**Техникалық сипаттамалары**

**Техникалық сипаттамалар.**

Жеткізуші бұрын пайдаланылмаған жаңа жабдықты пайдалануы керек. Жеткізуші келесі техникалық сипаттамалары бар аппараттық-бағдарламалық кешенді жеткізуге және орнатуға міндетті:

Білім беру ұйымдарына арналған интеграцияланған электрондық қызметтердің биометриялық жүйесінің аппараттық-бағдарламалық кешені (бұдан әрі – БАК) білім беру үдерісінің сапасын арттыратын озық ақпараттық технологияларды енгізуге арналған. Ол қол жеткізуді басқару және басқару қызметтерін, алақан арқылы контактісіз биометриялық сәйкестендіруді, ақпаратты көруге және енгізуге арналған мобильді қосымшаларды және аналитикалық қызметті қамтиды.

**Пакет мыналардан тұруы керек:**

Турникет, сканер, бағдарламалық қамтамасыз ету

**Турникет:**

Аналық тақша: арнайы IoT құрылғылары, ақылды терминалдар, NAS жүйелері, және өнеркәсіптік қолданбаларына арналған болуы керек, 4 ядро және 4 ағыннан кем емес 64 биттік процессор; Графикалық процессор алтернативті , gpu gpdr4-тен кем емес, eppl eeprom, 4KB-ден кем емес, ажыратымдылық төмен емес, Мобильдік платформаларда соңғы нұсқаларында ойнату режимінен төмен емес, мысалы, цикл, синхрондау және аралық, желі, Ethernet, WiFi, WiFi / BT5.0, WiFi / BT5.0, сымсыз Итералды кеңейту, WMV, AVI, FLV, RM, RM, RM, RM, MPEG, TS, MPEG, MPEC, PNG, GIF, GIF, GIF, GIF, GIF, ost \* 1), ABC2E интерфейсіне арналған MIPI камерасы, 01i3n0t0rwfacea \* m4era, сериялық порт RS232\*2,485\*1,TTL\*2,CAN порты\*1 GPS 30pin FPC Сыртқы GPS (қосымша) SATA қосқышы\*1, BT қолдауы, кірістірілген 2.4G WIFI, VT5.2 4G, Кірістірілген MINIPCIE 4G модулі қосқышы, Ethernet\* DudDP1 порты, Ethernet\* флеш картасы, ethernet 1000 қолдауы eDP порты\*1, Стандартты HDMI2.0 порты, MIPI СКД порты (FPC 40 істікшелі қосқыш), Кірістірілген қос арналы AV шығысы, әр арнаға 4R / 10 Вт немесе бір арна күшейткіші үшін 8R / 5 Вт қолдауы, Құлаққап ұясы, Кірістірілген 3,5 мм 4 полюсті ұясы, СКД синхрондау порты 4 қолдауы, MI қосқышы порт RJ45 қашықтан іске қосуды басқаруға арналған). ҚР СТ 3620-2020.

**Сканер:**

Кемінде 400 МГц төмен қуатты процессор

Кескін сенсоры 1/2,7 дюймден кем емес HDR CMOS, инфрақызылға жақын

Қосқыш кемінде 7 істікшелі USB 2.0 қосқышы, 1,25 мм

Байланыс интерфейсі USB 2.0 (жоғары жылдамдықты)

Қуатты тұтыну 0,5 Вт (күту режимі) / 1,5 Вт (жұмыс) артық емес

Жарықтандыру жағдайлары Тіркеу <800 люкс; Сәйкестендіру <2000 люкс

Ылғалдылық 0-ден 90% -ға дейінгі салыстырмалы ылғалдылық CE, FCC, RoHS сертификаты. ҚР СТ ИСО/МЭК 15423-2009.

**Сканердің оптикалық және бейнелеу сипаттамалары:**

Сенсор түрі Оптикалық

Кескін өлшемі (пиксельде) кемінде 480 x 640 (ені x биіктігі)

Сұр реңк 256 деңгейден кем емес

Динамикалық диапазон 83 дБ кем емес

Макс. кадр жылдамдығы секундына 25 кадрдан кем емес

Объектив IR түрі

Оптикалық толқын ұзындығы 840-860 нм кем емес

Көру өрісі (FOV) диагональ = 58°, көлденең = 37°, тік = 48°

Оптикалық бұрмалау коэффициенті ≤1% аспайды

Объектив кем дегенде 4 пластикалық линзадан және инфрақызыл сүзгіден (4P+11R) тұрады. ҚР СТ ИСО/МЭК 15423-2009.

**БАК мыналарды қамтуы керек:**

1. Алақан тамырларының үлгілеріне негізделген контактісіз биометриялық сәйкестендіруге арналған бағдарламалық және аппараттық шешімдер.

2. Қолжетімділікті бақылау және басқару қызметі: қызметкерлер мен студенттердің білім беру мекемесінің аумағы мен ресурстарына қолжетімділігін тиімді бақылау үшін есепке алу жүйелерімен және қол жеткізуді басқару құрылғыларымен интеграция.

3. Күйлерді көруге, хабарландыруларды алуға және профильдерді желіде басқаруға арналған пайдаланушының мобильді қосымшасы.

4. Топтық және жеке чаттарды басқару қызметі: сынып бойынша әртүрлі топтық чаттар немесе студенттердің жеке чаттары құруды қамтамасыз ету.

5. Ақпаратты жинау және талдау қызметі: оқу үдерісін оңтайландыру үшін қажетті ақпаратты жылдам және дәл талдау үшін әкімшілік пен оқытушылар құрамы үшін жүйелік қызметтердің әрқайсысы жинаған барлық деректер бойынша есептерді жасау, алмасу және экспорттау мүмкіндігі.

**БАК үшін минималды функционалдық талаптар**

1. Білім беру саласындағы ақпараттық технологиялар объектілеріне қойылатын ең төменгі талаптардың 33-1 тармағының талаптарына сәйкес болуы керек (Қазақстан Республикасы Білім министрлігінің 15.12.2012 ж. No 456 бұйрығы);

2. Бiлiм беру ұйымында цифрлық бiлiм беру ресурстарымен және (немесе) электрондық оқулықтармен және (немесе) қолжетiмдiлiктi бақылау және басқару жүйесiмен интеграциялау бойынша қызметтiң болуы қажет;

3. Білім алушыларға цифрлық білім беру ресурстарына және (немесе) электрондық оқулықтарға (егер орта (бастауыш, негізгі орта және жалпы орта), оның ішінде арнаулы және мамандандырылған білім беру ұйымдарында цифрлық білім беру ресурстарына және (немесе) электрондық оқулықтарға қолжетімділік болған жағдайда, тегін мобильді қосымшаның жеке кабинеті және интернет-ресурс арқылы бір рет тіркелу технологиясын пайдалана отырып) қамтамасыз ету функционалдығы болуы тиіс.

4. Бухгалтерлік есеп Palm ID технологиясын қолдану арқылы жүргізілуі керек (алақан венасының үлгісі).

5. Білім беру саласындағы ақпараттық технологиялар объектілеріне қойылатын ең төменгі талаптардың 14-тармағына сәйкес ақпараттық қауіпсіздік талаптарына (Қазақстан Республикасы Білім министрлігінің 14.11.2022 ж. No 456 бұйрығы) сәйкес болуы тиіс.

БАК барлық компоненттері бір-бірімен біріктірілуі керек. Қызметтерді өшіру, біріктіру және жаңаларын қосу тұтынушы тарапынан қосымша интеграциялық әрекеттерді қажет етпей жүзеге асырылуы керек. Әрбір қызметті орнату және енгізу процесі 24 сағаттан аспауы керек. Бұл кезең аяқталғаннан кейін тапсырыс беруші қосымша күш жұмсамай-ақ жаңа функцияларды пайдалана алуы керек: баптаулар, орнатулар, мердігердің техникалық мамандарының келуін күту, пайдаланушыларға арналған қосымшаларды қайта орнату немесе басқа да қосымша операцияларды орындау.

**Биометриялық ақпаратты қорғау 2 деңгейде ұйымдастырылуы керек:**

1) криптографиялық хэш-функциялардың көрсетілген алгоритмдерінің бірі: BelT, BLACK, Cube, Edonkey2k, FSB, Fugue, HAVAL, Hamsi, JH, Kupyna, Luffa, N-Hash, RIPEMD-128, RIPEMD-160, RIPEMD-256, SRIPEMD-SH2KHA, HAvite-3, SIMD, SWIFFT, Skein, Snefru, Tiger, Whirlpool.

2) Деректер симметриялық блоктық шифрлау алгоритмдерінің бірімен шифрланған: KCipher-2, MICKEY, MUGI, PIKE, Phelix 3,-WAY, ARIA, AES (Rijndael), Akelarre, KASUM, I Khafre, Khufu, MARS, MESH, MISSCCS0, ифер.

Барлық қызметтер алақандағы тамырлардың үлгісін сканерлеу арқылы пайдаланушыларды анықтауға негізделуі керек. Әрекеттерді авторизациялау, сәйкестендіру және растау үшін.

**Қол жеткізуді басқару және басқару жүйесі**

• Жұмыс компьютеріне арналған қолданба пайдаланушының жүйенің функционалдығы туралы түсінігін қысқаша қадамдық кіріспеден және АБЖ бастапқы орнату нұсқауларынан басталуы керек.

• Электрондық поштаңыздан құпия сөзді енгізу арқылы бастапқы кіру үшін тіркеліңіз.

• Ұйым туралы ақпаратты өз бетінше толтыру.

• Ұйымға қызмет көрсететін жүйелік әкімшінің тіркеу деректерін қолмен енгізу. Әкімшіні тіркеу жеке мәліметтер мен фото өрістерді автоматты түрде толтыру арқылы карта оқу құралы арқылы жеке басын куәландыратын құжатты оқу арқылы жүзеге асырылуы тиіс.

Жеке деректерді жинауға және өңдеуге келісіммен танысу және қол қою

Пайдаланушы фотосуреттерін қосу және өңдеу.

Тіркеу аяқталғаннан кейін әкімші өз алақанын авторизация кілті ретінде тіркеуі керек (логин мен парольдің орнына). Деректерді өңдеуге рұқсаты бар барлық пайдаланушылардың кейінгі рұқсаттары тек алақан тамырларының биометриялық сканері арқылы жүзеге асырылуы керек.

**Пайдаланушыны тіркеу 4 кезеңде орындалуы керек:**

1) Қазақстан Республикасы азаматының жеке куәлiгiнен жеке деректер мен фотосуреттердi оқу үшiн карта оқу құрылғысынан деректерді автоматты түрде енгізу. Сондай-ақ толық аты-жөнін, ЖСН, лауазымын, бөлімшесін, телефон нөмірін және фотосуретті қолмен енгізу немесе өңдеу мүмкіндігі болуы керек.

2) Дербес деректерді жинауға және өңдеуге келісімді электронды түрде оқу және растау.

3) Алақан тамырларының биометриялық сканерін қолдану арқылы екі алақанды тіркеу.

4) Сәтті/сәтсіз тіркеуді растау.

Тіркелген пайдаланушыларды әкімші графикалық интерфейс арқылы құқықтардың 3 тобына бөлуі керек: Әкімші (пайдаланушы тізімдерін қарайды, өңдейді және құқықтар береді), Редактор (пайдаланушы тізімдерін көреді, өңдейді), Бақылаушы (пайдаланушы тізімдерін көреді). Өңдеу құқықтары бөлек мәзірде орындалуы керек.

Сканерлеу сынағы. Алақан тамырларының үлгісін биометриялық сәйкестендіру жүйесінің функцияларын үйрету және сынау.

Қолданбаның пайдаланушы интерфейсіне қойылатын талаптар:

• Түрлі экран ажыратымдылықтарын қолдау.

• Көптілді интерфейс (қазақ, орыс және ағылшын).

• Интуитивті және пайдалану оңай дизайн.

• Сканерлеу:

- Сканерлеу үшін қолды құрылғыға жақындату мүмкіндігі.

- Оқиға түрін таңдаңыз: кіріс немесе шығыс.

Бақылау:

- Жүйедегі авторизация алақан тамырларының үлгісін сәтті сканерлегеннен кейін ғана.

- Жолдарды толтыру арқылы қызметкерлерді тіркеу.

- Жүйенің функционалдығын тексеру үшін сканерлеу сынағы.

- Кестемен өту тарихы (аты, орны, күні, уақыты, оқиғасы: кіру/шығу).

- Қызметкерлер тізімі (фотосурет, тіркеу күні мен уақыты, сканерленген алақандар, өңдеу/жою/қайта сканерлеу/шығару құқығы функциялары).

- Қол жеткізу құқықтарын басқару (әкімші, пайдаланушы, қонақ).

• Пайдаланушы белгішесі бар жоғарғы мәзір:

- Тариф және жазылымның жарамдылық мерзімі туралы ақпаратты көрсету.

- Орындаушының орнатушы-қызметкеріне ғана қолжетімді параметрлер

- Қолданбадан шығыңыз.

• Чат басқару:

- Чат топтарын құру. Сипаттамаларды өңдеу. Модерация функциялары.

- Сауалнамаларды құру. Түрді таңдаңыз. Сұрақты енгізу. Қатысуға шақыру. Дауыс беру нәтижелерін көрсету.

- Жаңалықтарды жариялау және алушыларды таңдау.

**Мобильді қосымша**

• Телефон нөмірі бойынша пайдаланушыларды тіркеу және авторизациялау.

**«Балалар» модулі**

• Балалардың профильдерін көру және өңдеу, соның ішінде фотосуреттер қосу.

• Күні мен уақыты бойынша баланың тарихын қараңыз.

• Чат және дауыс беру. Топтық және жеке чаттар. Ағымдағы жаңалықтар мен оқиғаларды көрсету. Пайдаланушылар арасында дауыс беруді өткізу мүмкіндігі.

• Оқиға туралы хабарландырулар. Турникет арқылы кіру/шығу, кітапты алу/қайтару туралы хабарландыруларды және чаттардағы жаңа хабарламалар туралы хабарландыруларды алыңыз. Пайдаланушы бойынша хабарландыру параметрлерін теңшеңіз.

**Өткізу модулі**

• Түс индикаторларымен кіру және шығу оқиғаларының тарихын көрсету.

• ACS жүйесі орнатылған ғимараттан өту тарихын көрсету.

• Жол жүру тарихын сүзу үшін кезеңді таңдаңыз.

Ақпаратты жинау және талдау қызметі:

• Жеткізуші/Өндірушінің веб-қызметіндегі авторизация жүйедегі пайдаланушының пайдаланушы аты мен құпия сөзі арқылы орындалуы керек.

• Браузер арқылы өту тарихы, толық аты-жөні, күні, уақыты және оқиғаның сипаттамасы туралы ақпаратты қараңыз. Нәтижелерді сұрыптау және сүзу мүмкіндігін қамтамасыз етіңіз.

• Әрбір пайдаланушының күнделікті әрекетін іздеңіз және көріңіз.

• Көрсетілген мерзім, пайдаланушы, бөлім бар pdf және xls пішіміндегі есептерді жүктеп алу.

• Әрбір қызметкер, бөлім немесе барлық қызметкерлер үшін кестелер мен демалыс күндерін жеке тағайындау.

• Белгіленген жұмыс кестелерін ескере отырып, әрбір қызметкердің кешіктіру және толық жұмыс істемеу уақытын есептеу.

• Әрбір пайдаланушы үшін аяқталмаған уақыт пен кешігу уақытын көрсететін pdf және xls файлындағы жиынтық есепті жүктеп алу.

• Бөлімшелер, сыныптар және тіркелген қызметкерлер туралы ақпаратты қарау.

Жүйеде клиент-сервер архитектурасы болуы керек. Бұлтты шешім қолданба мен бұлттық сервер арасында үздіксіз деректер алмасу арқылы қашықтағы жұмыс станцияларын біріктіруі керек. Жүйе қосымша конфигурацияны қажет етпей-ақ масштабтауға қолдау көрсетуі керек.

Веб-қызметтің клиенттік бөлігі көрсетілген нұсқадан төмен емес технологияларды қолдану арқылы жүзеге асырылуы керек: TypeScript 4.9 + React 18. Мемлекет менеджері - Redux Toolkit. Асинхронды сұраулармен жұмыс Redux Toolkit Query көмегімен жүзеге асырылуы керек. AntDesign UI құрамдас кітапханасы ретінде. Стильдермен жұмыс істеуді CSS Module + SASS препроцессоры (SCSS синтаксисі) арқылы шешу керек.

Интерфейс тілі: қазақ, орыс, ағылшын.

Тексеру кезінде сканерлеу әрекеттері таңдалған 3 тілдің бірінде: қазақ, орыс және ағылшын тілдерінде айтылуы керек.

Датчиктерде түсті индикатор болуы керек және жүйені пайдаланудың сәтті/сәтсіз сценарийлерін көрсетуі керек.

Кешен жеке техникалық ерекшелік шеңберінде Тапсырыс берушімен келісілген құрылғылардың, есептердің, статистиканың және басқа деректердің жай-күйі туралы ақпаратты беру бөлігінде API арқылы Тапсырыс берушінің басқа есепке алу жүйелерімен толық немесе ішінара біріктіру мүмкіндігін қамтамасыз етуі керек.

**Жүйе түйіндері:**

**Серверді қолдау:**

1. Деректерді сақтау және өңдеу үшін арнайы сервер сыйымдылығы.

2. Сервердің аппараттық құралдары Қазақстан Республикасының аумағында орналасуы керек.

3. Аппараттық құралдың өнімділігі Жүйенің 2 (екі) көшірмесінің жұмыс қабілеттілігін қамтамасыз ету үшін жеткілікті болуы керек.

4. Қолжетімді кеңістіктің көлемі есептеу деректерінің 2 (екі) данасын сақтау үшін жеткілікті болуы тиіс.

5. Аппараттық құрал орталық процессор ресурстарын пайдаланбай деректерді шифрлауды қамтамасыз етуі керек.

6. Серверді қолдаудың аппараттық-бағдарламалық кешені сыртқы шабуылдардың барлық түрлерінен қорғауды қамтамасыз етуі керек: DDoS, парольді болжау, жіберілетін деректерді ашу, MITM және т.б.

7. Секундына 100 000 қосылымға дейінгі жүктемелерде жұмыс істеу мүмкіндігі болуы керек.

Деректерді сақтау:

1. Дерекқорды басқару жүйесі (бұдан әрі – ДҚБЖ) ACID талаптарына сәйкес болуы керек.

2. ДҚБЖ Жүйенің жұмыс режиміне және бөлінген аппараттық ресурстарға сәйкес максималды өнімділік режимінде жұмыс істеуі керек.

3. Деректердің күнделікті сақтық көшірмесін AES-256 стандартынан төмен емес алгоритмді пайдалана отырып, көшірмелерді шифрлаумен қамтамасыз ету қажет.

4. Әрбір сақтық көшірме сервердің жергілікті жадында 7 күн және сыртқы қауіпсіз деректер жадында 30 күн бойы сақталуы керек.

5. Дерекқордағы алақан үлгілері AES-256 шифрлау стандарты арқылы шифрлануы керек, ал құпия деректерді сақтау үшін SHA512 хэштеу алгоритмі пайдаланылуы керек. ҚР СТ 34.016-2004.

**API**

1. API максималды өнімділік пен даму жылдамдығын қамтамасыз ететін жоғары деңгейлі бағдарламалау тілінде жазылуы керек.

2. API микросервис архитектурасына ие болуы және Kubernetes ортасында орналастыру үшін контейнерге оралуы керек.

3. API OWASP Top Ten қауіпсіздік талаптарына сәйкес болуы және JWT және OAuth 2.0 авторизациясын пайдалануы керек.

4. Әртүрлі авторизациялау механизмдері бар машиналар (компьютерлер) мен пайдаланушылар үшін рұқсатты бөлу жүзеге асырылуы тиіс. Машиналар криптографиялық күшті компьютер идентификаторымен байланыстырылуы және жүйеде бірегей болуы керек.

**Қолданбалы бағдарламалық қамтамасыз ету**

Бағдарламалық құралда бағдарлама файлдарын файлдық жүйеге орау үшін орнатушы және файлдарды файлдық жүйеден жою үшін жою құралы болуы керек.

1. Бағдарламалық құрал коды кері инженериядан және жад аймағын сканерлеу арқылы құпия деректерді алудан қорғалуы керек.

2. Үшінші тарап бағдарламаларының (Wireshark, Charles және т.б.) көмегімен желіге кіруді сканерлеуден қорғау қамтамасыз етілуі керек.

3. Бағдарламалық құрал параметрлері мен уақытша деректер SQLite протоколымен үйлесімді жергілікті дерекқорда кемінде AES-256 шифрлауын қолдану арқылы сақталуы керек.

4. Бағдарламалық жасақтама API арқылы деректерді серверге синхрондауы керек.

5. Бағдарламалық құралда қашықтан автоматты жаңарту мүмкіндігі болуы керек.

**Жеткізушіге қойылатын талаптар:**

1. Әлеуетті өнім беруші сенімді бағдарламалық қамтамасыз ету және электрондық өнімдер тізілімінен үзінді көшірмені ұсынуға міндетті.

2. Лицензияланбаған бағдарламалық қамтамасыз етуді болдырмау мақсатында жеткізуші лицензияланған бағдарламалық қамтамасыз етуді кемінде 3 жыл мерзімге ұсынады.

3. Әлеуетті өнім беруші техникалық ерекшелікте көрсетілген ұсынылатын тауарларға өндірушілердің немесе олардың (дилерлерінің немесе дистрибьюторларының) хаттарының (сертификаттарының, сертификаттарының) көшірмелерін, техникалық төлқұжаттарды, өнімнің сәйкестік сертификаттарын ұсынуға міндетті.

4. Өнім беруші нұсқаулықты/пайдаланушы нұсқаулығын (немесе оны алмастыратын басқа да нормативтік құжатты) ұсынуы тиіс, ол осы техникалық ерекшелікте көрсетілген кешеннің функционалдығын көрсетуі тиіс.

5. Ақпараттық қауіпсіздік процестерін зерттеу) «Ақпараттандыру туралы» Қазақстан Республикасының Заңына және Қазақстан Республикасы Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрінің 2019 жылғы 3 маусымдағы № 111/НҚ «Ақпараттық жүйелерді ақпараттық және сыни сыныбын өткізу қағидаларын бекіту туралы» бұйрығына сәйкес ақпараттық қауіпсіздік талаптарына сәйкестігіне тестілеуден өтуге бағдарламалық өнімге коммуникациялық инфрақұрылым объектілерінің ақпараттық қауіпсіздік талаптарына сәйкестігі туралы».

6. Жеткізуші Жүйені барлық байланысты шығындармен бірге кілт тапсыру негізінде жеткізуге және орнатуға міндетті. Қосылу және орнату үшін қажетті барлық шығын материалдары келісімшарт бағасына қосылуы керек.

7. Жұмысты орындау кезінде Жеткізуші 5 күнтізбелік күн ішінде шартқа қол қойғаннан кейін Тапсырыс берушінің өкілімен қажетті жабдықты орналастыруды келісу керек. Жабдықты жеткізгеннен кейін жеткізуші жабдықты орнатуы және конфигурациялауы, жүйені сынауы және жабдықты іске қосу үшін қажетті басқа жұмыстарды орындауы керек. Барлық іске қосу жұмыстары аяқталғаннан кейін Жеткізуші әрбір бөлме үшін шарт бойынша орнатылған барлық жабдықтың жоспар-сызбаларының 2 данасын ұсынуы қажет. Жабдықты монтаждау және реттеу бойынша барлық жұмыстар Қазақстан Республикасында қолданыстағы ҚНжЕ сәйкес жүргізілуі керек. Барлық тиісті қызметтер жасалған келісім шеңберінде орындалады. Жалпы талаптар: Шарт күшіне енген күннен бастап жеткізуші 16 күнтізбелік күні ішінде бүкіл жүйенің функционалдық сынақтарын ұйымдастыруы қажет.

**Кепілдік міндеттемелері**

Тапсырыс берушінің қол жеткізуді басқару жүйелерін монтаждау, конфигурациялау және қолданыстағы жабдыққа қосу кепілдігі жұмыстың аяқталуы туралы актіге қол қойылған күннен бастап кемінде 1 жылды құрайды. Тапсырыс беруші өтініш берген сәттен бастап Жеткізуші 10 күнтізбелік күннен аспайтын мерзімде өзінің Кепілдік міндеттемелерін орындауға міндетті.

**Кепілдік мерзімі ішінде рұқсатты басқару жүйесінің жабдықтарына техникалық қызмет көрсету**

Аппараттық құрал:

Алақан тамырларын оқуы:

1. Жұмысқа қабілеттілігін тексеру.

2. Бұзылған жағдайда жөндеу (жөндеу мүмкін болса).

**Контроллерлер (оның ішінде желілік):**

1. Жұмыс жағдайын тексеру және реттеу.

2. Қосылған контактілер тобының күйін тексеру.

3. Бұзылған жағдайда жөндеу (жөндеу мүмкін болса).

**Турникет тобы:**

1. Өнімділік диагностикасы.

2. Турникет есіктерін ашу және жабу функцияларын бағдарламалау параметрлерін тексеру.

3. Рұқсат етуді басқару жүйесінің жабдықтарымен диагностикалау және параметрлерді реттеу.

**Жүйе бөлігі:**

1. Жүйелік бағдарламалық құралды орнату.

2. Жүйеге қосымша модульдерді орнату және қосу.

3. Профильдер мен жабдық параметрлерінің резервтік көшірмелерін қалыптастыру, микробағдарламалық және бағдарламалық қамтамасыз ету нұсқаларын жаңарту.

4. Сақтық көшірмелерді қалпына келтіруді тексеру.

**Технические характеристики**

Поставщик должен использовать новое оборудование, не бывшим в употреблении. Поставщику необходимо осуществить поставку и установку программно аппаратного комплекса со следующими техническими характеристиками:

**Программно аппаратного комплекс биометрической системы (далее - ПАК)** интегрированных электронных сервисов для образовательных учреждений предназначен для внедрения передовых информационных технологий, повышающих качество образовательного процесса. В его состав входят сервисы управления и контроля доступа, бесконтактной биометрической идентификации по ладони, мобильные приложения для просмотра и ввода информации, сервис аналитики.

**Пак должен состоять из**:

Турникет , сканер, программного обеспечения

**Турникет:**

Материнская плата: должна быть разработана специально для устройств Интернета вещей, смарт-терминалов, систем NAS и промышленных приложений, с 64-разрядным процессором с не менее чем 4 ядрами и 4 потоками; Альтернативный графический процессор, gpu не ниже gpdr4, eppl eeprom, не менее 4КБ, разрешение не ниже, Не уступает последним версиям на мобильных платформах. Режим воспроизведения - поддерживаение несколько режимов воспроизведения, таких как циклический, синхронизирующий и промежуточный, Сеть не ниже 4G, Ethernet, WiFi / BT5.0, беспроводное периферийное расширение, Поддержка видеоформатов WMV, AVI, FLV, RM, RMVB, MPEG, TS, MP4 и т.д, Поддержка форматов фотографий BMP, JPEG, PNG, GIF, USB3.0\* 2 (ХОСТ \* 1, OTG \* 1), Разъем для подключения наушников камеры Mipi к интерфейсу ABC2E.,01i3n0te0rwfaCcea\*m4era, Последовательный порт RS232\*2,485\*1,TTL\*2,CAN-порт\*1 GPS 30pin FPC Внешний GPS (опционально) Разъем SATA\*1, поддержка BT, встроенный 2.4G WIFI, VT5.2 4G, Разъем для встроенного модуля MINIPCIE 4G, Ethernet 1000 М\*1, Поддерживание флэш-карта TF Trans, Двухканальный порт LVDS\*1 eDP x4 eDP-порт\*1, Стандартный порт HDMI2.0, ЖК-порт MIPI (40-контактный разъем FPC), Встроенный двухканальный AV-выход, поддержка усилителя 4R / 10 Вт на канал или 8R / 5 Вт на канал, Разъем для наушников, Встроенный 4-полюсный разъем 3,5 мм, Поддержка часов реального времени, Синхронизация включения / выключения ЖК-порта MIPI (40-контактный разъем FPC), Поддерживание AV-выход (порт RJ45 для удаленного управления запуском). СТ РК 3620-2020.

**Сканер:**

Процессор с низким энергопотреблением не ниже 400 МГц

Датчик изображений не менее 1/2.7", HDR CMOS, ближний инфракрасный диапазон

Разъем не менее 7-контактный разъем USB 2.0, 1.25 мм

Интерфейс связи USB 2.0 (Высокоскоростной)

Энергопотребление не более 0.5 Вт (режим ожидания) / 1.5 Вт (работа)

Условия освещения Регистрация <800 люкс; Идентификация <2000 люкс

Влажность от 0 до 90% относительной влажности

Сертификация CE, FCC, RoHS

**Оптические характеристики и характеристики изображения сканера:**

Тип сенсора Оптический

Размер изображения (в пикселях) не ниже 480 х 640 (ширина x высота)

Оттенки серого не ниже 256 уровней

Динамический диапазон не менее 83 дБ

Макс. частота кадров не ниже 25 кадров в секунду

Тип линзы ИК (IR)

Оптическая длина волны не менее 840-860 нм

Поле зрения (FOV) Диагональ = 58°, Горизонтальная = 37°, Вертикальная = 48°

Коэффициент оптических искажений не более ≤1%

Состав линзы из не менее 4 пластиковых линз и ИК- фильтра (4Р+11R). СТ РК ИСО/МЭК 15423-2009.

**В состав ПАК должны входить:**

1. Программно-аппаратные решения бесконтактной биометрической идентификации по рисунку вен ладони.

2. Сервис управления и контроля доступа: интеграция с учетными системами и контрольно-пропускными устройствами для эффективного контроля доступа персонала и учащихся к территории и ресурсам учебного заведения.

3. Мобильное приложение пользователя для просмотра статусов, получения уведомлений и управления профилями в режиме онлайн.

4. Сервис управления групповыми и личными чатами: для обеспечения создании различных групповых чатов в разрезе классов или личных чатов по учащимся.

5. Сервис сбора информации и аналитики: возможность формирования, обмена и экспорта отчетов по всем данным, собранным каждым из сервисов системы для администрации и преподавательского состава для быстрого и точного анализа информации, необходимой для оптимизации образовательного процесса.

**Минимальные функциональные требования к ПАК**

1. Должна соответствовать требованиям пункта 33-1 минимальных требований к объектам информатизации в области образования (Приказ МП РК №456 от 15.12.2012 года);

2. Необходимо наличие сервиса для интеграции с цифровыми образовательными ресурсами и (или) электронными учебниками и (или) системой контроля и управления доступом в организации образования;

3. Должен быть функционал по предоставлению обучающимся доступа к цифровым образовательным ресурсам и (или) электронным учебникам (при наличии доступа к цифровым образовательным ресурсам и (или) электронным учебникам у организации среднего (начального, основного среднего и общего среднего), в том числе специального и специализированного образования через личный кабинет бесплатного мобильного приложения и интернет-ресурса, с применением технологии единого входа (Single Sign-On).

4. Учет должен осуществляться с использованием технологий Palm ID (рисунок вен ладони).

5. Должна соответствовать требованиям информационной безопасности, в соответствии с пунктом 14 минимальных требований к объектам информатизации в области образования (Приказ МП РК №456 от 14.11.2022 года).

Все компоненты ПАК должны быть интегрированы друг с другом. Деактивация сервисов, интеграция и добавление новых должны осуществляться без необходимости проведения дополнительных интеграционных мероприятий со стороны заказчика. Процесс настройки и внедрения каждого сервиса не должен превышает 24 часов. По завершении этого периода заказчик должен иметь возможность пользоваться новыми функциями без дополнительных усилий: настройки, установки, ожидание приезда технических специалистов исполнителя, переустановки приложений у пользователей или проведения иных дополнительных операций.

**Защита биометрической информации должна быть организована на 2 уровнях:**

1) одном из указанных алгоритмов криптографических хеш функций: BelT, BLACK, Cube, Edonkey2k, FSB, Fugue, HAVAL, Hamsi, JH, Kupyna, Luffa, N-Hash, RIPEMD-128, RIPEMD-160, RIPEMD-256, RIPEMD-320, SHA-2, SHA-3 (Keccak), SHABAL, SHAvite-3, SIMD, SWIFFT, Skein, Snefru, Tiger, Whirlpool.

2) Данные зашифрованы одним из алгоритмов симметричного блочного шифрования: KCipher-2, MICKEY, MUGI, PIKE, Phelix 3,-WAY, ARIA, AES (Rijndael), Akelarre, KASUM,I Khafre, Khufu, MARS, MESH, MISTY1, NewDES, REDOC, SC2000, SHACAL, CS-Cipher.

Все сервисы должны основываться на идентификации пользователей по сканированию рисунка вен ладони. Для авторизации, идентификации и подтверждения действий.

**Система контроля и управления доступом**

• Приложение для рабочего компьютера должно начинаться с краткого пошагового ознакомления пользователя с функционалом системы и инструкцией по первоначальной настройке СКУД.

• Регистрации первоначального входа с помощью ввода пароля из электронной почты.

• Самостоятельное заполнение данных об организации.

• Ручной ввод регистрационных данных администратора системы, обслуживающего организацию. Регистрация администратора должно происходить с помощью считывания документа, удостоверяющего личность через картридер с автоматическим заполнением полей персональных данных и фотографии.

Ознакомление и подписание Согласия на сбор и обработку персональных данных

**Добавления фотографии пользователей и ее редактирования.**

По завершению регистрации, администратор должен зарегистрировать свою ладонь в качестве авторизационного ключа (вместо логина и пароля). Последующие авторизации всех пользователей, имеющих доступ к редактированию данных, должно осуществляться только через биометрический сканер вен ладони.

Регистрация пользователей должна производиться в 4 этапа:

1) Автоматический ввод данных с картридера для считывания персональных данных и фотографии с удостоверения личности гражданина РК. Так же должен быть доступен ручной ввод или редактирование ФИО, ИИН, должность, отдел, телефон, фото.

2) Прочтение и подтверждение электронного ознакомления с Согласием на сбор и обработку персональных данных.

3) Регистрация обоих ладоней с помощью биометрического сканера рисунка вен ладони.

4) Подтверждение успешной/не успешной регистрации.

Зарегистрированные пользователи должны быть разделены администратором через графический интерфейс на 3 группы прав: Администратор (просматривает списки пользователей, редактирует и наделяет правами), Редактор (просматривает списки пользователей, редактирует), Наблюдатель (просматривает списки пользователей). Редактирование прав должно осуществляться в отдельном меню.

Тест сканирования. Для обучения и проверки функций системы по биометрической идентификации рисунка вен ладони.

**Требования к пользовательскому интерфейсу приложения:**

• Поддержка различных разрешений экрана.

• Многоязычный интерфейс (казахский, русский и английский языки).

• Интуитивно понятный и легкий в использовании дизайн.

• Сканирование:

- Возможность поднесения руки к устройству для сканирования.

- Выбор типа события: вход или выход.

Управление:

- Авторизация в Системе только после успешного сканирования рисунка вен ладони.

- Регистрация сотрудника с заполнением полей.

- Тест сканирования для проверки работоспособности Системы.

- История проходов с таблицей (ФИО, должность, дата, время, событие: вход/выход).

- Список сотрудников (фото, дата и время регистрации, сканированные ладони, функции редактирования/удаления/повторного сканирования/выдачи прав).

- Управление правами доступа (администратор, пользователь, гость).

• Верхнее меню с иконкой пользователя:

- Отображение информации о тарифе и сроке окончания подписки.

- Настройки, доступные только установщику-сотруднику Исполнителя

- Выход из приложения.

• Управление чатом:

-Создание чат групп. Редактирование описаний. Функции модерации.

-Создание опросов. Выбор типа. Ввод вопроса. Приглашение к участию. Отображение результатов голосования.

- Публикация новостей и выбор получателей.

**Мобильное приложение**

• Регистрация и авторизация пользователей по номеру телефона.

**Модуль «Дети»**

• Просмотр и редактирование профиля детей, включая добавление фото.

• Просмотр истории проходов ребенка по дням и времени.

• Чаты и голосование. Групповые и личные чаты. Отображение актуальных новостей и событий. Возможность проведения голосований среди пользователей.

• Уведомления о событиях. Получение уведомлений о входе/выходе через турникет, получении/сдачи книги и оповещении новом сообщении в чатах. Настройка параметров уведомлений пользователем.

**Модуль проходы**

• Отображение истории проходов по событиям вход и выход с цветовыми индикаторами.

• Отображение истории проходов из здания, в которых установлена СКУД Системы.

• Выбор периода для фильтрации истории проходов.

**Сервис сбора информации и аналитики:**

• Авторизация в Web-сервисе Поставщика/Производителя должна производиться по логину и паролю пользователя в системе.

• Просмотр через браузер информации об истории проходов, ФИО, дате, времени и описании события. Предоставить возможность сортировки и фильтрации результатов.

• Поиска и просмотр подневной активности каждого пользователя.

• Выгрузка отчетов в формате pdf и xls файлов с установленным периодом, пользователям, отделом.

• Назначения графиков и выходных дней персонально на каждого работника, отдел, или всех сотрудников.

• Расчет времени опоздания и недоработки каждого сотрудника с учетом назначенных рабочих графиков.

• Выгрузка суммирующего отчета в pdf и xls файле, с указанием недоработанного времени и времени опоздания по каждому пользователю.

• Просмотр информации об отделах, классах и зарегистрированных сотрудниках.

Система должна иметь клиент-серверную архитектуру. Облачное решение должна объединять удаленные рабочие места посредством постоянного обмена данными между приложением и облачным сервером. Система должна поддерживать масштабируемость, не требующую дополнительной настройки.

Клиентскую часть Web сервиса должна быть реализована на технологиях, не ниже указанных версии: TypeScript 4.9 + React 18. State manager - Redux Toolkit. Работа с асинхронными запросами должна реализовываться посредством Redux Toolkit Query. AntDesign в качестве библиотеки UI-компонентов. Работа со стилями должна быть решена с помощью CSS Module + SASS preprocessor (SCSS синтаксис).

Язык интерфейсов: казахский, русский, английский.

Действия сканирования при верификации должны быть озвучены на одном из 3 выбранных языков: казахский, русский и английский.

Датчики должны обладать цветовой индикацией и должны отображать успешные/не успешные сценарии использования системы.

Комплекс должна предусматривать возможность полной или частичной интеграции по API с другими учетными системами Заказчика в части передачи информации о состоянии устройств, отчетов, статистик и др. данных, согласованных с Заказчиком в рамках отдельной технической спецификации.

**Узлы Системы:**

**Серверное обеспечение:**

1. Выделенные серверные мощности для хранения и обработки данных.

2. Серверное аппаратное обеспечение должно располагаться на территории Республики Казахстан.

3. Производительность аппаратного обеспечения должна быть достаточной для обеспечения работоспособности 2 (двух) экземпляров Системы.

4. Объем доступного пространства должно быть достаточным для хранения 2 (двух) экземпляров расчетных данных.

5. Аппаратное обеспечение должно обеспечивать шифрование данных без использования ресурсов центрального процессора.

6. Программно-аппаратный комплекс серверного обеспечения должно обеспечивать защиту от всех видов внешних атак: DDoS, перебор пароля, раскрытие передеваемых данных, MItM и т.д.

7. Должна быть обеспечена возможность работы при нагрузках до 100 000 соединений в секунду.

**Хранение данных:**

1. Система управления базами данных (далее — СУБД) должна соответствовать требованиям ACID.

2. СУБД должна работать в режиме максимальной производительности в соответствии с режимом работы Системы и выделенных аппаратных ресурсов.

3. Должно обеспечиваться ежедневное резервное копирование данных с шифрованием копий алгоритмом не ниже AES-256.

4. Каждая резервная копия должна храниться на локальном хранилище сервера в течении 7 дней и на внешнем защищенном хранилище данных в течении 30 дней.

5. Шаблоны ладоней в базе данных должны быть зашифрованы по стандарту шифрования AES-256, для хранения чувствительных данных должен быть использован алгоритм хэширования SHA512. СТ РК 34.016-2004.

**API**

1. API должен быть написан на языке программирования высокого уровня, обеспечивающего максимальную производительность и скорость разработки.

2. API должен иметь микросервисную архитектуру и быть упакован в контейнер для развертывания в среде Kubernetes.

3. API должен соответствовать требованиям безопасности OWASP Top Ten и использовать авторизацию через JWT и OAuth 2.0.

4. Должно быть осуществлено разделение доступов для машин (компьютеров) и пользователей с разными механиками авторизации. Машины должны быть привязаны к криптографически стойкому идентификатору компьютера и уникальны в системе.

**Прикладное программное обеспечение**

ППО должен иметь инсталлятор для распаковки файлов программы в файловую систему и деинсталлятор для удаления файлов из файловой системы.

1. Программный код должен быть защищен от реверс инжиниринга и от извлечения чувствительных данных путем сканирования области памяти.

2. Должна быть предусмотрена защита от сканирования обращения к сети с помощью сторонних программ (Wireshark, Charles и т.д.).

3. Настройки и временные данные ПО должны храниться с использованием шифрования не ниже AES-256 в локальной базе данных, совместимых с протоколом SQLite.

4. ППО должно синхронизировать данные на сервер с использованием API.

5. ППО должно иметь функционал удаленного автообновления.

**Требования к поставщику:**

1. Потенциальный поставщик должен предоставить выписку из реестра доверенного программного обеспечения и продукции электронной промышленности.
2. В целях недопущения нелицензионного программного обеспечения поставщик предоставляет лицензионное прогрмнное обеспечение сроком не менее чем на 3 года.
3. Потенциальный поставщик должен предоставить копий писем (сертификатов, свидетельств) от производителей либо их (дилеров или дистрибьюторов), технических паспортов, сертификатов соответствия продукции, на предлагаемые товары, указанные в технической спецификации.
4. Поставщик должен предоставить инструкцию/руководство пользователя (или иной его заменяющий регламентный документ), в котором должно быть отражен функционал комплекса, указанный в настоящей технической спецификации.
5. Обследование процессов обеспечения информационной безопасности) на программный продукт о прохождении испытания на соответствие требованиям информационной безопасности в соответствии с Законом Республики Казахстан «Об информатизации» и приказом Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года №111/НҚ «Об утверждении методики и правил поведения испытаний объектов информатизации «электронного правительства» и информационных систем, отнесенных к критически важным объектам информационно-коммуникационной инфраструктуры, на соответствие требованиям информационной безопасности».
6. Поставщик должен произвести доставку и установку Системы под ключ, со всеми сопутствующими расходами. Все расходные материалы, необходимые для подключения и установки, должны быть включены в стоимость договора.
7. При выполнении работ Поставщик должен согласовать размещение необходимого оборудования с представителем Заказчика после подписания договора в течении 5-и календарных дней. После поставки оборудования поставщик должен произвести установку и настройку оборудования, провести тестирование работы системы, а также другие работы необходимые для запуска оборудования в эксплуатацию. После завершения всех пусконаладочных работ Поставщик должен предоставить план-схемы всего установленного в рамках договора оборудования на каждое помещение в 2- х экземплярах. Все работы по монтажу и наладке оборудования должны проводиться в соответствии со СНиП, действующими на территории Республики Казахстан. Все сопутствующие услуги выполняются в рамках заключенного договора. Общие требования: По заключению договора поставщик должен организовать функциональное тестирование всей системы в течении 15 рабочих дней.

**Гарнатийные обезательства**

Гарантия по установке, настройке и подключению к имеющемуся оборудованию систем контроля управления доступом Заказчика не менее 1 года с момента подписания акта выполненных работы.. **В случае выхода из строя в гарантийный период ПАК все детали и расходные материалы оборудования должны быть заменены за счет Поставщика**. С момента обращения Заказчика Поставщик в срок не более 10 календарных дней должен выполнить свои Гарантийные обязательства.

**Обслуживание оборудования системы контроля управления доступом в гарантийный период**

**Аппаратная часть:**

**Считыватели вен ладони:**

1. Проверка работоспособности.

2. Ремонт в случае поломки (при наличии возможности ремонта).

Контроллеры (в том числе сетевые):

1. Проверка состояния работоспособности и регулировка.

2. Проверка состояния подключенной группы контактов.

3. Ремонт в случае поломки (при наличии возможности ремонта).

**Турникетная группа:**

1. Диагностика работоспособности.

2. Проверка настроек программирования функций открытия, закрытия створок турникета.

3. Диагностика и регулировка настроек с оборудованием системы контроля управления доступом.

**Системная часть:**

1. Настройка программного обеспечения системы.

2. Монтаж и подключение дополнительных модулей к системе.

3. Формирование резервных копий профилей и настроек оборудования, обновление версий микропрограмм и программного обеспечения.

4. Проверка восстановления резервных копий.