2026

ВИРТУАЛ ХӨРӨНГИЙН ҮЙЛЧИЛГЭЭ ҮЗҮҮЛЭГЧ БАЙГУУЛАГЫН КИБЕР ЗАЛИЛАНГИЙН ЭРСДЭЛЭЭС УРЬДЧИЛАН СЭРГИЙЛЭХ БОЛОМЖИЙН СУДАЛГАА

(зохицуулагч байгуулага, банк болон банк бус санхүүгийн байгуулага, виртуал хөрөнгийн үйлчилгээ үзүүлэгч, харилцагч хооронд)

Удирдсан багш: ***Э.Тамир/PhD, Санхүү Эдийн Засгийн Их Сургууль, Санхүүгийн танхим ахлах багш/***

Судлаач: ***Э.Ганди***

Мэргэжил: ***Бизнесийн удирдлага***

Курс: ***IV түвшин***

Агуулга

Судалгааны зорилго

VASP-ийн кибер залилангийн эрсдэлийг судалж, урьдчилан сэргийлэх арга замыг тодорхойлох

Хураангуй

- **Виртуал хөрөнгө (Virtual Asset)**
- **Кибер залилан (Cyber Fraud)**
- **VASP (Virtual Asset Service Provider)**
- **Эрсдэлийн удирдлага (Risk Management)**
- **AML/CFT (Anti-Money Laundering / Combating the Financing of Terrorism)**
- **FATF (Financial Action Task Force)**

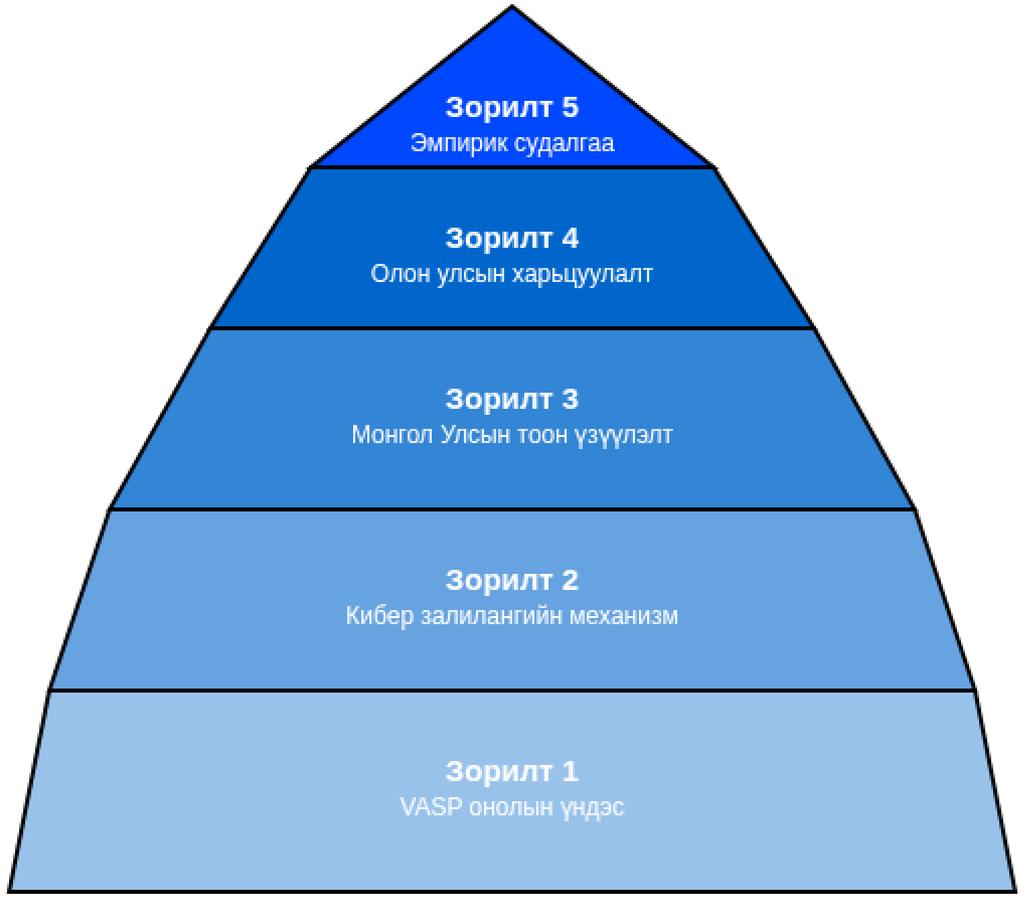
Судалгааны зорилго ба зорилтууд

Судалгааны зорилго

VASP экосистемийн оролцогч талуудын хооронд үүсч буй кибер залилангийн эрсдэлийн хүчин зүйлсийг тодорхойлж, Монгол Улсын нөхцөлд тохирох урьдчилан сэргийлэх арга хэмжээг санал болгох

Судалгааны зорилтууд

1. **VASP-ийн тодорхойлолт, ангилал, экосистемийн онолын үндсийг тогтоох**
2. **Кибер залилангийн механизм, төрөл, үе шатыг судлах**
3. **Монгол Улсын 2015-2024 оны тоон үзүүлэлт, FATF үнэлгээг дүн шинжилгээ хийх**
4. **Олон улсын харьцуулалт (Сингапур, БНСУ, Япон, ЕХ) хийх**
5. **Эмпирик судалгаагаар (N=200) эрсдэлийн ойлголт, институцийн чадавхыг үнэлэх**



Судалгааны зорилтуудын пирамид

Удиртгал: Дижитал шилжилт ба шинэ эрсдэл

- **Дэлхийн санхүүгийн системд дижитал шилжилт эрчимтэй явагдаж байна. Виртуал хөрөнгийн зах зээлийн хэмжээ 2024 онд $2.4 их наяд ам.доллар хүрсэн.**

Виртуал хөрөнгийн технологийн онцлог шинж чанарууд:

- Псевдо-нэр нууцлал (Pseudonymity) - хэрэглэгчийн бодит мэдээлэл нууцлагдсан
- Хил дамнасан гүйлгээ (Cross-border transactions) - зохицуулалтын хяналтаас гарах
- Буцаах боломжгүй (Irreversibility) - гүйлгээг цуцлах боломжгүй

- **Эдгээр шинж чанарууд нь кибер залилангийн эрсдэлийг нэмэгдүүлж, уламжлалт санхүүгийн хяналтын арга хэмжээг хангалтгүй болгож байна.**

Судалгааны шаардлага: VASP экосистемийн бүх оролцогч талуудын (зохицуулагч, банк, VASP, хэрэглэгч) хооронд үүсч буй эрсдэлийг олон талт түвшинд авч үзэх шаардлагатай.

VASP: тодорхойлолт ба ангиллын суурь

Виртуал хөрөнгө (VA)

Дижитал хэлбэрээр илэрхийлэгддэг, төлбөр тооцоо эсвэл хөрөнгө оруулалтын зорилгоор ашиглагдах өртгийн дижитал илэрхийлэл (FATF, 2019)

VASP

Виртуал хөрөнгөтэй холбоотой үйл ажиллагаа мэргэжлийн түвшинд эрхэлдэг хуулийн этгээд (Virtual Asset Service Provider)

VASP-ийн 6 төрөл (FATF ангилал)

1	**Криптовалютын бирж (CEX)**	Виртуал хөрөнгийн арилжаа, солилцоо хийх төвлөрсөн платформ	Binance, Coinbase, Kraken
2	**Хэтэвчний үйлчилгээ**	Виртуал хөрөнгийг хадгалах, шилжүүлэх цахим хэтэвч	MetaMask, Ledger, Trust Wallet
3	**Төлбөрийн үйлчилгээ**	Виртуал хөрөнгөөр төлбөр тооцоо хийх үйлчилгээ	BitPay, CoinGate
4	**OTC арилжааны тавцан**	Биржээс гадуур шууд арилжаа хийх платформ	LocalBitcoins, Paxful
5	**Bitcoin ATM**	Бэлэн мөнгө ба виртуал хөрөнгийг солих автомат	Genesis Coin, General Bytes
6	**DeFi платформ**	Төвлөрсөн бус санхүүгийн үйлчилгээ	Uniswap, Aave, Compound

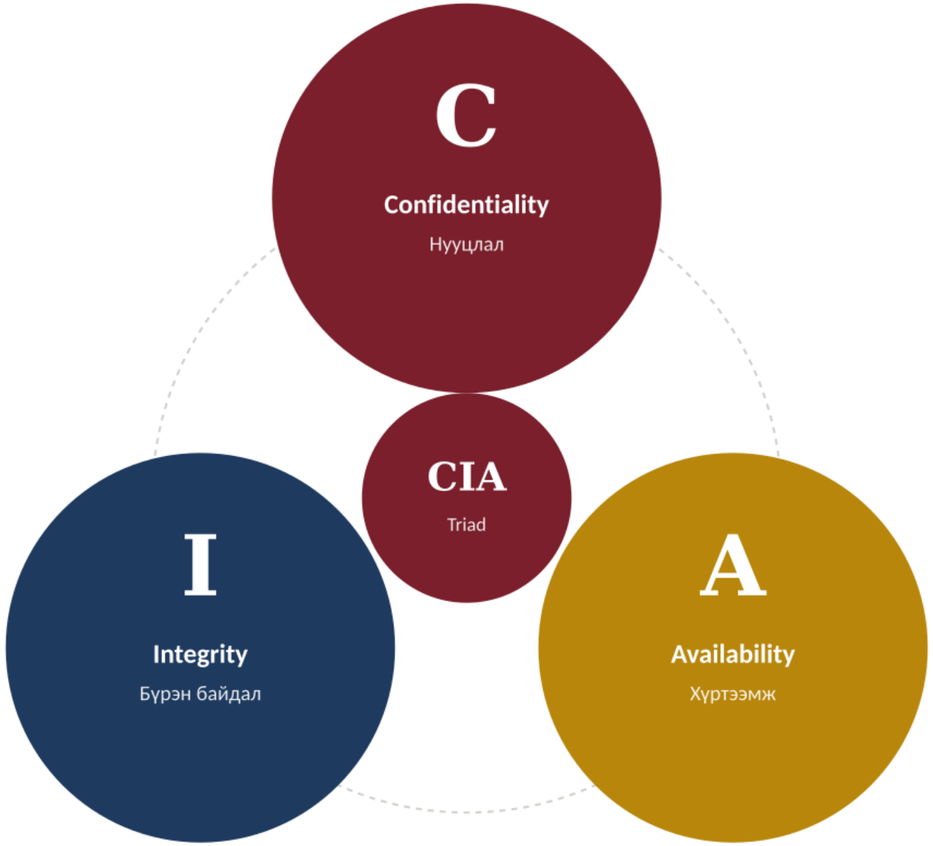
Эх сурвалж: FATF (2019), "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers"

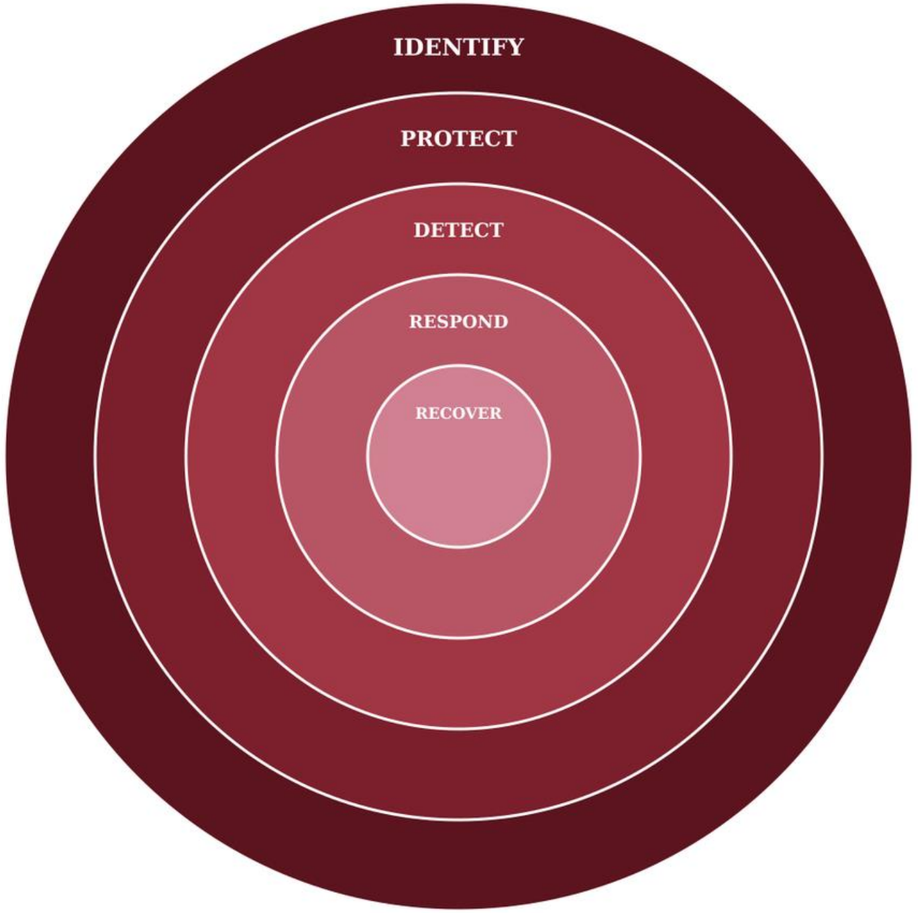
VASP-ийн 6 төрөл (ангилал)

Криптовалютын бирж (CEX)	Фиат ба виртуал хөрөнгийн солилцоо, арилжаа	Binance, Coinbase, Kraken
Хэтэвчний үйлчилгээ	Виртуал хөрөнгийн хадгалалт, удирдлага	MetaMask, Ledger, Trust Wallet
Төлбөрийн үйлчилгээ	Виртуал хөрөнгөөр төлбөр тооцоо	BitPay, CoinPayments
OTC арилжааны тавцан	Хоёр талын шууд арилжаа (peer-to-peer)	LocalBitcoins, Paxful
Bitcoin ATM	Бэлэн мөнгө ба виртуал хөрөнгийн солилцоо	Genesis Coin, General Bytes
DeFi платформ	Төвлөрсөн бус санхүүгийн үйлчилгээ	Uniswap, Aave, Compound

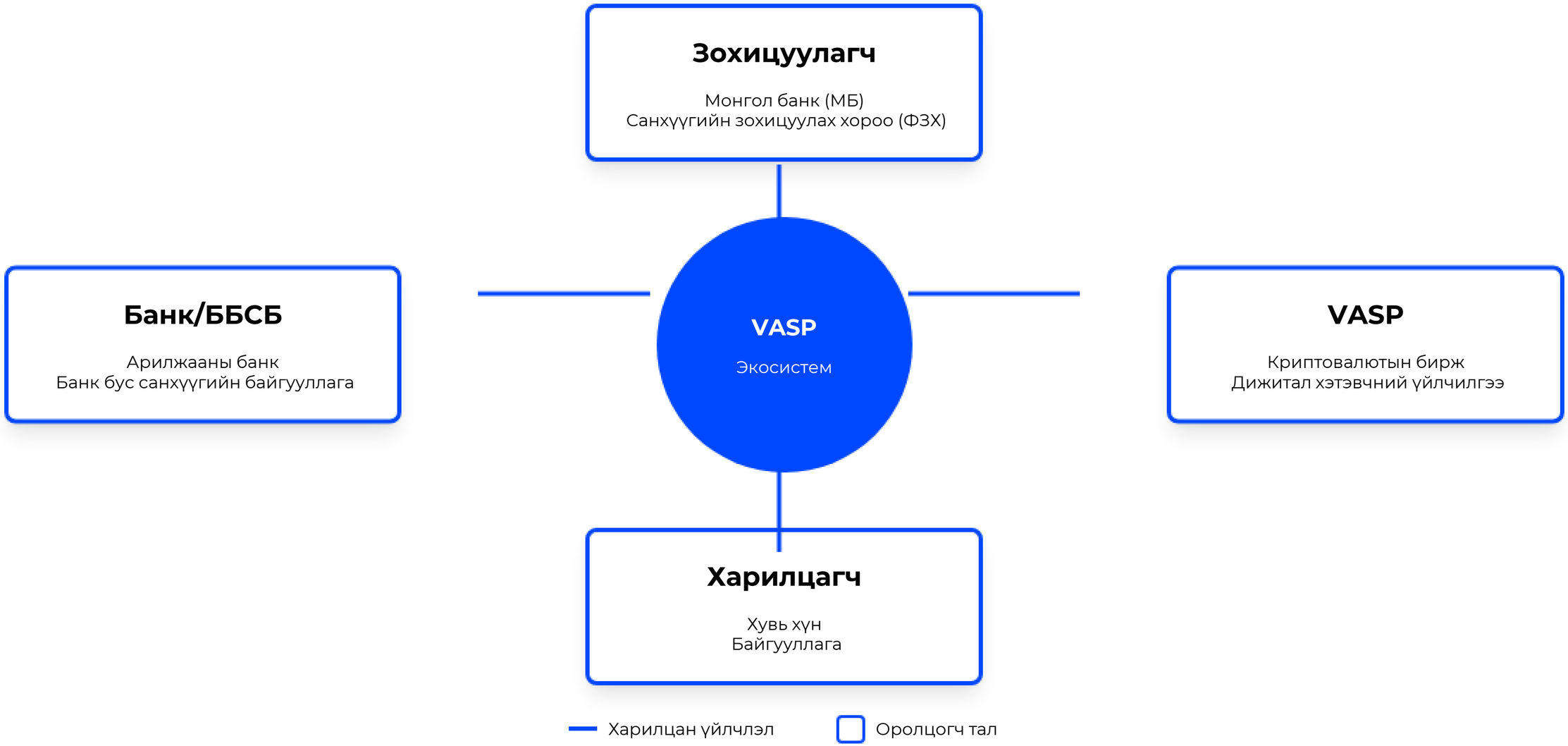
Эх сурвалж: FATF (2019), Chainalysis (2024)

Виртуал орчинд үйл ажиллагаа явуулж буй байгууллагуудын суурь хүчин зүйлс





VASP экосистем: 4 оролцогч тал



Оролцогч талуудын үүрэг ба хамгийн сул холбоос

Зохицуулагч (МБ, ФЗХ)

Эрх зүйн орчин бүрдүүлэх

Лиценз олгох, хяналт шалгалт хийх

AML/CFT стандарт тогтоох

FATF зөвлөмжийг хэрэгжүүлэх

VASP (Бирж, Хэтэвч үйлчилгээ)

Гүйлгээний дэд бүтэц хангах

KYC/CDD процесс хэрэгжүүлэх

SAR/STR тайлагнал илгээх

Дотоод комплаенс бодлого баримтлах

Банк/ББСБ

Фиат валют ба виртуал хөрөнгийн холбоос

Уламжлалт санхүүгийн системтэй гүүр

Гүйлгээний мониторинг

Харилцагч (Хэрэглэгч)

Үйлчилгээний эрэлт, хэрэглээ

Гол дүгнэлт

Хамгийн сул холбоос VASP-ийн дотоод комплаенс

Байгуулага хоорондын мэдээлэл солилцоо хангалтгүй, технологийн дэмжлэг сул, хүний нөөцийн чадавх хязгаарлагдмал

Эх сурвалж: RUSI (2023), "Crypto-Asset Compliance Gaps"

Кибер залилангийн 7 үндсэн төрөл

Төрөл	Механизм ба онцлог	Зорилтот тал	Хохирлын түвшин
Фишинг	Хуурамч вэбсайт, имэйл ашиглан нэвтрэх мэдээлэл хулгайлах	Хэрэглэгч, VASP	$1K-50K
Ransomware	Систем шифрлэх, золиос шаардах	Байгуулага, VASP	$1M+
Rug Pull	Хуурамч DeFi төсөл байгуулж, хөрөнгө зугтаах	Хөрөнгө оруулагч	Маш өндөр
Wallet Hacking	Хувийн түлхүүр, seed phrase хулгайлах	Хэрэглэгч	Хувьсах
Романтик залилан	Найрсаг харилцаа тогтоож, итгэлцэл бий болгох	Хэрэглэгч	Дунд-өндөр
Pump & Dump	Үнийг зохиомлоор өсгөж, огцом зарах	Хөрөнгө оруулагч	Өндөр
Хуурамч платформ	Хуурамч бирж, хэтэвч үүсгэж, хөрөнгө хулгайлах	Хэрэглэгч	Маш өндөр

Эх сурвалж: Chainalysis (2024), FBI IC3 (2024), RUSI (2023)

Гол тоон үзүүлэлтүүд (N=200)

Кибер гэмт хэргийн өсөлт

7,56

445

2015: 17 → 2024: 7,560 тохиолдол

0

Санхүүгийн хохирол

67.2 тэрбум ₮

33.6×

2016: 2.0 → 2020: 67.2 тэрбум ₮

Интернет нэвтрэлт

82.0%

+71.8p p

2010: 10.2% → 2024: 82.0%

Хохирогчдын хувь

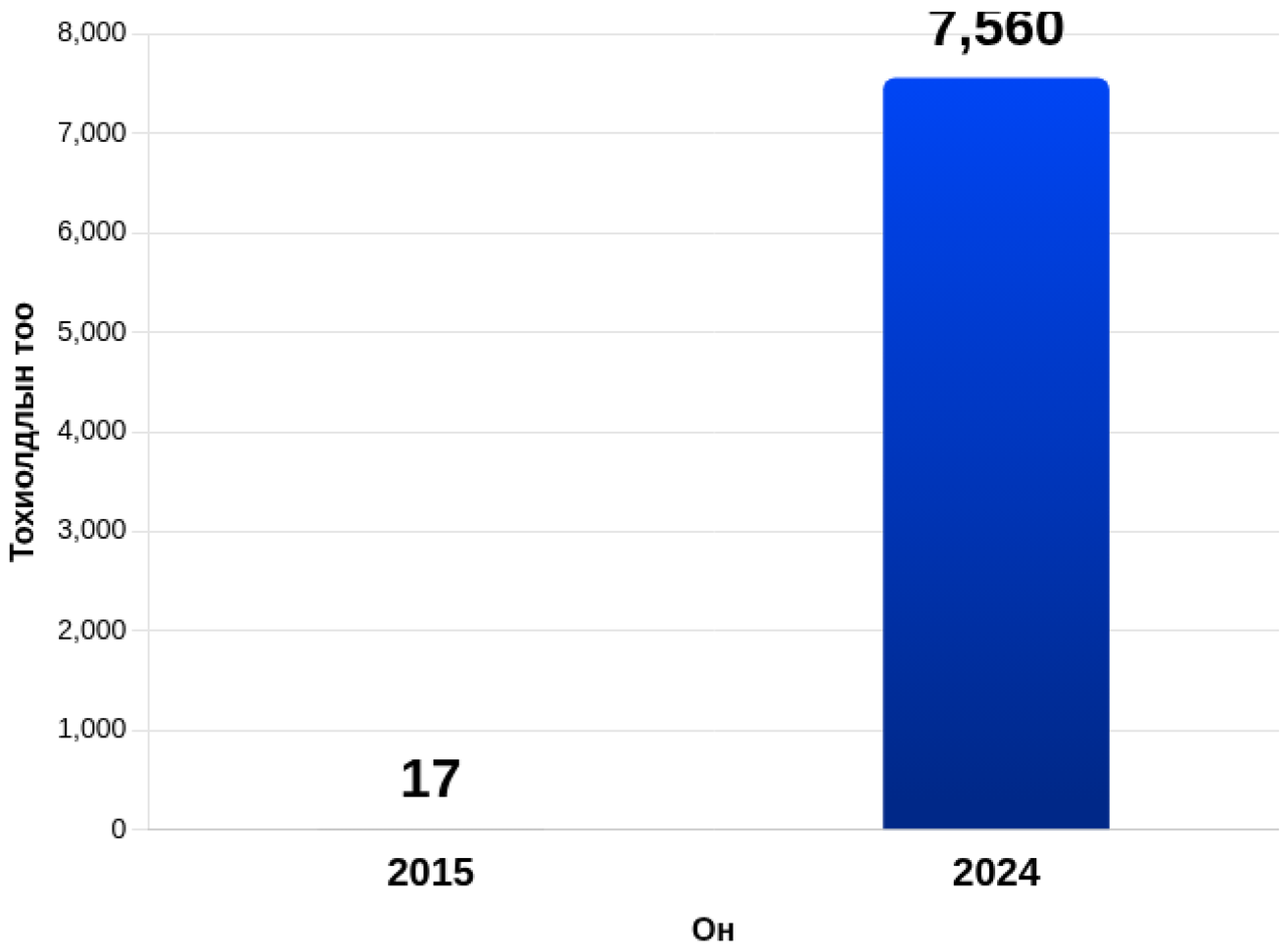
26.0% (52/200)

Мэдээлсэн: 21.2% (11/52)

21.2%

78.8% мэдээлээгүй

Монгол Улс: кибер гэмт хэргийн өсөлт (2015→2024)



Тохиолдлын өсөлт

445×

2015-2024 оны хооронд

2024 оны нийт тохиолдол

7,560

83% нь кибер залилангийн шинжтэй

2015 оны суурь түвшин: **17** тохиолдол

Эх сурвалж: Цагдаагийн ерөнхий газар, Монгол Улс (2015-2024)

Монгол Улсын тоон үзүүлэлт (2015–2024)

Хүснэгт 2.1: Кибер гэмт хэргийн динамик

2015	17	2.0	10.2
2016	342	5.9	21.4
2017	485	12.3	35.8
2018	728	23.7	48.2
2019	1,156	45.8	56.7
2020	1,420	67.2	65.3
2021	2,834	98.5	72.1
2022	4,567	134.2	76.8
2023	6,123	167.9	79.5

Эх сурвалж: Цагдаагийн ерөнхий газар (2024), Харилцаа холбооны зохицуулах хороо (2024)

445 дахин өсөлт

33.6 дахин өсөлт (хохирол, 2016-2020)

2015

2024

Монгол Улс: чиг хандлага ба бүтэц

Мэдээлэл алдагдал

2.3 сая иргэн

Хувийн мэдээлэл алдагдсан (2020-2021)

Кибер залилангийн бүтэц

- **Социал инженеринг: 35-40%**
- **OTP код хуурах: 25-30%**
- **Хуурамч хөрөнгө оруулалт: 20%**
- **Криптовалют залилан: 10-15%**

Эх сурвалж: Цагдаагийн ерөнхий газар, Монгол банк (2020-2024)

FATF үнэлгээ: Монгол Улсын замнал

Саарал жагсаалтад орсон

20/40 зөвлөмж хангалтгүй

12 сарын дотор гарсан

6 стратегийн дутагдал арилгасан

39/40 зөвлөмж нийцсэн

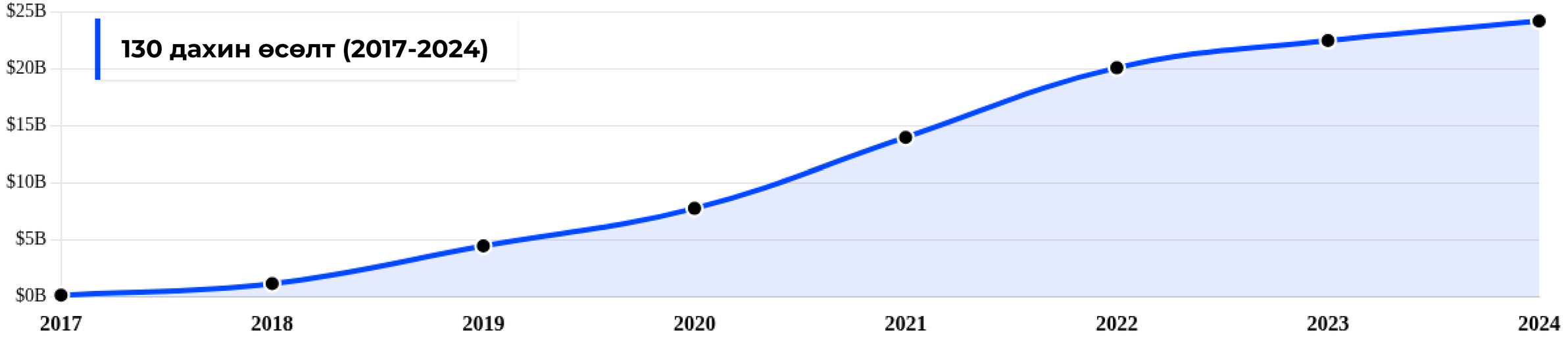
"Ихэнхдээ нийцсэн" статус

15

Зөвлөмж 15 (VASP зохицуулалт)

Статус: **"Хэсэгчлэн нийцсэн"** хэвээр байна

Дэлхийн крипто гэмт хэрэг: өсөлт ба жишиг кейсүүд



Danske Bank
$200B

Madoff
$65B

PlusToken
$2-3B

Судалгааны хөгжлийн 4 үе шат (2008–2025)

I үе шат

2008-2016

Онолын суурь

Nakamoto (2008)
Scheau et al. (2013)
Блокчейн технологи

II үе шат

2017-2019

Эмпирик судалгаа

FATF Зөвлөмж 15 (2019)
Weber et al. (2018)
AML/CFT стандарт

III үе шат

2020-2022

AI/ML дэвшил

Li et al. (2021)
GNN: 94.7% нарийвчлал
Graph Neural Network

IV үе шат

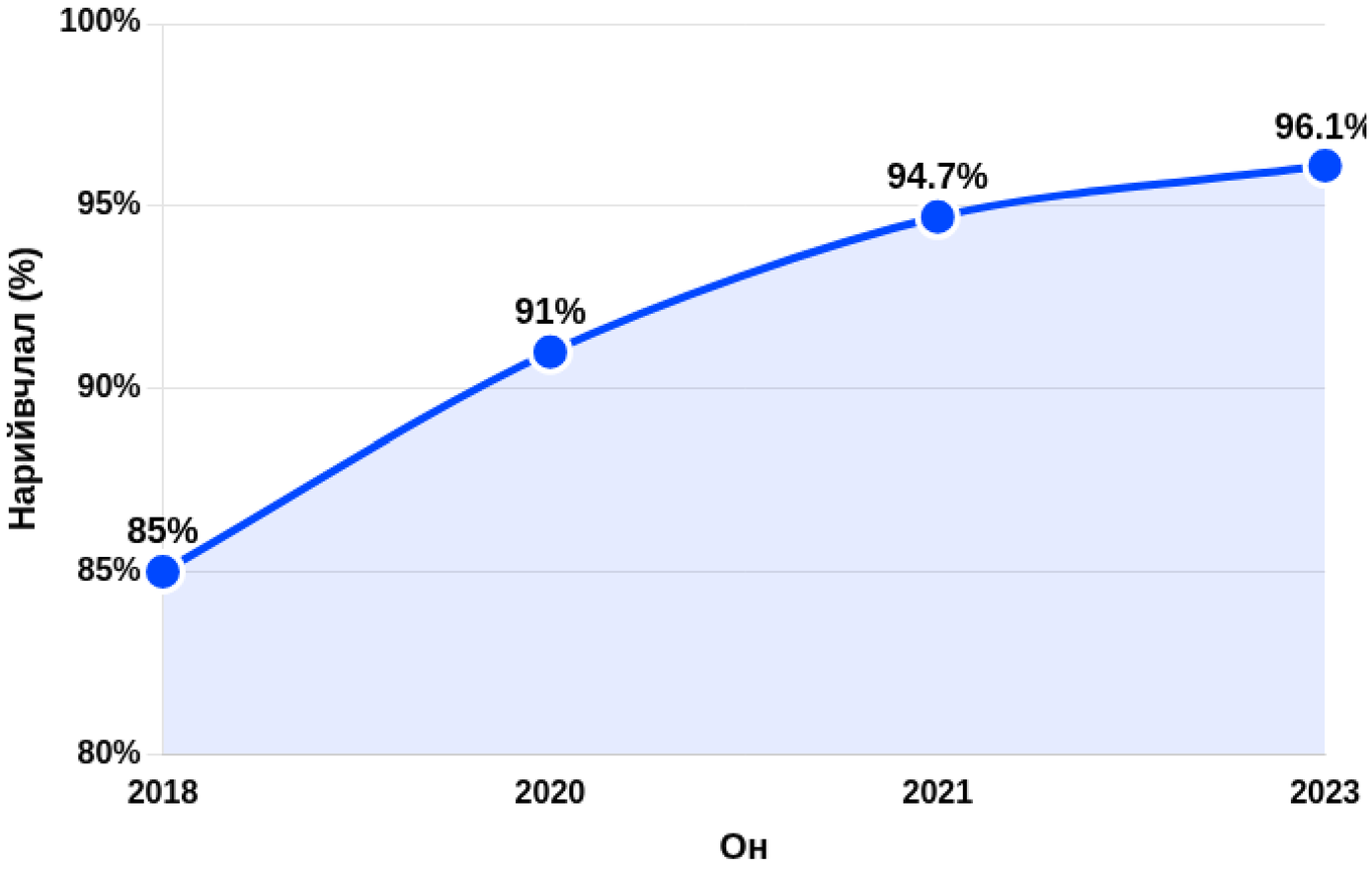
2023-2025

Transformer архитектур

Huang et al. (2023)
BERT4ETH: 96.1% нарийвчлал
Federated Learning

Гол дүгнэлт: AI/ML загваруудын нарийвчлал 2018-2023 онд 85.2%-аас 96.1% хүртэл сайжирсан. Transformer архитектур (BERT4ETH) нь Graph Neural Network-ээс илүү өндөр гүйцэтгэлтэй.

AI/ML загваруудын нарийвчлалын хувьсал



- **Random Forest (2018)**

  Анхны машин сургалтын загвар, 85% нарийвчлал

- **XGBoost (2020)**

  Сайжруулсан gradient boosting, 91% нарийвчлал

- **GNN (2021)**

  Graph Neural Network, блокчейн гүйлгээний сүлжээ шинжилгээ, 94.7% нарийвчлал

- **BERT4ETH (2023)**

  Transformer архитектур, Ethereum гүйлгээний контекст ойлголт, 96.1% нарийвчлал

Гол дүгнэлт

5 жилийн хугацаанд AI/ML загваруудын нарийвчлал 11.1 пунктээр сайжирч, крипто залилан илрүүлэх чадвар эрс нэмэгдсэн

Олон улсын AML/CFT системийн харьцуулалт

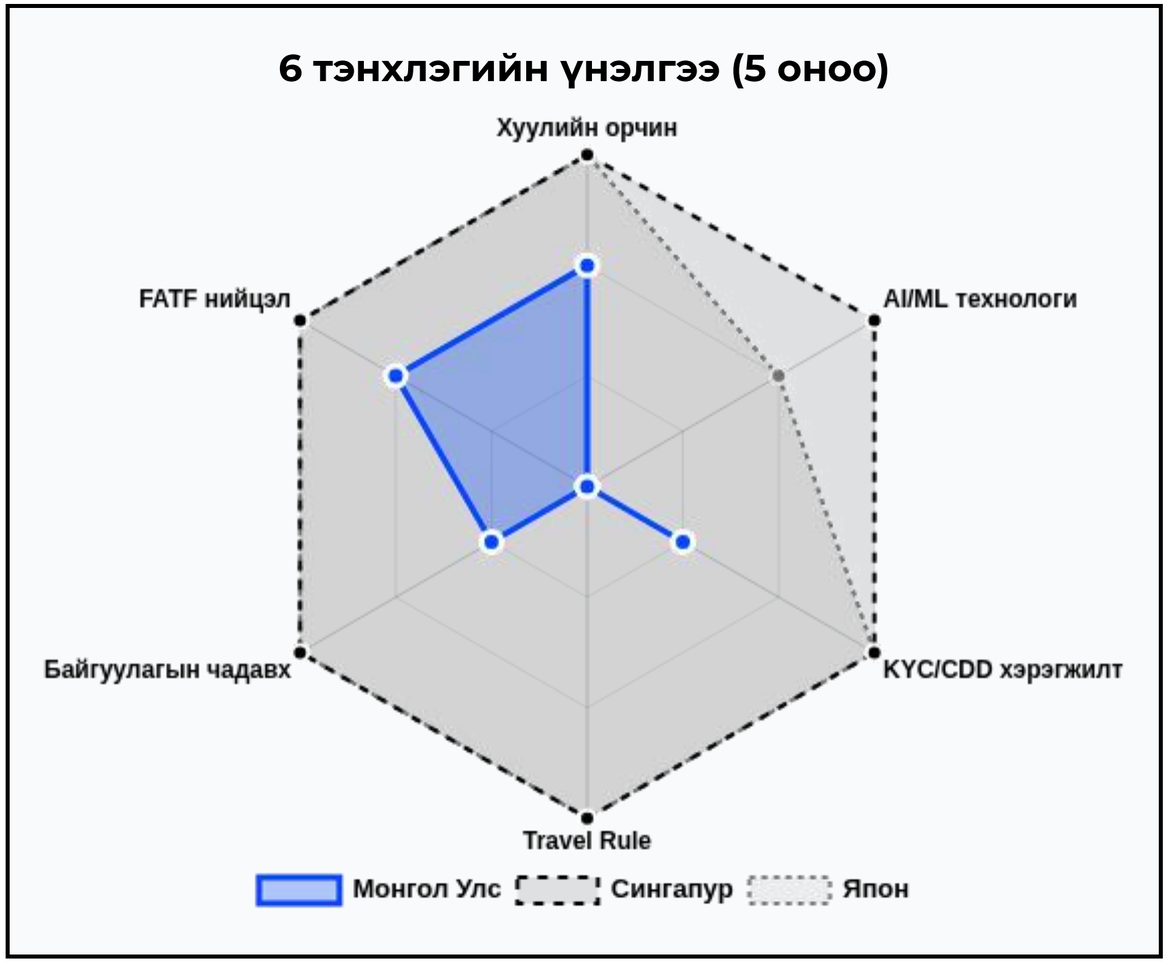
Сингапур	MAS	Risk-Based Approach хяналт, лиценз	AI/ML мониторинг, Chainalysis, Elliptic	**Давуу:** Дэвшилтэт технологи, олон улсын стандарт **Сул:** Жижиг зах зээл, өндөр зардал
БНСУ	FSC, DAXA	Real-name account заавал, ISMS гэрчилгээ	KYC автоматжуулалт, ISMS-P сертификат	**Давуу:** Хэрэглэгч хамгаалалт өндөр, банк холбоос **Сул:** DeFi хязгаарлалт, хатуу зохицуулалт
Япон	FSA, JVCEA	Cold wallet заавал, Travel Rule	Multisig хадгалалт, hot wallet хязгаарлалт	**Давуу:** Хадгалалтын аюулгүй байдал өндөр **Сул:** Хэт нарийн шаардлага, зардал өндөр
Хонг Конг	SFC	2023 VASP лиценз дэглэм	Блокчейн аналитик, KYC/AML платформ	**Давуу:** Санхүүгийн төв, олон улсын хүлээн зөвшөөрөл **Сул:** Шинэ дэглэм, туршлага хомс
ЕХ/MiCA	EBA, ESMA	MiCA нэгдмэл хүрээ (2024)	RegTech платформ, AI-based AML мониторинг	**Давуу:** 27 улсын нэгдсэн зах зээл, тодорхой **Сул:** Хэрэгжилт удаан, улс бүрийн зөрүү
Монгол Улс	**МБ, ФЗХ**	**VASP лиценз эхэлсэн (2024)**	**Уламжлалт KYC/CDD, гарын авлага**	**Давуу: Хуулийн суурь бүрдсэн, FATF 39/40** **Сул: AI/ML технологи байхгүй, мэргэжилтэн дутмаг**

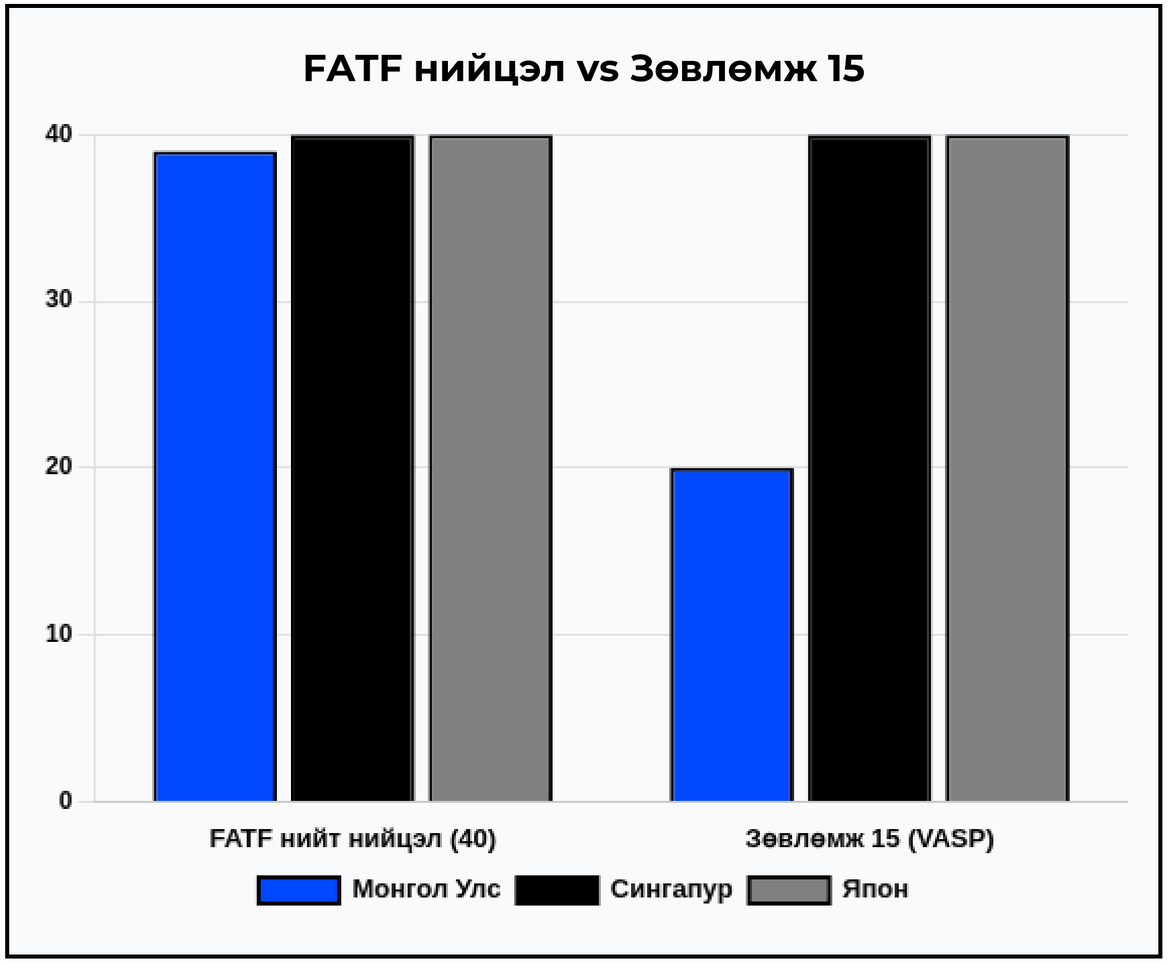
Эх сурвалж: Хүснэгт 4.1 (FATF, MAS, FSC, FSA, SFC, EBA 2023-2024)

Технологийн хэрэгжилт: 6 давтагдсан технологи

	Давтамж		
AI/ML аномали илрүүлэх	**5/5**	BERT4ETH 96.1%, GNN 94.7%	**Өндөр нарийвчлал** / Хар хайрцаг
KYC/CDD автоматжуулалт	**5/5**	Хүний алдаа 70%+ буурсан	**Хурдан боловсруулалт** / Нууцлалын эрсдэл
Блокчейн аналитик	**4/5**	$24.2B-ийн 40%+ мөрдсөн	**Гүйлгээний ул мөр** / Mixer хязгаар
Travel Rule	**4/5**	Мөнгө угаалт 28% буурсан	**Хил дамнасан хяналт** / DeFi хүндрэлтэй
Cold wallet/Multisig	**3/5**	Хакинг 67% буурсан	**Эрсдэл буурна** / Хурдан гүйлгээнд саад
Federated Learning	**2/5**	89.3% нарийвчлал, GDPR	**Нууцлал хамгаалалт** / Техникийн шаардлага

AML/CFT 6 тэнхлэгийн үнэлгээ ба FATF нийцэл





Дүгнэлт: Монгол Улс FATF нийт нийцэлд 39/40 хүрсэн боловч Зөвлөмж 15 (VASP) хэсэгчлэн нийцсэн. Гол зөрүү нь AI/ML технологи болон Travel Rule-ийн хэрэгжилтэд оршиж байна.

Монгол Улсад хэрэгжүүлэх боломжийн үнэлгээ

Шалгуур үзүүлэлт	Одоогийн байдал / Нотолгоо	Эрсдэл / Бэрхшээл
Хуулийн суурь	• МУЛУ хуулиар VASP зохицуулалт • FATF үнэлгээ: 39/40 зөвлөмж нийцсэн	• Зөвлөмж 15 хэсэгчлэн нийцсэн • Хэрэгжилтийн чадавх хязгаартай
Технологийн дэд бүтэц	• Интернет нэвтрэлт: 82.0% • Мобайл банкны хэрэглэгч: 6.4 сая	• Дижитал ур чадварын зөрүү том • AI/ML дэд бүтэц хөгжөөгүй
Зохицуулагчийн чадавх	• ФЗХ, МБ AML/CFT эрх бүхий • Egmont Group гишүүн (2007)	• AI/ML мэргэжилтэн дутагдалтай • Байгууллага хоорондын уялдаа сул
Олон улсын баталгаа	• Сингапур, БНСУ туршлага судлах • FATF, Egmont сүлжээний гишүүн	• Зах зээлийн хэмжээ жижиг • Хөрөнгө оруулалт хязгаартай

- **Дүгнэлт:** Хуулийн суурь бий боловч технологи, хүний нөөц, байгууллагын чадавхийг бэхжүүлэх шаардлагатай

Ye шаттай хэрэгжилтийн замнал (2025-2031)

1 2 3

Богино хугацаа

2025-2027

- Multi-Factor Authentication заавал болгох
- KYC/CDD автоматжуулалт
- Фишинг/OTP боловсролын кампанит ажил
- Travel Rule бүрэн хэрэгжилт
- VASP лицензийн хүрээ тодорхойлох

Дунд хугацаа

2027-2030

- AI/ML мониторинг систем
- Блокчейн аналитик платформ (Chainalysis, Elliptic)
- ФЗХ-МБ нэгдсэн мэдээллийн платформ
- Cold wallet/Multisig заавал болгох
- Байгууллага хоорондын мэдээлэл солилцоо сайжруулах

Урт хугацаа

2030-2031+

- Digital Asset Authority байгуулах (MiCA, JVCEA загвар)
- Federated Learning сүлжээнд нэгдэх (Egmont, Interpol Cyber)
- Бүс нутгийн AML/CFT хамтын ажиллагаа
- FATF Зөвлөмж 15 бүрэн нийцэл

Эмпирик судалгаа: арга зүй ба хүн ам зүй

Судалгааны арга зүй

Түүврийн хэмжээ	N = 200
Хэмжүүр	Likert 5 шатлалт
Асуулгын тоо	50 асуулт
Статистик арга	Cronbach's α, χ^2, t-test, ANOVA, Pearson r, регресс, PCA

Найдвартай байдал (Cronbach's α)

Мэдлэгийн түвшин	**α = 0.845**
Эрсдэлийн ойлголт	**α = 0.833**

Тайлбар: α > 0.80 нь өндөр найдвартай байдлыг илтгэнэ

Хүн ам зүйн үзүүлэлтүүд

Үзүүлэлт	Бүлэг	Тоо	Хувь
Хүйс	Эрэгтэй	95	**47.5%**
	Эмэгтэй	105	**52.5%**
Насны бүлэг	18-35 нас	127	**63.5%**
	36-50 нас	58	**29.0%**
	51+ нас	15	**7.5%**
Боловсролын түвшин	Бакалавр	112	**56.0%**
	Магистр+	67	**33.5%**
	Бусад	21	**10.5%**

Институцийн чадавх ба технологийн шийдэл

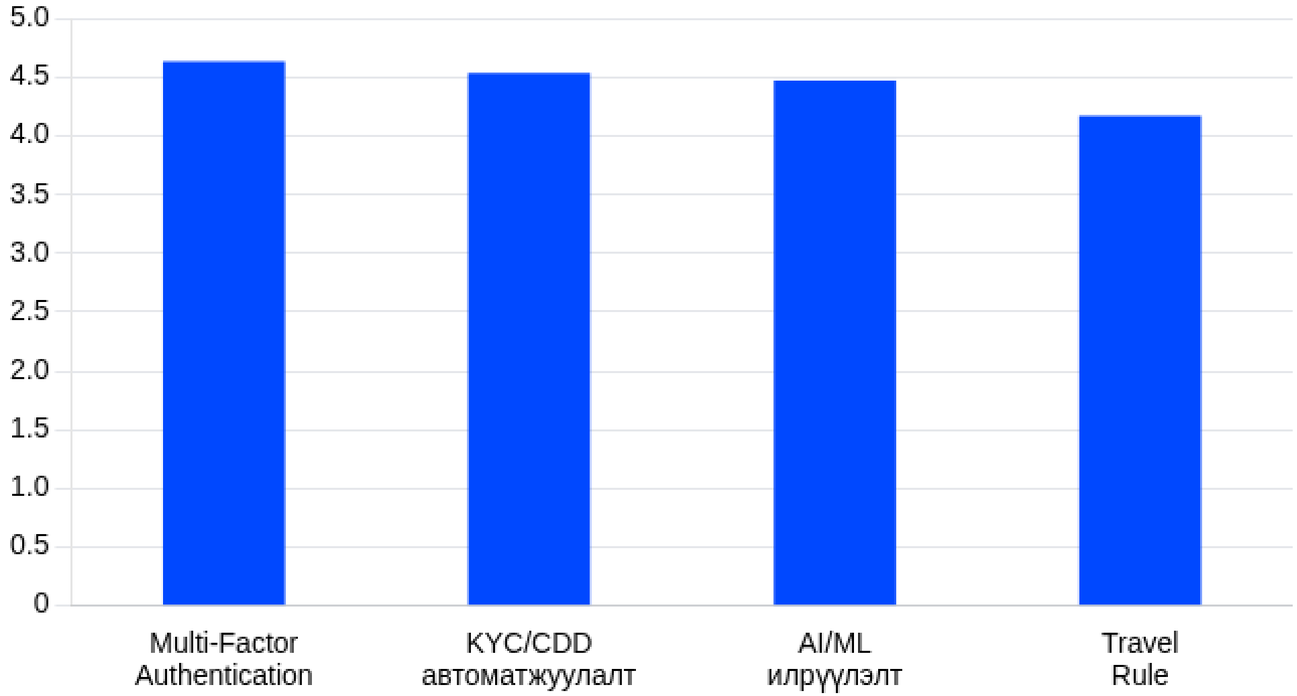
Институцийн чадавх (1-5 хэмжүүр)

- **Банкны дотоод хяналт:** M=3.375 (хамгийн өндөр)
- **Байгуулага хоорондын мэдээлэл солилцоо:**

  (хамгийн доогуур)

  ← RUSI 2023 баталгаажуулсан
- **VASP дотоод комплаенс:** M=2.700

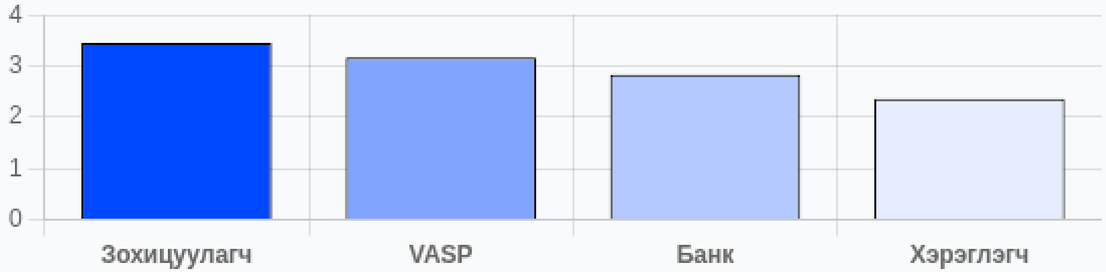
Технологийн шийдлийн зөвшөөрөл (бүгд ≥4.0)



ANOVA, корреляци ба регресс шинжилгээ

Оролцогч талуудын мэдлэгийн оноо (ANOVA)

F(3,196)=51.935, p<0.001, η^2=0.443 (том effect)



Bonferroni: Зохицуулагч ↔ Хэрэглэгч зөрүү хамгийн том (p<0.001)

Олон хувьсагчийн регресс

R^2=0.100, F(6,193)=3.587, p=0.0022**

- **TECH_mean:** β=0.244, p=0.0064** (хамгийн хүчтэй)
- **INST_mean:** β=0.189, p=0.0103*

→ Технологи ба институцийн чадавх нь итгэлцлийг нэмэгдүүлдэг

Pearson корреляци

KNOW ↔ TECH — хамгийн өндөр эерэг — **r = 0.664**

KNOW ↔ BEH — **r = 0.635**

KNOW ↔ RISK — **r = 0.562**

→ Мэдлэг нь технологи хүлээн зөвшөөрөх, зан төлөв, эрсдэлийн ойлголтыг тодорхойлдог

Кибер залиланд өртсөн байдал ба статистик шинжилгээ

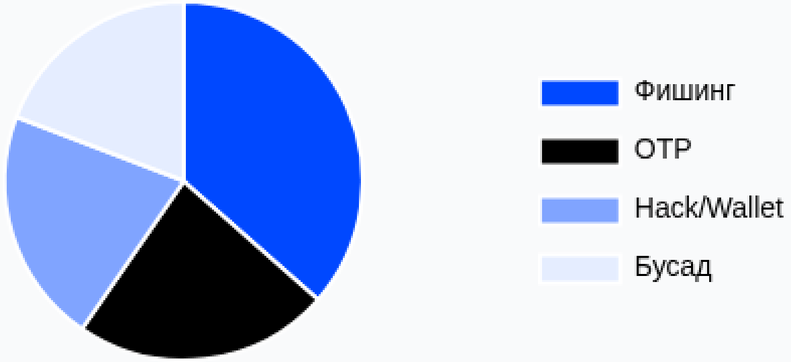
Нийт хохирогч

26%
(52/200)

Мэдээлсэн

21.2%
Underreporting асуудал

Хохирлын хэлбэр



χ^2-тест (Chi-Square)

Хүйс, оролцогч тал, насны бүлэг × Хохирол **p > 0.05 (ns)**

Дүгнэлт: **Бүх насны бүлэг эрсдэлд өртөмтгий**

t-test (Итгэлцлийн түвшин)

Бүлэг	Дундаж (M)	t-утга	p-утга	Effect size (d)
Хохирсон	**2.683**	-7.951	**< 0.001**	-1.258 (том)
Хохироогүй	**3.113**			

Дүгнэлт: **Хохирогчид системд итгэл алдсан**

Эрсдэлийн ойлголт ба мэдлэгийн түвшин

Эрсдэлийн ойлголтын эрэмбэ (Likert 1-5)

Мэдлэгийн түвшин

Боловсролын шаардлага

FATF Зөвлөмж 15-ын талаарх мэдлэг хамгийн доогуур (M=2.075) байгаа нь салбарын хэмжээнд тусгай сургалт, мэдээлэл түгээх зайлшгүй шаардлагатайг харуулж байна.

Дүгнэлт ба бодлогын зөвлөмж

- Фишинг/OTP зонхилох (социал инженеринг 35-40%, OTP 25-30%)
- VASP дотоод комплаенс ба байгуулага хоорондын мэдээлэл солилцоо хамгийн сул холбоос (M=2.5-2.7, RUSI 2023 баталгаажуулсан)
- Хэрэглэгчийн мэдлэг хамгийн доогуур (M=2.359), FATF Зөвлөмж 15 мэдлэг 2.075 (боловсролын шаардлага)
- Технологи (β=0.244, p=0.0064**) ба институцийн чадавх (β=0.189, p=0.0103*) итгэлцлийг нэмэгдүүлдэг
- Underreporting ноцтой асуудал (26% хохирогч, зөвхөн 21.2% мэдээлсэн, 78.8% нуусан)
- Кибер гэмт хэрэг 445 дахин өссөн (2015: 17 → 2024: 7,560), санхүүгийн хохирол 33.6 дахин өссөн

Бодлогын зөвлөмж

2025-2027 **Богино хугацаа**

- Multi-Factor Authentication заавал (E6, M=4.63)
- KYC/CDD автоматжуулалт (E2, M=4.54)
- Фишинг/OTP боловсролын кампанит ажил
- Travel Rule хэрэгжүүлэх (FATF Зөвлөмж 16)

2027-2030 **Дунд хугацаа**

- AI/ML аномали илрүүлэх систем (E1, M=4.47)
- Блокчейн аналитик платформ (Chainalysis/Elliptic)
- ФЗХ-МБ нэгдсэн мэдээллийн платформ

2030+ **Урт хугацаа**

- Digital Asset Authority (MiCA/JVCEA загвар)
- Federated Learning сүлжээ (Egmont/Interpol Cyber)
- Олон улсын стандартад нийцсэн зохицуулалт

Ном зүй

- *AKIpress. (2024). Mongolia records 7,560 cyber crimes in 2024. AKIpress News Agency.*
- *Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211.*
- *Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213–238.*
- *Chainalysis. (2020–2024). The Chainalysis Crypto Crime Report (2020, 2021, 2022, 2023, 2024 дугаарууд). Chainalysis Inc.*
- *ComplyAdvantage. (2024). Cryptocurrency regulations in Asia. ComplyAdvantage Insights.*
- *Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of computer technology. MIS Quarterly, 13(3), 319–340.*
- *FATF. (2019). Guidance for a risk-based approach to virtual assets and VASPs. Financial Action Task Force.*
- *FATF. (2021). Updated guidance for a risk-based approach to virtual assets and VASPs. Financial Action Task Force.*
- *FATF. (2022). Mutual evaluation report: Mongolia. Financial Action Task Force.*
- *FATF. (2024). Virtual assets: Targeted update on implementation of FATF standards. Financial Action Task Force.*
- *Financial Regulatory Commission of Mongolia (FRC). (2023). Annual AML/CFT Compliance Report. Улаанбаатар.*
- *Global Press Journal. (2023). Scams Skyrocket as Mongolia Goes Online.*
- *Huang, W., Gao, Z., & Zhou, X. (2023). BERT4ETH: A pre-trained transformer for Ethereum fraud detection. ACM Web Conference 2023, 2189–2197.*
- *IJEBMR. (2022). Money laundering risks and banking sector implications in emerging economies.*
- *ISO. (2018). ISO 31000:2018 Risk management — Guidelines. ISO.*
- *ITU. (2024). ICT Development Index 2024. International Telecommunication Union.*
- *Li, J., Guo, B., & Chen, X. (2021). Detection of illicit accounts over Ethereum blockchain using GNN. IEEE Transactions on Network and Service Management, 18(4).*
- *MDPI. (2025). AI and financial fraud prevention: Bibliometric lens. Journal of Risk and Financial Management, 18(6), 323.*
- *Mongolia Inc. (2020). Mongolia and FATF's grey list. https://mongoliainc.com/5712/*
- *Möser, M., Böhme, R., & Breuker, D. (2013). An empirical analysis of traceability in the Bitcoin blockchain. Financial Cryptography 2015.*
- *Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf*
- *NIST. (2024). Cybersecurity Framework 2.0. National Institute of Standards and Technology.*
- *Osterrieder, J. et al. (2022). Enhancing security in blockchain networks: Anomalies, frauds, and detection. arXiv:2402.11231.*
- *Rahman, M.A., & Asyhari, T. (2022). Blockchain and ML for fraud detection: Privacy-preserving approach. arXiv:2210.12609.*
- *RUSI. (2023). Institutional VASPs: A guide to AML/CFT compliance. Royal United Services Institute.*
- *Scheau, M.C. (2013). Bitcoin network and cybercrime. Journal of Financial Crime, 20(2).*
- *Scheau, M.C. (2017). Cryptocurrencies and cybercrime: New laundering frontiers. CyberLeninka.*
- *Vasek, M., & Moore, T. (2015). There's no free lunch, even using Bitcoin. Financial Cryptography.*
- *World Bank. (various years). Stolen Asset Recovery (StAR) Initiative reports.*

Анхаарал хандуулсанд баярлалаа.