БНХАУ болон ОХУ-ын кибер аюулгүй байдлыг хангах, хиймэл оюуныг хөгжүүлэх талаар хэрэгжүүлж буй бодлого, үйл ажиллагаа, тулгарч буй сорилтууд

Л.Энхцэцэг[1], Л.Оюунцэцэг[2]

[1]Цэргийн төв эмнэлгийн Холбоо, мэдээллийн алба
[2]Их засаг олон улсын их сургуулийн Үндэсний инженер, технологийн сургууль

Key words:
cyber security, cyber attack, cyber crime, Artificial Intelligence.

Abstract: In the era of the 4th and 5th revolutions in information technology and industry, the world has not yet been able to control its cyberspace. For this reason, cybersecurity is not only inextricably linked to the national security of any country, but also one of the most pressing issues that poses the greatest risk. Countries are developing their legal and regulatory environments to ensure cybersecurity, while also developing cooperation with neighboring countries and regions. In addition, artificial intelligence is increasingly being used to ensure cybersecurity.

Оршил

Сүүлийн жилүүдэд хиймэл оюун нь улс орны нийгэм, эдийн засаг, шинжлэх ухаан, технологи, батлан хамгаалах, аюулгүй байдал зэрэг бүхий л салбарт өргөн нэвтэрч, түүнийг үндэсний аюулгүй байдлыг хангахад ашиглах шинэ нөхцөл байдал бий болоод байна[1].

Кибер аюулгүй байдал ба хиймэл оюун (Artificial Intelligence, AI) нь мэдээллийн системийг хамгаалах, эмзэг байдлыг илрүүлэх, халдлагаас урьдчилан сэргийлэх, хариу үйлдэл үзүүлэх зорилгоор хиймэл оюуны хөгжүүлэлтийг ашигласан технологийн хувьд инновацын цогц систем юм. Энэхүү цогц систем нь дараах онцлогуудтай. Үүнд:

- Хиймэл оюун ашиглан кибер халдлага илрүүлэх, түүн дээр үндэслэн автомат хариу үйлдэл үзүүлэх чатботыг хөгжүүлэн нэвтрүүлэх, сэжигтэй өгөгдлийг шинжлэх;
- Системийн баталгаат байдал, хамгаалалт, халдлагаас урьдчилан сэргийлэх, халдлага илрүүлэх;
- Технологийн орчинд машин сургалт, өгөгдлийн шинжилгээ, нэгдсэн системийн автоматжуулалт, үүлэн системийг оновчтой ашиглах зэрэг болно.

Үндсэн хэсэг

Нэг. БНХАУ болон ОХУ-ын кибер аюулгүй байдлыг хангах, хиймэл

[1] *Аюулгүй байдал судлалын хүрээлэн. (2025.4.29). “Хиймэл оюун ухаан - аюулгүй байдал ба ёс зүй” долоо хоногийн тойм. https://niss.gov.mn/archives/4040;*

оюуныг хөгжүүлэх талаар хэрэгжүүлж буй бодлого

БНХАУ бол дэлхийн хамгийн олон хүн амтай, янз бүрийн үндэстэн ястан, зан заншил холилдсон 5000 гаруй жилийн соёл иргэншлийн түүхтэй том гүрэн бөгөөд 9 сая 600 мянган хавтгай дөрвөлжин километр квадрат нутаг дэвсгэртэй, 56 үндэстнээс бүрдсэн нийт 1,409 тэрбум хүн амтай[2].

Хятадын интернэт, сүлжээний мэдээллийн төв (China Internet Network Information Center, CNNIC) 2023 оны 12 сарын байдлаар Хятадын интернэт хэрэглэгчдийн тоо 1.092 тэрбумд хүрч, өмнөх оны мөн үеэс 24.8 саяар нэмэгдэж, интернэтийн нэвтрэлтийн түвшин 77.5% буюу 1.9 пунктээр өссөн гэж 2024 оны 3 сард мэдээлсэн. Үүнээс 1.091 тэрбум нь гар утсаараа интернэтэд холбогдсон нь интернэт хэрэглэгчдийн 99.9 хувийг эзэлж байна. Хөдөө орон нутгийн интернэт хэрэглэгчдийн 29.8% буюу 326 сая, хотын хэрэглэгчид 70.2% буюу 766 сая байна[3].

Дэлхийн хамгийн олон интернэт хэрэглэгчтэй Хятад улсад кибер гэмт хэргийн тоо жилээс жилд нэмэгдэж буй сорилтуудтай тулгарч байна. Хятадад гарч буй гэмт хэргийн 1/3 нь цахим гэмт хэрэг байгаа бөгөөд энэ нь жилдээ 30%-ийн өсөлттэй, жилд 95 тэрбум юаний алдагдалтай байгаа гэсэн мэдээлэл бий. Жишээ нь, 2016 онд Хятадын интернэтийн аюулгүй байдлын Qihoo компани 70,000 гар утас дээрэмдэх оролдлого, 197 сая фишинг халдлага, 20,000 нь мөнгөний алдагдал, Хятад дахь андройд утасны 99,99% нь аюулгүй байдлын сул талыг мэдээлснээр үзэхэд кибер гэмт хэрэг нь Хятадад хамгийн түгээмэл гэмт хэргийн төрөл болоод байна. Кибер гэмт хэрэг нь виртуал орон зай, бодит орон зайн аль алиныг нь холбоод зогсохгүй хил дамнасан шинжтэй болж байгаа тул олон улсын хамтын ажиллагааг улам илүү шаардаж байна.

БНХАУ нь 2022 онд 342,000 гаруй кибер халдлагад өртөж, эдгээр халдлагад Засгийн газар, цэрэг батлан хамгаалах, тагнуул, улс төрийн болон цэргийн нууц мэдээлэлд хууль бусаар хандах, хулгайлахад чиглэгдсэн. Санхүүгийн байгууллагуудын хувьд кибер залилан давамгайлж байна. Технологи ба харилцаа холбооны салбарт оюуны өмчийг хулгайлах, эрчим хүчний сүлжээ, газрын тос, байгалийн хийн салбаруудыг хяналтандаа авах эсвэл үйлчилгээг тасалдуулах, дотоодын үйлдвэрлэлийн хөгжүүлэлтэд оюуны өмч хулгайлах, хорлон сүйтгэх зэргээр зарим чухал үйлчилгээг тасалдуулахад чиглэгдсэн байна. Нэмж дурдахад, тус улсад интернэтийн гэмт хэрэг 850 тэрбум ам.долл.-т хүрсэн байна[4].

---

[2] Дашдорж, П., Сугар, Г. (2025). БНХАУ-ын үндэсний эв нэгдлээ хангах талаар хэрэгжүүлж байгаа бодлого, сорилт. -УБ., “Аюулгүй байдал, батлан хамгаалах судлал” сэтгүүл., № 39(49), ISSN: 2220-9115., х. 5-16;

[3] China Innovation Watch. (2024). https://www.ciw.news/p/china-internet-overview;

[4] Min Jiang. (2024). Cybersecurity Policies in China., https://www.researchgate.net/publication/348225744_Cybersecurity_Policies_in_China/ DOI: 10.1007/978-3-030-56405-6_5;

Хятадын халдлагад хариу үйлдэл үзүүлэх баг (CERNET Computer Emergency Response Team, CCERT) 2024 онд 2,573 аюулгүй байдлын будлианыг илрүүлсний 700 дотоодынх, 1,493 нь гадаадаас урсгалаас халдсан байна. Хятадын компьютер сүлжээний хадлагад хариу үйлдэл үзүүлэх боловсрол, судалгааны баг (China Education and Research Computer Network Emergency Response Team, CERNET) дээрх будлианы 379 тохиолдлыг системийг аюулгүй байдлыг хянах (Security Monitoring System) замаар илрүүлсэн байна[5].

Удирдлага, зохион байгуулалт: Хятадын Коммунист Намын Төв Хороо нь тус улсын шийдвэр гаргах дээд байгууллага бөгөөд тус төв хороо нь улс төрийн үзэл баримтлалыг тодорхойлж, үндэсний бодлого, тэргүүлэх чиглэлийг удирдан чиглүүлдэг. Төрийн эрх барих дээд байгууллага болох Төрийн зөвлөл нь ХКН-д харьяалагддаг бөгөөд Төв Хорооноос тогтоосон үүрэг чиглэлийн кибер аюулгүй байдлыг хангах ажлыг ажилладаг. ХКН-ын Төв хорооны дэргэдэх Хятадын Үндэсний аюулгүй байдлын хороо, Мэдээллийн аюулгүй байдлын төв, түүнчлэн цагдаа, тагнуулын байгууллагууд кибер орон зайн эмзэг байдлыг бууруулах, кибер халдлагыг илрүүлэх, таслан зогсоох, сэргээх, урьдчилан сэргийлэх арга хэмжээг авч байна[6]. Тухайлбал, тус улс батлан хамгаалах идэвхтэй стратегийг хэрэгжүүлэхдээ “улс оронд тулгарч буй үндэсний аюулгүй байдлын нийтлэг аюулд идэвхтэй хариу арга хэмжээ авах” гэсэн зорилтыг дэвшүүлсэн байна[7].

Хууль, эрх зүйн орчин: 2017 онд батлагдсан “Кибер аюулгүй байдлын тухай” хууль нь Хятадын кибер аюулгүй байдлыг хангах, эрх зүйн харилцааг зохицуулдаг хамгийн чухал, суурь хууль юм. Энэ хууль нь улс орныхоо мэдээллийн аюулгүй байдлыг хангах, сүлжээний хяналтын арга хэмжээнүүдийг авах, цахим орчинд иргэд, байгууллагын эрх ашгийг бүрэн хангах зорилготой бөгөөд мэдээллийн аюулгүй байдлын стандартыг тогтоох, цахим мэдээллийн хамгаалалтыг эрчимжүүлэхэд чиглэсэн. Түүнчлэн мэдээллийн чухал дэд бүтцийн оператор (Critical Information Infrastructure, CII)-уудад хатуу үүрэг хариуцлага хүлээлгэж, CII бус операторуудыг ижил төстэй дүрмийг дагаж мөрдөхийг уриалж, бүх онлайн үйлчилгээ үзүүлэгчдийн төрийн хяналтыг үр дүнтэйгээр өргөжүүлдэг[8].

---

[5] *APCERT report. (2024). https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2024.pdf., т61;*

[6] *Cybersecurity with Chinese characteristics. Digital governance in the Indo-Pacific and the Taiwanese alternative. (2025). ARTICLE 19, 2025 (Creative Commons License 4.0)., www.article19.org;*

[7] *Паламдорж, Ш. (2024). Батлан хамгаалах судлал. Онол, практикийн асуудлаарх эрдэм шинжилгээний өгүүллийн эмхэтгэл., Бүгд Найрамдах Хятад Ард Улсын батлан хамгаалах номлолын хувьсал өөрчлөлт., -УБ., “Соёмбо принтинг” ХХК., ISBN: 978-9919-0-293-1., х. 54-57;*

[8] *Cybersecurity with Chinese characteristics. Digital governance in the Indo-Pacific and the Taiwanese alternative. (2025). ARTICLE 19, 2025 (Creative Commons License 4.0)., www.article19.org;*

“Үндэсний тагнуулын тухай /шинэчилсэн найруулга/” хууль 2017 онд шинэчилсэн найруулгаар батлагдсан бөгөөд хувь хүн, байгууллагууд, тэр дундаа гадаад дахь технологийн фирмүүд тагнуулын үйл ажиллагаа, мэдээлэл цуглуулах, төр, байгууллагын болон хувийн нууцад хууль бусаар халдах, тандах ажиллагааг явуулах зэрэг эрх зүйн харилцааг зохицуулдаг[9].

Хятадын Засгийн газар 2016 онд баталсан “Хятадын кибер аюулгүй байдлын үндэсний стратеги” энэ нь үндэсний аюулгүй байдлыг хангах, тус улсын кибер орон зайг хамгаалах, мэдээллийн технологийг дэвшилтэт тэргүүлэгч салбар болгон хөгжүүлэх, кибер хүчин чармайлтыг бэхжүүлэх, цахим эдийн засгийг өргөжүүлэх зорилготой. Энэхүү үндэсний стратегийн үндсэн зорилт нь

- Мэдээллийн эдийн засгийг хамгаалах;
- Хувийн мэдээллийн аюулгүй байдлыг хангах;
- Гадны халдлагаас урьдчилан сэргийлэх, хариу үйлдэл үзүүлэх;
- Төр, бизнес, иргэдийн хоорондын хамтын ажиллагааг зохицуулах зэрэгт чиглэгдэж байна.

“Интернэтийн гадаад хяналт, зохицуулалтын стандарт”-ыг 2017 онд[10], “Гадаад байгууллага, интернэт үйлчилгээ эрхлэгчдэд тавигдах шаардлага” стандарт 2021 онд, мөн 2022 онд “Гадаад иргэд, аж ахуйн нэгжийн интернэтийн нэвтрэлтийг хянах журам” зэргийг батлан гарган мөрдөгдөж байна.

Нэмж дурдахад, дижитал торгоны зам[11] нь 2014 оны 11 сард батлагдсан “МХХТ-ийн чиглэлээр харилцаатай улс орнуудын хоорондын инфраструктурын бүтээн байгуулалтын төлөвлөгөө (MIIT’s plan for the Construction of Interconnected Infrastructure in Surrounding Countries)-ний нэг хэсэг юм.

2015 оны 3 сард Үндэсний хөгжлийн ба төслийн комисс (НДТТК)-оос батлан гаргасан “Бүсийн эдийн засгийн зам ба XXI зууны тэнгисийн цэргийн хамтарсан бүтээн байгуулалтыг дэмжих үзэл баримтлал” баримт бичиг нь хил хязгаарын чухал сүлжээнүүдийн бүтээн байгуулалтыг түргэтгэн, МХХТ хамтын ажиллагааг өргөжүүлэхийг Вьетнам, Индонез зэрэг Зүүн өмнөд Азийн орнуудад уриалсан.

ХКН-аас 2016 онд батлан гаргасан “Үндэсний мэдээлэлжүүлэлт 13 дахь таван жилийн төлөвлөгөө (13th Five-Year Plan for National Informatization)-нд тус улсын кибер аюулгүй байдлын талаар баримталж буй бодлогын зорилго нь АСЕАН-ы орнуудтай хамтын ажиллагаагаа өргөжүүлэн хөгжүүлэхэд чиглэгдэж, мөн оны 11 сард зохион байгуулсан “АСЕАН-Хятад” дээд

[9] *Мөн тэнд;*

[10] *Internet External Control and Regulation Standards;*

[11] *Digital Silk Road;*

хэмжээний чуулган уулзалтын үеэр “ASEAN–China Strategic Partnership Vision 2030” баримт бичгийг баталсан[12].

БНХАУ Индонез, Пакистан зэрэг 49 оронтой “Бүс ба Зам” хоёр дахь чуулга уулзалтыг 2019 онд зохион байгуулж, 85 орчим техникийн стандартын гэрээ байгуулсан. БНХАУ 2023 оны 10 сард зохион байгуулагдсан “Бүс ба Зам” гурав дахь чуулга уулзалтын үеэр дэлхийн дижитал засаглалын дүрэм, тэр дундаа кибер аюулгүй байдлын засаглалыг боловсруулсан нь тус улс энэ чиглэлээр манлайлах зорилгыг нотолж байна. Энэхүү зорилго нь “Дижитал торгоны зам”-ын тэргүүлэх чиглэлүүдтэй уялдан хөгжиж байна. Тухайлбал, БНХАУ-ын Үндэсний эдийн засаг, нийгмийг хөгжүүлэх XIV таван жилийн төлөвлөгөө (2021-2025 он), БНХАУ-ын 2035 он хүртэлх алсын хараа[13], кибер аюулгүй байдлын өнөөгийн нөхцөл байдал, хэтийн төлөвлөлтөд анхаарлаа хандуулж, кибер орон зай дахь үүргээ бэхжүүлэх хүсэл эрмэлзэлтэй байгаагаа илэрхийлсэн.

Хоёр: ОХУ-ын кибер аюулгүй байдлыг хангах, хиймэл оюуныг хөгжүүлэх талаар хэрэгжүүлж буй бодлого

ОХУ нь дэлхийн хамгийн том болох 17,075,400 хавтгай дөрвөлжин километр газар нутагтай, хүн амын тоогоороо 8 дугаарт ордог улс юм. Тус улс 2022 оны байдлаар 143 сая хүнтэй[14].

2024 оны эхний улирлын байдлаар ОХУ-д 130.4 сая интернэт хэрэглэгчтэй, интернэтийн нэвтрэлт 90.4 хувьтай байна. Нийгмийн сүлжээний 106.0 сая хэрэглэгчтэй байгаа нь хүн амын 73.5% эзэлж байгаа бол 219.8 сая гар утасны хэрэглэгч нь 152.5 хувьтай тэнцэж байна[15].

Ташрамд дурдахад, 2024 оны 11 сарын байдлаар тус улсын төрийн байгууллагууд руу чиглэсэн DDoS (Distributed Denial-of-Service) халдлага 355,000 илэрсэн нь 2023 оноос хойш 16%-аар өсжээ[16].

Хууль, эрх зүйн орчин: “Мэдээллийн аюулгүй байдлын тухай” хууль 2020 онд шинэчлэн батлагдсан бөгөөд энэ хуулийн зорилго нь кибер аюулгүй байдлыг хангах, орон нутгийн бүх мэдээллийн системийг хамгаалах тухайлбал, зөвшөөрөлгүй нэвтрэлт, халдлагаас хамгаалах, цахим халдлага, террорист үйл ажиллагааг хязгаарлах, мэдээллийн эрх зүйн орчныг боловсронгуй болгоход чиглэгдсэн.

“Хэрэглэгчийн эрхийг хамгаалах тухай” Холбооны хууль (ОХУ-ын хууль

---

[12] *Cybersecurity with Chinese characteristics. Digital governance in the Indo-Pacific and the Taiwanese alternative. (2025). ARTICLE 19, 2025 (Creative Commons License 4.0)., www.article19.org;*

[13] *2035 оны 3 сарын 20-нд нээлтээ хийсэн;*

[14] *https://mn.wikipedia.org/wiki/%D0%9E%D1%80%D0%BE%D1%81;*

[15] *DIGITAL 2024: THE RUSSIAN FEDERATION. (2024). https://datareportal.com/reports/digital-2024-russian-federation;*

[16] *Мөн тэнд;*

No 2300-I) анх 1992 онд батлагдаж, 2024 оны 7 дугаар сард нэмэлт өөрчлөлт оруулсан. Энэ хууль нь хэрэглэгчийн эрхийг хамгаалах, интернэт үйлчилгээ үзүүлэгч байгууллага болон онлайн үйлчилгээ үзүүлэгчийн хүлээх үүрэг хариуцлага, хэрэглэгчийн мэдээллийг хамгаалах, зөвшөөрөлгүй мэдээлэл (хууль бус агуулга бүхий худал ташаа мэдээ, төөрөгдүүлсэн мэдээлэл)-ийг мэдээлэх, хязгаарлах, нийгмийн сүлжээгээр тараахыг хориглох, блоклох, устгах зэрэг эрх зүйн харилцааг зохицуулдаг.

2017 онд батлагдсан “Кибер аюулгүй байдлын үндэсний стратеги”-ийн зорилго нь тус улсын кибер орчны аюулгүй байдлыг хангах, үндэсний аюулгүй байдлыг хамгаалах, цахим орчинд төрийн болон төрийн бус байгууллагууд, иргэдийн цахим ур чадавхыг нэмэгдүүлэхэд оршино. Энэхүү үндэсний стратеги нь дараах зорилтыг дэвшүүлсэн байна. Үүнд:

1. Кибер халдлагыг илрүүлэх, таслан зогсоох, хариу үйлдэл хийх чадавхыг бэхжүүлэх;
2. Кибер орчны найдвартай хамгаалалтыг хангах;
3. Кибер гэмт хэрэг, будлианыг илрүүлэх, шалгах, хууль хяналтын механизмыг боловсронгуй болгох;
4. Кибер орчинд улс, компани нэр хүндийг хамгаалах, эдийн засаг, үндэсний аюулгүй байдлыг хангах.

ОХУ нь кибер аюулгүй байдлыг хангах чиглэлээр олон байгууллага хамтран ажилладаг бөгөөд Холбооны аюулгүй байдлын алба (ФСБ) нэгдсэн хяналт тавьдаг. Түүнчлэн Цахим хөгжлийн яам, Кибер аюулгүй байдлын төв зэрэг байгууллагууд хариуцдагаас гадна Тагнуулын байгууллага, Дотоодын цэргийн хүчний кибер салбар зэрэг байгууллагууд ч оролцдог.

Роскомнадзор (Federal Service for Supervision of Communications, Information Technology and Mass Media) нь 2008 онд байгуулагдсан, ОХУ-ын мэдээллийн салбарын үндсэн хяналт тавьдаг гол байгууллага юм. Энэ байгууллага нь нь интернэтийн орчинд хяналт тавьж, аюулгүй байдлыг хангах, хууль зөрчсөн мэдээллийг шалгах, тэдгээрийг арилгах, зохицуулах үүрэгтэй[17]. Тухайлбал:

- Веб сайт, агуулга, цахим мэдээллийн аюулгүй байдал, интернэт дэх зөвшөөрөлгүй мэдээллийг хянах, зохицуулах, сэрэмжлүүлэг өгөх;
- Цахим халдлагаас хамгаалах, кибер аюулгүй байдлыг хангах зэрэг болно.

ОХУ нь 2019 оноос эхлэн үндэсний интернэтийн шифрлэлт “RU-NET”-ийг ашиглан мэдээллийн урсгал, хэрэглээний хяналт бүхий интернэтийн аюулгүй байдлын системийг үүсгээд байна[18].

[17] *Russia Ramps Up Cybersecurity Systems. (2025.2.6). https://jamestown.org/program/russia-ramps-up-cybersecurity-systems/;*

[18] *Russia Ramps Up Cybersecurity Systems. (2025.2.6). https://jamestown.org/program/rus-*

Гурав. Кибер аюулгүй байдал хийгээд хиймэл оюуны хосолмол хамтын ажиллагаа

Хятадын Засгийн газраас 2010-аад оны сүүлээр боловсруулсан “Хүчирхэг цахим улс” (Strong Cyber Power) бодлого нь мэдээллийн технологийн салбарыг үндэсний аюулгүй байдал, эдийн засаг, боловсрол, байгаль орчин зэрэг нийгмийн бүхий л салбарт өргөжүүлэх зорилготой[19]. Энэхүү бодлогын гол тулгуур хөгжүүлэх тэргүүлэх чиглэлд хиймэл оюун багтдаг бөгөөд Хятадын удирдагчид 2030 он гэхэд дэлхийд хиймэл оюунаар тэргүүлэх орон болох зорилгыг зарласан. Үүнд:

- Технологийн тэргүүлэх байр суурь болох цахим шилжилт, робот, автоматжуулалт, хиймэл оюуны системүүдийг боловсронгуй болгох.
- Ухаалаг хяналтын систем, интернэтийн аюулгүй байдал, хиймэл оюуны боловсрол, судалгаа, инновацыг хөгжүүлэх.
- АНУ, Европын холбооны технологи, инновацын салбарт өрсөлдөх чадвараа дээшлүүлэх зэрэг болно.

Хятадын Засгийн газраас 2017 онд батлан гаргасан “Шинэ үеийн хиймэл оюуныг хөгжүүлэх төлөвлөгөө (Next Generation AI Development Plan)”-нд энэ чиглэлийн судалгаа, хөгжүүлэлтийн үндэсний төвүүдийг байгуулах, олон улсын хамтын ажиллагааг өргөжүүлэх, инновацын дэд бүтцийг байгуулах зорилготой ажиллаж эхэлснээр тус улсад “Үндэсний хиймэл оюуныг хөгжүүлэх төв (National New Generation Artificial Intelligence Innovation Development Strategy Advisory Committee) байгуулагдсан гэж үзэж болно. Энэхүү төв нь юмсын интернэт (Internet of Thing, IoT)-д суурилсан ухаалаг хэрэглээний программууд, робот, машин сургалтыг хөгжүүлэх, хүний эрхийг хүндэтгэсэн хиймэл оюуны ёс зүй зэргээр эрдэм шинжилгээ, судалгааны ажил явуулдаг[20].

Түүнчлэн тус улсад Хиймэл оюуны академи (Academy of Artificial Intelligence), BAAI (Beijing Academy of Artificial Intelligence)[21] зэрэг олон байгууллага үйл ажиллагаа явуулж байна.

Эдгээр судалгааны байгууллага нь улсын болон орон нутгийн санхүүжилтээр судалгаа хөгжүүлэлтийн ажил явуулах, инновацыг дэмжих хэд хэдэн хөтөлбөр хэрэгжүүлж байгаагийн нэг жишээ нь “Шинэ үеийн хиймэл оюуныг хөгжүүлэх төлөвлөгөө” юм.

ОХУ, БНХАУ 2010 онд үндэсний аюулгүй байдал, инновацын салбаруудад хамтран ажиллах тухай гэрээ хэлэлцээрүүд хийсэн. Мөн Орос-Хятадын хамтын ажиллагааны стратегийн хамтын ажиллагааны чадавхыг

sia-ramps-up-cybersecurity-systems/;

[19] *The Chinese State Council Official Website;*

[20] *National People's Congress of China;*

[21] *2018 онд байгуулагдсан;*

нэмэгдүүлэх гэрээг 2014 онд баталсан. Эдгээр хамтын ажиллагаа нь дараах гол чиглэлүүдийг хамарч байна. Үүнд

- Хиймэл оюун, мэдээлэл технологи;
- Кибер аюулгүй байдал, мэдээллийн системийн хамтын ажиллагаа;
- Эдийн засгийн хамтын ажиллагаа, судалгаа, инновац зэрэг болно.

Хятадын кибер орон зайн хяналт, кибер аюулгүй байдлыг хангах байгууллагууд 2017 онд Оросын Роскомнадзортой хамтран ажиллах гэрээ байгуулсан.

Өдгөө Хятад, Оросын Засгийн газраас эрдэмтэн судлаачдын хамтарсан технологийн судалгаа хөгжүүлэлтийг дэмжихэд түлхүү анхаарч байна. Тухайлбал: хамтарсан судалгааны төвүүд байгуулж, хиймэл оюун, кибер аюулгүй байдал зэрэг салбаруудад хамтран ажиллаж байна. Мөн Төвөд, Алс Дорнод зэрэг бүс нутгуудад хамтарсан төслүүд хэрэгжүүлж байна.

Дүгнэлт

Сүүлийн жилүүдэд хиймэл оюун нь нийгмийн бараг бүх салбарт нэвтэрч, түүнд тулгуурлан кибер аюулгүй байдлыг хангахад ихээхэн хөрөнгө оруулалт хийгдэж байна. Машин сургалт (Machine learning), гүн сургалт (deep learning), ухаалаг агентууд (Intelligent agents) зэрэг технологийг хөгжүүлснээр кибер аюулгүй байдлын асуудлуудыг үр ашигтай шийдвэрлэх боломж бүрдэж, улс орнууд ч хамтарсан судалгаа хөгжүүлэлтийн ажлуудыг явуулж байна.

Орос, Хятад улс хамтран олон улсын цахим хууль зүйн шинэчлэл, шинэ стандарт боловсруулах ажлын хүрээнд кибер аюулгүй байдал хийгээд хиймэл оюуныг хамтран хөгжүүлэх зорилго бүхий нийтлэг стратеги боловсруулж байгаа нь түүний нэг жишээ юм.

Хиймэл оюуны тусламжтайгаар өндөр хурд, нарийвчлалтай тооцоолол хийж, асар их хэмжээний өгөгдлийг бодит цагт шинжлэх чадвар бий болоод байна[22]. Цэргийн ажиллагаа, батлан хамгаалах стратегид хиймэл оюуныг нэвтрүүлж байгаа нь бие даасан системийн дэвшил, мэдээллийн дүн шинжилгээ, аюул заналыг үнэлэх зэрэг орчин үеийн дайнд мэдэгдэхүйц өөрчлөлтийг авчирч байна. Эдгээр технологи нь тагнуул, логистик, шийдвэр гаргах үйл явцыг автоматжуулж, хүний амь насанд учрах эрсдэлийг бууруулах, шийдвэр гаргалтыг оновчтой болгох, үйл ажиллагааны үр ашгийг дээшлүүлэх боломжтой. Гэсэн хэдий ч автоматжуулсан процесст хэт найдлага тавих нь хариуцлагын зөрчил болон тэр дундаа мөргөлдөөнтэй бүс нутагт хүсээгүй үр дагаварт хүргэж болзошгүй[23].

---

[22] *Мэдээллийн аюулгүй байдал. https://www.isd.gov.mn/a/33;*

[23] *Аюулгүй байдал судлалын хүрээлэн. (2025.4.29). “Хиймэл оюун ухаан - аюулгүй байдал ба ёс зүй” долоо хоногийн тойм. https://niss.gov.mn/archives/4040;*

Кибер аюулгүй байдалд хиймэл оюун ашиглахын зарим ач тусыг дурдвал[24]:

1. Хиймэл оюуны шийдлүүд нь сүүдрийн өгөгдлийг тодорхойлж, өгөгдөлд хандах хэвийн бус байдлыг хянах, өгөгдөл эсвэл нууц мэдээлэлд хандсан хүн бүрт тулгарч болзошгүй эрсдэлийн талаар кибер аюулгүй байдлын мэргэжилтнүүдэд сэрэмжлүүлэх, бодит цаг хугацаанд асуудлыг илрүүлэх боломжтой болгодог.

2. Хиймэл оюуны технологи нь сүлжээний эмзэг байдлыг бууруулах, кибер гэмт хэргийг илрүүлэх, хамгаалах, урьдчилан сэргийлэх арга хэмжээ авахад тусална.

3. Хиймэл оюуны загварууд нь системд зөвшөөрөлгүй нэвтрэх оролдлого бүрийн эрсдэлд дүн шинжилгээ хийж, хувийн мэдээллээр дамжуулан хэрэглэгчийг баталгаажуулах зэргээр аюулгүй байдлыг тэнцвэржүүлэх боломжтой.

Эшлэл авсан сурвалж, судалгааны бүтээл

1. Аюулгүй байдал судлалын хүрээлэн. (2025.4.29). “Хиймэл оюун ухаан - аюулгүй байдал ба ёс зүй” долоо хоногийн тойм. https://niss.gov.mn/archives/4040;
2. Дашдорж, П., Сугар, Г. (2025). БНХАУ-ын үндэсний эв нэгдлээ хангах талаар хэрэгжүүлж байгаа бодлого, сорилт. -УБ., “Аюулгүй байдал, батлан хамгаалах судлал” сэтгүүл., № 39(49), ISSN: 2220-9115., х. 5-16;
3. China Innovation Watch. (2024). https://www.ciw.news/p/china-internet-overview;
4. Min Jiang. (2024). Cybersecurity Policies in China., https://www.researchgate.net/publication/348225744_Cybersecurity_Policies_in_China/ DOI: 10.1007/978-3-030-56405-6_5;
5. APCERT report. (2024). https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2024.pdf., т61;
6. Cybersecurity with Chinese characteristics. Digital governance in the Indo-Pacific and the Taiwanese alternative. (2025). ARTICLE 19, 2025 (Creative Commons License 4.0)., www.article19.org;
7. Паламдорж, Ш. (2024). Батлан хамгаалах судлал. Онол, практикийн асуудлаарх эрдэм шинжилгээний өгүүллийн эмхэтгэл., Бүгд Найрамдах Хятад Ард Улсын батлан хамгаалах номлолын хувьсал өөрчлөлт., -УБ., “Соёмбо принтинг” ХХК., ISBN: 978-9919-0-293-1., х. 54-57;
8. DIGITAL 2024: THE RUSSIAN FEDERATION. (2024). https://datareportal.com/reports/digital-2024-russian-federation;
9. Russia Ramps Up Cybersecurity Systems. (2025.2.6). https://jamestown.org/program/russia-ramps-up-cybersecurity-systems/;
10. IStories, Süddeutsche Zeitung: Russia’s censorship agency monitors negative com-

[24] *ШУА. МТТХ. Кибер аюулгүй байдал дахь хиймэл оюуны хэрэглээ. 2023.11.24. https://imdt.ac.mn/post/17868;*

ments about Putin and his health online and keeps track of protest attitudes. (9 February, 2023). https://novayagazeta.eu/articles/2023/02/08/istories-suddeutsche-zeitung-russias-censorship-agency-monitors-negative-comments-about-putin-and-his-health-online-and-keeps-track-of-protest-attitudes-en-news: In February 2023, it was revealed that Belarusian Cyberpartisans had hacked and leaked Roskomnadzor data to journalists. The leak exposed surveillance and censorship programs and ways to discredit journalists;

11. The Chinese State Council Official Website;
12. National People’s Congress of China;
13. Мэдээллийн аюулгүй байдал. https://www.isd.gov.mn/a/33;
14. ШУА. МТТХ. Кибер аюулгүй байдал дахь хиймэл оюуны хэрэглээ. 2023.11.24. https://imdt.ac.mn/post/17868.