DEFENSE RESEARCH INSTITUTE OF MONGOLIA

Journal of Security and Defense Studies

Journal homepage:
https://mids.gov.mn/category/ayulgui_baidal-2/

ISSN: 2220-9115, E-ISSN: 2708-1230

Research Article

DOI: https://doi.org/10.65816/jsds.2026.01.022

Cybersecurity Issues in Smart Energy-Efficient Systems

Batjargal Dolgormaa[1], Boldbaatar Luwsanwaanjil[2]

[1] *M.A., Second lieutenant, Information technology specialist, Defense Research Institute of Mongolia*
E-mail address: dolgormaa@mids.gov.mn, ORCID:0009-0004-4847-5942

[2] *Second lieutenant, Company Commander, Military Unit No. 013, Armed Forces*
E-mail address: waanjilw@gmail.com, ORCID: 0009-0006-2951-7865

Received: 13 February 2026 *Revised: 15 March 2026*
Accepted: 24 March 2026 *Published online: 30 March 2026*

ABSTRACT

In recent years, smart energy-efficient systems have undergone rapid development, and as their adoption continues to expand, the risk of exposure to cyberattacks has increased accordingly. Within the scope of this study, the most common types of cyberattacks targeting smart devices were identified, and potential preventive and protective measures were analyzed and evaluated. Furthermore, a smart energy-efficient system, a web-based platform for system management, and source code for detecting Distributed Denial-of-Service (DDoS) attacks were designed and developed, followed by validation through simulation and laboratory-based experiments. By assembling and testing a smart device in a real-world environment, this study experimentally demonstrates the feasibility of system modeling, web platform integration, and the implementation of software capable of detecting cyberattacks targeting the device.

Keywords: *Smart Energy-Efficient System, Cyberattack, Cybersecurity Protection Methods, Intrusion Detection Software, Hardware Testing, Internet of Things (IoT).*

Эрчим хүч хэмнэлтийн ухаалаг системийн кибер аюулгүй байдлыг хангах зарим асуудал

Батжаргал Долгормаа[1], Болдбаатар Лувсанваанжил[2]

[1]*Батлан хамгаалахын эрдэм шинжилгээний хүрээлэнгийн Мэдээлэл, технологийн мэргэжилтэн, магистр, дэслэгч, dolgormaa@mids.gov.mn, ORCID:0009-0004-4847-5942*

[2]*Зэвсэгт хүчний 013 дугаар ангийн ротын захирагч, дэслэгч, waanjilw@gmail.com, ORCID: 0009-0006-2951-7865*

ХУРААНГУЙ

Эрчим хүч хэмнэлтийн ухаалаг системүүд сүүлийн жилүүдэд эрчимтэй хөгжиж, хэрэглээ нь өргөжин тэлж буйтай холбогдон кибер халдлагад өртөх эрсдэл мөн адил нэмэгдэж байна. Энэхүү судалгааны хүрээнд ухаалаг төхөөрөмжүүдэд хамгийн түгээмэл тохиолддог кибер халдлагын төрлүүдийг тодорхойлж, тэдгээрээс урьдчилан сэргийлэх болон хамгаалах боломжит арга, шийдлүүдийг судалж дүгнэсэн. Түүнчлэн эрчим хүч хэмнэлтийн ухаалаг систем, уг системийг удирдах веб суурьтай платформ, мөн DDoS халдлагыг илрүүлэх

программын кодыг загварчлан боловсруулж, симуляцийн болон лабораторийн орчинд туршилт явуулсан. Ухаалаг төхөөрөмжийг бодит орчинд угсарч турших замаар тухайн системийг хэрхэн загварчлах, веб платформтой холбох, улмаар төхөөрөмжид чиглэсэн кибер халдлагыг илрүүлэх программ хангамжийг хэрэгжүүлэх боломжтой.

Түлхүүр үг: *Эрчим хүч хэмнэлтийн ухаалаг систем, кибер халдлага, халдлагаас хамгаалах арга, халдлага илрүүлэх программ, төхөөрөмжийн туршилт, зүйлсийн интернэт.*

Удиртгал

Эрчим хүч хэмнэлтийн ухаалаг систем (ЭХХУС) нь эрчим хүчний хэрэглээ, үйлдвэрлэл, дамжуулалт, түгээлтийн процессыг автоматжуулан оновчтой болгох зорилготой. “Эрчим хүч хэмнэлтийн систем гэдэг нь эрчим хүчийг аль болох бага зарцуулж, үр ашигтай ашиглах, алдагдлыг бууруулах, мөн хэрэглээг хянах, удирдах зорилготой технологи, төхөөрөмж, программ хангамж, удирдлагын бодлого, процессын цогц юм” гэж ISO50001 стандартад заасан байдаг *(Jaimish 2025)*.

Эрчим хүчний хэмнэлт болон эрчим хүчний үр ашгийг (efficiency) тооцоолохдоо Системийн онол (Systems Theory), Гэдрэг холбооны удирдлагын онол (Feedback Control Theory), Оновчлолын онол (Optimization Theory) зэрэг техник болон системийн онолуудыг ашигладаг *(Narantuya V. et al. 2025)*.

Олон улсын туршлагаас харахад эрчим хүч хэмнэлтийн бодлого, стандарт, технологийг нэвтрүүлэх нь эрчим хүчний хэрэглээг 10-40% хүртэл бууруулж чаддаг байна *(“Why Energy Efficiency Matters” 2026)*.

ЭХХУС-ийг шат дараатайгаар хэрэгжүүлэх нь эрчим хүчний хэрэглээ буурах, ашиглалтын зардал багасах, төхөөрөмжийн ашиглалтын хугацаа уртсах, байгаль орчинд ээлтэй, тогтвортой хэрэглээ хэвших, хүний хөдөлмөрийг хөнгөвчлөх гэх мэт ач холбогдолтой.

ЭХХУС-ийн сүлжээний хэрэглээ нь бидний өдөр тутмын үйл ажиллагаа, бизнес, гэр ахуй, олон нийтийн ажил, эрүүл мэндийн үйлчилгээ, үзвэр, барилга гэх мэт олон салбаруудад нэвтэрч, хүлэмжийн хийг бууруулан уур амьсгалын өөрчлөлтийг сааруулахад нэн чухал *(Bayarmunkh B. and Sodnomtsog D. 2025)*.

ЭХХУС-ийн талаар Н.Лхагва-Очир “IoT суурилсан үйлдвэрлэлийн автоматжуулалт” 2020; Б.Энхбаяр “220В-ийн цахилгаан хангамжийн IoT удирдлагын загвар” 2024; Б.Эрболд “Эрчим хүчний хэмнэлтийн менежментийг сайжруулах нь: Эрдэнэт үйлдвэрийн Дулааны цахилгаан станцын жишээн дээр” 2025; Ч.Хосбаяр “Юмсын интернэт аюулгүй байдлын судалгаа” 2024; Matthias Weigold, Michael Frank Borys Ioshchikhes.2024; A Systematic Review of Expert Systems for Improving Energy Efficiency in the Manufacturing Industry; Hamed Khosravi, Hadi Sahebi, Rahim khanizad, Imtiaz Ahmed 2023; Building Energy Efficiency through Advanced Regression Models and Metaheuristic Techniques for Sustainable Management; Stephanie D¨unhaupt “Vulnerabilities of Industrial Automation Systems” 2012; Final Report - Study on cybersecurity in the energy sector of the Energy Community”.2019; GW Ten, M Govindarasu, CC Liu, “Cybersecurity for electric power control and automation systems” 2007 гэх мэт судалгаанууд хийгдсэн байна. Эдгээр судалгаа нь цаг үеийн шинжтэй дүн шинжилгээ хийсэн судалгааны ажлууд бөгөөд зарим судалгааны ажил нь симуляцийн орчинд ухаалаг төхөөрөмжийн нэгэн хэсгийг туршсан судалгаанууд байна. Монгол улсын кибер аюулгүй байдлын салбарын хувьд Засгийн газрын харьяа байгууллагууд кибер халдлагад

өртөх эрсдэл маш өндөр байгаа ба халдлагын хэв шинжтэй, сэжигтэй хандалтууд “ОХУ (128,118,675), БНХАУ (50,599,140), АНУ (65,410,867)”-аас хамгийн их ирж байгаа талаар мэдээллийг “Цахим хөгжил, инновац, харилцаа холбооны яам” пэйж хуудаснаа мэдээлсэн. Мөн Засгийн газрын харьяа байгууллагууд (70%), эрүүл мэндийн салбар (14%), Улсын их хурал (11%) болон хууль сахиулах байгууллагууд (1%) кибер халдлагад өртөх эрсдэлтэй байна.

Судалгааны зорилго, зорилт

Сүүлийн жилүүдэд техник, технологи хурдацтай хөгжиж буйтай холбоотойгоор тэдгээртэй уялдсан эрсдэлүүд мөн адил нэмэгдэж байна. Үүний улмаас хэрэглэгчид өдөр тутамдаа ашиглаж буй ухаалаг төхөөрөмжөөр дамжуулан мэдээллийн аюулгүй байдал алдагдах эрсдэлтэй нүүр тулгарч байна. Энэхүү судалгаа нь эрчим хүч хэмнэлтийн ухаалаг системийг зохион бүтээж, хамгийн их тохиолдож буй кибер халдлагуудыг тодорхойлж, тэдгээрээс хамгаалах аргуудыг судлан, халдлага илрүүлэх системийг Python программчлалын хэл дээр загварчлан туршилт хийн үр дүн гаргана.

Судалгааны арга зүй

Энэхүү судалгааны ажилд шинжлэх ухаанд өргөн хэрэглэгддэг харьцуулах арга, системийн задлан шинжилгээ болон синтез, нэгтгэн дүгнэх аргачлалуудыг түүнчлэн компьютерын симуляц болон лабораторийн туршилтын аргуудыг ашиглан туршилт, судалгааны үр дүнг тодорхойлохыг зорьсон болно. Эдийн засгийн хөгжлөөр тэргүүлэгч улс орнууд аливаа шинэ техник, технологийг нэвтрүүлэхдээ эхлээд компьютер симуляцийн орчинд туршиж үздэг. Ингэснээр эдийн засгийн үр өгөөжийг нэмэгдүүлэхийн зэрэгцээ аливаа эрсдэлээс урьдчилан сэргийлэх боломжтой.

Дэлхийд техник, технологиороо тэргүүлэгч улсуудыг судлан үзэхэд:

АНУ-ын хэрэглэгчдийн хэмнэлт: Parks Associates-ийн судалгаагаар АНУ-ын ухаалаг эрчим хүчний ухаалаг төхөөрөмжүүд ашигладаг өрхүүдийн 70% нь эрчим хүчний хэрэглээг бууруулж, зардлыг хэмнэсэн гэж мэдээлсэн байна *(Parks Assoc. 2016)*.

Их Британийн хэрэглэгчдийн хэмнэлт: Их Британийн өрхүүдийн 63% нь эрчим хүчний хэмнэлттэй шинэчлэлүүдийг хийснээр жилд дунджаар 283.90 фунт стерлинг хэмнэсэн байна. Мөн 2023 онд 3.3 сая ухаалаг тоолуур суурилуулсан нь эрчим хүчний хэмнэлтэд хувь нэмэр оруулсан байна *(Parks Assoc. 2016)*.

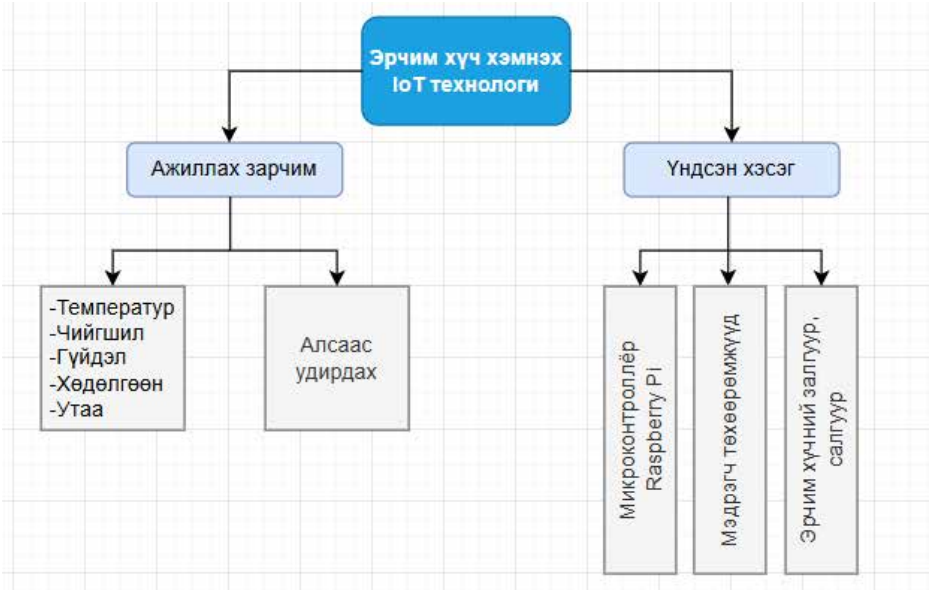
Дани улсын хэрэглэгчдийн хэмнэлт: Дани улсын судалгаагаар гэрийн эрчим хүчний ухаалаг удирдлагын системүүдийг ашигласнаар өвлийн улиралд эрчим хүчний хэрэглээг 30% хүртэл бууруулсан байна.

ОХУ-ийн хэрэглэгчдийн хэмнэлт: ОХУ-ын Белгород муж 2023 онд 2,144 төрийн байгууллагын 5,332 барилгаас эрчим хүчний зардал 4.8 тэрбум рубль байсан бол үүнийг 5 жилийн хугацаанд 8%-иар бууруулсан байна *(Koshlich et al. 2024)*.

БНХАУ-ын хэрэглэгчдийн хэмнэлт: Цэвэр эрчим хүчний эх үүсвэрүүдийн үйлдвэрлэл 2024 онд 3,200 тэрбум кВт.ц хүрч, өмнөх оноос 8%-иар өссөн бөгөөд 2023 онд эрчим хүчний хэмнэлт 0.5%-иар буурсан үзүүлэлттэй гарсан байна *(Reuters 2024)*.

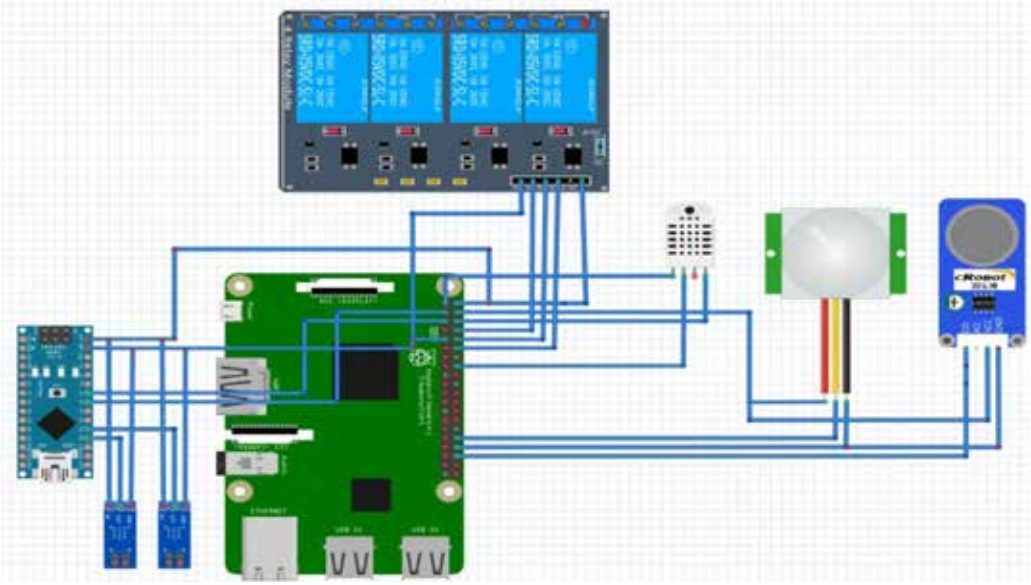
Иймээс энэхүү өгүүлэл нь Монгол улсад ашиглагдаж байгаа ухаалаг төхөөрөмжүүдийг хэрхэн загварчилж, веб платформ хэрхэн үүсгэж холбогддог, энэхүү үйл явцад нийтлэг гардаг кибер халдлагыг судлан, тэдгээр халдлагуудаас хамгийн их үйлдэгдсэн халдлагыг хэрхэн илрүүлэх программ зохиож болох талаар туршилтаар батлахыг зорьж байна.

Манай орны хувьд ч энэ жишгийг дагаж, шинэ техник, технологийг гаднаас шууд импортлохын оронд өөрсдийн симуляцийн орчинд туршиж, судлах нь өндөр ач холбогдолтой юм. ЭХХУС-ийг лабораторийн болон симуляцийн орчинд туршсан бөгөөд энэхүү туршилтын бүтцийн схем, төхөөрөмжийн холбогдсон байдал, мэдрэгч төхөөрөмжүүдийн туршилтын үр дүнг дараах байдлаар харуулав.



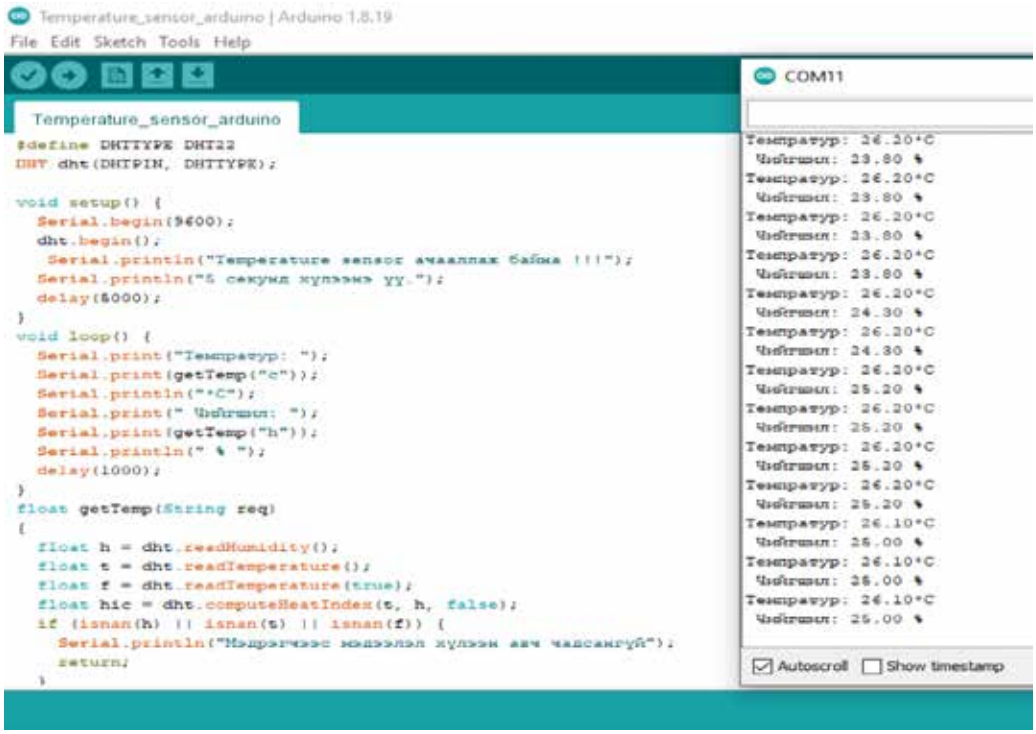
Зураг 1. *ЭХХУС – ийн бүтцийн схем*

Зураг 2. *а. угаарийн хий мэдрэгч б. хөдөлгөөн мэдрэгч в. Raspberry Pi г. Arduino Mega25 д. гүйдэл мэдрэгч е. релей ё. соронзон пускатель ж. температур, чийгшил мэдрэгч*

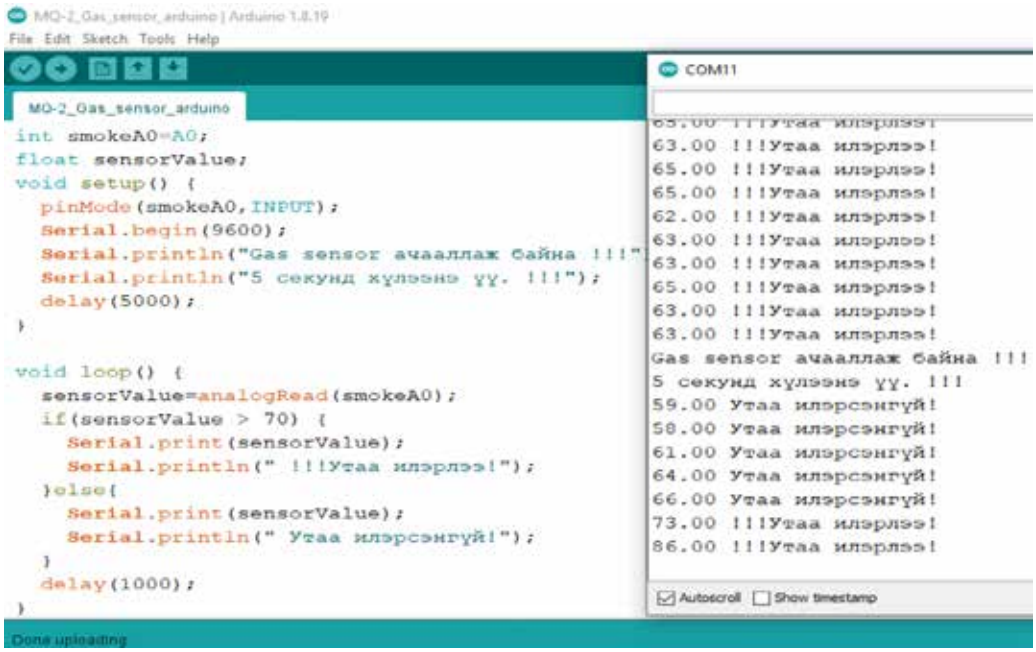


Зураг 3. *Туршилтын ЭХХУС-ийн Fritzing программ дээрх холболтын дүрслэл*

Зураг 4. *Удирдлагын хавтангийн төхөөрөмжүүд холбогдсон туршилтын загвар харагдах интерфейс*

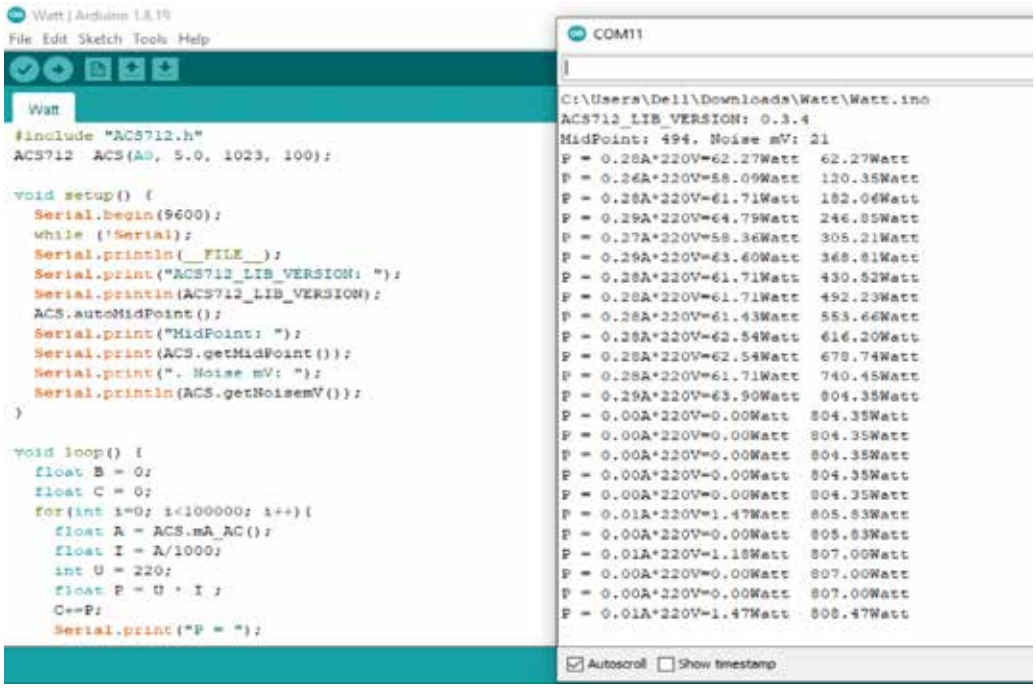


Зураг 5. *DHT22 (температур, чийгшил) мэдрэгчийн туршилт, үр дүн*

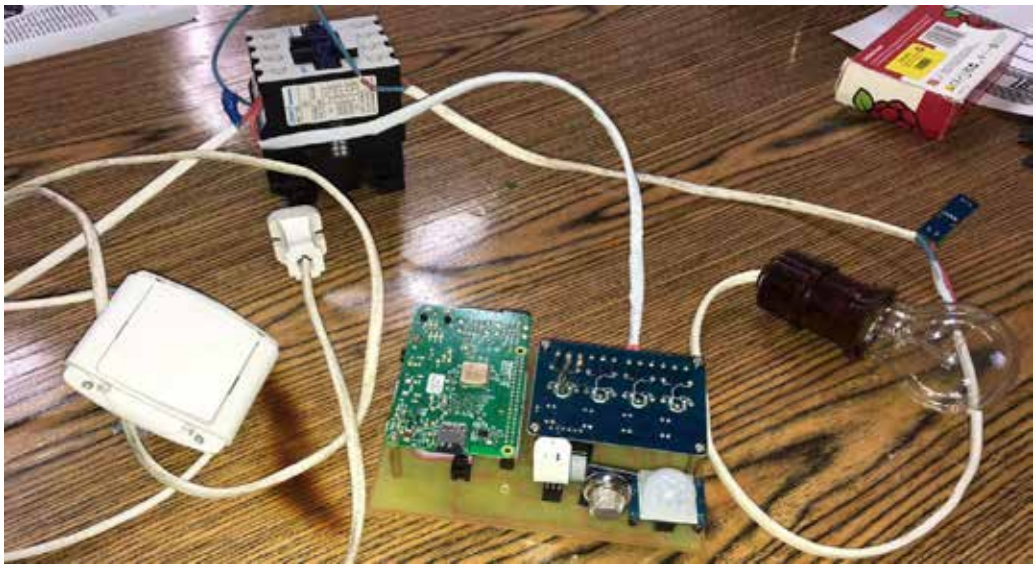


Зураг 6. *Угаарын хий мэдрэгчийн туршилт, үр дүн*

ACS712 гүйдэл мэдрэгчийн туршилт хийж (220v-ийн гэрэл асааж гүйдэл мэдрэгчийг холбосон), Arduino программ дээр код ажиллуулан сериал монитор хийн үр дүнг 6 дугаар зурагт харуулав.

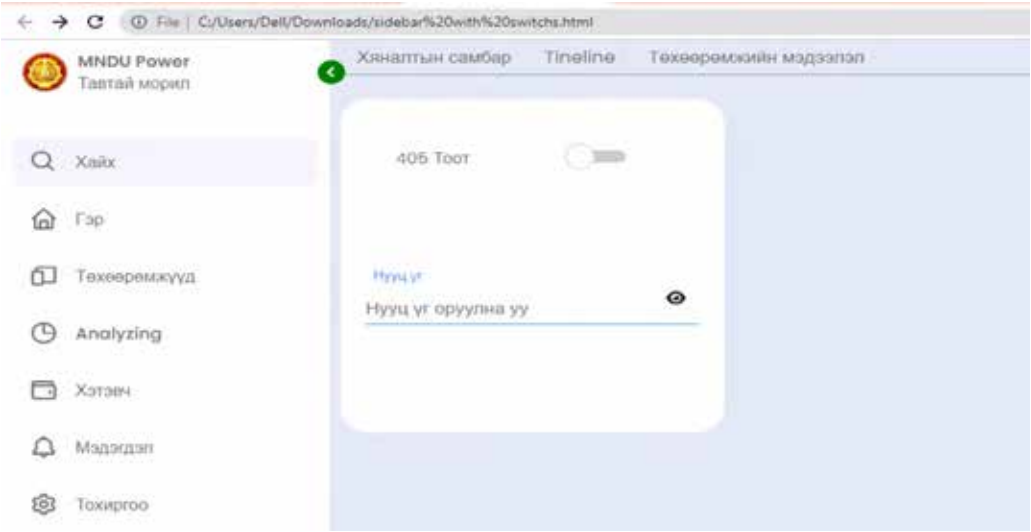


Зураг 7. *ACS712 гүйдэл мэдрэгчийн туршилт, үр дүн*



Зураг 8. *Соронзон автомат унтраалгыг удирдлагын хавтантай холбосон холболт*

Өгөгдлийг хянахын тулд хэрэглээний программ буюу веб хуудас, аппликейшин шаардлагатай болно. Иймд веб хуудсыг үүсгэхийн тулд Javascript, PHP, HTML, CSS, Python гэх мэт программчлалын хэлийг ашиглан хөгжүүлэлт хийсэн. Харагдах интерфейс дизайны хувьд сайжруулалт хийгдсэн веб хуудасны харагдах байдлыг 9 дүгээр зурагт харуулав.



Зураг 9. *Сайжруулсан веб хуудас харагдах байдал*

Эрчим хүч хэмнэлтийн ухаалаг системд гардаг нийтлэг кибер халдлагууд

ЭХХУС-д хамгийн их үйлдэгддэг 12 төрлийн кибер халдлагыг CrowdStrike компанийн 2024 оны 5-р сарын 12-ны өдөр цахим хуудсандаа нийтэлсэн байна. Нийтлэг гардаг 12 халдлагыг доор дурдъя.

1. *Фишинг (Phishing) халдлага*
2. *Сошиал инженерчлэл (Social Engineering)*
3. *Distributed Denial-of-Service (DDoS) attack*
4. *Botnet халдлага*
5. *Code injection attack (код оруулах халдлага)*
6. *Supply chain attack (сүлжээний хангамжийн халдлага)*
7. *Insider threats (дотоод аюул)*
8. *DNS (Domain Name System) Tunneling*
9. *Malware (хортой программ)*
10. *IoT-Based attack (интернэтэд суурилсан ухаалаг төхөөрөмжийн халдлага)*
11. *AI-д суурилсан халдлага*

Дээрх халдлагаас DDoS халдлага, AI-д суурилсан халдлага, Botnet халдлага нь эрчим хүч хэмнэлтийн ухаалаг системд хамгийн их үйлдэгдсэн байна.

Хэрэглэгчид өөрсдөө КАБ-ын талаар суурь мэдлэггүй байгаагаас шалтгаалж халдлагад амархан өртдөг. Иргэдийн 35 хувь нь цахим орчин дахь нууц үгийг хялбар тохируулснаар хувийн мэдээллээ алдсан байна. Мөн Европын холбооны КАБ-ын агентлагаас жил бүрийн есдүгээр сард эрхлэн гаргадаг “Кибер халдлагын тойм мэдээ”-нд мэдээлснээр 2023 оны долоодугаар сараас 2024 оны есдүгээр сарын хооронд Европын холбоо руу чиглэсэн нийт 11079 кибер халдлага, зөрчил 19754 эмзэг цэг/vulnerability бүртгэгдсэнээс DOS/DDOS/RDOS халдлага 4200 удаа буюу хамгийн их үйлдэгдсэн байна. Энэ нь нийт халдлагын 41.1 хувийг эзэлж байгаа бол ransomware халдлага 2590 буюу 25.79 хувь, өгөгдөлтэй холбоотой халдлага 1910 удаа буюу 19.01 хувь, сошиал инженеринг 610 буюу 6 хувь, malware халдлага 520 удаа буюу 5.19 хувийг эзэлж байна *(“Кибер Аюулгүй Байдал Шинэ Технологи Ба Тулгарч Буй Сорилт” 2024)*.

ЭХХУС нь дэлхий даяар хурдацтай өсөж байгаа технологийн нэг бөгөөд энэ

нь олон салбарт, тэр дундаа ухаалаг хот, үйлдвэрлэл, гэр ахуйн хэрэглээ зэрэгт өргөнөөр ашиглаж байна. Дэлхийн ЭХХУС-ын тоо 2024 онд 17.7 тэрбум, 2025 онд 19.8 тэрбум байсан бол 2034 он гэхэд өсөн нэмэгдсээр 40.6 тэрбумд (*График 1*) хүрэх төлөвтэй байна *(Taylor 2026)*.

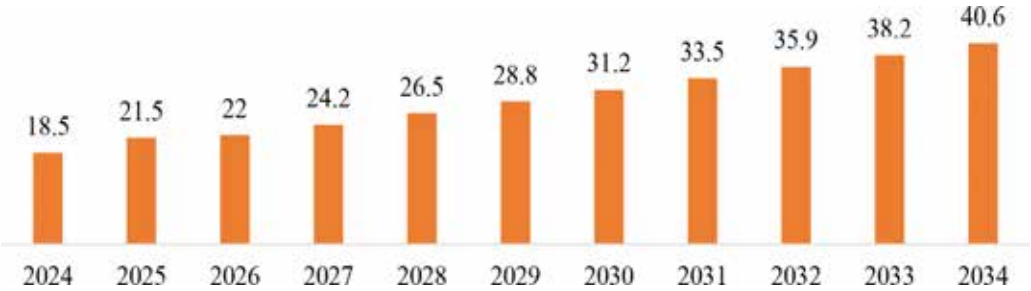


График 1. *Эрчим хүч хэмнэлтийн ухаалаг системийн2034 он хүртэлх интернэтэд холбогдох төхөөрөмжийн тоо*

Ухаалаг төхөөрөмжүүдийн тоо нэмэгдэхийн хэрээр эрсдэл мөн дагаад өндөр болно гэсэн үг. Тэдгээр халдлагаас хамгаалах аргуудыг хэрэглэж өөрсдөдөө аюулгүй байдлыг хангах нь зүйтэй.

Судалгааны үр дүн

DDoS халдлага нь ЭХХУС-д түгээмэл илэрдэг халдлагын нэг юм. Түүнийг илрүүлэх программын кодыг Python программчлалын хэл ашиглаж бичиж, лабораторийн орчинд туршилт хийж үзэв. Тухайн программ нь аль ч сайтад ажиллах боломжтой.

1. Халдлага илрүүлэх программын туршилтын үр дүн

Тухайн халдлагыг илрүүлэх программын кодыг ачаалуулахад дараах үр дүнгүүд гарсан.

```
Dataset shape: (12000, 8)
Label distribution:
0: 0.88, 1: 0.12
```

Зураг 10. *Халдлага илрүүлэх программын туршилт 1*

Дээрх үр дүнгээс харахад:

- 12,000 flow өгөгдөл үүссэн, 0 → хэвийн урсгал, 1 → халдлагын урсгал гэж харуулж байна.
- 88% нь хэвийн, 12% нь DDoS маягийн халдлага орж ирж байна гэсэн үр дүнг программ харуулж байна.

```
0      1.0000    1.0000    1.0000      130
1      1.0000    1.0000    1.0000      245
```

Зураг 11. *Халдлага илрүүлэх программын туршилт 2*

Дээрх туршилтын үр дүн нь:

- 0=хэвийн сүлжээний урсгал (халдлага агуулаагүй хэвийн сүлжээний урсгалын тоо 130 байна)
- 1=халдлага илэрсэн сүлжээний урсгал (DDoS халдлага байж болзошгүй сүлжээний урсгал 245 ширхэг илэрсэн байна)

2. DDos халдлагаас сэргийлэх дараах арга хэмжээнүүд байна.

- Байгууллага бүрийн дэд бүтцэд интернэтийн траффик буюу сүлжээний урсгалыг мэргэжлийн чиглэлийн ажилчид нэг бүрчлэн мэддэг байх.
- Үүлэн (Cloud) үйлчилгээ ашиглах.
- Сүлжээний аюулгүй байдлын шийдлүүдийг хэрэгжүүлэх.
- Сошиал аюулгүй байдлыг хангах.
- Эрсдэлийн үнэлгээ хийх.
- DDos халдлагад хариу арга хэмжээ авах төлөвлөгөө боловсруулах.

3. Ботнет халдлагаас хамгаалах сүүлийн үеийн аргууд:

1. Bot Detection & Filtering (Бот илрүүлэлт, шүүлтүүр)
2. AI / Машин сургалт (ML) суурилсан хамгаалалт
3. Network-Level Security (Сүлжээний түвшний хамгаалалт)
4. Edge & Gateway Security (Сүлжээний урсгалын хамгаалалт)
5. Endpoint Security (Төхөөрөмжийн хамгаалалт)
6. Системийн шинэчлэл, Патч менежмент
   - OS, firmware, IoT төхөөрөмжийн патчийг тогтмол хийх;
   - Default passwordуудыг сольж, аюулгүй нууц үг ашиглах;
7. Security Framework ба стандарт мөрдөх
   - ISO 27001, NIST зэрэг стандарт мөрдөж ажиллагааны бодлого бий болгох;
8. ISP / Үндэсний түвшний хамгаалалт
   - Харилцан мэдээлэл солилцох;
   - Том ботнетийг таслан зогсоох орчин бий болгох;
9. Хэрэглэгчийн боловсрол, Cyber Hygiene
   - Хүчтэй нууц үг, 2FA ашиглах;
   - Сэжигтэй линк, и-мейл дээр дарж болохгүйг мэдэх;
   - IoT төхөөрөмжийг зөв ашиглах;
10. Ботнетийн команд серверийг таслан зогсоох
   - International botnet takedown ажиллагаанд оролцох;
   - Команд серверүүдийг илрүүлж таслан зогсоох (Vandantseren, May 31, 2018);

4. AI-д суурилсан хадлагаас хамгаалах аргууд:

1. Бодит цагийн аномали илрүүлэлт (Real-time Anomaly Detection)
2. Модульчилсан AI архитектур
3. Мэдээллийн болон өгөгдлийн баталгаажуулалт (Data Validation & Sanitization)
4. Машин сургалтын моделийн хамгаалалт

5. Нууцлал ба нэвтрэлт хяналт (Privacy & Access Control)

6. Системийн хяналт ба аудит (Monitoring & Auditing)

7. Сургалт, мэдлэгийн шинэчлэлт (Continuous Learning & Updates)

8. Өгөгдөл нөөцлөх:

9. Zero Trust аюулгүй байдлын загварыг хэрэгжүүлэх: ZT аюулгүй байдлын загварууд нь баталгаажуулалт, зөвшөөрөлгүй хэрэглэгчдийн хандалт, программууд болон төхөөрөмжүүдэд гадны этгээд нэвтрэхийг оролдоход баталгаажуулалт үүсгэж байнгын хяналт, шалгалт хийдэг систем юм.

10. Хамгаалалтын төхөөрөмжүүд суулгах;

11. Сүлжээний хамгаалалт ашиглах;

12. Шифрлэлт ашиглах (Encryption).

Дээрх халдлагаас хамгаалах аргачлалуудыг бүрэн хэрэгжүүлснээр тухайн төхөөрөмж болон сүлжээнд гарах кибер эрсдэл, аюулуудад өртөх магадлал багасаж, бүрэн хамгаалагдана.

Мөн энэхүү өөрийн бүтээсэн IoT төхөөрөмж болон түүний DDoS халдлага илрүүлэх, хамгаалах программ хослон ажилласнаар Батлан хамгаалах салбарт ухаалаг хяналтын систем, талбарын монитор, дрон, автоматжуулсан тоног төхөөрөмжзэрэгмэдээлэлцуглуулахнэгжүүдийгөндөрнарийвчлалтай,тасалдалгүй, аюулгүй ажиллуулах боломжийг бүрдүүлж, цэргийн объектын хамгаалалт, хил хяналт, тактикийн мэдээлэл дамжуулалт, командлалын системүүдийн найдвартай ажиллагааг хангах стратегийн ач холбогдолтой интеграцлагдсан технологийн шийдэл болж хөгжих боломжтой. Зөвхөн Батлан хамгаалах үйл хэрэгт ашиглах биш, Зэвсэгт хүчний анги байгууллагуудад хэрэглээний системүүдийг автоматжуулах боломжтой хөрвөх чадвартай бүтээл юм.

Дүгнэлт

Эрчим хүч хэмнэлтийн ухаалаг систем (ЭХХУС), IoT технологи, ухаалаг төхөөрөмжүүдийн хөгжил нь хүн төрөлхтөнд амьдралыг хөнгөвчилж, тав тухыг бий болгож байгаа хэдий ч кибер аюулгүй байдлын асуудлыг улам бүр хурцатгаж байна. Орчин үед IoT төхөөрөмжүүд хамгаалалтын түвшин сул, халдлагад өртөх эрсдэл өндөр байгаа нь үндэсний аюулгүй байдалд ч нөлөөлөх хэмжээнд хүрч болох юм. ЭХХУС зохион бүтээж симуляцийн болон лабораторийн орчинд туршихад программын болон техникийн илт алдаа заагаагүй. Мөн энэхүү төхөөрөмжийг удирдах вэбсайт, DDoS халдлага илрүүлэх программын код бичиж, туршсан болно. Эдгээр программ болон төхөөрөмжийг төр, хувийн хэвшлийн байгууллагуудад ашиглах боломжтой юм.

Технологийн аюулгүй байдлыг хангаснаар мэдээлэл, систем, сүлжээг зөвшөөрөлгүй нэвтрэлт болон алдагдлаас хамгаалж, байгууллага, иргэний нууцлал ба итгэлцлийг баталгаажуулахын зэрэгцээ системийн найдвартай ажиллагааг нэмэгдүүлж, кибер халдлагаас үүдэх эдийн засгийн хохирлыг бууруулан, хэрэглэгчийн итгэлийг дээшлүүлж, хууль, стандартын шаардлагыг ханган ажиллах нөхцөл бүрдүүлж, улмаар нийгэм, байгууллага, улс орны кибер орчны дархлааг бэхжүүлнэ.

Дээр дурдсан халдлагаас хамгаалах аргуудыг тогтмол хэрэгжүүлж хэвшвэл

ЭХХУС-ийг кибер халдлагаас хамгаалах боломжтой бөгөөд системийн найдвартай ажиллагаа, өгөгдлийн аюулгүй байдал хангагдана.

Олон орнуудын туршлагаас харахад эрчим хүч хэмнэлтийн бодлого, стандарт, технологийг түгээмэл нэвтрүүлэх нь нийт эрчим хүчний хэрэглээг 10-40% хүртэл бууруулж чаддаг. Энэ нь улс орны хэмжээнд эрчим хүчний хэрэглээг бууруулж, эрчим хүчний үйлдвэрлэл, импортын хэмжээг багасгахад шууд нөлөөлдөг.

Өөрийн бүтээсэн IoT төхөөрөмж болон түүний DDoS халдлага илрүүлэх, хамгаалах программ хослон ажилласнаар Батлан хамгаалах салбарт ухаалаг хяналтын систем, талбарын монитор, дрон, автоматжуулсан тоног төхөөрөмж зэрэг мэдээлэл цуглуулах нэгжүүдийг өндөр нарийвчлалтай, тасалдалгүй, аюулгүй ажиллуулах боломж бүрдүүлж, цэргийн объектын хамгаалалт, тактикийн мэдээлэл дамжуулалт, командлалын системүүдийн найдвартай ажиллагааг хангах стратегийн ач холбогдолтой интеграцлагдсан технологийн шийдэл болж хөгжих боломжтой.

Энэхүү судалгааны хүрээнд ухаалаг төхөөрөмжүүдэд хамгийн түгээмэл тохиолддог кибер халдлагын төрлүүдийг тодорхойлж, тэдгээрээс урьдчилан сэргийлэх болон хамгаалах боломжит арга, шийдлүүдийг судалж дүгнэсэн. Түүнчлэн эрчим хүч хэмнэлтийн ухаалаг систем, уг системийг удирдах веб суурьтай платформ, мөн DDoS халдлагыг илрүүлэх программын кодыг загварчлан боловсруулж, симуляцийн болон лабораторийн орчинд туршилт явуулсан. Ухаалаг төхөөрөмжийг бодит орчинд угсарч турших замаар тухайн системийг хэрхэн загварчлах, веб платформтой холбох, улмаар төхөөрөмжид чиглэсэн кибер халдлагыг илрүүлэх программ хангамжийг хэрэгжүүлэх бүрэн боломжтойг туршилтаар нотолсон болно.

Талархал

Энэхүү бүтээл болон туршилт судалгааг явуулахад эрдэм мэдлэгээ харамгүй хайрлан зааж зөвлөсөн ҮБХИС-ийн эрдэм шинжилгээ инновацын хэлтэсийн ахлах мэргэжилтэн Л.Бямбажаргал, ҮБХИС-ийн Эрдмийн сургуулийн доктор (Ph.D) дэд профессор Б.Баярмөнх, доктор /Ph.D/, профессор хурандаа Д.Содномцог багш нартаа талархал илэрхийлье.

Эшлэл авсан сурвалж, судалгааны бүтээл:

1. Bayarmunkh B. and Sodnomtsog D. 2025. “Introducing the Information Security Software ‘Crypto-Daichin.’” Preprint, SSRN. *https://doi.org/10.2139/ssrn.5523538.*
2. Jaimish. 2025. “Energy Efficiency: Definition, Challenges & Levers.” April 11. *https://d-carbonize.eu/energy-efficiency/*.
3. Koshlich, Yu., P. Trubaev, Aleksei Bulanin, and D. Buhanov. 2024. “ASSESSMENT OF ENERGY SAVING POTENTIAL IN BUDGETARY INSTITUTIONS IN THE ENERGY RESOURCES MANAGEMENT SYSTEM.” *Energy Systems* 8 (4): 65–94. *https://doi.org/10.34031/es.2023.4.006*.
4. Narantuya V., Bayarmunkh B., and Enkhtuya O. 2025. “Cyber Defence Pact of Mongolia.” Preprint, SSRN. *https://doi.org/10.2139/ssrn.5762565*.
5. Parks Associates. 2016. “70% Of U.S. Households With Smart Energy Devices Report Saving.” April 5. *https://www.parksassociates.com/blogs/in-the-news/70--of-u-s--households-with-smart-energy-devices-report-saving-*.

6. *Reuters*. 2024. “China’s Emissions, Efficiency Targets under Threat after Falling Short in 2023.” March 12. *https://www.reuters.com/sustainability/climate-energy/chinas-emissions-efficiency-targets-under-threat-after-falling-short-2023-2024-03-12/*.
7. Taylor, Petroc. 2026. “IoT Connections Worldwide 203.” January 9. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.
8. “Why Energy Efficiency Matters.” 2026. *https://www.energy.gov/energysaver/why-energy-efficiency-matters*.
9. “Кибер Аюулгүй Байдал Шинэ Технологи Ба Тулгарч Буй Сорилт.” 2024. In *Аюулгүй Байдал Стратеги Тойм*, vol. 29. Стратеги судалгааны хүрээлэн. *https://drive.google.com/file/d/15R0bzO-mDUzbz9LHbClfdLqzmLBHCDax/view*.