Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university



Ақпаратты қорғау аппараттық құралдары: HSM және TPM

Ақпараттық қауіпсіздіктің өзекті маңызы

Қазіргі цифрлық дәуірде ақпараттық қауіпсіздік кез келген ұйым мен мемлекет үшін стратегиялық маңызға ие болып отыр. Киберқауіпсіздік сарапшылары мен халықаралық ұйымдардың зерттеулері көрсеткендей, ақпараттық шабуылдардың күрделілігі мен саны жыл сайын өсуде.

Kaspersky компаниясының 2025 жылғы деректері бойынша, ақпараттық шабуылдар саны бір жылда 35% өскен. Қазақстан Республикасы үшін де бұл мәселе өзекті болып табылады – ақпараттық қауіпсіздік ұлттық приоритетке айналды және мемлекеттік деңгейде қолдауға ие.

35%

Шабуылдар өсімі

2025 жылы тіркелген

$4.5M

Орташа шығын

Бір инциденттен

Ақпаратты қорғау аппараттық құралдары дегеніміз не?

Аппараттық қауіпсіздік құралдары – бұл ақпаратты заңсыз қолжетімділіктен, бұрмалаудан, ұрлаудан және жоюдан қорғау үшін арнайы әзірленген физикалық жабдықтар мен құрылғылар. Программалық қорғаныстан айырмашылығы, аппараттық шешімдер жоғары деңгейдегі физикалық қауіпсіздік пен өнімділікті қамтамасыз етеді.

Аппараттық деңгей

Физикалық қорғаныс механизмдері арқылы шабуылдарға қарсы тұрақтылық

Криптографиялық функциялар

Кілттерді қауіпсіз генерациялау, сақтау және басқару мүмкіндігі

Сертификаттау

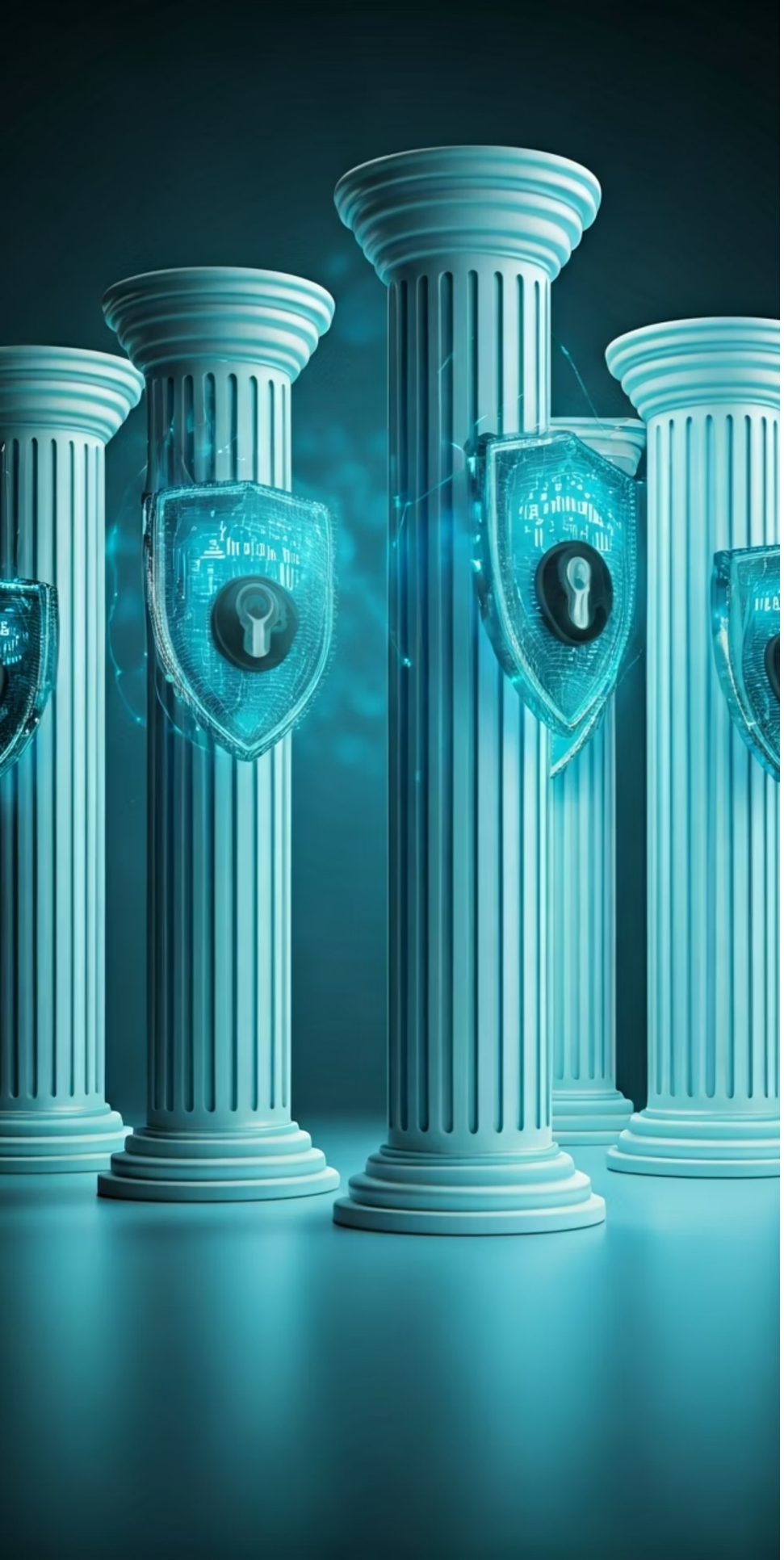
Халықаралық стандарттар мен сертификаттарға сәйкестік

HSM (Hardware Security Module) және TPM (Trusted Platform Module) – қазіргі заманғы ең сенімді және кеңінен қолданылатын аппараттық қорғаныс шешімдері болып табылады.

Ақпарат ағып кетуінің салдары

Ірі компаниялар мен мемлекеттік мекемелер үшін ақпараттық инциденттер миллиондаған доллар шығынға әкелуде. IBM Security компаниясының зерттеуі бойынша, орташа деректер ағып кету инцидентінің құны 4.5 миллион доллардан асады.

Қаржылық шығындардан басқа, ұйымдардың беделіне зиян келуі, клиенттердің сенімін жоғалту және құқықтық салдарлар да туындайды. Сондықтан аппараттық қорғаныс шешімдеріне инвестиция салу стратегиялық қажеттілік болып табылады.



Ақпаратты қорғаудың негізгі қағидалары

Ақпараттық қауіпсіздік жүйесі үш негізгі тірекке сүйенеді: қолжетімділік, тұтастық және құпиялылық. Бұл қағидалар CIA триадасы (Confidentiality, Integrity, Availability) ретінде белгілі және кез келген қауіпсіздік жүйесінің іргетасын құрайды.

Қауіпсіздік саясаты мен кепілдік жүйесі осы қағидаларды практикада іске асыруға мүмкіндік береді. Ұйым деңгейінде әзірленген саясаттар, регламенттер және технологиялық шешімдер кешенді қорғанысты қамтамасыз етеді.

Ақпараттық қауіпсіздіктің үш негізгі қағидасы

Қолжетімділік

Рұқсат етілген пайдаланушылар үшін ақпарат пен ресурстарға кез келген уақытта дұрыс қол жеткізу мүмкіндігін қамтамасыз ету

- Жүйенің үздіксіз жұмысы
- Резервтік көшірмелер
- Қалпына келтіру жоспары



Тұтастық

Ақпараттың толықтығын, дұрыстығын және өзгермей сақталуын қамтамасыз ету, рұқсатсыз өзгерістерден қорғау

- Өзгерістерді бақылау
- Цифрлық қолтаңбалар
- Хэш-функциялар

Құпиялылық

Ақпаратты рұқсатсыз қолжетімділіктен қорғау, тек уәкілетті пайдаланушыларға ғана қол жеткізуге рұқсат беру

- Шифрлау механизмдері
- Қолжетімді басқару
- Аутентификация

Ақпаратты қорғау жүйесінің құрылымы

Кешенді ақпараттық қауіпсіздік жүйесі үш негізгі компоненттен тұрады: ұйымдастырушылық, программалық және аппараттық құралдар. Олардың әрқайсысы өз рөлін атқарады және тек кешенді қолданғанда ғана максималды тиімділікке жетуге болады.

Аппараттық құралдардың басты артықшылығы – физикалық деңгейде қауіпсіздікті қамтамасыз ету, жоғары өнімділік және программалық шабуылдарға төзімділік. Олар криптографиялық операцияларды жылдам орындайды және кілттерді қауіпсіз сақтайды.

Ұйымдастырушылық құралдар

Саясаттар, регламенттер, нұсқаулықтар, қызметкерлерді оқыту

Программалық құралдар

Антивирустар, брандмауэрлер, DLP жүйелері

Аппараттық құралдар

HSM, TPM, биометриялық сканерлер, токендер

Қорғаныстың эшелонды құрылымы

Заманауи ақпараттық жүйелерде қорғаныс бірнеше қабаттан тұрады. Аппараттық қабат – ең төменгі және сенімді деңгей, ол барлық жоғары қабаттар үшін негіз болады. Программалық қабат икемділік пен функционалдық мүмкіндіктерді қамтамасыз етеді. Ұйымдастырушылық қабат адами факторды басқарады және қауіпсіздік мәдениетін қалыптастырады.

Осы үш қабаттың үйлесімді жұмысы ғана толыққанды қорғанысты қамтамасыз ете алады. Аппараттық құралдар физикалық қауіпсіздік пен өнімділікті береді, ал программалық және ұйымдастырушылық шаралар икемділік пен бейімделуді қамтамасыз етеді.



HSM (Hardware Security Module) дегеніміз не?

HSM (Hardware Security Module) – бұл криптографиялық кілттерді қауіпсіз генерациялау, сақтау және басқару үшін арнайы әзірленген аппараттық криптографиялық модуль. Ол физикалық қауіпсіздік механизмдерімен қорғалған және криптографиялық операцияларды орындауға оптимизацияланған.

HSM құрылғылары банктер, қаржы институттары, мемлекеттік мекемелер және ірі корпорацияларда қолданылады. Олар өте құнды криптографиялық активтерді қорғауға және жоғары деңгейдегі қауіпсіздікті қажет ететін операцияларды орындауға арналған.

HSM-нің негізгі функциялары

Кілттерді генерациялау

Криптографиялық кілттерді қауіпсіз генерациялау, кездейсоқ сандар генераторын пайдалану арқылы жоғары сапалы кілттер жасау

Қауіпсіз сақтау

Кілттерді физикалық қауіпсіздік механизмдерімен қорғалған ортада сақтау, экспорттауға жол бермеу

Кілттерді басқару

Кілттердің өмірлік циклін басқару: жасау, белсендіру, архивтеу, жою процестерін автоматтандыру

Шифрлау операциялары

Деректерді шифрлау және дешифрлау, симметриялық және асимметриялық алгоритмдерді қолдау

Цифрлық қолтаңба

Құжаттарға және транзакцияларға электрондық цифрлық қолтаңба қою, аутентификация мен тұтастықты қамтамасыз ету

Сертификаттарды қолдау

PKI инфрақұрылымын қолдау, сертификаттарды басқару және өңдеу функциялары

HSM-нің басты артықшылықтары

Аппараттық деңгейдегі қорғаныс

- Физикалық шабуылдарға төзімділік
- Тампердің (бұзудың) автоматты анықталуы
- Логикалық шабуылдарға қарсы қорғаныс
- Кілттерді экспорттаудың мүмкін еместігі

Жоғары өнімділік

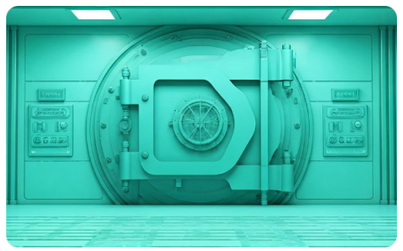
- Арнайы криптопроцессорлар
- Параллельді операцияларды орындау
- Мыңдаған транзакцияны секундына өңдеу
- Минималды кешігу уақыты

Сертификатталған қауіпсіздік

- FIPS 140-2/140-3 сертификаттары
- Common Criteria стандарттары
- EAC сертификациясы
- Халықаралық қауіпсіздік талаптары

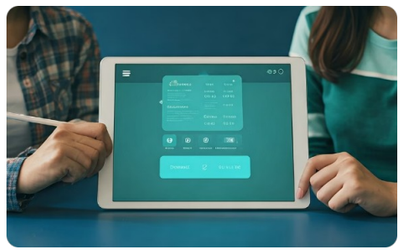
HSM құрылғылары ең жоғары деңгейдегі қауіпсіздікті қажет ететін салаларда қолданылады. Олар физикалық және логикалық шабуылдарға қарсы тұру үшін арнайы әзірленген және халықаралық стандарттарға сәйкес сертификатталған.

HSM қолдану салалары



Банктер мен қаржы институттары

Банктік транзакцияларды қорғау, төлем карталарын шығару, PIN-кодтарды басқару, банкаралық трансферттерді қауіпсіз өңдеу



Электрондық үкімет

Мемлекеттік қызметтердің қауіпсіздігі, электрондық құжаттарға қол қою, азаматтардың деректерін қорғау



ЭЦҚ инфрақұрылымы

Сертификаттау орталықтары, электрондық цифрлық қолтаңбаларды басқару, PKI жүйелерін қолдау



Телекоммуникациялар

Байланыс арналарын шифрлау, абоненттік деректерді қорғау, аутентификация жүйелері

Қазақстандағы HSM қолдану тәжірибесі



«Ұлттық ақпараттық технологиялар» АҚ

Қазақстанда HSM технологиясының ең ірі қолданушысы – «Ұлттық ақпараттық технологиялар» АҚ (ҰАТ). Компания республикалық ЭЦҚ инфрақұрылымын басқарады және мемлекеттік органдар мен бизнес үшін электрондық цифрлық қолтаңба қызметтерін көрсетеді.

ҰАТ-тың HSM құрылғылары миллиондаған сертификаттарды басқаруға және күніне жүздеген мыңдаған ЭЦҚ операцияларын өңдеуге қабілетті. Бұл жүйелер мемлекеттік құпия ақпаратты қорғауда да маңызды рөл атқарады.

ҰАТ инфрақұрылымындағы HSM жүйелері FIPS 140-2 Level 3 сертификатына ие және ең жоғары деңгейдегі қауіпсіздікті қамтамасыз етеді.

HSM құрылғысының ішкі архитектурасы

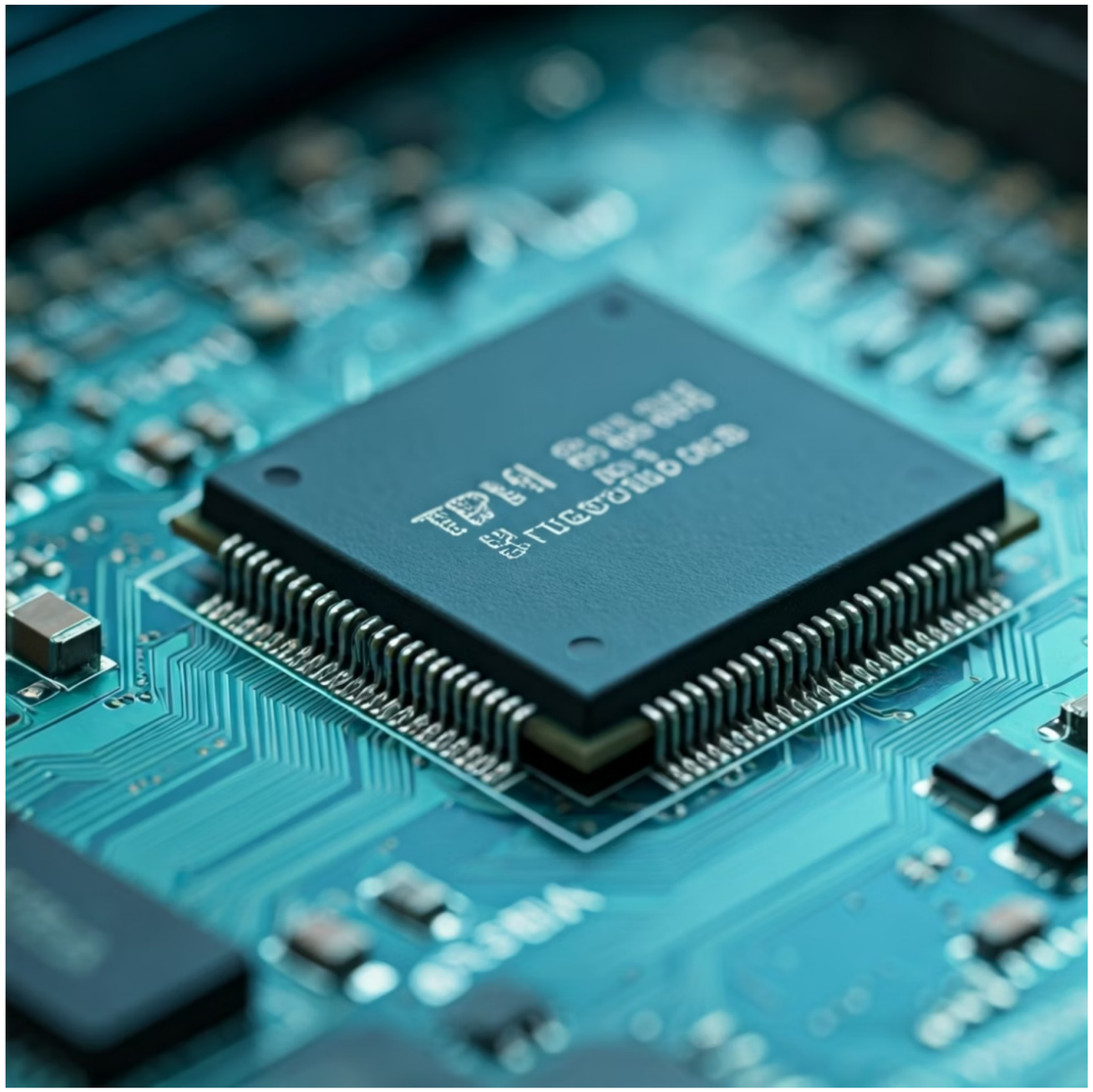
HSM модулінің ішінде арнайы криптопроцессорлар, қорғалған жад және физикалық қауіпсіздік механизмдері орналасқан. Құрылғы корпусы тамперге қарсы қорғанышпен жабдықталған – кез келген физикалық араласу әрекетін анықтайды және автоматты түрде кілттерді жояды.

Криптографиялық операциялар арнайы процессорларда орындалады, бұл өте жоғары өнімділікті қамтамасыз етеді. Кілттер ешқашан құрылғыдан тыс шықпайды және барлық операциялар HSM ішінде орындалады.

TPM (Trusted Platform Module) дегеніміз не?

TPM (Trusted Platform Module) – бұл компьютердің аналық тақтасына тікелей интеграцияланған немесе дискретті микросхема ретінде орнатылған қауіпсіздік модулі. Ол платформа деңгейінде сенімділікті қамтамасыз етеді және құрылғының бүтіндігін растайды.

TPM технологиясы Trusted Computing Group (TCG) консорциумы әзірлеген және қазір көптеген лаптоптар мен десктоп компьютерлерде стандартты болып табылады. Windows 11 операциялық жүйесі TPM 2.0 болуын міндетті талап етеді.



TPM-нің негізгі функциялары мен мүмкіндіктері

01

Құпия кілттерді сақтау

TPM чипінде криптографиялық кілттер мен сертификаттарды қауіпсіз сақтау, оларды программалық шабуылдардан қорғау

02

Платформа күйін өлшеу (Attestation)

BIOS, жүктеуші және операциялық жүйенің бүтіндігін тексеру, бұзылмағандығын растау

03

Қауіпсіз жүктеу (Secure Boot)

Тек расталған программалық қамтамасыз етуді жүктеуге рұқсат беру, зиянды кодтардың іске қосылуын болдырмау

04

Құрылғы аутентификациясы

Желіде құрылғының сәйкестігін растау, сенімді платформа екенін дәлелдеу

05

Деректерді шифрлау

BitLocker және басқа шифрлау технологияларымен біріктіріліп жұмыс істеу

TPM технологиясының артықшылықтары

Құрылғы деңгейінде қауіпсіздік

Аппараттық деңгейде енгізілген қорғаныс механизмдері программалық шабуылдарға төзімді. TPM чипі операциялық жүйеден тәуелсіз жұмыс істейді және зиянды программалар оған қол жеткізе алмайды.

Платформа сенімділігі

Жүктеу процесінің әрбір кезеңін бақылау арқылы платформаның бұзылмағанын және сенімді екенін растау мүмкіндігі. Бұл rootkit және bootkit түріндегі зиянды программаларды анықтауға көмектеседі.

Кілттердің қауіпсіздігі

Криптографиялық кілттер TPM чипінен ешқашан шықпайды және программалық жолмен экспорттауға болмайды. Бұл фишинг және басқа да әлеуметтік инженерия әдістеріне қарсы қорғанысты күшейтеді.

Бұзылуды анықтау

Аппараттық немесе программалық деңгейде бұзылу әрекеттерін анықтау және тиісті шаралар қабылдау мүмкіндігі. TPM өзгерістерді тіркейді және ескертулер жібереді.

TPM қолдану салалары және сценарийлері

- **Корпоративтік лаптоптар**

  Қызметкерлердің жұмыс құрылғыларын қорғау, деректердің ағып кетуін болдырмау

- **Жұмыс станциялары**

  Өндіріс ортасында құпия деректерді өңдейтін стационарлық компьютерлерді қорғау

- **Серверлер**

  Сервер инфрақұрылымының сенімділігін қамтамасыз ету, қауіпсіз жүктеу

- **IoT құрылғылары**

  Заттар интернеті құрылғыларында аутентификация және деректерді қорғау

- **Қашықтан жұмыс**

  Үйден жұмыс істейтін қызметкерлердің құрылғыларының қауіпсіздігін қамтамасыз ету

- **Сенімді желілер**

  Корпоративтік желіге қосылатын құрылғылардың сенімділігін тексеру

TPM технологиясы ерекше лицензиялау немесе қосымша шығындарды қажет етпейді, өйткені ол көптеген заманауи құрылғыларда қазірдің өзінде орнатылған.

HSM және TPM: негізгі айырмашылықтар

HSM

- Серверлер мен дата-орталықтарда қолданылады
- Жоғары өнімділікті қамтамасыз етеді
- Өте жоғары құны (мыңдаған доллар)
- Орталықтандырылған кілттерді басқару
- FIPS 140-2/3 Level 3-4 сертификаттары
- Көп пайдаланушылық режим

TPM

- Жеке компьютерлер мен ноутбуктарда
- Платформа деңгейінде қауіпсіздік
- Төмен құн (құрылғыға енгізілген)
- Жергілікті кілттерді сақтау
- TCG стандарттары (TPM 2.0)
- Бір құрылғыға арналған

HSM және TPM бір-бірін толықтырады: HSM орталық инфрақұрылымда қолданылса, TPM соңғы пайдаланушы құрылғыларын қорғайды. Кешенді қауіпсіздік стратегиясында екеуі де маңызды рөл атқарады.

Аппараттық қауіпсіздік құралдарының салыстырмалы сипаттамасы

HSM құрылғылары – бұл корпоративтік деңгейдегі шешім, ол жоғары жүктемелерді көтеруге және миллиондаған транзакцияларды өңдеуге арналған. Олар банктер, ірі корпорациялар және мемлекеттік мекемелер үшін өте маңызды.

TPM модульдері массалық нарыққа арналған және кез келген заманауи компьютерде болуы мүмкін. Олар жеке пайдаланушылар мен шағын-орта бизнес үшін қолжетімді қауіпсіздік шешімі болып табылады.

Аппараттық қорғаныстың заманауи трендтері

Ақпараттық қауіпсіздік саласы тез дамып келеді және аппараттық қорғаныс технологиялары да жаңа трендтерге бейімделуде. Қазіргі кезеңде бірнеше маңызды бағыттар байқалады: бұлттық технологиялармен интеграция, виртуализация, жасанды интеллектті қолдану және кванттық криптографияға дайындық.

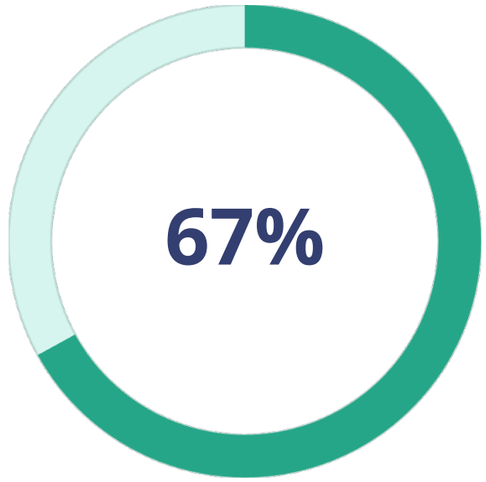
Бұл трендтер аппараттық қауіпсіздік шешімдерінің қолжетімділігін арттырады, олардың икемділігін жоғарылатады және жаңа қауіптерге жауап беру қабілетін күшейтеді.



Бұлттық HSM және виртуализация

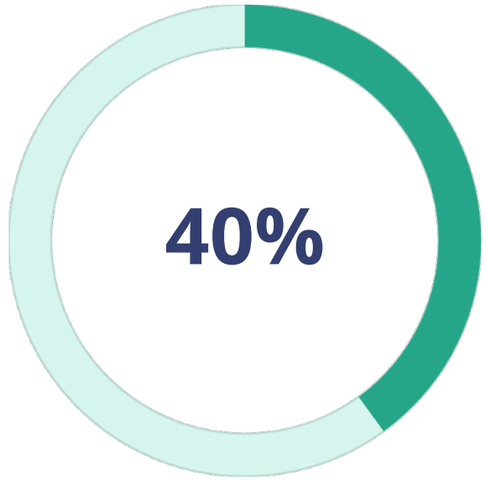
Дәстүрлі HSM құрылғылары физикалық жабдық ретінде дата-орталықтарда орналасады. Бірақ бұлттық технологиялардың дамуымен Cloud HSM немесе HSM-as-a-Service шешімдері пайда болды. Олар қауіпсіздіктің сол деңгейін сақтай отырып, икемділік пен масштабталуды қамтамасыз етеді.

Amazon AWS CloudHSM, Azure Dedicated HSM және Google Cloud HSM сияқты қызметтер компанияларға қымбат жабдықты сатып алмай-ақ HSM мүмкіндіктерін пайдалануға мүмкіндік береді.



Бұлттық HSM өсімі

2024-2025 жж. арасы



Құн үнемдеу

CAPEX vs OPEX моделі

Бұлттық HSM шешімдері физикалық HSM сияқты FIPS 140-2 сертификаттарына ие және сол деңгейде қауіпсіздікті қамтамасыз етеді.

Жасанды интеллект пен машиналық оқыту

Қауіптерді болжау

ЖИ алгоритмдері үлгілерді талдап, әлеуетті қауіптерді алдын ала анықтай алады

Аномалияларды табу

Қалыпты емес әрекеттерді автоматты түрде табу және ескерту жіберу

Автоматты жауап

Қауіптерге нақты уақытта жауап беру, адам араласуынсыз шабуылдарды тоқтату

Жасанды интеллект аппараттық қауіпсіздік жүйелерін интеллектуалды етеді. SIEM жүйелерімен интеграция арқылы HSM мен TPM логтары талданады және қауіптер уақытында анықталады. Машиналық оқыту модельдері жаңа шабуыл әдістерін үйреніп, бейімделе алады.

Қазақстандағы ақпараттық қауіпсіздік инфрақұрылымы

АҚҰҰО – Ұлттық үйлестіру орталығы

Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы (АҚҰҰО) Қазақстан Республикасының киберқауіпсіздік саласындағы басты органы болып табылады. Орталық ақпараттық қауіптерді мониторингілейді, инциденттерге жауап береді және ұлттық деңгейде үйлестіруді жүзеге асырады.

Мемлекеттік техникалық қызмет

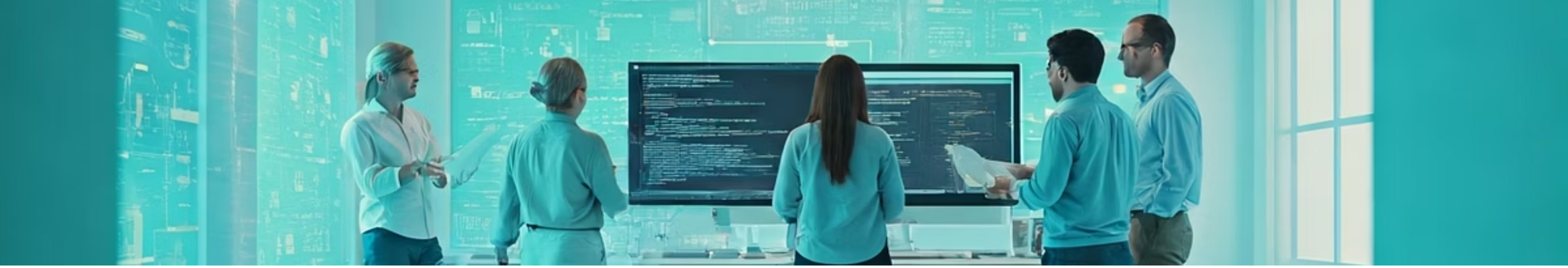
Мемлекеттік техникалық қызмет (МТҚ) құпия ақпаратты қорғау және арнайы техникалық шараларды жүзеге асыру жөнінде жұмыс жүргізеді. МТҚ аппараттық қауіпсіздік құралдарын сертификаттау мен бақылауда маңызды рөл атқарады.

Бұл екі орган Қазақстанның ақпараттық қауіпсіздік экожүйесінің тіректері болып табылады және аппараттық қорғаныс технологияларының дамуына үлес қосады.

Ұлттық қауіпсіздік экожүйесі

Қазақстанда ақпараттық қауіпсіздік инфрақұрылымы бірнеше деңгейлерден тұрады: ұлттық мониторинг орталығы, салалық SOC-тар (Security Operations Center), корпоративтік қауіпсіздік жүйелері және соңғы пайдаланушы құрылғылары. HSM мен TPM осы экожүйенің маңызды компоненттері болып табылады.

Мемлекет цифрлық инфрақұрылымды дамытуға және ақпараттық қауіпсіздікті нығайтуға үлкен назар аударады. «Цифрлық Қазақстан» бағдарламасы аясында қауіпсіздік технологияларын енгізу мен кадрлар даярлау жүргізілуде.



Аппараттық қорғаныстыенгізу тәжірибесі

Теориялық білімнен практикаға көшу үшін нақты енгізу тәжірибесін қарастыру маңызды. Бұл бөлімде біз ірі ұйымдардың HSM мен TPM технологияларын қалай пайдаланатынын, қандай қиындықтарға тап болатынын және қандай шешімдер табатынын талқылаймыз.

Аппараттық қауіпсіздік құралдарын енгізу – бұл тек техникалық емес, сонымен қатар ұйымдастырушылық процесс. Ол жоғарғы басшылықтың қолдауын, бюджет бөлуді, қызметкерлерді оқытуды және регламенттерді әзірлеуді қажет етеді.

Мемлекеттік сектордағы TPM пайдалану

Қазақстан Республикасының бірнеше министрліктері мен ведомстволары өз қызметкерлерінің жұмыс құрылғыларына TPM технологиясын міндетті түрде енгізуді бастады. Бұл шара мемлекеттік құпия ақпаратты қорғау және киберқауіпсіздікті нығайту мақсатында жүзеге асырылды.

1. **2022 ж. 1-тоқсан**

   Талаптарды әзірлеу және регламенттерді бекіту

2. **2022 ж. 2-3 тоқсан**

   TPM-мен жабдықталған құрылғыларды сатып алу

3. **2022 ж. 4-тоқсан**

   Пилоттық енгізу және тестілеу

4. **2023 ж. 1-жарты жыл**

   Қызметкерлерді оқыту және толық енгізу

5. **2023 ж. 2-жарты жыл**

   Мониторинг және оптимизация

Нәтижесінде барлық құпия деректермен жұмыс істейтін құрылғылар BitLocker шифрлауымен және TPM растауымен қорғалды. Бұл ұрланған немесе жоғалған құрылғылардан деректер ағып кетуін болдырмады.

Енгізу кезіндегі қиындықтар мен шешімдер

Қиындық: Жоғары құн

HSM құрылғылары өте қымбат (10-100 мың доллар)

Шешім: Кезеңдік енгізу

Сыни маңызды жүйелерден бастап біртіндеп кеңейту, ROI есептеу

Қиындық: Интеграция күрделілігі

Ескі жүйелермен үйлесімділік мәселелері

Шешім: Кәсіби қолдау

Өндірушілер мен интеграторлардың қолдау қызметін пайдалану

Қиындық: Білікті кадрлар жетіспеушілігі

HSM/TPM бойынша мамандардың тапшылығы

Шешім: Оқыту бағдарламалары

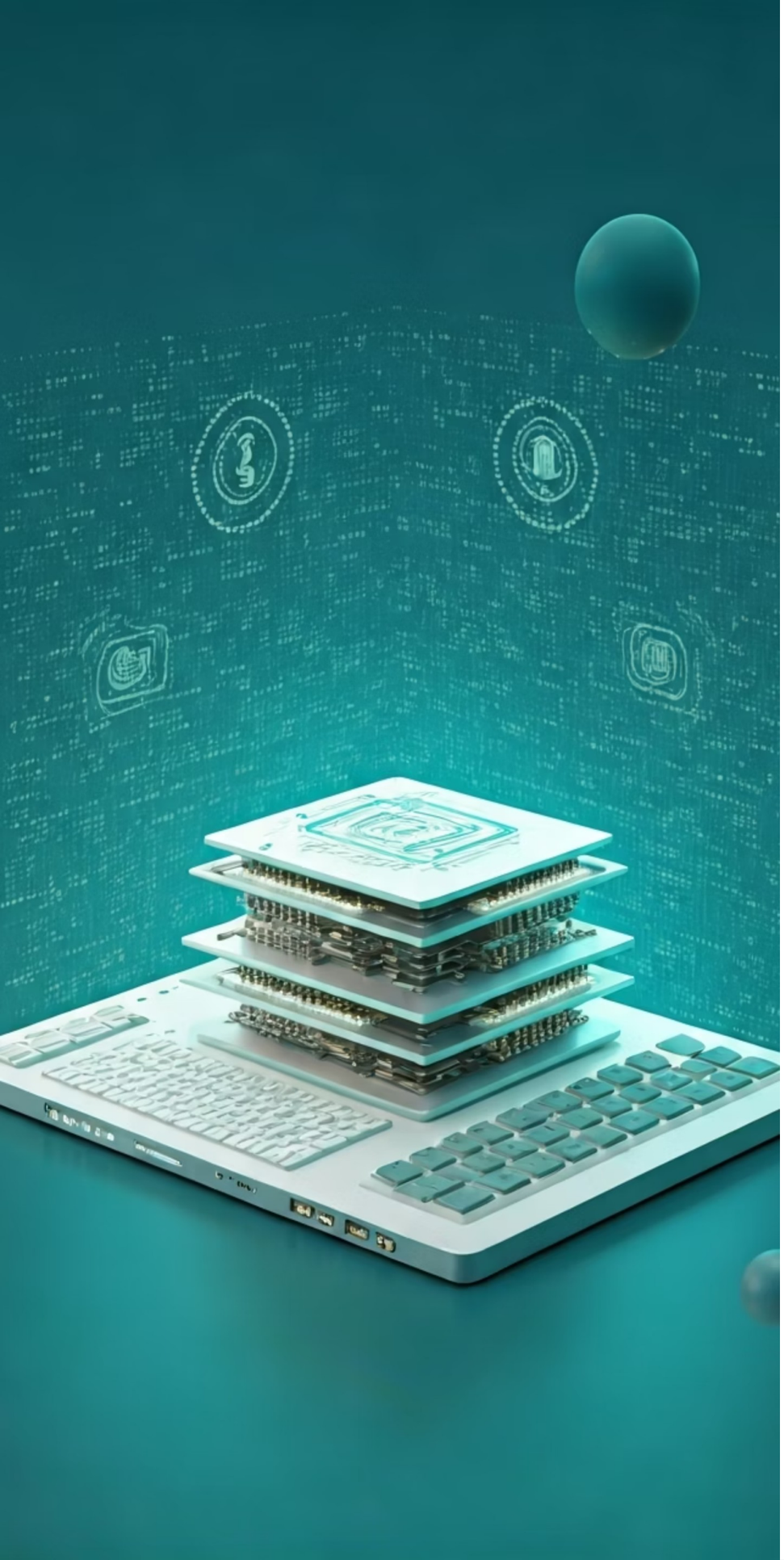
Қызметкерлерді сертификаттау және үздіксіз оқыту

Инциденттер мен сабақтар

2023 жылы бір қазақстандық компанияда ірі ақпараттық инцидент болды: зиянды программа корпоративтік желіге енді. Бірақ HSM арқылы қорғалған құпия кілттер мен сертификаттар қауіпсіз қалды.

Бұл оқиға аппараттық қорғаныстың маңыздылығын тағы бір рет дәлелдеді. Программалық қорғаныс бұзылса да, аппараттық деңгей сенімді қалқан болып қала алады.

> «Егер HSM болмаса, біз барлық криптографиялық кілттерімізді жоғалтып, бизнесіміз тоқтап қалар еді. Аппараттық қорғаныс – бұл инвестиция емес, міндеттілік» – компания IT директоры



Болашаққа көзқарас

Аппараттық қауіпсіздік технологиялары тоқтап қалмайды – олар үнемі дамып, жаңа қауіптерге бейімделуде. Келесі онжылдықта бірнеше маңызды трендтер күтіліп отыр: кванттық криптографияға көшу, биометриялық аутентификацияның кеңеюі, Zero Trust архитектурасының енгізілуі және Edge Computing қауіпсіздігі.

Қазақстан да осы трендтерге бейімделуде. Ұлттық инновациялық жобалар аясында болашақ технологияларға дайындық жүргізілуде.

Кванттық криптография және Post-Quantum қауіпсіздік

Кванттық компьютерлер дамуы қазіргі криптографиялық алгоритмдерге қауіп төндіруде. RSA, ECC сияқты алгоритмдер кванттық компьютерлерге осал болуы мүмкін. Сондықтан Post-Quantum криптография алгоритмдерін әзірлеу және енгізу өзекті міндет.

HSM өндірушілері қазірдің өзінде кванттық-қауіпсіз алгоритмдерді қолдау функцияларын енгізуде. NIST ұйымы Post-Quantum стандарттарын бекіту процесінде.

Қазіргі кезең

Дәстүрлі криптография (RSA, ECC)

Көшу кезеңі

Гибридті шешімдер (классикалық + PQ)

Болашақ

Толық Post-Quantum криптография

Қазақстандағы инновациялық жобалар



ҰАТ ЖИ экожүйесі

«Ұлттық ақпараттық технологиялар» АҚ жасанды интеллект және машиналық оқытуды қауіпсіздік жүйелеріне енгізуде. HSM логтарын талдау және қауіптерді болжау жобалары іске асырылуда.



Цифрлық инфрақұрылымды жетілдіру

Мемлекеттік цифрлық инфрақұрылымда аппараттық қауіпсіздікті арттыру жобалары жүзеге асырылуда. Барлық маңызды мемлекеттік жүйелерде HSM енгізу жоспарлануда.



Блокчейн және аппараттық қауіпсіздік

Блокчейн технологияларын HSM-мен біріктіру бойынша пилоттық жобалар жүргізілуде. Бұл крипто-активтерді қауіпсіз басқаруға мүмкіндік береді.

Аппараттық қорғаныс – қауіпсіздіктің іргетасы

Ақпараттық қауіпсіздік жүйесінің тиімділігі оның ең әлсіз буынымен анықталады. Программалық және ұйымдастырушылық шаралар қаншалықты күшті болса да, аппараттық деңгейде сенімді қорғаныс болмаса, жүйе осал қалады.

HSM және TPM технологиялары аппараттық деңгейде физикалық және логикалық қорғанысты қамтамасыз етеді. Олар криптографиялық кілттерді қауіпсіз сақтайды, шифрлау операцияларын жылдам орындайды және платформа сенімділігін растайды.



Сенімділік деңгейі



Қолжетімділік



Құпиялылық

Қазіргі заманғы киберқауіптер жағдайында аппараттық қауіпсіздік құралдарын енгізу – бұл таңдау емес, қажеттілік. Қазақстан да осы бағытта белсенді қадамдар жасауда.

Практикалық ұсыныстар

1

Аппараттық қорғанысты кеңейту

Барлық сыни маңызды жүйелерде HSM немесе TPM технологияларын енгізу. Кезеңдік жоспар құру және ROI есептеу.

- Инфрақұрылымды аудит жүргізу
- Сыни активтерді анықтау
- Енгізу жоспарын әзірлеу

2

Қызметкерлерді оқыту

IT мамандары мен қауіпсіздік қызметі қызметкерлерін HSM/TPM технологиялары бойынша үздіксіз оқыту және сертификаттау.

- Негізгі оқу курстары
- Практикалық жаттығулар
- Халықаралық сертификаттау

3

Ақпараттық мәдениетті арттыру

Барлық қызметкерлер арасында ақпараттық қауіпсіздік мәдениетін қалыптастыру, қауіптер туралы хабардар ету.

- Жалпы ақпараттандыру семинарлары
- Фишингке қарсы жаттығулар
- Қауіпсіздік саясатын үгіттеу

4

Мемлекет-бизнес ынтымақтастығы

Мемлекеттік органдар мен жеке сектор арасында ақпараттық қауіпсіздік саласында ынтымақтастықты күшейту.

- Ақпарат алмасу платформалары
- Бірлескен оқиғаларды талдау
- Үздік тәжірибелерді тарату

Қауіпсіздік мәдениеті – команда жұмысы

Ақпараттық қауіпсіздік – бұл тек технология емес, бұл мәдениет. Ең заманауи HSM құрылғылары мен TPM чиптері болса да, қызметкерлер қауіпсіздік қағидаларын сақтамаса, жүйе осал қалады. Сондықтан барлық деңгейдегі қызметкерлерді оқыту және қауіпсіздік мәдениетін қалыптастыру өте маңызды.

Әрбір қызметкер ақпараттық қауіпсіздіктің бір бөлігі екенін түсінуі керек. Біріккен әрекет пен жауапкершілік арқылы ғана толыққанды қорғанысқа қол жеткізуге болады.

Қосымша ақпарат пен ресурстар

Қазақстан Республикасының заңнамалары

- «Ақпараттандыру туралы» ҚР Заңы
- «Мемлекеттік құпияларды қорғау туралы» ҚР Заңы
- «Электрондық құжат және электрондық цифрлық қолтаңба туралы» ҚР Заңы
- АҚҰҰО регламенттері мен нормативтік құжаттары

Ұлттық стандарттар

- ҚР СТ ISO/IEC 27001 – Ақпараттық қауіпсіздікті басқару
- ҚР СТ ISO/IEC 27002 – Қауіпсіздік бақылаулары
- СТ РК ГОСТ Р ИСО/МЭК 15408 – Қауіпсіздік критерийлері

Халықаралық стандарттар мен сертификаттар

- FIPS 140-2/140-3 – Криптографиялық модульдер стандарты (АҚШ)
- Common Criteria (ISO/IEC 15408) – Халықаралық қауіпсіздік критерийлері
- PCI DSS – Төлем карталары индустриясының қауіпсіздік стандарты
- TCG TPM 2.0 – Trusted Platform Module спецификациясы

Пайдалы ресурстар

- АҚҰҰО ресми сайты
- ҰАТ АҚ корпоративтік порталы
- NIST Cryptographic Standards
- Trusted Computing Group (TCG)

Байланыс және консультациялар

«Ұлттық ақпараттық технологиялар» АҚ

Электрондық цифрлық қолтаңба және ақпараттық қауіпсіздік қызметтері бойынша ұлттық оператор

Мекенжайы: Астана қ., Мәңгілік Ел д., 55/20

Сайт: nit.kz

Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы (АҚҰҮО)

Киберқауіпсіздік саласындағы мониторинг, үйлестіру және инциденттерге жауап беру орталығы

Мекенжайы: Астана қ.

Сайт: gov.kz

Техникалық қолдау және консультациялар

HSM және TPM технологиялары бойынша кәсіби консультациялар алу үшін біздің техникалық қолдау қызметіне жүгініңіз

Email: support@security.kz

Телефон: +7 (7172) 00-00-00