Техникалық құралдар және ақпаратты қорғау әдістері

Ержан Асел Ануаркызы,Ph.D., қауымдастырылған профессор

Assel.yerzhan@satbayev.university



Ақпаратты қорғаудағы аутентификация және авторизация әдістері



Ақпараттық қауіпсіздіктің негіздері

Ақпараттық қауіпсіздік – бұл ақпаратты рұқсатсыз қол жеткізуден, өзгертуден және жоюдан қорғау жүйесі. Қазіргі заманғы технологиялар дамуымен қатар, қауіпсіздік қатерлері де күрделене түсуде. Сондықтан қауіпсіздіктің негізгі компоненттерін түсіну әрбір мамандың міндеті болып табылады.

Қауіпсіздік жүйесі үш негізгі процеске негізделеді: пайдаланушыны анықтау, оның жеке басын растау және рұқсат деңгейін белгілеу. Бұл үш компонент бірлесіп жұмыс істегенде ғана толық қорғаныс қамтамасыз етіледі.

Ақпараттық қауіпсіздік үш тірегі

Идентификация

Пайдаланушыны анықтау процесі. Жүйеге кім кіргісі келетінін білдіру кезеңі. Бұл – қауіпсіздік тізбегінің бірінші буыны.

Аутентификация

Пайдаланушының шынайылығын растау. Ол шын мәнінде өзі екенін дәлелдеу процесі. Біліміңіз, иеліктегі заттарыңыз немесе биометрияңыз арқылы расталады.

Авторизация

Рұқсат деңгейін анықтау. Пайдаланушыға қандай ресурстарға қол жеткізуге болатынын белгілеу. Құқықтар мен рөлдерді басқару механизмі.

Осы үш процесс бір-бірімен тығыз байланысты және бірін-бірі толықтырады. Әрқайсысы жүйенің жалпы қауіпсіздігіне өз үлесін қосады және олардың біреуі әлсіз болса, бүкіл қорғаныс жүйесі тәуекел астында қалуы мүмкін.



Ақпараттық қауіпсіздік үшбұрышы



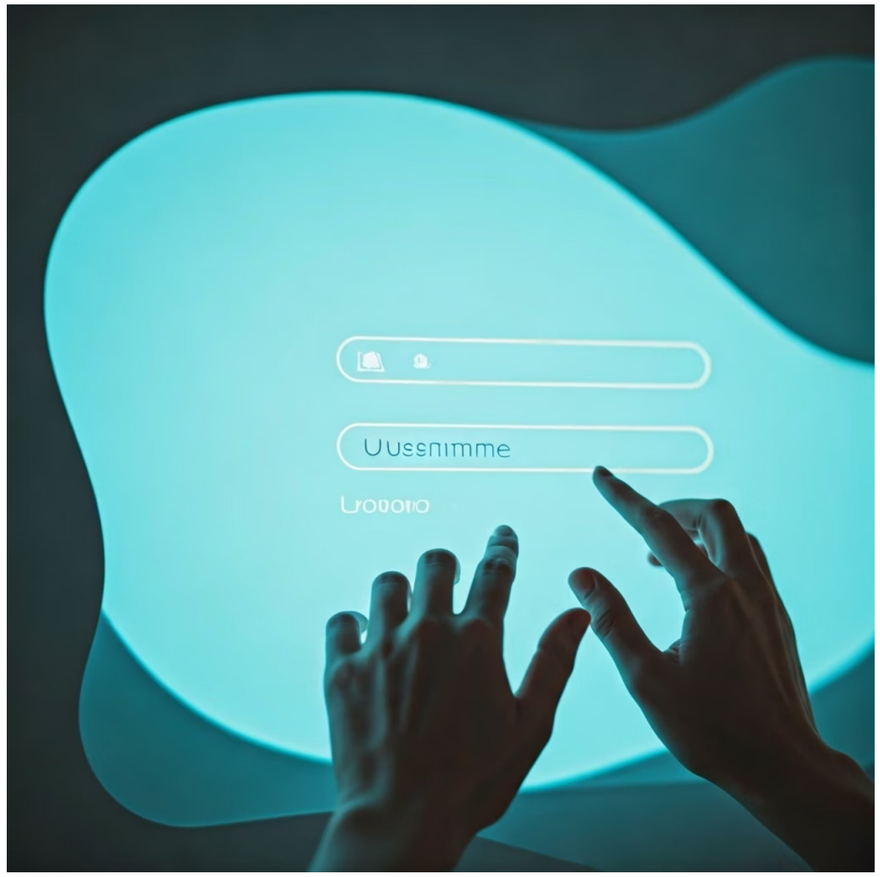
Қауіпсіздік үшбұрышы – идентификация, аутентификация және авторизация процестерінің өзара байланысын көрсететін концепция. Бұл үш элемент бір-бірінсіз жұмыс істей алмайды және қауіпсіздіктің тұтас жүйесін құрайды.

Идентификация дегеніміз не?

Идентификация – пайдаланушының жеке басын анықтау процесі. Бұл қауіпсіздік тізбегінің бірінші сатысы болып табылады. Идентификация кезінде пайдаланушы жүйеге өзінің кім екенін хабарлайды, бірақ әлі де оны дәлелдемейді.

Идентификаторлар әртүрлі болуы мүмкін:

- Жеке сәйкестендіру нөмірі (ЖСН)
- Пайдаланушы аты немесе логин
- Электрондық пошта мекенжайы
- Телефон номері
- Жеке идентификациялық код



Идентификация – бұл өзіңізді таныстыру, ал аутентификация – өзіңіз екеніңізді дәлелдеу.

Қазақстанда ең көп қолданылатын идентификатор – бұл ИИН (жеке сәйкестендіру нөмірі). Ол электрондық үкімет жүйелерінде, банктік қызметтерде және басқа да цифрлық платформаларда кеңінен пайдаланылады.

Аутентификация әдістері

Құпия сөздер мен PIN-кодтар

Ең көне және кең таралған әдіс. Пайдаланушы тек өзі білетін құпия ақпаратты енгізеді. Қарапайымдылығына қарамастан, әлсіз құпия сөздер жүйенің негізгі осалдығы болып табылады.

Биометриялық мәліметтер

Саусақ ізі, бет-әлпет тану, көз қарашығының сканері, дауыс тану сияқты биологиялық сипаттамалар. Қазіргі смартфондар мен ноутбуктардың көпшілігінде орнатылған.

Электрондық цифрлық қолтаңба

ЭЦҚ – Қазақстанда кеңінен қолданылатын аутентификация құралы. Ұлттық куәландырушы орталығы шығарған сертификаттар негізінде жұмыс істейді және заңды күші бар.

Заманауи жүйелер көбінесе бірнеше аутентификация әдісін біріктіреді. Бұл көпфакторлы аутентификация деп аталады және қауіпсіздік деңгейін айтарлықтай арттырады.

Авторизация: Қауіпсіздік деңгейін басқару

Қол жеткізу құқықтарын анықтау

Авторизация – пайдаланушы аутентификациядан өткеннен кейін оған қандай ресурстарға қол жеткізуге рұқсат етілетінін анықтау процесі. Бұл қауіпсіздік жүйесінің үшінші және соңғы сатысы.

Авторизация келесі сұрақтарға жауап береді:

- Пайдаланушы қандай файлдарды көре алады?
- Қандай деректерді өзгерте алады?
- Қандай функцияларды орындай алады?
- Қандай әрекеттерге құқығы бар?

Авторизация жүйелері

1 Рөлдік авторизация (RBAC)

Пайдаланушыларды рөлдерге бөлу және әр рөлге белгілі құқықтар тағайындау.

2 Атрибуттық авторизация (ABAC)

Пайдаланушы атрибуттары, ресурс сипаттамалары және орта контексті негізінде құқықтарды анықтау.



Авторизацияның визуалды бейнесі

> Авторизация – бұл дұрыс кілтті дұрыс құлыпқа салу сияқты. Әрбір пайдаланушының өзінің кілттері бар, ал жүйе қайсысына қай есікті ашуға рұқсат беретінін білуі керек.

Құлып пен кілт – авторизацияның классикалық метафорасы. Кілт (аутентификация деректері) дұрыс болғанымен, ол белгілі бір құлыптарды ғана (ресурстарды) аша алады.

Аутентификацияның заманауи әдістері

Технологиялардың дамуымен аутентификация әдістері де үнемі жетілдіріліп отырады. Қазіргі заманғы жүйелер қауіпсіздік пен ыңғайлылықты теңестіруге тырысады. Биометрия, көпфакторлы аутентификация және жасанды интеллект негізіндегі шешімдер стандартқа айналып келеді.

Бұл бөлімде біз аутентификацияның ең заманауи және тиімді әдістерін қарастырамыз.



Құпия сөздердің шектеулері

81%

Әлсіз парольдер

Ақпараттық қауіпсіздік бұзылуларының 81%-ы әлсіз немесе ұрланған құпия сөздермен байланысты.

65%

Қайталанатын парольдер

Пайдаланушылардың 65%-ы бірнеше жүйеде бір құпия сөзді қолданады.

Негізгі мәселелер

- **Әлсіз құпия сөздер:** "123456", "password" сияқты оңай болжамды комбинациялар
- **Фишинг шабуылдары:** алдау арқылы құпия сөздерді ұрлау
- **Brute force әдісі:** барлық мүмкін комбинацияларды қарау
- **Деректер базаларының бұзылуы:** ірі компаниялардан құпия сөздердің ағуы
- **Адамдық фактор:** құпия сөздерді жазып қою немесе басқалармен бөлісу

Зерттеулер көрсеткендей, орташа пайдаланушы 100-ден астам парольді есте сақтауға тырысады.

Осы мәселелерді шешу үшін қауіпсіздік саласы құпия сөздерден гөрі сенімді әдістерге көшуде. Биометрия, токендер және көпфакторлы аутентификация келешектің бағыты болып табылады.

Көпфакторлы аутентификация (MFA)

Көпфакторлы аутентификация (MFA) – қауіпсіздікті арттырудың ең тиімді әдістерінің бірі. Ол бірнеше тәуелсіз растау әдістерін біріктіреді, бұл шабуылшыларға жүйеге кіруді айтарлықтай қиындатады.

01

Біліміңіз (Knowledge)

Құпия сөз, PIN-код немесе тек сіз білетін басқа ақпарат

02

Иеліктегі заттарыңыз (Possession)

Смартфон, токен, смарт-карта немесе сізде бар басқа құрылғы

03

Биометриялық деректер (Inherence)

Саусақ ізі, бет-әлпет, көз қарашығы немесе дауыс

MFA-ның артықшылықтары

- Қауіпсіздік деңгейінің айтарлықтай артуы
- Фишинг шабуылдарынан қорғау
- Парольдердің ұрлануынан сақтандыру
- Нормативтік талаптарға сәйкестік

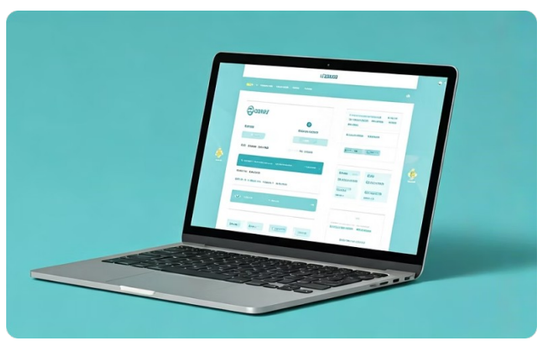
Қолдану мысалдары

- Банктік қосымшалар: пароль + SMS код
- Корпоративтік жүйелер: смарт-карта + PIN
- Бұлтты қызметтер: пароль + аутентификатор қосымшасы



Қазақстандағы MFA тәжірибесі

Қазақстанда көпфакторлы аутентификация белсенді енгізілуде. Мемлекеттік және коммерциялық ұйымдар бұл технологияны қауіпсіздікті арттыру үшін белсенді қолданады.



eGov порталы

Электрондық үкімет порталы бірнеше аутентификация әдістерін ұсынады: ЭЦҚ, мобильді қосымша арқылы растау, логин/пароль + SMS коды. Пайдаланушылар қауіпсіздік деңгейіне қарай әдісті таңдай алады.



QR-код аутентификациясы

Көптеген қазақстандық жүйелер QR-код арқылы кіруді қолдайды. Пайдаланушы экрандағы кодты сканерлейді және мобильді қосымша арқылы расталады. Бұл әдіс жылдам әрі қауіпсіз.



ЭЦҚ + қосымша фактор

Маңызды транзакциялар үшін ЭЦҚ басқа аутентификация әдістерімен толықтырылады. Мысалы, электрондық қолтаңба + SMS растау немесе биометрия.

Электрондық цифрлық қолтаңба (ЭЦҚ)

ЭЦҚ – Қазақстанда қолданылатын аутентификация мен құжаттарды куәландырудың заңды тұрғыдан танылған әдісі. Ұлттық куәландырушы орталығы (ҰКО) шығарған электрондық сертификаттар негізінде жұмыс істейді.

ЭЦҚ-ның негізгі функциялары:

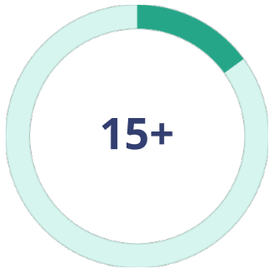
- **Аутентификация:** электрондық жүйелерге кіру
- **Қолтаңба қою:** электрондық құжаттарға қол қою
- **Шифрлау:** деректерді қорғау
- **Тұтастықты растау:** құжаттың өзгермегенін дәлелдеу

Қолдану салалары:

1. Электрондық үкімет порталы
2. Банктік жүйелер және төлемдер
3. Электрондық сауда алаңдары
4. Мемлекеттік сатып алу порталы
5. Салық және кеден жүйелері



Маңызды: ЭЦҚ сертификатының заңды күші қағаз қолтаңбамен тең. "Электрондық құжат және электрондық цифрлық қолтаңба туралы" ҚР Заңымен реттеледі.



жыл ҚР-да ЭЦҚ қолданылуда





ЭЦҚ технологиясы

Ашық кілт

Сертификатта сақталады, кез келген адам қол жеткізе алады. Қолтаңбаны тексеру және деректерді шифрлау үшін қолданылады.

Жабық кілт

Токенде немесе смарт-картада қауіпсіз сақталады. Құжатқа қол қою және деректерді дешифрлау үшін қолданылады. Ешқашан құрылғыдан шықпайды.

Сертификат

ҰКО шығарған электрондық құжат. Иесінің деректері, ашық кілті, қолдану мерзімі және ҰКО-ның ЭЦҚ-сы бар.

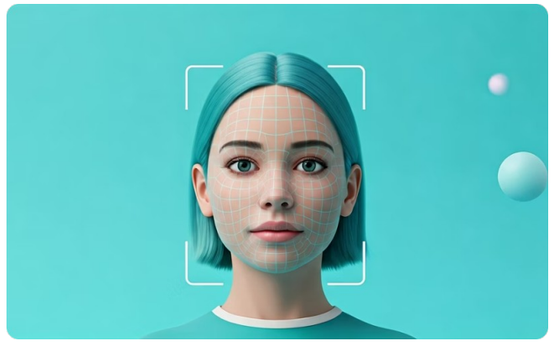
Биометриялық аутентификация

Биометриялық аутентификация – адамның бірегей физиологиялық немесе мінез-құлық сипаттамаларын пайдаланатын әдіс. Бұл технология соңғы жылдары тез дамып, күнделікті өмірдің ажырамас бөлігіне айналды.



Саусақ ізі сканері

Ең кең таралған биометриялық әдіс. Смартфондар, ноутбуктар, сейфтер және есік құлыптарында қолданылады. Жылдам, дәл және ыңғайлы.



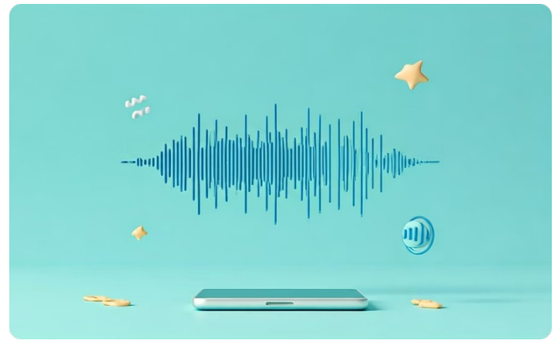
Бет-әлпет тану

3D камералар немесе жоғары ажыратымдылықты сенсорлар арқылы адамның бетін талдайды. Apple Face ID және Windows Hello сияқты жүйелерде кеңінен қолданылады.



Көз қарашығын сканерлеу

Көздің ішкі құрылымын талдайды. Өте жоғары дәлдік деңгейі, бірақ арнайы жабдық қажет. Әуежайлар мен жоғары қауіпсіздік талап етілетін жерлерде қолданылады.



Дауыс тану

Адамның дауысының ерекшеліктерін талдайды. Қашықтан аутентификация үшін ыңғайлы, мысалы телефон арқылы банкпен байланыста.

Артықшылықтары

- Құпия сөзді есте сақтау қажет емес
- Жоғалту немесе ұрлау мүмкін емес
- Жылдам және ыңғайлы
- Өте жоғары дәлдік

Кемшіліктері

- Жабдықтың қымбаттығы
- Қолайсыз жағдайда қателер (кір қолдар, нашар жарық)
- Жеке өмірдің құпиялылығына қатысты алаңдаушылық
- Биометриялық деректерді жаңарту мүмкін емес

Авторизация әдістері мен тәжірибелері

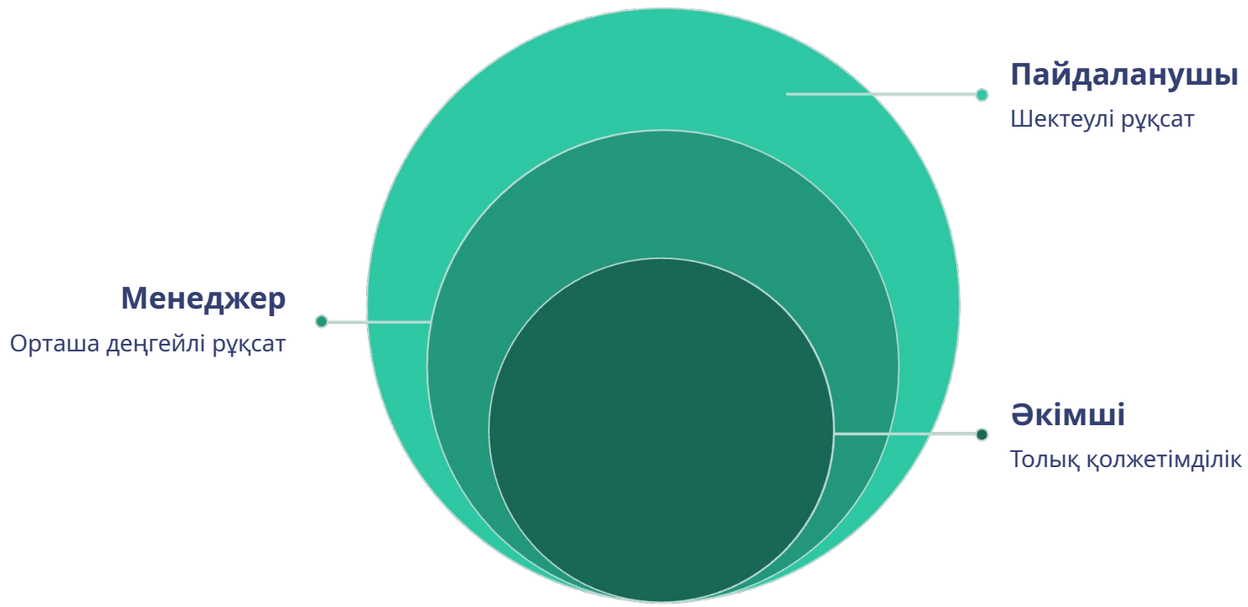
Авторизация – пайдаланушылардың жүйедегі құқықтары мен рұқсаттарын басқару процесі. Аутентификациядан өткеннен кейін жүйе пайдаланушыға нені көруге, өзгертуге немесе орындауға болатынын анықтайды.

Тиімді авторизация жүйесі қауіпсіздікті қамтамасыз етумен қатар, пайдаланушыларға олардың міндеттерін орындау үшін қажетті ресурстарға ыңғайлы қол жеткізуді ұсынады.



Рөлдік негізделген авторизация (RBAC)

RBAC (Role-Based Access Control) – авторизацияның ең танымал және кеңінен қолданылатын моделі. Бұл әдісте пайдаланушыларға тікелей емес, рөлдер арқылы құқықтар беріледі.



Әкімші (Administrator)

Жүйенің барлық функцияларына толық қол жеткізу. Пайдаланушыларды басқару, параметрлерді өзгерту, барлық деректерді көру және өңдеу құқығы.

Менеджер (Manager)

Өз бөлімінің немесе жобасының деректеріне қол жеткізу. Есептер жасау, өз командасының жұмысын қарау және координациялау мүмкіндігі.

Қарапайым пайдаланушы (User)

Тек өз жұмысына қажетті функциялар мен деректерге қол жеткізу. Жеке ақпаратты көру және қарапайым әрекеттерді орындау.

Қонақ (Guest)

Ең шектеулі құқықтар жиынтығы. Тек жалпыға қолжетімді ақпаратты көру, ешқандай өзгерістер енгізе алмайды.

RBAC-тың артықшылықтары

- Құқықтарды басқаруды жеңілдетеді
- Масштабталатын шешім
- Аудит және бақылау жеңілдетіледі
- Қателіктер тәуекелін азайтады
- Нормативтік талаптарға сәйкестік

Қолдану мысалдары

- Корпоративтік ERP жүйелер
- Бухгалтерлік бағдарламалар
- Контент басқару жүйелері (CMS)
- Электрондық құжат айналымы
- Ақпараттық жүйелер мен дерекқорлар

Атрибуттық негізделген авторизация (ABAC)

ABAC (Attribute-Based Access Control) – контекстке сезімтал авторизация моделі. Қол жеткізу шешімдері пайдаланушы атрибуттары, ресурс сипаттамалары және қоршаған орта контексті негізінде қабылданады.

Уақыт

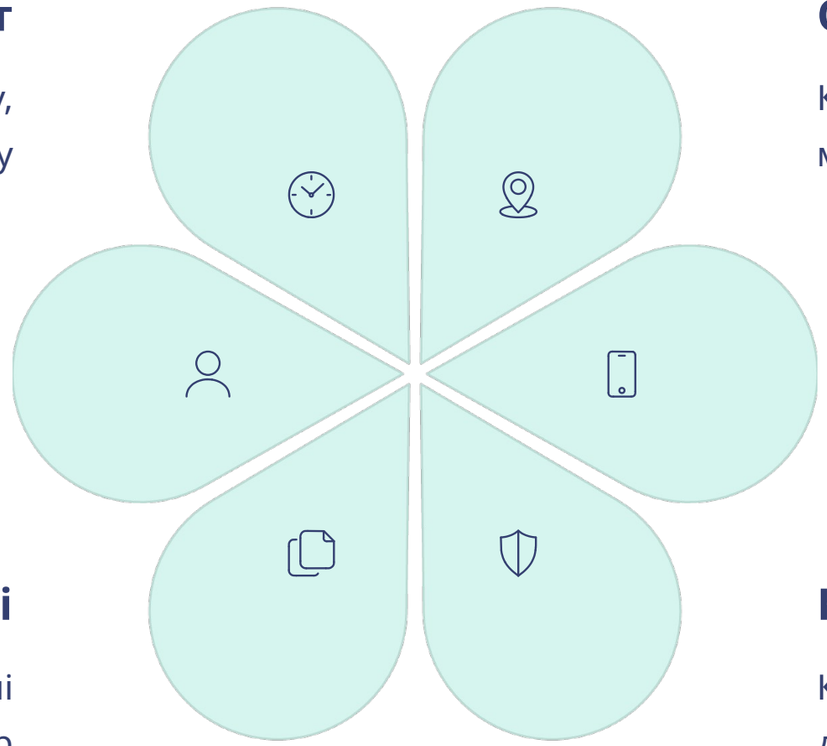
Жұмыс уақытында ғана қол жеткізу, демалыс күндері шектеу

Пайдаланушы атрибуттары

Бөлім, лауазым, жобалар, жұмыс өтілі негізінде құқықтар

Ресурс түрі

Әр түрлі құжат түрлері үшін әртүрлі құқықтар



Орын

Кеңседен немесе белгілі IP мекенжайлардан ғана кіру мүмкіндігі

Құрылғы

Тек корпоративтік немесе растайтын құрылғылардан қол жеткізу

Қауіпсіздік деңгейі

Құпия деректерге тек жоғары қауіпсіздік деңгейінде қол жеткізу

ABAC моделі икемді және күрделі бизнес қағидаларын жүзеге асыруға мүмкіндік береді. Мысалы: "Қаржы бөлімінің менеджері жұмыс уақытында кеңседен корпоративтік құрылғыдан 100,000 теңгеге дейінгі төлемдерді бекіте алады."

Қазақстандағы ақпараттық жүйелердегі авторизация

Электрондық үкімет жүйелері

Қазақстанның электрондық үкімет порталы күрделі авторизация жүйесін қолданады. Әр қызмет үшін әртүрлі рұқсат деңгейлері белгіленген.

1 Жеке тұлғалар

ИИН негізінде сәйкестендіру, жеке деректерге қол жеткізу, өз атынан өтініштер беру

2 Заңды тұлғалар

БИН негізінде сәйкестендіру, ұйым деректеріне қол жеткізу, бизнес-процестерді басқару

3 Мемлекеттік қызметкерлер

Кеңейтілген құқықтар, азаматтардың өтініштерін өңдеу, статистика мен есептерге қол жеткізу

ҰКО сертификаттары



Ұлттық куәландырушы орталығы шығарған сертификаттар әртүрлі деңгейлерге бөлінеді:

- **1-класс:** жеке тұлғаларға арналған, электрондық үкімет қызметтері үшін
- **2-класс:** заңды тұлғаларға арналған, электрондық сауда және банктік операциялар үшін
- **3-класс:** мемлекеттік органдарға арналған, жоғары қауіпсіздік талап етілетін операциялар үшін

Әр класс сертификаттың қолдану аясын және берілетін құқықтарды анықтайды.

eGov авторизациясы

Электрондық үкімет порталы – Қазақстандағы ең ірі авторизация жүйелерінің бірі. Күніне миллионнан астам пайдаланушыға қызмет көрсетеді және мемлекеттік қызметтерге қауіпсіз қол жеткізуді қамтамасыз етеді.

12M+

Тіркелген пайдаланушылар

eGov порталында

700+

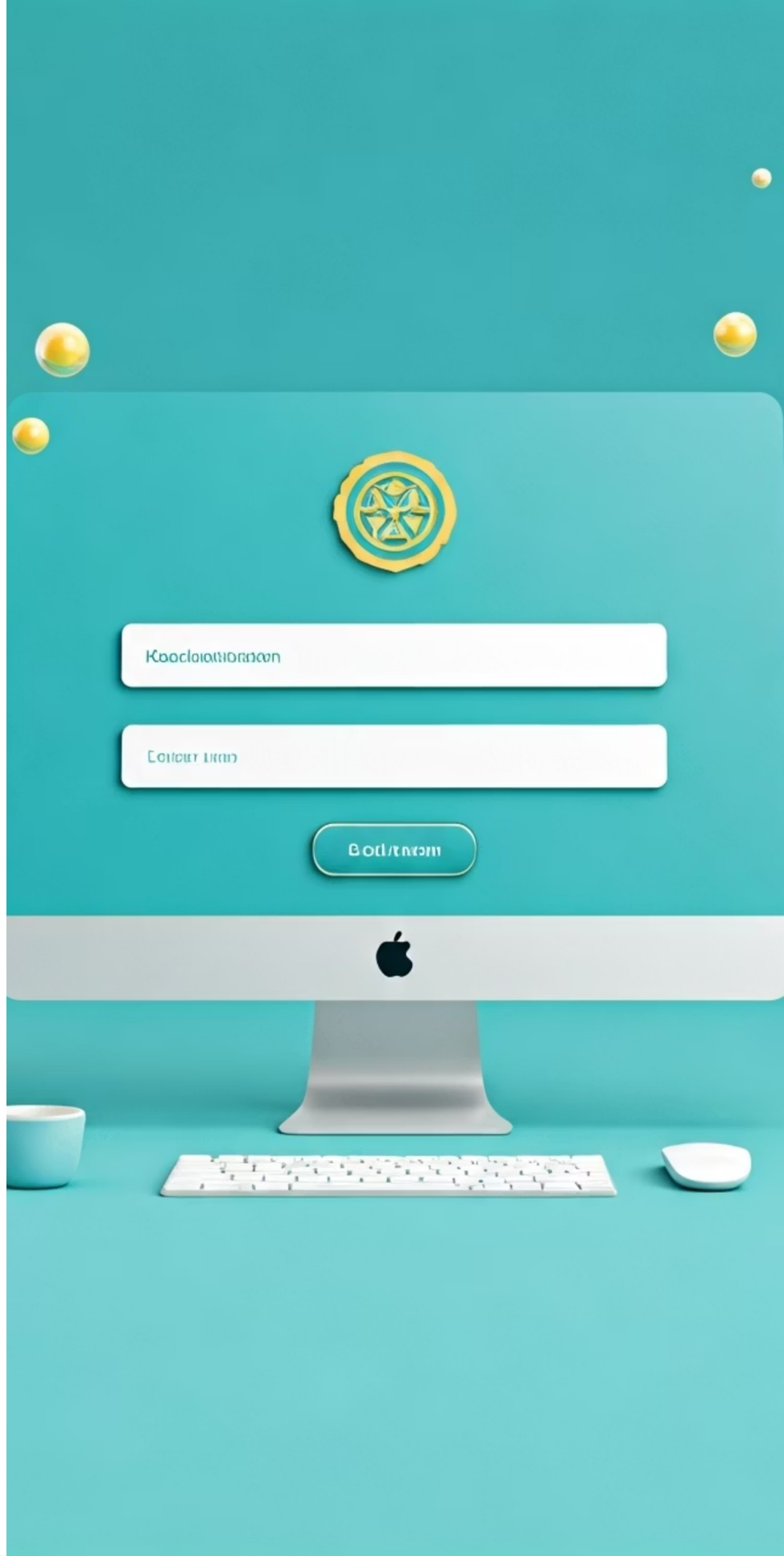
Мемлекеттік қызметтер

Онлайн қолжетімді

99.9%

Жүйенің қолжетімділігі

Жыл бойы





Қауіпсіздік хаттамалары мен стандарттары

Аутентификация мен авторизацияны жүзеге асыру үшін индустрияда қабылданған стандарттар мен хаттамалар қолданылады. Олар әртүрлі жүйелер арасында үйлесімділікті қамтамасыз етеді және қауіпсіздік деңгейін арттырады.

Бұл бөлімде біз заманауи ақпараттық жүйелерде қолданылатын негізгі хаттамалар мен стандарттарды қарастырамыз.

OAuth және OpenID Connect

OAuth 2.0

OAuth 2.0 – авторизацияның ашық стандарты. Үшінші тарап қосымшаларына құпия сөзді бермей-ақ, ресурстарға шектеулі қол жеткізуді беруге мүмкіндік береді.

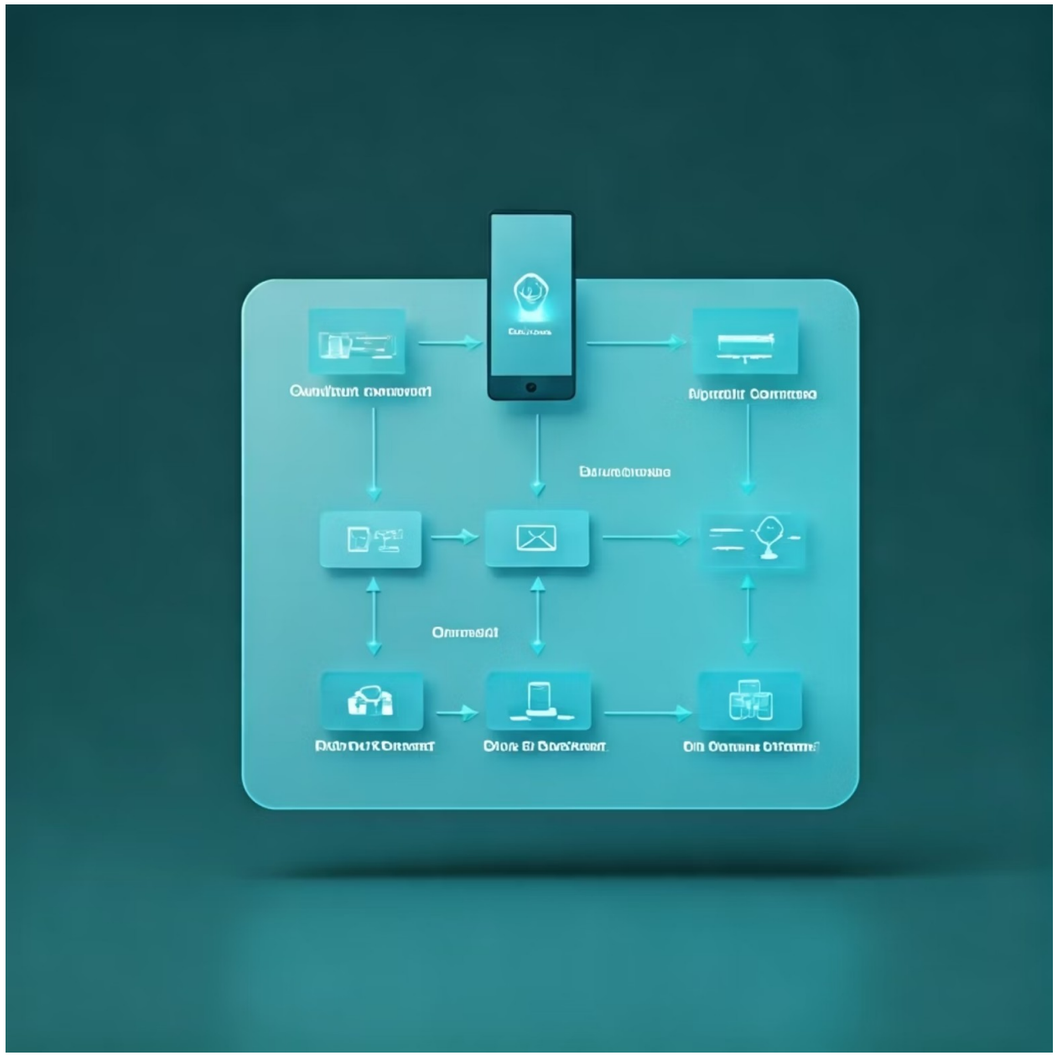
Негізгі ұғымдар:

- **Resource Owner:** ресурстің иесі (пайдаланушы)
- **Client:** қосымша немесе қызмет
- **Authorization Server:** рұқсаттарды беретін сервер
- **Resource Server:** қорғалған ресурстар орналасқан сервер
- **Access Token:** рұқсат берілгенін растайтын токен

1. **1. Пайдаланушы кіруді сұрайды**
   Қосымша авторизация серверіне бағыттайды
2. **2. Аутентификация**
   Пайдаланушы өз деректерін енгізеді
3. **3. Рұқсат беру**
   Пайдаланушы қосымшаға рұқсат береді
4. **4. Токен алу**
   Қосымша access token алады
5. **5. Ресурстарға қол жеткізу**
   Токен арқылы деректерді алады

OpenID Connect

OpenID Connect – OAuth 2.0 үстіне құрылған аутентификация қабаты. Пайдаланушының жеке басын растауға мүмкіндік береді.



Мысал: Google, Facebook немесе Apple аккаунты арқылы басқа қосымшаларға кіру – бұл OAuth және OpenID Connect технологияларының қолданылуы.

SAML (Security Assertion Markup Language)

SAML – ұйымдар арасында аутентификация мен авторизация деректерін алмасу стандарты. Корпоративтік ортада бір рет кіру (Single Sign-On, SSO) функционалын жүзеге асыру үшін кеңінен қолданылады.



SAML компоненттері

1 Identity Provider (IdP)

Пайдаланушыны аутентификациялайтын және растау хабарламаларын (assertions) жасайтын жүйе. Мысалы, Active Directory.

2 Service Provider (SP)

Пайдаланушыға қызмет көрсететін жүйе. IdP-дан растауды қабылдайды және негізінде рұқсат береді.

3 SAML Assertions

Пайдаланушы туралы ақпарат, аутентификация мәліметтері және авторизация шешімдері бар XML құжаттары.

SAML артықшылықтары

- Бір рет кіру (SSO) – бір аутентификация арқылы барлық жүйелерге қол жеткізу
- Орталықтандырылған пайдаланушыларды басқару
- Құпия сөздерді азайту және қауіпсіздікті арттыру
- Индустриялық стандарт, кең қолдау
- Платформа-тәуелсіз шешім

Қолдану салалары

- Корпоративтік ішкі жүйелер (ERP, CRM)
- Бұлтты қызметтер (Office 365, Salesforce)
- Ұйымаралық интеграция
- Білім беру порталдары

Қазақстандағы SSO жүйелері

Қазақстанда да SSO технологиялары белсенді қолданылуда. Электрондық үкімет порталы өзінің SSO жүйесін ұсынады, ол пайдаланушыларға бір рет аутентификациядан өткеннен кейін көптеген мемлекеттік қызметтерге қол жеткізуге мүмкіндік береді.

1

2008 жыл

egov.kz порталының іске қосылуы, негізгі аутентификация жүйесі

2

2013 жыл

ЭЦҚ арқылы аутентификацияның енгізілуі

3

2016 жыл

SSO функционалының іске қосылуы, бір рет кіру мүмкіндігі

4

2019 жыл

Мобильді қосымша арқылы аутентификация және биометрия

5

2023 жыл

Жаңартылған SSO жүйесі, көптеген үшінші тарап қызметтерімен интеграция

Қазақстандағы SSO мүмкіндіктері

- 700+ мемлекеттік қызметке бір кіруден қол жеткізу
- ЭЦҚ, логин/пароль, мобильді қосымша арқылы аутентификация
- Мемлекеттік және коммерциялық сервистерді біріктіру
- Қауіпсіздік және деректердің қорғалуы
- Пайдаланушы үшін ыңғайлылық және уақыт үнемдеу

Нормативтік негіз

- ҚР «Ақпараттандыру туралы» Заңы
- «Электрондық құжат және ЭЦҚ туралы» Заң
- Үкіметтің қаулылары электрондық үкімет туралы
- ҰКО техникалық регламенттері
- Ақпараттық қауіпсіздік стандарттары

SSO архитектурасы

SSO жүйесінің архитектурасы пайдаланушыларға бірнеше қосымша мен қызметтерге бір аутентификация арқылы қол жеткізуге мүмкіндік береді. Бұл құпия сөздердің санын азайтады және жүйелік әкімшілендіруді жеңілдетеді.

Пайдаланушы кіреді

Кез келген қосымшаға кіруге тырысады

Рұқсат беру

Қосымша токенді тексеріп, қол жеткізу береді

Қосымшаға қайту

Токенмен бірге қосымшаға қайтарылады



SSO серверіне бағыттау

Қосымша пайдаланушыны орталық серверге жібереді

Аутентификация

Егер сессия жоқ болса, деректерді енгізу сұралады

Токен жасау

SSO сервері аутентификация токенін жасайды

Қауіпсіздік қатерлері мен оларды болдырмау

Аутентификация мен авторизация жүйелері үнемі шабуылдарға ұшырайды. Қауіпсіздік қатерлерін түсіну және оларға қарсы қорғану шараларын білу өте маңызды.

Статистика көрсеткендей, шабуылдардың көпшілігі адами факторға негізделген – әлсіз құпия сөздер, фишинг, әлеуметтік инженерия. Сондықтан техникалық шаралармен қатар, пайдаланушыларды оқыту да маңызды рөл атқарады.



Фишинг және әлеуметтік инженерия

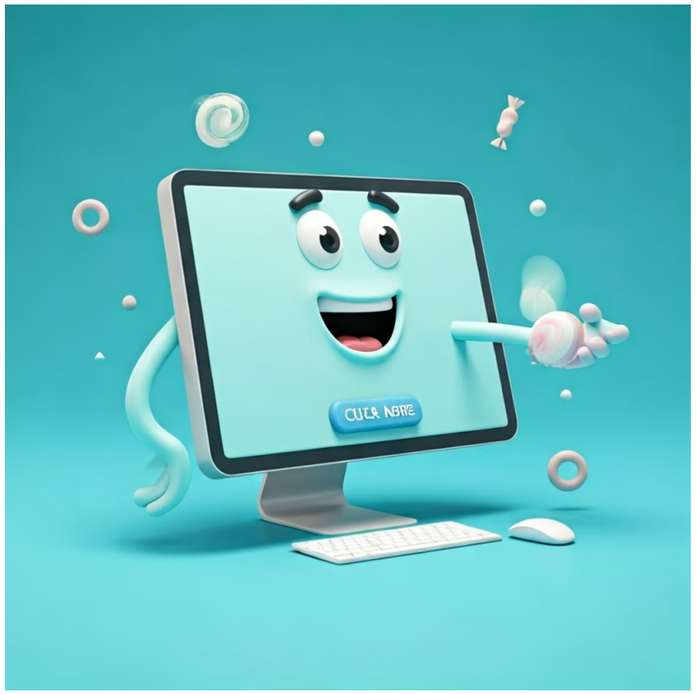
Фишинг – құпия ақпаратты ұрлаудың ең кең таралған әдістерінің бірі. Шабуылшылар өздерін сенімді ұйым ретінде көрсетіп, пайдаланушыларды алдайды.

Фишинг түрлері:

- **Email фишинг:** жалған электрондық хаттар арқылы
- **Spear фишинг:** нақты адамдарға бағытталған шабуылдар
- **Whaling:** жоғары лауазымды тұлғаларға шабуыл
- **Smishing:** SMS арқылы алаяқтық
- **Vishing:** телефон қоңырауы арқылы алдау
- **Pharming:** пайдаланушыларды жалған сайттарға бағыттау

Әлеуметтік инженерия тәсілдері:

1. Қорқыту (жедел әрекет қажет деп сендіру)
2. Сенімділік (таныс немесе билік иесі болып көрсету)
3. Алғыс айту (көмек ұсыну немесе сыйлық уәде ету)
4. Қызығушылық (қызықты ақпарат немесе жаңалықтар)



Қорғану шаралары

Сақ болыңыз

Күдікті хаттар мен сілтемелерді ашпаңыз

Тексеріңіз

Жіберушінің мекенжайы мен URL дұрыстығын қарап шығыңыз

MFA қолданыңыз

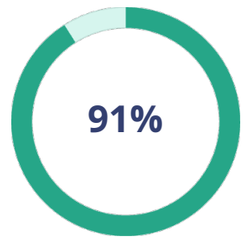
Көпфакторлы аутентификация қосымша қорғаныс қабаты

Оқытыңыз

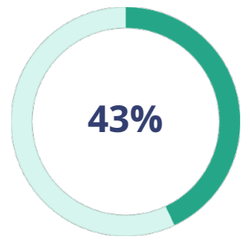
Қызметкерлерге қауіпсіздік мәдениетін үйретіңіз

Бағдарлама жаңартыңыз

Браузерлер мен қорғаныс құралдарын үнемі жаңартып отырыңыз



кибершабуылдар фишингпен басталады



компаниялар соңғы жылы фишинг шабуылына ұшыраған

Құпия сөздерді басқару жүйелері

Құпия сөздерді басқару жүйелері (Password Managers) – күшті және бірегей парольдерді қауіпсіз сақтау үшін арналған бағдарламалар. Олар барлық құпия сөздерді шифрлап сақтайды және тек бір мастер-парольді немесе биометрияны есте сақтау жеткілікті.

Негізгі функциялар

Шифрлау

Барлық деректер AES-256 немесе ұқсас күшті алгоритммен шифрланады

Пароль генерациясы

Күшті және кездейсоқ парольдерді автоматты түрде жасау

Автотолтыру

Веб-сайттарда және қосымшаларда логин/парольді автоматты енгізу

Синхронизация

Барлық құрылғылар арасында деректерді синхрондау

Қауіпсіздік талдауы

Әлсіз, қайталанатын немесе ескірген парольдер туралы ескерту

2FA кодтары

Екі факторлы аутентификация кодтарын сақтау және генерациялау

Танымал password менеджерлер

- **1Password:** кең функционал, отбасылық тарифтер
- **LastPass:** тегін нұсқа, браузерлік кеңейтімдер
- **Bitwarden:** ашық код, бюджетті баға
- **Dashlane:** VPN кіреді, қауіпсіздік мониторингі
- **KeePass:** тегін, жергілікті сақтау

Қазақстанда қолдану

Қазақстандық пайдаланушылар арасында password менеджерлердің танымалдығы артуда. Банктер мен корпорациялар қызметкерлеріне осындай құралдарды ұсынады.

Кеңес: Мастер-парольді өте күшті етіп жасаңыз (16+ символ, әріптер, сандар, арнайы белгілер) және ешқашан ешкіммен бөліспеңіз.

Қауіпсіздік аудиті және мониторинг

Қауіпсіздік аудиті мен мониторинг – жүйелердегі әлсіз жерлерді анықтау және инциденттерге жедел жауап беру үшін қажет. Проактивті тәсіл көптеген шабуылдардың алдын алуға көмектеседі.

Қауіпсіздік аудиті

Жүйелердің қауіпсіздік талаптарға сәйкестігін мезгіл-мезгіл тексеру. Осалдықтарды, дұрыс конфигурацияланбаған параметрлерді және потенциалды тәуекелдерді анықтау.

24/7 мониторинг

Жүйелік журналдарды, желілік трафикті және пайдаланушы әрекеттерін үздіксіз бақылау. Күдікті белсенділікті анықтау және жедел жауап беру.

Инцидентке жауап беру

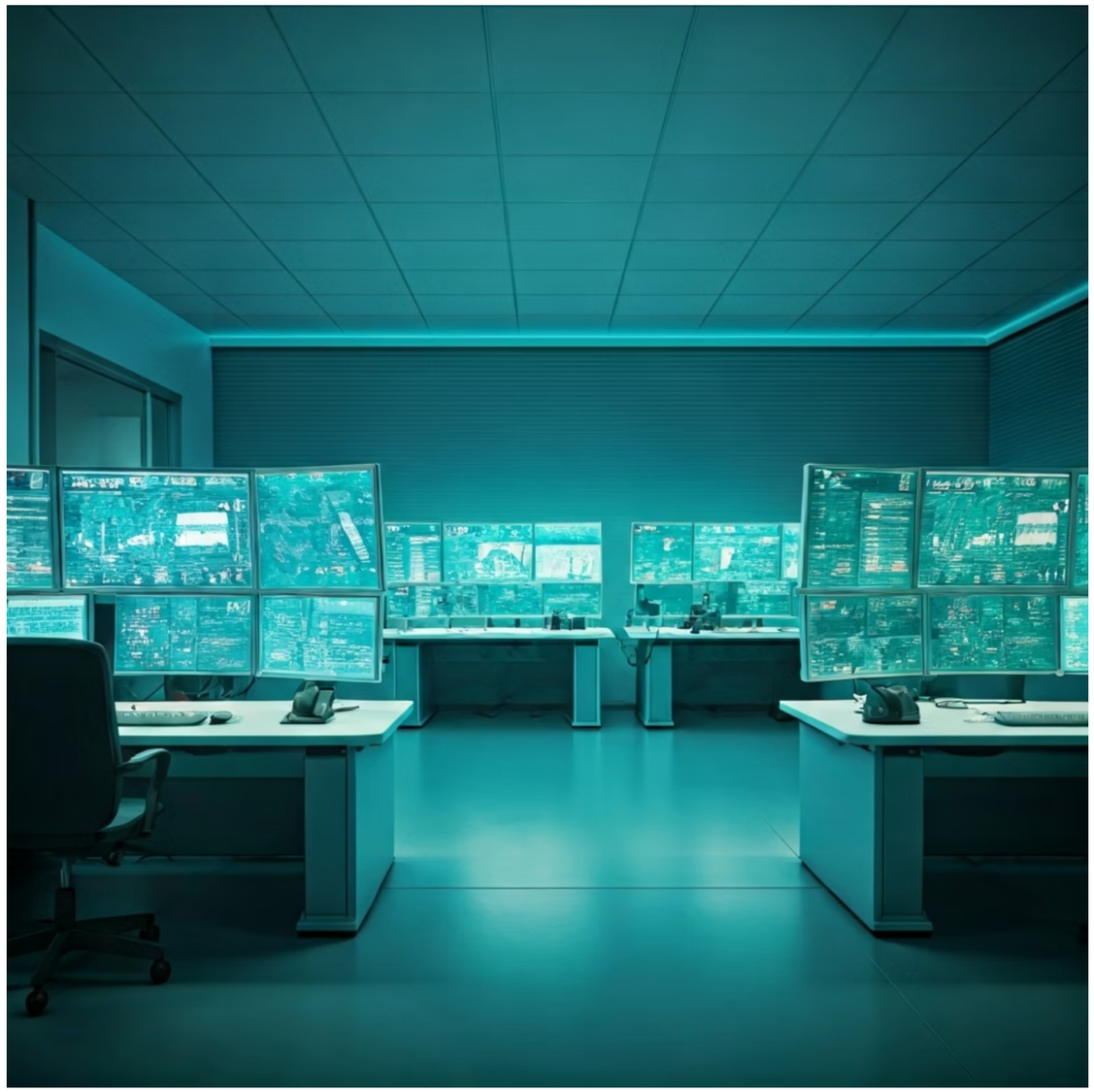
Қауіпсіздік оқиғаларын тіркеу, талдау және жою бойынша регламенттелген процедуралар. Апаттан кейін қалпына келтіру жоспарлары.

Аудит объектілері

- Пайдаланушы есептік жазбалары мен құқықтары
- Аутентификация және авторизация механизмдері
- Құпия сөздер саясаты және орындалуы
- Желілік қауіпсіздік конфигурациясы
- Бағдарламалық қамтама жаңартулары
- Деректердің шифрлануы және сақталуы
- Физикалық қауіпсіздік шаралары
- Резервтік көшірмелер жүйесі

Мониторинг құралдары

- SIEM жүйелері (Security Information and Event Management)
- IDS/IPS (Intrusion Detection/Prevention Systems)
- Log менеджменті және талдау платформалары
- Желілік трафикті талдау құралдары
- Endpoint Detection and Response (EDR)
- Vulnerability scanners





Қазақстандағы ұлттық тәжірибелер

Қазақстан Республикасы электрондық үкімет және ақпараттық қауіпсіздік саласында белсенді дамуда. Ұлттық деңгейде аутентификация мен авторизация жүйелерінің құрылуы елдің цифрлық трансформациясының негізі болып табылады.

Бұл бөлімде біз Қазақстандағы ақпараттық қауіпсіздік инфрақұрылымын, оның дамуын және болашақ перспективаларын қарастырамыз.

ҚР Ұлттық куәландырушы орталығы (ҰКО)



Негізгі функциялар

- Электрондық цифрлық қолтаңба сертификаттарын шығару
- Сертификаттардың қолданыс мерзімін басқару
- Кері қайтарылған сертификаттардың тізімін жүргізу (CRL)
- Уақыт белгілерін (timestamp) беру қызметі
- Техникалық қолдау және консультация
- Аккредитацияланған куәландырушы орталықтарды бақылау

Ұлттық куәландырушы орталығы – Қазақстанның электрондық цифрлық қолтаңба инфрақұрылымасының басты элементі. 2008 жылдан бері электрондық сертификаттар шығарумен және олардың жұмыс істеуін қамтамасыз етумен айналысады.

15+

Жыл тәжірибе

ҰКО 2008 жылдан бері жұмыс істейді

8.5M+

Сертификаттар

Шығарылған ЭЦҚ сертификаттарының жалпы саны

20+

Аккредиттелген ОКО

Облыстық куәландырушы орталықтардың желісі

99.99%

Қолжетімділік

Сервистердің үздіксіз жұмыс істеуі

ҰКО Қазақстанның цифрлық экономикасының дамуында маңызды рөл атқарады. Электрондық құжат айналымы, электрондық сауда, мемлекеттік қызметтер – бәрінде ҰКО технологиялары қолданылады.

ЭЦҚ кілттерін алу және пайдалану

Қазақстанда ЭЦҚ кілттерін алу процесі стандартталған және оңай. Жеке тұлғалар мен заңды тұлғалар әртүрлі тәсілдер арқылы сертификат алуы мүмкін.

01

Құжаттарды дайындау

Жеке куәлік, ИИН (заңды тұлғаларға БИН, құрылтай құжаттары қажет)

02

ҰКО немесе ОКО-ға жүгіну

Қазақстанның кез келген қалаларында орналасқан куәландырушы орталықтарға барып, өтінім беру

03

Жеке басын растау

Биометриялық деректерді жинау және құжаттарды тексеру

04

Токен немесе смарт-карта алу

Кілттік тасығышты таңдау: E-token, Kaztoken, JaCarta немесе басқа сертификатталған құрылғылар

05

Сертификатты жүктеу

Кілттер жұбын генерациялау және сертификатты токенге жазу

06

PIN-код орнату

Токенді қорғау үшін жеке PIN-код белгілеу

Кілттік тасығыштар

- **E-token:** USB интерфейсі, кең таралған
- **Kaztoken:** қазақстандық өндіріс
- **JaCarta:** жоғары қауіпсіздік деңгейі
- **Смарт-карталар:** банктік карта форматы
- **Мобильді ЭЦҚ:** смартфонда сақтау (жаңа технология)

Қашықтан алу

2023 жылдан бастап қашықтан сәйкестендіру технологиясы енгізілді. Пайдаланушылар мобильді қосымша арқылы биометрияны өткізіп, үйден шықпай-ақ ЭЦҚ ала алады.

ЭЦҚ сертификатының қолдану мерзімі – 1 немесе 2 жыл. Мерзімі аяқталғанда жаңартып отыру қажет.

Заңнамалық база және нормативтер

Қазақстанда ақпараттық қауіпсіздік, аутентификация және авторизация мәселелерін реттейтін толық заңнамалық база қалыптасқан. Бұл заңдар электрондық құжат айналымының заңдылығын және деректердің қорғалуын қамтамасыз етеді.

«Ақпараттандыру туралы» ҚР Заңы

Ақпараттандыру саласындағы негізгі заң. Ақпараттық жүйелер, олардың қауіпсіздігі, деректерді қорғау және электрондық үкімет принциптерін белгілейді.

«Электрондық құжат және электрондық цифрлық қолтаңба туралы» ҚР Заңы

ЭЦҚ-ның заңды күшін, электрондық құжаттардың қағаз құжаттармен теңдігін, куәландырушы орталықтардың жұмысын реттейді.

«Дербес деректер және оларды қорғау туралы» ҚР Заңы

Жеке деректерді жинау, сақтау, өңдеу және қорғау талаптарын белгілейді. GDPR сияқты халықаралық стандарттарға жақындауды көздейді.

Үкіметтің 2016 жылғы 28 желтоқсандағы №832 қаулысы

«Ақпараттық қауіпсіздік бойынша нормативтік құқықтық актілерді бекіту туралы». Техникалық қауіпсіздік талаптарын анықтайды.

СТ РК стандарттары

Ақпараттық қауіпсіздік бойынша ұлттық стандарттар. Криптографиялық қорғау құралдары, аутентификация әдістері, аудит жүргізу талаптары.

Халықаралық стандарттарға сәйкестік

- ISO/IEC 27001 – ақпараттық қауіпсіздік менеджменті
- ISO/IEC 27002 – қауіпсіздік бақылау шаралары
- NIST Cybersecurity Framework
- COBIT – IT басқару негіздері
- PCI DSS – төлем карталары деректерінің қауіпсіздігі

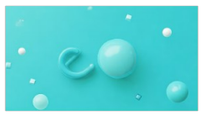
Жауапкершілік

Ақпараттық қауіпсіздік талаптарын бұзғаны үшін әкімшілік және қылмыстық жауапкершілік көзделген:

- Деректердің жария болуы
- Рұқсатсыз қол жеткізу
- Ақпараттық жүйелерді бұзу
- ЭЦҚ-ны дұрыс пайдаланбау

ҰКО инфрақұрылымасы






> Ұлттық куәландырушы орталығы – Қазақстанның цифрлық сенім инфрақұрылымасының іргетасы. Ол мемлекеттік, коммерциялық және жеке пайдаланушыларға қауіпсіздік пен сенімділікті қамтамасыз етеді.

Болашақ трендтер мен инновациялар

Аутентификация мен авторизация технологиялары үнемі дамып, жаңа деңгейге көтеріліп келеді. Жасанды интеллект, блокчейн, биометрияның жетілдірілуі – мұның бәрі ақпараттық қауіпсіздіктің болашағын қалыптастырады.

Келесі 5-10 жылда біз қауіпсіздік пен ыңғайлылықтың тамаша балансын көреміз. Пайдаланушылар парольдарды мүлдем ұмытып, биометрия мен АИ негізіндегі жүйелерге көшетін болады.



Биометрияның дамуы

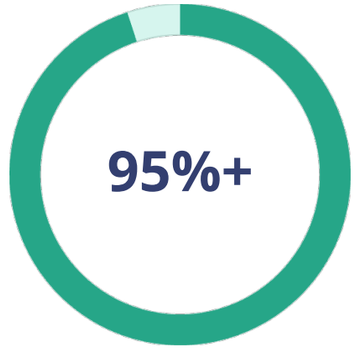
Жасанды интеллект және машиналық оқыту

AI технологиялары биометриялық жүйелердің дәлдігін айтарлықтай арттыруда. Машиналық оқыту алгоритмдері жалған оң және жалған теріс нәтижелерді азайтады.

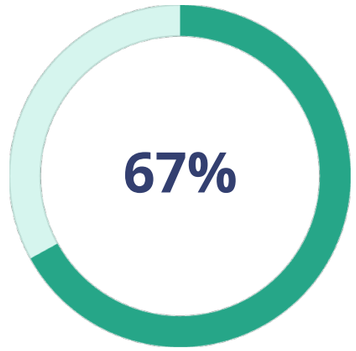


Мультимодальды биометрия

Бірнеше биометриялық параметрлерді бір уақытта пайдалану тренд болып отыр. Мысалы, бет-әлпет + дауыс + мінез-құлық талдауы.



дәлдік деңгейі мультимодальды жүйелерде



биометрия нарығының өсуі 2025 жылға қарай



Мінез-құлық биометриясы

Теру стилі, тінтуірді жылжыту, телефонды ұстау әдісі – бұл барлығы бірегей идентификаторлар. Үздіксіз аутентификация мүмкіндігі.



Жүрек соғу ырғағы

Әр адамның жүрек соғу үлгісі бірегей. Арнайы сенсорлар немесе смарт-сағаттар арқылы аутентификация жүргізуге болады.



Жүріс танымы

Адамның жүру стилі де биометриялық параметр болуы мүмкін. Камералар немесе сенсорлар арқылы қашықтықтан анықтау.



Қан тамырлары үлгісі

Қолдағы немесе саусақтағы тамырлар торабы бірегей және жасырын. Жоғары қауіпсіздік және алдауға қарсы тұрақтылық.

Болашақта биометрия еркін және үздіксіз болады – пайдаланушы байқамай-ақ аутентификация өтеді. Жүйе мінез-құлық пен контекстік деректерді үнемі талдап, күдікті белсенділікті анықтайды.

Блокчейн технологиясы

Блокчейн – орталықсыздандырылған және өзгертуге болмайтын дерекқор. Бұл технология аутентификация мен авторизация саласында революция жасауы мүмкін.

Өзін-өзі басқаратын цифрлық сәйкестік (Self-Sovereign Identity)

Пайдаланушылар өз жеке деректерінің толық иелері болады. Үшінші тараптарға (Google, Facebook) тәуелділік жоқ. Блокчейнде сақталған сәйкестік деректері өзгертуге және бұрмалауға қарсы.

Дербес деректермен қауіпсіз алмасу

Пайдаланушылар кімге, қандай деректерді, қанша уақытқа беретінін бақылайды. Смарт-контракттар арқылы автоматты құқықтарды басқару. Деректердің барлық қолданылуының тарихы сақталады.

Бір орталық дерекқордың болмауы

Деректер таратылған түрде сақталады, бірыңғай шабуыл нүктесі жоқ. Хакерлер үшін барлық торапты бұзу өте қиын. Жүйенің тұрақтылығы мен сенімділігі артады.

Қазақстандағы блокчейн жобалары

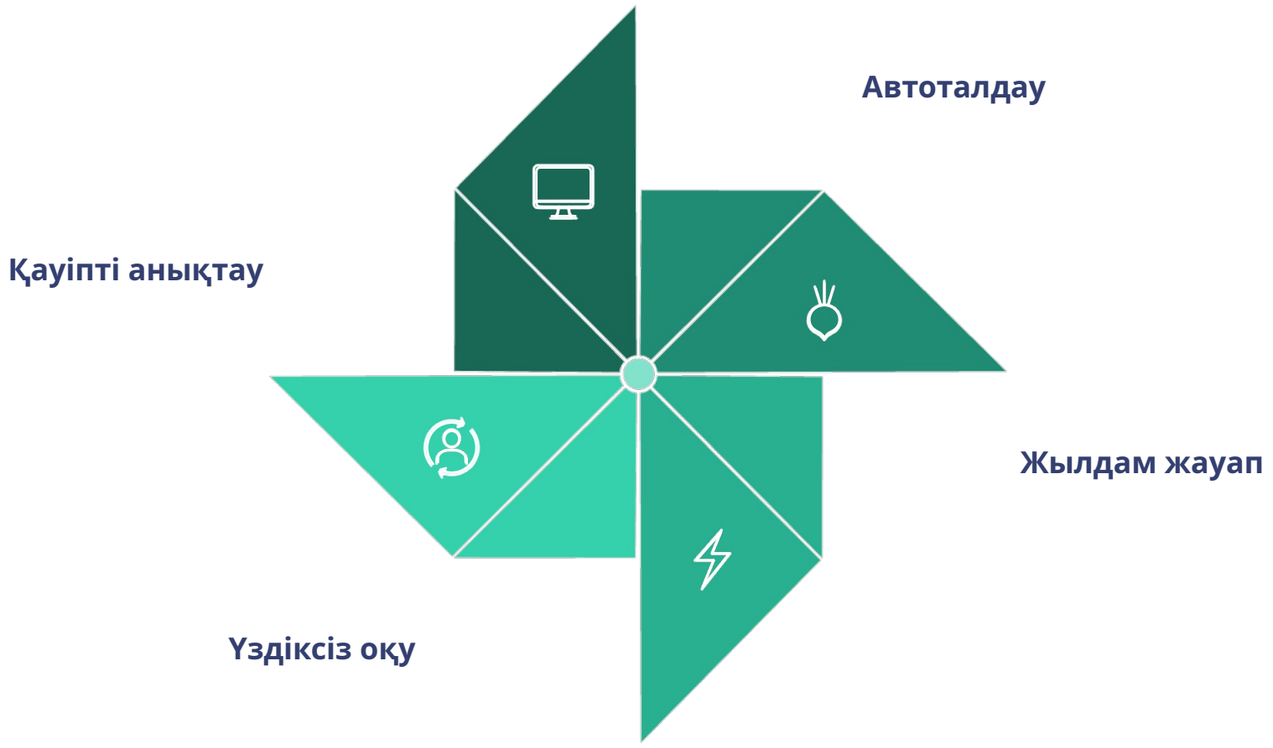
- Astana Hub – блокчейн негізіндегі сәйкестендіру платформасы
- Мемлекеттік қызметтерде блокчейн технологияларын сынау
- Банктік секторда блокчейн пилоттары
- Білім беру саласында дипломдарды растау

Болашақ мүмкіндіктер

- Біріктірілген ұлттық цифрлық сәйкестік
- Трансшекаралық сәйкестендіру
- Құқықтарды автоматты басқару
- Деректердің ашықтығы мен қауіпсіздігінің балансы

Қауіпсіздік автоматтандыруы

Қауіпсіздік операцияларын автоматтандыру – қазіргі кибер қауіптердің көптігі мен күрделілігіне жауап. Адам қателіктерін азайту және инциденттерге жедел жауап беру үшін автоматтандыру өте маңызды.



Қауіп-қатерлерді анықтау (Threat Intelligence)

AI жүйелері жаһандық қауіп-қатерлер туралы деректерді жинап, талдайды. Жаңа шабуыл векторларын үйреніп, проактивті қорғаныс стратегияларын ұсынады. Real-time режимінде миллиондаған оқиғаларды өңдейді.

Қауіпсіздік оркестрациясы (SOAR)

Security Orchestration, Automation, and Response платформалары әртүрлі қауіпсіздік құралдарын біріктіреді. Рутинды тапсырмаларды автоматтандырып, аналитиктерге күрделі мәселелерге көп уақыт қалдырады. Инциденттерге жауап беру жылдамдығы 10 есе артады.

Автоматты жауап беру

Жүйе өзі күдікті белсенділікті анықтап, алдын алу шараларын қолданады: пайдаланушыны блоктау, желіден ажырату, құжаттарды карантинге алу. Адамның қатысуы қажет болғанда ғана ескертеді.

SOC (Security Operations Center)

Қауіпсіздік операциялары орталығы – 24/7 мониторинг жүргізетін командалар мен технологиялар кешені. Қазақстанда ірі ұйымдар мен мемлекеттік органдарда SOC құрылуда.

- Үздіксіз мониторинг және бақылау
- Инциденттерге жедел жауап беру
- Криминалистикалық талдау
- Есептілік және сәйкестік



Қорытынды: Аутентификация мен авторизацияның маңызы

> Аутентификация мен авторизация – қазіргі цифрлық әлемнің сенімділігі мен тұрақтылығының іргетасы. Олар тек техникалық процестер емес, сонымен қатар әлеуметтік сенім пен экономикалық қауіпсіздіктің негізі.

Негізгі тұжырымдар

- **Қауіпсіздік – инвестиция:** ақпараттық қауіпсіздікке жұмсалған шығын табыстың 5-10%-ын құрайды, бірақ инциденттен кейін шығын 100 есе көп болуы мүмкін
- **Көпқабатты қорғаныс:** бір ғана әдіс емес, бірнеше деңгейлі қорғаныс жүйесі қажет
- **Адами фактор:** технологиялармен қатар, пайдаланушыларды оқыту өте маңызды
- **Үздіксіз жаңарту:** қауіпсіздік – бір реттік әрекет емес, үздіксіз процесс
- **Баланс:** қауіпсіздік пен ыңғайлылықтың арасында тепе-теңдік табу

Қазақстанның перспективалары

Қазақстан электрондық үкімет және цифрлық экономика саласында белсенді дамуда. Ұлттық куәландырушы орталығы, egov порталы, блокчейн пилоттары – бұл барлығы елдің технологиялық көшбасшылыққа ұмтылысын көрсетеді.

Инфрақұрылым

Қуатты ЭЦҚ және аутентификация жүйесі

Заңнамалық база

Толық реттелетін ақпараттық қауіпсіздік саласы

Инновациялар

Жаңа технологияларды енгізуге дайындық

Цифрлық трансформация үдеп келе жатқанда, қауіпсіз аутентификация мен авторизация жүйелері мемлекеттің, бизнестің және әрбір азаматтың жетістігінің кепілі болып табылады.