Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасының Ішкі істер министрлігі" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасының Ішкі істер министрлігі" мемлекеттік мекемесі
Конкурстың №:	№ 17868418-1
Конкурстың атауы:	2027 жылға арналған ақпараттық ресурстарға қол жеткізу қызметтеріне конкурс
Лоттың нөмірі:	№ 88114334-ОК1
Лоттың атауы	Бағдарламалық өнімді пайдалану қызметі
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	620920.000.000014
Қызметтің атауы:	Бағдарламалық өнімді пайдалану қызметі
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	841379.31
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	841379.31
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	2027 жылғы 31 желтоқсанға дейін
Аванстық төлем мөлшері:	0
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	«QYZMET-POLICE.KZ» БАҒДАРЛАМАЛЫҚ ҚАМТАМАСЫЗ ЕТУГЕ ҚОЛ ЖЕТКІЗУ БОЙЫНША ТЕХНИКАЛЫҚ СИПАТТАМА. Қызметтер 2027 жылғы 31 желтоқсанды қоса алғандағы мерзімге көрсетілуі тиіс. Қызмет азаматтарды ІІМ органдарына қабылдау процестерін автоматтандыруға арналған бағдарламалық қамтамасыз етуге қол жеткізуді қамтамасыз етеді. Жүйе онлайн түрде өтініштерді қабылдауды, деректерді автоматты өңдеуді, қажетті құжаттар тізімін қалыптастыруды, бекітілген іріктеу кезеңдерінен өту және сыртқы мемлекеттік ақпараттық жүйелермен өзара әрекеттесуді қамтамасыз етеді. Қол жеткізу біріккен сандық платформаны пайдаланып, қабылдау процестерінің ашықтығын арттырады, өтініштерді қарау мерзімін қысқартады және кадр бөлімшелерінің жұмысын жеңілдетеді. Азаматтар барлық кезеңдерді қашықтықтан өтіп, кадр қызметіне жеке келмей-ақ жұмысқа орналаса алады. Қол жеткізудің мақсаты - азаматтарды ІІМ органдарына қабылдау рәсімдерін жетілдіру арқылы бірыңғай сандық қабылдау жүйесін құру. Бағдарламалық қамтамасыз ету келесі процестерді автоматтандырады: ● ІІМ-ге қабылдану үшін электронды өтініштерді беру; ● Құжаттарды жинау, тексеру және өңдеу; ● Міндетті кезеңдерден өту және нәтижелерді алу; ● Электрондық жеке істерді қалыптастыру және жүргізу; ● Адам факторын рәсімдеу процесіне әсерін азайту; ● Ашықтықты арттыру және сыбайлас жемқорлық тәуекелдерін азайту; ● Өтініштерді қарау мерзімін қысқарту және кадрлық рәсімдерді оңтайландыру. 1. Автоматтандырылатын процестер: Бағдарламалық қамтамасыз ету келесі функцияларды автоматтандырады: ● ІІМ қызметі туралы ақпарат беру; ● Бос орындарды және қабылдау шарттарын қарау; ● Кандидаттың болжамды ақысын есептеу; ● Электрондық өтініш беру; ● Өтінішті қабылдау, бастапқы өңдеу және тіркеу; ● Өтініштің жағдайын және орындалу мерзімін бақылау; ● Электрондық жеке істі қалыптастыру; ● Кандидатты кезеңдерден өту және құжаттарды ұсыну қажеттілігі туралы хабарландыру; ● Міндетті рәсімдердің нәтижелерін алу (медкомиссия, ФИЗО, полиграф, тестілеу, сұхбат); ● Кандидаттың біліктілік талаптарына сәйкестігін тексеру; ● Өтініштер мен олардың қаралу нәтижелерінің электрондық мұрағатын қалыптастыру және сақтау. Қол жеткізу құқықтарын бөлу: Бағдарламалық қамтамасыз етуге пайдаланушылардың қол жеткізуі бекітілген рөлдер арқылы анықталады. Жалпы 8 пайдаланушы рөлі бар: Жүйе әкімшісі: пайдаланушыларды тіркеу, рөлдерді тағайындау, өзгерту және жою, есептік жазбаларды басқару, ПО әкімшілігі, жаңарту және техникалық қызмет көрсету, сақтық көшірме жасау, ұйымдық құрылымды басқару, анықтамалықтар жүргізу, қауіпсіздік талаптарының сақталуын бақылау. Кадр қызметінің басшысы: барлық өтініштерді қарау, өңдеу кезеңдерін бақылау, орындалу мерзімдерін қарау, бас тартуларды талдау, өтініштерді орындаушылар арасында бөлу, жеке істер мен аналитикаға қол жеткізу. Орындаушы (кадр қызметкері): бос орындарды құру және өңдеу, түскен өтініштерді тексеру, жеке істі қалыптастыру, өтініш берушіні түзетуге жіберу, кезеңдердің нәтижелерін алу (медкомиссия, ФИЗО, полиграф, тестілеу, сұхбат), мұрағатпен

	жұмыс. ЦВВК қызметкері: Кірген өтініштерді қарайды; құжаттардың дұрыстығын тексереді; өтінішті қабылдайды немесе қабылдамайды; медициналық қорытынды жасайды және жүктейді; архивпен жұмыс істейді. Дене дайындығы инспекторы (ФИЗО): Өтініштер мен жеке істерді қарайды; нормативтерді тапсыру күнін және уақытын белгілейді; нәтижелерді енгізеді; растайтын құжаттарды тіркейді; архивпен жұмыс істейді. Полиграфолог: Өтініштер мен жазбалар күнтізбесіне қол жеткізе алады; зерттеу уақытын тағайындайды; жеке істі қарайды; нәтижелерді енгізеді және қорытындыны жүктейді; архивпен жұмыс істейді. Конкурс комиссиясы: Жеке істерді қарайды; сұхбат уақыты мен күнін белгілейді; онлайн-сұхбат өткізеді; соңғы шешімді тіркейді; құжаттар мен комментарийлерді тіркейді; кандидаттың әрі қарайғы бағытын анықтайды. Кандидат: Вакансияларды және шарттарды қарауға қол жеткізеді; ұйым мен лауазымды таңдайды; өтініш толтырады және береді; статусты бақылайды; кезеңдерге күн мен уақытты таңдайды; тестілеуден өтеді; хабарламалар алады; құжаттарды жүктейді; өтініштерді ЭЦҚ арқылы қол қояды; ФИЗО тапсыруға жолдама алады. Үдерістерді сипаттау Бағдарламалық қамтамасыз ету азаматтарды ішкі істер органдарына қызметке қабылдаудың толық циклі бойынша автоматтандырылған өңдеуді қамтамасыз етеді, оған кандидаттың тіркелуі, электрондық өтініштің жасалуы, іріктеу кезеңдерінен өту және соңғы шешім қабылдау кіреді. Жүйе өтініштердің жауапты қатысушылар арасында кезең-кезеңімен бағытталуын қолдайтын біртұтас цифрлық сервис ретінде жұмыс істейді. Бағдарламалық қамтамасыз ету қамтамасыз етеді: ● кандидаттар мен кадр бөлімдерінің қызметкерлерінің жеке кабинеттін құру және жүргізу; ● қызметке қабылдау үшін электрондық өтініштерді қалыптастыру, тіркеу және сақтау; ● бекітілген бизнес-процеске сәйкес өтініштердің өңдеу кезеңдері арасындағы автоматтандырылған маршрутизациясы; ● кандидатты тексеруге қажетті мәліметтерді алу үшін сыртқы мемлекеттік ақпараттық жүйелермен интеграциялық деректер алмасу; ● енгізілген деректер мен алынған тексеру нәтижелеріне негізделген электрондық жеке істі автоматтандырылған түрде қалыптастыру; ● міндетті процедуралардан өтуге өтініштердің берілуі (медициналық тексеру, полиграфологиялық зерттеу, физикалық дайындық, тестілеу, сұхбат); ● аталған процедуралардан өткен нәтижелерді электрондық түрде алу және тіркеу; ● тағайындалған процедураларға қолжетімділік күнтізбелерін қамтамасыз ету және кандидатқа уақытты таңдау мүмкіндігін беру; ● кадр қызметкерлерімен, әскери-медициналық комиссиямен, полиграфологтармен, ФИЗО инспекторларымен және конкурс комиссиясымен электрондық өзара әрекеттесу; ● процедуралар нәтижелері мен уәкілетті тұлғалардың шешімдеріне сәйкес өтініштердің мәртебесін автоматты түрде өзгерту; ● ары қарайғы кезеңдерге өту немесе өтуге рұқсат бермеу туралы соңғы шешімдерді қалыптастыру, сондай-ақ ІІМ білім беру ұйымдарына (бастапқы дайындық академиялары) жолдау құру; ● өтініштердің және олардың қаралу хаттамаларының электрондық архивін жүргізу. Бағдарламалық қамтамасыз

	етудің жұмысы деректерді өңдеудің регламенттелген маршруттарына негізделген. Кезеңдер арасындағы өту логикасы, автоматты тексеру критерийлері, өту, қабылдамау немесе қайта өңдеуге қайтару шарттары жүйенің функционалдық моделіне енгізілген және серверлік бөлімі арқылы пайдаланушының қатысуынсыз қамтамасыз етіледі. Жүйе қолдайды: ● өту немесе қабылдамау шарттары нормативтік талаптармен анықталатын жағдайларда автоматты шешім қабылдауды; ● сыртқы жүйелерден процедуралардың нәтижелерін қабылдауды (мысалы, «Damumed» ИС-інен медициналық қорытынды немесе прокторинг деректері); ● барлық аралық деректерді, файлдық материалдарды және тексеру нәтижелерін құрылымдық түрде сақтау; ● оқиғалар журналын, мәртебелер өзгерістерінің логтарын, комиссия шешімдерінің хаттамаларын және кадр іс жүргізу ережелерінде қарастырылған басқа да деректерді қалыптастыру. Бағдарламалық қамтамасыз ету орталықтандырылған сервис ретінде жұмыс істейді, өтініштерді өңдеудің біртұтас технологиялық контурын, олардың тексерілуін, барлық міндетті іріктеу кезеңдерінен өтуін және соңғы нәтижесін ІІМ кадрлық жүйелеріне жеткізуді қамтамасыз етеді. 2. Функционалдық талаптар Процестерді сипаттау Бағдарламалық қамтамасыз ету пайдаланушыларға тағайындалған рөлдерге сәйкес функционалға қолжетімділікті қамтамасыз етеді және ішкі істер органдарына азаматтарды қызметке қабылдау бизнес-процесінде қарастырылған операцияларды орындауды қамтамасыз етеді. Тіркеусіз қолжетімділік Тіркелмеген пайдаланушылар келесі бөлімдерге қол жеткізе алады: ● ІІО қызметі туралы жалпы ақпарат; ● аймақ, департамент және аудан бойынша сүзгілеумен бос орындар тізімі; ● болжамды айлық мөлшерін есептейтін калькулятор. Бұл функциялар тек қарау режимінде жұмыс істейді. Негізгі ақпараттық бет Басты бет көрсетеді: ● ІІО қызметі туралы жалпы мәліметтер; ● нормативтік ақпарат пен талаптар; ● консультация алу үшін Call-орталықтың байланыс деректері. «Бос орындар» бөлімі Бөлімнің функционалы қамтамасыз етеді: ● бос орындардың толық тізімін көрсету; ● аймақ, департамент және аудан бойынша сүзгілеу; ● таңдалған параметрлерге сәйкес бос орындарды автоматты түрде шығару; ● бос орын картасын толық сипаттамасымен көрсету (лауазым, бөлімше, талаптар, міндеттер, лауазым түрі және т.б.); ● өтініш беру бетіне өту (тіркелген пайдаланушылар үшін). «Калькулятор» бөлімі Калькулятор: ● үміткердің болжамды табысын есептейді; ● бос орын параметрлерін пайдаланады (санат, біліктілік, мемлекеттік құпияға қолжетімділік және т.б.); ● енгізілген деректерге (лақап, жұмыс өтілі және т.б.) негізделген нәтижені қалыптастырады. Тіркеу және авторизация Бағдарламалық қамтамасыз ету: ● үміткерді тіркеу формасын ұсынады; ● телефон нөмірін растауды сұрайды; ● тіркеуден кейін жеке кабинет құрады; ● ЭЦҚ немесе логин/құпия сөз арқылы авторизацияны қамтамасыз етеді. Өтінішті қалыптастыру және жіберу Өтініш беру функционалы қамтиды: ● бірегей нөмір тағайындаумен электрондық өтініш жасау; ● ЭЦҚ негізінде ФИО және ЖСН-ді автоматты түрде толтыру; ● анкетаны

	толтыру, соның ішінде білім, байланыс деректері және туыстары туралы мәліметтер; ● сканерленген құжаттарды жүктеу; ● жобасын сақтау немесе өтінішті жіберу; ● жіберу кезінде ЭЦҚ арқылы қол қою. Әрбір бос орын жеке өтініш жасайды. Өтініш мәртебесін қадағалау «Менің өтініштерім» бөлімі: ● үміткердің барлық өтініштерін көрсетеді; ● ағымдағы мәртебе мен өңдеу кезеңін көрсетеді; ● келесі кезеңге өткенде мәртебені автоматты түрде жаңартады; ● хабарламалар мен пікірлерді қалыптастырады. Кадрлық қызметкерлердің өтініштерді өңдеуі Кадрлық қызметкер: ● түскен өтініштерді қарастырады; ● деректер мен тіркелген құжаттардың дұрыстығын тексереді; ● өтінішті қабылдау, бас тарту немесе түзетуге жіберу туралы шешім қабылдайды; ● үміткердің электрондық жеке ісін қалыптастырады; ● мемлекеттік ИС арқылы алынған деректерді пайдаланады; ● шешімдерді жүйеде тіркейді. Есептілікті қалыптастыру Жүйе: ● бекітілген параметрлер бойынша есептер қалыптастырады; ● статистиканы кезеңдер, аймақтар және өңдеу кезеңдері бойынша көрсетеді; ● тіркелген пайдаланушылар, бас тартулар, түзетулер, архив және ағымдағы жүктеме туралы деректерді ұсынады. Ведомстволық рөлдердің функционалы Әскери-медициналық комиссия (ӘМК): ● медициналық тексеруге өтініштерді қарайды; ● құжаттарды тексереді; ● қорытындыны тіркейді; ● өтініштерді қабылдайды немесе бас тартады; ● өңделген нәтижелерді кадрлық орындаушыға жібереді. Кадрлық қызмет орындаушысы: ● өтініштермен барлық кезеңдерде жұмыс істейді; ● мемлекеттік базаларға сұраныстар жасайды; ● тексеру нәтижелерін алады; ● жеке істі қалыптастырады және жаңартады. Интеграциялар арқылы алынатын деректер тізімі (техникалық мүмкіндігі болған жағдайда) Жүйе алады және көрсетеді: ● үміткердің жеке деректері; ● ЖСН деректері; ● туыстары туралы мәліметтер; ● кәсіпкерлік қызмет туралы деректер; ● салықтық ақпарат және декларациялар; ● табыс пен ұсталған салықтар туралы деректер; ● несие тарихы; ● жеке деректерді өңдеуге келісім; ● мобильді азаматтар базасындағы мәртебе; ● мүгедектік туралы мәліметтер; ● білім, еңбек қызметі, зейнетақы аударымдары туралы деректер; ● қылмыстық әрекеттер, құқық бұзушылықтар, шектеулер туралы мәліметтер; ● диспансерлерден медициналық деректер. Ақпарат асинхронды түрде келеді және өңдеуден кейін көрсетіледі. Бос орындарды жариялау Бөлім ұсынады: ● бос орындарды жасау, өңдеу, жою; ● жарияланған бос орындарды үміткерге автоматты түрде көрсету. Есептерді қалыптастыру Жүйе басшыға құралдар ұсынады: ● өтініштер бойынша есептерді қалыптастыру; ● есеп материалдарын сақтау және басып шығару. Басшының функционалы Басшы: ● барлық түскен өтініштерді қарайды; ● олардың өңделу процесін бақылап отырады; ● өтініштерді орындаушыларға бөледі; ● қызметкерлердің жүктемесін басқарады. 3. Жүйенің функционалды емес талаптары және архитектурасы Функционалды емес талаптар Пайдаланушы интерфейсі Жүйенің пайдаланушы интерфейсі көптілділікті қолдайды (қазақ және орыс тілдері) әрі болашақта тілдік қолдауды кеңейтуге мүмкіндік береді. Интерфейс экранның

	1024×600 пиксель және одан жоғары рұқсатында дұрыс көрсетіледі. Жүйе келесі браузерлердің өзекті тұрақты нұсқаларында жұмыс істейді: ● Google Chrome ● Mozilla Firefox ● Safari ● Microsoft Edge «Өзекті тұрақты нұсқа» деп браузер әзірлеушісі тарапынан пайдалануға арналған тұрақты релиз ретінде жарияланған нұсқасы түсіндіріледі. Эксплуатациялық сипаттамалар Бағдарламалық қамтамасыз ету келесі технологиялық стек бойынша жұмыс істейді: ● Backend: C#, ASP.NET MVC 3.0 ● Бағдарламалау тілі: C# ● СУБД: PostgreSQL Дерекқордың резервтік көшірмесі жеткізуші тарапынан ай сайын жасалады. Клиенттік және серверлік деңгей арасындағы деректер алмасу SOAP протоколы арқылы жүзеге асырылады, ол деректерді алу, өзгерту және өңдеу сұраныстарын орындау үшін қолданылады. 4. Жүйенің архитектурасы Жалпы құрылым Жүйенің архитектурасы екі контекстке бөлінеді: ● Сыртқы контур - үміткерлерге веб-портал арқылы қолжетімді сервистер. ● ІІМ ішкі контур - өтініштерді өңдеу және ІІМ қызметкерлерінің өзара әрекеттесуі. Контурларды бөлу жеке деректермен қауіпсіз жұмыс жасау және ішкі ресурстарға қолжетімділікті шектеу мүмкіндігін қамтамасыз етеді. Жүйе модульдері Өтініштерді беру модулі (Сыртқы контур) Модуль ашық функционалды ұсынады: ● қызмет және бос орындар туралы ақпаратқа қолжетімділік; ● ЭЦҚ арқылы электрондық өтінішті толтыру және қол қою; ● өтінішті серверлік бөлікке жіберу әрі әрі қарай өңдеу; ● пайдаланушы деректерін қалыптастыру және дерекқорға сақтау. Сыртқы модульге интернет арқылы персоналды компьютерлерден қосылуға болады. Өтініштерді өңдеу модулі (ІІМ ішкі контур) Ішкі модуль ІІМ қызметкерлеріне өтініштерді толық өңдеу циклін қамтамасыз етеді. Функционалды қасиеттері: ● ЖСН бойынша мемлекеттік ИС арқылы SmartBridge арқылы деректерді автоматты алу; ● алынған ақпаратты ІІМ қорғалған дерекқорына жазу; ● ІІМ қызметкерлерінің өтініш деректері, құжаттар, тексеру нәтижелеріне қолжетімділігі; ● ішкі интерфейстер арқылы үміткерлермен өзара әрекеттесу; ● өтініштердің тарихын, операция журналдарын және архивін жүргізу. Қолжетімділік тек ІІМ ішкі қорғалған желісінен қамтамасыз етіледі, интернетке шығу жоқ. Желілік талаптар Сыртқы желі Сыртқы желінің функциялары: ● пайдаланушылардың веб-порталға интернет арқылы қолжетімділігі; ● веб-қосымша серверлері мен API жұмысы, кіріс сұраныстарын өңдеу; ● HTTPS протоколы бойынша қорғалған қосылымды қамтамасыз ету. Ішкі желі ІІМ ішкі желісі қамтамасыз етеді: ● қызметкерлердің тек қорғалған ішкі арналар арқылы қолжетімділігі; ● дерекқорлар мен жеке деректерді оқшауланған серверлерде сақтау; ● (техникалық мүмкіндік болған жағдайда) мемлекеттік жүйелермен (ЕТС, SmartBridge және т.б.) қорғалған арналар арқылы интеграция. Архитектуралық модель сипаттамасы Жүйенің архитектурасы: ● веб-порталды (сыртқы контур) және өтініштерді өңдеу серверін (ІІМ ішкі контур) бөледі; ● деректерді тексеру үшін SmartBridge және ЕТС интеграциялық механизмдерін қолданады (техникалық мүмкіндік болған жағдайда); ● пайдаланушы сервистері мен жеке деректерді

	өңдейтін сервистердің логикалық оқшауланuын қамтамасыз етеді; ● қосалқы жүйелер арасында қауіпсіз өзара әрекеттесуді және үміткерлердің жеке деректерін қорғауды қолдайды. Мұндай архитектура жүйенің тұрақтылығын, ақпараттың қорғалуын және өтініштерді беру мен өңдеу процестерін оңтайландыруды қамтамасыз етеді. Сыртқы және ішкі желілер арасындағы өзара әрекет сценарийі Жалпы өзара әрекет схемасы Жүйе сыртқы контур (өтініштерді беру веб-порталы) мен ІІМ ішкі контур (өтініштерді өңдеу интерфейсі) арасында деректердің қауіпсіз алмасуын қамтамасыз етеді. Өзара әрекеттесу электрондық үкіметтің қорғалған шлюзі (ШЭП/ВШЭП) арқылы SOAP протоколымен криптографиялық қорғауды қолданып жүзеге асады, бұл деректердің тұтастығы, шынайылығы және құпиялылығын кепілдейді. Контурлар арасындағы логикалық өзара әрекет реттілігі 1-кезең. Сыртқы контур: өтінішті қалыптастыру және жіберу Сыртқы портал электрондық өтініш қалыптастырады, оны дерекқорында сақтайды және SOAP-пакетті дайындайды, онда өтініштің бірегей идентификаторы, ЖСН және басқа құрылымдық атрибуттар болады. Дайындалған хабар ІІМ ішкі контурына ШЭП/ВШЭП арқылы HTTPS қорғалған арнадан жіберіледі. 2-кезең. Ішкі контур: өтінішті қабылдау және өңдеу Ішкі контур SOAP-хабарламаны қабылдайды, қолтаңбаны және қауіпсіздік параметрлеріне сәйкестікті тексереді. Тексеру сәтті өткен соң өтініш деректері ІІМ қорғалған ішкі дерекқорына сақталады. Жүйе SmartBridge арқылы мемлекеттік ақпараттық жүйелерге автоматты сұраныстар жібереді, соның ішінде үміткердің жеке басы, құқықтық мәртебесі, құқық бұзушылық тарихы, әлеуметтік және медициналық мәртебесі туралы мәліметтер алу. Тексеру нәтижелері ішкі контурда тіркеледі. 3-кезең. ІІМ қызметкерлерінің жұмысы Авторизацияланған ІІМ қызметкерлері жабық желіде жұмыс істейтін ішкі веб-интерфейс арқылы өтініш деректеріне қол жеткізеді. Қызметкерлер деректерді талдайды, өтініш мәртебесін жаңартады және өңдеу нәтижелерін тіркейді. Мәртебе өзгергеннен кейін жүйе жаңартылған деректері бар SOAP-хабарламаны сыртқы контурға ШЭП/ВШЭП арқылы жібереді, бұл контурлар арасындағы мәртебелердің синхрондалуын қамтамасыз етеді. Деректер алмасуды жүзеге асырудың техникалық сипаттамалары Қорғалған шлюз ШЭП/ВШЭП ● құрылымдық деректермен алмасу үшін SOAP протоколын қолданады; ● хабарламаларды криптографиялық шифрлау және аутентификациялау қамтамасыз етеді; ● WS-Security стандартына сәйкес ҚР ҰЦК берген ЭЦҚ-ны тексереді және өңдейді; ● әр хабарламаның тұтастығын бақылайды. SOAP өзара әрекеті ● C# тілінің стандартты кітапханаларын пайдалана отырып жүзеге асырылады; ● барлық кіріс және шығыс SOAP-пакеттерді журналдайды; ● контурлар арасындағы өзара әрекеттесуді аудиттеу, мониторинг және диагностика қамтамасыз етеді. Дерекқорлар ● сыртқы және ішкі дерекқорлар физикалық және логикалық түрде оқшауланған; ● ішкі дерекқорға қолжетімділік тек ІІМ ішкі желісінде рұқсат етілген; ● деректер жеке деректерді қорғау талаптарына сәйкес шифрланған түрде сақталады. ШЭП/ВШЭП деректер алмасу талаптары Жүйелер арасындағы

	өзара әрекет нормативтік талаптарға сәйкес жүзеге асады: ● қорғалған HTTPS протоколы қолданылады; ● негізгі алмасу протоколы ретінде SOAP қолданылады; ● хабарламалардың цифрлық қолтаңбасы WS-Security стандартына сәйкес орындалады; ● XML-қолтаңбалардың құрылымы W3C «XML Signature Syntax and Processing» спецификациясына сәйкес; ● (техникалық мүмкіндік болған жағдайда) интеграция ҚР Үкіметінің 2016 жылғы 20 желтоқсандағы №832 Қаулысына сәйкес ИКТ және АҚЕЕ саласындағы Біртұтас талаптардың 139-бабының 7) және 11) тармақтарына сәйкес. Міндетті оқиғаларды тіркеу: ● операциялық жүйелер оқиғалары; ● СУБД оқиғалары; ● антивирус қорғау оқиғалары; ● қолданбалы бағдарламалық қамтамасыз ету оқиғалары; ● телекоммуникациялық жабдық оқиғалары; ● шабуылдарды анықтау және алдын алу жүйелерінің оқиғалары; ● контентті басқару жүйелерінің оқиғалары. ШЭП/ВШЭП қайтару кодтарының классификаторы ● SCSS001 - сәтті өңдеу; ● SCSE002 - бизнес деректеріндегі қате; ● SCSE003 - өңделмеген ерекшелік. Дербес деректерді қорғау: Дербес деректерді өңдеу, сақтау және беру Қазақстан Республикасының «Дербес деректер және оларды қорғау туралы» Заңына сәйкес жүзеге асырылады. Төмендегілерді қамтамасыз ететін ұйымдастырушылық және техникалық шаралар іске асырылады: ● дербес деректер субъектісінің мәліметтерге қол жеткізу, оларды түзету және жою құқықтарын сақтау; ● дербес деректерді жинау, сақтау, өңдеу және беру тәртібін, сондай-ақ деректердің тізбесін, өңдеу мақсаттары мен әдістерін айқындайтын ішкі құпиялылық саясатын қолдану; ● Қазақстан Республикасы Үкіметінің 20.12.2016 ж. № 832 қаулысымен бекітілген АКТ және АҚ Бірыңғай талаптарының 48 және 90-1-тармақтарын сақтай отырып деректерді беру; ● байланыс арналарын қорғау және мәліметтердің үшінші тарап жүйелеріне рұқсатсыз берілуін болдырмау. Ақпараттық қауіпсіздікті қамтамасыз ету шаралары Жүйе ақпараттық қауіпсіздік шаралары кешенін қолдана отырып жұмыс істейді, оған келесі тізім кіреді: ● Қазақстан Республикасының «Ақпараттандыру туралы» Заңына сәйкес электрондық ақпараттық ресурстарды және ақпараттандыру объектілерін қорғау; ● қол жеткізуді бақылауды, тұтастықты мониторингтеуді және қатерлерді уақтылы жоюды қоса алғанда, ақпараттық жүйенің үздіксіз және қорғалған жұмысын қамтамасыз ету; ● қол жеткізу регламенттерін және деректерді өңдеу қағидаларын белгілеу; ● ақпараттық қауіпсіздік қатерлерін анықтау, тіркеу және жолын кесу, инциденттерге әрекет ету, олар туралы ақпаратты MISP жүйесіне беру; ● қолжетімділігі шектеулі деректерге рұқсатсыз қол жеткізуді болдырмау және оларды құқықтық негізсіз таратуды болдырмау; ● электрондық ақпараттық ресурстарды сақтау, көшіру, тарату шарттарын айқындау; ● жүйенің тұрақты және қауіпсіз жұмысын қамтамасыз ету бойынша регламенттік және профилактикалық жұмыстарды орындау; ● жүйенің үздіксіз жұмысын қамтамасыз ететін жауапты мамандардың өзекті байланыс деректерін ұсыну. Оқиғаларды журналдау талаптары Жүйе қол жеткізуге, пайдаланушылардың операцияларына және модульдердің жұмыс істеуіне байланысты

	оқиғаларды міндетті түрде тіркеуді қамтамасыз етеді, оның ішінде: ● аутентификацияның сәтті және сәтсіз әрекеттері; ● пайдаланушыларды және конфигурациялық деректерді құру, өзгерту, көшіру, жылжыту және жою; ● пайдаланушының сәтсіз операциялары; ● қорғалатын ресурстарға қол жеткізу және басқа ақпараттық жүйелерге сұрауларды бастау; ● сыртқы ақпараттық жүйелермен деректер алмасу. Әрбір оқиға бір жолда мәтіндік форматта тіркеледі және келесі мәліметтерді қамтиды: ● КК.АА.ЖЖЖЖ СС:ММ:СС форматындағы күн мен уақыт; ● оқиға көзі (модуль, қызмет, компонент); ● пайдаланушының ID-і немесе аты; ● клиенттің IP-мекенжайы; ● операцияның басталу және аяқталу уақыты; ● оқиға деңгейі (Alerts, Critical, Errors, Warning, Notifications, Informational, Debug); ● оқиға санаты (INFO, WARN, ERROR, DEBUG); ● бірегей сәйкестендіргіш (ID); ● оқиғаның сипаттамасы. Журналдау келесі талаптарды сақтай отырып жүзеге асырылады: ● журналдарды кемінде үш жыл сақтау, жедел қолжетімділікте - кемінде үш ай; ● уақытты сенімді уақыт көзімен синхрондау; ● UTF-8 кодтамасын қолдану; ● бір журнал файлы шегінде деректердің бірыңғай форматы; ● «кілт-мән» жұптарын пайдалану; ● журналдарды мәтіндік форматта, XML форматында немесе дерекқордың кестелік құрылымында сақтау мүмкіндігі; ● syslog протоколы мен форматы бойынша SIEM-жүйелерімен интеграцияны қолдау; ● журналдарға қол жеткізу тек Жүйе әкімшісіне беріледі. Жүйе барлық ерекшелік жағдайларды тіркейді және қате сипаттамасы бар журнал жазбасын қалыптастырады. Екі факторлы аутентификация (2FA) Жұмыс қағидаттары Пайдаланушылардың қол жеткізуін қорғау үшін екі факторлы аутентификация іске асырылады, оған келесі тізім кіреді: ● «білім» факторы - ЭЦҚ немесе авторизация деректерін пайдалана отырып жеке тұлғаны растау; ● «иелену» факторы - жүйеге кіруді немесе аса маңызды операцияларды растау үшін пайдаланушыға жіберілетін бір реттік код. 2FA дербес деректерді өңдеуге байланысты тіркеу, авторизация және әрекеттерді орындау кезінде қолданылады. 5. Техникалық қолдау және сүйемелдеу Бағдарламалық қамтамасыз етудің тұрақты, қауіпсіз және үздіксіз жұмысын қамтамасыз ету үшін техникалық қолдау мен пайдалану кезіндегі сүйемелдеудің толық кешені ұйымдастырылады. Қолдау жүйенің жұмыс қабілеттілігін мониторингтеуді, инциденттерге жедел әрекет етуді, пайдаланушыларға кеңес беруді, деректерді резервтік көшіруді және жаңартуларды сүйемелдеуді қамтиды. Техникалық қолдау тәулік бойы (24/7) жұмыс істейді. Бағдарламалық қамтамасыз етудің қолжетімділік деңгейі айына кемінде 99,5% болуы тиіс, алдын ала келісілген регламенттік жұмыстарды қоспағанда. Барлық профилактикалық және регламенттік іс-шаралар алдын ала жоспарланады, ІІМ уәкілетті өкілдерін хабардар етумен және техникалық оқиғалар журналында міндетті түрде тіркеумен қатар жүргізіледі. Тәулік бойы автоматтандырылған мониторинг қамтамасыз етіледі: ● веб-порталдың функционалдық модульдерінің қолжетімділігі; ● серверлік және желілік жабдықтың жай-күйі; ● дерекқорлардың жұмысы және транзакциялардың күйі; ●

	мемлекеттік ақпараттық жүйелермен интеграциялардың дұрыстығы мен тұрақтылығы; ● жүктеме деңгейі, операцияларды орындау қателері, кідірістер мен істен шығулар. Ауытқулар анықталған жағдайда ақауларды оқшаулау және жою бойынша іс-шаралар басталады. Инциденттер сындылық деңгейі бойынша жіктеледі. Әр деңгей үшін әрекет ету мерзімдері белгіленеді: Сындарлы деңгей (порталдың қолжетімсіздігі немесе өтінімдерді беру/өңдеудің мүмкін еместігі): - әрекет етуді бастау: 15 минутқа дейін; - жұмыс қабілеттілігін қалпына келтіру: мүмкіндігінше қысқа мерзімде, әдетте бірнеше сағат ішінде. Жоғары деңгей (жекелеген негізгі модульдердің қолжетімсіздігі: медициналық комиссия, ФИЗО, полиграф, әңгімелесу, авторизация, ЭЦҚ): - әрекет етуді бастау: 30 минутқа дейін. Орта деңгей (жүйенің жалпы жұмыс қабілеттілігіне әсер етпейтін функционалдық қателер): - әрекет етуді бастау: 2 сағатқа дейін. Төмен деңгей (интерфейстік сәйкессіздіктер, ұсақ ескертулер): - түзету жоспарлы режимде жүзеге асырылады. Қажет болған жағдайда ақау толық жойылғанға дейін сындарлы операцияларды орындауды қамтамасыз ететін уақытша шешімдерді қолдануға жол беріледі. Пайдаланушыларға (кандидаттар мен ІІМ қызметкерлеріне) келесі арналар арқылы консультациялық қолдау көрсетіледі: ● телефон; ● электрондық пошта; ● мессенджерлер; ● жеке кабинеттегі кіріктірілген өтініш формасы. Барлық өтініштер тіркеледі, есепке алынады, жіктеледі және техникалық қолдау регламентіне сәйкес өңделеді. Барлық инциденттер, пайдаланушылардың сұраулары және орындалған техникалық операциялар міндетті түрде тіркелуге жатады. Мерзімді түрде келесі мәліметтерді қамтитын есептер қалыптастырылады: ● өтініштердің жалпы саны; ● әрекет ету уақыты және жою уақыты; ● инциденттердің түрлері мен себептері; ● қолжетімділіктің бұзылуы туралы мәліметтер ● қабылданған түзету шараларының тізбесі. Есептер белгіленген мерзімдерде ІІМ уәкілетті өкілдеріне ұсынылады. ● Жаңартулар міндетті тестілеуден кейін ғана жүзеге асырылады. Әрбір жаңарту төмендегісін қамтиды: ● өзгертілген компоненттерді құжаттау; ● іске асырылған жетілдірулер мен түзетулердің сипаттамасы; ● орнатудан кейін жұмыстың дұрыстығын тексеру; ● ІІМ уәкілетті өкілдерін хабардар ету.Жаңартулар өтінімдерді беру және өңдеу процестерін бұзу қаупінсіз және елеулі тоқтап қалусыз орнатылады. Резервтік көшіру және қалпына келтіру Төмендегі тізім қамтамасыз етіледі: ● деректер мен жүйелік конфигурацияларды тұрақты резервтік көшіру; ● резервтік көшірмелерді ақпараттық қауіпсіздік талаптарына сәйкес сақтау; ● істен шығулар кезінде жүйені жедел қалпына келтіру мүмкіндігі; ● деректердің жоғалуын және жұмыстың ұзақ уақытқа тоқтап қалуын болдырма 6. Өнім беруші Шарт күшіне енгеннен кейін күнтізбелік 5 күн ішінде: 1) Тапсырыс берушіге бекітілген жұмыс тобы мамандарының рөлдерін, телефон нөмірлерін, ТАӘ, қызметкерлерді көрсете отырып, өнім берушінің жұмыс тобының құрамы туралы хат, сондай-ақ нотариус куәландырған тиісті сертификаттарды ұсыну; 2) Тапсырыс берушіге қызметтердің барлық кешенін

	орындаудың күнтізбелік жоспарын-кестесін әзірлеуге, келісуге және бекітуге ұсынуға міндетті; 3) Жұмыс тобының әрбір қызметкеріне құпия ақпаратты қағаз жеткізгіште жарияламау туралы келісімді ұсынуға міндетті; 4) Өнім беруші көрсетілетін қызметтердің әрбір түрінің құнының егжей-тегжейлі сипаттамасы мен негіздемесін, оларды көрсету шарттарын, кезеңділігін қамтитын көрсетілетін қызметтерді ұсыну жөніндегі шығындардың егжей-тегжейлі толық жазылуын ұсынады. Бұл ретте шығындарды таратып жазудың жалпы сомасы жасалған шарттың сомасына тең болуға тиіс; 7. Электрондық актілерге қол қою тәртібі: 1) Өнім беруші көрсетілген қызметтердің актісін веб-портал арқылы ресімдейді, бұл ретте өнім беруші мен Тапсырыс берушінің салалық қызметі қол қойған шығындар мен қызметтердің толық жазылуы бар қосымшаның электрондық көшірмесін ұсынады; 2) Актіге қосымшаны ресімдеу алдында Тапсырыс беруші мен өнім беруші көрсетілген қызметтерді есепті кезеңдегі өтінімдерге сәйкес салыстырып тексеруді жүргізеді; 3) Актілер веб-портал арқылы тоқсан сайын есепті кезеңнен кейінгі айдың 15-күнінен кешіктірілмей берілуі қажет.
Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Министерство внутренних дел Республики Казахстан"
Наименование организатора	Государственное учреждение "Министерство внутренних дел Республики Казахстан"
№ конкурса:	№ 17868418-1
Наименование конкурса:	Конкурс на услуги доступа к информационным ресурсам на 2027 год
Номер лота:	№ 88114334-ОК1
Наименование лота:	Услуги по пользованию программными продуктами
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	620920.000.000014
Наименование услуги:	Услуги по пользованию программными продуктами
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	841379.31
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	841379.31
Срок оказания услуги:	по 31 декабря 2027 года
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ ПО ПРЕДОСТАВЛЕНИЮ УСЛУГ ДОСТУПА И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ «QYZMET-POLICE.KZ». Услуги должны быть оказаны в срок по 31 декабря 2027 года включительно. Услуга предусматривает предоставление доступа к Программному обеспечению, предназначенному для автоматизации процессов приёма граждан на службу в органы внутренних дел. Система обеспечивает подачу заявлений в онлайн-формате, автоматическую обработку данных, формирование перечня необходимых документов, прохождение установленных этапов отбора и взаимодействие с внешними государственными информационными системами. Предоставляемый доступ позволяет использовать единую цифровую платформу для приёма на службу, повышает прозрачность процедур, сокращает сроки рассмотрения заявлений и облегчает работу кадровых подразделений. Граждане получают возможность пройти все этапы трудоустройства дистанционно, без личного посещения кадровых служб. Целью предоставления доступа является совершенствование процедур оформления граждан Республики Казахстан на службу в органы внутренних дел путем создания единой цифровой системы приема. Программное обеспечение обеспечивает автоматизацию следующих процессов: • подача электронных заявлений на поступление на службу в ОВД; • сбор, проверка и обработка документов; • прохождение обязательных этапов трудоустройства и получение результатов; • формирование и ведение электронного личного дела; • минимизация влияния человеческого фактора на процесс оформления; • повышение прозрачности и снижение коррупционных рисков; • сокращение сроков рассмотрения заявлений и оптимизация кадровых процедур 1. Автоматизируемые процессы: Программное обеспечение обеспечивает автоматизацию следующих функций: • предоставление информации о службе в ОВД; • просмотр доступных вакансий и условий приема; • расчет предполагаемого денежного содержания кандидата; • подача электронного заявления на поступление на службу; • прием, первичная обработка и регистрация заявки; • контроль состояния и сроков исполнения заявки; • формирование электронного личного дела; • уведомление кандидата о прохождении этапов и необходимости предоставления документов; • получение результатов обязательных процедур (медкомиссия, ФИЗО, полиграф, тестирование, собеседование); • проверка кандидата на соответствие квалификационным требованиям; • формирование и хранение электронного архива заявок и результатов их рассмотрения. Распределение прав доступа: Доступ пользователей к функционалу Программного обеспечения определяется закреплёнными ролями. Всего используется 8 пользовательских ролей. Администратор системы: Имеет возможность: регистрировать пользователей; назначать, изменять и удалять роли; управлять учетными записями; администрировать ПО; выполнять обновления и технического обслуживания; резервное копирования; управлять организационной структурой; ведения справочников; контролировать соблюдения требований безопасности. Руководитель кадровой службы: Обеспечивает просмотр всех заявок; контроль этапов

	обработки; просмотр сроков исполнения; анализ отказов; распределение заявок между исполнителями; доступ к архиву личных дел и аналитике. Исполнитель (кадровый сотрудник): Осуществляет создание и редактирование вакансий; проверку поступивших заявок; формирование личного дела; направление заявителя на доработку; получение результатов этапов отбора (медкомиссия, ФИЗО, полиграф, тестирование, собеседование); работу с архивом. Сотрудник ЦВВК: Просматривает поступившие заявки; проверяет корректность документов; принимает либо отклоняет заявку; формирует и загружает медицинское заключение; работает с архивом. Инспектор по физической подготовке (ФИЗО): Просматривает заявки и личные дела; назначает дату и время сдачи нормативов; вносит результаты; прикрепляет подтверждающие документы; работает с архивом. Полиграфолог Имеет доступ к заявкам и календарю записей; назначает время исследования; просматривает личное дело; вносит результаты и загружает заключение; работает с архивом. Конкурсная комиссия Просматривает личные дела; назначает время собеседования; проводит онлайн-собеседование; фиксирует итоговое решение; прикрепляет документы и комментарии; определяет дальнейший маршрут кандидата. Кандидат: Получает доступ к просмотру вакансий и условий; выбирает организацию и должность; заполняет и подает заявление; отслеживает статус; выбирает дату и время прохождения этапов; проходит тестирование; получает уведомления; загружает документы; подписывает заявления ЭЦП; получает направление на сдачу ФИЗО. Описание процессов: Программное обеспечение обеспечивает автоматизированную обработку полного цикла поступления граждан на службу в органы внутренних дел, включая регистрацию кандидата, формирование электронного заявления, прохождение этапов отбора и принятие итогового решения. Система функционирует как единый цифровой сервис, поддерживающий последовательную маршрутизацию заявок между ответственными участниками процесса. Программное обеспечение обеспечивает: • создание и ведение личных кабинетов кандидатов и сотрудников кадровых подразделений; • формирование, регистрацию и хранение электронных заявлений на поступление; • автоматическую маршрутизацию заявок между этапами обработки в соответствии с утверждённым бизнес-процессом; • интеграционный обмен данными с внешними государственными информационными системами для получения сведений, необходимых для проверки кандидата; • автоматизированное формирование электронного личного дела на основании введённых данных и полученных результатов проверок; • передачу заявок на прохождение обязательных процедур (медицинское обследование, полиграфологическое исследование, физическая подготовка, тестирование, собеседование); • получение и фиксацию результатов прохождения указанных процедур в электронном виде; • обеспечение календарей доступности для назначаемых процедур и возможность выбора времени, предоставляемую кандидату; • электронное взаимодействие с кадровыми сотрудниками, военно-врачебной комиссией, полиграфологами,

	инспекторами ФИЗО и конкурсной комиссией; • автоматическое изменение статусов заявок в соответствии с результатами процедур и решений уполномоченных лиц; • формирование итоговых решений о допуске или недопуске к дальнейшим этапам, а также формирование направления в образовательные учреждения МВД (академии первоначальной подготовки); • ведение электронного архива заявок и протоколов их рассмотрения. Работа Программного обеспечения организована на основе регламентированных маршрутов обработки данных. Логика переходов между этапами, критерии автоматических проверок, условия допуска, отказа или возврата на доработку встроены в функциональную модель системы и обеспечиваются её серверной частью без участия пользователя. Система поддерживает: • автоматическое принятие решений в случаях, когда условия допуска или отказа определяются нормативными требованиями; • приём результатов процедур от внешних систем (например, медицинское заключение из ИС «Damumed» или данные прокторинга); • хранение всех промежуточных данных, файловых материалов и результатов проверок в структурированном виде; • формирование журналов событий, логов изменений статусов, протоколов решений комиссий и других данных, предусмотренных правилами ведения кадрового делопроизводства. Программное обеспечение функционирует как централизованный сервис, обеспечивающий единый технологический контур обработки заявок, их проверку, прохождение всех обязательных этапов отбора и передачу итогового результата в кадровые системы МВД. 2. Функциональные требования Описание процессов Программное обеспечение предоставляет пользователям доступ к функционалу в соответствии с назначенными ролями и обеспечивает выполнение операций, предусмотренных бизнес-процессом приёма граждан на службу в органы внутренних дел. Доступ без регистрации Незарегистрированные пользователи имеют доступ к следующим разделам: • общая информация о службе в ОВД; • перечень вакансий с фильтрами по региону, департаменту и району; • калькулятор предполагаемого денежного содержания. Эти функции работают в режиме просмотра. Основная информационная страница Главная страница отображает: • общие сведения о службе в ОВД; • нормативную информацию и требования; • контактные данные Call-центра для получения консультаций. Раздел «Вакансии» Функционал раздела обеспечивает: • отображение полного списка вакансий; • фильтрацию по региону, департаменту и району; • автоматическую выдачу вакансий, соответствующих выбранным параметрам; • отображение карточки вакансии с полным описанием (должность, подразделение, требования, обязанности, тип должности и др.); • переход к подаче заявки (для авторизованных пользователей). Раздел «Калькулятор» Калькулятор: • рассчитывает предполагаемый доход кандидата; • использует параметры вакансии (категория, квалификация, допуск к гостайне и др.); • формирует результат на основе введённых данных (звание, стаж и пр.). Регистрация и авторизация Программное обеспечение: • предоставляет форму регистрации кандидата; •

	запрашивает подтверждение номера телефона; • формирует личный кабинет после регистрации; • обеспечивает авторизацию через ЭЦП или логин/пароль. Формирование и подача заявки Функционал подачи заявки включает: • создание электронной заявки с присвоением уникального номера; • автоматическое заполнение ФИО и ИИН на основе ЭЦП; • заполнение анкеты, включая образование, контакты и данные о родственниках; • загрузку скан-документов; • сохранение черновика или отправку заявки; • подписание ЭЦП при отправке. Каждая вакансия создаёт отдельную заявку. Отслеживание статуса заявки Раздел «Мои заявки»: • отображает список всех заявок кандидата; • показывает текущий статус и этап обработки; • обновляет статус автоматически при переходе на следующий этап; • формирует уведомления и комментарии. Обработка заявок кадровыми сотрудниками Кадровый сотрудник: • просматривает поступившие заявки; • проверяет корректность данных и приложенных документов; • принимает решение о принятии заявки, отказе или направлении на доработку; • формирует электронное личное дело кандидата; • использует данные, полученные через интеграции с государственными ИС; • фиксирует решения в системе. Формирование отчётности Система: • формирует отчёты по установленным параметрам; • отображает статистику в разрезе периодов, регионов и этапов обработки; • предоставляет данные о зарегистрированных пользователях, отказах, доработках, архиве и текущей нагрузке. • Функционал ведомственных ролей Военно-врачебная комиссия (ВВК): • просматривает заявки на медосвидетельствование; • проверяет документы; • прикрепляет заключение; • принимает или отклоняет заявки; • отправляет обработанные результаты кадровому исполнителю. Исполнитель кадровой службы: • работает с заявками на всех этапах; • инициирует запросы в государственные базы; • получает результаты проверок; • формирует и актуализирует личное дело. Перечень данных, поступающих через интеграции (при технической возможности) Система получает и отображает: • персональные данные кандидата; • данные УДЛ; • сведения о родственниках; • данные о предпринимательской деятельности; • налоговые сведения и декларации; • данные о доходах и удержанных налогах; • кредитную историю; • согласие на обработку персональных данных; • статус в базе мобильных граждан; • сведения об инвалидности; • данные об образовании, трудовой деятельности, пенсионных отчислениях; • сведения о судимости, правонарушениях, ограничениях; • медицинские сведения из диспансеров. Информация поступает асинхронно и отображается после обработки. Публикация вакансий Раздел предоставляет: • создание, редактирование, удаление вакансий; • автоматическое отображение опубликованных вакансий кандидату. Формирование отчётов Система предоставляет руководителю инструменты: • формирования отчётов по заявкам; • сохранения и печати отчётных материалов. Функционал руководителя Руководитель: • просматривает все поступившие заявки; • контролирует процесс их обработки; • распределяет заявки между исполнителями; •

	управляет загрузкой сотрудников. 3. Нефункциональные требования и архитектура системы Нефункциональные требования Интерфейс пользователя Пользовательский интерфейс системы поддерживает мультиязычность (казахский и русский языки) с возможностью последующего расширения языковой поддержки. Интерфейс корректно отображается при разрешении экрана от 1024×600 пикселей и выше. Система функционирует в актуальных стабильных версиях следующих браузеров: • Google Chrome • Mozilla Firefox • Safari • Microsoft Edge Под «актуальной стабильной версией» понимается версия браузера, опубликованная разработчиком как стабильный релиз на момент эксплуатации. Эксплуатационные характеристики Программное обеспечение функционирует на технологическом стеке: • Backend: C#, ASP.NET MVC 3.0 • Язык программирования: C# • СУБД: PostgreSQL Резервное копирование базы данных выполняется поставщиком на ежемесячной основе. Обмен данными между клиентским и серверным уровнем обеспечивается через протокол SOAP, который используется для выполнения запросов на получение, изменение и обработку данных. 4. Архитектура системы Общая структура Архитектура системы разделена на два контекста: 1. Внешний контур — сервисы, доступные кандидатам через веб-портал. 2. Внутренний контур МВД — сервисы обработки заявок и взаимодействия сотрудников МВД. Сегментация контуров обеспечивает безопасную работу с персональными данными и ограничение доступа к внутренним ресурсам. Модули системы Модуль подачи заявок (Внешний контур) Модуль предоставляет общедоступный функционал: • доступ к информации о службе и вакансиям; • заполнение и подписание электронной заявки через ЭЦП; • передачу заявки в серверную часть для дальнейшей обработки; • формирование пользовательских данных и сохранение их в базе данных. К внешнему модулю можно подключаться с персональных компьютеров через интернет. Модуль обработки заявок (Внутренний контур МВД) Внутренний модуль обеспечивает полный цикл обработки заявок сотрудниками МВД. Функциональные свойства: • автоматическое получение данных по ИИН из государственных ИС через SmartBridge; • запись полученной информации в защищённую базу данных МВД; • доступ сотрудников МВД к деталям заявок, документам, результатам проверок; • взаимодействие с кандидатами через внутренние интерфейсы; • ведение истории, журналов операций и архивов заявок. Доступ обеспечивается только из внутренней защищённой сети МВД, без выхода в интернет. Сетевые требования Внешняя сеть Функции внешней сети включают: • доступ пользователей к веб-порталу через интернет; • работу серверов веб-приложения и API для обработки входящих запросов; • обеспечение защищённого соединения по протоколу HTTPS. Внутренняя сеть Внутренняя сеть МВД обеспечивает: • доступ сотрудников только через защищённые внутренние каналы; • хранение баз данных и персональных сведений на изолированных серверах; • интеграцию (при технической возможности) с государственными системами (ЕТС, SmartBridge и др.) через защищённые каналы. Описание

	архитектурной модели Архитектура системы: • разделяет веб-портал (внешний контур) и сервер обработки заявок (внутренний контур МВД); • использует интеграционные механизмы (при технической возможности) SmartBridge и ЕТС для проверки данных; • обеспечивает логическую изоляцию пользовательских сервисов и сервисов обработки персональной информации; • поддерживает безопасное взаимодействие между подсистемами и защиту личных данных кандидатов. Такая архитектура обеспечивает устойчивость системы, защищённость информации и оптимизацию процессов подачи и обработки заявок. Сценарий взаимодействия между внешней и внутренней сетями Общая схема взаимодействия Система обеспечивает безопасный обмен данными между внешним контуром (веб-портал для подачи заявок) и внутренним контуром МВД (интерфейс обработки заявок). Взаимодействие осуществляется через защищённый шлюз электронного правительства (ШЭП/ВШЭП) по протоколу SOAP с использованием криптографической защиты, что гарантирует целостность, подлинность и конфиденциальность передаваемых данных. Логическая последовательность взаимодействия между контурами Этап 1. Внешний контур: формирование и передача заявки Внешний портал формирует электронную заявку, сохраняет её в своей базе данных и подготавливает SOAP-пакет, содержащий уникальный идентификатор заявки, ИИН и другие структурированные атрибуты. Подготовленное сообщение отправляется во внутренний контур МВД через ШЭП/ВШЭП по защищённому каналу HTTPS. Этап 2. Внутренний контур: приём и обработка заявки Внутренний контур принимает SOAP-сообщение, выполняет валидацию подписи и соответствие параметрам безопасности. После успешной проверки данные заявки сохраняются в защищённой внутренней базе данных МВД. Система инициирует автоматические запросы в государственные информационные системы через SmartBridge, включая получение сведений о личности, правовом статусе, истории правонарушений, социальном и медицинском статусе кандидата. Результаты проверок фиксируются во внутреннем контуре. Этап 3. Работа сотрудников МВД Авторизованные сотрудники МВД получают доступ к данным заявок через внутренний веб-интерфейс, функционирующий в закрытой сети. Сотрудники анализируют данные, обновляют статус заявки и фиксируют результаты обработки. После изменения статуса система формирует SOAP-сообщение с обновлёнными данными и передаёт его во внешний контур через ШЭП/ВШЭП, обеспечивая синхронизацию статусов между контурами. Технические характеристики реализации обмена Защищённый шлюз ШЭП/ВШЭП • использует протокол SOAP для обмена структурированными данными; • обеспечивает криптографическое шифрование и аутентификацию сообщений; • проверяет и обрабатывает ЭЦП, выданную НУЦ РК, в соответствии со стандартом WS-Security; • обеспечивает контроль целостности каждого сообщения. SOAP-взаимодействие • реализовано с использованием стандартных библиотек языка C#; • включает логирование всех входящих и исходящих SOAP-пакетов; • обеспечивает аудит, мониторинг и диагностику взаимодействия между

	контурами. Базы данных • внешняя и внутренняя БД физически и логически изолированы; • доступ к внутренней БД разрешён только во внутренней сети МВД; • данные хранятся в зашифрованном виде в соответствии с требованиями по защите персональных данных. Требования ШЭП/ВШЭП к обмену данными Взаимодействие между системами осуществляется согласно установленным нормативным требованиям: • используется защищённый протокол HTTPS; • применяется SOAP как основной протокол обмена; • цифровая подпись сообщений выполняется по стандарту WS-Security; • структура XML-подписей соответствует спецификации W3C «XML Signature Syntax and Processing»; • интеграция (при технической возможности) соответствует положениям подпунктов 7) и 11) пункта 139 Единых требований в области ИКТ и ИБ (Постановление Правительства РК № 832 от 20.12.2016 г.). Обязательная регистрация событий включает: • события операционных систем; • события СУБД; • события антивирусной защиты; • события прикладного программного обеспечения; • события телекоммуникационного оборудования; • события систем обнаружения и предотвращения атак; • события систем управления контентом. Классификатор кодов возврата ШЭП/ВШЭП • SCSS001 — успешная обработка; • SCSE002 — ошибка в бизнес-данных; • SCSE003 — необработанное исключение. Защита персональных данных: Обработка, хранение и передача персональных данных осуществляются в соответствии с Законом Республики Казахстан «О персональных данных и их защите». Реализуются организационные и технические меры, обеспечивающие: • соблюдение прав субъекта персональных данных на доступ, корректировку и удаление сведений; • применение внутренней политики конфиденциальности, устанавливающей порядок сбора, хранения, обработки и передачи персональных данных, а также перечень данных, цели и методы их обработки; • передачу данных с соблюдением пунктов 48 и 90-1 Единых требований ИКТ и ИБ, утверждённых Постановлением Правительства РК № 832 от 20.12.2016 г.; • защиту каналов связи и исключение несанкционированной передачи сведений в сторонние системы. Меры по обеспечению информационной безопасности: Система функционирует с применением комплекса мер информационной безопасности, включающих: • защиту электронных информационных ресурсов и объектов информатизации в соответствии с Законом Республики Казахстан «Об информатизации»; • обеспечение непрерывной и защищённой работы информационной системы, включая контроль доступов, мониторинг целостности и своевременное устранение угроз; • установление регламентов доступа и правил обработки данных; • выявление, фиксацию и пресечение угроз ИБ, реагирование на инциденты, передачу информации о них в систему MISP; • предотвращение несанкционированного доступа к данным ограниченного доступа и исключение их распространения без правового основания; • определение условий хранения, копирования, распространения электронных информационных ресурсов; • выполнение регламентных и профилактических работ по обеспечению устойчивой и безопасной работы системы; •

	предоставление актуальных контактных данных ответственных специалистов, обеспечивающих бесперебойность функционирования системы. Требования к журналированию событий Система обеспечивает обязательную фиксацию событий, связанных с доступом, операциями пользователей и функционированием модулей, включая: • успешные и неуспешные попытки аутентификации; • создание, изменение, копирование, перемещение и удаление пользователей и конфигурационных данных; • неуспешные операции пользователя; • предоставление доступа к защищаемым ресурсам и инициирование запросов к другим информационным системам; • обмен данными с внешними ИС. Каждое событие фиксируется в текстовом формате в одной строке и содержит: • дату и время в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС; • источник события (модуль, служба, компонент); • ID или имя пользователя; • IP-адрес клиента; • время начала и окончания операции; • уровень события (Alerts, Critical, Errors, Warning, Notifications, Informational, Debug); • категорию события (INFO, WARN, ERROR, DEBUG); • уникальный идентификатор (ID); • описание события. Журналирование осуществляется с соблюдением следующих требований: • хранение журналов не менее трёх лет, в оперативном доступе — не менее трёх месяцев; • синхронизация времени с доверенным источником времени; • кодировка UTF-8; • единый формат данных в пределах одного файла журнала; • использование пар «ключ—значение»; • возможность хранения журналов в текстовом формате, XML или в табличной структуре БД; • поддержка интеграции с SIEM-системами по протоколу и формату syslog; • доступ к журналам имеет только Администратор системы. Система фиксирует все исключительные ситуации и формирует запись в журнале с описанием ошибки. Двухфакторная аутентификация (2FA) Принципы работы Для защиты доступа пользователей реализуется двухфакторная аутентификация, включающая: • фактор «знания» — подтверждение личности с использованием ЭЦП либо авторизационных данных; • фактор «владения» — одноразовый код, направляемый пользователю для подтверждения входа или критически важных операций. 2FA применяется при регистрации, авторизации и выполнении действий, связанных с обработкой персональных данных. 5. Техническая поддержка и сопровождение Для обеспечения устойчивой, безопасной и бесперебойной работы Программного обеспечения организуется полный комплекс технической поддержки и эксплуатационного сопровождения. Поддержка охватывает мониторинг работоспособности, оперативное реагирование на инциденты, консультирование пользователей, резервирование данных и сопровождение обновлений. Техническая поддержка функционирует круглосуточно (24/7). Доступность Программного обеспечения должна составлять не менее 99,5 % в месяц, за исключением заранее согласованных регламентных работ. Все профилактические и регламентные мероприятия планируются заранее, сопровождаются уведомлением уполномоченных представителей МВД и обязательной фиксацией в журнале технических событий. Обеспечивается круглосуточный автоматизированный мониторинг: •

	доступности функциональных модулей веб-портала; • состояния серверного и сетевого оборудования; • работы баз данных и состояния транзакций; • корректности и стабильности интеграций с государственными ИС; • уровня нагрузки, ошибок выполнения операций, задержек и отказов. При выявлении отклонений инициируются мероприятия по локализации и устранению неисправности. Инциденты классифицируются по уровню критичности. Для каждого уровня устанавливаются предельные сроки реагирования: Критический уровень (недоступность портала или невозможность подачи/обработки заявок):— начало реагирования: до 15 минут;— восстановление работоспособности: в максимально короткие сроки, как правило в пределах нескольких часов. Высокий уровень (недоступность отдельных ключевых модулей: медкомиссия, ФИЗО, полиграф, собеседование, авторизация, ЭЦП):— начало реагирования: до 30 минут. Средний уровень (функциональные ошибки, не влияющие на работоспособность системы в целом):— начало реагирования: до 2 часов. Низкий уровень (интерфейсные несоответствия, мелкие замечания): — исправление выполняется в плановом режиме. При необходимости допускается временное решение, обеспечивающее выполнение критических операций до полного устранения неисправности. Пользователям (кандидатам и сотрудникам МВД) предоставляется консультационная поддержка через следующие каналы: • телефон; • электронная почта; • мессенджеры; • встроенная форма обращений в личном кабинете. Все обращения фиксируются, регистрируются, классифицируются и обрабатываются в соответствии с регламентом технической поддержки. Все инциденты, запросы пользователей и выполненные технические операции подлежат обязательной регистрации. Периодически формируются отчёты, включающие: • общее количество обращений; • время реакции и время устранения; • типы и причины инцидентов; • сведения о нарушениях доступности; • перечень принятых корректирующих мер. Отчёты предоставляются уполномоченным представителям МВД в установленные сроки. Обновления осуществляется только после обязательного тестирования. Каждое обновление включает: • документирование изменённых компонентов; • описание реализованных улучшений и исправлений; • проверку корректности работы после установки; • уведомление уполномоченных представителей МВД. Обновления устанавливаются без существенных простоев и без риска нарушения процессов подачи и обработки заявок. Резервное копирование и восстановление Обеспечивается: • регулярное резервное копирование данных и системных конфигураций; • хранение резервных копий в соответствии с требованиями информационной безопасности; • возможность оперативного восстановления системы при сбоях; • предотвращение потери данных и длительных остановок работы. 6. Поставщик в течение 10 календарных дней после вступления Договора в силу должен предоставить: • 1) Письмо о составе Рабочей группы Поставщика, с указанием ролей специалистов Рабочей группы, номеров телефонов, ФИО; • 2) Разработать, согласовать и предоставить Заказчику на утверждение

	календарный план-график исполнения всего комплекса услуг; • 3) Соглашения о неразглашении конфиденциальной информации на каждого работника рабочей группы на бумажном носителе; • 4) Поставщик предоставляет детальную расшифровку затрат по предоставлению услуг, включающую детальное описание и обоснование стоимости каждого вида услуг, условия, периодичность их оказания. При этом общая сумма расшифровки затрат равняется сумме заключенного договора; 7. Порядок подписания электронных актов: • 1) Поставщик оформляет акт оказанных услуг посредством веб-портала, при этом предоставляет электронную копию приложения с расшифровкой затрат и услуг подписанную поставщиком и отраслевой службой заказчика; • 2) Перед оформлением приложения к акту Заказчик и Поставщик проводят сверку оказанных услуг в соответствии с заявками за отчетный период; • 3) Акты посредством веб-портала предоставляется ежеквартально не позднее 15 числа месяца следующего за отчетным периодом.
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	