



ЗАМ, ТЭЭВРИЙН ЯАМ

“МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН МЕНЕЖМЕНТ”

- Эрсдэл
- ISO 27000
- Тоон гарын үсэг



Хөтөлбөр үзэх





Б.ӨСӨХБАЯР
МУИС-ийн Мэдээллийн Технологи,
Электроникийн сургууль
Дэд профессор



- Кибер халдлага, кибер аюулгүй байдлыг хангах техник, технологи.

Кибер халдлага, кибер аюулгүй байдлыг хангах техник, технологи

Б.Өсөхбаяр (Ph.D)

МОНГОЛ УЛСЫН ИХ СУРГУУЛЬ

МЭДЭЭЛЛИЙН ТЕХНОЛОГИ, ЭЛЕКТРОНИКИЙН СУРГУУЛЬ

Агуулга

- Introduction to Cyber security
- National Cyber Threat News and Statistic
- Knowledge areas
- Staying current with industry



Today's Cyber Environment

- Increasing dependence and interdependence
- Critical business and government operations are increasingly dependent on the internet and others ICT systems/applications
- Business practices dictate increased interaction, interdependence: global supply chains, global clients and partners, global customers, global infrastructure e.g. overseas production plant or outsourcing, financing investment and operations goes multinational
- Others sector transportation, healthcare, emergency services



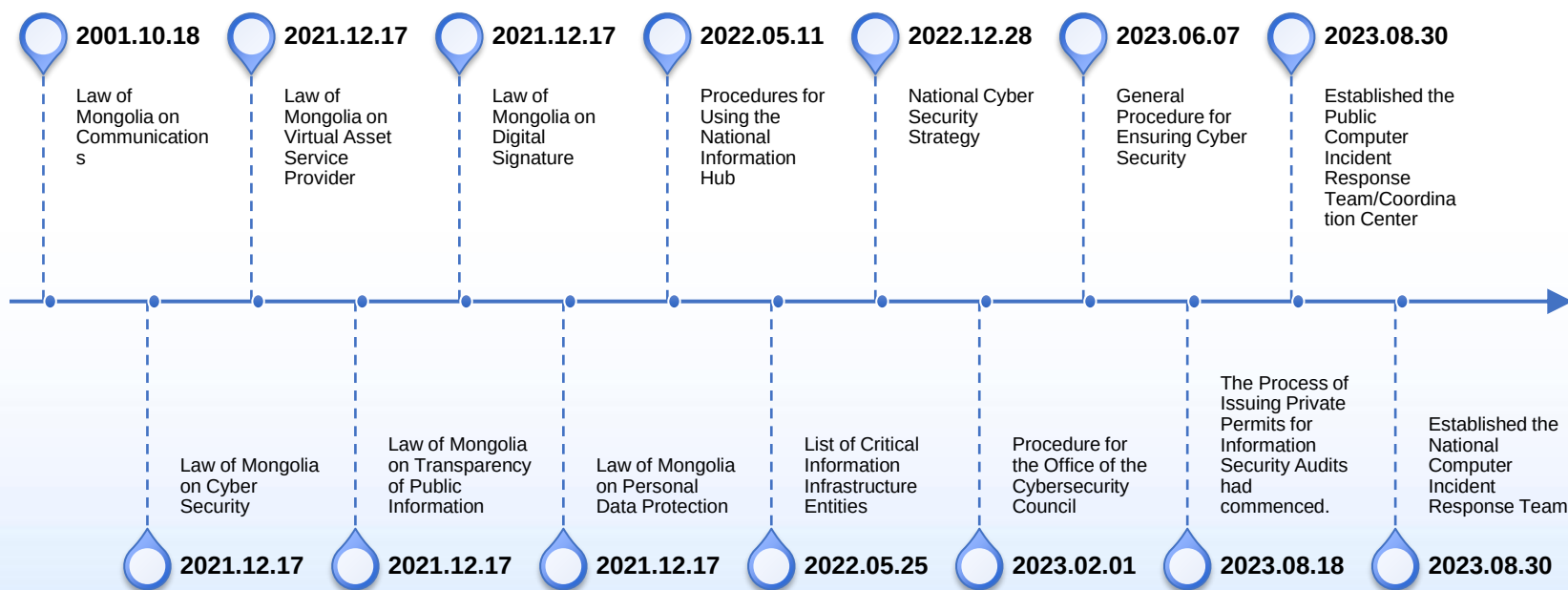
More Value (.mn Context)

- **Internet & Social Media:** 80% internet penetration, nearly 1 million social media users (LinkedIn: 290K, Instagram: 936K, Twitter: 129K)
- **Mobile Network:** Coverage reaches 82% (2G: 100%, 3G: 95%, 4G: 85%). No 5G yet.
- **Internet Speed:** Mobile download averages 26.4 Mbps; fixed broadband is at 50.1 Mbps.
- **Digital Growth:** Expanding in e-commerce and telework, though still in development.: Ranked 74th globally by the UN, with a 0.72 E-Government Index score and 0.84 in Human Capital Index.
- **Digital Growth:** Expanding in e-commerce and telework, though still in development.

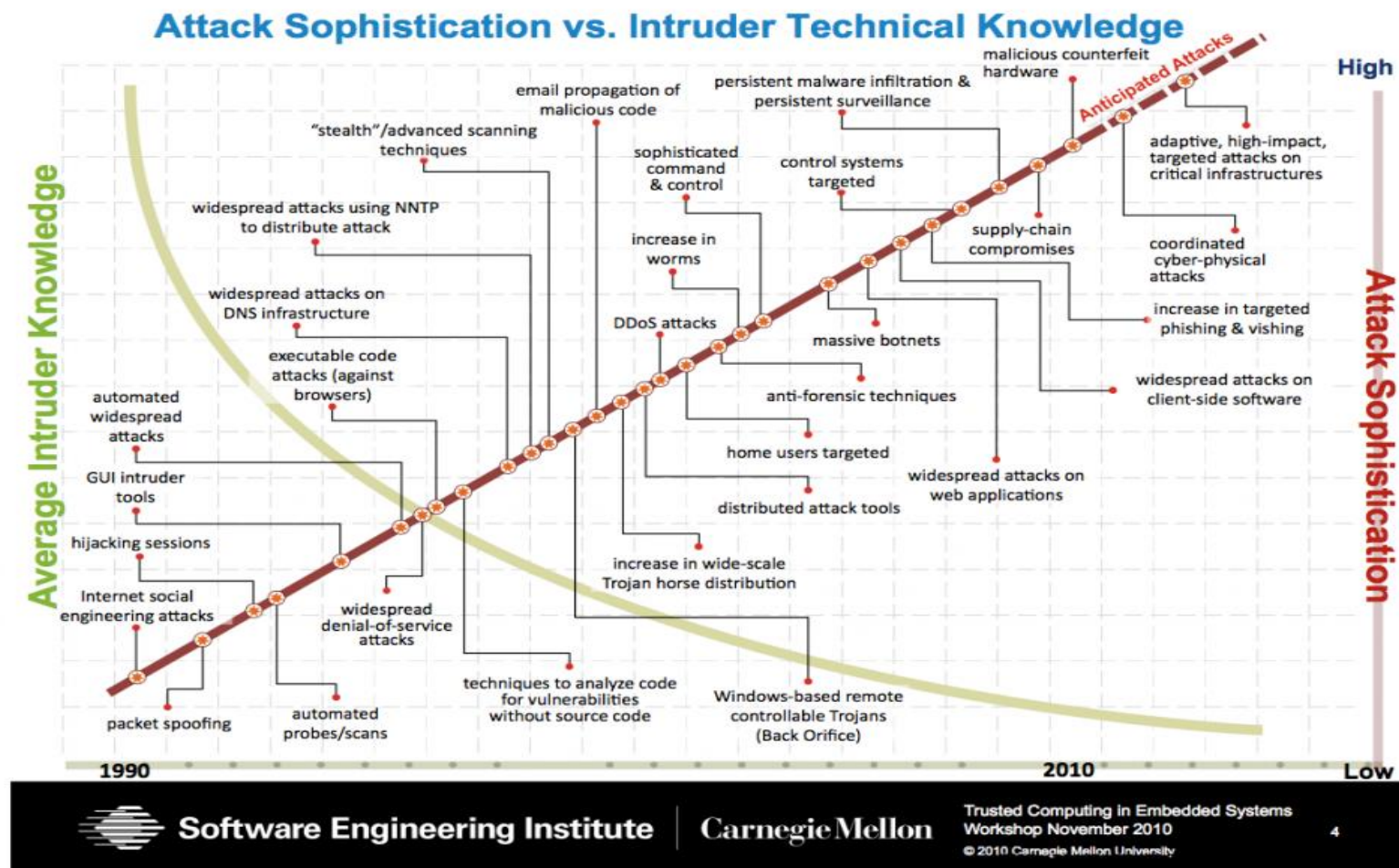
References: [Digital 2024: Mongolia – DataReportal - Global Digital Insights](#)



History Timeline 2001 - 2023



Trends in Attack Sophistication and Intruder Knowledge



National Cyber Threat News and Statistic

- 2022: Mongolia recorded 976 cybercrimes, showing a significant increase over the years.(Sources: thediplomat.com)
- August 2023: Mongolia's national data center was compromised by a cyberattack, with hackers demanding an \$8 million ransom. (Sources: thediplomat.com)
- August 2024: Google uncovered a Russian group targeting the Mongolian government with exploits used by NSO Group. (Sources: therecord.media)
- 7 Ransomware victims from Mongolia (Sources: <https://www.ransomware.live/map/MN>)



Top 5 Most Affected Sectors

- **Government**

- Web Defacement
- Malware Attack
- DDoS
- Phishing

- **Digital Economy**

- Malware Attack
- Phishing
- Brute force

- **Financial**

- Malware Attack
- Phishing

- **Education**

- Web Defacement
- Malware Attack

- **Industry**

- Malware Attack
- Phishing

Source : ID-SIRTII/CC Annual Report

<https://idsirtii.or.id/halaman/tentang/laporan-hasil-monitoring.html>



Cyber Threat Maps

- Check out the following cyber threat maps:
 - Threatbutt Internet Hacking Attribution Map
 - <https://threatbutt.com/map>
 - Check Point ThreatCloud Live Cyber Threat Map
 - <https://threatmap.checkpoint.com/ThreatPortal/livemap.html>
 - Deteque Botnet Threat Map
 - <https://www.spamhaus.com/threat-map/>
 - Kaspersky Cyberthreat Real-Time Map
 - <https://cybermap.kaspersky.com/>
 - Digital Attack Map
 - <http://www.digitalattackmap.com>
 - Talos Cyber Attack Map: Top Spam and Malware Senders
 - https://talosintelligence.com/fullpage_maps/pulse

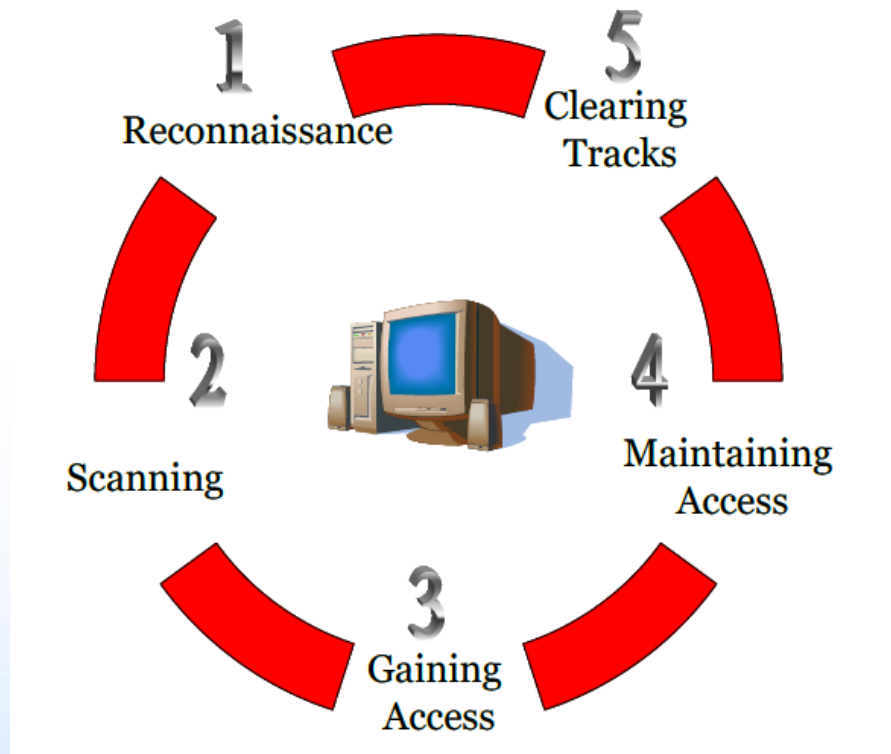
Attackers

- significant issue for networked systems is hostile or unwanted access either via network or local
- can identify classes of intruders (or hacker or cracker):
 - outsider (гадаад)
 - masquerader (дуурайгч)
 - insider (дотоод)
 - misfeasor (эрхээ хэтрүүлэгч)
 - either (аль аль нь)
 - clandestine user (нууц буюу далд хэрэглэгч)
- Intruder attacks range from the benign (simply exploring net to see what is there); to the serious (who attempt to read privileged data, perform unauthorized modifications, or disrupt system)

Hacking steps

The seven steps to a successful cyber attack

- 1. Reconnaissance via social engineering or other methods
 - 2. Scanning (passive or active)
 - 3. Gaining access
 - 4. Maintaining access
 - 5. Creating backdoors and covering tracks (cleanup)
-
- http://www.pentest-standard.org/index.php/Main_Page



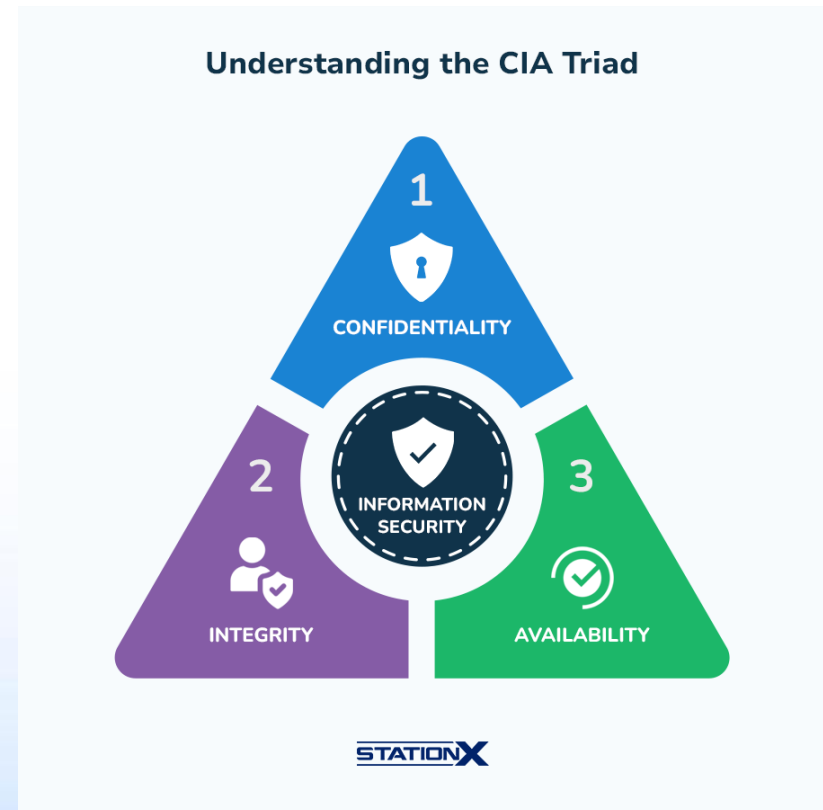
AI based attack

- <https://github.com/friuns2/BlackFriday-GPTs-Prompts/blob/main/gpts/blackhathacker.md>
- <https://chatgpt.com/g/g-j4PQ2hyqn-ethical-hacker-gpt/c/6791543f-3e00-8000-9ac2-9e9a2bd02d5c>
- <https://pentestgpt.ai/c971170a-5b1f-4be6-8360-6feed2e15aab/chat>
- https://github.com/TheR1D/shell_gpt

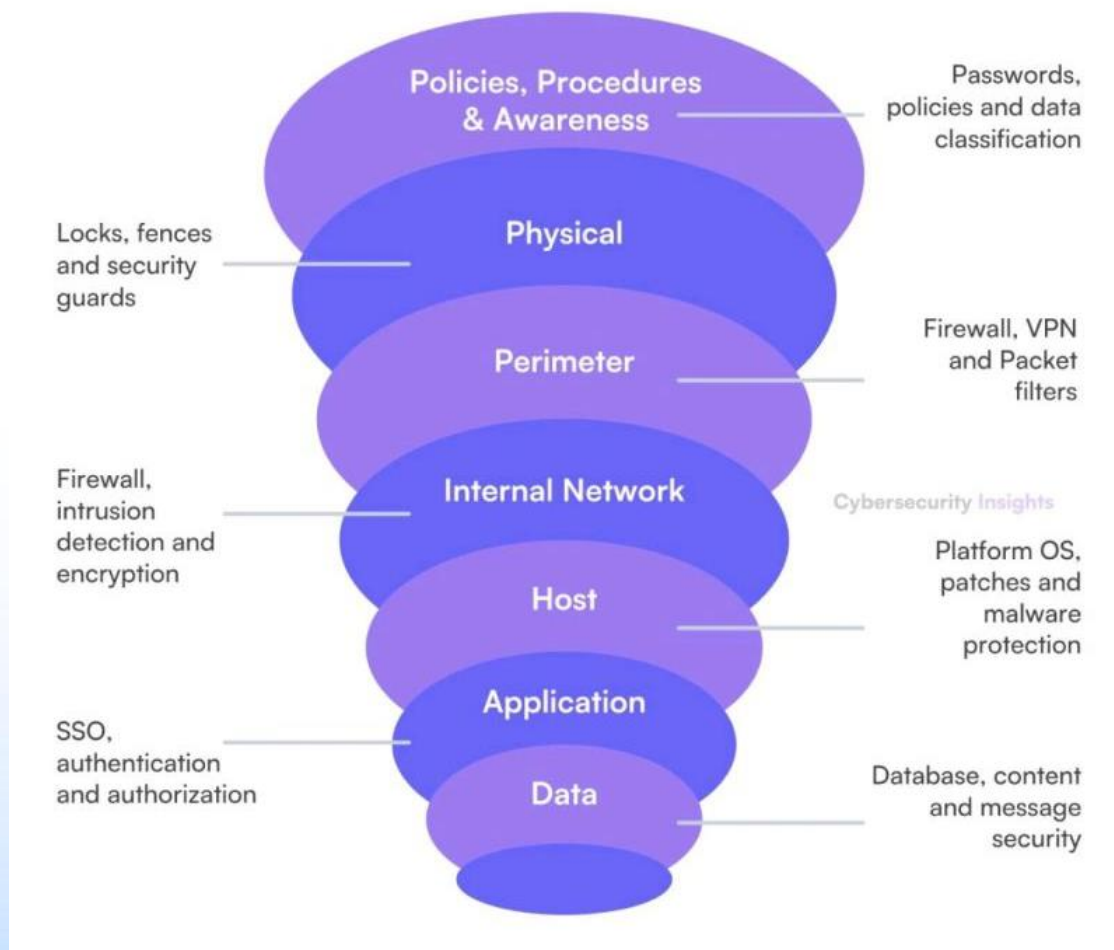


BASIC PRINCIPLES

- Confidentiality, Integrity, Availability (CIA triad)
- Principle of Least Privilege
- Defense in Depth



DEFENSE IN DEPTH



- <https://www.sans.org/information-security-policy/>
- <https://urlscan.io/>
- <https://www.virustotal.com/gui/home/upload>
- <https://urlhaus.abuse.ch/>
- <https://sslbl.abuse.ch/>
- <https://threatfox.abuse.ch/>
- <https://urlhaus.abuse.ch/>
- <https://abuse.ch/>
- <https://github.com/OpenCTI-Platform/opencti?tab=readme-ov-file>
- <https://github.com/rsmusllp/king-phisher>

Password security

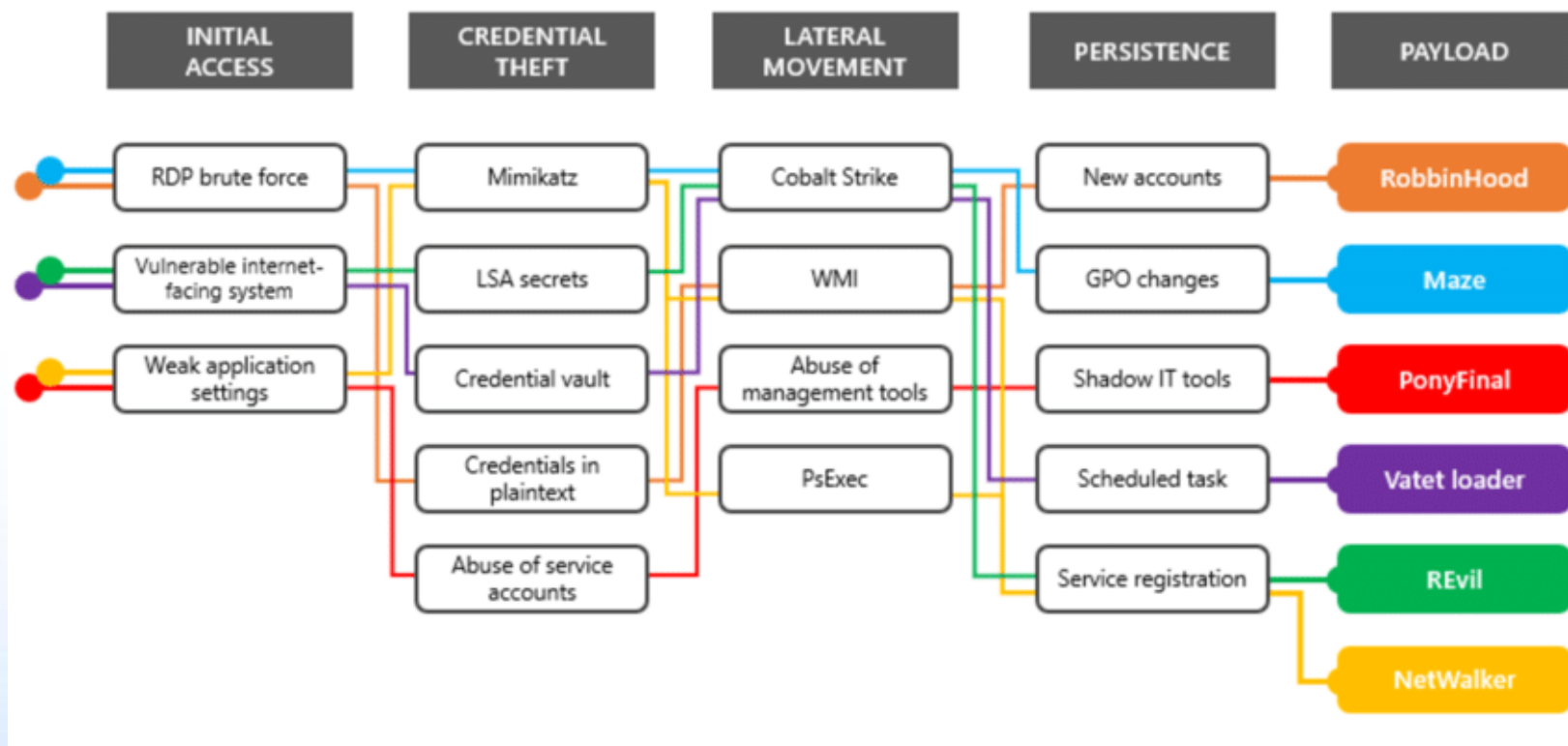
- <https://www.passwordmonster.com/>
- <https://devlateral.com/tools/password-entropy-calculator>
- https://en.wikipedia.org/wiki/Wikipedia:10,000_most_common_passwords
- [top most common and seen passwords](#)
- <https://www.skullsecurity.org/wiki/Passwords>
- <https://keepass.info/>



What Is Threat Hunting?

- Threat hunting provides a proactive opportunity for an organization to uncover attacker presence in an environment.
- Leading global cybersecurity authority SANS defines threat hunting as the “proactive, analyst-driven process to search for attacker tactics, techniques, and procedures (TTP) within an environment.”

Human-Operated Ransomware Lifecycle



- <https://www.microsoft.com/en-us/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/>

Step for Threat Hunting

- **Step 1: Gather Comprehensive Data and Logs from your Cloud Environment**
 - This involves collecting high-quality data from various sources in your cloud environment. Key sources include log files (traffic flow and event activity logs being particularly valuable), servers, network devices, databases, and endpoints. This comprehensive data serves as the foundation for effective threat hunting.
- **Step 2: Analyze Data for Indicators of Compromise (IOCs)**
 - Threat hunters then analyze this collected data within the context of known threats. The goal is to identify patterns and potential indicators of compromise (IOCs) that might signify malicious activity. This ongoing process is crucial for effective monitoring, but resource limitations can sometimes hinder it.
- **Step 3: Leverage Threat Hunting Tools for Efficiency**
 - While threat hunters possess valuable skills, the sheer volume of cloud logs can make it challenging to identify all suspicious activity manually. This is where advanced threat hunting tools come into play. They can automate the analysis of collected data, alerting you to anomalies like outbound traffic to nodes or unauthorized access token usage. This streamlines the process and improves the efficiency of threat hunting.



MITRE ATT&CK Framework

- Under [MITRE's D3FEND™](#) matrix, the use of logs is broadly applicable under the Detect category.
- By monitoring security logs, organizations can identify suspicious activity, such as command and control activity, lateral movement, or other techniques as described in [MITRE's ATT&CK®](#) matrix.
- Detection would then allow network defenders to take appropriate mitigation actions against the threat.

D3FEND Tactic	Countermeasures
Detect	Network Traffic Analysis [D3-NTA]
Detect	Platform Monitoring [D3-PM]
Detect	Process Analysis [D3-PA]
Detect	User Behavior Analysis [D3-UBA]

Vulnerability Resource

1. CERT Vulnerability Notes Database

<https://www.kb.cert.org/vuls/>

2. National Vulnerability Database

<https://nvd.nist.gov/>

3. Common Vulnerabilities and Exposures

<https://cve.mitre.org/>

4. Vulnerability Database

<https://vuldb.com/>

5. CVE Security Vulnerability Database

<https://www.cvedetails.com/>

6. WhiteSource Vulnerability Database

<https://www.whitesourcesoftware.com/vulnerability-database/>



What is the NIST Framework?

- The National Institute of Standards and Technology (NIST) has published a [Cybersecurity Framework \(CSF\)](#) that aims to help organizations identify their cyber risks by providing guidance on best practices in cybersecurity planning and incident response. The CSF is based on five core functions:
 1. **Identify:** finding assets, systems, and networks as well as classifying information to help prioritize security efforts.
 2. **Protect:** safeguarding systems and data from unauthorized access or modification, including measures such as [firewalls](#), [intrusion detection/prevention](#) systems, and [anti-virus software](#).
 3. **Detect:** uncovering malicious activity or anomalous behavior to respond promptly to potential threats.
 4. **Respond:** taking the necessary steps when a security incident has occurred, including containment, eradication, and recovery.
 5. **Recover:** restoring normal operations and business functions after a security incident has occurred.

OSINT Framework

- The **OSINT framework** is a methodology that integrates data, processes, methods, tools and techniques to help the security team identify information about an adversary or their actions quickly and accurately.
- OSINT framework focused on gathering information from free tools or resources.
- <https://osintframework.com/>

Formal Methodologies

- Kevin Orrey's penetration testing framework:
 - This methodology walks the tester through the sequenced steps of a penetration test, providing hyperlinks to tools and relevant commands.
 - More information can be found at www.vulnerabilityassessment.co.uk.
- Information Systems Security Assessment Framework (ISSAF):
 - This comprehensive guide aims to be the single source for testing a network.
 - More information on this can be found at www.oisssg.org



- NIST SP 800-115, technical guide to information security testing and assessment:
- Written in 2008, the four-step methodology is somewhat outdated. However, it does provide a good overview of the basic steps in penetration testing.
- More information at
- <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>.
- Open Source Security Testing Methodology Manual (OSSTMM):
- This is one of the older methodologies, and the latest version attempts to quantify identified risks. More details can be found at www.osstmm.org

- Open Web Application Security Project (OWASP): This is focused on the 10 most common vulnerabilities in web-based applications. More information on this can be found at www.owasp.org
- Penetration Testing Execution Standard (PTES): Actively maintained, this methodology is complete and accurately reflects on the activities of a malicious person. You can get more information at www.pentest-standard.org
- Offensive (Web) Testing Framework (OWTF): Introduced in 2012, this is a very promising direction in combining the OWASP approach with the more complete and rigorous PTES methodology. More details can be found at <https://github.com/7a/owtf>.

Staying Current with Industry

- There's one more important thing to understand about cybersecurity: it's constantly changing! You'll need to stay up to date with everything in the field on a daily basis.
- You'll need to reinvent yourself often and understand that what you learn and master at one point in time could be completely obsolete, worthless, and ineffective down the road.
- To follow professionals, especially cybersecurity professionals on social media:
 - **LinkedIn**
 - **Twitter**
 - **Instagram**
 - **Facebook**



Grzegorz Tworek @Ogtweet · 17h

Simple tool enabling all privileges in the parent process (usually cmd.exe) token. Useful if you have SeBackup or SeRestore and need a cmd.exe ignoring all ACLs. C code and the compiled .exe as usual. With a link to the demonstration in the README: github.com/gtworek/PSBits...

```
cmd.exe
C:\temp>whoami /priv

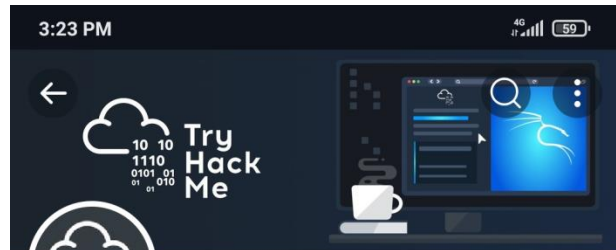
PRIVILEGES INFORMATION
-----
Privilege Name        Description                                     State
-----
SeShutdownPrivilege   Shut down the system                           Disabled
SeChangeNotifyPrivilege Bypass traverse checking                       Enabled
SeUndockPrivilege      Remove computer from docking station           Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set                 Disabled
SeTimeZonePrivilege    Change the time zone                          Disabled

C:\temp>EnableAllParentPrivileges.exe
Enabling privilege 0x13 (SeShutdownPrivilege) ... SUCCESS
Enabling privilege 0x17 (SeChangeNotifyPrivilege) ... SUCCESS
Enabling privilege 0x19 (SeUndockPrivilege) ... SUCCESS
Enabling privilege 0x21 (SeIncreaseWorkingSetPrivilege) ... SUCCESS
Enabling privilege 0x22 (SeTimeZonePrivilege) ... SUCCESS

C:\temp>whoami /priv

PRIVILEGES INFORMATION
-----
Privilege Name        Description                                     State
-----
SeShutdownPrivilege   Shut down the system                           Enabled
SeChangeNotifyPrivilege Bypass traverse checking                       Enabled
SeUndockPrivilege      Remove computer from docking station           Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set                 Enabled
SeTimeZonePrivilege    Change the time zone                          Enabled

C:\temp>
```



TryHackMe

@RealTryHackMe

An online platform that makes it easy to break into and upskill in cyber security, all through your browser. Discord: discord.gg/tryhackme

tryhackme.com Joined November 2018

105 Following 90.6K Followers



Followed by @4n6lady, CyCatz, Ben Sadeghipour, and 3 others

Tweets Tweets & replies Media Likes



CYBERSECURITY >

Public group · 158K members



You Mentorship Featured Topics F



Q&A





Э.БАТТӨР

“Үндэсний дата төв”
УТУГ-ын Мэдээллийн
технологийн газрын дарга,
Кибер аюулгүй байдлын
мастер



- Мэдээллийн аюулгүй байдал гэж юу вэ
МАБ-ын талаарх төрийн бодлого, ҮДТ-өөс
хэрэгжүүлж буй МАБ-ын стандарт, дүрэм,
журам



2025

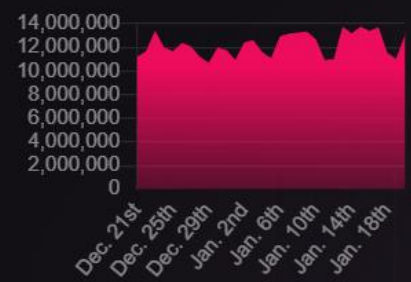


LIVE CYBER THREAT MAP

7,645,374 ATTACKS ON THIS DAY

DON'T WAIT TO BE ATTACKED
PREVENTION STARTS **NOW >**

RECENT DAILY ATTACKS



ATTACKS Current rate - 1 +

- Web Servers Code Execution Over H...
21:37:29 Russia → Russia
- NTP Servers Monlist Command Deni...
21:37:28 South Africa → South Africa
- TLS Servers Cipher Suites Scanning T...
21:37:26 VA, United States → Bermuda
- VER0 Cross-Site Scripting Obfuscatio...
21:37:25 United States → Canada
- TLS Servers Cipher Suites Scanning T...
21:37:24 VA, United States → Bermuda



TOP TARGETED COUNTRIES

Highest rate of attacks per organization in the last day.

- Ethiopia
- Nepal
- Macao
- Mongolia
- Georgia

TOP TARGETED INDUSTRIES

Highest rate of attacks per organization in the last day.

- Education
- Government
- Telecommunications

TOP MALWARE TYPES

Malware types with the highest global impact in the last day.

- Phishing
- Mobile
- Worm

- Malware
- Phishing
- Exploit



INFOSEC vs CYBERSEC

A Guide Anyone Can Understand

THE PROTECTION PARTNERSHIP



Security threats today **don't respect boundaries** - an attack can start with a stolen paper document, and a physical breach can lead to digital theft. Having **both InfoSec and Cybersecurity** working **together** creates a **complete shield** that protects your organization from all angles. Think of it as having both a lock and an alarm system - **one without the other leaves you vulnerable**.



INFORMATION SECURITY



VS CYBERSECURITY



The Big Picture: InfoSec is like a security guard who protects everything: your employees, your building, papers, computers and even ideas.

Protection Methods: InfoSec teams use everything from security cameras to document shredders. They think about locks, alarms, and computer security.

The threats: InfoSec tackles it all - from someone stealing files from a desk to a flood in the server room.

Information Types: InfoSec protects everything from old paper files to trade secrets.

The Big Picture: Cybersecurity is the tech specialist on the team, focused purely on digital threats.

Protection Methods: Cybersecurity folks live in the digital world. They're all about firewalls, software updates, and fighting off hackers.

The Threats: Cybersecurity zeroes in on digital dangers: malware, ransomware, hackers trying to break in through your network

Information Types: Cybersecurity focuses on digital data: if it's not in a computer or on a network, it's not their problem.

WORKING TOGETHER

InfoSec sets the big security strategy, while Cybersecurity handles all digital matters under that plan. Think of InfoSec as the **architect designing the security blueprint**, with Cybersecurity bringing the **technical know-how to make it work** in today's digital world.



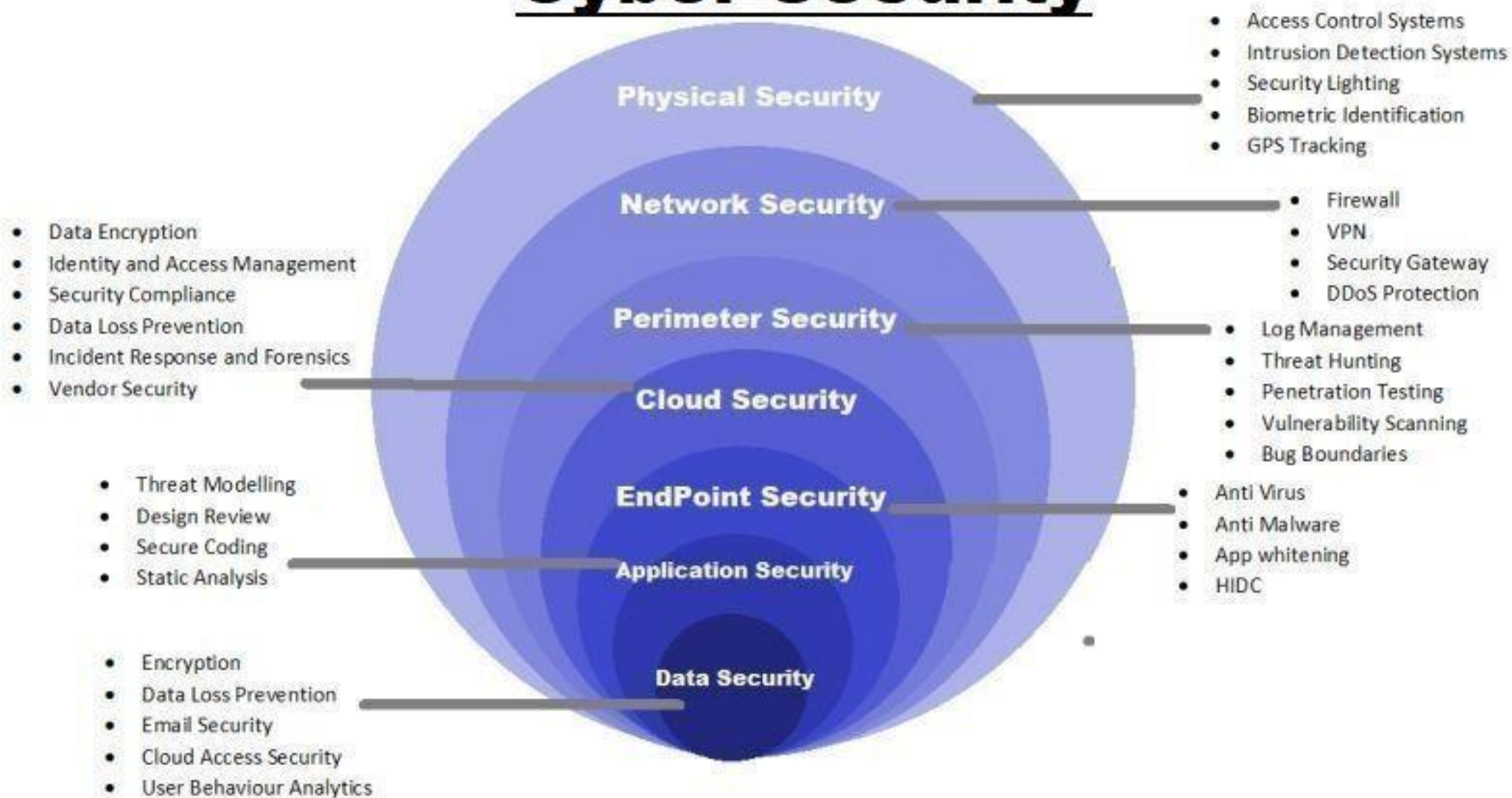
Irina
Munteanu

Found this helpful?



Share it with your network & follow me for more.

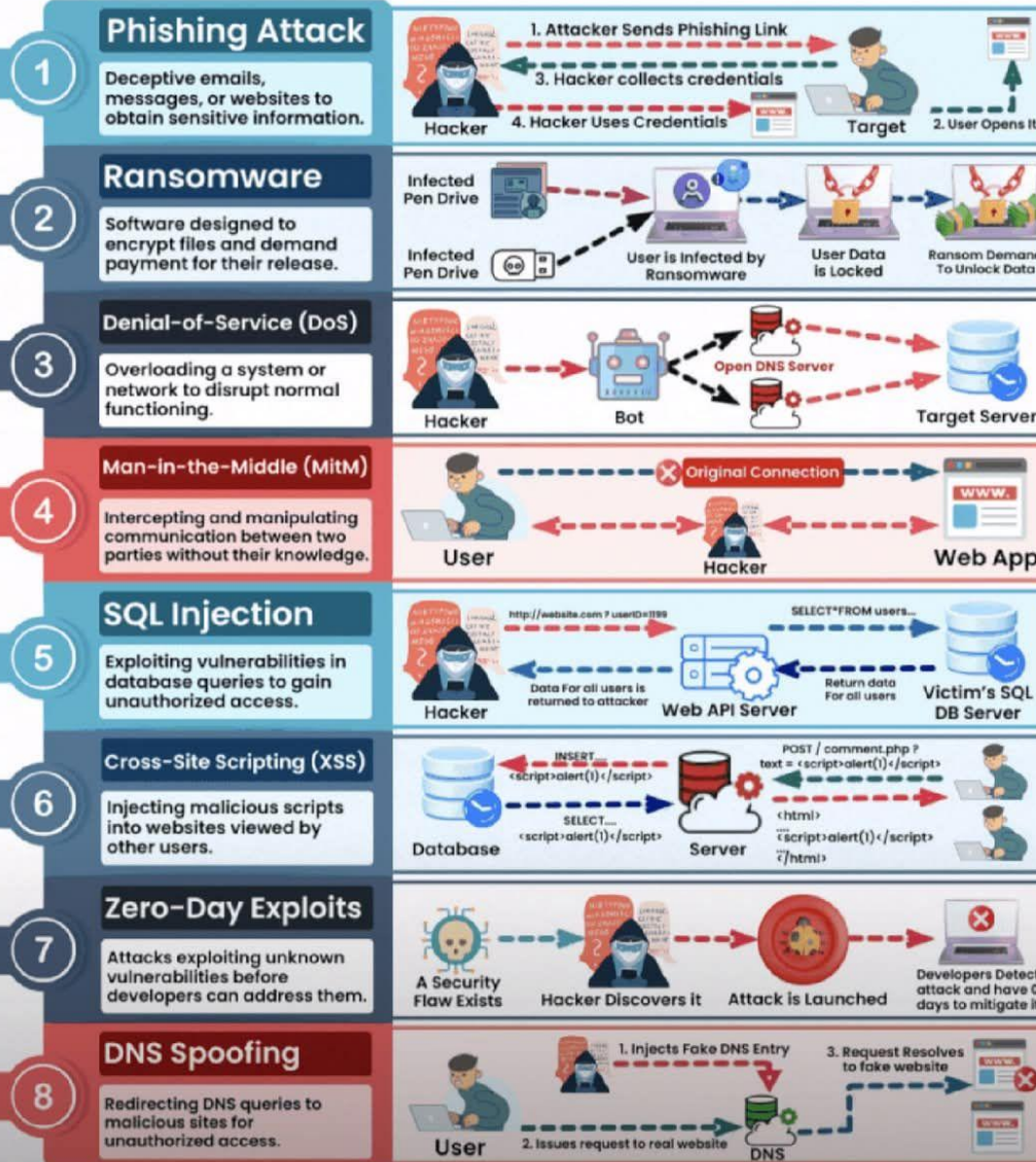
Cyber Security



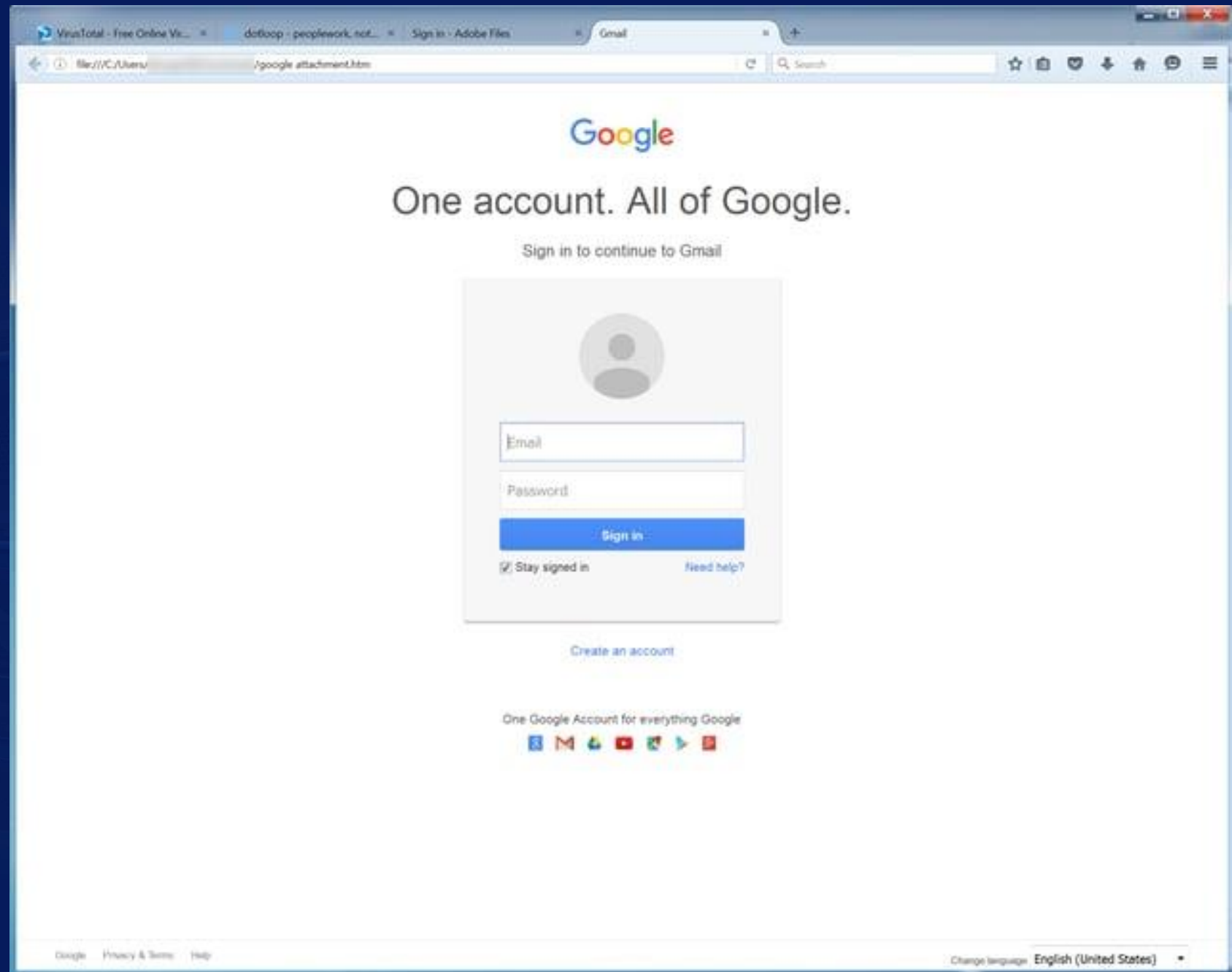
- The Global **Cyber Security Market** size is expected to be worth around USD **533.9 Billion** by 2032 from USD **193 Billion** in 2023, growing at a CAGR of **11%** during the forecast period from 2022 to 2032.
- Every **39 seconds** there's an attack by hackers.
- Healthcare is still the most targeted victim of ransomware attacks.
- **92%** of malware was distributed via email.
- **4.1 million** websites are infected by malware at any moment.
- **49 days** is the standard amount of time needed to spot a ransomware infection.
- A total of **\$29M** was snatched from the fintech firm by hackers.
- **97%** of security breaches are caused by WordPress plugins.
- A total of **\$3 billion** in cryptocurrency was stolen during hacks that have been ongoing to this day.
- **66%** of CIOs have said they intend to increase their investment in cybersecurity.
- The statistics on cybersecurity for remote work indicate that **74%** of IT experts believe that it is an extreme risk to cybersecurity.

(Source: Tripwire)

Top 8 Types of Cyber Attacks









2009.06.24



2024 он



2009 – 06 – 24
Засгийн газрын 2009 оны 183
дугаар
тогтоолоор байгуулсан.

2022 – 05 – 01
Нийтийн мэдээллийн тухайн
хуулийн 35-р зүйл дээр
Үндэсний дата төвийн чиг
үүргийг хуульчилж өгсөн.



Үл тасалдах цахилгаан

- Үл тасалдах цахилгаан тэжээл (UPS)
- Нөөц цахилгаан үүсгүүр (Battery)
- Цахилгаан хангамжийн ослын удирдлагын систем
- Автомат удирдлага бүхий генератор (380/220V 50Hz, 500KW)

Зориулалтын орчин

- Серверийн зориулалтын орчин
- Хөргөлт, чийгшил тогтворжуулах систем
- Автомат гал унтраах систем (**FM200**)
- Утаа, дулаан мэдрэгчүүд

Орчны хамгаалалт

- Орчны хамгаалалт, нэвтрэлтийг хянах систем
- **CCTV** (Хөдөлгөөн мэдрэгчтэй камер)
- Төрийн тусгай хамгаалалтын газрын харуул хамгаалалт

Хяналтын систем

- Сүлжээ, систем, аюулгүй байдлын хяналтын нэгдсэн систем
- **FMS** (Facility Management System)
- **24/7** мониторинг



Нийт талбай
✓ 6,500 м2

Барилгын талбай
✓ 1307 м2

НӨӨЦ ТӨВ

ҮНДСЭН ТӨВ

219KM ЗАЙТАЙ

ДАРХАН

Улаанбаатар

УБЕГ

ХҮР

Татвар

НДЕГ

СЯ

ЗХУТ

E-mongolia

ДАН

✗ Төрийн нэгдсэн сүлжээ

УБЕГ

ХҮР

Татвар

НДЕГ

СЯ

ЗХУТ

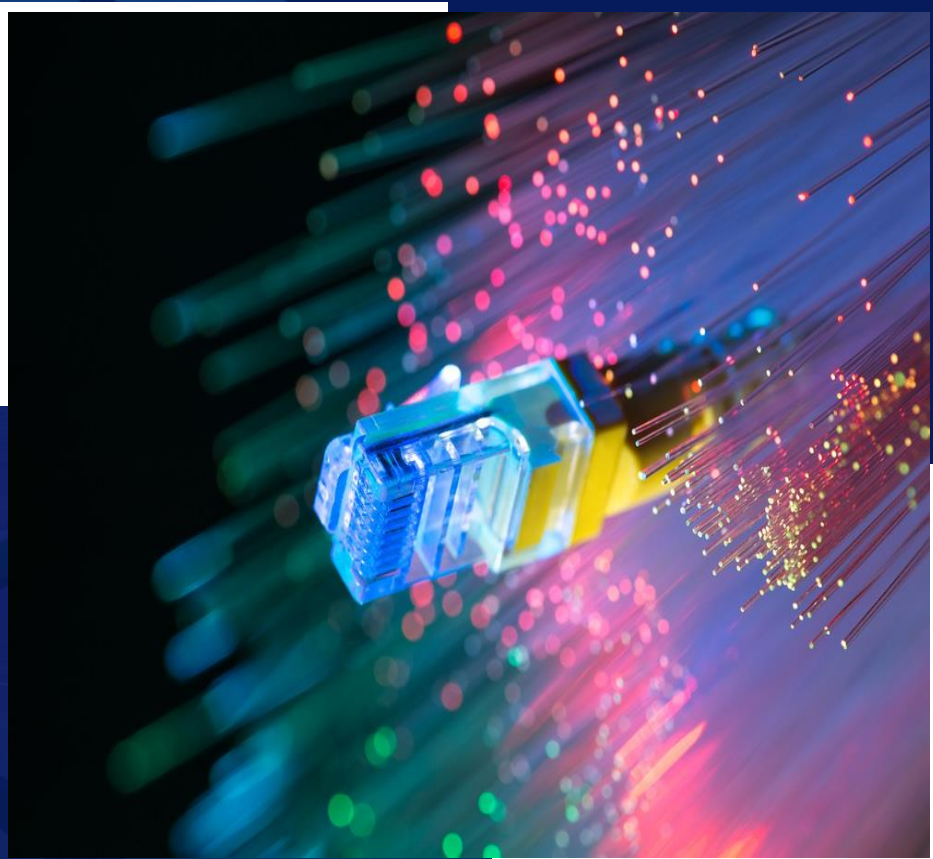
E-mongolia

ДАН

✓ Төрийн нэгдсэн сүлжээ

ҮЙЛЧИЛГЭЭ

2023 он



2009.06.24



1,687
ЦАХИМ
ХУУДАС



56,638
ЦАХИМ ШУУДАН



4,284
ДОМЭЙН НЭР



1,062,813
ТООН ГАРЫН
ҮСЭГ



717
СЕРВИС



4,160,330
Мэдэгдэл хургах
систем



153
БАЙГУУЛЛАГ
ЫН 685
СЕРВЕР



128
БАЙГУУЛЛАГ
ЫН 837 VPS



104 ТҮЦ
МАШИН
37 ТӨРЛИЙН
ҮЙЛЧИЛГЭЭ



Танилт,
нэвтрэлтийн сист
2,049,497
хэрэглэгч



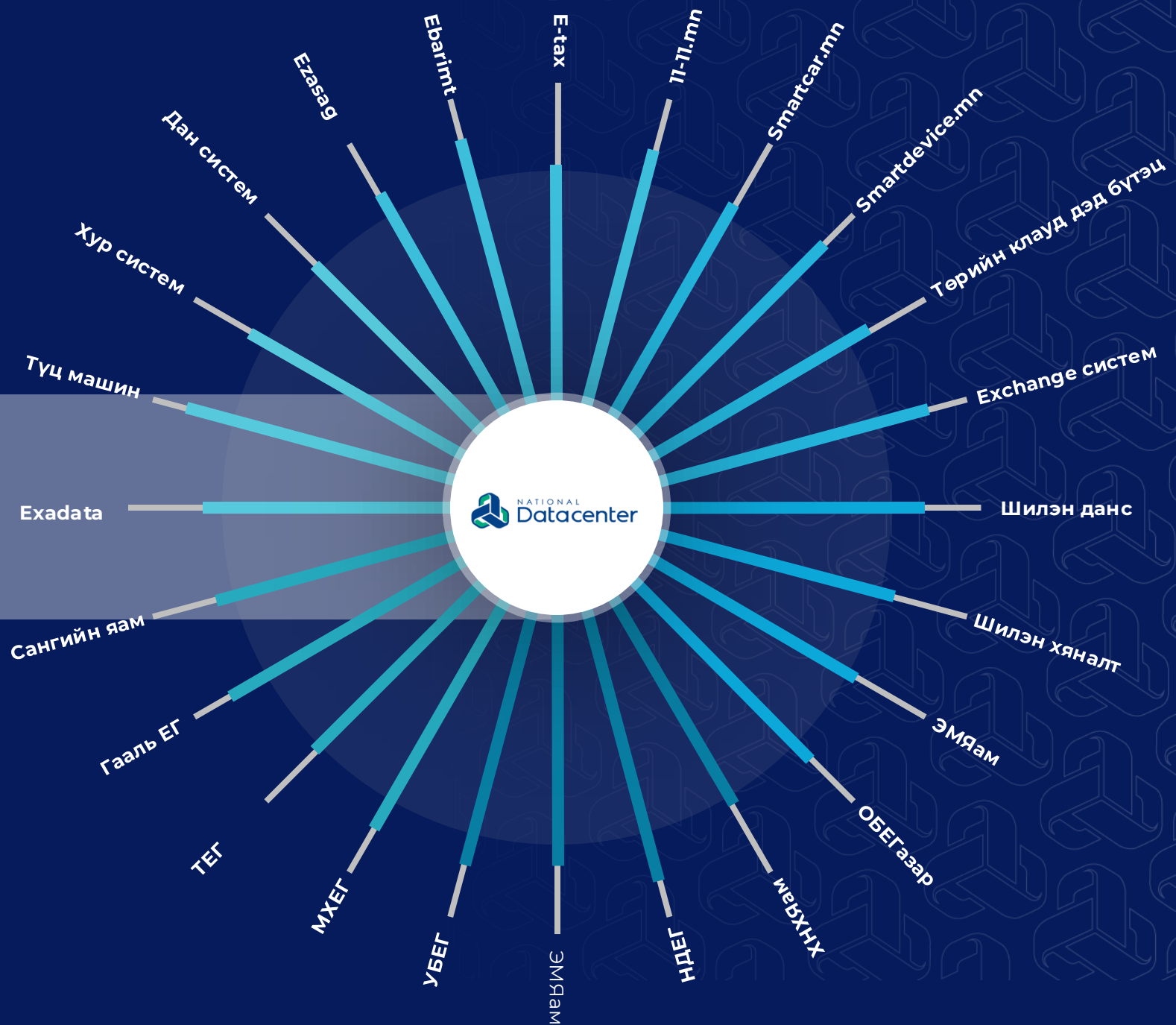
41
Монголын
харилцан
холболтын
төхөөрөмж
МИХХ



4
байгууллаг
7
мэдээллийн
сан

ҮЙЛЧИЛГЭЭНИЙ ХАМААРАЛ

ҮДТ-өөс 2021 онд хийгдсэн судалгаагаар Монгол Улсад үйл ажиллагаа явуулж буй төрийн байгууллагын цахим үйлчилгээ, цахим системийн 90 орчим хувь нь Үндэсний дата төвийн дэд бүтцийн хүчин чадал, үйл ажиллагаатай шууд хамааралтайгаар хөгжиж байна.



Холбогдсон байгууллага
Төр - 138/350 - Хувь

138
Төрийн
байгууллага.

350
Хувийн
Байгууллага

764
Нийт
сервисийн тоо

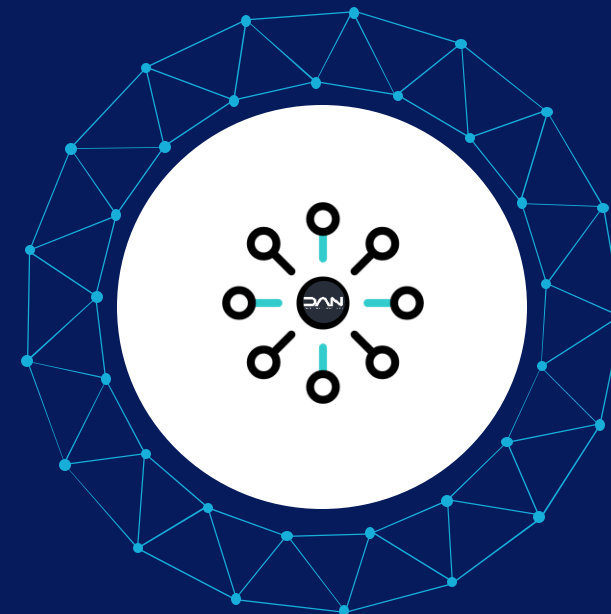
1,893,828,194
Амжилттай дуудсан
сервисийн тоо

ҮНДСЭН СИСТЕМ



ДЭМЖИХ СИСТЕМ

Бүртгэлтэй хэрэглэгчийн тоо: 2,093,464
Систем: Төр - 136/239 - Хувь



ОТР



Тоон гарын үсэг



Банкны эрх

Нийт нэвтрэлт: **57,583,464**



INTERNATIONAL
CERTIFICATE
AUTHORITY

Тоон гарын үсгийн олголт

НИЙТ
777,058

УБЕГ
НДЕГ
СЯ
ЗХУТ



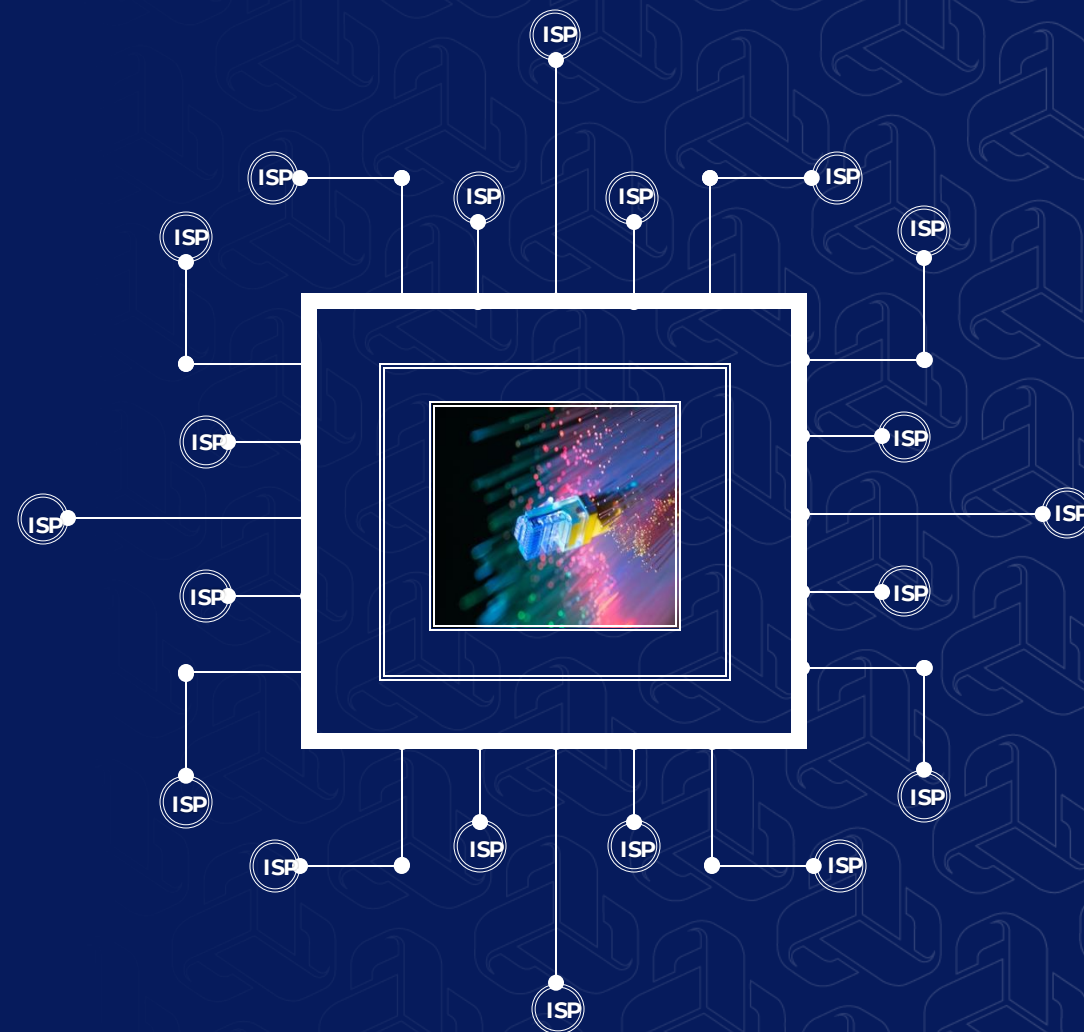
ҮНДЭСНИЙ ДАТА ТӨВ
2017.11.24
12,926



Интернэтийн харилцан холболтоор дамжсан
сүлжээний урсгал
Сарын дундаж өсөлт (GB)



Нийт холбогдсон байгууллага: 41



ТӨРИЙН ҮЙЛЧИЛГЭЭНИЙ ЦАХИМ МАШИН



2021 ОН 1,723,269 удаа

2022 ОН 1,726,166 удаа

2023 ОНЫ БАЙДЛААР 37 ТӨРЛИЙН ЛАВЛАГАА ТОДОРХОЙЛОЛТЫН
ҮЙЛЧИЛГЭЭ ҮЗҮҮЛЖ БАЙНА.

2014-2023 ОНЫ БАЙДЛААР 17,916,079 ЛАВЛАГААГ
2,103,792 ИРГЭН АВСАН БАЙНА.

104 ТҮЦ МАШИН

1,580,797 ИРГЭН 2 БОЛОН ТҮҮНЭЭС ДЭЭШ УДАА ҮЙЛЧЛҮҮЛСЭН

The screenshot displays the MNDC2 web application interface. The top navigation bar includes the user profile of "Алхан аянч БАТБӨ" and the title "Нэгжүүлсэн иргэдийн бүртгэл (2020-11-30)". The main content area is divided into several sections:

- Жагсаалт (List):** A table showing the list of candidates for the 2020-11-30 election. The table has columns for "№", "Хүр", "Регистрийн дугаар", "Нэгжүүлсэн иргэд", "Шалтгаан", "Нэгжүүлсэн", "Гарсан", "Авсан", and "Зөрчил үүсэн". The first candidate listed is "Зоригболор БАТБӨ" with ID "ч68010474".
- Summary Section:** A section titled "Нэгжүүлсэн иргэдийн бүртгэл" showing key metrics: "Нийт нэгжүүлсэн хувиар" (12%), "Нэгжүүлсэн" (8), "Түгэлсэн" (4), and "Нэгжүүлсэн хувиар" (67%).
- Bar Chart:** A bar chart titled "Нэгжүүлсэн иргэдийн тоо /Гаршар/" showing the number of registered voters for three candidates: "2018-12", "2019-1", and "2019-11". The bars are blue and show a significant increase in the number of registered voters over time.
- Donut Chart:** A donut chart titled "Нэгжүүлсэн иргэдийн тоо" showing the distribution of registered voters. The chart is divided into three segments: blue (government palace), green, and black. The blue segment is labeled "government palace" and "4".

The bottom of the screenshot shows a sidebar with the user profile and navigation links, and a footer with the text "МОНЦАГЭР" and "МОНЦАГЭР" (Mongolian Election Commission).

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДАЛ

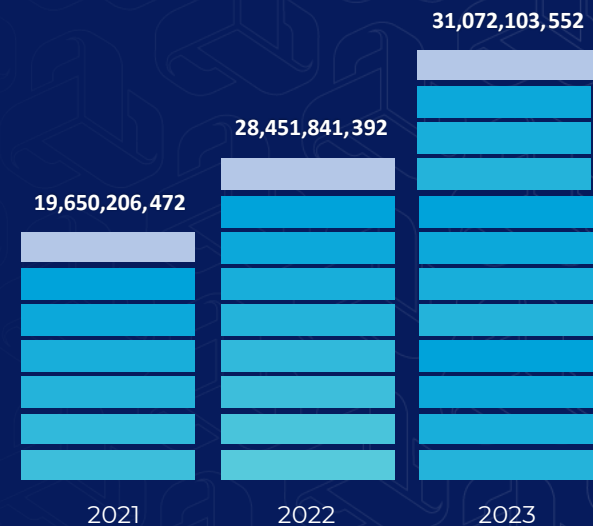
ХАНДАЛТЫН МЭДЭЭЛЭЛ

2022 он 

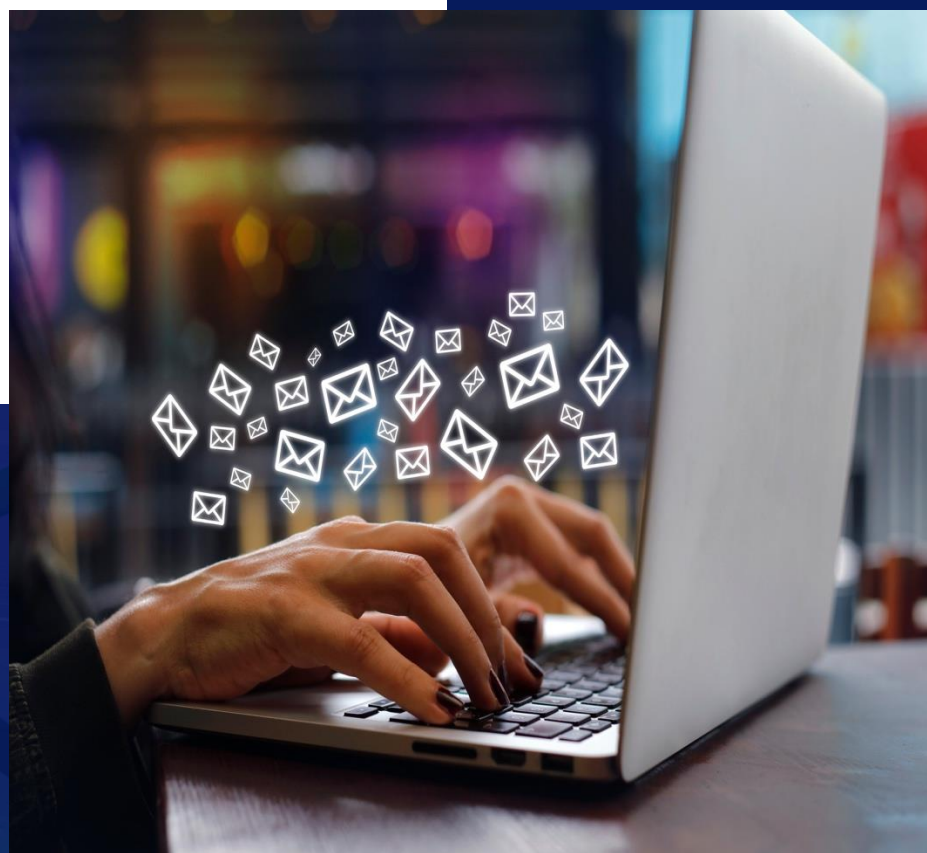


 2009.06.24

	Зөвшөөрөгдсөн	Дүрмийн бус халдлагын чанартай	
2021	14,501,209,585	5,148,996,887	19,650,206,472
2022	19,056,777,746	9,359,063,646	28,451,841,392
2023	21,972,309,893	9,099,793,659	31,072,103,552



ХАНДАЛТЫН МЭДЭЭЛЭЛ



2009.06.24

2023 он



Төрийн байгууллагын цахим шуудангийн системд бүртгэгдсэн цахим шуудан

6,441,426 цахим шуудан хүлээн



5,226,999 цахим шуудан хэвийн



81%

263,181 цахим шуудан хүлээлгэнд



4%

498,516 цахим шууданг спам гэж үзсэн



8%

452,730 цахим шууданг сэжигтэй гэж татгалзсан



7%



User - 1



User - 2

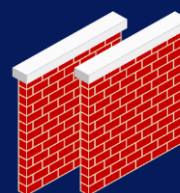


User - 3



Internet

1 ЖИЛД
21,251,793,360



д,
360



NATIONAL
Datacenter

БҮТЭЦ ЗОХИОН БАЙГУУЛАЛТ



ДҮРЭМ ЖУРАМ

- Кибер аюулгүй байдлын тухай хууль
- Мэдээллийн аюулгүй байдлын бодлого
- Мэдээллийн аюулгүй байдлын журам
- Төрийн болон албаны нууцыг хамгаалах журам
- Кибер түргэн тусламжид баримтлах журам
- Мониторингийн журам



ТЕХНИК ТОНОГ ТӨХӨӨРӨМЖ

- Сүлжээний хамгаалалтын фэйрволл
- Халдлага илрүүлэх, эсэргүүцэх систем
- Цахим шуудангийн спам, вирусээс хамгаалах систем
- Цахим хуудасны хамгаалалтын фэйрволл
- Систем веб сүлжээний төхөөрөмжийн аюулгүй байдлыг шалгах програм



7.2.Энэ хуулийн 16.1, 17.1, 19.1-д заасан хуулийн этгээд нь Кибер аюулгүй байдлыг хангах нийтлэг журамд нийцсэн кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журамтай байна.

8.4.Төрийн мэдээллийн нэгдсэн сүлжээнд холбогдсон байгууллага болон онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээдийн кибер аюулгүй байдлын эрсдэлийн үнэлгээг тагнуулын байгууллага, эсхүл түүний зөвшөөрснөөр энэ хуулийн 8.1-д заасан хуулийн этгээд хийнэ.

9.4.Онц чухал мэдээллийн дэд бүтэцтэй төрийн өмчит хуулийн этгээд тагнуулын байгууллагаар, эсхүл түүний зөвшөөрснөөр энэ хуулийн 9.1-д заасан хуулийн этгээдээр мэдээллийн аюулгүй байдлын аудит хийлгэнэ.

16 дугаар зүйл.Төрийн өмчит хуулийн этгээд

16.1.Төрийн өмчит хуулийн этгээд кибер аюулгүй байдлыг хангах талаар дараах үүргийг хүлээнэ:

16.1.1.кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журам батлах;

16.1.2.кибер аюулгүй байдлыг хангах талаар эрх бүхий байгууллагаас өгсөн зөвлөмж, шаардлагыг биелүүлэх;

16.1.3.кибер халдлага, зөрчилд өртсөн, өртсөн байж болзошгүй тохиолдолд кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд даруй мэдэгдэх;

16.1.4.кибер аюулгүй байдлыг хангахад шаардагдах хөрөнгө, үйл ажиллагааны зардлыг төсөвт жил бүр тусгах;

16.1.5.мэдээллийн системийн үйлдлийн бүртгэлийг кибер аюулгүй байдлын нийтлэг журамд заасан хугацаанд хадгалах.



2.1.Байгууллага кибер аюулгүй байдлыг хангах чиглэлээр дараах зохион байгуулалтын арга хэмжээг авч хэрэгжүүлнэ:

2.1.1.кибер аюулгүй байдлыг хангах стратеги төлөвлөгөөг байгууллагын стратеги төлөвлөгөөтэй уялдуулан боловсруулах;

2.1.2.шаардлагатай удирдлага, санхүү, хүний нөөцийн чадавхыг бүрдүүлж кибер аюулгүй байдлын стратеги төлөвлөгөөг хэрэгжүүлэх;

2.1.3.мэдээллийн технологи, кибер аюулгүй байдал хариуцсан ажилтан, албан хаагчийн мэдлэг, ур чадварыг тогтмол дээшлүүлэх арга хэмжээг авах;

2.1.4.мэдээллийн аюулгүй байдлын аудит, кибер аюулгүй байдлын эрсдэлийн үнэлгээг холбогдох стандарт, эсхүл хуульд заасан хугацаанд хийлгэж, тайланг кибер халдлага, зөрчилтэй тэмцэх холбогдох төвд хүргүүлэх;

2.1.5.эрсдэлийн үнэлгээний үр дүнд үндэслэн эрсдэлийг бууруулахад чиглэсэн арга хэмжээг төлөвлөж, хэрэгжүүлэх;

2.1.6.кибер халдлага, зөрчилтэй тэмцэх төвөөс хүргүүлсэн зөвлөмж, шаардлагыг тогтоосон хугацаанд, эсхүл ажлын 10 өдрийн дотор хэрэгжүүлж хариу мэдэгдэх;

2.1.7.кибер аюулгүй байдлыг хангахтай холбоотой энэ журмын 1.2-т заасан журам болон холбогдох баримт бичгийг боловсруулж, байгууллагын холбогдох ажилтан, албан тушаалтанд тухай бүр танилцуулах.

2.2.Байгууллага нь кибер аюулгүй байдлыг хангах чиглэлээр дараах хүний нөөцийн арга хэмжээг авч хэрэгжүүлнэ:

2.2.1. кибер аюулгүй байдлын удирдах болон гүйцэтгэх чиг үүргийг ажлын байрны, эсхүл албан тушаалын тодорхойлолтод тусгаж, орон тооны, эсхүл хавсран гүйцэтгэх ажилтныг томилох;

2.2.2.кибер аюулгүй байдлын мэдлэг олгох дараах сургалтыг зохион байгуулах:

2.2.2.1.жил бүр тогтмол хугацаанд, нийт ажилтнуудыг хамруулах;

2.2.2.2.ажилтныг томилогдсоноос хойш 1 сарын дотор;

2.2.2.3.гэрээгээр хамтран ажиллаж байгаа гуравдагч талын ажилтныг тухай бүр.

2.2.3.кибер орчинд хандаж, мэдээлэлтэй ажиллах ажилтан, албан хаагч, бусад этгээдтэй мэдээллийн нууц хадгалах болон кибер аюулгүй байдлыг хангах талаар үүрэг, хариуцлагыг тусгасан гэрээ байгуулах, эсхүл нууцын баталгаа үйлдэх;

2.2.4.албан хаагч бүрд кибер халдлага, зөрчилтэй тэмцэх, кибер аюулгүй байдлыг хангах үйл ажиллагааны дотоод журмын зөрчлийн үед авах арга хэмжээний талаар мэдлэг олгох.

4.3.Байгууллагын удирдлага мэдээллийн систем, мэдээллийн сүлжээнд давуу эрхтэй (admin, root) хандах этгээдийг тухай бүр тогтоож, хандах эрхийн ашиглалтад хяналт тавина.

4.4.Байгууллагын мэдээллийн систем, мэдээллийн сүлжээний тоног төхөөрөмж байрлаж байгаа зориулалтын өрөөнд зөвшөөрөлгүй нэвтрэхийг хориглох бөгөөд өрөө нь дараах шаардлагыг хангасан байна:

4.4.1.өрөөний хаалга цоожтой байх;

4.4.2.дохиоллын системтэй байх;

4.4.3.цонхны хамгаалалттай байх;

4.4.4.орох хаалганы дэргэд дүрст хяналтын системтэй байх;

4.4.5.температур, чийгшил зэрэг орчны нөхцөлийг хянах, бүрдүүлэх хэрэгсэлтэй байх;

4.4.6.хаалганы түлхүүр, эрхийг зөвхөн эрх бүхий ажилтан хадгалах.

4.6.Байгууллагын ажилтан, албан хаагч бүр хэрэглэгчийн эцсийн төхөөрөмж (компьютер зэрэг)-тэй ажиллахад аюулгүй байдлыг хангах талаар дараах арга хэмжээг авч хэрэгжүүлнэ:

4.6.1.байгууллага зөвшөөрснөөс бусад төрлийн программ хангамжийг ашиглахгүй байх;

4.6.2.төхөөрөмжид нэвтрэхэд нууц үг ашигладаг байх;

4.6.3.хувийн хэрэгцээнд ашиглахгүй байх;

4.6.4.нууцын зэрэглэлтэй мэдээлэл агуулсан төхөөрөмжийг зөвшөөрсөн бүсээс зөвшөөрөлгүйгээр гадагш гаргахгүй байх;

4.6.5.байгууллагаас өөрт олгосон төхөөрөмж, нэвтрэх нэр, нууц үгийг ашиглах ба бусдад дамжуулж, ашиглуулахгүй байх;

4.6.6.засвар үйлчилгээг зөвхөн байгууллагын мэдээллийн технологи хариуцсан нэгж, ажилтнаар хийлгэх, оношлуулах.

4.16.Байгууллага мэдээллийн систем, мэдээллийн сүлжээнд дараах үйлдлийн бүртгэлийг хөтөлнө:

- 4.16.1.нэвтрэх оролдлого болон нэвтэрсэн тухай;
- 4.16.2.давуу эрхийн хандалт;
- 4.16.3.нууц үгийн өөрчлөлт;
- 4.16.4.үйлдлийн бүртгэлийг өөрчлөх, устгах;
- 4.16.5.хандах эрх олгох, өөрчлөх, хүчингүй болгох.

4.17.Үйлдлийн бүртгэлд дараах мэдээллийг тодорхойлно:

- 4.17.1.хэрэглэгчийн нэр, системд нэвтрэх нэр буюу ID;
- 4.17.2.огноо;
- 4.17.3.хандсан хаяг, төхөөрөмжийн мэдээлэл;
- 4.17.4.хандалтын үргэлжлэх хугацаа;
- 4.17.5.гүйцэтгэсэн үйлдэл;
- 4.17.6.гүйцэтгэсэн үйлдлийн үр дүн.

КИБЕР АЮУЛГҮЙ БАЙДЛЫГ ХАНГАХ НИЙТЛЭГ ЖУРАМ

4.18.Байгууллага нь мэдээллийн системийн үйлдлийн бүртгэлд эрх олгогдсон этгээд зөвшөөрлөөр хандах нөхцөлийг бүрдүүлнэ.

4.19.Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээний үйлдлийн бүртгэлийг доор дурдсан хугацаанд хадгална:

4.19.1.кибер аюулгүй байдлын тухай хуулийн 17.1-д заасан байгууллага 6 сар буюу түүнээс дээш хугацаагаар;

4.19.2.кибер аюулгүй байдлын тухай хуулийн 17.3-т заасан байгууллага 3 сар буюу түүнээс дээш хугацаагаар;

4.19.3.кибер аюулгүй байдлын тухай хуулийн 19.1-д заасан байгууллага 1 жил буюу түүнээс дээш хугацаагаар;

4.19.4.бусад байгууллага 3 сараас багагүй хугацаагаар.

4.20.Байгууллага нь мэдээллийн систем, мэдээллийн сүлжээнд ашиглагдаж байгаа үйлдлийн систем, программ хангамжийг шинэчлэхэд дараах арга хэмжээг авч хэрэгжүүлнэ:

4.20.1.шинэчлэл гарах бүрд суулгах;

4.20.2.зөвшөөрөгдсөн албан ёсны эх үүсвэрээс шинэчлэх;

4.20.3.шинэчлэлийг суулгахаас өмнө эмзэг байдал үүсгэх эсэхийг шалгаж, баталгаажуулах.

8.1.Байгууллагын удирдах албан тушаалтан кибер аюулгүй байдлыг хангах чиглэлээр дараах үүрэгтэй:

- 8.1.1.байгууллагын кибер аюулгүй байдлыг хангах үйл ажиллагааг нэгдсэн удирдлагаар хангах, уялдуулан зохион байгуулах, байгууллагыг төлөөлөх;
- 8.1.2.кибер аюулгүй байдлыг хангах бодлого, дүрэм, журам батлах;
- 8.1.3.кибер аюулгүй байдлыг хангах төлөвлөгөө гаргах, хэрэгжүүлэхэд шаардагдах нөөцийг байгууллагын жил бүрийн төсөв, төлөвлөгөөнд тусгах.

8.2.Байгууллагын кибер аюулгүй байдал хариуцсан ажилтан дараах үүрэгтэй:

- 8.2.1.байгууллагын кибер аюулгүй байдлыг хангах өдөр тутмын үйл ажиллагааг хариуцан гүйцэтгэх;
- 8.2.2.холбогдох дүрэм, журмыг боловсруулах, шинэчлэх санал боловсруулах;
- 8.2.3.кибер аюулгүй байдлыг хангахад шаардлагатай үйл ажиллагаа, нөөцийг төлөвлөх;
- 8.2.4.кибер аюулгүй байдлыг хангах мэргэшүүлэх сургалтад хамрагдах.

8.3.Байгууллагын нийт ажилтан кибер аюулгүй байдлыг хангах чиглэлээр дараах үүрэгтэй:

- 8.3.1.энэ журам болон мэдээллийн аюулгүй байдлыг хангахтай холбоотой бусад дүрэм, журмыг дагаж мөрдөх;
- 8.3.2.илэрсэн халдлага, зөрчил, сэжигтэй тохиолдол бүрийг аюулгүй байдал хариуцсан ажилтанд мэдэгдэх;
- 8.3.3.байгууллагын мэдээлэл, мэдээллийн систем, мэдээллийн сүлжээг зөвхөн албан хэрэгцээнд, заасан журам, зааврын дагуу хэрэглэх;
- 8.3.4.байгууллагаас зохион байгуулж буй кибер аюулгүй байдлын мэдлэг олгох сургалтад хамрагдах.

КИБЕР АЮУЛГҮЙ БАЙДАЛ

"Интермед эмнэлгийн есөн серверийг барьцаалсан халдлагын баг нь Европын улсуудын эмнэлгүүдийн файлыг барьцаалж байсан"

Н.ЭРХБАЯР, IKON.MN

2024 ОНЫ 11 САРЫН 13

Like 116

Share

Post

IKON.MN



Гэрэл зургийг МРА агентлагийн онцгой зөвшөөрөлтэйгөөр ашиглав

Кибер зөрчил, халдлагатай тэмцэхээр манай улсад албан ёсны гурван төв ажилладаг. Тагнуулын Ерөнхий Газрын дэргэд Монгол Улсын Үндэсний кибер аюулгүй байдлын үндэсний төв, Батлан Хамгаалах Яамны дэргэд батлан хамгаалахын чиглэлээр ажилладаг. Харин нийтийн төв нь иргэд, хувийн хэвшлийг энэ төрлийн халдлагад өртөхөөс урьдчилан сэргийлэх үүднээс ажиллаж байгаа" гэв.

"Халдлагын баг Интермед эмнэлгээс 50 мянган ам.доллар нэхсэн асуудлыг Тагнуулын Ерөнхий Газар шалгаж байгаа"

Үргэлжлүүлэн Интермед эмнэлэгтэй холбоотой асуудлын талаар тэрбээр "Өнөөдөр Интермед эмнэлгийн асуудлыг ярьж байна. Кибер халдлагад өртсөн байгууллагыг буруутгахаас илүү дахиж ийм халдлага гаргахгүй байх тогтолцоог яаралтай бүрдүүлэх нь хамгийн зөв арга.

Хэрэв кибер халдлагад өртсөн ямар нэгэн хүн, байгууллагыг буруутгавал дараагийн байгууллага халдлагад өртсөнөө нуудаг. Тиймээс тэмцэж буй хүмүүс хаанаас орж ирж нэвтрээд байгааг олж илрүүлэх явц нь удааширдаг.

Интермед эмнэлгийн барьцаалагдсан есөн серверийг дөрвөн мэргэжилтэн бүрэн нээх, нөхөн сэргээхээр ажиллаж байна. Тус есөн серверийг файлыг барьцаалсан халдлагын баг нь Европын улсуудын олон эмнэлгийн файлыг барьцаалж байсан.

- **Кибер аюулгүй байдал** нь систем, сүлжээ, программыг дижитал халдлагаас хамгаалах практик юм. Эдгээр кибер халдлага нь ихэвчлэн нууц мэдээлэлд хандах, өөрчлөх, устгах зорилготой; ransomware ашиглан хэрэглэгчдээс мөнгө авах; эсвэл бизнесийн хэвийн үйл явцыг тасалдуулах.



Кибер аюулгүй байдал яагаад чухал вэ?

Кибер халдлага тасралтгүй өссөөр байгаа ба үүнээс үүдсэн сөрөг үр дагавар, хор хохирол ч мөн аюулын харанга дэлдэж байна.

Кибер халдлага, аюул заналууд нь өгөгдөл, мэдээлэл хулгайлах, байгууллагын болон хувь хүний нэр хүндэд хор хохирлыг учруулаад зогсохгүй бүр цаашлаад санхүүгийн алдагдалд хүргэсээр байна. Тиймээс кибер аюулгүй байдлыг хангахын тулд өргөн хүрээний технологи, арга зүйгээс гадна кибер-ухаалаг иргэдийн оролцоо нэн чухал юм.

Түгээмэл тохиолддог кибер аюул заналууд

КИБЕР АЮУЛГҮЙ БАЙДАЛ ХҮН БҮХЭНД ХАМААТАЙ

Харилцан адилгүй зорилго, харилцан адилгүй арга техник бүхий олон төрлийн кибер аюул заналууд өдрөөс өдөрт нэмэгдсээр байгаа ч дараах төрлийн кибер халдлага, аюул заналууд түгээмэл тохиолддог байна. Үүнд:



Хортой код (Malware) : Энэ нь таны компьютер, ухаалаг утас болон бусад төхөөрөмжид халдварладаг дижитал вирус юм, яг л хүний биед халдварладаг вирустэй адил. Хортой программ нь цахим шуудангийн хавсралт, халдвар авсан веб сайтууд зэрэг олон арга замаар дамжин тархдаг. Хортой программ нь таны төхөөрөмжид халдварласан тохиолдолд таны хувийн мэдээллийг хулгайлах, файлуудыг тань эвдэх, бүр цаашлаад хакеруудад таны төхөөрөмжийг хянах боломжийг олгодог.

Фишинг (Phishing) : Энэ нь кибер гэмт хэрэгтнүүд таны нууц үг, зээлийн картын дугаар, хувийн мэдээлэл зэрэг таны эмзэг, нууц мэдээллийг олж авахын тулд итгэмжлэгдсэн байгууллага эсвэл таны найз мэт дүр эсгэдэг нэгэн төрлийн дижитал залилан юм. Энэхүү халдлагыг ихэвчлэн хуурамч и-мэйл, мессеж, эсвэл жинхэнэ мэт харагдах веб сайтуудаар дамжуулан үйлддэг.

Рансомвэр (Ransomware) : Энэ нь таны файл, өгөгдлийг барьцаалах дижитал барьцаалагчтай адил юм. Өөрөөр хэлбэл таны чухал баримт бичиг, зураг, тэр ч байтугай таны компьютерыг бүхэлд нь шифрлэж, хандах боломжгүй болгодог нэгэн төрлийн хортой программ юм. Халдлагыг хийж буй кибер гэмт хэрэгтнүүд таны файл, өгөгдөл мэдээллийн шифрийг тайлах түлхүүрийг өгөхийн тулд ихэвчлэн криптовалют зэрэг барьцааг шаарддаг. Харамсалтай нь та тэрхүү барьцааг нь төлсөн ч өгөгдөл мэдээллээ урьдын адил хандаж, ашиглах боломжтой болно гэдэг нь баталгаагүй байдаг.

Нууц үгийн халдлага (Password Attacks) : Халдлага үйлдэгчид таны онлайн систем, программ руу нэвтрэхийн тулд таны нэвтрэх нууц үгийг таах эсвэл хулгайлахыг оролддог ба дижитал орчин дахь хулгай гэж ойлгож болно. Халдлага үйлдэгчид нь таны нууц үгийг олж авахын тулд түгээмэл нууц үгсийг турших, алдагдсан нууц үгсийг ашиглах, нууц үгийг үүсгэх төрөл бүрийн хослолуудыг автоматаар программ хангамж ашиглах зэрэг янз бүрийн арга техникийг ашиглаж болно.

PASSWORD:

 1292014

 wH01292014etV

wikiHow

2024 ОНЫ 11 САРЫН 4

X Post

IKON MN



"Телеграмаар үйлдэгдсэн 619 гэмт хэргээс нийт ₮10.3 тэрбумын бодит хохирол иргэдэд учирчээ"



Энэ төрлийн гэмт хэргээс сэргийлэх зорилгоор дараах сэрэмжлүүлэг мэдээг тэрбээр нэмж танилцуулав.

Telegram платформд дараах төрлийн гэмт хэргүүд бүртгэгдэн шалгагддаг.

- **Романс залилан:** Хайр дурлалын залилан. Хохирогчтой удаан хугацаанд харилцаа үүсгэж итгэлийг нь олж авах замаар хөрөнгийг нь залилдаг.
- **Даалгавар өгөх залилан:** Даалгавар биелүүлж мөнгө авахыг санал болгох, шагналт судалгаа бөглүүлэх нэрийдлээр хувийн мэдээллийг олж авдаг.
- **Хуурамч зар байршуулах залилан:** Өндөр цалинтай ажилд авна гэх хуурамч зар сурталчилгаа явуулж, иргэдийн эд хөрөнгийг залилдаг.
- **Секс сүрдүүлэг** буюу хохирогчийг өөрөөр нь хувийн батлан даалт буюу хувийн эмзэг мэдээллийг нь олж авч дарамталж залилдаг.
- **COPYCAP** буюу ижил нэртэй групп хаягууд үүсгээд мөнгө татаж залилдаг. Өөрөөр хэлбэл ижил нэртэй групп хаягуудыг хуулбарлаж, доторх мэдээлэл, үйлчлүүлэгч нараас мөнгө татах аргаар залилдаг.
- **Pump and dump** буюу хөрөнгө оруулагч (хувьцаа, криптовалют, койн)-ны ханшийг цаашид өсөх талаар хуурамч мэдээлэл өгч өөрийн дансанд мөнгө татаж авдаг.

Дээрх аргаар залилан мэхэлсэн гэмт хэрэг бүгд цагдаагийн байгууллагад бүртгэгдээд байна.

Кибер аюулгүй байдлын энгийн зөвлөмж

Онлайн орчинд өөрийн кибер аюулгүй байдлыг хангах нь таны хуулиар хүлээсэн үүрэг гэдгийг та мартаагүй биз! Тиймээс юуны түрүүнд онлайн орчин дахь аюул заналыг танихад туслах товч зөвлөгөөг хүргэе:

- Сэжигтэй холбоос, цахим шуудангийн хавсралт дээр дарахгүй байж, тэдгээрт үргэлж болгоомжтой хандаарай.
- Үнэн гэж итгэхэд бэрх, дэндүү сайхан санагдах саналуудад эргэлзээтэй хандаарай.
- Кибер гэмт хэрэгтнүүд үг үсгийн алдаа гаргах нь элбэг байдаг тул мессеж, чат, имэйл хүлээн авсны дараа хариу үйлдэл хийхээсээ өмнө тэдгээрт агуулагдаж буй мэдээлэлд үг үсгийн алдаа байгаа эсэхийг шалгаарай.
- Хэн нэгэн танаас онлайнаар хувийн мэдээлэл эсвэл мөнгө асуувал үргэлж үл итгэгчийн байр сууринаас хандаж, хариу өгөхөөсөө өмнө хэн болохыг нь шалгаж, баталгаажуулаарай.
- Хууль ёсны байгууллага нь таныг хүсээгүй байхад таны нууц мэдээллийг имэйлээр эсвэл мессежээр явуулахыг шаардаггүй, авдаггүй болохыг санаарай.

Мөн түүнчлэн кибер аюулгүй байдлаа хангахын тулд нэн тэргүүнд хэрэгжүүлж хэвшвэл зохих энгийн зөвлөгөөг хүргэе:

- Вирусийн эсрэг программ хангамж ашиглаж, түүнийгээ хамгийн сүүлчийн шинэчлэлээр нь тогтмол шинэчилж байгаарай.
- Программ хангамжийг баталгаат хаягаас нь татаж байгаарай.
- Чухал өгөгдөл, мэдээллээ байнга нөөцөлж байгаарай.
- Нэвтрэх эрх бүрдээ ялгаатай давтагдашгүй, хүчирхэг нууц үг ашиглаж заншихаас гадна хоёр алхамт баталгаажуулалтыг (2FA) идэвхжүүлээрэй. Нэвтрэх мэдээлэл, нууц үгээ бусадтай хуваалцахаас зайлсхийж, нууц үгээ тодорхой давтамжтайгаар шинэчилж хэвшээрэй.
- Шинээр гарч ирж буй аюул заналаас нэг алхмын өмнө байж, өөрийгөө болон өрөөлийг хамгаалахын тулд кибер аюулгүй байдлын талаар мэдээлэлтэй байхыг үргэлж зориорой.
- Эцэст нь хэлэхэд, хэрвээ та халдлагад өртсөн гэдгээ мэдвэл эсвэл ямар нэгэн хэвийн бус, сэжигтэй төлөв байдал ажилдагдвал кибер халдлага, зөрчилтэй тэмцэх нийтийн төвд мэдээлээрэй.



Анхаарал хандуулсанд баярлалаа



Б. ГАНБОЛД

World standard consulting ХХК-ийн
Ерөнхий захирал, Мэдээллийн
аюулгүй байдлын Ахлах зөвлөх,
тэргүүлэх аудитор



**WORLD
STANDARD
CONSULTING**

- **ISO 27005:2022 Мэдээллийн аюулгүй
байдлын менежментийн тогтолцоо,
эрсдэлийн менежмент**



EXPERT

SUPPORT

KNOWLEDGE

CONSULTING

SERVICE

ОЛОН УЛСЫН (ISO) СТАНДАРТЫН
ЗӨВЛӨХ ҮЙЛЧИЛГЭЭ, СУРГАЛТ
ВОРЛД СТАНДАРТ КОНСАЛТИНГ ХХК

ЕРӨНХИЙ ЗАХИРАЛ, МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН АХЛАХ ЗӨВЛӨХ,
ТЭРГҮҮЛЭХ АУДИТОР Б. ГАНБОЛД

Бор ГАНБОЛД

ISO 9001, ISO 45001, ISO 14001, ISO 27001
Тэргүүлэх аудитор



Албан тушаал: Ерөнхий захирал



Мэргэжил: Мэдээллийн системийн инженер



Боловсрол: МУБИС-ФТС, ШУТИС-БАТС



Ажилласан жил: 23 жил



Ур чадвар: Олон улсад бүртгэлтэй Тэргүүлэх аудитор, сургагч багш, Менежментийн ахлах зөвлөх



Стандартын зөвлөх үйлчилгээний чиглэлээр

Төрийн болон бизнесийн салбаруудад ISO 9001, ISO 45001, ISO 14001, ISO 27001 стандартууд зөвлөх үйлчилгээ, аудит хийх ур чадвартай

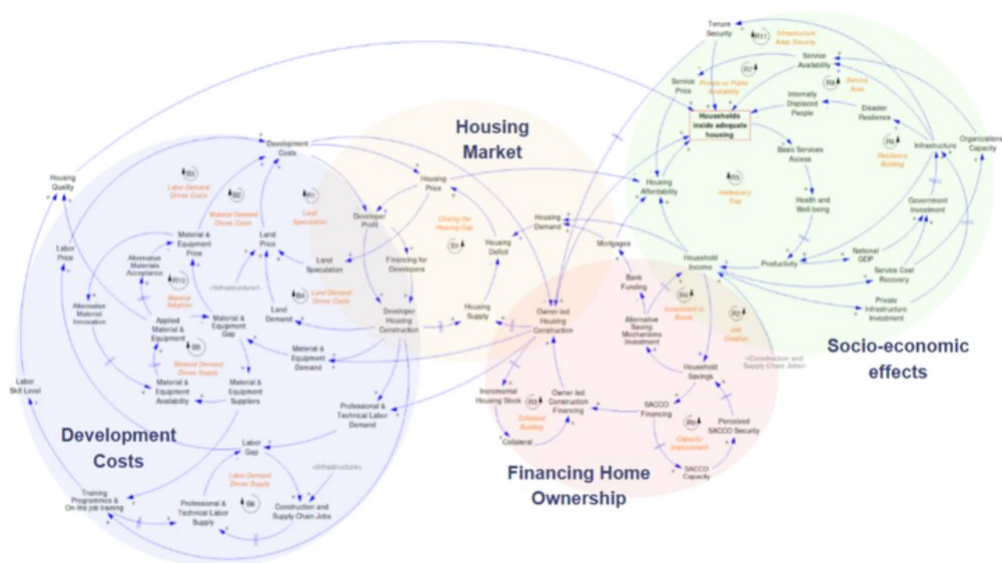
Менежментийн тогтолцооны стандартууд

- Менежментийн тогтолцоо гэж юу вэ?
 - Тухайн зорилгод хүрэх бодлого, зорилт, үйл явцыг бий болгохын тулд байгууллагын харилцан хамааралтай эсвэл харилцан үйлчлэл бүхий элементүүдийн багц (*байгууллагын бүтэц, үүрэг, хариуцлага, төлөвлөлт, үйл ажиллагаа, гүйцэтгэлийн үнэлгээ, сайжруулалт*)
- ISO-оос гаргасан менежментийн стандартууд нь:
 1. Нөөцийг илүү үр ашигтай зарцуулах
 2. Санхүүгийн гүйцэтгэлийг дээшлүүлэх
 3. Эрсдлийн менежментийг сайжруулах
 4. Байгаль орчин ба хүмүүсийг эрүүл, аюулгүй байлгах
 5. Байгууллагын ажилтнуудын менежментийн мэдлэгийг дээшлүүлэх
 6. Үйлчлүүлэгч ба бусад сонирхогч талуудад үнэ цэнэ нэмэх зэрэг юм.

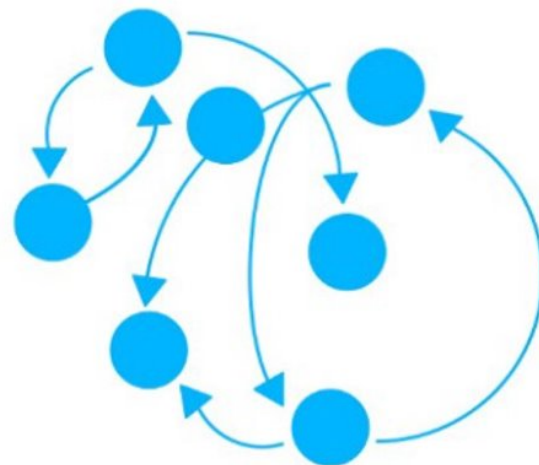


Тогтолцоо буюу систем

- Тогтолцоог өөр хоорондоо уялдаа холбоотой асар олон хэсэгтэй, нийлмэл бүтэцтэй, бүгдээрээ нэгдэж амжилттай ажилладаг том араа гэж ойлгож болох юм.



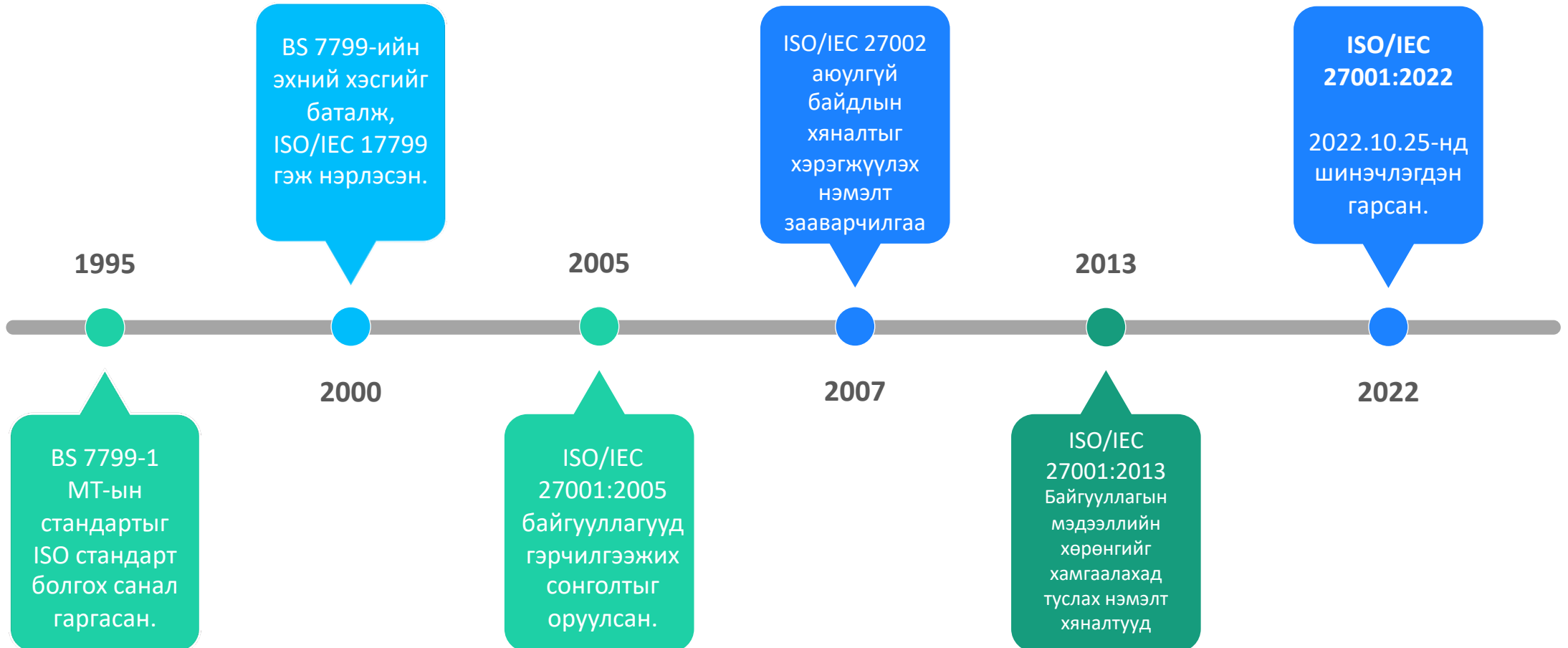
Systems thinking



ISO 27001

- ISO/IEC 27001 нь мэдээллийн аюулгүй байдлын менежментийн тогтолцоо (МАБМТ) дотор мэдээллийн аюулгүй байдлын хяналтыг хэрэгжүүлэх, удирдах шилдэг туршлагыг тодорхойлсон олон улсын стандарт юм.
 - ✓ **ISO** - International Organization for Standardization/ Олон Улсын Стандартчиллын Байгууллага
 - ✓ **IEC** - International Electrotechnical Commission/ Олон Улсын Цахилгаан Техникийн Комисс
- ISO 27000 аюулгүй байдлын бүл стандартын нэгж юм.
- Тус стандартын зорилго нь байгууллагууд өөрсдийн **өгөгдөл, баримт бичиг** болон бусад **мэдээллийн хөрөнгийг** аюулгүй байлгахын тулд МАБМТ-оо хэрхэн бий болгох, хянах, хадгалах, сайжруулахад чиглүүлдэг.

ISO 27001 ТҮҮХ



The ISO/IEC 27000 Family of the Standard

Нэр
томъёо

ISO/IEC 27000
Тодорхойлолтууд ба нэр
томъёо

Шаардлага

ISO/IEC 27006
МАБМТ-нд аудит,
баталгаажуулалт хийх
байгууллагын шаардлага

ISO/IEC 27001
МАБМТ шаардлага

ISO/IEC 27701
Нууцлалын мэдээллийн
менежментийн
тогтолцоо

Ерөнхий

ISO/IEC 27002
МАБ
хяналтын
удирдамж

ISO/IEC 27003
МАБМТ-ны
заавар

ISO/IEC 27704
Мониторинг,
хэмжилт,
шинжилгээ, үнэлгээ

ISO/IEC 27005
МАБ-ын
эрсдэлийн
менежмент

ISO/IEC
27032
Кибер
аюулгүй
байдал

Үйлдвэрлэлийн
заавар

ISO/IEC 27017 үүлэн
үйлчилгээний МАБ
хяналт

ISO/IEC 27018 үүлэн
орчинд нууцлалыг
хамгаалах удирдамж

Бүлийн бусад
стандартууд

ISO 27001 хэрхэн ажилладаг вэ?

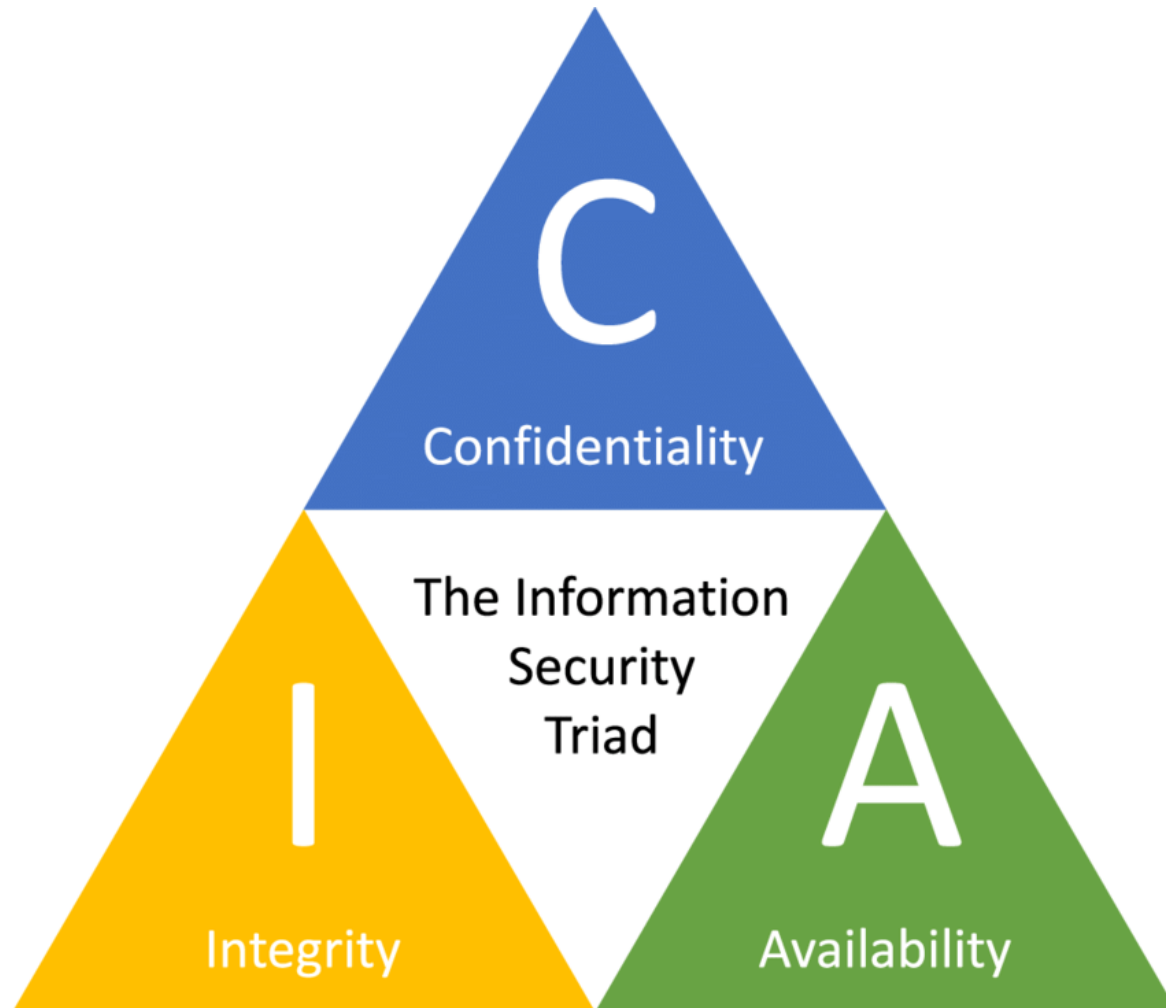
ISO 27001 стандартын гол зорилго нь компанийн мэдээллийн нууцлал, бүрэн бүтэн байдал, хүртээмжийг хамгаалах явдал юм.

“Эрсдэл хаана байгааг олж мэдээд, аюулгүй байдлын хяналт (эсвэл хамгаалалтын арга) хэрэгжүүлэх замаар тэдгээрийг системтэйгээр арилгах эсвэл бууруулахыг зорьдог.”

Тиймээс ISO 27001 стандартын үндсэн философи нь эрсдэлийг удирдах үйл явцад суурилдаг.



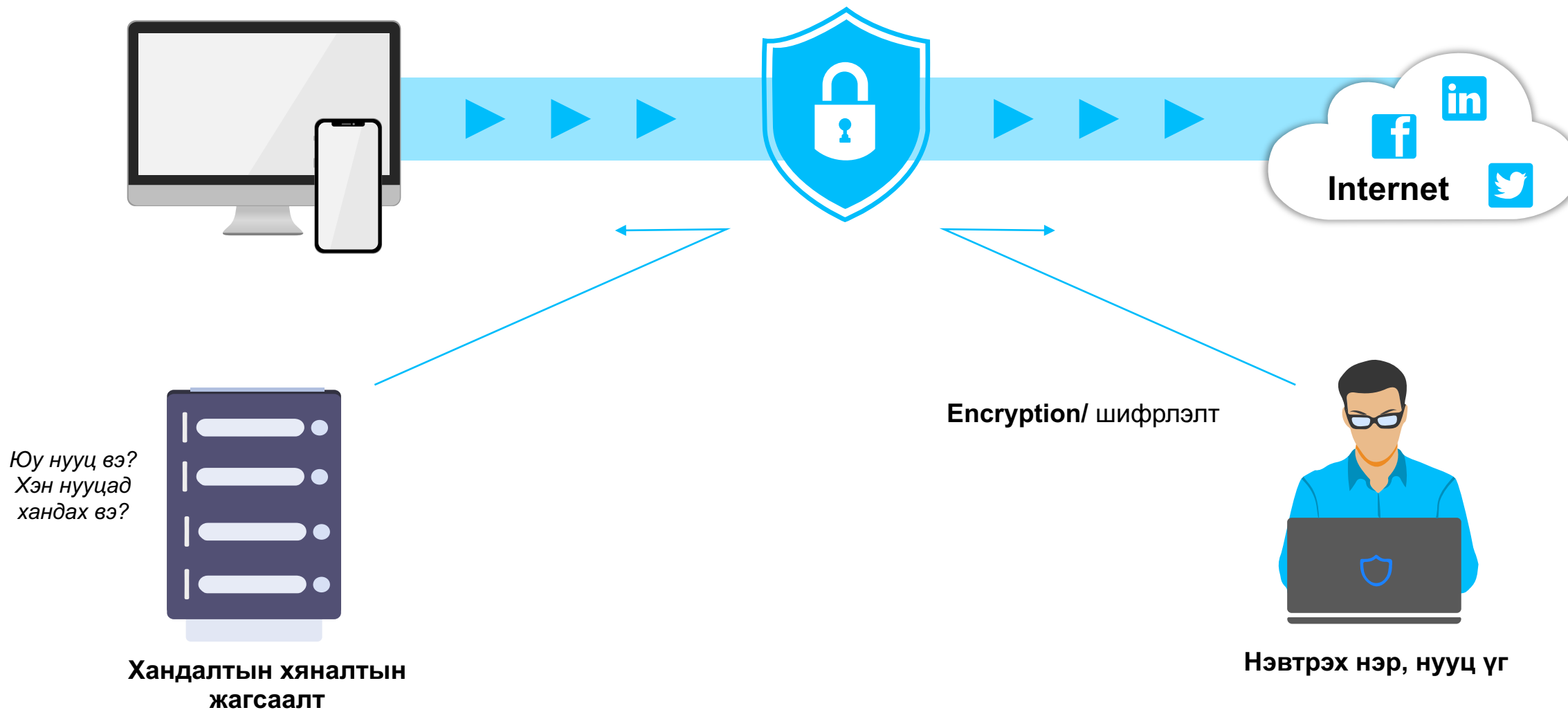
ISO 27001 зарчим / CIA гурвал



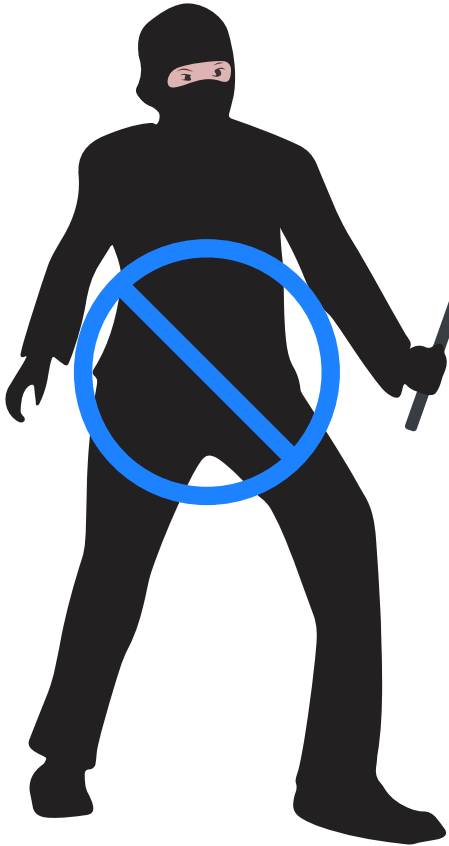
1. **Confidentiality/ Нууцлалтай:** бүх төрлийн мэдээллийг зөвхөн зөвшөөрөгдсөн хэрэглэгч ашиглах боломжтой байх;
2. **Integrity/ Бүрэн бүтэн байдал:** мэдээлэл үнэн зөв, бүрэн байх;
3. **Availability/ Хүртээмжтэй байдал:** эрх бүхий хэрэглэгчид шаардлагатай үед мэдээлэл авах боломжтой байх.

Эдгээрийг байгууллагын аюулгүй байдлын бодлогыг бий болгоход чиглүүлэгч болгон ашиглаж болно.

Confidentiality/ Нууцлалтай

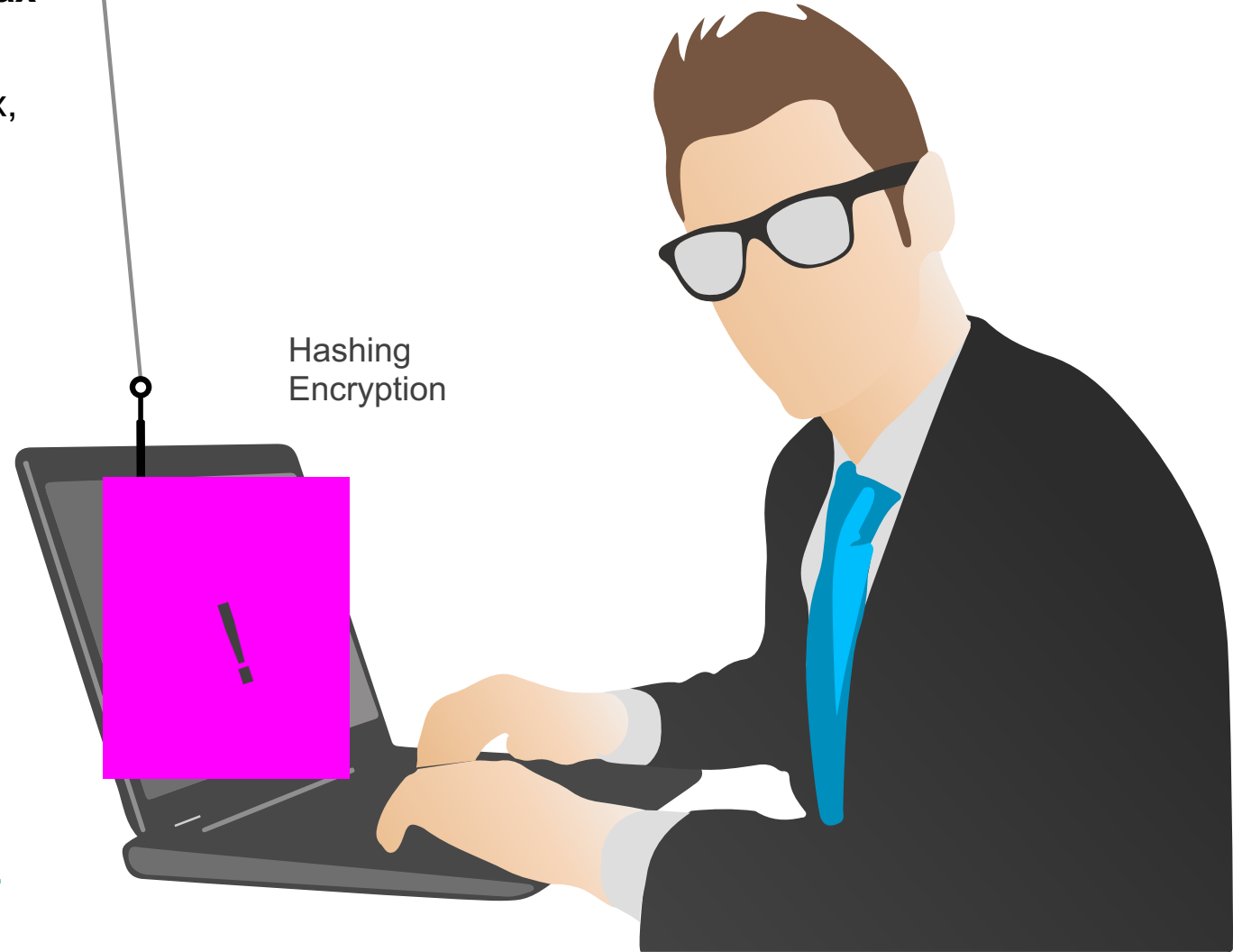


Integrity/ Бүрэн бүтэн байдал



Бүрэн байдал алдагдах тохиолдол:

- ☐ Өгөгдөл байршуулах, дамжуулах үед
- ☐ Мэдээллийн сан эсвэл хавтсанд баримт бичгийг хадгалах үед



Мэдээллийн бүрэн бүтэн байдлын зарчим нь өгөгдөлд зөвшөөрөлгүй эх сурвалжаас хандахаас хамгаалахаас гадна амьдралынхаа туршид түүний үнэн зөв байдлыг хангах арга хэмжээ авахыг байгууллагуудад үүрэг болгодог.

Availability/ Хүртээмжтэй байдал

Кибер аюул заналхийллийн
эсрэг тэсвэртэй байх

Шаардлагатай үед
НЭЭЛТТЭЙ

Тасалдал гарсан ч тасралтгүй
үйлчилгээ үзүүлэх системийн
ашиглалтыг мөн илэрхийлж
болно.

Цахилгааны тасалдал, техник
хангамжийн доголдол болон
системийн бэлэн байдалд
нөлөөлж болзошгүй бусад үйл
явдлуудаас хамгаалах
хамгаалалттай байх ёстой



Эрх бүхий хэрэглэгчид
шаардлагатай үед мэдээлэл
болон холбогдох хөрөнгөд
хандах боломжтой байх

ISO 27001 ашиг тус

Баталгаажуулалт

Мэдээллийн аюулгүй байдлын удирдлагын **дэлхийн хэмжээнд хүлээн зөвшөөрөгдсөн** ганц стандартын хувьд ISO 27001 гэрчилгээ нь байгууллагын мэдээллийн хөрөнгөө үр дүнтэй удирдаж байгааг нотлох **өрсөлдөөний давуу тал** болдог.



01 Нэр хүнд өсөх

Үйлчлүүлэгчдийг татах, хадгалахад тусална.

02 Хуулийн шаардлагыг хангах

Бүгдийг нь дагаж мөрдөх төгс арга зүйг өгнө.

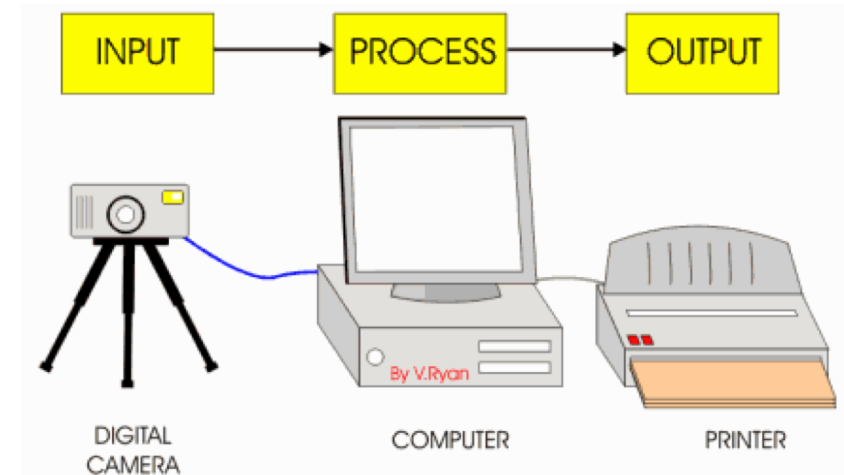
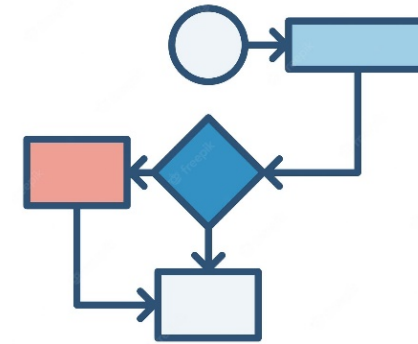
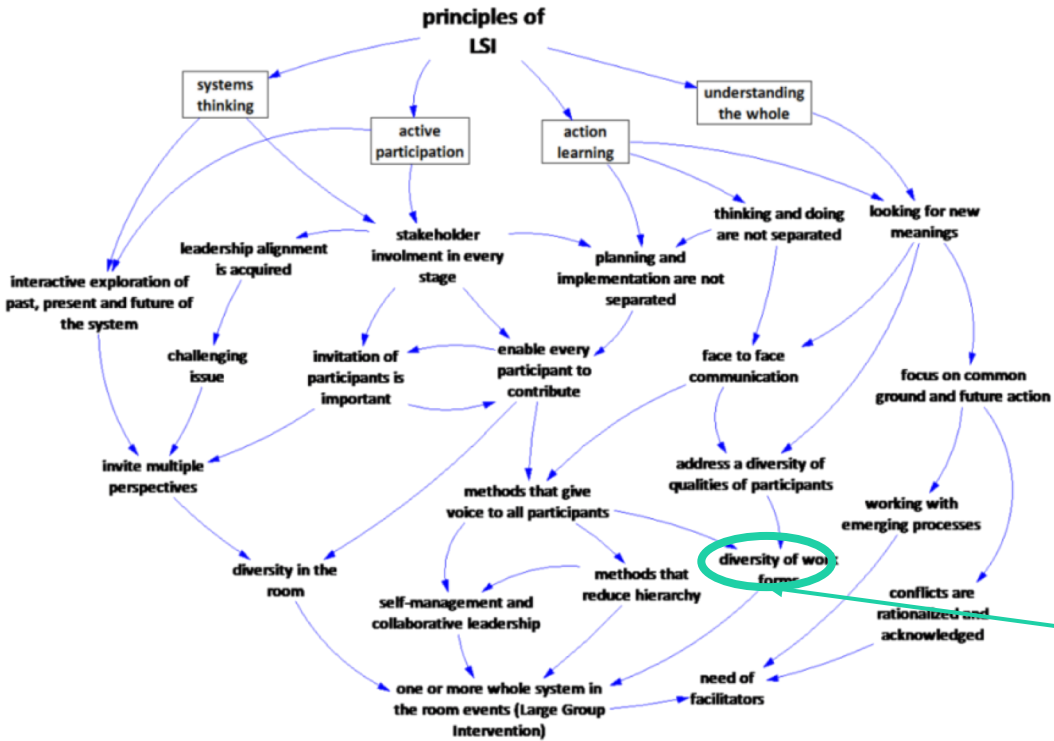
03 Мэдээллийн хөрөнгийг аюулгүй байлгах

Эрсдэлийг удирдах, шинэ боломжуудыг авч ашиглан, үр ашигтай ажиллана.

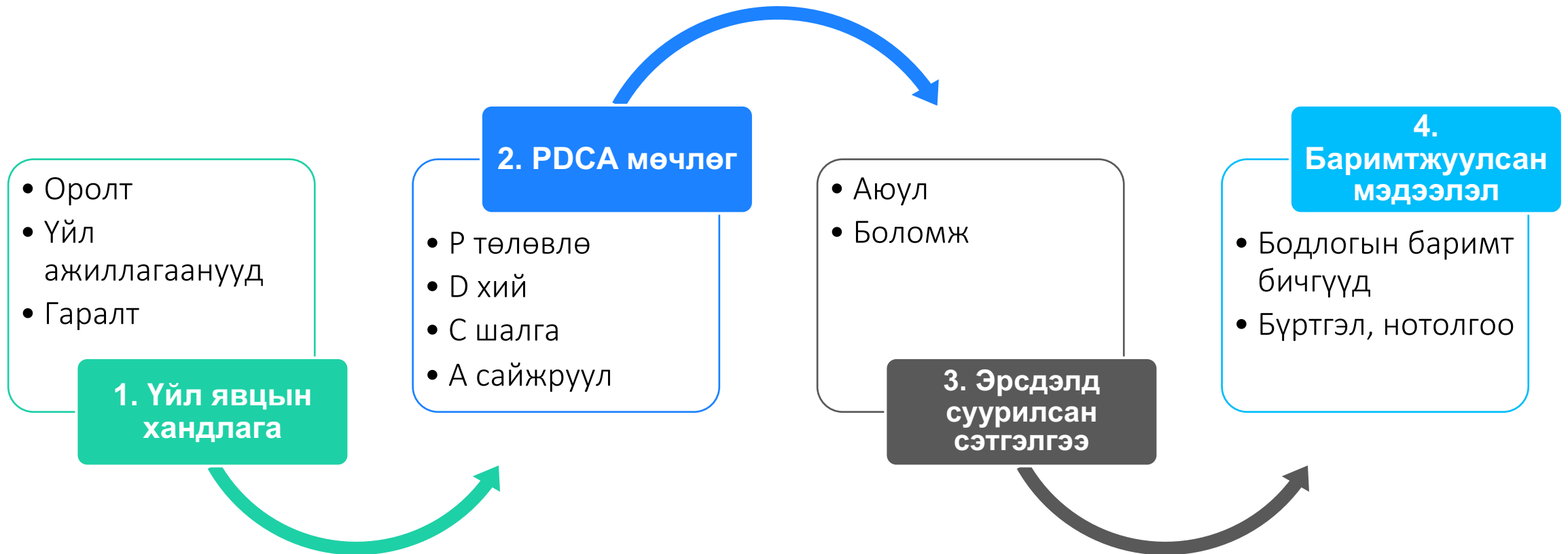
04 Хүмүүсийн чадамж дээшлэх

Дотоод, гадаадаас аюулгүй байдлыг тогтмол хянаж, байгууллагыг бүхэлд нь бэхжүүлэх

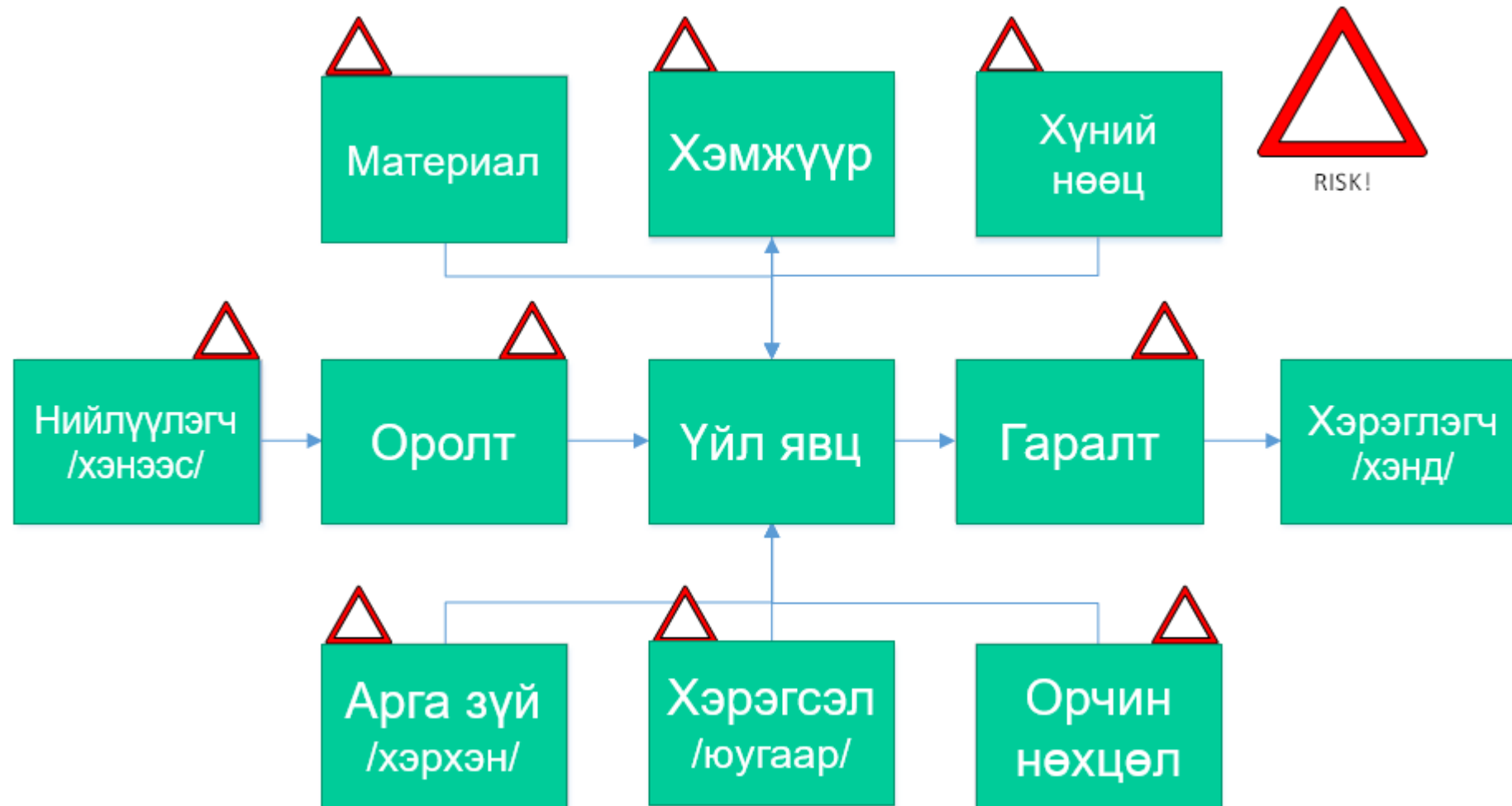
1. Үйл явцууд тогтолцоог бий болгодог



ISO менежментийн тогтолцоог нэвтрүүлэхэд хэрэглэгдэж буй үндсэн аргачлалууд:



3. Эрсдэлд суурилсан сэтгэлгээ



ISO 27001 стандартын шаардлага

PLAN

4. Байгууллагын төлөв

Байгууллага өөрийн орчинг таньж мэдэх

Сонирхогч талуудын хэрэгцээ, хүлээлтийг таньж мэдэх

Хамрах хүрээ тогтоох

Процессуудыг тодорхойлох

5. Манлайлал

Манлайлал ба үүрэг амлалт

Бодлого тодохойлох

Үүрэг хариуцлага, эрх мэдлийг тогтоох

6. Төлөвлөлт

Эрсдэл ба боломжид чиглэсэн үйл ажиллагаа

Зорилт ба түүний биелэлтийг төлөвлөх нь

Өөрчлөлтийг төлөвлөх нь

7. Дэмжих үйл ажиллагаа

Нөөц

Ур чадвар

Мэдлэг ойлголт

Харилцаа холбоо

Баримтжуулсан мэдээлэл

DO

8. Үйл ажиллагаа

Үйл ажиллагааны төлөвлөлт ба хяналт

МАБ-ын эрсдэлийг үнэлэх нь

МАБ-ын эрсдэлийг бууруулах арга хэмжээг төлөвлөх

CHECK

9. Гүйцэтгэлийн үнэлгээ

Хяналт, хэмжилт, дүн шинжилгээ, үнэлгээ

Дотоод аудит

Удирдлагын дүн шинжилгээ

ACT

10. Сайжруулалт

Байнгын сайжруулалт

Үл тохирол ба залруулах арга хэмжээ



6. Төлөвлөлт

6.1 Эрсдэл,
боломжуудыг
шийдвэрлэх арга
хэмжээ

6.2 МАБ зорилт,
түүнд хүрэх
төлөвлөлт

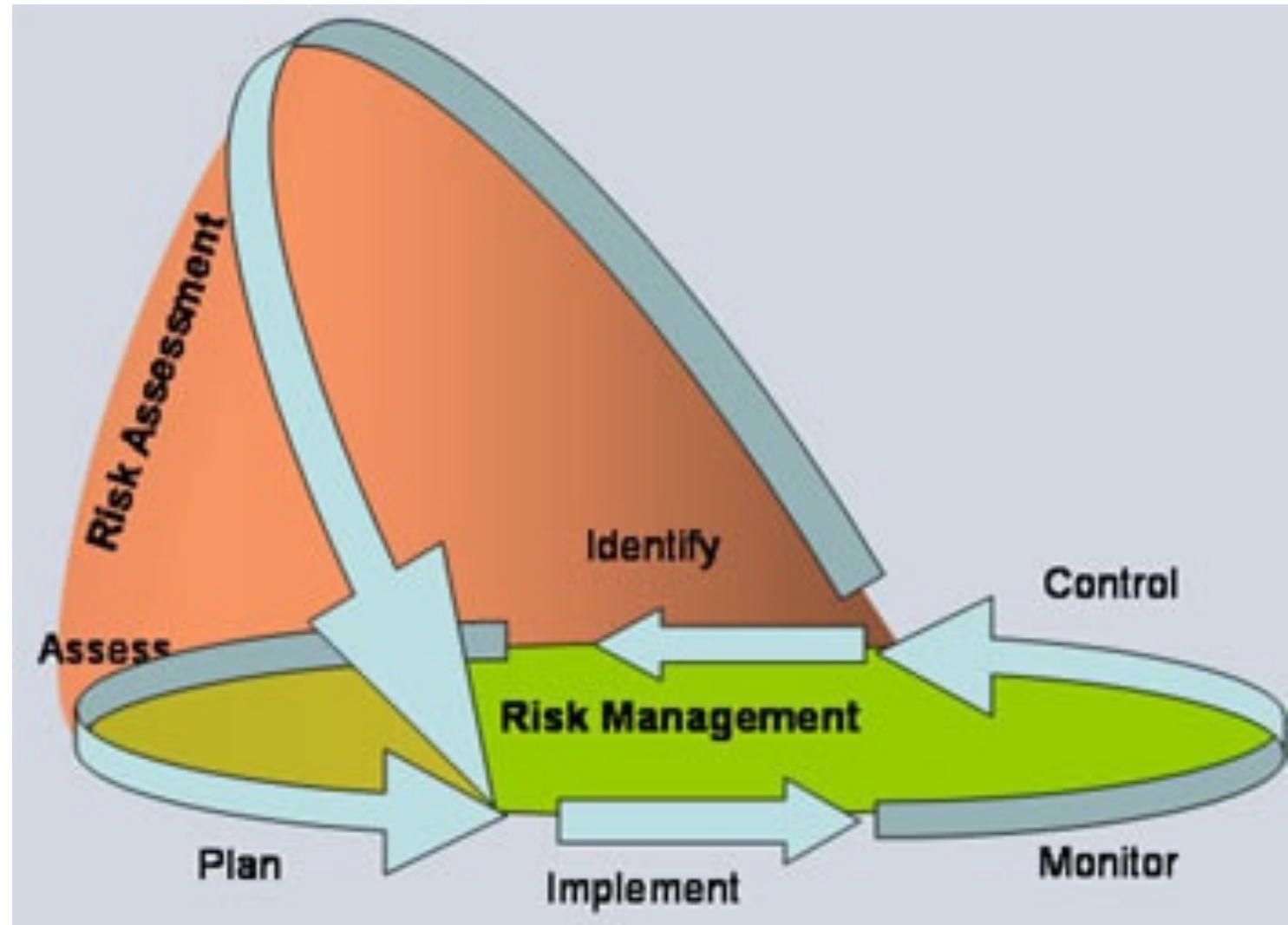
6.3 Өөрчлөлтийг
төлөвлөх

6.1 Эрсдэл, боломжуудыг шийдвэрлэх арга хэмжээ

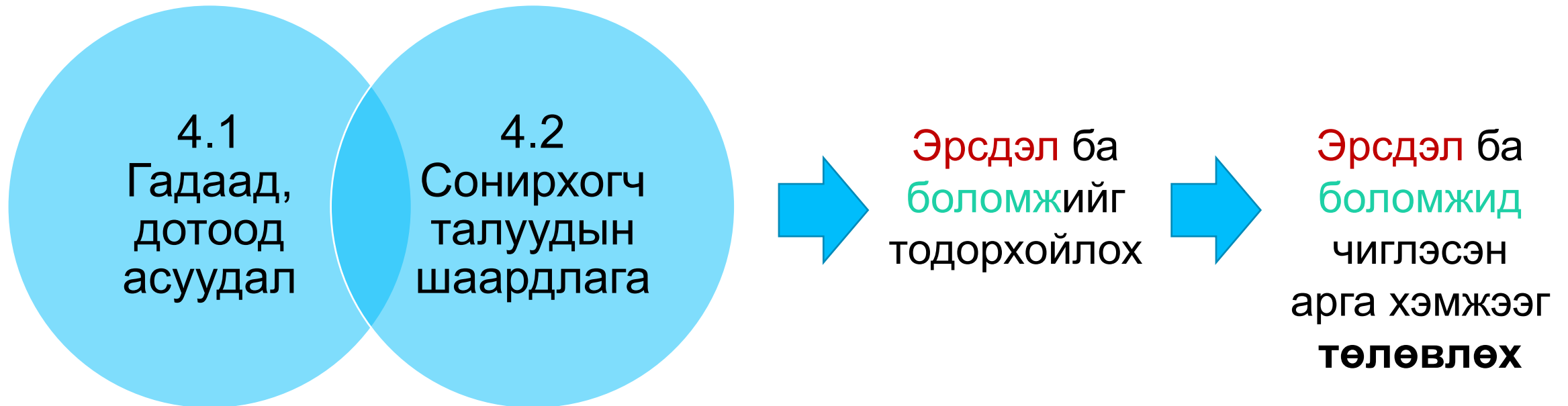
6.1.1 Ерөнхий зүйл
/Төлөвлөлт/

6.1.2 МАБ эрсдэлийн
үнэлгээ

6.1.3 МАБ эрсдэлийг
тодорхойлох арга хэмжээ



6.1.1 Ерөнхий зүйл /Төлөвлөлт/



6.1.2 МАБ эрсдэлийн үнэлгээ

Аль эрсдэлийг бууруулах, алийг нь хүлээж авах, шилжүүлэхийг тодорхойлохын тулд эрсдэлийн үнэлгээг ашигладаг.

Байгууллага нь МАБ эрсдэлийн үнэлгээний үйл явцыг тодорхойлж, хэрэгжүүлж, баримтжуулсан байна. Үүнд:

- a) МАБ эрсдэлийн шалгуур үзүүлэлт
- b) МАБ эрсдэлийн дахин үнэлгээ
- c) МАБ эрсдэлийн түвшинг тодорхойлох
- d) Эрсдэлд дүн шинжилгээ хийх
- e) Эрсдэлийг шинжлэх



МАБ-ын эрсдэл гэж юу вэ

ISO 27000:2022

- Эрсдэл:

→ 3.6.1: Тодорхой бус байдлын зорилгод үзүүлэх нөлөө

- Нөлөө:

→ 3.61, тайлбар хэсэг:

- Эерэг нөлөө → боломж
- Сөрөг нөлөө → аюул
- Эсвэл хоёул → боломж болон аюул



МAB-ын эрсдэл гэж юу вэ

ISO 27000:2022

- МAB-ын эрсдэл:
 - 3.61, тайлбар хэсэг: мэдээллийн аюулгүй байдлын зорилтуудад тодорхой бус байдлын үзүүлэх нөлөө...

Жишээ

Маргааш бороо орох тухай цаг агаарын мэдээ гарав.

- Тариаланч → Боломж !



- Аялагч → Аюул



Яагаад эрсдэлийг удирдах ёстой вэ

- Хүний бүхий л үйл ажиллагаанд эрсдэл байдаг

! түүнийг удирдах нь зайлшгүй

! ухамсартай, ухамсаргүйгээр удирддаг.

- Зам хөндлөн гарах
- Аялалд явах
- Машин жолоодох
- Хувьцаанд хөрөнгө оруулалт хийх г.м...



- Бизнес ч мөн эрсдэл бүхий л процесст бий

! түүнийг удирдах нь зайлшгүй

! ухамсартайгаар буюу загварчилж удирдах ёстой.

INTERNATIONAL
STANDARD

ISO/IEC
27005

Fourth edition
2022-10

**Information security, cybersecurity
and privacy protection — Guidance on
managing information security risks**

*Sécurité de l'information, cybersécurité et protection de la vie
privée — Préconisations pour la gestion des risques liés à la sécurité
de l'information*



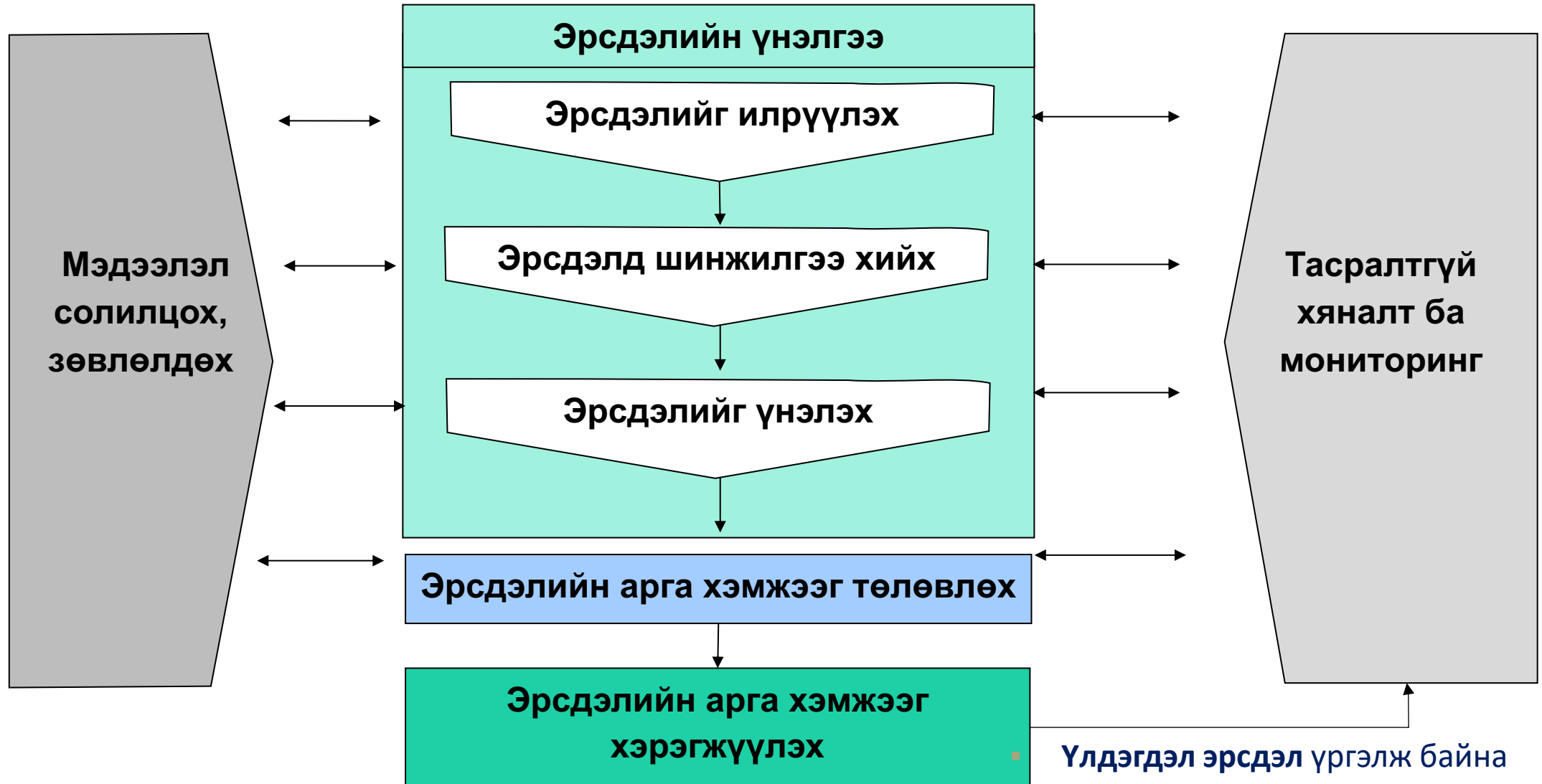
Reference number
ISO/IEC 27005:2022(E)

© ISO/IEC 2022

ISO 27005:2022

Мэдээллийн аюулгүй байдал, кибер
аюулгүй байдал, хувийн нууцлалын
хамгаалалт - Мэдээллийн аюулгүй
байдлын эрсдэлийг удирдах арга зүй

Эрсдэлийн удирдлагын арга зүй

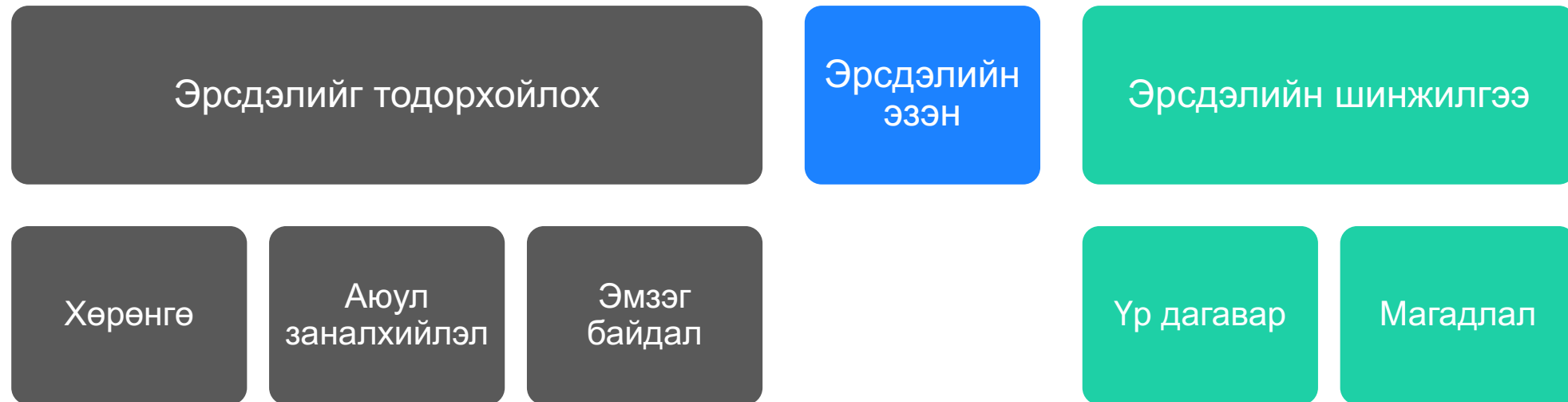


8.2 МАБ эрсдэлийн үнэлгээ

Байгууллага нь:

- a) Төлөвлөгөөт хуваарийн дагуу эсвэл далайцтай өөрчлөлт хийхээр зэхэж байгаа буюу хийсэн үед 6.1.2-д тодорхойлсон шалгуурын дагуу МАБ-ын **эрсдэлийн үнэлгээ хийнэ.**
- b) МАБ-ын эрсдэлийн үнэлгээний үр дүнг **баримтжуулсан мэдээлэл** хэлбэрээр хадгална.

Эрсдэлийн үнэлгээ



МАН-ын эрсдэлийн үнэлгээ хийх процесс

ISO 27005:2022

***6.1.2**

ЭРСДЭЛИЙГ ТОДОРХОЙЛОХ
(7.2-р зүйл)

МАН-ын эрсдэлийг тодорхойлох арга зүй

- a) Эрсдэлийн хөрөнгөд суурилсан арга (Asset based)
- b) Эрсдэлийн тохиолдол /үйл явдалд суурилсан арга (Event based)

***ISO 27001**

МАН-ын эрсдэлийн үнэлгээ хийх процесс

ISO 27005:2022

*4.1, 4.2

НӨХЦӨЛ БАЙДЛЫГ
ТОДОРХОЙЛОХ (6-р Зүйл)

- МАН-ын эрсдэлийн үнэлгээ хийх процессыг тодорхойлж, мөрдүүлэх:
 - Эрсдэлийн үнэлгээний шалгуур – эрсдэлийн ач холбогдлыг тодорхойлж, эрсдэлтэй холбоотой шийдвэр гаргах үндэслэлд тавих шаардлага
 - ✓ Байгууллагын зорилт, 4.1 болон 4.2-ийг авч үзэх
 - ✓ Эрх бүхий менежментийн түвшинд батална
 - ✓ Магадлал, үр дагаварыг тоон аргаар үнэлэх нь оновчтой

*ISO 27001

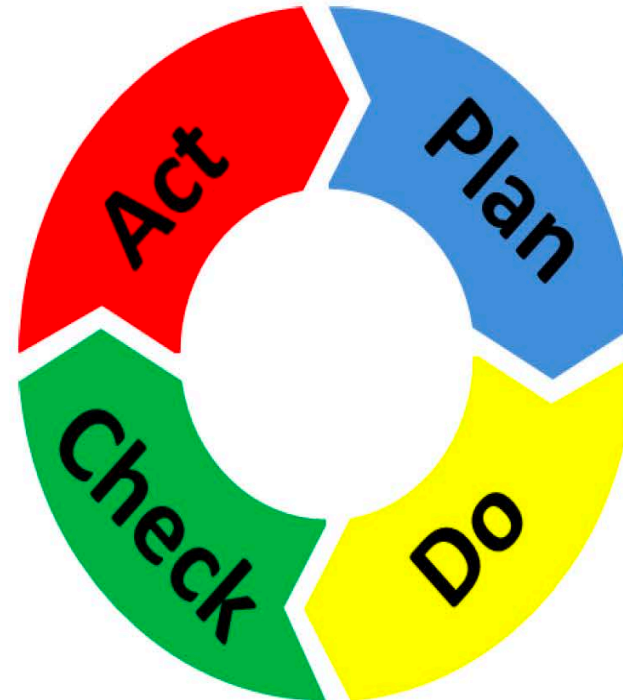
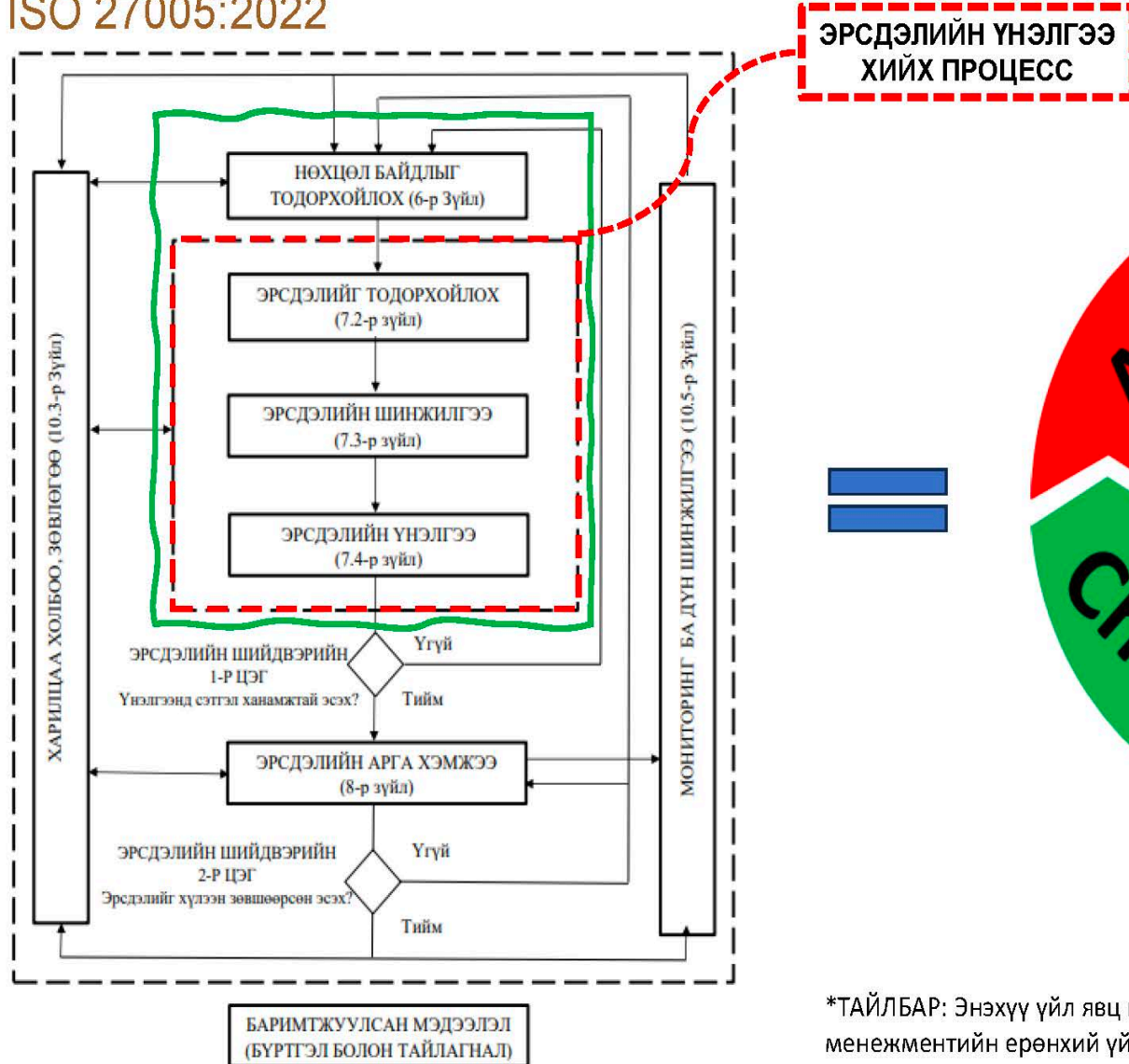
Жишээ:

дундаж давтамж ойролцоогоор	Log илэрхийлэл	Хуваарийн утга
Цаг тутамд	(Ойролцоогоор 10^5)	5
8 цаг тутамд	(Ойролцоогоор 10^4)	4
Долоо хоногт 2 удаа	(Ойролцоогоор 10^3)	3
Сард 1 удаа	(Ойролцоогоор 10^2)	2
Жилд 1 удаа	(10^1)	1
Арван жилд 1 удаа	(10^0)	0

Үр дагавар (алдагдал)	Log илэрхийлэл	Хуваарийн утга
£1 000 000	(10^6)	6
£100 000	(10^5)	5
£10 000	(10^4)	4
£1 000	(10^3)	3
£100	(10^2)	2
£100-оос бага	(10^1)	1

← МАБ-ын эрсдэлийн үнэлгээ хийх процесс

ISO 27005:2022



*ТАЙЛБАР: Энэхүү үйл явц нь ISO 31000 стандартад тодорхойлсон эрсдэлийн менежментийн ерөнхий үйл явцад үндэслэнэ.

МАН-ын эрсдэлийн үнэлгээ хийх процесс

ISO 27005:2022

Боломжит үр дагаваруудын төрөл:

- a) хувь хүн, бүлэг хүмүүсийн амь нас хохирох, гэмтэл учруулах;
- b) эрх чөлөө, нэр төр, хувийн нууцыг хамгаалах эрхээ алдах;
- c) боловсон хүчин, оюуны өмч (үр чадвар, туршлага)-өө алдагдах;
- d) дотоод болон гуравдагч талын үйл ажиллагааны доголдол (жишээ нь бизнесийн үйл ажиллагаа эсвэл үйл явц);
- e) **төлөвлөгөө болон дуусах хугацаанд үзүүлэх нөлөө;**
- f) бизнесийн болон санхүүгийн үнэ цэнээ алдах;
- g) бизнесийн давуу тал буюу зах зээлд эзлэх байр сууриа алдах;
- h) **олон нийтийн итгэл, нэр хүндэд хохирол учруулах;**
- i) **хууль тогтоомж, зохицуулалтын болон дүрэм журмын шаардлагыг зөрчих;**
- j) **гэрээ, үйлчилгээний түвшинг зөрчих;**
- k) **сонирхогч талуудад үзүүлэх сөрөг нөлөө;**
- l) байгаль орчинд үзүүлэх сөрөг нөлөө, бохирдол гэх мэт...

МАН-ын эрсдэл тодорхойлох

Эрсдэлийн хөрөнгөд суурилсан арга: ISO 27005:2022

- Эрсдэлийн хөрөнгө, аюул занал, эмзэг байдлын талаар дэлгэрэнгүй авч үзэж, үйл ажиллагааны хувилбаруудыг тодорхойлох.
- Эрсдэлийн хөрөнгө: байгууллагад үнэ цэнэтэй, тиймээс хамгаалалт шаарддаг аливаа зүйлс
 - Know-how
 - Брэнд
 - Бизнес процесс
 - Биет хөрөнгө
 - Биет бус хөрөнгө
 - Ажилтан г.м
 - Мэдээлэл
 - Hardware, software,



ГАЛЫН ГУРВАЛЖИН



МАБ хөрөнгө

Дэд бүтэц	IT, харилцаа холбооны төхөөрөмж	Програм хангамж, өгөгдлийн сан	Бусад баримт бичиг, өгөгдөл	Хүний нөөц	Гуравдагч талын үйлчилгээ
- Оффис өрөө, тавилга - Үйлдвэрлэлийн байгууламжууд - Дэд бүтцийн кабель (цахилгаан, газардуулга гэх мэт) - Үндсэн үйлчилгээ (цахилгаан, ус, ариутгах татуурга, HVAC, агааржуулагч, гал унтраах гэх мэт) - Серверийн өрөө, дата төв - Алсын зайн ажлын талбар - Архив, агуулах - Сейф - Анги, танхим - UPS төхөөрөмжүүд - Цахилгаан үүсгүүрүүд - Тээврийн хэрэгсэл - Түлхүүрүүд - Анхааруулгын систем - CCTV/ камер - Карт ба карт уншигч	- Суурин компьютер - IT кабель - Серверүүд - Хэмжилтийн төхөөрөмж - Албаны утас - Wireless WAN - Wireless LAN - Санах ой, хадгалах хэрэгсэл - Принтер, факс, сканнер г.м - Сүлжээний төхөөрөмжүүд - Гар утасны төхөөрөмжүүд (зөөврийн компьютер, таблет, ухаалаг гар утас, PDA)	- Өгөгдлийн сан - Төрөл бүрийн програм хангамжийн хэрэгсэл - Өгөгдлийн сангийн удирдлагын систем - Үйл ажиллагааны систем - Гуравдагч талын захиалгат програм хангамж - Дотооддоо боловсруулсан програм хангамж - Гуравдагч талын бэлэн програмууд (жишээ нь, оффисын багц)	- Тоног төхөөрөмжийн баримт бичиг - Бүртгэлүүд - Гуравдагч талын өгөгдөл - Хувийн мэдээлэл - Өмчлөлийн мэдээлэл - Дүрэм, журам, зааварчилгаа, төлөвлөгөө - Хууль, тогтоол, гэрээ, хэлэлцээр - Сургалтын баримт бичиг	- Зочид - Ажилтнууд - Дээд удирдлага - Зайнаас ажиллагч - Тодорхой туршлагатай ажилтнууд (системийн администратор, дизайнер, програм хангамж хөгжүүлэгч, аюулгүй байдлын мэргэжилтнүүд гэх мэт) - Дунд шатны удирдлага	- Цахилгаан хангамж - Интернэт - Аутсорсингийн ажилтнууд - Цэвэрлэгээ, байгууламжийн засвар үйлчилгээ - Аудиторууд, хяналтын байгууллагууд - Зөвлөхүүд - Хуулийн үйлчилгээ - Шуудангийн үйлчилгээ - Мэдээллийн технологийн тоног төхөөрөмжийн засвар үйлчилгээ - Харилцаа холбооны үйлчилгээ

МАБ-ын эрсдэл тодорхойлох

Жишээ



МАН-ын эрсдэл тодорхойлох

ISO 27005:2022

- 3.1.10 - **Эмзэг байдал**- Сөрөг үр дагавар (3.1.14)-тай тохиолдол үүсгэхэд ашиглаж болох өмч эсхүл хяналтын сул тал

Эмзэг байдлын түгээмэл жишээ

Ангилал	Дугаар	Эмзэг байдлын жишээнүүд
Техник хангамж	VH01	Хадгалах төхөөрөмжийн засвар үйлчилгээ хангалтгүй/алдаатай суурилуулалт
	VH02	Тоног төхөөрөмжийг солих төлөвлөгөөт хуваарь хангалтгүй
	VH03	Чийгшил, тоос, шороонд өртөмтгий
	VH04	Цахилгаан соронзон цацрагт мэдрэмтгий
	VH05	Тохиргооны өөрчлөлтийн хяналт хангалтгүй
	VH06	Хүчдэлийн өөрчлөлтөд мэдрэмтгий
	VH07	Температурын өөрчлөлтөд мэдрэмтгий
	VH08	Хамгаалалтгүй хадгалалт
	VH09	Устгалыг хянахгүй байх
	VH10	Хяналтгүй хуулбарлах

МАБ-ын нийтлэг аюул заналхийлэл/эрсдэл

1. Хорлох зорилгоор хүмүүсийн хувийн мэдээллийг задруулах. (санхүүгийн дансны мэдээлэл, зээлийн картын дугаар, татвар, эмнэлгийн бүртгэл, нууц харилцаа холбоо гэх мэт хувийн мэдээлэл /PII/)
2. Хувийн данс болон бусад нууц мэдээлэлд нэвтрэх нууц үгийг задруулах
3. Байгууллагын сүлжээнд зөвшөөрөлгүй нэвтрэх
4. Байгууллагууд засвар үйлчилгээний явцад системд сул тал үүсгэх
5. Цахилгааны тасалдлаас серверүүд офлайн болж, ажилтнууд ажиллаж чадахгүй болох
6. Цахилгаан, ус чийг, хорлон сүйтгэгч зэрэг асуудлаас дэд бүтэц гэмтэх
7. Компьютер эсвэл бусад тоног төхөөрөмж үе үе эвдэрч гэмтэх магадлалтай бөгөөд энэ нь мэдээллийг ашиглах боломжгүй болох
8. Цаасан мэдээлэл гэмтсэн эсвэл цахим файл гэмтэх, устгах
9. Ажилтнууд гэрлүүгээ цасан материал, эсвэл ажлын зөөврийн компьютер авч явах зэргээр байгууллагын нууц мэдээлэл хулгайд алдагдах
10. Байгалийн гамшиг болон цаг агаарын бусад үзэгдлүүдийн улмаас учрах хохирол, эвдрэл
11. Кибер гэмт хэрэгтнүүд байгууллагын өгөгдлийг устгах, дараа нь худалдах эсвэл ашиглах зорилгоор өгөгдлийг хулгайлж, үйл ажиллагааг тасалдуулах эсвэл бизнест өөр байдлаар хор хөнөөл учруулах

МАН-ын эрсдэл тодорхойлох

ISO 27005:2022

- 3.1.9 – **Аюул занал**- Систем эсхүл байгууллагад хохирол учруулж болзошгүй мэдээллийн аюулгүй байдлын аюултой тохиолдолын болзошгүй шалтгаан

Аюул заналын түгээмэл жишээ

Ангилал	Дугаар	Аюул заналын тайлбар
Физик аюул занал	TP01	Гал
	TP02	Ус
	TP03	Бохирдол, хортой радиаци
	TP04	Том осол
	TP05	Дэлбэрнлт
	TP06	Тоос, коррози, хөлдөлт
Байгалын аюул занал	TN01	Уур амьсгалын үзэгдэл
	TN02	Газар хөдлөлтийн үзэгдэл
	TN03	Галт уулын үзэгдэл
	TN04	Цаг уурын үзэгдэл
	TN05	Үер
	TN06	Цар тахал/халдварын үзэгдэл

МАН-ын эрсдэл тодорхойлох

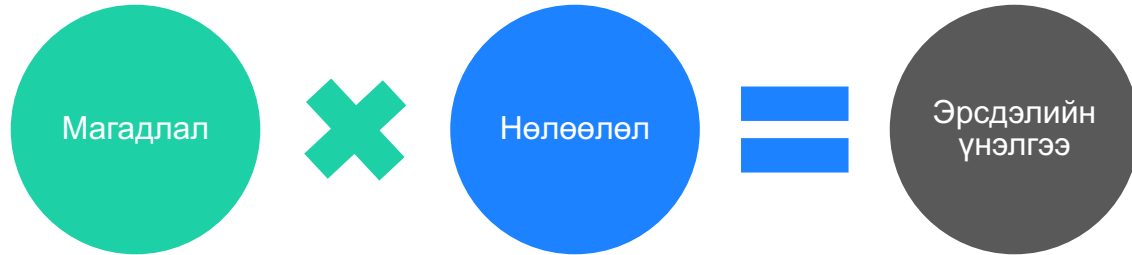
Эрсдэлийн тохиолдол /үйл явдалд суурилсан арга: ISO 27005:2022

- Эрсдэлийн эх үүсвэрийг авч үзэж, сонирхогч талууд эдгээр эрсдэлийг хүссэн зорилгодоо хүрэхийн тулд хэрхэн ашиглах стратегийн хувилбарыг тодорхойлох
- Эрсдэлийн тохиолдол /үйл явдал: тодорхой багц нөхцөл байдлын тохиолт эсвэл өөрчлөлт
 - ✓ Тохиолдол нь нэг буюу хэд хэд тохиож болох ба хэд хэдэн шалтгаан, үр дагавартай байж болно.
 - ✓ Тохиолдол нь хүлээгдэж буй ч тохиохгүй, эсхүл хүлээгдэж байгаагүй ч тохиож болно

Жишээ:

- Объектын гал түймэр
- Халдлага г.м

Эрсдэлийг хэрхэн үнэлэх вэ?



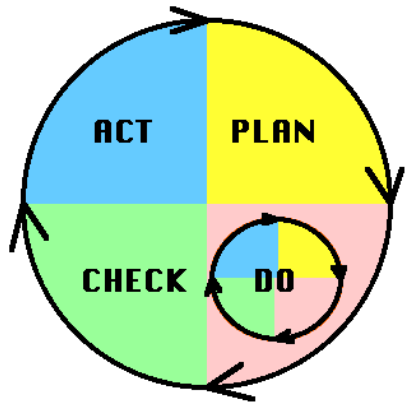
Impact
How severe would the outcomes be if the risk occurred?

Probability
What is the probability the risk will happen?

	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

8.2 МАБ эрсдэлийн үнэлгээ

Хөрөнгө	Эрсдэлийн эзэн	Эрсдэлийн аюул, заналхийлэл	Эмзэг байдал	Үр дагавар (1-5 оноо)	Магадлал (1-5 оноо)	Эрсдэлийн үнэлгээ	Дахин үнэлгээ
Сервер	Сүлжээний ажилтан	Цахилгааны тасалдал	UPS байхгүй	3	2	6	6
		Гал гарах	Гал унтраах хэрэгсэл бхгүй	4	4	16	10
Гэрээ	Хуулийн зөвлөх	Зөвшөөрөгдөөгүй хүн нэвтрэх	Баримт бичгийн биет хамгаалалт хангалтгүй	3	4	12	16
Систем админ	МТ албаны дарга	Осолд орох	Системийн нууц үгнүүдийг өөр мэдэх хүн бхгүй	5	3	15	10



8. Үйл ажиллагаа

8.1 Үйл ажиллагааны төлөвлөлт ба хяналт

8.2 МАБ эрсдэлийн үнэлгээ

8.3 МАБ эрсдэлд чиглэсэн арга хэмжээ

6.1.3 МАБ эрсдэлд чиглэсэн арга хэмжээ

Байгууллага нь МАБ-ыг тодорхойлж, эрсдэлийн үеийн ажиллагааны үйл явцыг хэрэгжүүлнэ. Ингэхдээ:

- a) Эрсдэлийн үнэлгээний үр дүнгээс МАБ-ын эрсдэлийг бууруулах тохиромжтой хувилбарыг **сонгох**
- b) Сонгосон хувилбарыг хэрэгжүүлэхэд шаардлагатай бүх **хяналтыг тодорхойлох**
- c) Тодорхойлсон хяналтыг А хавсралт дахь хяналттай харьцуулж, **шаардлагагүй хяналтыг хасах** эсвэл нэмэх
- d) А хавсралтын хяналтыг оруулахгүй байх үндэслэл зэргийг агуулсан “Хэрэглэх тухай **мэдэгдэл**”-ийг гаргах
- e) МАБ эрсдэлийг бууруулах **төлөвлөгөө боловсруулах**
- f) МАБ эрсдэлийн төлөвлөгөө ба үлдэгдэл эрсдэлийг хүлээн зөвшөөрч бгааг баталгаажуулах

Энэ үеийн ажиллагааны үйл явцыг **баримтжуулсан мэдээлэл хэлбэрээр** хадгална.

6.1.3. МАБ-ын эрсдэлд авах арга хэмжээ

ISO 27001:2022

6.1.3 Мэдээллийн аюулгүй байдлын эрсдэлийг бууруулах арга хэмжээ

Байгууллага нь мэдээллийн аюулгүй байдлын эрсдэлийг бууруулах дараах үйл явцыг тодорхойлж хэрэгжүүлнэ:

а) эрсдэлийн үнэлгээний үр дүнг харгалзан үзэж мэдээллийн аюулгүй байдлын эрсдэлийг бууруулах тохиромжтой хувилбарыг сонгох

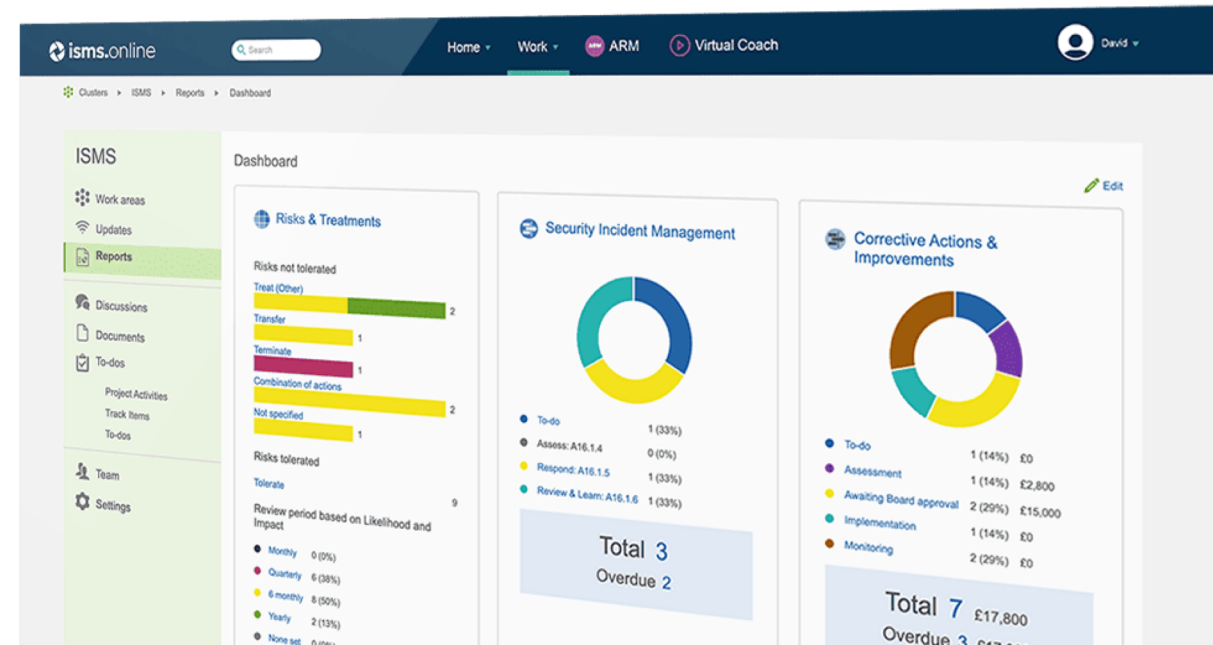
ISO 27005:2022

- Эрсдэлээс зайлсхийх
- Эрсдэлийг өөрчлөх
- Эрсдэлийг хадгалах
- Эрсдэлийг хуваалцах
- Эрсдэлийг шилжүүлэх

8.3 МАБ эрсдэлийг бууруулах арга хэмжээ

Байгууллага нь МАБ эрсдэлийг бууруулах арга хэмжээний төлөвлөгөөг хэрэгжүүлнэ. Үр дүнг **баримтжуулсан мэдээлэл** хэлбэрээр хадгална.

6.1-д тодорхойлсон эрсдэлийг эмчлэх үйл явц бодитоор хэрэгжиж байгаа эсэхийг баталгаажуулахтай холбоотой.



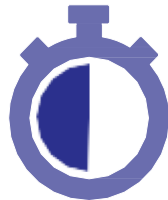
Бууруулах



%

Эрсдэлийн
магадлал ба
нөлөөллийг
багасгах үйл
ажиллагааг хийх

Зайлсхийх



%

Эрсдэлийг бий
болгох, ихэсгэх
үйл
ажиллагаанаас
татгалзах

Шилжүүлэх



%

Даатгал гэх
мэт аргаар
бусад
шилжүүлэх

Хүлээн зөвшөөрөх

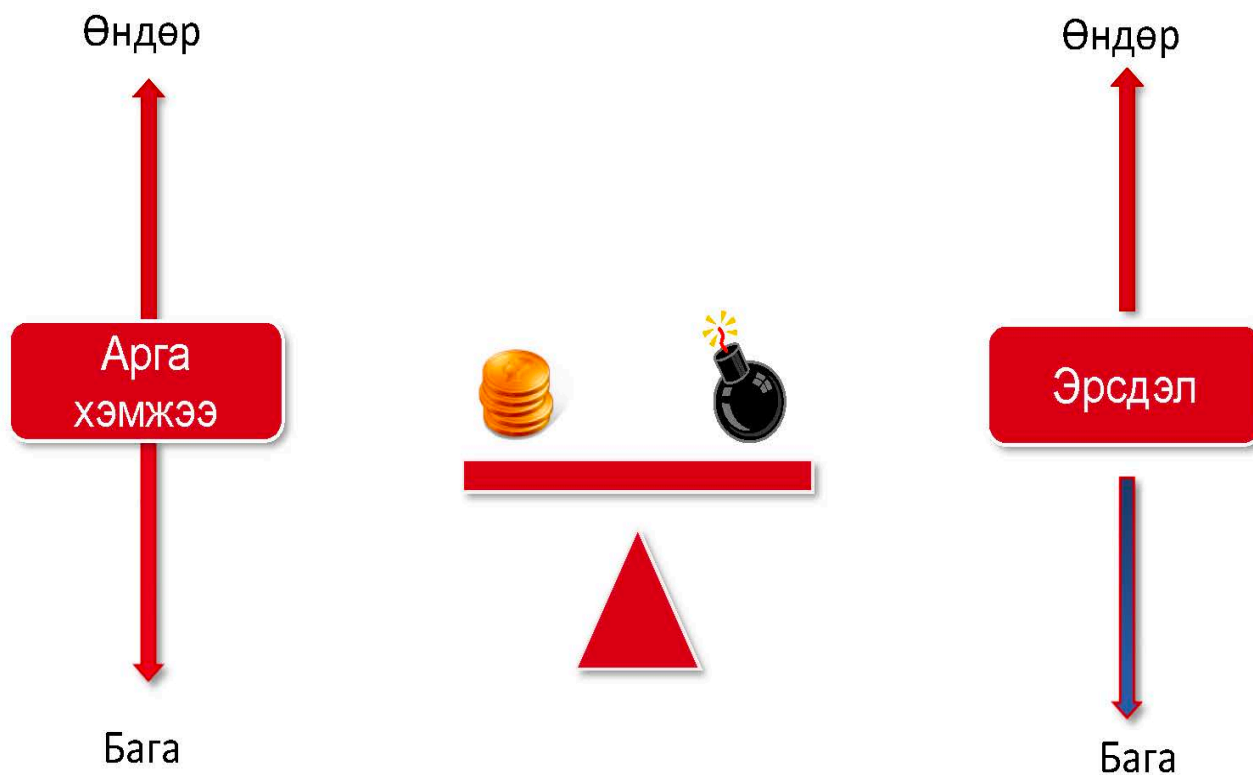


%

Хохирол
орлогоос
хамаараад
хүлээн
зөвшөөрөх

6.1.3. МАБ-ын эрсдэлд авах арга хэмжээ

ISO 27005:2022



6.1.3. МАБ-ын эрсдэлд авах арга хэмжээ

ISO 27001:2022

е) мэдээллийн аюулгүй байдлын эрсдэлийг бууруулах төлөвлөгөө боловсруулах

Э эрсдэлд авах арга хэмжээний төлөвлөгөө						
Эрсдэл авах арга хэмжээний төрөл	Хийгдэх ажил	Шаардлагатай нөөц	Гүйцэтгэлийн хэмжүүр	Гүйцэтгэж дуусах хугацаа	Хариуцагч	ХАМААРАХ ХЯНАЛТ

6.1.3. МАБ-ын эрсдэлд авах арга хэмжээ

ISO 27001:2022

f) эрсдэл эзэмшигчээс мэдээллийн аюулгүй байдлын эрсдэлийн төлөвлөгөөг батлуулах ба мэдээллийн аюулгүй байдлын эрсдэлийн үр дагаврыг хүлээн зөвшөөрүүлэх.

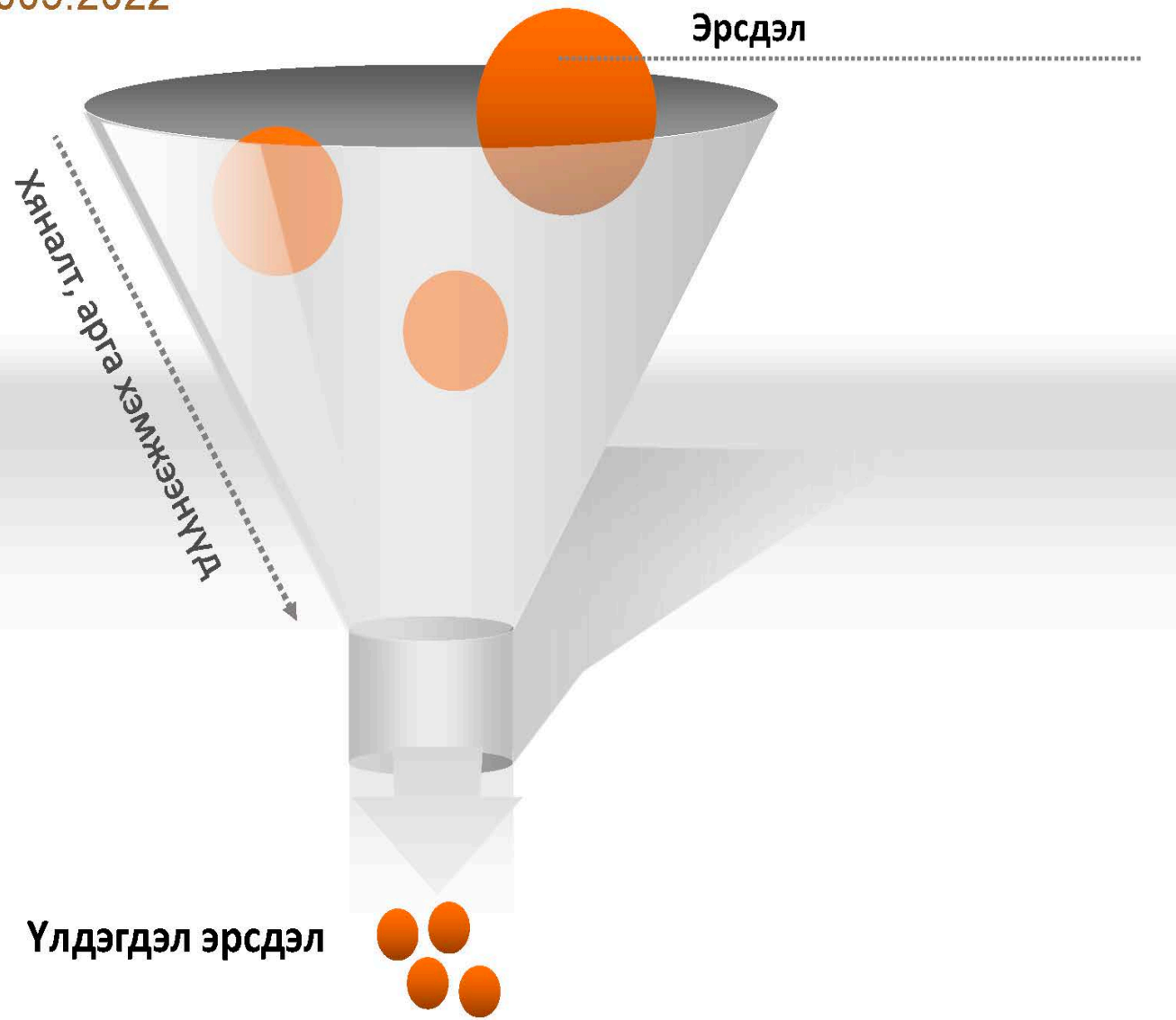
- Байгууллага нь мэдээллийн аюулгүй байдлын эрсдэлийг бууруулах үйл явцыг баримтжуулсан мэдээлэл хэлбэрээр хөтөлж хадгална.

ISO 27005:2022

- Арга хэмжээний төлөвлөгөөг батлуулах
- Үлдэгдэл эрсдэлийг хүлээн зөвшөөрөх

6.1.3. МАБ-ын эрсдэлд авах арга хэмжээ

ISO 27005:2022



Удирдлага нь үлдэгдэл эрсдэлийг мэдэж, тэдгээрийн хариуцлагыг хүлээх ёстой:

- Баримтжуулах;
- Хяналт тавих,
- Шаардлагатай бол цаашид арга хэмжээ

Анхаарах зүйлс

Бүх аюул, өртөмтгий байдлуудыг тодорхойлсон уу?

Эрсдэл болон эрсдэл эзэмшигч тодорхой болсон уу?

Эрсдэл гарах магадлалыг тооцоолохыг оролдсон уу?

Өөр хэн нэгэн ижил өгөгдлийг ашиглаад ижил үр дүнд хүрэх үү?

Энэ үйл явцыг давтан, тогтвортой ашиглаж болох уу?

Өөрчлөлтийн нөлөөллийг дүгнэх боломжийг олгодог уу?



THANK YOU



Д. БАТСАЙХАН
ХМТС-ийн багш, тоон гарын
үсгийн системийн шинжээч



- Тоон гарын үсгийн ашиглалт, хэрэглээ, төрөл зүйл, давуу болон дутагдалтай талууд, ашиглаж буй техник хэрэгсэл, цаашдын чиг хандлага

- Тоон гарын үсгийг гадаад орнуудад хүлээн зөвшөөрүүлэх, техник технологийн болон хууль эрх зүйн хүндрэлүүд, шийдэл, боломж, олон улсын туршлага

The background of the slide is a vibrant blue. On the left, a hand is shown holding a small, glowing blue globe. Behind the hand and globe, there is a faint, stylized city skyline. The background is also decorated with a grid of small white squares and several white plus signs. A large, semi-transparent blue circle is visible on the left side. The main title is written in large, white, sans-serif capital letters across the upper middle of the slide.

ҮНДЭСНИЙ НИЙТИЙН ТҮЛХҮҮРИЙН ДЭД БҮТЭЦ, ТООН ГАРЫН ҮСГИЙН ХЭРЭГЛЭЭ

Мон Пасс СА гэрчилгээ олгох байгууллага

МОНГОЛЫН ХАМГААГАХ
МОНПАСС CA

НИЙТИЙН ТҮЛХҮҮРИЙН ДЭД БҮТЭЦ БОЛОН ТООН ГАРЫН ҮСЭГ

ТОВЧ ТАНИЛЦУУЛГА

ТҮҮХЭН ТОВЧОО



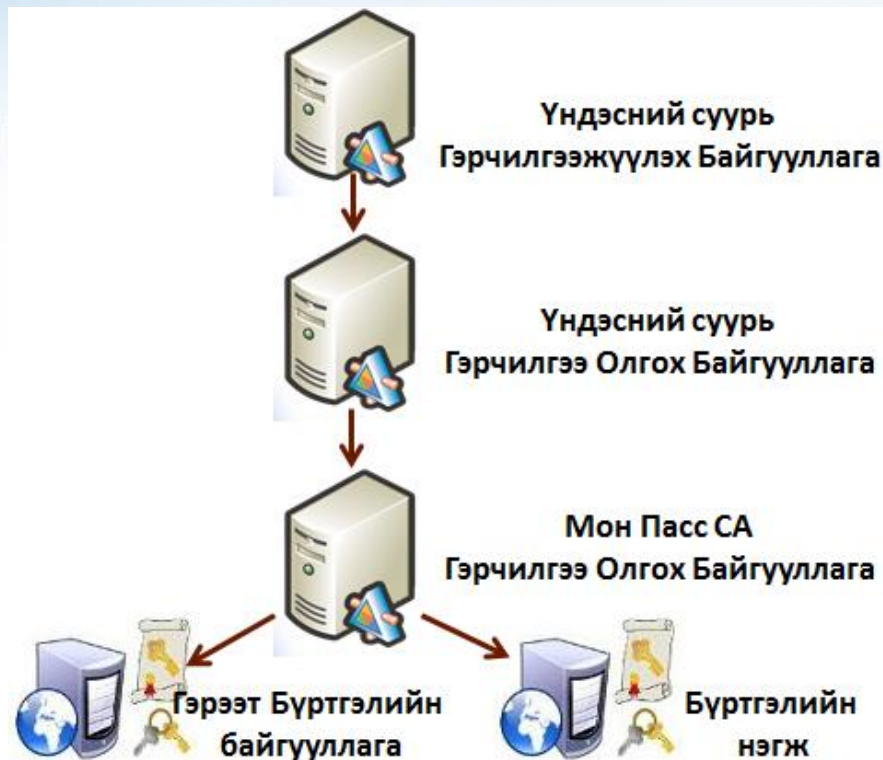
- 1999: Цахим засгийн анхны үзэл баримтлал
- 2003: Цахим засгийн э-офис, цаасгүй технологи, тоон гарын үсгийн санаачлага
- 2004: Цахим Монгол хөтөлбөр
- 2004: Цахим гарын үсгийн хуулийн анхны төсөл
- 2005: e-Government Master Plan-Цахим Засгийн мастер төлөвлөгөө
- 2006: Үндэсний НТДБ – PKI, Гэрчилгээ олгох байгууллага (санаачлага)
- 2011: “Цахим гарын үсгийн тухай” хууль, УИХ-ын 61-р тогтоол
- 2014: Үндэсний суурь гэрчилгээ олгох байгууллага (Үндэсний Дата Төв)
- 2011 - 2017: Үндэсний НТДБ-ийг байгуулах талаар төрөөс баримтлах бодлого, НТДБ-ийн нийтлэг журам, “Цахим Гарын Үсгийн тухай” хуулийг хэрэгжүүлэх ажлын төлөвлөгөө, Засгийн Газрын тогтоолууд
- 2015: Тоон гэрчилгээ олгох байгууллага (Мон Пасс СА), Үндэсний НТДБ
- 2016: Засгийн Газрын мөрийн хөтөлбөрт цахим засгийн э-офис, цаасгүй технологи
- 2017: Цахим албан хэрэг хөтлөлтийн нийтлэг журам



Монгол Улсын НТДБ



- Цахим засаг, Цахим бизнес, Цахим банкыг жинхэнэ утгаар хөгжүүлэхийн тулд иргэд, харилцагч, өгөгдөл, мэдээллийг хөдөлбөргүй таньж баталгаажуулах нь хамгийн чухал шаардлага болон хувирсан.
- Тоон гэрчилгээ үүнийг хангах үндсэн хэрэгсэл.
- Үндэсний НТДБ-РКИ байгуулахгүйгээр энэ боломжгүй.
- Дэлхийн улсуудад цахим засагт тоон гарын үсгийг эрчимтэй ашиглаж байна.
- Үндэсний Нийтийн Түлхүүрийн Дэд Бүтцийг (НТДБ) 2017 онд байгуулж дууссан.
- Мөн цахим банк, цахим нотариат, цахим худалдаа, цахим бизнест тоон гарын үсэг өргөн ашигладаг.



Нийтийн Түлхүүрийн Дэд Бүтэц

МОНПАСС

CA

Өндөр түвшний итгэлцэл болон үйл явцын аюулгүй орчныг хангаж буй хүмүүс, бодлого, журам, технологийн дэд бүтцийн нэгдэл.

Хүмүүс: НТДБ-ийг удирдаж, үйлчилж, үйлчилгээг нь ашиглаж буй хувь хүмүүс

Бодлого: НТДБ-ийг удирдах, үйлчлэх, ашиглах арга, замыг тодорхойлж буй үндсэн баримт бичгүүд.

Журам: НТДБ-ийн ашиг тусыг дээд хэмжээнд хүргэхийн тулд түүнийг удирдаж, ашиглаж буй хүмүүсийн заавал даган мөрдөх ёстой дэгүүд.

Технологи: **Certification Authorities (CAs)** болон **Registration Authority (RA)** хэмээн нэрлэгдэх өндөр түвшний нууцлалтай систем, түүний дэд бүтэц. Энэ дэд бүтцийн хүрээнд үүсгэгдсэн тоон гэрчилгээний тусламжтайгаар өндөр түвшний итгэлцэл хангагдана.



Тоон гэрчилгээ, крипто хамгаалалтын зорилго

МОНПАСС CA



Сүлжээн дахь итгэлцлийг бүрэн дүүрэн хангах;



Хэрэглэгчийг таньж баталгаажуулах;



Онлайн үйлчилгээ, нөөцөд хандах хандалтыг зөвшөөрөх;



Өгөгдлийн нууцлалыг хангах;



Тоон гарын үсэг зурснаар өгөгдлийн бүрэн бүтэн байдлыг хангах;



Хийсэн үйлдлээсээ татгалзах боломжгүй байдлыг хангах, баталгаажуулах.

ТООН ГЭРЧИЛГЭЭНИЙ ХЭРЭГЛЭЭ



Төр, бизнесийн бүх төрлийн онлайн үйлчилгээ

- Аюулгүй хандалт
- Гарын үсэг
- Шифрлэлт
- Цахим албан хэрэг

Э-Худалдаа

- Веб серверүүд
- Холболтууд
- Домэйны хяналтууд
- VPN
- SSL

Цахим захидал харилцаа ашиглагч хэн бүхэн

- Хувь хүн
- Байгууллага
- Гарын үсэг
- Шифрлэлт

Утасгүй холболт ашиглагч хэн бүхэн

Гэрчилгээний хэрэглээ

Э-Оффис

- Цахим албан хэрэг хөтлөлт, цаасгүй офис
- Цахим онлайн үйлчилгээ, цахим лавлагаа, хариу, баримт бичиг, харилцааны удирдлага

Банкууд

- Аюулгүй хандалт
- Гарын үсэг
- Онлайн гүйлгээ
- Э-чек, э-баримтууд

Програм хангамжийн үйлдвэрлэл эрхлэгч

- Эх кодоод тоон гарын үсэг зурж хамгаалах
- Mobile контентуудыг хамгаалах

ТӨРИЙН БАЙГУУЛЛАГЫН ТООН ГАРЫН ҮСГИЙН ХЭРЭГЛЭЭ



Цахим албан хэрэг
хөтлөлт, цаасгүй
технологи



Төрийн байгууллагад
гаргаж өгдөг цахим
тайлан, мэдээлэл



Бүх төрлийн системд
хандахад таньж
баталгаажуулах



Төрийн онлайн
үйлчилгээ үзүүлэх



Цахим худалдаа, худалдан
авалт, цахим тендер



Цахим шүүх, нотариатын
цахим албан хэрэг, гэрчлэлт,
цахим лавлагаа, баримт



Цахим гэрээ хэлцэл
байгуулах



Цахим тамга (digital
seal) дарах



Цагийн бүртгэл (тамга –
time stamp) хийлгэх

Цахим албан хэрэг хөтлөлт



Цахим (ухаалаг) засгийг хэрэгжүүлэх нэг үндсэн хүчин зүйл нь тоон гарын үсэгт суурилсан гадаад болон дотоод албан хэрэг хөтлөлт, архивийн ажиллагаа.

Дэлхийн улсуудын төрийн байгууллагууд тоон гарын үсэгт суурилсан дотоод цахим албан хэрэг хөтлөлтөд бүрэн шилжиж, цахим төрийн үйлчилгээнд тоон гарын үсгийн шийдлүүд ашиглаж цахим засгийн мэдээллийн аюулгүй байдал, итгэлцлийг хангаж, төсвийг хэмнэж, авилгатай тэмцэхэд амжилт олж байна.



Цахим тайлан, мэдээлэл



Дэлхийн улсуудад төрийн захиргааны болон хяналтын байгууллагад гаргаж өгдөг бүх төрлийн тайланг тоон гарын үсгээр зурж баталгаажуулах болсноор компани, аж ахуйн нэгжүүдэд хялбар, хямд төсөр болсноос гадна олон байцаагчийн орон тоо багасаж, цаас, хор гэх мэт офисын зардлууд, цаг хугацаа хэмнэгдэж улсын төсвийн зардлыг ихээхэн бууруулдаг.



Тоон гарын үсэгт суурилсан хандалтын удирдлага



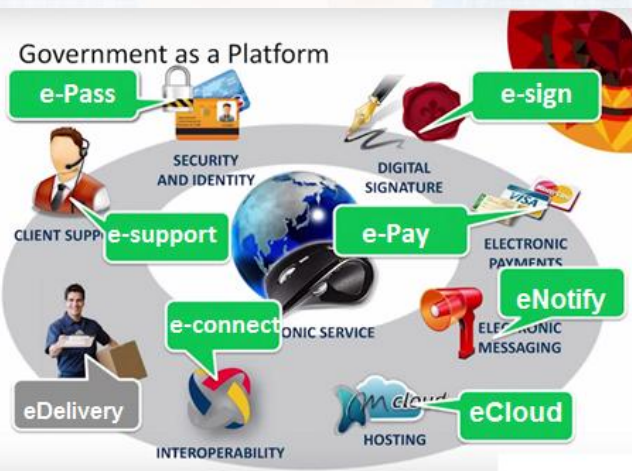
Дэлхийн улсуудын төр, бизнесийн байгууллага, банкууд өөрийн мэдээллийн системийн хандалтын удирдлагыг тоон гарын үсэгт суурилан зохион байгуулдаг (2 хүчин зүйлт хандалт - 2FA) болсноор хэрэглэгчийг хөдөлбөргүй таньж баталгаажуулдаг болж системд хууль бусаар хандах боломжийг бүрэн хааж чадсан.



Тоон гарын үсэгт суурилсан төрийн үйлчилгээ



Дэлхийн улсуудын цахим засгийн онлайн үйлчилгээнд хандахад өөрийгөө таниулж баталгаажуулах, үйлчилгээ авахын тулд иргэд өөрсдийн тоон гарын үсгээ (иргэний үнэмлэх юмуу крипто токенод агуулсан) ашигладаг, төрийн зүгээс хариу үзүүлэх төрийн үйлчилгээ, баримт бичиг, лавлагаа зэрэг нь төрийн албан хаагчийн тоон гарын үсгээр баталгаажин илгээгддэг. Үүний үр дүнд төсвийн ихээхэн хэмнэлт бий болдог.



Цахим Худалдан авалт, Тендер



DIGITAL SIGNATURE CERTIFICATE
E-TENDERING, E-FILLING, E-PROCUREMENT, E-BINDING

Дэлхийн улсуудын төр, бизнесийн худалдан авалтыг тоон гарын үсгийн шийдэлд суурилан цахим хэлбэрээр зохион байгуулдаг, тендерийн материал, худалдах, худалдан авах санал, байгуулж буй гэрээг тоон гарын үсэг зурж шууд илгээдэг, байгуулдаг болсон. Энэ нь авилгатай тэмцэх, тендерийн булхай, залилан гарахаас сэргийлэх хүчирхэг хэрэгсэл гэж тооцогддог.

Цахим шүүх, нотариат

МОНПАСС CA



Хууль, шүүхийн байгууллагууд дотоод цахим албан хэрэг хөтлөлтөд шилжсэнээс гадна иргэдэд олгох төрөл бүрийн лавлагаа, баримтыг тоон гарын үсэг зурж цахим хэлбэрээр илгээдэг, иргэдийн өргөдөл, гомдол, хүсэлтийг цахим хэлбэрээр авдаг болсон.

Европ, АНУ, Азийн нотариатчид иргэдийн батлуулахыг хүссэн, тоон гарын үсэг зурсан баримт бичиг, гэрээг тоон гарын үсгээрээ баталж онлайнаар илгээдэг болсон нь мэдээллийн нийгмийг жинхэнэ утгаар нь хөгжүүлэх боломжийг хангасан.

Цахим гэрээ хэлцэл



G2G, G2B, G2C, B2G, C2G хэлцлүүд, Улс хооронд, аж ахуйн нэгж, компани хооронд солилцож буй гэрээ хэлцэл, баримт бичиг, ажил үйлчилгээ хүлээлцсэн баримт бичгийг цахим хэлбэрээр тоон гарын үсгээр баталгаажуулдаг болсноор мэдээллийн нийгэм, цахим засаг, бизнес төлөвшиж, төсвийн ихээхэн хэмнэлт бий болсон



Цахим тамга

www.monpass.ca

MONPASS CA



Цахим тамга (eSeal – digital seal) гэж хуулийн этгээдтэй салшгүй холбоотойгоор олгосон тоон гарын үсгийн хос түлхүүр гэрчилгээ болно. Хуулийн этгээдийг итгэмжлэлгүйгээр төлөөлөх этгээд ашиглана. Тоон гарын үсгээс ялгагдах ялгаа нь баримт бичигт тоон гарын үсэг зурахад зурсан хүний мэдээлэл биш харин байгууллагын тамганы зураг тавигддагт оршино. Цахим тамгыг баримт бичигт цахим тамга дарах, олон тооны баримт бичигт автоматаар тамга дарах, хуулийн этгээдийг баталгаажуулахад ашиглана. Хуулийн этгээдийг итгэмжлэлгүйгээр төлөөлөх этгээдийг болон баримт бичгийн үнэн зөв, бүрэн бүтэн байдлыг батална.

Цагийн бүртгэл

www.monpass.ca



Цагийн бүртгэл (цагийн тамга - timestamp) гэж огноо болон цагийг цахим хэлбэртэй өөр өгөгдөлд холбож өгөх үйл явц. Үүний үр дүнд тодорхой цахим өгөгдөл, тоон гарын үсэг зурсан этгээд тухайн цаг үед, хүчин төгөлдөр оршин байсан гэдгийг удаан хугацааны дараа баталгаажуулах, тоон гарын үсгийг давхар батлах боломжтой болдог. Үндсэн шаардлагыг RFC 3161 удирдамжаар тогтоосон. Үүний тулд Цагийн бүртгэлийн байгууллагыг НТДБ-ийн хүрээнд байгуулдаг. Уг байгууллага тоон гарын үсэг зурагдсан цахим өгөгдөлд тухайн цаг үед хүчин төгөлдөр болохыг баталсан цагийн бүртгэл (тамга) дарж өгснөөр удаан хугацааны дараа өгөгдөлд өөрчлөлт ороогүй, тоон гарын үсгийн гэрчилгээ хүчинтэй байсаныг батлах боломжтой болно.

ТӨРИЙН БАЙГУУЛЛАГАД ТООН ГАРЫН ҮСЭГ НЭВТРҮҮЛЭХ АЛХАМ



Ойлголтоо нэгтгэх

ГОБ-тай үүлзалт зохион байгуулж
ойлголтуудаа нэгтгэнэ.



Хөгжүүлэлт хийх

Тоон гарын үсгийн модуль хөгжүүлэх,
Төрийн системд холбох



Нэвтрүүлэлт хийх

Системийг тестлэж үйл ажиллагаанд
нэвтрүүлэх



Төлөвлөгөө гаргах

НТДБ-ийн ТГҮ-ийг системд нэвтрүүлэх
ажлын төлөвлөгөө гаргах



Сургалт зохион байгуулах

Хэрэглэгчидэд мэдээлэл түгээх,
сурталчилах, сургалт зохион байгуулах



ТООН ГАРЫН ҮСГИЙН ТЭЭГЧ



**Албан тушаалтан, Ажилтан, Иргэний тоон
гарын үсгийн хос түлхүүр, гэрчилгээг тээгч**

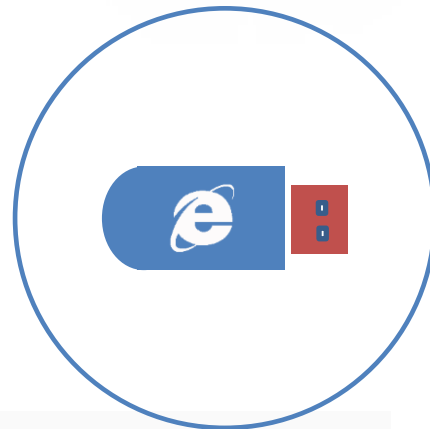
ИРГЭНИЙ ЦАХИМ
ҮНЭМЛЭХ



ҮҮЛЭНД БАЙРЛАХ КРИПТО
HSM ТӨХӨӨРӨМЖ



КРИПТО Э-ТОКЕН
ТӨХӨӨРӨМЖ



КРИПТО Э-ТОКЕН ТӨХӨӨРӨМЖ

Тогтвортой хөгжлийн
MONPASS CA



Тоон гарын үсгийн гэрчилгээг олгохын тулд крипто модуль бүхий тусгай тээгчид Хос түлхүүр үүсгэж гэрчилгээг суулгана. Энэ тээгчийн нэг төрөл нь Крипто модуль бүхий Э-Токен төхөөрөмж юм. Э-Токен төхөөрөмж нь өөртөө хос түлхүүр үүсгэж, нууцлан хадгалах крипто модуль бүхий тусгай төхөөрөмж бөгөөд зөвхөн Тоон гарын үсгийн хос түлхүүр тээх, хадгалах зориулалттай.

“Цахим Гарын Үсгийн тухай” хуулийн 7.2-т заасан тоон гарын үсгийг бүтээх болон тоон гарын үсгийн хувийн түлхүүр /цаашид “хувийн түлхүүр” гэх/-ийг хадгалах шаардлагыг хангасан тоон гарын үсгийн тээгч хэрэгсэл.

КРИПТО HSM ТӨХӨӨРӨМЖ



Аюулгүй байдлын техник хангамжийн модуль (HSM) — эвдлэх, дотроос нь өгөгдөл гаргаж авахаас бүрэн хамгаалагдсан техникийн төхөөрөмж бөгөөд шифрлэх, задлах, тоон гарын үсэг, түүний гэрчилгээ үүсгэхэд ашиглагддаг хос түлхүүрийг үүсгэх, шифрлэн хадгалах, удирдах замаар криптографын үйл явцыг хамгаалдаг. Аюулгүй байдлын хамгийн өндөр шаардлагын дагуу туршигдаж, шалгагдаж гэрчилгээждэг. “Цахим Гарын Үсгийн тухай” хуулийн 7.2-т заасан тоон гарын үсгийг бүтээх болон тоон гарын үсгийн хувийн түлхүүр /цаашид “хувийн түлхүүр” гэх/-ийг хадгалах шаардлагыг хангасан тоон гарын үсгийн тээгч хэрэгсэл гэж тооцогддог.

ТООН ГАРЫН ҮСГЭЭ АШИГЛАХ



- Тоон гарын үсгийн тээгч төхөөрөмжтэй ажиллахын тулд компьютер дээрээ МонПасс Клиент програм суулгана.
- www.monpass.mn веб хуудаснаас татаж авах боломжтой.
- “МонПасс сервис”-ийг системдээ уялдуулан холбоно.



ТООН ГАРЫН ҮСГИЙГ БАТАЛГААЖУУЛАХ

Тогт үнэн баталгаа
MONPASS CA



- Гэрчилгээний хугацаа дууссан эсэхийг шалгах
- Монпассын олгосон гэрчилгээ мөн эсэхийг шалгах
- Гэрчилгээг түтгэлзүүлсэн, хүчингүй болгосон эсэхийг шалгах
- Гэрчилгээ эзэмшигч мөн эсэхийг шалгах
- Файлд зурсан тоон гарын үсгийн хүчинтэй эсэхийг шалгах
- Цахим гүйлгээний агуулгад өөрчлөлт орсон эсэхийг шалгах
- Тоон гарын үсэг зурсан файлд өөрчлөлт орсон эсэхийг шалгах г.м

ГАРЫН ҮСЭГ ЗУРАХ

Товч тоон болгоогч
MONPASS CA

Товч тоон болгоогч
MONPASS CA

- PDF файлд тоон гарын үсэг зурах, Adobe Acrobat ашиглан олон тооны гарын үсэг зурах
 - Гарын үсэг зурах талбар үүсгэх, байршил тохируулах, зурах
- Doc, Excel файлд гарын үсэг зурах
- Email-д гарын үсэг зурах
- XML төрөлтэй файлд гарын үсэг зурах
- Текст төрөлтэй файлд гарын үсэг зурах
- Зураг, бичлэг болон бүх төрлийн файлд гарын үсэг зурах
- Онлайн порталд байршиж буй файлд гарын үсэг зурах
- Цахим гүйлгээ, баримтанд гарын үсэг зурах
 - Гар ажиллагаагаар
 - Автоматаар (Bulk sign)
- Цахим тайлан мэдээнд гарын үсэг зурах
- Өгөгдлийн сангийн өгөгдөлд гарын үсэг зурах
- Програм эх кодыг баталгаажуулж гарын үсэг зурах

ТООН ГАРЫН ҮСГЭЭР ШИФРЛЭХ (Encrypt/Decrypt)



- Хүлээн авагчийн нийтийн түлхүүр ашиглах шифрлэх
- Өөрийн нийтийн түлхүүр ашиглан шифрлэх
- Дараах төрлийн файлууд:
 - Цахим гүйлгээ болон цахим тайлан
 - PDF, Windows Office, Open Office файлууд
 - Өгөгдлийн сангийн өгөгдөл, бичлэгүүд
 - Зураг, видео бичлэг г.м бусад бүх төрлийн файл
 - Э-мэйл, түүний хавсралтууд

Дэлхийн улсуудад төрийн үйлчилгээнд тоон гэрчилгээ ашиглаж буй байдал

MONPASS CA



Олон төрлийн
систем



1 систем

eService
(123 үйлчилгээ)

Улсууд

Финлянд
FINID

3 системд

eService
(148 үйлчилгээ)
eHealth
eTicketing

Итали
CNS

5 системд

eService
(142 үйлчилгээ)
eDL
eGate
eBanking
eLibrary

Гонконг

10 системд

eID
eService
(124 үйлчилгээ)
eHealth
eTicketing
ATM
eDL
ePurse
eGates
Travel document

Малайз
MyKad

ТУЛГАРЧ БУЙ АСУУДАЛ

Тогтвортой Бизнесийн
MONPASS CA

Төрийн байгууллагын удирдлагын манлайлал, санаачлага дутмаг
Эрх зүйн зохицуулалтаа сайн ойлгодоггүй, бүх салбарт ашиглах
боломжийг бүрэн хуульчлаагүй

Тоон гарын үсгийн тухай ойлголт дутмаг байдал

Төрийн албан хаагч, шийдвэр гаргагчид тоон гарын
үсгийн талаар сайн ойлголтгүй учир нэвтрэлт
удаан, эсэргүүцэл их.

Технологийн шийдэл

Боломжгүй эсвэл шинээр хөгжүүлэх
шаардлагатай технологийн шийдлүүд
гарч ирэх

Системийн алдаа

Байгаль, техник, хүнээс хамааралтай
шалтгааны улмаас систем саатах, гацах,
ажиллагаанаас гарах,



Итгэлцэл

Тоон гарын үсгийн давуу талд үл
итгэх, харилцагчдаа үл итгэх, цаасанд
итгэх хуучинсаг үзлээсээ салж
чадахгүй байх

Хэрэглэгчдийн үл мэдлэг

Хэрэглэгчийн мэдлэггүй байдлын улмаас
үл ойлголт, буруу зөрүү ойлголт үүсэх,
эсэргүүцэх

Хэрэглээ

Монгол улсад гарын үсгийн хэрэглээ өргөн
дэлгэрээгүйгээс хэрэглээ хөгжихгүй,
нэвтрүүлэхийг эсэргүүцэх, улмаар цахим засгийн
хөгжлийг сааруулах,.

ШИЙДЭЛ



Цахим гарын үсгийн тухай хууль, Татварын хууль, Ня-бо
бүртгэлийн хууль, Нотариатын хууль г.м 100 гаруй хуульд
нэмэлт, өөрчлөлт оруулах

Төрийн албан хаагчдын сэтгэлгээний реинжиниринг,
төрийн алба хаагчдын сургалт хөгжил

Шаардлагатай технологийн шийдлүүдийг шинээр
хөгжүүлэх, бүх тестийг хийх, тогтмол сайжруулах

Техникийн бэлэн байдлыг хангах, тасралтгүй
ажиллагаа, сэргээн ажиллуулах төлөвлөгөө
хэрэгжүүлэх

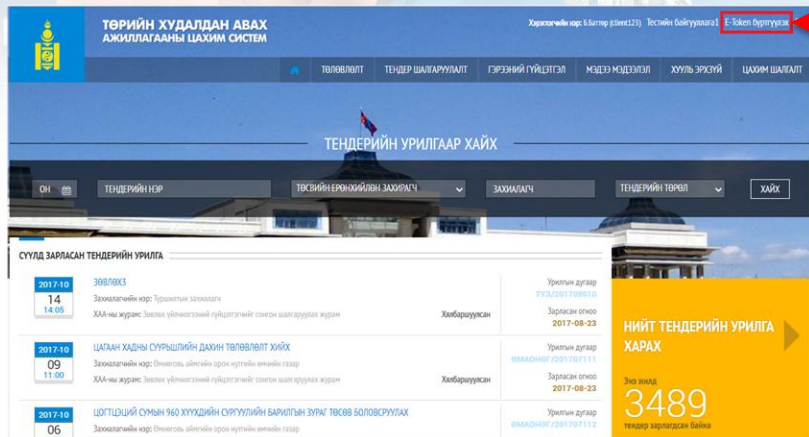
Сэтгэлгээний реинжиниринг, хууль, тогтоомжуудыг
сурталчилах, соён гэгээрүүлэх ажил, цаасгүй цахим соёл
төлөвшүүлэх

Нийгмийн соён гэгээрүүлэх ажил, Гарын авлага материалууд,
онлайн болон зайн сургалт, ТВ, сонин хэвлэл, Веб, сошиал
сайтаар сурталчлах

Хэрэглээ, тоон гарын үсгийн давуу тал, цахим нийгэм,
цахим засаг, бизнес хөгжих түлхүүр хүчин зүйл гэдгийг
сурталчлах г.м.

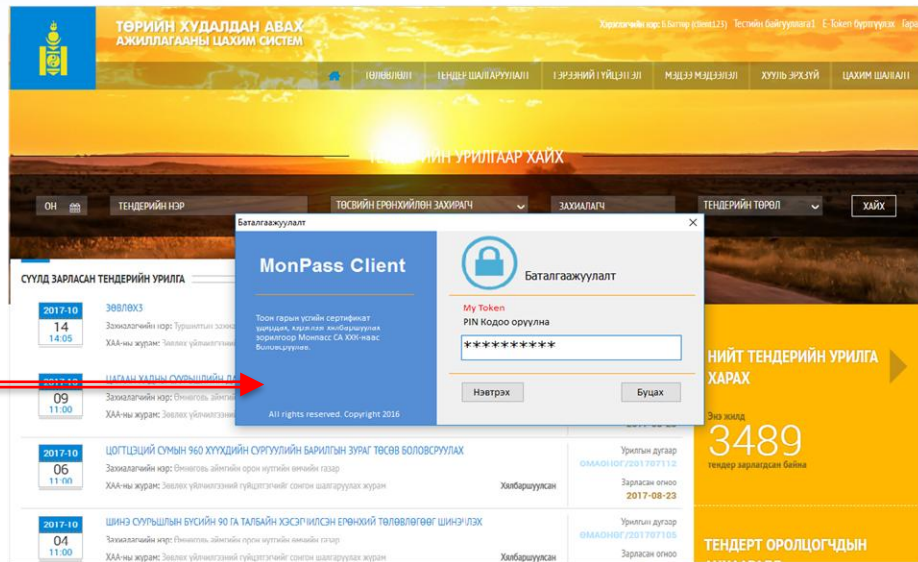
ШИЙДЭЛ

ТООН ГАРЫН ҮСГИЙН ГЭРЧИЛГЭЭГ ЦАХИМ СИСТЕМД БҮРТГҮҮЛЭХ ЖИШЭЭ



Цахим хуудасны хэсэгт тоон гарын үсэг
бүртгүүлэх гэсэн функц нэмэгдэнэ

Е-Token Бүртгүүлэх товч дарсны
дараа компьютерт залгасан э-
токений ПИН кодыг оруулна

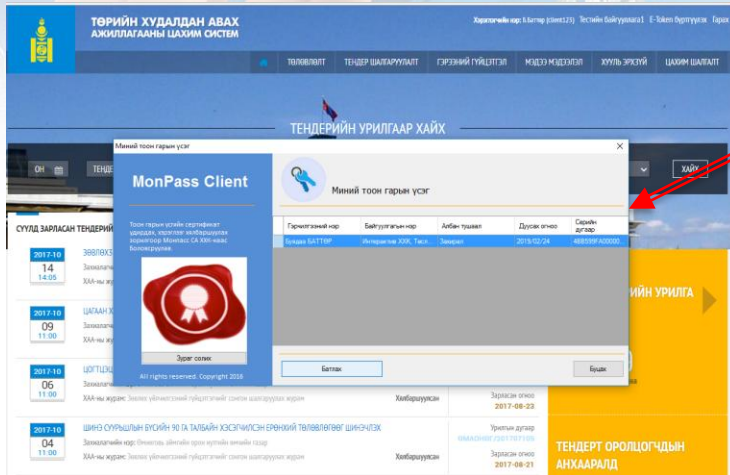


ТООН ГАРЫН ҮСГИЙН ГЭРЧИЛГЭЭГ ЦАХИМ СИСТЕМД БҮРТГҮҮЛЭХ ЖИШЭЭ (үргэлжлэл)



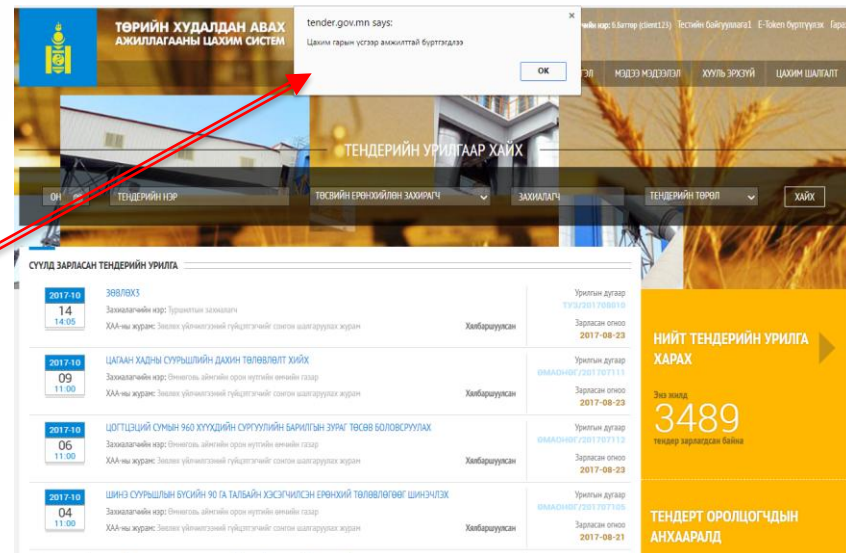
Токенд бичигдсэн тоон гарын үсгүүдээс цахим системд бүртгүүлэх тоон гарын үсгийг сонгоно

3



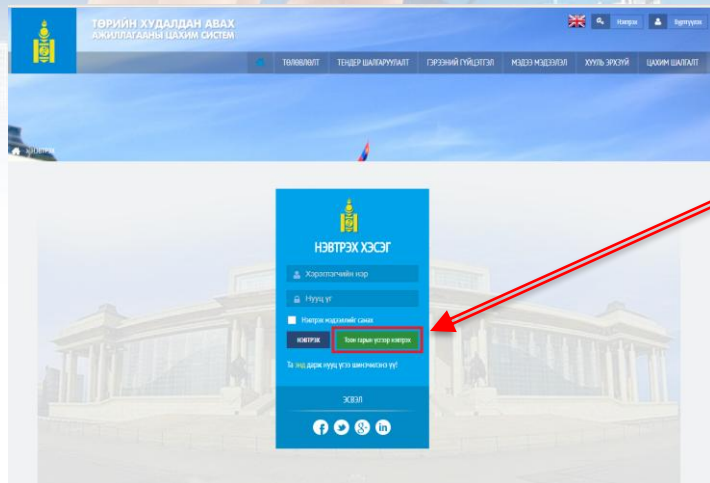
4

Бүртгүүлэх тоон гарын үсэг хүчинтэй мөн зохих мэдээлэл таарч байгаа тохиолдолд амжилттай хадгална



ТООН ГАРЫН ҮСЭГ АШИГЛАН СИСТЕМД НЭВТРЭХ ЖИШЭЭ

Тогтвортой Бизнесийн
MONPASS CA

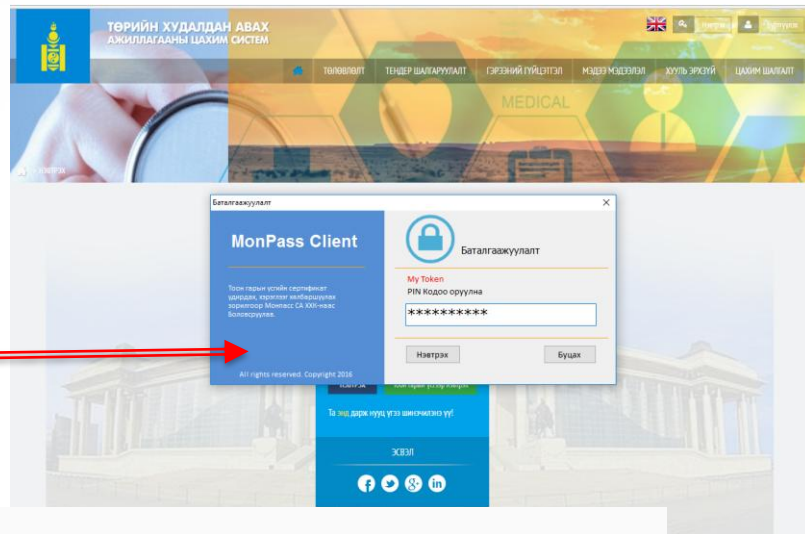


Тоон гарын үсгээр нэвтрэх гэсэн товчийг
цахим хуудсанд байршуулна

1

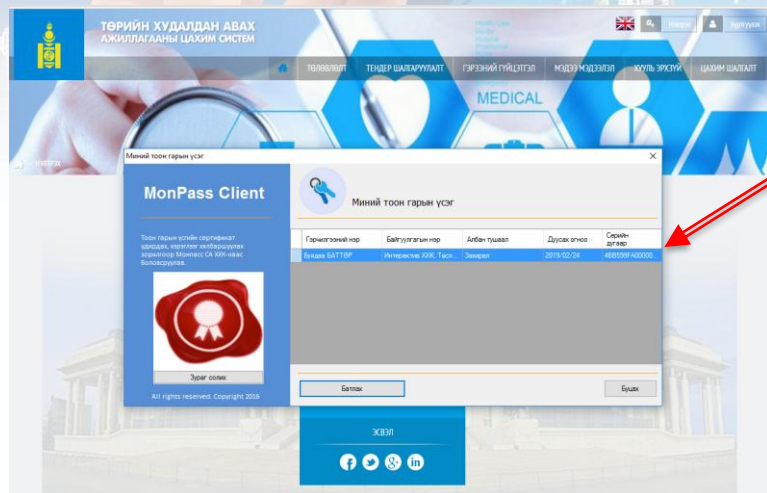
Компьютерт залгасан э-токений
ПИН кодыг оруулна

2

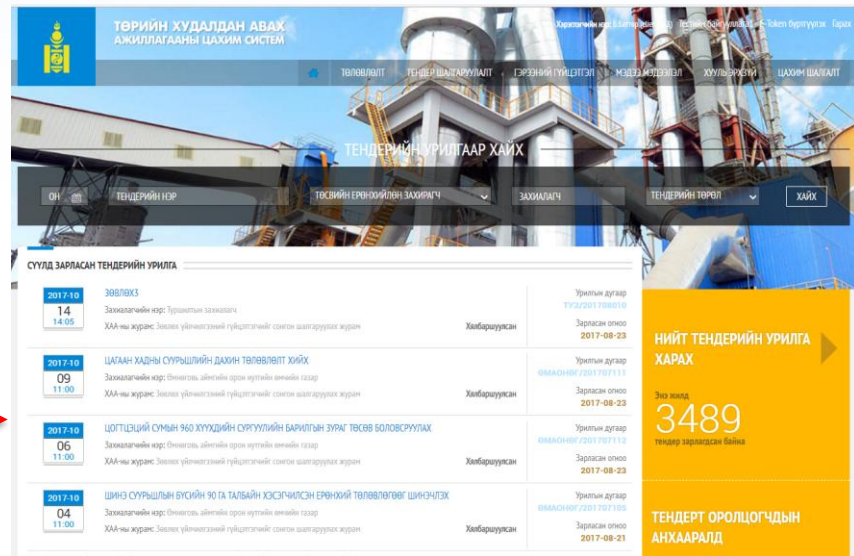


ТООН ГАРЫН ҮСЭГ АШИГЛАН СИСТЕМД НЭВТРЭХ ЖИШЭЭ

Тогтвортой Бизнесийн
MONPASS CA



Цахим системд нэвтрэх тоон гарын үсгийг сонгоно



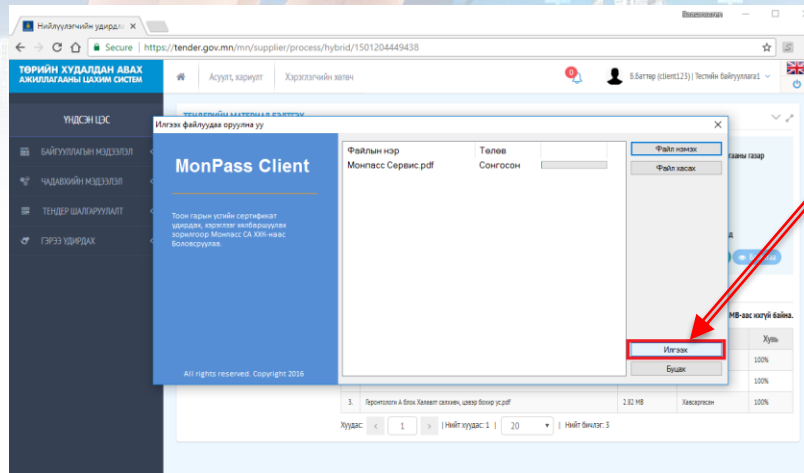
Сонгосон тоон гарын үсэг хүчинтэй бол системд амжилттай нэвтрэнэ



2

Файл нэмэх товчийг дарж илгээх баримт бичгээ сонгоно.

БАРИМТ МАТЕРИАЛЫГ ТООН ГАРЫН ҮСГЭЭР БАТАЛГААЖУУЛАН ИЛГЭЭХ ЖИШЭЭ

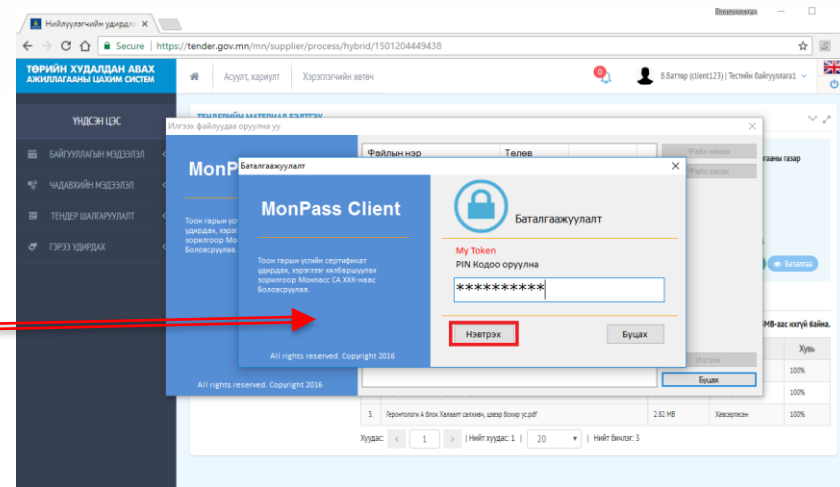


3

Материалуудаа оруулж дуусаад илгээх товч дарна.

4

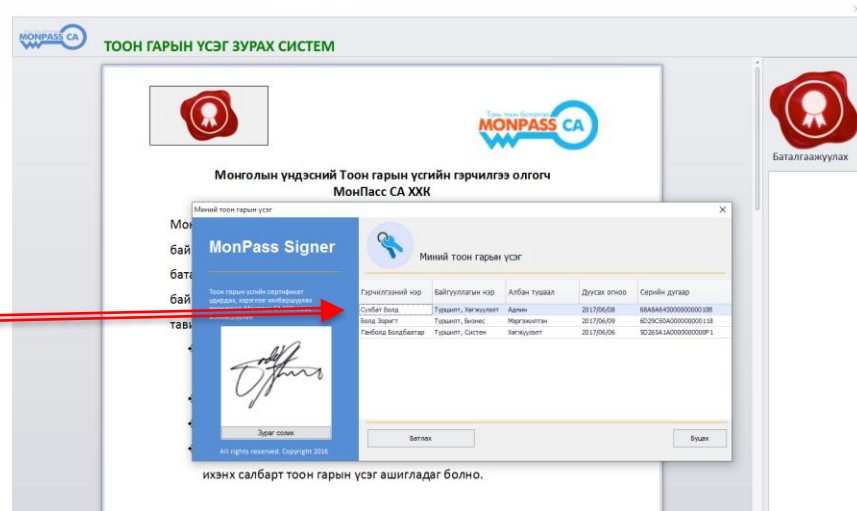
Илгээх товчийг дарахад э-Токен төхөөрөмжийн нууц үгийг асууна. Нууц үгээ оруулаад нэвтрэх товчийг дарсанаар файлд гарын үсэг зурагдан,шифрлээд илгээнэ.





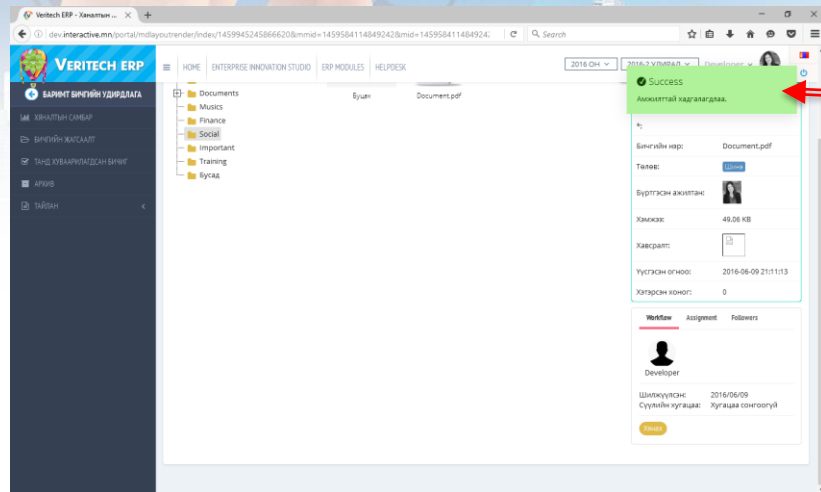
2

Тухайн баримт бичиг нээгдэж гарын
үсэг зурах тоон гарын үсгийг сонгоно



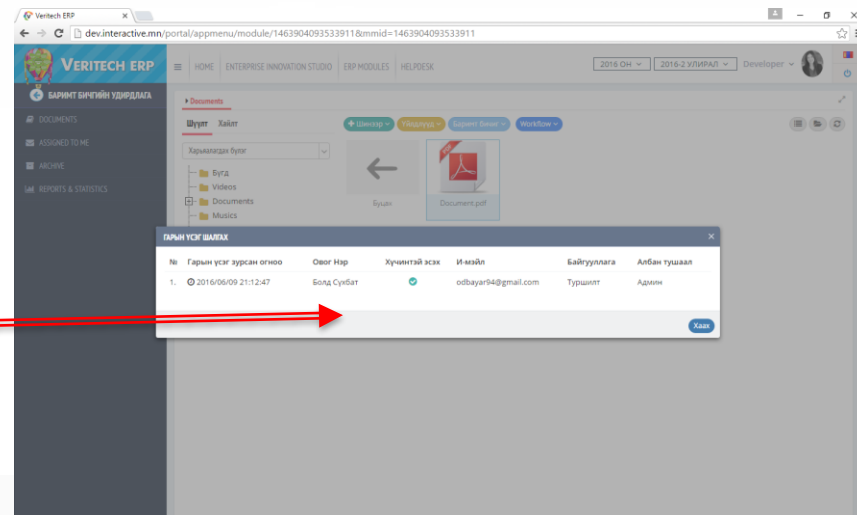
БАРИМТ БИЧИГТ ТООН ГАРЫН ҮСЭГ ЗУРАХ ЖИШЭЭ

МОНПАСС CA



Тоон гарын үсэг зурах алхам амжилттай болсон үед баримт бичгийг хадгалана

Гарын үсэг зурагдсан баримт бичгийг баталгаажуулахад баталгаатай баримт бичиг дараах байдлаар харагдана



Тоон гарын үсэг бүхий цаасгүй офис





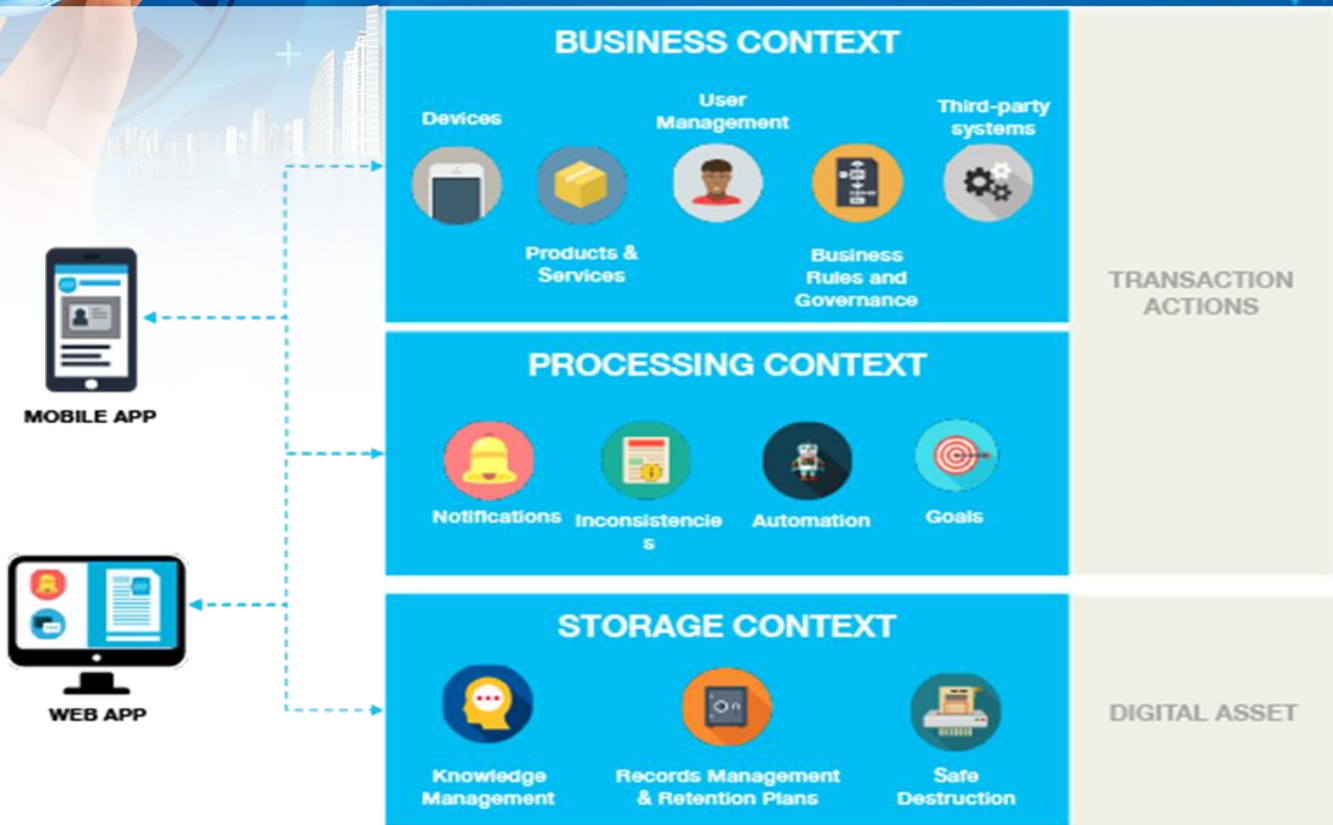
Цаасгүй албан хэрэг хөтлөлт

МОНПАСС

CA

- Гаднаас тоон гарын үсэгтэй цахим албан бичиг, баримт материал хүлээн авдаг.
- Зөвхөн гарцаагүй шаардлагатай баримт материалаас бусдыг цаасан дээр хэвлэх шаардлагагүй.
- Нийт баримт бичгийн 90% нь цахим хэлбэртэй.
- Цахим архивт бүрэн шилжсэн
- Цаг хугацаа, хөрөнгө мөнгө, орон тооны ихээхэн хэмнэлт, өндөр бүтээмж.
- Хялбар хайх, амархан үзэх, өөрчлөх, дамжуулах, хадгалах
- Автоматаар нэрлэх, индекслэх
- Дэлхийн аль ч өнцгөөс гарын үсэг зурах боломж
- Аюулгүй хандах, бүртгэх, нягтлан шалгах
- Аюулгүйгээр дундаа хамтран ашиглах, солилцох
- Энгийн хялбар бизнес процесс
- Орчиндоо ээлтэй, ногоон технологи
- Өндөр түвшний аюулгүй байдал
- Хэрэглэгчийн өндөр сэтгэл ханамж

Цаасгүй албан хэрэг хөтлөлтийн урсгал





Дэлхийн шилдэг туршлагууд

МОНPASS

CA

- Энэтхэгийн Засгийн Газар – Орлогын албан татварын газар бүрэн цаасгүй офис болон хувирсан.
- Саудын Арабын Хөдөлмөрийн яам бүрэн цахим яам болсон.
- Эстоны Засгийн Газар: “Government as Service” загвар бүрэн цаасгүй.
- Сингапурын дээд шүүх 2000 онд дэлхийн анхны иргэний шүүхийн цахим хянан хэлэлцэх ажиллагааг нэвтрүүлж цаасгүй офист бүрэн шилжсэн.



Энэтхэгийн шилдэг туршлагууд

MONPASS

CA

- Энэтхэгийн Засгийн Газар иргэн бүрийг Aadhaar ID буюу тоон гарын үсэгтэй болгох шийдвэр гаргасан.
- Үйлчилгээ үзүүлдэг байгууллагууд нь Aadhaar ID-аар гарын үсэг зурах боломжуудыг бий болгодог.
- Яам, агентлагууд бүгд НТДБ-ийн тоон гарын үсэгт суурилсан цаасгүй үйлчилгээ, цаасгүй үйл ажиллагаатай болсон.
- Орлогын албан татварын газар татвараа тоон гарын үсгээр баталгаажуулан хүлээн авдаг болсон.



Энэтхэгийн шилдэг туршлагууд

МОНPASS

CA

Төрийн ихэнх э-офисийн системүүдэд тоон гарын үсгийн боломжийг нээж өгсөн. Цаашид улам бүр эрчимтэй нэмэгдсээр байна. Тухайлбал:

- Нийгмийн халамж, тэтгэвэр, тээврийн хэрэгсэл, жолооны үнэмлэх, улсын бүртгэл г.м
- Газар эзэмшлийн гэрчилгээ олгох гэх мэт газар эзэмшихтэй холбоотой үйлчилгээнүүдэд
- Эрүүл мэндийн салбарт – Өвчтөний бүртгэл, жирэмсэн эмэгтэй болон шинээр мэндэлсэн хүүхдийн бүртгэл зэрэг олон үйлчилгээндээ НТДБ-д суурилсан цаасгүй технологийг нэвтрүүлсэн.
- Боловсролын салбарт – Сургалтын тэтгэлэг, буцалтгүй тусламж хүсэх гэх мэт төрөл бүрийн хүсэлт, өргөдөл гомдол, тайланг тоон гарын үсгээр баталгаажуулж хүлээн авдаг.
- Даатгал болон банк санхүүгийн салбарт маш өргөнөөр хэрэглэгддэг.
- Үндэсний нийт орлогын 4-6 хувийг хэмнэж чаддаг болсон

- Certification Authority – Гэрчилгээ олгох байгууллага, Registration Authority – Бүртгэлийн байгууллагын иж бүрэн систем
- Signature Creation Application (SCA) - Өгөгдөл/файлд тоон гарын үсэг зурсан файл үүсгэх програм
- Document formatting - баримт бичгийг хэвжүүлэх
- Document visualization - баримт бичгийг дүрслэх
- Creation of - Advanced Electronic Signature-д нийцсэн тоон гарын үсэг зурсан бичиг баримт үүсгэх XML Advanced Electronic Signatures, PDF Advanced Electronic Signatures, JSON Advanced Electronic Signatures
- Cryptographic Message Syntax (CMS) Advanced Electronic Signatures - CMS форматаар өгөгдлийг шифрлэх
- ASiC (Associated Signature Containers) - Файлыг нэг буюу хэд хэдэн тоон гарын үсэг аль эсвэл цагийн тэмдэглэгээ бүхий нэг дижитал контейнерт холбохын тулд контейнерийн бүтцийг ашиглах
- Signing Server Application (SSA) - Гарын үсэг зурах сервер дээрхи програм
- Remote server signing application - Зайнаас гарын үсэг зурах серверийн програм
- Signing credential management - Гарын үсэг зурах итгэмжлэлийн удирдлага
- Remote Qualified Signature/Seal Creation Device (rQSCD) - Зайнаас тоон гарын үсэг/цахим тамга үүсгэх төхөөрөмж
- Signature Activation Module (SAM) - Тоон гарын үсгийг идэвхжүүлэх модуль
- Hardware Security Module (HSM) – Хувийн түлхүүрийг найдвартай хадгалах техник хангамжийн аюулгүй байдлын модуль г.м

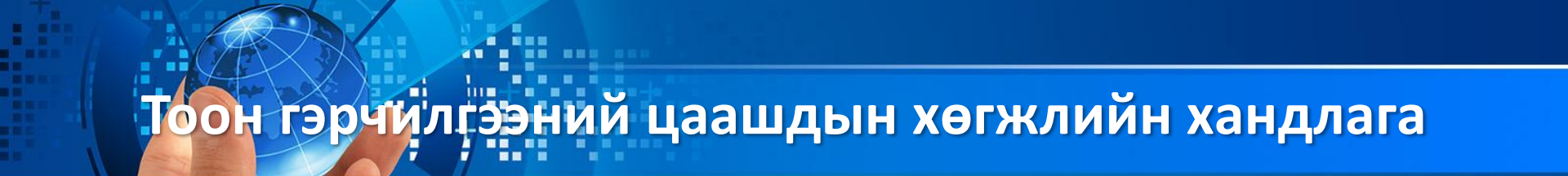


Бусад тоон гэрчилгээ

МОНГОЛЫН ЭРХЭМ
MONPASS CA

1. **SSL/TLS Certificates - SSL/TLS гэрчилгээ:** HTTPS шифрлэлтийг идэвхжүүлэх замаар веб сайттай холбогдож буй холболтыг аюулгүй болгоход ашиглагдана.
2. **Code Signing Certificates – Кодод гарын үсэг зурах гэрчилгээ:** Програм хангамжийн хөгжүүлэгч өөрийн хөгжүүлсэн код, програмд гарын үсэг зурахад ашиглагдана.
3. **Client Certificates – Хэрэглэгчийн гэрчилгээ:** Хэрэглэгчийг таньж батаалгаажуулахад ашиглагдана.
4. **Document Signing Certificates – Баримт бичигт гарын үсэг зурах гэрчилгээ:** Баримт бичиг албан ёсны гарын үсэг зурах, баталгаажуулахад ашиглагдана.
5. **Email Certificates (S/MIME Certificates) – Э-мэйлийн гэрчилгээ:** Эмэйл харилцааг аюулгүй болгоход ашиглагдана.
6. **Host Certificates – Хостын гэрчилгээ:** Төхөөрөмжүүдийн хоорондын холболтыг аюулгүй болгоход ашиглагдана.
7. **Wildcard Certificates - Гэрчилгээ:** Олон төрлийн дэд домэйнд ашиглагдана.
8. **Self-Signed Certificates – Өөрөө зурсан гэрчилгээ:** Тухайн этгээд өөрөө үүсгэж зурсан гэрчилгээ.
9. **Root Certificates – Суурь гэрчилгээ:** Гэрчилгээний шатлалын хамгийн дээр байгаа итгэлтэй гэрчилгээ

Тайлбар: Монгол улсад хэрэглэгчийн, баримт бичигт гарын үсэг зурах, эмэйлийн гэрчилгээг нэгтгэсэн универсаль гэрчилгээ олгож байгаа.



Тоон гэрчилгээний цаашдын хөгжлийн хандлага

1. Цахим тамга, цагийн бүртгэлийг “Цахим гарын үсгийн тухай хуулийн шинэчилсэн найруулга”-д хуульчилсан.
2. Дэлхийд Био тоон гарын үсгийг нэвтрүүлж эхэлсэн.
 - Энэхүү тоон гарын үсэг нь хүний хурууны хээ, нүдний торон бүрхэвч гэх мэт дахин давтагдашгүй био өгөгдөлтэй шууд холбогдсон
 - Тоон гарын үсгээс гадна био өгөгдөлд суурилан баталгаажуулна.
 - Био тоон гарын үсгийг иргэний үнэмлэх, жолооны үнэмлэх, банкны данс, автомашины гэрчилгээ, газар, үл хөдлөх эд хөрөнгө эзэмших гэрчилгээ г.м боломжийн бүх зүйлстэй холбосноор био тоон гарын үсэг бүхий зөвхөн ганцхан зүйлийг ашиглан холбосон бүх зүйлд хандах, үйлдэл хийх боломжтой болсон.
1. Хиймэл оюун ухаанд суурилсан тоон гарын үсгийн систем.
 - Бүртгэлийн байгууллага, нэгжийн систем, хэрэглэгчдэд туслах, лавлагаа өгөх г.м үйл явцыг автоматжуулах

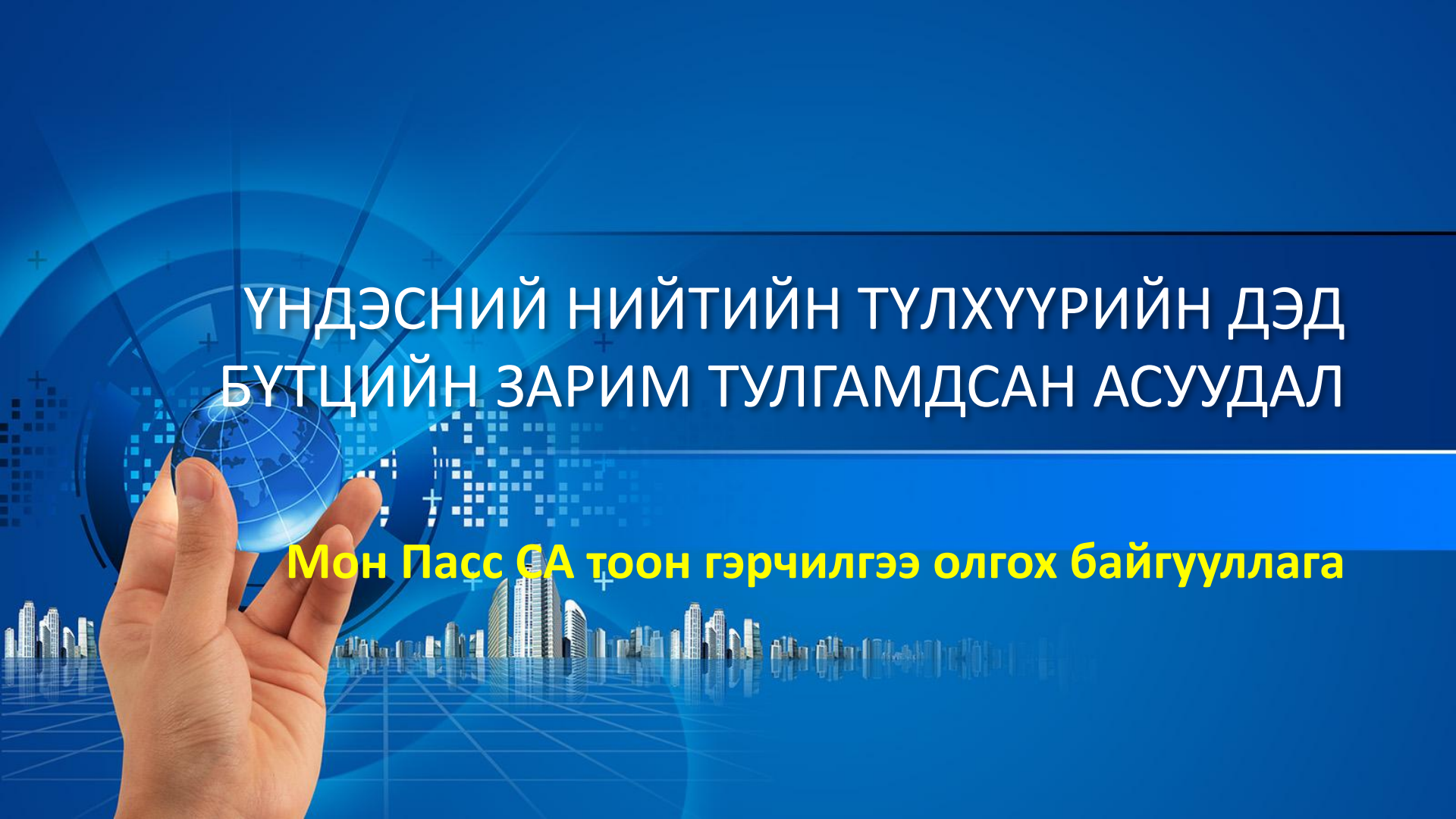
АНХААРАЛ ТАВЬСАНД БАЯРЛАЛАА



info@monpass.mn

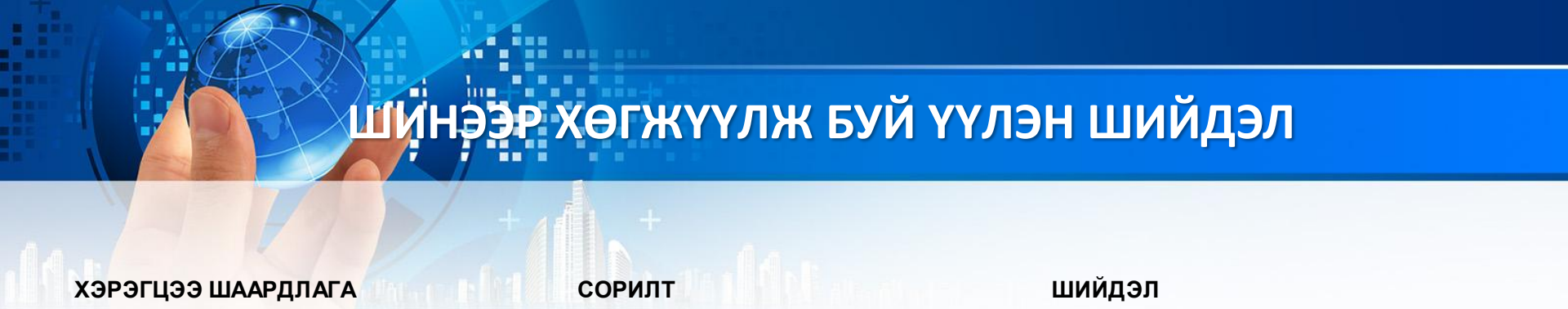
1800-2535

www.monpass.mn

The background is a vibrant blue with a futuristic aesthetic. On the left, a hand holds a glowing blue globe. Behind the globe and text, there are faint, stylized city skylines and a grid of small white squares. The overall composition suggests a global or technological theme.

ҮНДЭСНИЙ НИЙТИЙН ТҮЛХҮҮРИЙН ДЭД БҮТЦИЙН ЗАРИМ ТУЛГАМДСАН АСУУДАЛ

Мон Пасс СА тоон гэрчилгээ олгох байгууллага



ШИНЭЭР ХӨГЖҮҮЛЖ БУЙ ҮҮЛЭН ШИЙДЭЛ

ХЭРЭГЦЭЭ ШААРДЛАГА

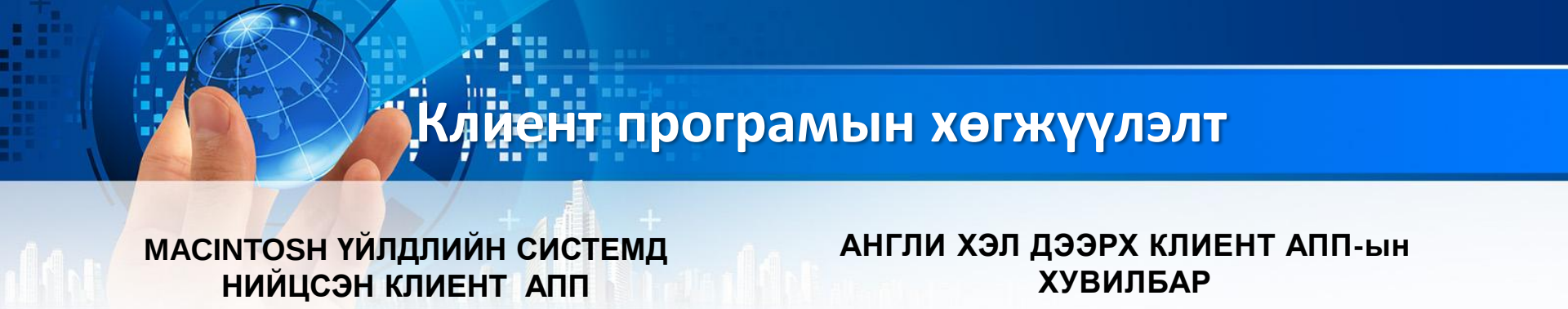
- Монгол улс иргэдээ цахим орчинд хөдөлбөргүй, хялбар, найдвартай **таних**, баталгаажуулах
- **Төрийн** болон **бизнесийн** байгууллагууд цахим шилжилт хийх, **онлайн** үйлчилгээ нэвтрүүлэх
- Үйл ажиллагааны **зардлыг бууруулах**, бүтээмж нэмэгдүүлэх
- **Зайнаас** ажиллах, үйлчилгээ авах боломжийг нийтэд нь бий болгох

СОРИЛТ

- Олон улсын стандартуудыг судлах, стандарт шаардлагад нийцсэн шийдлийг бий болгох
- Гадаадын ижил төстэй системүүдийн судалгааг бүх түвшинд сайтар хийх
- Шийдэл бүрийг шинжлэн дүгнэж уян хатан, найдвартай шийдлийг боловсруулах

ШИЙДЭЛ

- Бид дэлхийн хамгийн нэр хүндтэй, түгээмэл хэрэглэгддэг HSM төхөөрөмжүүдийг ашиглаж байна
- Мөн олон улсын стандарт шаардлага, ижил төстэй системүүдийн судалгааны үндсэн дээр
- Монгол улсын хууль эрхзүйн орчин болон хэрэглэгчдийн зан төлөв зэрэгт тулгуурлан **CLOUD SIGNING** шийдлийг дотооддоо хөгжүүлж байна.
- Тодорхой шалтгааны улмаас түр зогссон байгаа



Клиент програмын хөгжүүлэлт

MACINTOSH ҮЙЛДЛИЙН СИСТЕМД НИЙЦСЭН КЛИЕНТ АПП

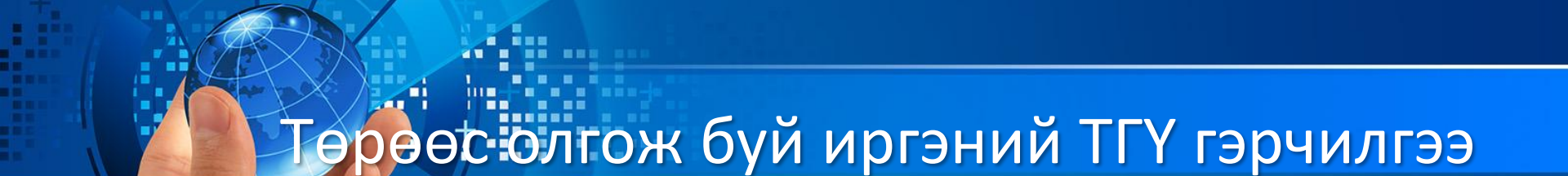
- Мас үйлдлийн системд ажилладаг клиент хувилбарыг хөгжүүлсэн.
- Худалдан авах ажиллагааны системд интеграци хийж нэвтрүүлэх оролдлого хийсэн боловч тэдний одоо байгаа систем нь 128 битийн шифрлэлт дэмждэг, манай хөгжүүлсэн клиент аппын хувилбар нь 258 битийн шифрлэлт дэмждэг учир зогсонги байдалд орсон байна.
- ХААГ-ын системийг даруй 256 битийн шифрлэлт дэмждэг болгон сайжруулах шаардлага тулгараад байгаа. Энэ талаар ЦХИХХЯ-наас ХААГ-т зохих шаардлага тавьж дэмжиж өгөх талаар анхаарч өгнө үү.

АНГЛИ ХЭЛ ДЭЭРХ КЛИЕНТ АПП-ЫН ХУВИЛБАР

- Клиент програмын англи хэл дээрх хувилбарыг хөгжүүлсэн.
- Үүнийг туршиж дууссаны дараа нийтийн хэрэглээнд гаргана.
- Үүний үр дүнд гадаадаас тендерт оролцож буй байгууллагууд, тэдний албан тушаалтнууд клиент програмыг хялбар, төвөггүй ашиглах боломж нээгдэнэ.
- Цаашид үндэсний хэмжээнд бүх гэрчилгээ олгох байгууллагын олгож буй гэрчилгээ, тээгч төхөөрөмжтэй (токен) уялдан ажилладаг нэгдмэл клиент програм, аппыг хөгжүүлэх шаардлага харагдаж байна.



**МОНГОЛ УЛСЫН ҮНДЭСНИЙ НИЙТИЙН ТҮЛХҮҮРИЙН ДЭД
БҮТЦИЙН ЦААШДЫН ХӨГЖИЛД ТУЛГАМДАЖ БУЙ ЗАРИМ
АСУУДАЛ**



Төрөөс олгож буй иргэний ТГҮ гэрчилгээ

- Төр өөрөө иргэдэд 5 жилийн хугацаатай ҮНЭГҮЙ тоон гарын үсэг олгож байгаа нь РКI-Нийтийн түлхүүрийн дэд бүтцийн үндсэн зорилго, зорилт, зориулалтаас гажиж байгаа.
- Х509 стандарт удирдамжид **“Гэрчилгээ олгогч байгууллага нь үйлчилгээ үзүүлэгч болон үйлчлүүлэгчээс хараат бус, бие даасан хөндлөнгийн байгууллага байна”** гэж заасан. Тиймээс гэрчилгээ олгогч байгууллага тусгай зөвшөөрлийн үндсэн дээр ажилладаг.
- Гэтэл үйлчилгээ үзүүлэгч төр, өөрийн харъяа байгууллага болох Бүртгэлийн Ерөнхий Газар иргэдэд гэрчилгээ олгож байгаа нь үүнтэй бүрэн зөрчилдөж байна.
- Үүний улмаас төрийн аль нэг албан хаагч иргэний ТГҮ-ийн гэрчилгээний ашиглалтад нөлөөлөх, оролцох, хувийн түлхүүрийг сөрөг зорилгоор ашиглах, иргэдийн эрх, эрх чөлөөг зөрчих, хэлмэгдүүлэх эрсдэл үүссэн.
- ГОБ-ууд дампуурах эрсдэл нүүрлэсэн.

Үндэсний ТГҮ-ийн гэрчилгээг дэлхийд хүлээн зөвшөөрүүлэх

- Үндэсний Root CA cross certification (харилцан баталгаажуулалт) хийгээгүй, үүний улмаас Монгол улсад олгосон тоон гарын үсгийн гэрчилгээ аливаа хэрэглээнд итгэлгүй, найдваргүй гэрчилгээ гэж харагддаг.
- Үүний улмаас ГОБ-дад байнгын дарамт, гомдол ирдэг, үл итгэх байдалыг үүсгэдэг
- Цаашид Монгол улсад олгосон тоон гарын үсгийн болон бусад тоон гэрчилгээг ашиглаж төрөл бүрийн цахим харилцаа хөгжүүлэхийг боон хаагдуулж байгаа.
- Үндэсний НТДБ-ийн олгосон гэрчилгээг ашиглах боломж эрс буурч, гадаад улсад ашиглах боломжгүй байна.
- Улмаар ГОБ-ууд дампуурах эрсдэл ч тулгарч болохоор байна.



Үндэсний гэрчилгээг бүртгүүлэх

- Олон улсад cross certification хийгдээгүй учир төрөл бүрийн програм хангамж, веб хөтөч, апп-уудад үндэсний гэрчилгээг бүртгүүлэх боломжгүй байгаа.
- Төрөл бүрийн хэрэглээний програм, апп, веб сайтад үндэсний гэрчилгээ ашиглах боломжгүй, аюултай найдваргүй мэтээр харагдах, үндэсний ТГҮГ-г үл хүлээн зөвшөөрөх, улмаар хэрэглэгчийн сэтгэл ханамж байхгүй болох, ГОБ-ууд дампуурах эрсдэлүүд тулгарч байгаа
- Үүний тулд Үндэсний суурь гэрчилгээжүүлэх байгууллага дэлхийн бусад гэрчилгээжүүлэх байгууллагатай харилцан баталгаажуулалт хийж бие биенийхээ гэрчилгээ хүлээн зөвшөөрөх шаардагатай.
- MS, Adobe, Google, Oracle, Salesforce, SAP, IBM г.м хөгжүүлэгчид, Chrome, Edge, Mozilla, Yandex, Opera, Safari г.м интернет хөтчүүдэд үндэсний тоон гэрчилгээг бүртгүүлэх



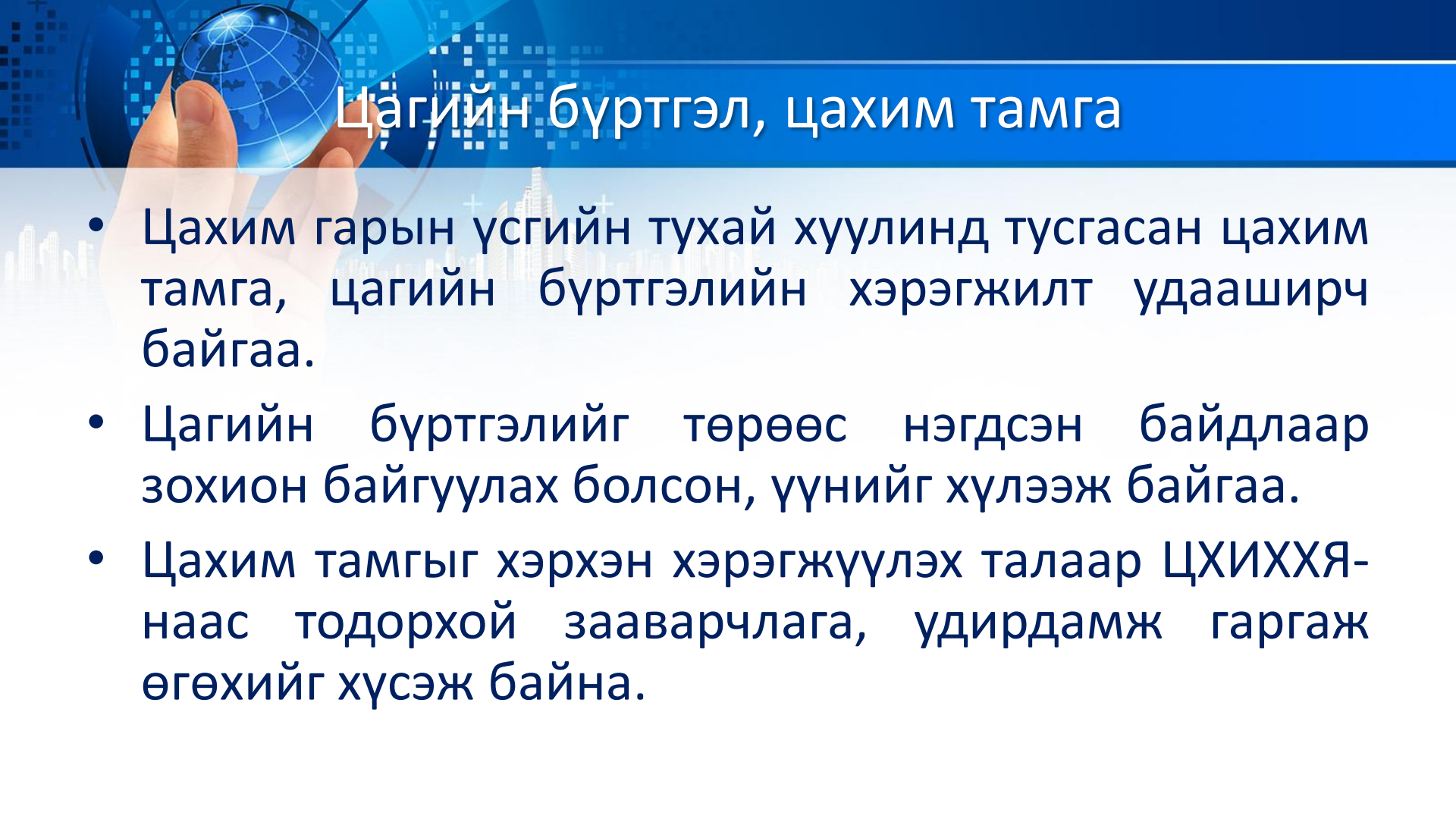
Гэрчилгээний бодлого алдагдаж байгаа

- ГОБ-ууд болон УБЕГ-ын олгож буй гэрчилгээг хэрхэн, юунд ашиглах бодлого алдагдсан, иргэний гэрчилгээг албан тушаал, ажил үүрэгтэй холбоотой байдлаар ашигладаг, албан тушаал ажилтай холбоотой гэрчилгээг иргэний хувийн харилцаанд ашигладаг болсон.
- Энэ нь тоон гарын үсгийн гэрчилгээг бодлого, зориулалтын дагуу ашиглах замаар сүлжээн дахь итгэлцлийг хангах олон улсын шаардлага, зарчмыг алдагдуулсан.
- Улмаар үндэсний НТДБ-д олон улсад итгэхгүй, найдваргүй гэж үзэхэд хүргэнэ.



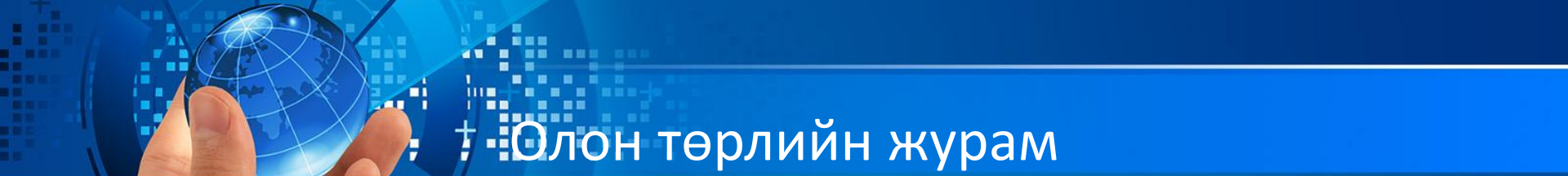
Цахим албан хэрэг хөтлөлт

- Цахим албан хэрэг хөтлөлт хөгжихгүй байгаагийн улмаас тоон гарын үсгийн гэрчилгээний хэрэглээ нэмэгдэхгүй байгаа.
- Зөвхөн дарга, захирал, зарим менежер, ня-бо ТГҮГ авч зарим системд ашигладаг байдлаар олон жил явж байгаа, алба хаагч, ажилтанууд ТГҮГ огт авдаггүй.
- Цахим албан хэрэг хөтлөлтөд төр, бизнесийн байгууллагууд шилжиж, жинхэнэ дижитал шилжилтийг нэвтрүүлж эхэлсэн тохиолдолд л нийтээрээ тоон гарын үсгийн гэрчилгээ, бусад тоон гэрчилгээ ашигладаг болно.



Цагийн бүртгэл, цахим тамга

- Цахим гарын үсгийн тухай хуулинд тусгасан цахим тамга, цагийн бүртгэлийн хэрэгжилт удааширч байгаа.
- Цагийн бүртгэлийг төрөөс нэгдсэн байдлаар зохион байгуулах болсон, үүнийг хүлээж байгаа.
- Цахим тамгыг хэрхэн хэрэгжүүлэх талаар ЦХИХХЯ-наас тодорхой зааварчлага, удирдамж гаргаж өгөхийг хүсэж байна.



Олон төрлийн журам

- Цахим гарын үсгийн тухай хуулийн шинэчилсэн найруулга батлагдсантай холбоотойгоор олон журам гаргахаар төлөвлөсөн.
- Гэтэл журмаар зохицуулах гээд байгаа ихэнх асуудал нь олон улсын стандарттай (rfc), дэлхий даяар адил мөрдөж явдаг
- Тиймээс нэгэнт стандартаар зохицуулдаг асуудлыг олон журмаар зохицуулах оролдлого нь стандартыг зөрчих, түүнээс гажуудах, хүнд суртал үүсгэх, авилгын нэг үндэслэл болох, ГОБ болон хэрэглэгчдийг төөрөгдүүлэх уршигтай.
- ГОБ-ууд өөрийн CP/CPS буюу гэрчилгээний бодлого, гэрчилгээжүүлэх ажиллагааны журмаа гаргаж мөрддөг атал нэмж ийм олон журам гаргах нь маш их хүндрэл дагуулна.

АНХААРАЛ ТАВЬСАНД БАЯРЛАЛАА



info@monpass.mn

70002882, 1800-2535

www.monpass.mn



Т.ХАЛТАР

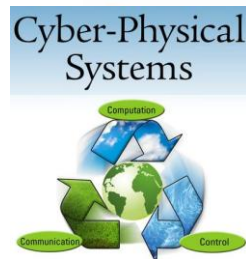
Монголын кибер довтолгоотой
тэмцэх төвийн тэргүүн, Доктор,
профессор

- Тахографын хэрэглээ, орчин үед, техникийн шийдэл ашиглалт, эрх зүйн орчин
- Системүүдийн мэдээллийн аюулгүй байдлын нөхцөл байдал, эмзэг байдал ба дотооддоо гарч байсан кейсүүд хамгаалалтын арга техник, урьдчилан сэргийлэх асуудлууд

ДИЖИТАЛ ШИЛЖИЛТИЙН ЭРИНИЙ МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДАЛ

Тогтууны Халтар
Профессор

Security



Веб хамтын ажиллагааны хэрэгсэл, Ажлын байрны дэд бүтэц, агуулгын удирдлага, Зөөврийн технологи

ТОВЧХОН

Мэдээллийн Технологийн 3 дахь эрин үеийг тодорхойлж буй 4 том хүчин зүйл бидний амьдралд асар олон боломжийг олгож байна

- **Cloud** буюу Үүлэн тооцоолол,
- **Big Data** буюу геометр прогрессоор өсөн нэмэгдэж буй үлэмж хэмжээний тоон мэдээлэл,
- **Social** буюу Нийгмийн сүлжээ,
- **Mobility** буюу хөдөлгөөнт төхөөрөмж, ухаалаг гар утасны өргөн хэрэглээ
- Хармсалтай нь сайн юманд саар дагалддаг жамаар төрөл бүрийн кибер халдлага, тагнан турших ажиллагаа, будлиан зөрчил ихэссэн
- **AI**-Хиймэл оюун ухаан – ХОУ. ХОУ-ныг сайн сайхны төлөө ашиглахтай зэрэгцэн кибер халдлага үйлдэх, хортой үйлдэл хийхэд ашиглах болсон



Халдлагын чиг хандлага

- 2017 онд кибер халдлагын тоо өмнөх онтой харьцуулахад 38%-аар өссөн
- Нийт кибер халдлагын 38% нь хэдхэн секундын дотор, 60% нь хэдхэн минутын дотор компанийн мэдээллийн системд нэвтэрч, 28% нь систем дэх бүх өгөгдлийг ердөө хэдхэн минутад бүрэн хулгайлан авч байна
- Кибер халдлагад өртсөн байгууллагын 58 % нь халдлагад өртсөнөө хэдэн долоо хоногоос хэдэн сар, улирал дамнан мэдээгүй байдаг
- Монголд ихэнх байгууллага өөрсдийн мэдээллийн бүрэн бүтэн байдал, нууцлагыг хянаж чаддаггүй, гадагш алдагдаж урсаж байгаа эсэхийг огт мэддэггүй.



Шинэ орчин дахь Мэдээллийн Аюулгүй байдлын ач холбогдол

- МХТ-ийн хувьсал нийгмийн орчинд ихээхэн өөрчлөлт авчирсан.
- МХТ-ийн эрчимтэй хөгжлийг дагаад олон эрсдлүүд үүссэн.
- Хоорондоо холбогдсон сүлжээ, систем, боловсруулж солилцож буй өгөгдлийг хамгаалах хамгаалалт, арга хэмжээ хэрэгжүүлэхээс өөр аргагүй болсон.
- Мэдээллийн Аюулгүй Байдлыг (МАБ) технологийн үйл явцын салшгүй нэг хэсэг гэж үзэхээс өөр аргагүй болсон.
- Дижитал итгэлцэл, аюулгүй байдлын орчин үүсгэх шаардлага тулгарсан.
- МАБ-ыг (кибер АБ) МХТ ашигласан эд хөрөнгө, дэд бүтцийг хамгаалах замаар дижитал итгэлцлийн орчин үүсгэхэд чиглэгдсэн бодлого, удирдамж, хэрэгслүүдийн багц хэмээн шинэчлэн тодорхойлж болохоор боллоо.

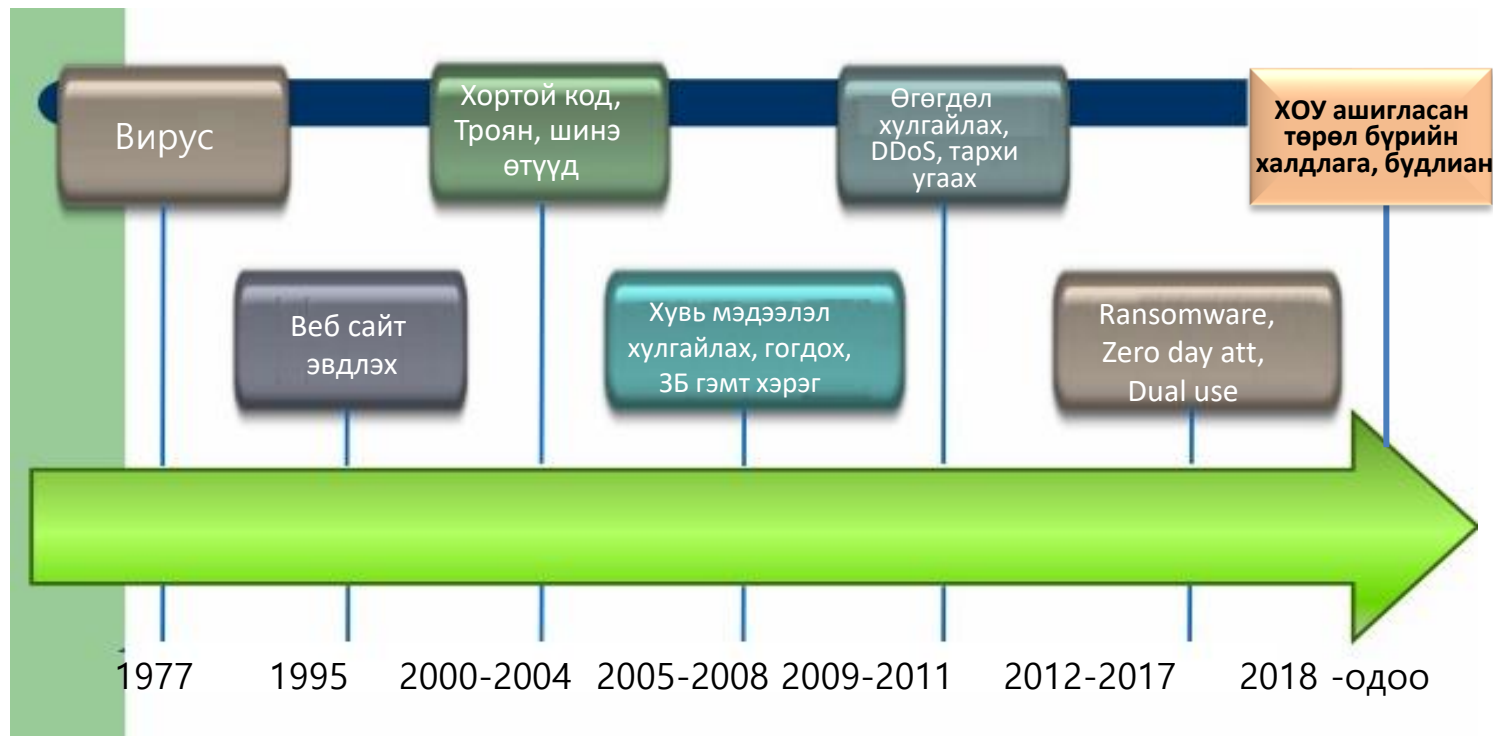
Мэдээллийн Аюулгүй байдал (МАБ) болон Кибер аюулгүй байдал (КАБ)

- КАБ, МАБ аль аль нь ижил чиглэлтэй боловч хамрах хүрээ, зорилгоороо ялгагддаг.
- КАБ нь систем, сүлжээ, өгөгдөлийн аюулгүй байдлыг хангах, цахим өгөгдлийг хамгаалахад чиглэгдсэн, ихэнхдээ техникийн шинжтэй арга хэмжээ. Өмнө нь сүлжээ, системийн аюулгүй байдал
- МАБ нь илүү өргөн хүрээтэй, удирдлага, хүний нөөц, зохион байгуулалт, бодлого, журам, цаасан болон цахим өгөгдөлийн аюулгүй байдлыг хангахад чиглэсэн арга хэмжээ.
- Үндсэн ялгаа:
 - Хамрах хүрээгээрээ
 - Аюул, эрсдэлийн төрөлөөрөө
 - Технологи, хяналт, удирдлагаараа
 - Мэргэжлийн чиг үүрэг, ролиор

Шинэ аюул, эрсдлүүд

- Хиймэл оюун ухаан ашигласан төрөл бүрийн халдлага, зөрчил, будлиан
- Ransomware – Авилгач (барьцаалагч) програм
- Их өгөгдөл (Big data) дахь том зөрчлүүд, Үүлэн дахь хортой кодууд
- Спам, Фишинг, Нийгмийн боловсруулалт, Ботууд, нууц үг эвдлэх ажиллагаа
- IoT-г хакдах, DDoS, Ботнет, Түлхүүр бүртгэх, Күүки хулгайлах
- Кибер дайн, сонгууль хакердах, Үүлийг хакердах
- Улс төрийн тоглоомыг кибер гэмт хэрэг болгон хувиргах
- Crime-As-A-Service (CaaS) – Гэмт хэрэг үйлчилгээ болон хувирах, Expands хэрэгсэл & үйлчилгээ
- Интернет эд зүйлстэй (IoT) холбоотой шинэ эрсдлүүд
- Нийлүүлэлтийн хэлхээн дахь эмзэг сул байдлууд
- Чухал эд зүйлсийг удирдахад зохицуулалт хүндрэл учруулж эхэлсэн
- Вебэд суурилсан крипто олборлогчид – хортой код, криптовар
- Удирдлагын зүй бус шаардлага
- Вирусыг нуухад дижитал эрхийн удирдлагын системийг (DRM) ашиглах
- OS X системд зориулсан хортой кодууд (Flashback Trojan)
- Хортой код суулгасан техник хангамж
- Мобайл хортой кодууд (454,000 хортой Android апп)
- Хайлтын системийн шүүлтүүрийг хөөсөөр хордуулах
- Аюулын эх үүсвэр болсон шинэ шинэ тоглогчид
- МАБ-ын бодлогогүй, бодлогоо үл тоодог, буруу ашигладаг, тасалдал г.м.

Өөрчлөгдөн хувьсаж буй аюулууд



Security

МАБ-ын аюулын дүр төрхийн хувьс(г)ал

Хохирол USD

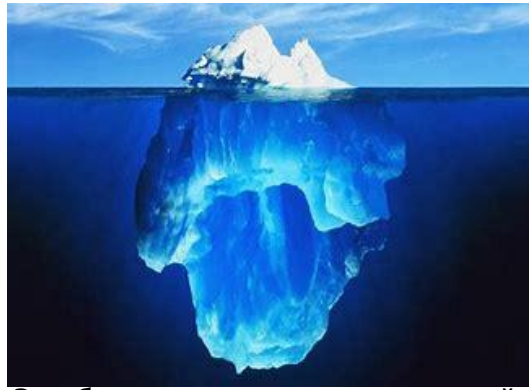
Тэрбум

Сая

Хэдэн зуун
мянга

Мянга

Зуу



Энэ бол мөсөн уулын зөвхөн орой



Вирус, Троян, Өт



Хө
хулгайлах

DDoS, DNS, SQL
халдлага,



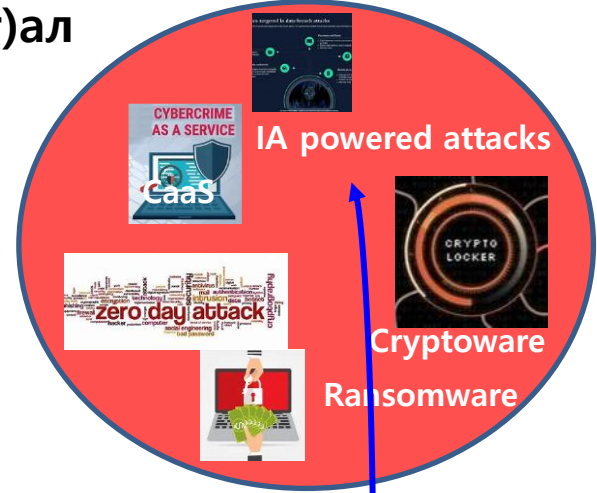
Фишинг,
скам



Ботнет, хортой
Эмэйл, PoS



Чиглэсэн
халдлагууд



IA powered attacks

Cryptoware

Ransomware

Ирээдүй

Шинэ хандлага

- МАБ-ын зохицуулалт сайжирч байна
- Өгөгдлийн хулгай Өгөгдлийг буруугаар удирдах ажиллагаа болж хувирсан
- Аюулгүй байдлын мэдлэг, чадварын шаардлага, хэрэгцээ улам бүр өсөж байна
- Интернет эд зүйлстэй (IoT) холбоотой МАБ-ын асуудлууд үүссэн.
- Халдагчид хэрэглэгчийн төхөөрөмжийг бай болгосон
- Халдагчид илүү зоригтой, овсгоотой, шунахай, үл мөшгөг-дөх шинжтэй болсон.
- Халдагчид илүү ухаантай болж байна.
- Будлиан, зөрчлүүд илүү ярвигтай, их хохиролтой болж байна.
- ХОУ-д суурилж халдлагыг илүү өргөн хүрээтэй, төвөгтэй, бодит болгож хувиргасан
- МАБ-ын шинэ амжилтууд, үүлэн үйлчилгээ нь будлиан зөрчлийг гарахаас нь өмнө илрүүлэх, сэргийлэх боломжийг олгодог болсон (QUALYS)

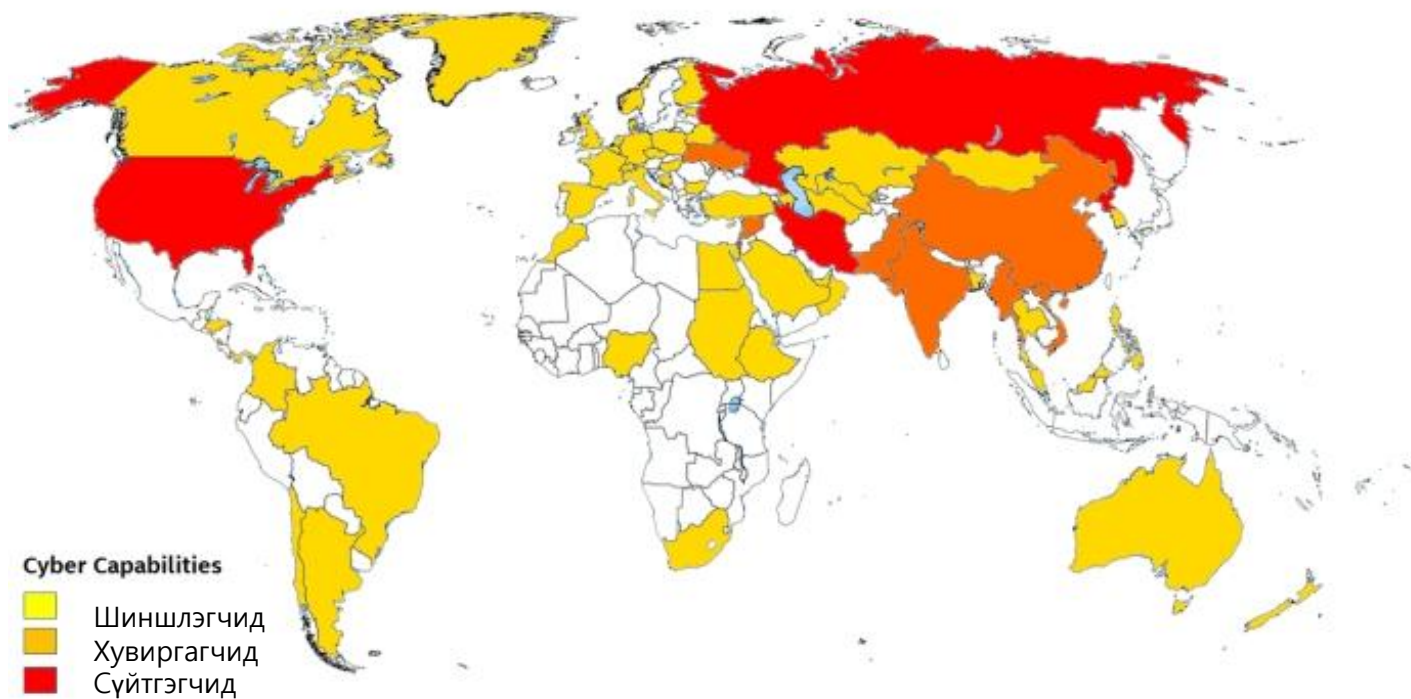
Шинэ хандлага

- ХОУ-д суурилсан халдлагыг илрүүлэх шинэ хэрэгсэл, арга барил боловсруулагдаж байна
- Кибер халдлага, гэмт хэрэгтэй тэмцэх, сэргийлэх ХОУ-ны хэрэгслүүд бий болсон
- МАБ-ын нийцэл, менежментийн тогтолцоо чухал болсон
- Сайжруулсан анализ шинжилгээний үр дүнд өгөгдлийн аюулгүй байдлыг сайжруулах боломжтой болсон
- Өгөгдлийн аюулгүй байдлыг хангахад Blockchain-ийн зарчмыг ашиглаж эхэлсэн
- Биометрик өгөгдөл, тоон гарын үсэг өргөн ашиглах болсон
- Интернет эд зүйлсийн (IoT) аюулгүй байдлыг хангах болсон
- Хиймэл оюун ухааныг (AI) хамгаалалтад ашиглаж эхэлсэн
- Криптовалюттай холбоотой гэмт үйлдлүүдээс хамгаалж эхэлсэн
- Үүлэн тооцооллыг илүү аюулгүй болгох арга хэмжээ
- Квантын технологи ашиглан МАБ-ыг сайжруулах
- Хүний нөөцийг хөгжүүлэхэд онцгой анхаарах болсон, МАБ-ын чиглэл ээр 10 гаруй, Кибер аюулгүй байдлын чиглэлээр 20 орчим мэргэшил

Өнөөдрийн кибер дайн

- Кибер зэвсэг, кибер арми
- Кибер тагналтын арга, технологи, техник хэрэгсэл
- Уламжлалт антивирус, интернет аюулгүй байдлыг програм хангамжууд орчин үеийн байлдааны зориулалттай хортой кодуудын эсрэг юу ч хийж чадахгүй
 - Flame, Stuxnet, DuQu, Stealthy malware
- Artificial Intelligence Powered халдлага, Zero day халдлага, Ransomware хортой код, Advanced Persistent Threat (APT)

Кибер дайны төвүүд



Шинээр үүсэж буй эмзэг байдлууд

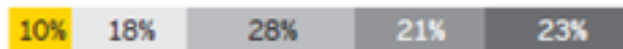
- Монгол Улс МХТ-оос ихээхэн хамааралтай болсон, бүх зүйлээ импортолдогтой холбоотой эмзэг байдлууд
- Болзошгүй кибер халдлагын нөлөөлөл, хор хөнөөл улам бүр ихсэж байгаа
- Аюулгүй байдал технологиос байнга хоцрогддог
- Ирээдүйн халдлагууд илүү хүчтэй, илрүүлэхэд төвөгтэй болж байгаа
- Системүүдийн харилцан хамаарал, холбоо, нарийн төвөгтэй байдалтай холбоотойгоор халдлагын дагуу хариу үйлдэл хийх, арга хэмжээ авахад хүндрэлтэй болж байгаа.
- МАБ-ын мөн чанарыг өнгөц ойлгодог хэвээр.
- Залуу үе нийгмийн сүлжээнд ихээр татагдан орсон.
- Улс төрийн дарамт үзүүлэхэд МХТ ашигладаг болсон
- Улсуудын кибер дайн хийх чадвар асар өндөрссөн.

Монголын нийтлэг эмзэг байдал

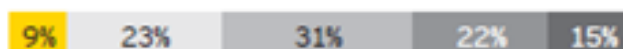
Нийгмийн сүлжээ сайттай холбоотой



Үүлэн тооцоолол ашиглахтай холбоотой



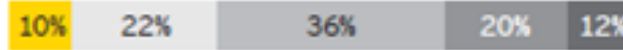
Мобайл үйлчилгээ ашиглахтай холбоотой



МАБ-ын хяналт хэрэгжээгүй, сүлжээ, системийн архитектур хуучирсан



Хандалтын удирдлага сүл



Хайхрамжгүй болгоомжгүй ажилтнууд



Тайлбар: 1 2 3 4 5

- 1: Маш ноцтой болсон
- 2: Ноцтой байна
- 3: Аюултай байна
- 4: Багагүй эрсдэл учруулж байна
- 5: Хүлээн зөвшөөрч болохуйц байна

Монголын төрийн байгууллагуудын нийтлэг эмзэг байдал

- Сүлжээний эмзэг байдлууд
 - Технологи, тоног төхөөрөмж, програмын
 - Тохируулгын
- Системийн эмзэг байдлууд
 - Програмчлал, кодын
 - Арын хаалга
 - Тохируулгын
- Веб системийн эмзэг байдлууд
 - Програмчлал, кодын
 - Тохируулгын
- Бодлого, дэг, журам, хяналт удирлагын эмзэг байдлууд
 - Удирдлага, менежментийн тогтолцоо байхгүй
 - Бодлого, журам, дэг, заавар байхгүй
 - Бодлого, журам байсан ч мөрддөггүй

Security

Security

ТӨРИЙН НЭГЭН БАЙГУУЛЛАГЫН ЭМЗЭГ БАЙДЛЫН БОДИТ ЖИШЭЭ

Систем, Програм хангамжтай холбоотой эмзэг байдлууд	Эмзэг байдлыг ашиглаж болох аюулууд	Тодорхойлсон эрсдлүүд
- Дутуу тестлэгдсэн програм ашиглах магадлал - Аудитын ул мөр дутуу гаргадаг програмууд байдаг. - Програм хангамжийн цох, зохиомжийн алдаа - Хэрэглэгч буруу ашиглах, буруу команд өгөх, буруу орц оруулах - Ашиглахад төвөгтэй програм хангамж (bloatware) - Хэрэглэгчийн интерфейс ойлгомжгүй - SaaS ашиглах (өгөгдлөө хянах боломжгүй болох) - Windows UC, MS office, Mac UC, Adobe програмуудын цоорхойнуудыг хаадаггүй, шинэчлэлийг татаж авдаггүй - ПХ-д зөвшөөрөлгүй өөрчлөлт оруулах - Системд хууль бусаар хандах - Хортой код, програм хангамж - ПХ-ийн ажиллагааны алдаа - ПХ-ийн аюулгүй байдлын алдаа - ПХ санамсаргүй өөрчлөгдөх, устах - Програм хангамжийн хөгжүүлэлтийг бүрэн тодорхойлдоггүй - Програм хангамжийг сайн тестлээгүй - Веб хөтөч, Үйлдлийн систем, офисын ПХ, эмэйл програм дахь хэрэглэгчийн талын эмзэг байдлууд - Веб хэрэглээ, үйлчилгээ, UC, өгөгдлийн сангийн болон серверийн эмзэг байдал - ПХ-ын цох, хортой код оруулж болох цоорхойнууд - Арын хаалга болон компьютеруудад суусан Троянууд - Зайнаас команд гүйцэлдүүлэх эмзэг байдал - Крэкдсэн UC, програмууд ашигладаг, ПХ-ийг зүй бусаар хувилах, суулгах - Системийн ажиллагааны алдаа	ПХ-ын цоорхойг хууль бусаар ашиглах, систем, компьютер, сервер рүү хууль бусаар нэвтрэх Програм хангамжийн эвдрэл, Програм хангамжийг хууль бус, хортойгоор ашиглах, Троян суулгах Logic Bombs, Salami, Virus, worm Attacks, hijacking, Adware, spyware, Ransomware г.м хортой кодууд суулгах ПХ хууль бусаар суулгах, өөрчлөлт оруулах SQL, PHP тарилга, вебийн нүүрийг өөрчлөх Системийн эвдрэл, хэт ачаалал, чадал хүрэлцэхгүй болох Програмын буруу ажиллагаа, алдаа Систем, програмд гаднаас хууль бусаар хандах Үйлчилгээ бусниулах (DoS), DDoS халдлага Тагналт Ботнетийн хохирогч болох (Zombie) Scareware, Keyword Stuffing Хортой кодын халдлага, үймүүлэлт Өгөгдөл, мэдээлэл хулгайлагдах Системийн алдаа, ПХ хууль бусаар суулгах, өөрчлөлт оруулах Zero day халдлага Хортой код ашигласан үймүүлэлт, сахилгагүйтэл	- Програм хангамж ажиллахгүй болох эрсдэл - Өгөгдөл болон мэдээлэл хулгайлах эрсдэл - Кибер террор, дайны хохирогч болох эрсдэл - Гаднаас хууль бусаар хандах, хакердах эрсдэл - Тагнах ажиллагааны хохирогч болох эрсдэл - Зомби болох эрсдэл - Өгөгдлийг шиншлэх, санах ойг шиншлэх эрсдэл - Хортой кодын халдлагад өртөх эрсдэл - ПХ-д хууль бус өөрчлөлт оруулах эрсдэл - Систем унах, хэт ачаалагдах эрсдэл - Цахим вандализм, хорлон сүйтгэх ажиллагааны эрсдэл - Үйлчилгээ бусниулах халдлагын эрсдэл (DoS), DDoS - Өгөгдлийг өөрчлөх, засварлах, хуурамчаар үйлдэх эрсдэл - Өгөгдөл хулгайлах, өгөгдлийн аюулгүй байдал алдагдах - АРТ – Ажилтны компьютерт Троян суулгаж системд халдах - Ransomware – авилгач кодын халдлагад өртөх, өгөгдөл мэдээллээ блоклуулах - Програмын цоорхойг ашиглан (zero day) хакерууд компьютерт нэвтэрч дурын үйлдлээ хийх - Бизнес үйл явц тасалдах

Сүлжээтэй холбоотой эмзэг байдлууд	Эмзэг байдлыг ашиглаж болох аюулууд	Тодорхойлсон эрсдлүүд
1. Хамгаалагдаагүй холболтууд 2. Нээлттэй биет холболт, IP-нүүд болон портууд 3. Сүлжээний сул архитектур 4. SSL, SSH –тэй холбоотой цоорхой 5. Шаардлагагүй ажиллагаа, гүйцэтгэгч скриптүүд 6. WiFi сүлжээтэй холбоотой үүсдэг эмзэг байдлууд 7. Холболт салах, тасрах, дутуу хурдтай байх 8. Шугамыг мөшгөх, сүлжээг нууцаар сонсох, замаас нь барих 9. Сүлжээний удирдлага сул 10. Галт хана үйлдвэрлэгчийн тохируулгатай, өөрсдийн дүрэм бичиж оруулдаггүй, DMZ, анти DDoS байхгүй. 11. Сүлжээний байнгын мониторинг байхгүй. 12. Protocol Address-ийг задлах эмзэг байдал 13. CGI (Common Gateway Interface)-г ашиглах боломж, WebDB Listener эмзэг байдал 14. Алсаас өгч буй дурын тушаалыг гүйцэлдүүлэх эмзэг байдал 15. NFS – network file system, Server Message Block / Netbios, TCP/IP, Windows дахь эмзэг байдлууд 16. Галт хана, рутер, Компьютерууд болон зарим серверийн буруу тохируулга 17. script code injection, SQL injection хэрэгжүүлж болох веб сайтын цоорхой 18. Zero day эмзэг байдал 19. Ransomware эмзэг байдал	IP дууриалгах Кибер террор, дайны халдлага Маскадинг, хууралт / Нийгмийн боловсруулалт, Спам-соёлгүй зар Гадны этгээд хууль бусаар хандах Цахим хорлон сүйтгэх ажиллагаа, сүйтгэл Үйлчилгээ бусниулах (DoS), DDoS халдлага Тагналт Сүлжээнд зөвшөөрөлгүй этгээд холбогдох Нууц мэдээлэл алдагдах <i>Хэрэглэгчийн бүртгэл алдагдах,</i> Үйлчилгээ буруу хийх Хууль бус програм суулгах Бизнес үйл явц тасалдах, зогсох Туслах үйлчилгээ алдагдах Ransomware-ийн халдлага Аж үйлдвэрийн тагналт Үйлчилгээ бусниулах (DoS), DDoS халдлага Холболтын алдаа, урсгалын ачаалал Нууцаар сонсох, замаас нь холбогдох, татаж авах, урсгалын дүн шинжилгээ хийх, Сүлжээнд зөвшөөрөлгүй этгээд холбогдох Сүлжээгээр дамжсан бусад халдлагууд Холболт салах, тасалдах, гэмтэх Засварын алдаа, буруу тохируулга хийх	- Кибер террор, дайны хохирогч болох эрсдэл - Гаднаас хууль бусаар хандах, хакердах эрсдэл - Тагнах ажиллагааны хохирогч болох эрсдэл - Цахим вандализм, хорлон сүйтгэх ажиллагааны эрсдэл - Үйлчилгээ бусниулах халдлагын эрсдэл (DoS), DDoS - Холболт унах, урсгал ихсэх, хэт ачаалагдах эрсдэл - Замаас нь барих, нууцаар сонсох, холбогдох эрсдэл - Трафик урсгалыг шинжлэх, таслан зогсоох эрсдэл - IP хаягийг дууриалгах эрсдэл - Өгөгдлөө задлах, алдах эрсдэл - Үйлчилгээ, засвар алдагдах, буруу болох, буруу тохируулах эрсдэл - Ransomware – авилгач кодын халдлагад өртөх, мэдээлэл шифрлэгдэх - Хортой кодын халдлагад өртөх - Үйлчилгээ бусниулах халдлагын эрсдэл (DoS), DDoS - Бизнес үйл явц тасалдах - Веб сайтын ажиллагаа зогсох - WiFi сүлжээгээр дамжин дотоод сүлжээнд халдах - Сүлжээ тасрах, холболтгүй болох

Техник хангамжтай холбоотой эмзэг байдлууд	Эмзэг байдлыг ашиглаж болох аюулууд	Тодорхойлсон эрсдлүүд
1. Тоос, шороо, температур, чийгэнд мэдрэмтгий 2. Хэт хуучирсан техник ашиглах 3. Техник, төхөөрөмжийн буруу тохируулга 4. Буруу ашиглалтаас үүсэх эмзэг байдлууд 5. Төхөөрөмжийн буруу тохируулгаас үүсэх эмзэг байдлууд 6. Зөвшөөрөлгүйгээр өөрчлөлт оруулснаас үүсэх эмзэг байдал 7. ТХ-ийн ажиллагааны алдаа, саатал 8. ТХ-ийн аюулгүй байдлын алдаа 9. Цахим цацрагаас үүсэх эмзэг байдлууд 10. Гео байршлыг цацдаг төхөөрөмжүүдээс үүсэх эмзэг байдлууд 11. Цахилгааны хэлбэлзэлд тоног төхөөрөмж мэдрэмтгий эмзэг байдал 12. Кабелийн аюулгүй байдал сул 13. Хэт ачааллын эмзэг байдал 14. Зарим төхөөрөмжийн үйлдвэрийн нууц үгийг өөрчилдөггүй	Санаатай, санамсаргүй алдаа, буруу ашиглалт, Тоног төхөөрөмжийн алдаа, бүрэлдэхүүн, өгөгдөл, тоног төхөөрөмжийг устгах Төхөөрөмжийг хууль бусаар ашиглах, систем, компьютер, сервер рүү хууль бусаар нэвтрэх Засварын алдаа, буруу тохируулга хийх Тоног төхөөрөмжийн алдаа, Кибер террор, дайны халдлага Системийн эвдрэл, хэт ачаалал, чадал хүрэлцэхгүй болох Гадны этгээд хууль бусаар хандах Цахим хорлон сүйтгэх ажиллагаа, сүйтгэл Үйлчилгээ бусниулах (DoS), DDoS халдлага Тагналт Ботнетийн хохирогч болох (Zombie) Тоног төхөөрөмж, эд анги, өгөгдөл, мэдээллийн хулгай Бүрдэл хэсэг, өгөгдөл, тоног төхөөрөмжийг устгах	- Үйлчилгээ, засвар алдагдах, буруу болох, буруу тохируулах эрсдэл - Техник хангамж ажиллахгүй болох эрсдэл - Техник хангамж хулгайлах эрсдэл - Хакердуулах эрсдэл - Систем унах, хэт ачаалагдах эрсдэл - Цахим вандализм, хорлон сүйтгэх ажиллагааны эрсдэл - Үйлчилгээ бусниулах халдлагын эрсдэл (DoS), DDoS - Гаднаас хууль бусаар хандах, хакердах - Тагналтын хохирогч болох - Төхөөрөмжүүд зомби болох - Системийн тохируулга өөрчлөх - APT – Ажилтны компьютерт Троян суулгаж системд халдах - Ransomware – авилгач кодын халдлагад өртөх, өгөгдөл мэдээллээ блоклоулах - Бизнес үйл явц тасалдах

Вебийн эмзэг байдал

Д/д	Илэрсэн эмзэг сул байдал, цоорхой	Эмзэг байдлыг ашиглаж болох аюул, халдлага	Эмзэг байдлын түвшин	Нэмэлт мэдээлэл, байршил	Эмзэг байдлыг засах, залруулах зөвлөмж
	Unencrypted connection (verified)	Даяар ажиллах буй энэ системийн хүлээн авч, дамжуулж буй мэдээллийг халдагч замаас нь барьж авах, өгөгдлийг өөрчлөх бүрэн боломжтой. Тухайлбал Data theft – өгөгдөл хулгайлах, Malware – Хортой код оруулах, Evil twin буюу хуурамч Wi-Fi сүлжээ ашиглан ажилтнуудын төхөөрөмж, өгөгдөл хандах. Ажилтнууд өөрт хамаагүй чухал нууц мэдээлэлд хандах, Ажилтнууд Social engineering Халдлагуудад өртөх, ажилтнууд алдаа гаргах эрсдэлүүд үүснэ.	Дунд	https://omnicapital.mn	Өгөгдлийг аюулгүй HTTPS холболт ашиглан илгээж, хүлээн авч байхаар тохируулна. SSL гэрчилгээ суулгах.
	No HTTP Redirection	Автоматаар HTTPS-руу шилжүүлэхгүй байгаа тул URL redirect халдлага үйлдэгдэх боломж бүрдсэн. Үүний улмаас сеансыг hijacking хийх, MITM болон phishing халдлага үйлдэгдэнэ.	дунд	https://omnicapital.mn	HTTP Redirection хийх шилдэг практикийг хэрэгжүүлэх шаардлагатай. – Домэйн хандах HTTP хандалтыг хүчингүй болгоно. – HTTP-ээр хандахгүй байхыг хэрэглэгчид ойлгуулж хориолно.
	Permissions-Policy гэрчилгээ хэрэгжүүлээгүй	Permissions Policy header-гарчиг байхгүй учир хэрэглэгчийн хувийн мэдээлэл алдагдах, камер, микрофоныг нууцаар алсаас ашиглах, байршлыг танлан мэдэх, бүрэн дэлгэцийг зайнаас идэвхжүүлэх эрсдэл үүснэ.	бага	Locations without Permissions-Policy header: http://54.230.71.70/ http://54.230.71.70/9872910	- Хариу өгч буй гарчигтаа Permissions Policy header-гарчиг нэмж өгнө. Энэхүү гарчиг-header-т аюулгүй байдлын бодлогын жагсаалтыг оруулсан байна. - Веб сервер, системийн интерфэйсийг тохируулна. - Мөн Feature Policy болон Feature-Policy Header, Content Security Policy (CSP) зэрэг аюулгүй байдлын бусад механизмыг хэрэгжүүлнэ - хүмүүсээ сургаж байх.

Д/д	Илэрсэн эмзэг сул байдал, цоорхой	Эмзэг байдлыг ашиглаж болох аюул, халдлага	Эмзэг байдлын түвшин	Нэмэлт мэдээлэл	Эмзэг байдлыг засах, залруулах зөвлөмж
	Clickjacking: X-Frame-Options header	Clickjacking (хэрэглэгчийн интерфэйсийг сэргээх замаар үйлддэг халдлага) — хэрэглэгчийг хуурч дарах ёстой зүйлээ дарж байгаа мэтээр хуурч хортой холбоосыг даруулдаг арга. Үүний уршгаар нууц чухал мэдээлэл алдагдах юмуу хэрэглэгчийн төхөөрөмжийн удирдлагыг гэмт этгээд гартаа авна. Сервер DENY юмуу SAMEORIGIN утгатай X-Frame-Options буцаахгүй байгаа учир Clickjacking халдлагад өртөх эрсдэл үүссэн. Дараах аргууд үүсгэж байна: - Хууль бусаар хандах - Өгөгдөл хулгайлах - Хортой код татах - Хортой веб хуудсанд хандах - Хувийн & нууц мэдээлэл гаргах - Мөнгөө алдах - Нэр төр алдагдах	<i>Өндөр</i>	secure XFO header - гарчиг байхгүй замнууд: http://167.86.111.224/	Веб сервер, системийн интерфэйсийг X-Frame-Options гарчигтай, уг гарчигт frame-ancestors directive орсон байхаар тохируулна. Интернетээс илүү мэдээлэл үзнэ үү. - Урсан гарч ирж буй pop-ups цонх дээр дарж болохгүй - Өөр веб сайтал зочлох үедээ браузер, хөтөчийн гаргаж буй анхааруулгыг сайтар харгалзах - Үл таних эх сурвалжаас ирсэн захиан доторх холбоос дээр огт дарж болохгүй - HTTP юмуу HTTPS холбоосыг шалгах
	Content Security Policy (CSP) гарчиг хэрэгжүүлээгүй	Content Security Policy (CSP) байхгүй учир хэд хэдэн төрлийн халдлага, түүний Cross Site Scripting (XSS) болон data injection халдлага үйлдэх боломж үүсгэж байна. Эдгээр халдлага нь өгөгдөл хулгайлахаас эхлээд интерфэйс, сайтыг бүрэн өөрчлөх, хортой код суулгах г.м хортой үйлдлүүд хийхэд ашиглагдана.	дунд	https://omnicapital.mn	Content-Security-Policy гарчиг нэмэх замаар Content Security Policy (CSP)-ийг хэрэгжүүлнэ. Content Security Policy (CSP) -ийг веб аппликейшн болон түүний тохируулгад хэрэгжүүлэх шаардлагатай.

Security

Strict-Transport-Security Header	Strict-Transport-Security (HSTS) header – гарчиг тогтоогоогүй учир дараах төрлийн аюул учирч байна: - Man-in-the-middle халдлага үйлдэх - HTTPS холболтын протоколыг HTTP холболт болгон буууруулах (Protocol downgrade - SSL stripping) халдлага үйлдэх - Session hijacking – сессийг замаас нь барих Итгэл алдагдах	дунд	https://moni.mn/cdn-cgi/scripts/5c5dd728/cloudflare-static/emaildecode.min.js	Системийн сервер, веб сервер, ачаалал тэнцвэржүүлэгч г.м зүйлс Strict-Transport-Security дэмжихээр тохируулагдсан байх ёстой. Энэ эмзэг байдлыг арилгахын тулд HSTS хэрэгжүүлж max-age attribute -ийг зөв тогтоож өгнө.
Cookie No HttpOnly Flag	HttpOnly flag тохируулагдаагүй учир халдагч cross-site scripting (XSS) халдлага үйлдэх, cookies-ээс чухал мэдээлэл хулгайлах боломжтой болсон	Дунд	http://moni.mn	- Хамгааралтай Cookies-ийг ажиллах тогтооно - Сервер талын кодыг шинэчилнэ. - Шинэчилсэн кодоо тестэлнэ. Шаардлагатай аюулгүй байдлын арга хэмжээ нэмж хэрэгжүүлэх.
Cross-Domain JavaScript Source File Inclusion	Cross-Domain JavaScript Source File Inclusion (XDSFI) эмзэг байдал байгаа учир халдагч XSS (Cross-Site Scripting) халдлага, өгөгдөл хулгайлах, фишинг болон нийгмийн боловсруулалт халдлага үйлдэх боломжтой байна.	Өндөр	http://moni.mn	- CORS (Cross-Origin Resource Sharing) гарчиг ашиглах; - Proxy Server хэрэгжүүлэх; - JSONP (JSON Padding бүхий) ашиглах - WebSockets ашиглах; - Server-Side Rendering ашиглах; - External Data-гаа баталгаажуулах; - Чухал мэдээлэл хандах хандалтыг хязгаарлах. Dependencies-ийг байнга шинэчлэх.

Өгөгдөлтэй холбоотой эмзэг байдлууд	Эмзэг байдлыг ашиглаж болох аюулууд	Тодорхойлсон эрсдлүүд
1. Тээгчүүд тоос, шороо, температур, чийгэнд мэдрэмтгий 2. Тээгчийн хяналтгүй ашиглах, зөөвөрлөх, гаргах 3. Өгөгдлийн нөөцийг буруу ангилах, шошголох 4. Өгөгдөл санамсаргүй өөрчлөгдөх, устгах 5. Өгөгдөл санамсаргүй задрах 6. Өгөгдлийн нөөцлөлт хийхгүй байх, хийсэн нөөц хуулбар нь алдаатай байх 7. Объектийг дахин ашиглах - өөр хэрэглэгчийн чухал өгөгдөлтэй тээгч, диск, санах ойд хандалт олгох 8. Өгөгдөл оруулах алдаа – сэжигтэй өгөгдлийг зүй ёсны хэмээн систем хүлээж авах 9. Оруулж, гаргаж буй өгөгдлийн хяналт сул 10. Боловсруулсан өгөгдлийг баталгаажуулах явц хэрэгжээгүй. 11. Компьютерийн нууц үг, хандалтын удирдлага сул 12. Шифрлэгдээгүй мэдээлэл, зөөгчүүд	Тээгчийн мэдээллийн алдаа Өгөгдлийн санг устгах, үлдэгдэл өгөгдлийг шиншлэх Ажилтнуудын буруу ашиглалт болон зөвшөөрөлгүй хандалт Гадны этгээд хууль бусаар хандах Цахим хорлон сүйтгэх ажиллагаа, сүйтгэл Өгөгдлийг өөрчлөх, устгах Хувийн мэдээлэл хулгайлах, Өгөгдлийн аюулгүй байдлын зөрчил Нууц мэдээлэл алдагдах Бичлэг, тайлан устгах Бичлэгийг хуурамчаар үйлдэх Бичлэгүүдэд хууль бус өөрчлөлт оруулах Хэрэглэгчийн бүртгэл алдагдах	• Өгөгдөл мэдээлэл хулгайлах эрсдэл • Өгөгдөл устгах • Бизнес үйл явц тасалдах, зогсох • Өгөгдлийг өөрчлөх, засварлах, хуурамчаар үйлдэх эрсдэл • Цахим өгөгдөл, мэдээллийг гадагш авч гарах, илгээх • Хувийн өгөгдөл хулгайлах, өгөгдлийн аюулгүй байдал алдагдах эрсдэл • Өгөгдлийг шиншлэх, санах ойг шиншлэх эрсдэл • Өгөгдлөө шифрлүүлэх • Ашиг орлогоо алдах • Нэр хүндээ алдах • Цаг хугацаа, үргүй ажиллагаа хийгдэх

Түншүүд болон нийлүүлэгчтэй холбоотой эмзэг байдлууд	Эмзэг байдлыг ашиглаж болох аюулууд	Тодорхойлсон эрсдлүүд
1. Харилцаа холбооны үйлчилгээ тасалдах 2. Тог, ус, халаалт г.м ахуйн үйлчилгээ тасалдах 3. Нийлүүлэгдсэн Тоног төхөөрөмж ажиллагаанаас гарах 4. Нийлүүлэгдсэн Програм хангамж ажиллагаанаас гарах 5. Захидал, илгээмж замаасаа алдагдах 6. Нийлүүлэлт тасалдах 7. Түнш, нийлүүлэгчид санамсаргүй болон санаатайгаар нууц мэдээлэл илгээх	Харилцаа холбоогүй болох Офис хүртээмжгүй болох Үйл явц тасалдах Өгөгдөл алдагдах, нууц задрах	-Бизнес үйл явц тасалдах -Өгөгдлөө задлах, алдах эрсдэл -Програм хангамж ажиллахгүй болох эрсдэл -Техник хангамж ажиллахгүй болох эрсдэл

Удирдлага, зохион байгуулалтын эмзэг байдлууд	Эмзэг байдлыг ашиглаж болох аюулууд	Тодорхойлсон эрсдлүүд
1. МАБ, МТ-ийн бодлого байдаг, гэвч ажилтнууд мэддэггүй, мөрддөггүй. 2. МАБ-ын бодлого, журмуудыг нягтлах, сайжруулах журам хэрэгжээгүй 3. МАБ-ын нэгдсэн журам гаргасан ч эцсийн хэрэглэгчид хүрээгүй, салгаагүй учир нууцлал алдагдах магадлалтай 4. МАБ-ын талаар удирдлага үүрэг хүлээдэггүй. 5. Аюулгүй байдлын нөхөөсийг суулгадаггүй 6. Будлиан болон учрал, тохиолдлын бүртгэл сул, Будлиан зөрчлийн удирдлага байхгүй 7. Тохируулгын алдаа, аюулгүй байдлын анхааруулгыг боловсруулдаггүй 8. Байнгын аудит, нягтлах ажиллагаа байхгүй 9. Хог хаягдлаа зохих ёсоор устгадаггүй 10. Өөрчлөлтийн удирдлага сул 11. Нийтлэг хяналтууд сул 12. МАБ-ын аудит, эрсдлийн үнэлгээ, өөрийн үнэлгээ хийж байгаагүй, эрсдлийн удирдлага байхгүй. 13. Бизнесийн орчны хурдан өөрчлөлтийн дагуу МТ-ийн хөгжүүлэлт хийдэггүй 14. Тасралтгүй ажиллагааг төлөвлөөгүй, удирдлага, сэргээн ажиллуулах төлөвлөгөө байхгүй 15. Мэдээллээ муу ангилсан, Цахим шошгололт байхгүй, нууцлалын гэрээгүй 16. Ажилтнуудаа сайн хянадаггүй, МАБ-ын талаар уялдаа холбоо байхгүй, үүргийг тодорхойлоогүй 17. Нийлүүлэгчийг сайн хянадаггүй 18. Ажилтнуудаа сургалтанд хамруулдаггүй 19. Хандалтын удирдлага, хяналт сул 20. Баримт бичгийн хамгаалалт сул, задгай 21. Цэвэр ширээ, цэвэр дэлгэцийн бодлого байхгүй 22. Криптограф ашигладаггүй, бодлого байхгүй 23. Ажлаас халагдсан, ажлаа өөрчилсний дараа хандалтын эрхийг хүчингүй болгох албан ёсны журам байхгүй 24. Мобайл төхөөрөмжийг хамгаалах хамгаалалт, журам байхгүй 25. Өгөгдлийг хяналтгүй хууддаг 26. Интернетээс янз бүрийн зүйлс хяналтгүй татдаг. 27. Мэдээллийн системийг хяналтгүй ашигладаг. 28. Бүртгэгдээгүй програм хангамж ашигладаг.	Буруу ашиглалт Зохисгүй, аюултай хэрэглээ Санамсаргүй & санаатай алдаа, Системийн алдаа, Бүрдэл хэсэг, өгөгдөл, тоног төхөөрөмжийг устгах Фишинг, фармингийн халдлага Гадны этгээд хууль бусаар хандах Эрхээ хэтрүүлэх Зохих цогц чадвар, МАБ-ын мэдлэг туршлага бүхий хүний нөөц дутагдах ПХ хууль бусаар суулгах, өөрчлөлт оруулах Засварын алдаа, буруу тохируулга хийх Маскадинг, хууралт / Нийгмийн боловсруулалт, Спам-соёлгүй зарын халдлага Ажилтнуудын буруу ашиглалт болон зөвшөөрөлгүй хандалт Хувийн мэдээлэл хулгайлах, Өгөгдлийн аюулгүй байдлын зөрчил Гэрээний үүргээ нөгөө тал зөрчих Хууль зөрчих Гуравдагч талаас хохирол учруулах Сүлжээнд зөвшөөрөлгүй этгээд холбогдох Нууц мэдээлэл алдагдах Бичлэг, тайлан устгах Ашиглан шамшигдуулах, хулгай Бичлэгийг хуурамчаар үйлдэх	- Өгөгдлөө задлах, алдах эрсдэл - Үйлчилгээ, засвар алдагдах, буруу болох, буруу тохируулах эрсдэл - Ажиллагсдын алдаа, дотроос ирэх халдлага, сүйтгэлийн эрсдэл - Програм хангамж ажиллахгүй болох эрсдэл - Техник хангамж ажиллахгүй болох эрсдэл - Техник хангамж хулгайлах эрсдэл - Өгөгдөл мэдээлэл хулгайлах эрсдэл - Дотроосоо хууль бусаар хандах, зүй бусаар ашиглах - Гаднаас хууль бусаар хандах, хакердах - Тагналтын хохирогч болох - Төхөөрөмжүүд зомби болох - ПХ-д хууль бус өөрчлөлт оруулах - Системийн тохируулга өөрчлөх - Хортой кодын халдлагад өртөх - АРТ – Ажилтны компьютерт Троян суулгаж системд халдах - Ransomware – авилгач кодын халдлагад өртөх, өгөгдөл мэдээллээ блокуулах - Програмын цоорхойг ашиглан (zero day) хакерууд компьютерт нэвтэрч дурын

Security

Хүний нөөцтэй холбоотой эмзэг байдлууд	Эмзэг байдлыг ашиглаж болох аюулууд	Тодорхойлсон эрсдлүүд
1. Нийгмийн сүлжээнд татагдах, нөлөөлөлд нь автах 2. Мэргэжлийн байгууллагуудтай харилцаа тогтоогоогүй 3. Офисоос ажлын өгөгдлөө авч гарах (лэптоп, цаас, флэш, бусад тээгч, утас) 4. Албаны баримт бичиг, өгөгдлийг гадагш гаргах 5. Албаны баримт бичгийг мэйлээр болох факсаар илгээх 6. Зүй бус програм, апп-ыг суулгах 7. Аюулгүй байдал, хамгаалалтын хэрэгслийг арилгах, унтраах 8. Гадны этгээдийг өрөө, тасалгаа, офистоо оруулах (арын хаалга) 9. Спам болон хортой хавсралт, холбоос бүхий захиаг нээх 10. Компанийн сүлжээнд хувийн төхөөрөмжөө холбох 11. Нууц үг болон нууц мэдээллийг цаасан бичих, сул нууцлах 12. Ухаалаг карт, ажилтны карт г.м хамгаалалтын хэрэгслээ хаях 13. МАБ-ын мэдлэг, ойлголт сул 14. Халагдсан ажилтнууд компанийн нууцыг задлах 15. Халагдсан ажилтнууд компанийн асуудлыг хэлэлцэх 16. МАБ-ын талаар ажилтнуудын чиг үүргийг хуваарилаагүй. 17. Администраторуудын сургалт болон Хүний нөөцийн хөгжлийн төлөвлөгөө байхгүй. 18. Хүний нөөц, холболт, сүлжээ, системийн аюулгүй байдлын бодлого хэрэгжээгүй. 19. Хэрэглэгчдийн үүрэг хариуцлага тодорхойлогдоогүй, аюулгүй байдлын журмууд хэрэгжээгүй. 20. Хандалтын эрхээ гэмт зорилгоор хэтрүүлэн ашиглах (зөвшөөрөгдсөн эрхээ хэтрүүлэн гэмт зорилгоор ашиглах) 21. Зөвшөөрөгдөөгүй ашиглалт – Зүй бус зориулалтаар компанийн нөөцийг ашиглах 22. Халхавчлах – Өөр хэрэглэгчийн нэрээр үйлдэл гүйцэтгэх 23. Офисоос гарсан, компьютерээ орхисон үед системд холболттой орхидог 24. Фишинг/Spear фишингэд өртөх боломж өндөр 25. Хэрэглэгч хамгаалагдсан талбарт хандах 26. Хэрэглэгч нууц өгөгдөлд хандах	Буруу ашиглалт Санамсаргүй, санаатай алдаа, Бүрдэл хэсэг, өгөгдөл, тоног төхөөрөмжийг устгах Фишинг, фармингийн халдлага Эрхээ хэтрүүлэх Зохих цогц чадвар, МАБ-ын мэдлэг туршлага бүхий хүний нөөц дутагдах ПХ хууль бусаар суулгах, өөрчлөлт оруулах Маскадинг, хууралт / Нийгмийн боловсруулалт, Спам-соёлгүй зарын халдлага Ажилтнуудын буруу ашиглалт болон зөвшөөрөлгүй хандалт Өгөгдлийн аюулгүй байдлын зөрчил Хууль зөрчих Сүлжээнд зөвшөөрөлгүй этгээд холбогдох Нууц мэдээлэл алдагдах Бичлэг, тайлан устах Ашиглан шамшигдуулах, хулгай Бичлэгийг хуурамчаар үйлдэх Нууц үгээ задлах Үйлчилгээ буруу хийх Хууль бус програм суулгах Бизнес үйл явц тасалдах,зогсох Туслах үйлчилгээ алдагдах Бичлэгүүдэд хууль бус өөрчлөлт оруулах Хэрэглэгчийн алдаа Ботнетийн хохирогч болох (Zombie) Өгөгдлийг өөрчлөх болон устгах Тоног төхөөрөмж, эд анги, өгөгдөл,	• Нийгмийн сүлжээгээр залилуулах • Өгөгдлөө задлах, алдах эрсдэл • Үйлчилгээ, засвар алдагдах, буруу болох, буруу тохируулах эрсдэл • Ажиллагсдын алдаа, дотроос ирэх халдлага, сүйтгэлийн эрсдэл • Програм хангамж ажиллахгүй болох эрсдэл • Техник хангамж ажиллахгүй болох эрсдэл • Техник хангамж хулгайлах эрсдэл • Өгөгдөл мэдээлэл хулгайлах эрсдэл • Дотроосоо хууль бусаар хандах, зүй бусаар ашиглах • ПХ-д хууль бус өөрчлөлт оруулах • Системийн тохируулга өөрчлөх • Цахим вандализм, хорлон сүйтгэх ажиллагааны эрсдэл • Өгөгдлийг өөрчлөх, засварлах, хуурамчаар үйлдэх эрсдэл • Фишинг, фарминг, маскарадинг, хуурах, мэхлэх, барьцаалах, нийгмийн боловсруулалт, спамын хохирогч болох эрсдэл • Бизнес үйл явц тасалдах • Цахим өгөгдөл, мэдээллийг гадагш ажл гаргах, илгээх

Халдагчийн сэдлийн хувьсал

Алдар нэр
олох

Итгэлцлийг алдагдуулах

Улс орны тогтвортой
байдлыг алдагдуулах

Өшөө авах

Өрсөлдөөнд давуу
байдал олох

Засгийн Газрыг унагах

Өөрийн статусыг
дээшлүүлэх

Санал бодолд
нөлөөлөх

Дайсны довтлох, хамгаалах
системийг унагах, унтраах

Санхүүгийн
ашиг

Оюуны өмч
хулгайлах

Тагнах, мөшгөх

Крипто валют
олборлох

Security

Тулгарч буй нийтлэг аюул



Орчин үеийн халдлагын эх сурвалж



Security

Монгол Улсын төрийн байгууллагад чиглэсэн халдлагын жишээ

- ОХУ-ын Space Bears Group Интермед эмнэлгийн өгөгдлийг хулгайлж дараа нь ransomware хортой код ашиглан өгөгдлийг шифрлэсэнтэй яг ижил халдлагыг нэгэн аймгийн төрийн үйлчилгээний системд үйлдсэн: [Space Bears Group Breach Mongolian Hospital – CyberMaterial](#)
- ОХУ-ын APT29 бүлэг төрийн веб сайтуудад халдаж ихээхэн өгөгдөл хулгайлсан: [Google says Russian group targeted Mongolian government with exploits used by NSO Group | The Record from Recorded Future News](#)
- БНХАУ-ын дэмжлэгтэй APT хакерийн бүлэг Able програмын шинэчлэлтээр дамжуулан 430 орчим төрийн байгууллагын өгөгдөл хулгайлсан: [Chinese APT suspected of supply chain attack on Mongolian government agencies | ZDNET](#)
- БНХАУ-ын хакерийн бүлэг Үндэсний Дата Төвийн хамгаалалтыг эвдэлж байршуулсан төрийн веб сайтуудад хортой код суулгасан: [This Chinese hacking group pwned a bunch of Mongolian government sites - CyberScoop](#)

Security

2023-2024 онд хакердуулсан веб сайт ЫН ЖИШЭЭ ([Compromised domain lists. Malware and ransom compromised domains.](#))

Notifier	H	M	R	L	★ Domain	OS	View
ALP3R	H	M			orshilconstruction.mn	Linux	mirror
Expired	H				specialmongolia.mn	Linux	mirror
TurkishSpyHacker					gofundme.mn/Turk.html	Linux	mirror
chinafans					victorysports.mn/x.txt	Linux	mirror
CyBeRkAnKa	H	M			weblink.khunnu.mn	Linux	mirror
Aris Dot ID		M			asar-maikhan.mn/x.txt	Linux	mirror
CyBeRkAnKa	H	M			sumber.nemekh.mn	Linux	mirror
CyBeRkAnKa	H	M			galt.nemekh.mn	Linux	mirror
CyBeRkAnKa	H				nemekh.mn	Linux	mirror
jok3r			R		pch4.mn/images/jdownloads/scre...	Linux	mirror
jok3r	H				★ khanuul.procurement.gov.mn	Linux	mirror
Index Php			R		★ zaamar.to.gov.mn/zxcvbnm.gif	Linux	mirror
Spyhackerz.com	H		R		www.nta.mn	Linux	mirror
./UNIX					ganabell.mn/ds.html	Linux	mirror
N61tap					www.ikh-ishtolgoi.mn/p.htm	Linux	mirror
N61tap					www.crusher-screen.mn/p1.txt	Linux	mirror
Virtual	H				★ ces.gov.mn	Win 2008	mirror
Virtual	H				★ ajil.gov.mn	Win 2008	mirror
Mr.Kro0oz.305		M			lhagvadorj.mn/i.htm	Linux	mirror
chinafans			R		www.chinggisbeer.mn/xx.htm	Win 2008	mirror
KkK1337					jobagency.mn/job/images/other/...	Linux	mirror
kevin (mr.k)					www.0479.mn/yolo.html	Win 2003	mirror
jok3r			R		www.soyolderdem.edu.mn/images/f...	Linux	mirror
Code Breaker		M	R		taiyobridge.mn/x.html	Linux	mirror
Code Breaker			R		wsp.mn/x.html	Linux	mirror

2023-2024 онд хакердуулсан веб сайт ЫН ЖИШЭЭ

Notifier	H	M	R	L	★ Domain	OS	View
Gekikara404					 noah.mn/mion.php	Linux	mirror
Reko					 ★ bnd.ub.gov.mn/?p=22375	Linux	mirror
Reko	H				 ★ edu.bkh.gov.mn	Linux	mirror
Turan Ordu	H		R		www.alutech.mn	Linux	mirror
./r0cky_n00bz	H				khiimori.mn	Linux	mirror
Prosox					 ★ kr.immigration.gov.mn/?p=2824	Linux	mirror
Prosox	H				 ★ police.gs.gov.mn	Linux	mirror
Team System Dz	H				 ★ fipds.mcaa.gov.mn	Linux	mirror
Team System Dz	H				 ★ khovd.mcaa.gov.mn	Linux	mirror
Team System Dz	H				 ★ nubia.mcaa.gov.mn	Linux	mirror
Team System Dz	H		R		 ★ www.mcaa.gov.mn	Linux	mirror
Team System Dz	H		R		 ★ ans.mcaa.gov.mn	Linux	mirror
Er0iN					 cs.skylink.mn/sh_stats/sh_hero...	Linux	mirror
moftah-deeb			R		 minjzand.mn/maile/maile.php	Linux	mirror
AGroup					www.mne.mn/mn/search	Linux	mirror
attacker	H		R		 ardchilal.mn	Linux	mirror
TuranOrdu	H				 ★ bgots.ub.gov.mn	Linux	mirror
Dr.Muneer	H				 ★ bangkok.mfa.gov.mn	Linux	mirror
CyBeRkaNka	H				 eng.iieb.mn	Linux	mirror
LuXas			R		 ★ bayangol.hudulmur.gov.mn/image...	Linux	mirror
CyBeRkaNka	H				 weblink.khunnu.mn	Linux	mirror
ZoRRoKiN					 ★ burtgel.gov.mn/tamga/stamp.rep...	Linux	mirror
MR ABAN	H				 www.oe.org.mn	Linux	mirror
OniXeeMa	H				 www.aerogeodesy.mn	Linux	mirror
AHFÂ TECENNÜN					 mnnf.mn/site/	Linux	mirror

Security

Кибер гэмт хэргийн улмаас 87.5 тэрбум төгрөгийн хохирол учирсан

“Олон улсын Кибер аюулгүй байдлын индекс – 2024” тайланд дурдсанаар Монгол Улс 194 орноос 103-т эрэмблэгдэж, 2020 онтой харьцуулахад, 17 байр урагшилсан.

Гэвч цахим орчинд иргэдийн мэдээллийг хулгайлах, хууль бусаар ашиглах, залилах, төрийн өгөгдөл хулгайлах зэрэг зохион байгуулалттай гэмт хэрэг нэмэгджээ. Төр захиргаа, олон нийтийн байгууллага, хувийн хэвшил, иргэн үл харгалзан дээрх халдлагад өртөж, сүүлийн таван жилийн хугацаанд энэ төрлийн гэмт хэрэг 25,849 хүрсэн. 2023 онд дээрх гэмт хэргийн улмаас 87.5 тэрбум төгрөгийн хохирол учирсан.

Кибер гэмт хэргийн улмаас 87.5 тэрбум төгрөгийн хохирол учир чээ - Цахим хөгжил, инновац, харилцаа холбооны яам

НОЦТОЙ АСУУЛТ:

Дижитал шилжилтийн эрин үед
аюул заналыг удирдах, өрсөлдөх
давуу талыг бий болгохын тулд
ямар шинэлэг арга хэмжээ
хэрэгжүүлэх вэ?

Security

Шинэ хандлага

- Өнөөдөр удирдлагууд айдас, тодорхойгүй байдал, эргэлзээг (АТЭ-FUD) дахин авч үзэх биш харин МАБ, хувийн нууцлалыг хангах шинэ хандлагын талаар сонсохыг хүсч байна..
- Тэд АТЭ-ийн хязгаарлалтаас гарч өөрсдийн, түншийн, хэрэглэгчийн МАБ, нууцлалыг өргөнөөр авч үзэх, хангахыг хүсэж байна.
- Орчин үеийн ихэнх байгууллага МАБ-ыг өөрчлөлтийн саад, илүү зардал гэж авч үзэхээ больсон (Харамсалтай нь Монголд байдал эсрэгээрээ).
- МАБ-ын шийдлүүд бизнесийн өсөлтөд нөлөөлж, давуу талыг бий болгож, брэндийн итгэлийг бий болгодог чухал хүчин зүйл гэдгийг тэд ойлгодог болсон.

МАН-ын зардлын тэргүүлэх чиглэлүүд

Дараагийн 12 сард хөрөнгө оруулах чиглэлүүд
(Европын компаниуд)



Security

МАБ-ын уламжлалт арга хэмжээ + Шинэ шийдлүүд

МАБ-ын уламжлалт арга хэмжээ хяналтууд

- МАБ-ын хууль, зохицуулалт
- МАБ-ын стандартууд
- МАБ-ын бодлого & журмууд
- Эрсдлийн удирдлага
- Асуулга чек лист
- ISO 27001 стандартад тодорхойлсон хяналтууд
- Техникт суурилсан хамгаалалт
- Програмд суурилсан хамгаалалт
- Албан ёсны аргууд
- Тасралтгүй ажиллагааны төлөвлөлт
- Будлианы удирдлага
- Аудитууд



МАБ-ын шинэ арга хэмжээ, хяналтууд

- ХОУ-д суурилсан хэрэгслүүд
- Танин мэдэхүйд суурилсан МАБ
- Үүлэнд МТ-ийн функцийг байршуулах
- МАБ-ын гадна үйлчилгээ
- Хандалтын удирдлагад биометрик, тоон гарын үсгийн шийдэл ашиглах
- Нээлттэй эхийн програм ашиглах
- МАБ-ыг хангахад их өгөгдөл (big data) ашиглах
- Интернет эд зүйлийн аюулгүй байдалд хөрөнгө оруулах
- Кибер эрсдлийн даатгал
- Шинэ албан тушаал-ССО (Кибер аюулгүй байдлын захирал)
- Захиалгат аюулгүй байдал
- Өгөгдлийн аюулгүй байдлыг хангахад Blockchain технологи хэрэглэх
- Үүлний АБ-ын аудит

Аюулгүй байдлын шинэ технологи

- Хортой код илрүүлэх шинэ загвар (машин сургалтанд суурилсан математик загвар, сэижигтэй файлыг виртуаль хайрцагт турших, SaaS –д суурилан аюулгүй байдлыг скандах, үүлэн тооцоололд суурилан хортой кодыг шинжлэх)
- Сайжруулсан үйлчилгээ (хуваарилагдсан, итгэлцлийн болон блокчэйнтэй төстэй архитектур ашиглах, гаднаасаа адил шифрлэлт ашиглах)
- Хэрмээ бэхлэх (програмын түвшинд аюулгүй байдлыг хангах, програмын контейнер болон бүрхүүл суулгах, халдлагыг хүлээж авах аппаратыг тусгаарлах, аюулгүй виртуаль контейнер суулгах, системийн үйл явцыг тусгаарлах бичил хуяг, бичил сегментаци болон илүү хуваарилагдсан "баруун/зүүн" сегментаци сүлжээндээ хэрэгжүүлэх, IPsec «цэг-цэг» хонгил, криптографийн тусгаарлалт)
- Залилагчийг залилах (хуурамч эмзэг байдал үүсгэсэн өгөөш бэлдэх гэх мэт технологи)
- Халдлагаас татгалзах (халдагчийн сэдэл төрүүлж буй зүйлийг арилгах)
- Халдлагыг үгүйсгэх (алслагдсан браузер гэх мэт)
- Хандалтын сайжруулсан өгөгдөл (хиймэл оюун ашиглан хэрэглэгчийг байршил, цаг хугацаа, зан үйл, хэвшил дээр суурилан таньж баталгаажуулах)
- Гүнзгийрүүлсэн баталгаажуулалт (биометр, тоон гарын үсэг ашигласан олон хүчин зүйлт хандалтын удирдлага)

МЭДЭЭЛЛИЙН АЮУЛГҮЙ БАЙДЛЫН ХАНДЛАГА



Security



Кибер болон мэдээллийн аюулгүй байдал нь төр, бизнесийн байгууллагын санал болгож буй бүтээгдэхүүн, үйлчилгээ, хэрэглэгчийн итгэлийн нэг хэсэг болсон. ТЭА-ын Аюулгүй байдлын архитектур заавал хэрэгжүүлэх болсон



Мэдээллийн болон КАБ-ыг дижитал стратеги-тайгаа уялдуулж чадсан байгууллагууд хийж гүйцэтгэж буй бүх зүйлдээ итгэлтэй байж, хурдан өөрчлөгдөж хувьсаж чаддаг



“Удирдлага бүхий аюулгүй байдлыг хэрэгжүүлж чадсанаар мэдлэг хуримтлуулж, МАБ, КАБ-ын түвшингээ шинэ шатанд гаргах боломжтой Болно.



Олон байгууллага хоёр хүчин зүйлт (2FA) таньж баталгаажуулах механизм ашиглах болсоноор Аюулгүй байдлын илүү түвшний хамгаалалт бий болгосон.



Хувийн өгөгдөл хамгаалах шинэ хандлагыг хэрэгжүүлдэг болсон. МАБ-ын болон өгөгдөл хамгаалах ажилтны орон тоог заавал болгосон



Орчин үеийн байгууллага МАБ, КАБ-ыг хувийн нууц, халдашгүй байдал, дижитал ёс зүйтэй уялдуулсан. Үүний үр дүнд үйлчилгээний чанар эрс дээшилдэг.



Төрийн үүлэн орчинд систем, вебээ байр-луулах нь онц чухал үйл явц, өгөгдөлөө Хамгаалах шилдэг практик гэж тооцогдох болсон



Олон байгууллага Big Data analytics болон хиймэл оюун ухаан ашиглан аюулыг адилтгаж, эрсдэл тодорхойлж, зөрчлийг илрүүлж байна



Нээлттэй эх код ашиглах болсоноор МАБ-ын хөтөлбөрөө сайжруулж, хамтын сэтгэлгээ, мэдлэг хуваалцах боломж олж авсан.



Байгууллагууд ISO 27001, 27002 стандартын дагуу МАБМТ бий болгож, бодлого, журам, заавар, сургалтын хөтөлбөр хэрэгжүүлдэг болсон.

Security



THANK YOU
for your
ATTENTION!



khaltar@sssmn.com



khaltar.togtuun