Vol. 25 No 56 (2026)

Article

# Cyber immunity and its implications

*Tsogzolboo Otgonbayar*[*], *Ankhbayar Davaanaym*[2*], *Ariunzul Enkhbat*[3]
*Lecturer, Department of Natural Sciences*
*Mongolian National Defense University, Ulaanbaatar, Mongolia*

*DOI: https://doi.org/10.65902/tsats.2026.02.002*

**ARTICLE INFO:**
**RECEIVED:** 06 March 2026
**ACCEPTED:** 15 April 2026
**PUBLISHED:** 02 June 2026



**CORRESPONDING AUTHOR:**
*Ankhbayar Davaanyam

**KEYWORDS:**
Cyber immunity, cybersecurity, artificial immune system, KasperskyOS, information security

## Abstract

*In today's digital era, cyberattacks are increasing year after year, exposing the limitations of traditional defense approaches and creating a need for new paradigms. Based on existing studies, this paper examines the theoretical foundations of cyber immunity, its global applications, the current state of cybersecurity in Mongolia, and relevant defense mechanisms.*

*Cyber immunity, inspired by the principles of biological immune systems, represents a modern approach to cybersecurity. Key mechanisms include minimal trusted code, operating systems such as KasperskyOS that rely on continuous monitoring, and artificial intelligence–driven threat detection systems, all of which are widely used globally. According to Gartner's forecast, by 2025, organizations that adopt cyber immunity systems are expected to reduce downtime by up to 80%.*

## Introduction

Human security in the cyber environment is a constantly evolving field, and with each new technological advancement, new risks and opportunities arise. To ensure human security, it is necessary to take all of the above factors into account and take comprehensive measures.[1]

Cyber immunity refers to the ability of information systems to autonomously detect cyber attacks and threats, protect themselves, and recover on their own[2]. This concept originated from applying the principles of the biological immune system to

[1] DOI: 10.65902/tsats.2026.01.002 Experience and Lessons from Human security in the cyber environment: Risks and key protection issues

[2] Kaspersky. (2022, November 23). What is cyber immunity and how to build an operating system based on the concept. Kaspersky Blog. https://www.kaspersky.com/blog/how-to-create-cyberimmune-system/46314/ Wlodarczak, P. (2017). Cyber immunity. In I. Rojas & F. Ortuño (Eds.), Bioinformatics and Biomedical Engineering (Lecture Notes in Computer Science, Vol. 10209, pp. 1–9). Springer. https://doi.org/10.1007/978-3-319-56154-7_19

information technology and has become an important area of modern cybersecurity research.

Eugene Kaspersky, founder of Kaspersky Lab, defined cyber immunity as "*A cyber-immune system is a system designed to be secure, which continues to perform its core functions even after being attacked*[3]."

*Comparison With Biological Immunity:*

The concept of cyber immunity shares several similarities with biological immune systems:

*Table 1*

| No. | Biological Immunity | Cyber Immunity |
|---|---|---|
| 1 | Detect viruses, bacteria | Detect malicious code and attacks |
| 2 | Generate antibodies | Generate security rules |
| 3 | Immune memory | Attack intelligence database |
| 4 | Self-repair | Automatic system recovery |
| 5 | Foreign object detection | Anomaly detection |

*Core principles of Cyber Immunity*

Cyber immune systems are based on the following core principles:

1. Security by design: The principle of ensuring security from the system's inception, which is built into its core architecture.

2. Least Privilege: The principle that each system component has only the minimum privileges required for its function.

3. Isolation: Isolating parts of the system so that an attack on one part cannot affect other parts;

4. Continuous Monitoring: Continuously monitors system operations to detect abnormal activity;

5. Adaptability: Ability to adapt to new types of attacks and automatically update defenses.

*Consequences Of Weak Cyber Immunity***:**

Weak cyber immunity is not just a technical issue but a complex phenomenon that affects multiple sectors of a country's social, economic, and political life. Threat actors exploit these vulnerabilities to operate at the individual, organizational, and national levels for their respective objectives.

*At the individual level:*

A person's weak cyber immunity directly affects the security of their personal information. In today's digital environment, individuals rely on a variety of information systems in their daily activities, such as online banking, social media, and e-commerce. As this reliance grows, the risk of cyberattacks also increases. Additionally, attackers can use methods such as phishing, social engineering, and malware to steal personal information and financial credentials. As a result, individuals not only suffer financial

[3] Kaspersky, E. (2021, November 12). Transition from cybersecurity to cyber-immunity. IRISSCON 2021. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/transition-cyber-immunity-kaspersky/

losses but also face the risk of reputational damage and loss of personal privacy. According to studies, the harm suffered by individuals from cyberattacks is increasing year after year, making the need to strengthen cyber immunity all the more apparent.

*At the organizational level,* A weak cyber posture gives competitors and cybercriminals an advantage. An attacker who gains access to an organization's information systems can steal customer databases, intellectual property, financial information, and more. This type of attack not only causes direct financial losses but also leads to long-term consequences such as loss of customer trust and reduced market share. Globally, major corporations are suffering tens of millions of dollars in losses from cyberattacks, demonstrating that strengthening an organization's cyber immunity has become an essential strategic requirement.

*At the national level,* A weakness in cyber immunity can directly impact a nation's national security. Foreign intelligence agencies and hostile nation-state cyber units can exploit poorly protected infrastructure to obtain classified government information and to launch attacks on the power supply, communications, and financial systems.

For countries with weak cyber immunity, these risks become not just technological issues but strategic threats that impact political and economic stability. Therefore, international researchers emphasize the need to consider cyber immunity an integral part of national security policy.

**Research Section: Global Cyberattack Statistics and Examples.**

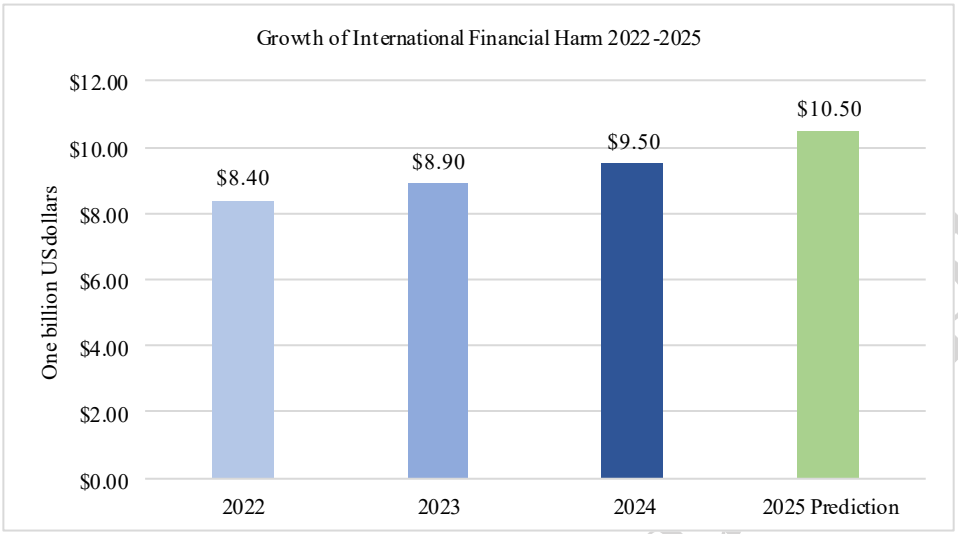
In the modern digital environment, the number of cyberattacks is increasing sharply year after year. According to research by Check Point Research, in the third quarter of 2024, the global average of cyberattacks per organization per week was 1,876, a 75 percent increase compared to the same period in 2023[4]. This clearly shows that the trend of increasing cyberattacks is continuing unabated.

In terms of financial losses, the global cost of cybercrime in 2024 is estimated to reach $9.5 trillion, a figure that Cybersecurity Ventures projects will rise to $10.5 trillion by 2025[5]. The average cost of a data breach in 2024 reached $4.88 million, a 10 percent increase over the previous year[6]. Global statistics on cyber attacks



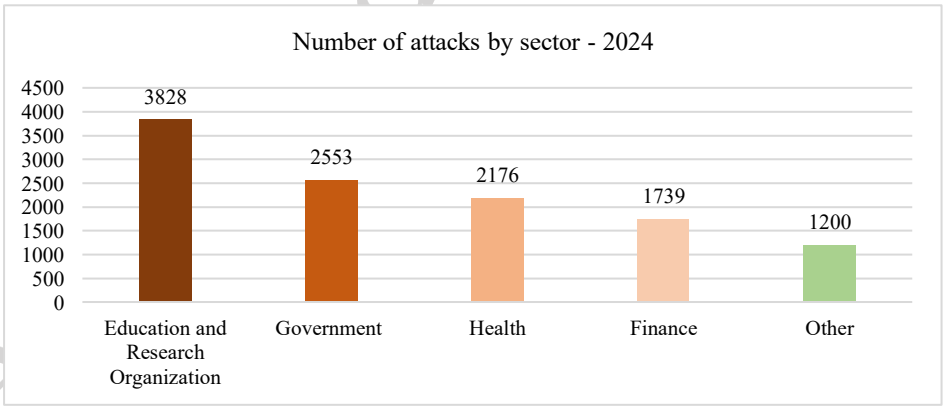
[4] Check Point Research. (2024). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Blog. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/
[5] Cobalt. (2024). Top cybersecurity statistics for 2024. https://www.cobalt.io/blog/cybersecurity-statistics-2024
[6] SentinelOne. (2024). Key cyber security statistics. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

*Figure 1*




In terms of sectors, education and research institutions are the most at-risk, suffering an average of 3,828 attacks per week, followed by government and military organizations and the healthcare sector. In terms of ransomware or malicious software attacks, more than 1,230 cases were recorded in the third quarter of 2024, with 57 percent of victims concentrated in North America[7].

*Figure 2*




*Global Development of Cyber Immunity*

The shift of the concept of cyber immunity from the theoretical realm into practical application is a significant development in the modern cybersecurity field. Within the framework of the Industrial Internet of Things (IIoT) and Industry 4.0, the convergence of information technology and industrial technology has dramatically

[7] Check Point Research. (2024). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Blog. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

expanded the arena for cyber attacks and, by exposing the limitations of traditional cybersecurity defenses, has given rise to the new concept of cyber immunity[8].

A leading example of the practical application of cyber immunity in countries around the world is the KasperskyOS operating system developed by Kaspersky Lab. The primary method for implementing cyber immunity is to divide information systems into isolated segments. It is based on the principle of dividing information systems into isolated components and controlling their interactions, rendering most attacks against such systems ineffective and allowing the system to continue performing its core functions even in a hostile environment[9]. In the industrial sector, the application of cyber immunity is becoming particularly important. Netflix's use of the "chaos engineering" methodology—intentionally breaking and crashing its own systems—to uncover vulnerabilities, adapt in real time, and build self-healing infrastructure has become a major example of the practical implementation of a cyber-immunity system[10]. Researchers estimate that the global market for cyber immunity systems will grow from $16.8 billion in 2022 to $57 billion by 2032[11].

*Current State of Cybersecurity in Mongolia:*

The ITU's Global Cybersecurity Index (GCI) plays a crucial role in assessing a country's cybersecurity level internationally. According to the GCI 2024 report, Mongolia scored 56.36 points, ranking 103rd out of 194 countries, in the "Establishing" tier. (Establishing) level, a 17-place improvement compared to its 2020 score of 26.20[12]. When examined by each core indicator, Mongolia has shown significant growth in legal framework, institutional arrangements, and capacity building, meeting the regional average score for the Asia-Pacific region. In terms of the legal and regulatory environment, since 2021, Mongolia has enacted the Law on Cybersecurity, The enactment of the Law on the Protection of Personal Data and the accompanying rules and regulations, and the continuous improvement of the legal environment, indicating that it has approached the top score in GCI's legal indicators[13]. However, the increasing number of cyberattacks and the growing extent of damage are a cause for concern. Over the past five years, the number of cyberattack victims—across government agencies, public organizations, the private sector, and individuals—has reached 25,849, with



[8] Butt, U. A., Amin, R., Aldabbas, H., Garg, S., Alroobaea, R., & Almotiri, S. H. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. PMC/NCBI. https://pmc.ncbi.nlm.nih.gov/articles/PMC8200965/
[9] Kaspersky Lab. (2025). What is cyber immunity? Kaspersky IT Encyclopedia. https://encyclopedia.kaspersky.com/glossary/cyberimmunity/
[10] Software Engineering Institute. (2024). DevOps case study: Netflix and the Chaos Monkey. Carnegie Mellon University. https://www.sei.cmu.edu/blog/devops-case-study-netflix-and-the-chaos-monkey/
[11] Allied Market Research. (2023). Digital immune system market size, share, competitive landscape and trend analysis report: Global opportunity analysis and industry forecast, 2023–2032. https://www.alliedmarketresearch.com/digital-immune-system-market-A77311
[12] International Telecommunication Union. (2024). Global Cybersecurity Index 2024. ITU. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024
[13] State Great Khural of Mongolia. (2021a). Law on Cybersecurity. https://legalinfo.mn/mn/detail?lawId=16390365491061
State Great Khural of Mongolia. (2021b). Law on the Protection of Personal Data. https://www.undp.org/sites/g/files/zskgke326/files/2024- /biznesiyn_bayguullaguudad_zoriulsan_garyn_avlaga.pdf

losses in 2023 amounting to 87.5 billion tugriks[14]. In Mongolia, over 90,000 cyber attacks and violation incidents are detected per week, and in 2023, an average of 91,788 suspicious access attempts were recorded per week across 8,699 IP addresses belonging to 38 companies[15]. In terms of technical capacity, of the 184,576 registered IP addresses in Mongolia in 2024, 11 suspicious activities were detected on 012 IP addresses, causing approximately 90 billion MNT in damages, and countermeasures were taken against 145 IP addresses[16]. To strengthen institutional capacity, in 2023, national and public centers for combating cyber attacks and violations were established, and at the national level, government, citizen, the opportunity has been created for the government, citizens, and legal entities have been provided with the opportunity to receive professional assistance in the event of a cyberattack[17].

*Table 2*

| Year | Indicator | Damage Caused | Number of Suspicious Activities |
|---|---|---|---|
| 2023 | Suspicious activity | 87.5 billion Tugrik (MNT) | 91,788 |
| 2024 | Suspicious activity | Approximately 90 billion Tugrik (MNT) | 11,012 |

Looking ahead, Mongolia is implementing a technical cooperation project with the Japan International Cooperation Agency (JICA) to strengthen cybersecurity human resources. In collaboration with researchers at the University of Oxford, a study is being conducted to assess the current level of cybersecurity[18].

*Cyber-Immunity Defense Mechanisms*

Cyber-immune security mechanisms are based on principles that differ significantly from traditional security measures. Traditional operating systems consist of a base layer, application layer, and security layer, and if the security layer is breached, an attacker can penetrate the lower layers and take full control of the system's operations.

Kaspersky Lab's KasperskyOS operating system is a leading example of putting cyber-immune protection mechanisms into practice. Each component of the cyber-

[14] Ministry of Digital Development, Innovation, and Communications. (2024, October 10). Cybercrime caused 87.5 billion MNT in damages. https://mddc.gov.mn/eng/2024/10/19291/

[15] Zolbayar, Ch. (2024, January 15). Over 90,000 cyberattacks are detected in Mongolia per week. itoim.mn. https://itoim.mn/a/2024/01/15/society/yek

[16] Ministry of Digital Development, Innovation, and Communications. (2025, January 29). Countermeasures were taken against 145 IP addresses that were attacked by malicious code in 2024. https://mddc.gov.mn/eng/2025/01/20833/

[17] National Center for Cyber Attack and Incident Response. (2023). About Us. https://ncsirt.gov.mn/p/3 Government of Mongolia. (2023, August 30). On establishing a state budget enterprise for the "Public Center for Combating Cyber Attacks and Incidents" (Resolution No. 319). https://legalinfo.mn/mn/detail?lawId=16760334026011

[18] Ministry of Digital Development, Innovation and Communications. (2024a, September 18). Collaborating with JICA to train cybersecurity and drone specialists. https://mddc.gov.mn/mn/2024/09/18657/ Ministry of Digital Development, Innovation, and Communications. (2025, February 19). Oxford: Mongolia needs to increase investment to ensure cybersecurity. https://mddc.gov.mn/eng/2025/02/21011/

immune system is completely isolated from the others and from the external environment, eliminating any uncontrolled interactions. The flow of information between system components is continuously checked for compliance with security policies, and the amount of trusted code that directly affects critical system assets and functions is minimized[19]. Artificial intelligence and machine learning play a crucial role in enhancing cyber immunity by enabling early detection and prediction of vulnerabilities. According to Gartner's forecast, by 2025, organizations that invest in digital immunity systems will see their downtime reduced by 80%, which will lead to significantly increased customer satisfaction[20].

In terms of modern cybersecurity trends, identity fabric immunity—the proactive and reactive protection of identity systems—and cybersecurity assurance or oversight, New mechanisms—such as continuously validating technology, human processes, and identity fabric immunity—have become top priorities for 2024–2025[21].

For artificial immune systems in information technology that apply the principles of the biological immune system, cyber immune systems are new, mimicking the adaptive immune systems of humans and animals. They are capable of detecting and neutralizing unknown cyberattacks previously. While traditional firewalls and intrusion detection systems have struggled to detect previously unseen attacks, cyber-immune systems overcome this limitation by employing technologies inspired by biological immunity[22].

## Conclusion

Based on the issues in the theory of cyber immunity, global best practices, the current state of cybersecurity in Mongolia, and its defense mechanisms, the following conclusions are drawn.

First, cyber immunity is an innovative concept that enables overcoming the limitations of traditional defense methodologies. This approach, modeled on the biological immune system, makes systems resilient to attacks by relying on the principles of innate security, isolation, and continuous monitoring.



[19]Kaspersky Lab. (2024a). Kaspersky Security System. KasperskyOS. https://os.kaspersky.com/technologies/kaspersky-security-system/
Kaspersky Lab. (2024b). Microkernel. KasperskyOS. https://os.kaspersky.com/technologies/microkernel/
[20] Gartner. (2022). What is a digital immune system and why does it matter? Gartner. https://www.gartner.com/en/articles/what-is-a-digital-immune-system-and-why-does-it-matter
[21] Gartner. (2024, February 22). Gartner identifies top cybersecurity trends for 2024. https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024
[22] Kousalya, G., et al. (2023). Artificial immune systems in local and network cybersecurity: An overview of intrusion detection strategies. Advances in Computational Intelligence and Its Applications Journal. https://www.acigjournal.com/Artificial-Immune-Systems-in-Local-and-Network-Cybersecurity-An-Overview-of-Intrusion,184306,0,2.html
DOI: 10.65902/tsats.2026.01.002 Experience and Lessons from Human security in the cyber environment: Risks and key protection issues

Secondly, the fact that the number of cyberattacks and the amount of damage worldwide are sharply increasing year after year underscores the urgent need to implement a cyber immunity system. Strengthening cooperation between the public and private sectors is a crucial prerequisite for ensuring that everyone benefits from the fruits of digital development in order to combat modern, sophisticated cyber threats.

Third, the Mongolian Republic is rated Tier 3, or "Improving," in the GCI 2024 report. This assessment indicates clear progress in cybersecurity but underscores the need to further strengthen technical capacity, human resource training, and international cooperation.

Fourth, integrating artificial intelligence and machine learning technologies into cyber immune systems is becoming a key trend in future cybersecurity. Cybersecurity leaders are focusing in 2025 on implementing more centralized cybersecurity programs that emphasize business continuity and joint risk management.

## Recommendations

Based on the above conclusions, the following recommendations are made for the Mongolian Republic: Incorporate the concept of cyber immunity into the national cyber security policy and introduce cyber immunity–based technologies, such as KasperskyOS, into strategic infrastructure. It is necessary to address the issue by intensifying investment in developing artificial intelligence-based threat detection systems and increasing the number of cybersecurity professionals.

## References:

[1] Kaspersky. (2022, November 23). What is cyber immunity, and how to build an operating system based on the concept? Kaspersky Blog. https://www.kaspersky.com/blog/how-to-create-cyberimmune-system/46314/

[2] DOI: 10.65902/tsats.2026.01.002 Experience and Lessons from Human security in the cyber environment: Risks and key protection issues

[3] Wlodarczak, P. (2017). Cyber immunity. In I. Rojas & F. Ortuño (Eds.), Bioinformatics and biomedical engineering (Lecture Notes in Computer Science, Vol. 10209, pp. 1-9). Springer. https://doi.org/10.1007/978-3-319-56154-7_19 https://doi.org/10.1007/978-3-319-56154-7_19

[4] Kaspersky, E. (2021, November 12). Transition from cybersecurity to cyber-immunity. IRISSCON 2021. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/transition-cyber-immunity-kaspersky/

[5] Check Point Research. (2024). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Blog. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

[6] Cobalt. (2024). Top cybersecurity statistics for 2024. https://www.cobalt.io/blog/cybersecurity-statistics-2024

[7] SentinelOne. (2024). Key cybersecurity statistics. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

[8] Check Point Research. (2024). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Blog. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/
[9] Butt, U. A., Amin, R., Aldabbas, H., Garg, S., Alroobaea, R., & Almotiri, S. H. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. PMC
[10] Kaspersky Lab. (2025). What is cyber immunity? Kaspersky IT Encyclopedia. https://encyclopedia.kaspersky.com/glossary/cyberimmunity/
[11] Software Engineering Institute. (2024). DevOps case study: Netflix and the Chaos Monkey. Carnegie Mellon University. https://www.sei.cmu.edu/blog/devops-case-study-netflix-and-the-chaos-monkey/
[12] Allied Market Research. (2023). Digital immune system market size, share, competitive landscape and trend analysis report: Global opportunity analysis and industry forecast, 2023-2032. https://www.alliedmarketresearch.com/digital-immune-system-market-A77311
[13] International Telecommunication Union. (2024). Global Cybersecurity Index 2024. ITU. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024
[14] State Great Khural of Mongolia. (2021a). Law on Cybersecurity. https://legalinfo.mn/mn/detail?lawId=16390365491061
[15] State Great Khural of Mongolia. (2021b). Law on the Protection of Personal Data. https://www.undp.org/sites/g/files/zskgke326/files/2024-04/biznesiyn_bayguullaguudad_zoriulsan_garyn_avlaga.pdf
[16] Ministry of Digital Development, Innovation, and Communications. (2024, October 10). Cybercrime caused 87.5 billion MNT in damages. https://mddc.gov.mn/eng/2024/10/19291/
[17] Zolbayar, Ch. (2024, January 15). Over 90,000 cyberattacks are detected in Mongolia each week. itoim.mn. https://itoim.mn/a/2024/01/15/society/yek https://doi.org/10.1149/MA2024-01115mtgabs
[18] Ministry of Digital Development, Innovation, and Communications. (2025, January 29). In 2024, countermeasures were taken against 145 IP addresses affected by malicious code attacks. https://mddic.gov.mn/eng/2025/01/20833/
[19] National Center for Combating Cyber Attacks and Incidents. (2023). About Us. https://ncsirt.gov.mn/p/3
[20] Government of Mongolia. (2023, August 30). On the establishment of the "Public Center for Combating Cyber Attacks and Incidents" as a state budget enterprise. (Decision No. 319). https://legalinfo.mn/mn/detail?lawId=16760334026011
[21] Ministry of Digital Development, Innovation, and Communications. (2024a, September 18). Collaborating with JICA to train cybersecurity and drone specialists. https://mddc.gov.mn/mn/2024/09/18657/
[22] Ministry of Digital Development, Innovation, and Communications. (2025, February 19). Oxford: Mongolia needs to increase investment to ensure cybersecurity. https://mddic.gov.mn/eng/2025/02/21011/
[23] Kaspersky Lab. (2024a). Kaspersky Security System. KasperskyOS. https://os.kaspersky.com/technologies/kaspersky-security-system/
[24] Kaspersky Lab. (2024b). Microkernel. KasperskyOS. https://os.kaspersky.com/technologies/microkernel/

[25] Gartner. (2022). What is a digital immune system and why does it matter? Gartner. https://www.gartner.com/en/articles/what-is-a-digital-immune-system-and-why-does-it-matter

[26] Gartner. (2024, February 22). Gartner identifies top cybersecurity trends for 2024. https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024

[27] [Ousalya, G. et al. (2023). Artificial immune systems in local and network cybersecurity: An overview of intrusion detection strategies. Advances in Computational Intelligence and Its Applications Journal. https://www.acigjournal.com/Artificial-Immune-Systems-in-Local-and-Network-Cybersecurity-An-Overview-of-Intrusion,184306,0,2.html https://doi.org/10.60097/ACIG/162896

[28] Stanton, C., Katz, G., & Song, D. (2024). Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response. IEEE Access. https://www.researchgate.net/publication/383758233

Vol. 25 No 56 (2026) Article

# Кибер дархлаа, түүний нөлөөллийн асуудалд

**Отгонбаяр Цогзолбоо[1], Дабааням Анхбаяр[2*], Энхбат Ариунзул[3]**
*Багш, Байгалийн ухааны тэнхим*
*Үндэсний Батлан Хамгаалахын Их Сургууль, Монгол Улс*

***Хураангуй:*** *Өнөөгийн дижитал эрин үед кибер халдлагын тоо жил ирэх тусам эрс нэмэгдэж байгаа нь уламжлалт хамгаалалтын аргачлалуудын хязгаарлагдмал байдлыг илрүүлж, шинэ хандлага хайх шаардлагыг бий болгоод байна. Судалгаануудаас харвал биологийн дархлааны системийн зарчмуудад тулгуурласан кибер дархлаа (Cyber Immunity) гэсэн үзэл баримтлалын онолын үндэс, дэлхийн жишиг хэрэглээ, Монгол Улсын кибер аюулгүй байдлын өнөөгийн байдал болон хамгаалалтын механизмуудыг судалж шинжилгээ хийв. Кибер дархлааны хамгаалалтын механизмуудын хувьд хамгийн бага итгэмжлэгдсэн код[23], тасралтгүй хяналтын системд суурилсан KasperskyOS үйлдлийн систем болон хиймэл оюун ухаанд тулгуурласан аюул илрүүлэх системүүд дэлхийн хэмжээнд ихээхэн өргөн хэрэглэгдэж байна. Gartner[24]-ийн таамаглалаар 2025 он гэхэд кибер дархлааны системд хөрөнгө оруулалт хийсэн байгууллагуудын хөрөнгө оруулалтын зогсонги байдал 80 хувиар багасах төлөвтэй байна гэжээ.*

***Түлхүүр үг:*** *Кибер дархлаа, кибер аюулгүй байдал, хиймэл дархлааны систем, KasperskyOS, мэдээллийн аюулгүй байдал.*

**Үндсэн хэсэг:** Цахим орчин дахь хүний аюулгүй байдал нь тасралтгүй хувьсан өөрчлөгдөж байгаа салбар бөгөөд технологийн шинэ дэвшил бүрийн хамт шинэ эрсдэл, боломжууд бий болсоор байна. Хүний аюулгүй байдлыг хангахын тулд дээрх бүх хүчин зүйлсийг харгалзан үзэж, цогц арга хэмжээ авах шаардлагатай байна.[25]

Кибер дархлаа гэдэг нь мэдээллийн системүүд кибер халдлага, аюул заналхийллийг өөрөө илрүүлж, өөрөө хамгаалж, өөрөө сэргээгдэх чадварыг хэлнэ[26]. Энэхүү үзэл баримтлал нь биологийн дархлааны системийн зарчмуудыг мэдээллийн технологид хэрэглэснээр үүссэн бөгөөд орчин үеийн кибер аюулгүй байдлын судалгааны чухал чиглэл болоод байна.



[23] Системийн аюулгүй байдлыг хангахад шууд оролцдог кодын хэмжээг аль болох бага байлгах зарчим юм.
[24] Gartner бол АНУ-д байрладаг дэлхийн тэргүүлэх мэдээллийн технологийн судалгаа, зөвлөгөө өгдөг компани юм. 1979 онд Жидеон Гартнер үүсгэн байгуулсан бөгөөд өнөөдөр дэлхийн 100 гаруй орны 15,000 гаруй байгууллагад үйлчилдэг.
[25] D DOI: 10.65902/tsats.2026.01.002 Experience and Lessons from Human security in the cyber environment: Risks and key protection issues
[26] Kaspersky. (2022, November 23). What is cyber immunity and how to build an operating system based on the concept. Kaspersky Blog. https://www.kaspersky.com/blog/how-to-create-cyberimmune-system/46314/
Wlodarczak, P. (2017). Cyber immunity. In I. Rojas & F. Ortuño (Eds.), Bioinformatics and biomedical engineering (Lecture Notes in Computer Science, Vol. 10209, pp. 1–9). Springer. https://doi.org/10.1007/978-3-319-56154-7_19

Касперскийн лабораторийн үндэслэгч Евгений Касперский кибер дархлааг *"Кибер дархлааны систем гэдэг нь аюулгүй байхаар зохиогдсон, халдлагад өртсөн ч үндсэн үүргээ гүйцэтгэсээр байдаг систем юм*[27]*"* гэж тодорхойлсон.

Биологийн дархлаатай харьцуулж үзвэл:

Кибер дархлааны үзэл баримтлал нь биологийн дархлааны системтэй олон талаараа төстэй:

*1 дүгээр хүснэгт*

| Д/д | Биологийн дархлаа | Кибер дархлаа |
|---|---|---|
| 1 | Вирус, бактери илрүүлэх | Хортой код, халдлага илрүүлэх |
| 2 | Эсрэг бие үүсгэх | Хамгаалалтын дүрэм боловсруулах |
| 3 | Дархлааны санах ой | Халдлагын мэдээллийн сан |
| 4 | Өөрийгөө сэргээх | Системийг автоматаар сэргээх |
| 5 | Гадны биетийг таних | Хэвийн бус байдал илрүүлэх |

Кибер дархлааны системүүд дараах үндсэн зарчмуудад тулгуурладаг:

1. *Төрмөл аюулгүй байдал*: Систем зохиогдох үеэс нь аюулгүй байдлыг хангах зарчим бөгөөд үндсэн бүтцэд нь суулгасан байдаг;

2. *Хамгийн бага эрх*: Системийн бүрэлдэхүүн хэсэг бүр зөвхөн өөрийн үүрэгт шаардлагатай хамгийн бага эрхтэй байх зарчим;

3. *Тусгаарлалт*: Системийн нэг хэсэгт халдлага гарсан ч бусад хэсэгт нөлөөлөхгүй байхаар тусгаарладаг;

4. *Тасралтгүй хяналт*: Системийн үйл ажиллагааг тасралтгүй хянаж, хэвийн бус үйлдлийг илрүүлдэг;

5. *Дасан зохицох чадвар*: Шинэ төрлийн халдлагад дасан зохицож, хамгаалалтаа автоматаар шинэчлэх чадвар гэж үзэж болно.

*Кибер дархлаа сул байх үр дагавар:* Кибер дархлаа сул байх нь зөвхөн техникийн асуудал биш бөгөөд улс орны нийгэм, эдийн засаг, улс төрийн олон салбарын хүрээнд нөлөөлдөг нарийн төвөгтэй үзэгдэл юм. Энэхүү сул байдлыг ашиглах сонирхолтой этгээдүүд хувь хүн, байгууллага, улсын түвшинд тус тусын зорилгоор үйл ажиллагаа явуулдаг байна.

*Хувь хүний түвшинд:* Хувь хүний кибер дархлаа сул байх нь хүний хувийн мэдээллийн аюулгүй байдалд шууд нөлөөлдөг. Орчин үеийн дижитал орчинд хувь хүн өдөр тутмын үйл ажиллагаандаа цахим банк, нийгмийн сүлжээ, цахим худалдаа зэрэг олон төрлийн мэдээллийн системийг ашигладаг болсон. Энэхүү хамаарал нэмэгдэхийн хэрээр кибер халдлагын эрсдэл ч нэмэгдэж байна. Мөн халдагч этгээдүүд фишинг, нийгмийн инженерчлэл (social engineering), хортой программ зэрэг аргуудыг ашиглан хувийн мэдээлэл, санхүүгийн эрхийг хулгайлах боломжтой болдог. Үүний үр дүнд хувь хүн санхүүгийн хохирол амсахаас гадна нэр төрөө унагаах, хувийн нууцаа алдах эрсдэлд өртдөг байна. Судалгаануудаас харвал кибер халдлагын улмаас хувь хүний хохирол жил ирэх тусам өсөн

[27] Kaspersky, E. (2021, November 12). Transition from cybersecurity to cyber-immunity. IRISSCON 2021. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/transition-cyber-immunity-kaspersky/

нэмэгдэж байгаа бөгөөд энэ нь кибер дархлааг бэхжүүлэх шаардлагыг улам тодорхой болгож байна.

Байгууллагын түвшинд: Байгууллагын түвшинд кибер дархлаа сул байдал нь өрсөлдөгч байгууллага болон кибер гэмт хэрэгтнүүдэд давуу тал олгодог. Байгууллагын мэдээллийн системд нэвтрэх боломж олдсон халдагч этгээд нь үйлчлүүлэгчдийн мэдээллийн сан, оюуны өмч, санхүүгийн мэдээлэл зэргийг хулгайлах эсвэл ransomware буюу хортой программ ашиглан байгууллагын үйл ажиллагааг бүхэлд нь саатуулж мөнгөн төлбөр нэхэх боломжтой болдог. Энэ төрлийн халдлага нь байгууллагад санхүүгийн шууд хохиролоос гадна хэрэглэгчдийн итгэлцлийг алдах, зах зээлд эзлэх байр сууриа сулруулах зэрэг урт хугацааны сөрөг үр дагавар авчирдаг. Дэлхийн хэмжээнд томоохон корпорациуд кибер халдлагын улмаас хэдэн арван сая долларын хохирол амсаж байгаа нь байгууллагын кибер дархлааг бэхжүүлэх нь стратегийн зайлшгүй шаардлага болсныг харуулж байна.

Улсын түвшинд: Улсын түвшинд кибер дархлааны сул байдал нь улс үндэстний үндэсний аюулгүй байдалд шууд нөлөөлөх чадвартай. Гадаад орны тагнуулын байгууллага болон дайсагнасан улс орнуудын кибер нэгжүүд нь сул хамгаалалттай дэд бүтцийг ашиглан засгийн газрын нууц мэдээлэл олж авах, цахилгаан хангамж, харилцаа холбоо, санхүүгийн системд халдах бүрэн боломжтой болдог.

Кибер дархлаа сул байгаа улс орнуудын хувьд эдгээр эрсдэл нь зөвхөн технологийн асуудал биш, харин улс төр, эдийн засгийн тогтвортой байдалд нөлөөлөх стратегийн аюул болж хувирдаг. Иймд олон улсын судлаачид кибер дархлааг үндэсний аюулгүй байдлын бодлогын салшгүй хэсэг болгон авч үзэх шаардлагатайг онцолж байна.

**Судалгааны хэсэг:** Кибер халдлагын дэлхийн статистик, жишээ.

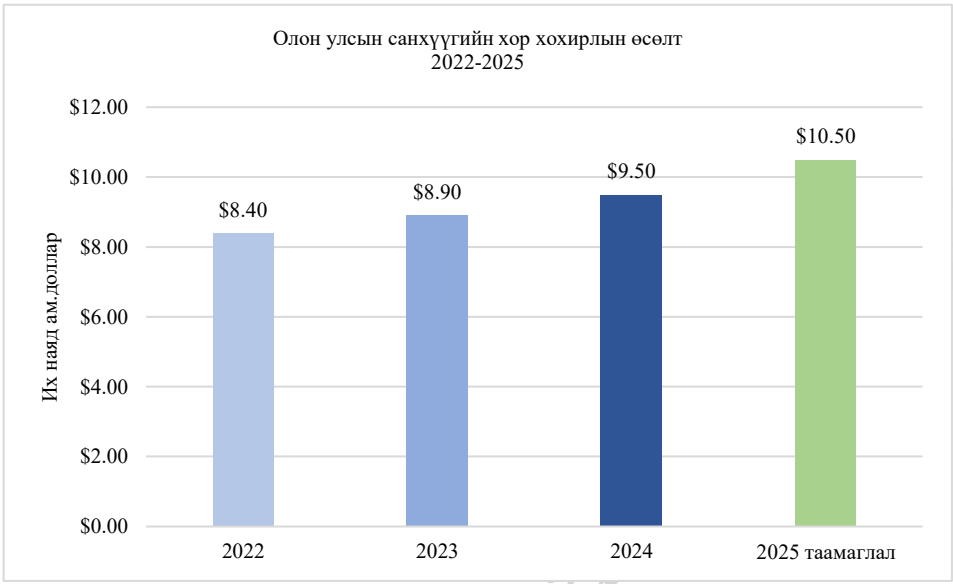
Орчин үеийн дижитал орчинд кибер халдлагын тоо жил ирэх тусам эрс нэмэгдэж байна. Check Point Research-ийн судалгааны дүнгээр 2024 оны гуравдугаар улиралд дэлхий даяар нэг байгууллагад долоо хоногт дунджаар 1,876 кибер халдлага бүртгэгдсэн нь 2023 оны мөн үетэй харьцуулахад 75 хувиар өссөн үзүүлэлт юм[28]. Энэ нь кибер халдлагын өсөлтийн хандлага тасралтгүй үргэлжилж байгааг тодорхой харуулж байна.

Санхүүгийн хохирлын хувьд 2024 онд дэлхий даяар кибер гэмт хэргийн улмаас учрах хохирол 9.5 их наяд ам.доллард хүрэхээр тооцогдсон бөгөөд энэ үзүүлэлт 2025 он гэхэд 10.5 их наяд ам.долларт хүрнэ гэж Cybersecurity Ventures таамаглаж байна[29]. Мөн нэг өгөгдлийн зөрчлийн дундаж зардал 2024 онд 4.88 сая

[28] Check Point Research. (2024). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Blog. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/
[29] Cobalt. (2024). Top cybersecurity statistics for 2024. https://www.cobalt.io/blog/cybersecurity-statistics-2024

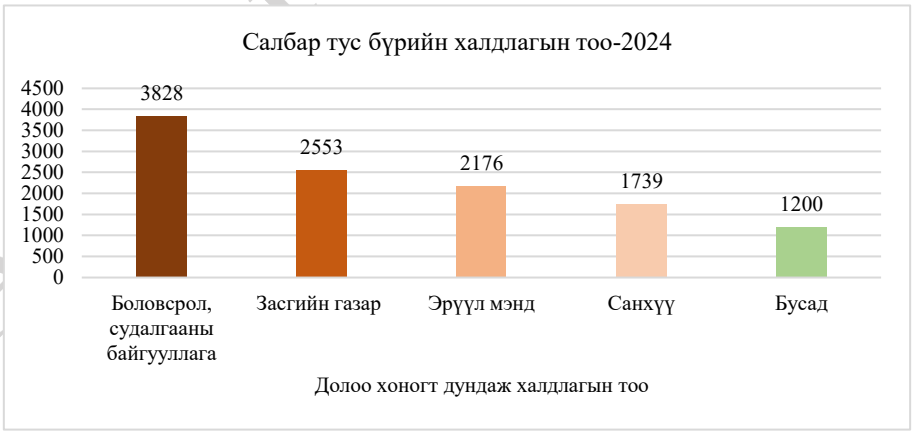
ам.доллар болж, өмнөх оноос 10 хувиар өссөн байна[30]. Кибер халдлагын дэлхийн статистик үзүүлэлтүүд

*1 дүгээр график*




Салбарын хувьд боловсрол, судалгааны байгууллагууд долоо хоногт дунджаар 3,828 халдлагад өртдөг хамгийн эрсдэлтэй салбар болоод байгаа бөгөөд засгийн газар, цэргийн байгууллага болон эрүүл мэндийн салбар түүнийг дагаж байна. Ransomware буюу хортой программын халдлагын хувьд 2024 оны гуравдугаар улиралд 1,230 гаруй тохиолдол бүртгэгдсэн бөгөөд хохирогчдын 57 хувь нь Хойд Америкт төвлөрчээ[31].

*2 дугаар график*




[30] SentinelOne. (2024). Key cybersecurity statistics. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

[31] Check Point Research. (2024). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Blog. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

*Дэлхийн улс орнуудын кибер дархлааны өнөөгийн байдал.*

Кибер дархлааны үзэл баримтлал нь онолын хүрээнээс гарч практик хэрэглээнд нэвтрэх болсон нь орчин үеийн кибер аюулгүй байдлын салбарын чухал хөгжил юм. Үйлдвэрлэлийн интернет (Industrial Internet of Things-IIoT) болон Industry 4.0-ийн хүрээнд мэдээллийн технологи болон үйлдвэрлэлийн технологийн нэгдэл нь кибер халдлагын талбарыг эрс нэмэгдүүлж, уламжлалт кибер аюулгүй байдлын хамгаалалтын хязгаарлагдмал байдлыг илрүүлсний үндсэн дээр кибер дархлааны шинэ үзэл баримтлал бий болсон байна[32].

Дэлхийн улс орнуудын кибер дархлаа практик хэрэглээний тэргүүлэх жишээ бол Касперскийн лабораторийн боловсруулсан KasperskyOS үйлдлийн систем юм. Кибер дархлааг хэрэгжүүлэх үндсэн арга нь мэдээллийн системийг тусгаарлагдсан хэсгүүдэд хуваах, тэдгээрийн харилцан үйлчлэлийг хянах зарчимд тулгуурладаг бөгөөд ийм системд учрах ихэнх халдлага үр дүнгүй болж, систем нь дайсагнасан орчинд ч үндсэн үүргээ гүйцэтгэсээр байна[33].

Аж үйлдвэрийн салбарт кибер дархлааны хэрэглээ онцгой ач холбогдолтой болж байна. Netflix компани өөрийн системийг санаатайгаар эвдэрч унагах "chaos engineering" аргачлалыг ашиглан эмзэг байдлыг илрүүлж, агшин зуур дасан зохицож, өөрөө сэргээгддэг дэд бүтцийг бий болгосон нь кибер дархлааны системийн практик хэрэгжилтийн нэг томоохон жишээ болжээ [34] . Кибер дархлааны системийн дэлхийн зах зээл 2022 онд 16.8 тэрбум амдоллар байснаас 2032 он гэхэд 57 тэрбум амдолларт хүрнэ гэж судлаачид таамаглагдаж байна[35].

*Монгол Улсын кибер аюулгүй байдлын өнөөгийн байдал:* Монгол Улсын кибер аюулгүй байдлын түвшинг олон улсын хэмжээнд үнэлэхэд ITU-ийн Дэлхийн кибер аюулгүй байдлын индекс (GCI) чухал үүрэг гүйцэтгэдэг. GCI 2024 тайлангаар Монгол Улс 56.36 оноо авч, 194 орноос 103 дугаарт буюу "Бэхжиж буй" (Establishing) гэсэн 3 дугаар түвшинд үнэлэгдсэн нь 2020 оны 26.20 оноотой харьцуулахад 17 байр урагшилсан үзүүлэлт юм[36].

Тулгуур хэмжигдэхүүн бүрээр авч үзвэл Монгол Улс хууль эрх зүй, бүтэц зохион байгуулалт, чадавх бэхжүүлэлтийн хувьд эрчимтэй өсөлт үзүүлж, Ази Номхон далайн бүс нутгийн дундаж үнэлгээг хангасан байна.

Хууль эрх зүйн орчны хувьд Монгол Улс 2021 оноос хойш Кибер аюулгүй байдлын тухай хууль, Хүний хувийн мэдээлэл хамгаалах тухай хууль болон тэдгээрийг дагалдан гарах дүрэм, журмуудыг баталж хууль эрх зүйн орчныг

[32] Butt, U. A., Amin, R., Aldabbas, H., Garg, S., Alroobaea, R., & Almotiri, S. H. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. PMC/NCBI. https://pmc.ncbi.nlm.nih.gov/articles/PMC8200965/

[33]Kaspersky Lab. (2025). What is cyber immunity? Kaspersky IT Encyclopedia. https://encyclopedia.kaspersky.com/glossary/cyberimmunity/

[34] Software Engineering Institute. (2024). DevOps case study: Netflix and the Chaos Monkey. Carnegie Mellon University. https://www.sei.cmu.edu/blog/devops-case-study-netflix-and-the-chaos-monkey/

[35] Allied Market Research. (2023). Digital immune system market size, share, competitive landscape and trend analysis report: Global opportunity analysis and industry forecast, 2023–2032. https://www.alliedmarketresearch.com/digital-immune-system-market-A77311

[36]International Telecommunication Union. (2024). Global Cybersecurity Index 2024. ITU. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

тасралтгүй сайжруулсан нь GCI-ийн хууль эрх зүйн үзүүлэлтийн дээд оноонд ойртсоныг илэрхийлж байна[37]. Гэсэн хэдий ч кибер халдлагын тоо, хохирлын хэмжээ өсөн нэмэгдэж байгаа нь анхаарал татаж байна. Сүүлийн таван жилийн хугацаанд төр захиргаа, олон нийтийн байгууллага, хувийн хэвшил, иргэнийг үл харгалзан кибер халдлагад өртсөн тохиолдол 25,849-д хүрч, 2023 онд учирсан хохирол 87.5 тэрбум төгрөгт хүрсэн байна[38]. Монгол Улсад долоо хоногт 90 гаруй мянган кибер халдлага, зөрчлийн тохиолдол илэрдэг бөгөөд 2023 онд долоо хоногт дунджаар 38 компанийн 8,699 IP хаягт 91,788 удаагийн сэжигтэй хандалт илэрсэн байна[39]. Техникийн чадавхын хувьд 2024 онд Монгол Улсад 184,576 IP хаяг бүртгэлтэй байгаагийн 11,012 IP хаягт сэжигтэй үйлдэл илэрч, 90 орчим тэрбум төгрөгийн хохирол учруулж, 145 IP хаягт хариу арга хэмжээ авсан байна[40]. Институцийн чадавхыг бэхжүүлэх чиглэлд 2023 онд кибер халдлага, зөрчилтэй тэмцэх үндэсний болон нийтийн төвүүд байгуулагдаж, улсын хэмжээнд төр, иргэн, хуулийн этгээд кибер халдлагад өртсөн тохиолдолд мэргэжлийн дэмжлэг авах боломж бүрдсэн байна[41].

*2 дугаар хүснэгт*

| Он | Үзүүлэлт | Учруулсан хор хохирол | Сэжигтэй хандалтын тоо |
|---|---|---|---|
| 2023 | Сэжигтэй хандалт | 87.5 тэрбум төгрөг | 91.788 |
| 2024 | Сэжигтэй хандалт | 90 орчим тэрбум төгрөг | 11.012 |

Цаашдын чиглэлийн хувьд Монгол Улс Япон Улсын Олон улсын хамтын ажиллагааны байгууллага (ЖАЙКА)-тай хамтран кибер аюулгүй байдлын хүний нөөцийг чадавхжуулах техникийн хамтын ажиллагааны төслийг хэрэгжүүлж, Оксфордын их сургуулийн эрдэмтэдтэй хамтран кибер аюулгүй байдлын өнөөгийн түвшнийг үнэлэх судалгааг явуулж байна[42].

[37]Монгол Улсын Их Хурал. (2021а). Кибер аюулгүй байдлын тухай хууль. https://legalinfo.mn/mn/detail?lawId=16390365491061
Монгол Улсын Их Хурал. (2021б). Хүний хувийн мэдээлэл хамгаалах тухай хууль. https://www.undp.org/sites/g/files/zskgke326/files/2024-04/biznesiyn_bayguullaguudad_zoriulsan_garyn_avlaga.pdf
[38] Цахим хөгжил, инновац, харилцаа холбооны яам. (2024, 10-р сарын 10). Кибер гэмт хэргийн улмаас 87.5 тэрбум төгрөгийн хохирол учирчээ. https://mddc.gov.mn/eng/2024/10/19291/
[39] Золбаяр, Ч. (2024, 1-р сарын 15). Долоо хоногт Монголд 90 гаруй мянган кибер халдлага илэрдэг. itoim.mn. https://itoim.mn/a/2024/01/15/society/yek
[40] Цахим хөгжил, инновац, харилцаа холбооны яам. (2025, 1-р сарын 29). 2024 онд хортой кодын халдлагад өртсөн 145 IP-т хариу арга хэмжээ авчээ. https://mddic.gov.mn/eng/2025/01/20833/
[41] Кибер халдлага, зөрчилтэй тэмцэх үндэсний төв. (2023). Бидний тухай. https://ncsirt.gov.mn/p/3Монгол Улсын Засгийн газар. (2023, 8-р сарын 30). "Кибер халдлага, зөрчилтэй тэмцэх нийтийн төв" улсын төсөвт үйлдвэрийн газар байгуулах тухай (Тогтоол № 319). https://legalinfo.mn/mn/detail?lawId=16760334026011
[42] Цахим хөгжил, инновац, харилцаа холбооны яам. (2024а, 9-р сарын 18). Кибер аюулгүй байдал, дроны мэргэжилтнүүдийг бэлдэх чиглэлд ЖАЙКА-тай хамтран ажиллана. https://mddc.gov.mn/mn/2024/09/18657/
Цахим хөгжил, инновац, харилцаа холбооны яам. (2025, 2-р сарын 19). Oxford: Монгол Улс кибер аюулгүй байдлыг хангах хөрөнгө оруулалтыг нэмэгдүүлэх шаардлагатай. https://mddic.gov.mn/eng/2025/02/21011/

*Кибер дархлааны хамгаалалтын механизмууд:*

Кибер дархлааны хамгаалалтын механизмууд нь уламжлалт аюулгүй байдлын арга хэмжээнүүдээс эрс ялгаатай зарчимд тулгуурладаг. Уламжлалт үйлдлийн системүүд суурь давхарга, аппликейшны давхарга, аюулгүй байдлын давхарга гэсэн гурван түвшний бүтэцтэй бөгөөд аюулгүй байдлын давхарга зөрчигдвөл халдагч этгээд доод давхаргуудад нэвтэрч, системийн үйл ажиллагааг бүхэлд нь удирдах боломжтой болдог.

Касперскийн лабораторийн KasperskyOS үйлдлийн систем нь кибер дархлааны хамгаалалтын механизмыг практикт хэрэгжүүлсэн тэргүүлэх жишээ юм. Кибер дархлааны системийн бүрэлдэхүүн хэсэг бүр бие биенээсээ болон гадаад орчноос бүрэн тусгаарлагдсан байдаг бөгөөд ямар нэгэн хяналтгүй харилцан үйлчлэлийг бүрэн арилгадаг. Системийн бүрэлдэхүүн хэсгүүдийн хоорондын мэдээллийн урсгал нь аюулгүй байдлын бодлогод нийцэж байгаа эсэхийг тасралтгүй шалгадаг бөгөөд системийн чухал хөрөнгө, функцид шууд нөлөөлдөг итгэмжлэгдсэн кодын хэмжээ хамгийн бага байхаар тохируулагддаг[43].

Хиймэл оюуны болон машин сургалтын технологи кибер дархлааны системийг улам боловсронгуй болгоход чухал үүрэг гүйцэтгэж байна. Хиймэл оюун ухаан болон машин сургалт нь эмзэг байдлыг эрт илрүүлэх, таамаглахад туслан байгууллагуудад болзошгүй кибер аюулаас урьдчилан хамгаалах идэвхтэй арга хэмжээ авах боломж олгодог. Gartner-ийн таамаглалаар 2025 он гэхэд цахим дархлааны системд хөрөнгө оруулалт хийсэн байгууллагуудын зогсолтын хугацаа 80 хувиар буурах бөгөөд энэ нь хэрэглэгчдийн сэтгэл ханамжийг мэдэгдэхүйц нэмэгдүүлэхэд хүргэнэ[44].

Орчин үеийн кибер аюулгүй байдлын чиг хандлагын хувьд таних мэдэрхүйний дархлааны систем буюу identity fabric immunity нь таних мэдэрхүйний системийг идэвхтэй болон хариу үйлдлийн аргаар хамгаалах, кибер аюулгүй байдлын баталгаажуулалт буюу хяналт, технологи, хүний үйл явцыг тасралтгүй баталгаажуулах зэрэг шинэ механизмууд 2024-2025 онд тэргүүлэх ач холбогдолтой болсон байна[45].

Биологийн дархлааны системийн зарчмыг мэдээллийн технологид хэрэглэсэн хиймэл дархлааны системийн хувьд кибер дархлааны системүүд нь хүн болон амьтны дасан зохицогч дархлааны системийг дуурайлган шинэ, өмнө нь үл мэдэгдэх кибер халдлагыг илрүүлж, саармагжуулах чадвартай байдаг. Уламжлалт галт хана болон халдлага илрүүлэх системүүд өмнө нь тохиолдож байгаагүй халдлагыг илрүүлэхэд хүндрэлтэй байсан бол кибер дархлааны систем

[43]Kaspersky Lab. (2024a). Kaspersky Security System. KasperskyOS. https://os.kaspersky.com/technologies/kaspersky-security-system/
Kaspersky Lab. (2024b). Microkernel. KasperskyOS. https://os.kaspersky.com/technologies/microkernel/
[44] Gartner. (2022). What is a digital immune system and why does it matter? Gartner. https://www.gartner.com/en/articles/what-is-a-digital-immune-system-and-why-does-it-matter
[45]Gartner. (2024, February 22). Gartner identifies top cybersecurity trends for 2024. https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024

биологийн дархлаанаас санаа авсан технологиудыг ашиглан энэ хязгаарлагдмал байдлыг даван туулдаг[46] байна.

## Дүгнэлт

Кибер дархлааны онолын асуудал, дэлхийн жишиг хэрэглээ, Монгол Улсын кибер аюулгүй байдлын өнөөгийн байдал, хамгаалалтын механизмуудыг үндсэн дээр дараах дүгнэлтүүдэд хүрч байна.

Нэгдүгээрт, кибер дархлаа нь уламжлалт хамгаалалтын аргачлалуудын хязгаарлагдмал байдлыг даван туулах боломжийг олгодог шинэлэг үзэл баримтлал юм. Биологийн дархлааны системийг загвар болгосон энэхүү хандлага нь төрмөл аюулгүй байдал, тусгаарлалт, тасралтгүй хяналтын зарчмуудад тулгуурлан системүүдийг халдлагад тэсвэртэй болгож байна.

Хоёрдугаарт, дэлхийн хэмжээнд кибер халдлагын тоо, хохирлын хэмжээ жил ирэх тусам эрс өсч байгаа нь кибер дархлааны системийг нэвтрүүлэх зайлшгүй шаардлагыг тодорхойлж байна. Орчин үеийн нарийн төвөгтэй кибер аюул заналхийлэлтэй тэмцэхийн тулд нийтийн болон хувийн секторийн хоорондын хамтын ажиллагааг бэхжүүлэх нь цахим хөгжлийн үр шимийг хүн бүрт хүргэх чухал нөхцөл болж байна.

Гуравдугаарт, Монгол Улс GCI 2024 тайлангаар Tier-3 буюу "Бэхжиж буй" түвшинд үнэлэгдсэн нь кибер аюулгүй байдлын чиглэлд тодорхой ахиц гарсныг харуулж байгаа боловч техникийн чадавх, хүний нөөцийн бэлтгэл, олон улсын хамтын ажиллагааг цаашид бэхжүүлэх шаардлагатайг илэрхийлж байна.

Дөрөвдүгээрт, хиймэл оюун ухаан болон машин сургалтын технологийг кибер дархлааны системд нэгтгэх нь ирээдүйн кибер аюулгүй байдлын гол чиг хандлага болж байна. Кибер аюулгүй байдлын удирдагчид 2025 онд бизнесийн тасралтгүй байдал болон хамтарсан эрсдэлийн менежментийг чухалчилсан, илүү төвлөрсөн кибер аюулгүй байдлын хөтөлбөрүүдийг хэрэгжүүлэхэд анхаарлаа хандуулж байна.

## Судалгааны үр дүн

Дээрх дүгнэлтүүдэд үндэслэн Монгол Улсын хувьд дараах саналыг гаргаж байна: Кибер дархлааны үзэл баримтлалыг үндэсний кибер аюулгүй байдлын бодлогод тусгах, KasperskyOS зэрэг кибер дархлааны зарчимд суурилсан технологиудыг стратегийн дэд бүтцэд нэвтрүүлэх, хиймэл оюун ухаанд суурилсан аюул илрүүлэх системийг хөгжүүлэх, мөн кибер аюулгүй байдлын мэргэжилтнүүдийн тоог нэмэгдүүлэх чиглэлд хөрөнгө оруулалтыг эрчимжүүлэх нь асуудлыг авч үзэх шаардлагатай юм.

---

[46] Kousalya, G., et al. (2023). Artificial immune systems in local and network cybersecurity: An overview of intrusion detection strategies. Advances in Computational Intelligence and Its Applications Journal. https://www.acigjournal.com/Artificial-Immune-Systems-in-Local-and-Network-Cybersecurity-An-Overview-of-Intrusion,184306,0,2.html
Stanton, C., Katz, G., & Song, D. (2024). Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response. IEEE Access. https://www.researchgate.net/publication/383758233

## Эш татсан сурвалж, судалгааны бүтээлийн жагсаалт

[1] Kaspersky. (2022, November 23). What is cyber immunity, and how to build an operating system based on the concept? Kaspersky Blog. https://www.kaspersky.com/blog/how-to-create-cyberimmune-system/46314/

[2] DOI: 10.65902/tsats.2026.01.002 Experience and Lessons from Human security in the cyber environment: Risks and key protection issues

[3] Wlodarczak, P. (2017). Cyber immunity. In I. Rojas & F. Ortuño (Eds.), Bioinformatics and biomedical engineering (Lecture Notes in Computer Science, Vol. 10209, pp. 1-9). Springer. https://doi.org/10.1007/978-3-319-56154-7_19 https://doi.org/10.1007/978-3-319-56154-7_19

[4] Kaspersky, E. (2021, November 12). Transition from cybersecurity to cyber-immunity. IRISSCON 2021. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/transition-cyber-immunity-kaspersky/

[5] Check Point Research. (2024). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Blog. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

[6] Cobalt. (2024). Top cybersecurity statistics for 2024. https://www.cobalt.io/blog/cybersecurity-statistics-2024

[7] SentinelOne. (2024). Key cybersecurity statistics. https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-statistics/

[8] Check Point Research. (2024). A closer look at Q3 2024: 75% surge in cyber attacks worldwide. Check Point Blog. https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/

[9] Butt, U. A., Amin, R., Aldabbas, H., Garg, S., Alroobaea, R., & Almotiri, S. H. (2021). Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. PMC

[10] Kaspersky Lab. (2025). What is cyber immunity? Kaspersky IT Encyclopedia. https://encyclopedia.kaspersky.com/glossary/cyberimmunity/

[11] Software Engineering Institute. (2024). DevOps case study: Netflix and the Chaos Monkey. Carnegie Mellon University. https://www.sei.cmu.edu/blog/devops-case-study-netflix-and-the-chaos-monkey/

[12] Allied Market Research. (2023). Digital immune system market size, share, competitive landscape and trend analysis report: Global opportunity analysis and industry forecast, 2023-2032. https://www.alliedmarketresearch.com/digital-immune-system-market-A77311

[13] International Telecommunication Union. (2024). Global Cybersecurity Index 2024. ITU. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

[14] State Great Khural of Mongolia. (2021a). Law on Cybersecurity. https://legalinfo.mn/mn/detail?lawId=16390365491061

[15] State Great Khural of Mongolia. (2021b). Law on the Protection of Personal Data. https://www.undp.org/sites/g/files/zskgke326/files/2024-04/biznesiyn_bayguullaguudad_zoriulsan_garyn_avlaga.pdf

[16] Ministry of Digital Development, Innovation, and Communications. (2024, October 10). Cybercrime caused 87.5 billion MNT in damages. https://mddc.gov.mn/eng/2024/10/19291/

[17] Zolbayar, Ch. (2024, January 15). Over 90,000 cyberattacks are detected in Mongolia each week. itoim.mn. https://itoim.mn/a/2024/01/15/society/yek

https://doi.org/10.1149/MA2024-01115mtgabs

[18] Ministry of Digital Development, Innovation, and Communications. (2025, January 29). In 2024, countermeasures were taken against 145 IP addresses affected by malicious code attacks. https://mddic.gov.mn/eng/2025/01/20833/
[19] National Center for Combating Cyber Attacks and Incidents. (2023). About Us. https://ncsirt.gov.mn/p/3
[20] Government of Mongolia. (2023, August 30). On the establishment of the "Public Center for Combating Cyber Attacks and Incidents" as a state budget enterprise. (Decision No. 319). https://legalinfo.mn/mn/detail?lawId=16760334026011
[21] Ministry of Digital Development, Innovation, and Communications. (2024a, September 18). Collaborating with JICA to train cybersecurity and drone specialists. https://mddc.gov.mn/mn/2024/09/18657/
[22] Ministry of Digital Development, Innovation, and Communications. (2025, February 19). Oxford: Mongolia needs to increase investment to ensure cybersecurity. https://mddic.gov.mn/eng/2025/02/21011/
[23] Kaspersky Lab. (2024a). Kaspersky Security System. KasperskyOS. https://os.kaspersky.com/technologies/kaspersky-security-system/
[24] Kaspersky Lab. (2024b). Microkernel. KasperskyOS. https://os.kaspersky.com/technologies/microkernel/
[25] Gartner. (2022). What is a digital immune system and why does it matter? Gartner. https://www.gartner.com/en/articles/what-is-a-digital-immune-system-and-why-does-it-matter
[26] Gartner. (2024, February 22). Gartner identifies top cybersecurity trends for 2024. https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024
[27] [Ousalya, G. et al. (2023). Artificial immune systems in local and network cybersecurity: An overview of intrusion detection strategies. Advances in Computational Intelligence and Its Applications Journal. https://www.acigjournal.com/Artificial-Immune-Systems-in-Local-and-Network-Cybersecurity-An-Overview-of-Intrusion,184306,0,2.html https://doi.org/10.60097/ACIG/162896
[28] Stanton, C., Katz, G., & Song, D. (2024). Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response. IEEE Access. https://www.researchgate.net/publication/383758233