"Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв" УТҮГ-ын 2025 оны 12 дугаар сарын 15-ны өдрийн 01/235 дугаар албан бичгийн хавсралт

"КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ" УЛСЫН ТӨСӨВТ ҮЙЛДВЭРИЙН ГАЗРЫН 2025 ОНЫ ГҮЙЦЭТГЭЛИЙН ТАЙЛАН

Д/д	Стратеги төлөвлөгөө болон үндэслэж байгаа бусад бодлогын баримт бичиг, хууль тогтоомж	Төсөв	Шалгуур үзүүлэлт	Суурь түвшин	Зорилтот түвшин	Хүрсэн түвшин буюу хэрэгжилт /хүрээгүй бол тайлбар /	Гүйцэтгэлийн хувь
Зорилго 1. ХУУЛИАР ОЛГОСОН ЧИГ ҮҮРГИЙГ ХЭРЭГЖҮҮЛЭХ ЗОРИЛГЫН ХҮРЭЭНД							
Зорилт 1. Захиргаа удирдлагаар хангаж, хүний нөөцийн чадавхыг бэхжүүлэх							**100%**
1	Арга хэмжээ 1.1. Монгол Улсын Засгийн газрын 2020 оны 12 дугаар сарын 16-ний өдрийн 217 дугаар тогтоолоор батлагдсан "Байгууллагын гүйцэтгэлийн төлөвлөгөө боловсруулах, гүйцэтгэлийн зорилт, шалгуур үзүүлэлтийг тогтоох, тайлан гаргах" журмын дагуу Нийтийн төвийн Гүйцэтгэлийн төлөвлөгөө, тайланг боловсруулан удирдах дээд байгууллагад хүргүүлэх;	-	Хүргүүлсэн баримт бичгийн тоо	-	3	"Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв" УТҮГ-аас дараах баримт бичгүүдийг албан бичгээр хүргүүлсэн. Үүнд: 1.2025 оны 01 дүгээр сарын 20-ны өдрийн 07 дугаартай албан бичгээр 2025 оны гүйцэтгэлийн төлөвлөгөөг; 2.2025 оны 07 дугаар сарын 08-ны өдрийн 01/110 дугаартай албан бичгээр 2025 оны хагас жилийн гүйцэтгэлийн тайланг; 3.2025 оны 12 дугаар сарын 15-ны өдрийн 01/235 дугаартай албан бичгээр 2025 оны жилийн эцсийн гүйцэтгэлийн тайланг тус тус хүргүүлсэн болно.	100%
2	Арга хэмжээ 1.2. Сургалтын төлөвлөгөө боловсруулж, батлуулах;	-	Баталсан баримт бичгийн тоо	-	1	2025 оны 03 дугаар сарын 26-ны өдөр Захирлын А/17 дугаар тушаалаар батлагдсан сургалтын төлөвлөгөөний дагуу мэргэжилтнүүдийг нарийн мэргэшүүлэн чадавхжуулах зорилгоор улсын төсөв болон олон улсын байгууллагын санхүүжилтээр холбогдох сургалтуудад тогтмол хамруулан ажиллаж байна.	100%
3	Арга хэмжээ 1.3. Нийт ажилтнуудыг чадавхжуулах, нарийн мэргэшүүлэх сургалт, арга хэмжээнд тогтмол хамруулах;	Улсын төсвийн санхүүжилт, Олон улсын	Сургалт, арга хэмжээний тоо	-	8	Нийт ажилтнуудын мэдлэг, ур чадварыг дээшлүүлэх, мэргэжлийн чадавхыг бэхжүүлэх зорилгоор 2025 онд дотоод, гадаадын байгууллагуудын сургалтуудад давхардсан	100%

		төсөл хөтөлбөр				тоогоор 48 ажилтан хамрагдаж тухайн чиглэлээр, сертификат авсан болно. Үүнд: Японы Олон улсын хамтын ажиллагааны байгууллага ЖАЙКА (JICA)-аас зохион байгуулсан Comprehensive Understanding: SOC, CompTIA CySA+, мөн ЖАЙКА болон Шинжлэх Ухаан, Технологийн Их Сургуулийн хамтарсан "Хортой кодын шинжилгээ" сургагч багш бэлтгэх сургалтуудад нийт 11 ажилтан; Empasoft болон GMO Internet Group-ийн охин компани GMO IERAE-аас зохион байгуулсан Web Basic сургалтад 2 ажилтан, Өсвөр үеийнхний дундах цахим мөрийтэй тоглоом сэдэвт цахим сургалтад албан хаагчид хамрагдан сэтгэл зүй, нийгмийн эрсдэлийн талаарх ойлголтоо гүнзгийрүүлсэн. Мөн байгууллагын дотоод хяналтыг сайжруулах хүрээнд дотоод аудитын сургалт зохион байгуулагдаж 4 ажилтан; СЕН мэргэжлийн сургалт, Архивын ерөнхий газраас зохион байгуулсан "Албан хэрэг хөтлөлт, архивын ажилтан" сургалтад холбогдох албан хаагчид амжилттай хамрагдсан.	
Зорилт 2. Нийтийн төвийн гадаад, дотоод хамтын ажиллагааг өргөжүүлэх							**100%**
4	Арга хэмжээ 2.1. Монгол Улсын болон гадаад орны ижил төстэй байгууллагатай эрх хэмжээний хүрээнд хамтран ажиллах;	Улсын төсвийн санхүүжилт	Хамтын ажиллагаа эхлүүлсэн байгууллагын тоо	2	2	1."Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв" УТҮГ болон Цагдаагийн ерөнхий газрын Эрүүгийн цагдаагийн алба 2025 оны 03 дугаар сарын 21-ны өдөр хамтын ажиллагааны санамж бичиг; 2."Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв" УТҮГ болон Аюулгүй байдал судлалын хүрээлэн 2025 оны 02 дугаар сарын 24-ны өдөр хамтын ажиллагааны санамж бичгийг тус тус байгуулан санамж бичгийн хүхээнд хамтран ажиллаж байна. 3.Цахим хөгжил, инновац, харилцаа холбооны яам болон Их Британийн Засгийн газар хамтран хэрэгжүүлж буй Монгол Улсын кибер	100%

						аюулгүй байдлын эрсдэлийг тодорхойлох судалгааны ажлын багийн бүрэлдэхүүнд Кибер халдлагаас урьдчилан сэргийлэх газрын дарга болон ахлах мэргэжилтнүүд оролцон ажиллав.	
5	Арга хэмжээ 2.2. Олон улсад зохион байгуулагдах салбарын арга хэмжээнд оролцсон байх;	Улсын төсвийн санхүүжилт	Оролцсон арга хэмжээний тоо	3	5	1.Тайланд улсын Бангкок хотод 2025 оны 02 дугаар сарын 17-22-ны хооронд зохион байгуулагдсан “CPX2025” олон улсын сургалт, уулзалтад Кибер халдлагад хариу үзүүлэх газрын дарга болон Халдлага хариуцсан мэргэжилтэн; 2.Олон улсын харилцаа холбооны зохицуулах газраас АНЭУ-ын Дубай хотод зохион байгуулсан “Кибер бэлтгэл-2025” олон улсын хурал, арга хэмжээнд Аюулгүй байдлын шинжээч; 3.Оросын Холбооны Улсын элчин сайдын яамны 1077 тоот бичгийн дагуу ОХУ-ын Нижний новогрод хотод зохион байгуулагдсан “Аж үйлдвэрч Орос орны цахим үйлдвэрлэл” олон улсын хуралд 2025 оны 06 сарын 06-09-ны өдрүүдэд Нийтийн төвийг төлөөлөн Ахлах шинжээч, Кибер аюулгүй байдлын мэргэжилтнүүд; 4.Европын холбооны дэмжлэгтэйгээр Эстони улсын Талин хотод 2025 оны 06 дугаар сарын 16-20-ны хооронд зохион байгуулагдсан “Кибер аюулгүй байдлын зуны уулзалт, сургалт”-д Мэдээлэл, дүн шинжилгээний газрын дарга; 5.Бүгд Найрамдах Энэтхэг Улсад 2025 оны 11 дүгээр сарын 03-ны өдрөөс 2025 оны 11 дүгээр сарын 14-ны хооронд зохион байгуулагдсан Квант компьютерын сургалт, арга хэмжээнд Аюулгүй байдлын ахлах шинжээч тус тус оролцож салбарын олон улсын туршлагаас амжилттай судалж, сургалт арга хэмжээний сертификатыг эзэмшиж ирэв.	100%

6	Арга хэмжээ 2.3. Олон улсын кибер аюулгүй байдлыг хамгаалах чиглэлээр үйл ажиллагаа явуулдаг байгууллага, холбоотой хамтран ажиллах, шаардлагатай гэрээ хэлэлцээрийг байгуулах;	Улсын төсвийн санхүүжилт	Хамтын ажиллагаа эхлүүлсэн байгууллагын тоо	2	2	1.Тус Нийтийн төв нь Ази, Номхон далайн бүсийн кибер халдлага, зөрчилтэй тэмцэх төвүүдийн сүлжээ болох APCERT (Asia Pacific Computer Emergency Response Team)-ийн албан ёсны гишүүнээр 2025 оны 07 дугаар сарын 28-нд элсэж, бүс нутгийн болон олон улсын түвшинд хүлээн зөвшөөрөгдсөн. 2.Бүгд Найрамдах Энэтхэг Улсын Цахилгаан холбоо, мэдээллийн технологийн яамны харьяа Энэтхэгийн компьютерын яаралтай тусламжийн баг (CERT-In) болон "Кибер Халдлага Зөрчилтэй Тэмцэх Нийтийн Төв" УТҮГ хооронд кибер аюулгүй байдлын салбарт хамтын ажиллагаагаа өргөжүүлэхээр 2025 оны 09 дүгээр сарын 09-нд харилцан ойлголцлын санамж бичиг байгууллаа.	100%
Зорилт 3. Кибер халдлага, зөрчлийн мэдээллийн сан бүрдүүлэх, Кибер аюулгүй байдлын зөвлөлийг мэдээллээр хангах							**100%**
7	Арга хэмжээ 3.1. Эх сурвалжуудаас ирсэн мэдээллийг нэгтгэх, тайлан мэдээ боловсруулах үйл ажиллагааг автоматжуулах;	Улсын төсвийн санхүүжилт	Систем, тоо	-	3	Эх сурвалжуудаас ирсэн мэдээллийг нэгтгэх, задлан шинжлэх, тайлан мэдээ боловсруулах үйл ажиллагааг автоматжуулах зорилгоор дараах 3 системийг хөгжүүлж, ашиглалтад оруулсан болно. Үүнд: **1. Threat Intelligence Dashboard систем** Олон эх сурвалжаас (Shadowserver, Sinkhole, Kaspersky гэх мэт) ирсэн мэдээллийг нэгтгэн задлан шинжилж, кибер халдлагын төрөл, давтамж, аюулын түвшин, эх сурвалж, порт скан, outlier detection зэрэг аналитик мэдээллийг харуулдаг үндсэн систем. Мөн Халдлагыг scan, malware, device, honeypot зэрэг өргөн хүрээнд ангилан харах, Sample татан авч дэлгэрэнгүй шинжлэх, Англи, Монгол хоёр хэлний дэмжлэгтэй, Light, Dark theme ашиглах зэрэг нэмэлт сайжруулалтуудыг хийсэн. **2. Аюулгүй, Zero Trust орчинд ажиллах TI платформ систем** Threat Intelligence Dashboard-ын суурь кодыг шинэчилж, Zero Trust архитектур, өгөгдөл	100%

						болон тохиргооны шифрлэлт, программын бүрэн бүтэн байдлын шалгалт, Single Page Application (SPA) орчны гүйцэтгэл сайжруулалт (state management, memory leak бууруулалт) бүхий аюулгүй ажиллагааг хангасан платформ систем. **3. Тайлан автоматжуулалтын веб систем** Кибер аюулын талаарх долоо хоног тутмын тайланг автоматаар боловсруулах веб суурьтай дашбоард апп хэсгийн судалгаа, хөгжүүлэлтийг хийсэн. Тус системд С2 халдлагуудын мэдээллийг API хандалтаар татан авч дэлгэрэнгүйгээр харуулахаар оруулж, орчуулгыг хавсаргасан мөн хорт программын дотоод тархалтын мэдээллийг өдөрт нь автоматаар татан авч дата-г илүү нарийвчлалтай гарах боломжтой болсон.	
8	Арга хэмжээ 3.2. Монгол Улсын кибер орчин дахь аюул занал, нөхцөл байдлын мэдээллийн сан бүрдүүлэх;	Улсын төсвийн санхүүжилт	Мэдээллийн сан, тоо	-	1	Монгол Улсын кибер орчин дахь аюул занал, эмзэг байдлын өнөөгийн нөхцөл байдлыг бодитой үнэлэх, урьдчилан сэргийлэх арга хэмжээг төлөвлөх зорилгоор Threat Intelligence-д суурилсан мэдээллийн санг үе шаттайгаар бүрдүүлж байна. Уг ажлын хүрээнд дараах үндсэн чиглэлээр мэдээлэл цуглуулж, ангилан хадгалж байна. Үүнд: 1.**Эмзэг байдлын мэдээлэл (CVE):** Threat Intelligence эх үүсвэрүүдээс ирж буй мэдээлэлд үндэслэн Монгол Улсад хамааралтай илэрсэн эмзэг байдлууд (CVE)-ын дэлгэрэнгүй мэдээллийг цуглуулж, нөлөөлөл, эрсдэлийн түвшингээр нь ангилан мэдээллийн санд бүртгэн хадгалж байна. **2.Хорт программын статистик мэдээлэл:** Securelist Threat Intelligence эх үүсвэрээс ирж буй Монгол Улсад илэрч буй хорт программын талаарх статистик мэдээлэл, төрөл, тархалтын чиг хандлага болон холбогдох нэмэлт мэдээллийг тогтмол шинэчлэн хадгалж, дүн шинжилгээ хийж байна.	100%

						3.Сүлжээ, IP хаягийн илрэлтүүдийн мэдээлэл: Shodan, Censys, AbuseIPDB зэрэг олон улсын нээлттэй мэдээллийн сангуудаас cache зарчмаар Монгол Улсад хамааралтай IP хаягууд дээр илэрч буй эмзэг байдал, буруу тохиргоо, сэжигтэй үйл ажиллагааны талаарх мэдээллийг цуглуулан хадгалж байна. **4.Кибер зөрчил илэрсэн байгууллагуудын бүртгэл:** Кибер халдлага болон зөрчил илэрсэн байгууллагуудын IP хаяг, илэрсэн зөрчлийн төрөл, давтамжийн мэдээллийг бүртгэн авч, цаашид урьдчилан сэргийлэх болон эрсдэлийн үнэлгээнд ашиглаж байна.	
9	Арга хэмжээ 3.3. Кибер аюулгүй байдлын зөвлөлийг мэдээллээр хангах;	Улсын төсвийн санхүүжилт	Хүргүүлсэн тайлангийн тоо	-	4	Тус төвөөс гаргадаг долоо хоног тутмын тайлангийн хамрах хугацаанд Монгол улсад бүртгэлтэй IP хаягуудад харгалзах сүлжээний траффикт илэрсэн аливаа сэжигтэй үйлдэл, олон улсын халдлага, зөрчлийн индикаторт суурилан Монгол улсын кибер орчин дахь аюул занал, эмзэг байдал, түүний нөхцөл байдлын тайланг боловсруулж, Кибер аюулгүй байдлын зөвлөлийн ажлын албанд долоо хоног бүрийн баасан гаригт тогтмол, нийт **41** удаа цахимаар хүргүүлсэн. Мөн Кибер аюулгүй байдлын зөвлөлийн ажлын албанд зөвлөлийн 2025 оны улирлын үйл ажиллагааны төлөвлөгөөний гүйцэтгэлийн тайлан болон кибер халдлага, зөрчлийн тайланг 2025 оны 03 дугаар сарын 25-ны өдрийн 01/38 дугаартай албан бичгээр I улирлын, 2025 оны 06 дугаар сарын 25-ны өдрийн 01/103 дугаартай албан бичгээр II улирлын, 2025 оны 08 дугаар сарын 25-ны өдрийн 01/134 дугаартай албан бичгээр III улирлын тайланг тус тус хүргүүлсэн бөгөөд IV улирлын тайланг 2025 оны 12 дугаар сарын 18-ны өдөр хүргүүлэхээр төлөвлөж байна.	100%

Зорилт 4. Кибер халдлага, зөрчлийн талаар судалгаа, дүн шинжилгээ хийх, кибер халдлага зөрчлийн талаарх мэдээлэл солилцох суурь дэд бүтцийг хөгжүүлэх							**89.58%**
10	Арга хэмжээ 4.1. Dark Web орчинд кибер аюул заналын судалгаа хийх;	Улсын төсвийн санхүүжилт	Судалгаа тоо	-	3	**1."Dark Web орчинд алдагдсан зарим Монгол нууц үгийн дүн шинжилгээ" сэдэвт судалгааны ажил** Dark Web орчинд алдагдсан Монгол хэрэглэгчдийн нууц үгсийн аюулгүй байдлын түвшнийг үнэлэх зорилгоор нийт 4,255 нууц үгийг хамруулж, олон улсын түвшинд түгээмэл ашиглагддаг нууц үгийн хүч чадал (entropy) тодорхойлох аргуудыг ашиглан тоон болон чанарын дүн шинжилгээ хийж зөвлөмж, тайлан боловсруулсан. Судалгааны үр дүнд: -Алдагдсан нууц үгсээс тоон болон чанарын өгөгдөл гарган авах, Холбогдох нэмэлт мэдээллийг цуглуулж, олон улсын кибер аюулгүй байдлын судалгаа, шинжилгээнд түгээмэл хэрэглэгддэг арга зүй, статистик загварчлалын хүрээнд судалгааны асуудал дэвшүүлэх, Нэгтгэсэн судалгааны тайлан, дүгнэлт боловсруулах, Шийдвэр гаргалтад зориулсан бодитой зөвлөмж боловсруулах боломжтой болсон. **2."Дарк веб орчин дахь мэдээллийн илрүүлэлт, тандалтын судалгаа"** Dark web орчинд мэдээлэл хайхад хэрэглэгдэх megadose/onionsearch, katana, DedSecinside/owasp Torbot арга хэрэгслүүд болон сар бүрийн төлбөртэй Socradar үйлчилгээний талаар судалгаа хийсэн. Тус судалгааны үр дүнд эдгээр арга хэрэгслийн боломж, давуу болон сул талыг харьцуулан үнэлж, цуглуулсан мэдээлэлд тулгуурлан Dark Web орчны дүн шинжилгээг гүйцэтгэж байна.	66.66%
11	Арга хэмжээ 4.2. Кибер аюулгүй байдлыг хангахад тулгамдаж буй асуудлын талаар бодлогын судалгаа хийх;	Улсын төсвийн санхүүжилт	Судалгаа тоо	-	2	1."Аюулгүй байдал судлалын хүрээлэн"-тэй хамтын ажиллагааны хүрээнд "Кибер дипломат ажиллагаа ба Монгол Улс: Дижитал эринд олон улсын харилцааг хөгжүүлэх	100%

						боломж ба сорилт" сэдэвт судалгааг боловсруулж, хэвлүүлсэн. 2."Монгол Улсын кибер аюулгүй байдлын өнөөгийн нөхцөл, цаашид авч хэрэгжүүлэх арга хэмжээ" сэдэвт судалгааг хийж, сар тутмын цахим сэтгүүлд нийтэлсэн.	
12	Арга хэмжээ 4.3. Тоон шинжилгээний хэрэгслийн судалгаа хийх;	-	Судалгаа тоо	-	Хэрэгжилтээр	Тоон шинжилгээний хэрэгслийн судалгааны хүрээнд OpenCTI системийг судалж, серверийн орчинд суурилуулан тохируулж, abusedb-ээс өгөгдөл татах туршилтыг амжилттай гүйцэтгэсэн. Мөн Chainsaw хэрэгслийг судалж, ашиглах зааварчилгааг боловсруулсан.	100%
13	Арга хэмжээ 4.4. Судалгааны журам боловсруулж, батлуулах;	-	Батлагдсан журмын тоо	-	1	"Судалгааны ажлыг төлөвлөх, гүйцэтгэх, тайлагнах" журмыг AS-IF ба TO-BE аргачлалаар боловсруулж 2025 оны 11 дүгээр сарын 03-ны өдрийн Захирлын А/61 дугаар тушаалаар батлсан.	100%
14	Арга хэмжээ 4.5. Кибер халдлага, зөрчлийн талаарх дуудлага, мэдээлэл хүлээн авах сувгуудын тасралтгүй үйл ажиллагааг хангах;	Улсын төсвийн санхүүжилт	Тасралтгүй үйл ажиллагааг хангах	-	Хэрэгжилтээр	-Тайлант хугацаанд 113 тусгай дугаараар нийт 2,446 дуудлага хүлээн авснаас нийтийн төвд хамааралтай 836 дуудлага бүртгэгдэж, 146 байгууллагад хортой кодын илрүүлэлт болон бусад шаардлагатай зөвлөмж, мэдээллийг хүргэн ажилласан ба 70001113 суурин утсаар нийт 4 дуудлага хүлээн авсан байна. Мөн www.113.mn цахим хуудасны хэвийн, тасралтгүй ажиллагааг бүрэн ханган ажиллаж, тус цахим хуудсаар нийт 36 мэдээлэл хүлээн авсан байхаас 28 мэдээллийг иргэн, 8 мэдээллийг байгууллагаас тус тус ирүүлсэн байна. -113 тусгай дугаарыг автомат хариулагчтай болгох судалгаа хийгдэж, 70001113, 260113 байгууллагын суурин утас руу дуудлага хийхэд IVR автомат хариултаар дамжин байгууллагын дотуур дугаар болох 11132 суурин утсанд дуудлага хүлээн авдаг болж кибер халдлага, зөрчлийн мэдүүлэг авах сувгийн тоог нэгээр нэмэгдүүлсэн.	100%

						-Фейсбүүк хуудасны чатбот хэсэгт кибер халдлага, зөрчлийн талаар мэдээлэл өгөх сувгийн дэлгэрэнгүй мэдээллийг автоматаар хариулж байх тохиргоог нэмсэн.	
15	Арга хэмжээ 4.6. Кибер халдлага, зөрчлийн бүртгэлийн системийг сайжруулах техникийн даалгавар боловсруулж, системийн сайжруулалтыг хийх;	Улсын төсвийн санхүүжилт	Систем сайжруулсан байх	-	1	Техникийн даалгаврыг боловсруулж, систем хөгжүүлэлтийн дараах ажлууд хийгдээд байна. Үүнд: • Долоо хоногийн тайлан автоматаар гаргах • С2 халдлагуудын мэдээллийг API хандалтаар татан авч дэлгэрэнгүй харуулах • Тайлан мэдээллийг нэгтгэж график байдлаар харуулах мөн мэдээлэлд анализ, дүн шинжилгээ хийх • Хорт программуудын дотоод тархалтыг автоматаар цуглуулан, мэдээллийн баазад хавсаргах, тайланд нэгтгэн тусгах.	100%
16	Арга хэмжээ 4.7. Өгөгдлийн сангийн сервер байгуулах;	Дэлхийн банк	Сервер, тоо	-	1	Тус Нийтийн төвөөс өгөгдлийн сангийн хоёр сервер байрлуулах зориулалт бүхий өрөөг засварлан бэлтгэсэн болно. Гэвч “Ухаалаг засаг-II” төслийн “Кибер халдлага, зөрчилтэй тэмцэх төвүүдийн халдлага илрүүлэх, таслан зогсоох, хариу үйлдэл үзүүлэх чадавхыг бэхжүүлэх, техник технологиор хангах” ажлын хүрээнд 2025 оны хэрэгжилтийн явц, мөн Сангийн яамнаас ирүүлсэн төсвийн хязгаар тогтоох чиглэлийн дагуу төслийн холбогдох төлөвлөгөөнд өөрчлөлт оруулах шаардлага үүссэн. Үүнтэй холбогдуулан өгөгдлийн сангийн сервер байгуулах ажил түр хугацаанд хойшлогдоод байна.	50%
17	Арга хэмжээ 4.8. Нийтийн төвийн хэмжээнд мэдээлэл солилцох, мэдээллийн аюулгүй байдлыг хангасан Монгол улсад байршилтай мэдээллийн сувгийг ашиглалтад оруулах, нэвтрүүлэх;	Улсын төсвийн санхүүжилт	Нэвтрүүлсэн тоо	-	1	Төвийн мэдээллийн аюулгүй байдлыг хангах үүднээс Mattermost чат системийг судалж, мэдээллийн сувгийн серверийг Дата төв дээр байршуулан тохиргоог хийж 2025 оны 02 дугаар сарын 06-ны өдөр дотооддоо амжилттай нэвтрүүлэн ашиглаж байна.	100%
Зорилт 5. Бүх нийтийн кибер аюулгүй байдлын мэдлэг, ойлголтыг дээшлүүлэх							**95.71%**

18	Арга хэмжээ 5.1. Кибер аюулгүй байдлын тухай хуулийн 17 дугаар зүйл, 19 дугаар зүйл дэх салбарын байгууллагуудтай уулзалт зохион байгуулах, мэдээллээр хангах;	Улсын төсвийн санхүүжилт	Зохион байгуулсан уулзалтын тоо	5	10	Онц чухал мэдээллийн дэд бүтэцтэй хувийн хэвшлийн байгууллагуудад кибер халдлагаас урьдчилан сэргийлэх болон халдлагад хариу үзүүлэх арга хэмжээнүүдийг таниулах, кибер аюулгүй байдлыг хангахад тулгарч буй асуудлын талаар мэдээлэл солилцох, хамтын ажиллагааг бэхжүүлэх, холбогдох хууль тогтоомжийг таниулах зорилгоор 2025 оны 02 дугаар сарын 24-ний өдрөөс 2025 оны 05 дугаар сарын 15-ны өдрийн хооронд Кибер аюулгүй байдлын тухай хуулийн 17.1, 19.1-д заасан хувийн хэвшлийн 160 гаруй байгууллагын 260 орчим төлөөллийг хамруулсан нийт 10 удаагийн уулзалт, хэлэлцүүлгийг зохион байгуулсан. Дээрх арга хэмжээний үр дүнд нийт 18 байгууллагын 23 домэйн нэр, 45 IP хаягийг www.113.mn цахим хуудсанд бүртгүүлж, 5 байгууллага “Honey pot” системийг суурилуулсан байна. Мөн Монгол Улсад зонхилон илэрч буй хортой программуудыг автоматаар устгах ажлын хэсгийг Кибер аюулгүй байдлын зөвлөлийн Ажлын албаны даргын тушаалаар байгуулж, уг арга хэмжээний хууль зүйн үндэслэлийг боловсруулан, техникийн туршилтыг амжилттай гүйцэтгэсэн.	100%
19	Арга хэмжээ 5.2. Сар тутмын цахим товхимол гаргах;	Улсын төсвийн санхүүжилт	Цахим товхимлын тоо	-	3	“CyberRead” цахим сэтгүүлийн гурван дугаарыг бэлтгэн, онц чухал мэдээллийн дэд бүтэцтэй хувийн хэвшлийн байгууллагуудад цахим хэлбэрээр хүргүүлээд байна. Тус сэтгүүлийн эхний хоёр дугаарыг байгууллагын албан ёсны цахим хуудас болон олон нийтийн сүлжээнд 2025 оны 10 дугаар сарын 03, 11 дүгээр сарын 03-ны өдрүүдэд тус тус нийтэлсэн. Сэтгүүлийн эхний дугаарт Хорт программын шинжээч Э.Бямбасүрэнгийн “Дижитал сүүдэр: Андромеда ботнетийн нууцыг илрүүлсэн нь” сэдэвт судалгааны өгүүллийг, хоёр дахь	100%

						дугаарт Захиргаа удирдлагын газрын дарга Д.Алтанчимэг, Кибер халдлагаас урьдчилан сэргийлэх газрын дарга Г.Гантуяа нарын хамтран бичсэн "Монгол Улсын кибер аюулгүй байдлын өнөөгийн нөхцөл, цаашид авч хэрэгжүүлэх арга хэмжээ" сэдэвт судалгааны өгүүллийг тус тус онцлон нийтэлсэн. Харин гурав дахь дугаарт Аюулгүй байдал судлалын хүрээлэнгийн гэрээт судлаач Ц.Мөнхбаярын "Үндэсний аюулгүй байдалд хиймэл оюуны үзүүлэх нөлөө" сэдэвт судалгааны өгүүллийг онцолсон бөгөөд 2025 оны 12 дугаар сарын 22-ны өдөр нийтлэхээр төлөвлөж байна.	
20	Арга хэмжээ 5.3. "Хүний хувийн мэдээлэл хамгаалах тухай хууль"-ийн хэрэгжилтийн хүрээнд олон нийтийн мэдлэг ойлголтыг дээшлүүлэх, сэргийлэх өдөрлөг зохион байгуулах;	Улсын төсвийн санхүүжилт	Зохион байгуулсан өдөрлөгийн тоо	-	1	"Хүний хувийн мэдээлэл хамгаалах тухай хууль"-ийн хэрэгжилтийн хүрээнд олон нийтийн мэдлэг, ойлголтыг дээшлүүлэх, урьдчилан сэргийлэх зорилготой өдөрлөгийг 2025 оны 06 дугаар сарын 20 болон 06 дугаар сарын 30-ны өдрүүдэд зохион байгууллаа. Тус өдөрлөгөөр хуулийн талаарх мэдлэг, ойлголтыг нэмэгдүүлэх зорилгоор "А , Б тест" асуулгыг байгууллагын нийт албан хаагчид болон www.ubn.mn сайтын сэтгүүлч, ажилтнуудын дунд амжилттай зохион байгуулж, нийт 5 контент бэлтгэн олон нийтийн цахим сувгуудаар түгээсэн.	100%
21	Арга хэмжээ 5.4. Кибер орчинд хүүхэд хамгаалах арга хэмжээг хэрэгжүүлэх;	Улсын төсвийн санхүүжилт	Арга хэмжээний тоо	-	1	2025 оны 09 дүгээр сарын 30-ны өдөр ШУТИС-ийн Коосэн технологийн коллежтой, 2025 оны 10 дугаар сарын 15-ны өдөр ерөнхий боловсролын 111 дүгээр дунд сургууль болон нийслэлийн Жаргалан дунд сургуультай хамтран сурагчдад зориулсан "Цахим орчинд хүүхэд хамгаалах" арга хэмжээг зохион байгууллаа. Уг арга хэмжээнд нийт 400 орчим оюутан, сурагч хамрагдаж, батлагдсан хөтөлбөрийн дагуу мэдлэг, ойлголтоо дээшлүүлэв. Мөн хүүхдүүдийн зөвшөөрөл, идэвхтэй оролцоонд үндэслэн нийт 3 контент,	100%

						2 пост бэлтгэн олон нийтийн сувгуудаар түгээсэн.	
22	Арга хэмжээ 5.5. Ерөнхий боловсролын сургуулийн “Мэдээллийн технологи” хичээлийн сургалтын хөтөлбөрт тусгах кибер аюулгүй байдлыг хангах талаар агуулга боловсруулж, холбогдох газарт санал хүргүүлэх;	Улсын төсвийн санхүүжилт	Хүргүүлсэн саналын тоо	-	1	Ерөнхий боловсролын дунд сургуулийн “Мэдээллийн технологи” хичээлийн 6-12 дугаар ангийн хөтөлбөрт тусгагдсан мэдээллийн аюулгүй байдал, кибер аюулгүй байдлын агуулгад судалгаа хийж, анги тус бүрийн түвшнийг үнэлэн, олон улсад хэрэгжиж буй жишиг хөтөлбөрүүдтэй харьцуулан сайжруулах санал, зөвлөмжийг боловсруулсан.	70%
23	Арга хэмжээ 5.6. Иргэд, олон нийтэд зориулсан кибер аюулгүй байдлыг хангах сургалтыг хамтран зохион байгуулах;	Улсын төсвийн санхүүжилт	Зохион байгуулсан сургалтын тоо	-	4	1.Дижитал шилжилтийг эрчимжүүлэх, технологийн бизнесийг хөгжүүлэх, мэдээллийн технологийн боловсролын хүртээмжийг нэмэгдүүлэх, бүс нутгийн эдийн засагт технологийн үүргийг тодорхойлоход дэмжлэг үзүүлэх зорилготой “Зүүн бүсийн мэдээллийн технологийн чуулган”-ы нээлтийн үйл ажиллагааг 2025.03.29-ний өдөр Хэнтий аймгийн төв Чингис хаан хотод Цахим хөгжил, инновац, харилцаа холбооны яамтай хамтран зохион байгуулж, мэдээллийн аюулгүй байдлын талаар хичээл заасан. 2.Мэдээлэл технологийн үндэсний паркийн хүсэлтээр хөгжлийн бэрхшээлтэй иргэдэд 2025 оны 04 сарын 04-ны өдөр сургалт зохион байгуулсан. Сургалтад нийт 15 иргэн хамрагдсан. 3.Төрийн Цахим Үйлчилгээний Зохицуулалтын Газрын Говьсүмбэр, Дорноговь аймгууд дахь Цахим шилжилт, үйлчилгээний хэлтэстэй хамтран 2025 оны 11 дүгээр сарын 20-оос 11 дүгээр сарын 24-ны өдрүүдийн хооронд төрийн албан хаагчид, ахмад настан, сурагчдыг хамруулсан кибер аюулгүй байдлын сургалтыг зохион байгууллаа. 4.Төрийн Цахим Үйлчилгээний Зохицуулалтын Газрын Орхон, Хөвсгөл, Булган аймгууд дахь Цахим шилжилт, үйлчилгээний хэлтэстэй хамтран 2025 оны 11 дүгээр сарын 25-аас 11	100%

						дүгээр сарын 30-ны өдрүүдийн хооронд төрийн албан хаагчид, ахмад настан, сурагчдыг хамруулсан кибер аюулгүй байдлын сургалтыг зохион байгууллаа. Тус 5 удаагийн сургалтаар цахим орчинд кибер аюулгүй байдлыг хангах, түгээмэл тохиолдож буй халдлагууд болон тэдгээрээс урьдчилан сэргийлэх арга зам, мэдээллийн аюулгүй байдлын бодлого, журмыг нэвтрүүлэх, мөрдөх асуудлаар Кибер аюулгүй байдлын сургалт хариуцсан мэргэжилтэн Н.Дөлгөөн сургалт орж, нийт 1000 гаруй төрийн албан хаагч, ахмад настан, сурагчид хамрагдсан байна.	
24	Арга хэмжээ 5.7. Кибер аюулгүй байдлыг хангах талаар тараах материал боловсруулж, хэвлүүлэх;	Улсын төсвийн санхүүжилт	Боловсруулсан материалын тоо	-	1	Онц чухал мэдээллийн дэд бүтэцтэй хувийн хэвшлийн байгууллагуудад тараах материалын эхийг 2025 оны 03 дугаар сарын 14-ны өдөр дараах агуулгын хүрээнд бэлтгэн, 540 хувь хэвлүүлж олон нийтийг хамарсан сургалт, арга хэмжээнд ашигласан. Үүнд: -Нийтийн төвийн танилцуулга; -Аудит эрсдэлийн үнэлгээний зөвлөмж; -113 болон халдлагад хариу үзүүлэх процессын талаарх танилцуулга.	100%
Зорилт 6. Мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээг Мэдээллийн аюулгүй байдлын аудит хийх зөвшөөрөл бүхий хуулийн этгээдээр хийлгэх хуулийн хэрэгжилтийг хангуулж ажиллах							**75%**
25	Арга хэмжээ 6.1. Мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээний тайланг хүлээн авч зөвлөмж, шаардлага хүргүүлэх;	-	Хамрагдсан байгууллага, хувь	10.5%	Хэрэгжилтээр	Онц чухал мэдээллийн дэд бүтэцтэй байгууллага болон хувийн хэвшлийн байгууллагуудад шаардлага, зөвлөмж хүргүүлж, 2025 оны 03 дугаар сарын 11-ээс 11 дүгээр сарын 07-ны өдрүүдийн хооронд “ХАС БАНК” ХХК, “Магнай Трейд” ХХК, “Клин Энержи” ХХК-ийн Салхит салхин цахилгаан станц, “Баянзүрх эмнэлэг” ХХК, “Дата Бэйнк” ХХК, “Богд Банк” ХК, “Тээвэр хөгжлийн банк” ХК, “Мэдээлэл холбооны сүлжээ” ХХК, “Бүрэн скор ЗМС” ХХК, “Энержи Ресурс” ХХК, “Капитрон Банк” ХХК, “Юнител” ХХК, “Юнивишн” ХХК, “Ашид Капитал ББСБ” ХХК, “Ариг Банк” ХХК, “Хаан Банк” ХХК зэрэг нийт	100%

						20 (26%) байгууллагаас Мэдээллийн аюулгүй байдлын аудитын тайланг хүлээн авсан. Мөн кибер аюулгүй байдлын эрсдэлийн үнэлгээг 2025 оны 03 дугаар сарын 11-ээс 11 дүгээр сарын 04-ний өдрүүдийн хооронд “Клин Энержи Ази” ХХК, “Чингис Хаан Банк” ХХК, “Капитрон Банк” ХХК, “Грандмед эмнэлэг” ХХК, “Ариг Банк” ХХК, “Магнай Трейд” ХХК, “ХасБанк” ХХК, “Энержи Ресурс” ХХК зэрэг нийт 11 (14%) байгууллагаас тайлан хүлээн авсан. Онц чухал мэдээллийн дэд бүтэцтэй байгууллага нь өөрийн хариуцсан мэдээллийн систем, дэд бүтцийн хэвийн найдвартай тасралтгүй байдлыг хангах, гэмтэл саатлын үед сэргээн ажиллуулах төлөвлөгөөтэй байх, кибер аюулгүй байдлын эрсдэлийн үнэлгээ болон мэдээллийн аюулгүй байдлын аудитыг хуульд заасан хугацаанд хүргүүлэх тухай 01/100 дугаар албан бичгийг нийт 60 байгууллагад хүргүүлсэн. Мөн “Мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээний тайланг цахимаар хүргүүлэх, хүлээн авах, тайлангийн мэдээллийг ашиглах журам”-ын төслийг боловсруулан, хянуулж байна.	
26	Арга хэмжээ 6.2. Төвийн үйл ажиллагаанд Мэдээллийн аюулгүй байдлын менежментийн тогтолцооны MNS ISO/IEC 27001:2023 стандартыг нэвтрүүлэх;	Улсын төсвийн санхүүжилт	Нэвтрүүлсэн стандартын тоо	-	1	Төвийн үйл ажиллагаанд “MNS ISO/IEC 27001:2023 Мэдээллийн аюулгүй байдлын менежментийн тогтолцооны стандарт”-ыг нэвтрүүлэх ажлын хүрээнд захирлын А/04 дүгээр тушаалаар ажлын хэсэг байгуулж, ажлын хэсгийн төлөвлөгөөний дагуу стандартын 4, 5, 6 дугаар бүлэг, мэдээллийн аюулгүй байдлын бодлогын төслийг боловсруулсан. Стандартын зөрүүгийн шинжилгээ, хуулийн нийцэл, ашиглаж буй 19 системийн эрсдэлийн үнэлгээг хийсэн. Стандарт нэвтрүүлэх зөвлөх үйлчилгээ үзүүлэх хуулийн этгээд сонгон шалгаруулах ажлын урилга, ажлын даалгаврыг	50%

						боловсруулан батлуулж, байгууллагын цахим хуудсанд олон нийтэд нээлттэй байршуулан 4 үнийн санал авсан. Одоогоор төсөв шийдэгдээгүй байна.	
Зорилт 7. Кибер аюулгүй байдлыг хангах чиглэлээр сургалт зохион байгуулах, салбарын болон дотоодын хүний нөөцийн чадавхыг сайжруулах, олон нийтийг соён гэгээрүүлэх ажлыг зохион байгуулах							**100%**
27	Арга хэмжээ 7.1. Онц чухал мэдээллийн дэд бүтэцтэй хувийн хэвшлийн байгууллагуудын дунд жилд нэг удаа кибер аюулгүй байдлын дадлага сургуулилт зохион байгуулах;	Улсын төсвийн санхүүжилт	Зохион байгуулсан сургуулилтын тоо	-	1	Кибер халдлага, зөрчилтэй тэмцэх нийтийн төвд харьяалагдах онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудын дунд “Системийн эмзэг байдлаас үүдэлтэй зөрчилд хариу үзүүлэх” сэдвийн хүрээнд цахим сургуулилтыг 2025 оны 3 сараас 4 дүгээр сарын хооронд бэлтгэх, гүйцэтгэх, үнэлэх гэсэн гурван үе шаттайгаар цахим хэлбэрээр зохион байгуулсан. Тус сургуулилтаар байгууллагуудын кибер аюулгүй байдлын зөрчилд хариу үзүүлэх төлөвлөгөө, чадавх, зөрчлийн үе дэх харилцаа холбоо, шуурхай ажиллагааны бэлэн байдлыг бодитоор үнэлэх боломж бүрдсэн.	100%
28	Арга хэмжээ 7.2. Кибер халдлага, зөрчлийн мэдээлэл солилцох протоколын оролцогч талуудыг нэмэх;	Улсын төсвийн санхүүжилт	Нэмэгдсэн тоо	10	18	Кибер аюулгүй байдлын зөрчил зохицуулахтай холбоотой харилцан мэдээлэл солилцох протоколыг банкны системийн нөлөө бүхий зургаан банктай 2025 оны 5 дугаар сарын 2-ноос 5 дугаар сарын 9-ний өдрүүдэд байгуулж, мэдээлэл солилцох үйл ажиллагааг эхлүүлсэн бөгөөд үүнд Хаан банк, Голомт банк, Төрийн банк, Хас банк, Ариг банк, Тээвэр хөгжлийн банк хамрагдсан. Мөн 2025 оны 5 дугаар сарын 9-ний өдөр хувийн хэвшлийн гурван байгууллагатай кибер аюулгүй байдлын зөрчилтэй холбоотой мэдээлэл солилцох протокол байгуулсан бөгөөд үүнд Датабэйнк ХХК, Vertex, iSAT компаниуд хамрагдсан.	100%
29	Арга хэмжээ 7.3. Мэдээллийн аюулгүй байдлын захиалгат сургалтыг зохион байгуулах;	Улсын төсвийн санхүүжилт	Зохион байгуулсан сургалтын тоо	-	24	Тайлант хугацаанд мэдээллийн аюулгүй байдлын чиглэлээр захиалгат сургалтыг нийт **36 удаа** зохион байгуулж, сургалтад **2519 албан хаагч**, **860 оюутан, сурагч** хамрагдсан	100%

						байна. Сургалтуудыг төрийн байгууллага, төрийн өмчит болон хувийн хэвшлийн байгууллага, их, дээд сургууль, ерөнхий боловсролын сургуулийн сурагчдад зориулан танхим, цахим болон хосолсон хэлбэрээр зохион байгуулсан. Сургалтын хүрээнд мэдээллийн аюулгүй байдал, кибер аюулгүй байдлын суурь ойлголт, хортой код, вэб болон сүлжээний аюулгүй байдал, dark web, фишинг халдлагын талаарх мэдлэг олгох, фишинг халдлагын туршилт хийх, кибер аюулгүй байдлын мэргэжлийг сурталчлах сэдвүүдийг хамруулсан. Тухайлбал Мэдээлэл холбооны сүлжээ ХК, Монгол шуудан ХК, Грандмед эмнэлэг, Онцгой байдлын ерөнхий газар, Зэвсэгт хүчний жанжин штаб, Үндэсний статистикийн хороо, Сангийн яам, Зам тээврийн яам, Монголын хөрөнгийн бирж ХК зэрэг байгууллагуудын албан хаагчдад зориулсан сургалтуудыг амжилттай зохион байгуулсан. Мөн Төрийн цахим үйлчилгээний зохицуулалтын газар, Шинжлэх ухаан технологийн их сургууль, Хөдөө аж ахуйн их сургууль, Коосэн технологийн коллежийн оюутнуудад болон аймаг, орон нутгийн “Хурдан” клубийн сурагчдад чиглэсэн мэдээллийн аюулгүй байдлын сургалтуудыг тогтмол зохион байгуулж, хүүхэд, залуусын кибер аюулгүй байдлын мэдлэг, хандлагыг дээшлүүлэхэд анхаарч ажилласан. Дээрх сургалтуудын үр дүнд төр, хувийн хэвшил, боловсролын байгууллагын албан хаагч, суралцагчдын мэдээллийн болон кибер аюулгүй байдлын талаарх мэдлэг, ухамсар нэмэгдэж, зөрчлөөс урьдчилан сэргийлэх чадавхыг бэхжүүлэхэд бодитой хувь нэмэр оруулсан болно.	

30	Арга хэмжээ 7.4. Кибер аюулгүй байдлыг хангах, Иргэд олон нийтийг соён гэгээрүүлэх ажлыг цахим сүлжээнд түгээн дэлгэрүүлэх, мэдээ мэдээлэл олгох;	Улсын төсвийн санхүүжилт	Мэдээний тоо	-	Гүйцэтгэлээр	Тус Нийтийн төв нь 2025 оны 01 дүгээр сарын 02-ны өдрөөс 2025 оны 12 дугаар 01-ний өдрийг хүртэл нийт 80 гаруй контент бэлдэн, байгууллагын цахим хуудас, олон нийтийн сүлжээ (фейсбүүк) -ээр дамжуулан түгээсэн. Байгууллагын фейсбүүк хуудасны нийт хандалт 2025 оны 12 дугаар сарын 01-ний өдрийн байдлаар 4200 дагагчтай болж, өмнөх онтой харьцуулахад хандалт 77%-иар өссөн байна. Жишээ нь: Зам тээврийн яамны газруудын төлөөлөл, яамны харьяа авто тээвэр, авто зам, төмөр зам, далайн тээвэр болон иргэний нисэхийн салбарын мэдээллийн аюулгүй байдал хариуцсан нийт албан хаагч, ажилтнуудад байгууллагын кибер аюулгүй байдлын сургалт болон халдлагын туршилтыг хослуулан зохион байгуулсан сургалтаар бэлтгэсэн мэдээг www.pubcert.mn цахим хуудсанд 2025 оны 05 дугаар сарын 19-ны өдөр нийтэлсэн.	100%
31	Арга хэмжээ 7.5. Төвүүдийн хамтын ажиллагааг сайжруулах сургуулилт зохион байгуулах;	Улсын төсвийн санхүүжилт	Зохион байгуулсан тоо	-	4	Кибер аюулгүй байдлыг хангах хүний нөөцийн чадавхыг сайжруулах, дотоод болон гадаад хамтын ажиллагааг хөгжүүлэх замаар кибер орчин дахь мэдээллийн аюулгүй байдал, нууцлал, хүртээмжийг хангах зорилтын хүрээнд Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв нь дараах байгууллагуудтай хамтран “Зеро дэй арена” сэдэвт сургуулилтыг амжилттай зохион байгуулж хэрэгжүүллээ. Тухайлбал: -2025 оны 01 дүгээр сарын 10-ны өдөр Эрүүгийн цагдаагийн албаны Кибер гэмт хэрэгтэй тэмцэх газартай, -2025 оны 01 дүгээр сарын 17-ны өдөр Эрүүгийн цагдаагийн албаны Кибер гэмт хэрэгтэй тэмцэх газрын өөр багтай, -2025 оны 03 дугаар сарын 26-ны өдөр Монголын үүрэн холбооны оператор Юнител групптэй,	100%

						-2025 оны 06 дугаар сарын 10-ны өдөр банк, санхүүгийн үйлчилгээ эрхлэгч Голомт банктай тус тус хамтран зохион байгуулсан байна. Тус сургуулилтын хүрээнд нэг болон олон цоорхойтой системийн эмзэг байдлыг тодорхойлох, тэдгээрийг ашиглах замаар кибер халдлага, зөрчилд хариу арга хэмжээ авах чадварыг дээшлүүлэхэд чиглэсэн практик сургалтуудыг амжилттай хэрэгжүүлэн ажилласан.	
32	Арга хэмжээ 7.6. Кибер халдлагад хариу үзүүлэх дотоод сургуулилт зохион байгуулах;	Улсын төсвийн санхүүжилт	Зохион байгуулсан тоо /сар бүр/	-	12	Байгууллагын мэдээллийн аюулгүй байдлын хамгаалалтын чадавхыг бодит нөхцөлд үнэлэх, кибер халдлагад хариу үзүүлэх ажилчдын мэргэжлийн ур чадварыг бодит орчинд дээшлүүлэх, харилцан суралцах боломжийг бүрдүүлэх, мөн шинэ арга техник, шийдлийг турших, үйл ажиллагаанд илэрч буй сул талыг тодорхойлон цаашдын сайжруулалтад дэмжлэг үзүүлэх зорилтын хүрээнд кибер халдлагад хариу үзүүлэх дотоод сургуулилтыг зохион байгуулсан. Сургуулилтыг байгууллагын дотооддоо ашигладаг мэдээлэл солилцох платформоор дамжуулан оролцогчдыг RED болон BLUE багт хуваан, өгөгдсөн хувилбар, даалгаврын дагуу гүйцэтгүүлсэн. Уг сургуулилт нь 2025 оны 02 дугаар сарын 26, 03 дугаар сарын 12, 04 дүгээр сарын 21, 05 дугаар сарын 12, 06 дугаар сарын 30, 07 дугаар сарын 04, 07 дугаар сарын 22, 08 дугаар сарын 27, 09 дүгээр сарын 10, 09 дүгээр сарын 26, 10 дугаар сарын 09, 11 дүгээр сарын 17-ны өдрүүдэд тус тус нийт 12 удаа амжилттай зохион байгуулагдсан. Тус сургуулилтын үр дүнд халдлагыг илрүүлэх, хариу арга хэмжээ авах, бодит нөхцөлд шийдвэр гаргах чадавхыг нэмэгдүүлсэн.	100%
33	Арга хэмжээ 7.7. Цахим хуудасны аюулгүй байдлын талаарх 10 лекцээс	-	Зохион байгуулсан	-	10	Цахим хуудасны аюулгүй байдал (Web security)-ын талаарх сургалтыг байгууллагын	100%

	бүрдсэн хичээлийг нийтийн төвийн мэргэжилтнүүдэд орох;		сургалтын тоо			нийт ажилтнуудын дунд 2025 оны 03 дугаар сарын 13-ны өдрөөс 03 дугаар сарын 23-ны өдрийн хооронд нийт 10 удаа амжилттай зохион байгуулж, лабораторийн ажлын гүйцэтгэлээр тэргүүлсэн 2 ажилтныг шалгаруулсан.	
Зорилт 8. Иргэн, хуулийн этгээдийн мэдээллийн систем, мэдээллийн сүлжээнд чиглэсэн кибер халдлага, зөрчлийг илрүүлэх, таслан зогсоох, халдлагад хариу арга хэмжээ авах, кибер халдлага, зөрчилд өртсөн мэдээллийн системийг нөхөн сэргээхэд дэмжлэг үзүүлэх							**100%**
34	Арга хэмжээ 8.1. Кибер халдлага, зөрчил хүлээн авах сувгуудаар иргэд, хуулийн этгээд, хувийн өмчит онц чухал мэдээллийн дэд бүтэцтэй байгууллагуудаас хүлээн авсан, хүргүүлсэн мэдээлэлд тулгуурлан кибер халдлага, зөрчилд шинжилгээ хийж хариу үзүүлэх;	Улсын төсвийн санхүүжилт	Гүйцэтгэлээр	9	-	Хуулиар хүлээсэн чиг үүрэгт хамааралтай халдлагад өртсөн нийт 43 байгууллагын мэдээлэл бүртгэгдэж, 2025 оны 02 дугаар сараас 12 дугаар сарын 04-ний өдрийг хүртэлх хугацаанд 15 байгууллагад газар дээр нь очиж ажилласан бол 28 байгууллагад зайнаас хариу арга хэмжээ авч ажилласан. Мөн Монгол Улсын харьяалал бүхий 487 IP хаягийн хэрэглэгчийн мэдээллийн систем хортой кодын халдлагад өртсөнийг илрүүлж, интернэт үйлчилгээ үзүүлэгч байгууллагуудтай хамтран холбогдох эзэмшигчдийг тогтоон, үүнээс 146 IP хаягийн хэрэглэгчдэд хортой кодын халдлагыг таслан зогсоох, нөхөн сэргээх талаарх зөвлөмжийг тухай бүр хүргүүлэн ажилласан.	100%
35	Арга хэмжээ 8.2. Хувийн хэвшлийн байгууллагуудын мэдээллийн сүлжээ, мэдээллийн системд эмзэг байдал илрүүлэх шалгалтыг тогтмол хийх;	Улсын төсвийн санхүүжилт	Эмзэг байдал илрүүлсэн тоо	35	70	Нийтийн төвд харьяалагдах халдлагын хаягуудад тулгалт хийж, эмзэг байдал илэрсэн 43 байгууллагад 2025 оны 02 дугаар сараас 12 дугаар сарын 04-ний өдрийг хүртэлх хугацаанд 15 байгууллагад газар дээр нь очиж ажилласан бол 28 байгууллагад зайнаас хариу арга хэмжээ авч ажилласан байна.	100%
36	Арга хэмжээ 8.3. Кибер халдлагад өртсөн, эмзэг байдал илэрсэн талаар мэдээлэл хүргүүлэх;	Улсын төсвийн санхүүжилт	Илэрсэн эмзэг байдлыг мэдээлсэн тоо	-	Гүйцэтгэлээр	Нийтийн төвд харьяалагдах халдлагын хаягуудад тулгалт хийж, эмзэг байдал илэрсэн 43 байгууллага руу холбогдож зохих арга хэмжээг авч, хортой кодын халдлагыг таслан зогсоох, нөхөн сэргээх талаарх зөвлөмжийг тухай бүр хүргүүлэн зохих арга хэмжээг авч ажилласан.	100%

37	Арга хэмжээ 8.4. Монгол улсын интернэт сүлжээний орчин дахь кибер аюул занал, нөхцөл байдлын талаар 7 хоног тутамд тандалт хийх, тандалтын эх сурвалжуудыг нэмэх;	Улсын төсвийн санхүүжилт	Тайлангийн тоо	52	64	Монгол улсын IP хаягт хамаарал бүхий сэжигтэй үйлдэл, халдлагын мэдээллийг Abuse.ch, DataPlane.org, SANS ISC, ShadowServer, Spamhaus Private, Team Cymru, Telia ZONE-H гэх мэт индикатор эх сурвалжаас цуглуулж 2025 оны 01 дүгээр сараас 12 дугаар сар хүртэлх хугацаанд долоо хоног тутам кибер аюул заналын нөхцөл байдлын тандалт, дүн шинжилгээ хийж, тайланг долоо хоног бүр тогтмол Мэдээлэл, дүн шинжилгээний газарт хүргүүлэн ажилласан. Нийт 65 тайлан хүргүүлсэн байна. Open Threat Exchange/OTX/ системийг судалж, тандалтын эх сурвалжид нэмсэн.	100%
38	Арга хэмжээ 8.5. Жижиг, дунд бизнесийн байгууллагуудад ашиглаж болохуйц кибер аюулгүй байдлын SOC-н систем хөгжүүлэх, нэвтрүүлэх, хянах;	Улсын төсвийн санхүүжилт	Нэгдсэн систем хөгжүүлсэн тоо	-	1	Жижиг, дунд бизнесийн байгууллагуудад зориулсан кибер аюулгүй байдлын нэгдсэн хамгаалалтын системийг бүрдүүлэх ажлын хүрээнд байгууллагуудын SIEM системтэй холбоотой хүндрэл, тусгай программ хангамжийн өндөр зардал, мэргэжлийн хүний нөөцийн дутагдлыг шийдвэрлэх зорилгоор Wazuh-д суурилсан цогц шийдлийг боловсруулж, хэрэгжилтийг ханган ажиллав. Тус ажлын хүрээнд Wazuh системийг нарийвчлан судалж, тохиргоо, логийн хяналт, сэрэмжлүүлгийн механизмыг байгууллагуудын хэрэгцээнд нийцүүлэн нэгдсэн байдлаар ашиглах боломжтой загвар орчныг бүрдүүлсэн. Уг шийдэлд тохиргооны дэлгэрэнгүй заавар, ашиглалтын зөвлөмж, бодит хэрэглээнд суурилсан жишээ, аргачлалуудыг багтааж, нийтэд нээлттэй, төвлөрсөн байдлаар ашиглагдах боломжтой хэлбэрээр боловсруулан 2025 оны 08 дугаар сарын 15-ны өдөр газрын даргад танилцуулсан. Мөн таван байгууллагын орчинд honeypot системийг байршуулж, дотоод сүлжээнд үүсэх сэжигтэй үйлдлүүд болон гадаад орчноос чиглэсэн халдлагын оролдлогуудыг илрүүлэх	100%

						туршилтын орчныг амжилттай бүрдүүлсэн. Үүний үр дүнд жижиг, дунд бизнесийн байгууллагууд бодит халдлагын хэв маяг, зан төлөвийг илүү нарийвчлан ойлгох, кибер эрсдэлийг бууруулах, хамгаалалтын бодлого, дүрэм журмыг тасралтгүй сайжруулах боломж бүрдсэн болно.	
39	Арга хэмжээ 8.6. Төвийн дотоод мэдээллийн аюулгүй байдлыг хангах, чадавхыг сайжруулах;	Улсын төсвийн санхүүжилт	Нэвтрүүлсэн тоо	-	Хэрэгжилтээр	1.Төвийн хэмжээнд нийтээр ашиглах Passbolt нууц үгийн менежментийн системийг 2025 оны 04 дүгээр сард ашиглалтад оруулсан. 2.Нийт ажилтнуудад нийтийн түлхүүрийн дэд бүтэц (PKI)-ийг ашиглан шифрлэсэн цахим шуудан солилцох талаар сургалтыг 2025 оны 04 дүгээр сарын 07-ны өдөр зохион байгуулж, байгууллагын хэмжээнд бүрэн хэрэгжүүлж, үйл ажиллагаандаа ашиглаж байна.	100%

Тайланг хянасан: **Төсвийн Ерөнхийлөн захирагч**

ЦАХИМ ХӨГЖИЛ, ИННОВАЦ,
ХАРИЛЦАА ХОЛБООНЫ САЙД ..... /Э.БАТШУГАР/

2025 оны 12 дугаар сарын 30.

Төлөвлөгөөг тайлагнасан: **Төсвийн Шууд захирагч**

"КИБЕР ХАЛДЛАГА, ЗӨРЧИЛТЭЙ ТЭМЦЭХ НИЙТИЙН ТӨВ"
УЛСЫН ТӨСӨВТ ҮЙЛДВЭРИЙН ГАЗРЫН ЗАХИРАЛ ..... /Э.АМАРСАНАА/

2025 оны ..... дугаар сарын .....