Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university

Физикалық қорғау және қолжетімділікті бақылау жүйелері





Физикалық қорғау жүйелерінің маңызы мен міндеттері

Физикалық қорғау жүйелері – бұл адам өмірі мен материалдық құндылықтарды қорғаудың негізгі құралы. Қазіргі қауіп-қатерлер жағдайында кез келген объектінің қауіпсіздігін қамтамасыз ету үшін кешенді көзқарас қажет. Әлемдік тәжірибе көрсеткендей, тиімді қорғау жүйелері инциденттердің алдын алуда және қауіпсіздік деңгейін арттыруда шешуші рөл атқарады.

Физикалық қорғау жүйелерінің негізгі міндеттері

Қауіпсіздік деңгейін арттыру

Кешенді технологиялар мен құралдарды пайдалану арқылы объектінің жалпы қорғаныс деңгейін жоғарылату және қауіп-қатерлерді минимизациялау

Қолжетімділікті бақылау

Рұқсатсыз кіруді болдырмау, кіру-шығу режимін қатаң реттеу және қауіпсіз аймақтарды сақтау арқылы объектінің тұтастығын қамтамасыз ету

Жедел әрекет ету

Қауіп-қатерді алдын алу, инциденттерді тез анықтау және қауіпсіздік қызметінің дер кезінде жауап беруін қамтамасыз ету

Бұл міндеттердің орындалуы объектінің толық қауіпсіздігін және оның ішіндегі адамдар мен материалдық құндылықтардың сақталуын қамтамасыз етеді.



Қолжетімділікті бақылау жүйелері дегеніміз не?

Қолжетімділікті бақылау жүйелері – бұл адамдар мен көліктердің объектіге кіруін реттейтін, бақылайтын және жазып алатын технологиялар мен құралдар кешені. Бұл жүйелер электрондық кілттер, биометриялық сканерлер, бейнебақылау камералары және басқа да заманауи құрылғыларды біріктіреді.

01

Сәйкестікті растау

Пайдаланушының кім екенін анықтау

02

Рұқсат тексеру

Кіру құқығын тексеру

03

Қолжетімділік беру

Есік немесе тосқауылды ашу

04

Оқиғаны тіркеу

Кіру фактісін жазып алу



Қауіпсіздік технологияларының интеграциясы

Қазіргі заманғы объектілерде қауіпсіздік камералары мен қолжетімділікті бақылау терминалдары бірлесіп жұмыс істейді. Бұл кешенді көзқарас максималды қорғау деңгейін қамтамасыз етеді және инциденттерді тиімді анықтауға мүмкіндік береді.



Физикалық қорғау жүйелерінің құрамдас бөліктері

Тиімді қауіпсіздік жүйесі бірнеше негізгі элементтерден тұрады. Әрбір компонент белгілі бір функцияны орындайды, ал олардың үйлесімді жұмысы объектінің толық қорғалуын қамтамасыз етеді. Заманауи технологиялар осы элементтерді бір біріне интеграциялауға және орталықтандырылған басқаруға мүмкіндік береді.

Негізгі элементтер

Қауіпсіздік камералары (CCTV)

Объектіні үздіксіз бейнебақылау, жазып алу және жедел мониторинг жүргізу үшін арналған жүйе. Жоғары ажыратымдылықтағы камералар түнде де жақсы сапада түсіру қамтамасыз етеді.

Қолжетімділікті бақылау терминалдары

Карталар, биометриялық сканерлер және PIN-кодтар арқылы объектіге кіру-шығуды реттейтін құрылғылар. Әрбір кіру оқиғасы жүйеде тіркеліп, есепте сақталады.

Қауіпсіздік дабылдары

Рұқсатсыз кіру, өрт, су тасқыны және басқа қауіпті жағдайларды анықтайтын сигнализациялар мен сенсорлар. Дабыл беру жүйесі қауіпсіздік қызметін дереу хабардар етеді.

Қауіпсіздік камераларының түрлері

IP камералар



Желі арқылы жұмыс істейді, жоғары ажыратымдылық, қашықтан басқару мүмкіндігі, аналитика функциялары бар.

Аналогтық камералар



Дәстүрлі, қарапайым және арзан шешім. Орнату оңай, бірақ функционалдығы шектеулі.

Смарт камералар



Қозғалыс детекторлары, түнгі көру, бет-әлпет тану және автоматты аналитика мүмкіндіктері.

Камераларды таңдау объектінің ерекшеліктеріне, қауіпсіздік талаптарына және бюджетке байланысты жүргізіледі. Қазіргі трендтер IP және смарт камераларға қарай бағытталған.

Қолжетімділікті бақылау құрылғылары

1 RFID карталар мен чиптер

Жанасу арқылы немесе қашықтан оқылатын электрондық идентификаторлар. Оңай пайдалану, жоғалған жағдайда тез блоктау мүмкіндігі, көптеген кіру нүктелерінде бір карта.

2 Биометриялық сканерлер

Саусақ ізі, бет-әлпет, көз торы арқылы сәйкестікті растау. Жоғары дәлдік, бұрмалау мүмкін емес, ыңғайлы пайдалану.

3 PIN-код жүйелері

Сандық кодтар арқылы кіру. Қарапайым, арзан, карта немесе биометрия қажет емес. Бірнеше қорғаныс деңгейі үшін басқа әдістермен үйлестіріледі.

Ең жоғары қауіпсіздік үшін екі немесе үш әдісті біріктіру (мультифакторлы аутентификация) ұсынылады.



Биометриялық технологиялардың жұмыс принципі

Биометриялық жүйелер адамның бірегей физиологиялық немесе мінез-құлық сипаттамаларын пайдаланады. Бұл технология ең жоғары қауіпсіздік деңгейін қамтамасыз етеді, өйткені биометриялық деректерді көшіру немесе беру мүмкін емес. Заманауи алгоритмдер 99.9% дәлдікпен адамды тануды қамтамасыз етеді.

Қолданылатын технологиялар мен инновациялар

Қауіпсіздік саласында технологиялық революция болып жатыр. Жасанды интеллект, машиналық оқыту, заттар интернеті (IoT) және үлкен деректерді талдау қауіпсіздік жүйелерін принципті жаңа деңгейге көтереді. Бұл инновациялар қауіп-қатерлерді алдын ала болжауға, автоматты шешім қабылдауға және адам факторына тәуелділікті азайтуға мүмкіндік береді.





IoT және смарт қауіпсіздік жүйелері

Заттар интернеті (Internet of Things) технологиясы барлық қауіпсіздік құрылғыларын бір желіге біріктіреді. Камералар, сенсорлар, дабылдар және бақылау терминалдары үздіксіз деректермен алмасып, орталықтандырылған басқару жүйесіне ақпарат жібереді.

Деректерді жинау

Барлық сенсорлар мен құрылғылар нақты уақытта ақпарат жібереді

Бұлтта өңдеу

Үлкен деректер талданады және жіктеледі

Визуализация

Оператор бірыңғай интерфейсте барлығын бақылайды

Автоматты әрекет

Жүйе дербес шешім қабылдап, әрекет етеді

Қашықтан басқару функциясы қауіпсіздік қызметіне кез келген жерден жүйені мониторингілеуге және басқаруға мүмкіндік береді.

Автоматтандырылған өрт дабылдары мен эвакуация жүйелері

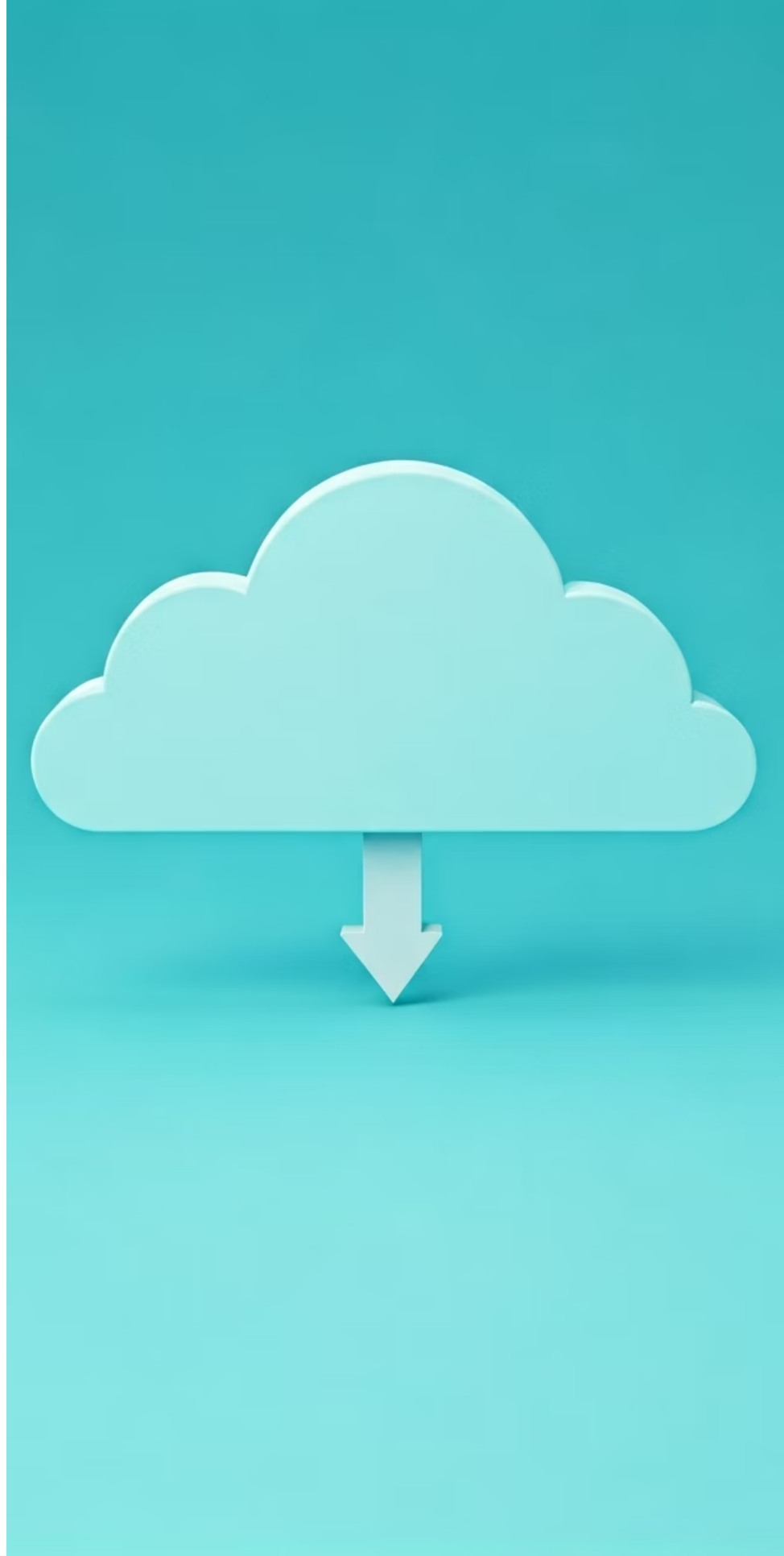


Өрт қауіпсіздігі жүйелері адам өмірін сақтаудың критикалық элементі болып табылады. ҚР Үкіметінің 2008 жылғы №796 қаулысына сәйкес, барлық қоғамдық және өндірістік объектілерде автоматты өрт дабыл жүйелері орнатылуы тиіс.

- **Түтін детекторлары мен жылу сенсорлары өртті анықтайды**
- **Дабыл жүйесі адамдарды дереу хабардар етеді**
- **Эвакуация жолдары автоматты жарықтандырылады**
- **Өрт сөндіру жүйелері іске қосылады**
- **Өрт қауіпсіздігі қызметіне сигнал жіберіледі**

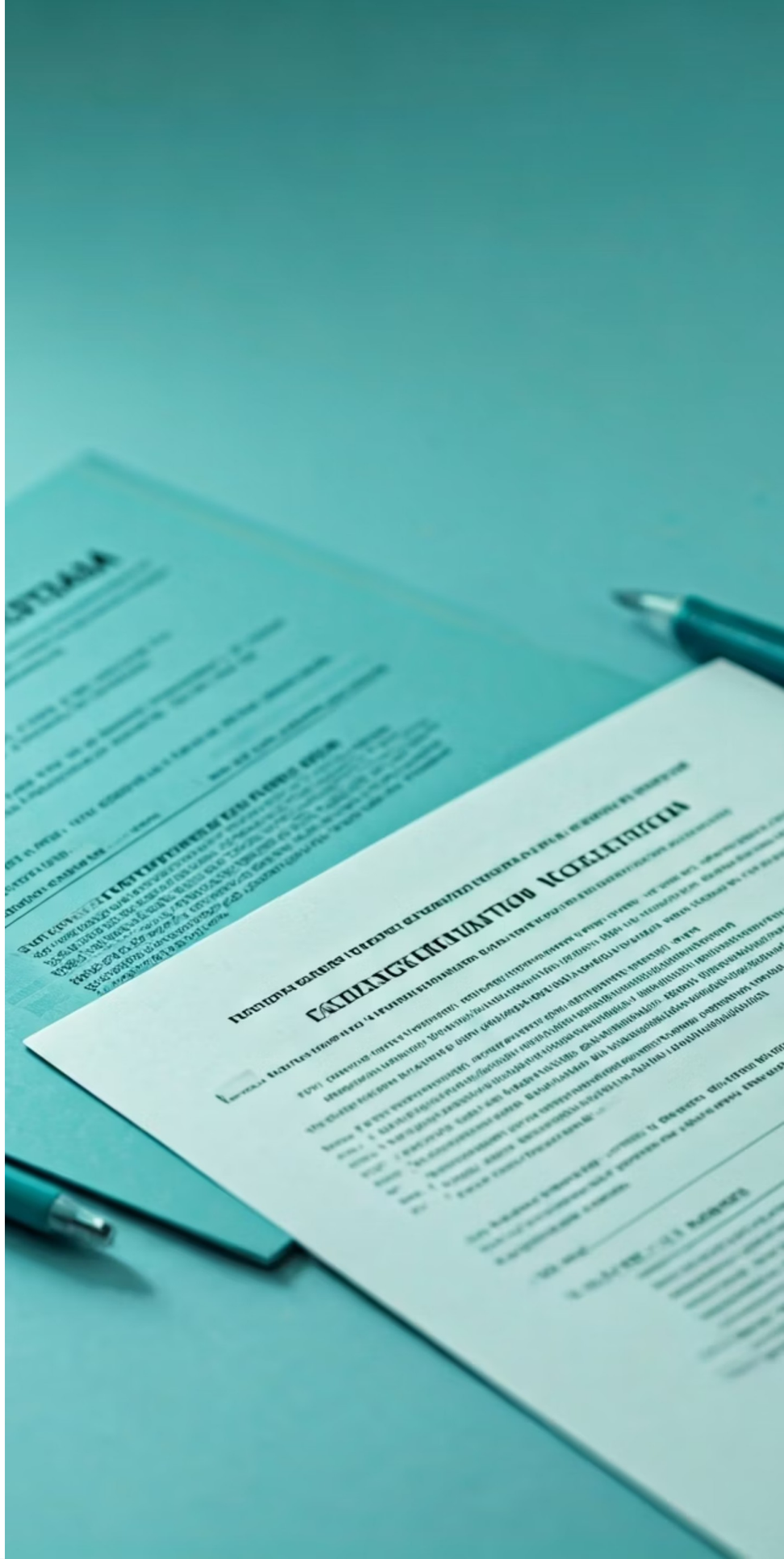
Смарт қауіпсіздік жүйесінің архитектурасы

Қазіргі заманғы қауіпсіздік жүйелері көп деңгейлі архитектураға негізделген. Дереккөздер деңгейінде сенсорлар мен камералар деректер жинайды, желілік деңгейде ақпарат беріледі, қолданбалар деңгейінде талдау және шешім қабылдау жүргізіледі, ал пайдаланушы деңгейінде визуализация және басқару жүзеге асырылады.



Құқықтық және нормативтік негіздер

Физикалық қорғау жүйелерін жобалау, орнату және пайдалану қатаң нормативтік-құқықтық базаға негізделуі тиіс. Қазақстан Республикасында қауіпсіздік жүйелеріне қойылатын талаптар техникалық регламенттер, мемлекеттік стандарттар және салалық нормативтер арқылы реттеледі.



Қазақстандағы техникалық регламенттер

1 "Объектілерді қорғауға арналған өрт техникасының қауіпсіздігіне қойылатын талаптар"

Қабылданған: 2017 жыл

Бұл регламент өрт қауіпсіздігі жүйелерінің техникалық сипаттамаларын, сертификаттау тәртібін, орнату және техникалық қызмет көрсету талаптарын белгілейді. Барлық өрт дабылдары мен автоматты өрт сөндіру жүйелері осы талаптарға сай болуы тиіс.

2 "Қозғалыс дабылының, бөгеуінің, байланысының және оны ақпараттандырудың қауіпсіздігіне қойылатын талаптар"

Қабылданған: 2018 жыл

Регламент қауіпсіздік жүйелерінің сигнал беру, тосқауылдар, байланыс желілері және ақпараттық компоненттеріне арналған. Жүйелердің үйлесімділігі, сенімділігі және киберқауіпсіздік талаптары қамтылған.

Барлық қауіпсіздік жүйелері мемлекеттік стандарттарға сертификатталуы және тиісті құжаттама болуы міндетті.

Қолжетімділікті бақылау жүйелеріне қойылатын талаптар

Құрылғылардың сәйкестігі

Қолданылатын барлық құрылғылар (терминалдар, сканерлер, карта оқығыштар) ҚР техникалық регламенттеріне сәйкес сертификатталуы тиіс. Өндіруші немесе жеткізуші қауіпсіздік сертификатын және сәйкестік декларациясын беруі міндетті.



Деректерді қорғау нормалары

Жеке деректерді өңдеу "Жеке деректер және оларды қорғау туралы" ҚР Заңына сәйкес жүргізілуі тиіс. Биометриялық деректер ерекше қорғау санатына жатады және оларды сақтау мен өңдеуге қосымша талаптар қойылады.



Құпиялылықты сақтау принциптері: деректерді шифрлау, рұқсат берілген қызметкерлердің ғана қолжетімділігі, аудит журналдарын жүргізу, тұрақты резервтік көшірмелер жасау.

Функционалдық қауіпсіздік стандарттары

1 Басқару жүйелерінің сенімділігі

Жүйе 24/7 режимінде үздіксіз жұмыс істеуі тиіс. Қосарланған серверлер, резервтік қуат көздері, автоматты сақтық көшірмелер міндетті. Жүйе істен шыққан жағдайда қалпына келтіру уақыты 1 сағаттан аспауы керек.

2 Мемлекеттік бақылау

Қауіпсіздік жүйелері мемлекеттік органдардың тұрақты бақылауына жатады. Жылына кемінде бір рет техникалық тексеру және аудит жүргізіледі. Сәйкессіздіктер анықталған жағдайда жоюға белгілі мерзім беріледі.

3 Аудит талаптары

Барлық кіру-шығу оқиғалары, жүйелік хабарламалар және ұйым әрекеттері журналға жазылуы және кемінде 1 жыл сақталуы тиіс. Аудит журналдары өзгертілуден қорғалуы керек.



Нормативтік-құқықтық база

Қазақстан Республикасының техникалық регламенттері мен стандарттары халықаралық тәжірибені ескере отырып әзірленген. Олар ISO, IEC халықаралық стандарттарына сәйкес келеді және еуропалық EN стандарттарын ескереді. Бұл отандық қауіпсіздік жүйелерінің әлемдік деңгейге сәйкестігін қамтамасыз етеді.



Физикалық қорғау жүйелерінің жобалануы мен енгізілуі

Қауіпсіздік жүйесін сәтті енгізу жан-жақты жоспарлауды және кезең-кезеңімен орындауды талап етеді. Әрбір кезең өзінің міндеттері мен нәтижелерімен сипатталады. Жобалау процесі объектінің ерекшеліктерін толық ескеруі және тұтынушының барлық талаптарын қанағаттандыруы тиіс.

Қауіпсіздік аудиті және тәуекелдерді бағалау

Объектінің ерекшеліктерін анықтау

- Ғимараттың сәулет-жоспар шешімдері
- Кіру-шығу нүктелерінің саны мен орналасуы
- Қорғалатын аймақтардың саны
- Қызметкерлер мен келушілер саны
- Қолданыстағы қауіпсіздік шаралары

Қауіп-қатерлерді талдау

- Рұқсатсыз кіру ықтималдығы
- Ұрлық және вандализм қаупі
- Өрт қауіпсіздігі тәуекелдері
- Табиғи апаттар қаупі
- Ішкі қауіп-қатерлер (қызметкерлер әрекеттері)

Аудит қорытындысы бойынша тәуекелдер матрицасы құрылады және әрбір тәуекел үшін азайту шаралары әзірленеді. Жүйелік шешімдер барлық анықталған қауіп-қатерлерді жабуы тиіс.



Жүйені жобалау кезеңдері

Қажеттіліктерді анықтау

Тұтынушымен бірлесіп техникалық тапсырма әзірлеу, функционалдық және техникалық талаптарды нақтылау, бюджет пен мерзімдерді келісу.

Құрылғыларды таңдау

Техникалық сипаттамалар бойынша жабдықты таңдау, өндірушілер мен жеткізушілерді салыстыру, сертификаттар мен кепілдіктерді тексеру.

Жобалау

Толық жоба құжаттамасын дайындау: сызбалар, сметалар, техникалық спецификациялар, орнату кестелері.

Интеграциялау

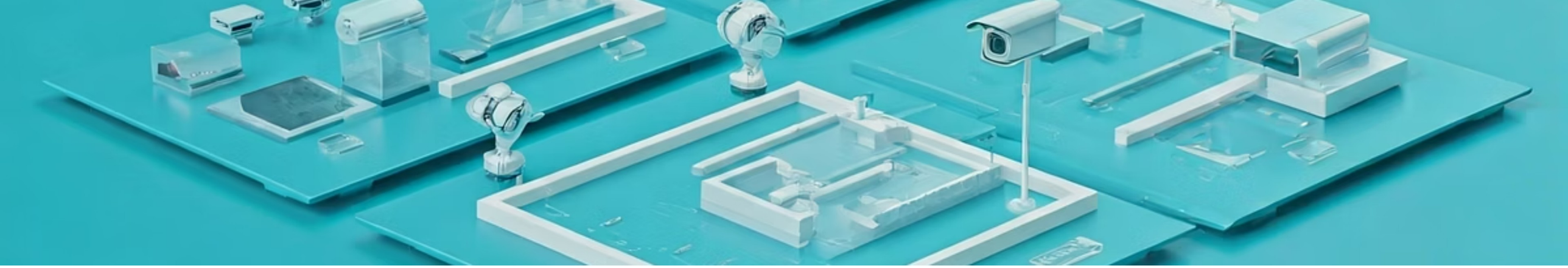
Барлық жүйелерді бір платформаға біріктіру, қолданыстағы инфрақұрылыммен үйлестіру, деректер алмасу протоколдарын баптау.

Орнату және тестілеу

Жабдықты монтаждау, желілік инфрақұрылыманы жайластыру, жүйені баптау және кешенді сынақтан өткізу.

Пайдалануға беру

Қызметкерлерді оқыту, қолдау регламентін белгілеу, құжаттаманы тапсыру және кепілдік қызметін бастау.



Өндірістік объектідегі қауіпсіздік жүйесінің жоспары

Толық жүйе периметрлік қорғаныс, аймақтық бақылау және критикалық нүктелердегі күшейтілген қауіпсіздік деңгейлерін біріктіреді. Орталық бақылау бөлмесінен барлық жүйелер нақты уақытта басқарылады және мониторингіленеді.

Қолжетімділікті бақылау жүйелерінің артықшылықтары мен шектеулері

Қолжетімділікті бақылау жүйелері объектінің қауіпсіздігін айтарлықтай арттырады, бірақ олардың шектеулері мен қиындықтары да бар. Жүйені енгізу туралы шешім қабылдағанда барлық жағдайларды қарастыру маңызды.



При создании этого изображения произошла ошибка

Артықшылықтары

Қауіпсіздікті арттыру

Рұқсатсыз кіруді болдырмау, инциденттер санын азайту, объектінің жалпы қорғау деңгейін жоғарылату. Статистика бойынша, қауіпсіздік жүйелері ұрлықтар мен вандализм оқиғаларын орташа 60-70%-ға қысқартады.

Қозғалысты бақылау

Қызметкерлер мен келушілердің қозғалысын толық мониторингілеу. Кім, қашан, қайда кіргенін нақты білу. Жұмыс уақытын есепке алу және еңбек тәртібін жақсарту мүмкіндігі.

Құқық бұзушылықтарды азайту

Қауіпсіздік жүйелерінің болуы өзі профилактикалық әсер етеді. Адамдар бақылауда екенін білгенде заң бұзу ықтималдығы төмендейді. Инцидент болған жағдайда жазбалар дәлел ретінде пайдаланылады.

Шектеулері

1

Жеке деректерді қорғау мәселелері

Биометриялық деректерді жинау мен сақтау құпиялылық туралы сұрақтар туғызады. Заңнамаға сәйкес келу, қызметкерлер мен келушілердің келісімін алу, деректердің қауіпсіздігін қамтамасыз ету қажет. Дұрыс басқарылмаған жағдайда құқықтық тәуекелдер туындайды.

2

Техникалық ақаулар

Кез келген техника істен шығуы мүмкін. Жабдықтың сапасына, климаттық жағдайларға, электр желісінің тұрақтылығына тәуелділік. Резервтік жүйелер мен қосарлау арқылы тәуекелдерді азайтуға болады, бірақ бұл қосымша шығындар талап етеді.

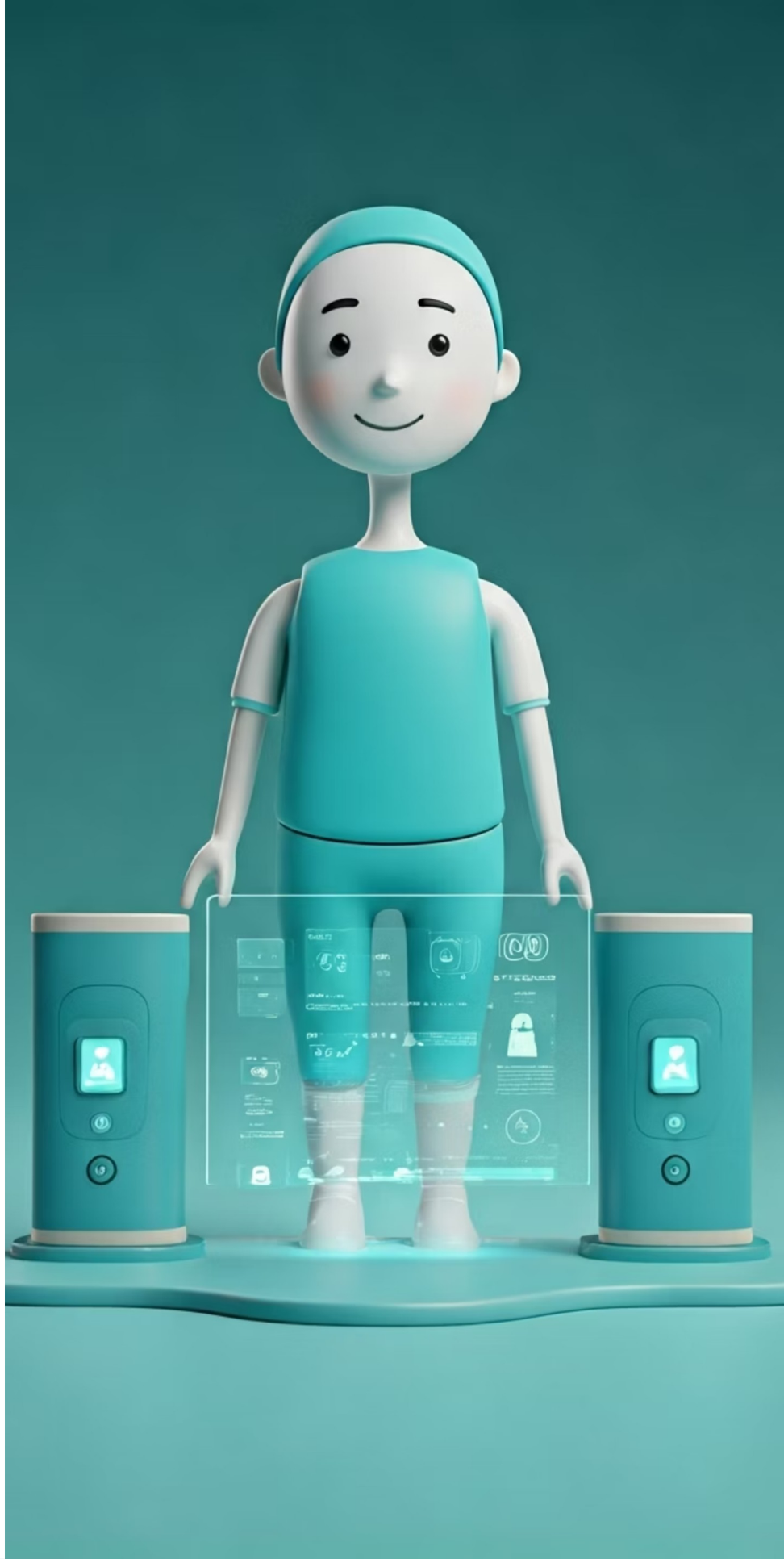
3

Қаржылық шығындар

Жүйені сатып алу мен орнатудың бастапқы құны жоғары болуы мүмкін. Тұрақты техникалық қызмет көрсету, жөндеу, жаңарту қажет. Оператор мен қауіпсіздік қызметкерлерін оқытуға кететін шығындар. Дегенмен, ұзақ мерзімді перспективада инвестиция өтеледі.

Қазіргі заманғы трендтер мен болашақ бағыттар

Қауіпсіздік технологиялары қарқынды дамуда. Жасанды интеллект, үлкен деректерді талдау, биометрияның жаңа әдістері, IoT құрылғыларының кеңеюі – бұл трендтер келесі жылдары қауіпсіздік жүйелерін түбегейлі өзгертеді. Автоматтандыру деңгейі артып, адам қатысуының қажеттілігі азаяды.



Биометрияның дамуы

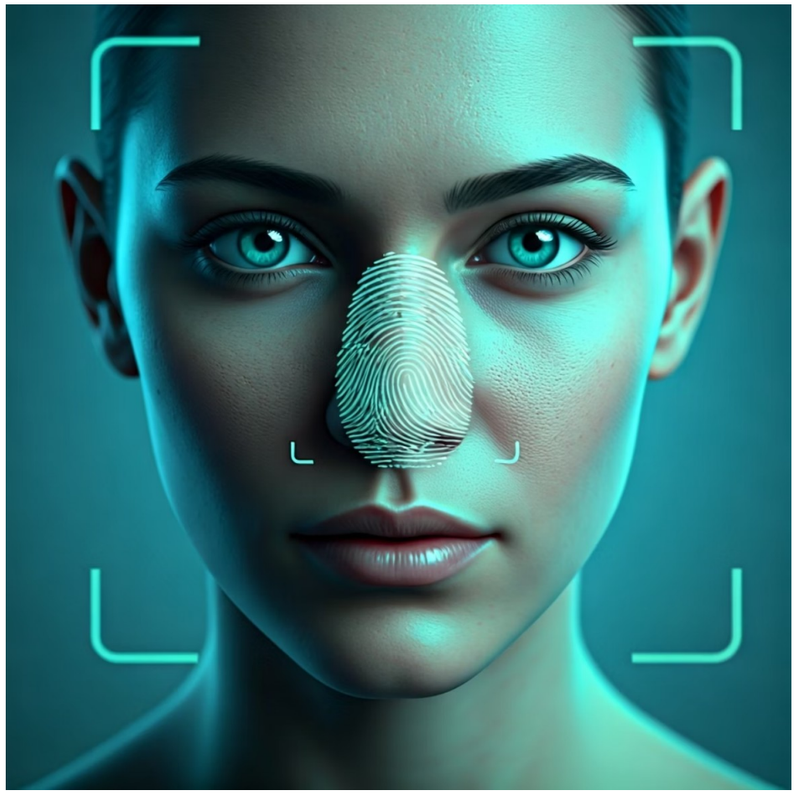
Биометриялық технологиялар жылдан жылға жетіліп келеді. Дәлдік пен жылдамдық артып, құны төмендеп жатыр. Жаңа әдістер: жүрісті тану, дауысты талдау, жүрек соғысын анықтау, веналық өрнекті сканерлеу.



Тану дәлдігі



Процесс жылдамдығы (секунд)



Көп факторлы биометриялық аутентификация (мысалы, бет-әлпет + саусақ ізі) максималды қауіпсіздік қамтамасыз етеді. Бұрмалау мүмкіндігі іс жүзінде нөлге тең.

Жасанды интеллект пен аналитика

Қауіп-қатерді болжау

ЖИ тарихи деректерді талдап, келесі инциденттердің ықтималдығын есептейді

Мінез-құлықты талдау

Адамдардың қозғалыс үлгілерін оқып, күдікті әрекеттерді анықтайды

Автоматты шешім

Жүйе өзі шешім қабылдап, қауіпсіздік шараларын іске қосады

Үздіксіз оқу

Машиналық оқыту арқылы жүйе үнемі жақсарып отырады

Жасанды интеллект жалған дабылдар санын 80%-дан астамға қысқартады және инциденттерге жауап беру уақытын 10 есеге дейін азайтады.
.Операторға шынайы қауіп-қатерлер ғана хабарланады





Смарт ғимараттар мен интеграцияланған қауіпсіздік жүйелері

Смарт ғимараттар концепциясы барлық инженерлік жүйелерді бір платформада біріктіреді. Қауіпсіздік жүйелері жарықтандыру, климат-бақылау, лифттер, өрт қауіпсіздігі жүйелерімен тығыз байланыста жұмыс істейді.

Бір платформа

Барлық жүйелер бірыңғай интерфейстен басқарылады. Оператор бір экраннан қауіпсіздік, климат, жарық, лифттерді реттей алады. Жүйелер бір-бірімен ақпарат алмасады.

Энергия үнемдеу

Қолжетімділік жүйесі қызметкерлердің болу-болмауын анықтап, жарық пен климат-бақылауды автоматты реттейді. Бос бөлмелерде жарық сөніп, кондиционер тоқтайды.

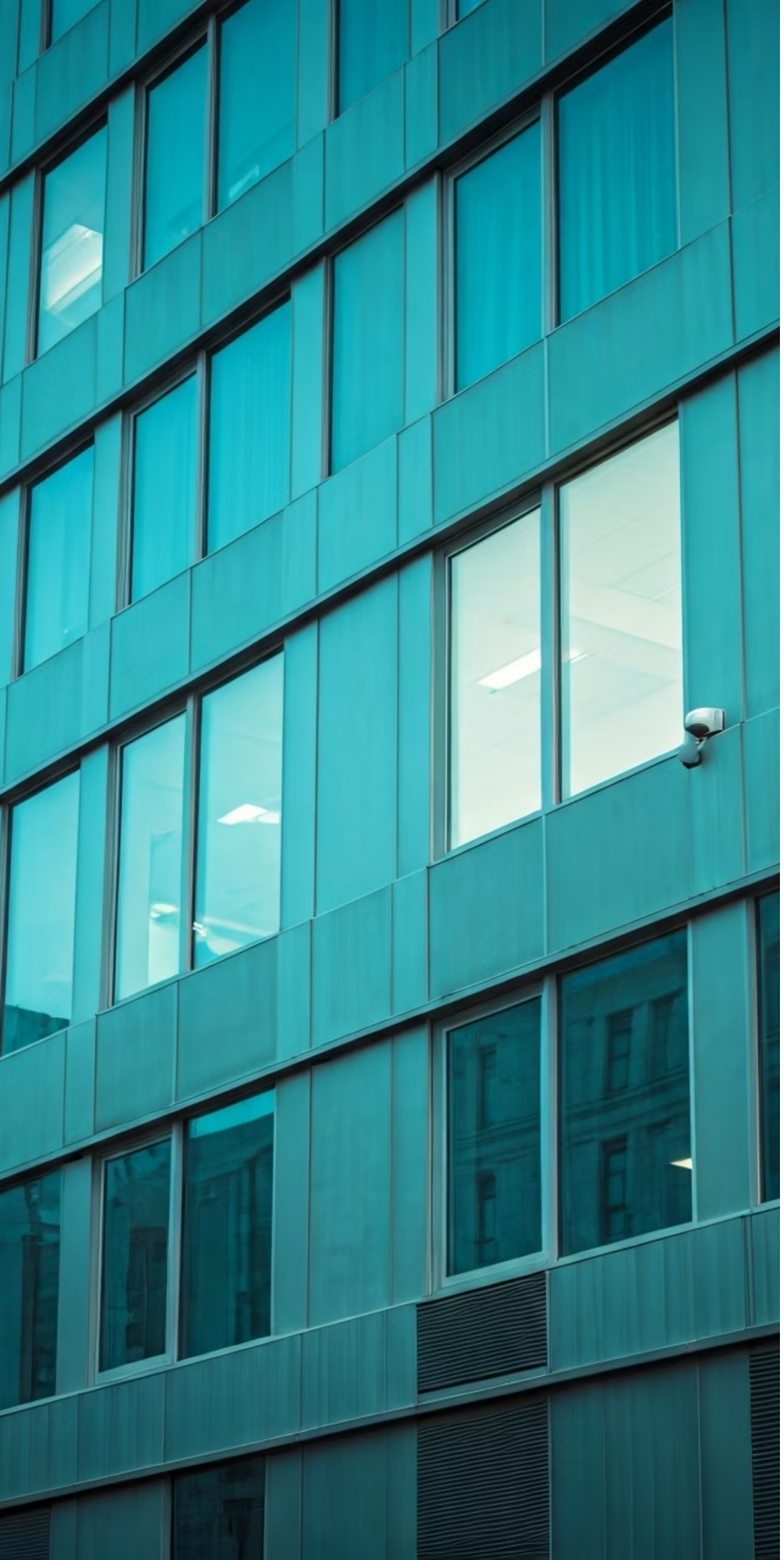
Тиімділік

Автоматтандыру операциялық шығындарды 30-40%-ға қысқартады. Қызмет көрсету оңайланып, проблемаларды жедел анықтау мүмкіндігі пайда болады.

Болашақ қауіпсіздік жүйелері

Алдағы 5-10 жылда қауіпсіздік жүйелері танымайтындай өзгереді. Голографиялық интерфейстер, дронмен патрульдеу, квант шифрлау, нейро-интерфейстер – бұлар ғылыми фантастика емес, болашақтың нақты технологиялары. Әрбір адамның цифрлық қосағы болып, виртуалды және физикалық қауіпсіздік толық интеграцияланады.





Іс жүзіндегі мысалдар мен тәжірибелер

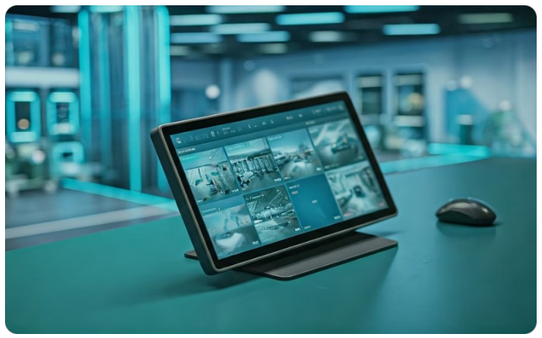
Теория мен практиканың айырмашылығы үлкен. Нақты объектілерде қауіпсіздік жүйелерін енгізу тәжірибесі құнды сабақтар береді. Қазақстандағы және әлем бойындағы сәтті жобалар басқа ұйымдарға бағдар болады.

Қазақстандағы ірі нысандардағы физикалық қорғау жүйелері



Астана қаласындағы әкімшілік ғимараттар

Мемлекеттік органдардың ғимараттарында көп деңгейлі қауіпсіздік жүйелері енгізілген. Периметрлік қорғаныс, биометриялық қолжетімділік бақылау, бейнеталдау жүйелері 24/7 режимінде жұмыс істейді. Кіру-шығуды бақылаудың 4 деңгейі бар.



Өндірістік кешендердегі қауіпсіздік

Қарағанды және Атырау облыстарындағы өндірістік кешендерде кешенді қауіпсіздік шаралары қолданылады. Камералар, датчиктер, автоматты дабыл жүйелері құнды жабдық пен қызметкерлердің қауіпсіздігін қамтамасыз етеді.

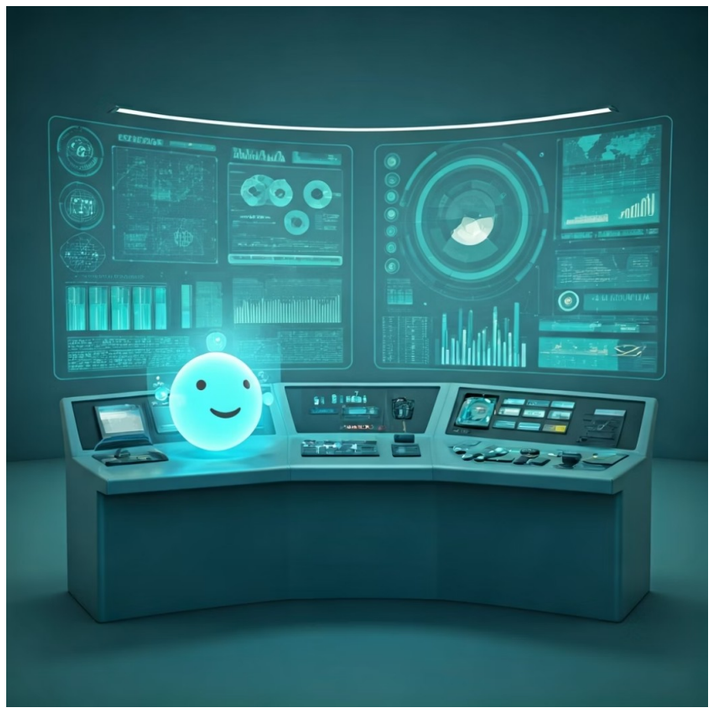


Сауда орталықтары

Алматы мен Астанадағы ірі сауда орталықтарында жетілдірілген қауіпсіздік жүйелері қолданылады. Келушілердің санын есептеу, бет-әлпет тану, автоматты инцидент анықтау функциялары іске қосылған.

Халықаралық тәжірибе

АҚШ



Америкада қауіпсіздік технологияларына жылына 100 млрд доллардан астам инвестиция салынады. Жасанды интеллект, квант шифрлау, автономды қауіпсіздік роботтары белсенді пайдаланылады.

Еуропа



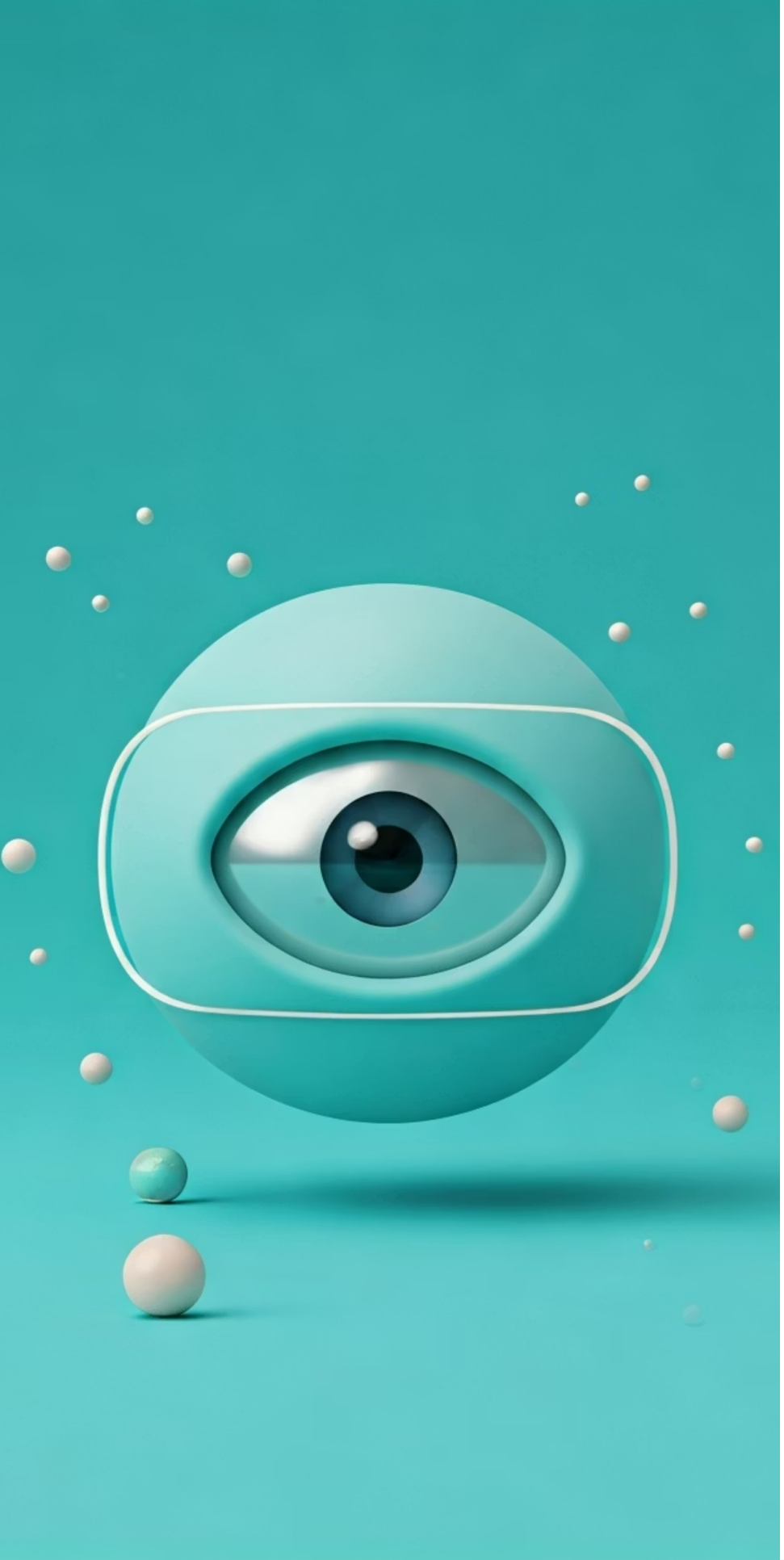
Еуропалық елдерде құпиялылық пен қауіпсіздік арасындағы теңгерім басты назарда. GDPR талаптарына сәйкес жүйелер енгізіліп, деректерді қорғау ең жоғары деңгейде.

Азия



Жапония, Оңтүстік Корея, Сингапур қауіпсіздік инновацияларының көшбасшылары. Смарт қалалар концепциясы, бет-әлпет тану технологиялары, IoT сенсорлар кеңінен қолданылады.

Қазақстан үшін озық халықаралық тәжірибені зерделеу және ұлттық ерекшеліктерді ескере отырып бейімдеу маңызды.



Қауіпсіздік саласындағы инновациялық жобалар

Компьютерлік көру жобалары

Қазақстанда бірнеше IT-компаниялар компьютерлік көру технологияларын әзірлеуде. Бұл жобалар объектілерді автоматты тану, мінез-құлықты талдау, инциденттерді болжау функцияларын қамтиды. Отандық әзірлемелер импорттық шешімдерден 2-3 есе арзан.

ЖИ негізіндегі қауіпсіздік

Жасанды интеллект үлкен деректер массивін талдап, қауіп-қатер үлгілерін анықтайды. Машиналық оқыту алгоритмдері үнемі жетіліп, дәлдік артып отырады. Интеллектуалды аналитика қауіпсіздік қызметінің тиімділігін 5-7 есе арттырады.

Құрметбек Бекболаттың 2023 жылғы зерттеуі компьютерлік көрудің Қазақстан жағдайларында тиімділігін растайды.