

МОНГОЛ УЛСАД ҮЙЛДЭГДЭЖ БУЙ ШИНЭ ТӨРЛИЙН ГЭМТ ХЭРЭГ:
КИБЕР ГЭМТ ХЭРЭГ, ОНЛАЙН ЗАЛИЛАН
"NEW TYPES OF CRIMES COMMITTED IN MONGOLIA:
CYBERCRIME, ONLINE FRAUD"

Б.Ганболд,
Дотоод Хэргийн Их Сургуулийн Цагдаагийн
сургуулийн Гүйцэтгэх ажлын тэнхимийн
ахлах багш, цагдаагийн ахмад

B. Ganbold,
senior lecturer of the Department of Criminal
intelligence at the Police School of the University
of Internal Affairs, police captain

Хураангуй: Монгол Улс, газар зүйн байршил, тусгаар тогтнол, эдийн засгийн хувьд дэлхий дахинд буй байр сууриа бэхжүүлсээр байгаа ч, кибер гэмт хэрэгтэй тэмцэх асуудал дээр бусад орноос доогуур байгаа нь хууль эрх зүйн орчин, олон улсын хамтын ажиллагаа, дэд бүтэц, мэргэшсэн боловсон хүчинтэй болох хэрэгцээ шаардлага улам бүр чухал болж байна гэдгийн харуулсаар байна.

Abstract: Mongolia, while strengthening its position in terms of geographical location, sovereignty, and economy globally, still lags behind other countries in tackling cybercrime. This highlights the increasing need for improvements in the legal framework, international cooperation, infrastructure, and the development of skilled human resources to effectively combat cybercrime.

Түлхүүр үгс: Кибер гэмт хэрэг, фишинг / хуурамч цахим сайт, төлбөрийн хэрэгсэл ашиглан хувь хүний нэвтрэх нэр, нууц үгийг хулгайлахад чиглэсэн хортой программ/, мэдээллийн аюулгүй байдал

Keywords: "Cybercrime, phishing (using fake websites and payment tools to steal personal login credentials and passwords), information security."

Оршил: Дижитал эрин үед кибер гэмт хэрэг нь дэлхийг даяар хувь хүн, бизнес, засгийн газар зэрэг бүх салбаруудад нөлөөлж, томоохон сорилтыг хүн төрөлхтний өмнө бий болгоод байна. Монгол Улс, газар зүйн байршил, тусгаар тогтнол, эдийн засгийн хувьд дэлхий дахинд буй байр сууриа улам бүр бэхжүүлсээр байгаа болов ч, кибер гэмт хэрэгтэй тэмцэх асуудал дээр бусад улс орноос доогуур байгаа нь хууль эрх зүйн орчин, олон улсын хамтын ажиллагаа, дэд бүтэц, мэргэшсэн боловсон хүчинтэй болох хэрэгцээ шаардлага улам бүр чухал болж байна гэдгийн харуулсаар байна.

Монгол Улс мэдээллийн технологи, интернэтийн хэрэглээг өргөнөөр нэвтрүүлж байгаатай холбогдуулан кибер гэмт хэргийн төрөл, гаралт ихсэж үйлдлийн арга улам нарийсаж байна. Энэ нийтлэлд Монгол улсад кибер гэмт хэрэг ямар байдлаар илэрч буй, үүний шалтгаан, нийгэмд үзүүлэх нөлөө, мөн энэ асуудлыг шийдвэрлэх чиглэлээр хийж буй оролдлогуудыг товчхон авч судлахыг хичээлээ.

Монгол Улс дахь кибер гэмт хэргийн нөхцөл байдал:

Кибер гэмт хэрэг нь интернет болон бусад дижитал харилцааны хэрэгслүүдийг ашиглан үйлдэгддэг шинэ төрлийн гэмт хэрэг юм. Эдгээр гэмт хэргүүд нь онлайн залилан, хувийн мэдээллийн хулгай, санхүүгийн залилан, кибер хүчирхийлэл, харилцаа холбооны сүлжээнд хууль бусаар нэвтрэх буюу хакердах, вирус тараах зэрэг олон төрлийн үйлдлүүдийг хамардаг.

Манай улсад хамгийн түгээмэл тохиолдож буй кибер гэмт хэрэг нь санхүүгийн залилан, фишинг халдлага болон харилцаа холбооны сүлжээнд хууль бусаар халдах зэрэг үйлдлүүд байна.

Онлайн санхүүгийн залилан, энэ төрлийн гэмт хэрэг нь хуурамч вэбсайтууд болон фишинг имэйлүүд ашиглан хувь хүний мэдээллийг хулгайлдаг. Мөн дараагийн түгээмэл үйлдэгддэг кибер гэмт хэрэг бол хувийн болон төрийн байгууллагууд руу чиглэсэн халдлагууд юм. Монгол улсад интернетийн хэрэглээ өргөжиж, илүү олон хүн онлайн үйлчилгээ ашиглаж эхэлсэнтэй зэрэгцэн кибер гэмт хэрэгтнүүд улам нарийн, илүү өндөр технологи ашиглан халдаж гэмт хэрэг үйлдсэн хэвээр байна.

Онлайн Залилах болон Санхүүгийн Залилангийн гэмт хэрэг:

Онлайн залилах болон санхүүгийн залилан гэдэг нь дижитал платформуудыг ашиглан хуурамч мэдээлэл өгч, хувь хүмүүсийн мөнгө болон хувийн мэдээллийг хулгайлах гэмт хэргийг хэлдэг. Монгол улсад энэ төрлийн гэмт хэрэг нь интернетийн хэрэглээ нэмэгдэхийн хэрээр өсч байгаа олон гэмт хэргийн нэг төрөл юм. Сошиал медиа платформууд, цахим худалдааны вебсайтууд болон онлайн төлбөрийн системүүд нь гэмт хэрэгтнүүдэд иргэдийг онилон, судлан, залилах таатай орчныг бүрдүүлж өгч байна.

Монгол улсад хамгийн түгээмэл тохиолддог онлайн залилах гэмт хэргийн нэг төрөл нь "фишинг" халдлага гэж дээр дурьдсан. Гэмт хэрэгтнүүд хуурамч имэйл илгээж, эсвэл танил сайтуудыг хуурамчаар дуурайлган хийж, иргэдийн хувийн мэдээлэл, банкны данс, нууц үг, картын дугаарыг залилж авч хулгайлдаг. Эдгээр хуурамч сайтууд нь танил брэндүүдийн цахим худалдааны вэбсайтууд болон банкны сайтыг дуурайж, хэрэглэгчдийг хууран мэхлэх зорилгоор бүтээгдсэн байдаг.

Мөн санхүүгийн залилангийн өөр нэг түгээмэл хэлбэр нь хөрөнгө оруулалтын залилан юм. Залилагчид өндөр өгөөж амлаж, иргэдийг криптовалют эсвэл үл хөдлөх хөрөнгө гэх мэт салбарт хөрөнгө оруулахад урьдаг. Иргэн мөнгөө шилжүүлсний дараа залилагчид усанд хаясан чулуу мэт алга болж, хохирогчид өөрийн хөрөнгийг буцааж авах боломжгүй болж хоцордог. Энэ төрлийн залилан нь Монгол улсад амьдарч буй дунд давхаргын хүмүүсийн хөрөнгө оруулах хүсэлд тулгуурлан чиглэгддэг бөгөөд эдийн засгийн эрсдэлээс зайлсхийхийн тулд олон хүн хөрөнгө оруулах хүсэлд хөтлөгдөн энэ төрлийн залилах гэмт хэргийн хохирогч болсоор байна.

Мөн Монгол улсад дижитал төлбөрийн системүүдийн хурдтай хөгжиж байгаа нь гэмт хэрэгтнүүдэд мөнгө хулгайлах, гэмт хэргийн замаас олсон мөнгөө угаах боломжийг олгодог. Зарим цахим худалдааны вебсайтууд болон банкны системүүдийн аюулгүй байдлын стандартууд хангалтгүй байдаг бөгөөд энэ нь гэмт хэрэгтнүүдэд гэмт хэрэг үйлдэхдээ ашиглах боломжийг бүрдүүлж өгч байна.

Шалтгаан нөхцөл:

Манай улсад кибер гэмт хэрэг нэмэгдэхэд хэд хэдэн хүчин зүйл нөлөөлж байна. Нэгдүгээрт, Монгол улсад цахим шилжилт хурдацтай явагдаж интернетийн хэрэглээ, ялангуяа гар утсаар дамжуулан интернетийн үйлчилгээ авч ашиглаж буй хүн амын тоо эрс өссөн. Гэвч эдгээр хүмүүсийн мэдээллийн аюулгүй байдалд анхаарал хандуулахгүй, мэдлэг тааруу хэнэггүй байхаас шалтгаалан, цахим гэмт хэрэгт өртөх эрсдэл нэмэгдсээр байна. Монголд улсад кибер аюулгүй байдлын боловсрол, мэдлэг, ойлголт харьцангуй бага байгаа нь иргэдийг цахим гэмт хэргээс өөрийгөө хамгаалах хязгаарлагдмал боломжийг бий болгож байна.

Хоёрдугаарт, Өнөөдрийн байдлаар Монгол Улсад кибер гэмт хэргийн эсрэг хуулийн хүрээ, хэрэглээ хангалттай хөгжөөгүй байна. Хэдийгээр Монгол Улс сүүлийн жилүүдэд кибер гэмт хэрэгтэй тэмцэх чиглэлд томоохон алхам хийсэн байгаа ч хууль эрх зүйн орчин нь чамлалттай хэвээр байна. Хууль сахиулах байгууллагууд нь техник, технологийн мэдлэг дутмаг байгаа бөгөөд кибер гэмт хэргийг мөрдөж, шийдвэрлэхэд шаардлагатай мэдлэг чадвартай хүний нөөц дутагдалтай байна. Мөн интернэт орчин нь олон улсын хил хязгаарыг давж гарах боломжийг олгодог тул кибер гэмт хэргүүдийг илрүүлэх, мөрдөн шалгах нь улс орнуудын хоорондын хууль тогтоомж, эрх зүйн харилцан туслалцаа үзүүлэх зэрэг асуудлуудаас болж хүндрэлтэй хэвээр байна.

Кибер Гэмт Хэрэгний хор уршиг:

Монгол улсад кибер гэмт хэргийн нөлөө маш өргөн хүрээтэй. Санхүүгийн хувьд, байгууллагууд болон хувь хүмүүс залилах, хакердах болон бусад төрлийн кибер халдлагаас болж

сэтгэл санаа болон эд хөрөнгийн хохирол их амсдаг. Ихэнх тохиолдолд хохирогчид хулгайлагдсан эд хөрөнгөө буцааж авах боломжгүй үлддэг. Кибер гэмт хэрэг нь олон нийтийн сүлжээ, шинэ дижитал платформуудын талаар буруу ойлголт төрүүлж итгэлийг алдагдуулж, Монгол улсын цахим эдийн засгийн өсөлтөд саад учруулж байна. Онлайн худалдаа, цахим үйлчилгээний талбарууд дахь хэрэглэгчид хуурамч вэбсайтууд болон өөр төрлийн залилах гэмт хэрэгт өртөх эрсдэлээс айж, цахим орчинд санхүүгийн гүйлгээ хийхээс зайлсхийдэг.

Мөн кибер гэмт хэрэг нь нийгэмд болон иргэдийн сэтгэлзүйд хортой нөлөөлж байна. Кибер хүчирхийлэл, онлайн доромжлолын гэмт хэргийн хохирогчид сэтгэл зүйн хүндрэлд орох, хувь хүний мэдээллийн хулгай, бусдын нэр төр алдар хүндэд халдах зэрэг гэмт хэрэгт өртөж урт хугацааны сөрөг үр дагаврыг амсах эрсдэлтэй. Мөн интернэт кибер орчин нь гэмт хэрэгтнүүдэд өөрсдийгөө халхавчлах, нуугдах, ял завших, зайлсхийх боломжийг олгодог тул кибер гэмт хэргийн гаралт ихсэж иргэд өөрсдийгөө хамгаалахад улам бүр хүндрэлтэй болсоор байна.

Бизнес эрхлэгчдийн хувьд үр дагавар нь бас хүнд байна. Иргэд өөрсдийн брэндтэй холбоотой луйврын хохирогч болсон тохиолдолд ялангуяа жижиг бизнесүүд нэр хүндэд нь хүнд хохирол учруулж болзошгүй. Цаашилбал, санхүүгийн гүйлгээг онлайнаар хийдэг байгууллагууд аюулгүй байдлын асуудалтай тулгарч кибер халдлагын бай болж болзошгүй. Гэмтсэн системийг засварлах, алдагдсан өгөгдлийг сэргээх, олон нийттэй харилцах хямралыг зохицуулах нь маш их зардал дагуулдаг.

Дүгнэлт. Монголын засгийн газар кибер гэмт хэргийн өсөлтийг хүлээн зөвшөөрч, уг асуудлыг шийдвэрлэхийн тулд хэд хэдэн арга хэмжээг авч хэрэгжүүлжээ. 2017 онд Монгол Улс анхны Кибер Аюулгүй Байдлын Хуулийг баталсан бөгөөд энэ хуулиар дижитал технологийн хэрэглээг зохицуулах, мэдээллийн аюулгүй байдлыг хамгаалах, кибер гэмт хэргийг таслан зогсоох, мөрдөн шалгах хууль эрх зүйн орчинг бүрдүүлэх анхны суурь тавигджээ.

Мөн Монгол Улс кибер аюулгүй байдлыг хангах төрийн тусгайлсан чиг үүрэг бүхий байгууллагыг бий болгосон бөгөөд энэ агентлаг нь улс орондоо кибер аюулгүй байдлыг бэхжүүлэх, мэдээллийн аюулгүй байдлын талаар олон нийтэд боловсрол олгох, технологийн аюулгүй байдлыг сайжруулах ажлуудыг зохион байгуулж байна.

Үүнээс гадна Монгол улсын төрийн болон хувийн хэвшил өөрсдийн цахим эд хөрөнгийг хамгаалахын тулд кибер аюулгүй байдалд хөрөнгө оруулалт хийж эхэлсэн байна. Олон компаниуд шифрлэлт, цахим хамгаалалтын системүүдийг бий болгож өөрсдийн ажилчдын дунд кибер аюулгүй байдлын талаарх мэдлэг олгох сургалт арга хэмжээ авч байна. Гэвч технологийн хурдтай хувьсан өөрчлөгдөж буй байдал нь байгууллагуудыг тогтмол шинэчлэл хийж байх шаардлагатайг сануулсаар байна.

Монгол Улсад кибер гэмт хэрэг өссөөр байгаа нь үндэсний аюулгүй байдалд нөлөөлөх чухал асуудал бөгөөд үүнийг шийдвэрлэхэд ганц төрийн болон хувийн хэвшлийн байгууллагууд гэлтгүй хувь хүмүүсийн хамтын хүчин чармайлт хамгаас чухал юм. Дижитал шилжилт, цахим эдийн засагт оролцож буй иргэдийн тоо нэмэгдэж буй энэ үед кибер гэмт хэргийн эрсдэл өсөх нь дамжиггүй. Эдгээр эрсдэлийг бууруулахын тулд кибер аюулгүй байдлын хуулийг сайжруулах, олон нийтэд мэдээллийн аюулгүй байдлын талаар ойлголт өгөх, хууль сахиулах байгууллагуудын чадавхыг бэхжүүлэх шаардлагатай. Монгол Улс дижитал эринд аюулгүй орчин бүрдүүлэхийн тулд энэ асуудлыг шийдвэрлэх чиглэлээр идэвхтэй арга хэмжээнүүдийг шат дараалан авч хэрэгжүүлэх ёстой.

Санал. Кибер гэмт хэрэгтэй тэмцэх арга замыг сайжруулахад нөлөөлж болох дараах саналуудыг авч үзлээ. Үүнд:

1. Хууль эрх зүйн чадамжийг сайжруулах

- **Кибер гэмт хэрэгтэй холбоотой хууль тогтоомж:** Манай улс кибер гэмт хэрэг, хакердах, хувийн мэдээлэл хулгайлах, өгөгдөл алдах, онлайн луйвар зэрэг кибер гэмт хэрэгт чиглэсэн хүчтэй хуулиудыг батлах хэрэгтэй. Эдгээр хууль нь олон улсын стандартад нийцэж байх ёстой бөгөөд дэлхий даяар хамтын ажиллагааг хангахад чухал юм.
- **Хуулийг шинэчлэх:** Хууль тогтоомжуудад шинэ технологиуд, кибер гэмт хэрэгт ашиглагддаг арга барилтай холбогдсон шинэчлэлтүүдийг үргэлж хийж байх шаардлагатай.

- **Тохирох шийтгэл болон хэрэгжилт:** Кибер гэмт хэргийн үйл ажиллагаанд заасан шийтгэлийг чангатгаж, хууль сахиулах байгууллагуудын кибер гэмт хэрэгтэй тэмцэх тусгай нэгжүүдээр дамжуулан үр дүнтэй хэрэгжүүлэх.
2. Хоёрдогч хамгаалалтын технологиудыг хөгжүүлэх
- **Галт хана (Firewall) ба Шифрлэлтийн системүүд:** Хувийн мэдээллийг хууль бус хандалтаас хамгаалах, хулгайд алдахаас урьдчилан сэргийлэх зорилгоор хүчтэй галт хана /хамгаалагч/ болон шифрлэлтийн техникүүдийг хэрэглэх.
 - **Дотоод сүлжээг хянах систем (IDS):** Сүлжээгээр дамжих бусад үйл ажиллагааг хянах, холбогдох гэмт хэрэгтэй тэмцэхэд шаардагдах мэдээлэл олж авах зорилгоор IDS ашиглах.
 - **Хиймэл оюун ухаан (AI) ба Машин бие даан суралцах (ML):** Эдгээр технологиуд нь сүлжээнд болж буй эрсдэлтэй үйлдлийг таньж, кибер халдлагын оролдлогыг цаг алдалгүй илрүүлэхэд тусална.
 - **Хоёр шатлалт баталгаажуулалт (2FA):** Онлайн дансанд хэт олон тооны нэвтрэх эрхээс хамгаалах зорилгоор хоёр шатлалт баталгаажуулалтыг хэрэглэгчдэд уриалах.
3. Кибер аюулгүй байдлын сургалт ба ойлголтыг хүртээмжтэй болгох
- **Олон нийтэд чиглэсэн сургалт:** Иргэдэд онлайн аюулгүй байдлын зөв дадал зуршлыг зөвлөж, цахим хуудас болон сэжигтэй холбоосуудаас хэрхэн сэргийлэх, баталгаажуулсан нууц үг зохиох аргуудыг сургах.
 - **Ажилтнуудад зориулсан сургалт:** Байгууллагууд өөрсдийн ажилтнуудаа кибер аюулгүй байдлын ойлголт, дадал зуршлыг тогтмол сургаж, хүний алдаа болон халдлагаас урьдчилан сэргийлэх мэдлэг чадварыг олгож байх.
 - **Сургалтын хөтөлбөрүүд:** Сургууль болон их дээд сургуульд кибер аюулгүй байдлын боловсролыг түлхүү хөгжүүлэх нь кибер аюулгүй байдалтай нүүр тулж, давж гарах чадвартай боловсон хүчин бэлтгэхэд тусална.
4. Олон улсын хамтын ажиллагааг сайжруулах
- **Олон улсын хамтын ажиллагаа:** Кибер гэмт хэрэг нь хил хязгааргүй үндэстэн дамнаж үйлдэгддэг гэмт хэрэг тул хууль сахиулах байгууллагууд (жишээ нь, Интерпол, Европол) хоорондын хамтын ажиллагаа кибер гэмт хэрэгтэнг илрүүлэх болон шүүхийн байгууллагад шилжүүлэхэд чухал үүрэгтэй.
 - **Шийтгэл эдлүүлэх гэрээ хэлэлцээрүүд:** Улсууд кибер гэмт хэргийн үйлдэгчдийг эх оронд нь шилжүүлэн авчрах зорилгоор экстрадицийн гэрээ байгуулах.
 - **Дэлхий даяар хүлээн зөвшөөрөгдсөн стандартууд ба тогтолцоо:** Нэгдсэн Үндэстний Байгууллага, Европын Холбоо зэрэг олон улсын байгууллагууд кибер гэмт хэрэгтэй тэмцэх дэлхий нийтийн ёс зүйн тогтолцоог тогтоох .
5. Хууль сахиулах байгууллагын бүрэлдэхүүн нэгж тус бүр дээр кибер гэмт хэрэгтэй тэмцэх тусгай тасгийг байгуулах
- **Кибер гэмт хэрэгтэй тэмцэх тусгай нэгжүүд:** Олон улсад өөрсдийн цагдаагийн байгууллага дотор кибер гэмт хэргийн тусгай нэгжийг байгуулж, кибер гэмт хэргийн эсрэг тэмцдэг. Манай улсын хувьд кибер гэмт хэрэгтэй тэмцэх ганцхан нэгж байдаг. Эрүүгийн цагдаагийн газрын харьяа Кибер гэмт хэрэгтэй тэмцэх газар. Бусад хот сууринд байрлах цагдаагийн газар хэлтэст шинэ төрлийн гэмт хэрэг болох кибер гэмт хэргийн таньж мэдэх, илрүүлэх, мөрдөн шалгах, таслах зогсоох мэдлэг чадамж дутмаг байсаар байна.
 - **Хувийн секторын хамтын ажиллагаа:** Хууль сахиулах байгууллагууд технологийн компаниуд, интернет үйлчилгээ үзүүлэгчид (ISP), кибер аюулгүй байдлын компаниудтай хамтран кибер гэмт хэрэг үйлдэгчдийг илрүүлэх таслан зогсоох чиглэлээр мэдээлэл солилцдог байх хэрэгтэй.
6. Яаралтай хариу арга хэмжээ үзүүлэх таслан сэргийлэх тусгай баг бий болгох.
- **Хариу арга хэмжээ үзүүлэх баг:** Байгууллагууд болон засгийн газар кибер халдлагын үед хариу үйлдэл үзүүлэх тусгай багтай байх ёстой бөгөөд гэмт хэргийг хэрхэн үйлдсэн болохыг

цаг алдалгүй тооцоолох мөн түүнээс болж учирсан хохирлыг тодорхойлох, таслан зогсоох үүрэгтэй.

- **Өгөгдлийн нөөцлөлт:** Үндсэн өгөгдлөө тогтмол нөөцөлж байх, халдлага болж өгөгдөл алдсан тохиолдолд хурдан сэргээн босгох боломжтой байх.
- **Олон нийтийн болон хувийн хэвшлийн хамтын ажиллагаа:** Засгийн газар болон хувийн байгууллагуудын хамтын ажиллагаа нь кибер халдлагад илүү хурдан хариу өгөх боломжийг олгодог.

7. Хар Веб (Dark Web) дээрх үйл ажиллагааг хянах

- **Хар вебийг хянах (dark web):** Кибер гэмт хэрэг, хулгайлагдсан мэдээлэл эсвэл хууль бус үйлчилгээг борлуулж буй үйл ажиллагаа нь хар веб дээр ихэвчлэн явагддаг. Хууль сахиулах байгууллагууд нь эдгээр үйл ажиллагааг таслан зогсоох урьдчилан сэргийлэх болон мөрдөн шалгах зорилгоор тогтмол хянаж байх.
- **Технологийн компаниудтай хийх хамтын ажиллагаа:** Нийгмийн сүлжээ, хайлтын систем, төлбөрийн үйлчилгээний компаниуд нь хууль сахиулах байгууллагуудтай хамтран хууль бус үйл ажиллагааг илрүүлж, устгахад чухал үүрэг гүйцэтгэж байдаг.

8. Этик хакердалт (Цагаан малгайт хакерууд)

- **Этик хакеруудын дунд алдаа засах урамшуулалт хөтөлбөр зарлах:** Цагаан малгайт хакерууд нь байгууллагуудын систем дэх сул талуудыг олж, эдгээрийг мэдээлэх замаар кибер гэмт хэрэг үйлдэхээс өмнө урьдчилан сэргийлэх боломжийг олгодог.
- **Хактивизм:** Этик хакерууд нь кибер аюулгүй байдлын талаарх мэдлэгийг олон нийтэд түгээх, байгууллагуудын сул талуудыг илрүүлэх зэрэг үүрэг гүйцэтгэж болно.

9. Бизнесийн байгууллагын кибер гэмт хэрэгтэй тэмцэх хөтөлбөрүүд

- **Кибер аюулгүй байдлын бодлого болон аудит:** Байгууллагууд нь бүхэлдээ кибер аюулгүй байдлын бодлогыг хэрэгжүүлж, халдлагаас урьдчилан сэргийлэхийн тулд тогтмол аюулгүй байдлын аудит хийдэг байх.
- **Өгөгдлийн хандалтын хяналт:** Хувийн мэдээллийг зөвхөн шаардлагатай хүмүүст хүргэх нь халдлагын аюулыг хязгаарлахад тусална.
- **Гэмт хэргийн тухай мэдээлэл өгөх:** Ажилтнууд болон хэрэглэгчдийг сэжигтэй үйл ажиллагаа болон зөрчилд цаг алдалгүй хууль сахиулах байгууллагад мэдээлэхийг уриалснаар кибер халдлагаас сэргийлэх боломжтой.

10. Олон нийтийн болон хувийн секторын хамтын ажиллагаа

- Засгийн газар, хувийн байгууллага, болон төрийн бус байгууллагууд хамтран кибер аюулгүй байдал болон кибер гэмт хэрэгтэй тэмцэх нэгдсэн арга хэмжээг хэрэгжүүлэх.
- **Мэдээлэл солилцох:** Төр, хувийн хэвшлийн хооронд мэдээлэл солилцох платформуудыг бий болгох нь кибер гэмт хэрэгтнүүдийн үйлдлийг таслан зогсооход тусална.