫН ХАНДЛАГА БИЙ БОЛГОХ 67
D 3.2 КИБЕР АЮУЛГҮЙ БАЙДЛЫН БОЛОВСРОЛ 70
D 3.3 КИБЕР АЮУЛГҮЙ БАЙДЛЫН МЭРГЭЖЛИЙН СУРГАЛТ 72
D 3.4 КИБЕР АЮУЛГҮЙ БАЙДЛЫН СУДАЛГАА, ИННОВАЦ 76
ЗӨВЛӨМЖ 77

ХЭМЖЭЭС 4 ..... *82*
ХУУЛЬ, ЭРХ ЗҮЙН ЗОХИЦУУЛАЛТ *82*
ҮР ДҮНГИЙН ТОЙМ 83
D 4.1 ХУУЛЬ, ЭРХ ЗҮЙН ЗОХИЦУУЛАЛТУУД 83
D 4.2 ХОЛБОГДОХ ХУУЛЬ ЭРХ ЗҮЙН ОРЧИН 91
D 4.3 ХУУЛЬ, ЗОХИЦУУЛАЛТЫН ЧАДАМЖ БОЛОН ХҮЧИН ЧАДАЛ 94
D 4.4 КИБЕР ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ АЛБАН БОЛОН АЛБАН БУС ХАМТЫН АЖИЛЛАГААНЫ ТОГТОЛЦОО 97
ЗӨВЛӨМЖ 98
ХЭМЖЭЭС 5 ..... *102*
СТАНДАРТ БОЛОН ТЕХНОЛОГИ *102*
ҮР ДҮНГИЙН ТОЙМ 103
D 5.1 СТАНДАРТЫН УЯЛДАА ХОЛБОО 103
D 5.2 АЮУЛГҮЙН БАЙДЛЫН ХЯНАЛТУУД 106
D 5.3 ПРОГРАММ ХАНГАМЖИЙН ЧАНАР 109
D 5.4 ХАРИЛЦАА ХОЛБОО БОЛОН ИНТЕРНЭТ ДЭД БҮТЭЦ 110
D 5.5 КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЗАХ ЗЭЭЛ 111
D 5.6 ХАРИУЦЛАГАТАЙГААР МЭДЭЭЛЭЛ ИЛ БОЛГОХ 112
ЗӨВЛӨМЖ 114
НЭМЭЛТЭЭР АНХААРАХ ЗҮЙЛС 117
ХАВСРАЛТ *118*
СУДАЛГААНЫ АРГА ЗҮЙ –ТҮВШНИЙГ ХЭМЖИХ НЬ 118

Баримт бичгийн удирдлага

Тэргүүлэх судлаачид: *Луиз Аксон, Жо Фулвуд*

Хянасан: *Профессор Уильям Даттон, Профессор Майкл Голдсмит, Доктор Жэйми Сондерс, Профессор Дэвид Уолл, Профессор Басие Вон Солмс*

Баталсан: *Профессор Майкл Голдсмит*

Хувилбар	*Огноо*	*Тэмдэглэл*
1	*08/12/2024*	Тэргүүлэх судлаачид төслийн анхны хувилбарыг Оксфордын Их сургуулийн Олон Улсын Кибер Аюулгүй Байдлын Чадавхын Төвийн (GCSCC) техникийн зөвлөлд хүргүүлэв.
2	*20/12/2024*	Хоёр дахь хувилбарыг судалгаа зохион байгуулагчдад хүргүүлэв.
3	*20/01/2025*	Зохион байгуулагчдын зүгээс санал хүсэлт хүлээн авсан.
4	*26/01/2025*	Гурав дахь хувилбарыг судалгаа зохион байгуулагчдад илгээв.
5	*04/02/2025*	Зохион байгуулагчдаас эцсийн санал хүсэлт хүлээн авав.
6	*05/02/2025*	Эцсийн тайлан зохион байгуулагчдад хүлээлгэн өгөв.

Товчилсон үгсийн тайлбар

APT	Зорилтот халдлага (Advanced Persistent Threat)
CA	Гэрчилгээжүүлэлтийн байгууллага (Certification Authority)
CII	Онц чухал мэдээллийн дэд бүтэц (Critical Information Infrastructure)
CSIRT	Компьютерын аюулгүй байдлын зөрчилд хариу үзүүлэх баг (Computer Security Incident Response Team)
CTI	Кибер аюул заналын мэдээлэл (Cyber threat intelligence)
EU	Европын Холбоо (European Union)
FIRST	Зөрчлийн хариу арга хэмжээ болон аюулгүй байдлын багуудын форум (Forum of Incident Response and Security Teams)
GCI	Дэлхийн кибер аюулгүй байдлын индекс (Global Cybersecurity Index)
GDPR	Мэдээлэл хамгаалах ерөнхий зохицуулалт (General Data Protection Regulation)
GIA	Тагнуулын Ерөнхий Газар (General Intelligence Agency)
ISAC	Мэдээлэл солилцоо, шинжилгээний төв (Information Sharing and Analysis Centre)
ISO	Олон улсын стандартчиллын байгууллага
KPI	Гүйцэтгэлийн түлхүүр үзүүлэлт (Key Performance Indicator)
ISMS	Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо (Information Security Management System)
ISP	Интернэт үйлчилгээ үзүүлэгч (Internet Service Provider)
IXP	Интернэт солилцооны төв (Internet Exchange Point)
ITU	Олон улсын цахилгаан холбооны холбоо (International Telecommunication Union)
JICA	Японы олон улсын хамтын ажиллагааны байгууллага (Japan International Cooperation Agency)
MDDIC	Цахим хөгжил, инновац, харилцаа холбооны яам (Ministry of Digital Development, Innovation and Communication)
MNCERT/CC	Цахим аюулгүй байдлын мэдээлэл, удирдлагын төв
MoU	Харилцан ойлголцлын санамж бичиг (Memorandum of Understanding)
NATO	Умард Атлантын гэрээний байгууллага (North Atlantic Treaty Organization)
NCS	Кибер аюулгүй байдлын үндэсний стратеги (National Cybersecurity Strategy)
NDCI	Үндэсний дата төв (National Data Centre)
NGO	Төрийн бус байгууллага (Non-Governmental Organisation)
NIDS	Сүлжээний халдлага илрүүлэх систем (Network Intrusion-Detection System)
NRI	Сүлжээний бэлэн байдлын индекс (Network Readiness Index)
OSCE	Европын аюулгүй байдал, хамтын ажиллагааны байгууллага (Organization for Security and Co-operation in Europe)
PCI DSS	Төлбөрийн картын аюулгүй байдлын стандарт (Payment Card Industry Data Security Standard)
PKI	Нийтийн түлхүүрийн дэд бүтэц (Public-Key Infrastructure)
TLS	Тээвэрлэлтийн давхаргын аюулгүй байдал (Transport Layer Security)
UN	Нэгдсэн Үндэстний Байгууллага (United Nations)
UNDP	НҮБ-ын Хөгжлийн Хөтөлбөр (United Nations Development Program)

ОРШИЛ

Японы Олон Улсын Хамтын Ажиллагааны Байгууллага /цаашид ЖАЙКА гэх/ -тай хамтран Дэлхийн Кибер Аюулгүй Байдлын Чадавхын Төв /ДКАБЧТ, эсхүл цаашид "Чадавхын Төв" гэх/ нь Монгол Улсын кибер аюулгүй байдлын чадавхын үнэлгээг Цахим Хөгжил, Инновац, Харилцаа Холбооны Яам /цаашид ЦХИХХЯ гэх)-ын урилгаар хийж гүйцэтгэв. Энэхүү үнэлгээний зорилго нь Монгол Улсад кибер аюулгүй байдлын чадавхын талаарх ойлголтыг бий болгож, кибер аюулгүй байдлын хөрөнгө оруулалтыг стратегийн ач холбогдолтой эрэмблэн, оновчтой төлөвлөх боломжийг бүрдүүлэхэд оршино.

2024 оны 10 сарын 2-7 хооронд зохион байгуулагдсан дугуй ширээний хэлэлцүүлэгт боловсролын байгууллагууд, эрүүгийн шүүх, хууль сахиулах байгууллагууд, мэдээллийн технологийн мэргэжилтнүүд, төрийн байгууллагуудын төлөөлөгчид, онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын төлөөлөл, бодлого боловсруулагчид, төр болон хувийн хэвшлийн мэдээллийн технологийн албан хаагчид (санхүүгийн байгууллагуудыг оролцуулан), харилцаа холбооны компаниуд, банкны салбар болон олон улсын түншүүд гэсэн тал бүрийн оролцогч талууд оролцсон.

Энэхүү хэлэлцүүлэг уулзалтыг Чадавхын Төвийн боловсруулсан Кибер Аюулгүй Байдлын Чадавхын Төлөвшлийн Загвар (цаашид ЧТЗ гэх) ашиглан зохион байгуулсан бөгөөд ЧТЗ нь төлөвшлийг дараах таван хэмжээсээр тодорхойлдог:

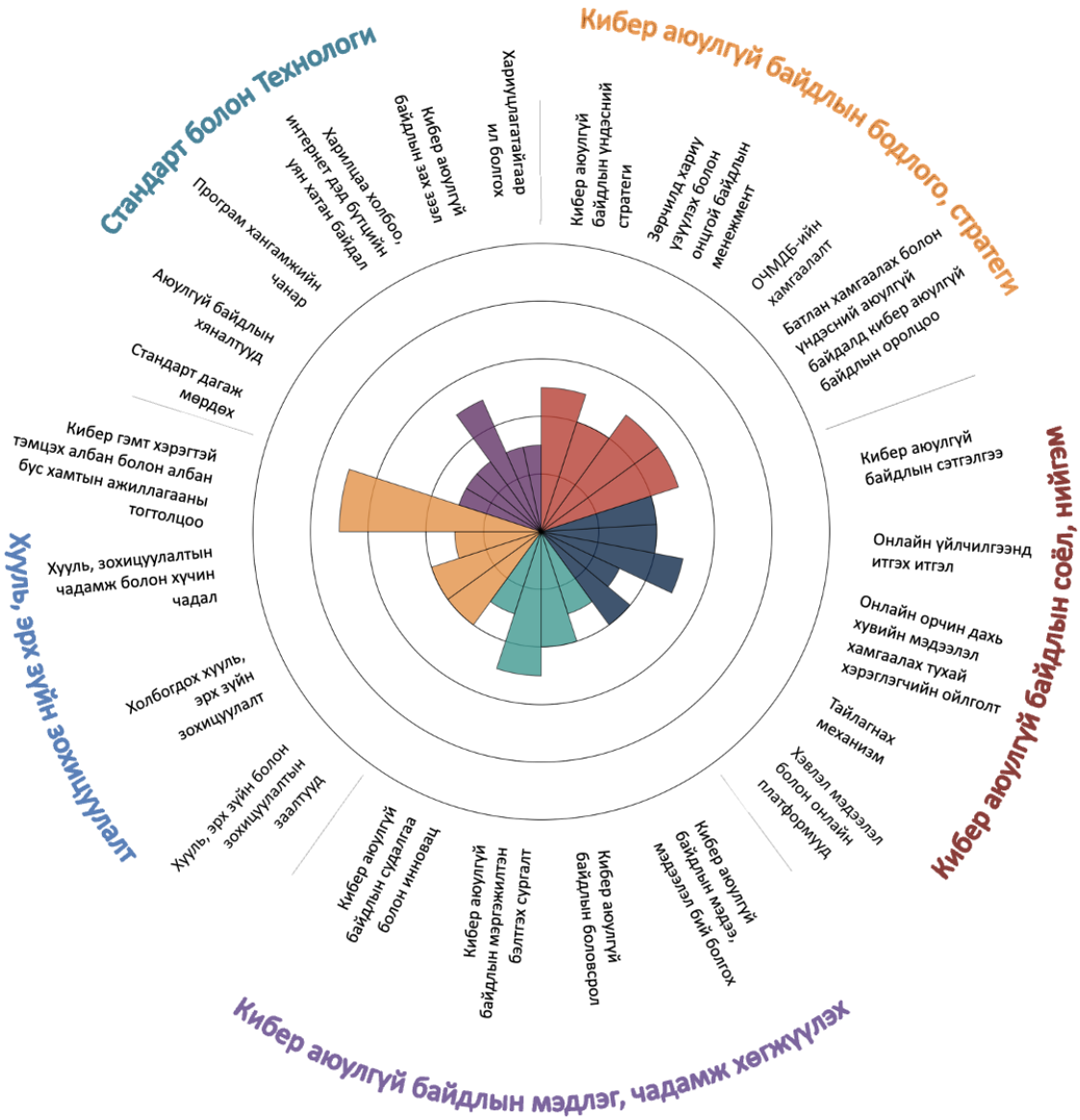
- *Кибер аюулгүй байдлын бодлого болон стратеги*
- *Кибер аюулгүй байдлын соёл болон нийгэм*
- *Кибер аюулгүй байдлын мэдлэг болон чадамж*
- *Хууль эрх зүй болон зохицуулалтын орчин*
- *Стандарт болон технологи*

Хэмжээс бүр нь кибер аюулгүй байдлын чадавхтай холбоотой хэд хэдэн хүчин зүйлээс бүрдэнэ. Хүчин зүйл бүр нь холбогдох үзүүлэлтүүдийг нэгтгэсэн бүрдэл хэсгүүдтэй бөгөөд эдгээр нь төлөвшлийн үе шатыг тодорхойлох алхмууд болон үйлдлүүдийг илэрхийлнэ.

Төлөвшлийн таван түвшин байх бөгөөд ***эхлэл*** түвшнээс (start-up) ***динамик*** түвшин (dynamic) хүртэл үнэлэгдэх боломжтой. Эхлэл түвшин нь кибер аюулгүй байдлын хүрээнд аливаа зохицуулалт, хэрэгжүүлэлт байхгүй бол, динамик түвшин нь стратегийн хүрээнд хөгжсөн, аливаа өөрчлөлтөд дасан зохицох, шинэчлэгдэх чадвартай түвшин юм. Үнэлгээний талаарх дэлгэрэнгүй мэдээллийг авахаар бол төлөвшлийн үнэлгээ хийх баримт бичигтэй[1] танилцана уу.

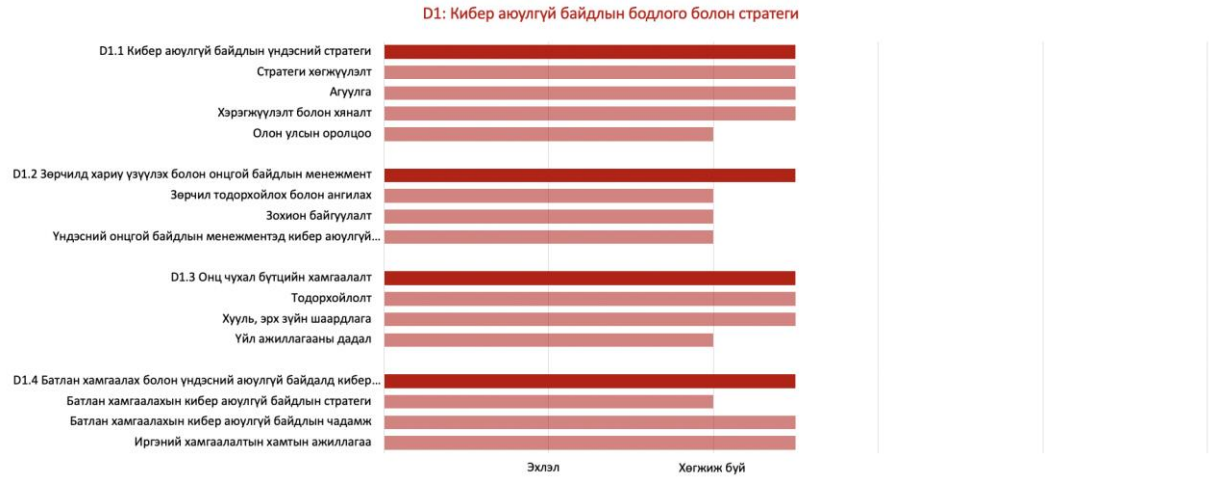
Зураг 1-т Монгол Улсын кибер аюулгүй байдлын чадавхын ерөнхий дүр зургийг харуулж, хэмжээс тус бүрд төлөвшлийн үнэлгээг дүрслэн үзүүлэв. График нь таван хэсэгтэй бөгөөд хэмжээс тус бүрийн таван түвшин төвөөс зах руу чиглэнэ: "Эхлэл" түвшин нь төвдөө, "Динамик" түвшин нь захад байрлана.

[1] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition," February 2017, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.



Зураг 1: Монгол Улсын кибер аюулгүй байдлын чадавхын ерөнхий зураглал

Кибер аюулгүй байдлын бодлого болон стратеги



Анхны *кибер аюулгүй байдлын үндэсний стратеги* (цаашид КАБҮС гэх) нь 2022 оны 12 сарын 28-нд Монгол Улсын Засгийн газрын 493 дугаар шийдвэрээр батлагдсан. КАБҮС -ийн боловсруулалтыг дэмжих зорилгоор ЦХИХХЯ болон Тагуулын Ерөнхий Газар /цаашид ТЕГ гэх/ судалгаа хийсэн бөгөөд энэхүү судалгааны хүрээнд улсын хэмжээнд тулгарч буй кибер аюулгүй байдлын эрсдэлийн талаарх тодорхой ойлголтыг олж авсан байдаг. Үүнтэй уялдуулан Үндэсний хэмжээнд кибер аюулгүй байдлын эрсдэлийн бүрэн зураглал гаргахад уг судалгаанаас гадна ямар мэдээлэл, судалгаа хэрэгтэй гэдгийг тодорхойлох нь чухал. КАБҮС нь Үндэсний Кибер Аюулгүй Байдлын Зөвлөлийг байгуулах, Кибер халдлага, зөрчилтэй тэмцэх төвүүд болон бусад арга хэмжээг хэрэгжүүлэх замаар онц чухал мэдээллийн дэд бүтцийг хамгаалах, кибер гэмт хэргийг бууруулах арга хэмжээг хэрэгжүүлэх, олон нийтийн кибер аюулгүй байдлын мэдлэгийг дээшлүүлэх зэрэг тодорхой үйл ажиллагаануудыг дотроо багтаасан.

КАБҮС -ийг хоёр үе шаттайгаар хэрэгжүүлэхээр төлөвлөсөн бөгөөд I үе шат нь 2022-2025 он, II үе шат нь 2026-2027 оныг хамарсан байна. Стратегийн хүрэх үр дүнгүүд нь тодорхой бөгөөд гүйцэтгэлийн түлхүүр үзүүлэлт (KPI)-ийг ашиглан хэмжихээр төлөвлөсөн. КАБҮС -ийг дагалдуулан үйл ажиллагааны төлөвлөгөө боловсруулсан бөгөөд уг төлөвлөгөөнд хийх ажил тус бүрийн үндсэн хариуцагч талуудыг тодорхойлж, шаардлагатай хамтран ажиллах байгууллагуудыг тусгаж өгсөн. КАБҮС -ийг хэрэгжүүлэх хөтөлбөрийн зохицуулалтыг Засгийн газар болон Кибер Аюулгүй Байдлын Зөвлөл хариуцаж ажиллана. КАБҮС -ийн хэрэгжилтийн явц хараахан үнэлэгдээгүй бөгөөд эхний үнэлгээ нь I үе шат дуусах буюу 2025 онд урьдчилан тодорхойлсон шалгуур үзүүлэлт, зорилтот түвшний дагуу хийхээр төлөвлөгдсөн. Одоо байгаа бүтцийн дагуу кибер аюулгүй байдлын зөвлөлийн үр нөлөөг тогтмол үнэлэх, КАБҮС-ийн хэрэгжилтэд шаардлагатай санхүүжилтийн дутагдлыг илрүүлж, асуудлыг шийдвэрлэх, түүнчлэн хувийн хэвшил болон иргэний нийгмийн байгууллагуудыг стратегийн хэрэгжилт болон засаглалын хяналтад оролцуулах механизмыг судлах нь чухал ач холбогдолтой.

Монгол Улсад үндэсний хэмжээнд кибер халдлага, зөрчилтэй тэмцэх 4 баг үйл ажиллагаа явуулж байна. 2021 оны *Кибер аюулгүй байдлын тухай хуульд* Кибер халдлага, зөрчилтэй тэмцэх Үндэсний төв /цаашид “Үдэсний төв” гэх/, Кибер халдлага, зөрчилтэй тэмцэх Нийтийн төв /цаашид “Нийтийн төв” гэх/ болон Кибер халдлага, зөрчилтэй тэмцэх Зэвсэгт хүчний төв /цаашид “Зэвсэгт хүчний төв” гэх/ тус бүрийг байгуулах тухай

заасан[2]. Уг хуулийн дагуу Монгол Улсын онц чухал мэдээллийн дэд бүтэцтэй байгууллагууд руу чиглэсэн халдлага, зөрчилд ТЕГ -н харьяанд байгуулагдсан Үндэсний төв хариу арга хэмжээг аван ажиллаж байгаа бол ЦХИХХЯ -ны харьяанд байгуулагдсан Нийтийн төв нь иргэд болон хувийн байгууллагыг хариуцан тус тус ажиллаж байна. Мөн 2014 оноос хувийн хэвшлийн байгууллагуудын (банк, үүрэн телефоны операторууд, томоохон интернэт үйлчилгээ үзүүлэгчид (ISP)) дунд үйл ажиллагаа явуулж буй төрийн бус байгууллага болох Цахим аюулгүй байдлын мэдээлэл, удирдлагын төв /цаашид MNCERT гэх/ нь Монгол Улсын кибер аюулгүй байдлыг хангахад чухал үүрэг гүйцэтгэн ажиллаж байна. Түүнчлэн Үндэсний Дата Төв (цаашид "Дата төв" эсхүл ҮДТ гэх) нь зөрчилд хариу арга хэмжээ авахад тодорхой үүрэг гүйцэтгэдэг. Тус төв нь төрийн байгууллагуудын системийг байршуулдаг тул *Кибер аюулгүй байдлын тухай хууль* батлагдахаас өмнө болон хойш зөрчлийн илрүүлэлт, хариу арга хэмжээнд дэмжлэг үзүүлсээр ирсэн.

Кибер аюулгүй байдлын тухай хуулийн дагуу Үндэсний төв нь кибер аюулгүй байдлын зөрчлийн мэдээллийн санд улсын хэмжээнд тохиолдож буй кибер аюулгүй байдлын зөрчлийн мэдээллийг хадгалах үүрэгтэй. Бодит байдал дээр Үндэсний төв болон Нийтийн төв нь харьцангуй шинэ байгууллагууд тул зөрчлийн мэдээллийн сан нь одоогоор бүрэн ажиллагаанд ороогүй байгаа тухай мэдэгдсэн. Одоогийн байдлаар мэдээллийн санд зөвхөн Үндэсний төвд хамрах хүрээнд байгаа зөрчлүүд бүртгэгдсэн бөгөөд Нийтийн төвөөс Үндэсний төв рүү мэдээлэл үр ашигтай солилцох дээр дутагдалтай байна. Түүнчлэн уг зөрчлийн мэдээллийн санд бий болох кибер зөрчлийн мэдээлэл нь улсын хэмжээнд кибер хадлага, зөрчлийн бүрэн зураглалыг бий болгох чухал эх сурвалж болох тул тус 2 төвийн мэдээлэл солилцох түвшнээс ихээхэн хамааралтай. Энэхүү бүрэн зураглалыг гаргах нь улсын хэмжээнд нөлөөлж болзошгүй эрсдэлтэй аюул заналыг тодорхойлох, эрэмбэлэх боломжийг бий болгохоос гадна тулгарч буй тулгарч буй аюул заналын талаар илүү өргөн хүрээтэй ойлголтыг бий болгох, үндэсний кибер аюулгүй байдлын эрсдэлийг үнэлэхэд дэмжлэг үзүүлэх болно.

Үндэсний болон Нийтийн төвүүд нь харьцангуй шинэ учраас чадавх нь бүрэн туршигдаагүй. Одоогийн бүтцийн дагуу улсын хэмжээнд тохиолдож болзошгүй төрөл бүрийн кибер зөрчилд хариу арга хэмжээ авахад шаардлагатай нөөц, ур чадвар, процессыг хангаж буй эсэхийг үнэлэх шаардлагатай хэвээр байна. Үндэсний болон Нийтийн төвүүд нь хариуцсан бүх салбаруудын хэрэгцээг хангах нөөц, ур чадвар нь хязгаарлагдмал байж болох асуудал буйг илэрхийлсэн. Иймд төвүүд хэрхэн хамтын нөөцөө үр дүнтэй ашиглах, экосистемийн бусад хэсгүүд болох MNCERT, Үндэсний Дата Төв (ҮДТ), хувийн хэвшил гэсэн талуудыг үр дүнтэй ашиглах талаар тодорхойлох нь нэн тэргүүнд тавигдах зүйл юм. Үүнээс гадна оролцогч талуудаас мэдээлэл цуглуулах замаар КАБҮС -ийн хүрээнд хэрэгжиж буй хөтөлбөрүүдийн засаглалын холбоо уялдаа холбоог сайтар хангах нь чухал. Ингэснээр мөн төвүүд үр дүнтэй ажиллаж байгаа эсэхийг тодорхойлох, аливаа дутагдалтай талуудыг илрүүлэх боломжтой болно.

Үндэсний хэмжээний кибер халдлага, зөрчилд хариу үзүүлэх төлөвлөгөө 2024 оны 9 сард батлагдсан. Өмнө нь тал бүрийн оролцогч талуудыг хамруулсан кибер сургуулилтууд хийгдсэн боловч шинээр батлагдсан үндэсний хэмжээний онцгой байдлын төлөвлөгөөний дагуу бүх холбогдох оролцогчдыг хамруулсан сургуулилтуудыг явуулах

[2] https://legalinfo.mn/en/edtl/16531350476261

нь чухал ач холбогдолтой. Ингэснээр улс оронд тулгарч болзошгүй төрөл бүрийн онцгой нөхцөл байдлыг шийдвэрлэхэд шаардлагатай үйл явц, харилцаа холбооны тогтолцоо бүрэн бүрдсэн эсэх, мөн холбогдох байгууллагуудын чадавх хангалттай байгаа эсэхийг баталгаажуулахад дэмжлэг болох болно.

2021 онд батлагдсан *Кибер аюулгүй байдлын тухай хуульд* онц чухал мэдээллийн дэд бүтцийн /цаашид ОЧМДБ гэх/ салбар жагсаалтыг тодорхой болгосон бол салбар бүрд хамаарах байгууллагуудыг мөн тодорхойлж, жагсаалтыг 2022 онд нийтэлсэн. Тус жагсаалтад орсон байгууллагууд нь кибер аюулгүй байдлын тодорхой үүрэг хариуцлагыг биелүүлэх ёстой бөгөөд үүнд байгууллага кибер аюулгүй байдлын дотоод журам боловсруулах, кибер халдлагад хариу үзүүлэх төлөвлөгөөтэй байх, кибер аюулгүй байдлыг хариуцсан ажилтан томилох, жил бүр кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийлгэх, хоёр жил тутамд мэдээллийн аюулгүй байдлын аудит хийлгэх, зөрчлийг тайлагнах зэрэг багтана.

Кибер аюулгүй байдлын тухай хуулийн шаардлагад ОЧМДБ-н хуулийн нийцэлд үнэлгээ хийх албан ёсны процессыг тодорхойлсон бөгөөд нийцлийн хэрэгжилтийг хянах ажлыг 2025 оноос эхлэх гэж буйг мэдээлсэн. Иймд кибер аюулгүй байдлын сайн туршлагуудын хэрэгжилт нь эдгээр байгууллагуудад тогтворжиж амжаагүй байна. Илүү хөгжсөн зарим салбарууд кибер аюулгүй байдлын стандарт дагаж мөрдөх, байгууллагууд хооронд аюул занал болон эмзэг байдлын талаарх мэдээлэл хуваалцах зэрэг туршлагууд ажиглагдсан.

Кибер аюулгүй байдлын тухай хуулийн заалтууд нь эдгээр онц чухал мэдээллийн дэд бүтэцтэй байгуллагуудын кибер аюулгүй байдлын түвшнийг сайжруулах зорилготой боловч хуулийг үр дүнтэй хэрэгжүүлэхэд хэд хэдэн сорилтууд тулгараад байна. Нэн түрүүнд тулгарч буй асуудал нь хуулийн шаардлага хэрэгжүүлэх чадавхи болоод байна. Зарим байгууллага энэ шаардлагыг хангаж чадах эсэхдээ эргэлзэж буйг илэрхийлсэн. Хоёр дахь асуудал нь хуулийн талаар оролцогч талуудын ойлголттой холбоотой буюу зарим зүйл дээр үл ойлголцол үүсэх, аль түвшин хүртэл дэлгэрүүлж авч үзэх ёстой дээр санал зөрөх зэрэг асуудал үүсээд байна. Гурав дахь сорилт нь холбогдох оролцогч талуудын хуулийг хэрэгжүүлэх чадамжтай холбоотой юм. Цаашид хуулийг амжилттай хэрэгжүүлэхийн тулд оролцогч талуудын ур чадварыг хэрхэн дээшлүүлэх, шаардлагатай тохиолдолд итгэлцлийг бий болгох дээр анхаарч ажиллах хэрэгтэй.

Дүгнэвэл, *Кибер аюулгүй байдлын тухай хууль* болон түүнийг дагалдах журмууд нь ОЧМДБ байгууллагуудыг хамгаалах чиглэлд чухал ахиц гаргаж байна. Хуулийн шаардлагыг зөв ойлгож, хэрэгжүүлэх тал дээр эдгээр байгууллагуудын чадавхыг тогтмол хянах нь чухал байх бөгөөд аливаа дутагдал үүссэн тохиолдолд засах, шаардлагатай дэмжлэгийг үзүүлэх боломжоор хангах ёстой. КАБҮС нь онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын кибер аюулгүй байдлын практик дахь ахицыг хэмжих "кибер аюулгүй байдлын эрсдэлд суурилсан практикийг хэрэгжүүлсэн ОЧМДБ байгууллагуудын өсөлтийн хувь", "нөхөн сэргээх, тасралтгүй байдлын менежментийн системийг бүрдүүлсэн байгууллагуудын өсөлтийн хувь" зэрэг хэрэгжилтийн явцыг хянахад туслах үзүүлэлтүүдийг агуулсан. Түүнчлэн, хуулийн хэрэгжилт хэрэгжиж эхлэхтэй зэрэгцэн төлөвлөсөн зохицуулалтын арга барилын үр нөлөөг турших нь чухал.

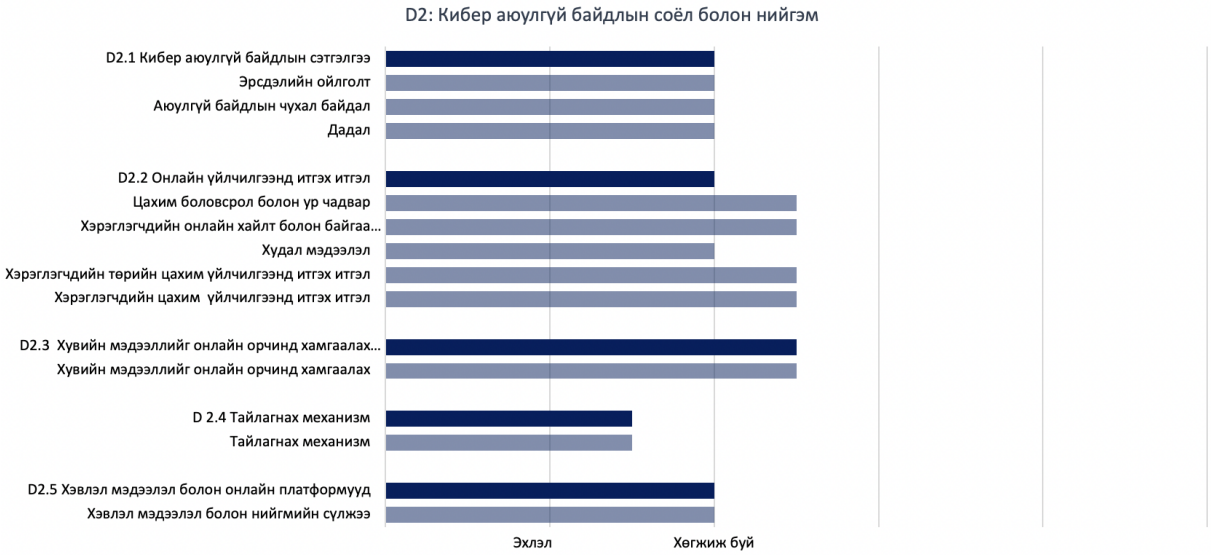
Батлан хамгаалах, зэвсэгт хүчний кибер аюулгүй байдлын стратеги хараахан нийтлэгдээгүй бөгөөд ийм стратеги боловсруулагдаж байгаа тухай мэдээлэл оролцогчдоос ирүүлээгүй. Кибер аюулгүй байдлын тухай хуулийн 14-р зүйл заалт нь зэвсэгт хүчний кибер аюулгүй байдлыг хариуцсан байгууллагад хэд хэдэн шаардлага тавьдаг. Тухайн заалтуудыг стратегийн зорилтуудыг тодорхойлж байгаа гэж үзэж болох

юм. Үндэсний аюулгүй байдал болон батлан хамгаалахад кибер аюулгүй байдлын үзүүлэх боломжит нөлөөг үнэлсэн эсэх нь тодорхойгүй. Энэхүү үнэлгээг хийх нь батлан хамгаалах салбарын кибер аюулгүй байдлын стратеги, түүнтэй холбоотой үйл ажиллагааны зарчим болон мөрдөх журам боловсруулах ажилд дэмжлэг үзүүлэхэд чухал ач холбогдолтой.

Зэвсэгт хүчний Кибер Аюулгүй Байдлын Команд байгуулагдсан бөгөөд энэхүү бүтэц дотор 2021 онд Умард Атлантын Гэрээний Байгууллага (NATO)-ын дэмжлэгтэйгээр Кибер халдлага, зөрчилтэй тэмцэх Зэвсэгт хүчний төвийг байгуулсан. Тус төвийн команд, штабын сургалт Монголын Үндэсний Батлан Хамгаалах Их Сургууль болон бусад улс орнуудтай хамтын ажиллагааны хүрээнд үргэлжилж байна. Мөн бэлтгэгдсэн мэргэжилтний дутагдалтай байдал хэвээр бөгөөд одоогийн чадамжийн хангалттай байдлыг үнэлсэн нотолгоо байхгүй байна.

Мөн кибер аюулгүй байдлын тухай хуульд зэвсэгт хүчин нь "*шаардлагатай үед улсын кибер аюулгүй байдлыг хангах үйл ажиллагаанд дэмжлэг үзүүлэх*" үүрэгтэй гэж заасан. Иргэний болон батлан хамгаалахын байгууллагуудын кибер аюулгүй байдлын хамтын ажиллагааг 2024 онд батлагдсан үндэсний хэмжээний кибер халдлага, зөрчилд хариу үзүүлэх төлөвлөгөөгөөр албан ёсоор тодорхойлсон. Энэхүү төлөвлөгөө шинэ, хараахан туршигдаагүй боловч тогтмол сургуулилт хийх зорилготой. Тиймээс одоогоор иргэний болон батлан хамгаалахын байгууллагуудын хамтын ажиллагааны үр нөлөөний тодорхой нотолгоо байхгүй байна. Батлан хамгаалах байгууллагын иргэний болон ОЧМДБ байгууллагуудад хамааралтай байдлын үнэлгээ хийгдсэн гэх нотолгоо байхгүй. Эдгээр хамаарлыг үнэлэх механизм бий болгох, иргэний болон ОЧМДБ байгууллагууд нь эдгээр үйлчилгээг тасралтгүй хангах боломжтой эсэхийг баталгаажуулах нь чухал.

Кибер аюулгүй байдлын соёл болон нийгэм



Монгол Улс нь цахим шилжилт болон кибер аюулгүй байдалтай холбоотой эрсдэлүүдийн талаарх ойлголтоо нэмэгдүүлж байна. 2021 онд кибер аюулгүй байдлын цогц хууль эрх зүйн зохицуулалтыг танилцуулснаар энэ чиглэлийн мэдлэг, ач холбогдлын түвшин эрс нэмэгдсэн. Түүнчлэн 2022 оны *Кибер аюулгүй байдлын үндэсний стратеги* болон түүний хэрэгжилтийн төлөвлөгөө нь Монгол Улсын Засгийн газар кибер аюулгүй байдлыг ухамсарлаж, чухал чиглэл болгон анхаарч буйн нотолгоо болж байна. Салбарын оролцогч талуудын дунд кибер аюулгүй байдлын талаар тодорхой хэмжээний ойлголт бий болсон хэдий ч төрийн байгууллага, иргэний нийгэм, олон нийтийн дунд уг сэдвийн талаарх мэдлэг, мэдээлэл дутмаг хэвээр байна. Кибер аюулгүй байдлын цогц хууль нь энэ талаарх мэдлэг, ач холбогдлыг нэмэгдүүлэхэд тодорхой хувь нэмэр оруулсан ч бүх түвшинд жигд нөлөөлж чадаагүй бөгөөд зарим гол оролцогч талууд эдгээр хуулийн талаар бага мэдээлэлтэй байна. Мөн удирдах түвшний менежерүүд болон улс төрчдийн дунд кибер аюулгүй байдлын талаарх ойлголт хангалтгүй байгаа нь төрийн болон хувийн хэвшлийн аюулгүй байдалд тулгараад буй асуудал юм. Энэ нь ялангуяа төсвийн хязгаарлагдмал байдалд ихээхэн нөлөөлж байна.

Тэргүүлэх бүлэг оролцогчдоос гадна, голлох бүлгийн хэлэлцүүлгээс үзэхэд ихэнх хэрэглэгчид кибер аюулгүй байдлын сайн туршлагыг мөрдөхгүй байгаа нь тогтоогдсон. Мөн нууц үгийн зохисгүй удирдлага, албан ёсны мэдээлэл солилцоонд хувийн цахим шуудан болон мессежийн платформ ашиглах, хоёр шатлалт нэвтрэлтийг хэрэглэхгүй байх зэрэг нийтлэг буруу дадлуудын талаар онцолсон.

Монгол Улсад цахим үйлчилгээ, олон нийтийн мэдээллийн хэрэгслийг өдөр тутмын амьдралын нэг хэсэг болгон тогтмол хэрэглэдэг, цахим орчныг ашиглах чадамжтай интернэт хэрэглэгчдийн тоо өсөн нэмэгдэж байна. Энэхүү хэрэглээ нь мэдээлэл, харилцаа холбооны дэд бүтцээр дамжуулан хэрэглэгчдийн холболтыг дэмжиж буйтай холбоотой. Цахим үйлчилгээг үзүүлж буй төрийн болон хувийн хэвшлийн гол оролцогч талууд аюулгүй байдлын баталгааг хангах хэрэгцээ шаардлага үүсээд буйг олж харсан бөгөөд ОЧМДБ байгууллагуудын хувьд хууль эрх зүйн хүрээнд энэхүү шаардлага тавигдаж байна. Гэсэн хэдий ч тус бүрийн аюулгүй байдал нь тухайн системийг хариуцаж буй удирдлагаас шууд хамаарч байгаа бөгөөд зарим байгууллагууд бусдаас илүү өндөр түвшинд аюулгүй байдлын хяналтуудыг хэрэгжүүлсэн байна.

Монгол Улсад хэрэглэгчийн түвшинд цахим боловсрол өндөр, цахим үйлчилгээ ашиглалт их байгаа хэдий ч , аюулгүй байдлын сайн дадал, зуршлыг тогтмол хэрэглэх болон онлайн орчинд аюулгүй байдлыг хэрхэн хангах мэдлэгийн хувьд дутагдалтай байна. Мөн Монгол Улсын ихэнх интернэт хэрэглэгчид хууль ёсны болон хууль бус вэбсайт, цахим үйлчилгээг хооронд нь ялгаж чадахгүй талаар мэдэгдсэн. Зарим голлох бүлгийн хэлэлцүүлэгт оролцогч нар нь тэднийг “хууртахад амархан” эсхүл "цахим мунхаг" гэж тодорхойлсон.

Хувийн нууц нь Монгол Улсын Үндсэн хуулиар хамгаалагдсан хүний үндсэн эрх бөгөөд Монгол Улсад 2021 онд батлагдсан “*Хүний хувийн мэдээлэл хамгаалах тухай*” хуулиар хувийн мэдээллийг хамгаалах хүчтэй тогтолцоо үйлчилж байна. Энэ хууль нь мэдээлэл цуглуулах, боловсруулах, ашиглах болон аюулгүй байдлыг хангах талаар "Мэдээллийн хариуцагч /controller/"-д дагаж мөрдөх шаардлагуудыг тусгасан. Түүнчлэн аюулгүй байдал болон хяналтын заалтуудаар дамжуулан нууцлал болон аюулгүй байдлын хэрэгцээг тэнцвэржүүлэх тодорхой хэмжүүрүүдийг тогтоосон. Гэсэн хэдий ч хэрэглэгчийн түвшинд иргэд хувийн мэдээллээ онлайн орчинд хэрхэн хамгаалах ёстойгоо мэдэхгүй байна. Соёлын хувьд Монголын хүн амыг ерөнхийд нь авч үзвэл өөрсдийн цахим мэдээлэл онлайн орчинд хэрхэн ашиглагдаж буй талаар ойлголтгүй бөгөөд ихэнх иргэд өөрсдийн мэдээллийн нууцлалтай байдлыг хангуулах эрхийн талаар сайтар ойлголтгүй байна гэж дүгнэгдсэн.

Кибер аюулгүй байдлын зөрчлүүд, кибер гэмт хэргүүд болон бусад кибер аюул занал, хохирлын мэдээлэл хүлээн авах механизм Монгол Улсад бий болж, тодорхой хэмжээнд уялдаатай ажиллаж байна. Цагдаагийн Ерөнхий Газар, Үндэсний төв болон Нийтийн төв нь 2021 онд батлагдсан “*Кибер аюулгүй байдлын тухай хуулийн”* хүрээнд кибер гэмт хэрэг, кибер халдлага болон бусад зөрчилтэй холбоотой мэдээллийг харьяа байгууллагуудаас хүлээн авах үүрэг хүлээсэн байдаг. Тал бүрийн оролцогч талуудтай хийсэн голлох бүлгийн хэлэлцүүлгүүдийн үр дүнгээс харахад эдгээр мэдээлэх механизм нь хоорондоо нягт уялдаа холбоотой ажиллах хэрэгцээ, хүсэл эрмэлзэл байгаа ч одоогоор системтэй, зохион байгуулалттайгаар үйл ажиллагаа явуулж чадахгүй байна. Харин, мэдээлэх механизмууд ихэвчлэн тус тусдаа, уялдаагүй байдлаар ажиллаж байгаа нь ажиглагдсан.

Уламжлалт болон цахим хэвлэл мэдээллийн сувгууд кибер аюулгүй байдлын асуудлыг үе үе хөндөж нийтэлдэг. Үүнд олон улсын кибер аюулгүй байдлын мэдлэгийн сар, кибер аюулгүй байдлын арга хэмжээ, бодлогын хөгжүүлэлт, кибер гэмт хэргийн тохиолдлууд болон бусад асуудлуудын талаар мэдээлэл оруулдаг. Зарим тохиолдолд хэвлэл мэдээллийн хэрэгслүүд уншигч, үзэгчдэд зориулан өөрсдийгөө онлайнаар хамгаалах практик, хэрэгжүүлэх боломжтой кибер аюулгүй байдлын арга хэмжээний талаар мэдээлэл багтаасан байдаг.

Кибер аюулгүй байдлын мэдлэг болон чадамж бий болгох

Монголын хөдөлмөрийн зах зээлд кибер аюулгүй байдлын хүний нөөцийн хомсдол нь олон салбарт нөлөөлж буй асуудал бөгөөд улсын кибер аюулгүй байдлын чадавх болон төлөвшлийг сайжруулах чадварт ноцтой сөрөг үр дагавар авчирч байна. Төлөвшлийн үнэлгээний голлох бүлгийн хэлэлцүүлэгт оролцсон бүх оролцогч талуудын зүгээс кибер аюулгүй байдлын чадварлаг мэргэжилтнүүдийг ажилд авах, тогтвортой ажиллуулах нь 2021 оны “*Кибер аюулгүй байдлын хуулийг”* хэрэгжүүлэхээс эхлээд хүүхдүүдэд зориулсан кибер аюулгүй байдлын сургалтын хөтөлбөр боловсруулах хүртэл аливаа үйл ажиллагааг хэрэгжүүлэхэд тулгамдсан гол асуудал болж буй талаар нэгэн дуугаар санал нэгдсэн. Энэ асуудлыг зохих ёсоор авч үзэж, бодитой хөрөнгө оруулалт хийхгүй бол Монгол Улсын хэмжээнд кибер аюулгүй байдлын тогтвортой байдлыг сайжруулах хүчин чармайлтыг бүрэн сулруулах эрсдэлтэй юм.

Монгол Улсад кибер аюулгүй байдлын талаарх олон төрлийн мэдлэг олгох хөтөлбөр, үйл ажиллагаанууд байдаг ч эдгээрийг төрөл бүрийн байгууллагууд уялдаа холбоогүйгээр хэрэгжүүлж байна. Стратегийн түвшинд олон нийтийн кибер аюулгүй байдлын мэдлэгийг дээшлүүлэх, энэ чиглэлээр кампанит ажил, сургалт, семинар зохион байгуулж, иргэдэд кибер аюулгүй байдлын талаарх ойлголт, мэдлэгийг түгээх нь 2022 оны Үндэсний Кибер Аюулгүй Байдлын Стратегийн гол зорилтуудын нэг юм. Гэсэн хэдий ч олон нийтийн кибер аюулгүй байдлын мэдлэгийг үр дүнтэй нэмэгдүүлэхийн тулд илүү тогтвортой, нэгдсэн стратеги шаардлагатай бөгөөд энэ чиглэлд дорвитой ажлууд хийх шаардлагатай хэвээр байна. Голлох бүлгийн хэлэлцүүлэг болон нэмэлт судалгааны үр дүнд хувийн болон төрийн байгууллагын удирдах түвшний албан тушаалтнуудад зориулсан иж бүрэн кибер аюулгүй байдлын мэдлэг олгох сургалтын хөтөлбөр байхгүй болох нь тогтоогдсон. Олон хүмүүс гүйцэтгэх түвшний шийдвэр гаргагчдад зориулж тусгайлан боловсруулсан мэдлэг олгох хөтөлбөрүүдийг хэрэгжүүлэх хүсэлтэй байгаагаа илэрхийлсэн. Ингэснээр кибер аюулгүй байдлын зардал, тэргүүлэх чиглэл болгох асуудалд тулгардаг сорилтыг даван туулахад чухал хувь нэмэр оруулах юм.

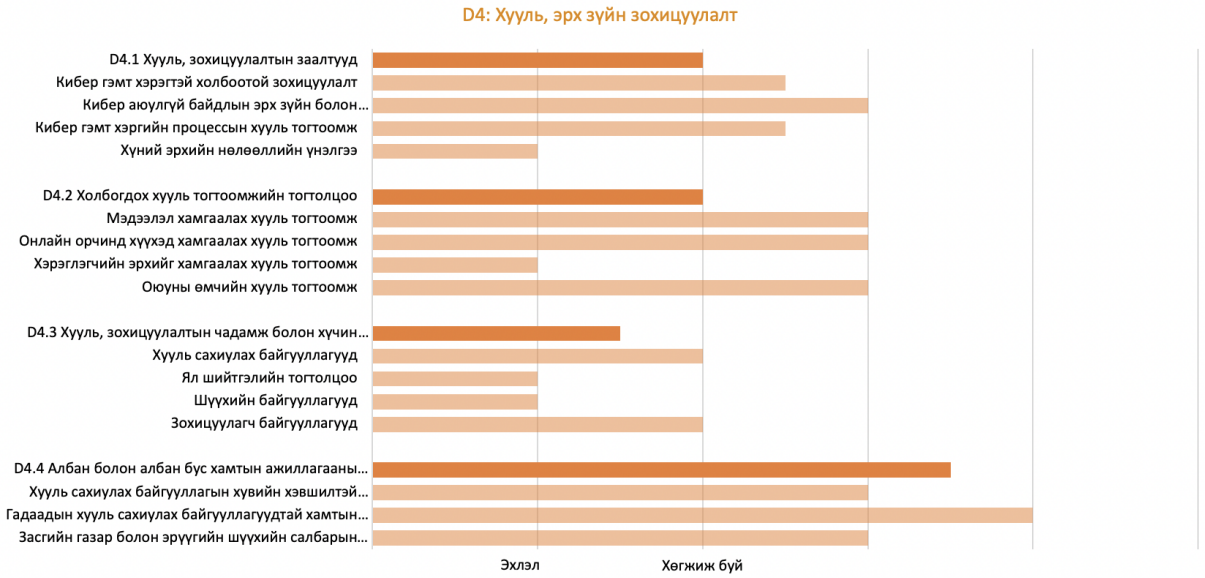
Монгол Улсын хэд хэдэн тэргүүлэх их дээд сургуулиудад кибер аюулгүй байдалтай холбоотой дээд боловсролын зэрэг олгох хөтөлбөрүүд байдаг. Кибер аюулгүй байдлын мэргэшсэн мэргэжилтнүүдийн эрэлт их байгаа хэдий ч их дээд сургуулиуд салбарын

хэрэгцээ, хүлээлтэд нийцсэн төгсөгчдийг бэлтгэх шаардлагатай тоног төхөөрөмж, боловсон хүчний хувьд дутагдалтай. Түүнчлэн их, дээд сургуулиуд нь өөрсдийн багшлах боловсон хүчнийг ажилд авах, тогтвортой ажиллуулахад хүндрэлтэй байгаагаа мэдээлсэн. Үүний шалтгаан нь хувийн хэвшил болон гадаадын байгууллагуудаас санал болгож буй өндөр цалин, эрэлттэй байдал, мөн их хэмжээний ажлын ачаалал зэргээс үүдэн эдгээр ажлын байрууд сонирхол татахуйц бус болсон явдал юм. Кибер халдлага, хамгаалалтын туршилт /симуляц/ хийх, тоон дүн шинжилгээний сургалт явуулах зэрэг техникийн чадварыг хөгжүүлэх бие даасан сургалтын орчин хязгаарлагдмал байгаа нь боловсролын чанарыг улам дордуулж байна.

Дээд боловсролын салбараас гадна, Монгол Улсад бүтэцлэгдсэн болон түр зуурын хэлбэрээр зохион байгуулагддаг кибер аюулгүй байдлын олон төрлийн сургалтын хөтөлбөрүүд байдаг. Эдгээр сургалтуудыг мэргэжлийн боловсролын төвүүд, хувийн кибер аюулгүй байдлын сургалтын төвүүд, олон улсын чадавх бэхжүүлэх түншүүд хэрэгжүүлж байна. Ялангуяа хууль сахиулах байгууллагын ажилтнуудад зориулсан сургалтууд олон улсын түншүүдийн дэмжлэгтэйгээр тогтмол зохион байгуулагддаг. Голлох бүлгийн хэлэлцүүлгээс үзэхэд төрийн болон хувийн хэвшлийн аж ахуйн нэгжүүд санхүүгийн боломжтой үедээ эдгээр сургалтуудад байнга хамрагддаг бөгөөд Монголын байгууллагуудын дунд кибер аюулгүй байдлын мэргэжилтнүүдийг сургах эрэлт өндөр байна. Гэвч кибер аюулгүй байдлын ажилтнуудыг сургах, ажлын байранд хадгалж үлдээх хүндрэл төрийн байгууллагуудад хамгийн түгээмэл тулгардаг асуудал бөгөөд үүний шалтгаан нь хатуу цалингийн тогтолцоо, яам хоорондын уялдаагүй байдал, хувийн хэвшилтэй харьцуулахад өрсөлдөх чадваргүй нөхцөл байдал зэрэгтэй холбоотой. Монголын засгийн газар төрийн байгууллагууд дахь боловсон хүчний хомсдолыг шийдвэрлэх, ажилд авах үйл явцыг сайжруулах чиглэлд тодорхой арга хэмжээ авч байгаа боловч энэ сорилтыг даван туулахын тулд илүү их хүчин чармайлт шаардлагатай байна. Засгийн газраас гадна хувийн хэвшлийн ажил олгогчид ч мөн хэрэгцээгээ хангахуйц кибер аюулгүй байдлын мэргэжилтнүүдийг олоход хүндрэлтэй байгаа бөгөөд тэд дотоодын болон олон улсын ажил олгогчдын өрсөлдөөн их байгааг онцолжээ.

Монгол Улсын *Кибер аюулгүй байдлын үндэсний стратегид* аюулгүй байдлын чиглэлээр мэргэшсэн боловсон хүчнийг нэмэгдүүлэх зорилтыг тусгасан. Энэхүү зорилтын хүрээнд "кибер аюулгүй байдлын судлаачдын сургалт, судалгаа, академик ажлыг дэмжих хөтөлбөр хэрэгжүүлэх" нь үндсэн үйл ажиллагаануудын нэг гэж заасан. Мөн Кибер аюулгүй байдлын тухай хуулийн дагуу "цахим хөгжил, харилцаа холбоог хариуцсан төрийн төв захиргааны байгууллага нь кибер аюулгүй байдлын чиглэлээр шинэ техник, технологи, инновац, судалгаа, хөгжүүлэлтийн үйл ажиллагаа явуулах" үүрэгтэй. Гэвч бодит байдал дээр Монгол Улсад дотоод судалгаа, хөгжүүлэлтийн үйл ажиллагааг дэмжих чиглэлд бодитой арга хэмжээ авагдаагүй байна.

Хууль, эрх зүйн зохицуулалт



2015 оны Эрүүгийн тухай хуулиар компьютерын өгөгдөл, системийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдалтай холбоотой кибер гэмт хэргийн суурь зааltуудыг хуульчлан баталсан. Мөн хүүхдүүдийг гэмт хэргээс хамгаалахтай холбоотой зааltуудыг багтаасан бөгөөд эдгээр хамгаалалтыг онлайн орчинд хэрэгжүүлэх зохицуулалтуудыг тусгасан байдаг. Монгол Улсад кибер гэмт хэргийн эрүүгийн процессын талаар 2017 оны *Эрүүгийн хэрэг хянан шийдвэрлэх хуулиар* бүрэн зохицуулсан. Монгол Улсын хуулиар тогтоогдсон кибер гэмт хэргийн үйлдэлд үр дүнтэй, зохистой, айдас төрүүлэхүйц /урьдчилан сэргийлэх/ шийтгэл оногдуулах зэрэг шаардлагатай арга хэмжээг агуулсан байдаг. Хэдийгээр хууль нь олон төрлийн ял шийтгэл оногдуулах боломжийг олгодог боловч голлох бүлгийн хэлэлцүүлгийн явцад шүүхэд шилжиж, амжилттай шийдвэрлэгдсэн зарим кибер гэмт хэргүүд зөвхөн бага хэмжээний торгууль ногдуулах төдийхнөөр шийдэгддэг болохыг тэмдэглэгдсэн.

2021 оны *Кибер аюулгүй байдлын тухай хуулиар* ОЧМДБ байгууллагууд болон бусад оролцогч талуудад зориулсан кибер аюулгүй байдлын цогц шаардлагыг тогтоосон. *Кибер аюулгүй байдлын тухай хуулиар* тодорхойлогдсон бүх хуулийн этгээд, тэр дундаа онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудад хамаарах нэмэлт үүрэг хариуцлагыг "*Кибер аюулгүй байдлын нийтлэг журам*" -д тусгайлан заасан. Уг хууль болон дагалдах нийтлэг журам нь Монгол Улсын хууль эрх зүйн болон засаглалын орчинд тодорхой ахиц гаргасан нь эргэлзээгүй тодорхой боловч шинэчлэгдсэн хууль, зохицуулалтыг хэрэгжүүлэх, дагаж мөрдөхөд тулгарч буй үргэлжилсэн сорилтууд нь үндэсний түвшний ахиц дэвшлийг сааруулж байна.

Хүний хувийн мэдээлэл хамгаалах тухай хуулиар хувийн мэдээлэл цуглуулах, боловсруулах, ашиглах, түүний аюулгүй байдлыг зохицуулдаг бол Үндэсний Хүний Эрхийн Комисс нь уг хуулийн хэрэгжилтийг хянах бүрэн эрх, үүрэгтэй. Нийтлэг байдлаар уг хууль нь Монгол Улсын иргэдийн хүний эрх, эрх чөлөөг өргөн хүрээний мэдээллийн удирдлагын тогтолцоонд хамгаалах, хадгалах үүрэгтэй. 2002 оны *Иргэний хууль* нь хэрэглэгчийн гэрээний хүрээнд худалдааны ерөнхий нөхцөлийг тодорхойлсон боловч онлайн орчинд хэрэглэх боломжтой заалт агуулаагүй байна. Харин 2021 оны *Зохиогчийн эрхийн тухай хууль* нь Монгол Улсын оюуны өмчийн хууль эрх зүйн

зохицуулалтын үндэс суурийг бүрдүүлсэн. Уг хууль эрх зүйн зохицуулалтыг цахим орчинд хэрэглэх нөхцөл хангалттай тодорхойлогдсон байна.

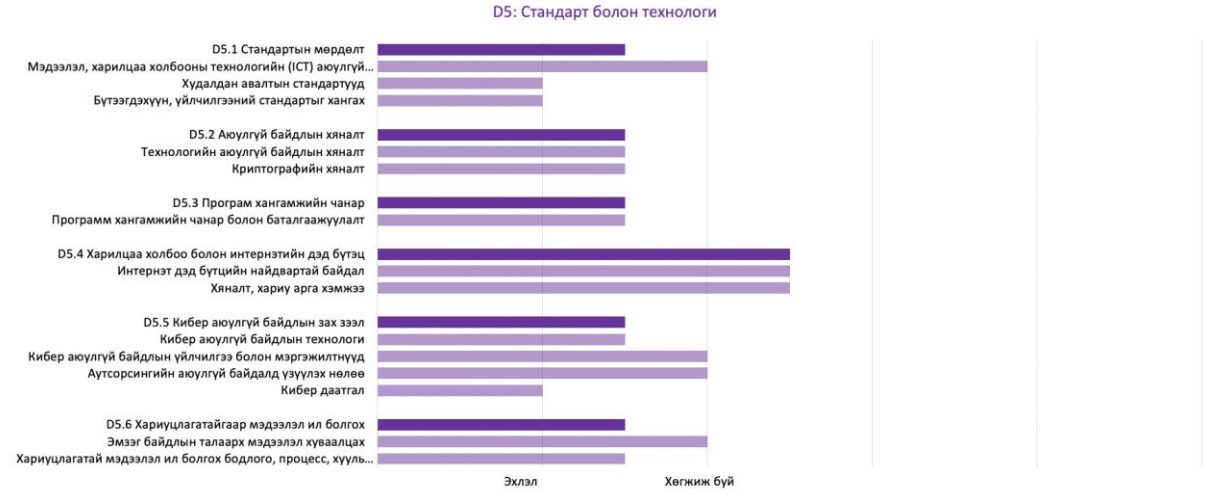
Монгол Улсын хууль сахиулах байгууллагууд, прокурорын байгууллага болон шүүхийн байгууллагууд кибер гэмт хэргийг мөрдөн шалгах тодорхой хэмжээний суурь чадавхитай боловч техник, хүний нөөцийн болон санхүүгийн хомсдолоос үүдэн байгууллагын өргөн хүрээний чадавхыг хөгжүүлэхэд бэрхшээл тулгарч байна. "Монгол Улсын Статистикийн эмхэтгэл 2023"-д дурдсан гэмт хэргийн мэдээллээс үзэхэд, Монгол Улсын хууль эрх зүйн байгууллагууд кибер гэмт хэргийг шалгаж шийдвэрлэх тодорхой түвшний чадамжтай болох нь харагдаж байна. Эдгээр статистик мэдээллээс харахад кибер гэмт хэргийг хянан шийдвэрлэх чадавх жил бүр өсөн нэмэгдэж буйг харуулж байгаа ч бүртгэгдэж буй кибер гэмт хэргийн өсөлттэй харьцуулахад хангалттай түвшинд хараахан хүрээгүй байна. Энэ нь голлох бүлгийн хэлэлцүүлгээр яригдсан прокурор болон шүүхийн байгууллагууд кибер гэмт хэргийг үр дүнтэй, үр ашигтайгаар шийдвэрлэх институцийн чадавх дутмаг байгаа талаарх мэдээлэлтэй нийцэж байна.

Хууль сахиулах байгууллагын түвшинд кибер ур чадварын хомсдолыг нөхөх, сургалтын боломжуудыг бий болгох хүчин чармайлт гаргаж байгаа хэдий ч ажилтнуудын шилжилт хөдөлгөөн өндөр байгаа нь хүний нөөцийн чадамжийг сайжруулахад саад болж байна. Хувийн хэвшил болон бусад салбаруудаас санал болгож буй өндөр цалин, хангамж нь чадварлаг кибер аюулгүй байдлын мэргэжилтнүүдийг хадгалж үлдэхэд хүндрэл учруулж буйг онцолсон.

Монгол Улсын засгийн газар нь хууль сахиулах салбартай нягт хамтран кибер гэмт хэргийн хууль, стратегийг хөгжүүлэх, сургалт явуулах болон кибер гэмт хэргийн талаарх мэдээллийг солилцох чиглэлээр ажиллаж байна. Кибер халдлага, зөрчилтэй тэмцэх Нийтийн төв нь ЦХИХХЯ-ийн харьяанд, Үндэсний төв нь ТЕГ-ийн харьяанд байдаг бөгөөд эдгээр байгууллагууд нь Монгол Улсын засгийн газар болон хууль сахиулах байгууллагуудын хооронд кибер гэмт хэргийн талаарх мэдээлэл солилцох, хамтран ажиллах албан ёсны механизмыг бүрдүүлдэг.

Харин олон улсын түвшинд Монгол Улс нь харилцан эрх зүйн туслалцааны гэрээнүүдийг (MLATs) дэмждэг хууль эрх зүйн тогтолцоотой. Цагдаагийн Ерөнхий Газраас мэдээлснээр сүүлийн жилүүдэд олон улсын түншүүдтэй хамтран ажиллах чадамж эрс сайжирсан байна. G7 24/7 сүлжээ болон Интерпол /INTERPOL/-той харилцах харилцаа зэрэг механизмууд нь энэ чиглэлд ихээхэн тус дөхөм болж байгаа талаар мэдэгдсэн. Мөн олон улсын хамтрагчид болон дотоодын хууль сахиулах байгууллагуудтай хамтран явуулсан амжилттай хил дамнасан мөрдөн шалгалтуудын тухай сүүлийн үед хэвлэл мэдээллийн хэрэгслээр нийтэлсэн байна.

Стандарт болон технологи



Монгол Улсад олон улсын кибер аюулгүй байдлын стандартуудыг тодорхойлж, Монголын байгууллагууд ашиглах боломжтойгоор нутагшуулсан байна. Зарим оролцогч талууд олон улсын стандартууд шинэчлэгдэж буйтай холбоотой эдгээр нутагшуулсан стандартуудыг шинэчлэх шаардлагатайг онцолсон. Энэ нь *Кибер аюулгүй байдлын үндэсний стратегид* дурдсан "кибер аюулгүй байдлыг хангах олон улсын стандартыг нутагшуулах, эдгээрийг дагаж мөрдөх дүрэм, журам баталж хэрэгжүүлэх" гэсэн үйл ажиллагаатай нийцэж байна.

Эдгээр стандартуудыг дагаж мөрдөх түвшин байгууллага бүрд харилцан адилгүй бөгөөд зарим салбарт олон улсын стандартуудыг хэрэгжүүлэх хандлага нэмэгдэж байгааг харуулсан нотолгоо байгаа ч дэлгэрэнгүй мэдээлэл дутмаг байгаа нь салбар хоорондын стандарт мөрдөлтийн түвшинг тодорхойлоход хүндрэлтэй болгож байна. *Кибер аюулгүй байдлын тухай хуулийн* дагуу онц чухал мэдээллийн дэд бүтэцтэй байгууллагууд кибер аюулгүй байдлын стандартуудыг нэвтрүүлэх үүрэгтэй боловч хэрэгжилтийн үйл явц одоо ч үргэлжилж байгаа бөгөөд эхний аудитын хугацаа хараахан болоогүй байна. Санхүүгийн салбар нь *Кибер аюулгүй байдлын тухай хууль* батлагдахаас өмнө зохицуулагч байгууллага нь салбарын байгууллагууддаа кибер аюулгүй байдлын стандартыг нэвтрүүлэхийг шаардсан цорын ганц салбар юм. Бусад салбаруудад тодорхой хэмжээнд стандарт мөрдөж байгаа боловч энэ нь тухайн байгууллагын төлөвшилт болон олон улсын хэмжээнд үйл ажиллагаа явуулах шаардлагаас шалтгаалан ялгаатай байна.

ОЧМДБ болон төрийн байгууллагуудаас гадна бусад байгууллагууд кибер аюулгүй байдлын стандартуудыг хэрхэн нэвтрүүлж буйг үнэлэх, хэмжих нотолгоо байхгүй байна. Иймд эдгээр стандарт болон нийтлэг журмыг бусад хувийн хэвшлийн байгууллагуудад сурталчлах, хэрэгжилтийг хэмжих схемийг хэрэгжүүлэх талаар бодож үзэх хэрэгтэй.

Монгол Улсад зарим төрийн болон хувийн хэвшлийн байгууллагууд кибер аюулгүй байдлын хяналтуудыг нэвтрүүлж байгаа боловч энэ нь салбар бүрд жигд хэрэгжээгүй байна. Харин санхүүгийн салбарт кибер аюулгүй байдлын стандарт нэвтрүүлэхийг хуульчлан шаардсан тул эдгээр байгууллагууд технологийн, криптографийн аюулгүй байдлын хяналтуудыг хэрэгжүүлж байгаа. Одоогийн байдлаар Монголын байгууллагуудын технологи, криптографийн аюулгүй байдлын хяналтуудыг хэрэгжүүлэх байдал нь тухайн байгууллагын нөөц, кибер аюулгүй байдлын талаарх

ойлголт, стандарт дагаж мөрдөх түвшнээс хамаарч харилцан адилгүй байна. Боловсролын байгууллагууд болон кибер аюулгүй байдлын хувийн компаниудын судалгаагаар зарим салбарууд, ялангуяа эрүүл мэндийн салбарт аюулгүй байдлын хяналт хангалтгүй байгааг тогтоосон байна.

Төрийн байгууллагын төлөөлөгчид төрийн байгууллага руу чиглэсэн амжилттай халдлага, жишээлбэл зорилтот халдлага /APT/, түүний тархалттай холбоотой санаа зовнилоо илэрхийлсэн. Төрийн байгууллагуудын хувьд кибер аюулгүй байдлын хяналтуудыг хэрэгжүүлэхэд төсвийн асуудал байгааг мөн мэдээлсэн. Иймд, Сангийн яам төрийн байгууллагуудад шаардлагатай төсвийг хангалттай хэмжээгээр хуваарилах механизмыг тодорхойлох шаардлагатай гэж үзэж байна. Төрийн байгууллагаас гадна зарим хувийн хэвшлийн байгууллагууд ч кибер аюулгүй байдлын хяналтуудыг хэрэгжүүлэх төсөв хангалтгүй байдаг талаар илэрхийлсэн. Байгууллагын удирдлагууд кибер аюулгүй байдлыг чухал гэж авч үзэхгүй байгаа нь асуудал болж буй талаар санал бодол солилцсон. Иймд байгууллагын удирдлагуудад зориулсан кибер аюулгүй байдлын мэдлэгийг нэмэгдүүлэх санаачилгууд хэрэгжүүлэхийг судалж үзэх нь үр ашигтай.

Зарим байгууллага программ хангамжийн чанарын шаардлага тодорхойлох процесс байдаг бол зарим хувийн ОЧМДБ байгууллага аюулгүй байдлын шалгалт, туршилт хийх болон программ хангамжийн шинэчлэлт, засвар үйлчилгээний төлөвлөгөөтэй ажилладаг. Гэвч ийм түвшний төлөвшсөн, чанартай, аюулгүй програм хангамж ашиглах байдал нь бүх байгууллагын хувьд жигд биш байна.

Мөн зарим байгууллагууд кибер аюулгүй байдлын технологи, программ хангамжийн лиценз худалдан авах боломжгүйгээс болж лицензгүй программ хангамж ашиглах нөхцөл байдал үүсдэг байна.

Гадаадаас худалдан авсан програм хангамж нь илүү стандартчилсан, найдвартай байх хандлагатай байдаг гэсэн байр суурийг илэрхийлсэн. Хувийн хэвшлийн байгууллагын оролцогчид дотоодын програм хангамж ашиглахад илүү их аюулгүй байдлын хяналт, туршилтыг өөрсдөө хийх шаардлагатай болдог талаар дурдсан. Учир нь дотоодын програм хангамж ихэвчлэн стандартчилалгүй байдаг бөгөөд аюулгүй байдал нь хөгжүүлсэн компанийн чадвар, чанараас шууд хамаардаг. Түүнчлэн байгууллагууд худалдан авалт хийхдээ лавлагаа авах боломжтой баталгаажсан програм хангамжийн платформын каталог байдаггүй.

Монгол Улсад найдвартай интернэт үйлчилгээ өргөн хүрээнд ашиглагдаж байна. Интернэтийн дэд бүтцийг Харилцаа Холбооны Зохицуулах Хороо албан ёсоор удирдаж, Интернэт Үйлчилгээ Үзүүлэгчдэд (ISP) лиценз олгож, зохицуулалт хийдэг. Жишээлбэл, ISP-дийн урсгалын тодорхой хувийг нэмэлт замаар /redundancy/ чиглүүлэхийг шаардсанаар сүлжээний найдвартай байдлыг сайжруулах зохицуулалт үйлчилж байна. Мөн ISP харилцагч нартаа үйлчилгээ тасалдуулах /DDoS/ халдлагаас хамгаалах үйлчилгээ үзүүлэх үүрэгтэй боловч бүх ISP энэхүү шаардлагыг биелүүлэхэд хангалттай нөөц бололцоо байхгүй талаар мэдэгдсэн. Нэмэлт замчлалын /redundancy/ хувьд, Үндэсний Дата Төвд байрладаг Монголын Интернэт Солилцооны Цэг (IXP) нь ISP хооронд урсгал солилцох боломжийг бүрдүүлдэг бөгөөд аль нэг ISP доголдсон тохиолдолд найдвартай ажиллагааг маш сайн хангадаг тухай оролцогчид онцолсон. Түүнчлэн, ISP болон Харилцаа холбооны зохицуулах хороо IXP тоог нэмэгдүүлэх асуудлаар хэлэлцүүлэг хийж байгаа талаар мэдээлсэн.

Кибер аюулгүй байдлын тухай хуулийн дагуу томоохон харилцаа холбооны байгууллагуудыг онц чухал мэдээллийн дэд бүтэцтэй байгууллага гэж тодорхойлсон. Үүнтэй холбоотойгоор тун удахгүй хэрэгжиж эхлэх хэд хэдэн шаардлага тавигдсан бөгөөд үүнд эрсдэлийн үнэлгээ, аудит хийлгэх, дотоод кибер аюулгүй байдлын журам, стандартуудыг хэрэгжүүлэх, мөн зөрчилд хариу арга хэмжээ авах төлөвлөгөө боловсруулах үүрэг багтаж байна.

Одоогоор энэ салбар нь кибер аюулгүй байдлын зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, хариу арга хэмжээ авах процесс хэрэгжүүлэх зохицуулалтгүй хэвээр байна. Үүний улмаас харилцаа холбооны байгууллагуудын хэрэгжилтийн түвшин харилцан адилгүй байгаа нь ажиглагдсан.

Кибер аюулгүй байдлын бүтээгдэхүүн үйлдвэрлэдэг компани байхгүй. Монголд ашиглагдаж буй кибер аюулгүй байдлын бүтээгдэхүүнүүдийг гадаадын нийлүүлэгчид хангадаг бөгөөд зарим борлуулагчид Монголд үйл ажиллагаа явуулдаг. Гадны технологид хэт их найдсанаар үүсэх эрсдэлийг багасгахын тулд дотоодын бүтээгдэхүүн хөгжүүлэхийг дэмжих зорилготой байгааг *Кибер аюулгүй байдлын үндэсний стратегид* тусгасан.

Оролцогчдын зүгээс Монгол Улсад кибер аюулгүй байдлын үйлчилгээний салбар сүүлийн гурван жилд хурдацтай өргөжсөн гэж мэдээлсэн. Компаниуд кибер аюулгүй байдлын стандартын нийцэлд аудит хийх, нэвтрэлтийн шалгалт (penetration testing) гүйцэтгэх, Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо (ISMS) хэрэгжүүлэх зэрэг үйлчилгээг санал болгож байна. ОЧМДБ байгууллагуудын зарим нь дотоодын кибер аюулгүй байдлын зөвлөх үйлчилгээг ашиглаж байсан туршлагатай талаар мэдээлсэн. Төрийн байгууллагын зарим оролцогчид кибер аюулгүй байдлын үйлчилгээ үзүүлэгчдийн тоо нэмэгдэж байгаа хэдий ч эрэлт хэрэгцээг хангахад хангалтгүй хэвээр байгааг онцолсон. Ялангуяа, *Кибер аюулгүй байдлын тухай хуулийн* шаардлагыг биелүүлэхэд хангалттай үйлчилгээ үзүүлэгчид байхгүй байгааг тэмдэглэсэн. *Кибер аюулгүй байдлын тухай хуулийн* дагалдах журмуудад онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудад аудит хийх үйлчилгээ үзүүлэгчид нь мэргэжлийн холбоо эсхүл стандартын байгууллагаар баталгаажсан мэргэжилтнийг бүтэн цагаар ажиллуулсан байх шаардлагатай гэж заасан. Үүний дагуу ЦХИХХЯ-с үнэлгээ хийсэн бөгөөд уг шаардлагыг маш цөөн тооны үйлчилгээ үзүүлэгч нар хангаж байна.

Зарим байгууллага мэдээллийн технологийн үйлчилгээгээ аутсорсинг байдлаар шийдэж байна. Төрийн зарим байгууллагын хувьд мэдээллийн системийг заавал төрийн үүлэн технологи (government cloud) эсхүл Үндэсний Дата Төвд шууд байрлуулах шаардлагатай байдаг. Зарим төрийн агентлагуудыг оруулаад бусад байгууллагууд ҮДТ-д үйлчилгээ байршуулахыг сонгох боломжтой бөгөөд зарим нь олон улсын үүлэн технологид суурилсан үйлчилгээ зэрэг гуравдагч талын үйлчилгээ үзүүлэгчийг сонгодог. Аутсорсингоос үүсэх эрсдэлүүдийг тодорхойлох, бууруулах процесс нь байгууллага бүрд харилцан адилгүй бөгөөд тухайн байгууллагын төлөвшлийн түвшнээс хамаарч байна. Уг эрсдэлийг бууруулахтай холбоотой зарим хууль, эрх зүйн зохицуулалтууд бий. Тухайлбал, *Хүний хувийн мэдээлэл хамгаалах тухай хуульд* Монгол Улсын иргэдийн хувийн мэдээллийг заавал улсын хил дотор биет байдлаар хадгалах шаардлагыг тусгасан байдаг. ҮДТ нь ЦХИХХЯ -тай хамтран мэдээллийг ангилах түвшин болон хаана байршуулж болох талаар тодорхой чиглэл өгөх бодлогыг боловсруулах төлөвлөгөөтэй байгаагаа мэдээлсэн.

Кибер даатгалын үйлчилгээ Монгол Улсад шинээр хөгжиж буй бөгөөд Үндэсний төвийн цахим хуудаст кибер даатгалын талаарх танилцуулга болон зөв зохистой даатгалын бүтээгдэхүүнийг сонгох зөвлөмж нийтлэгдсэн. Харин оролцогч талууд дотоодын компаниуд кибер даатгалын үйлчилгээ үзүүлж байгаа талаар огт мэдээлэлгүй байсан бөгөөд олон улсын нийлүүлэгчид Монголын компаниудад ийм төрлийн бүтгээдэхүүн үйлчилгээ санал болгодог талаар дурдсан. Кибер даатгалын хэрэглээ одоогоор анхан шатандаа байгаа бөгөөд үнэлгээний хүрээнд зөвлөлдсөн оролцогчдын дунд кибер даатгалын бүтээгдэхүүн ашиглаж байсан туршлагатай хүн байгаагүй.

Зарим салбар байгууллагууд нь өөр хоорондоо аюул занал болон эмзэг байдлын мэдээллийг хуваалцах механизм хэрэгжиж байна. Тухайлбал, банкны салбарт Аюулгүй Байдлын Мэдээлэл Хуваалцах, Шинжилгээний Төв (ISAC) ажиллаж байгаа бөгөөд үүгээр дамжуулан санхүүгийн байгууллагууд аюул занал болон эмзэг байдлын мэдээллээ солилцдог гэж мэдээлсэн. Санхүүгийн салбарын зарим байгууллагууд олон улсын кибер аюул, заналын мэдээлэл (CTI) хүлээн авах, түгээх сувгуудад бүртгэлтэй байдаг гэж тэмдэглэсэн. Түүнчлэн, томоохон хувийн хэвшлийн байгууллагуудаас бүрдсэн MNCERT/CC-ийн гишүүд өөр хоорондоо мэдээлэл солилцож байна. Гэсэн хэдий ч илүү өргөн хүрээний байгууллагууд ашиглаж болох мэдээлэл хуваалцах механизмыг Монгол Улсад хөгжүүлэх нь аюул занал болон эмзэг байдлын талаарх мэдээллийн солилцоог нэмэгдүүлэхэд тустай байх болно гэж үзэж байна.

Монгол Улсад ёс зүйтэй халдлага хийх соёл болон эмзэг байдлын мэдээлэл ил болгох практик тодорхой хэмжээгээр хөгжиж байна. Цоорхой олох (bug-bounty) хөтөлбөрийг хэрхэн хэрэгжүүлэх талаар зохион байгуулагдсан арга хэмжээнүүдийн үр дүнд зарим компаниуд өөрсдийн системийн эмзэг байдлыг илрүүлэхийн тулд судлаач нарыг урьж оролцуулсан тохиолдлууд гарсан. Түүнчлэн зарим байгууллага эмзэг байдлын мэдээлэл хариуцлагатайгаар ил болгох журамтай бөгөөд энэ нь тэдний програм хангамж эсхүл вэбсайтад эмзэг байдал илэрсэн тохиолдолд дагаж мөрдөх үйл явцыг нарийвчлан тодорхойлсон байдаг. Энэхүү үйл явц нь байгууллагын соёл болон төлөвшлийн түвшнээс хамааралтай бөгөөд ихэвчлэн хувийн хэвшлийн санхүүгийн байгууллага дунд түгээмэл ажиглагдаж байна. Одоогоор хариуцлагатай мэдээлэл ил болгох механизмыг тууштай хэрэгжүүлээгүй нь төрийн болон бусад байгууллагуудын аюулгүй байдлын эмзэг байдлыг үр дүнтэй мэдээлэх, засварлах үйл явцад саад учруулж болзошгүй юм.

Эмзэг байдлын мэдээллийг хариуцлагатайгаар ил болгодог судлаачдыг хамгаалах хууль эрх зүйн зохицуулалт одоогоор Монгол Улсад байхгүй байна. Монгол дахь ёс зүйтэй халдлага хийх (ethical hacking) бүлгэм дэх зарим оролцогчын мэдээлсэнээр компаниудад хандахаас эмээдэг бөгөөд энэ нь хууль эрх зүйн хариуцлага хүлээхээс айх айдастай холбоотой байж болзошгүй гэж тэмдэглэсэн. Судлаачдыг хамгаалах механизмыг хөгжүүлэх нь ашигтай бөгөөд үүнийг Монгол Улсын нөхцөл байдалд тохирсон байдлаар хэрэгжүүлэх шаардлагатай гэж үзэж байна.

ТАНИЛЦУУЛГА

Цахим Хөгжил, Инноваци, Харилцаа Холбооны Яам (ЦХИХХЯ)-ын урилгаар болон Японы Олон Улсын Хамтын Ажиллагааны Байгууллага (ЖАЙКА)-тай хамтран Дэлхийн Кибер Аюулгүй Байдлын Чадавхын Төв нь Монгол Улсын кибер аюулгүй байдлын чадавхын үнэлгээг хийв. Энэхүү үнэлгээний зорилго нь Монгол Улсад кибер аюулгүй байдлын чадавхын тодорхой чиглэлүүдийг тодорхойлж, үндэсний кибер аюулгүй байдлын нөхцөл байдлыг сайжруулахын тулд засгийн газар стратегийн хөрөнгө оруулалт хийх боломжтой салбаруудыг тодорхойлох боломжийг олгоход оршино.

Кибер аюулгүй байдлын чадавхын хэмжээс

Зөвлөлдөх уулзалтуудыг Дэлхийн Кибер Аюулгүй Байдлын Чадавхын Төв (GCSCC) -ийн Кибер Аюулгүй Байдлын Чадавхын Төлөвшлийн Загвар (ЧДЗ) [3]-ын дагуу зохион байгуулсан бөгөөд энэхүү загвар нь кибер аюулгүй байдлын чадавхын таван хэмжээснээс бүрдэнэ.

Хэмжээс тус бүр нь кибер аюулгүй байдлын чадавхыг тодорхойлох, тайлбарлах хүчин зүйлсээс бүрдэх бөгөөд эдгээр нь тухайн чиглэлд чадавхыг бүрдүүлэхэд ямар шаардлага хангасан байх ёстойг тодорхойлдог.

Доорх хүснэгтэд эдгээр таван хэмжээс болон тэдгээрт хамаарах хүчин зүйлсийг харууллаа.

[3] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), 2021 Edition," March 2021, https://gcscc.ox.ac.uk/the-cmm#/.

ХЭМЖЭЭСНҮҮД	ХҮЧИН ЗҮЙЛС
Хэмжээс 1 **Кибер аюулгүй байдлын бодлого болон стратеги**	D1.1 Стратеги хөгжүүлэлт D1.2 Зөрчилд хариу үзүүлэх болон онцгой байдлын менежмент D1.3 Онц чухал мэдээллийн дэд бүтцийн хамгаалалт D1.4 Батлан хамгаалах болон үндэсний аюулгүй байдалд кибер аюулгүй байдлын оролцоо
Хэмжээс 2 **Кибер аюулгүй байдлын соёл болон нийгэм**	D2.1 Кибер аюулгүй байдлын сэтгэлгээ D2.2 Онлайн үйлчилгээнд итгэх итгэл D2.3 Онлайн орчин дахь хувийн мэдээлэл хамгаалах тухай хэрэглэгчийн ойлголт D2.4 Тайлагнах механизм D2.5 Хэвлэл мэдээлэл болон онлайн платформууд
Хэмжээс 3 **Кибер аюулгүй байдлын мэдлэг болон чадамж бий болгох**	D3.1 Кибер аюулгүй байдлын талаарх мэдлэгийг нэмэгдүүлэх D3.2 Кибер аюулгүй байдлын боловсрол D3.3 Кибер аюулгүй байдлын мэргэжлийн сургалт D3.4 Кибер аюулгүй байдлын судалгаа болон инновац
Хэмжээс 4 **Хууль, эрх зүйн зохицуулалт**	D4.1 Хууль, эрх зүйн зохицуулалтын заалтууд D4.2 Холбогдох хууль, эрх зүйн хүрээ D4.3 Хууль, эрх зүйн чадамж болон хүчин чадал D4.4 Кибер гэмт хэрэгтэй тэмцэх албан болон албан бус хамтын ажиллагааны тогтолцоо
Хэмжээс 5 **Стандарт болон технологи**	D5.1 Стандартын мөрдөлт D5.2 Аюулгүй байдлын хяналтууд D5.3 Програм хангамжийн чанар D5.4 Харилцаа холбоо болон интернэт дэд бүтцийн уян хатан байдал D5.5 Кибер аюулгүй байдлын зах зээл D5.6 Хариуцлагатайгаар ил болгох

Кибер аюулгүй байдлын чадавхын төлөвшлийн үе шат

Хэмжээс тус бүр нь кибер аюулгүй байдлын чадавхыг тодорхойлох хэд хэдэн *хүчин зүйлээс* бүрдэнэ. Хүчин зүйл бүр нь холбогдох *үзүүлэлтүүдийг* нэгтгэсэн бүрэлдэхүүн хэсгүүдтэй бөгөөд эдгээр үзүүлэлтүүд нь тухайн хүчин зүйлийн төвөвшлийн түвшнийг тодорхойлдог.

Кибер аюулгүй байдлын чадавхыг *эхлэл* түвшнээс (start-up) *динамик* түвшин (dynamic) хүртэл таван үе шаттайгаар үнэлдэг. Эхлэл түвшин нь чадавхыг хөгжүүлэхэд эмх цэгцгүй, түр зуурын арга барилтай байгааг илэрхийлэх бол, динамик түвшин нь стратегийн хандлага баримталж, орчны нөхцөл байдлыг харгалзан уян хатан зохицох, өөрчлөлт хийх чадвартай болохыг илтгэнэ. Эдгээр таван түвшинг дараах байдлаар тодорхойлно:

- Эхлэл түвшин (start-up): Энэ түвшинд кибер аюулгүй байдлын чадавх байхгүй, эсхүл маш анхан шатны түвшинд гэж үзнэ. Кибер аюулгүй байдлын чадавхыг хөгжүүлэх талаар анхны яриа хэлэлцүүлэг хийгдсэн байж болох ч бодит арга хэмжээ авч хэрэгжүүлээгүй буюу бодит нотолгоо хангалтгүй.
- Хөгжиж буй түвшин (formative): Тухайн чиглэлийн зарим элементүүд хөгжиж эхэлсэн бөгөөд тодорхой хэмжээнд бүрэлдэн тогтож байгаа боловч түр зуурын, эмх замбараагүй, тодорхой бус эсхүл шинээр үүсэж буй байдалтай байж болно. Гэсэн хэдий ч энэ үйл ажиллагаа бодитойгоор хэрэгжиж буйг нотлох баримтууд тодорхой харагдана.
- Тогтворжсон түвшин (established): Хэмжээсийг үнэлэх үзүүлэлтүүд тогтсон бөгөөд тэдгээр нь ажиллаж байгааг нотлох баримтууд бий. Гэсэн хэдий ч нөөцийн оновчтой хуваарилалтад нарийн дүн шинжилгээ хийгдээгүй. Хэрэгжилтийн хувьд тодорхой түвшинд хүрсэн боловч хөрөнгө оруулалт, стратегийн оновчтой шийдвэр гаргах үйл явц хараахан хөгжөөгүй гэж үзнэ.
- Стратегийн түвшин (strategic): Аль хүчин зүйл нь өндөр ач холбогдолтой, аль нь бага ач холбогдолтой болохыг тодорхойлсон. Энэ түвшин нь тухайн улс эсхүл байгууллагын нөхцөл байдлаас шалтгаалан стратегийн шийдвэр гаргасныг илэрхийлдэг.
- Динамик түвшин (dynamic): Энэ түвшинд улс орны кибер аюулгүй байдлын стратегийг нөхцөл байдалтай уялдуулан өөрчлөх, шинэчлэх тодорхой механизм бүрдсэн байдаг. Үүнд аюул заналын орчинтой холбоотой технологийн өөрчлөлт, олон улсын зөрчил мөргөлдөөн, тодорхой асуудлын (жишээлбэл, кибер гэмт хэрэг эсхүл нууцлал) огцом өөрчлөлт багтаж болно. Мөн энэ түвшинд кибер аюулгүй байдлын чиглэлээр олон улсад манлайлж буй нотолгоо харагдана. Гол салбарууд хөгжлийн аливаа шатанд стратегиа өөрчлөх аргыг боловсруулсан байдаг. Хурдан шийдвэр гаргах, нөөцийг дахин хуваарилах, орчны өөрчлөлтөд байнгын анхаарал хандуулах зэрэг нь энэхүү түвшний онцлох шинж чанарууд юм.

Төлөвшлийн үе шатны үнэлгээ нь цуглуулсан нотолгоонд суурилдаг бөгөөд энэ нь оролцогч талуудын санал, баримт бичигт тулгуурласан судалгаа, үнэлгээ хийж буй судлаачдын мэргэжлийн дүгнэлт дээр үндэслэгддэг. Чадавхын төв нь дээрх аргачлалыг ашиглан энэхүү тайланд Монгол Улсын кибер аюулгүй байдлын чадавхын үнэлгээний үр дүнг танилцуулж, цаашид сайжруулах боломжтой арга хэмжээнүүдийг зөвлөмж хэлбэрээр тусгасан болно.

МОНГОЛЫН КИБЕР АЮУЛГҮЙ БАЙДЛЫН НӨХЦӨЛ БАЙДАЛ

Монгол Улс нь Зүүн Азид оршдог, 1.5 сая км.кв талбайтай өргөн уудам нутагтай улс юм. [4] Хойд талаараа Орос, өмнө талаараа Хятадтай хиллэдэг далайд гарцгүй орон. Монгол Улсад 3.5 сая орчим хүн амьдардаг ба энэ нь нийт газар нутгийн хэмжээтэй харьцуулахад маш цөөн хүн амтай (1 кв.км тутамд дунджаар 2.2 хүн). Хот суурин газарт 2.5 сая орчим хүн амьдардаг бөгөөд нийслэл Улаанбаатар хотод 1.7 сая хүн амьдардаг. Хөдөө орон нутагт амьдардаг 1 сая орчим хүний дийлэнх нь нүүдэлчин иргэд юм. [5]

2024 оны байдлаар Монгол Улсад 2.9 сая орчим интернэт хэрэглэгч байсан ба тэдний ихэнх нь гар утасны өргөн зурвасын технологи ашигладаг. Мөн 2 сая орчим хүн ухаалаг гар утас хэрэглэж[6], 2.5 сая хүн олон нийтийн сүлжээ ашигладаг байна. [7] Монгол Улс нь цахим технологийн хэрэглээгээрээ дэлхийн 133 орноос 88-д жагсдаг[8] бөгөөд хүн амын ихэнх хэсэг 3G сүлжээнд холбогдсон, олон нийтийн сүлжээ идэвхтэй хэрэглэдэг, цахим банк болон цахим худалдааны боломжуудтай зэрэг давуу талуудтай.

Монгол Улс нь Олон Улсын Цахилгаан Холбооны Нийгэмлэгээс гаргадаг Дэлхийн Кибер Аюулгүй Байдлын Индексээр 2024 онд 5 түвшнээс 3-р түвшинд ("Бэхжиж буй") буюу дунд зэрэгт үнэлэгдсэн. Уг үнэлгээгээр "Хууль, эрх зүйн хэмжүүр" болон "Зохион байгуулалтын хэмжүүр" талууд хүчтэй байсан бөгөөд эдгээр ангилалд Монгол Улс Ази, Номхон далайн бүсийн дундаж онооноос илүү өндөр оноо авсан. Харин "Техник, технологийн хэмжүүр" болон "Хамтын ажиллагааны хэмжүүр" талбарууд сул үнэлэгджээ.

Монгол Улс сүүлийн жилүүдэд цахим шилжилтийг дэмжих, кибер аюулгүй байдлыг хангах чиглэлээр хэд хэдэн чухал арга хэмжээ авсан байна.

2021 онд *Кибер Аюулгүй Байдлын тухай хуулийг* баталсан нь энэ салбарт хууль эрх зүйн орчныг бүрдүүлэхэд чухал алхам болсон. 2022 онд Монгол Улсын анхны *Кибер Аюулгүй Байдлын Үндэсний Стратеги* (КАБҮС)-ийг боловсруулсан нь кибер аюулгүй байдлын удирдамж, чиглэлийг тодорхойлоход ач холбогдолтой.

Түүнчлэн, кибер аюулгүй байдлыг хариуцсан шинэ агентлагуудыг байгуулсан нь энэ чиглэлд үйл ажиллагааг идэвхжүүлэх, зохицуулахад чухал үүрэг гүйцэтгэж байна.

---

[4] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf

[5] https://www.1212.mn/en/statistic/file-library/view/86813402

[6] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf

[7] https://download.networkreadinessindex.org/reports/data/2024/nri-2024.pdf

[8] https://download.networkreadinessindex.org/reports/data/2024/nri-2024.pdf

Тухайлбал, 2022 онд Цахим Хөгжил, Харилцаа Холбооны Яам (ЦХИХХЯ), 2023 онд Үндэсний Кибер Аюулгүй Байдлын Зөвлөл, мөн ЦХИХХЯ болон Тагнуулын Ерөнхий Газрын (ТЕГ) харьяанд Кибер халдлага, зөрчилтэй тэмцэх Үндэсний болон Нийтийн төвүүдийг шинээр байгуулсан.

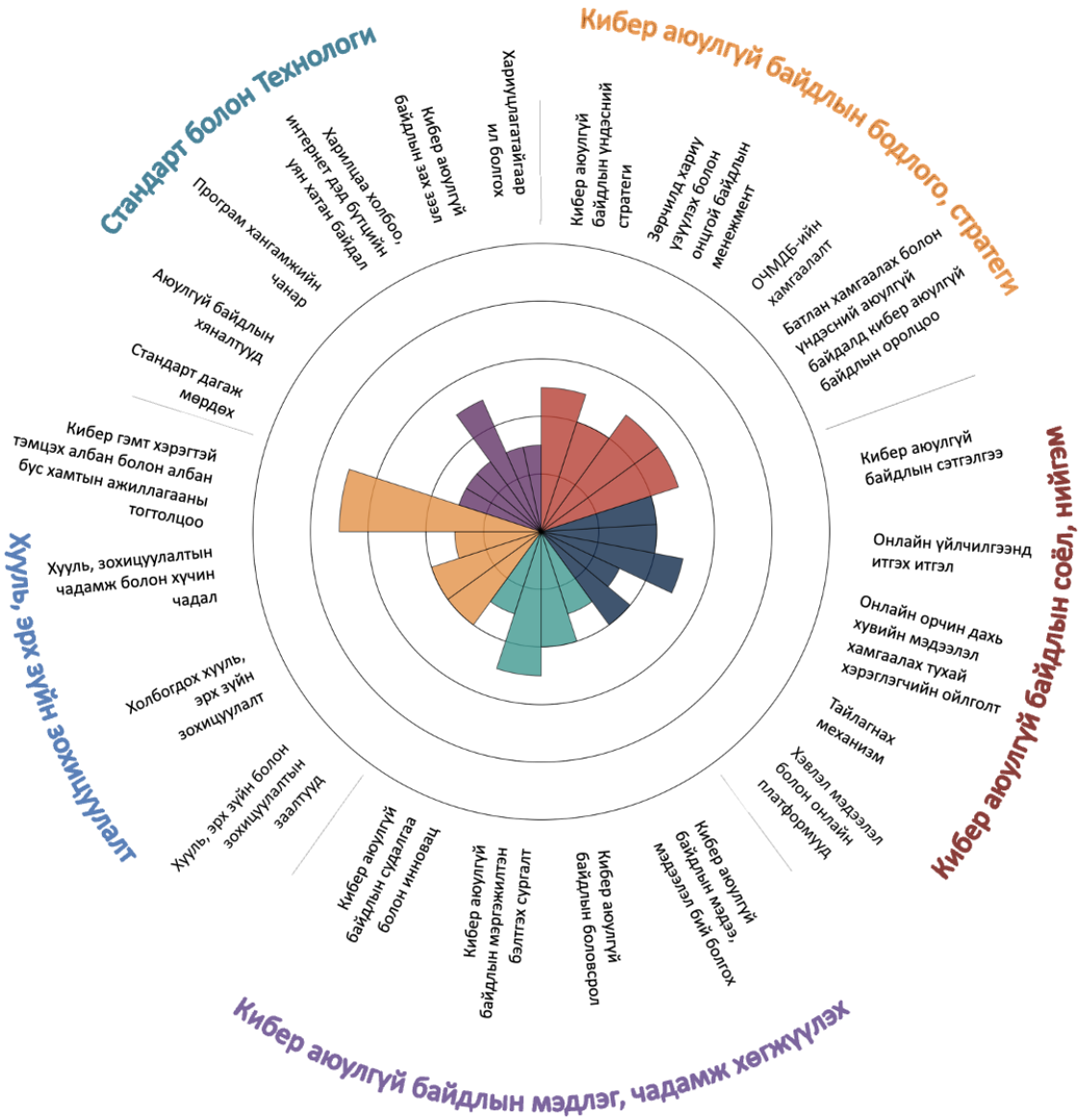
Энэхүү тайлангийн зөвлөмжүүд нь Монгол Улсын кибер аюулгүй байдлын чадавх, чадамжийг сайжруулахад чухал ач холбогдолтой бөгөөд зөвлөмжүүд нь одоогийн хэрэгжиж буй төслүүдийн хүрээнд хийгдэж буй ажлуудыг үргэлжлүүлэн дэмжих, цаашид шаардлагатай арга хэмжээнүүдийг авахад чиглэсэн.

2025 онд *Кибер аюулгүй байдлын тухай хууль* хэрэгжиж эхлэхтэй холбогдуулан энэ цаг үед төлөвшлийн үнэлгээг хийж, ирээдүйн үйл ажиллагааг дэмжихэд чиглэсэн зөвлөмжүүдийг боловсруулах нь ихээхэн ач холбогдолтой.

ҮНЭЛГЭЭНИЙ ТАЙЛАН

Хураангуй

Энэ хэсэг нь Монгол Улсын кибер аюулгүй байдлын чадавхын ерөнхий төлөвийг харуулж байна. *Зураг 2*-т хэмжээс бүрийн төлөвшлийн түвшний үнэлгээг үзүүлэв. Хэмжээс бүр графикийн тавны нэгийг илэрхийлэх бөгөөд хүчин зүйл бүрийн хөгжлийн таван үе шат нь төвөөс гадагш чиглэн байрлана. Төвд нь "эхлэл" (start-up) түвшин байршиж, хамгийн гадна талд "динамик" (dynamic) түвшин байрлана.

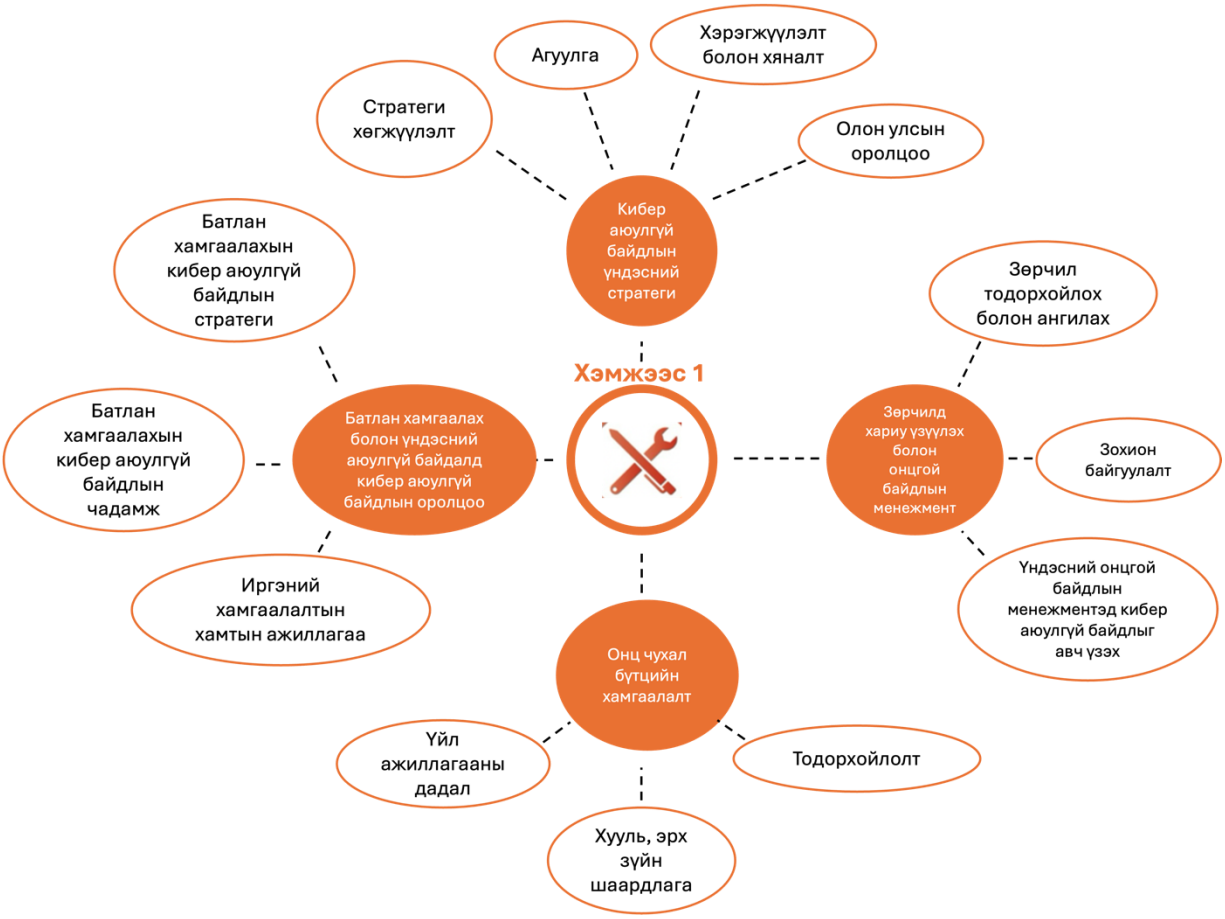


Зураг 2: Монгол Улс дахь кибер аюулгүй байдлын чадавхын ерөнхий зураглал.

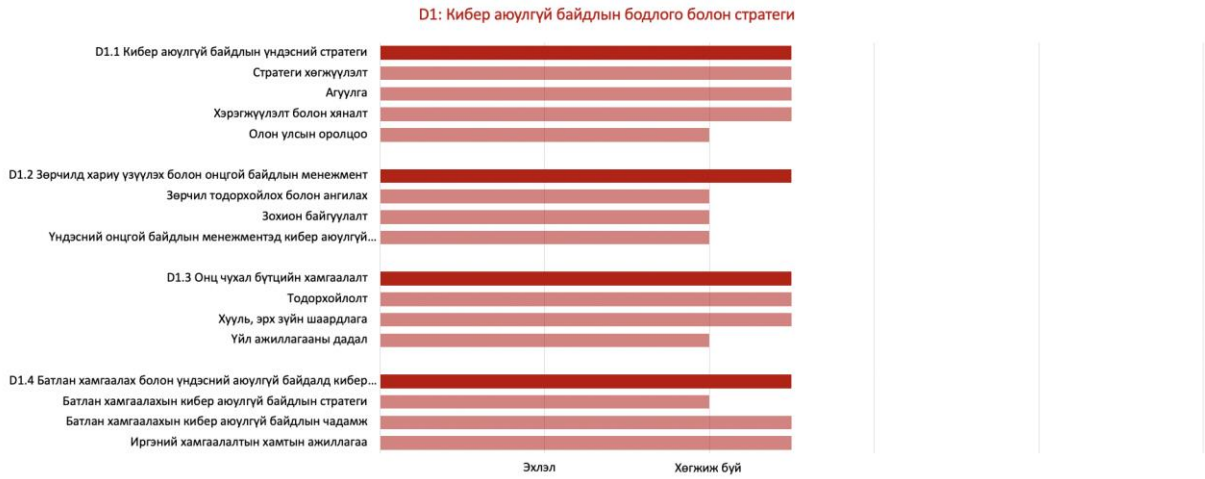
ХЭМЖЭЭС 1

КИБЕР АЮУЛГҮЙ БАЙДЛЫН БОДЛОГО БОЛОН СТРАТЕГИ

Энэхүү хэмжээс нь Монгол Улсын кибер аюулгүй байдлын стратеги боловсруулах, хэрэгжүүлэх, кибер аюулгүй байдлын төлөвшлийг сайжруулах чадавхыг үнэлэхэд оршино. Үүнд зөрчилд хариу арга хэмжээ авах, кибер хамгаалалт, онц чухал мэдээллийн дэд бүтцийг хамгаалах чадавхыг нэмэгдүүлэх боломжийг авч үзнэ. Энэхүү хэмжүүр нь үндэсний кибер аюулгүй байдлын чадамжийг үр дүнтэй хэрэгжүүлэх стратеги, бодлогыг харгалзан үзэхийн зэрэгцээ, төр, олон улсын бизнес, нийгэмд зайлшгүй шаардлагатай кибер орон зайд давуу талуудыг хадгалах асуудлыг хамардаг.



ҮР ДҮНГИЙН ТОЙМ



D 1.1 КИБЕР АЮУЛГҮЙ БАЙДЛЫН ҮНДЭСНИЙ СТРАТЕГИ

Кибер аюулгүй байдлын стратеги нь төрийн түвшинд кибер аюулгүй байдлын асуудлыг бодлогын үндсэн чиглэл болгон нэгтгэхэд чухал ач холбогдолтой. Мөн кибер аюулгүй байдлыг нэн тэргүүний бодлогын чиглэл болгон тодорхойлж, төрийн болон төрийн бус байгууллагын гол оролцогч талуудын үүрэг, хариуцлагыг тодорхойлохын зэрэгцээ, шинээр үүсэж буй болон тулгамдаж буй кибер аюулгүй байдлын асуудлуудад чиглэсэн нөөцийн хуваарилалтыг удирдан чиглүүлнэ.

Түвшин: **Хөгжиж буй түвшнээс Тогтворжсон түвшинд**

Монгол Улсын анхны *Кибер Аюулгүй Байдлын Үндэсний Стратеги* (КАБҮС) нь 2022 оны 12-р сарын 28-нд Монгол Улсын Засгийн газрын 493 дугаар тогтоолоор батлагдсан.[9] Энэхүү стратеги нь 2021 оны 12-р сард батлагдсан *Кибер аюулгүй байдлын тухай хуулийн* 10.1.1-р зүйлийн дагуу боловсруулагдсан бөгөөд *Кибер Аюулгүй Байдлын Үндэсний Стратегийг*[10] боловсруулах, Үндэсний Кибер Аюулгүй Байдлын Зөвлөлийг[11] байгуулах тухай заалтуудыг агуулжээ.

Түүнчлэн, 2021 оны 12-р сард *Кибер аюулгүй байдлын тухай хуулийн* төслийг УИХ-д өргөн барьсантай холбогдуулан Цахим хөгжил, инновац харилцаа холбооны яам (ЦХИХХЯ) нь үндэсний хэмжээнд кибер аюулгүй байдлыг хангах чиглэлээр ажилладаг төрийн захиргааны төв байгууллага болсон юм[12].

КАБҮС-ийг боловсруулахад ЦХИХХЯ, ТЕГ болон Зэвсэгт хүчний ерөнхий штабаас бүрдсэн ажлыг хэсэг байгуулагдсан. Хамтарсан ажлын хэсэг байгуулагдан ажилласан бөгөөд тухайн ажлын хэсэгт мөн их, дээд сургуулиудын төлөөлөл, иргэний нийгмийн байгууллагуудын төлөөлөл багтан ажилласан. КАБҮС-ын хөгжүүлэлтийг ЦХИХХЯ

[9] https://legalinfo.mn/mn/detail?lawId=16532522757001
[10] https://legalinfo.mn/mn/claw/16390365491061/1646096916023354
[11] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf
[12] https://mddc.gov.mn/eng/%d0%b1%d2%af%d1%82%d1%8d%d1%86

болон ТЕГ-аас явуулсан судалгааны дэмжлэгтэйгээр боловсруулсан. Тус судалгааны хүрээнд 600 гаруй төрийн байгууллага болон ОЧМДБ байгууллагуудын халдлагад өртөх магадлалыг тодорхойлох судалгаа, олон нийтийн кибер аюулгүй байдлын талаарх мэдлэгийн түвшний судалгаа, Ази, Европын бусад улс орнуудын Үндэсний кибер аюулгүй байдлын стратегийн судалгаа зэрэг багтана. КАБҮС-д кибер аюулгүй байдлын эрсдэлийг үнэлэх зорилготой *"Кибер халдлагаас хамгаалах төлөвлөгөө боловсруулж, тасралтгүй сайжруулах хяналтын арга хэмжээнүүдийг хэрэгжүүлэх нь*" гэсэн үйл ажиллагааг тусгасан[13]. Түүнчлэн энэхүү төлөвшлийн үнэлгээгээр олж авсан мэдлэг, дүгнэлтийг цаашдын КАБҮС-ийн шинэчлэлд ашиглах шаардлагатай.

КАБҮС-ын алсын хараа "Засгийн газар, иргэд болон хуулийн этгээдийн мэдээллийн аюулгүй байдал, нууцлалтай , хүртээмжтэй байдлыг кибер орчинд үндэсний түвшинд хангана." гэж тодорхойлсон. Уялдах стратегийн зорилго нь: "Кибер аюулгүй байдлын эрх зүйн орчныг сайжруулах, нэгдсэн удирдлагын тогтолцоог бий болгох, ОЧМДБ-ийн кибер аюулгүй байдлыг хангах, уян хатан байдлыг нэмэгдүүлэх, олон нийтийн кибер аюулгүй байдлын мэдлэгийг дээшлүүлэх, хүний нөөцийн чадамжийг дотоод болон гадаад талаасаа сайжруулах юм. Энэхүү стратегийн зорилго нь хамтын ажиллагааг хөгжүүлэх замаар кибер орчин дахь мэдээллийн аюулгүй байдал, нууцлал, хүртээмжийг үндэсний түвшинд хангахад чиглэнэ." Үүний тулд КАБҮС дараах стратегийн зорилтуудыг дэвшүүлсэн байна. Үүнд:

1. Хууль эрх зүйн орчныг сайжруулж, нэгдсэн удирдлагын системийг бүрдүүлэх замаар кибер аюулгүй байдлыг бэхжүүлэх.
2. Онц чухал мэдээллийн дэд бүтцийн кибер аюулгүй байдлыг бэхжүүлэх.
3. Кибер аюулгүй байдлын салбарт ажиллаж буй хүний нөөцийн чадавхыг дээшлүүлэх, шинэ боловсон хүчнийг бэлтгэх, давтан сургах замаар мэргэшсэн хүний нөөцийг бүрдүүлэх.
4. Кибер аюулгүй байдлын чиглэлээр хамтын ажиллагааг өргөжүүлэх.
5. Кибер аюулгүй байдлын уян хатан байдлыг нэмэгдүүлж, халдлага, зөрчилд хариу үйлдэл үзүүлэх, сэргээн засварлах чадавхыг бэхжүүлэх.

Эдгээр зорилтуудын хүрээнд нарийвчилсан үйл ажиллагаануудыг тодорхойлсон. Үүнд Үндэсний Кибер Аюулгүй Байдлын Зөвлөлийг байгуулах ажил багтсан бөгөөд уг зөвлөл нь "кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлага, зохицуулалтаар хангах, хэрэгжилтийг зохион байгуулах, мэдээлэл солилцох, үйл ажиллагааг уялдуулах" үүрэгтэйгээр байгуулагдсан. Мөн онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудыг хамгаалах зорилгоор Кибер халдлага, зөрчилтэй тэмцэх Үндэсний төвийг байгуулах, кибер гэмт хэргийг бууруулах арга хэмжээнүүдийг хэрэгжүүлэх, олон нийтийн кибер аюулгүй байдлын мэдлэгийг нэмэгдүүлэх зэрэг ажлууд тусгагдсан. КАБҮС нь цахим орчинд хүүхэд хамгаалал болон хүний эрхийг хамгаалах хууль эрх зүйн тогтолцоог сайжруулах зэрэг өргөн хүрээний бодлогын зорилтуудыг дэмжих үйл ажиллагааг мөн багтаасан байна.

Кибер аюулгүй байдлын үндэсний стратеги (КАБҮС) нь шинэ дэвшилтэт технологи хэрэглээнээс үүдэлтэй эрсдэлүүдийг хянах шаардлагатайг тусган, дараах үйл ажиллагааг тодорхойлсон: "их өгөгдөл (Big Data), хиймэл оюун ухаан (AI), зүйлсийн интернет (IoT), үүлэн технологи, машин сургалт зэрэг дэвшилтэт технологийн хэрэглээнээс үүсэж болзошгүй эмзэг байдал болон аюул заналыг тодорхойлж, эрсдэлийг бууруулах

[13] https://legalinfo.mn/mn/detail?lawId=16532522791411&showType=1

чадамжийг сайжруулах”. Кибер халдлага, зөрчилтэй тэмцэх төвүүд D1.2-т дурдсанчлан тодорхой үүрэг гүйцэтгэх бөгөөд тэдний үйл ажиллагаа, оруулах хувь нэмрийг *Кибер Аюулгүй Байдлын Үндэсний Стратеги* (КАБҮС) болон Үйл Ажиллагааны Төлөвлөгөөг шинэчлэхэд ашиглах нь чухал юм.

КАБҮС нь хоёр үе шаттай хэрэгжиж байгаа бөгөөд I үе шат 2022-2025 он, II үе шат 2026-2027 оныг хамарч байна. Зорилтуудын хэрэгжилтийг үнэлэхдээ тодорхой, хэмжигдэхүйц үр дүнг тодорхойлсон бөгөөд Гүйцэтгэлийн Түлхүүр Үзүүлэлт (KPI)-ийн дагуу үнэлнэ. Жишээлбэл, эрх зүйн зохицуулалтыг бэхжүүлэх тухай зорилт I-ийн хувьд тодорхойлсон нэг үзүүлэлт нь батлагдсан кибер аюулгүй байдлын зохицуулалтын тоо юм.

KPI-д хэмжих нэгж, суурь түвшин, хэрэгжилтийн I болон II үе шатын төгсгөлд хүрэх зорилтот түвшин, мөн шаардлагатай тохиолдолд тухайн үзүүлэлтийн хэрэгжилтийг үнэлэх мэдээллийн эх сурвалжуудыг тусгасан. Үүнд төлөвлөгдсөн төрийн судалгаанууд, академик судалгаанууд, Олон Улсын Цахилгаан Холбооны Холбоо (ITU), Зөрчилд Хариу Үзүүлэх болон Аюулгүй Байдлын Багуудын Форум (FIRST) зэрэг олон улсын байгууллагуудаас гаргасан эх сурвалжууд багтана.

КАБҮС-ийн зэрэгцээ ЦХИХХЯ, ТЕГ, Зэвсэгт Хүчний Ерөнхий Штаб хамтран Үйл Ажиллагааны Төлөвлөгөөг боловсруулсан. Энэхүү төлөвлөгөө нь Засгийн газрын албан ёсны стратегийн үйл ажиллагааны төлөвлөгөөний форматыг дагаж, үйл ажиллагаа бүрийг хариуцах үндсэн байгууллагуудыг тодорхойлж, шаардлагатай хамтрагч байгууллагуудыг заасан болохыг мэдээлсэн. Жишээлбэл, олон нийтийн кибер аюулгүй байдлын мэдлэгийг дээшлүүлэхтэй холбоотой арга хэмжээг Боловсролын яам хариуцаж байгаа нь салбар дундын хамтын ажиллагааг хангахад чухал үүрэгтэй.

КАБҮС-д дурдсанаар, стратегийг хэрэгжүүлэх хөтөлбөрийн уялдаа зохицуулалт нь засгийн газар болон Үндэсний кибер аюулгүй байдлын зөвлөлийн хариуцлага юм. Стратегийн хэрэгжилтийн үнэлгээ одоогоор хийгдээгүй байна. Анхны үнэлгээ нь стратегид тодорхойлогдсон үзүүлэлтүүд болон зорилтот түвшнүүдийн дагуу хэрэгжилтийн I үе шатны төгсгөлд (2025 он) хийхээр төлөвлөгдсөн. ЦХИХХЯ нь үнэлгээний байгууллагаар ажиллаж, үр дүнг Кибер Аюулгүй Байдлын Зөвлөлд танилцуулна. Хэрэв тогтоосон зорилтууд биелэхгүй бол Кибер Аюулгүй Байдлын Зөвлөлийн ажлын алба залруулах арга хэмжээ авах, зөвлөмж боловсруулах үүрэгтэй нь хариуцлагын механизмыг мөн бүрдүүлж байна.

Үндэсний Кибер Аюулгүй Байдлын Зөвлөл нь байгуулагдаад удаагүй бөгөөд 2023 оны 2 сарын 1-ний өдрийн Засгийн газрын 42 дугаар тогтоолын 01 дүгээр хавсралтад тусгасан журмын дагуу байгуулагдсан. Зөвлөлийн зорилго нь улирал тутам болон онцгой нөхцөл байдал үүссэн үед хуралдах боловч гишүүдийн боломжит цаг хомс байгаагаас шалтгаалан цөөн хуралдаан зохион байгуулагдсан.

Зөвлөлийн бүрэлдэхүүн өргөн хүрээг хамардаг бөгөөд Ерөнхий сайд, Цахим хөгжил, харилцаа холбооны сайд, Тагнуулын ерөнхий газрын дарга нар тэргүүлдэг. Зөвлөлийн гишүүд дараах байгууллагуудаас бүрдэнэ:

- Хууль зүй, дотоод хэргийн сайд болон Ерөнхий прокурор
- Цахим хөгжил, инновац, харилцаа холбооны яамны Төрийн нарийн бичгийн дарга
- Цагдаагийн ерөнхий газрын дэд дарга
- Монгол Улсын Зэвсэгт хүчний жанжин штабын нэгдүгээр орлогч дарга
- Үндэсний Кибер халдлага, зөрчилтэй тэмцэх төвийн дарга

- Кибер халдлага, зөрчилтэй тэмцэх нийтийн төвийн дарга
- Зэвсэгт хүчний Кибер халдлага, зөрчилтэй тэмцэх төвийн дарга
- Үндэсний Дата Төвийн захирал
- Мэдээлэл, холбооны сүлжээ ХХК-ийн захирал
- Кибер аюулгүй байдлын зөвлөлийн ажлын албаны дарга
- Монгол Улсын Харилцаа холбооны зохицуулах хорооны дарга [14]

Энэхүү бүрэлдэхүүн нь КАБҮС-ийг хэрэгжүүлэх хөтөлбөрийг үр дүнтэй уялдуулан зохицуулахад шаардлагатай харагдах байдал болон эрх мэдлийг хангаж, аливаа дутагдлыг арилгахад арга хэмжээ авахад туслах ёстой.

Гэсэн хэдий ч, *Кибер аюулгүй байдлын үндэсний стратеги* (КАБҮС)-ийн хэрэгжилтийн явцыг уялдуулан зохицуулах, хянах чиглэлээр Зөвлөлийн үр нөлөөг тасралтгүй үнэлэх нь чухал юм. Ялангуяа, Зөвлөл хангалттай тогтмол хуралдаж, хэрэгжилтийн явц дахь яаралтай эрсдэл, хамааралтай хүчин зүйлс болон төсвийн дутагдлыг тодорхойлж, КАБҮС-ийн үе шатуудын хэрэгжилтийн явцад тулгарч буй асуудлуудыг шийдвэрлэх механизмыг бүрдүүлэх нь нэн чухал юм.

Цаашлаад, КАБҮС-ийн хэрэгжилтийн удирдлага, хяналтын үйл явцад хувийн хэвшил болон иргэний нийгмийн байгууллагуудыг татан оролцуулах механизм бий болгох нь үр дүнтэй байж болох юм. КАБҮС-ийн хэрэгжилтийн үйл ажиллагаанд хариуцсан төрийн байгууллагууд өөрсдийн төсвийг хянаж, хэрэгжилтэд шаардлагатай төсвийг өөрийн харъяа яамны санхүүжилтээр шийдвэрлэх эсхүл өөр эх үүсвэрээс хангах үүрэгтэй. Монгол Улсын Засгийн газрын 493 дугаар тогтоолд: "*Засгийн газрын гишүүд, аймаг, нийслэлийн засаг дарга нар нь "Кибер аюулгүй байдлын үндэсний стратеги"-д тусгагдсан зорилт, үйл ажиллагааг хэрэгжүүлэхэд шаардлагатай хөрөнгийг жил бүрийн улсын төсөвт тусгах, хувийн хэвшлийн хөрөнгө оруулалтыг татах, гадаадын зээл, тусламжийн санхүүжилтийн эх үүсвэрээр санхүүжүүлэх арга хэмжээ авах*" [15] гэж заасан байдаг.

КАБҮС-д зааснаар эдгээр төсвийг төв болон орон нутгийн засгийн газрын төсвөөс гаргахын зэрэгцээ, "хандивлагч орнууд, олон улсын банкууд, санхүүгийн байгууллагуудын зээл, буцалтгүй тусламж, хувийн хэвшлийн хамтын ажиллагааны хөрөнгө оруулалт" зэрэг эх үүсвэрүүдээр санхүүжүүлэхээр төлөвлөсөн.

Кибер аюулгүй байдлын үндэсний стратеги (КАБҮС)-ийг бүрэн хэрэгжүүлэхэд шаардлагатай санхүүгийн нөөцийг Цахим хөгжил, инновац, харилцаа холбооны яам (ЦХИХХЯ) тооцоолсон. ЦХИХХЯ-ны төлөөлөгчид энэхүү төсвийн тодорхой хэсгийг төрийн санхүүжилтээр шийдвэрлэх боломжтой гэж үзсэн бол үлдсэн санхүүжилтийг гадны эх үүсвэрээс босгох шаардлагатайг тэмдэглэсэн. Гэсэн хэдий ч хөтөлбөрийг бүрэн хэрэгжүүлэхэд шаардлагатай бүх санхүүгийн эх үүсвэрийг гадаад санхүүжилтээр баталгаажуулсан эсэх нь тодорхойгүй байна.

Мөн хэлэлцүүлэгт оролцогчид төрөөс кибер аюулгүй байдлын санхүүжилтийг шийдвэрлүүлэхэд тулгарч буй хүндрэлүүдийг хөндсөн бөгөөд төрийн байгууллагуудад зориулсан кибер аюулгүй байдлын төсвийг Сангийн яам үргэлж баталдаггүй асуудал байгааг онцолсон. Түүнчлэн, кибер аюулгүй байдлын мэргэжилтнүүдийн хомсдол нь

[14] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf

[15] https://legalinfo.mn/mn/detail?lawId=16532522757001

КАБҮС-ийн хэрэгжилтэд хүндрэл учруулж буй нэмэлт хүчин зүйл болохыг өргөн хүрээнд дурдсан.

Нөгөө талаас, КАБҮС-ын Зорилт 4 -ийн хүрээнд олон услын оролцоог өрөгжүүлэхтэй холбоотой үйл ажиллагааг тусгасан бөгөөд Монгол Улсын үндэсний эрх ашгийг хөндөхгүйгээр кибер аюулгүй байдал, гэмт хэрэгтэй тэмцэх чиглэлээр олон улсын болон бүс нутгийн байгууллагуудтай хамтран ажиллах, олон улсын байгууллагын гишүүнчлэлд элсэх боломжийг эрэлхийлэх зорилтыг дэвшүүлсэн. КАБҮС-ийн I үе шатын төгсгөлд олон улсын кибер аюулгүй байдлын байгууллагуудад гишүүнээр элссэн өсөлтийг хэмжихээр төлөвлөсөн байна.

Цахим хөгжил, инновац, харилцаа холбооны яам (ЦХИХХЯ) болон Тагнуулын ерөнхий газрын (ТЕГ) төлөөлөгчид кибер аюулгүй байдлын бодлогын талаарх олон улсын хэлэлцүүлэгт идэвхтэй оролцдог. Үүнд Нэгдсэн Үндэстний Байгууллагын (НҮБ) Кибер гэмт хэргийн конвенци, кибер аюулын заналын мэдээлэл (CTI) мэдээлэл солилцооны асуудлаарх НҮБ-ын хэлэлцүүлгүүд, Европын Аюулгүй Байдал, Хамтын Ажиллагааны Байгууллага (OSCE), мөн Кибер аюулгүй байдлын холбооны харилцан ахиц дэвшлийн сүлжээ (Cybersecurity Alliance Mutual Progress Network)[16] зэрэг олон улсын байгууллагуудын хуралдаанууд багтдаг. Түүнчлэн, Будапештийн конвенцид нэгдэхэд зориулсан тусгай хороо байгуулагдсан бөгөөд уг конвенцид нэгдэх бэлтгэл ажлууд хийгдэж байгаа талаар мэдээлсэн.

Тагнуулын Ерөнхий Газар (ТЕГ) нь НҮБ-ын Кибер гэмт хэргийн конвенцын хэлэлцүүлэгт оролцохдоо Цахим хөгжил, инновацын хамтын ажиллагааны яам (ЦХИХХЯ) болон Кибер Аюулгүй Байдлын Зөвлөлийн зөвлөлдөөнөөр дэмжлэг авсан болохыг мэдээлжээ. Олон улсын ийм төрлийн оролцоог үр дүнтэй дэмжихийн тулд кибер аюулгүй байдлын бодлоготой холбоотой олон улсын хэлэлцүүлгүүд Монгол Улсын ашиг сонирхол болон олон улсын байр сууринд хэрхэн нөлөөлж байгааг үнэлэх, хамтын ажиллагааны зорилтуудыг албан ёсны болгож тодорхойлох нь оновчтой байх болно.

Монгол Улсын зарим байгууллагууд олон улсын түвшний хамтын ажиллагааны байгууллагуудад идэвхтэй оролцож байна. Тухайлбал, цагдаагийн байгууллагын төлөөлөгчид G7 24/7 сүлжээнд нэгдэн кибер гэмт хэрэгтэй холбоотой мэдээлэл солилцдог болохыг мэдээлсэн. MNCERT/CC болон Үндэсний төв нь APCERT болон FIRST (Forum of Incident Response and Security Teams) -ийн гишүүн бөгөөд Нийтийн төв нь APCERT-д элсэх үйл явц явагдаж байгаа аж. Үндэсний төв нь харьцангуй шинэ байгууллага бөгөөд эдгээр олон улсын байгууллагад саяхан элссэн бол MNCERT/CC нь удаан хугацааны гишүүнчлэлтэй, тогтмол хуралдаанд оролцож, санал өгдөг, үйл ажиллагааны гишүүдийн сүлжээнд идэвхтэй ажилладаг болохыг мэдээлжээ. MNCERT/CC-ийн оролцоо өнөөг хүртэл сайн дурын үндсэн дээр явагдаж ирсэн бол, шинэ кибер, халдлага зөрчилтэй тэмцэх бүтэц бий болсноор эдгээр байгууллагуудын хооронд илүү зохицуулалттай хамтын ажиллагаа хөгжих хүлээлт үүсээд байна.

Монгол Улс бусад улс орнуудтай хоёр талт зарим гэрээ байгуулсан. Үүнд, ЦХИХХЯ болон Израилын Үндэсний Кибер Зохицуулалтын Газрын хооронд байгуулсан Харилцан ойлголцлын санамж бичиг (MOU) багтдаг бөгөөд энэхүү санамж бичиг нь кибер аюулгүй байдлын бодлого, зөрчил болон шилдэг туршлагуудын талаар мэдээлэл солилцох, мөн кибер аюулгүй байдлын чадавхыг хөгжүүлэх зорилготой. Мөн 2019 онд АНУ болон

[16] https://www.cybersec-alliance.org/camp/membership.do

Монгол Улсын хооронд байгуулсан хамтын ажиллагааны гэрээний хүрээнд MITRE байгууллагаас Зэвсэгт хүчний CSIRT хөгжүүлэхэд дэмжлэг үзүүлэх, ОЧМДБ байгууллагуудад сургалт зохион байгуулах, кибер аюулгүй байдлын чадавхыг бэхжүүлэх ажлыг хэрэгжүүлэх талаар мэдээлжээ.

Үүнээс гадна, Монгол Улсад кибер аюулгүй байдлын чадавхыг нэмэгдүүлэх чиглэлээр Японы Олон Улсын Хамтын Ажиллагааны Байгууллага, Нэгдсэн Үндэстний Байгууллагын Хөгжлийн Хөтөлбөр (UNDP), Дэлхийн Банк зэрэг олон улсын байгууллагууд чухал дэмжлэг үзүүлж байгаа талаар мэдээлэл өгсөн.

D 1.2 ЗӨРЧИЛД ХАРИУ ҮЗҮҮЛЭХ БОЛОН ОНЦГОЙ БАЙДЛЫН МЕНЕЖМЕНТ

Энэхүү хүчин зүйл нь үндэсний хэмжээнд зөрчлийг системтэйгээр тодорхойлох, онцлог шинжийг нь тогтоохтой хамаатай төрийн чадавхыг хөндөнө. Мөн засгийн газар нь кибер зөрчлийн хариу арга хэмжээг зохион байгуулах, уялдуулах, хэрэгжүүлэх чадамжтай эсэх, түүнчлэн кибер аюулгүй байдлыг үндэсний онцгой байдлын менежментийн тогтолцоонд нэгтгэсэн эсэхийг үнэлнэ.

Түвшин: **Хөгжиж буй түвшинд**

Монгол Улсын хэмжээнд Кибер халддлага, зөрчилтэй тэмцэх 4 төв эсхүл баг ажиллаж байгаа нь кибер аюулгүй байдлыг хангах, кибер халдлагаас урьдчилан сэргийлэх, хариу арга хэмжээ авахад чухал үүрэгтэй[17]. 2021 оны *Кибер Аюулгүй Байдлын тухай хуульд* Үндэсний төв, Нийтийн төв, Зэвсэгт хүчний харъяа төвийг байгуулах тухай заалтыг оруулсан. [18]

Үндэсний төв нь *төрийн онц чухал мэдээллийн дэд бүтэц болон төрийн мэдээллийн нэгдсэн сүлжээтэй холбогдсон байгууллагуудын мэдээллийн системийн аюулгүй байдлыг хангах, кибер халдлагаас урьдчилан сэргийлэх, илрүүлэх, таслан зогсоох, хариу арга хэмжээ авах, зөрчил үүссэн системийг сэргээхэд дэмжлэг үзүүлэх үүрэгтэй.* Өөрөөр хэлбэл засгийн газрын сүлжээ, системүүд болон төрийн өмчит ОЧМДБ байгууллагуудыг хамгаалахад чиглэгддэг.

Харин Нийтийн төв нь Үндэсний төвийн хамрах хүрээнээс гадуурх хувийн ОЧМДБ болон бусад байгууллага, иргэдэд кибер аюулгүй байдлын үйлчилгээ үзүүлэх үүрэгтэй. Ингэснээр улс орны хэмжээнд кибер аюулгүй байдлыг хангах, кибер халдлагаас урьдчилан сэргийлэх, хариу арга хэмжээ авах тогтолцоог бүрдүүлэхэд чухал ач холбогдолтой юм.

Түүнчлэн, Монгол Улсад 2014 онд байгуулагдсан удаан хугацааны туршид үйл ажиллагаа явуулж буй төрийн бус байгууллага MNCERT/CC мөн байна.

---

[17] https://legalinfo.mn/en/edtl/16531350476261

[18] https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf

Кибер аюулгүй байдлын тухай хуульд зааснаар Үндэсний төв нь улсын хэмжээнд кибер аюулгүй байдлын Зөрчлийн мэдээллийн санг бүрдүүлэх үүрэгтэй бөгөөд Үндэсний төвийн үйл ажиллагааны журам нь тодорхойлогдсон.[19] Уг журамд "*Кибер халдлага, зөрчлийн дэлгэрэнгүй мэдээллийг Кибер аюулгүй байдлын зөрчлийн мэдээллийн санд бүртгэж, тогтмол шинэчилнэ*" гэж заасан. Мөн зөрчлийн мэдээллийг бүртгэхэд тавигдах шаардлагад халдлагын огноо, байршил, эх сурвалж, шалтгаан, шинж тэмдэг болон нөлөөлөлд өртсөн системийн тухайн үеийн нөхцөл байдлын мэдээлэл багтсан.

Хуулийн (21-р зүйл)-д Үндэсний төвийн дараах холбогдох чиг үүргийг тодорхойлсон. Үүнд:

"Дүн шинжилгээ хийх, мэдээллийн санд хуримтлуулах, статистик мэдээлэл, судалгаа боловсруулах, зөвлөмж, кибер халдлага болон зөрчилтэй холбоотой мэдээлэл, зөвлөмжүүдийг улс орон даяар түгээх" болон "Улсын хэмжээнд бүртгэгдсэн кибер халдлага, зөрчлийн ангилал, боловсруулалт хийх, холбогдох байгууллагуудад дамжуулах зорилгоор холбогдох байгууллагын төлөөллөөс бүрдсэн баг ажиллуулна " гэж заасан.

Нийтийн төвийн журам[20] нь мөн тодорхойлогдсон бөгөөд судалгааны багт өгсөн мэдээллийн дагуу Нийтийн төв нь "Кибер халдлага, зөрчлийн мэдээллийн сан бүрдүүлэх" үүрэгтэй гэж заасан. Кибер аюулгүй байдлын тухай хуульд зааснаар Кибер халдлага, зөрчилтэй тэмцэх Нийтийн төв нь Үндэсний төвтэй мэдээлэл солилцох үүрэгтэй ("*энэ хуулийн 20.1.1-д заасан төвүүд болон 20.2-т заасан хуулийн этгээдүүдтэй хамтран ажиллаж, мэдээлэл солилцоно*").

Бодит байдал дээр эдгээр төвүүд нь харьцангуй шинэ тул зөрчлийн мэдээллийн сан бүрэн ажиллагаанд ороогүй. Одоогоор зөвхөн Үндэсний төвийн хариуцсан зөрчлүүдийг бүртгэж байгаа бөгөөд Нийтийн төвөөс Үндэсний төвд мэдээлэл дамжуулах механизм бүрэн туршигдаагүй байна. Энэ нь Кибер аюулгүй байдлын Зөрчлийн мэдээллийн санд улсын хэмжээнд бүрэн гүйцэд мэдээлэл бүртгэхэд чухал үүрэгтэй байх юм. Үүнийг бүрэн хэрэгжүүлснээр улс орны хэмжээнд учирч болзошгүй аюул заналыг бүрэн ойлгох, үндэсний кибер аюулгүй байдлын эрсдэлийн бүрэн үнэлгээг хийх боломж бүрдэх юм.

Зарим байгууллагууд зөрчлийг тодорхойлох, ангилах, Үндэсний болон Нийтийн төвд тайлагнах дотоод процесстой. Гэхдээ энэ чадамж нь байгууллагын төлөвшлийн түвшнээс хамаарах бөгөөд санхүү, харилцаа холбооны салбарын томоохон байгууллагууд илүү өндөр чадамжтай. Хэлэлцүүлэгт оролцогчид төрийн байгууллагууд зөрчил илрүүлэх, удирдах тал дээр хүндрэлтэй байгааг мэдээлсэн. Олон байгууллага зөрчлийг өөрсдөө илрүүлэх чадамжгүй, хариу арга хэмжээ авах, эмзэг байдлыг арилгах боломжгүй байгаа нь зарим төрийн байгууллагуудад зөрчил дахин давтагдах шалтгаан болж байна.

Кибер аюулгүй байдлын тухай хуульд бүх ОЧМДБ байгууллагууд зөрчил илрүүлэх системтэй байх, зөрчлийг Үндэсний төв эсхүл Нийтийн төвд мэдээлэх шаардлагатай гэж заасан бөгөөд дараах шаардлагууд тусгагдсан. Үүнд:

---

[19] Annex 2 of Government Resolution No. 318 dated August 30, 2023 OPERATING PROCEDURES OF THE NATIONAL CENTER FOR FIGHTING CYBER ATTACKS AND VIOLATIONS

[20] Government No. 08 of 2023 Appendix 1 of Resolution No. 319 dated March 30 "PUBLIC CENTER FOR FIGHTING CYBER ATTACKS AND VIOLATIONS" STATE BUDGET INDUSTRY DEPARTMENT RULES

- Кибер халдлага, зөрчлийг илрүүлэх, бүртгэх, таслан зогсоох мэдээллийн системтэй байх
- Кибер халдлага, зөрчлөөс үүдэн мэдээллийн систем, дэд бүтцийн тасралтгүй ажиллагаанд саатал үүссэн тохиолдолд холбогдох төвд нэн даруй мэдээлэх
- Төлөвлөгөөт шалгалт, аудит, сүлжээ, системийн тасалдал, онцгой нөхцөл байдлын улмаас дэд бүтцийн тасралтгүй ажиллагаанд саатал үүссэн тохиолдолд холбогдох төвд нэн даруй мэдээлэх.

D1.3-т дэлгэрэнгүй тайлбарласнаар хууль хэрэгжүүлэх эхний шатанд байгаа тул бүх ОЧМДБ байгууллагууд эдгээр шаардлагыг бүрэн хангаагүй байна.

Үндэсний төв болон Нийтийн төв нь харьцангуй шинэ байгууллагууд тул тэдгээрийн бүрэн чадамж хараахан туршигдаагүй байна. Одоогоор эдгээр байгууллагууд улс орны хэмжээнд тохиолдох кибер зөрчлийн бүх хувилбарт бүрэн хариу арга хэмжээ авахад шаардагдах нөөц, ур чадвар, процессуудыг бүрэн хангаж чадаж байгаа эсэхийг үнэлэх шаардлагатай хэвээр байна. Хувийн хэвшлийн зарим оролцогчид эдгээр төрийн байгууллагууд шаардлагатай бүх зөрчлүүдэд бүрэн хариу арга хэмжээ авахад хангалттай хүчин чадалтай биш байх магадлалтай гэж үзсэн. Ялангуяа технологийн хөгжлийн хурдтай холбоотойгоор хувийн хэвшлийн байгууллагатай хамтын ажиллагааг сайжруулж, тэдний техникийн хүчин чадлыг ашиглах нь ашигтай байж болох юм гэсэн байр суурь илэрхийлсэн.

Нийтийн төв нь чадамж, хүний нөөцөө хөгжүүлэх шатанд байгаа бөгөөд MNCERT/CC-ээс зөвлөх үйлчилгээний хүрээнд чадамж хөгжүүлэх ажлыг эхлүүлсэн. Нийтийн төв нь өөрийн харьяа байгууллагуудын (хувийн ОЧМДББ орно) сүлжээг хянадаггүй, харин "иргэд, хуулийн этгээд, хувийн хэвшлийн байгууллагуудын мэдээллийн систем болон мэдээллийн сүлжээний аюулгүй байдлын талаар зөвлөмж гаргадаг" гэж журамдаа заасан. Зарим хувийн ОЧМДБ байгууллагуудын төлөөлөгчид кибер аюулгүй байдлын зөрчил гарсан тохиолдолд эхлээд *Кибер аюулгүй байдлын тухай хуулийн* дагуу Нийтийн төв-д[21] хандана гэж тэмдэглэсэн боловч техник туслалцаа авах зорилгоор MNCERT/CC-д мөн ханддаг гэж мэдээлсэн.

MNCERT/CC нь Монгол Улсын байгууллагуудын (санхүүгийн бүх салбар, төрийн болон хувийн хэвшил) кибер аюулгүй байдлыг дэмжихэд чухал үүрэг гүйцэтгэдэг. MNCERT/CC нь 2014 оноос хойш үйл ажиллагаа явуулж буй төрийн бус байгууллага бөгөөд хувийн хэвшлийн гишүүн байгууллагууд, үүнд банк, үүрэн телефоны оператор, томоохон интернэт үйлчилгээ үзүүлэгчид (ISP) багтдаг. Байгууллага нь бүтэн цагийн ажилтнууд болон сайн дурынхны оролцоотойгоор үйл ажиллагаа явуулдаг. Гол үйлчилгээ нь аюул заналын мэдээлэл түгээх, гишүүддээ зориулсан сургалт, кибер дадлага хийх, халдлагын хариу арга хэмжээний тест зохион байгуулах зэрэг үйл ажиллагааг хамардаг. Түүнчлэн жил бүр кибер аюулгүй байдлын хурал, олон нийтийн мэдлэг нэмэгдүүлэх компанит ажил, мөн кибер аюулгүй байдлын тэмцээн (Capture-the-Flag -CTF) уралдаанууд зохион байгуулдаг. Түүнчлэн MNCERT/CC нь тогтвортой үйл ажиллагаа явуулж буй, туршлагатай, өндөр чадвартай кибер аюулгүй байдлын мэргэжилтнүүдээс бүрдсэн байгууллага гэж үнэлэгддэг. Тус байгууллага нь олон улсын эх сурвалжууд болон нийлүүлэгчдээс аюул заналын мэдээлэл цуглуулан, дүн шинжилгээ

[21] https://mncert.org/#/en

хийн холбогдох мэдээллийг гишүүддээ MISP[22] (Malware Information Sharing Platform) буюу мэдээлэл түгээх платформ дээр суурилсан шийдэл ашиглан түгээдэг.

Мөн MNCERT/CC нь Нийтийн төвд зөвлөх үйлчилгээ үзүүлж, Монгол Улсын аюул заналын нөхцөл байдлын талаар тайлан гаргахад тусалсан. Тус байгууллагын төлөөлөгчид гишүүддээ зориулсан мэдлэг хуваалцах платформ хөгжүүлэхээр төлөвлөж байгаа бөгөөд үүнийг Үндэсний болон Нийтийн төвүүдтэй уялдуулах нь үр ашигтай гэж үзэж байна.

Хууль батлагдахаас өмнө шаардлагатай талуудад мэдээлэл хүргэх нь албан бус сувгуудаар хийгдэж байсан. Гэвч шинэ бүтцийн дагуу бүх мэдээлэл нь шаардлагатай ОЧМДБ байгууллага болон төвүүдэд хүрч байгаа эсэх нь тодорхой бус хэвээр байгааг зарим оролцогчид илэрхийлсэн.

Үндэсний Дата Төв (ҮДТ) нь мөн зөрчилд хариу арга хэмжээ авах үйл явцад оролцдог. Олон төрийн байгууллагуудын системийг байршуулдаг тул *Кибер аюулгүй байдлын тухай хууль* батлагдахаас өмнө ч зөрчил илрүүлэх, хариу арга хэмжээ авах үйл ажиллагаанд дэмжлэг үзүүлж байсан бөгөөд хууль хэрэгжиж эхэлснээс хойш энэ үүргээ үргэлжлүүлэн гүйцэтгэсээр байна. ҮДТ нь мөн Үндэсний төвийн бүх шаардлагатай зөрчилд хариу арга хэмжээ авах чадамжгүй байгаа асуудалд туслах үүрэг гүйцэтгэж байна.

ҮДТ-ийн төлөөлөгчдийн хэлсэнээр шинэ хууль болон төвүүд байгуулагдаад удаагүй байгаа тул мэдээллийн системээ тэдэнд байршуулсан зарим байгууллагууд одоог хүртэл ҮДТ-өөс аюулгүй байдлын тусламж авах тал дээр хамааралтай хэвээр байгааг онцлов. Энэ байдал нь ҮДТ-ийн нөөцийг анх төлөвлөсөн үүрэг хариуцлагаас нь хэтрүүлэн ажиллахад хүргээд байна. Түүнчлэн ҮДТ нь зорилтот халдлага (APT) зөрчилд хариу арга хэмжээ авах, хортой программ хангамжийн шинжилгээ хийх, мэдээлэл бий болгох, хуваалцах зэрэг дэвшилтэт боломжуудтай гэж мэдээлсэн.

Үндэсний болон Нийтийн төвүүд нь бүх хариуцсан байгууллагуудын хэрэгцээг бүрэн хангах нөөц, ур чадварын хязгаарлагдмал байдалд орж болзошгүй. Иймд төвүүдийн нэгдсэн нөөцийг илүү үр дүнтэй ашиглах, MNCERT/CC, ҮДТ болон хувийн хэвшлийн бусад оролцогч талуудыг илүү үр ашигтайгаар татан оролцуулах шаардлагатай эсэхийг тодорхойлох нь чухал байна. Одоогоор зөвлөх гэрээ гэх мэт албан бус байдлаар хэрэгжиж буй эдгээр харилцаануудыг албан ёсны болгосноор тогтвортой байдлыг нэмэгдүүлэх боломжтой.

Кибер халдлага, зөрчилтэй тэмцэх төвүүдийн уялдаа холбоотой ажиллах асуудал Кибер аюулгүй байдлын зөвлөлийн хэлэлцэх сэдвийн нэг болж байгаа талаар мэдээлсэн. Зарим оролцогчид Үндэсний төв нь өөрийн үүргийг үр дүнтэй гүйцэтгэхийн тулд, ялангуяа Тагнуулын байгууллагатай харилцан хамааралтай байдлыг харгалзан үзвэл, олон нийтийн итгэлийг нэмэгдүүлэх шаардлагатай гэсэн байр суурийг илэрхийлсэн.

Үндэсний хэмжээний зөрчилтэй тэмцэх байгууллагууд болон бусад төрийн болон хувийн хэвшлийн байгууллагууд нь аюул занал, эмзэг байдлын мэдээллийг хоорондоо тодорхой хэмжээнд хуваалцдаг. КАБҮС "*төр, хувийн хэвшлийн байгууллагууд кибер халдлага, зөрчлийн талаарх мэдээллийг харилцан солилцох эрх зүйн орчныг бүрдүүлэх*" гэсэн үйл ажиллагаа тусгагдсан. Зарим онц чухал мэдээллийн дэд бүтэцтэй төрийн

[22] https://misp.alert.mn/users/login

байгууллагууд Үндэсний Кибер халдлага, зөрчилтэй тэмцэх төвөөс аюул заналын талаарх мэдээлэл авч байсан талаар мэдээлсэн. Мөн төрийн байгууллагуудын хооронд аюул, заналын мэдээлэл (CTI) солилцох платформыг Үндэсний төв хөгжүүлж байгаа боловч хараахан дуусаагүй байна.

Түүнчлэн, MNCERT/CC гишүүддээ зориулан сар бүрийн уулзалт болон жил бүрийн чуулган зохион байгуулдаг бөгөөд энэ нь аюул заналын мэдээлэл солилцох, сайн туршлагыг хуваалцах боломжийг бүрдүүлж байна.

Мэдээлэл солилцоо тодорхой хэмжээнд явагдаж байгаа хэдий ч шаардлагатай бүх талуудад найдвартай хүрэхгүй байх тохиолдол гарч байгааг онцолсон. Үүний үр дүнд зарим зөрчлүүд дахин давтагдах нөхцөл байдал үүсэж байна. Мөн холбогдох байгууллагуудад зөрчил эсхүл эмзэг байдлын талаарх мэдээлэл хүргэх үйл явцтай холбоотой асуудлууд байгааг дурдсан. Оролцогчдын хэлснээр, одоогоор *Кибер аюулгүй байдлын тухай хуулийн* дагуу энэ мэдээлэл нь нууц гэж ангилагдах бөгөөд Монгол Улсын мэдээллийн ангиллын тухай хуульд зааснаар хэвлэмэл байдлаар илгээж, байгууллагын албан ёсны хүлээн авагч л үзэх эрхтэй байдаг. Энэ нь байгууллагуудад чухал мэдээлэл хүлээн авах хурдыг удаашруулж, мэдээллийг зөвхөн нэг хүнд хязгаарласнаар асуудлыг хурдан шийдвэрлэх үйл явцад саад учруулж байна.

Кибер халдлага, зөрчилтэй тэмцэх төвүүдийн зарим оролцогчид зөрчилд хариу арга хэмжээ авах явцад төвүүдийн хооронд мөрдөх харилцаа холбооны протоколыг тодорхой заах шаардлагатайг онцолсон. Мөн төвүүд болон тэдний харьяа байгууллагуудын хооронд харилцааг сайжруулахын тулд "эмзэг мэдээлэл ангилах систем" (Traffic Light Protocol) болон PGP (Pretty Good Privacy) шифрлэлт ашиглах аргачлалыг боловсруулах зорилготой байгааг дурдсан.

Аюул занал болон эмзэг байдлын мэдээлэл шаардлагатай кибер халдлага, зөрчилд хариу үзүүлэх байгууллагууд, төрийн болон хувийн хэвшлийн байгууллагуудад цаг тухайд нь хүрч байх механизмыг бий болгох нь чухал юм. Энэ нь *Кибер аюулгүй байдлын үндэсний стратегийн* (КАБҮС) зорилт 5-тай нийцэж байгаа бөгөөд уг зорилтын хүрээнд “Кибер халдлага, зөрчилтэй тэмцэх төвүүдийн хамтын ажиллагааг идэвхжүүлж, мэдээлэл солилцооны технологийн шийдлүүдийг нэвтрүүлэх” үйл ажиллагааг хэрэгжүүлэхээр тусгасан байна.

Улсын хэмжээнд үйл ажиллагаа явуулж буй кибер халдлага, зөрчилтэй тэмцэх зарим байгууллагууд олон улсын кибер халдлага, зөрчилд хариу үзүүлэх сүлжээнд гишүүнээр элссэн бөгөөд энэ нь олон улсын түншүүдтэй аюул занал, эмзэг байдлын мэдээлэл болон үйл ажиллагааны сайн туршлагыг тогтмол хуваалцах боломжийг олгож байна. MNCERT/CC нь APCERT[23] болон FIRST[24] байгууллагуудын удаан хугацааны гишүүн бөгөөд “Shadowserver” зэрэг олон улсын аюул, заналын мэдээлэл хуваалцах группүүдтэй хамтран ажиллах гэрээтэй. Үндэсний төв нь 2023 онд FIRST болон APCERT-д элссэн бол Нийтийн төв нь мөн APCERT-д элсэх үйл явцыг хэрэгжүүлж байгаа тухай мэдээлэл өгсөн.

КАБҮС-ийн зорилт 5-ын хүрээнд "онцгой байдлын үед улсын хэмжээнд кибер орон зайг хамгаалах чадавхыг хөгжүүлэх" гэсэн үйл ажиллагаа тусгагдсан. *Үндэсний хэмжээний*

---

[23] https://www.apcert.org/about/structure/members.html

[24] https://www.first.org/members/teams/mncert-cc

кибер халдлага, зөрчилд хариу үзүүлэх төлөвлөгөө 2024 оны 9 сард батлагдсан бөгөөд ТЕГ тэргүүлэн боловсруулж, ЦХИХХЯ-тай зөвлөлдсөн. Төлөвлөгөөний агуулга нууцлалтай тул судалгааны багт өгөгдөөгүй.

Оролцогчдын мэдээлснээр, үндэсний хэмжээний онцгой байдал үүсэж, кибер халдлагатай холбоотой нөхцөл байдал үүссэн тохиолдолд хариу арга хэмжээг удирдан зохион байгуулах ажлын хэсгийг байгуулах үүрэг Үндэсний Кибер Аюулгүй Байдлын Зөвлөлд оногддог. Төлөвлөгөөнд зааснаар, зөрчлийг удирдан зохицуулах үндсэн хариуцлага нь халдлагад өртсөн байгууллагын харьяа төвүүд байх бөгөөд бусад төвүүд дэмжлэг үзүүлэх үүрэгтэй. Мөн хүний нөөцийн хомсдол үүссэн тохиолдолд олон улсын түншүүдээс нэмэлт техникийн туслалцаа авах боломжтойг тусгасан. Түүнчлэн, уг төлөвлөгөө нь тогтмол дадлага хийх шаардлагатай гэсэн заалтуудыг агуулсан байна.

Энэхүү төлөвлөгөө нь одоогоор үндэсний хэмжээний онцгой байдлын менежментийн өргөн хүрээний тогтолцоонд нэгтгэгдээгүй бөгөөд тусдаа мэдээллийн технологийн асуудал мэтээр хандаж байгааг мэдээлсэн. Түүнчлэн, уг төлөвлөгөө саяхан эцэслэгдсэн тул хараахан практикт туршигдаагүй, хэрэгжүүлэлтэд ашиглагдаагүй байна. Гэсэн хэдий ч төлөвлөгөөг боловсруулах явцад түүний үйл явцыг сайжруулах зорилгоор хэд хэдэн сургуулилтуудыг явуулсан гэж тэмдэглэсэн.

Мөн өмнө нь Үндэсний болон Нийтийн төв, MNCERT/CC болон бусад байгууллагууд хамтарсан сургуулилтууд зохион байгуулж байсан. MNCERT/CC нь Нийтийн төвийн харьяа байгууллагууд, хувийн хэвшлийн онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын дунд кибер сургуулилтууд зохион байгуулсан бөгөөд эдгээрийг Нийтийн төвтэй хийсэн зөвлөх үйлчилгээний гэрээний хүрээнд хэрэгжүүлжээ. Уг сургуулилтаар оролцогч байгууллагууд кибер зөрчилд хариу арга хэмжээ авах сорилттой тулгарч, Нийтийн төв нь мэдээллийг хэрхэн зохицуулж байгааг (нэг ОЧМДБ байгууллагаас ирсэн мэдээллийг шаардлагатай бусад байгууллагуудад дамжуулах чадамж) шалгаж туршсан байна.

MNCERT/CC нь мөн Үндэсний Дата Төв (ҮДТ) болон Цагдаагийн байгууллагуудыг хамруулсан кибер сургуулилтууд зохион байгуулж байсан талаар мэдээлсэн.

Төлөвлөгөөнд төвүүдийн хооронд тогтмол кибер дасгал сургуулилт хийх ёстой гэж заасан байдаг. Өмнө нь тал бүрийн байгууллагуудтай хамтарсан дасгал сургуулилт хийгдэж байсан ч шинэчлэгдэн батлагдсан үндэсний онцгой байдлын менежментийн төлөвлөгөөний дагуу бүх холбогдох талуудыг хамруулсан дадлага сургууль явуулах нь чухал юм.

Үүнд зөвхөн кибер аюулгүй байдлын байгууллагуудаас гадна онцгой байдлын үед оролцох боломжтой ОЧМДБ байгууллагууд зэрэг бусад байгууллагуудыг багтаах ёстой. Ингэснээр тэдний хамаарал болон төлөвлөгөөт арга хэмжээнүүдийг бүрэн ойлгох боломжтой болно. Энэхүү дасгал сургуулилт нь улс орны хэмжээнд үүсэж болзошгүй онцгой байдлын нөхцөл байдлуудыг шийдвэрлэхэд шаардлагатай үйл явц, харилцаа холбоо бүрдүүлэх болон хариуцагч байгууллагуудын чадамж хангалттай эсэхийг баталгаажуулахад туслах юм.

Оролцогчид онцгой байдлын үед шаардлагатай хамтын ажиллагааг дэмжих нөөцүүд нэмэгдэж байгаа боловч одоогоор хангалттай түвшинд хүрээгүй байж болзошгүй гэсэн санаа зовнилыг илэрхийлсэн.

D 1.3 ОНЦ ЧУХАЛ БҮТЦИЙН ХАМГААЛАЛТ

Энэхүү хүчин зүйл нь төрийн онц чухал мэдээллийн дэд бүтцийн хөрөнгийг тодорхойлох чадавх, ОЧМДБ-ийн кибер аюулгүй байдлын талаархи зохицуулалтын шаардлагууд, ОЧМДБ байгууллагуудын кибер аюулгүй байдлын сайн туршлагын хэрэгжилтийг судалдаг.

Түвшин: **Хөгжиж буй түвшнээс Тогтворжсон түвшинд**

2021 онд баталсан Кибер аюулгүй байдлын тухай хуулиар ОЧМДБ салбаруудын жагсаалтыг тодорхойлсон. Үүнд:

- *Цахилгаан үйлдвэрлэх, түгээх, дамжуулах болон хяналтын системтэй байгууллагууд*
- *Цэвэр ус ба бохир ус, халаалтын эх үүсвэр, төвлөрсөн сүлжээ болон түгээх, хяналтын системтэй байгууллагууд*
- *Эрүүл мэндийн хоёрдугаар болон гуравдугаар түвшний байгууллагууд*
- *Хүний болон мал амьтны халдварт өвчний судалгааны лабораториуд*
- *Эмийн болон хорт бодис үйлдвэрлэдэг байгууллагууд*
- *Төлбөр, тооцоо, гүйлгээний нэгдсэн цахим системтэй банкнууд болон санхүүгийн байгууллагууд*
- *Харилцаа холбоо болон мэдээллийн технологийн салбарын давамгай эрхтэй монополын үйл ажиллагаа явуулж, зах зээлд давамгайлсан байр суурь эзэлдэг байгууллагууд*
- *Агаар, төмөр зам, усан зам, авто замын тээвэрлэлтийн хяналтын системтэй байгууллагууд*
- *Түлш импортлогч, үйлдвэрлэгч, түгээдэг байгууллагууд*
- *Стратегийн хүнсний бүтээгдэхүүн үйлдвэрлэх, хадгалах, түгээх байгууллагууд*
- *Мэдээлэл болон үйл ажиллагааг удирдах төвүүд*
- *Улсын радио, телевизийн байгууллагууд*
- *Үндсэн болон дэмжлэг мэдээллийн систем, мэдээллийн сангийн үндсэн мэдээлэл хариуцдаг байгууллагууд*
- *Өгөгдлийн төвүүд, тэдгээрийн салбарууд, нөөц төвүүдийн үйл ажиллагааг хариуцдаг байгууллагууд*
- *Хил хязгаарын портын хяналт, удирдлагын системийг хариуцдаг байгууллагууд*
- *Стратегийн ач холбогдол бүхий эрдэс баялаг олборлодог байгууллагууд*
- *Үндэсний хилээр зорчигч болон тээврийн хэрэгслийн бүртгэл, хяналтын мэдээллийн системүүдийг хариуцдаг байгууллагууд*

Эдгээр салбарын байгууллагууд дотор, тусгайлан заагдсан ОЧМДБ байгууллагуудыг тодорхойлж, 2022 онд “Чухал мэдээллийн дэд бүтцийн байгууллагуудын жагсаалт”-ыг Монгол Улсын Засгийн газар баталсан. 2022 онд Кибер аюулгүй байдлын тухай хуульд заасны дагуу 216 төрийн болон хувийн ОЧМДБ байгууллагууд тус жагсаалтад орсон.[25] ОЧМДБ-ийн тодорхойлолт болон холбогдох байгууллагуудыг тодорхойлох ажлыг удирдах ажлын хэсэг байгуулагдаж, холбогдох салбарын яамдтай зөвлөлдөж, тухайн салбартаа стратегийн чухал байр суурь эзлэх байгууллагуудыг тодорхойлох ажил хийгдсэн. Жишээлбэл, Хүнс, хөдөө аж ахуйн яам нь Монголын хүнс, хөдөө аж ахуйн

[25] https://legalinfo.mn/mn/detail?lawId=16530379619711&showType=1

үйлдвэрлэлд стратегийн ач холбогдолтой компаниудыг тодорхойлоход зөвлөгөө өгсөн гэж мэдээлсэн.

Төлөвшлийн үнэлгээний хэлэлцүүлэгт оролцсон онц чухал мэдээллийн дэд бүтэцтэй байгууллагууд өөрсдийн статус болон хамаарах шаардлагуудын талаар мэдлэгтэй байсан. Зарим парламентын харьяанд ажилладаг байгууллагууд (тухайлбал, Сонгуулийн Ерөнхий Хороо) одоогоор уг жагсаалтад ороогүй байгааг тэмдэглэж, үүнийг нэмэх хүсэлтийг Цахим хөгжил, инновац, харилцаа холбооны яам (ЦХИХХЯ)-д хүргүүлсэн талаар мэдээлсэн.

ОЧМДБ байгууллагуудын жагсаалтыг тогтмол шинэчилж байх нь чухал бөгөөд энэ нь улс орны нөхцөл байдал, технологийн болон геополитикийн орчны өөрчлөлтөд нийцүүлэн өөрчлөгдөх шаардлагатай. Түүнчлэн ОЧМДБ салбар болон байгууллагуудын хоорондын хамаарал, мөн бусад орнуудын дэд бүтцээс хамааралтай байдлыг тодорхойлох нь чухал бөгөөд ингэснээр энэ хамаарлыг зохицуулах боломжтой болно. ОЧМДБ байгууллагууд нь кибер халдлагаас урьдчилан сэргийлэх, арга хэмжээ авах төлөвлөгөө боловсруулах, мэдээллийн аюулгүй байдлыг хангах стандартуудыг нэвтрүүлэх, кибер аюулгүй байдлыг хариуцсан ажилтантай байх, жил бүр кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийлгэх, хоёр жил тутамд мэдээллийн аюулгүй байдлын аудит хийлгэх, болон зөрчил мэдээлэх зэрэг кибер аюулгүй байдлын хүрээнд биелүүлэх үүрэг хүлээсэн байна. Тодруулбал, *Кибер аюулгүй байдлын тухай хууль* (19-р зүйлийн дагуу) нь ОЧМДБ байгууллагуудад дараах үүрэг хариуцлагыг ногдуулсан. Үүнд:

- *Кибер аюулгүй байдлыг хангах дотоод журам батлах*
- *Кибер халдлага, зөрчил гарсан тохиолдолд арга хэмжээ авах төлөвлөгөө боловсруулах, хэрэгжүүлэх*
- *Мэдээллийн аюулгүй байдлыг хангах стандарт нэвтрүүлэх*
- *Кибер аюулгүй байдлыг хангах ажилтантай байх*
- *Жил бүр кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийлгэх, мэдээллийн систем болон сүлжээний өөрчлөлтөд зөвшөөрөгдсөн байгууллагын шаардлагын дагуу үнэлгээ хийлгэх*
- *Хоёр жил тутамд мэдээллийн аюулгүй байдлын аудит хийлгэх*
- *Мэдээллийн систем болон мэдээллийн сүлжээний аюулгүй байдлыг хангах удирдлагын арга хэмжээ, зохион байгуулалт, техникийн арга хэмжээг төлөвлөх, хэрэгжүүлэх*
- *Кибер халдлага, зөрчлийг илрүүлэх, бүртгэх, таслан зогсоох мэдээллийн системтэй байх*
- *Мэдээллийн системийн үйл ажиллагааны бүртгэлийг кибер аюулгүй байдлыг хангах журмын дагуу хадгалах*
- *Кибер аюулгүй байдлын эрсдэлийн үнэлгээ болон мэдээллийн аюулгүй байдлын аудитын тайланг холбогдох төвд нэг сарын дотор ирүүлж байх*
- *Холбогдох байгууллагын шаардлагыг биелүүлж, зөрчил илэрсэн тохиолдолд шаардлагатай арга хэмжээ авах*
- *Гадаадын иргэд болон гадаадын хууль ёсны этгээдүүдийн кибер аюулгүй байдлын эрсдэлийн үнэлгээ хийх тохиолдолд Тагнуулын ерөнхий газарт зөвшилцөх*
- *Мэдээллийн систем болон дэд бүтцийн хэвийн тасралтгүй ажиллагааг хангах, мөн гэмтэл, тасалдал үүссэн тохиолдолд сэргээх үйл ажиллагааны төлөвлөгөөг хэрэгжүүлэх*
- *Кибер халдлага болон зөрчлийн улмаас мэдээллийн систем болон дэд бүтцийн хэвийн тасралтгүй ажиллагаа алдагдсан тохиолдолд холбогдох төвд яаралтай мэдэгдэл хийх*

- *Төлөвлөгөөт шалгалт, аудит, гэмтэл болон сүлжээ, системийн гадаад хүчин зүйлүүдээс болж дэд бүтцийн хэвийн тасралтгүй ажиллагаа алдагдсан тохиолдолд холбогдох төвд яаралтай мэдэгдэл хийх зэрэг багтсан болно.*

Хуулийн дагуу ОЧМДБ байгууллагууд кибер аюулгүй байдлыг хангах стандартуудыг нэвтрүүлэх үүрэгтэй. ЦХИХХЯ нь хуулийг баталсны дараа олон нийтийн болон хувийн хэвшлийн байгууллагуудыг оролцуулсан нээлттэй хэлэлцүүлэг зохион байгуулсан бөгөөд эдгээр байгууллагууд кибер аюулгүй байдлын ямар стандартуудыг дагаж мөрдөх ёстой гэдгийг тодорхойлохоор оролдсон боловч зөвшилцөлд хүрч чадаагүй тул тодорхой нэг стандартыг заавал мөрдүүлэх нь боломжгүй гэж үзжээ. 2023 онд батлагдсан "*Кибер аюулгүй байдлын нийтлэг журам*" нь *Кибер аюулгүй байдлын тухай хуулийн* дагуу хэрэгжүүлж буй бодлого бөгөөд эдгээр байгууллагууд дагаж мөрдөх дотоод журмуудын дэлгэрэнгүй мэдээллийг өгдөг. ОЧМДБ байгууллагууд нь олон улсад хүлээн зөвшөөрөгдсөн кибер аюулгүй байдлын стандартуудыг болон "*Нийтлэг журам*" дагаж мөрдөх үүрэгтэй.

ЦХИХХЯ нь "*Нийтлэг журмыг*" ISO27001 болон NIST800 олон улсын стандартуудтай нийцүүлэн боловсруулсан бөгөөд суурь шаардлагыг бий болгоход оршино. Уг журмыг боловсруулах ажлын хүрээнд мөн ЦХИХХЯ нь 2021, 2022 онд засгийн газар, орон нутгийн болон ОЧМДБ байгууллагуудыг хамруулсан судалгаа явуулсан бөгөөд үүний үр дүнд нийтлэг асуудлуудыг тодорхойлсон. *Нийтлэг журмын* дагуу дагаж мөрдөх бусад стандартуудыг ч мөн тодорхойлсон бөгөөд үүнд эрсдэлийн үнэлгээ хийхэд зориулсан ISO 27005 зэрэг стандартуудыг агуулж байна.

Үүнээс гадна, кибер аюулгүй байдлыг хангах дотоод журмуудыг төрийн байгууллагууд ("*төрийн өмчит хуулийн этгээдүүд*"), мэдээллийн технологийн үйлчилгээ үзүүлэгчид ("*мэдээллийн технологийн үйлчилгээ үзүүлж, өгөгдөл боловсруулах, хадгалах, түгээх, компьютерийн аналитик хийх, цахим орчинд мэдээллийн системүүдийн хэвийн үйл ажиллагааг хангах үүрэгтэй хуулийн этгээдүүд*") болон онц чухал мэдээллийн дэд бүтэцтэй байгууллагууд заавал мөрдөх шаардлагатай. Иймд *Кибер аюулгүй байдлын нийтлэг журам* нь төрийн байгууллагууд болон мэдээллийн технологийн үйлчилгээ үзүүлэгчдийн дагаж мөрдөх кибер аюулгүй байдлын дотоод журмуудыг тодорхойлох үндсэн баримт бичиг болж үйлчилдэг.

ОЧМДБ байгууллагууд *Кибер аюулгүй байдлын тухай хуулийн* шаардлагыг хэрхэн хангаж байгааг үнэлэх албан ёсны үйл явцыг тодорхойлсон. Уг хуульд зааснаар, аудит болон эрсдэлийн үнэлгээг ЦХИХХЯ-д бүртгэгдсэн үйлчилгээ үзүүлэгч байгууллагууд хийж гүйцэтгэх ёстой. "*Мэдээллийн аюулгүй байдлын аудитын бүртгэл, аудитын журам*"[26] нийтлэгдсэн бөгөөд энэ нь аудит хийх үйлчилгээ үзүүлэгчид хэрхэн бүртгүүлэх, мөн аудитын тайлангийн хамрах хүрээний талаар тодорхой заасан. Уг журмаар үйлчилгээ үзүүлэгчид мэргэжлийн холбоо эсхүл стандартын байгууллагаар баталгаажсан гэрчилгээ бүхий бүтэн цагаар ажилладаг мэргэжилтэнтэй байх шаардлагатайг тогтоосон. Аудитын тайланг төрийн өмчит ОЧМДБ байгууллагуудын хувьд Тагнуулын ерөнхий газарт (ТЕГ), хувийн хэвшлийн ОЧМДБ байгууллагуудын хувьд ЦХИХХЯ-нд хүргүүлэх бөгөөд эдгээр байгууллагууд хууль, журмын хэрэгжилтийг хянах үүрэгтэй. ЦХИХХЯ уг зорилгоор хяналт, мониторингийн хэлтсийг

[26] https://legalinfo.mn/mn/detail?lawId=16760195603671&showType=1

саяхан байгуулсан талаар мэдээлсэн. Хууль зөрчсөн тохиолдолд төрийн албан хаагчдад хамаарах хууль тогтоомжийн дагуу хариуцлага ногдуулах бөгөөд үүнд торгууль зэрэг арга хэмжээ багтахыг заасан байна.

Оролцогчдын зүгээс *Кибер аюулгүй байдлын тухай хуулийн* хэрэгжилт бүрэн хангагдаагүй байгааг онцолсон. Учир нь дотоод бодлого болон аудиттай холбоотой дагалдах журам саяхан эцэслэгдсэн бөгөөд эрсдэлийн үнэлгээний дагалдах журам хараахан нийтлэгдээгүй байна. Аудит хийх тусгай зөвшөөрөл олгох үйл явц 2023 онд эхэлсэн бөгөөд Цахим хөгжил, инновац, харилцаа холбооны яам (ЦХИХХЯ) эхний аудитын компаниудыг саяхан албан ёсоор бүртгэж, аудитын үйл ажиллагаа эхлээд байна. Хуулийн хэрэгжилтийг хангах албадан шаардлагыг 2025 оноос эхлүүлэхээр төлөвлөсөн бөгөөд аудитын эхний хугацааг 2025 оны 8-р сард дуусгахаар заасан байна. ЦХИХХЯ хуулийн хэрэгжилт болон *Кибер аюулгүй байдлын нийтлэг журмын* талаар сургалт, мэдлэг олгох үйл ажиллагаа явуулж байгаа бөгөөд одоогоор 600 гаруй төрийн байгууллагын ажилтнуудад хүрч ажилласан гэж мэдээлсэн. ОЧМДБ байгууллагуудын зарим төлөөлөгчид ЦХИХХЯ-наас дотоод журам боловсруулах талаар өгсөн дэмжлэг нь үр дүнтэй байсан гэж тэмдэглэсэн. Зарим ОЧМДБ байгууллагууд хуулийн шаардлагыг хэрэгжүүлэх ажлыг эхлүүлсэн талаар мэдээлсэн бөгөөд үүнд байгууллагын удирдлагаасаа мэдээллийн аюулгүй байдлын тусдаа алба эсхүл хариуцсан албан тушаал бий болгох зөвшөөрөл авах, дотоод журмыг боловсруулах ажлууд багтаж байна.

Кибер аюулгүй байдлын сайн туршлагын практик хэрэгжилт нь ОЧМДБ байгууллагуудад ижил түвшинд биш байгаа бөгөөд сайжруулалт, нэвтрүүлэлтийг хэмжих үзүүлэлтийг КАБҮС -ийн хүрээнд тодорхойлсон байна. Зарим хөгжингүй салбарт кибер аюулгүй байдлын стандартуудыг нэвтрүүлж, аюул занал, эмзэг байдлын мэдээлэл болон сайн туршлагуудыг байгууллагууд хоорондоо хуваалцаж байна.
ОЧМДБ байгууллагууд болон кибер аюулгүй байдлын үйлчилгээ үзүүлэгчдийн зарим төлөөлөгчид нь санхүүгийн салбар нь кибер аюулгүй байдлын практик хэрэгжилтийн хувьд хамгийн өндөр түвшинд төлөвшсөн гэж үзэж байна. Энэ дүгнэлтийг өмнө нь MNCERT/CC-ийн зохион байгуулсан кибер сургуулилтуудын үр дүн мөн бататгаж байна. Эдгээр сургуулилтад ОЧМДБ байгууллагууд хамрагдсан бөгөөд санхүү, харилцаа холбооны салбарууд хамгийн өндөр түвшний кибер аюулгүй байдлын төлөвшилтэй болох нь тогтоогдсон (D1.2.3-г үзнэ үү). Гэвч бусад олон ОЧМДБ байгууллагуудын хувьд кибер халдлагаас урьдчилан сэргийлэх, зөрчлийг удирдахад шаардлагатай тоног төхөөрөмж, мэргэжлийн ур чадвар дутагдаж байгаа талаар мэдээлсэн. Мөн санхүүгийн салбарын байгууллагууд нь "*Банкны мэдээллийн технологийн шалгуур журам*"[27] дагуу кибер аюулгүй байдлын талаар Төв банкнаас баталсан зохицуулалттай байдаг гэж мэдээлсэн. Нэмэлтээр уг салбарын оролцогчид ISO 27001 стандартын шаардлагыг банканд лиценз авахад хэрэгжүүлэх ёстой бөгөөд тэдгээрийн үйл ажиллагааны төрлөөс хамааран *Төлбөрийн картын салбарын мэдээллийн аюулгүй байдлын стандарт* (PCI DSS) зэрэг шаардлагуудыг биелүүлэх ёстой байдаг. Мөн мэдээллийн аюулгүй байдлын мэдээлэл солилцох болон шинжилгээний төв (ISAC)-тай бөгөөд энэ нь санхүүгийн байгууллагуудад аюул занал, эмзэг байдлын мэдээлэл хуваалцах боломжийг олгодог.

[27] https://www.mongolbank.mn/file/beb8a25d6bc7b7f718f2a9a71f0c2b39/files/2018_03_06_A57.pdf

Зарим ОЧМДБ байгууллагууд, жишээлбэл, тээврийн салбарт үйл ажиллагаа явуулдаг байгууллагууд олон улсын түвшинд үйл ажиллагаа эрхлэхийн тулд Европын Холбооны (EU) Мэдээлэл хамгаалах ерөнхий зохицуулалт (GDPR) зэрэг олон улсын зохицуулалтыг дагаж мөрдөх үүрэгтэй байдаг. Оролцогчдын мэдээлснээр, зарим ОЧМДБ салбаруудад кибер аюулгүй байдлын сайн туршлагыг хэрэгжүүлэх явц хангалтгүй байна. Монголын их дээд сургуулиудын судалгаа болон кибер аюулгүй байдлын үйлчилгээ үзүүлэгчдийн үзэж буйгаар, эрүүл мэндийн салбар нь маш эмзэг мэдээлэлтэй харьцдаг учраас энэ асуудалд онцгой анхаарах шаардлагатай гэжээ.

Мөн бодит байдал дээр төрийн байгууллагуудын кибер аюулгүй байдал хувийн байгууллагтай харьцуулахад хамаагүй сул байна. Кибер аюулгүй байдлын хяналт хэрэгжүүлэх, кибер аюулгүй байдлын зөрчил илрүүлэх, удирдахад асуудалтай тулгарч буй талаар мэдээлсэн. Ялангуяа, төрийн байгууллагад кибер аюулгүй байдлын хяналт хэрэгжүүлэх төсөв болон ур чадвартай кибер аюулгүй байдлын мэргэжилтнүүд дутагдалтай байгааг оролцогчид тэмдэглэсэн. *Кибер аюулгүй байдлын тухай хуулийн* заалтууд нь ОЧМДБ байгууллагуудын кибер аюулгүй байдлын түвшнийг дээшлүүлэх зорилготой. Гэхдээ хууль хэрэгжүүлэхэд саад учруулж хэд хэдэн болзошгүй сорилтууд байгааг анхаарах нь чухал юм.

Эхний томоохон сорилт нь тодорхойлогдсон онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын хуулийн шаардлагуудыг хэрэгжүүлэх чадавхтай холбоотой асуудал юм. Зарим байгууллагуудын зүгээс эдгээр шаардлагыг хангах чадварын талаар санаа зовниж буйгаа илэрхийлсэн. Төрийн байгууллага, тээвэр, уул уурхайн зэрэг салбарын байгууллагууд кибер аюулгүй байдлын төсөвтэй холбоотой асуудлуудыг хөндөн, хувийн хэвшлийн байгууллагуудын удирдлагыг, мөн төрийн байгууллагуудын хувьд Сангийн яамыг кибер аюулгүй байдалд хөрөнгө оруулахын ач холбогдлыг ойлгуулахад хүндрэлтэй байгаагаа илэрхийлсэн. Зарим байгууллага хуучин технологи ашиглаж байгаа нь асуудал үүсгэж байгааг онцолж, програм хангамж болон кибер аюулгүй байдлын технологийн лиценз худалдан авах боломж хязгаарлагдмал байгаа талаар дурдсан. Харин нөгөө талаас, *Кибер аюулгүй байдлын тухай хууль* нь эдгээр байгууллагуудын кибер аюулгүй байдлын төсвийг нэмэгдүүлэх боломжийг бүрдүүлж болзошгүй гэж үзсэн.

Мөн эдгээр байгууллагуудын санаа зовж буй өөр нэг асуудал нь хуулийн шаардлагыг хэрэгжүүлэхэд дотооддоо хангалттай ур чадвартай кибер аюулгүй байдлын мэргэжилтний дутагтал юм. Үүнээс гадна, улсын хэмжээнд кибер аюулгүй байдлын өндөр ур чадвартай мэргэжилтнүүдийн хомсдол байсаар байгаа бөгөөд төрийн байгууллагын хувьд эдгээр мэргэжилтнүүдийг ажилд авах боломж хязгаарлагдмал байна (Дэлгэрэнгүйг D3-т харна уу). Жижиг байгууллагуудын хувьд нэмэлт дэмжлэг эсхүл өөр арга барил шаардлагатай байж болзошгүй юм. Хуулийн хэрэгжилтийг хянах үүрэгтэй төлөөлөгчид хязгаарлагдмал нөөц бололцоотой жижиг байгууллагуудаас хуулийн бүх шаардлагыг биелүүлэхийг хүлээх нь зохистой бус байж болохыг онцолсон.

Нөгөө талаас, хуулийн хэрэгжилттэй холбоотой талуудын ойлголт дутмаг байгаа нь асуудал үүсгэж байна. Тухайлбал, кибер аюулгүй байдлын үйлчилгээ үзүүлэгчид ОЧМДБ байгууллагуудын аудит хийх зөвшөөрөлтэй эсэх талаар төөрөгдөлтэй байгаа бол аудитын тайланг хэзээ, хаана ирүүлэх талаар ч мөн адил төөрөгдөл байсаар байна.

Эдгээр асуудлыг шийдвэрлэхийн тулд кибер аюулгүй байдлын мэргэжилтнүүдийг бэлтгэх, сургах, давтан сургах, мэргэшүүлэх чиглэлээр төрөөс дэмжлэг үзүүлэх, хууль эрх зүйн орчныг боловсронгуй болгох, холбогдох талуудад хуулийн заалтуудыг тодорхой тайлбарлах, сурталчлах шаардлагатай. Ингэснээр кибер аюулгүй байдлын салбарт тулгарч буй сорилтуудыг даван туулах, цаашдын хөгжлийг хангах боломжтой.

Хуулийн бүрэлдэхүүн хэсгүүдийг илүү тодорхой болгох талаар санал гарсан. Жишээ нь, Онц чухал мэдээллийн дэд бүтэцтэй байгууллагууд болон аудитын компаниуд дагаж мөрдөх шаардлагатай стандартуудын талаар илүү тодорхой заалт байх нь хэрэгжүүлэлтийг хялбарчлахад тустай гэж үзсэн. ЦХИХХЯ-ны зүгээс хэлэлцүүлгүүд дээр санал нэгдээгүй байдлыг харгалзан үзвэл зах зээл дээр хамгийн шилдэг стандартууд давамгайлах хүртэл энэ асуудлыг нээлттэй орхих нь хамгийн зөв шийдэл гэж үзэхээр байна. Хуульд кибер аюулгүй байдлын баг бий болгох эсхүл хариуцсан ажилтантай байх сонголт өгсөн нь том бүтэцтэй байгууллагуудад бүтэн баг байгуулах хүсэлтийг удирдлагын түвшинд тавих хөшүүргийг сулруулж буйг илэрхийлсэн. Зарим хувийн хэвшлийн байгууллагуудын зүгээс хуулиар заавал тайлагнах шаардлагатай нууц мэдээлэл (жишээ нь, аудитын тайлан) хэрхэн боловсруулагдах нь тодорхойгүй байгаа нь хувийн нууцлалтай холбоотой эрсдэлийн талаар санаа зовох шалтгаан болж, дэлгэрэнгүй мэдээлэл өгөхөөс цааргалах хандлага үүсгэж болзошгүй талаар мэдээлсэн.

Хуулийг зөв хэрэгжүүлэхийн тулд оролцогч талууд шаардлагуудыг тодорхой ойлгосон байх нь чухал учир холбогдох ОЧМДБ байгууллагуудтай хэлэлцүүлэг зохион байгуулж, хуулийн хэрэгжилтийн талаар санал хүсэлт авах, тодорхой нэмэлт заалт шаардлагатай хэсгүүдийг тодорхойлох хэрэгтэй.

Гурав дахь сорилт нь холбогдох оролцогч талуудын хууль хэрэгжүүлэх чадамж юм. Зарим оролцогчид ЦХИХХЯ-ийн лицензийн шаардлагыг хангахуйц дотоодын кибер аюулгүй байдлын үйлчилгээ үзүүлэгчдийн тоо нь бүх ОЧМДБ дээр аудит хийхэд хангалтгүй талаар тэмдэглэсэн. ЦХИХХЯ нь дотоод компаниуд дээрх шаардлагатай ажилтнуудын тоог саяхан үнэлж, хуульд заасан ОЧМДБ-н аудитын эрэлт хэрэгцээг хангах хангалттай тоо байхгүй талаар мэдээлсэн. Мөн зарим хувийн ОЧМДБ байгууллагууд холбогдох төрийн байгууллагуудын нууц мэдээллийг аюулгүй хадгалах чадамжид итгэлтэй биш байгаа нь мэдээлэл өгөх үйл явцыг сааруулах магадлалтай гэдгийг оролцогчид дурдаж байсан. Хуулийн хэрэгжилтийг амжилттай явуулахын тулд холбогдох оролцогч талуудын ур чадварыг сайжруулах, шаардлагатай бол итгэлцлийг нэмэгдүүлэх нь чухал.

Хуулийн хэрэгжилтийн талаар оролцогч талуудыг хамруулсан хэлэлцүүлэг зохион байгуулах зарим төлөвлөгөөг аль хэдийн боловсруулсан. Үүнд, Кибер аюулгүй байдлын зөвлөлийн жил бүр зохион байгуулдаг кибер аюулгүй байдлын форум багтаж байна. Төлөөлөгчид хэлэлцэх сэдвийн хүрээнд аудиттай холбоотой хүндрэлүүд болон хуулийн шаардлагын тодруулга зэргийг агуулах байдлын талаар хэлэлцэхээр төлөвлөж байгааг мэдээлсэн.

Дүгнэхэд, Кибер аюулгүй байдлын тухай хууль болон түүний дагалдах журам нь онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын хамгаалалтыг сайжруулах чиглэлээр томоохон ахиц гаргаж байна. Гэвч ОЧМДБ байгууллагууд хуулийн шаардлагыг хэрхэн

ойлгож, хэрэгжүүлж байгааг тасралтгүй хянах нь чухал бөгөөд ингэснээр аливаа дутагдлыг тодорхойлж, шаардлагатай дэмжлэгийг үзүүлэх боломж бүрдэх юм. Кибер аюулгүй байдлын үндэсний стратеги (КАБҮС) нь ОЧМДБ байгууллагуудын кибер аюулгүй байдлын хэрэгжилтийн ахицыг хэмжих тодорхой шалгуур үзүүлэлтүүдийг багтаасан. Үүнд “кибер аюулгүй байдлын эрсдэлд суурилсан тусгайлсан практикийг нэвтрүүлсэн байгууллагуудын өсөлтийн хувь” болон “нөхөн сэргээх, тасралтгүй ажиллагааны удирдлагын тогтолцоог бий болгосон байгууллагуудын өсөлтийн хувь” зэрэг хяналт тавихад туслах хэмжүүрийг багтаасан. Мөн хууль хэрэгжиж эхлэхийн хэрээр төлөвлөсөн зохицуулалтын арга барилын үр нөлөөг турших нь нэн чухал гэж үзэж байна.

D 1.4 БАТЛАН ХАМГААЛАХ БОЛОН ҮНДЭСНИЙ АЮУЛГҮЙ БАЙДАЛД КИБЕР АЮУЛГҮЙ БАЙДЛЫН ОРОЛЦОО

Энэхүү хүчин зүйл нь төр нь үндэсний аюулгүй байдал болон батлан хамгаалах салбарт кибер аюулгүй байдлын стратегийг боловсруулах, хэрэгжүүлэх чадвартай эсэхийг судална. Мөн үндэсний аюулгүй байдал, батлан хамгаалах байгууллагуудын кибер аюулгүй байдлын чадавх ямар түвшинд байгааг үнэлж, иргэний болон батлан хамгаалахын байгууллагуудын хооронд кибер аюулгүй байдлын хамтын ажиллагааны зохицуулалтууд хэрхэн хэрэгжиж байгааг шинжилнэ.

Түвшин: **Хөгжиж буй түвшнээс Тогтворжсон түвшинд**

Батлан хамгаалахын кибер аюулгүй байдлын стратеги албан ёсоор нийтлэгдээгүй бөгөөд оролцогчид энэ чиглэлээр тодорхой хөгжүүлэлт хийж байгаа талаарх мэдээлэл өгсөнгүй. *Кибер аюулгүй байдлын тухай хуулийн* 14-р зүйл нь батлан хамгаалах салбарын кибер аюулгүй байдлыг хариуцаж буй байгууллагад тавигдах хэд хэдэн шаардлагыг тодорхойлсон байна. Үүнийг стратегийн зорилтуудыг өндөр түвшинд тодорхойлсон гэж үзэж болох юм:

14.1.1. Батлан хамгаалах салбарт кибер аюулгүй байдлын хуулийг хэрэгжүүлэх ажлыг зохион байгуулах.

14.1.2. Дайн байлдааны нөхцөлд батлан хамгаалах мэдээллийн систем, мэдээллийн сүлжээний аюулгүй байдлыг хангах, шаардлагатай тохиолдолд улсын кибер аюулгүй байдлыг дэмжих.

14.1.3. Хуульд өөрөөр заагаагүй бол батлан хамгаалах командын нэгжүүд болон байгууллагын мэдээллийн систем, мэдээллийн сүлжээг шалгаж, баталгаажуулах.

14.1.4. Батлан хамгаалах командын нэгжүүд болон байгууллагуудад кибер аюулгүй байдлыг хангах сургалт зохион байгуулах, зөвлөмж боловсруулах.

14.1.5. Кибер аюулгүй байдлын чадамж, бэлтгэл байдлыг хангах зорилгоор дотоод болон олон улсын байгууллагуудтай мэдээлэл солилцох, хамтран ажиллах.

Оролцогчид батлан хамгаалахын кибер хамгааллын үйл ажиллагааны дүрэм, журмыг тодорхойлсон албан ёсны баримт бичиг байхгүй гэж мэдээлсэн. Түүнчлэн, олон улс

дамнасан зөрчилд хариу арга авах үед Үндэсний төв хариуцан удирдах зохицуулалттай гэж ойлгогдож байна.

Мөн кибер аюулгүй байдал нь улсын аюулгүй байдал болон батлан хамгаалахад үзүүлэх нөлөөллийг үнэлсэн эсэх нь тодорхойгүй байна. Иймд батлан хамгаалахын кибер аюулгүй байдлын стратеги, үйл ажиллагааны процесс, дүрэм журмыг хөгжүүлэхэд зайлшгүй шаардлагатай. Уг үнэлгээнд дараах асуудлуудыг тусгах шаардлагатай:

- Улсын зэвсэгт хүчний болон бусад аюулгүй байдлын салбарт хамаарах мэдээллийн дэд бүтцийг кибер орчинд дайны болон бусад онцгой нөхцөлд хэвийн ажиллагаатай байлгах эрсдэлийн үнэлгээ.
- Үндэсний аюулгүй байдал болон зэвсэгт хүчний байгууллагуудын хамааралтай байдал, тэдний мэдээллийн системийн аюулгүй байдалд тулгуурласан бие даасан байдлыг үнэлэх шаардлагатай.

Эдгээр үнэлгээг хийснээр батлан хамгаалахын кибер аюулгүй байдлын стратеги боловсруулах, түүнийг хэрэгжүүлэх төлөвлөгөө, бодлогын чиглэлүүдийг тодорхойлох үндэс суурь болно. Мөн кибер аюулгүй байдлын асуудлуудыг үндэсний аюулгүй байдал болон батлан хамгаалах стратегийн бусад холбогдох бүрэлдэхүүн хэсгүүдэд тусган боловсруулах нь чухал.

Батлан хамгаалахын кибер аюулгүй байдлын команд байгуулагдсан. Энэ бүтэц дотор, Батлан хамгаалахын кибер халдлага, зөрчилтэй тэмцэх төв нь 2021 онд НАТО-ийн дэмжлэгтэйгээр нээгдсэн.[28] Уг төвийг байгуулах нь Кибер аюулгүй байдлын тухай хуулиар батлагдсан бөгөөд Үндэсний болон Нийтийн төвүүдтэй хамтран ажиллах зорилготой. Үүнээс гадна улсын кибер хамгааллын чадавхыг бэхжүүлж, Батлан хамгаалах хүчний дэд бүтцийг хамгаалахад чиглэж байна.

Батлан хамгаалахын кибер аюулгүй байдлын команд болон төвийн ажилтнуудын сургалт үргэлжлэн явагдаж байна. Монголын Үндэсний Батлан Хамгаалах Их Сургуулиас Батлан хамгаалах, тагнуулын байгууллага, хил хамгаалах хүчин зэрэг байгууллагуудын ажилтнуудад зориулсан кибер аюулгүй байдлын сургалтын хөтөлбөрийг 2 жилийн өмнө байгуулсан гэж мэдээлсэн. Энэтхэг зэрэг бусад орнуудтай хамтран олон сургалтын хөтөлбөрүүд хэрэгжүүлсэн ч ур чадвартай мэргэжилтнүүд дутагдалтай байгааг мэдэгдсэн. Мөн АНУ, Энэтхэг, Солонгос, Япон улс болон НАТО-ийн хамтын ажиллагаагаар мэргэжилтэн бэлтгэх ажил явагдаж байгааг мэдээлсэн. Одоогийн ур чадамжийг үнэлсэн талаарх ямар ч нотолгоог судалгааны багт өгөөгүй болно.

Төлөвшлийн үнэлгээний хэлэлцүүлэгт оролцогчид батлан хамгаалахын байгууллагын үйл ажиллагааны болон командын сургалтанд кибер аюулгүй байдлыг нэгтгэсэн эсэх талаар мэдээлэлгүй байна. Өмнө дурдсанчлан, оролцогч талууд холбоотнуудтай хамтран сургалт явуулах механизмуудыг бий болгосон. Гэхдээ оролцогчдын мэдээлснээр хамтран ажиллах механизмууд нь шаардлагатай үед хамтарсан хариу арга хэмжээ авах боломжтой эсэх нь тодорхойгүй байна.

Кибер аюулгүй байдлын тухай хуульд зэвсэгт хүчин нь “шаардлагатай тохиолдолд улсын кибер аюулгүй байдлыг хангах үйл ажиллагаанд дэмжлэг үзүүлэх” үүрэгтэй гэж заасан. Иргэний болон батлан хамгаалах байгууллагуудын кибер аюулгүй байдлын хамтын

[28] https://www.nato.int/nato_static_fl2014/assets/pdf/2021/2/pdf/210208-sps-inauguration-mongolia.pdf

ажиллагааг үндэсний хэмжээний онцгой байдлын үед хэрэгжүүлэх зохицуулалтыг 2024 онд батлагдсан Үндэсний кибер халдлага, зөрчилд хариу арга хэмжээ авах төлөвлөгөөгөөр албан ёсоор тогтоосон. Оролцогчдын мэдээлснээр, уг төлөвлөгөөний дагуу онцгой байдал үүссэн үед Кибер халдлага, зөрчилтэй тэмцэх Үндэсний, Нийтийн болон Зэвсэгт хүчний төвүүдийн хамтын ажиллагааг хангах хамтарсан ажлын хэсэг байгуулах шаардлагатай гэж заасан. Зэвсэгт хүчний төлөөлөгчид шаардлагатай тохиолдолд дэмжлэг үзүүлэх чадвар, нөөц бололцоотой гэдгээ илэрхийлсэн. Төлөвлөгөө нь шинээр батлагдсан бөгөөд хараахан практикт туршигдаагүй байгаа боловч тогтмол сургуулилтууд хийх зорилготой байна. Тиймээс, одоогоор иргэний болон батлан хамгаалахын байгууллагуудын кибер аюулгүй байдлын хамтын ажиллагаа үр дүнтэй хэрэгжиж байгаа талаар тодорхой нотолгоо байхгүй байна.

Зэвсэгт хүчин нь иргэний болон онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын дэд бүтэцтэй хамааралтай эсэх талаар үнэлгээ хийгдсэн тухай ямар нэгэн нотолгоо өгөгдөөгүй. Энэ хамаарлыг үнэлэх процессыг бий болгох нь чухал бөгөөд ингэснээр иргэний болон ОЧМДБ байгууллагууд шаардлагатай үйлчилгээг тасралтгүй хангах чадамжтай байх нөхцөлийг бүрдүүлэх юм.

ЗӨВЛӨМЖ

Кибер аюулгүй байдлын бодлого, стратегийн төлөвшлийг үнэлэх үйл явцын хүрээнд танилцуулсан мэдээллийн дагуу Дэлхийн Кибер Аюулгүй Байдлын Чадавхын Төвөөс Монгол Улсын Засгийн газарт дараах зөвлөмжүүдийг боловсруулаад байна. Эдгээр зөвлөмжүүд нь тус төвийн Кибер аюулгүй байдлын төлөвшлийн загварын үзэл баримтлалын дагуу одоо байгаа кибер аюулгүй байдлын чадавхыг нэмэгдүүлэхэд чиглэгдсэн арга хэмжээ, алхмуудыг агуулна. Зөвлөмжийг хүчин зүйл бүрийн хувьд тусгайлан боловсруулсан болно.

КИБЕР АЮУЛГҮЙ БАЙДЛЫН ҮНДЭСНИЙ СТРАТЕГИ

R1.1.1 Үндэсний хэмжээнд кибер аюулгүй байдлын эрсдэлийн бүрэн дүр зургийг гаргахын тулд цаашид ямар ажлууд хийгдэх шаардлагатайг тодорхойлох, мөн өмнөх судалгаанууд үүнд хэрхэн хувь нэмэр оруулж болохыг үнэлэх нь чухал. Энэ хүрээнд ОЧМДБ, үндэсний аюулгүй байдлын байгууллагууд болон хувийн хэвшлийн төлөөлөл зэрэг холбогдох оролцогч талуудтай зөвлөлдөх ажлыг зохион байгуулах шаардлагатай. Мөн онц чухал дэд бүтцийн хүрээнд шинэ технологи ашигласнаас үүсэх кибер аюулгүй байдлын эрсдэлийг харгалзаж үзэх, өргөн хүрээнд эдийн засаг, нийгэмд үзүүлэх нөлөөллийг үнэлэх нь зүйтэй.

R1.1.2 Өөрчлөгдөж буй аюул занал, технологийн орчныг харгалзан, эрсдэлийн үнэлгээг тогтмол шинэчлэх процессыг боловсруулж, уг мэдээллийг ашиглан *Кибер аюулгүй байдлын үндэсний стратеги* (КАБҮС) болон түүний хэрэгжилтийн төлөвлөгөөг шинэчлэх.

R1.1.3 Эрсдэл болон хохирлыг бууруулах хөтөлбөрийн үр дүнтэй байдлыг хянах болон үр дүнд суурилсан хэмжүүрүүдийг тодорхойлох. Эдгээр хэмжүүрийг ашиглан үйл ажиллагааны төлөвлөгөөг тасралтгүй сайжруулж, санхүүжилт болон тэргүүлэх чиглэлүүдийг тодорхойлох.

R1.1.4 КАБҮС-ийн I үе шат дуусах үед хэрэгжилтийн явцыг үнэлэхдээ, стратеги хариуцсан байгууллагууд нь үр дүнг хянах, хэрэгжүүлэлттэй холбоотой асуудлуудыг илрүүлэх боломжоор хангах. Шаардлагатай сайжруулалтыг тодорхойлох.

R1.1.5 Кибер Аюулгүй Байдлын Зөвлөлийн тогтмол хуралдаануудыг үр дүнтэй зохион байгуулж, *Кибер аюулгүй байдлын үндэсний стратеги* (КАБҮС)-ийн хэрэгжилтийн явц дахь тулгамдсан асуудал, төсвийн дутагдал зэргийг цаг алдалгүй тодорхойлж, шийдвэрлэхэд чиглүүлэх. Мөн хувийн хэвшил, иргэний нийгмийн байгууллага зэрэг бусад оролцогч талуудыг КАБҮС-ийн засаглал, хэрэгжилтийн явцын хяналтад татан оролцуулах процессыг боловсруулах нь үр дүнтэй байж болно. Ингэснээр зөвлөлийн ачааллыг хөнгөвчлөхийн зэрэгцээ, өргөн хүрээний оролцогч талуудын санал бодлыг тусгах боломжийг бүрдүүлж, хөтөлбөрийн хэрэгжилтийн төрөл бүрийн асуудлыг илүү үр дүнтэй тодорхойлоход дэмжлэг үзүүлнэ.

R1.1.6 КАБҮС-ийн үйл ажиллагааны төлөвлөгөөг хэрэгжүүлэхэд шаардлагатай санхүүгийн нөөцийн үнэлгээг тогтмол хийх нөхцөлийг бүрдүүлэх. Мөн төсвийн дутагдал үүссэн тохиолдолд асуудлыг шийдвэрлэх санхүүгийн зохицуулалтын механизм ажиллах боломжоор ханган аль аль талыг нь авч үзсэн оновчтой шийдвэр гаргах боломжтой байх.

R1.1.7 Дараагийн *Кибер аюулгүй байдлын үндэсний стратеги* (КАБҮС)-ийг боловсруулах, шинэчлэх үйл явцыг албан ёсоор тогтоож, хэрэгжүүлэх нөхцөлийг бүрдүүлэх. Уг процесс нь одоогийн стратегийн хэрэгжилтээс гарсан сургамжуудыг хэрхэн тодорхойлох, үнэлэх талаар нарийвчлан тусгах ёстой.

R1.1.9 Кибер аюулгүй байдлын олон улсын хэлэлцүүлэгт Монгол Улсын оролцооны тодорхой зорилтуудыг тогтоохын тулд холбогдох оролцогч талуудтай зөвлөлдөж, эдгээр зорилтыг харгалзан Монгол Улсын төлөөлөгчдийн оролцоог зохицуулах. Зорилтууд тодорхой, ойлгомжтой байх дээр анхааран, хэрэгжилтийн явцыг хянах механизмыг бий болгох.

ЗӨРЧИЛД ХАРИУ ҮЗҮҮЛЭХ БОЛОН ОНЦГОЙ БАЙДЛЫН МЕНЕЖМЕНТ

R1.2.1 Кибер халдлага, зөрчилтэй тэмцэх төвүүдийн хуваарилсан бүтэц бүхий тогтолцоо нь шинэ кибер халдлага, зөрчлийн төлөвлөгөөний дагуу, олон салбарыг хамарсан томоохон кибер зөрчил эсхүл онцгой байдлын үед хэрхэн ажиллах чадвартайг турших. Үйл ажиллагааны болон ширээний (table-top) дасгал, сургуулилтууд зохион байгуулж, зөрчлийн хариу арга хэмжээнд оролцож боломжтой бүх байгууллагуудыг хамруулснаар тухайн процессыг тодорхой болгоход тусална. Энэ чадамжийг улс оронд үүсэж болзошгүй олон төрлийн кибер аюул, заналын нөхцөл байдалд турших нь чухал бөгөөд сургуулилтууд нь технологийн хөгжлийн болон аюул заналын орчны өөрчлөлтүүдийг харгалзан үзэх шаардлагатай. Эдгээр тестүүдээс гарсан сургамжуудыг тасралтгүй үнэлэх үндсэн дээр дараах арга хэмжээнүүдийг авч үзэх нь зүйтэй:

- Төв бүрийн чадамжийг хэрхэн сайжруулах боломжтойг судлах, үүнд хувийн хэвшлийн байгууллагын нөөц бололцоог ашиглан чадавхыг нэмэгдүүлэх боломжийг судлах;
- Зохицуулалт хийхэд шаардлагатай алхмууд, байгууллага хоорондын харилцааг хэрхэн сайжруулах боломжтойг судлах.

R1.2.2 Кибер аюулгүй байдлын зөрчлийн мэдээллийн санд бүртгэгдсэн мэдээлэл нь улсын хэмжээнд зөрчлийн бүрэн дүр зургийг өгч байгаа эсэхийг баталгаажуулах. Энэ нь Нийтийн болон Үндэсний төв хоорондын үр дүнтэй харилцаа холбооноос ихээхэн хамаарах бөгөөд онц чухал мэдээллийн дэд бүтэцтэй төрийн болон хувийн хэвшлийн

байгууллагуудын хариуцлагыг эдгээр хоёр төв хуваан хариуцдаг тул мэдээлэл солилцооны тогтолцоог бүрэн нэвтрүүлэх шаардлагатай.

R1.2.3 Кибер аюулгүй байдлын зөрчлийн мэдээллийн санд бүртгэгдсэн мэдээллийг ашиглан улсын хэмжээнд гарч буй кибер зөрчлүүдийг тодорхойлох, ангилах, хариу арга хэмжээг хэрэгжүүлэх тогтолцоог хангах. Эдгээр үйл явцын үр нөлөөг турших нь чухал бөгөөд үүнийг D1.2.1-д заасан туршилтуудын хүрээнд багтааж болно. Түүнчлэн, Монгол Улсад гарч буй кибер зөрчлүүдийн бүртгэл, мэдээлэл солилцоог хангалттай уялдуулан зохицуулж, аюул заналын чиг хандлага, эрсдэл, хохирол, алдагдлыг нарийвчлан шинжлэх боломжийг бүрдүүлэх нь чухал. Энэ нь үндэсний стратеги боловсруулах болон кибер аюулгүй байдлын үйл ажиллагаанд нөөц хуваарилах шийдвэр гаргалтыг дэмжих мэдээлэл болох юм.

R1.2.4 Төвүүд хооронд болон бусад оролцогч талуудтай (тухайн зөрчилд өртөж болзошгүй байгууллагуудыг багтаасан) мэдээлэл солилцох сувгийг сайжруулах боломжийг судлах. Ингэснээр аюул занал, эмзэг байдлын талаарх мэдээлэл шаардлагатай бүх байгууллагад цаг алдалгүй хүрэх нөхцөлийг бүрдүүлэх боломжтой. Үүнд "эмзэг мэдээлэл ангилах систем" (Traffic Light Protocol) болон мэдлэг хуваалцах платформ зэрэг харилцаа холбооны арга хэрэгслийг боловсруулах ажил орж болох бөгөөд MNCERT/CC-ийн олон жилийн туршлагыг ашиглаж болох.

ОНЦ ЧУХАЛ ДЭД БҮТЦИЙН ХАМГААЛАЛТ

R1.3.1 Хууль хэрэгжиж эхлэхийн хэрээр ОЧМДБ байгууллагуудын зохицуулалтын стандартыг дагаж мөрдөх байдал, зөрчил болон эмзэг байдлын мэдээлэл солилцох үйл явцын ахицыг хянах. Мөн зохицуулалтын хэрэгжилтийг үнэлэхээр төлөвлөсөн ажлын үр дүнтэй байдлыг хянан шалгах. R1.3.2, R1.3.3 болон R1.3.4-т энэ зөвлөмжийн бүрэлдэхүүн хэсгүүдийн талаар дэлгэрэнгүй мэдээлэл өгсөн болно.

R1.3.2 Тодорхойлогдсон онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын Кибер аюулгүй байдлын тухай хуулийн шаардлагыг хэрэгжүүлэх чадамжийг тогтмол хянах, мөн уг ахицыг Кибер аюулгүй байдлын зөвлөлийн гүйцэтгэлийн түлхүүр үзүүлэлтүүдэд (KPI) тусгах. Төлөвлөсөн аудитын үйл ажиллагааг ОЧМДБ байгууллагуудтай хийсэн зөвлөлдөх уулзалтуудаар өргөжүүлж, чадамжийн асуудлуудыг илүү нарийвчлан тодорхойлох боломжтой. ОЧМДБ салбарын байгууллагууд нь хуулийн шаардлагыг бүрэн хангаж буйг шалгах аргачлалуудыг судлах. Үүнд дараах арга хэмжээнүүдийг багтааж болно:

- Төрийн болон хувийн хэвшлийн онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудад зөрчлийг илрүүлэх, хариу арга хэмжээ авах чадамжийг сайжруулахад чиглэсэн заавар, дэмжлэг үзүүлэх.
- Хувийн хэвшлийн байгууллагуудад кибер аюулгүй байдлын технологи, мэргэжилтнүүдэд шаардагдах төсвийг нэмэгдүүлэх талаар дэмжлэг үзүүлэх. Үүнд байгууллагын удирдлагад кибер аюулгүй байдлын төсвийн хэрэгцээг хэрхэн танилцуулах тухай зөвлөмж боловсруулах, эсхүл удирдах албан тушаалтанд чиглэсэн зориулсан кибер аюулгүй байдлын мэдлэг олгох сургалтууд явуулах зэрэг хамаарч болно.
- Төрийн байгууллагуудад кибер аюулгүй байдлын төсвийг Сангийн яамнаас авахад нь дэмжлэг үзүүлэх. Төрийн байгууллагууд төсөв хүсэхдээ кибер аюулгүй байдлыг тусад нь ангилал болгон оруулах боломж бүрдүүлэх нь тустай байж болох талаар санал хэлэлцүүлгийн үед мөн дурдагдсан.

- Хязгаарлагдмал нөөцтэй жижиг байгууллагууд хуулийн шаардлагыг хангахад шаардлагатай дэмжлэгийг тодорхойлох. Үүнд, жижиг байгууллагуудад тохирсон дотоод кибер аюулгүй байдлын журам боловсруулах гарын авлага боловсруулах зэрэг арга хэмжээг багтааж болно.
- Дэмжлэг үзүүлэх боломжтой байгууллагуудыг тодорхойлох.

R1.3.3 ОЧМДБ байгууллагуудын төлөөлөлтэй хэлэлцүүлэг зохион байгуулж, Кибер аюулгүй байдлын тухай хуулийн талаар санал хүсэлт авах. Хэлэлцүүлгийн үеэр зарим оролцогч хуулийн тодорхой ойлгомжтой байдал болон нарийвчлалийн түвшинд санаа зовж буйг илэрхийсэн бөгөөд D1.3-т тухайлан дурдсан. Хууль хэрэгжилтийг саадгүй явуулахын тулд оролцогч талууд шаардлагуудын талаар зөв ойлголттой байх нь чухал юм.

R1.3.4 Хуулийг хэрэгжүүлэхэд оролцож буй талууд шаардлагатай чадвар, хамтын ажиллагааны харилцааг хангах. Мөн үүргээ үр дүнтэй биелүүлэхэд энэ шалгуурыг Кибер аюулгүй байдлын зөвлөлийн гүйцэтгэлийн гол үзүүлэлтүүдэд (KPI) тусгах. Үүнд дараах арга хэмжээнүүдийг хэрэгжүүлэх байдлаар авч үзэж болно:

- Онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын эрсдэлийн үнэлгээ, аудит хийх тусгай зөвшөөрөл бүхий кибер аюулгүй байдлын үйлчилгээ үзүүлэгчдийн нийлүүлэлт хангалттай эсэхийг үнэлэх.
- Үндэсний болон Нийтийн төвүүдийн харьяа байгууллагуудтай харилцах харилцааг хянах, мэдээлэл солилцох, тайлагнах үйл явц үр дүнтэй явагдаж буй эсэхийг баталгаажуулах.
- Тагнуулын ерөнхий газар (ТЕГ) болон Цахим хөгжил, инновац, харилцаа холбооны яам (ЦХИХХЯ) хууль, журмын хэрэгжилтийг зохицуулахад шаардлагатай чадамж, нөөц бололцоотой эсэхийг баталгаажуулах.

R1.3.5 Тодорхойлогдсон онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын жагсаалтыг улс орны нөхцөл байдал, технологийн болон геополитикийн орчны өөрчлөлтөд уялдуулан шинэчлэх боломжтой байх боломжийг бүрдүүлэх үүднээс тогтмол хянан шалгах процессыг хэрэгжүүлэх.

R1.3.6 ОЧМДБ байгууллагуудын харилцан хамаарал, түүнчлэн бусад ОЧМДБ бус байгууллага болон гадаад орны дэд бүтцээс хамаарах байдлыг тодорхойлох процессыг бий болгож, нийлүүлэлтийн сүлжээ болон системийн эрсдэлийг ойлгон, улмаар нэгдсэн эрсдэлийг хурдан илрүүлэх чадварыг сайжруулах. Эдгээр хамаарлыг удирдах аргачлалыг албажуулан баримтжуулах.

ҮНДЭСНИЙ БАТЛАН ХАМГААЛАХ САЛБАРЫН АЮУЛГҮЙ БАЙДАЛ

R1.4.1 Кибер аюулгүй байдлын аюул занал нь үндэсний аюулгүй байдал болон батлан хамгаалах салбарт үзүүлэх боломжит нөлөөллийг үнэлж, эрсдэлд чиглэсэн стратегийг боловсруулах. Энэхүү стратегийг хэрэгжүүлэхэд шаардлагатай үйл ажиллагааны зарчим, хариу арга хэмжээний дүрэм, зохицуулалтыг тодорхойлох.

R1.4.2 Зэвсэгт хүчин нь иргэний болон онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын дэд бүтцээс хамаарч буй эсэхийг үнэлэх, аргачлалыг бий болгох. Иргэний болон ОЧМДБ байгууллагуудын үзүүлж буй үйлчилгээнүүд нь найдвартай байдал болон чадамжийг хангасан эсэхийг баталгаажуулах.

R1.4.3 Батлан хамгаалахын кибер аюулгүй байдлын одоогийн чадамжийг дасгал, туршилтаар шалгах. Үүнд:

- Зэвсэгт хүчний сүлжээ, мэдээллийн системийг хамгаалах;
- Үндэсний хэмжээний онцгой байдлын үед иргэний байгууллагуудтай хамтран ажиллах, дэмжлэг үзүүлэх;
- Холбоотнуудтай хамтран мэдээлэл солилцох, зөрчилд хариу арга хэмжээ авах;

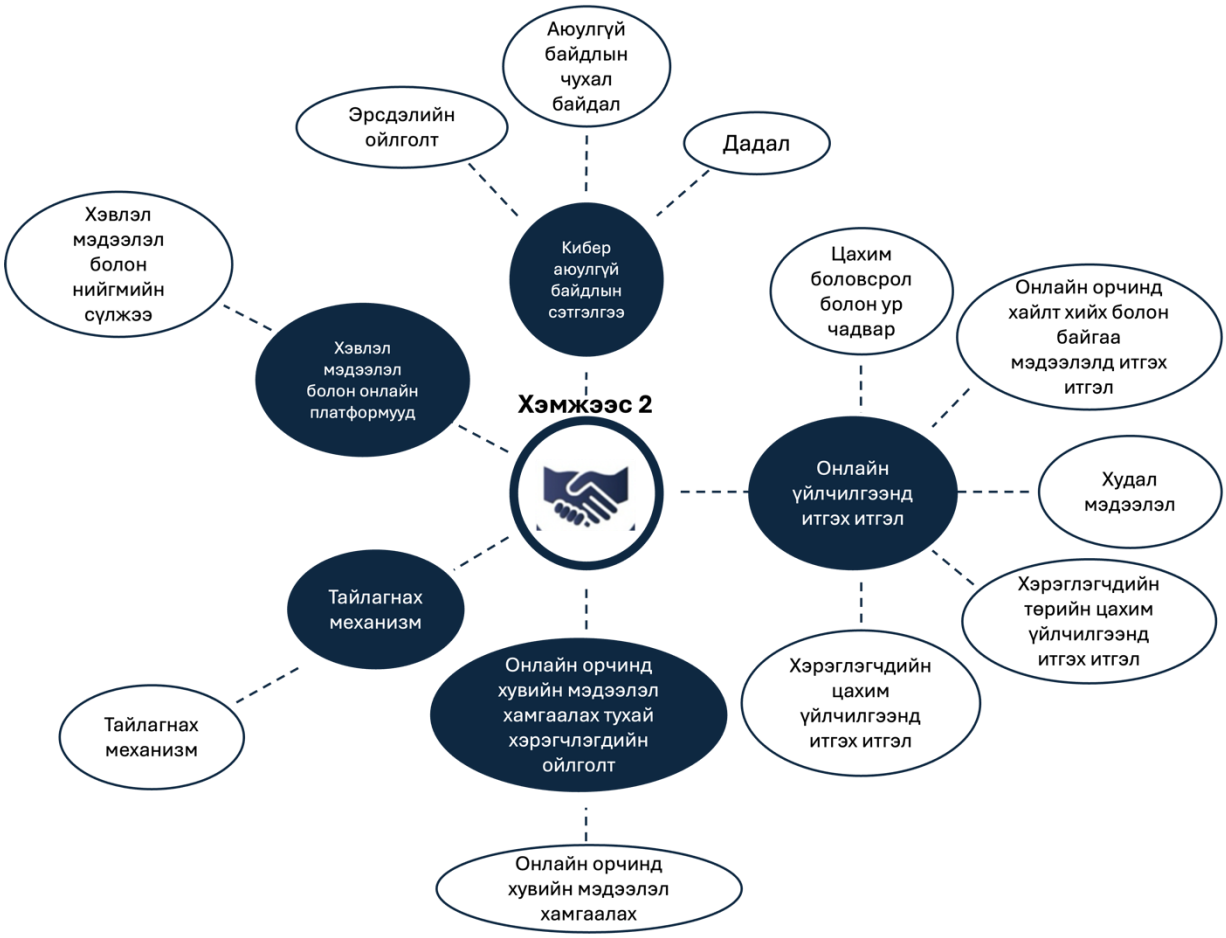
- Эдгээр үнэлгээний үр дүнг ашиглан нөөцийн хуваарилалт, сургалтын тэргүүлэх чиглэлийг тодорхойлох.

R1.4.4 Зэвсэгт хүчний байгууллагуудыг хамарсан үйл ажиллагаа, командын сургалтад кибер аюулгүй байдлын мэдлэг түгээх агуулга оруулах.

ХЭМЖЭЭС 2

КИБЕР АЮУЛГҮЙ БАЙДЛЫН СОЁЛ БОЛОН НИЙГЭМ

Энэхүү хэмжээс нь кибер аюулгүй байдлын хариуцлагатай соёлыг бүрдүүлэхэд чухал нөлөөтэй элементүүдийг үнэлэхэд чиглэгдэнэ. Үүнд, нийгэм дэх кибер эрсдэлийн талаарх ойлголт, интернетийн үйлчилгээ, цахим засаглал, цахим худалдаа үйлчилгээнд итгэх итгэлийн түвшин, хэрэглэгчдийн хувийн мэдээллээ цахим орчинд хамгаалах мэдлэг зэрэг асуудлууд багтана. Түүнчлэн, кибер гэмт хэргийг мэдээлэх механизм ажиллаж байгаа эсэх, хэрэглэгчдэд зориулсан тайлагнах сувгын үр дүнтэй байдлыг судална. Үүнээс гадна, кибер аюулгүй байдлын үнэт зүйл, хандлага, зан төлөвийг төлөвшүүлэхэд хэвлэл мэдээлэл болон олон нийтийн мэдээллийн хэрэгслийн гүйцэтгэж буй үүгийг авч үзэх болно.



D 2.1 КИБЕР АЮУЛГҮЙ БАЙДЛЫН СЭТГЭЛГЭЭ

Энэхүү хүчин зүйл нь кибер аюулгүй байдлыг төр, хувийн хэвшил, энгийн хэрэглэгч зэрэг нийгмийн бүхий л түвшинд хэр зэрэг чухалчилж, үнэт зүйл, хандлага, практикт, дадал зуршилд шингээсэн байдлыг үнэлнэ. ***К****ибер аюулгүй байдлын сэтгэлгээ гэдэг нь хэрэглэгч, мэргэжилтэн болон кибер орчны бусад оролцогчдын өдөр тутмын хандлага, дадал, үйл ажиллагаанд шингэсэн үнэт зүйлс, ойлголтуудын цогц юм. Энэ нь цахим орчинд өөрийгөө хамгаалах чадамжийг нэмэгдүүлэхэд чухал үүрэгтэй.*

Түвшин: Хөгжиж буй түвшинд

Монгол Улсад цахим шилжилт болон кибер аюулгүй байдлын эрсдэлийн талаарх ойлголт ааажмаар төлөвшиж байна. Энэ нь төрийн болон хувийн хэвшлийн салбарын мэдээлэлтэй гол оролцогч талуудтай хийсэн хэлэлцүүлгээс илэрхий харагдаж байв. Голлох бүлгийн хэлэлцүүлгийн үеэр хууль сахиулах байгууллага, зохицуулах байгууллага, үйлчилгээ үзүүлэгч байгууллага, санхүүгийн байгууллага, бизнесийн удирдагчид болон боловсролын салбарын мэргэжилтнүүд кибер аюул, хохирлын талаар дэлгэрэнгүй ярилцсан. Үүнд цахим залилан, мэдээллийн алдагдах, кибер дээрэлхэлт, худал мэдээлэл (disinformation) зэрэг асуудлууд багтсан бөгөөд эдгээрийг тасралтгүй бууруулах шаардлагатай гэж үзэж байна. Стратегийн түвшинд төрийн тэргүүлэх албан хаагчид болон хувийн хэвшлийн төлөөлөгчид кибер аюулгүй байдал нь үндэсний аюулгүй байдал, эдийн засгийн хөгжил, дижитал хөгжлийн бодлого, хувийн мэдээллийн нууцлал болон нийгмийн эв нэгдэлд хэрхэн эрсдэл учруулж болохыг цогцоор нь ойлгож, тодорхой тайлбарлах чадвартай байлаа.

2021 оноос хойш, ялангуяа Кибер аюулгүй байдлын тухай шинэ хууль эрхзүйн зохицуулалт (4.1-р хүчин зүйлд тайлбарласан) батлагдсанаас хойш кибер аюулгүй байдлын талаарх ойлголт, чухалчлан авч үзэх хандлага мэдэгдэхүйц нэмэгдсэн. Энэхүү эрх зүйн зохицуулалтын заавал биелүүлэх шаардлагууд нь ОЧМДБ байгууллагуудын

удирдлагуудаас кибер аюулгүй байдлын талаар суралцахаас гадна мэргэжлийн хүний нөөц, технологи болон дэд бүтцийн чиглэлээр бодитой хөрөнгө оруулалт хийхийг шаардсан.

Хууль батлагдахаас өмнө ч төр болон хувийн хэвшлийн хэд хэдэн оролцогч талууд өөрсдийн кибер аюулгүй байдлыг сайжруулах зорилгоор сайн дурын үндсэн дээр тодорхой алхмуудыг хэрэгжүүлсэн бөгөөд зарим нь хэрэгжүүлэхээр төлөвлөөд байжээ. Зарим байгууллага хууль хэрэгжиж эхэлснээс хойш Олон Улсын кибер аюулгүй байдлын стандартыг нэвтрүүлэх нэмэлт арга хэмжээ авч, кибер аюулгүй байдлын эрсдэлийг удирдахад илүү тууштай хандаж буйгаа харуулсан. Түүнчлэн Монгол Улсын Засгийн газар Кибер аюулгүй байдлын үндэсний стратеги 2022 болон түүний хэрэгжилтийн төлөвлөгөөг боловсруулсан нь кибер аюулгүй байдлын талаарх ойлголт, тэргүүлэх чиглэл болгон авч үзэж буйг илтгэх баримт болж байна. Стратеги боловсруулах явцад Монгол Улсын кибер аюулгүй байдлын талаарх ойлголтын түвшинг судалж, уг судалгааны үр дүнг стратегийн зорилт тодорхойлоход ашигласан. Голлох бүлгийн хэлэлцүүлгийн үеэр төрийн болон боловсролын байгууллагууд, мөн НҮБ-ын Хөгжлийн Хөтөлбөр (UNDP) зэрэг олон улсын түншүүд иргэдийн кибер аюулгүй байдлын мэдлэгийн талаар судалгаа хийсэн тухай дурдсан.

Кибер аюулгүй байдлын талаарх мэдлэг ойлголт тодорхой түвшинд бий болсон ч төрийн байгууллага, иргэний нийгэм болон нийт иргэдийн дунд кибер аюулын талаарх өргөн хүрээний мэдлэгийг бүрэн түгээж чадаагүй байна. Шинэ хууль, зохицуулалтууд хэрэгжиж эхэлснээр кибер аюулгүй байдлын талаарх ойлголт, ач холбогдол нэмэгдсэн ч бүх түвшинд хүрээгүй бөгөөд зарим гол оролцогч талууд эдгээр хуулийн талаарх ойлголт хомс хэвээр байна. Голлох бүлгийн хэлэлцүүлгийн үеэр кибер аюулгүй байдал хариуцдаг төрийн яамд, агентлагуудаас бусад ихэнх төрийн албан хаагч, ажилтнууд кибер аюулгүй байдал нь зөвхөн мэдээллийн технологийн хэлтэст хамааралтай бус, өөрсдөд нь чухал холбоотой асуудал гэдгийг ойлгоогүй тал ажиглагдсан. Хэд хэдэн оролцогч талуудын зүгээс дийлэнх төрийн албан хаагчдын дунд мэдээлэл болон кибер аюулгүй байдлыг чухалчлан хүлээн авдаггүй хандлага гүн суусан байдаг талаар онцолж, улмаар кибер аюулгүй байдлын сургалт, чадавхжуулах арга хэмжээнээс хойш суух хандлага түгээмэл байдаг талаар дурдсан. Хувийн хэвшлийн хувьд, санхүүгийн байгууллага, үйлчилгээ үзүүлэгч болон мэдээллийн технологийн мэргэжлийн компаниудаас бусад ихэнх компаниуд энэ асуудлыг бүрэн ойлгоогүй байна.

Улс төрчид, ахлах менежерүүд болон төрийн албан хаагчдын кибер аюулгүй байдлын талаарх мэдлэгийн түвшин хангалтгүй байгаа нь төр, хувийн хэвшлийн аюулгүй байдлыг сулруулах үр дагавартай, тулгамдсан асуудал гэж тодорхойлогдсон. Тухайн салбартаа хамгийн их мэдлэг, мэдээлэлтэйд тооцогддог оролцогч талууд хүртэл орчин үеийн цахим шилжилтийн хурдтай хөл нийлүүлэхэд хүндрэлтэй байгаагаа илэрхийлсэн бөгөөд ялангуяа хиймэл оюун ухааны хөгжлийн сүүлийн үеийн дэвшлүүдийг дагаж мөрдөхөд хүндрэлтэй байгаа талаар дурдсан. Эдгээр оролцогч талууд онц чухал мэдээлэлтэй харьцаж, стратегийн шийдвэр гаргах үүрэгтэй тул тэдний кибер аюулгүй байдлын ойлголтыг сайжруулах нь үндэсний кибер аюулгүй байдлын төлөвшлийг хөгжүүлэх тэргүүлэх чиглэл байх ёстой. Жишээлбэл, байгууллагын удирдлагуудын кибер аюулгүй байдлын мэдлэгийн түвшин бага байх нь төсвийн хуваарилалтад ноцтой нөлөө үзүүлдэг. Үүний үр дүнд мэдээллийн аюулгүй байдал, кибер аюулгүй байдлын санаачилгуудыг хэрэгжүүлэх төсөв нэмүүлэх саналууд ихэвчлэн батлагддаггүй. Кибер аюулгүй байдлын мэргэжилтнүүд төсвөө нэмэгдүүлэх, шинэ техник хэрэгсэл худалдан авах хүсэлт

хүргүүлэхэд удирдлага болон санхүүгийн хэлтсээс татгалзах нь түгээмэл байдаг талаар мэдээлсэн. Одоогийн санхүүгийн процессуудад кибер аюулгүй байдлын тусдаа ангилал байхгүй нь уг асуудлыг улам даамжруулж байгаа бөгөөд энэ талаар 5.2-р хүчин зүйлд дэлгэрэнгүй оруулсан.

Ерөнхийдөө, цахим аюулгүй байдал болон мэдээлэл хамгаалалтыг зөвхөн мэдээллийн технологийн мэргэжилтнүүд бус, төрийн байгууллагын бүх ажилтны хариуцлага гэж үзэх соёл, хандлагын өөрчлөлт хийх шаардлагатай байна. Улсын хэмжээнд цахим системүүдийг бүрэн хамгаалахад шаардагдах ажлын цар хүрээг харгалзан үзвэл зөвхөн томилогдсон кибер аюулгүй байдлын мэргэжилтнүүд энэ асуудлыг дангаар нь шийдвэрлүүлэх боломжгүйг хүлээн зөвшөөрөх нь зүйтэй. Байгууллагын кибер аюулгүй байдлын мэргэжилтний тоог нэмснээр асуудлыг бүрэн шийдэж чадахгүй бөгөөд бусад ажилтнууд өөрсдийн хамтарсан үүрэг, хариуцлагаа ойлгож, кибер аюулгүй байдлын мэдлэг, ур чадвараа сайжруулах зайлшгүй шаардлагатай. Энэхүү сорилтыг шийдвэрлэхийн тулд удирдах албан тушаалтнуудад зориулсан мэдлэг олгох цогц хөтөлбөр болон тогтмол мэдээллийн уулзалт зохион байгуулах арга хэмжээг авч үзэх нь зүйтэй.

Кибер аюулгүй байдлын мэдлэг, чухалчлах байдал нь ялгаатай түвшинд байгаатай адил, аюулгүй байдлын аюулгүй байдлын зөв дадал зуршлыг хэрэгжүүлэх байдал ч мөн адил хувьсамтгай, жигд бус түвшинд байна. 2021 онд батлагдсан *Кибер аюулгүй байдлын тухай хуулийн* дагуу, ОЧМДБ байгууллагад жил бүр мэдээллийн аюулгүй байдлын аудит, хоёр жил тутам кибер аюулгүй байдлын эрсдэлийн үнэлгээг хөндлөнгийн зөвшөөрөл бүхий үйлчилгээ үзүүлэгч байгууллагаар хийлгэж, зөвлөмжийг нь хэрэгжүүлэх ёстой. Мөн Кибер аюулгүй байдлын нийтлэг журмын шаардлагыг дагаж мөрдөх үүрэгтэй бөгөөд энэ талаар 4.1-р хүчин зүйлд дэлгэрэнгүй тусгасан. Бодит нөхцөл байдалд эдгээр шаардлагын хэрэгжилт бүрэн хангагдаагүй бөгөөд ОЧМДБ байгууллагуудын дагаж мөрдөх байдал жигд бус байна. Зарим ОЧМДБ байгууллагууд эхний эрсдэлийн үнэлгээгээ хийлгэж, зөвлөмжийг хэрэгжүүлэн, анхны мэдээллийн аюулгүй байдлын аудитад бэлдэж байгаа бол бусад байгууллагын хувьд тавиглаж буй шаардлага, эдгээрийг хэзээ хэрэгжүүлсэн байх талаар ойлголтгүй хэвээр байна. Хувийн хэвшлийн дунд санхүүгийн байгууллага болон интернет үйлчилгээ үзүүлэгчид кибер аюулгүй байдлын практикийг хэрэгжүүлэх чиглэлээр тэргүүлж байна. Эдгээр байгууллагуудын аргачлал ижил биш ч ихэнх нь олон улсын стандарт, зохицуулалтын шаардлагыг хангахын тулд аюулгүй кибер аюулгүй байдлын практикуудыг нэвтрүүлсэн байна. (Энэ талаар 5.2-р хүчин зүйлд дэлгэрэнгүй хэлэлцсэн.)

Голллох бүлгийн хэлэлцүүлгийн үеэр тэргүүлэх цөөн тооны оролцогч талуудаас бусад нийт хэрэглэгчдийн ихэнх нь кибер аюулгүй байдлын зөв дадал зуршлыг мөрдөхгүй байгаа нь илэрхий байв. Түгээмэл гарч буй тааруухан практикт нууц үгийн зохисгүй хэрэглээ, ажлын байранд хувийн имэйл болон мессежийн програм ашиглан албан мэдээлэл солилцох, давхар шатлалт баталгаажуулалтын арга (2FA) ашиглахгүй байх зэрэг асуудлууд багтаж байна. Нийгмийн инженерчлэл /social engineering/ болон фишинг (phishing) халдлагын тохиолдлуудыг авч үзвэл хэрэглэгчид аюулгүй байдлын зөв дадлуудыг хэрэгжүүлэхгүй байгаагийн нэг илрэл юм. Монгол Улсад цахим залилан өндөр түвшинд байгаагаас гадна кибер гэмт хэргийн өсөлт нэмэгдэж буй нь иргэдийн хувьд кибер аюулгүй байдлын сайн туршлагуудыг дагаж мөрдөхгүй байгааг харуулж байна.

D 2.2 ОНЛАЙН ҮЙЛЧИЛГЭЭНД ИТГЭХ ИТГЭЛ

Энэхүү хүчин зүйл нь кибер орчинд шаардлагатай чухал ур чадварууд, худал мэдээллийг удирдах чадамж, хэрэглэгчдийн ерөнхий цахим үйлчилгээ, тэр дундаа цахим засаг болон цахим худалдааны үйлчилгээнд хэрэглэгчдийн итгэл, найдварыг хэр зэрэг хүлээж байгааа түвшинг үнэлэхэд чиглэнэ.

Түвшин: **Эхлэх түвшнээс Хөгжиж буй түвшинд**

Монгол Улсад цахим ур чадвартай интернет хэрэглэгчдийн тоо нэмэгдэж байгаа бөгөөд эдгээр хэрэгчлэгчид өдөр тутмын амьдралдаа цахим нийгмийн платформ болон цахим үйлчилгээг тогтмол ашиглаж байна. Хэрэглэгчийн цахим холболтыг хангасан найдвартай мэдээлэл, харилцаа холбооны дэд бүтэц энэ үйл ажиллагааг дэмжин боломжтой болгож байна. (5.4-р хүчин зүйлд дэлгэрэнгүй тайлбарласан). Цахим болон хэвлэл мэдээллийн боловсролын ур чадварыг хөгжүүлэх хэд хэдэн хөтөлбөр хэрэгжиж байна. Үүнд Монгол Улсын бага, дунд сургууль болон мэргэжлийн боловсролын төвүүдэд идэвхтэй хэрэгжиж буй сургалтын хөтөлбөрүүд, НҮБ-ын Хөгжлийн Хөтөлбөр (UNDP[29]), ЮНЕСКО[30] зэрэг олон улсын хөгжлийн түнш байгууллагуудтай хамтарсан санаачилга, И-Монголиа Академи[31]-аар дамжуулан төрийн албан хаагчдад зориулсан тусгай сургалтууд багтаж байна. Өндөр түвшний интернет холболт болон өргөн хүрээний цахим ур чадвар олгох боломжууд хосолсноор интернет ашиглалтын хувьд итгэлтэй хэрэглэгчдийн тоо өсөн нэмэгдэж байна. Цахим үйлчилгээний талаарх хэрэглэгчдийн итгэлтэй байдлын түвшинг цахим ур чадварын түвшин, хэрэглэгчдийн цахим орчин дахь үйл ажиллагаа болон цахим чадамж зэрэг үзүүлэлтүүдийг харуулсан богино хугацааны үнэлгээгээр албан бусаар тодорхойлсон. Эдгээр үнэлгээнд НҮБ-ын Хөгжлийн Хөтөлбөрийн (UNDP) Монгол дахь Хурдасгуур Лаб[32], НҮБ-ын Худалдаа, хөгжлийн бага хурал (UNCTAD[33]), Дэлхийн банк[34] зэрэг байгууллагуудын судалгаа багтана. Дэлхийн банкны Global Findex Database 2021 тайланд Монгол Улсын хүн амын 99% нь гар утас ашиглах боломжтой, 97% нь цахим төлбөр хүлээн авч, гүйцэтгэдэг, 93% нь онлайнаар төлбөр хийсэн үзүүлэлтүүд дурдагдсан. Эдгээр цахим эдийн засгийн үйл ажиллагааны дийлэх хувь нь дотоодын зах зээлд өрнөж байгаа бөгөөд цахим худалдаа, цахим засаглалын үйлчилгээгээр дамжин хэрэгжиж байна. Үүнд онлайн банк, жижиглэн худалдаа, арга хэмжээний тасалбар борлуулалт, бизнесийн үйлчилгээ, мөн төрийн олон зуун үйлчилгээг үндэсний хэмжээнд хүргэдэг И-Монгол платформ багтаж байгаа бөгөөд монголын хүн ам нийтээрээ ашиглаж байна. Цахим засаглал нь Монгол Улсын Засгийн газрын стратегийн тэргүүлэх чиглэл бөгөөд "Цахим үндэстэн[35]" (E-Nation) болох зорилготой "Алсын хараа-2050" үндэсний хөгжлийн төлөвлөгөөний хүрээнд хөгжүүлж байна. Цахим засаглалын үйлчилгээний хөгжлийг олон улсын түншүүд, тэр дундаа

29 https://www.undp.org/mongolia/blog/experimenting-learning-and-innovating-improve-digital-inclusivity-and- literacy-mongolia

30 https://www.unesco.org/en/articles/ministry-education-unesco-and-icdl-asia-launches-teachers-digital-skills- training-pilot-project

31 https://blog-pfm.imf.org/en/pfmblog/2023/02/e-governance-and-e-treasury-systems-advance-in-mongolia

32 https://www.undp.org/mongolia/blog/iterating-mongolian-version-digital-literacy

33 https://unctad.org/publication/mongolia-etrade-readiness-assessment

34 https://www.worldbank.org/en/publication/globalfindex/Data

35 https://www.telecomreviewasia.com/news/interviews/2791-mongolia-to-take-digital-development-to-a-new- level/

Дэлхийн банк[36], Азийн хөгжлийн банк[37] зэрэг байгууллагууд идэвхтэй дэмжиж байна. Цахим үйлчилгээг хариуцагч хувийн болон төрийн байгууллагын гол оролцогч талууд аюулгүй байдлыг өндөр түвшинд хангасан байх шаардлагатайг хүлээн зөвшөөрдөг бөгөөд ОЧМДБ байгууллагуудын хувьд энэ нь хууль ёсны шаардлага юм (4.1-р хүчин зүйлд дурдсан). Үүний зэрэгцээ системийн аюулгүй байдал нь байгууллагын удирдлага, менежментээс хамаарч байдаг тул зарим байгууллага бусадтайгаа харьцуулбал илүү өндөр түвшинд аюулгүй байдлын хяналтыг хэрэгжүүлсэн байна. (5.2-р хүчин зүйлд дэлгэрэнгүй тайлбарласан). Монгол Улсын Засгийн газар 2021 оны Цахим гарын үсгийн тухай хуулийг хэрэгжүүлснээр цахим гүйлгээнд итгэх итгэлийг нэмэгдүүлэх, аюулгүй байдлын хяналтыг сайжруулах арга хэмжээнүүдийг авч хэрэгжүүлсэн. Цахим ур чадвар, технологийн хэрэглээний талаарх судалгаанууд хийгдсэн боловч цахим худалдаа болон цахим засаглалын үйлчилгээнд итгэх итгэлийг тодорхойлсон судалгаа одоогоор хийгдээгүй байна.

Хэрэглэгчийн түвшинд, Монгол Улсад цахим ур чадварын түвшин өндөр, цахим үйлчилгээг ашиглах байдал түгээмэл хэдий ч кибер аюулгүй байдлын зөв дадал хэвшлийг тогтмол мөрдөх, цахим орчинд өөрсдийгөө хамгаалах арга замын талаарх хангалттай ойлголт байхгүй. Голлох бүлгийн хэлэлцүүлгээр энгийн хэрэглэгч хууль ёсны эсхүл хууль бус вэбсайт болон цахим үйлчилгээг хооронд нь ялгаж таних чадваргүйг тодорхойлсон. Зарим оролцогчид хэрэглэгчдийн энэ сул талыг “хэт итгэмтгий” эсхүл “цахим орчны мэдлэггүй” байдлаас үүдэлтэй байж болох юм гэж тайлбарласан. Кибер аюулгүй байдлын талаар мэдлэг, боловсрол сул байгаа нь Монгол Улсад цахим хөгжлийг тогтвортой ахиулахад томоохон сорилт, эрсдэл болж байна (2.1-р хүчин зүйлд дэлгэрэнгүй тайлбарласан). Голлох бүлгийн хэлэлцүүлгээр хот, хөдөө орон нутгийн иргэдийн дунд цахим үйлчилгээний хэрэглээний ялгаа байгааг онцолсон. Хөдөө орон нутгийн иргэд цахим үйлчилгээг харьцангуй бага ашигладаг бөгөөд энэ нь сүлжээний холболтын хомсдолоос бус, харин шинэ цахим үйлчилгээг хэрхэн ашиглах мэдээллийг хангалттай авч чаддаггүйтэй холбоотой гэж үзсэн. Ерөнхийд нь авч үзвэл, Монголчуудын дунд хөдөө орон нутгийн иргэд болон бусад эмзэг бүлгийн хүмүүс цахим орчинд өөрсдийгөө хамгаалах ур чадвар хамгийн бага түвшинд байдаг гэсэн ойлголт түгээмэл байна.

Голлох бүлгийн хэлэлцүүлгээр Монгол Улсад худал болон төөрөгдүүлсэн мэдээлэл (mis- & disinformation) цахим платформоор дамжин илүү хурдтай тархаж байгаа нь одоогийн тулгамдсан асуудал болоод буйг онцолсон. Энэхүү асуудлыг шийдвэрлэхийн тулд иргэний нийгмийн тэргүүлэх байгууллагууд болон төрийн бус байгууллагууд тодорхой алхмуудыг хийж байна. Тухайлбал, Сэтгүүл зүйн инновац, хөгжлийн "Nest" төв 2023 онд баримт шалгах сүлжээ[38] байгуулж, Монгол Улсын иргэдэд буруу мэдээллийн эсрэг хэрэгцээтэй эх сурвалжийг олгох зорилгоор ажиллаж эхэлсэн. Өнөөдөр "Монголын браимт шалгах төв[39]" хэмээн нэрлэгдэж буй уг байгууллага нь Олон улсын баримт шалгах сүлжээ (International Fact Checking Network, IFCN)-ээс албан ёсны батламж авсан Монгол Улс дахь цорын ганц байгууллага юм. Эдгээр хүчин чармайлтаас гадна энэ чиглэлээр төр болон цахим платформ үйлчилгээ үзүүлэгчдийн зүгээс илэрхий бодлогын арга хэмжээ авч байгаа талаар ажиглагдаагүй. Онлайн орчинд худал болон төөрөгдүүлсэн мэдээллийг шийдвэрлэх талаар одоогоор төрийн стратегийн баримт бичгүүдийн алинд нь ч тусгагдаагүй байна.

---

36 https://www.worldbank.org/en/news/press-release/2022/06/06/mongolia-new-project-helps-the-government-go-digital-and-grow-the-economy

37 https://www.adb.org/sites/default/files/project-documents/55211/55211-001-tar-en.pdf

38 https://www.nestmongolia.org/facts-first-mongolia-7

39 https://meedan.com/post/meedan-and-nest-center-launch-mongolias-first-fact-checking-tipline

D2.3 ХУВИЙН МЭДЭЭЛЛИЙГ ОНЛАЙН ОРЧИНД ХАМГААЛАХ ТАЛААР ХЭРЭГЛЭГЧДИЙН ОЙЛГОЛТ

Энэхүү хүчин зүйл нь интернет хэрэглэгчид болон төр, хувийн хэвшлийн оролцогч талууд цахим орчинд хувийн мэдээллээ хамгаалах шаардлагатайг хэрхэн хүлээн зөвшөөрч, ойлгож байгаа эсэхийг үнэлнэ. Мөн өөрсдийн хувийн мэдээллийн нууцлалтай холбоотой эрхийн талаарх мэдлэгтэй эсэх**,** эрхээ хэрхэн хамгаалах талаар ойлголт бий эсэхийг үнэлнэ.

Түвшин: Хөгжиж буй түвшнээс Тогтворжсон түвшинд

Монгол Улсын үндсэн хуулиар хувийн нууц нь Монгол Улсын иргэдийн суурь хүний эрх гэж тодорхойлогдсон. Монгол Улсад хувийн мэдээллийн нууцлалыг хамгаалах бат бөх эрх зүйн зохицуулалт үйлчилж байгаа бөгөөд үүнд 2021 оны *Хүний хувийн мэдээлэл хамгаалах тухай хууль* голлох үүрэгтэй (4.2-р хүчин зүйлд дэлгэрэнгүй тайлбарласан). Энэхүү хууль нь хувийн мэдээллийг цуглуулах, боловсруулах, ашиглах, аюулгүй байдлыг хангах зохицуулалтыг тодорхойлсон бөгөөд бүх "Мэдээлэл хариуцагч" байгууллагууд дагаж мөрдөх ёстой. Хууль нь биет болон цахим орчинд адилхан үйлчилдэг. Эдгээр зохицуулалтын хүрээнд Мэдээлэл хариуцагч бүх байгууллага дотооддоо мэдээлэл цуглуулах, хянах, хамгаалах бодлого баталж, хэрэгжүүлэх үүрэгтэй. 2022 оноос хойш хүчин төгөлдөр мөрдөгдөж эхэлснээр, эдгээр бодлогыг Монголын улсад үйл ажиллагаа явуулж буй байгууллагууд өргөнөөр нэвтрүүлж эхэлсэн. Цахим хөгжил, инновац, харилцаа холбооны яам (ЦХИХХЯ) болон Үндэсний хүний эрхийн комисс нь уг хуулийн хэрэгжилтийг хянах үүрэгтэй. Аюулгүй байдал болон нууцлалын тэнцвэрийг хадгалах тодорхой зохицуулалтуудыг тус хуульд нарийвчлан тодорхойлсон. Монгол Улсад аюулгүй байдал болон хүний эрхийг хамгаалах асуудлыг тэнцвэржүүлэх талаар нээлттэй, өргөн хүрээний хэлэлцүүлэг тогтмол зохион байгуулагддаг. Эдгээр хэлэлцүүлгийн үеэр цахим эрх болон аюулгүй байдлын хамгаалалт зэрэг асуудлууд ч хөндөгдөж байсан. Мөн бүлгийн хэлэлцүүлгийн үеэр орон нутгийн иргэдийн санаа бодол, байр суурийг хэлэлцүүлсэн.

Хэрэглэгчийн түвшинд, хүмүүс өөрсдийн хувийн мэдээллийг онлайн орчинд хамгаалахад ямар арга хэмжээ авах ёстойгоо мэддэггүй. Бүлгийн хэлэлцүүлгээс үзэхэд төр болон хувийн хэвшлийн зарим хэрэглэгч, оролцогч талууд цахим өгөгдөл хэрхэн хадгалагддаг, мөн өөрсдийн мэдээллийг хэрхэн илүү сайн хамгаалж болох талаар хязгаарлагдмал ойлголттой байв. Харин энэ талын гүнзгий мэдлэг нь цөөн тооны мэдээлэл сайтай цөөнх бүлгийн хүрээнээс хэтрэхгүй байна. Соёлын хувьд, Монголын нийт хүн ам цахим орчинд тэдний мэдээлэл хэрхэн ашиглагдаж буйг төдийлөн мэдэхгүй байхаас гадна хууль тогтоомжид заасан өөрсдийн хувийн мэдээллийн нууцлалтай холбоотой эрхийн талаар ерөнхийдөө мэдлэг муутай байдаг. Бодит байдалд, Монголын интернэт хэрэглэгчдийн цөөн хэсэг нь кибер аюулгүй байдлыг дадал болгон мөрддөг бөгөөд ихэнх нь онлайн мэдээллээ хамгаалахын тулд шаардлагатай алхмыг авч чаддаггүй.

D 2.4 ТАЙЛАГНАХ МЕХАНИЗМ

Энэхүү хүчин зүйл нь интернет орчинд гэмт хэргийг мэдээлэх механизм байгаа эсэх, мэдээлэх суваг ажиллаж байгааг судлахад оршино. Уг суваг нь цахим залилан, кибер дээрэлхэлт, хүүхдийн эсрэг цахим гэмт хэрэг, хувийн мэдээлэл хулгайлах, нууцлал болон аюулгүй байдлын зөрчил, бусад төрлийн зөрчлүүдийг мэдээлэх суваг агуулна.

Түвшин: **Эхлэл түвшнээс Хөгжиж буй түвшинд**

Монгол Улсад кибер аюулгүй байдлын зөрчил, кибер гэмт хэрэг болон бусад цахим хохиролыг мэдээлэх механизм бүрдсэн бөгөөд тодорхой түвшинд зохицуулалттайгаар ажиллаж байна. 2021 оны *Кибер аюулгүй байдлын тухай хуулий*н хүрээнд Цагдаагийн ерөнхий газар (ЦЕГ), Кибер халдлага, зөрчилтэй тэмцэх Үндэсний болон Нийтийн төвүүд нь өөрсдийн харьяа салбараас кибер гэмт хэрэг, кибер халдлага болон бусад зөрчлийн мэдээлэл хүлээн авах үүрэгтэй. Үүнд:

- Цагдаагийн ерөнхий газар (ЦЕГ) – ихэвчлэн олон нийтээс мэдээлэл хүлээн авдаг.
- Үндэсний төв – төрийн байгууллагуудтай харилцдаг.
- Нийтийн төв – хувийн хэвшлийн онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудтай ажилладаг.

Оролцогч талууд эдгээр мэдээлэх механизмын талаар мэдээлтэлтэй бөгөөд зарим нь тухайн харьяалагдах байгууллагадаа мэдээлэх процессыг дотоод зөрчлийн хариу арга хэмжээний журамд албан ёсоор тусгасан гэж мэдэгдсэн. Эдгээр байгууллагаас гадна, И-Монгол платформ хүүхэд хамгааллын зөрчил мэдээлэх механизмтай[40] бөгөөд цахим орчинд үйлдэгдсэн гэмт хэргийн үед ашиглана. Мөн хүүхэдтэй холбоотой гэмт хэргийг мэдээлэх тусгай утасны дугаар[41] ажилладаг. Арилжааны банкуудын хүрээнд хувийн мэдээлэх механизм ажиллаж байгаа бөгөөд энэ нь банк хооронд мэдээлэл солилцох боломжийг бүрдүүлдэг.

Олон талт оролцогчдын бүлгийн хэлэлцүүлгээр талууд мэдээлэл хүлээн авах, дамжуулах тогтолцоог хоорондоо илүү уялдаа холбоотой ажиллуулах хэрэгцээ, сонирхолтой байгааг бататгасан боловч одоогоор эдгээр механизм зохион байгуулалттайгаар ажиллаж чадахгүй байна. 2021 оны *Кибер аюулгүй байдлын тухай хуулийн* 20.3 дугаар зүйлд Нийтийн төв нь Үндэсний төвтэй кибер халдлага болон зөрчлийн талаар мэдээлэл солилцох үүрэгтэй гэж заасан боловч мэдээлэл солилцоо тогтмол бус, нөхцөл байдлаас хамаарсан байдлаар явагдаж байна. Зарим оролцогч тал хэрэглэгчдийг мэдээлэх механизм ашиглуулахад хүндрэлтэй байгааг онцолсон бөгөөд ялангуяа хүүхдүүдийн хувьд энэ асуудал илүүтэй ажиглагдсан. Ичих мэдрэмж болон мэдлэгийн хомсдол нь хэрэглэгчид зөрчлийн талаар мэдээлэхээс зайлсхийх гол шалтгаан байх талтай гэж үзэж байна. Хэрэглэгчид кибер аюулгүй байдлын инцидентүүдийн талаар бие биедээ мэдээлэх зорилгоор олон нийтийн сүлжээний сувгуудыг ашигладаг гэх нотолгоо хомс байна.

Мэдээлсэн зөрчлийн тоо, төрөл зэрэг хэмжүүрт үзүүлэлтүүдийн талаарх мэдээлэл олдоц ерөнхийдөө муу байв. Гэсэн хэдий ч, 2021 оны *Кибер аюулгүй байдлын тухай* хуулийн

[40] https://www.ekids.mn/#/index

[41] https://108.mn

дагуу Үндэсний төв нь Кибер аюулгүй байдлын зөрчлийн мэдээллийн санд кибер халдлага болон зөрчлийн мэдээллийг бүртгэж, тогтмол шинэчлэх үүрэгтэй. Энэ нь мэдээлсэн зөрчлүүдийн тодорхой хэмжүүрүүд бүрдэж буйг илтгэх нэг үзүүлэлт болж байна.

D 2.5 ХЭВЛЭЛ МЭДЭЭЛЭЛ БОЛОН ОНЛАЙН ПЛАТФОРМУУД

Энэхүү хүчин зүйл нь кибер аюулгүй байдал олон нийтийн мэдээллийн хэрэгслээр тогтмол хөндөгддөг сэдэв эсэх, мөн нийгмийн сүлжээнд өргөн хүрээний хэлэлцүүлдэг асуудал мөн эсэхийг судална. Түүнчлэн хэвлэл мэдээллийн хэрэгслүүд олон нийтэд кибер аюулгүй байдлын талаарх мэдээллийг хэрхэн хүргэж байгааг үнэлэх бөгөөд энэ нь иргэдийн кибер аюулгүй байдлын үнэт зүйлс, хандлага, цахим орчин дахь зан төлөвт хэрхэн нөлөөлж буйг тодорхойлоход чиглэгдэнэ.

Түвшин: Хөгжиж буй түвшинд

Уламжлалт болон цахим хэвлэл мэдээллийн хэрэгслүүд кибер аюулгүй байдлын сэдвийг тогтмол бус ч үе үе хөндөж нийтэлдэг. Үүнд олон улсын Кибер аюулгүй байдлын сар, кибер аюулгүй байдлын арга хэмжээ, бодлогын өөрчлөлт, кибер гэмт хэргийн тохиолдлууд зэрэг[42] багтана. Зарим тохиолдолд, хэвлэл мэдээллийн хэрэгслээр уншигч, үзэгчдэд зориулан цахим орчинд өөрийгөө хамгаалахад хэрэгтэй урьдчилан сэргийлэх, хэрэгжүүлж болохуйц кибер аюулгүй байдлын арга хэмжээг мэдээлэл болгон хүргэдэг. Бүлгийн хэлэлцүүлгээр хэвлэл мэдээллийн хэрэгслээр кибер аюулгүй байдлын сэдвийг үе үе хөнддөг боловч ихэнх сэтгүүлчдийн хувьд тус сэдэв өндөр ач холбогдолтойд тооцогдоггүй байх гэсэн таамаглалтай байна. Түүнчлэн, оролцогч талуудын зүгээс хэвлэл мэдээллийн байгууллагууд кибер аюулгүй байдлын мэдээлэл, сурталчилгааны компанит ажилд идэвхтэй оролцдоггүй нь улсын хэмжээнд нийт иргэдийн кибер аюулгүй байдлын ойлголтыг сайжруулахад саад болж байгаа гэж үзсэн.

2.4-р хүчин зүйлд дурдсанчлан, кибер аюулгүй байдлын зөрчлийн талаар нийгмийн сүлжээг ашиглан хэлэлцэх нь хязгаарлагдмал байна. Интернет хэрэглэгчид кибер аюулгүй байдлын асуудлыг сэтгүүлчдийн адил чухалд авч үздэггүй. Гэсэн хэдий ч, кибер аюулгүй байдлын талаарх олон нийтийн ойлголтыг нэмэгдүүлэх зорилгоор байгууллагууд нийгмийн сүлжээг ашиглан кампанит ажил өрнүүлсэн тохиолдлуудыг баримтжуулсан байна.

Монгол Улсад шүгэл үлээгч/мэдээлэгч (whistleblower)-ийг хүлээн зөвшөөрөх эрэг хандлага төлөвшсөн байдаг. Энэхүү соёл нь Монгол Улсын ардчилал төлөвшихийн хэрээр улам бүр хөгжиж ирсэн. Одоогоор мэдээлэгчийг хамгаалах тухай хуулийг[43] Монгол Улсын парламентаар хэлэлцүүлж байгаа бөгөөд уг хууль батлагдсанаар энэ соёлыг албан ёсоор хуульчлах боломж бүрдэх юм. Гэсэн хэдий ч уг хуулийн хэрэгжүүлэх явц удааширснаас гадна жагсагчид, хэвлэлийн эрх чөлөөг хамгаалах байдал суларч

[42] https://www.zindaa.mn/3hh1
https://news.mn/r/2373711/?fbclid=IwY2xjawG6fJ5leHRuA2FlbQIxMQABHZjlsohDaTlb_geFXBXNPOhjVkshaxx4SYMufxrxkN4kMYcqTtS5vFfb_w_aem_aEn7mV15PrsgdCCbE1DSdw

[43] https://montsame.mn/en/read/316173

байгаа нь Монгол Улсад эерэг мэдээлэгчийн соёл төлөвших үйл явцад сөрөг нөлөө үзүүлж болзошгүй гэж зарим талууд санаа зовниж байна[44].

[44] https://uncaccoalition.org/uncacparallelreportmongolia/

ЗӨВЛӨМЖ

Хэлэлцүүлгийн үр дүнд үндэслэн, Кибер аюулгүй байдлын соёл, нийгмийн төлөвшлийн түвшинг сайжруулахтай холбоотой дараах зөвлөмжийг санал болгож байна. Эдгээр зөвлөмжүүд нь Дэлхийн Кибер Аюулгүй Байдлын Чадамжийн Төвийн (GCSCC) Чадавхын Төлөвшлийн Загварын хүрээнд Монгол Улсын кибер аюулгүй байдлын чадавхыг сайжруулах, цаашдын боломжит алхмуудыг тодорхойлох зорилготой болно.

КИБЕР АЮУЛГҮЙ БАЙДЛЫН СЭТГЭЛГЭЭ

R2.1.1 Кибер аюулгүй байдлын талаарх нийтлэг ойлголтыг сайжруулах, уг асуудлыг тэргүүлэх чиглэлд авч үзэхийн тулд **R3.1.1** болон **R3.3.1**-д тусгагдсан мэдлэг олгох, сургалт зохион байгуулах арга хэмжээг хэрэгжүүлэх. Ялангуяа байгууллагын удирдлага, төрийн албан хаагчид, онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын ажилтнууд болон эмзэг бүлгийн кибер аюулгүй байдлын мэдлэгийг сайжруулахтай тусгай арга хэмжээг багтаах.

R2.1.2 Монгол Улсын төрийн албан хаагчдын дунд кибер аюулгүй байдлын мэдлэг, ур чадварыг дээшлүүлэх зорилготой цахим сургалт үнэлгээний портал хөгжүүлэх. Уг портал нь кибер аюулгүй байдлын соёлыг төлөвшүүлж, үндэсний болон байгууллагын стандартад нийцлийг хангах үүднээс тухайн хүний үүрэг, хариуцлагад тохируулсан сургалт, интерактив модуль болон үнэлгээний хэрэгслүүдийг агуулсан байх ёстой.

R2.1.3 Кибер аюулгүй байдлын хяналтыг хэрэгжүүлэх, хэрэглэгчдийн кибер аюулгүй байдлын дадал, практикийг сайжруулахын тулд **R5.2**-т тусгагдсан аюулгүй байдлын хяналтын арга хэмжээнүүдийг хэрэгжүүлэх. Кибер аюулгүй байдлын дадал зуршлыг төрийн албанд сайжруулахын тулд аюулгүй байдлын үйл ажиллагааны журам болон Зохистой хэрэглээний бодлогыг ашиглах боломжтойг анхаарч үзэх хэрэгтэй.

R2.1.4 Монгол Улсын тэргүүлэгч кибер аюулгүй байдлын оролцогч талууд үндэсний кибер аюулгүй байдлын илүү тогтвортой сэтгэлгээг төлөвшүүлэхийн тулд байгууллага, хэрэглэгчид алдаа дутагдал, бие биенээсээ суралцахыг уриалсан, оролцогч талуудын хамтын ажиллагаа, уялдаа холбоог урамшуулсан өсөлтөнд чиглэсэн сэтгэлгээг кибер аюулгүй байдлын экосистемд төлөвшүүлэх арга хэмжээ авах хэрэгтэй.

R2.1.5 Хэрэглэгч, төр болон хувийн сектор дахь хандлагын талаар бүрэн ойлголт авахын тулд хэмжүүрийг тодорхойлж, судалгаа явуулах.

ОНЛАЙН ҮЙЛЧИЛГЭЭНД ИТГЭХ ИТГЭЛ

R2.2.1 И-Монгол Академи, RAGDS болон Нийтийн төв зэрэг оролцогч талуудыг дэмжихэд хөрөнгө оруулалт хийх, ингэснээр цахим ур чадвар олгох сургалтуудыг үргэлжлүүлэн зохион байгуулах, цахим засаглал болон цахим худалдааны үйлчилгээний хүртээмжийг сайжруулах боломжтой болно. Ялангуяа нийгмийн эмзэг бүлэг болон хөдөө орон нутгийн иргэдийг хамруулахад анхаарах. Энэхүү санаачилгыг **R3.3.1**-д санал болгосон өргөн хүрээний сургалтын хөтөлбөр болон **R3.1.1**-д тусгасан кибер аюулгүй байдлын мэдлэг олгох үйл ажиллагаатай уялдуулан зохион байгуулах.

R2.2.2 **R3.1.1**-д тусгагдсан мэдлэг олгох санаачилга болон **R2.2.1**-д дурдсан цахим ур чадвар олгох сургалтын хөтөлбөрт худал (misinformation) болон төөрөгдүүлсэн мэдээлэл (disinformation)-ийн модуль нэгтгэх.

R2.2.3 **R3.1.1**-д тусгагдсан мэдлэг олгох санаачилга болон **R2.2.1**-д дурдсан цахим ур чадвар олгох сургалтын хөтөлбөрт мэдээлэл, хэвлэл мэдээллийн боловсролын (media and information literacy) модулиудыг нэгтгэх. Эдгээр модулиуд нь иргэдэд онлайн мэдээлэлд шүүмжлэлтэй хандаж үнэлэх, хэт нэг талыг барьсан эсхүл худал агуулгыг таних, хэвлэл мэдээлэл олон нийтийн ойлголтод хэрхэн нөлөөлдөг талаар ойлгох чадварыг эзэмшүүлэх зорилготой байна.

R2.2.4 Цахим засаглалын аюулгүй байдлын тогтолцоог сайжруулах арга хэмжээг хэрэгжүүлэх, ингэснээр цахим залилан, кибер гэмт хэргийн эрсдэлийг бууруулах боломжтой болно. Эдгээр арга хэмжээг **R5.2**-т тусгагдсан аюулгүй байдлын хяналтын арга хэмжээнүүдтэй уялдуулан хэрэгжүүлэх.

R2.2.5 Цахим орчин дахь итгэх түвшнийг судлах үндэсний хэмжээний судалгаа зохион байгуулах. Судалгааны үр дүнг ашиглан цахим системд итгэх итгэлийг нэмэгдүүлэх, интернетийн аюулгүй байдлын мэдлэгийг сайжруулахад чиглэсэн бодлого, санаачилгуудыг боловсруулахад чиглүүлэх. **R3.1.1**-д санал болгосон үйл ажиллагаатай уялдуулан зохицуулах.

ОНЛАЙН ОРЧИН ДАХЬ ХУВИЙН МЭДЭЭЛЛИЙГ ХАМГААЛАХ ХЭРЭГЛЭГЧИЙН ОЙЛГОЛТ

R2.3.1 **R4.1.10**-д тусгагдсан хүний эрхийн нөлөөллийн үнэлгээний хүрээнд, Монгол Улсын хүний хувийн мэдээллийн аюулгүй байдал болон кибер аюулгүй байдлын хууль тогтоомжийг хэрэглэгчийн нууцлалын эрхтэй уялдуулан тогтмол давтамжтай дахин үнэлэх. Аюулгүй байдал болон нууцлал хоорондын зохистой тэнцвэрийг хадгалах зорилгоор хууль, эрх зүйн тогтолцоог тогтвортой хянах, шаардлагатай тохиолдолд сайжруулах арга хэмжээг хэрэгжүүлэх.

R2.3.2 Интернет хэрэглэгчдийн цахим орчин дахь хувийн нууцтай холбоотой асуудал болон Монгол Улсын хуулиар хамгаалагдсан эрхийн талаарх мэдлэг, ойлголтыг аажмаар нэмэгдүүлэх арга хэмжээ хэрэгжүүлэх шаардлагатай. Эдгээр хүчин чармайлтыг **R3.1.1**-д тусгагдсан үндэсний хэмжээний кибер аюулгүй байдлын мэдлэг олгох санаачилгатай уялдуулан хэрэгжүүлэх боломжийг судлах.

ТАЙЛАГНАХ МЕХАНИЗМ

R2.4.1 Мэдээлэл солилцоо, зохицуулалтыг сайжруулахын тулд мэдээлэх механизм хариуцсан байгууллагын хооронд итгэлцэл, хамтын ажиллагааг нэмэгдүүлэх арга хэмжээг хэрэгжүүлэх.

R2.4.2 Интернет хэрэглэгч болон Үндэсний төв, Нийтийн төвийн харьяа байгууллагуудын дунд боловсруулсан мэдээлэх механизмын талаарх ойлголтыг нэмэгдүүлэх санаачилгуудыг хэрэгжүүлэх.

- Мэдээлэх асуудлын төрлөөс хамааран аль байгууллагад хандахыг тодорхой, ойлгомжтой болгох арга хэмжээг авах.
- Нийгмийн сүлжээ, телевиз, олон нийтийн мэдээллийн хөтөлбөр зэрэг олон сувгийг ашиглан хэрэглэгчдэд кибер аюулгүй байдлын зөрчил, мэдээллийн алдагдал, сэжигтэй үйл ажиллагааг хаана, хэрхэн мэдээлэх талаар мэдээлэл хүргэх боломжийг судлах.
- Мэдээлэх үйл явцыг хялбар, хүртээмжтэй, ил тод болгох замаар хэрэглэгчдийн оролцоог нэмэгдүүлэх.

R2.4.3 Мэдээлэх бүх сувгаар ирсэн мэдээллийг хэмжүүр, судалгаанд нэгтгэн цуглуулах замаар мэдээлэл хүлээн авалт, тайлагналын үйл ажиллагааны бүрэн дүр зураг бүрдүүлэлтийг хангах. Шаардлагатай тохиолдолд, мэдээлэх механизмаар дамжуулан цуглуулсан

мэдээллийг (нийт мэдээллийн тоо хэмжээ, мэдээлсэн зөрчлийн төрөл, хэрэглэгчдийн демографик мэдээлэл) ашиглан дараах чиглэлд сайжруулах боломжийг судлах:

- Кибер аюулгүй байдлын эрсдэл, зөрчлийн хандлагыг тодорхойлох
- Хариу арга хэмжээний стратегийг оновчтой болгох
- Олон нийтийн мэдлэг олгох кампанит ажил болон мэдээлэх механизмын үр нөлөөг үнэлэх

ХЭВЛЭЛ МЭДЭЭЛЭЛ БОЛОН ОНЛАЙН ПЛАТФОРМУУД

R2.5.1 Хэвлэл мэдээллийн хэрэгслээр зөвхөн томоохон кибер аюулгүй байдлын зөрчлийн мэдээллээр хязгаарлахгүйгээр кибер аюулгүй байдлын шилдэг туршлага болон хувь хүний кибер аюулгүй байдлын мэдлэгийг нэмэгдүүлэх агуулгаар мэдээлэл түгээхийг дэмжих. Үүнийг хэрэгжүүлэхийн тулд хэвлэл мэдээллийн байгууллагуудад кибер аюулгүй байдлын хөгжлийн талаар илүү гүнзгий ойлголт өгөх, мэдээ, нийтлэл бэлтгэхэд туслах нэмэлт эх сурвалжуудыг (жишээлбэл, хэвлэлийн мэдээ, удирдах албан тушаалтнуудын ярилцлага, арга хэмжээний урилгууд гэх мэт) бэлтгэж хүргэх боломжийг судлах.

R2.5.2 Хэвлэл мэдээллийн байгууллагуудыг **R3.1.1**-д тусгагдсан мэдлэг олгох санаачилгуудтай илүү стратегийн түвшинд нэгтгэх арга замуудыг судлах.

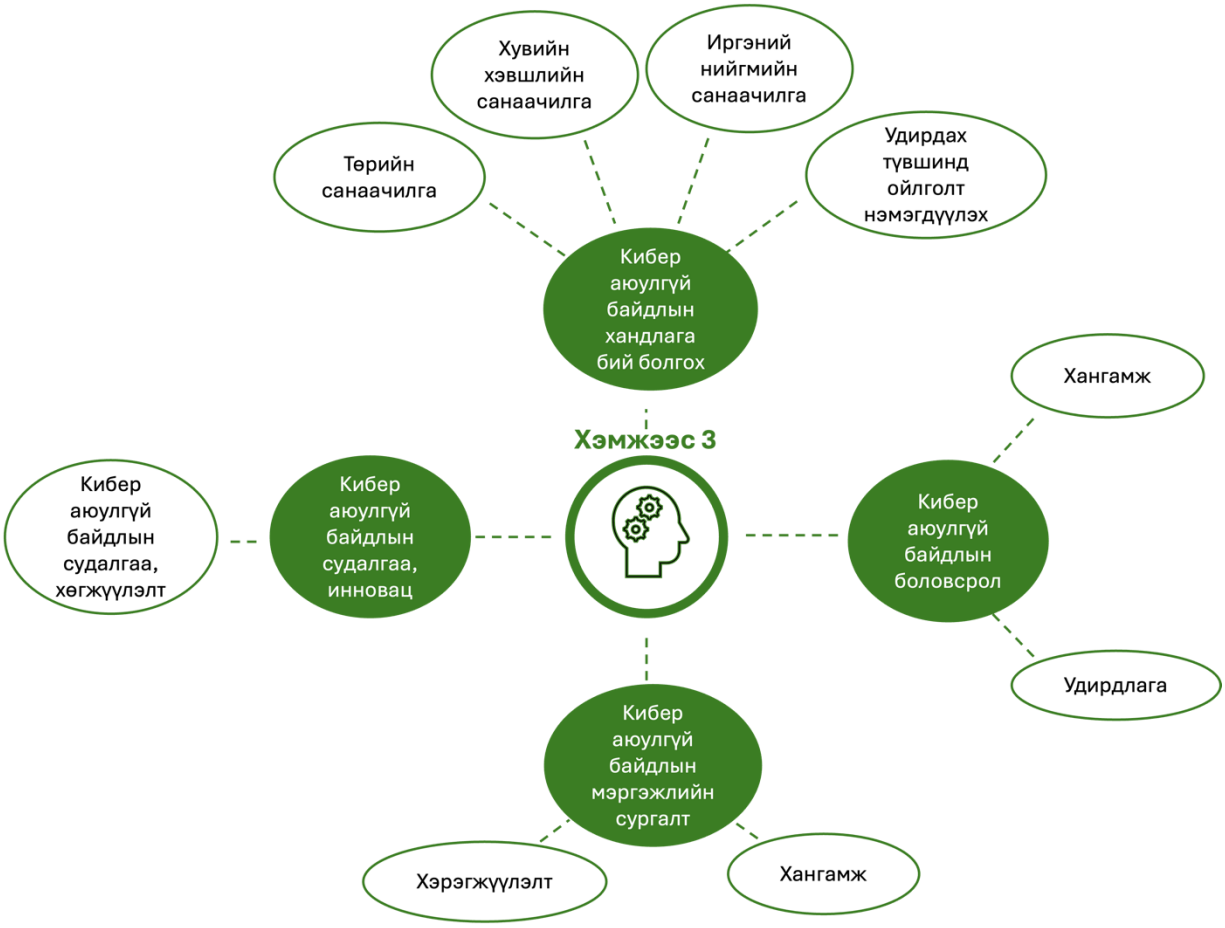
R2.5.3 Олон нийтийн сүлжээг кибер аюулгүй байдлын мэдлэгийн кампанит ажилд стратегийн хувьд хэрхэн холбох талаар авч үзэх **R3.1.1**.

R2.5.4 Мэдээлэгчийг хамгаалах тухай хуулийн төсөлд дахин хяналт хийж, түүнийг амжилттай батлах, хэрэгжүүлэх арга замуудыг судлах.

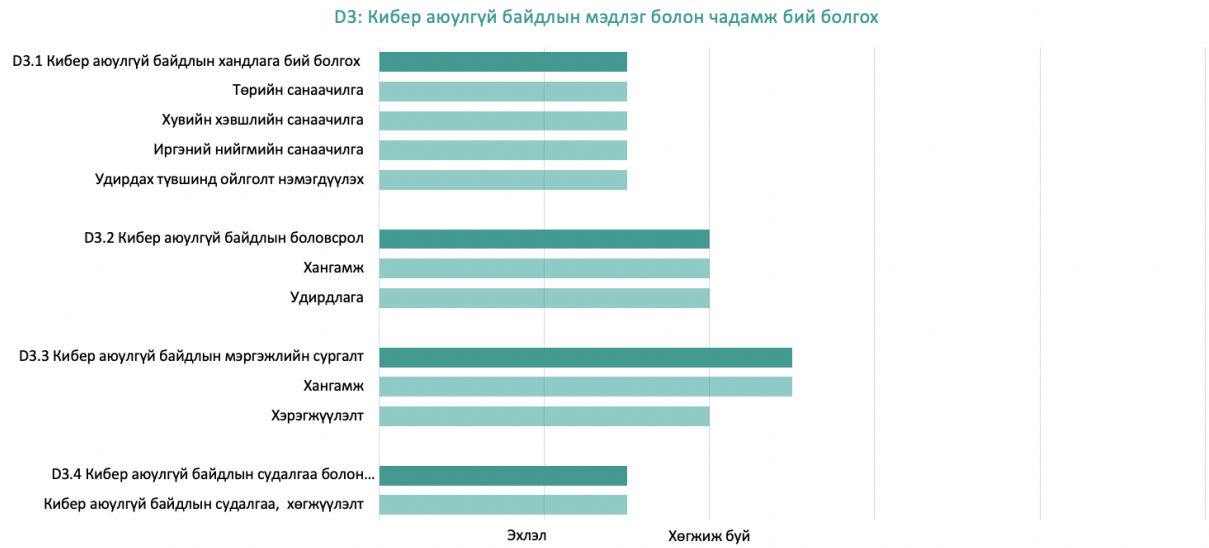
ХЭМЖЭЭС 3

КИБЕР АЮУЛГҮЙ БАЙДЛЫН МЭДЛЭГ БОЛОН ЧАДАМЖ БИЙ БОЛГОХ

Энэхүү хэмжээс нь төр, хувийн хэвшил болон нийт хүн ам зэрэг олон төрлийн оролцогч талуудад чиглэсэн хөтөлбөрүүдийн хүртээмж, чанар, хэрэгжилтийг үнэлнэ. Үүнд кибер аюулгүй байдлын талаарх мэдлэг олгох хөтөлбөрүүд, албан ёсны боловсролын хөтөлбөрүүд, мөн мэргэжлийн сургалтын хөтөлбөрүүд багтана.



ҮР ДҮНГИЙН ТОЙМ



D 3.1 КИБЕР АЮУЛГҮЙ БАЙДЛЫН ХАНДЛАГА БИЙ БОЛГОХ

Энэ хүчин зүйл нь улс орон даяар кибер аюулгүй байдлын талаарх мэдлэгийг нэмэгдүүлэх хөтөлбөрийн хүртээмжид төвлөрдөг бөгөөд кибер аюул, эрсдэл болон тэдгээрийг шийдвэрлэх арга замыг ойлгуулахад чиглэнэ.

Түвшин: **Эхлэл түвшнээс Хөгжиж буй түвшинд**

Монгол Улсад кибер аюулгүй байдлын мэдлэгийг нэмэгдүүлэх олон төрлийн хөтөлбөр, үйл ажиллагаа хэрэгжиж байгаа боловч тэдгээрийг өөр өөр байгууллагууд, хоорондоо уялдаа холбоогүйгээр хэрэгжүүлж байна. Үүнд Засгийн газрын зүгээс хэрэгжүүлж буй Харилцаа холбооны зохицуулах хороо (CRC), Засгийн газрын цахим үйлчилгээний зохицуулах агентлаг (RAGDS), Цагдаагийн ерөнхий газар, ЦХИХХЯ, мөн Үндэсний болон Нийтийн төвөөс[45] зохион байгуулж буй кампанит ажлууд хамаарна. Эдгээр кампанит ажлууд нь эрсдэлд илүү их өртөх магадлалтай гэж үзсэн тодорхой бүлгийн оролцогч талуудад чиглэсэн бөгөөд үүнд хүүхэд, өсвөр үеийнхэн, 40-с дээш насныхан, гэртээ байдаг эцэг эхчүүд, жижиг дунд бизнес эрхлэгчид багтана. Кампанит ажлын агуулга нь телевизийн сурталчилгаа, биечлэн танилцуулах сургалтууд, нөлөөлөгчидтэй /influencer/ хамтран ажиллах, нийгмийн сүлжээний контент бүтээх зэрэг олон агуулгаас бүрдэнэ.

Стратегийн түвшинд, олон нийтийн кибер аюулгүй байдлын талаарх мэдлэгийг нэмэгдүүлэх, мөн сургалт, семинар зохион байгуулж, кибер аюулгүй байдлын талаарх ойлголт, мэдлэг олгох нь 2022 оны Кибер аюулгүй байдлын үндэсний стратегийн гол зорилтуудын нэг юм. Хууль эрх зүйн үүднээс авч үзвэл, Цахим хөгжил, инновац, харилцаа холбооны яам (ЦХИХХЯ) нь 2021 оны Кибер аюулгүй байдлын тухай хуулийн

[45] https://crc.gov.mn/list/internetijn-s-lzhee-jlchilgee/mn?show=104
https://www.facebook.com/ekids.mn/
https://gogo.mn/r/o3d8j

хүрээнд кибер аюулгүй байдлын асуудал болон холбогдох хууль тогтоомжийн талаарх ойлголтыг олон нийтэд түгээх үүрэгтэй.

Сүүлийн нэг жилийн хугацаанд яам нь Кибер аюулгүй байдлын нийтлэг журмын талаар цуврал сургалтууд зохион байгуулж, жижиг, дунд бизнесүүдэд чиглэсэн хэд хэдэн компанит ажил хэрэгжүүлсэн[46]. Гэсэн хэдий ч, ихэнх тохиолдолд ЦХИХХЯ энэ үүргийг Нийтийн төвд хариуцуулан шилжүүлжээ. Голлох бүлгийн хэлэлцүүлгийн үеэр Нийтийн төвийн хэрэгжүүлж буй мэдлэг олгох үйл ажиллагааны чанар болон давтамжийн талаар харилцан адилгүй санал бодол илэрхийлж байсан. Оролцогч талуудын дунд кибер аюулгүй байдлын талаарх олон нийтийн ойлголтыг үр дүнтэй нэмэгдүүлэхийн тулд илүү тогтвортой, стратегитай хандлага шаардлагатай гэдэгт санал нэгдсэн. Өргөн хүрээнд авч үзвэл, эдгээр эерэг хүчин чармайлтуудаас үл хамааран, кибер аюулгүй байдлын талаарх ерөнхий мэдлэг тун бага түвшинд байгаа тул энэ чиглэлээр нэмэлт ажлууд хийх шаардлагатай. Иймд, кибер аюулгүй байдлын талаарх мэдлэгийг нэмэгдүүлэх нь стратегийн чухал ач холбогдолтой хэдий ч, төрийн байгууллагуудын хүрээнд энэ чиглэлээр уялдаа холбоотой, тогтвортой, бодит хэрэгцээнд нийцсэн үр дүнтэй мэдээлэл түгээх тогтолцоог хөгжүүлэх шаардлага хэвээр байна.

Төрийн байгууллагуудаас гадна, хувийн хэвшил кибер аюулгүй байдлын талаарх мэдлэгийг нэмэгдүүлэх чиглэлээр олон төрлийн үйл ажиллагаа зохион байгуулж байна. Үүнд Монгол Улсын Их Сургуулийн оюутны клуб болон банкны салбарын хамтын ажиллагааны хүрээнд зохион байгуулсан биечлэн оролцох боломжтой мэдээлэл түгээх арга хэмжээнүүд[47], мөн төрийн өмчит банкуудын аюулгүй кибер дадлыг сурталчлах ерөнхий идэвхжил багтана. Үүний тод жишээ нь улсын томоохон банкуудын төлөөлөл болох банкны YouTube хуудсанд байршуулсан, харилцагч болон олон нийтэд зориулсан олон өндөр чанартай цахим боловсрол, аюулгүй байдлын видео контентууд[48] юм. Голлох бүлгийн хэлэлцүүлгээр хувийн хэвшлийн байгууллагуудын ихэнх нь кибер төлөвшлийн хувьд илүү өндөр түвшинд байдаг гэж үздэг бөгөөд тэдгээр байгууллагууд дотооддоо мэдлэг олгох хөтөлбөр, ажилтнуудад зориулсан тусгай порталууд ажиллуулдаг нийтлэг жишигтэй болохыг онцолсон.

Иргэний нийгмийн салбарт MNCERT/CC буюу Нийтийн төв нь кибер боловсрол, мэдлэгийг дээшлүүлэх чиглэлээр идэвхтэй ажиллаж, мэдээлэл солилцох болон бусад чиг үүрэг бүхий арга хэмжээг сүүлийн арван жилийн турш хэрэгжүүлж ирсэн[49]. Хэдийгээр энэ нь шууд мэдлэг олгох хөтөлбөр биш боловч MNCERT/CC жил бүр Монгол Улсын хамгийн том кибер аюулгүй байдлын бага хурлыг зохион байгуулж, энэ салбарт ажилладаг олон талын оролцогчдыг нэгтгэж, кибер аюулгүй байдлын талаар хэлэлцүүлэг өрнүүлэх боломжийг бүрдүүлж байна[50]. Монгол Улсад олон улсын хөгжлийн түншүүд ч кибер аюулгүй байдлын мэдлэг олгох хөтөлбөрүүдийг хэрэгжүүлж ирсэн бөгөөд үүнд ЖАЙКА, НҮБ, USAID зэрэг байгууллагууд багтана. 2022 онд USAID нь "Миний цахим мэдээлэл минийх" нэртэй кампанит ажлыг санхүүжүүлсэн бөгөөд уг кампанит ажилд Монголын поп уран бүтээлчид оролцож, Meta-ийн “We Think Digital” санаачилга болон

[46] https://www.youtube.com/watch?v=coBpQk-sVkQ&list=PLuEgz5swNEEbCuqPam1qFh_f435jyCsYh

[47]https://news.mn/r/2373711/?fbclid=IwY2xjawG6fJ5leHRuA2FlbQIxMQABHZjlsohDaTlb_geFXBXNPOhjVkshaxx4SYMufxrxkN4kMYcqTtS5vFfb_w_aem_aEn7mV15PrsgdCCbE1DSdwhttps://www.youtube.com/watch?v=q9Vx7AvHVKo

[48] https://www.youtube.com/@KhanBank.officialv

[49] https://cscouncil.gov.mn/en/cybersecurity-professionals-participated-itactic-training

[50] https://mnsec.mncert.org/event/

Фаро (Faro) сангийн хамтын ажиллагааны хүрээнд хэрэгжсэн[51]. Сүүлийн үед НҮБ нь өөрийн инновацийн лабораторийн хөтөлбөрөөр дамжуулан Монголын олон талын оролцогчдын кибер аюулгүй байдлын боловсролыг дээшлүүлэх чиглэлээр ажиллаж байгаа бөгөөд "хэнийг ч орхигдуулахгүй байх" зарчмыг баримталж байна. Үүнээс гадна, тэд кибер аюулгүй байдлын мэдлэг дээшлүүлэх чиглэлээр онлайн сургалтын материал, кибер аюулгүй байдлын тоглоом, вэбинарт суурилсан сургалт, олон нийтийн хүрээнд сургалтын арга хэмжээ зохион байгуулж, улс даяар хэрэгжүүлсэн байна.

ЖАЙКА мөн кибер аюулгүй байдлын мэдлэг дээшлүүлэх чиглэлээр олон талын оролцоог хангасан хамтын ажиллагааны төсөл боловсруулахаар ажиллаж байгааг мэдээлсэн. Энэ төсөл нь эхний шатандаа явж байгаа бөгөөд хэрэгжүүлэлтийн явцад зарим хүндрэлүүдтэй тулгарсан гэж үзэж байна. Голлох бүлгийн хэлэлцүүлэг болон бичиг баримтад тулгуурласан судалгааны үр дүнд хувийн болон төрийн салбарын удирдах гүйцэтгэх удирдлагын түвшинд чиглэсэн цогц кибер аюулгүй байдлын мэдлэг олгох цогц сургалтын хөтөлбөр байхгүй болох нь тогтоогдсон. Голлох бүлгийн хэлэлцүүлэгт тодорхой хэмжээнд яригдсан цөөн тооны боломжууд байсан бөгөөд үүнд зарим яамдын удирдах ажилтнуудыг Япон руу явуулж, Японы мэргэжилтнүүдээс туршлага судлуулах нэг удаагийн хөтөлбөр болон Тагнуулын Ерөнхий Газар (ТЕГ)-аас зохион байгуулсан ганц нэг сургалтууд багтаж байсан боловч цогц, тогтвортой хөтөлбөр байхгүй байна.

Кибер аюулгүй байдлын мэргэжилтнүүдийн дунд удирдах түвшний удирдлагууд кибер аюулгүй байдлын асуудал болон тэдгээрийн үйл ажиллагаанд тулгарч буй сорилтуудыг стратегийн түвшинд ойлгохгүй байна гэсэн нийтлэг итгэл үнэмшил ажиглагдсан. Голлох бүлгийн олон оролцогчид кибер аюулгүй байдлын асуудалд байгууллагын удирдлагуудаас эсэргүүцэлтэй тулгардаг гэж мэдэгдсэн. Удирдлагууд кибер аюулгүй байдлын төсвийг нэмэгдүүлэхээс татгалзах, илүү бодитой, гүнзгийрүүлсэн сургалтын боломжийг дэмжихгүй байх байдал түгээмэл ажиглагдаж байна. Олон хүн энэ асуудлыг даван туулахын тулд удирдах түвшний шийдвэр гаргагчдад зориулсан тусгайлсан мэдлэг олгох хөтөлбөр хэрэгтэй гэдэг хүчтэй байр суурь илэрхийлсэн.

Монгол Улсад кибер аюулгүй байдлын олон төрлийн мэдээлэл түгээх, мэдлэг нэмэгдүүлэх хөтөлбөрүүд хэрэгжиж байгаа нь тодорхой боловч эдгээр нь стратегийн уялдаа холбоогүй, ихэвчлэн давхардсан агуулгатай бөгөөд Монголын хүн амын дунд өргөн хүрээний, тогтвортой ойлголт бий болгоход үр дүн төдийлөн үзүүлэхгүй байна (2.1-р хүчин зүйлд дурдсан). Голлох бүлгийн хэлэлцүүлгүүдийн үеэр олон нийтийн кибер аюулгүй байдлын талаарх мэдлэгийг нэмэгдүүлэх кампанит ажлуудын санхүүжилт хязгаарлагдмал байгаа нь гол бэрхшээл болж буйг тодорхойлсон бөгөөд үүн дээр удирдах түвшний шийдвэр гаргагчдын ойлголт хангалтгүй байгаа нь асуудлыг хүндрүүлж байна. Үүнээс гадна, олон нийтийн мэдээлэл түгээх кампанит ажлуудын үр нөлөөг үнэлэх үр дүнд чиглэсэн хэмжүүрүүд хангалтгүй байгааг голлох бүлгийн хэлэлцүүлгээр илрүүлсэн. Одоогийн байдлаар хэрэгжиж буй кампанит ажлуудын үр нөлөөний үнэлгээ хийгдээгүй, мөн тэдгээрийг үр дүн, хүлээн авагчдын санал хүсэлтэд үндэслэн шинэчлэх механизм байхгүй байна. Голлох бүлгийн оролцогчид илүү бодит мэдээлэлд суурилсан, үр дүнтэй кампанит ажил зохион байгуулахын тулд кибер аюулгүй байдлын өгөгдөл цуглуулах практикийг сайжруулах хэрэгтэй гэж үзсэн. Эцэст нь, кибер аюулгүй байдлын талаарх олон нийтийн мэдлэгийг нэмэгдүүлэх тодорхой зорилтууд

[51] https://www.usaid.gov/asia-regional/press-releases/feb-28-2022-usaid-launches-cybersecurity-awarenesscampaign

үндэсний стратегид тусгагдсан хэдий ч, энэхүү үйл ажиллагааг хэрхэн хэрэгжүүлэх тодорхой төлөвлөгөө багтаагүй байна.

D 3.2 КИБЕР АЮУЛГҮЙ БАЙДЛЫН БОЛОВСРОЛ

Түвшин: **Хөгжиж буй түвшинд**

Энэ хүчин зүйл нь өндөр чанартай кибер аюулгүй байдлын боловсролын хөтөлбөрүүдийн хүртээмж, хангамж болон хангалттай тооны мэргэшсэн багш, сургагч багш нарын хүртээмж, хангалттай байдал зэргийг авч үздэг. Мөн кибер аюулгүй байдлын боловсролыг үндэсний болон байгууллагын түвшинд сайжруулах хэрэгцээ, төр болон хувийн хэвшлийн хамтын ажиллагааг судалж, боловсролын хөрөнгө оруулалтыг бүх салбарын хэрэгцээнд нийцүүлэн оновчтой болгох асуудлыг судална.

Монгол Улсын Кибер аюулгүй байдлын үндэсний стратегийн хүрээнд хүний нөөцийн чадавхыг сайжруулах, шинэ боловсон хүчин бэлтгэх, тэднийг тогтвортой байлгах нь голлох зорилтуудын нэг болж байна. Энэ стратегийн хүрээнд кибер аюулгүй байдлын боловсролыг өргөжүүлэхтэй холбоотой хэд хэдэн арга хэмжээг тодорхойлсон бөгөөд боловсролын байгууллагын сургалтын хөтөлбөрт бүх түвшинд кибер аюулгүй байдлын мэдлэгийг багтаах зорилго агуулжээ.

Монгол Улсад кибер аюулгүй байдлын мэргэжилтний эрэлт өндөр байгааг бүх оролцогч талууд хүлээн зөвшөөрч байгаа бөгөөд байгууллагууд хүний нөөцийн төлөө байнгийн өрсөлдөөн дунд байна. Энэ эрэлт хэрэгцээ нь их, дээд сургуулиудын элсэлтийн үзүүлэлт болон Голлох бүлгийн хэлэлцүүлгээс тодорхой харагдах бөгөөд зарим тохиолдолд ур чадвартай боловсон хүчний эрэлт маш өндөр байх тул хувийн хэвшлийн байгууллагууд, Тагнуулын Ерөнхий Газар, Цагдаагийн Ерөнхий Газар нь хоёр болон гуравдугаар курсийн амжилттай суралцаж буй оюутнуудад урьдчилсан ажиллах гэрээ санал болгож байна. Гэхдээ Монгол Улсад засгийн газар, аж үйлдвэр, боловсролын салбарын хооронд кибер аюулгүй байдлын боловсон хүчнийг бэлтгэх чиглэлд нэгдсэн зохицуулалттай стратеги байхгүй байна.

Кибер аюулгүй байдлын чиглэлээр бакалавр, магистр, докторын зэргийг Монгол Улсын зарим их, дээд сургуульд олгож байна. Шинжлэх Ухаан, Технологийн Их Сургууль (ШУТИС) нь 2002 оноос "Мэдээллийн сүлжээ" хөтөлбөрийг санал болгож эхэлсэн бөгөөд сүүлийн жилүүдэд "Системийн аюулгүй байдал" хөтөлбөрийг нэмж оруулсан. Эдгээр хөтөлбөрийн хүрээнд хэдэн зуун бакалаврын түвшний мэргэжилтэн бэлтгэгдсэн[52]. Саяхан ШУТИС-д кибер аюулгүй байдлын чиглэлээр хоёр жилийн хугацаатай магистрын хөтөлбөр батлагдсан бөгөөд үүнийг ЦХИХХЯ болон ЛСА-ийн тэтгэлэгт хөтөлбөрийн хүрээнд дэмжиж байна.

Монгол Улсын Их Сургуулийн (МУИС) Мэдээлэл, компьютерын шинжлэх ухааны тэнхим "Мэдээллийн систем", "Мэдээллийн технологи", "Компьютерын ухаан", "Программ хангамж" зэрэг бакалаврын түвшний хөтөлбөрүүдийг санал болгодог[53]. Электрон болон Холбоо Инженерийн Тэнхим нь "Компьютерын сүлжээ" хөтөлбөрийг санал болгодог бөгөөд оюутнууд хичээлийн 40 хүртэлх хувийг кибер аюулгүй байдлын

[52] https://www.sict.edu.mn/en/210
[53] https://registration.num.edu.mn/Admission/Programs/2

чиглэлээр сонгон судлах боломжтой байдаг. Тус их сургууль сургалтуудаа "Сүлжээ, систем, кибер аюулгүй байдлын лаборатори"-д явуулдаг бөгөөд кибер аюулгүй байдал, мэдээллийн аюулгүй байдлын чиглэлээр мэргэшсэн гурван үндсэн багш, нэг гэрээт багш ажиллаж байна.

Монгол Олон Улсын Их Сургууль (MIU) нь компьютерын шинжлэх ухаан, программ хангамжийн бакалаврын хөтөлбөрүүдийг санал болгодог бөгөөд үүнд компьютерын аюулгүй байдлын холбогдох хичээлүүдийг багтаасан[54]. MIU нь мөн магистрын түвшний программ хангамжийн хөтөлбөртэй бөгөөд "Аюулгүй байдалд мэдрэмтгий программ хангамж" гэх тусгайлсан хичээлийг оруулсан байна[55]. Удирдлагын Академи нь Өмнөд Солонгосын их сургуулийн сургалтын хөтөлбөр дээр суурилсан мэдээллийн аюулгүй байдлын сургалтуудыг хэрэгжүүлж байгаа бөгөөд 2024 онд сургалтын хөтөлбөрөө шинэчлэн сайжруулсан. Үндэсний Батлан Хамгаалах Их Сургууль нь цэргийн кибер командын нэгжид ажиллах боловсон хүчин бэлтгэх кибер аюулгүй байдлын хөтөлбөрийг хэрэгжүүлж байна.

Голлох бүлгийн хэлэлцүүлгээс харахад Монгол Улсын мэргэжлийн сургалтын төвүүд кибер аюулгүй байдлын сургалтуудыг санал болгодог бөгөөд хөдөлмөрийн зах зээлийн олон төрлийн салбараас суралцагчдыг татаж байна. Оролцогч талуудын мэдээлснээр, бага анги болон мэргэжлийн боловсролын сургалтын хүрээнд мэдээллийн технологийн өргөн хүрээтэй хичээлийн агуулгаар дамжуулан кибер аюулгүй байдлын боловсролыг тодорхой хэмжээнд олгодог гэсэн ч тухайн мэдээллийг суурь судалгаагаар баталгаажуулах боломжгүй байсан.

Мөн бага ангийн хүүхдүүдэд кибер аюулгүй байдлын тухай ерөнхий ойлголт, эрх зүйн орчин, хувийн мэдээллийн хамгаалалт зэрэг мэдээлэл өгдөг гэж мэдээлсэн боловч аюулгүй байдлын нарийвчилсан сургалт ордоггүй. Голлох бүлгийн хэлэлцүүлэг болон бичиг баримтад тулгуурласан судалгааны үр дүнд дунд боловсролын хөтөлбөрт кибер аюулгүй байдлын хичээл албан ёсоор багтсан эсэх нь тодорхойгүй байна.

Хэдийгээр кибер аюулгүй байдлын мэргэшсэн мэргэжилтний эрэлт өндөр, албан ёсны боловсролын хөтөлбөрүүд хөгжиж, оюутнуудын сонирхол нэмэгдэж байгаа ч Монголын их, дээд сургуулиудад салбарын хүлээлтэд нийцсэн төгсөгчдийг бэлтгэхэд шаардлагатай тоног төхөөрөмж, хүний нөөц дутмаг байна. Их сургуулиуд мэргэжилтэн багш нарыг ажилд авах, тогтвортой ажиллуулах тал дээр хүндрэлтэй байгаагаа мэдээлсэн. Үүний гол шалтгаан нь кибер аюулгүй байдлын ур чадвартай мэргэжилтнүүд хувийн хэвшил болон гадаадын зах зээлд өндөр цалинтай ажлын байраар хангах боломжтой тул ачаалал ихтэй, харьцангуй бага цалинтай их дээд сургуулийн багшийн ажлыг сонирхох нь бага байна.
Кибер халдлагын эсрэг хамгаалалт, халдлагын симуляци хийх лаборатори, тоон шинжилгээний сургалтын орчин зэрэг техникийн дэд бүтэц дутмаг байгаа нь боловсролын чанарт сөргөөр нөлөөлж байна. Ийм төрлийн лаборатори, сургалтын орчныг байгуулах, ажиллуулах өртөг өндөр учраас их, дээд сургуулиуд дангаараа шийдвэрлэхэд хэцүү, засгийн газар болон хувийн хэвшлийн дэмжлэг шаардлагатай байна. НҮБ-ын Монгол дахь Мэдээлэл, харилцаа холбооны ур чадварын талаарх судалгаагаар, ихэнх сургалтын хөтөлбөрүүд онолын мэдлэг олгоход төвлөрсөн тул төгсөгчид шууд ажлын байранд гарахад хангалттай бэлтгэгдээгүй байгааг тэмдэглэжээ[56].

[54] https://miu.edu.mn/computer-science/
[55] https://miu.edu.mn/master-se/
[56] UN eTrade readiness assessment (p. 59)

Энэхүү асуудлыг шийдвэрлэхийн тулд зарим их, дээд сургуулиуд, тухайлбал ШУТИС (MUST), хоёр+хоёр хөтөлбөрийг нэвтрүүлж, оюутнуудыг хоёр өөр их сургуульд хуваарилан суралцах боломжийг бүрдүүлсэн. Энэ нь их сургуулиудын хүний нөөц, багш нарын чадамжийг нэгтгэж, сургалтын чадамжийн дутагдлыг нөхөх боломжийг олгож байна. ШУТИС нь Үндэсний Батлан Хамгаалах Их Сургууль болон Солонгос, Япон, Тайвны их сургуулиудтай хамтран хоёр+хоёр хөтөлбөр хэрэгжүүлдэг бөгөөд оюутнууд дунд өндөр эрэлттэй байдаг тул уг загварыг магистрын түвшинд нэг+нэг хөтөлбөр болгон өргөжүүлсэн байна. Зарим оюутнууд сураад төгссөний дараа эх орондоо буцаж ирэх сонирхол бага байгаа нь энэ хөтөлбөрийн амжилттай хэрэгжилтэд сөргөөр нөлөөлж болзошгүй гэсэн мэдээлэл байна.

Олон улсын түншүүдээс ЖАЙКА, UNESCO, UNODC зэрэг байгууллагууд тодорхой хэмжээний туслалцаа үзүүлж байгаа боловч эдгээр тусламж, дэмжлэгийн үйл ажиллагаа хоорондоо уялдаа холбоогүй, нэгдсэн зохицуулалтгүй байгаа нь боловсролын үр нөлөөг бууруулах эрсдэлтэй байна. ЖАЙКА-н "Кибер аюулгүй байдлын хүний нөөцийг хөгжүүлэх төсөл" боловсролын салбарт онцгой ач холбогдолтой санаачилга болж байгаа бөгөөд энэ чиглэлд хэрэгжиж буй хамгийн чухал төслүүдийн нэг гэж үзэж байна. 2023 онд эхэлсэн уг төсөл гурван гол зорилготой: кибер аюулгүй байдлын хүний нөөцийг хөгжүүлэх чиглэлээр аж үйлдвэр, эрдэм шинжилгээний байгууллага болон засгийн газрын хамтын ажиллагааны харилцааг бий болгох; оюутан болон ажил эрхлэгчдэд зориулсан кибер аюулгүй байдлын боловсролын хөтөлбөрийг боловсруулж, зохион байгуулах; мөн төрийн албан хаагчдад зориулсан кибер аюулгүй байдлын боловсролын хөтөлбөрийг боловсруулж, хэрэгжүүлэх юм. Энэ ажлын хүрээнд ЖАЙКА нь Монгол Улсад шаардлагатай кибер аюулгүй байдлын ур чадварын үнэлгээг хийж[57], их дээд сургуулиудын сургалтын хөтөлбөрийг шинэчлэх, мөн сургалтын багш, сургагч нарыг бэлтгэх (train-the-trainer) арга хэмжээнүүдийг хэрэгжүүлж байна. Энэхүү төслийн цар хүрээ, ач холбогдол нь боловсролын салбар дахь олон улсын чадавх бэхжүүлэх түншүүдийн үүрэг маш чухал болохыг харуулж байгаа бөгөөд эдгээр түншүүдийг дээд боловсролын стратегийн өргөн хүрээний төлөвлөлтөд нэгтгэн оруулах шаардлагатай гэдгийг онцолж байна.

D 3.3 КИБЕР АЮУЛГҮЙ БАЙДЛЫН МЭРГЭЖЛИЙН СУРГАЛТ

Энэхүү хүчин зүйл нь кибер аюулгүй байдлын мэргэжилтнүүдийг бэлтгэх зорилгоор боломжийн үнэтэй сургалтын хөтөлбөрийн хүртээмж, хэрэгжилтийг үнэлж, хянахтай холбоотой юм. Мөн, энэ хүчин зүйл нь кибер аюулгүй байдлын сургалтын хэрэгжилт, байгууллагын дотоод болон салбар хооронд мэдлэг, ур чадвар дамжуулах үйл явцыг судалж, энэ нь кибер аюулгүй байдлын мэргэжилтнүүдийн тоог тогтвортой нэмэгдүүлэхэд хэрхэн нөлөөлж буйг үнэлнэ.

Түвшин: **Хөгжиж буй түвшнээс Тогтворжсон түвшинд**

Кибер аюулгүй байдлын хүний нөөцийг хөгжүүлэх нь стратегийн чухал чиглэл гэж үздэг. Энэхүү стратегид "кибер гэмт хэрэг, терроризмтой тэмцэх онцгой чиг үүрэг бүхий байгууллагуудын хүний нөөцийг бэлтгэх", мөн "кибер аюулгүй байдлыг хангах хүний

[57] https://cybilportal.org/projects/project-for-development-of-human-resources-in-cyber-security/

нөөцийг чадавхжуулах, мэргэшүүлэх богино, дунд, урт хугацааны сургалтуудыг хэрэгжүүлэх" ажлуудыг тусгасан байна[58].

Монгол Улсад олон төрлийн бүтэцлэгдсэн болон тусгай зориулалтын кибер аюулгүй байдлын сургалтын хөтөлбөрүүд хэрэгжиж байгаа бөгөөд тэдгээрийн зарим нь олон улсад хүлээн зөвшөөрөгдсөн гэрчилгээ олгодог. Эдгээр сургалтуудыг төрөл бүрийн боловсролын байгууллага, мэргэжлийн сургалтын төвүүд болон олон улсын чадавх бэхжүүлэх түншүүд санал болгож байна. Үүнд ICT Training[59], Info Sec Plus[60], System Center[61], Empasoft Institute of Technology[62], МУИС (EC-Council, ACT, CISCO Academy-тэй хамтран), Үндэсний Мэдээлэл Технологийн Парк зэрэг байгууллагууд багтана. Сургалтын төлбөрийн хэмжээ харилцан адилгүй бөгөөд олон улсын гэрчилгээ олгох шалгалтын материал, төлбөр өндөр өртөгтэй байдаг тул зарим байгууллагууд тэдгээрийг санхүүжүүлэх боломжгүй гэж үзэж байна.

Хууль сахиулах байгууллагын ажилтнуудад зориулсан сургалтууд тогтмол зохион байгуулагддаг. Дотоод хэргийн их сургууль 4.3 хүчин зүйлд дурдсанчлан тусгай чиг үүрэг бүхий хууль сахиулагчдыг бэлтгэх академитай. Үүнээс гадна, ЖАЙКА, Энэтхэг, CISA, Carnegie Mellon, MITRE зэрэг олон улсын байгууллагуудын оролцоотойгоор ЦХИХХЯ нь сургалт зохион байгуулж байна. ЖАЙКА нь сургалт явуулах сургагч багш бэлтгэх хөтөлбөрүүд зэргээр академик болон мэргэжлийн боловсон хүчинд өргөн хүрээний дэмжлэг үзүүлсэн[63].

Үндэсний төв нь өөрийн бүрэлдэхүүнд багтдаг байгууллагуудад мэргэжлийн кибер аюулгүй байдлын сургалт зохион байгуулдаг[64]. Иргэний нийгмийн хүрээнд MNCERT/CC гишүүн байгууллагууддаа тогтмол кибер аюулгүй байдлын сургалт, дадлага зохион байгуулдаг бөгөөд эдгээр хаалттай сургалтын хөтөлбөрүүдийг оролцогчид өндөр үнэлдэг. Зарим томоохон төрийн болон хувийн хэвшлийн байгууллагууд өөрсдийн дотоодын кибер аюулгүй байдлын сургалтын хөтөлбөрүүдийг бий болгосон. ЦХИХХЯ олон улсын түншүүдтэй хамтран зохион байгуулсан сургалтуудад ихэнх онц чухал дэд бүтцийн байгууллагууд хамааруулсан. Гэвч ийм сургалтад нэг удаа 50-100 хүн оролцох боломжтой тул ахиц удаан талаар мэдээлсэн.

Монгол Улсад хэрэгжиж буй сургалтын ихэнх нь олон улсын ISO 27001 зэрэг аюулгүй байдлын стандарт, шилдэг туршлагад үндэслэн боловсруулагдсан байдаг. Гэсэн хэдий ч зарим сургалтын байгууллагууд материалыг шинэчилж орчуулах явцад хүндрэлтэй тулгарч байгаа талаар мэдээлсэн. Одоогоор сургалтын хэрэгжилтийн түвшин, үр нөлөөг хэмжих тодорхой үнэлгээний тогтолцоо байхгүй тул үр дүнг бүрэн тодорхойлоход хүндрэлтэй байна.

Голлох бүлгийн хэлэлцүүлгээр төр болон хувийн хэвшлийн аж ахуйн нэгжүүд эдгээр сургалтын боломжуудыг тогтмол ашигладаг бөгөөд боломжтой үедээ хамрагддаг болохыг дурдсан нь Монголын байгууллагуудын дунд кибер аюулгүй байдлын мэргэжлийн сургалтын эрэлт өндөр байгааг харуулж байна. Кибер аюулгүй байдлын

---

[58] Mongolia National Cybersecurity Strategy, p.2.
[59] https://www.ict-training.mn/courses#Security
[60] https://www.infosecplus.mn/
[61] https://systemcenter.io/
[62] https://empasoft.ider.edu.mn/home_english/#COMPUTER-NETWORK-AND-INFORMATIONSECURITY
[63] https://openjicareport.jica.go.jp/pdf/1000050862.pdf
https://cscouncil.gov.mn/en/japanese-experts-lead-cyber-security-training
[64] https://cscouncil.gov.mn/en/cybersecurity-professionals-participated-itactic-training

хууль, эрх зүйн зохицуулалтад орсон сүүлийн үеийн өөрчлөлтүүд, тухайлбал 2021 оны Кибер аюулгүй байдлын тухай хууль, Кибер аюулгүй байдлын нийтлэг журмын нэвтрүүлэлт нь эдгээр хөтөлбөрүүдийн эрэлтийг нэмэгдүүлэхэд нөлөөлсөн. ОЧМДБ байгууллагууд нь кибер аюулгүй байдлын ажилтан ажиллуулах, тогтмол эрсдэлийн үнэлгээ хийлгэх, мэдээллийн аюулгүй байдлын аудит хийлгэх зэрэг хууль эрх зүйн шаардлагатай болсноор байгууллагуудын удирдах түвшний удирдлагын дунд кибер аюулгүй байдлын ач холбогдлыг нэмэгдүүлэхэд нөлөөлсөн. Зарим байгууллагууд, тухайлбал, Тагнуулын ерөнхий газар нь хуулийн дагуу холбогдох ажилтнуудад кибер аюулгүй байдлын сургалт, дадлага зохион байгуулах үүрэгтэй байдаг (13.1.2-р зүйл).

Сүүлийн үеийн хууль эрх зүйн шинэчлэлүүдийн үр дүнд Монгол Улсын удирдах түвшний шийдвэр гаргагчид кибер аюулгүй байдлыг өмнөхөөс илүү ач холбогдолтой гэж үзэх болсон хэдий ч, голлох бүлгийн хэлэлцүүлгийн оролцогчид сургалтад хамрагдах зөвшөөрөл авахад хүндрэлтэй хэвээр байгааг онцолж байна. Байгууллагын удирдлагууд сургалтад хамрагдах ажилчдын ажлын байрнаас түр хугацаагаар чөлөөлөгдөх байдал, сургалтын зардал, мөн ажилчдаа сургаж хөгжүүлэх нь тэднийг илүү өндөр цалинтай ажилд шилжихэд дэмжлэг үзүүлэх эрсдэлтэй гэсэн түгшүүртэй хандлага гаргаж байгааг тэмдэглэсэн. Үүний үр дүнд, байгууллагын удирдлагууд урт хугацааны мэргэшүүлэх хөтөлбөрөөс илүүтэйгээр, богино хугацаатай, бага зардалтай сургалтуудыг илүүд үзэх хандлагатай байгаа талаар дурдсан.
Кибер аюулгүй байдлын ажилтнуудыг сургах, хадгалж үлдэх бэрхшээл нь ялангуяа төрийн байгууллагуудад ноцтой тулгарч байгаа бөгөөд үүнд уян хатан бус цалингийн систем, яамдын уялдаа холбоогүй байдал, хувийн хэвшилтэй харьцуулахад өрсөлдөх чадваргүй нөхцөл байдал багтдаг. Голлох бүлгийн оролцогчдын үзэж байгаагаар, төрийн байгууллагуудын авч хэрэгжүүлж буй эрэг сургалтын арга хэмжээнүүд нь байгууллагын дотоодын ур чадварын хомсдлыг нөхөхөөс илүүтэйгээр ажилтнууд хувийн хэвшилд орох эсхүл гадаад улс руу гарах "шат" болон ашиглагдаж байна гэж үзэж байв. Кибер аюулгүй байдлын ур чадвар эзэмшсэн ажилчид олон улсын гэрчилгээ авсны дараа эсхүл удаан хугацааны туршлага хуримтлуулсны дараа хөдөлмөрийн зах зээл дээр өндөр эрэлттэй ажилчид болж байгаа тул тэднийг урт хугацаанд төрийн байгууллагад үлдээхэд бэрхшээлтэй байна.

Шинэ ажилчдыг төрийн албанд татахад олон шат дамжлагатай шалгалт, өргөдлийн процесс шаарддаг тул улам бүр хүндрэлтэй болж байна. Энэ нь ажилд орох хугацааг удаашруулахаас гадна сонирхсон өргөдөл гаргагчдыг илүү хялбар сонгон шалгаруулалтын боломжийг хайхад хүргэдэг. Өмнө нь төрийн албаны уламжлалт давуу талууд ажилчдыг татахад хангалттай байсан ч энэ нь одоогийн залуу үеийн хувьд тийм ч чухал биш болсон.

Эдгээр сорилтуудыг даван туулах зорилгоор, Монгол Улсын Засгийн газар төрийн байгууллагын хүний нөөцийн дутагдалыг бууруулах, ажиллах хүчний бүрдүүлэлтийг сайжруулах чиглэлээр тодорхой арга хэмжээнүүдийг авч хэрэгжүүлж байна. Жишээлбэл, ЦХИХХЯ нь "сургагчыг-сургах" (train-the-trainer) хөтөлбөрийг санаачилж, кибер аюулгүй байдлын мэдлэгийг ажилтнуудын хооронд зорилтот түвшинд түгээх, орон нутгийн мэргэжилтнүүдийн ур чадварыг ашиглах боломжийг бүрдүүлж байна. Одоогийн байдлаар тус хөтөлбөрийн хүрээнд 100 сургагч багш бэлтгэгдээд байна. Цаашлаад, ЦХИХХЯ-ны манлайллаар Засгийн газар мэдээллийн аюулгүй байдлын мэргэжилтнүүдэд зориулсан шинэ ажлын байрны ангиллыг нэвтрүүлсэн нь тэдгээр мэргэжилтнүүдийг төрийн албан хаагчийн ангиллаас тусад нь авч үзэх боломжийг олгож байна.

Энэхүү ангилал нь мэдээллийн аюулгүй байдлын мэргэжилтнүүд илүү өндөр цалин авах, төрийн албанд уламжлалт байдлаар өргөдөл гаргах шаардлагагүй болох зэрэг давуу талтай боловч, төрийн албан хаагчдад олгогддог уламжлалт халамж, эрхийг эдлэхгүй байх нөхцөлтэй. Хэдийгээр энэхүү шинэ ажлын бүтэц болон бусад шийдлүүдийг бий болгон төрийн байгууллагуудын ур чадвар болон боловсон хүчний тогтвортой байдлыг хангахад чиглэж байгаа ч, одоогоор уг бүтэц дор тус бүрийн агентлаг хоёрхон ажилтан авах эрхтэй байгаа нь бодит хэрэгцээг хангахуйц бус гэдгийг голлох бүлгийн хэлэлцүүлгийн оролцогчид онцолжээ. ЦХИХХЯ-ны зүгээс уг схемийн хүрээг тэлэх нь амаргүй процесс байх бөгөөд эхний шатанд олгогдсон квот бүрэн дүүрсэний дараа л өргөтгөх боломжтой гэж үзэж байна. Одоогоор уг хөтөлбөрийг зарим агентлагууд эрэгээр хүлээн авч хэрэгжүүлж байгаа бол зарим нь огт анхаарал хандуулаагүй байна.

Энэхүү схемээс гадна, ЦХИХХЯ төрийн байгууллагад мэдээллийн аюулгүй байдлын мэргэжилтнүүдэд зориулсан тусгай урамшууллын систем нэвтрүүлэх боломжийг судалж байгаа нь одоо хүчин төгөлдөр хэрэгжиж буй "нууц мэдээлэл хариуцдаг төрийн албан хаагчдад" олгогддог нэмэгдэл урамшууллын загвартай төстэй байх аж. Уг шинэ санал болгож буй схемийн хүрээнд, кибер аюулгүй байдал хариуцсан мэргэжилтнүүд үндсэн цалин дээрээ 30%-ийн нэмэгдэл авах боломжтой болох юм.
Төрийн байгууллагаас гадна, хувийн хэвшлийн ажил олгогчид мөн өндөр ур чадвартай кибер аюулгүй байдлын мэргэжилтнүүдийг эрэлт хэрэгцээгээ хангахуйц хэмжээгээр олох асуудалтай тулгарч байна. Тэдний хөгжлийн түвшин өндөр байгаа хэдий ч дотоодын болон олон улсын ажил олгогчдын хоорондын хүчтэй өрсөлдөөний улмаас мэргэжилтнүүдийг олох, тогтоон барихад хүндрэлтэй байгааг олон байгууллагууд мэдээлжээ. Хувийн хэвшлийн тодорхой салбарууд, тухайлбал банк, санхүүгийн байгууллагууд харьцангуй өндөр чадвартай, нарийн мэргэшсэн кибер аюулгүй байдлын хүний нөөцөөр хангагдсан байдаг. Энэ нь ихэвчлэн тэд ажилчиндаа зах зээлийн ханшаас өндөр цалин олгох боломжтой бөгөөд өргөн хүрээний бичиг баримт шаардсан процессд баригдахгүй байдгаас шалтгаалдаг.

Гэхдээ голлох бүлгийн хэлэлцүүлэгт оролцогчид ажилчдын хувьд цалин нь ажил олгогчоо сонгох цорын ганц хүчин зүйл биш болохыг онцолсон. Бүтцийн хувьд тодорхой карьерын өсөлтийн боломж, удирдлагын чанар, ажлын соёл зэрэг нь мөн ажилчдын ажил олгогчоо сонгоход нөлөөлөх чухал хүчин зүйлсийн нэг болохыг оролцогчид дурдсан. Мөн кибер аюулгүй байдлын багийн бүрэлдэхүүн хангалтгүй байгаагаас үүдэн ажилчид хэт их ажлын ачаалалтай ажиллах нь тэднийг ажлаасаа гарах эсхүл ажлаа солих нийтлэг шалтгаан болж байгааг тэмдэглэжээ. Ажилчдыг тогтоон барих хүндрэл болон сургалтын хөтөлбөрийн үр өгөөж эргэлзээтэй байгаагаас гадна, сургалтын боломжийн тогтвортой байдал, чанарын талаар ч Голлох бүлгийн оролцогчид шүүмжилсэн. Одоогийн байдлаар ур чадварыг ажлын байран дээр албан бус байдлаар хөгжүүлэх нь нийтлэг үзэгдэл хэвээр байна. Төрийн албанд ажилладаг кибер аюулгүй байдлын мэргэжилтнүүдэд зориулагдсан урт хугацааны тусгай сургалтын хөтөлбөрүүд байдаггүй тул удирдлагууд болон ажилчид аль аль нь шинэ сургалтын боломжуудыг тогтмол хайх, санхүүжүүлэх асуудалтай тулгарч байна.

Олон улсын түншүүдийн тусламжийг Монголын байгууллагууд маш ихээр хүлээн авч байгаа бөгөөд олонх нь олон улсын багш нарын чанарыг дотоодын сургалтын сонголтуудаас илүүтэй үнэлдэг байна. ЦХИХХЯ нь олон улсын сургалтын боломжуудыг стратегийн түвшинд зохион байгуулахыг хичээж байгаа боловч эдгээр сургалтуудын тогтмол бус, гэнэтийн шинж чанар нь төлөвлөлтийн үүднээс найдвартай үндэс суурь болохгүй байгаа тул зохион байгуулалт хүндрэлтэй хэвээр байна. Зарим олон улсын сургалтын түншүүд, тухайлбал JICA нь ЦХИХХЯ-ны дэмжлэгтэйгээр Монголын эдийн

засгийн хэрэгцээ шаардлагад суурилсан үнэлгээ хийж, дотоод дахь мэдлэгийн зөрүүг нөхөхөд чиглэсэн зорилтот сургалтын хөтөлбөрүүдийг боловсруулан хэрэгжүүлсэн байна.

Хэдий олон улсын сургалтын байгууллагуудын чанар, үр өгөөж тодорхой ч, зөвхөн гадаад сургалтын эх сурвалжуудыг ашиглах нь Монгол Улсад тулгамдаж буй кибер аюулгүй байдлын ур чадварын хомсдлыг шийдвэрлэхэд шаардагдах хангалттай түвшинд дээшлүүлэх боломжгүй юм[65]. Дотоодын сургалтын байгууллагууд өөрсдийн нутагшуулсан сургалтын чадавхыг сайжруулахыг зорьж байгаа боловч олон улсын стандарт, шилдэг туршлагуудыг орчуулж, нутагшуулахад тулгарч буй хүндрэлүүд буйг онцолсон. Одоогийн байдлаар Монгол Улсад үйл ажиллагаа явуулж буй дээд боловсролын байгууллага, мэргэжлийн сургалтын байгууллагууд болон тасралтгүй боловсролын хөгжлийн бүтэц нь кибер аюулгүй байдлын салбарт шаардлагатай мэргэжилтнүүдийг хангалттай тоо, чанараар бэлтгэж чадахгүй байгаа нь улс орны хэрэгцээг хангах, стратегийн зорилтуудаа биелүүлэхэд томоохон саад болж байна.

D 3.4 КИБЕР АЮУЛГҮЙ БАЙДЛЫН СУДАЛГАА, ИННОВАЦ

Энэхүү хүчин зүйл нь кибер аюулгүй байдлын судалгаа, инновацид тавигдаж буй ач холбогдлыг үнэлж, технологийн, нийгмийн болон бизнесийн салбарын сорилтуудыг шийдвэрлэх, мөн улс оронд кибер аюулгүй байдлын мэдлэг, чадавхыг хөгжүүлэхэд чиглэсэн хүчин чармайлтыг үнэлэхэд оршино.

Түвшин: **Эхлэл түвшнээс Хөгжиж буй түвшинд**

Монгол Улсын Кибер аюулгүй байдлын үндэсний стратегид кибер аюулгүй байдлын чиглэлээр мэргэшсэн хүний нөөцийг чадавхжуулах зорилтыг тусгасан бөгөөд үүний хүрээнд кибер аюулгүй байдлын судлаачдын сургалт, судалгаа, эрдэм шинжилгээний ажлыг дэмжих хөтөлбөр хэрэгжүүлэх нь үндсэн үйл ажиллагааны нэг гэж заасан байна. Мөн Кибер аюулгүй байдлын тухай хууль (2021)-д “Мэдээлэл, харилцаа холбооны асуудал эрхэлсэн төрийн захиргааны төв байгууллага” нь кибер аюулгүй байдлын чиглэлээр шинэ техник, технологи, инновац, судалгаа, хөгжүүлэлтийн үйл ажиллагааг хэрэгжүүлэх үүрэгтэй гэж заасан байдаг. Энэхүү стратеги, хууль тогтоомжийн уялдаа нь Монгол Улсын Засгийн газар кибер аюулгүй байдлын судалгааг өргөжүүлж, дотоодын инновацыг хөгжүүлэх сонирхолтой байгааг илэрхийлж байна.

Монгол Улсад кибер аюулгүй байдлын судалгаа, хөгжүүлэлтийн ажил зарим оролцогч талуудын оролцоотойгоор хийгдэж байгаа хэдий ч өргөн хүрээнд хөгжсөн гэж үзэх боломжгүй байна. Монголын их, дээд сургуулийн судлаачид олон улсын сэтгүүлүүдэд кибер аюулгүй байдал, мэдээллийн аюулгүй байдлын чиглэлээр судалгааны бүтээл хэвлүүлсэн бөгөөд зарим их сургууль кибер аюулгүй байдлын инновацын судалгааг хөгжүүлэхэд анхаарч байгаа талаар мэдэгдсэн. Голлох бүлгийн хэлэлцүүлгийн үеэр Монголын их, дээд сургуулийн судалгаа, хөгжүүлэлтийн үйл ажиллагаанд техник, хүний нөөцийн хязгаарлагдмал байдал ихээхэн хүндрэл учруулж буйг онцолсон бөгөөд энэ нь D3.2 (Кибер аюулгүй байдлын боловсрол) хүчин зүйлд дурдсан асуудлуудтай уялдаж байна. Олон улсын болон бүс нутгийн судалгааны консорциум, хамтын ажиллагааны сүлжээнд идэвхтэй судалгааны баг байхгүй нь судалгааны хөгжлийг хязгаарлаж байгаа

[65] UN e-Mongolia Assessment, p. 59

нэг хүчин зүйл болж байна. Мөн судалгааны болон эрдэм шинжилгээний ажлын үр дүнг үнэлэх, мэргэжлийн үнэлгээ хийх тогтолцоо хангалтгүй байна. Академийн хүрээнээс гадна хувийн хэвшлийн байгууллагууд кибер аюулгүй байдлын судалгаа, хөгжүүлэлтийн чиглэлд идэвхтэй ажиллаж буйг харуулах нотолгоо илрээгүй.

ЗӨВЛӨМЖ

Кибер аюулгүй байдлын мэдлэг, чадавхыг хөгжүүлэх хүрээнд Монгол Улсын өнөөгийн байдалд хийсэн үнэлгээний үр дүнд дараах зөвлөмжүүдийг дэвшүүлж байна. Эдгээр зөвлөмжүүд нь Дэлхийн Кибер Аюулгүй Байдлын Чадавхын Үнэлгээний Загвар (GCSCC Cybersecurity Capacity Maturity Model)-ын зарчмуудыг харгалзан Монгол Улсын кибер аюулгүй байдлын чадавхыг нэмэгдүүлэхэд чиглэсэн арга хэмжээ, алхмуудыг тодорхойлох зорилготой.

КИБЕР АЮУЛГҮЙ СЭТГЭЛГЭЭ БИЙ БОЛГОХ

R3.1.1 Кибер аюулгүй байдлын зөвлөлийн удирдлага дор Монгол Улсын олон нийтэд зориулсан кибер аюулгүй байдлын нэгдсэн мэдлэг олгох хөтөлбөрийг бий болгох. Энэхүү хөтөлбөр нь дараах зүйлсийг агуулна:

- Монгол Улсад кибер аюулгүй байдлын мэдлэгийг дээшлүүлэх үйл ажиллагааг зохицуулах, цар хүрээг өргөжүүлэх, санаачилгуудын давхардлыг арилгах зорилготой зохицуулах хороо эсхүл бусад холбогдох байгууллагыг байгуулах. Энэ байгууллага нь доорх үйл ажиллагаанууд болон арга хэмжээнүүдийн хэрэгжилтийг хариуцна.
- Монгол Улсад цахим боловсрол, мэдлэгийн түвшний талаарх одоо байгаа судалгаануудыг нэгтгэн, мөн Үндэсний төвийн Кибер халдлага, зөрчлийн бүртгэлийн санд цугларсан кибер гэмт хэргийн мэдээлэлд үндэслэн нотолгоонд суурилсан үнэлгээг хийж, үндэсний хэмжээнд байгаа мэдлэгийн дутмаг байдлыг тодорхойлох.
- Засгийн газар, хууль сахиулах байгууллагууд, хувийн хэвшил, иргэний нийгэм, олон улсын түншүүдийн идэвхтэй оролцоог хангахын тулд зөвлөлдөх уулзалтууд зохион байгуулах, ингэснээр үндэсний хэмжээний кибер аюулгүй байдлын мэдлэг олгох санаачилгуудыг нэгтгэж, Кибер аюулгүй байдлын үндэсний стратегийн зорилтуудыг хангахуйц уялдаа бүхий хэрэгжилтийг баталгаажуулах.
- Олон төрлийн харилцаа холбооны сувгаар дамжуулан өргөн хүрээний сургалтын болон мэдээллийн материалыг бэлтгэж, сурталчлан түгээх.
    - Эдгээр материалыг зорилтот хэрэглэгчдийн мэдээлэл хүлээн авах дадал, хэв маягт нийцүүлэн агуулгын хувьд тохируулж боловсруулах.
    - Эмзэг бүлгүүд (жишээлбэл: бага орлоготой иргэд, цагаачид, алслагдсан бүс нутгийн оршин суугчид, ахмад настнууд, хөгжлийн бэрхшээлтэй иргэд) болон жижиг бизнесийн мэдлэгийг нэмэгдүүлэх тусгай хэсгийг багтаах.
    - Материалуудыг бүх хүнд хүртээмжтэй, соёлын болон хэлний хувьд тохиромжтой хэлбэрээр боловсруулах.
- Кибер аюулгүй байдлын талаарх мэдлэгийг нэмэгдүүлэхээс гадна зорилтот бүлгийн дунд хандлагын эерэг өөрчлөлтийг дэмжих зорилготой үйл ажиллагаа, материалуудыг боловсруулах.
- ЖАЙКА-н хэрэгжүүлж буй кибер аюулгүй байдлын мэдлэг олгох үйл ажиллагааг дэмжиж, илүү өргөн хүрээнд уялдуулан ажиллах.

- Өмнө болон одоо хэрэгжиж буй бүх мэдээлэл, мэдлэг нэмэгдүүлэх кампанит ажлын материалыг хадгалах, байнга сурталчлан түгээх зориулалттай үндэсний кибер аюулгүй байдлын портал (мэдээллийн нэгдсэн эх сурвалж) хөгжүүлэх.

R3.1.2 Өндөр түвшний шийдвэр гаргагчид болон бусад төр, хувийн хэвшлийн удирдлагад чиглэсэн кибер аюулгүй байдлын сургалт, мэдлэг олгох хөтөлбөрийг боловсруулах. Оролцогч талуудыг идэвхтэй хамруулахын тулд эдгээр хөтөлбөрт зохих гэрчилгээ олгох боломжийг судлах, мөн оролцоог нэмэгдүүлэх урамшууллын механизмыг харгалзан үзэх.

R3.1.3 Хөдөө орон нутгийн иргэдэд зориулсан тусгайлсан кибер аюулгүй байдлын сургалт, мэдлэг олгох хөтөлбөрийг боловсруулах. Эдгээр хөтөлбөрийг тухайн бүс нутгийн онцлогт нийцүүлэхийн тулд орон нутгийн удирдлагуудтай хамтран ажиллах боломжийг судлах, мөн сургалтыг зохион байгуулах зориулалттай тусгай сургалтын нэгжүүд эсхүл элч төлөөлөгчдийг томилох арга хэмжээг авч хэрэгжүүлэх. Эдгээр үйл ажиллагааг **R2.2.1**-д санал болгосон хөдөө орон нутгийн иргэдэд зориулсан цахим боловсролын сургалтуудтай уялдуулан хэрэгжүүлэх.

R3.1.4 Төрийн байгууллагуудын нийт албан хаагчдад зориулан кибер аюулгүй байдлын мэдлэг, чадварыг нэмэгдүүлэх, төрийн байгууллагуудын кибер тэсвэртэй байдлыг сайжруулах зорилгоор зорилтот сургалт болон мэдлэг олгох хөтөлбөрийг боловсруулах шаардлагатай. Уг хөтөлбөрийг **R2.1.2**-д санал болгосон цахим сургалт болон үнэлгээний порталтой уялдуулан зохицуулах.

R3.1.5 Үндэсний кибер аюулгүй байдлын мэдлэг олгох хөтөлбөрийг зохион байгуулах, хэрэгжүүлэх үйл ажиллагааг тогтвортой санхүүжилтээр хангах. Зохион байгуулах үйл ажиллагааг үр дүнтэй явуулах зорилгоор хүний нөөцийн зардлыг тусгайлан хуваарилах боломжийг судлах.

R3.1.6 Кибер аюулгүй байдлын боловсролын талаарх мэдээллийг цуглуулах үндэсний хэмжүүрийн (Metrics) системийг бий болгож, боловсролын үйл ажиллагааг хянан үнэлэх, сайжруулахад ашиглах. Энэхүү систем нь кибер аюулгүй байдлын мэдлэгийн хангамж, эрэлт хэрэгцээний статистик мэдээллийг агуулж болно.

КИБЕР АЮУЛГҮЙ БАЙДЛЫН БОЛОВСРОЛ

R3.2.1 Бага болон дунд сургуулийн боловсролын бодлого, хөтөлбөрийн удирдах байгууллагыг кибер аюулгүй байдлын тэргүүлэх байгууллагуудтай хамтран ажиллуулж, сургуулийн үндэсний хөтөлбөрт суурь түвшний кибер аюулгүй байдлын мэдлэг, аюулгүй байдлын агуулгыг тусгах зорилгоор үнэлгээ хийж, шинэчлэн сайжруулах ажлыг хэрэгжүүлэх шаардлагатай.

R3.2.2 Ерөнхий боловсролын сургууль болон их, дээд сургуулийн түвшинд сурагчдад кибер аюулгүй байдлын карьерийн боломжуудыг тодорхой ойлгомжтой хүргэх, сурталчлах арга замуудыг тодорхойлох. Ингэснээр кибер чиглэлийн дээд боловсролын хөтөлбөрт ирээдүйн элсэлтийг сааруулахуйц мэргэжлийн ойлголт, мэдээллийн хомсдолыг арилгах боломжтой болно.

R3.2.3 Компьютерийн ухааны (эсхүл STEM) бус чиглэлийн хүмүүсийг кибер аюулгүй байдлын хичээл, сургалтанд хамрагдахыг уриалах, дэмжих арга хэмжээг хэрэгжүүлэх.

R3.2.4 Монгол Улсын Засгийн газар болон дээд боловсролын салбар хамтран кибер аюулгүй байдлын хөтөлбөрт элсэхэд тулгарч буй санхүүгийн саад бэрхшээлийг арилгах, бууруулах арга хэмжээг хэрэгжүүлэх шаардлагатай. Үүнд тэтгэлэг, сургалтын төлбөрийн хөнгөлөлт, салбарын хамтарсан санхүүжилт зэрэг арга хэмжээг ашиглах боломжийг

судалж, суралцагчдын санхүүгийн дарамтыг бууруулж, кибер аюулгүй байдлын хөтөлбөрийг илүү сонирхолтой, хүртээмжтэй болгох.

R3.2.5 Монголын ерөнхий боловсролын сургууль болон дээд боловсролын байгууллагуудад ажилын байранд бэлэн, чадварлаг кибер аюулгүй байдлын мэргэжилтэн бэлтгэхэд шаардлагатай мэдээллийн технологийн сургалтын орчныг сайжруулах. Ингэхийн тулд их дээд сургууль, хувийн хэвшил болон төрийн байгууллагуудын хамтарсан санхүүжилтийн загваруудыг судалж, хэрэгжүүлэх боломжийг тодорхойлох нь зүйтэй.

R3.2.6 Дотоодын боловсролын салбарын хязгаарлалтуудыг даван туулах зорилгоор "хоёр дээр нэмэх хоёр" (2+2) хөтөлбөрүүдийг өргөжүүлж, сайжруулах. Үүний зэрэгцээ, оюутнуудыг гадаадад суралцаж төгссөний дараа эх орондоо буцаж ажиллах нөхцөлийг хангах зохицуулалтыг хэрэгжүүлэх. Жишээлбэл, тэтгэлэгт хөтөлбөрийг гадаадад суралцаад буцаж ирж дотоодын хөдөлмөрийн зах зээлд ажиллах нөхцөлтэйгөөр олгох боломжийг судлах.

R3.2.7 Монгол Улсад кибер аюулгүй байдлын багш, судлаачдын чадавхыг нэмэгдүүлэх, энэ чиглэлээр ажиллах боловсон хүчнийг нэмэгдүүлэх зорилгоор сургалтын хөтөлбөрт хөрөнгө оруулах. Эдгээр хөтөлбөрүүдийг ЖАЙКА -н энэ чиглэлээр хэрэгжүүлж буй үйл ажиллагаанд тулгуурлан хөгжүүлж, “сургагчыг сургах” (train-the-trainer) аргачлалыг багтаах.

R3.2.8 Кибер аюулгүй байдлын сургалтын хөтөлбөрүүдийн хэрэгцээ, хангамж болон төгсөгчдийн хөдөлмөрийн зах зээл дэх эрэлт, нийлүүлэлтийг хянах зорилгоор хөтөлбөрийн үнэлгээний процесс болон үр дүнд чиглэсэн хэмжүүрүүдийг хэрэгжүүлэх.

R3.2.9 *Кибер аюулгүй байдлын үндэсний стратегид* (КАБҮС) тусгагдсан зорилтуудтай нийцүүлэн, дээрх зөвлөмжүүдийг ашиглан кибер аюулгүй байдлын үндэсний боловсролын стратегийг боловсруулах. Энэхүү стратеги нь кибер аюулгүй байдлын боловсролын хүртээмж, зохион байгуулалтыг сайжруулах урт хугацааны нийтлэг зорилтыг тодорхойлохын зэрэгцээ, стратегийн олон төрлийн бүрэлдэхүүн хэсгүүдийг хэрэгжүүлэх хариуцлагатай оролцогч талуудыг томилж, тогтвортой санхүүжилт хуваарилах механизмыг бүрдүүлэх шаардлагатай.

КИБЕР АЮУЛГҮЙ БАЙДЛЫН МЭРГЭЖЛИЙН СУРГАЛТ

R3.3.1 Кибер Аюулгүй Байдлын Зөвлөлийн удирдлага дор төр, хувийн хэвшил, олон улсын түншүүд болон эрдэм шинжилгээний байгууллагуудын оролцоотойгоор тогтвортой санхүүжилттэй үндэсний кибер аюулгүй байдлын хүний нөөцийн сургалтын санаачлагыг хэрэгжүүлж, кибер аюулгүй байдлын мэргэжилтний чанар болон тоог нэмэгдүүлэх шаардлагатай. Уг хөтөлбөр дараах арга хэмжээг хэрэгжүүлэх шаардлагатай:

- Монгол Улс дахь кибер аюулгүй байдлын сургалтын хөтөлбөрүүдийг тодорхойлох, уялдуулан зохицуулах, өргөжүүлэх ажлыг хариуцах, олон нийтийн хүчтэй дэмжлэг бүхий удирдах хороо/зөвлөл байгуулах эсхүл бусад тодорхойлогдсон байгууллагыг ашиглан, дараах арга хэмжээг хэрэгжүүлэх шаардлагатай.
- Одоогийн судалгаа эсхүл шинэ үнэлгээнд тулгуурлан, Монгол Улсын мэргэжлийн ажиллах хүчний кибер ур чадварын зөрүүг нотолгоонд суурилсан байдлаар судалж, сургалтын хөрөнгө оруулалтын тэргүүлэх чиглэлүүдийг тодорхойлох.
- Илэрсэн ур чадварын зөрүүг арилгахын тулд холбогдох оролцогч талуудтай өргөн хүрээний зөвлөлдөх уулзалтуудыг зохион байгуулж үндэсний кибер аюулгүй байдлын хүний нөөцийн хөгжлийн стратеги, хэрэгжилтийн төлөвлөгөө боловсруулах.

- Одоогийн мэргэжлийн сургалтын хөтөлбөрүүд, шинжээчдийн туршлага дээр тулгуурлан хэрэгжилтийн төлөвлөгөөг удирдан зохион байгуулж, давхардсан санаачилгуудыг арилгах.
- Кибер аюулгүй байдлын модулиудыг сургууль, мэргэжил сургалтын төв, олон нийтийн бүлгүүдийн цахим ур чадварын сургалтын хөтөлбөрт нэгтгэх.
- Кибер аюулгүй байдлын хамгийн сүүлийн үеийн олон улсын стандартыг Монголын нөхцөл байдалд нийцүүлэн орчуулах, нутагшуулах ажлыг дэмжих. Энэ нь дотоодын боловсролын чанарыг сайжруулахад тус дөхөм болох бөгөөд **R4.1.4** болон **R5.1.2**-тэй уялдуулан хэрэгжүүлнэ.
- Сургалтын хөтөлбөрийн үр өгөөж, үр дүнг нэмэгдүүлэхийн тулд шаардлагатай хүмүүсийг зөв сургалтад хамруулах механизмыг тодорхойлох.
- Сургалтын зардлын хүндрэлийг бууруулах, арилгах боломжит механизмуудыг судалж, оролцооны түвшинг нэмэгдүүлэх урамшууллын арга хэмжээг хэрэгжүүлэх. **R3.2.4**-тэй уялдуулах.

R3.3.2 **R3.1.4**-д заасны дагуу, кибер аюулгүй байдлын боловсролын талаар мэдээлэл цуглуулах үндэсний хэмжүүрийн (Metrics) системийг бий болгож, боловсролын үйл ажиллагаа болон сургалтын хөтөлбөрийг хянан үнэлэх, шинэчлэхэд ашиглах. Энэхүү систем нь кибер аюулгүй байдлын мэдлэгийн хангамж, эрэлт хэрэгцээний статистик мэдээллийг агуулж байх боломжтой.

R3.3.3 ЦХИХХЯ-ийн кибер аюулгүй байдлын мэргэжилтнүүдэд зориулсан тусгай цалингийн хөнгөлөлт олгох хүчин чармайлтыг дэмжих, ингэснээр төрийн байгууллагууд хувийн салбартай өрсөлдөх чадвар бүрдэнэ. Одоогийн кибер аюулгүй байдлын тусгайлсан квотын талаарх агентлагуудын мэдлэг, ашиглах байдлыг нэмэгдүүлэх арга замуудыг судлах. Мэргэшсэн кибер аюулгүй байдлын ажилтнуудад зориулсан боломжит цалингийн нэмэгдлийн талаар авч үзэх.

R3.3.4 Төрийн албанд кибер аюулгүй байдлын мэргэжилтнүүдийг тогтвортой ажиллуулах нөхцөлийг сайжруулахын тулд, сургалтын боломжууд болон цалин хөлсний өсөлтийг агуулсан, бүтэцлэгдсэн, ил тод карьерийн замнал боловсруулах. Үндэсний аюулгүй байдалд чухал ач холбогдолтой кибер аюулгүй байдлын хүний нөөцтэй хамтран, тухайн ажилтны зорилго, нөхцөл байдалд тохирсон тусгай карьерийн төлөвлөгөө боловсруулахыг судлах. Мөн олон улсын гэрчилгээ олгоход дэмжлэг үзүүлэх, үүнийг тодорхой хугацаанд төрийн байгууллагад ажиллах шаардлагатайгаар холбох зэрэг урамшууллын механизмуудыг эдгээр төлөвлөгөөнд тусгах боломжийг судлах.

R3.3.5 Төрийн албанд ажиллаж буй кибер аюулгүй байдлын мэргэжилтнүүдийн тогтвортой байдлыг сайжруулахын тулд, хүний нөөцийн хэт ачааллыг бууруулах, мэргэжлийн ядаргаа үүсэхээс сэргийлэх удирдлага болон ажлын ачааллыг хуваарилах зохицуулалтыг хэрэгжүүлэх. ЦХИХХЯ, ТЕГ зэрэг тэргүүлэх кибер аюулгүй байдлын байгууллагуудын удирдлагын үйл ажиллагааг дэмжиж, бүх боломжит ажлын байрыг бүрэн бүрдүүлэхэд нэмэлт арга хэмжээ авах. Мөн шаардлагатай тохиолдолд, ажилтнуудын тоог нэмэгдүүлэх боломжийг судлах.

R3.3.6 Кибер аюулгүй байдлын чиглэлээр олон нийтийн болон хувийн хэвшлийн түншлэлийг бэхжүүлж, салбар хоорондын мэдлэг солилцоо, чадавхыг хөгжүүлэх арга хэмжээг хэрэгжүүлэх. Мөн хувийн хэвшлийн мэргэжилтнүүдийг төрийн байгууллагын кибер аюулгүй байдлын албан тушаалд тодорхой хугацаагаар ажиллуулах (secondment) боломжийг судлах нь үр өгөөжтэй байж болохыг анхаарах.

КИБЕР АЮУЛГҮЙ БАЙДЛЫН СУДАЛГАА, ИННОВАЦ

R3.4.1 ХИХХЯ-д Кибер аюулгүй байдлын тухай хуульд заасан дагуу кибер аюулгүй байдлын чиглэлээр судалгаа, хөгжүүлэлтийн үйл ажиллагаа явуулахад зориулан санхүүжилт олгох.

R3.4.2 Кибер аюулгүй байдлын үндэсний стратегид (КАБҮС) заасны дагуу, кибер аюулгүй байдлын судалгааг дэмжих зорилгоор их, дээд сургуулиудад судалгааны тэтгэлэг олгох санхүүжилтийн механизмыг бий болгох.

R3.4.3 Монгол Улсын Засгийн газар их, дээд сургуулийн судлаачдад дэмжлэг үзүүлж, тэдний судалгааны бүтээгдэхүүнийг арилжааны хэлбэрт шилжүүлэх, дотоодын кибер аюулгүй байдлын зах зээлийг өргөжүүлэх боломжийг судлах хэрэгтэй.

R3.4.4 Үндэсний болон стратегийн түвшинд хамгийн өндөр хэрэгцээтэй кибер аюулгүй байдлын судалгааны төслүүдийг тодорхойлох санаачилгуудыг хөгжүүлж, эдгээр төслүүдийг дэмжих боломжийг судлах.

ХЭМЖЭЭС 4
ХУУЛЬ, ЭРХ ЗҮЙН ЗОХИЦУУЛАЛТ

Энэхүү хэмжээс нь кибер аюулгүй байдалтай шууд болон шууд бусаар холбоотой үндэсний хууль тогтоомжийг боловсруулах, хэрэгжүүлэх төрийн чадавхыг үнэлнэ. Тус үнэлгээ нь кибер аюулгүй байдлын зохицуулалтын шаардлага, кибер гэмт хэрэгтэй холбоотой хууль тогтоомж болон холбогдох бусад эрхзүйн зохицуулалтыг онцгойлон авч үзнэ. Ийм хууль тогтоомжийг хэрэгжүүлэх чадамжийг хууль сахиулах байгууллага, прокурорын байгууллага, зохицуулагч байгууллага болон шүүхийн тогтолцооны чадамжийн хүрээнд үнэлдэг. Мөн, энэхүү хэмжээс нь кибер гэмт хэрэгтэй тэмцэхэд чиглэсэн албан болон албан бус хамтын ажиллагааны механизмуудыг судлах болно.

ҮР ДҮНГИЙН ТОЙМ

D 4.1 ХУУЛЬ, ЭРХ ЗҮЙН ЗОХИЦУУЛАЛТУУД

Энэхүү хүчин зүйл нь кибер аюулгүй байдалтай холбоотой хууль, зохицуулалтын заалтуудыг авч үздэг бөгөөд үүнд хууль, зохицуулалтын шаардлага, кибер гэмт хэргийн материаллаг болон процессын хууль тогтоомж, хүний эрхийн нөлөөллийн үнэлгээ зэрэг асуудлууд багтана.

Түвшин: Эхлэл түвшнээс Тогтворжсон түвшинд

Кибер гэмт хэргийн зохицуулалтууд:

2015 оны *Эрүүгийн хуулийн* 26.1, 26.2 дугаар зүйлд компьютерийн өгөгдөл, системийн нууцлал, бүрэн бүтэн байдал, хүртээмжтэй байдлыг хамгаалах кибер гэмт хэргийн материаллаг эрх зүйн зохицуулалтыг тусгасан. Эдгээр зүйл заалтад хууль бус хандалт; өгөгдөлд халдах; системд халдах; төхөөрөмжийг зүй бусаар ашиглах; мэдээллийг хууль бусаар замаас нь барьж авах гэх мэт заалтууд багтсан. Уг хууль нь мэдээллийн систем, мэдээллийн сүлжээ, төрийн нэгдсэн мэдээллийн сүлжээ болон төрийн нууц мэдээллийг агуулсан онц чухал мэдээллийн дэд бүтцийн эсрэг үйлдсэн хууль бус халдлагад хатуу хариуцлага хүлээлгэх зохицуулалттай. Өмнө нь эдгээр гэмт хэргийг мөрдөн шалгах хариуцлагыг зөвхөн Цагдаагийн байгууллага хүлээж байсан бол хуульд орсон өөрчлөлтийн дагуу одоо Тагнуулын ерөнхий газар (ТЕГ) нь төрийн сүлжээ, онц чухал мэдээллийн дэд бүтцийн байгууллага болон төрийн нууцтай холбоотой халдлагыг мөрдөн шалгах үүрэг хүлээх болсон.

2015 оны *Эрүүгийн хууль* нь компьютертэй холбоотой гэмт хэргийг зохицуулсан заалтыг агуулсан бөгөөд эдгээр нь залилан, хуурамч баримт үйлдэхтэй холбоотой асуудлыг гэмт хэрэгт тооцно.

Жишээлбэл, компьютер ашиглан хуурамч баримт бүрдүүлэхтэй холбоотойгоор, 23.2 дугаар зүйлд "Хуурамч баримт бичиг үйлдэх, ашиглах" гэмт хэргийг хууль бус үйлдэл хэмээн тодорхойлсон бөгөөд энэ нь "биет бус" буюу цахим баримтуудыг ч хамрах боломжтой. Энэ зүйлд хөрөнгө эзэмших, ашиглах эсхүл зарах эрхийг хуурамчаар олгосон баримтуудыг тодорхой зааж дурдсан байна. Компьютер ашиглан залилан үйлдэхтэй холбоотой 17-р бүлэг "Өмчийн эсрэг гэмт хэрэг"-ийн 17.3 дугаар зүйлд баримт бичиг, эд зүйл, цахим төхөөрөмж ашиглан бусдыг төөрөгдүүлэх үйлдлийг гэмт хэрэгт тооцсон. Мөн Эрүүгийн хуулийн 18-р бүлэг "Эдийн засгийн гэмт хэрэг"-ийн 18.7 дугаар хэсэгт "Хуурамч мөнгөн тэмдэгт, үнэт цаас, төлбөрийн хэрэгсэл бэлтгэх, ашиглах" үйлдлийг гэмт хэрэг гэж үзсэн бөгөөд үүнд цахим карт болон бусад төлбөрийн хэрэгслээр дамжуулан хуурамч санхүүгийн баримт бүрдүүлэх үйлдэл багтана. Үүний адил 18.18 дугаар зүйлд Монгол Улсын "Үндэсний төлбөрийн систем"-ийн хүрээнд төлбөрийн үйлчилгээ үзүүлэгч операторууд компьютер ашиглан залилан үйлдэхийг гэмт хэрэгт тооцсон байна. Эцэст нь, 2015 оны Эрүүгийн хууль нь цахим орчинд үйлдэгдсэн гэж тодорхой заагаагүй ч, агуулгын хувьд цахим үйл ажиллагаанд хамаарах хэд хэдэн гэмт хэргийг агуулдаг. Үүнд:

- 13.12 дугаар зүйл "Хууль бус мөшгих"
- 13.14 дугаар зүйл "Худал мэдээлэл тараах"
- 14.1 дугаар зүйл "Ялгаварлан гадуурхах"

Монгол Улсын хуулиар тогтоосон кибер гэмт хэрэг бүр нь үр дүнтэй, зохистой, урьдчилан сэргийлэх зорилготой шийтгэл хүлээлгэх шаардлагатай арга хэмжээг агуулдаг. Эдгээр шийтгэлд санхүүгийн торгууль болон эрх чөлөөг хасах ял багтах бөгөөд гэмт хэргийн ноцтой байдал, шинж чанарт тохируулан өөрчлөх боломжтой байдаг. 2015 оны *Эрүүгийн хууль* болон түүний кибер гэмт хэрэгтэй холбоотой заалтуудыг хэрэгжүүлэхэд 2019 оны "Гэмт хэрэг, зөрчлөөс урьдчилан сэргийлэх тухай хууль" дэмжлэг үзүүлдэг. Тус хууль нь тодорхой гэмт хэрэг, зөрчлийн шалтгаан, нөхцөлийг арилгах чиглэлээр эрх бүхий байгууллагуудын авч хэрэгжүүлж болох арга хэмжээг тодорхойлсон байдаг. Голлох бүлгийн хэлэлцүүлэгт оролцогч зарим хүмүүс кибер гэмт хэргийг мөрдөн шалгаж, шүүхээр шийдвэрлэсэн тохиолдолд ихэвчлэн гэмт этгээдэд бага хэмжээний торгууль ногдуулдаг гэж үзэж байгаагаа илэрхийлсэн. Гэсэн хэдий ч кибер гэмт хэргийн шийтгэлийн ноцтой байдал нь хэд хэдэн нөхцөл байдлаас хамаарах тул дээрх мэдээллийн үнэн зөв байдал баталгаажаагүй болно. Зарим оролцогчдын дунд гэмт этгээдэд оногдуулж буй эрүүгийн ял шийтгэл нь кибер гэмт хэргийг үр дүнтэйгээр таслан зогсоож чадахгүй байгаа гэх түгээмэл ойлголт байгааг анхаарах нь зүйтэй.

Баримт бичигт тулгуурласан судалгаа болон бүлгийн хэлэлцүүлгийн явцад кибер гэмт хэрэгтэй холбоотой "оролдлого, туслалцаа үзүүлэх болон хамтран үйлдэх" гэсэн заалтууд Монгол Улсын хууль тогтоомжид бүрэн тодорхойлогдсон эсэх нь илрээгүй. Үүний зэрэгцээ байгууллагын эрх зүйн хариуцлагын талаар (өөрөөр хэлбэл, хууль эрх зүйн этгээдүүд кибер гэмт хэрэг үйлдэхэд хариуцлага хүлээх зохицуулалт) хангалттай байж чадахгүй байна. Иймээс Монгол Улсын хууль тогтоомж нь олон улсын гэрээ, конвенцүүдэд заасан кибер гэмт хэргийн зохицуулалтуудаас давсан зохицуулалттай эсэх нь тодорхойгүй байна. Мөн хиймэл оюун ухаан, машин сургалт, квант тооцоолол зэрэг шинэ технологиудтай холбоотой кибер аюул заналыг тооцсон хууль эрх зүйн өөрчлөлт хийгдсэн гэсэн нотолгоо илрээгүй.

Үнэлгээ хийгдэж байх үед Монгол Улс кибер гэмт хэрэгтэй холбоотой бүс нутгийн болон олон улсын гэрээ, конвенцүүдийг батлаагүй байсан боловч Будапештын Конвенц зэрэг

олон улсын эрх зүйн баримт бичгийн сайн туршлагыг нэвтрүүлэх алхмууд хийж байна. Голлох бүлгийн хэлэлцүүлгээс харахад 2023 онд Монгол Улс Будапештын Конвенцод нэгдүүлэх бэлтгэл хангах үүрэг бүхий хороо байгуулагдсан бөгөөд энэхүү хороо нь Дэд сайдын удирдлага дор ажиллаж байгаа гэж мэдээлэгдсэн.

Кибер аюулгүй байдлын хууль эрх зүй болон зохицуулалтын шаардлагууд:

2021 оны *Кибер аюулгүй байдлын тухай хууль* нь онц чухал мэдээллийн дэд бүтэцтэй байгууллагууд болон бусад холбогдох оролцогч талууд мөрдөх кибер аюулгүй байдлын иж бүрэн шаардлагыг тогтоосон. 2022 оноос хүчин төгөлдөр үйлчилж эхэлсэн уг хуульд заасны дагуу, 16, 17, 19 дүгээр зүйлд тодорхойлсон хуулийн этгээд нь Кибер аюулгүй байдлын нийтлэг журмыг мөрдөх, тогтмол кибер аюулгүй байдлын эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудит хийлгэх үүрэгтэй. Эдгээр үйл ажиллагааны тодорхой шаардлагуудыг тус хуулийн 7, 8, 9 дүгээр зүйлд тусгасан. Тус хуулийг зөрчсөн тохиолдолд хүлээлгэх эрүүгийн болон иргэний хариуцлагыг 2015 оны Эрүүгийн хууль, 2019 оны Гэмт хэрэг, зөрчлөөс урьдчилан сэргийлэх тухай хууль, 2017 оны Төрийн албаны тухай хууль, 1999 оны Хөдөлмөрийн тухай хуульд тус тус заасан байдаг.

Ялангуяа ОЧМДБ байгууллагуудтай холбоотойгоор, 2021 оны *Кибер аюулгүй байдлын тухай хуулийн* 19-р зүйл нь ямар байгууллагууд уг ангилалд хамаарахыг тодорхойлж, дагаж мөрдөх шаардлагуудыг тогтоосон. Үүнд, гэхдээ үүгээр хязгаарлагдахгүй: кибер аюулгүй байдлыг хангах дотоод журмыг хэрэгжүүлэх; кибер халдлага болон зөрчлийн үед авах арга хэмжээний төлөвлөгөө боловсруулах, хэрэгжүүлэх; кибер аюулгүй байдлыг хариуцсан ажилтан эсхүл нэгж байгуулах; жил бүр эрсдэлийн үнэлгээ хийлгэх; хоёр жил тутамд мэдээллийн аюулгүй байдлын аудит хийлгэх; мөн мэдээллийн систем, дэд бүтцийн хэвийн, тасралтгүй ажиллагаа кибер халдлага, зөрчилтэй холбоотойгоор доголдсон тохиолдолд холбогдох кибер хадлага, зөрчилтэй тэмцэх төвд тэр даруй мэдээлэх зэрэг үүргүүд багтана.

2021 оны ОЧМДБ оруулаад *Кибер аюулгүй байдлын тухай хуульд* заасан бүх хуулийн этгээд, тэдгээрийн нэмэлт үүрэг, хариуцлагыг *Кибер аюулгүй байдлын нийтлэг журмаар* нарийвчлан заасан байдаг. Эдгээр нь кибер аюулгүй байдлын удирдлага зохион байгуулалтаас авхуулаад кибер халдлага, зөрчлөөс урьдчилан сэргийлэх, илрүүлэх, мэдээллийн систем болон сүлжээг сэргээх шаардлагуудаас бүрдэнэ. Энэхүү журмыг боловсруулахдаа ЦХИХХЯ нь NIST, ISO зэрэг олон улсын стандартад нийцүүлэхийг зорьж, байгууллагууд нэмэлт дүрэм журмыг сонгон ашиглах боломжийг олгох байдлаар боловсруулжээ. Уг журмын 1.3-р зүйлд “зохицуулалтын шаардлагууд давхацсан тохиолдолд хамгийн өндөр шаардлага тогтоосон олон улсын стандарт, зохицуулалт, журам хүчин төгөлдөр байна” гэж заасан тул хамрах хүрээнд нь хамаарах байгууллагуудын хувьд уг журам нь дээд хязгаар биш, харин үндэсний суурь стандартын үүрэг гүйцэтгэдэг. ЦХИХХЯ нь ОЧМДБ байгууллагуудтай хамтран шинэ хууль, шаардлагуудыг тайлбарлах сургалтуудыг зохион байгуулсан.

Бүлгийн хэлэлцүүлгээр ОЧМДБ байгууллагууд олон улсын стандартыг өөрсдөө сонгох боломж олгосон шийдвэрийг оролцогч талууд янз бүрийн байдлаар хүлээн авсан. Зарим байгууллага энэ эрх чөлөөг сайшаан хүлээж авч, Засгийн газраас тодорхой стандарт мөрдөхийг заагаагүйд сэтгэл хангалуун байгаагаа илэрхийлсэн. Харин зарим оролцогч талууд илүү нэгдмэл арга барилыг дэмжиж, Засгийн газар илүү тодорхой чиглэл өгөөгүйд шүүмжлэлтэй хандсан байна. Засгийн газраас баримталж буй уян хатан

хандлагатай холбоотой нэг бэрхшээл нь олон улсын стандартуудыг Монгол улсын нөхцөл байдал, хэлний онцлогт онцлогт тохируулан хөрвүүлж, нутагшуулах ажил хангалтгүй байгаад оршиж байна. Үүний улмаас аюулгүй байдлын түвшингээ сайжруулж, суурь шаардлагуудыг давуулан хэрэгжүүлэхийг хүссэн байгууллагуудын хувьд энэ үйл явцыг бодит байдал дээр хэрэгжүүлэхэд хүндрэлтэй болгож байна. Кибер аюулгүй байдлын үндэсний стратеги (КАБҮС)-д олон улсын стандартыг нутагшуулахыг үндэсний зорилго гэж тодорхойлсон боловч баримт бичгийн судалгаа, бүлгийн хэлэлцүүлгээр уг асуудлыг шийдвэрлэх ойрын хугацааны төлөвлөгөөг илрүүлж чадаагүй. Дэлгэрэнгүй мэдээллийг 5.1-р хүчин зүйлээс харна уу.

2021 оны *Кибер аюулгүй байдлын тухай хуулийн* гол зорилтуудын нэг нь кибер засаглалын албан ёсны тогтолцоог бүрдүүлэх явдал байсан бөгөөд үүний үр дүнд хэд хэдэн ач холбогдолтой өөрчлөлтүүд бий болсон. Тус хууль нь Монгол Улсад кибер аюулгүй байдлын асуудлыг хариуцах байгууллагуудын чиг үүргийг албан ёсоор тогтоосон. Үүний хүрээнд Кибер аюулгүй байдлын зөвлөл, Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн төв байгууллага (ЦХИХХЯ), Тагнуулын ерөнхий газар (ТЕГ), Зэвсэгт хүчний төрийн аюулгүй байдлын байгууллага болон Цагдаагийн ерөнхий газрын үүрэг хариуцлагыг тодорхойлсон. Хуулийн 4-р бүлэг "Кибер халдлага, зөрчилтэй тэмцэх үйл ажиллагаа" нь кибер халдлага, зөрчилтэй тэмцэх гурван төвийн хамрах хүрээ, үүрэг хариуцлагыг нарийвчлан тогтоосон. Үүнд: Үндэсний төв, Нийтийн төв болон Зэвсэгт хүчний төв багтаж байна. Энэхүү зохицуулалт нь "Кибер аюулгүй байдлын тогтолцоо"-г тодорхой болгосон бөгөөд бүлгийн хэлэлцүүлэгт оролцогчид үүнийг өмнөх засаглалын бүтцээс илүү дэвшилтэт, сайжруулсан арга хэмжээ гэж үзэж байна.

Хууль болон түүнийг дагалдах нийтлэг журам нь Монгол Улсын хууль эрх зүй, засаглалын орчныг сайжруулахад гарцаагүй хувь нэмэр оруулсан хэдий ч шинэчлэгдсэн хууль эрх зүй, зохицуулалтын тогтолцоог хэрэгжүүлэх, дагаж мөрдөхтэй холбоотой асуудлууд хэвээр үлдэж, үндэсний хэмжээнд цаашдын ахицыг сааруулж байна. Бүлгийн хэлэлцүүлэгт оролцогчид *Кибер аюулгүй байдлын тухай хууль* (2021) болон *Кибер аюулгүй байдлын нийтлэг журамд* хамаарах олонх байгууллага эдгээр шаардлагуудыг хэрэгжүүлээгүй, цаашлаад ойрын болон дунд хугацаанд хэрэгжүүлэх чадваргүй байгаа тухай дурдсан. Энэ нь тодорхой хэмжээгээр хууль саяхан буюу 2022 онд хүчин төгөлдөр болсон, мөн дагалдах журам 2025 оны хоёрдугаар хагасаас хэрэгжиж эхлэхээр төлөвлөгдсөнтэй холбоотой. Үүний зэрэгцээ хуулийн хамрах хүрээнд багтаж буй байгууллагууд өөрсдийн хариуцлагыг бүрэн хэрэгжүүлэх чадавх муу байгаагаас гадна Монгол улсын кибер аюулгүй байдлын салбарын байгууллагууд эдгээр хэрэгцээг хангах чадамж хомс байгаа нь ч нөлөөлж байна.

Төсөв, хүний нөөцийн хязгаарлагдмал байдал нь энэхүү тогтолцоог үр дүнтэй хэрэгжүүлэхэд тулгарч буй томоохон саад бэрхшээлүүдийн нэг бөгөөд энэ талаар 3.2 болон 3.3 дугаар хүчин зүйлд дэлгэрэнгүй тусгасан. Хууль болон дагалдах журам хэрэгжиж эхэлснээр Монгол Улсад кибер аюулгүй байдлын мэргэжилтнүүдийн эрэлт мэдэгдэхүйц нэмэгдэж, аль хэдийн хязгаарлагдмал байсан дотоодын мэргэшсэн ажиллах хүчний хүрэлцээтэй асуудал улам хүндэрч байна. Жил тутмын кибер аюулгүй байдлын эрсдэлийн үнэлгээ, хоёр жил тутмын мэдээллийн аюулгүй байдлын аудит, мөн “кибер аюулгүй байдлыг хариуцах алба, нэгж байгуулах” зэрэг шаардлагууд нь ОЧМДБ байгууллагуудад ихээхэн дарамт учруулахаас гадна цаашлаад хүний нөөц, санхүүгийн

хязгаарлагдмал байдлаас шалтгаалан хэрэгжүүлэх боломжгүй гэж төлөөлөгчид үзэж байна. Тэд шинэ үүрэг хариуцлагад тохирсон чадварлаг ажилтнуудыг ажилд авах, эсхүл үнэлгээ хийх мэргэшсэн аудитор, шинжээч олох боломжгүй байгааг онцолж, тогтолцооны хэрэгжилтэд бухимдалтай байна. Одоогийн ажиллах хүчний хувьд хэт ачаалалтай ажиллаж, өргөн цар хүрээтэй ажил үүргээ бүрэн биелүүлэхэд хүндрэлтэй байдалд ордог бөгөөд олонх ажилтан мэргэжлийн ядаргаанд орох асуудал түгээмэл ажиглагддаг. Ялангуяа, энэ асуудал төрийн байгууллагад илүү ноцтой ажиглагдаж байна. Төрийн албаны хязгаарлагдмал цалин урамшуулал, өндөр ажлын ачаалал нь одоо ажиллаж байгаа болон ирээдүйн ажил хайгч нарт төдийлөн сонирхол татахуйц ажил олгогчид тооцогдохгүй байна. Энэ нь дэлхийн хэмжээнд төрийн болон хувийн хэвшлийн байгууллагууд ур чадвартай кибер аюулгүй байдлын мэргэжилтнийг татан ажиллуулах, хөрөнгө оруулах чадавх болон хүсэл эрмэлзлэл хоорондын тэнцвэргүй байдлыг тусган харуулж байна. Үүнээс гадна кибер аюулгүй байдлын төсвийн ангилалгүй, техникийн тоног төхөөрөмж худалдан авах, ховор мэргэшсэн кибер аюулгүй байдлын ажиллах хүчинд чиглэсэн зохих санхүүжилт хангалтгүй байгаа нь эдгээр асуудлыг улам даамжруулж байна.

Эдгээр сорилт нь зөвхөн онц чухал мэдээллийн дэд бүтэц (ОЧМДБ) болон төрийн байгууллагаар хязгаарлагдахгүй бөгөөд энэ тогтолцоог амжилттай хэрэгжүүлэхэд чухал үүрэгтэй кибер аюулгүй байдлын салбарын оролцогч талуудад ч нөлөөлж байна. Бүлгийн хэлэлцүүлгийн үр дүнд 2021 оны Кибер аюулгүй байдлын тухай хуулийн дагуу жил бүр болон хоёр жил тутам хийх эрсдэлийн үнэлгээ, мэдээллийн аюулгүй байдлын аудит хийхээр бүртгүүлсэн хувийн хэвшлийн байгууллагуудын олонх нь хүний нөөцийн хомсдолоос болж эдгээр үүргийг биелүүлэх бодит чадавхгүй байгааг тогтоосон. Засгийн газар байгууллагыг бүртгэхдээ шаардлагатай нөөц, туршлагатай эсэхийг баталгаажуулах шалгуур механизмтай ч кибер аюулгүй байдлын ажиллах хүчний зах зээл байнга өөрчлөгдөж байдаг тул эдгээр баталгаажуулалтын хүчин төгөлдөр байдал урт хугацаанд хадгалагдана гэх баталгаа сул байна.

Иймд Монгол Улс шинэ кибер аюулгүй байдлын хууль, зохицуулалтын тогтолцоог үр дүнтэй хэрэгжүүлэхэд олон талт, нарийн төвөгтэй сорилтуудтай тулгараад байна. Энэхүү тогтолцоог нэвтрүүлснээр хэдийнээ хомс байсан кибер аюулгүй байдлын мэргэжилтнүүдийн эрэлт эрс нэмэгдсэн бөгөөд хэрэгжилтийн бүхий л түвшинд мэргэшсэн хүний нөөцийн дутагдал нь оролцогч талуудын үүргээ биелүүлэх чадварыг сулруулж байна. Үүн дээр санхүүгийн хязгаарлагдмал байдал нэмэгдсэнээр төрийн байгууллагууд хувийн хэвшилтэй өрсөлдөх боломжгүй болж, шаардлагатай мэргэжилтнүүдийг хангалттай хэмжээнд ажиллуулахад бэрхшээл үүсгэж байна. Гэсэн хэдий ч энэ нь уг тогтолцоо хэрэгжих боломжгүй, эсхүл нэн даруй өөрчлөх шаардлагатай гэсэн үг биш юм. Чухамдаа, хууль зохицуулалтын орчныг богино хугацаанд хөгжүүлж эхэлсэн нь төр болон кибер аюулгүй байдлын өргөн хүрээний экосистемийн хувьд гаргасан ахиц дэвшил юм. Ялангуяа, хүний нөөц, төсвийн хязгаарлалтад байсаар ирсэн нөхцөлд энэ амжилт илүү онцлох ач холбогдолтой. Харин энэхүү нөхцөл байдал нь урт хугацааны зогсонги байдал, итгэл алдрах байдлаас урьдчилан сэргийлэхийн тулд хэрэгжилтийн сорилтыг стратегийн түвшинд шийдвэрлэх арга хэмжээг шууд авах шаардлагатайг онцолж байна. Монгол Улс бат бөх суурийг аль хэдийн тавьсан тул цаашид энэхүү тогтолцоог улам сайжруулж, үр ашигтай, үр дүнтэй болгох чиглэлд хөгжүүлэн ажиллах ёстой.

2021 оны *Кибер аюулгүй байдлын тухай хуулиас* гадна, Монгол Улсын өргөн хүрээний хууль тогтоомжийн тогтолцоонд цахим орчинтой холбоотой нэмэлт зохицуулалт хамаарна. 2021 оны *Цахим гарын үсгийн тухай хууль* нь тоон гарын үсэг, цахим тамга болон цахим баримтыг ашиглах эрх зүйн үндсийг тогтоож, үүнтэй холбоотой аюулгүй байдлын шаардлагуудыг мөн тодорхойлсон. Уг хуулийн 6, 7 дугаар зүйлд гарын үсэг, цахим тамгыг шифрлэх болон тайлахад ашиглагдах нийтийн болон хувийн түлхүүрийн хэрэглээг зохицуулсан, харин 8 дугаар зүйлд энэ үйл явцад ашиглагдах тоон гарын үсгийн хэрэгслийн шаардлагуудыг тусгасан. Мөн 9 дүгээр зүйл нь өгөгдлийн бүрэн бүтэн байдлыг хангах цагийн бүртгэлийн зохицуулалтыг багтаасан. Уг хуулийн 7-р бүлэг нь нийтийн түлхүүрийн дэд бүтцийн (PKI) зохицуулалтын тогтолцоог тодорхойлсон бөгөөд үүнд технологийг хэрэгжүүлэх зохицуулалтыг Цахим хөгжил, инновац, харилцаа холбооны яам (ЦХИХХЯ) болон Харилцаа холбооны зохицуулах хороо (ХХЗХ)-д хуваарилсан. Энэхүү зохицуулалтын хүрээнд эдгээр байгууллагууд дараах үүрэг хүлээнэ:

- Нийтийн түлхүүрийн гэрчилгээг үүсгэх, ашиглах, хадгалахтай холбоотой аюулгүй байдлын хяналтын баримт бичгүүдийг боловсруулах;
- Нийтийн түлхүүрийн дэд бүтцийн стандартыг хөгжүүлэх, хэрэгжилтийг хянах;

Мөн, 2001 оны *Харилцаа холбооны тухай хууль* нь харилцаа холбооны болон интернет үйлчилгээ үзүүлэгчдийг зохицуулдаг. Уг хууль нь "Харилцаа холбооны зохицуулах хороо" (ХХЗХ)-д харилцаа холбооны зах зээлд шударга өрсөлдөөний нөхцөлийг бүрдүүлэх үүрэг хүлээлгэсэн. Хуулийн 9-р зүйлд ХХЗХ-ны бүрэн эрхийг тодорхойлж, сүлжээний тоног төхөөрөмжийн гэрчилгээжүүлэлт, харилцаа холбооны стандарт боловсруулах зэрэг зохицуулалтын чиг үүрэг багтдаг. Гэсэн хэдий ч уг хуульд аюулгүй байдалтай холбоотой тусгай зохицуулалт эсхүл харилцаа холбооны зохицуулах байгууллагад харилцаа холбооны болон интернет үйлчилгээ үзүүлэгчдийн цахим аюулгүй байдлыг зохицуулах эрх олгосон заалт тусгагдаагүй байна. Баримт бичгийн судалгаа, голлох бүлгийн хэлэлцүүлгээр ХХЗХ нь мэдээллийн болон кибер аюулгүй байдлын талаар тодорхой стандарт гаргасан гэх баримт олдоогүй. Гэсэн хэдий ч, ОЧМДБ гэж ангилагдсан харилцаа холбооны үйлчилгээ үзүүлэгчид нь 2021 оны *Кибер аюулгүй байдлын тухай хуульд* заасан шаардлагыг дагаж мөрдөх үүрэгтэй. ХХЗХ нь контенттой холбоотой зарим зохицуулалтыг гаргасан бөгөөд үйлчилгээ үзүүлэгчдэд өөрсдийн платформ дээр тодорхой төрлийн контентыг хориглох үүрэг өгсөн. Эдгээр хязгаарлалтууд нь порнографи, терроризм, шашин шүтлэгтэй холбоотой хэрцгий үйлдлүүд, олон нийтийн эмх замбараагүй байдал, зохиогчийн эрх болон бусад ангиллыг хамардаг[66].

Монголбанкны тухай хууль (1996) болон *Монгол Улсын Үндэсний төлбөрийн системийн тухай хууль (2017)* хүрээнд Монголбанкны үүрэг нь Монгол улсын банкны салбар болон "Үндэсний төлбөрийн систем"-ийг хянах зохицуулах үүрэгтэй. Харин 2005 оны "*Санхүүгийн зохицуулах хорооны эрх зүйн байдлын тухай хууль*"-ийн дагуу Санхүүгийн зохицуулах хороо (СЗХ) нь Монгол Улсад үйл ажиллагаа явуулж буй банк бус санхүүгийн байгууллагуудыг хянан зохицуулах үүрэгтэй. Үүнд даатгалын компаниуд, үнэт цаасны зах зээлд оролцогчид, үл хөдлөх хөрөнгө зуучлагчид болон бусад санхүүгийн байгууллагууд багтана. Бүлгийн хэлэлцүүлгийн үеэр эдгээр хоёр

[66]https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.swift.com/swiftresource/251951/download&ved=2ahUKEwiV2JXm-4iKAxVUU0EAHdJQCaAQFnoECBcQAQ&usg=AOvVaw1r1TSBQQJFldru_toTJheo

байгууллага өөрсдийн зохицуулалтын хүрээнд үйл ажиллагаа явуулж буй хуулийн этгээдээс тухайлсан олон улсын стандартыг дагаж мөрдөхийг шаардсан мэдээллийн аюулгүй байдлын зохицуулалтыг гаргасан гэсэн мэдээлэл дурдагдсан. Гэвч баримт бичгийн судалгааны үр дүнд үүнийг батлах баримт олдоогүй. Монгол Улсын санхүүгийн байгууллагууд олон улсад үйл ажиллагаа явуулахын тулд олон улсын аюулгүй байдлын стандартуудыг дагаж мөрдөх шаардлагатай байдаг. Эдгээр зохицуулалтын шаардлагууд нь санхүүгийн салбарт мэдээллийн аюулгүй байдлын тогтвортой, институцчилсан чадвар бий болгосон бөгөөд энэ нь голлох бүлгийн хэлэлцүүлэгээр тодорхой харагдахаас гадна онлайн эх сурвалжуудад сайн тэмдэглэгдсэн байна[67].

Кибер гэмт хэргийг зохицуулах хууль тогтоомж:

Монгол Улс нь 2017 оны Эрүүгийн хэрэг хянан шийдвэрлэх тухай хуульд кибер гэмт хэрэгтэй холбоотой хэрэг бүртгэлт, мөрдөн шалгах ажиллагааны зохицуулалтыг бүрэн хэмжээнд тусгасан. Тус хууль нь цахим нотлох баримтыг цуглуулах, ашиглах (16, 21, 22 дугаар бүлэг), компьютерт хадгалагдаж буй өгөгдөл болон сүлжээний мэдээллийг яаралтай хамгаалах (22 дугаар бүлэг), нотлох баримт гаргуулах (22 дугаар бүлэг), компьютерт хадгалагдаж буй өгөгдлийг хайх, хураах (24 дүгээр бүлэг), бодит цагийн сүлжээний мэдээллийг цуглуулах (26 дугаар бүлэг), контентын мэдээллийг тагнах, хянах (26 дугаар бүлэг) зэрэг зохицуулалтыг багтаасан. Цаашилбал, хууль нь 2-р бүлэгт шүүхийн эрх мэдлийн тухай заалтуудыг агуулдаг бөгөөд эдгээр заалт нь тодорхой нөхцөлд улсын хил хязгаарыг давсан гэмт хэргийн үйл ажиллагаанд шүүхийн эрх мэдлийг тэлэх боломжийг олгодог (2.1.2-р зүйл). Ийм тохиолдолд эрүүгийн хэргийн танхимын Ерөнхий шүүгчийн шийдвэрээр харьяаллыг тогтоох ёстой. Голлох бүлгийн хэлэлцүүлгүүд болон ширээний судалгаа нь дээр дурдсан заалтуудыг 2015 оны Эрүүгийн хуульд заасан кибер гэмт хэргийн зүйл ангид хэрхэн хэрэгжүүлж байгаа талаар тодорхой мэдээлэл олдоогүй болно. Дээрх зохицуулалтын заримыг хуульд тодорхой заагаагүй ч цахим орчинд цаашлаад кибер гэмт хэрэгт хамаарах боломжтой гэж тайлбарлах нөхцөл үүсэж байна. Судалгааны багт тэдгээрийн хэрэгжилтийг баталж эсхүл няцаахад шаардлагатай хууль зүйн практик мэдээлэл дутагдалтай байлаа.

2017 оны Эрүүгийн хэрэг хянан шийдвэрлэх тухай хуулийн 42-р бүлэг нь хил дамнасан мөрдөн байцаалт болон мэдээлэл солилцооны хууль эрх зүйн шаардлагыг тодорхойлсон бөгөөд үүнд кибер гэмт хэрэгтэй холбоотой олон улсын хамтын ажиллагаа мөн хамаарна. Тус бүлэгт зааснаар олон улсын хамтын ажиллагаа нь хоёр талт гэрээ болон харилцан эрх зүйн туслалцааны гэрээ (MLAT), эсхүл бусад олон улсын гэрээ, хэлэлцээрийн хүрээнд хэрэгжиж болно. Монгол Улс ямар нэгэн олон улсын кибер гэмт хэрэгтэй тэмцэх гэрээ, хэлэлцээрт одоогоор нэгдээгүй боловч, хэд хэдэн улстай байгуулсан MLAT-ууд нь кибер гэмт хэргийн асуудлаар олон улсын хамтын ажиллагааг процессын түвшинд хөнгөвчлөх боломжтой. 2015 оны *Эрүүгийн хуулийн* 1.7 дугаар зүйлд зааснаар, Монгол Улсад гэмт хэрэг үйлдсэн гадаад улсын иргэнийг тухайн улс орон аюулгүй байдлыг нь хангах хангалттай үндэслэл байгаа тохиолдолд шилжүүлэн өгөх боломжтой. Тус зүйлд мөн, Монгол Улсын иргэнийг гадаад улсын эрүүгийн мөрдөн байцаалтад шилжүүлэхийг хориглосон бөгөөд энэ нь *Монгол Улсын Үндсэн хуулийн* 15-р зүйлтэй нийцэж байна.

Хүний эрхийн нөлөөллийн үнэлгээ:

[67]https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.swift.com/swiftresource/251951/download&ved=2ahUKEwiV2JXm-4iKAxVUU0EAHdJQCaAQFnoECBcQAQ&usg=AOvVaw1r1TSBQQJFldru_toTJheo

Монгол Улсын Үндсэн хуулийн 2-р бүлэг нь улсын хэмжээнд хүний эрх, эрх чөлөөг хамгаалах зааltуудыг агуулсан. Үндсэн хуулийн 16-р зүйлд Монгол Улсын иргэн үзэл бодлоо илэрхийлэх, мэдээлэл авах, эрх чөлөөтэй байх, аюулгүй байх, хувийн нууцтай байх, шашин шүтэх, улс төрийн холбоо байгуулах эрхтэй болохыг тодорхой заасан. 2020 оны *Монгол Улсын Хүний эрхийн тухай* хууль нь "Хүний эрхийг хамгаалах үндэсний тогтолцоо"-г бий болгосон бөгөөд Монгол Улсад хүний эрхийг хамгаалах, дэмжих зорилготой. Уг хуулийн 2-р бүлгийн дагуу комиссын нэг үүрэг нь хуулийн төслүүд болон захиргааны шийдвэрүүдийг хүний эрхийн үүрэгтэй нийцэж байгаа эсэхийг үнэлэх, төрийн байгууллагуудын хүний эрхийн хариуцлагыг хянах явдал юм. Комисс нь хүний эрх зөрчигдөх шалтгаан, нөхцөлийг арилгах заавал биелүүлэх зөвлөмж гаргах эрхтэй. Монгол Улс Нэгдсэн Үндэстний Байгууллагын гишүүн бөгөөд Хүний эрхийн түгээмэл тунхаглалд гарын үсэг зурсан. 1974 онд Иргэний болон улс төрийн эрхийн олон улсын фактыг баталсан тул олон улсын хүний эрхийн стандартад нийцэж байна. Кибер аюулгүй байдлын үндэсний стратегийн (КАБҮС) хүрээнд Монгол Улс кибер орчинд хүний эрхийг хамгаалах хууль эрх зүйн орчныг сайжруулах стратегийн зорилт тавьсан.

Хэдий бат бөх хууль эрх зүйн болон стратегийн түвшинд хүний эрхийн тогтолцоотой байсан ч голлох бүлгийн хэлэлцүүлэг болон баримт бичгийн судалгааны үр дүнд Монгол Улсын кибер аюулгүй байдал болон кибер гэмт хэрэгтэй холбоотой хууль тогтоомжид хүний эрхийн нөлөөллийн үнэлгээ хийгдсэн эсэх нь тодорхойгүй байна. Мөн судалгаанаас үзэхэд холбогдох хүний эрхийн мэргэжилтнүүдийг хууль, зохицуулалт боловсруулах үйл явцад оролцуулсан гэх нотолгоо байхгүй. Мэдээллийн хяналт, улс төрийн хяналттай холбоотой асуудлууд, тухайлбал сэтгүүлчдийг шийтгэх, хорих зэрэг баримтууд байгаа нь төрийн байгууллагууд заримдаа Монгол Улсын хүний эрхийн тогтолцоонд тусгагдсан иргэдийн эрхийг бүрэн хамгаалдаггүй болохыг харуулж байна.[68]

2021 оны *Кибер аюулгүй байдлын тухай хууль* нь хүний эрхэд үзүүлэх нөлөөллийн талаар олон нийт шүүмжлэлтэй хандах хандлага ажиглагдсан. Голлох бүлгийн хэлэлцүүлэгт төрийн болон хувийн хэвшлийн ОЧМДБ байгууллагуудын төлөөлөгчид тус хууль нь төрийн байгууллагуудын мэдээлэл хянах хэт их эрх мэдлийг олгох нь хэр зохистой талаар болгоомжлолтой байгаагаа илэрхийлсэн.

Хуулийн 22-р зүйлд Нийтийн төв нь нийтийн ОЧМДБ рүү чиглэсэн кибер халдлагыг илрүүлэх, судлах, Үндэсний төвтэй мэдээлэл хуваалцах үүрэгтэй гэж заасан. Үүнтэй адил, 21-р зүйлд Үндэсний төвд ижил төрлийн эрх, үүргийг хуваарилсан байдаг. Оролцогч талуудын хувьд эдгээр зааltууд нь хувийн мэдээллийн нууцлалын талаарх тодорхойгүй байдлыг нэмэгдүүлж байгаа гэж үзэж байна. Энэ болгоомжлол нь авторитар коммунист засаглалтай холбоотой үндэсний түүхээс үүдэлтэй бөгөөд нийгмийн зарим гишүүдийн хувьд төрийн байгууллагад итгэх итгэл сул байгаагаас болж улам нэмэгдсэн. Монгол Улсад мэдээлэл хамгаалах хууль хүчтэй хэрэгжиж байгаа бөгөөд үүнийг 4.2-р хүчин зүйлд дэлгэрэнгүй тайлбарлагдсан. Гэсэн хэдий ч эдгээр хуулиуд нь ISP буюу интернэт үйлчилгээ үзүүлэгчдэд хамаарах бөгөөд Кибер аюулгүй байдлын тухай хуулийн хэрэгжилтэд шууд үйлчлэхгүй болох нь анхаарал татаж байна.

[68] https://www.state.gov/reports/2023-country-reports-on-human-rights-practices/mongolia/

D 4.2 ХОЛБОГДОХ ХУУЛЬ ЭРХ ЗҮЙН ОРЧИН

Энэ хүчин зүйл нь кибер аюулгүй байдлын холбогдох хууль эрх зүйн хүрээ, үүнд мэдээллийн хамгаалалт, хүүхдийн хамгаалалт, хэрэглэгчийн хамгаалалт, оюуны өмчийг хамарсан хууль тогтоомжуудыг авч үзэх болно.

Түвшин: **Эхлэл түвшнээс Тогтворжсон түвшинд**

Хувийн мэдээлэл хамгаалах хууль тогтоомж:

Хүний хувийн мэдээлэл хамгаалах тухай хууль(2021*)* нь хувийн мэдээлэл цуглуулах, боловсруулах, ашиглах болон аюулгүй байдлыг зохицуулдаг. Энэхүү зохицуулалт нь дээр дурдсан аливаа үйл ажиллагаанд оролцохоор зорьж буй бүх хуулийн этгээд, хууль бус этгээд болон хувь хүнд хамаарах бөгөөд техник хангамж эсвэл програм хангамжийн тусламжтайгаар хийгдэж буй бүх үйл ажиллагаанд ижил тэгш үйлчлэх зориулалттай. Хуулийн 4-р зүйлд "хувийн мэдээлэл" болон "эмзэг мэдээлэл" гэсэн мэдээллийн хоёр ангиллыг тодорхойлсон. Хувийн мэдээллийг “хүнийг шууд болон шууд бусаар тодорхойлох, эсхүл тодорхойлох боломжтой өгөгдөл”, харин эмзэг мэдээллийг “хүний арьсны өнгө, угсаа гарал, шашин шүтлэг” зэрэгт хамаарах мэдээлэл хэмээн тус тус тодорхойлсон.

Төр, хувийн хэвшлийн байгууллага болон хувь хүн мэдээлэл хэрхэн цуглуулж, ашиглах талаар хуулийн 6, 7-р зүйлд заасан. Аль ч тохиолдолд мэдээлэл цуглуулах, хадгалах, ашиглахын өмнө хувь хүний зөвшөөрлийг заавал авах ёстой. Зөвшөөрөл авах шаардлагыг 8-р зүйлд зааж, ямар мэдээлэл цуглуулах, хэр хугацаанд хадгалах, хэрхэн ашиглах, зөвшөөрлөө хэрхэн цуцлах зэрэг мэдээллээр хангах ёстойг тусгасан.

*Хүний хувийн мэдээлэл хамгаалах тухай хуулийн(*2021 он*)* хэрэгжилтийг хянах гол байгууллагуудыг томилсон. Хуулийн 25-р зүйлийн дагуу цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн төв байгууллага буюу ЦХИХХЯ нь хууль хэрэгжүүлэх, олон нийтэд мэдээлэл түгээх, шаардлага хангасан байгууллагад дэмжлэг үзүүлэх үүрэгтэй. Түүнчлэн, ЦХИХХЯ нь өгөгдөл цуглуулах, боловсруулах, ашиглахтай холбоотой технологийн болон аюулгүй байдлын журмыг батлах үүрэгтэй гэж хуулийн 20.2-т заасан.

Энэ үүргийн хүрээнд ЦХИХХЯ анхны ерөнхий журам болох "Мэдээллийн аюулгүй байдлын шаардлага"-ыг 2023 онд баталсан байна. Ингэснээр хувийн мэдээллийг цуглуулах, боловсруулах, ашиглах үйл ажиллагааны аюулгүй байдлыг хангах, стандартчилагдах нөхцөл бүрдсэн гэж үзэж болно. [69] Эдгээр шаардлагууд нь мэдээлэл хариуцагч нарын дагаж мөрдөх ёстой хэд хэдэн зарчмуудыг, түүнчлэн технологийн аюулгүй байдлын шаардлага болон серверийн боловсруулалтын шаардлагыг тодорхойлсон байна.[70]

Монгол Улсын Хүний эрхийн үндэсний комисс нь *Хүний хувийн мэдээлэл хамгаалах тухай хуулийн (*2021 он*)* 24-р зүйлд хэрэгжилтийг хянах, олон нийтэд мэдээлэл өгөх, мэдээллийн эзний өргөдөл, гомдлыг хүлээн авах, байгууллагуудад мэдээллийн менежментийн талаар зөвлөмж өгөх үүрэгтэй гэж заасан. Энэ нь хувийн мэдээллийг

---

69 https://www.dlapiperdataprotection.com/index.html?t=security&c=MN

70 ht//www.dlapiperdataprotection.com/index.html?t=security&c=MN

хамгаалах, иргэдийн эрхийг хангахад чухал үүрэг гүйцэтгэх юм. Цаашилбал, хуулийн 5-р зүйлд байгууллага мэдээллийг хамгаалахтай холбоотой дагаж мөрдөх ерөнхий аюулгүй байдлын шаардлагыг агуулах бөгөөд үүнд мэдээллийн аюулгүй байдлыг тасралтгүй хангах, мэдээллийн үнэн зөв, бүрэн бүтэн байдлыг хангах шаардлагууд орно. Энэ нь хувийн мэдээллийг алдах, устгах, өөрчлөхөөс урьдчилан сэргийлэхэд чиглэсэн чухал заалт юм.

Дэлгэрэнгүй авч үзвэл, хуулийн 20-р зүйлийн "Мэдээллийн аюулгүй байдлыг хангах арга хэмжээ" хэсэгт мэдээлэл хариуцагч нар өөрсдийн хадгалж буй мэдээллийг хамгаалах журам боловсруулах, мэдээлэл цуглуулах, боловсруулах, ашиглах системийн бүрэн бүтэн байдал, нууцлал, хүртээмжтэй байдлыг хангах байдалд үнэлгээ хийх үүрэгтэй гэж заасан. Энэ нь мэдээллийн аюулгүй байдлыг хангах, эрсдэлийг бууруулахад чиглэсэн чухал шаардлага юм. Мэдээлэл хариуцагч нар мэдээлэл алдсан тохиолдолд авч хэрэгжүүлэх үйл ажиллагааны төлөвлөгөө боловсруулах үүрэгтэй бөгөөд энэ төлөвлөгөөнд мэдээлэл эзэмшигч болон холбогдох байгууллагад хэрхэн мэдээлэх талаар тодорхой заалт багтаах шаардлагатай гэж хуулийн 20-р зүйлд заасан байна. Ингэснээр мэдээлэл алдагдсан тохиолдолд хурдан шуурхай арга хэмжээ авах, мэдээллийн эзнийг мэдээллээр хангах, хохирлыг бууруулахад чухал ач холбогдолтой. Мөн хуулийн 23-р зүйлд мэдээлэл хариуцагч нар цахим мэдээлэл боловсруулах технологи ашиглахыг зөвшөөрсөн боловч хэрэв энэ систем нь эмзэг мэдээллийг тогтмол боловсруулах, эсхүл мэдээллийн эзний эрх, эрх чөлөө, ашиг сонирхолд нөлөөлж болзошгүй шийдвэр гаргах функцтэй бол түүний ашиглалтыг үнэлэх шаардлагатай гэж заасан. Энэ нь автоматжуулсан системийн аюулгүй, найдвартай байдлыг хангах, мэдээлэл эзэмшигчдийн эрхийг хамгаалах чухал ач холбогдолтой.

Үндэсний хүний эрхийн комисс эдгээр үнэлгээнд зөвлөмж өгөх эрхтэй бөгөөд мэдээлэл хариуцагч нар уг зөвлөмжийг дагаж мөрдөх үүрэгтэй гэж хуульд заасан. Энэ нь мэдээлэл хариуцагч нарын үйл ажиллагаанд хяналт тавих, мэдээллийн эзний эрхийг хамгаалахад чухал үүрэг гүйцэтгэнэ. Хэрэв мэдээллийн эзэн өөрсдийн мэдээллийг хэрхэн ашиглаж байгаад санаа зовж буй бол зохих байгууллагад гомдол гаргах боломжтой гэж хуульд заасан. Хуулийн зөрчлийн шинж чанараас хамааран 2019 оны Гэмт хэрэг, зөрчлөөс урьдчилан сэргийлэх тухай хууль, 2017 оны Төрийн албаны тухай хууль, 1999 оны Хөдөлмөрийн тухай хууль, 2015 оны Эрүүгийн хууль зэрэг хуулиудын дагуу зохицуулалт хийгдэнэ. Энэ нь мэдээлэл эзэмшигчийн эрхийг хамгаалах, хууль бусаар мэдээлэл ашигласан этгээдэд хариуцлага тооцох механизм бүрдүүлэхэд чухал ач холбогдолтой юм.

Хүүхэд хамгаалалт (онлайн орчин):

2015 оны *Эрүүгийн хууль* нь хүүхдийн эсрэг гэмт хэргүүдийг хуульчилж, онлайн орчинд үйлчлэхээр тодорхойлсон нь хүүхдийг интернетээр дамжин үйлдэгдэх гэмт хэргээс урьдчилан сэргийлэх, хамгаалахад чухал ач холбогдолтой юм. Хуулийн 16.8, 16.9-р зүйлүүд нь хүүхдийн эсрэг садар самуунтай холбоотой үйлдлүүдийг гэмт хэрэгт тооцож, хатуу хориглосон нь хүүхдийн эрхийг хамгаалахад чиглэсэн чухал алхам болсон.

2016 оны *Хүүхэд хамгаалах тухай хууль* нь хэвлэл мэдээлэл болон цахим орчинд хүүхдийн эрхийг хамгаалах нэмэлт зохицуулалтыг оруулсан. Хуулийн 8-р зүйлд зааснаар эцэг эх, сургууль болон төрийн байгууллага зэрэг тодорхой хууль эрх зүйн этгээд нь хүүхдийг эрүүл мэнд, хүмүүжил, насанд хүрэх байдалд сөрөг нөлөө үзүүлж болох тоглоом, ном, урлаг, мэдээлэл, зар сурталчилгаа болон бусад цахим орчноос

хамгаалах үүрэгтэй. Ерөнхийдөө, хууль эрх зүйн хүрээ нь Монгол улсад хүүхдийн эрхийг хамгаалах бодит хууль зүйн хамгаалалтыг хангаж, шилдэг туршлага олон улсын стандартуудтай, тухайлбал Будапештийн конвенцтэй нийцэж байна.

Гэвч голлох бүлгийн хэлэлцүүлэг, судалгаагаар онлайн орчинд хүүхэд хамгааллын хууль тогтоомжийн үр дүнг тогтмол үнэлдэг эсэх, шинэ технологид нийцүүлэн хуульд өөрчлөлт оруулах талаар судалгаа хийдэг эсэх нь тодорхойгүй байгаа нь анхаарал татаж байна. Цаашид энэ чиглэлээр илүү нарийвчилсан судалгаа, үнэлгээ хийх, шаардлагатай тохиолдолд хуульд нэмэлт, өөрчлөлт оруулах нь зүйтэй юм. Ингэснээр хүүхдийг интернетээр дамжин үйлдэгдэх гэмт хэргээс урьдчилан сэргийлэх, хамгаалах тогтолцоог бэхжүүлэх боломжтой.

Хэрэглэгчийн эрхийг хамгаалах хууль тогтоомж:

2002 оны Иргэний хууль нь хэрэглэгчийн гэрээний хүрээнд бараа худалдах, худалдан авах ерөнхий нөхцөлийг 200–2002 дугаар зүйлд тусгасан байдаг. Уг хуулийн 42.1-р зүйлд Монгол Улсад цахим хэлбэрээр гүйлгээ хийхийг зөвшөөрсөн байдаг. Харин 2003 оны Хэрэглэгчийн эрхийг хамгаалах тухай хууль нь бараа бүтээгдэхүүн худалдах, худалдан авах, ажил үйлчилгээ гүйцэтгэхтэй холбоотой хэрэглэгчийн эрхийн харилцааг зохицуулдаг бөгөөд уг хуулийг Шударга өрсөлдөөн, хэрэглэгчийн төлөө газрын дэргэдэх Хэрэглэгчийн эрхийг хамгаалах газар хэрэгжүүлдэг.

Тус хуульд хэрэглэгчдийг залилан мэхлэх, хуурч мэхлэх зэрэг хууль бус бизнесийн үйл ажиллагаанаас хамгаалах зохицуулалтууд тусгагдсан хэдий ч онлайн орчинд эдгээр зохицуулалтууд хэрхэн хамаарах талаар тодорхой заалтууд агуулаагүй байна. Мөн баримт бичгийн судалгаа, бүлгийн хэлэлцүүлгээр хэрэглэгчийн эрхийг хамгаалах хууль нь цахим орчинд нийцүүлэн шинэчлэгдэж буй талаар нотолгоо олдоогүй болно. Харин 2015 оны Эрүүгийн хуульд цахим луйврыг гэмт хэрэгт тооцсон байдаг ч (Factor 4.1-д дурдсанчлан) спам мессеж зэрэг цахим бизнесийн нийтлэг зөрчлийг тусгайлан зохицуулсан заалт одоогоор байхгүй байна.

Оюуны өмчийн хууль тогтоомж:

2021 оны *Зохиогчийн эрхийн тухай хууль* нь Монгол Улсын оюуны өмчийн эрх зүйн тогтолцоог бүрдүүлсэн бөгөөд шинжлэх ухаан, утга зохиол, урлагийн бүтээлүүдийг хамгаалдаг. Энэхүү хууль нь цахми орчинд оюуны өмчийн эрхийг хамгаалах үндсэн зарчмуудыг тусгасан. 52-р зүйлд интернэт үйлчилгээ үзүүлэгчид (ISP), вэбсайтын эзэд, харилцаа холбооны үйлчилгээ үзүүлэгчид, телевизийн байгууллагууд болон бусад этгээдүүд сүлжээн дэх оюуны өмчийн зөрчлөөс урьдчилан сэргийлэх үүрэгтэй болохыг заасан.

53-р зүйлд зохиогчийн эрхийг хамгаалахын тулд ашиглаж буй технологийг эвдэх, устгах, гэмтээхийг хориглосон. Энэ төрлийн төхөөрөмж үйлдвэрлэх, импортлох, худалдааны зорилгоор сурталчлахыг мөн гэмт хэрэг гэж үздэг.

2015 оны *Эрүүгийн хууль* нь 18.16, 18.17-р зүйлүүдээр барааны тэмдэг эзэмшигч, зохиогчийн эрх болон холбогдох эрхийн зөрчлийг хориглосон.

Олон улсын түвшинд Монгол Улс Дэлхийн Оюуны Өмчийн Байгууллагын (WIPO) гишүүн бөгөөд WIPO-ийн Интернэтийн гэрээнүүдэд гарын үсэг зурсан. Түүнчлэн, Монгол Улс Утга зохиол, урлагийн бүтээлийг хамгаалах тухай Берний конвенц, Дэлхийн

худалдааны байгууллага (WTO)-ын гишүүн бөгөөд Оюуны өмчийн эрхтэй холбоотой худалдааны талын гэрээ (TRIPS)-нд нэгдсэн.

Мөн Монгол Улс Будапештын конвенцын 10-р зүйлд (зохиогчийн эрх болон холбогдох эрхийн зөрчилтэй холбоотой гэмт хэргүүд) нийцэж байгаа[71].

Иймд, Монгол Улс онлайн орчин дахь оюуны өмчийн хамгаалалтыг хууль эрх зүйн хүрээнд бүрэн тогтоосон бөгөөд олон улсын стандарт, шилдэг туршлагуудтай нийцэж байна[72].

Гэсэн хэдий ч Монгол Улс энэхүү эрх зүйн тогтолцоог бодит үйл ажиллагаанд нэвтрүүлэхэд хүндрэлтэй тбайгаа нь судалгааны үр дүнгээс харагдаж байна. Судалгаагаар оюуны өмчийн хууль тогтоомжийн үр дүнг тогтмол үнэлдэг эсэх, шинэ технологид нийцүүлэхээр өөрчлөлт оруулж буй эсэх талаар нотолгоо олдоогүй.

D4.3 ХУУЛЬ, ЗОХИЦУУЛАЛТЫН ЧАДАМЖ БОЛОН ХҮЧИН ЧАДАЛ

Энэхүү хүчин зүйл нь хууль сахиулах байгууллагуудын кибер гэмт хэргийг мөрдөн шалгах чадвар, прокурорын байгууллагын кибер гэмт хэрэг болон цахим нотлох баримттай холбоотой хэргүүдийг шүүхэд танилцуулах чадамж, мөн шүүхийн байгууллагын кибер гэмт хэрэг болон цахим нотлох баримт бүхий хэргүүдийг хянан шийдвэрлэх чадамжийг судална. Мөн кибер аюулгүй байдлын тодорхой зохицуулалтуудын хэрэгжилтэд хяналт тавих үүрэг бүхий олон салбарын зохицуулах байгууллагууд бий эсэхийг хянан судална.

Түвшин: **Эхлэл түвшнээс Хөгжиж буй түвшинд**

Монгол Улсын хууль сахиулах байгууллагууд, прокурорын газар, шүүх нь кибер гэмт хэргийг мөрдөн шалгах үндсэн чадамжтай ч техник, хүний нөөц болон санхүүгийн нөөцийн хомсдол нь илүү өргөн хүрээтэй институтийн чадамжийг хөгжүүлэхэд саад учруулж байна. Кибер гэмт хэргийн мөрдөн байцаалт болон цахим нотлох баримтын техник арга зүйтэй холбоотой олон улсын дэмжлэгтэй сургалтууд Монгол Улсад тогтмол бус зохион байгуулагдаж, олон жил үргэлжилж байна. Үүнд НҮБ-ын Хар тамхи, гэмт хэрэгтэй тэмцэх газар (UNODC)[73], Японы Олон улсын хамтын ажиллагааны байгууллага (ЖАЙКА)[74], Олон улсын шилжилт хөдөлгөөний байгууллага (IOM)[75] зэрэг байгууллагын хөтөлбөрүүд багтана. Эдгээр сургалтуудын ихэнх нь хууль сахиулах байгууллагын ажилтнанд чиглэгдсэн бөгөөд прокурор, шүүгчдэд зориулсан ижил түвшний сургалтын боломжийг тодорхойлоогүй байна.

Эдгээр олон улсын сургалтаас гадна Цагдаагийн ерөнхий газар нь Дотоод хэргийн их сургуулийн харьяа Цагдаагийн академийн хүрээнд кибер гэмт хэргийн чиглэлээр хоёр жилийн сургалтын хөтөлбөрийг хэрэгжүүлдэг[76]. "Кибер аюулгүй байдлын

---

71 [73]https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-11/Mongolia_Digital_Readiness_Assessment.pdf

72 https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-11/Mongolia_Digital_Readiness_Assessment.pdf

73 https://www.unodc.org/roseap/en/2024/05/mongolia-translational-organized-crime/story.html

74 https://cybilportal.org/projects/countermeasures-against-cybercrime/

75 https://www.iom.int/project/strengthening-mongolias-cyber-crime-investigations-human-trafficking

76 https://drive.google.com/drive/folders/1RETJak8qmhR4XP1Ngeqnr1rpCX-S1KkK

мэргэжилтний хөтөлбөр" нь тус академаас санал болгодог мэргэшүүлэх сургалтын чиглэлүүдийн нэг бөгөөд хууль сахиулах алба хаагчдад кибер гэмт хэргийг мөрдөн шалгах хууль эрх зүй болон мэргэжлийн ур чадвар олгох зорилготой.
Боломжтой цөөн тооны нотолгооноос харахад энэ сургалтын тогтолцоо нь Монгол Улсын хууль сахиулах байгууллагуудад кибер гэмт хэргийн мөрдөн байцаалтыг амжилттай явуулах боломжийг олгосон гэж дүгнэж болохоор байна. Үүний тодорхой жишээ нь 2024 онд Монгол Улсын цагдаагийн байгууллага INTERPOL-тай хамтран дэлхий даяар 22,000 хортой IP хаягийг илрүүлэн устгах ажиллагаанд оролцсон бөгөөд Монгол Улсад 21 удаагийн нэгжлэг хийсэн явдал юм[77]. 2019 онд Цагдаагийн ерөнхий газар 800 хятад иргэнийг кибер гэмт хэрэг үйлдсэн хэргээр баривчилж, хэдэн зуун компьютер, гар утсыг хураан авсан. Гэвч эдгээр хэргийн эцсийн шийдвэр, ял шийтгэл оногдуулсан эсэх талаар нээлттэй мэдээлэл байхгүй учраас прокурор шүүхийн байгууллага эдгээр хэргийг амжилттай шийдвэрлэсэн эсэх нь тодорхойгүй байна.
"Монгол Улсын 2023 оны Статистикийн эмхэтгэл"-д дурдсанаар, Монгол Улсад кибер гэмт хэрэгтэй холбоотой хэргийг хууль эрх зүйн хүрээнд шийдвэрлэх тодорхой хэмжээний чадамж байгаа нь ажиглагдаж байна. 2023 онд Цагдаагийн ерөнхий газарт нийт 388 кибер гэмт хэрэг бүртгэгдсэн нь өмнөх оноос 49.8%-иар өссөн. Эдгээр хэргүүдээс 155 сэжигтэн яллагдагчаар бүртгэгдсэн байна[78]. Монгол Улсын анхан шатны шүүхийн мэдээллээс харахад 2023 онд 14 кибер гэмт хэргийг шүүхээр шийдвэрлэсэн бөгөөд энэ тоо 2022 онд шийдвэрлэгдсэн 4 хэрэгтэй харьцуулахад өссөн үзүүлэлт юм[79].

Эдгээр статистик мэдээллээс үзэхэд Монгол Улсад кибер гэмт хэргийг шүүх, прокурорын байгууллагууд хянан шийдвэрлэх чадамж жилээс жилд өсөж байгаа боловч бүртгэгдсэн кибер гэмт хэргийн тоо нэмэгдэж байгаатай зэрэгцэн хангалттай түвшинд хүрээгүй байгааг харуулж байна. Энэ нь голлох бүлгийн хэлэлцүүлгийн дүнтэй нийцэж байгаа бөгөөд прокурор, шүүх байгууллагууд кибер гэмт хэргийг үр дүнтэй, хурдтай шийдвэрлэх институтийн чадамж дутагдаж байгааг илэрхийлж байна.

Эдгээр хязгаарлагдмал чадамж болон хууль сахиулах байгууллагын кибер гэмт хэрэгтэй тэмцэх сургалтын тогтолцоо бүрдсэн хэдий ч, Монгол Улсад хууль эрх зүйн оролцогч талуудын кибер гэмт хэргийг мөрдөн шалгах, яллах, шүүн таслах нийт чадамжид томоохон дутагдал байсаар байна. Байгууллагууд техник, хүний нөөц болон төсвийн хомсдолд орсоноор цаашдын чадавхийг нэмэгдүүлэх боломж хязгаарлагдмал болж байна. Хүний нөөцийн хувьд прокурор болон шүүхийн байгууллагад уг сорилтыг давахад чиглэсэн албан ёсны сургалтын хөтөлбөр байхгүй. Хууль сахиулах байгууллагын зүгээс сургалтын боломжийг нэмэгдүүлэх, кибер ур чадварын дутагдлыг нөхөх оролдлого хийж байгаа ч, ажилтнуудын шилжилт хөдөлгөөн өндөр байгаа нь хүний нөөцийн чадавхийг нэмэгдүүлэхэд сөргөөр нөлөөлж байна. Кибер аюулгүй байдлын чадварлаг мэргэжилтний хувьд бусад салбаруудтай хүчтэй өрсөлдөөн үүсэж, хувийн хэвшилд илүү өндөр цалинтай ажлын байранд шилжих хандлага нь эдгээр мэргэшсэн ажилтнуудыг алдахад хүргэж байна. Үүний үр дүнд, кибер гэмт хэрэгтэй тэмцэх чиглэлээр, туршлагатай, тогтвортой мэргэжилтнүүдийн баг бий болохын оронд, мэдлэгтэй хувь хүмүүсийн сүлжээ бүрдэж байна.

---

77 [79]https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-cyber-operation-takes-down-22-000-malicious-IP-addresses

78 P. 371 of National Statistics Report

79 National statistics report (confirm page no.)

Одоогийн нөхцөлд үүссэн ур чадварын хомсдлыг зөвхөн сургалтыг нэмэгдүүлэх, сайжруулах чиглэлээр хязгаарлагдмал арга хэмжээ авч шийдвэрлэх боломжгүй. Голлох бүлгийн хэлэлцүүлгээр хууль сахиулах байгууллагын цалин өрсөлдөх чадваргүй, хэт их хүнд сурталтай гэж шүүмжилсэн бөгөөд энэ нь чадварлаг кибер аюулгүй байдлын мэргэжилтнүүдийг ажилд татах, тогтвортой ажиллуулахад хүндрэл учруулж байна. Төрийн салбарт хуулийн хэрэгжилтийн байгууллагуудад тулгарч буй санхүүгийн хязгаарлалтууд, тухайлбал хатуу тогтсон, уян хатан бус цалингийн системийг өөрчлөх нь зөвхөн хууль сахиулах байгууллага төдийгүй, кибер ур чадварын хомсдолыг нөхөхийн тулд шаардлагатай мэргэжилтнүүдийг сургах зэрэг нь өргөн хүрээний олон талын оролцоог шаарддаг асуудал юм. Энэ асуудлыг илүү нарийвчлан 3.3-р хүчин зүйлд авч үзсэн. Хууль эрх зүйн тогтолцоог үр ашигтай, үр дүнтэй ажиллуулахын тулд хууль сахиулах байгууллага, прокурорын байгууллага, шүүх эрх мэдлийн байгууллагууд хамтран ажиллаж, кибер гэмт хэргийн сургалтын тогтолцоог институцчилах, мөн эдгээр бүтцийн санхүүгийн хязгаарлалтыг даван туулах шаардлагатай.

Технологийн хязгаарлагдмал байдал нь хууль эрх зүйн байгууллагуудын кибер гэмт хэргийг шийдвэрлэх чадамжид сөргөөр нөлөөлж буй бас нэгэн хүчин зүйл юм. Голлох бүлгийн хэлэлцүүлгүүдийн үеэр хууль эрх зүйн байгууллагууд нь кибер гэмт хэргийг мөрдөн шалгах, яллах, шүүн таслах үйл ажиллагааг өндөр түвшинд гүйцэтгэхэд шаардлагатай технологийн тоног төхөөрөмжөөр хангалттай хангагдаж чаддаггүй тухай дурдагдсан. Жишээлбэл, 2021 оны Кибер аюулгүй байдлын тухай хуульд ЦЕГ нь кибер халдлагыг мөрдөн шалгах, түүнтэй тэмцэх зориулалттай дижитал лаборатори ажиллуулах үүрэгтэй гэж заасан байдаг. Гэсэн хэдий ч, голлох бүлгийн хэлэлцүүлгийн мэдээллээр уг лаборатори өнөөдрийг хүртэл байгуулагдаагүй байна. Түүнчлэн, хууль сахиулах байгууллагын албан тушаалтнууд удирдлагуудаасаа эмзэг мэдээллийг хамгаалахад шаардлагатай технологийн тоног төхөөрөмжийн төсвийн дэмжлэг хүсч удаа дараа хүсэлт гаргасан боловч, өнөөг хүртэл ийм дэмжлэг авч байгаагүй гэж мэдээлэгдсэн.

Зохицуулалтын үүднээс авч үзвэл, зохицуулагч байгууллагуудын чадамж, хүчин чадал харилцан адилгүй байна. Төв банк болон Санхүүгийн зохицуулах хороо (СЗХ) зэрэг илүү тогтвортой, туршлагатай зохицуулагчид нь өөрсдийн салбар дахь кибер аюулгүй байдлын зохицуулалтын хэрэгжилтэд хяналт тавих ур чадвар, нөөц бололцоотой байна. Гэсэн хэдий ч, 2021 оны Кибер аюулгүй байдлын тухай хууль болон түүний дагалдах "*Кибер аюулгүй байдлын нийтлэг журам*"-ын хэрэгжилтэд хяналт тавих үүрэгтэй зохицуулагч байгууллагуудын чадавхи хязгаарлагдмал хэвээр байна. Кибер аюулгүй байдлын нийтлэг журмаар тогтоосон зохицуулалтын үндсэн шаардлагын хэрэгжилтэд хяналт тавих байгууллагууд нь Үндэсний төв, Нийтийн төв болон ЦХИХХЯ-д бүртгэлтэй эрсдэлийн үнэлгээ, аудитын байгууллагууд юм. Голлох бүлгийн хэлэлцүүлгийн үеэр эдгээр бүлгийн чадавхид ялгаа байгааг онцолсон. Үндэсний төв нь төрийн ОЧМДБ байгууллагуудын эрсдэлийн үнэлгээг хийх зэрэг зарим зохицуулалтын үүргээ амжилттай биелүүлсэн гэж мэдэгдсэн бөгөөд мөн зарим бүртгэлтэй аудит, эрсдэлийн үнэлгээний байгууллагууд ч үүргээ хангалттай биелүүлж байгаа тухай дурдсан. Гэсэн хэдий ч, бусад аудит болон эрсдэлийн үнэлгээний байгууллагууд нь хүлээсэн үүргээ гүйцэтгэхэд шаардлагатай мэргэжлийн ур чадвар дутмаг байгаа талаар дурдагдсан (4.1-р хүчин зүйл). Нийтэд нь авч үзвэл, голлох бүлгийн хэлэлцүүлэгт

оролцогчид зохицуулагч байгууллагууд өөрсдөө зохицуулалтыг хэрэгжүүлэх чадавхаа сайжруулахын тулд нэмэлт сургалт авах шаардлагатай гэсэн байр суурийг хүчтэй илэрхийлсэн. Зохицуулагч байгууллагууд нь хяналт тавьж буй хуулийн этгээдээс юуг шаарддаг талаар ойлголт муутай байгаа нь олон удаагийн шүүмжлэлд өртсөн. Гэвч эдгээр шүүмжлэл хэр зэрэг үндэслэлтэй болох, мөн ямар байгууллагууд илүү мэдээлэлтэй, ямар нь мэдээлэл дутмаг байгаа талаар санал зөрөлдсөн тохиолдол байв. Аль ч тохиолдолд, зохицуулалтын тогтолцоог хэрэгжүүлэх явцад оролцогч талууд зохицуулалтын хүрээний талаар хязгаарлагдмал ойлголттой байгаа нь бодит сорилт болж буй нь ажиглагдсан. Санхүүгийн хязгаарлагдмал байдал нь энэ асуудлыг улам хүндрүүлж буй бас нэгэн хүчин зүйл хэмээн дурдагдсан.

D 4.4 КИБЕР ГЭМТ ХЭРЭГТЭЙ ТЭМЦЭХ АЛБАН БОЛОН АЛБАН БУС ХАМТЫН АЖИЛЛАГААНЫ ТОГТОЛЦОО

Энэхүү хүчин зүйл нь дотоодын байгууллагууд болон хил дамнасан хамтын ажиллагааг хөнгөвчлөх, кибер гэмт хэргээс урьдчилан сэргийлэх, тэмцэхэд чиглэсэн албан ёсны болон албан бус механизм оршин байгаа эсэх, тэдгээрийн үйл ажиллагааг судална.

Түвшин: **Тогтворжсон түвшнээс Стратегийн түвшинд**

Хууль сахиулах байгууллага болон хувийн хэвшлийн оролцогч талууд хооронд кибер гэмт хэргийг мөрдөн шалгахад дэмжлэг үзүүлэх зорилгоор мэдээлэл тогтмол, албан бусаар солилцдог. ЦЕГ-н төлөөлөгчидтэй хийсэн хэлэлцүүлгийн явцад, тэд банк, интернэт, харилцаа холбооны үйлчилгээ үзүүлэгч байгууллагуудтай тогтоосон харилцаа холбоондоо бүрэн итгэдэг бөгөөд эдгээр байгууллагуудтай байнга мэдээлэл солилцдог гэж онцолсон. Хууль сахиулах байгууллагууд мэдээлэл солилцооны хурд зарим тохиолдолд хүссэн хэмжээнд хүрэхгүй удаашрах асуудал гардаг гэж дурдсан боловч бүх оролцогч талууд чадлынхаа хэрээр ажиллаж буйг хүлээн зөвшөөрсөн. Эдгээр саад бэрхшээлийг даван туулах, хууль сахиулах байгууллагууд болон хувийн хэвшлийн гол төлөөлөгчдийн хооронд мэдээлэл солилцооны процессыг хурдасгахын тулд ЦЕГ найдвартай мэдээлэл солилцох системийг хөгжүүлж байна. Энэхүү албан ёсны хамтын ажиллагааны механизм нь Харилцаа холбооны зохицуулах хороо (ХХЗХ)-той хамтран хөгжүүлж буй төсөл юм. Мөн хувийн хэвшлийн өргөн хүрээг хамарсан гишүүнчлэл бүхий байгууллага болох MNCERT/CC нь хувийн хэвшил болон хууль сахиулах байгууллагуудын хооронд мэдээлэл солилцоог хөнгөвчлөх үүрэг гүйцэтгэдэг. Улсын хэмжээнд хамгийн удаан хугацаанд үйл ажиллагаа явуулж буй кибер халдлагад хариу арга хэмжээ үзүүлэх багийн хувьд MNCERT/CC нь голлох бүлгийн хэлэлцүүлэгт оролцсон олон оролцогч талуудаас чадамжтай байгууллага гэж өндөр үнэлгээ авсан.

Хууль сахиулах байгууллагуудын хувийн хэвшилтэй хамтын ажиллагааг хууль тогтоомжийн хүрээнд дэмжиж байгаа бөгөөд үүнд 2017 оны *Эрүүгийн хэрэг хянан шийдвэрлэх тухай хууль* (22-р бүлэг) болон 2021 оны *Кибер аюулгүй байдлын тухай хууль* (15.1.1 болон 15.1.2-р зүйл) хамаарна. Дотоод болон олон улсын кибер гэмт хэрэгтэй тэмцэх хамтын ажиллагаа, мэдээлэл солилцоог өргөжүүлэхэд Кибер аюулгүй байдлын үндэсний стратеги (КАБҮС) мөн дэмжлэг үзүүлдэг. КАБҮС нь талууд хооронд мэдээлэл солилцох "дэд бүтцийг" сайжруулах, кибер аюулгүй байдлын төв хоорондын "хамтын

ажиллагааг идэвхжүүлэх", мөн "кибер гэмт хэрэгтэй тэмцэх чиглэлээр олон улсын, бүс нутгийн болон мэргэжлийн байгууллагуудтай мэдээлэл солилцох нөхцөлийг бүрдүүлэх" зорилтуудыг багтаасан.

Олон улсын түвшинд Монгол Улс харилцан эрх зүйн туслалцааны гэрээ (MLATs)-г дэмжих хууль эрх зүйн зохицуулалттай бөгөөд үүнийг 4.1-р хүчин зүйлд тайлбарласан. Хууль сахиулах байгууллагуудтай хийсэн хэлэлцүүлгээс үзэхэд эдгээр гэрээнүүдийг кибер гэмт хэрэгтэй тэмцэхэд ашиглаж байгаа нь батлагдсан. Цагдаагийн ерөнхий газар олон улсын түншүүдтэй хамтын ажиллагаагаа сүүлийн жилүүдэд сайжруулсан тухай мэдээлсэн бөгөөд G7-ийн 24/7 сүлжээ, INTERPOL-тай хамтын ажиллагаа зэрэг механизмууд үүнд чухал үүрэг гүйцэтгэсэн байна. Сүүлийн жилүүдэд олон улсын хамтын ажиллагааны хүрээнд хил дамнасан мөрдөн шалгах ажиллагаанууд амжилттай хэрэгжсэн тухай мэдээлэл хэвлэл мэдээллийн хэрэгслээр гарчээ.[80] Цагдаагийн ерөнхий газар ЦХИХХЯ-тай хамтарсан хороо байгуулах ажлыг хэрэгжүүлж байгаа бөгөөд энэ нь хил дамнасан кибер гэмт хэрэгтэй тэмцэх чадамжийг нь нэмэгдүүлэхэд тустай гэж үзэж байна. Монгол Улсын Засгийн газар хууль сахиулах байгууллагуудтай нягт хамтын ажиллагаатай бөгөөд кибер гэмт хэрэгтэй холбоотой хууль тогтоомж, стратеги боловсруулах, сургалт зохион байгуулах, мэдээлэл солилцох чиглэлээр хамтран ажилладаг. ЦХИХХЯ-ны харьяа Нийтийн төв, ТЕГ-ийн харьяа Үндэсний төв нь Монгол Улсын Засгийн газар болон хууль сахиулах байгууллагуудын хооронд албан ёсны хамтын ажиллагааны механизмыг бүрдүүлдэг. Үндэсний болон Нийтийн төвүүд нь кибер халдлагыг илрүүлэх, холбогдох оролцогч талуудтай мэдээлэл солилцох чадамжаа хөгжүүлж байгаа ч цаашид сайжруулах шаардлагатай байна. Гэсэн хэдий ч эдгээр төвүүдийн ачаар Засгийн газар болон хууль сахиулах байгууллагуудын хооронд кибер гэмт хэрэгтэй холбоотой мэдээлэл тогтмол солилцох албан ёсны бүтэц бүрдсэн. MNCERT/CC, Нийтийн төв, Үндэсний төв нь бүгд FIRST (Forum of Incident Response and Security Teams)-ийн гишүүд юм. Мөн Нийтийн болон Үндэсний төв нь APCERT (Asia Pacific Computer Emergency Response Team)-ийн гишүүн бөгөөд эдгээр харилцаа нь дээрх байгууллагуудын сүлжээг өргөжүүлж, Монгол Улсын хууль сахиулах байгууллагуудад хэрэг болох кибер гэмт хэрэгтэй холбоотой мэдлэг, мэдээлэл авах боломжийг нэмэгдүүлж байна.

ЗӨВЛӨМЖ

Кибер аюулгүй байдлын хууль, зохицуулалтын орчны төлөвшлийн үнэлгээний мэдээлэлд үндэслэн Монгол Улсад дараах зөвлөмжийг хүргэж байна. Эдгээр зөвлөмжүүд нь GCSCC-ийн Кибер аюулгүй байдлын чадавхийн төлөвшлийн загварын үзэл баримтлалын дагуу, одоо байгаа кибер аюулгүй байдлын чадавхийг бэхжүүлэхэд чиглэсэн зөвлөгөө, хэрэгжүүлэх алхмуудыг санал болгох зорилготой юм.

ХУУЛЬ ЭРХ ЗҮЙ БОЛОН ЗОХИЦУУЛАЛТЫН ЗААЛТУУД

R4.1.1 Монгол Улсыг Кибер гэмт хэргийн тухай Будапештийн конвенцид нэгдэх үйл явцыг удирдаж буй хорооны удирдлагын дор, Монгол Улсын эрүүгийн материаллаг болон

[80] https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-cyber-operation-takes-down-22-000-malicious-IP-addresses

процессын хууль тогтоомжид бүрэн хэмжээний үнэлгээ хийх. Энэхүү үнэлгээ нь Будапештийн конвенц болон Монгол Улсын хууль эрх зүйн тогтолцоо хоорондын боломжит зөрүүг тодорхойлох, нөхөх арга хэмжээг тодорхойлох зорилготой байна.

R4.1.2 R4.1.1-тэй уялдуулан, Европын Зөвлөлтэй хамтран ажиллаж, Кибер гэмт хэрэгтэй тэмцэх Будапештийн конвенцод албан ёсны урилгаар нэгдэн, гишүүнээр хүлээн зөвшөөрөгдөхөд шаардлагатай арга хэмжээг авах.

R4.1.3 R4.1.1-тэй уялдуулан, Монгол Улсад хүчин төгөлдөр мөрдөгдөж буй эрүүгийн материаллаг болон процессын хууль тогтоомжийг нягтлан шалгах, шаардлагатай тохиолдолд хиймэл оюун ухаан, квант тооцоолол зэрэг шинэ болон шинээр гарч буй технологийг харгалзан хууль тогтоомжийг шинэчлэх.

R4.1.4 Цахим хөгжил, харилцаа холбооны асуудал эрхэлсэн төрийн төв захиргааны байгууллагыг хамгийн сүүлийн үеийн тэргүүлэх олон улсын стандартуудыг Монгол хэлнээ орчуулж, нутагшуулах үүрэг хүлээлгэх. Энэхүү үйл ажиллагааг R5.1.2-тэй уялдуулах.

R4.1.5 Кибер аюулгүй байдлын бодлого болон хууль эрх зүйн мэргэжлийн ур чадвар хөгжүүлэх зорилгоор зохион байгуулсан үндэсний хөтөлбөрт хөрөнгө оруулалт хийж, кибер хууль эрх зүйн хүрээний дагуу бүх байгууллагууд хууль, зохицуулалтын үүргээ хэрэгжүүлэх боломжийг бүрдүүлэх хэрэгтэй. R3.3.1-тэй уялдуулан хэрэгжүүлэх.

R4.1.6 R1.3.1-д заасны дагуу, 2021 оны Кибер аюулгүй байдлын тухай хууль хүчин төгөлдөр мөрдөгдөж эхлэхтэй зэрэгцэн, онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын зохицуулалтын стандартыг мөрдөж буй байдал, зөрчил, эмзэг байдлын ил тод байдлыг хангах үйл явцыг хянах. Мөн, нийцлийн үнэлгээг хийхээр төлөвлөсөн үйл ажиллагааны үр нөлөөг тогтмол хянан үнэлэх.

R4.1.7 R1.3.4-д заасны дагуу, онц чухал мэдээллийн дэд бүтэц (ОЧМДБ)-ийн оролцогч талуудтай хэлэлцүүлэг зохион байгуулж, Кибер аюулгүй байдлын тухай хуулийн талаар санал хүсэлтийг нь авах. Кибер аюулгүй байдлын төлөвшлийн загвар (СММ)-ын хүрээнд зарим оролцогчид хуулийн ойлгомжгүй байдал, нарийвчлалын түвшинтэй холбоотой санаа зовнилоо илэрхийлсэн болохыг анхаарч үзэх. Хуулийг саадгүй хэрэгжүүлэхийн тулд бүх оролцогч талууд шаардлагыг тодорхой ойлгож байгаа эсэхийг баталгаажуулах нь чухал.

R4.1.8 Кибер аюулгүй байдлын зөвлөлийн удирдлага дор, хууль, эрх зүйн тогтолцооны хэрэгжилт, үйл ажиллагааг хангахад зайлшгүй шаардлагатай кибер аюулгүй байдлын мэргэжилтний гүйцэтгэх ажлыг тодорхойлж, тэргүүлэх чиглэлд авч үзэх. Үүнд, хууль тогтоомжийг үр дүнтэй хэрэгжүүлэх, үйл ажиллагаанд нэвтрүүлэхэд чухал үүрэгтэй ЦХИХХЯ, ТЕГ зэрэг байгууллагын гол албан тушаалыг оролцуулан ойлгож болно.

R4.1.9 2021 оны Кибер аюулгүй байдлын тухай хууль, дагалдах Кибер аюулгүй байдлын нийтлэг журмын талаарх одоогийн сургалтын хөтөлбөрүүдийг өргөжүүлж, ОЧМДБ байгууллагын хуулийн дагуу хүлээх үүргийг нэмэгдүүлэх, шинэ кибер хууль, зохицуулалтын тогтолцооны тодорхойгүй байдлыг багасгах. R1.3.4-тэй уялдуулах.

R4.1.10 Монгол Улсын иргэдийн цахим орчин дахь хүний эрхийг хамгаалахын тулд, хүчин төгөлдөр мөрдөгдөж буй эрүүгийн материаллаг болон процессын хууль тогтоомжид хүний эрхийн нөлөөллийн үнэлгээ хийх.

ХОЛБОГДОХ ХУУЛЬ, ЭРХ ЗҮЙН ЗОХИЦУУЛАЛТ

R4.2.1 Одоогийн хэрэглэгчийн эрхийг хамгаалах хууль тогтоомжийг дахин хянаж, түүний цахим орчинд бүрэн хэмжээнд хэрэгжих нөхцөлийг хангахад шаардлагатай арга хэмжээг авах.

ЭРХ ЗҮЙ БОЛОН БОЛОВСОН ХҮЧНИЙ ЧАДАМЖ

R4.3.1 Кибер гэмт хэрэг, кибер аюулгүй байдлын хэргийн мөрдөн шалгах, яллах, шийдвэрлэх хамтын чадавхийг сайжруулах зорилгоор хууль сахиулах байгууллагууд, прокурорын байгууллага болон шүүхийн оролцогч талуудад чиглэсэн үндэсний хэмжээнд уялдаа холбоог хангасан кибер аюулгүй байдлын ур чадварын хөгжлийн хөтөлбөрийг боловсруулах. Энэхүү хөтөлбөр нь одоо байгаа чадавхийн зөрүүг арилгах стратегийн чиглэлтэй байх бөгөөд олон улсын түнш байгууллагуудын туршлага, дэмжлэгийг тусгах ёстой.

R4.3.2 Хууль сахиулах байгууллагуудын кибер гэмт хэргийг илүү дэвшилтэт аргаар үр дүнтэй мөрдөн шалгах боломжийг хангахын тулд, 2021 оны Кибер аюулгүй байдлын тухай хуулийн 15.1.4-д заасан “тоон шинжилгээний лаборатори”-г байгуулахад хөрөнгө оруулалт хийх.

R4.3.3 Хууль сахиулах байгууллагын ажилтнуудын тогтвор суурьшилтай ажиллах нөхцөлийг сайжруулж, хүний нөөцийн тогтвортой байдлыг нэмэгдүүлэх урамшууллын тогтолцоог бий болгох. R3.3.4-д тусгагдсан зөвлөмжүүдтэй уялдуулан, кибер аюулгүй байдлын мэргэжилтнүүдэд зориулсан илүү бүтэцтэй, ил тод карьерын замналыг хөгжүүлэх талаар авч үзэх боломжтой. Үүнд, тогтмол сургалтын боломжууд болон цалин хөлсний шаталсан өсөлтийг тусгах хэрэгтэй.

R4.3.4 R4.1.5-тэй уялдуулан, кибер аюулгүй байдлын хууль, эрх зүйн зохицуулалтын хүрээнд холбогдох зохицуулагч байгууллагуудын чадавхыг сайжруулж, хэрэгжилтийг үр дүнтэй хянах боломжийг нэмэгдүүлэхэд хөрөнгө оруулалт хийх.

АЛБАН БОЛОН АЛБАН БУС ХАМТЫН АЖИЛЛАГААНЫ ТОГТОЛЦОО

R4.4.1 Хууль сахиулах байгууллага, төрийн байгууллага, хувийн хэвшил болон олон улсын хууль сахиулах байгууллага хооронд мэдээлэл солилцоог тасралтгүй үргэлжлүүлэхийн тулд эдгээр байгууллагуудын чадавх, хамтын ажиллагааг тасралтгүй хөгжүүлэх. Үүнд, хууль сахиулах байгууллагуудыг үндэсний болон бүс нутгийн арга хэмжээнд оролцуулах, сургалт, сүлжээ байгуулах боломжийг нэмэгдүүлэх, төр болон хувийн хэвшлийн түншлэлийг санаачлах, харилцан ойлголцлын санамж бичиг (MOU) байгуулах зэрэг арга хэмжээг хэрэгжүүлэх боломжтой.

R4.4.2 Хууль сахиулах байгууллага болон хувийн хэвшлийн оролцогч талуудын хооронд кибер гэмт хэргийн мөрдөн шалгах ажиллагаанд зориулсан аюулгүй мэдээлэл солилцооны механизмыг бий болгох тасралтгүй хүчин чармайлтыг дэмжих. Боловсруулж буй аливаа механизмууд нь Монгол Улсын иргэдийн цахим эрхийг хамгаалсан байдлыг хангах арга хэмжээг авах. R1.2.4-тэй уялдуулан, хууль сахиулах байгууллага болон кибер аюулгүй байдлын экосистемийн бусад гол оролцогч талууд (жишээ нь, Кибер халдлага, зөрчилтэй тэмцэх төвүүд) хооронд ижил төрлийн мэдээлэл солилцооны механизмыг бий болгох асуудлыг авч үзэх.

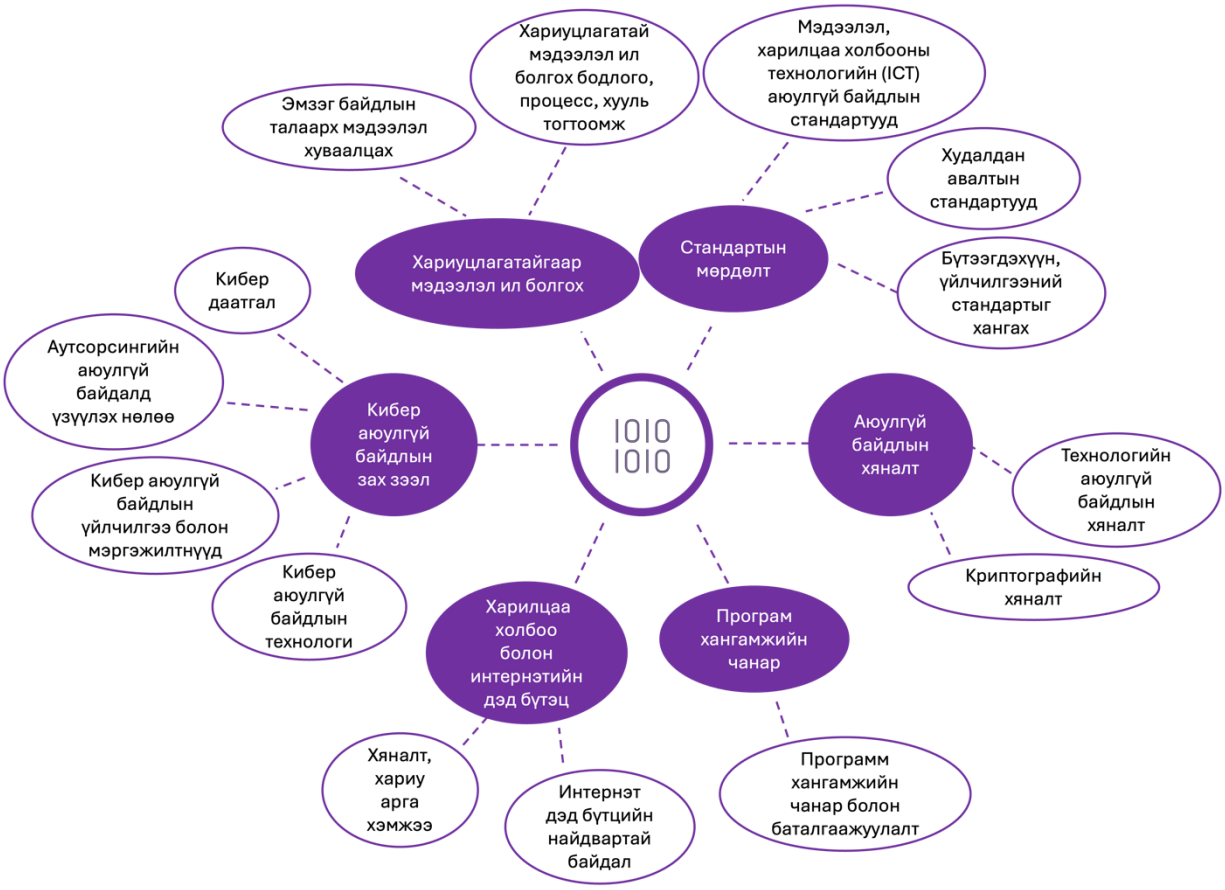
R4.4.3 Олон нийт, бизнес эрхлэгчид болон байгууллагууд хууль сахиулах байгууллагад кибер аюулгүй байдлын зөрчлийг мэдээлэх одоогийн арга замыг хянаж үзэх. Эдгээр тайлангаас цуглуулсан мэдээллийг тодорхой төрлийн кибер гэмт хэргийн шинж чанар, эзлэх хувь хэмжээг илүү сайн ойлгоход хэрхэн ашиглаж болохыг судлах. Уг хяналт, шинжилгээний үр дүнгээс олж авсан сургамжийг ирээдүйн стратегийн шийдвэр гаргах үйл явцад тусгах.

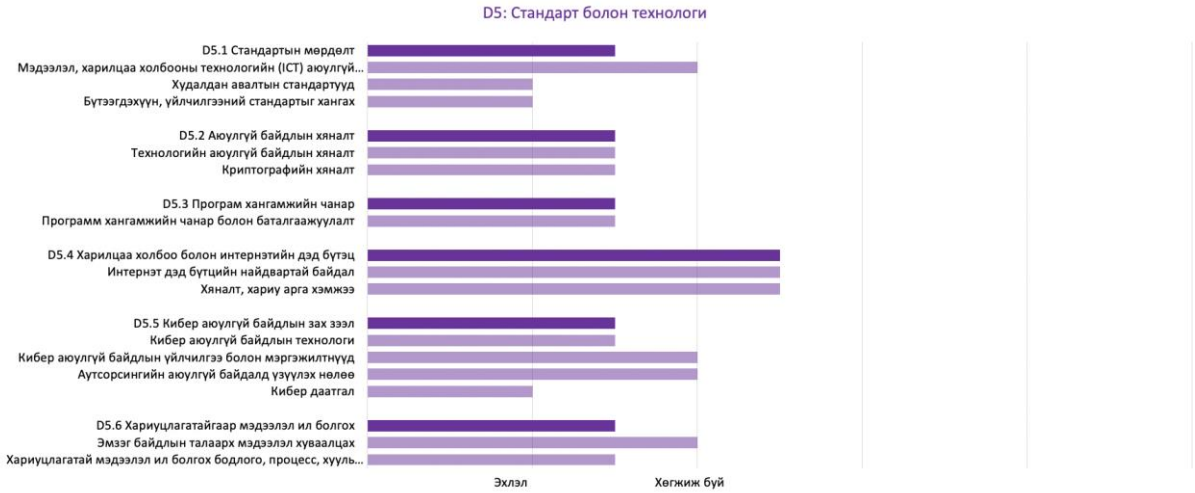
R4.4.4 Засгийн газрын байгууллага, хууль сахиулах байгууллага, прокурор, шүүгч, хувийн хэвшил болон олон улсын түншүүдийн хамтын ажиллагааны харилцааг хянаж, эдгээр харилцааны үр нөлөөг нэмэгдүүлэх боломжуудыг тодорхойлох.

ХЭМЖЭЭС 5

СТАНДАРТ БОЛОН ТЕХНОЛОГИ

Энэ хэмжээс нь хувь хүн, байгууллага болон улсын дэд бүтцийг хамгаалахад чиглэсэн кибер аюулгүй байдлын технологийн үр дүнтэй, өргөн хэрэглээг хамарна. Тус хэмжээс нь кибер аюулгүй байдлын эрсдэлийг бууруулахын тулд кибер аюулгүй байдлын стандарт болон шилдэг туршлагуудыг хэрэгжүүлэх, үйл явц, хяналтыг нэвтрүүлэх, технологи, бүтээгдэхүүн хөгжүүлэх асуудлуудыг нарийвчлан судлахад оршино.





D 5.1 СТАНДАРТЫН УЯЛДАА ХОЛБОО

Энэ хүчин зүйл нь олон улсын кибер аюулгүй байдлын стандартыг болон сайн туршлагыг сурталчлах, хэрэгжилтийг үнэлэх, мөрдөлтийг хянах чиглэлээрх засгийн газрын чадавхыг хянаж үнэлнэ.

Түвшин: **Эхлэл түвшнээс Хөгжиж буй түвшинд**

Олон улсын кибер аюулгүй байдлын стандартыг тодорхойлон, Монгол Улсын орчин нөхцөлд тохируулан нутагшуулж, байгууллагын ашиглах боломжийг бүрдүүлсэн. Тухайлбал, дараах стандартууд албан ёсоор батлагдсан:[81]

- MNS ISO/IEC 17799:2007 – Олон улсын ISO/IEC 17799 стандартыг Монголын үндэсний стандарт болгон нутагшуулсан хувилбар бөгөөд энэ нь ISO/IEC 27002 стандартын өмнөх хувилбар юм.
- MNS ISO/IEC 13335-1:2009 – ISO/IEC 13335-1:2004 стандартыг үндэслэсэн Монголын үндэсний стандарт бөгөөд мэдээлэл, харилцаа холбооны технологийн аюулгүй байдлыг удирдах зааварчилгааг өгдөг.
- MNS 5969:2009 – "Мэдээллийн технологи — Аюулгүй байдлын аргачлалууд — Мэдээллийн аюулгүй байдлын эрсдэлийн удирдлага" нэртэй Монголын үндэсний стандарт бөгөөд байгууллагад мэдээллийн аюулгүй байдлын эрсдэлийг тодорхойлох, үнэлэх, удирдах талаар практик зөвлөмжөөр хангадаг.
- ISO/IEC 27000 бүлийн 5 стандарт.

Оролцогчдын зарим нь эдгээр нутагшуулсан стандартуудыг шинэчлэх шаардлагатай гэж үзсэн. Учир нь олон улсын стандартууд дахин шинэчлэгдсэн бөгөөд орчуулсан байгаа нь өмнөх хувилбар нь юм. Энэ нь Кибер аюулгүй байдлын үндэсний стратегийн "Кибер аюулгүй байдлыг хангах олон улсын стандартыг нутагшуулах, эдгээрийн дагуу дүрэм, журмыг баталж хэрэгжүүлэх" зорилготой нийцэж байна. Гэвч эдгээр стандартуудыг мөрдөх түвшин харилцан адилгүй байна. Зарим салбарт олон улсын стандартууд болон

[81] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Mongolia.pdf

шилдэг туршлагыг хэрэгжүүлэх хандлага ажиглагдаж байгаа боловч нарийвчилсан судалгаа дутмаг байгаа нь тэдгээрийг бүх салбарт хэрхэн дагаж мөрдөж байгааг тодорхойлоход хүндрэл учруулж байна.

Санхүүгийн салбар нь *Кибер аюулгүй байдлын тухай хуулиас* өмнө кибер аюулгүй байдлын стандартуудыг дагаж мөрдөхийг зохицуулалтын байгууллагаас албадан хэрэгжүүлсэн цорын ганц салбар юм. Санхүүгийн салбарын оролцогчид банкны лиценз авахын тулд ISO/IEC 27001 стандартыг мөрдөх шаардлагатай байсан тухай мэдээлсэн бөгөөд үйл ажиллагааныхаа онцлогоос хамааран PCI DSS (Картын төлбөрийн системийн мэдээллийн аюулгүй байдлын стандарт) зэрэг бусад стандартыг дагаж мөрдөх шаардлагатай болсон байна.[82]

Бусад салбарын хувьд, стандартыг дагаж мөрдөх байдал байгууллагын Хөгжиж буй түвшин болон олон улсын хэмжээнд үйл ажиллагаа явуулах шаардлагаас хамаарч өөр өөр байна. Томоохон харилцаа холбооны компаниуд ISO 27001 стандартыг 10 гаруй жилийн турш мөрдөж ирснээ мэдээлсэн бол, зарим төрийн байгууллага болон тээврийн салбарын байгууллагууд уг стандартад нийцэхээр ажиллаж байгаа тухай дурджээ.

Монголын Үндэсний Итгэмжлэлийн Газар ISO 27001 стандартаар итгэмжлэл олгох хамрах хүрээгээ 2024 оны 12 сард өргөжүүлсэн бөгөөд одоо дотоодын зарим итгэмжлэлийн төвүүд ISO 27001 гэрчилгээ олгох чадвартай болсон байна. Энэ нь Монголын байгууллагуудын хувьд өмнө нь энэ итгэмжлэл авахын тулд олон улсын байгууллагатай хамтран ажиллах шаардлагатай байсан асуудлыг шийдэж, хүртээмжийг сайжруулж байгаа юм.

Кибер аюулгүй байдлын тухай хуулийн (дэлгэрэнгүйг D1.3.2-оос харна уу) дагуу ОЧМДБ байгууллагууд олон улсын хэмжээнд хүлээн зөвшөөрөгдсөн кибер аюулгүй байдлын стандартуудыг мөрдөх үүрэгтэй. Мөн ЦХИХХЯ-наас ISO 27001 болон NIST 800 стандартад нийцүүлэн боловсруулсан "*Кибер аюулгүй байдлын нийтлэг журам*"-ыг мөрдөх ёстой. Гэхдээ энэ хуулийн шаардлагуудыг одоогоор бүрэн хэрэгжүүлээгүй бөгөөд ОЧМДБ байгууллагууд хуульд заасан аудитын хугацаа (2025 оны 8 сар)-д нийцэх шаардлагатай гэж мэдээлж байна. ОЧМДБ байгууллагуудын дунд ямар стандартуудыг заавал дагаж мөрдөх ёстойг илүү нарийвчлан тогтоох эсэх талаар маргаан гарсан байна (дэлгэрэнгүйг D1.3-аас үзнэ үү).

Түүнчлэн, төрийн байгууллага болон технологийн үйлчилгээ үзүүлэгчид кибер аюулгүй байдлыг хангах дотоод журам боловсруулах үүрэг хүлээдэг. ЦХИХХЯ-наас "*Кибер аюулгүй байдлын нийтлэг журам*"-ыг сурталчлах, байгууллагуудыг сургалтанд хамруулах ажлыг зохион байгуулсан бөгөөд одоогоор 600 гаруй төрийн албан хаагч хамрагдаад байна.

Зарим томоохон ОЧМДБ байгууллагууд эдгээр стандартыг хэрэгжүүлэх хангалттай нөөцтэй боловч жижиг, дунд байгууллагууд санхүү, хүний нөөцийн хүндрэлтэй тулгарч болзошгүй талаар санал гарсан. Иймээс жижиг, дунд байгууллагад тохирсон стандарт эсхүл шилдэг туршлагын удирдамж боловсруулах боломжийг судлах хэрэгтэй.

ОЧМДБ болон төрийн байгууллагуудаас бусад байгууллагууд кибер аюулгүй байдлын стандартуудыг ямар түвшинд мөрдөж байгаа талаар үнэлсэн нотолгоо байхгүй байна. Гэхдээ хувийн хэвшлийн байгууллагуудад кибер аюулгүй байдлын стандартуудыг сурталчлах, "*Кибер аюулгүй байдлын нийтлэг журам*"-ыг хэрэгжүүлэх, тэдгээрийн ашиглалтыг хэмжих механизм боловсруулах нь ач холбогдолтой байж болох юм.

---

[82] https://www.mongolbank.mn/file/beb8a25d6bc7b7f718f2a9a71f0c2b39/files/2018_03_06_A57.pdf

Монголын байгууллагууд бараа, үйлчилгээ худалдан авах үйл явцыг зохицуулахдаа (үүнд эрсдэлийн удирдлага, ашиглалтын хугацааны менежмент, программ хангамж болон техник хангамжийн баталгаажуулалт, гадаад аутсорсинг, үүлэн үйлчилгээ ашиглалт зэрэг орно) ямар стандартыг ашиглах талаар засгийн газраас тодорхой удирдамж өгсөн зүйл байхгүй байна. Зарим илүү хөгжсөн байгууллагууд эдгээр үйл явцыг зохицуулахдаа стандарт ашиглаж байгаа боловч хэрэгжилт нь тогтмол бус, уялдаа холбоогүй байна. Хэлэлцүүлэгт оролцогчдын зүгээс худалдан авалтын стандарттай холбоотой удирдамж шаардлагатай гэж үзсэн бөгөөд энэ нь байгууллагууд бүтээгдэхүүн худалдан авахдаа ямар шалгуур үзүүлэлтийг анхаарах ёстойг тодорхой зааж өгөх ёстой гэжээ.

ОЧМДБ болон төрийн байгууллагуудын хувьд, бүтээгдэхүүний аюулгүй байдлыг шалгах чиглэлээр тодорхой ахиц гарсан байна. Кибер аюулгүй байдлын үндэсний стратегид “Төрийн болон үндэсний ач холбогдол бүхий дэд бүтцийн байгууллагуудын ашиглаж буй мэдээлэл, харилцаа холбооны тоног төхөөрөмж болон мэдээллийн системийг шалгаж, баталгаажуулах тоон шинжилгээний лаборатори байгуулах” зорилт тусгагдсан. Энэхүү лаборатори аль хэдийн байгуулагдсан талаар мэдээлсэн бөгөөд ОЧМДБ байгууллагуудын ашиглаж буй техник, программ хангамжийн кибер аюулгүй байдлыг баталгаажуулах үүрэгтэй. Гэвч уг лаборатори нь ОЧМДБ байгууллагуудын авч буй шинэ техник, програм хангамжийг урьдчилан илрүүлэх, үнэлэх албан ёсны механизм байхгүй тул одоогоор кибер аюулгүй байдлын үнэлгээг тогтвортой хийж чадахгүй байгаа юм. Оролцогчид мөн төрийн байгууллагын худалдан авалтын хууль нь аюулгүй, нийцтэй бүтээгдэхүүн авахад хүндрэл үүсгэх боломжтойг онцолсон. Учир нь тус хуулийн гол зорилго нь хамгийн хямд үнийн саналыг сонгох зарчим дээр тулгуурладаг гэж үзжээ. Тиймээс холбогдох талуудтай хамтран энэхүү хуулийн болзошгүй хүндрэлүүдийг судлах нь чухал.

Мөн программ хангамж хөгжүүлдэг технологийн үйлчилгээ үзүүлэгчдийн тоо нэмэгдэж байгаа ч (дэлгэрэнгүйг D5.3-аас харна уу), төр засгаас стандартыг хэрхэн мөрдөж буйг сурталчлах, хянах үйл ажиллагаа явуулж байгаа талаар нотолгоо байхгүй байна.

Кибер аюулгүй байдлын тухай хууль технологийн үйлчилгээ үзүүлэгчдэд өөрсдийн байгууллагын аюулгүй байдлыг хангах үйл явц нэвтрүүлэх шаардлага тавьсан. Гэхдээ уг хуульд бүтээгдэхүүн хөгжүүлэх явцад аюулгүй байдлын стандартыг дагаж мөрдөх шаардлагын талаар тодорхой заалт байхгүй байна. Иймээс програм хангамжийн хөгжүүлэлт, техник хангамжийн чанарын баталгаажуулалт, менежменттэй болон үүлэн үйлчилгээ үзүүлэх явцад технологи болон үйлчилгээ үзүүлэгч байгууллагууд стандартыг хэрхэн ашиглаж буйг дэмжих болон хянах боломжийг судлах нь чухал.

D 5.2 АЮУЛГҮЙН БАЙДЛЫН ХЯНАЛТУУД

Энэ хүчин зүйл нь хэрэглэгчид болон төр, хувийн хэвшлийн байгууллагуудын хэрэгжүүлж буй аюулгүй байдлын хяналтын арга хэмжээнүүдийн нотолгоог үнэлж, кибер аюулгүй байдлын технологийн хяналтын багц нь батлагдсан кибер аюулгүй байдлын хүрээний дагуу зохион байгуулагдсан эсэхийг шалгана.

Түвшин: **Эхлэл түвшнээс Хөгжиж буй түвшинд**

Монгол Улсын зарим төрийн болон хувийн хэвшлийн байгууллагууд аюулгүй байдлын хяналтыг нэвтрүүлж байгаа боловч энэ нь бүх салбарт ижил түвшинд хэрэгжиж чадахгүй байна. Санхүүгийн салбарт байгууллагууд кибер аюулгүй байдлын стандарт дагаж мөрдөх зохицуулалттай учир технологийн болон криптографийн аюулгүй байдлын хяналтыг хэрэгжүүлдэг.

Одоогийн байдлаар технологийн болон криптографийн аюулгүй байдлын хяналтын хэрэгжилт нь тухайн байгууллагын нөөц бололцоо, кибер аюулгүй байдлын талаарх мэдлэг, мөн стандарт мөрдөх байдлаас (D5.1-г үзнэ үү) хамааран харилцан адилгүй байна. 5.1-р хэсэгт тайлбарласанчлан, 2025 оны 8 сард хяналт, шалгалтын хугацаа дуусах үед *Кибер аюулгүй байдлын тухай хуулийн* дагуу ОЧМДБ ангилалд багтах байгууллагууд кибер аюулгүй байдлын дотоод журам боловсруулах, стандарт мөрдөх үүрэг хүлээх бөгөөд технологийн, криптографийн хяналтын хэрэгжилтийг хянах болно. Үүний үр дүнд, эдгээр байгууллагуудын аюулгүй байдлын хяналтууд илүү жигд хэрэгжих төлөвтэй байна.

Судалгааны байгууллага болон хувийн хэвшлийн кибер аюулгүй байдлын компаниудын судалгаагаар зарим салбарт аюулгүй байдлын хяналтын хэрэгжилт хангалтгүй байгаа нь тогтоогдсон. Тухайлбал, эрүүл мэндийн салбарыг энэ асуудалтай салбаруудын нэгээр онцолж байна.

Засгийн газрын төлөөлөгчид төрийн байгууллагуудад чиглэсэн кибер халдлагын, тухайлбал зорилтот халдлагын (APT) тархалттай холбоотой асуудалд санаа зовниж буйгаа илэрхийлсэн. Түүнчлэн төсвийн асуудал нь кибер аюулгүй байдлын хяналтыг хэрэгжүүлэхэд хүндрэл учруулж байгаа талаар мэдээлсэн. Иймд Сангийн яамнаас байгууллагуудад кибер аюулгүй байдлын хяналтыг хэрэгжүүлэхэд шаардлагатай төсөв хуваарилах механизмыг судлах хэрэгтэй. Зарим оролцогчид байгууллагын кибер аюулгүй байдлын төсөв хүсэх боломжийг бий болгохын тулд тусдаа төсвийн ангилал үүсгэх санал гаргасан.
Төрийн байгууллагаас гадна хувийн хэвшлийн байгууллагууд ч мөн адил аюулгүй байдлын хяналтын хэрэгжилтэд зориулсан төсөв гаргах асуудлаар санаа тавьж байна. Байгууллагын удирдлагуудын зүгээс кибер аюулгүй байдлыг санхүүжилтийн хувьд тогтмол тэргүүлэх ач холбогдолтой асуудал гэж үздэггүй тул энэ чиглэлд удирдлагын түвшинд мэдлэг, ойлголтыг нэмэгдүүлэх санаачилга хэрэгжүүлэх нь үр дүнтэй байж болно.

Төрийн байгууллагууд өөрсдийн системийг ҮДТ-д байршуулдаг бөгөөд ТЕГ-н Мэдээллийн аюулгүй байдлын газраас (МАБГ) ажиллуулдаг төрийн мэдээллийн нэгдсэн сүлжээнд холбосон байдаг. Энэхүү сүлжээ нь холбогдсон төрийн байгууллагуудын

хооронд мэдээлэл солилцох зориулалттай. МАБГ-аас засгийн газрын мэдээллийн сүлжээнд сүлжээний түвшний аюулгүй байдлын хяналтууд, жишээлбэл, сүлжээний халдлага илрүүлэх систем (Network based Intrusion Detection Systems) хэрэгжүүлдэг ч төрийн байгууллагын системүүд дээр төгсгөлийн цэгийн түвшний аюулгүй байдлын хяналтуудыг хэрэгжүүлдэггүй гэж мэдэгдсэн. Эдгээр хяналтуудыг хэрэгжүүлэх үүрэг нь тухайн байгууллагад өөрсдөд нь хамаарна. D1.2-д дурдсанчлан, ҮДТ нь өөрийн хариуцаж буй төрийн системд кибер аюулгүй байдлын зөрчил үүссэн тохиолдолд хариу арга хэмжээ авахад дэмжлэг үзүүлдэг тохиолдлууд байдаг. Мөн ҮДТ нь төрийн байгууллагуудын вэбсайт болон үйлчилгээний серверүүдийг байршуулдаг боловч тэдгээрийн аюулгүй байдлыг хариуцдаггүй. ҮДТ нь мөн төрийн үүлэн технологид суурилсан үйлчилгээг (government cloud) байршуулахын зэрэгцээ түүний аюулгүй байдлыг хариуцдаг. Уг үүлэн технологид суурилсан үйлчилгээ нь зарим төрийн байгууллагын имэйл системийг байршуулдаг бөгөөд төрийн байгууллагын ашиглах боломжтой тооцооллын нөөц юм. ҮДТ-ийн аюулгүй байдлын хяналтын хэрэгжилтийн хувьд, тус байгууллага нь ISO 27001 стандартыг мөрдөн хэрэгжүүлж, уг стандартаар баталгаажсан болохыг мэдээлсэн. Түүнчлэн газар зүйн байршлын хувьд тусгаарлагдсан мэдээлэл нөхөн сэргээх нөөц төвийг ажиллуулдаг.

Төрийн үйлчилгээ улам бүр цахимжиж буй энэ үед аюулгүй байдлын хяналтыг тууштай хэрэгжүүлэх нь чухал юм. И-Монголиа вэбсайт[83] нь иргэд болон байгууллагад зориулсан төрийн үйлчилгээг цахим хэлбэрээр улам бүр өргөжүүлэн хүргэж байна. Үүнд, иргэдийг нэгдсэн цахим таних систем (ҮДТ-өөс ажиллуулдаг нэг удаагийн нэвтрэх систем буюу single-sign-on) ашиглан төрийн цахим үйлчилгээнд хандах боломжийг олгох зэрэг хүчирхэг аюулгүй байдлын боломжууд багтсан. Гэвч төрийн байгууллагуудын байршуулсан системийн аюулгүй байдал сул байвал эрсдэл үүсгэж болзошгүй юм. Төрийн төлөөлөгчид мэдлэг, шилдэг туршлагаа солилцох боломжтой платформ эсхүл бага хурал зохион байгуулах нь үр өгөөжтэй байж болох тухай санал гарсан.

Төрийн болон хувийн хэвшлийн олон байгууллагад кибер аюулгүй байдлын туршлагатай ажилтны хомсдолтой байгаа нь хяналт хэрэгжүүлэхэд хүндрэл учруулж байгаа талаар тэмдэглэсэн. Ихэнх томоохон байгууллагууд мэдээллийн технологи хариуцсан зөвхөн нэг ажилтантай бөгөөд кибер аюулгүй байдлын тусгай мэргэжилтэн байхгүй байна. *Кибер аюулгүй байдлын тухай хууль* хүчин төгөлдөр болох үед ОЧМДБ байгууллагууд кибер аюулгүй байдлын ажилтан эсхүл тусгай нэгжтэй байх ёстой гэсэн шаардлага тавигдсан. Гэсэн хэдий ч өндөр ур чадвартай ажиллах хүчний хомсдол болон төрийн салбарын байгууллагууд харьцангуй бага цалинтай тул туршлагатай мэргэжилтнийг ажилд татахад асуудал тулгараад байна. Зарим байгууллагууд хуульд нийцэхийн тулд кибер аюулгүй байдлын ажилтан ажилд авах оролдлого хийж байгаа боловч энэ нь бэрхшээлтэй хэвээр байна.

Зарим хувийн хэвшлийн оролцогчид криптографийн хяналт болон мэдээлэл боловсруулах аргачлалыг мэдээллийг оршин буй төлөвт (data at rest) хамгаалахад ашиглаж байгааг дурдсан. Гэхдээ энэ нь байгууллага бүрд ижил түвшинд хэрэгждэггүй. Жишээ нь, төрийн албан хаагчид зарим тохиолдолд эмзэг мэдээллийг нийгмийн сүлжээгээр дамжуулдаг, мөн оршин буй төлөвт буй мэдээлэл, тэр дундаа хувийн мэдээллийг хамгаалахад хангалттай эрхийн хяналт байхгүй гэх асуудал гарсан. Зарим төрийн байгууллага нь ТЕГ-тай хамтран мэдээлэл дамжуулах, хадгалах бодлогоо

[83] https://e-mongolia.mn/home

сайжруулах чиглэлээр ажиллаж байна. Үүнийг сайжруулахын тулд төрийн байгууллагын мэдээлэл дамжуулахад нийгмийн сүлжээг ашиглахыг хориглох нэгдсэн бодлого боловсруулах, мөн төрийн албан хаагчдад зориулсан аюулгүй, хяналттай харилцааны платформ бий болгох зэрэг арга хэмжээг санал болгосон. Түүнчлэн байгууллагын хоорондын криптографийн шаардлагуудын уялдаа байхгүй нь мэдээлэл солилцоонд хүндрэл үүсгэдэг тул үүнийг зохицуулж, стандартчилах арга замыг судлах хэрэгтэй.

Монгол Улсад Интернэт үйлчилгээ үзүүлэгчид тодорхой хэмжээгээр аюулгүй байдлын үйлчилгээ үзүүлж байна. Оролцогчдын мэдээлснээр, Харилцаа холбооны зохицуулах хорооноос интернет үйлчилгээ үзүүлэгч нь харилцагчдад DDoS халдлагаас хамгаалах үйлчилгээ үзүүлэхийг шаарддаг зохицуулалт байгаа боловч бүх үйлчилгээ үзүүлэгч байгууллагууд энэ шаардлагыг хангах хангалттай нөөц бололцоотой биш байна. Зарим нь галт хана (firewall) болон эмзэг байдал шалгагч (vulnerability scanning) зэрэг аюулгүй байдлын үйлчилгээ санал болгодог гэж мэдээлжээ.

Монгол Улсад нийтийн түлхүүрийн дэд бүтэц (PKI) хэрэгждэг бөгөөд үндсэн гэрчилгээжүүлэх байгууллага (CA)-ыг ЦХИХХЯ эзэмшдэг бөгөөд Үндэсний Дата Төв (ҮДТ) дээр байршдаг. Улсын хэмжээнд нийт гурван гэрчилгээжүүлэх байгууллага байдаг. Гэсэн хэдий ч эдгээр гэрчилгээжүүлэх байгууллагуудын олгож буй цахим гэрчилгээнүүд нь гадаадын үндсэн гэрчилгээжүүлэх байгууллагад хамаардаг (өөрөөр хэлбэл, Монгол Улсад дотоодын үндсэн гэрчилгээжүүлэх байгууллага байхгүй). *Кибер аюулгүй байдлын үндэсний стратегид* үндэсний тоон гарын үсгийг олон улсад ашиглах боломж бүрдүүлэх зорилтот үйл ажиллагаа багтсан бөгөөд үүнд одоогийн дэд бүтцийг шинэчлэх, олон улсын итгэмжлэгдсэн жагсаалтад оруулах ажлыг хэрэгжүүлэх шаардлагатай гэж заасан.

ҮДТ-ийн мэдээлснээр, зарим өндөр хөгжсөн хэрэглэгчид вэбсайтын өгөгдлийг Transport Layer Security (TLS) ашиглан тоон гарын үсэг зурах болон шифрлэхийн тулд цахим гэрчилгээ авах хүсэлт гаргадаг боловч бүгд биш юм. 2021 оны *Тоон гарын үсгийн тухай хууль* нь Монгол Улсад тоон гарын үсэг ашиглах хууль эрх зүйн нөхцөлийг тодорхойлсон.

Зарим байгууллагууд өөрсдийн вэбсайт, үйлчилгээнд аюулгүй байдлын функцүүдийг хэрэгжүүлэхэд олон нийтийн кибер аюулгүй байдлын талаарх мэдлэг хангалтгүй байгаагаас болж хүндрэл учирч байгаа талаар дурдсан. Тухайлбал, аюулгүй байдлын нэмэлт функцууд хэрэглэгчдэд хүндрэл учруулж байгаа мэт ойлголтыг төрүүлж байгаа тул зарим байгууллагууд тэдгээрийг хэрэгжүүлэхээс татгалзах сонголт хийхэд хүрч байна. Кибер аюулгүй байдлын үйлчилгээ үзүүлэгч зарим байгууллага энэ нөхцөл байдлын улмаас хэрэглэгчдэд чиглэсэн үйлчилгээндээ тодорхой аюулгүй байдлын функцуудыг хэрэгжүүлэхээс зайлсхийж байгаа талаар мэдээлсэн. Энэ нь байгууллагуудыг аюулгүй байдлыг хангах, хэрэглэгчдийн сэтгэл ханамжийг хадгалах гэсэн хоёрдмол сонголтод оруулж байна.

D 5.3 ПРОГРАММ ХАНГАМЖИЙН ЧАНАР

Энэ хүчин зүйл нь төрийн болон хувийн хэвшлийн салбарт програм хангамжийг нэвтрүүлэх чанар болон үйл ажиллагааны шаардлагуудыг судалдаг. Түүнчлэн, энэ хүчин зүйл нь эрсдэлийн үнэлгээ болон үйлчилгээний чухал байдлын үндсэн дээр програм хангамжийн шинэчлэлт, засвар үйлчилгээний бодлого, үйл явцын оршин тогтнол болон сайжруулалтын түвшинг хянаж үнэлнэ.

Түвшин: Эхлэл түвшнээс Хөгжиж буй түвшинд

Зарим байгууллагууд программ хангамжийн чанарын шаардлагыг хүлээн зөвшөөрдөг. Хувийн хэвшлийн онц чухал мэдээллийн дэд бүтэцтэй байгууллагын зарим оролцогчид худалдан авсан программ хангамжид аюулгүй байдлын хяналт, туршилтын үйл явцыг хэрэгжүүлдэг талаар дурдсан бөгөөд программ хангамжийн шинэчлэлт, засвар үйлчилгээг тогтмол хийх хөгжингүй үйл ажиллагааны тогтолцоотой байдаг гэж онцолсон.

Гэсэн хэдий ч өндөр чанартай, аюулгүй программ хангамж ашиглах энэ түвшний чадамж бүх байгууллагад ижил хэмжээнд хэрэгждэггүй. Зарим байгууллага лицензтэй програм хангамж болон кибер аюулгүй байдлын технологи худалдан авах нөөц эсхүл мэдлэг дутагдалтайгаас үүдэн лицензгүй эсхүл хууль бус програм хангамж ашиглах асуудал гарч болох талаар илэрхийлсэн. ЦХИХХЯ-ы долоон өөр төрийн байгууллагын дунд явуулсан сүүлийн судалгааны үр дүнгээс харахад нэг гол асуудал нь лицензгүй программ хангамж ашиглаж байсан явдал байсныг онцолсон нь мөн уг асуудлыг бататгаж байна. Лицензгүй программ хангамж ашиглах нь ОЧМДБ байгууллагууд болон бусад төрийн байгууллагууд мөрдөх шинэ "*Нийтлэг журам*"-нд харшилж байгаа ч, журам нь бүрэн хэрэгжиж, аудит хийгдээгүй байна.

Оролцогчдын мэдээлснээр, дотоодын программ хангамж хөгжүүлэгч компаниуд сүүлийн үед программ хангамж хөгжүүлэхдээ аюулгүй байдлын стандартуудыг ашиглах нь нэмэгдэж байгаа ч энэ нь өмнө нь бараг хэрэглэгдэж байгаагүй. Энэхүү өөрчлөлтийн шалтгаан нь кибер аюулгүй байдлын үйлчилгээ үзүүлэгчдийн тоо нэмэгдэж, дотоодын программ хангамжийн компаниудын ашиг орлого өсөж, кибер аюулгүй байдлын үйлчилгээг худалдан авах боломжтой болж байгаатай холбоотой гэж тайлбарлаж байна. Зарим оролцогчдын зүгээс, гадаадаас худалдан авсан программ хангамж нь илүү стандартчилагдсан, найдвартай байдаг гэсэн байр суурь илэрхийлсэн. Хувийн хэвшлийн байгууллагуудын төлөөлөгчид дотоодын программ хангамжийг ашиглахдаа илүү анхааралтай хандах, нэмэлт аюулгүй байдлын хяналт, туршилт хийх шаардлагатай гэж онцолсон. Учир нь ихэнх дотоодын программ хангамж стандартчилагдаагүй байдаг болон түүний аюулгүй байдал нь хөгжүүлэгч компанийн чанараас хамаардаг.

Одоогоор баталгаажсан программ хангамжийн платформуудын албан ёсны каталог байхгүй тул байгууллагууд худалдан авалт хийхдээ чиглүүлэх мэдээлэл авах дээр дутмаг байна. Төрийн байгууллагуудын аюулгүй программ хангамж худалдан авах, ашиглах үйл явцыг хангах механизм хангалтгүй байж болзошгүй. Оролцогчдын зүгээс төрийн байгууллагууд программ хангамж хөгжүүлэх тендер зарлахдаа эхний техникийн тодорхойлолтод кибер аюулгүй байдлын шаардлагыг тусгадаггүй гэсэн шүүмж гарсан. Зарим тохиолдолд ЦХИХХЯ төслийн явцад аюулгүй байдлын шаардлагыг нэмэх

шаардлагатай болдог бөгөөд энэ нь нэмэлт ажлын ачаалал үүсгэж, төслийн явцыг хүндрүүлдэг. Яамд хоорондын уялдаа холбоог нэмэгдүүлж, төрийн тендерийн шалгуурт кибер аюулгүй байдлын шаардлагуудыг эхнээс нь тусгах нь илүү үр ашигтай.

D 5.4 ХАРИЛЦАА ХОЛБОО БОЛОН ИНТЕРНЭТ ДЭД БҮТЭЦ

Энэ хүчин зүйл нь улс оронд найдвартай интернет үйлчилгээ болон дэд бүтэц оршин байгаа эсэх, мөн хувийн болон төрийн секторт стандарт өндөр аюулгүй байдлын үйл явц хэрэгжиж байгаа эсэхийг хөнддөг. Түүнчлэн, энэ хүчин зүйл нь төр өөрийн интернет дэд бүтцэд хэр зэрэг хяналт тавьж байгаа болон сүлжээ, системүүдийг хэрхэн аутсорсинг хийж буй судалдаг.

Түвшин: **Хөгжиж буй түвшнээс Тогтворжсон түвшинд**

Монгол Улсад найдвартай интернэт үйлчилгээ өргөн хүрээнд ашиглагдаж байгаа гэж мэдээлсэн. 2024 онд улсын хэмжээнд 2.9 сая орчим интернэт хэрэглэгч байсан бөгөөд тэдний ихэнх нь гар утасны өргөн зурвасын технологи ашигладаг байна.[84]
Дэд бүтэц нь газар доогуур дамжих шилэн кабелийн сүлжээнээс бүрддэг бөгөөд энэ нь ОХУ-аар дамжин Европын орнууд руу, мөн БНХАУ-аар дамжин АНУ руу холбогддог. Мөн улсын 21 аймгийг хамарсан өргөн цар хүрээтэй үндэсний шилэн кабелийн сүлжээ бий.[85] Алслагдсан бүс нутгуудын хувьд интернэтийн хүртээмжийг хиймэл дагуулын холболтоор нэмэгдүүлж байгаа бөгөөд Starlink хиймэл дагуулын холболтоор сүлжээний хүртээмж, хурдыг сайжруулсан талаар дурджээ. Гэсэн хэдий ч зарим алслагдсан бүс нутагт холболтын асуудал байсаар байна.
Интернэт дэд бүтцийг албан ёсоор Харилцаа холбооны зохицуулах хороо (CRC) удирддаг. CRC нь интернэт үйлчилгээ үзүүлэгчдэд лиценз олгож, зохицуулалт хийдэг. Тухайлбал, ISP-үүдийн интернэт урсгалын тодорхой хувийг өөр замаар чиглүүлэх шаардлагыг тавьдаг нь сүлжээний найдвартай байдлыг нэмэгдүүлэх зорилготой.
Мөн ISP нарыг үйлчлүүлэгч байгууллагуудад DDoS халдлагаас хамгаалах үйлчилгээ үзүүлэх шаардлага тавигддаг. Гэвч бүх ISP-үүд энэ шаардлагыг хангах нөөц бололцоотой биш бөгөөд энэ шаардлагыг тууштай хэрэгжүүлж байгаа эсэх нь тодорхойгүй байна. Сүлжээний найдвартай байдлын талаар, Үндэсний Дата Төв (УДТ) нь Монголын Интернэт Солилцооны Цэг (IXP)-ийг ажиллуулдаг бөгөөд энэ нь ISP-үүдийн хооронд өгөгдөл солилцох боломжийг бүрдүүлж, аль нэг ISP доголдсон тохиолдолд урсгалыг хэвийн үргэлжлүүлэхэд тусалдаг. Шинэ IXP байгуулах талаар ISP-үүд болон Харилцаа холбооны зохицуулах хороо хооронд хэлэлцэж байгаа талаар мэдээлсэн.

Оролцогчдын үзэж байгаагаар, Монголд интернэт үйлчилгээг цахим худалдаа болон цахим бизнесийн гүйлгээ хийхэд ерөнхийдөө найдвартай гэж үздэг. Үүнтэй холбоотой хэмжилтүүд цуглуулсан гэх нотолгоо байхгүй бөгөөд, үүнийг хэмжих нь аливаа асуудлыг илрүүлэхэд туслах боломжтой.

---

84 https://pubcert.mn/sites/default/files/2024-04/Cyber%20book.pdf

85 https://www.apt.int/sites/default/files/2019/09/ADF-16_INP-17_Mongolia_Development_of_National_Broadband_infrastructure_in_Mongolia_and_its_usage.pdf

Кибер аюулгүй байдлын тухай хуулийн дагуу харилцаа холбооны байгууллагуудыг ОЧМДБ байгууллага гэж тодорхойлсон. Ингэснээр тус салбарт эрсдэлийн үнэлгээ, аудит хийх, дотоод кибер аюулгүй байдлын журам, стандарт хэрэгжүүлэх, кибер халдлагад хариу үзүүлэх төлөвлөгөө боловсруулах зэрэг хэд хэдэн үүрэг хүлээж байна. Энэхүү хууль хэрэгжихээс өмнө харилцаа холбооны салбар нь кибер аюулгүй байдлын талаар зохицуулалтгүй байсан гэж тэмдэглэсэн.

D 5.5 КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЗАХ ЗЭЭЛ

Энэ хүчин зүйл нь кибер аюулгүй байдлын өрсөлдөх чадвартай технологиуд, кибер даатгалын бүтээгдэхүүн, кибер аюулгүй байдлын үйлчилгээ, мэргэжлийн ур чадварын хүртээмж, мөн аутсорсингийн аюулгүй байдлын үр дагавар зэрэг асуудлуудын хүртээмж болон хөгжлийг авч үздэг.

Түвшин: **Эхлэл түвшнээс Хөгжиж буй түвшинд**

Монголын компаниудаас гаргасан кибер аюулгүй байдлын бүтээгдэхүүн байхгүй гэж оролцогчид мэдээлсэн. Монголд ашиглагдаж буй кибер аюулгүй байдлын бүтээгдэхүүнийг гадаад нийлүүлэгчид хангадаг бөгөөд зарим борлуулагчид Монголд үйл ажиллагаа явуулдаг. Гадаад технологид хэт найдах эрсдэлийг харгалзан, дотоодын бүтээгдэхүүн үйлдвэрлэлийг нэмэгдүүлэх зорилго тавьж байгаа бөгөөд Кибер аюулгүй байдлын үндэсний стратегид "мэдээлэл, харилцаа холбооны тоног төхөөрөмж, программ хангамж, электроникийн үндэсний үйлдвэрлэл, инновац, судалгаа, шинжилгээг дэмжиж, технологийн хамаарлыг бууруулах" үйл ажиллагаа тусгагдсан байна. Зарим оролцогчид тодорхой улсуудаас технологи худалдан авах нь эрсдэлтэй байж болзошгүй гэж үзэж байна. Учир нь зарим Монголын байгууллагууд APT буюу төрийн дэмжлэгтэй халдлагад өртсөн тохиолдол гарч байсан. Энэ асуудлыг цаашид хэлэлцэх шаардлагатай.

Монголын кибер аюулгүй байдлын үйлчилгээний салбар сүүлийн гурван жилийн хугацаанд хурдацтай өргөжсөн гэж оролцогчид тэмдэглэсэн. Одоогоор компаниуд кибер аюулгүй байдлын стандартын аудит, нэвтрэлтийн шалгалт (penetration testing), Мэдээллийн аюулгүй байдлын менежментийн тогтолцоо (ISMS) хэрэгжүүлэх үйлчилгээ санал болгож байна. ОЧМДБ зарим байгууллагууд дотоодын кибер аюулгүй байдлын зөвлөх үйлчилгээ ашиглаж байсан туршлагатай гэж мэдээлсэн. Гэхдээ олон улсын мэргэжлийн гэрчилгээтэй үйлчилгээ үзүүлэгчдийн тоо хязгаарлагдмал байна.

Засгийн газрын зарим оролцогчдын зүгээс кибер аюулгүй байдлын үйлчилгээ үзүүлэгчдийн тоо өсөж байгаа ч одоо ч эрэлт хэрэгцээг хангахгүй байгааг онцолсон. Тэр дундаа, *Кибер аюулгүй байдлын тухай хуулийн* шаардлагыг хангахын тулд хангалттай тооны үйлчилгээ үзүүлэгч байх шаардлагатай. Уг хуулийн дагалдах журамд ОЧМДБ байгууллагын аудит хийх үйлчилгээ үзүүлэгч нь мэргэжлийн холбоо эсхүл стандартын байгууллагад хүлээн зөвшөөрөгдсөн гэрчилгээтэй бүтэн цагийн ажилтантай байх ёстой гэж заасан. ЦХИХХЯ уг шаардлагыг хангасан үйлчилгээ үзүүлэгчдийг үнэлэхэд маш цөөн тооны компани уг шаардлагыг хангаж байгаа нь тогтоогджээ.

ОЧМДБ байгууллагад аудит, эрсдэлийн үнэлгээ хийх үйлчилгээ үзүүлэгчдэд хууль эрх зүйн тусгай шаардлага тавигддаг. *Кибер аюулгүй байдлын тухай хуулийн* дагуу эдгээр үйлчилгээ үзүүлэгчид ЦХИХХЯ-ны албан ёсны зөвшөөрөлтэй байх ёстой, мөн гадаад байгууллагуудаас хийгдсэн эрсдэлийн үнэлгээ нь ТЕГ-аар баталгаажсан байх

шаардлагатай. Гэхдээ бусад байгууллагууд үйлчилгээ үзүүлэгч сонгоход дагах удирдамж байхгүй гэж тэмдэглэсэн. Зарим оролцогчид байгууллагууд өөрсдийн хэрэгцээг бүрэн ойлгох хангалттай мэргэжлийн мэдлэггүй учраас чанар муутай үйлчилгээ авах эрсдэлтэй гэж үзэж байна.

Кибер аюулгүй байдлын үйлчилгээ үзүүлэгчдийг итгэмжлэх үндэсний байгууллага байхгүй. Иймм байгууллага байгуулах нь итгэмжлэл олгох замаар чанарыг баталгаажуулж, байгууллагуудыг зөв үйлчилгээ үзүүлэгчийг сонгоход туслах боломжтой.

Зарим байгууллагууд мэдээллийн технологийн үйлчилгээгээ аутсорсинг хийж байна. Мөн төрийн байгууллагуудын хувьд мэдээллийн системээ төрийн үүлэн технологид суурилсан үйлчилгээнд (government cloud) эсхүл ҮДТ-д байрлуулах ёстой гэсэн шаардлага байдаг. Харин зарим төрийн байгууллага болон бусад байгууллагууд ҮДТ-д байршуулах эсхүл гуравдагч талын үүлэн үйлчилгээ ашиглах боломжтой.

Аутсорсинг хийх үед эрсдэлийг тодорхойлж, удирдах чадвар нь байгууллагуудын хөгжлийн түвшнээс хамааран харилцан адилгүй байна. Монгол Улсын *Хүний хувийн мэдээлэл хамгаалах тухай хуульд* Монгол Улсын иргэдийн хувийн мэдээллийг улсын нутаг дэвсгэрт байршуулсан байх шаардлагатай гэж заасан. ҮДТ нь ЦХИХХЯ-тэй хамтран мэдээллийн ангиллын түвшин болон хаана хадгалах тухай бодлого боловсруулах төлөвлөгөөтэй гэж мэдээлэв.

Зарим байгууллагууд аутсорсингийн үйлчилгээний тасалдах эрсдлийг бууруулах зорилгоор бизнесийн тасралтгүй ажиллагааны төлөвлөгөөг боловсруулсан байна. Гэхдээ энэ нь байгууллагын кибер аюулгүй байдлын хөгжлийн түвшнээс хамаарч ялгаатай. ОЧМДБ байгууллагуудын хувьд *Кибер аюулгүй байдлын тухай хуульд* "мэдээллийн систем, дэд бүтцийн тасралтгүй, хэвийн ажиллагааг хангах, мөн эвдрэл, доголдлын үед сэргээх төлөвлөгөөтэй байх ёстой" гэж заасан учраас бизнесийн тасралтгүй үйл ажиллагааны төлөвлөгөөг боловсруулах шаардлага бий. КАБҮС-ийн хэрэгжилтийн явцыг үнэлэх нэг үзүүлэлт нь бизнесийн тасралтгүй ажиллагааны төлөвлөгөө хэрэгжүүлсэн байгууллагын тоо байх болно (дэлгэрэнгүйг D1.1-ээс харна уу).

Кибер даатгалын бүтээгдэхүүн Монголд бий болж эхэлж байна. Үндэсний төвийн вэбсайт дээр кибер даатгалын талаар танилцуулга болон зөв даатгалын бүтээгдэхүүн сонгох удирдамж байршуулсан байна.[86] Оролцогчид дотоодын компаниуд кибер даатгал санал болгож байгаа талаар мэдээлэлгүй байсан ч зарим олон улсын үйлчилгээ үзүүлэгчид Монголын компаниудад ийм бүтээгдэхүүн санал болгодог талаар дурдсан. Кибер даатгалын хэрэглээ анхан шатандаа явж байгаа бөгөөд төлөвшлийн үнэлгээний үеэр оролцогчдоос кибер даатгал ашиглаж байсан туршлагатай хүн байгаагүй гэж тэмдэглэжээ.

D 5.6 ХАРИУЦЛАГАТАЙГААР МЭДЭЭЛЭЛ ИЛ БОЛГОХ

Энэ хүчин зүйл нь салбарын хооронд эмзэг байдлын мэдээллийг хүлээн авах, түгээх хариуцлагатай ил тод мэдээлэлтэй холбоотой (responsible disclosure) тогтолцоог бий болгох, мөн уг тогтолцоог тасралтгүй хянаж, шинэчлэх хангалттай чадавх байгаа эсэхийг судалдаг.

[86] https://ncsirt.gov.mn/a/26

Түвшин: Эхлэл түвшнээс Хөгжиж буй түвшинд

Монгол Улсад зарим салбарт үйл ажиллагаа явуулж буй байгууллагууд хоорондоо аюул занал болон эмзэг байдлын мэдээлэл хуваалцах механизм бий. Санхүүгийн байгууллагууд Банкны мэдээлэл хуваалцах, дүн шинжилгээ хийх төв (ISAC)-аар дамжуулан аюул занал болон эмзэг байдлын мэдээллээ хуваалцдаг гэж мэдээлсэн. Санхүүгийн салбарын зарим байгууллагууд мөн олон улсын кибер аюул заналын мэдээллийн (CTI) эх сурвалжаас авч ашигладаг байна.

MNCERT/CC-ийн гишүүд, ихэвчлэн томоохон хувийн хэвшлийн байгууллагууд, мөн хоорондоо мэдээлэл солилцдог.

Мөн Монгол Улсад илүү олон байгууллага ашиглаж болох мэдээлэл хуваалцах механизмууд байх нь аюул занал болон эмзэг байдлын мэдээллийг солилцох үйл явцыг хөнгөвчлөх болно гэж үзэж байна. Энэ нь Кибер аюулгүй байдлын үндэсний стратегийн 5-р зорилттой нийцэж байгаа бөгөөд тус стратегид “Кибер халдлага, зөрчлийн мэдээлэл солилцох үндсэн дэд бүтцийг хөгжүүлэх” зорилтыг багтаасан.

Хэрэгжүүлэх арга нь салбар бүрт суурилсан мэдээлэл хуваалцах механизм эсхүл илүү өргөн хүрээнд ашиглах боломжтой систем байж болох. Зарим оролцогчид кибер аюулгүй байдлын мэдээллийг бусад байгууллагуудтай хуваалцахад болгоомжлол, хойрго хандлага байдаг гэж онцолж, мэдээлэл солилцооны ач холбогдлыг нэмэгдүүлэх санаачилга хэрэгжүүлэх нь үр дүнтэй байж болохыг тэмдэглэв.

Монгол Улсад ёс зүйтэй халдлага хийх соёл болон эмзэг байдлын мэдээлэл ил болгох (vulnerability disclosure) систем тодорхой хэмжээгээр хөгжиж байгаа. Зарим цоорхой илрүүлэх (Bug Bounty) хөтөлбөрүүд амжилттай зохион байгуулагдсан байна. MNCERT/CC нь Монголын банкны холбоотой хамтран уг хөтөлбөрийг хэрхэн хэрэгжүүлэх талаар санхүүгийн байгууллагад мэдлэг олгох арга хэмжээнүүд зохион байгуулжээ.

Мөн жил бүр зохион байгуулагддаг Харуул занги кибер аюулгүй байдлын ёс зүйт хакерын тэмцээн нь зарим компанид судлаачдыг өөрсдийн систем дэх эмзэг байдлыг хайж олоход урьж оролцуулах сэдэл өгсөн гэж мэдэгдсэн.

Зарим байгууллагууд эмзэг байдлын мэдээлэл хариуцлагатайгаар ил болгох бодлоготой бөгөөд энэ нь программ хангамж, вэбсайтад эмзэг байдал илэрсэн тохиолдолд ямар процесс дагаж мөрдөх, мэдээлэл хэзээ ил болох, хэрхэн шийдвэрлэх хуваарьтай байх зэргийг тусгасан байдаг. Гэсэн хэдий ч энэ нь байгууллагын соёл, хөгжлийн түвшнээс хамааралтай бөгөөд ихэвчлэн хувийн санхүүгийн байгууллагууд дээр ажиглагдаж байна. Одоогийн байдлаар эмзэг байдлын мэдээллийг хариуцлагатай ил болгох тогтвортой механизм байхгүй байгаа нь төрийн болон хувийн хэвшлийн байгууллагуудад аюулгүй байдлын асуудлуудыг үр дүнтэй тайлагнах, засварлахад хүндрэл учруулж байна.

Монгол Улсад эмзэг байдлын мэдээллийг хариуцлагатайгаар ил болгож буй судлаачдыг хамгаалах хууль эрх зүйн зохицуулалт байхгүй. Ёс зүйт хакерын олон нийтийн бүлгүүдийн зарим оролцогчид байгууллагуудад эмзэг байдлын мэдээлэл хүргэхээс эмээдэг, учир нь үр дагавраас (хуулийн хариуцлага хүлээх, буруутгагдах) болгоомжилж байгаа гэж мэдээлсэн. Үүнийг харгалзан, Монгол Улсын нөхцөл байдалд тохирсон судлаачдыг хамгаалах механизм боловсруулах нь үр өгөөжтэй гэж үзэж байна.

Гэхдээ оролцогчид хакерууд вэбсайтыг унагаж, засахын тулд төлбөр шаардах тохиолдол гарч байгааг мэдээлсэн бөгөөд энэ төрлийн гэмт хэрэг болон хариуцлагатай ил тод мэдээлэл өгч буй хүмүүст хамгаалалт үзүүлэх зорилготой хууль тогтоомжийн хооронд ялгааг тодорхой болгох шаардлагатайг тэмдэглэсэн.

ЗӨВЛӨМЖ

Кибер аюулгүй байдлын стандарт, технологийн хөгжлийн үнэлгээний дагуу Монгол Улсад дараах зөвлөмжийг өгч байна. Эдгээр зөвлөмжүүд нь GCSCC-ийн Кибер Аюулгүй Байдлын Чадавхын Үнэлгээний Загвар-ын дагуу одоо байгаа чадавхыг сайжруулах зөвлөмж, хэрэгжүүлэх алхмуудыг агуулна.

СТАНДАРТ ДАГАЖ МӨРДӨХ

R5.1.1 Үндэсний хэмжээнд зөвшөөрөгдсөн суурь стандарт нь дараах чиглэлүүдийг багтаахаар өргөжүүлэх:

- Кибер аюулгүй байдлын стандарт болон худалдан авах үйл явцыг удирдах сайн туршлага (эрсдэлийн удирдлага, амьдралын мөчлөгийн удирдлага, програм хангамж, техник хангамжийн баталгаажуулалт, аутсорсинг, үүлэн технологид суурилсан үйлчилгээний ашиглалт зэрэг багтана);
- Бүтээгдэхүүн, үйлчилгээ үзүүлэхэд зориулсан кибер аюулгүй байдлын стандартыг боловсруулах (програм хангамж хөгжүүлэлт, техник хангамжийн чанарын баталгаажуулалт, удирдлагатай үйлчилгээ үзүүлэх болон үүлэн аюулгүй байдал гэх мэт).

R5.1.2 Олон улсын стандартыг шинэчлэгдсэн хөгжлийн чиг хандлагатай уялдуулан, одоо хүчин төгөлдөр мөрдөгдөж буй үндэсний хэмжээнд батлагдсан, нутагшуулсан кибер аюулгүй байдлын стандартыг шинэчлэх шаардлагатай эсэхийг судлах.

R5.1.3 Жижиг, дунд байгууллагад санхүү болон хүний нөөцийн хязгаарлагдмал байдалд тохируулан суурь түвшний кибер аюулгүй байдлын хяналтуудыг хэрэгжүүлэх талаар зөвлөмж гаргах. Их Британийн “Cyber Essentials” схемийг жишээ болгон авч үзэж болно.

R5.1.4 Төрийн болон хувийн хэвшлийн байгууллагуудын кибер аюулгүй байдлын стандартуудын хэрэглээг хэмжих үүргийг тодорхой нэг байгууллагад хариуцуулах. Энэ нь ялангуяа шинэ зохицуулалтад хамрагдахгүй байгаа ОЧМДБ болон төрийн бус байгууллагуудад хамааралтай. Эрдэм шинжилгээний байгууллагууд болон судалгааны хүрээлэнгүүдтэй хамтран ажиллах нь хяналт, дүн шинжилгээнд үр өгөөжтэй байх болно.

R5.1.5 Монгол Улсын байгууллагуудад кибер аюулгүй байдлын стандартуудыг хэрэгжүүлэх, худалдан авалтын стандарт болон бүтээгдэхүүн, үйлчилгээний стандартыг нэвтрүүлэхийг дэмжих төрийн хөтөлбөрүүдийг бий болгох. R5.1.4-ийн хүрээнд гарсан судалгааны үр дүнд үндэслэн, стандарт нэвтрүүлэлт бага түвшинд үнэлэгдсэн байгууллагуудын дунд мэдлэгийг нэмэгдүүлэх.

R5.1.6 Төрийн худалдан авах ажиллагааны хууль тогтоомж нь аюулгүй бүтээгдэхүүн худалдан авах, холбогдох стандартуудтай зөрчилдөж байгаа эсэхийг судлах, хэрэв зөрчил байвал шийдвэрлэх арга хэмжээ авах.

R5.1.7 ОЧМДБ байгууллагын программ хангамж, техник хангамжийн кибер аюулгүй байдлыг шалгах шинэ лаборатори нь технологийн худалдан авалтад тогтмол, шуурхай аюулгүй байдлын үнэлгээ хийх чадамж, механизмаар хангах.

АЮУЛГҮЙ БАЙДЛЫН ХЯНАЛТУУД

R5.2.1 Монгол Улсын төрийн болон хувийн хэвшлийн байгууллагуудад кибер аюулгүй байдлын стандартын хэрэглээг нэмэгдүүлэх, ингэснээр байгууллагын ашиглаж буй технологийн болон криптографийн аюулгүй байдлын хяналтын багцууд нь тогтсон кибер аюулгүй байдлын хүрээ, стандартад болон шилдэг туршлагуудтай нийцэх боломжийг хангах.

R5.2.2 Сангийн яамны зүгээс төрийн байгууллагуудын аюулгүй байдлын хяналтуудыг хэрэгжүүлэхэд шаардлагатай төсөв хангалттай хуваарилах механизмыг боловсруулах. Үүний хүрээнд байгууллагууд кибер аюулгүй байдлын санхүүжилт хүсэх боломжтой тусгай ангилал үүсгэх саналыг судлах.

R5.2.3 Монгол Улсад байгууллагад аюулгүй байдлын хяналтыг үр дүнтэй хэрэгжүүлсэн амжилттай кейсүүдийг тодорхойлох судалгааг хийх. Эдгээр кейсийг аюулгүй байдлын хяналтын ач холбогдлыг харуулах сургалт, ухуулга сурталчилгаанд ашиглах.

R5.2.4 Байгууллагын удирдлагуудын кибер аюулгүй байдлын талаарх мэдлэгийг нэмэгдүүлэх санаачилгыг хэрэгжүүлэх, ингэснээр тэдгээр байгууллагууд кибер аюулгүй байдлыг санхүүжилтийн хувьд илүү тэргүүлэх ач холбогдолтой гэж үзэх хандлагыг төлөвшүүлэх.

R5.2.5 Төрийн албан хаагчдын мэдээлэл солилцооны аюулгүй байдлыг сайжруулах, нийгмийн сүлжээгээр эмзэг, чухал мэдээлэл солилцохоос урьдчилан сэргийлэх боломжуудыг судлах. Үүнд дараах арга хэмжээг авч үзэж болно:

- Төрийн байгууллагын хооронд нийгмийн сүлжээг мэдээлэл дамжуулахад ашиглахыг хориглосон нэгдсэн бодлого боловсруулах (зарим байгууллагууд ийм бодлоготой ч, нийт төрийн түвшинд стандартчилагдаагүй байна);
- Төрийн албан хаагчдад зориулсан аюулгүй, хяналттай харилцааны платформ хөгжүүлэх;
- Төрийн байгууллагын хооронд мэдээлэл солилцох криптографийн шаардлагыг стандартчилах, мөн хувийн хэвшлийн байгууллагуудтай мэдээлэл солилцохдоо мөрдөх аюулгүй байдлын стандартыг боловсруулах.

R5.2.6 Төрийн албан хаагчид кибер аюулгүй байдлын мэдлэг, шилдэг туршлагуудыг хуваалцах боломж бүхий платформ эсхүл бага хурлууд зохион байгуулах.

R5.2.7 Монгол Улсад цахим гэрчилгээний хэрэглээг нэмэгдүүлэх арга хэмжээг авч үзэх. Үүнд олон нийтийн мэдлэгийг нэмэгдүүлэх компанит ажил явуулах зэргийг судлах.

R5.3.1 Программ хангамжийн аюулгүй байдал, дутагдлын нотолгоог цуглуулах, мөн программ хангамжийн найдвартай байдал, хэрэглээний хялбар байдал, гүйцэтгэл, аюулгүй байдлыг олон улсын стандарт болон шилдэг туршлагад нийцүүлэн үнэлэх үүрэг бүхий байгууллагыг тодорхойлох. Үүний хүрээнд олон улсын байгууллагуудтай хамтран ажиллаж, шилдэг туршлагуудыг судлах, одоогийн чадавхыг олон улсын түвшинд харьцуулж үнэлэх боломжийг судлах.

R5.3.2 R5.3.4-өөс гарсан мэдээллийг ашиглан бүх байгууллагад зориулсан, аюулгүй, найдвартай программ хангамжийн платформууд болон программуудыг таних гарын авлага боловсруулах. Энэ нь:

- Баталгаажсан программ хангамжийн каталог хэлбэрээр байж болно, эсхүл
- Программ хангамжийн чанар, үйл ажиллагаа болон аюулгүй байдлын шаардлагыг үнэлэх аргачлалын талаарх зааварчилгаа байж болно.

R5.3.3 Бүх байгууллагад зориулсан программ хангамжийн шинэчлэл болон засвар үйлчилгээний гарын авлага гаргах (үүнд “patch management” багтана).

R5.3.4 Байгууллагуудад программ хангамжийн аюулгүй байдлыг хэмжих, программ хангамжийн засвар үйлчилгээний бодлогыг хэрэгжүүлэх тогтолцоог хөгжүүлэх (жишээлбэл, статистик мэдээлэл цуглуулах, дүн шинжилгээ хийх гэх мэт).

R5.3.5 Төрийн байгууллагын програм хангамж худалдан авахтай холбоотой асуудлын (лицензгүй программ хангамжийн хэрэглээ гэх мэт) шалтгааныг тодорхойлох, эдгээр асуудлыг хэрхэн шийдвэрлэх боломжтойг судлах зорилгоор судалгаа эсхүл хэлэлцүүлэг зохион байгуулах.

R5.3.6 Дотоодын программ хангамжийн аюулгүй байдлыг судлах, мөн дотоодын програм хангамж болон гадаадаас худалдан авсан програм хангамжийн чанарын зөрүүг ялгааг арилгах арга хэмжээг тодорхойлох судалгаа, хэлэлцүүлэг зохион байгуулах. Үүнд:

- Дотоодын программ хангамжийн хөгжүүлэлтийн практикийг сайжруулахад төрөөс дэмжлэг үзүүлэх эсхүл урамшууллын систем бий болгох боломжийг судлах.

ХАРИЛЦАА ХОЛБОО БОЛОН ИНТЕРНЕТИЙН ДЭД БҮТЦИЙН ТОГТВОРТОЙ БАЙДАЛ

R5.4.1 Кибер аюулгүй байдлын тухай хуулийн шаардлагуудын хэрэгжилтийг хянах, ялангуяа ОЧМДБ хамаарах ISP-үүдийн үйл ажиллагааг хянаж, эдгээр байгууллагууд кибер аюулгүй байдлын зөрчлийг бууруулах, хариу арга хэмжээ авах хяналтуудыг хангалттай түвшинд хэрэгжүүлж чадаж байгаа эсэхийг баталгаажуулах.

R5.4.2 Жижиг ISP-дийн кибер аюулгүй байдлын практикийг сайжруулахад хэрхэн дэмжлэг үзүүлэх талаар судлах. Үүнд шилдэг туршлагуудыг хуваалцах, сургалт явуулах, техникийн дэмжлэг үзүүлэх зэрэг аргуудыг авч үзэх.

R5.4.2 Монгол Улсад цахим худалдаа, цахим бизнесийн гүйлгээ хийхэд интернет үйлчилгээний найдвартай байдалд итгэх итгэлийг хэмжих механизмуудыг (жишээ нь, судалгаа явуулах) бий болгох.

- Цуглуулсан өгөгдлийг ашиглан асуудлуудыг тодорхойлж, шийдвэрлэх.
- Хэмжигдэхүүний үр дүнг тогтмол нийтэлж, ил тод байдал болон хариуцлагыг дэмжих.

КИБЕР АЮУЛГҮЙ БАЙДЛЫН ЗАХ ЗЭЭЛ

R5.5.1 Олон улсын кибер аюулгүй байдлын технологид хэт найдах нь аюулгүй байдлын ямар эрсдэл дагуулж болох талаар хэлэлцэх зорилгоор холбогдох талуудыг хамруулсан уулзалт зохион байгуулах. Болзошгүй эрсдэлийг бууруулах шаардлагатай арга хэмжээ байгаа эсэхийг судлах.

R5.5.2 Гадны технологид найдсанаар үүсэж болох аюулгүй байдлын эрсдэлийг тодорхойлох, удирдах талаар Монголын байгууллагад зориулсан удирдамж гаргаж, сурталчлах.

R5.5.3 Дотоодын кибер аюулгүй байдлын технологийн зах зээлийг хөгжүүлэхэд олон улсын стандартад нийцсэн аюулгүй хөгжүүлэлтийн процесс нэвтрүүлэхийг дэмжих. Аюулгүй хөгжүүлэлтийн практикийг хэрхэн урамшуулж, дэмжих талаар авч үзэх хэрэгтэй.

R5.5.4 Монгол Улсад кибер аюулгүй байдлын үйлчилгээ үзүүлэгчдийн эрэлт, нийлүүлэлтийг судалж, хангаж байгаа эсэхийг үнэлэх.

R5.5.5 Кибер аюулгүй байдлын үйлчилгээ үзүүлэгчдийг итгэмжлэх үүрэгтэй байгууллага томилох.

R5.5.6 Кибер аюулгүй байдлын үйлчилгээ үзүүлэгчийг хэрхэн сонгох талаар байгууллагуудад зориулсан удирдамж гаргах. Ялангуяа ОЧМДБ-д хамаарахгүй байгууллагуудад энэ нь чухал ач холбогдолтой.

R5.5.7 Гуравдагч талын үйлчилгээ үзүүлэгчээс аутсорсинг үйлчилгээ авахдаа кибер аюулгүй байдлын эрсдэлийг хэрхэн удирдах талаар байгууллагад зориулсан удирдамж эсхүл сургалт явуулах.

R5.5.8 Монгол Улс дахь байгууллагуудын кибер даатгалын хэрэгцээг тодорхойлох зорилгоор төр болон хувийн хэвшлийн санхүүгийн эрсдэлийг үнэлэх, зөвлөлдөх уулзалт зохион байгуулах. Мөн даатгалын бүтээгдэхүүн хөгжүүлэхэд тулгарч буй бэрхшээлийг судлах. Судалгааны үр дүнг ашиглан кибер даатгалын зах зээлийг хөгжүүлэх арга хэмжээг тодорхойлох, дэмжих.

ХАРИУЦЛАГАТАЙ МЭДЭЭЛЭЛ ИЛ БОЛГОХ

R5.6.1 Төр болон хувийн хэвшлийн байгууллагын дунд эмзэг байдлыг хариуцлагатайгаар ил болгох (responsible disclosure)-ын ач холбогдлын талаар ойлголт нэмэгдүүлэх санаачилгуудыг хэрэгжүүлэх (мөн энэ нь жинхэнэ халдлага, дарамтаас хэрхэн ялгаатай болохыг ойлгуулах).

R5.6.2 Монголд илүү олон байгууллагуудыг хамруулсан эмзэг байдлыг хариуцлагатай ил болгох бодлого, суваг, шийдэл боловсруулах, болон цоорхой илрүүлэх (bug-bounty) хөтөлбөрийг хөгжүүлэхийг дэмжих. Үүнийг R5.6.1-д заасан мэдлэг олгох үйл ажиллагаагаар дэмжих.

R5.6.3 Эмзэг байдлыг хариуцлагатайгаар илрүүлж, мэдээлсэн этгээдийг хамгаалах, мөн эмзэг байдлыг илрүүлж мэдээлэх нь ямар нөхцөлд гэмт хэрэгт тооцогдох эсэхийг тодорхой заасан хууль тогтоомжийг боловсруулахаар анхаарч үзэх шаардлагатай. Үүнийг боловсруулахдаа Кибер аюулгүй байдлын дэлхийн форум (GFCE)-ын “Эмзэг байдлыг зохион байгуулалттай илрүүлж мэдээлэх тухай сайн туршлагын баримт бичиг”-ийг ашиглах боломжтой. Мөн уг хууль тогтоомжийн хэрэгжих боломж, бодит үр нөлөөг хангах үүднээс ёс зүйн хакеруудын нийгэмлэгтэй хамтран туршиж үзэх нь зүйтэй.

R5.6.4 Монгол Улсад илүү олон байгууллагыг хамарсан аюул занал болон эмзэг байдлын мэдээлэл солилцох механизм хөгжүүлэх.

R5.6.5 Байгууллагуудын мэдээлэл солилцох механизмыг ашиглах идэвхийг нэмэгдүүлэхийн тулд мэдээлэл солилцооны үр ашиг, ач холбогдлын талаарх ойлголтыг нэмэгдүүлэх санаачилгууд хэрэгтэй эсэхийг авч үзэх. Ийм төрлийн сурталчилгааг үр дүнтэй болгохын тулд байгууллагуудын мэдээлэл хуваалцахаас татгалзах шалтгаан, саад бэрхшээлийг судалсан судалгаанд тулгуурлах шаардлагатай. Мөн мэдээлэл солилцооны талаарх мэдлэгийг нэмэгдүүлэх үйл ажиллагааг салбар бүрд тохируулан хэрэгжүүлснээр тухайн салбарын мэдээлэл солилцооны механизмуудад байгууллагуудын оролцоог нэмэгдүүлэх боломжтой.

НЭМЭЛТЭЭР АНХААРАХ ЗҮЙЛС

Оролцогч талуудын оролцоо сайн байсан бөгөөд оролцогч талуудын төлөөлөл, бүрэлдэхүүн ерөнхийдөө тэнцвэртэй, өргөн хүрээтэй байв. Энэ нь үнэлгээний багт төвөлшлийн үнэлгээг гүйцэтгэх, дэмжих хангалттай нотолгоо цуглуулах боломжийг олгосон.

ХАВСРАЛТ

СУДАЛГААНЫ АРГА ЗҮЙ – ТҮВШНИЙГ ХЭМЖИХ НЬ

Төлөвшлийн үнэлгээг гүйцэтгэхдээ оролцогч талуудтай тус улсад хэлэлцүүлэг уулзалт хийх(ихэвчлэн гурван өдрийн хугацаанд), зайнаас баримт бичигт тулгуурласан судалгаа явуулах байдлаар мэдээлэл цуглуулдаг. Энэ нь тухайн улсын засгийн газрын төлөөлөгчдөд хүлээлгэн өгөх нотолгоонд суурилсан тайлан боловсруулах зорилготой. Тайлан нь дараах зөвлөмжүүдийг агуулна:

- Улс орны кибер аюулгүй байдлын чадавхийн төлөвшлийн түвшнийг үнэлэх;
- Кибер аюулгүй байдлын чадавхыг хөгжүүлэхэд хувь нэмэр оруулах бодитой үйл ажиллагааны нарийвчилсан төлөвлөгөө гаргах;
- Төлөвшлийн түвшний зөрүүг тодорхойлох;
- Хөрөнгө оруулалт болон ирээдүйн чадавх хөгжүүлэх тэргүүлэх чиглэлийг тогтоох.

Тухайлсан хэмжээсийн үзүүлэлтийг холбогдох оролцогч талын бүлгүүдтэй хэлэлцэнэ. Оролцогч талын бүлэг бүр төлөвшлийн үнэлгээний нэг эсхүл хоёр хэмжээсний хүрээнд өөрсдийн мэргэшсэн чиглэлээр хариулт өгнө. Жишээлбэл, Академик хүрээлэл, Иргэний нийгмийн байгууллагууд, Интернэт засаглалын бүлгүүд уг үнэлгээний 2-р хэмжээс “Кибер аюулгүй байдлын соёл болон нийгэм” болон 3-р хэмжээс “Кибер аюулгүй байдлын мэдлэг болон чадавх бүрдүүлэх” талаар хэлэлцүүлэгт оролцох болно.

Мэдээлэл цуглуулалт

Үнэлгээний баг дараах аргаар төлөвшлийн түвшнийг тогтоох нотолгоо цуглуулна:

- Бичиг баримтад тулгуурласан судалгаа
- Дэлгэрэнгүй хэлэлцүүлэг, ярилцлага
- Голлох бүлгийн хэлэлцүүлэг

Үүний тулд Загварчилсан Талбарын Кодчлолын (SFC) хэрэгсэл ашиглаж үр дүнг баримтжуулна[87]. Үнэлгээний багийн үүрэг нь хэлэлцүүлгийг удирдан чиглүүлэх, тэмдэглэл хөтлөх явдал юм[88].

---

[87] Williams, M. (2003). Questionnaire design. In *Making sense of social research* (pp. 104-123). SAGE Publications,
Ltd, https://www.doi.org/10.4135/9781849209434; Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. (Ed.), *Successful focus groups: Advancing the state of the art* (pp. 35-50). SAGE Publications, Inc., https://www.doi.org/10.4135/9781483349008; Richard A. Krueger, R. A., & Mary
Anne Casey, M. A., (2009) Focus-groups: A Practical Guide for Applied Research. SAGE Publications, London.

[88] Kitzinger, J. (1994). The methodology of focus groups: the importance of interaction between research participants. Sociology of health & illness, 16(1), 103-121. https://doi.org/10.1111/1467-9566.ep11347023 Kitzinger, J. (1995). Qualitative research: introducing focus groups. Bmj, 311(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299; Fern, E. F. (1982). The use of Focus Groups for Idea Generation: The Effects of Group Size, Acquaintanceship, and Moderator on Response Quantity and Quality. Journal of Marketing Research, 19(1), 1–13. https://doi.org/10.1177/002224378201900101

Төлөвшлийн үнэлгээ нь голлох бүлгийн хэлэлцүүлгийн арга зүйг ашигладаг бөгөөд энэ нь дэлгэрэнгүй ярилцлага, бичиг баримтад тулгуурласан судалгааг баталгаажуулж, нэмэлт мэдээлэл олж авахад чиглэдэг[89]. Бүлгийн хэлэлцүүлгийн давуу тал нь оролцогчид харилцан ярилцах явцад тал бүрийн үзэл бодол, ойлголтууд гарч ирэх боломжтой байдаг. Тодорхой оролцогчдод асуулт тавихын оронд судлаач оролцогчдын хооронд хэлэлцүүлгийг удирдан явуулж, тэднийг өөр өөр үзэл бодлыг хүлээн авах, хамгаалах эсхүл тайлбарлах боломжийг олгодог. Энэ арга нь бусад аргуудтай харьцуулахад илүү үр дүнтэй бөгөөд оролцогчдын дунд харилцан ойлголцолд хүрэх, кибер аюулгүй байдлын практик, чадамжийг дээшлүүлэх боломжийг бүрдүүлдэг.

Кибер аюулгүй байдлын чадавхын төлөвшлийн түвшинг тодорхойлохын тулд тухайн бүрэлдэхүүн бүр нь төлөвшлийн таван шатад харгалзах үзүүлэлтийн багцтай байна. Хэлэлцүүлэг нь хамтын зөвшилцлийн аргаар явагдах бөгөөд оролцогч талууд тухайн улс хэр олон үзүүлэлтийг хэрэгжүүлсэн талаар нотолгоо гаргаж, төлөвшлийн түвшнийг тогтооно. Голлох бүлгийн хэлэлцүүлгийн үеэр судлаачид хэлэлцүүлгийг холбогдох үзүүлэлтүүдийн хүрээнд чиглүүлэхийн тулд хагас бүтэцлэгдсэн асуулт ашигладаг. Оролцогч талуудын хэлэлцүүлгээр үзүүлэлтүүдийн хэрэгжилтийн талаарх нотолгоог бүрдүүлдэг. Хэрэв тодорхой түвшний бүх үзүүлэлтэд нотолгоо байхгүй бол тухайн улс тэрхүү төлөвшлийн түвшинд хараахан хүрээгүй гэж үзнэ.

Оролцогч талуудын хооронд зөрүүтэй ойлголт гарах нь зайлшгүй. Мөн нэг салбарын оролцогчийн мэдэж буй мэдээлэл нь бусад салбарын хувьд танил бус байх тохиолдол бий. Иймд эдгээр мэдээллийн зөрүүг Хяналтын баг (Review Team) илрүүлж, нарийвчлан судлах үүрэгтэй.

Судалгаа болон өөрчлөн зохион байгуулсан голлох бүлгийн хэлэлцүүлгүүд нь зайлшгүй зарим нэмэлт асуулт болон зөрүүтэй мэдээллийг үүсгэдэг. Иймээс чухал, зарим тохиолдолд онцгой тохиолдлыг илүү гүнзгий ойлгохын тулд судалгааны үеэр эсхүл дараа нь дэлгэрэнгүй ярилцлагууд ч мөн давхар зохион байгуулдаг.

Мэдээллийн дүн шинжилгээ

Оролцогчдын урьдчилсан зөвшөөрлийн дагуу бүх хуралдаанууды бичлэг хийдэг. Хувь хүний хариултыг нууцлалтайгаар авч үзэх болон үр дүнг тайлагнахдаа Chatham House дүрмийг мөрдөнө[90]. Улс орны үнэлгээг хийсний дараа оролцогч талуудтай хийсэн уулзалтын үеэр цуглуулсан мэдээлэл болон хуралдааны үеэр тэмдэглэсэн тэмдэглэлүүдийг ашиглан нотолгоо олж тогтоох, үнэлгээний бүрэлдэхүүн хэсэг тус бүрийн төлөвшлийн түвшинг тодорхойлох үйл явц явагдана. Үнэлгээний тайланд энэхүү мэдээллийг нэгтгэн тус бүрийн чадавхын түвшнийг үнэлж, тухайн улсын кибер аюулгүй байдлын чадавхыг тодорхойлдог. Аль ч тохиолдолд үнэлгээний баг тодорхой нэг эх сурвалжийг давуу эрхтэй гэж үзэхгүй бөгөөд загварын үзүүлэлт тус бүрийн хамгийн бодит төлөв байдлын талаар зөвшилцөлд хүрэхийг эрмэлздэг.

[89] Kitzinger, J. (1995). Qualitative research: introducing focus groups. *Bmj*, *311*(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299

[90] https://www.chathamhouse.org/about/chatham-house-rule

Зөвлөмж боловсруулах

Хэмжээс тус бүрт тухайн улсын кибер аюулгүй байдлын чадавхыг сайжруулахын тулд дараагийн алхмуудыг тусгасан зөвлөмжийг боловсруулна. Хэрэв тухайн улсын тодорхой нэг хэмжээс төлөвшлийн эхний шатанд байгаа бол үнэлгээний загварт заагдсан үзүүлэлтүүдийг ашиглан дараагийн шатанд шилжих арга хэмжээг тодорхойлох боломжтой. Зөвлөмжүүд нь төлөвшлийн үнэлгээний дагуу одоогийн кибер аюулгүй байдлын чадамжийг нэмэгдүүлэхэд чиглэсэн алхмуудыг агуулдаг. Эдгээр зөвлөмжүүд нь тус бүрийн хүчин зүйлд тухайлан зориулсан байдаг.

Үнэлгээнд техникийн зөвлөлийн хяналт хийсний дараа урьдчилсан тайланг дотоод зохион байгуулагч (Local Host)-д хүргүүлж, тэдний саналыг авна. Хэрэв шинэ нотолгоо гарч ирвэл тайланг дахин хянаж, үнэлгээний бүрэлдэхүүн хэсэг болон хүчин зүйлийн төлөвшлийн түвшинг шинэчлэн тогтооно. Бүх талууд урьдчилсан тайланд зөвшөөрөл өгсний дараа дотоод зохион байгуулагч нь тайлангийн нийтлэлийн үйл явцыг хариуцна. Тайлан нийтлэх зөвшөөрөл тухайн улс орны төрийн эрх мэдэлд байдаг бөгөөд хэрэв нийтлэхийг зөвшөөрвөл албан ёсны төрийн байгууллагын вэбсайт эсхүл бусад сувгаар олон нийтэд түгээх нь зохистой юм.

Мэдээллийн менежмент болон ёс зүйн асуудал

Бүлгийн хэлэлцүүлгүүд тухайн улсын сонгосон платформын дагуу Microsoft Teams™ болон Zoom™-ээр онлайнаар явагдана. Өгөгдөл болон цуглуулсан мэдээллийн нууцлалыг хангах үүднээс гадны бичигч төхөөрөмжүүдээр бичлэг хийнэ. Энэхүү бичлэгүүд нь нэргүй, нууцлалтай хэвээр үлдэнэ.
Баримт бичгийн судалгаа, нарийвчилсан, дэлгэрэнгүй ярилцлага, бүлгийн хэлэлцүүлгээс гарсан үр дүнг дүн шинжилгээнд нэгтгэнэ.

Дэлхийн Кибер Аюулгүй Байдлын Чадавхын Төв (Global Cyber Security Capacity Centre)
Компьютерын ухааны тэнхим,
Оксфордын Их Сургууль,
Вольфсон Барилга, Оксфорд OX1 3QD,
Их Британи

Tel: +44 (0)1865 287434

Email: cybercapacity@cs.ox.ac.uk

Websites: https://gcscc.ox.ac.uk/home-page#/ www.oxfordmartin.ox.ac.uk/cyber-security