СӘТБАЕВ УНИВЕРСИТЕТІ

SATBAYEV UNIVERSITY

Статистика және деректерді талдау

Ержан Асел Ануаркызы,Ph.D., «Ақпараттық жүйелер» кафедрасының қауымдастырылған профессоры

Assel.yerzhan@satbayev.university

№1 Статистикаға кіріспе. Деректер түрлері

Статистиканың негізгі ұғымдарын, зерттеу кезеңдерін және қоғамдық ғылымдардағы рөлін бірге қарастырамыз.



Статистика дегеніміз не?

Негізгі анықтама

Статистика — деректерді жинау, өңдеу, талдау және интерпретациялауға арналған ғылыми пән. Ол сандық әдістер арқылы қоғамдық құбылыстарды зерттеп, заңдылықтарды ашуға мүмкіндік береді.

Деректерді жинау және өңдеу

Бастапқы мәліметтерді жүйелі түрде жинау және ретке келтіру

Талдау және интерпретациялау

Математикалық және логикалық әдістер арқылы нәтижелерді түсіндіру

Сандық зерттеу

Қоғамдық құбылыстарды объективті сандық тілмен сипаттау

Статистиканың мақсаттары

□ Нақты ақпарат алу

Шешім қабылдауға негіз болатын сенімді және дәл деректерді алу, субъективті пікірлерді объективті фактілермен алмастыру

□ Болжам жасау

Тарихи деректер негізінде болашақтағы үрдістерді болжау және стратегиялық шешімдер қабылдауға қолдау көрсету

🔍 Заңдылықтарды ашу

Деректер жиынтығындағы жасырын үлгілерді, тәуелділіктер мен ауытқуларды анықтап, себеп-салдарлық байланыстарды орнату



Сандық белгілер

Сандық белгілер өлшенетін немесе есептелетін мәліметтерді сипаттайды. Олар екі негізгі топқа бөлінеді:

Дискретті белгілер

Тек нақты, бүтін сандық мәндерді қабылдайды. Аралықта ешқандай мән болмайды.

- Адам саны — 1, 2, 3...
- Балалар саны отбасында
- Тіркелген инциденттер саны
- Қателер мен оқиғалардың жиілігі

Үздіксіз белгілер

Белгілі бір аралықта кез келген мәнді қабылдай алады. Өлшеу дәлдігіне байланысты.

- Салмақ — 70.5 кг, 71.2 кг...
- Бой, температура, уақыт
- Деректер беру жылдамдығы
- Желілік кідіріс (latency) мәні

Сапалық белгілер

Сапалық белгілер сандық емес, сипаттамалық ақпаратты беретін белгілер. Олар жіктеу немесе реттеу мақсатында қолданылады.

Категориялық (номиналды) белгілер

Бір-бірінен тәуелсіз, реттелмеген санаттарға жатады. Арасында "жоғары–төмен" қатынасы жоқ.

- Жыныс: ер, әйел
- Түстер: қызыл, жасыл, көк
- Мамандық түрі, ел атауы

Ранжирленген (реттелген) белгілер

Санаттар белгілі бір ретпен орналасады, бірақ аралардың тең болуы міндетті емес.

- Білім деңгейі: орта, жоғары
- Дәрежелер: жоғары, орта, төмен
- Қауіпсіздік деңгейлері: 1-4 класс

Зерттеу кезеңдері: Жоспарлау

Кез келген статистикалық зерттеу мұқият жоспарлаудан басталады. Бұл кезеңде қателіктерге жол бермеу зерттеудің сапасын айқындайды.

01

Нысан мен мақсатты анықтау

Зерттеу объектісін, генеральды жиынты мен зерттеу сұрақтарын нақты тұжырымдау

02

Әдістеме мен құралдарды таңдау

Іріктеу тәсілін, өлшеу шкаласын және деректерді жинаудың оңтайлы жолын белгілеу

03

Уақыт кестесін жасау

Зерттеудің әрбір кезеңіне мерзім белгілеу, ресурстарды бөлу және нәтижелерді бақылау тетіктерін орнату



Мәліметтерді жинау

Анкеталар мен сұрау парақтары

Мақсатты аудиториядан жүйелі түрде жауаптар жинау. Ашық және жабық сұрақтарды біріктіру арқылы сапалы деректер алынады.

Тікелей бақылау әдістері

Зерттеу объектісін табиғи ортасында бақылау. Бақылаушы учаскеге қатыспай, объективті деректерді тіркейді.

Статистикалық есеп құжаттары

Мемлекеттік органдар, кәсіпорындар мен ұйымдардың ресми есептілік деректеріне сүйену — сенімді бастапқы ақпарат көзі.

Статистикалық талдау әдістері

Орташа және салыстырмалы шамалар

Арифметикалық орта, медиана, мода — деректердің орталық тенденциясын сипаттайды. Салыстырмалы шамалар пропорция мен динамиканы көрсетеді.

Корреляция және дисперсиялық талдау

Белгілер арасындағы байланысты өлшеу. Дисперсиялық талдау топаралық айырмашылықтардың маңыздылығын тексереді.

Графикалық визуализация

Гистограммалар, диаграммалар, бөліну кестелері — күрделі деректерді анық түрде беру және аудиторияға жеткізу.



Статистика және қоғамдық ғылымдар

Экономикалық талдау

ЖІӨ динамикасы, инфляция деңгейі, жұмыссыздық үрдістері — барлығы статистикалық модельдер арқылы зерттеледі

Әлеуметтік зерттеулер

Халықтың тұрмыс деңгейі, білімге қолжетімділік, қылмыс статистикасы сандық сипаттама алады

Зерттеу дәлдігі

Іріктеме теориясы мен статистикалық критерийлер зерттеу нәтижелерінің ғылыми негізділігін қамтамасыз етеді



Бөлім 2: Ақпараттық қауіпсіздікке кіріспе

Ақпараттық қауіпсіздіктің негізгі ұғымдары, қауіп-қатер түрлері және қорғаныс механизмдерін зерттейміз.



Ақпарат — негізгі ресурс

XXI ғасырда ақпарат мұнай мен газға тең бағаланатын стратегиялық ресурсқа айналды. Цифрлық экономиканың дамуы мен мемлекеттік басқарудың ақпараттандырылуы деректердің қорғалуын бұрынғыдан да маңызды етіп отыр.

Қоғамның даму қозғалтқышы

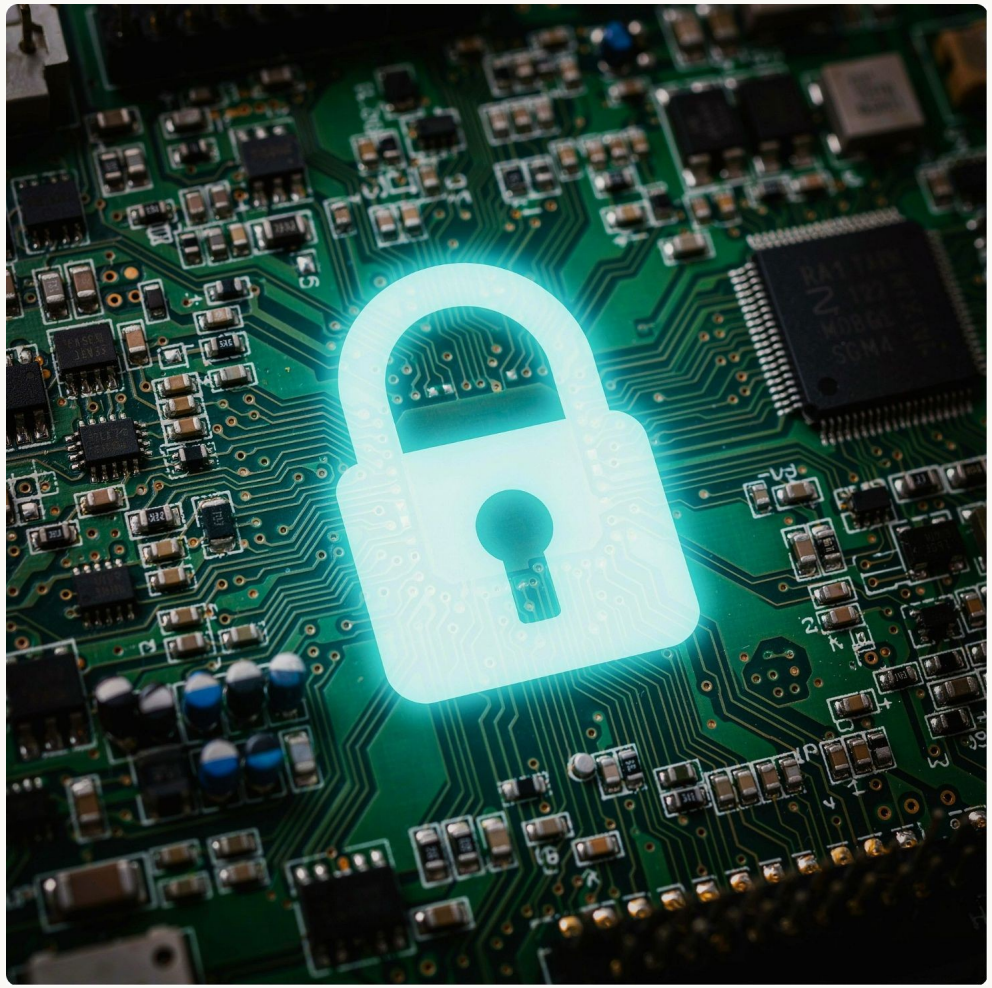
Ақпараттық ресурстар бизнесті, мемлекетті және азаматтарды байланыстырады

Ресурстарды қорғау

Деректердің жоғалуы немесе бұрмалануы орасан зиян келтіруі мүмкін

Мемлекеттік және жеке мүдделер

Азаматтардың жеке деректері мен мемлекеттік құпиялар бірдей қорғалуды талап етеді



Ақпараттық қауіпсіздік анықтамасы

Ақпараттық қауіпсіздік — ақпаратты заңсыз жария ету, бұрмалау, жою және қолжетімсіздіктен қорғауға бағытталған ұйымдастырушылық, техникалық және құқықтық шаралардың кешені.

1

Заңдылықтарды сақтау

Тек заңды пайдаланушылар мен процестер ғана ақпаратқа қол жеткізе алады

2

Тұтастықты қамтамасыз ету

Деректер рұқсатсыз өзгертілмейді, мазмұны сенімді болып қалады

3

Қолжетімділікті сақтау

Ақпарат қажет уақытта заңды пайдаланушыларға қолжетімді болады

Негізгі элементтер: CIA Триадасы



CIA триадасы — Жасырындылық (Confidentiality), Тұтастық (Integrity) және Қолжетімділік (Availability) — кез келген ақпараттық қауіпсіздік жүйесінің іргетасы болып табылады. Бұл үш элементтің тепе-теңдігі сенімді қорғанысты қамтамасыз етеді.



Қауіптер және осалдықтар

Осалдық (Vulnerability)

Жүйедегі шабуылдаушы пайдалана алатын әлсіз тұстар. Бағдарламалық қателіктер, конфигурация кемшіліктері немесе адам факторы болуы мүмкін.

Тәуекел (Risk)

Осалдықтың пайдаланылу ықтималдығы мен зиянның ауырлығының туындысы. Тәуекелді бағалау қорғанысқа басымдық беруге мүмкіндік береді.

Шабуыл (Attack)

Қауіпсіздікті бұзуға бағытталған іс-қимылдар тізбегі. Мақсаты — деректерді ұрлау, жүйені бұзу немесе қызметті тоқтату.

Ақпараттық қауіпсіздік саясаты

Саясат дегеніміз не?

Ақпараттық қауіпсіздік саясаты — мекеменің ақпараттық активтерін қалай өңдеу, сақтау және қорғау керектігін нақты регламенттейтін ресми құжаттар жиынтығы. Ол барлық қызметкерлер мен жүйелерге қолданылады.

- **Қорғау ережелері мен директивалары:** рұқсатты пайдалану, парольдік саясат, шифрлау талаптары
- **Активтерді өңдеу тәртібі:** деректерді жіктеу, сақтау мерзімдері, жою процедурасы
- **Қауіпсіздік сервистерінің критерийлері:** аутентификация, авторизация, аудит журналдары
- **Жауапкершілік бөлінісі:** қауіпсіздік рөлдері мен міндеттерін нақты бекіту

Қауіпсіздік механизмдері және олардың рөлі

Шабуылдарды анықтау жүйелері

IDS/IPS жүйелері желілік трафикті бақылап, күдікті әрекеттерді нақты уақыт режимінде анықтайды және оларды автоматты түрде блоктайды.

Бағдарламалық қорғаныс

Антивирустар, брандмауэрлер, шифрлау алгоритмдері, VPN — бағдарламалық деңгейде деректерді қорғаудың негізгі құралдары.

Аппараттық қорғаныс кешендері

HSM модульдері, смарт-карталар, биометриялық сенсорлар — физикалық деңгейдегі сенімді аутентификация мен деректерді қорғау.

Желілік шабуылдар классификациясы



Активті шабуылдар

Жүйеге тікелей әсер ететін, деректерді өзгертетін немесе қызметтің жұмысын бұзатын шабуылдар. Зардабы дереу байқалады.

- Деректерді модификациялау
- DoS / DDoS шабуылдары
- Жалған пакеттер жіберу

Пассивті шабуылдар

Жүйені өзгертпей, ақпаратты жасырын тыңдап, жинайды. Анықтауы өте қиын.

- Трафикті тыңдау (sniffing)
- Мета-деректерді жинау
- Ақпаратты OSINT арқылы талдау

Кибершабуылдардың қауіпті түрлері



DoS / DDoS шабуылдары

Мақсатты жүйені жалған сұраныстармен толтырып, заңды пайдаланушыларға қызмет көрсетуді тоқтату. Банктер мен мемлекеттік порталдарға ең жиі қолданылатын шабуыл түрі.



Man-in-the-Middle (MitM)

Шабуылдаушы екі тарап арасындағы байланысқа кіріп, хабарламаларды тыңдайды немесе өзгертеді. Шифрланбаған желілерде ерекше қауіпті.



Деректерді модификациялау

Мәліметтер базасындағы немесе файлдардағы деректерді заңсыз өзгерту. Қаржылық есептер мен медициналық жазбалар үшін өте қауіпті.

Қауіпсіздік сервистерінің деңгейлері



Қауіпсіздік сервистерінің әрбір деңгейі алдыңғысына сүйенеді: аутентификациясыз жасырындылықты, жасырындылықсыз тұтастықты қамтамасыз ету мүмкін емес.

Ақпараттандыруды мемлекеттік реттеу

Ашықтық презумпциясы

Мемлекеттік ақпарат заңмен шектелмесе, азаматтарға еркін қолжетімді болуы тиіс. Бұл демократиялық басқарудың негізі.

Негізгі реттеу бағыттары

- **Мемлекеттік органдардың міндеттері:** ақпаратты жариялау, есептілік, аудит
- **Жеке деректерді қорғау:** жинау, өңдеу және сақтаудың заңдық талаптары
- **Цифрлық инфрақұрылым:** маңызды жүйелерді бақылаудың құқықтық негіздері
- **Киберқылмыспен күрес:** заңнамалық жауапкершілік механизмдері



2025: Цифрлық деректерді басқару стандарты

1

ISO 27001 талаптары

Халықаралық стандартқа сәйкес ақпараттық қауіпсіздікті басқару жүйесін (ISMS) енгізу және сертификаттау

2

Тәуекелге бағдарланған қорғаныс

Барлық активтерді бірдей емес, тәуекел деңгейіне сәйкес саралап қорғайтын архитектура

3

Корпоративтік мониторинг

Ішкі аудит, ауытқуларды бақылау және үздіксіз жетілдіру арқылы стандарттардың орындалуын қадағалау

Киберщит жобасы: Қазақстанның қорғанысы



«Киберщит Қазақстан» — мемлекеттік маңызы бар ақпараттық инфрақұрылымды орталықтандырылған қорғауға арналған кешенді бағдарлама.

QazCloud мониторингі

Тәулік бойы үздіксіз кибер-қауіптерді бақылау және ерте ескерту жүйесі

Автоматтандырылған сканерлеу

Ұлттық инфрақұрылым нысандарының осалдықтарын жүйелі түрде тексеру

Гео-резервтеу

Деректерді географиялық таратып сақтау арқылы апаттарға төзімділікті арттыру

"Қара жәшік" моделі бойынша тестілеу

Қара жәшік (Black-box) тестілеу

Шабуылдаушының позициясынан инфрақұрылымды тексеру — ішкі ақпаратсыз, тек сыртқы перспективадан осалдықтарды іздеу.

- **Ішкі инфрақұрылым:** серверлер, желілік жабдықтар, қолданбалы бағдарламалардың осалдықтарын анықтау
- **Веб-ресурстарды OSINT талдауы:** ашық дереккөздерден ұйым туралы ақпаратты жинап, шабуыл векторларын анықтау
- **Сыни осалдықтар:** табылған критикалық кемшіліктерді жедел жою жөніндегі іс-қимыл жоспары
- **Нәтижелер есебі:** анықталған тәуекелдер бойынша детальды есептілік және ұсыныстар



Инциденттермен жұмыс және криминалистика

Кибер-инциденттерді тергеудің ғылыми-техникалық әдістері және цифрлық криминалистиканың негіздері.

Кибер-инциденттерді тергеу: Негізгі қадамдар



Анықтау

Дәлел сақтау

Құрылғы диагностикасы

Есеп және қорытынды

Инциденттерді тергеу процесінде оқиғалар тізбегін дұрыс қалпына келтіру және дәлелдерді сот талқылауына жарамды түрде сақтау — ең маңызды міндеттер.

Деректерді қалпына келтіру және сараптама



01

Дискілерден кескін алу

HDD/SSD дискілерінің форензикалық сенімді көшірмелерін жасау. Бастапқы дерекке тиіспей жұмыс жасалады.

02

Жойылған файлдарды қалпына келтіру

Арнайы бағдарламалар арқылы өшірілген файлдар мен артефактілерді іздеу және қалпына келтіру

03

Журналдарды талдау

Операциялық жүйе оқиға журналдары (Event Logs), браузер тарихы, ЖЖҚ үйінділерін (RAM dumps) кешенді талдау



Ақпараттық қауіпсіздік мәдениеті және стандарттар

Ұйымдастырушылық шаралар мен халықаралық стандарттар — техникалық қорғанысты толықтыратын маңызды элементтер.

ISO 27001: Тәуекелге бағдарланған тәсіл

ISO/IEC 27001 — ақпараттық қауіпсіздікті басқару жүйелеріне арналған жетекші халықаралық стандарт. Ол ұйымдарға ақпараттық активтерді жүйелі түрде қорғауға мүмкіндік береді.

Корпоративтік қорғаныс стандарты

Ақпараттық активтерді анықтау, бағалау және тәуекелге негізделген қорғаныс шараларын таңдау. Ұйымның барлық деңгейлерін қамтиды.

Бизнес үздіксіздігі

Инциденттер кезінде де бизнес-процестердің үздіксіздігін қамтамасыз ету. Апаттан қалпына келтіру жоспарларын міндеттейді.

Қол жеткізуді шектеу

«Ең аз артықшылық» принципі бойынша пайдаланушылар тек қажет ресурстарға ғана қол жеткізе алады. Рөлдік рұқсат жүйесі енгізіледі.

Ақпараттық мәдениетті қалыптастыру



Оқыту статистикасы 2025

9 194 қызметкер арнайы тренингтен өтті. Бұл — тек нормативтік талапты орындау емес, ақпараттық мәдениет қалыптастырудың негізі.



17 077 оқу сағаты

Фишинг симуляциялары, социалды инженерия сценарийлері, парольдік гигиена — практикалық дағдыларға бағытталған тренингтер.



Озық тәжірибелер

Нормативтік минимумнан тыс халықаралық стандарттарды ендіру арқылы ұйымдардың киберсауаттылық деңгейін үздіксіз арттыру.

Қорғаныстың қара жәшік моделі

Тексеру мазмұны

- **Ішкі инфрақұрылым:** желілік сегменттер, серверлер, IAM жүйелері
- **Әлеуметтік инженерия:** фишинг шабуылдарына қызметкерлердің реакциясын тексеру
- **SPOF нүктелері:** жалғыз істен шығу нүктелерін анықтау және жою

Техникалық жетілдіру

- **Гео-резервтеу:** деректерді географиялық таратып сақтау, апаттан тез қалпына келу
- **Серверлік оңтайландыру:** жабдықтың жүктемесін теңестіру, артық жаттылықты арттыру
- **Үздіксіз мониторинг:** автоматтандырылған ескерту жүйелері арқылы тәулік бойы бақылау

Киберқауіпсіздік: Қазақстан тәжірибесі

Қазақстанның ұлттық киберқауіпсіздік инфрақұрылымын дамытудағы жетістіктері мен алдыңғы қатарлы тәжірибелері.



Киберщит жобасы: Орталықтандырылған мониторинг

QazCloud мониторингі

Тәулік бойы ұлттық деңгейдегі кибер-қауіптерді бақылау және жедел ден қою орталығы

27 164 инцидент — 2025

Инциденттер санының өсуі мониторинг жүйесінің жетілдірілуімен де байланысты — бұрын байқалмаған оқиғалар тіркеле бастады

Ерте анықтау жүйесі

Мониторинг сезімталдығын арттыру арқылы шабуылдарды алдын ала анықтап, зардапты минималды деңгейге дейін төмендету



Мұнай-газ секторындағы деректер қауіпсіздігі

Мұнай-газ саласындағы деректер қауіпсіздігі — жай ақпараттық қорғаныс емес, өндірістік шешімдердің дұрыстығын қамтамасыз ету мәселесі.

🛢 Қабаттық флюидтер мәселесі

Зертхана алған сынамалар жерастындағы нақты жағдайды толық көрсете ала ма? «Қара жәшік» мәселесі — деректердің репрезентативтілігін тексеру өте маңызды.

📊 Зертхана → Кәсіпшілік

Зертханалық жағдайда алынған деректерді нақты кәсіпшілік жағдайларына дұрыс аудару — статистикалық модельдердің негізгі міндеті.

□ Репрезентативтілік

Жинақталған деректердің генеральды жиынтықты дұрыс бейнелеуі — жобаның тиімділігі мен инвестицияның қайтарымдылығының кепілі.

Болашақ технологиялар мен алгоритмдер

Жасанды интеллект, цифрлық егіздер және ядролық қауіпсіздік саласындағы деректерді басқарудың жаңа парадигмалары.



Деректерді басқарудағы статистикалық модельдер



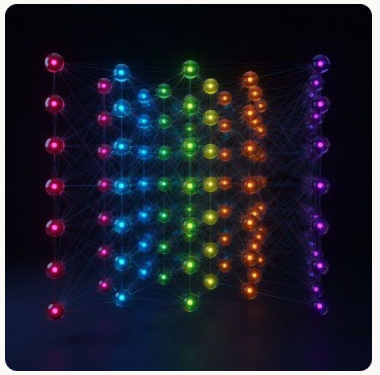
МО және ЖИ — деректер өндірудің негізі

Машиналық оқыту мен жасанды интеллект деректерді талдаудың дәстүрлі тәсілдерін толығымен қайта анықтады. Үлкен деректер массивтерінен заңдылықтарды тиімді ашуға мүмкіндік береді.



Бақыланатын МО: Болжамды талдау

Сызықтық және логистикалық регрессия арқылы ақпараттық қауіпсіздік инциденттерінің ықтималдығын болжау — проактивті қорғаныстың негізі.



Терең оқыту: Аномалияларды анықтау

CNN және RNN желілері желілік трафиктегі, пайдаланушы мінез-құлқындағы аномалияларды дәлдікпен анықтап, шабуылдарды ерте байқауға мүмкіндік береді.

Қара жәшік моделі және тәуекелдер

Black-box мәселесі

Терең нейрондық желілер жоғары дәлдікпен жұмыс жасаса да, шешім қабылдау процесі адамға түсініксіз болып қалады. «Неліктен осындай шешім?» деген сұраққа жауап беру қиын.

Стратегиялық тәуекелдер

- **Автономды көліктер:** апат жағдайында алгоритм шешімінің негізі түсіндірілмесе заңды жауапкершілік мәселесі туады
- **Мұнай бұрғылау:** дұрыс емес болжам орасан шығынға, экологиялық апатқа әкелуі мүмкін
- **Деректердің бұрмалануы:** оқыту деректеріндегі қателіктер жасырын, жүйелі қателерге алып келеді

⚠ Ашық жасанды интеллект (Explainable AI) — стратегиялық шешімдерде міндетті талап.

Цифрлық егіздер: Өнеркәсіптік қауіпсіздік

🏭 Виртуалды көшірме

Цифрлық егіз — нақты өндірістік нысанның деректермен синхрондалған виртуалды моделі. Физикалық жүйеге зиян тигізбей симуляция жасауға мүмкіндік береді.

🔧 Болжамды диагностика

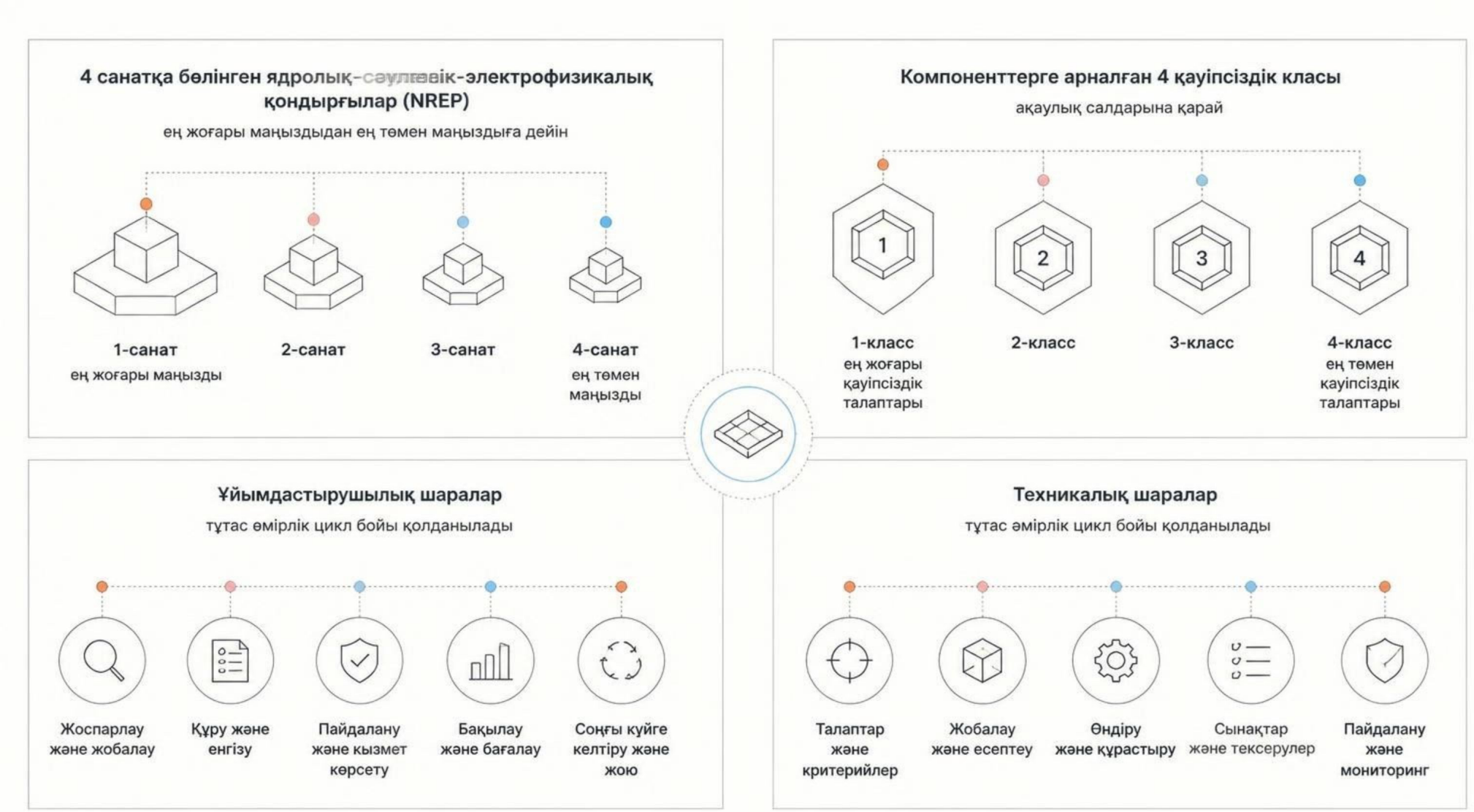
Операциялық мониторинг арқылы жабдықтың ақауланууын алдын ала болжап, апаттық тоқтаулардың алдын алу. Жөндеу шығындарын минималдайды.

📊 Деректер сапасы

Жоғары сапалы синхронды деректер — цифрлық егіздің сенімділік негізі. Байланыс кешігуі мен деректер дәлдігі критикалық маңызға ие.



Ядролық және радиациялық қауіпсіздік регламенті



Тіршілік циклінің барлық кезеңінде — жобалаудан пайдалануға, сондай-ақ жүйені жоюға дейін — ұйымдастырушылық және техникалық іс-шаралар жүйесі дәйекті іске асырылады.

Тасманиядағы «Жердің қара жәшігі» жобасы



«Жердің қара жәшігі» — Тасмания аралындағы 10 метрлік болат монолит. Ұшақтың қара жәшігінен үлгі алынып, адамзат тарихын, климаттық өзгерістерді және саяси жаңалықтарды үздіксіз тіркеп отырады.

Автономды жүйе

Күн энергиясымен жұмыс істейді. Атмосфералық CO_2 деңгейі, мұхит температурасы, жаһандық жаңалықтар — барлығы сақталады.

Болашаққа мұра

Жаһандық апат немесе өркениеттің құлауы жағдайында болашақ ұрпаққа немесе өзге зияткерлік тіршілікке ақпаратты жеткізу мақсаты.

Болашаққа болжам: Ақпараттық қауіпсіздік мәдениеті



Деректерді сауатты талдау

Жеке адамнан бастап мемлекеттік деңгейге дейін — деректерді дұрыс оқу, интерпретациялау және негізге алу қауіпсіздіктің кепілі



Статистикалық ойлау + Киберқауіпсіздік

Статистикалық модельдерді ақпараттық қауіпсіздік стандарттарымен ұштастыру — болашақтың гибридтік қорғаныс архитектурасы



Қазақстанның халықаралық позициясы

Киберщит, ISO 27001 сертификациясы, аймақтық ынтымақтастық — Қазақстанның халықаралық арена-дағы цифрлық беделін нығайтады



Болашаққа көзқарас: Цифрлық егемендік және жауапкершілік

🚀 Технологиялық жетістіктер

Суперкомпьютерлер мен отандық Неуробокс секілді шешімдер Қазақстанның ақпараттық қауіпсіздігін жаңа деңгейге көтерді. Бұл — тек техникалық жетістік емес, ұлттық егемендіктің цифрлық бекінісі.

⚖️ Алгоритмдердің этикасы

Жасанды интеллект дәуірінде тиімділік жеткіліксіз — алгоритмдердің ашықтығы, этикалық нормалар мен адам құқықтарын қорғау ең алдыңғы орынға шығуы тиіс.

🤝 Жауапты цифрлық мәдениет

Деректерді басқару — бұл тек статистикалық талдау емес. Технологияларды адамзат игілігі мен қауіпсіздігі үшін басқаратын жауапты қоғамды қалыптастырудың негізгі құралы.

Деректер — күш. Оны дұрыс пайдалану — біздің ортақ жауапкершілігіміз.