

**Сатып алынатын қызметтердің Техникалық ерекшелігі
(тапсырыс беруші толтырады)**

Тапсырыс берушінің атауы:	"Халықаралық бағдарламалар орталығы" акционерлік қоғамы
Ұйымдастырушының атауы:	"Халықаралық бағдарламалар орталығы" акционерлік қоғамы
Конкурстың №:	№ 17792455-1
Конкурстың атауы:	«е-Болашақ» БАЖ ақпараттық қауіпсіздігінің аттестаттаудан өтуіне дайындық жөніндегі қызметтер
Лоттың нөмірі:	№ 88023749-OK1
Лоттың атауы	Диагностикалау/сараптау/талдау/сынау/тестілеу/тексеріп қарау бойынша қызметтер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	712019.000.000009
Қызметтің атауы:	Диагностикалау/сараптау/талдау/сынау/тестілеу/тексеріп қарау бойынша қызметтер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	15000000
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	15000000
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	шарт жасалған күннен бастап 15 күнтізбелік күн өткеннен кейін және 2026 жылғы 31 желтоқсанға дейін

Аванстық төлем мөлшері:	0
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Параметр Мәні Тапсырыс беруші «Халықаралық бағдарламалар орталығы» акционерлік қоғамы, БСН 050440007456, Қазақстан, Астана қ., Есіл ауданы, Сығанақ к-сі, 70-ғимарат. Қызметтің атауы (ТЖҚ БНА бойынша) Диагностикалау/сараптама/талдау/сынақтар/тестілеу/тексеріп-қарау жөніндегі қызметтер Қызметтің сипаттамасы (ТЖҚ БНА бойынша) Ақпараттандыру объектілерін ақпараттық қауіпсіздік талаптарына сәйкес келтіру ТЖҚ БНА коды 712019.000.000009 Қосымша сипаттама «е-Болашақ» КФАЖ цифрлық объектісін (бұдан әрі — Жүйе) «Киберқауіпсіздік туралы» Қазақстан Республикасы Заңының 49-бабына сәйкес аккредиттелген сынақ зертханасы жүргізетін киберқауіпсіздік талаптарына сәйкестікке сынақтарға дайындау Өлшем бірлігі / саны Бір қызмет / 1 Сатып алу тәсілі Ашық конкурс (goszakur.gov.kz мемлекеттік сатып алу веб-порталы) Қызмет көрсету орны Қазақстан, Астана қ., Есіл ауданы, Сығанақ к-сі, 70-ғимарат. Қызметтердің жекелеген түрлері (қашықтан талдау, сканерлеу, консультациялар) Тапсырыс берушімен келісу бойынша қашықтан көрсетілуі мүмкін Қызмет көрсету мерзімі Шарт жасалған күннен бастап 2026 жылғы 20 желтоқсанға дейін Төлем шарттары көрсетілген қызметтер актісі негізінде қызметтер іс жүзінде көрсетілгені бойынша Осы құжатта «е-Болашақ» КФАЖ цифрлық объектісін (бұдан әрі — Жүйе, сынақ объектісі) киберқауіпсіздік талаптарына сәйкестікке сынақтарға дайындау жөніндегі қызметтердің мазмұнын, көлемін, көрсету шарттарын және нәтижелеріне қойылатын талаптарды айқындайтын техникалық ерекшелік ұсынылған. Сатып алу нысанасы Жүйені зерттеп-қарау, киберқауіпсіздік талаптарына сәйкессіздіктерді анықтау, ұсынымдар дайындау, сәйкессіздіктерді жоюды сүйемелдеу, орындалған түзетулерді тексеру және ресми сынақтар үшін құжаттар жиынтығын дайындау болып табылады. Ресми сынақтарды Тапсырыс беруші бөлек ұйымдастырады және оларға ақы төлейді. Ресми сынақтарды жүргізетін ұйым Қазақстан Республикасының заңнамасына және қолданылатын Сынақ қағидаларына сәйкес айқындалады. 1.1. Терминдер Термин Анықтама Тапсырыс беруші «Халықаралық бағдарламалар орталығы» акционерлік қоғамы - Жүйенің меншік иесі (иеленушісі) Әлеуетті өнім беруші Мемлекеттік сатып алу туралы шарт жасасуға үміткер кәсіпкерлік қызметті жүзеге асыратын жеке тұлға, заңды тұлға (егер Қазақстан Республикасының заңдарында өзгеше белгіленбесе, мемлекеттік мекемені қоспағанда), заңды тұлғалардың уақытша бірлестігі (консорциум) Жүйе (сынақ объектісі) «е-Болашақ» КФАЖ цифрлық объектісі, оның жұмыс істеуін қамтамасыз ететін қолданбалы БҚ, дерекқорларды, виртуалдандыру ортасын, серверлік және желілік жабдықты қоса алғанда Киберқауіпсіздік (КҚ) Цифрлық объектілердің құпиялылығының, тұтастығының немесе қолжетімділігінің бұзылуынан қорғалу жай-күйі. 2026 жылға дейін қабылданған НҚА мен стандарттарда «ақпараттық қауіпсіздік» (АҚ) термині қолданылады; осы техникалық ерекшеліктің мақсаттары үшін терминдер баламалы Сынақтар Цифрлық объектіні «Киберқауіпсіздік туралы» ҚР Заңының 49-бабына және Сынақ әдістемесі мен қағидаларына сәйкес КҚ талаптарына
--	--

	сәйкестікке сынау Зертхана Сынақтарды жүргізетін аккредиттелген сынақ зертханасы (мемлекеттік техникалық қызмет) Бірыңғай талаптар ҚР Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысымен бекітілген Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар Сынақ әдістемесі мен қағидалары 2019 жылғы 3 маусымдағы № 111/НҚ бұйрықпен бекітілген «Цифрлық үкіметтің» цифрлық объектілері мен аса маңызды цифрлық объектілерін киберқауіпсіздік талаптарына сәйкестікке сынақтар жүргізу әдістемесі мен қағидалары Мониторинг қағидалары 2018 жылғы 28 наурыздағы № 52/НҚ бұйрықпен бекітілген «Цифрлық үкіметтің» цифрлық объектілері мен аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидалары Сәйкессіздік Жүйенің, оның конфигурациясының, құжаттамасының немесе процестерінің жай-күйінің 3-бөлімде көрсетілген НҚА мен стандарттардың талаптарынан ауытқуы Осалдық КҚ-ны бұзу үшін пайдаланылуы мүмкін БҚ-ның, конфигурацияның немесе архитектураның кемшілігі Соңғы нүкте Тапсырыс берушінің EDR жүйесінің агенті орнатылатын жұмыс станциясы немесе сервері Статикалық талдау құралы Әлеуетті өнім беруші Жүйенің бастапқы кодын талдау үшін қолданатын SAST класындағы бағдарламалық құрал (6.14-тармақ) 1.2. Қысқартулар Қысқарту Толық жазылуы БСН Бизнес-сәйкестендіру нөмірі ТЖҚ БНА Тауарлардың, жұмыстардың және көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы АҚ Ақпараттық қауіпсіздік (2026 жылға дейін қабылданған НҚА мен стандарттардың термині; «Киберқауіпсіздік» қараңыз) КҚ Киберқауіпсіздік ЖАЭ Желіаралық экран ДМ Бағдарламалық қамтамасыз етудің декларацияланбаған мүмкіндіктері НҚА Нормативтік құқықтық акт ОЖ Операциялық жүйе СБД ҚР СТ ISO/IEC 15408-3-2017 бойынша сенімнің бағалау деңгейі АҚЖО Ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталығы (киберқауіпсіздіктің жедел орталығы) БҚ Бағдарламалық қамтамасыз ету ҚР Қазақстан Республикасы АҚҚҚ Ақпаратты қорғау құралдары ҚР СТ Қазақстан Республикасының ұлттық стандарты ДБЖ Дерекқорларды басқару жүйесі API, REST API Қолданбалы бағдарламалау интерфейсі (Application Programming Interface); REST API — REST архитектуралық стилі бойынша құрылған бағдарламалық интерфейс CI/CD Үздіксіз интеграция және жеткізу (Continuous Integration / Continuous Delivery) CVE Common Vulnerabilities and Exposures — жалпыға белгілі осалдықтардың тізілімі CVSS Common Vulnerability Scoring System — осалдықтардың сындарлылығын бағалау жүйесі (3.1 немесе одан кейінгі нұсқасы қолданылады) CWE, CWE/SANS Common Weakness Enumeration — БҚ кемшіліктерінің жіктемесі; CWE/SANS Top 25 — БҚ-ның аса қауіпті кемшіліктерінің тізбесі EDR Endpoint Detection and Response — соңғы нүктелердегі қатерлерді анықтау және оларға ден қою жүйесі EXE, DLL Windows ОЖ-ның орындалатын файлдары мен динамикалық кітапханалары HIPAA Health Insurance Portability and Accountability Act — медициналық деректерді қорғау стандарты (АҚШ); статикалық талдау құралының есептілік
--	---

	үлгілерінің бірі ретінде пайдаланылады HIPS Host Intrusion Prevention System — хост деңгейінде басып кірулердің алдын алу жүйесі HTTP/HTTPS, POP3/POP3S, SMTP, IMAP/IMAPS, SMB, RPC, RDP, SSL Желілік хаттамалар: гипермәтінді беру (оның ішінде қорғалған), электрондық поштаны қабылдау және жіберу, файлдарға қол жеткізу, процедураларды қашықтан шақыру, қашықтағы жұмыс үстелі, қорғалған көлік деңгейі хаттамалары IDS Intrusion Detection System — басып кірулерді анықтау жүйесі JAR, WAR, EAR, AAR, APK, IPA, APP Java/Scala, Android, iOS және macOS компиляцияланған қосымшаларының пакеттер (архивтер) форматтары MITRE ATT&CK; MITRE корпорациясы жүргізетін қаскүнемдердің тактикалары мен техникалары туралы білім базасы OWASP Top 10, OWASP Mobile Top 10, OWASP MASVS OWASP жобасының веб- және мобильді қосымшалар қауіпсіздігінің аса сыни тәуекелдерінің тізбелері және мобильді қосымшалар қауіпсіздігін верификациялау стандарты PCI DSS Payment Card Industry Data Security Standard — төлем карталары индустриясының деректер қауіпсіздігі стандарты SARIF Static Analysis Results Interchange Format — статикалық талдау нәтижелерімен алмасу форматы SAST Static Application Security Testing — қосымшалардың бастапқы кодының қорғалуын статикалық талдау SIEM Security Information and Event Management — қауіпсіздік оқиғалары мен ақпаратын басқару жүйесі SOAR Security Orchestration, Automation and Response — инциденттерді оркестрлеу, автоматтандыру және оларға ден қою жүйесі UEFI Unified Extensible Firmware Interface — компьютердің кіріктірілген БҚ (жүктеуіші) интерфейсі URL Uniform Resource Locator — Интернет желісіндегі ресурс мекенжайы VDI Virtual Desktop Infrastructure — виртуалды жұмыс үстелдерінің инфрақұрылымы WMI Windows Management Instrumentation — Windows ОЖ басқару құралдары Git, SVN Бастапқы код нұсқаларын бақылау жүйелері CSV, HTML, PDF, XML, YAML Файл форматтары: үтірмен бөлінген мәндер; гипермәтіндік белгілеу тілі; тасымалданатын құжат форматы; кеңейтілетін белгілеу тілі; деректерді сериялау форматы 2. Қызмет көрсету мақсаты Қызмет көрсету мақсаты — Жүйені Қазақстан Республикасының нормативтік құқықтық актілерінде және Қазақстан Республикасының аумағында қолданылатын стандарттарда белгіленген киберқауіпсіздік талаптарына сәйкес келтіру және Жүйені Зертханада сынақтардан табысты өтуге дайындау. Мақсатқа қол жеткізу үшін Өлеуетті өнім беруші Жүйенің техникалық құжаттама, КҚ саласындағы нормативтік құқықтық актілер мен стандарттар талаптарына сәйкестігін бағалау, сәйкессіздіктер мен осалдықтарды анықтау, оларды Тапсырыс берушінің (Жүйе әзірлеушісінің) күшімен жоюды сүйемелдеу және Зертханаға ұсыну үшін құжаттар мен мәліметтер жиынтығын дайындау жөніндегі талдамалық, консультациялық және аспаптық жұмыстар кешенін орындайды. 3. Нормативтік құқықтық актілер және стандарттар 3.1. Қызметтер мынадай нормативтік құқықтық актілер мен стандарттарға (қызметтер көрсетілген күнгі қолданыстағы редакцияларында) сәйкес көрсетіледі: 3.1.1. Қазақстан Республикасының 2026 жылғы 9
--	---

	қаңтардағы № 255-VIII Цифрлық кодексі; 3.1.2. «Киберқауіпсіздік туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы (оның ішінде 49 «Киберқауіпсіздік талаптарына сәйкестікке сынақтар», 50 «Киберқауіпсіздік аудиті» баптары, 9 «Цифрлық объектілерді қорғау» тарауы); 3.1.3. «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы; 3.1.4. «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы; 3.1.5. Қазақстан Республикасы Цифрлық даму, қорғаныс және аэроғарыш өнеркәсібі министрінің 2019 жылғы 3 маусымдағы № 111/НҚ ««Цифрлық үкіметтің» цифрлық объектілері мен аса маңызды цифрлық объектілерін киберқауіпсіздік талаптарына сәйкестікке сынақтар жүргізу әдістемесі мен қағидаларын бекіту туралы» бұйрығы; 3.1.6. Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы № 52/НҚ ««Цифрлық үкіметтің» цифрлық объектілері мен аса маңызды цифрлық объектілерінің киберқауіпсіздігін қамтамасыз етуге мониторинг жүргізу қағидаларын бекіту туралы» бұйрығы; 3.1.7. ҚР СТ ISO/IEC 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік менеджменті жүйелері. Талаптар»; 3.1.8. ҚР СТ ISO/IEC 27002-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару құралдары»; 3.1.9. ҚР СТ ISO/IEC 27005-2022 (ақпараттық қауіпсіздік тәуекелдерінің менеджменті); 3.1.10. ҚР СТ ISO/IEC 15408-1-2017, ҚР СТ ISO/IEC 15408-2-2017, ҚР СТ ISO/IEC 15408-3-2017 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялар қауіпсіздігін бағалау критерийлері» (1-3-бөліктер); 3.1.11. ҚР СТ 2199-2012 (веб-қосымшалардың қауіпсіздігіне қойылатын талаптар); 3.1.12. Жүйенің санатын, мақсатын, өңделетін деректердің құрамын және пайдалану шарттарын ескере отырып, оған тікелей қолданылатын Қазақстан Республикасы заңнамасының өзге де міндетті талаптары. Өлеуетті өнім беруші сәйкестік матрицасында нақты нормативтік құқықтық актіні, талаптың тармағын және оны қолдану негізін көрсетеді. Қосымша ерікті стандарттар Тапсырыс берушімен келісу бойынша қолданылады. 4. Қызметтер көрсету объектісі 4.1. Қызметтер көрсету объектісі — «цифрлық үкімет» объектілеріне жататын және мемлекеттік ақпараттық жүйелермен және өзге де цифрлық объектілермен интеграцияланатын, меншік иесі (иеленушісі) Тапсырыс беруші болып табылатын, Тапсырыс берушінің Сығанақ к-сі, 70-ғимарат мекенжайындағы меншікті серверлік үй-жайында және QazTech деректерді өңдеу орталығында орналастырылған «Халықаралық бағдарламалар орталығы» АҚ-ның «е-Болашақ» көпфункционалды ақпараттық жүйесі (бұдан әрі — «е-Болашақ» КФАЖ). 4.2. Қызметтер Жүйеге толық құрамда — қолданбалы бағдарламалық қамтамасыз етуге, дерекқорларға, виртуалдандыру ортасына, серверлік және желілік
--	--

	жабдыққа, ақпаратты қорғау құралдарына, әкімшілердің автоматтандырылған жұмыс орындарына және Жүйенің жұмыс істеуін қамтамасыз ететін барлық өзге де компоненттерге — олардың санына қарамастан көрсетіледі. Серверлердің, виртуалды машиналардың, желілік құрылғылардың және өзге де компоненттердің саны қызметтердің көлемі мен құнын өзгертуге негіз болып табылмайды. 4.3. Жүйе компоненттерінің нақты құрамын Әлеуетті өнім беруші 1-кезеңде (5-бөлім) Тапсырыс беруші ұсынатын құжаттама мен мәліметтер негізінде нақтылайды және ол зерттеп-қарау туралы есепте (7-бөлім) тіркеледі. 5. Қызметтер көрсетудің құрамы мен кезеңдері 5.1. Қызметтер көрсету мынадай кезеңдерге бөлінеді: № Кезең Мазмұны Нәтиже (есептік құжаттар) 1 Жүйе инфрақұрылымының КҚ-ын талдау (зерттеп-қарау) Бастапқы деректерді жинау, архитектураны, конфигурацияларды, журналдауды, физикалық қорғауды талдау, аспаптық сканерлеу, жүктемелік тестілеу, бастапқы кодты талдау (6.1, 6.3, 6.5, 6.7, 6.9, 6.10, 6.13, 6.14-тармақтар) Зерттеп-қарау туралы есеп; сканерлеу, жүктемелік тестілеу және бастапқы кодты талдау бойынша есептер 2 Сәйкессіздіктерді анықтау және ұсынымдар беру Зерттеп-қарау нәтижелерін 3-бөлімнің талаптарымен салыстыру, басымдықтарын белгілей отырып және жою жөніндегі ұсынымдармен сәйкессіздіктер мен осалдықтардың тізбесін қалыптастыру (6.2, 6.4, 6.6, 6.8, 6.15-тармақтар) Сәйкессіздіктер тізбесі және оларды жою жөніндегі іс-шаралар жоспары 3 Сәйкессіздіктерді жоюды консультациялық сүйемелдеу Сәйкессіздіктерді жою кезінде Тапсырыс беруші мен Жүйе әзірлеушісіне консультация беру, бақылау (қайталама) тексерулері, Зертханаға ұсыну үшін құжаттар жиынтығын дайындау (6.11, 6.12, 6.16, 6.17-тармақтар) Қайталама тексерулер бойынша есептер; Жүйенің сынақтарға дайындығы туралы қорытынды есеп 4 Тапсырыс беруші персоналының хабардарлығын арттыру 6.2, 6.4, 6.6, 6.8, 6.11, 6.15, 6.17-тармақтарды орындау барысында Жүйе әкімшілеріне және Тапсырыс берушінің КҚ-ға жауапты тұлғаларына анықталған сәйкессіздіктер, қолданылған қорғау шаралары және сынақтарға дайындалу тәртібі бойынша консультация беру және нұсқама жүргізу Консультациялар хаттамалары (тиісті тармақтар бойынша есептерде тіркеледі) 5.2. Кезеңдердің күнтізбелік мерзімдері қызметтер көрсетудің жоспар-кестесімен айқындалады, оны Әлеуетті өнім беруші шарт жасалған күннен бастап 10 жұмыс күні ішінде Тапсырыс берушіге келісуге ұсынады. Егер бұл жұмыстардың логикасына қайшы келмесе, кезеңдер қатар орындалуы мүмкін. 6. Қызметтердің толық сипаттамасы Әлеуетті өнім беруші қызметтер көрсету шеңберінде мыналарды орындауға тиіс: 6.1. Қолданбалы бағдарламалық қамтамасыз етудің, дерекқордың (Жүйе әзірлеушісімен бірлесіп), виртуалдандыру ортасының және серверлік жабдықтың операциялық жүйелерінің функционалының қауіпсіздігін Бірыңғай талаптарға және ҚР СТ ISO/IEC 27002-2023-ке сәйкестігіне талдау, оның ішінде: есептік жазбаларды және қол жеткізу құқықтарын басқару, парольдік саясат және көпфакторлы аутентификация, жаңартуларды басқару, пайдаланылмайтын қызметтер мен
--	---

порттарды өшіру, компоненттердің өзара іс-қимыл арналарын қорғау, резервтік көшіру конфигурациясы. 6.2. Қолданбалы бағдарламалық қамтамасыз етуді, дерекқорды (Жүйе әзірлеушісімен бірлесіп), виртуалдандыру ортасын және серверлік жабдықтың операциялық жүйелерін КҚ жөніндегі талаптарға сәйкес баптау (қорғалуын күшейту) бойынша анықталған әрбір сәйкессіздік бойынша жазбаша ұсынымдар бере отырып консультация беру. 6.3. Қолданбалы бағдарламалық қамтамасыз етудің, дерекқордың (Жүйе әзірлеушісімен бірлесіп), виртуалдандыру ортасының және серверлік жабдықтың операциялық жүйелерінің оқиғаларын журналдауды талдау: тіркелетін оқиғалардың құрамы, толықтығы, сақтау мерзімдері, журналдарды өзгертуден қорғау, уақытты синхрондау. 6.4. Қолданбалы бағдарламалық қамтамасыз етудің, дерекқордың, виртуалдандыру ортасының және серверлік жабдықтың операциялық жүйелерінің оқиғаларын журналдауды Мониторинг қағидаларына және Бірыңғай талаптарға сәйкес, оның ішінде оқиғаларды КҚ-ны қамтамасыз ету мониторингі жүйесіне беруге қойылатын талаптарды қоса алғанда, баптау бойынша консультация беру. 6.5. Желілік жабдықтың (желіаралық экрандар, маршрутизаторлар, коммутаторлар, қашықтан қол жеткізу құралдары) конфигурациясын талдау: желіні сегменттеу, трафикті сүзгілеу қағидалары, басқару интерфейстерін қорғау, пайдаланылатын хаттамалар, есептік жазбалар. 6.6. Желілік жабдықты Бірыңғай талаптарға сәйкес баптау бойынша жазбаша ұсынымдар бере отырып консультация беру. 6.7. Желілік жабдық оқиғаларын журналдауды талдау. 6.8. Желілік жабдық оқиғаларын журналдауды Мониторинг қағидаларына және Бірыңғай талаптарға сәйкес баптау бойынша консультация беру. 6.9. Серверлік үй-жайдың физикалық қорғалуын (Өлеуетті өнім берушінің Жүйе орналасқан жерге баруы) Бірыңғай талаптарға сәйкестігіне тексеру: қол жеткізуді бақылау және есепке алу, күзет және өрт дабылы, өрт сөндіру, климаттық жабдық, үздіксіз электрмен қоректендіру, жабдықты орналастыру, келушілер журналдарын жүргізу; нәтижелері бойынша — сәйкессіздіктер тізбесі және оларды жою жөніндегі ұсынымдар көрсетілген есеп. 6.10. Жүйенің серверлерін, желілік жабдығын және веб-қосымшасын аудит режимінде (Тапсырыс беруші ұсынған есептік жазбаларды пайдалана отырып) және енуге тестілеу режимінде (есептік жазбаларсыз, сыртқы және ішкі периметрден) осалдықтар базасы өзекті қорғалуды талдау құралын пайдалана отырып, осалдықтардың болуына аспаптық сканерлеу, сондай-ақ келісілген шекараларда қолмен енуге тестілеу. Анықталған осалдықтар CVSS 3.1 немесе одан жаңа нұсқасына сәйкес сындылық деңгейі бойынша жіктеледі; әрбір осалдық бойынша жою жөніндегі ұсынымдар беріледі. Сканерлеу Тапсырыс берушімен келісілген уақыт аралықтарында жүргізіледі. 6.11. Серверлерді, желілік жабдықты және веб-қосымшаны сканерлеу нәтижелері бойынша анықталған осалдықтарды жоюды Тапсырыс берушімен (Жүйе әзірлеушісімен) бірлесіп пысықтау: жою тәсілдері бойынша консультация беру, қолданылған шараларды тексеру. 6.12. Осалдықтар жойылғаннан кейін аудит және енуге тестілеу режимдерінде

	осалдықтардың болуына қайталама аспаптық сканерлеу. Аяқтау өлшемшарты: сындылығы сыни және жоғары деңгейдегі осалдықтардың болмауы (CVSS базалық бағасы 7,0 және одан жоғары). Бұғаттаушы сәйкессіздіктер үшін «дайын емес» мәртебесін және қажетті әрекеттер тізбесін көздеу. 6.13. Тапсырыс берушімен келісілген әдістеме бойынша (сценарийлер, бір мезгілдегі пайдаланушылар саны, сұраныстар қарқындылығы, бақыланатын көрсеткіштер: жауап беру уақыты, қателер үлесі, ресурстарды пайдалану) ең жоғары жүктемені айқындау үшін Жүйені жүктемелік тестілеу, оңтайландыру жөніндегі ұсынымдар беру; ұсынымдар іске асырылғаннан кейін — нәтижелерді салыстыра отырып, қайталама жүктемелік тестілеу. 6.14. Жүйенің бастапқы кодын осалдықтардың және декларацияланбаған мүмкіндіктердің (ДМ) болуына статикалық талдау құралымен (SAST) талдау, нәтижелерді жіктей отырып (CWE, OWASP Top 10) және жою жөніндегі ұсынымдар бере отырып; анықталған кемшіліктер жойылғаннан кейін — нәтижелерді салыстыра отырып қайталама талдау. Бастапқы кодты Тапсырыс беруші (Жүйе әзірлеушісі) ұсынады. Талдауды Әлеуетті өнім беруші өз алаңында меншікті статикалық талдау құралын пайдалана отырып — талдау құралын Тапсырыс берушінің инфрақұрылымында өрістетпей және оған лицензияларды Тапсырыс берушіге бермей орындайды; нәтижесі 6.14.5-тармаққа және 7-бөлімге сәйкес ресімделген сканерлеу туралы есеп (бастапқы және қайталама) болып табылады. Әлеуетті өнім беруші қолданатын статикалық талдау құралы 6.14.1-6.14.10-тармақтардың талаптарына сәйкес келуге тиіс. Әлеуетті өнім беруші 6.14-тармақты орындау кезінде қолданатын бастапқы кодты статикалық талдау құралы мынадай ең төменгі талаптарға сәйкес келуге тиіс: 6.14.1. Жалпы функционалдық талаптар: бағдарламалық қамтамасыз етуді бастапқы код бойынша КҚ талаптарына сәйкестігіне талдау; бастапқы кодтар және жөндеу ақпараты болмаған кезде байт-код (бинарлық код) бойынша статикалық талдау әдісімен талдау; декларацияланбаған мүмкіндіктерді (ДМ) іздеу; талдау нәтижелері бойынша пайдаланылуын ақпаратты қорғау құралдарын (АҚК) баптау арқылы болдырмауға болатын осалдықтар мен ДМ үшін АҚК-ны баптау жөніндегі ұсынымдар беру. 6.14.2. Талдау әдістері: осалдықтар мен ДМ-ді іздеу кемінде мынадай статикалық талдау әдістерін қолдана отырып жүзеге асырылуға тиіс: үлгілер бойынша талдау; басқару ағынын талдау; taint-талдау (деректер ағындарын талдау); синонимдерді талдау; тұрақтыларды тарату. Әдістер бастапқы (байт-) код трансляцияланатын ішкі ұсынымға қолданылады. 6.14.3. Бастапқы код бойынша талдау: бағдарламалау тілдерін қолдау: Java, JavaScript, TypeScript, PHP, Python, C#, Go, PL/SQL, T-SQL, HTML5, SQL, Bash, PowerShell, XML, YAML; тілдерді автоматты түрде тани отырып, көптілді жобаларды талдау; құрастыру құралдарымен интеграция. 6.14.4. Жүйеде бастапқы коды қолжетімсіз компоненттер болған кезде бинарлық (байт-) код бойынша талдау: 6.14.2-тармақтың әдістерін қолдана отырып, Java/Scala (JAR, WAR, EAR, AAR), C/C++ (DLL, EXE), Android (APK), Apple iOS (IPA), Apple macOS (APP) тілдерінен
--	---

трансляциялау арқылы алынған байт-кодты талдау. 6.14.5. Нәтижелер және есептілік: орыс және ағылшын тілдерінде CSV, HTML, PDF және SARIF форматтарында есептер қалыптастыру; PCI DSS, OWASP Top 10, OWASP Mobile Top 10, HIPAA, CWE/SANS, OWASP MASVS стандарттары мен жіктемелеріне сәйкестік туралы есептер; әрбір осалдық және ДМ бойынша — сипаттамасы, сындылық дәрежесі, кодтағы орны (оның ішінде бастапқы код болмаған кезде), қауіптілігін және пайдаланудың ықтимал тәсілдерін түсіндіру, түзету жөніндегі ұсынымдар, сыртқы дереккөздерге және жіктемеге сілтемелер; сканерлеу тарихы және жобаны сканерлеу нәтижелерін салыстыру (қайталама талдау нәтижелері бойынша кемшіліктердің жойылғанын растау үшін); қосымшаның қауіпсіздік метрикаларын есептеу және сындылық дәрежесі бойынша жиынтық статистика; есеп құрамын баптау (қосымшалар мен осалдық санаттарын таңдау). 6.14.6. Интерфейс және рөлдер: ақпаратқа бірыңғай қол жеткізу нүктесі; орыс және ағылшын тілдеріндегі интерфейс; функцияларды кемінде «әкімші», «қауіпсіздік офицері», «әзірлеуші», «басшы» пайдаланушылар санаттары үшін рөлдік ажырату; талдау үшін қосымшаны жүктеу және репозиторий мен әзірлеу тармағына жолды көрсету; әкімші интерфейсінде пайдаланушыларды және олардың құқықтарын басқару. Тапсырыс берушінің сұрауы бойынша Әлеуетті өнім беруші талдау нәтижелерін құрал интерфейсінде (оның ішінде қашықтан) көрсетеді. 6.14.7. Интеграция: талданатын кодты нұсқаларды басқару жүйелерінен (Git, SVN) және мұрағат түрінде жүктеуді қолдау; үздіксіз интеграция сервистерімен (CI/CD) және қателерді қадағалау жүйелерімен интеграцияны қолдау; ашық API болуы. Осы қызметтер шеңберінде Жүйені әзірлеушінің инфрақұрылымымен интеграция орындалмайды. 6.14.8. Талдау құралының қауіпсіздігі: әкімші баптайтын құқықтарға сәйкес иерархия деңгейлері бойынша қол жеткізуді ажырату; пайдаланушы мен әкімші функцияларына тек жеке тіркелгі деректері бойынша қол жеткізу; парольдерді шифрланған (хештелген) түрде сақтау; тіркелгі деректерін енгізудің қате әрекеттерінің санын бапталатын шекпен шектеу; парольді тұрақты ауыстыруға және оның қолданылу мерзіміне қойылатын бапталатын талаптар; пайдаланушы белсенді болмаған кезде сеансты автоматты түрде аяқтау; пайдаланушылар мен әкімшілер әрекеттерін толық журналдау. 6.14.9. Бастапқы кодты орналастыру және онымен жұмыс істеу: талдау құралы Әлеуетті өнім берушінің Қазақстан Республикасы аумағындағы алаңында орналастырылады және Тапсырыс берушінің инфрақұрылымында өрістетілмейді; Жүйенің бастапқы коды Тапсырыс берушімен (Жүйені әзірлеушімен) Әлеуетті өнім берушіге қорғалған арна арқылы не қабылдау-беру актісі бойынша жеткізгіште беріледі, Әлеуетті өнім берушінің оқшауланған ортасында сақталады, үшінші тұлғаларға берілмейді және Қазақстан Республикасынан тыс жерлердегі бұлттық сервистерге жүктелмейді; қызметтер көрсету аяқталғаннан кейін Әлеуетті өнім берушідегі бастапқы кодтың көшірмелері 8.4-тармақта белгіленген тәртіппен жазбаша растаумен жойылады. 6.14.10. Пайдалану заңдылығын растау: Әлеуетті өнім

беруші статикалық талдау құралын заңды негізде (лицензия, жазылым немесе пайдаланудың өзге құқығы) қолданады. Әлеуетті өнім беруші конкурстық өтінімнің құрамында статикалық талдау құралының өндірушісінен (құқық иеленушісінен) Тапсырыс берушінің атына ресімделген, лоттың (сатып алудың) атауы мен нөмірі, талдау құралының атауы мен нұсқасы, сондай-ақ Әлеуетті өнім берушінің Тапсырыс берушіге қызметтер көрсету кезінде оны пайдалану құқығын растау көрсетілген авторизациялық хатты қоса беруге тиіс. Хаттың мәтіні шет тілінде болған жағдайда хат нотариалды куәландырылуға және қазақ немесе орыс тілдеріне аударылуға тиіс.

6.15. Тапсырыс берушінің КҚ жөніндегі қолданыстағы техникалық құжаттамасын (КҚ саясаты, Бірыңғай талаптарда көзделген қағидалар мен регламенттер, Жүйеге арналған құжаттама) толықтығына, 3-бөлімнің талаптарына және Зертхана сұрататын құжаттар тізбесіне сәйкестігіне талдау; оны өзектендіру бойынша консультациялар және жетіспейтін құжаттардың жобаларын дайындау.

6.16. Әлеуетті өнім беруші Тапсырыс берушінің ресми сұрауы бойынша Тапсырыс берушінің инфрақұрылымын соңғы нүктелердегі қатерлерді анықтау және оларға ден қою жүйесімен (EDR) (бұдан әрі — EDR жүйесі) кемінде 25 (жиырма бес) лицензия (қорғалатын соңғы нүктелердегі — жұмыс станциялары мен серверлердегі EDR агенттері) көлемінде, лицензиялардың қолданылу мерзімі кемінде 2026 жылғы 31 желтоқсанға дейін болатындай етіп жарақтандыруға тиіс. EDR жүйесі 6.16.1–6.16.10-тармақтардың талаптарына сәйкес келетін орталықтандырылған басқару құралдарын, жұмыс станциялары мен серверлерді қорғау компоненттерін және анықтау және ден қою модулін қамтуға тиіс. Серверлік компоненттер Тапсырыс берушінің инфрақұрылымында өрістетіледі (жергілікті орналастыру). Осы тармақ бойынша қызметтер көлеміне мыналар кіреді: EDR жүйесін пайдалану құқықтарын (лицензияларды) беру; серверлік компоненттерді орнату және баптау; Тапсырыс берушінің соңғы нүктелерінде агенттерді өрістету; қорғау саясаттары мен анықтау қағидаларын базалық баптау; Тапсырыс берушінің әкімшілеріне жүйені пайдалану бойынша нұсқама беру; лицензиялардың қолданылу мерзімі ішінде өндірушінің техникалық қолдауы.

6.16-тармақ бойынша жеткізілетін EDR жүйесі мынадай ең төменгі талаптарға сәйкес келуге тиіс:

6.16.1. Жалпы талаптар: барлық компоненттердің интерфейсі, оның ішінде басқару консолі, контекстік анықтама және пайдалану құжаттамасы (оның ішінде орнатуды, баптауды және пайдалануды сипаттайтын әкімші нұсқаулығы) — орыс және ағылшын тілдерінде; өндірушінің телефон және электрондық пошта арқылы орыс тіліндегі техникалық қолдауы, қажет болған жағдайда — Тапсырыс берушіге барумен; өндірушінің веб-сайтында техникалық қолдау бөлімі мен білім қорының болуы.

6.16.2. Орталықтандырылған басқару консолі: бүкіл инфрақұрылымның қорғалуын сертификатпен қорғалған қосылым арқылы бірыңғай веб-интерфейстен басқару; басты және бағынышты басқару серверлерінің иерархиясы; Windows, Linux және macOS басқаруындағы соңғы нүктелердің жабдықтары мен бағдарламалық қамтамасыз

	етуін түгендеу; агенттерді, қорғау компоненттерін және бөгде БҚ-ны қашықтан орнату және жою, алдын ала орнатылған конфигурациясы бар орнату пакеттерін қалыптастыру (оның ішінде оқшауланған желілер үшін); саясаттар мен тапсырмаларды автоматты түрде тағайындайтын статикалық және динамикалық топтар, компьютерлер, пайдаланушылар және топтар құрылымын Active Directory-ден импорттау; экспорттау және импорттау мүмкіндігі бар кірістірілген және пайдаланушылық саясаттар; әкімшілер құқықтарын рөлдік ажырату, Active Directory топтары арқылы аутентификация, әкімшілерді екі факторлы аутентификациялау; барлық әрекеттер мен конфигурация өзгерістерінің аудит журналы; мониторинг тақтасы және электрондық поштаға кесте бойынша жіберілетін бапталатын есептер (PDF, CSV); syslog және REST API арқылы SIEM-мен интеграция; Интернетке қол жеткізу мүмкіндігі жоқ желілер үшін жаңартулардың жергілікті айнасы; өзін-өзі қорғау тетіктері, автоматты жаңартуы және командалық жолдан басқаруы бар тәуелсіз басқару агенті; VDI орталарын қолдау; ОЖ өндірушілерінің қолдау өмірлік циклінде тұрған Windows, Linux және macOS өзекті нұсқаларын қолдау. 6.16.3. Жұмыс станцияларын қорғау: вирустардан, трояндық, тыңшылық және жарнамалық бағдарламалардан, фишингтен, ықтимал қажетсіз және қауіпті бағдарламалардан, руткиттерден нақты уақыт режимінде, сұрау бойынша және кесте бойынша қорғау, оның ішінде ОЖ іске қосылған кезде сканерлеу, жүктеу секторларын және UEFI-ді, тізім мен WMI-ді, жедел жадты сканерлеу; сигнатуралық талдауды, эвристиканы және машиналық оқытуды үйлестіру; эксплойттардан қорғау, бопсалаушы бағдарламалардан мінез-құлықтық қорғау, пайдаланушылық қағидалары бар хостта басып кіруді болдырмау жүйесі (HIPS), өндірушінің бұлттық базасында процестердің беделін тексеру; сыртқы құрылғыларды түрі, өндірушісі, моделі және сериялық нөмірі бойынша домен пайдаланушылары мен топтарына және уақыт аралықтарына байланыстыра отырып бақылау; пошта трафикін (POP3/POP3S, SMTP, IMAP/IMAPS) және тіркемелерді тексеру; SSL-сертификаттарды бақылай отырып, фишингтік ресурстарды, ботнет серверлерін және басқарушы серверлерді бұғаттай отырып, URL тізімдерімен HTTP/HTTPS-трафикті тексеру; желі профильдері, желілік шабуылдарды анықтау модулі (IDS) және CVE көрсетілген желілік хаттамалардың (SMB, RPC, RDP) осалдықтарын пайдаланудан қорғауы бар дербес брандмауэр; домен пайдаланушылары мен топтары үшін санаттар бойынша веб-бақылау; базаларды тәулігіне кемінде 24 рет жергілікті айнадан және резервтік көздерден кері қайтару мүмкіндігімен жаңарту; баптауларды парольмен қорғау; қашықтан орнату; Windows 10/11 және кең таралған Linux дистрибутивтерін қолдау. 6.16.4. Серверлерді қорғау: тиісті ерекшеліктерді құра отырып, сервер рөлдерін автоматты түрде анықтау; жұмыс станцияларындағыдай (6.16.3-тармақ) анықтау тетіктерімен нақты уақыт режимінде, сұрау бойынша және кесте бойынша қорғау, оның ішінде эксплойттардан және бопсалаушы бағдарламалардан қорғау, HIPS, UEFI мен жедел жадты сканерлеу; Hyper-V виртуалды
--	--

	машиналарын агенттер орнатпай сканерлеу; сыртқы құрылғыларды бақылау; пошта және веб-трафикті тексеру; домен және жұмыс тобы кластерлерінде жұмыс істеу; сканерлеу ағындарының санын баптау; терминалдық серверлер үшін графикалық интерфейссіз режим; параметрлерді өзгертуден және жоюдан парольмен қорғау; қашықтан орнату; Windows Server 2016–2025 және кең таралған серверлік Linux дистрибутивтерін (Red Hat Enterprise Linux, Ubuntu, Debian, SUSE Linux Enterprise Server, Oracle Linux, Rocky/Alma Linux) қолдау. 6.16.5. Анықтау және ден қою модулі (EDR) — анықтау: EDR серверімен басқарылатын коннектор (агент) арқылы соңғы нүктелерден телеметрияны деректерді жергілікті сақтай отырып жинау; тек сигнатуралық анықтау негізінде ғана емес, қағидалар (әдепкі қағидалар жиынтығы және XML-де өңделетін меншікті қағидалар) негізінде аномальды мінез-құлықты анықтау; ескертулерді сыни деңгейі бойынша автоматты түрде жіктеу, басымдық беру және топтастыру (түрі, компьютер, қағида, процесс, файл бойынша); жиынтық ақпараты (уақыт, компьютер, пайдаланушы, процесті бастамашылаған орындалатын файл), оқиға сипаттамасы, ықтимал себептері, тәуекелдері мен ұсынымдары бар анықтау карточкасы; MITRE ATT&CK; техникаларымен салыстыру; түпкі себептерді талдау және файлдық жүйе, тізілім, желілік қосылымдар және URL өзгерістерін егжей-тегжейлі көрсететін процестердің толық ағашы; орындалатын файлдар (EXE/DLL) мен скрипттерді сыни деңгейі бойынша автоматты түрде жіктеу; мақсатты шабуылдарды анықтау үшін беделі, таралуы, цифрлық қолтаңбасы және мінез-құлқы бойынша сүзгілер; соңғы нүктелердегі барлық орындалатын файлдар мен скрипттерді түгендеу; іздеу тапсырмаларын сақтай отырып, бүкіл телеметрия базасы бойынша кез келген параметрлер (оның ішінде командалық жол фрагменттері) бойынша іздеу; аномальды оқиғалар мониторингінің тақтасы. 6.16.6. Анықтау және ден қою модулі (EDR) — ден қою: барлық соңғы нүктелерде орындалатын файлдарды бақылау сомасы бойынша бұғаттау, қара және ақ тізімдер, егжей-тегжейлі ерекшеліктер (бақылау сомасы, жол, цифрлық қолтаңба); файлдарды қашықтан жою және карантинге орналастыру; бір рет басу арқылы бұзылған құрылғыны желіден оқшаулау және оқшаулаудан шығару; қашықтан қайта жүктеу және өшіру; тереңдетілген сканерлеуді іске қосу; ОЖ күйінің суретін жасау (процестер, желілік қосылымдар, тізілім, жоспарлағыш, пайдаланушылар және артықшылықтар, сыни файлдар); талдау үшін соңғы нүктелерден күдікті файлдар мен скрипттерді жүктеп алу және оларды консольден сыртқы бедел сервистерінде тексеру; сүзгілеу үшін объектілерге тегтер тағайындау; SIEM, SOAR және тапсырмаларды өңдеу жүйелерімен интеграцияға арналған бағдарламалық интерфейс (API); әкімшілерді екі факторлы аутентификациялау; коннектордың Windows 10/11, кең таралған Linux дистрибутивтерін және macOS қолдауы. 6.16.7. Бұлттағы кеңейтілген талдау (жеткізілетін лицензиялар құрамында болған жағдайда): күдікті файлдарды жұмыс станциялары мен серверлерден машиналық оқытуды қолдана отырып талдау үшін өндірушінің бұлттық
--	---

	құмсалғышына автоматты және қолмен жіберу; бастапқы талдау нәтижелері бойынша (бірнеше секундтан 6 минутқа дейін) және ұзақ бақылау кезінде нөлдік күн қатерлерін бұғаттау; үлгілерді жіберу мен сақтаудың бапталатын саясаттары; талдау нәтижелері туралы есептер. 6.16.8. Сенімнің бағалау деңгейі: EDR жүйесінің бағдарламалық өнімі ҚР СТ ISO/IEC 15408-3-2017 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық технологиялар қауіпсіздігін бағалау критерийлері. 3-бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар» бойынша 4-тен төмен емес сенімнің бағалау деңгейіне (СБД) ие болуға тиіс. Тапсырыс беруші Әлеуетті өнім берушіден сұрау салынған күннен бастап 3 (үш) жұмыс күні ішінде бағдарламалық өнімнің ҚР СТ ISO/IEC 15408-3-2017 талаптарына сәйкестік сертификатын (сәйкестікті растайтын құжатты) 4-тен төмен емес сенімнің бағалау деңгейін көрсете отырып талап етуге құқылы. 6.16.9. Әлеуетті өнім беруші конкурстық өтінімнің құрамында EDR жүйесі өндірушісінің (құқық иеленушісінің) Тапсырыс берушінің атына ресімделген, бағдарламалық өнімнің атауы мен нұсқасы, лицензиялардың саны мен қолданылу мерзімі көрсетілген, сондай-ақ Әлеуетті өнім берушінің Қазақстан Республикасының аумағында пайдалану құқықтарын беруге (лицензияларды жеткізуге) және техникалық қолдау көрсетуге құқығы расталған авторизациялық хатын қоса беруге тиіс. Хаттың мәтіні шет тілінде болған жағдайда хат нотариат куәландырған және қазақ немесе орыс тілдеріне аударылған болуға тиіс; 6.16.10. Берілетін құжаттар: өрістету нәтижелері бойынша Әлеуетті өнім беруші Тапсырыс берушіге лицензиялардың саны мен қолданылу мерзімі көрсетілген лицензиялық құжаттарды (белсендіру кілттерін/сертификаттарын), пайдалану құжаттамасын және қорғалған соңғы нүктелердің тізбесі көрсетілген EDR жүйесін орнату және баптау актісін береді. 6.17. Сынақтарға дайындық мәселелері бойынша мемлекеттік органдармен, Зертханамен және Жүйені әзірлеушімен хат алмасуды жүргізу кезінде Тапсырыс берушіге жәрдем көрсету, оның ішінде Тапсырыс берушінің Зертханаға кейіннен ұсынуы үшін Сынақ әдістемесі мен қағидаларына сәйкес сынақтар жүргізуге арналған өтінімнің және қоса берілетін құжаттар топтамасының жобаларын дайындау. 7. Нәтижелерге және есептік құжаттарға қойылатын талаптар 7.1. Қызметтер көрсету нәтижелері бойынша Әлеуетті өнім беруші Тапсырыс берушіге мынадай есептік құжаттарды ұсынады: № Құжат Мазмұнына қойылатын талаптар / мерзімі 1 Қызметтер көрсетудің жоспар-кестесі Кезеңдер, мерзімдер, жауаптылар, Тапсырыс берушіден қажетті деректер мен қолжетімділіктердің тізбесі. Шарт жасалған күннен бастап 10 жұмыс күні ішінде 2 Жүйенің КҚ зерттеп-қарау туралы есеп Архитектураның және зерттеп-қарау периметрінің сипаттамасы; 6.1, 6.3, 6.5, 6.7, 6.9-тармақтар бойынша талдау нәтижелері; 3-бөлімнің талаптарына сәйкестікті бағалау 3 Сәйкессіздіктердің тізбесі және оларды жою жөніндегі іс-шаралар жоспары Әрбір сәйкессіздік: сипаттамасы, НҚА/стандарт талабына сілтеме, сыншылдық деңгейі, ұсыным, жауапты тарап,
--	--

	болжамды мерзімі 4 Осалдықтарға сканерлеу бойынша есептер (бастапқы және қайталама) Периметр, режимдер, CVSS бағалауы бар осалдықтардың тізбесі, ұсынымдар; бастапқы және қайталама сканерлеу нәтижелерін салыстыру; сканерлеу құралынан экспорт 5 Жүктемелік тестілеу бойынша есептер (бастапқы және қайталама) Әдістеме, сценарийлер, алынған көрсеткіштер, анықталған ең жоғары жүктеме, ұсынымдар, нәтижелерді салыстыру 6 Бастапқы кодты сканерлеу туралы есептер (бастапқы және қайталама) Периметр (модульдердің тізбесі, кодтың тармағы/нұсқасы, берілген архивтердің бақылау сомалары), талдау құралы және оның нұсқасы, жіктелуі мен сыншылдық дәрежесі көрсетілген анықталған осалдықтар мен ДМ, жою жөніндегі ұсынымдар, бастапқы және қайталама сканерлеу нәтижелерін салыстыру; талдау құралынан PDF және SARIF/CSV форматындағы түсірілім 7 Серверлік үй-жайдың физикалық қорғалуын тексеру туралы есеп 6.9-тармақ бойынша тексеру нәтижелері, Тапсырыс берушімен келісу бойынша фототіркеу, сәйкессіздіктер мен ұсынымдар 8 КҚ жөніндегі құжаттама бойынша қорытынды Қолда бар және жетіспейтін құжаттардың тізбесі, ескертулер, өзектендіру жөніндегі ұсынымдар, құжаттардың жобалары 9 EDR жүйесі бойынша құжаттар (Тапсырыс берушінің сұрауы бойынша жарақтандырған кезде, 6.16-тармақ) Лицензиялардың саны мен қолданылу мерзімі көрсетілген лицензиялық құжаттар (белсендіру кілттері/сертификаттары); пайдалану құжаттамасы; қорғалған соңғы нүктелердің тізбесі көрсетілген орнату және баптау актісі (6.16.10-тармақ); Тапсырыс берушінің сұрауы бойынша — СБД 4-тен төмен емес ҚР СТ ISO/IEC 15408-3-2017 сәйкестік сертификаты және өндірушінің авторизациялық хаты (6.16.8, 6.16.9-тармақтар) 10 Жүйенің сынақтарға дайындығы туралы қорытынды есеп Жиынтық нәтижелер, сәйкессіздіктерді жою мәртебесі, қабылданған тәуекелдердің тізбесі, Зертханаға ұсынуға арналған құжаттар топтамасы 7.2. Есептік құжаттар орыс тілінде немесе Тапсырыс берушінің талабы бойынша қазақ тілінде электрондық түрде (PDF форматында және өңделетін форматта) және Тапсырыс берушінің талабы бойынша қағаз жеткізгіште 1 (бір) данада ұсынылады. Осалдықтар мен конфигурациялар туралы мәліметтерді қамтитын есептік құжаттар қорғалған арналар арқылы не жеткізгіште қолхат арқылы беріледі. 8. Қызметтер көрсету шарттары 8.1. Тапсырыс беруші жоспар-кестемен келісілген мерзімдерде Әлеуетті өнім берушіге: Жүйеге арналған техникалық құжаттаманы, желі схемаларын, компоненттердің тізбесін, жұмыстарды орындау үшін қажетті есептік жазбалар мен қолжетімділіктерді, Тапсырыс беруші өкілінің сүйемелдеуімен серверлік үй-жайға кіруді, сондай-ақ Тапсырыс беруші мен Жүйені әзірлеуші тарапынан байланыс тұлғаларын ұсынады. 8.2. Жүйенің қолжетімділігіне әсер етуі мүмкін жұмыстар (аспаптық сканерлеу, жүктемелік тестілеу) тек Тапсырыс берушімен келісілген уақыт терезелерінде, жазбаша хабарламадан кейін және Тапсырыс берушіде Жүйенің өзекті резервтік көшірмесі болған жағдайда орындалады. Жүктемелік тестілеу тестілік стендте / өнеркәсіптік ортада ең жоғары жүктеме сағаттарынан тыс
--	---

	уақытта жүргізіледі. 8.3. Жұмыстарды жүргізу кезінде деструктивті әсер ететін осалдықтарды пайдалануға, Тапсырыс берушінің деректерін өзгертуге немесе жоюға, Тапсырыс берушімен келіспей Жүйенің конфигурациясына өзгерістер енгізуге жол берілмейді. Барлық өзгерістерді Әлеуетті өнім берушінің ұсынымдары негізінде Тапсырыс беруші (Жүйені әзірлеуші) не Тапсырыс берушінің жазбаша тапсырмасы бойынша Әлеуетті өнім беруші орындайды. 8.4. Әлеуетті өнім беруші Қазақстан Республикасының заңнамасына сәйкес қызметтер көрсету барысында алынған барлық ақпараттың, оның ішінде осалдықтар, конфигурациялар туралы мәліметтер мен дербес деректердің құпиялылығын қамтамасыз етеді; жұмыстар басталғанға дейін тараптар жария етпеу туралы келісімге қол қояды. Қызметтер көрсету нәтижелері Тапсырыс берушінің меншігі болып табылады; қызметтер көрсету аяқталғаннан кейін Әлеуетті өнім беруші жұмыстар барысында алынған Тапсырыс беруші деректерінің көшірмелерін растаумен жояды. 8.5. Әлеуетті өнім беруші пайдаланатын қорғалуды талдау, жүктемелік тестілеу және бастапқы кодты талдау құралдары заңды негізде (лицензиялық не еркін таратылатын) қолданылуға, осалдықтардың/қағидалардың өзекті базаларына ие болуға және есептерді электрондық түрде қалыптастыруды қамтамасыз етуге тиіс. Бастапқы кодты статикалық талдау құралына қойылатын талаптар және оны пайдаланудың заңдылығын растау тәртібі 6.14.1-6.14.10-тармақтарда белгіленген. 8.6. Қызметтерді Әлеуетті өнім берушінің білікті персоналы көрсетеді. Әлеуетті өнім берушіге қойылатын біліктілік және өзге де талаптар конкурстық құжаттамамен белгіленеді. 8.7. Тараптардың өзара іс-қимылы тағайындалған жауапты өкілдер арқылы жүзеге асырылады; жұмыс мәселелері кеңестердің хаттамаларымен немесе ресми хат алмасумен (оның ішінде электрондық пошта арқылы) тіркеледі. 9. Қызметтерді тапсыру-қабылдау тәртібі 9.1. Қызметтерді тапсыру-қабылдау қызметтер көрсету тұтастай аяқталғаннан кейін ұсынылған есептік құжаттар (7-бөлім) және Қазақстан Республикасының мемлекеттік сатып алу туралы заңнамасында белгіленген тәртіппен ресімделетін көрсетілген қызметтер актісі негізінде жүзеге асырылады. 9.2. Әлеуетті өнім беруші ескертулерді оларды алған күннен бастап 10 (он) жұмыс күні ішінде жояды. 9.3. Қызметтер 7-бөлімнің талаптарына сәйкес келетін есептік құжаттардың толық топтамасы ұсынылған және 6.12, 6.13 және 6.14-тармақтарда белгіленген өлшемшарттар орындалған кезде тиісінше көрсетілген болып есептеледі. 10. Қызметтер көрсету мерзімі мен орны 10.1. Қызметтер көрсету мерзімі: шарт жасалған күннен бастап 2026 жылғы 20 желтоқсанға дейін. 10.2. Қызметтер көрсету орны: Қазақстан, Астана қ., Есіл ауданы, Сығанақ к-сі, 70-ғимарат. Қатысуды талап ететін жұмыстар (физикалық қорғалуды тексеру, персоналды оқыту, қашықтан қолжетімділіксіз Тапсырыс беруші желісіндегі жұмыстар) Жүйе (Тапсырыс беруші) орналасқан жерде орындалады; қалған жұмыстар Тапсырыс берушімен келісу бойынша қашықтан орындалуы мүмкін.
--	--

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)	11. Қызметтер көрсету нәтижелері бойынша Әлеуетті өнім берушінің міндеттемелері 11.1. Әлеуетті өнім беруші қызметтер көрсету мерзімі шегінде анықталған сәйкессіздіктерді жою мәселелері бойынша Тапсырыс берушіні консультациялық сүйемелдеуді, оның ішінде олардың жойылуын қайта тексеруді қамтамасыз етеді. 11.2. Әлеуетті өнім беруші есептік құжаттардың толықтығы мен дұрыстығы және берілген ұсынымдардың негізділігі үшін жауапты болады. Тапсырыс берушінің көрсетілген қызметтер актісіне қол қойылғаннан кейін 30 (отыз) күнтізбелік күн ішінде анықталған есептік құжаттарға ескертулерін Әлеуетті өнім беруші қосымша ақысыз жояды. 11.3. Әлеуетті өнім берушінің міндеттемелері Жүйенің сынақтарға дайындығы туралы қорытынды есеп (7-бөлімнің 10-тармағы) бойынша көрсетілген қызметтер актісіне қол қойылған сәттен бастап толық көлемде орындалған болып есептеледі. Әлеуетті өнім беруші Тапсырыс берушінің (Жүйені әзірлеушінің) берілген ұсынымдарды жоймауы, қызметтер көрсету аяқталғаннан кейін Жүйенің құрамының немесе конфигурациясының өзгеруі, сондай-ақ Әлеуетті өнім берушіге ұсынылған деректер мен қолжетімділіктердің толық болмауы салдарынан туындаған сәйкессіздіктер үшін жауапты болмайды. 11.4. Әлеуетті өнім берушінің кепілдік міндеттемелері Егер осы техникалық ерекшеліктің 10.1-тармағында белгіленген қызметтер көрсету мерзімі аяқталғанға дейін осы техникалық ерекшелікте көзделген жекелеген іс-шаралар Тапсырыс берушіге байланысты емес себептер бойынша, оның ішінде анықталған сәйкессіздіктерді, осалдықтарды жою, Жүйені пысықтау, қайта тексерулер, сканерлеулер мен тестілеулер жүргізу қажеттілігіне байланысты аяқталмаған жағдайда, Әлеуетті өнім беруші кепілдік міндеттемелер шеңберінде 2027 жылғы 1 қарашаны қоса алғанға дейін Тапсырыс берушіден қосымша ақы алмай оларды одан әрі сүйемелдеуді және орындауды қамтамасыз етеді. 11.5. Кепілдік міндеттемелер анықталған сәйкессіздіктер мен осалдықтарды жоюды консультациялық сүйемелдеуге, осы техникалық ерекшелікте көзделген қайта тексерулерді, сканерлеулер мен тестілеулерді жүргізуге, Әлеуетті өнім беруші бұрын дайындаған есептік материалдарды өзектендіруге, сондай-ақ көрсетілген қызметтердің нәтижелеріне қатысты ескертулерді жоюға қолданылады. 11.6. Көрсетілген іс-шараларды кепілдік кезеңі ішінде орындауды Әлеуетті өнім беруші жасалған шарт бойынша қызметтердің құны есебінен жүзеге асырады және ол шарт құнының ұлғаюына, қосымша шарт жасасуға не Тапсырыс берушіде өзге де қаржылық міндеттемелердің туындауына әкеп соқпайды.
--	---

**Техническая спецификация
закупаемых услуг
(заполняется заказчиком)**

Наименование заказчика	Акционерное общество "Центр международных программ"
Наименование организатора	Акционерное общество "Центр международных программ"
№ конкурса:	№ 17792455-1
Наименование конкурса:	Услуги по подготовке к прохождению аттестации информационной безопасности МИС «е-Болашак»
Номер лота:	№ 88023749-ОК1
Наименование лота:	Услуги по диагностированию/экспертизе/анализу/испытаниям/тестированию/осмотру
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	712019.000.0000009
Наименование услуги:	Услуги по диагностированию/экспертизе/анализу/испытаниям/тестированию/осмотру
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	15000000
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	15000000
Срок оказания услуги:	по истечению 15 календарных дней с даты заключения договора и по 31 декабря 2026 года
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Параметр Значение Заказчик Акционерное общество «Центр международных программ», БИН 050440007456, Казахстан, г. Астана, район Есиль, ул. Сыганак, зд. 70. Наименование услуги (по ЕНС ТРУ) Услуги по диагностированию/экспертизе/анализу/испытаниям/тестированию/осмотру Характеристика услуги (по ЕНС ТРУ) Приведение объектов информатизации в соответствие требованиям информационной безопасности Код ЕНС ТРУ 712019.000.000009 Дополнительная характеристика Подготовка цифрового объекта «МИС е-Болашак» (далее — Система) к испытаниям на соответствие требованиям кибербезопасности, проводимым аккредитованной испытательной лабораторией в соответствии со статьёй 49 Закона Республики Казахстан «О кибербезопасности» Единица измерения / количество Одна услуга / 1 Способ закупки Открытый конкурс (веб-портал государственных закупок goszakur.gov.kz) Место оказания услуг Казахстан, г. Астана, район Есиль, ул. Сыганак, зд. 70. Отдельные виды услуг (удалённый анализ, сканирование, консультации) могут оказываться дистанционно по согласованию с Заказчиком Срок оказания услуг С даты заключения договора до 20 декабря 2026 года Условия оплаты по факту оказания услуг на основании акта оказанных услуг В настоящем документе представлена техническая спецификация, определяющая содержание, объём, условия оказания и требования к результатам услуг по подготовке цифрового объекта «МИС е-Болашак» (далее — Система, объект испытаний) к испытаниям на соответствие требованиям кибербезопасности. Предметом закупки является обследование Системы, выявление несоответствий требованиям кибербезопасности, подготовка рекомендаций, сопровождение устранения несоответствий, проверка выполненных исправлений и подготовка комплекта документов для официальных испытаний. Официальные испытания организуются и оплачиваются Заказчиком отдельно. Организация, проводящая официальные испытания, определяется в соответствии с законодательством Республики Казахстан и применимыми Правилами испытаний. 1.1. Термины Термин Определение Заказчик Акционерное общество «Центр международных программ» - собственник (владелец) Системы Потенциальный поставщик Физическое лицо, осуществляющее предпринимательскую деятельность, юридическое лицо (за исключением государственного учреждения, если иное не установлено законами Республики Казахстан), временное объединение юридических лиц (консорциум), претендующие на заключение договора о государственных закупках Система (объект испытаний) Цифровой объект «МИС е-Болашак», включая прикладное ПО, базы данных, среду виртуализации, серверное и сетевое оборудование, обеспечивающие его функционирование Кибербезопасность (КБ) Состояние защищённости цифровых объектов от нарушения их конфиденциальности, целостности или доступности. В НПА и стандартах, принятых до 2026 года, применяется термин «информационная безопасность» (ИБ); для целей настоящей технической спецификации термины равнозначны Испытания Испытания цифрового объекта на соответствие требованиям КБ в соответствии со статьёй 49 Закона
---	---

	РК «О кибербезопасности» и Методикой и Правилами испытаний Лаборатория Аккредитованная испытательная лаборатория (государственная техническая служба), проводящая испытания Единые требования Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утверждённые постановлением Правительства РК от 20 декабря 2016 года № 832 Методика и Правила испытаний Методика и правила проведения испытаний цифровых объектов «цифрового правительства» и критически важных цифровых объектов на соответствие требованиям кибербезопасности, утверждённые приказом от 3 июня 2019 года № 111/НҚ Правила мониторинга Правила проведения мониторинга обеспечения кибербезопасности цифровых объектов «цифрового правительства» и критически важных цифровых объектов, утверждённые приказом от 28 марта 2018 года № 52/НҚ Несоответствие Отклонение состояния Системы, её конфигурации, документации или процессов от требований НПА и стандартов, указанных в разделе 3 Уязвимость Недостаток ПО, конфигурации или архитектуры, который может быть использован для нарушения КБ Конечная точка Рабочая станция или сервер Заказчика, на который устанавливается агент системы EDR Средство статического анализа Программное средство класса SAST, применяемое Потенциальным поставщиком для анализа исходного кода Системы (пункт 6.14) 1.2. Сокращения Сокращение Расшифровка БИН Бизнес-идентификационный номер ЕНС ТРУ Единый номенклатурный справочник товаров, работ и услуг ИБ Информационная безопасность (термин НПА и стандартов, принятых до 2026 года; см. «Кибербезопасность») КБ Кибербезопасность МЭ Межсетевой экран НДВ Недекларированные возможности программного обеспечения НПА Нормативный правовой акт ОС Операционная система ОУД Оценочный уровень доверия по СТ РК ISO/IEC 15408-3-2017 ОЦИБ Оперативный центр информационной безопасности (оперативный центр кибербезопасности) ПО Программное обеспечение РК Республика Казахстан СЗИ Средства защиты информации СТ РК Национальный стандарт Республики Казахстан СУБД Система управления базами данных API, REST API Программный интерфейс приложения (Application Programming Interface); REST API — программный интерфейс, построенный по архитектурному стилю REST CI/CD Непрерывная интеграция и доставка (Continuous Integration / Continuous Delivery) CVE Common Vulnerabilities and Exposures — реестр общеизвестных уязвимостей CVSS Common Vulnerability Scoring System — система оценки критичности уязвимостей (применяется версия 3.1 или новее) CWE, CWE/SANS Common Weakness Enumeration — классификация недостатков ПО; CWE/SANS Top 25 — перечень наиболее опасных недостатков ПО EDR Endpoint Detection and Response — система выявления и реагирования на угрозы на конечных точках EXE, DLL Исполняемые файлы и динамические библиотеки ОС Windows HIPAA Health Insurance Portability and Accountability Act — стандарт защиты медицинских данных (США); используется как один из шаблонов отчётности средства статического анализа HIPS Host Intrusion Prevention
--	--

	System — система предотвращения вторжений на уровне хоста HTTP/HTTPS, POP3/POP3S, SMTP, IMAP/IMAPS, SMB, RPC, RDP, SSL Сетевые протоколы: передачи гипертекста (в том числе защищённой), приёма и отправки электронной почты, доступа к файлам, удалённого вызова процедур, удалённого рабочего стола, защищённого транспортного уровня IDS Intrusion Detection System — система обнаружения вторжений JAR, WAR, EAR, AAR, APK, IPA, APP Форматы пакетов (архивов) скомпилированных приложений Java/Scala, Android, iOS и macOS MITRE ATT&CK; База знаний о тактиках и техниках злоумышленников, поддерживаемая корпорацией MITRE OWASP Top 10, OWASP Mobile Top 10, OWASP MASVS Перечни наиболее критичных рисков безопасности веб- и мобильных приложений и стандарт верификации безопасности мобильных приложений проекта OWASP PCI DSS Payment Card Industry Data Security Standard — стандарт безопасности данных индустрии платёжных карт SARIF Static Analysis Results Interchange Format — формат обмена результатами статического анализа SAST Static Application Security Testing — статический анализ защищённости исходного кода приложений SIEM Security Information and Event Management — система управления событиями и информацией безопасности SOAR Security Orchestration, Automation and Response — система оркестрации, автоматизации и реагирования на инциденты UEFI Unified Extensible Firmware Interface — интерфейс встроенного ПО (загрузчика) компьютера URL Uniform Resource Locator — адрес ресурса в сети Интернет VDI Virtual Desktop Infrastructure — инфраструктура виртуальных рабочих столов WMI Windows Management Instrumentation — инструментарий управления ОС Windows Git, SVN Системы контроля версий исходного кода CSV, HTML, PDF, XML, YAML Форматы файлов: значения, разделённые запятыми; язык гипертекстовой разметки; переносимый формат документов; расширяемый язык разметки; формат сериализации данных 2. Цель оказания услуг Цель оказания услуг — приведение Системы в соответствие требованиям кибербезопасности, установленным нормативными правовыми актами Республики Казахстан и действующими на территории Республики Казахстан стандартами, и подготовка Системы к успешному прохождению испытаний в Лаборатории. Для достижения цели Потенциальный поставщик выполняет комплекс аналитических, консультационных и инструментальных работ по оценке соответствия Системы требованиям технической документации, нормативных правовых актов и стандартов в сфере КБ, выявлению несоответствий и уязвимостей, сопровождению их устранения силами Заказчика (разработчика Системы) и подготовке комплекта документов и сведений для представления в Лабораторию. 3. Нормативные правовые акты и стандарты 3.1. Услуги оказываются в соответствии со следующими нормативными правовыми актами и стандартами (в редакциях, действующих на дату оказания услуг): 3.1.1. Цифровой кодекс Республики Казахстан от 9 января 2026 года № 255-VIII; 3.1.2. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «О кибербезопасности» (в том числе статьи 49
--	---

	«Испытания на соответствие требованиям кибербезопасности», 50 «Аудит кибербезопасности», глава 9 «Защита цифровых объектов»); 3.1.3. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»; 3.1.4. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»; 3.1.5. Приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года № 111/НК «Об утверждении методики и правил проведения испытаний цифровых объектов «цифрового правительства» и критически важных цифровых объектов на соответствие требованиям кибербезопасности»; 3.1.6. Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НК «Об утверждении Правил проведения мониторинга обеспечения кибербезопасности цифровых объектов «цифрового правительства» и критически важных цифровых объектов»; 3.1.7. СТ РК ISO/IEC 27001-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования»; 3.1.8. СТ РК ISO/IEC 27002-2023 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью»; 3.1.9. СТ РК ISO/IEC 27005-2022 (менеджмент рисков информационной безопасности); 3.1.10. СТ РК ISO/IEC 15408-1-2017, СТ РК ISO/IEC 15408-2-2017, СТ РК ISO/IEC 15408-3-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (части 1-3); 3.1.11. СТ РК 2199-2012 (требования к безопасности веб-приложений); 3.1.12. Иные обязательные требования законодательства Республики Казахстан, непосредственно применимые к Системе с учётом её категории, назначения, состава обрабатываемых данных и условий эксплуатации. Потенциальный поставщик указывает конкретный нормативный правовой акт, пункт требования и основание его применимости в матрице соответствия. Дополнительные добровольные стандарты применяются по согласованию с Заказчиком. 4. Объект оказания услуг 4.1. Объектом оказания услуг является многофункциональная информационная система «е-Болашак» АО «Центр международных программ» (далее — МИС «е-Болашак»), относящаяся к объектам «цифрового правительства» и интегрируемая с государственными информационными системами и иными цифровыми объектами, собственником (владельцем) которого является Заказчик, размещённый в собственном серверном помещении Заказчика по адресу: ул. Сыганак, зд. 70 и в центре обработки данных QazTech. 4.2. Услуги оказываются в отношении Системы в полном составе — прикладного программного обеспечения, баз данных, среды виртуализации, серверного и сетевого оборудования, средств защиты информации, автоматизированных рабочих мест администраторов и всех иных компонентов, обеспечивающих функционирование Системы, — независимо от их
--	---

	количества. Количество серверов, виртуальных машин, сетевых устройств и иных компонентов не является основанием для изменения объёма и стоимости услуг. 4.3. Фактический состав компонентов Системы уточняется Потенциальным поставщиком на этапе 1 (раздел 5) на основании документации и сведений, предоставляемых Заказчиком, и фиксируется в отчёте об обследовании (раздел 7). 5. Состав и этапы оказания услуг 5.1. Оказание услуг разделяется на следующие этапы: № Этап Содержание Результат (отчётные документы) 1 Анализ (обследование) КБ инфраструктуры Системы Сбор исходных данных, анализ архитектуры, конфигураций, журналирования, физической защиты, инструментальное сканирование, нагрузочное тестирование, анализ исходного кода (пункты 6.1, 6.3, 6.5, 6.7, 6.9, 6.10, 6.13, 6.14) Отчёт об обследовании; отчёты по сканированию, нагрузочному тестированию и анализу исходного кода 2 Выявление несоответствий и выдача рекомендаций Сопоставление результатов обследования с требованиями раздела 3, формирование перечня несоответствий и уязвимостей с приоритизацией и рекомендациями по устранению (пункты 6.2, 6.4, 6.6, 6.8, 6.15) Перечень несоответствий и план мероприятий по их устранению 3 Консультационное сопровождение устранения несоответствий Консультации Заказчика и разработчика Системы при устранении несоответствий, контрольные (повторные) проверки, подготовка комплекта документов для представления в Лабораторию (пункты 6.11, 6.12, 6.16, 6.17) Отчёты по повторным проверкам; итоговый отчёт о готовности Системы к испытаниям 4 Повышение осведомлённости персонала Заказчика Консультирование и инструктаж администраторов Системы и ответственных за КБ лиц Заказчика по выявленным несоответствиям, применённым мерам защиты и порядку подготовки к испытаниям — в ходе выполнения пунктов 6.2, 6.4, 6.6, 6.8, 6.11, 6.15, 6.17 Протоколы консультаций (фиксируются в отчётах по соответствующим пунктам) 5.2. Календарные сроки этапов определяются планом-графиком оказания услуг, который Потенциальный поставщик представляет Заказчику на согласование в течение 10 рабочих дней с даты заключения договора. Этапы могут выполняться параллельно, если это не противоречит логике работ. 6. Подробное описание услуг Потенциальный поставщик в рамках оказания услуг должен выполнить следующее: 6.1. Анализ безопасности функционала прикладного программного обеспечения, базы данных (совместно с разработчиком Системы), среды виртуализации и операционных систем серверного оборудования на соответствие Единым требованиям и СТ РК ISO/IEC 27002-2023, включая: управление учётными записями и правами доступа, парольную политику и многофакторную аутентификацию, управление обновлениями, отключение неиспользуемых служб и портов, защиту каналов взаимодействия компонентов, конфигурацию резервного копирования. 6.2. Консультации по настройке (усилению защищённости) прикладного программного обеспечения, базы данных (совместно с разработчиком Системы), среды виртуализации и операционных систем серверного оборудования в
--	---

	соответствии с требованиями по КБ, с выдачей письменных рекомендаций по каждому выявленному несоответствию. 6.3. Анализ журналирования событий прикладного программного обеспечения, базы данных (совместно с разработчиком Системы), среды виртуализации и операционных систем серверного оборудования: состав регистрируемых событий, полнота, сроки хранения, защита журналов от изменения, синхронизация времени. 6.4. Консультации по настройке журналирования событий прикладного программного обеспечения, базы данных, среды виртуализации и операционных систем серверного оборудования в соответствии с Правилами мониторинга и Едиными требованиями, включая требования к передаче событий в систему мониторинга обеспечения КБ. 6.5. Анализ конфигурации сетевого оборудования (межсетевые экраны, маршрутизаторы, коммутаторы, средства удалённого доступа): сегментация сети, правила фильтрации трафика, защита интерфейсов управления, используемые протоколы, учётные записи. 6.6. Консультации по настройке сетевого оборудования в соответствии с Едиными требованиями, с выдачей письменных рекомендаций. 6.7. Анализ журналирования событий сетевого оборудования. 6.8. Консультации по настройке журналирования событий сетевого оборудования в соответствии с Правилами мониторинга и Едиными требованиями. 6.9. Проверка физической защиты серверного помещения (выезд Потенциального поставщика по месту размещения Системы): контроль и учёт доступа, охранный и пожарный сигнализация, пожаротушение, климатическое оборудование, бесперебойное электропитание, размещение оборудования, ведение журналов посещений — на соответствие Единым требованиям; по результатам — отчёт с перечнем несоответствий и рекомендациями по их устранению. 6.10. Инструментальное сканирование серверов, сетевого оборудования и веб-приложения Системы на наличие уязвимостей в режимах аудита (с использованием учётных записей, предоставленных Заказчиком) и тестирования на проникновение (без учётных записей, с внешнего и внутреннего периметра) с использованием средства анализа защищённости с актуальной базой уязвимостей, а также ручное тестирование на проникновение в согласованных границах. Выявленные уязвимости классифицируются по уровню критичности в соответствии с CVSS версии 3.1 или новее; по каждой уязвимости выдаются рекомендации по устранению. Сканирование проводится в согласованные с Заказчиком временные окна. 6.11. Совместная с Заказчиком (разработчиком Системы) отработка устранения уязвимостей, выявленных по результатам сканирования серверов, сетевого оборудования и веб-приложения: консультации по способам устранения, проверка применённых мер. 6.12. Повторное инструментальное сканирование на наличие уязвимостей в режимах аудита и тестирования на проникновение после устранения уязвимостей. Критерий завершения: отсутствие уязвимостей критического и высокого уровня (базовая оценка CVSS 7,0 и выше). Для блокирующих несоответствий предусмотреть статус «не готова» и перечень необходимых действий. 6.13. Нагрузочное тестирование
--	--

	Системы для определения пиковой нагрузки по методике, согласованной с Заказчиком (сценарии, количество одновременных пользователей, интенсивность запросов, контролируемые показатели: время отклика, доля ошибок, использование ресурсов), с выдачей рекомендаций по оптимизации; после реализации рекомендаций — повторное нагрузочное тестирование с сопоставлением результатов. 6.14. Анализ исходного кода Системы средством статического анализа (SAST) на наличие уязвимостей и недекларированных возможностей (НДВ), с классификацией результатов (CWE, OWASP Top 10) и выдачей рекомендаций по устранению; после устранения выявленных недостатков — повторный анализ с сопоставлением результатов. Исходный код предоставляется Заказчиком (разработчиком Системы). Анализ выполняется Потенциальным поставщиком с использованием собственного средства статического анализа на своей площадке — без развёртывания средства анализа в инфраструктуре Заказчика и без передачи Заказчику лицензий на него; результатом является отчёт о сканировании (первичный и повторный), оформленный в соответствии с пунктом 6.14.5 и разделом 7. Применяемое Потенциальным поставщиком средство статического анализа должно соответствовать требованиям пунктов 6.14.1-6.14.10. Средство статического анализа исходного кода, применяемое Потенциальным поставщиком при выполнении пункта 6.14, должно соответствовать следующим минимальным требованиям: 6.14.1. Общие функциональные требования: анализ программного обеспечения на соответствие требованиям КБ по исходному коду; анализ по байт-коду (бинарному коду) методом статического анализа при отсутствии исходных кодов и отладочной информации; поиск недекларированных возможностей (НДВ); выдача по результатам анализа рекомендаций по настройке средств защиты информации (СЗИ) для тех уязвимостей и НДВ, эксплуатация которых может быть предотвращена настройкой СЗИ. 6.14.2. Методы анализа: поиск уязвимостей и НДВ должен осуществляться с применением, как минимум, следующих методов статического анализа: анализ по шаблонам; анализ потока управления; taint-анализ (анализ потоков данных); анализ синонимов; распространение констант. Методы применяются к внутреннему представлению, в которое транслируется исходный (байт-) код. 6.14.3. Анализ по исходному коду: поддержка языков программирования: Java, JavaScript, TypeScript, PHP, Python, C#, Go, PL/SQL, T-SQL, HTML5, SQL, Bash, PowerShell, XML, YAML; анализ мультязычных проектов с автоматическим распознаванием языков; интеграция со средствами сборки. 6.14.4. Анализ по бинарному (байт-) коду при наличии в Системе компонентов, исходный код которых недоступен: анализ байт-кода, полученного трансляцией из языков Java/Scala (JAR, WAR, EAR, AAR), C/C++ (DLL, EXE), Android (APK), Apple iOS (IPA), Apple macOS (APP), с применением методов пункта 6.14.2. 6.14.5. Результаты и отчётность: формирование отчётов на русском и английском языках в форматах CSV, HTML, PDF и SARIF; отчёты о соответствии стандартам и классификациям PCI DSS, OWASP Top 10,
--	--

	OWASP Mobile Top 10, HIPAA, CWE/SANS, OWASP MASVS; по каждой уязвимости и НДВ — описание, степень критичности, место в коде (в том числе при отсутствии исходного кода), объяснение опасности и возможных способов эксплуатации, рекомендации по исправлению, ссылки на внешние источники и классификацию; история сканирований и сравнение результатов сканирований проекта (для подтверждения устранения недостатков по результатам повторного анализа); расчёт метрик безопасности приложения и сводная статистика по степени критичности; настройка состава отчёта (выбор приложений и категорий уязвимостей). 6.14.6. Интерфейс и роли: единая точка доступа к информации; интерфейс на русском и английском языках; ролевое разграничение функций не менее чем для категорий пользователей «администратор», «офицер безопасности», «разработчик», «руководитель»; загрузка приложения для анализа и указание пути к репозиторию и ветке разработки; управление пользователями и их правами в интерфейсе администратора. По запросу Заказчика Потенциальный поставщик демонстрирует результаты анализа в интерфейсе средства (в том числе дистанционно). 6.14.7. Интеграция: поддержка загрузки анализируемого кода из систем контроля версий (Git, SVN) и в виде архива; поддержка интеграции с сервисами непрерывной интеграции (CI/CD) и системами отслеживания ошибок; наличие открытого API. Интеграция с инфраструктурой разработчика Системы в рамках настоящих услуг не выполняется. 6.14.8. Безопасность средства анализа: разграничение доступа по уровням иерархии в соответствии с правами, настраиваемыми администратором; доступ к функциям пользователя и администратора только по индивидуальным учётным данным; хранение паролей в зашифрованном (хешированном) виде; ограничение количества неверных попыток ввода учётных данных с настраиваемым порогом; настраиваемые требования к регулярной смене пароля и сроку его действия; автоматическое завершение сеанса при неактивности пользователя; полное журналирование действий пользователей и администраторов. 6.14.9. Размещение и обращение с исходным кодом: средство анализа размещается на площадке Потенциального поставщика на территории Республики Казахстан и в инфраструктуре Заказчика не развёртывается; исходный код Системы передаётся Заказчиком (разработчиком Системы) Потенциальному поставщику по защищённому каналу либо на носителе по акту приёма-передачи, хранится в изолированной среде Потенциального поставщика, не передаётся третьим лицам и не загружается в облачные сервисы за пределами Республики Казахстан; по завершении оказания услуг копии исходного кода, находящиеся у Потенциального поставщика, уничтожаются в порядке пункта 8.4 с письменным подтверждением. 6.14.10. Подтверждение правомерности использования: Потенциальный поставщик применяет средство статического анализа на законных основаниях (лицензия, подписка или иное право использования). Потенциальный поставщик в составе конкурсной заявки должен приложить авторизационное письмо от производителя (правообладателя)
--	---

	средства статического анализа, оформленное на имя Заказчика, с указанием наименования и номера лота (закупки), наименования и версии средства анализа, а также подтверждением права Потенциального поставщика на его использование при оказании услуг Заказчику. В случае текста письма на иностранном языке письмо должно быть нотариально заверено и переведено на казахский или русский языки. 6.15. Анализ действующей технической документации Заказчика по КБ (политика КБ, правила и регламенты, предусмотренные Едиными требованиями, документация на Систему) на полноту и соответствие требованиям раздела 3 и перечню документов, запрашиваемых Лабораторией; консультации по её актуализации и подготовка проектов недостающих документов. 6.16. Потенциальный поставщик по официальному запросу Заказчика должен оснастить инфраструктуру Заказчика системой выявления и реагирования на угрозы на конечных точках (EDR) (далее — система EDR) в объёме не менее 25 (двадцати пяти) лицензий (агентов EDR на защищаемых конечных точках — рабочих станциях и серверах), со сроком действия лицензий не менее чем до 31 декабря 2026 года. Система EDR должна включать средства централизованного управления, компоненты защиты рабочих станций и серверов и модуль выявления и реагирования, соответствующие требованиям пунктов 6.16.1-6.16.10. Серверные компоненты развёртываются в инфраструктуре Заказчика (локальное размещение). В объём услуг по настоящему пункту входят: передача прав использования (лицензий) на систему EDR; установка и настройка серверных компонентов; развёртывание агентов на конечных точках Заказчика; базовая настройка политик защиты и правил выявления; инструктаж администраторов Заказчика по эксплуатации системы; техническая поддержка производителя в течение срока действия лицензий. Система EDR, поставляемая по пункту 6.16, должна соответствовать следующим минимальным требованиям: 6.16.1. Общие требования: интерфейс всех компонентов, включая консоль управления, контекстная справка и эксплуатационная документация (в том числе руководство администратора с описанием установки, настройки и эксплуатации) — на русском и английском языках; техническая поддержка производителя на русском языке по телефону и электронной почте, при необходимости — с выездом к Заказчику; наличие у производителя раздела технической поддержки и базы знаний на веб-сайте. 6.16.2. Консоль централизованного управления: управление защитой всей инфраструктуры из единого веб-интерфейса по соединению, защищённому сертификатом; иерархия главного и подчинённых серверов управления; инвентаризация оборудования и программного обеспечения конечных точек под управлением Windows, Linux и macOS; удалённая установка и удаление агентов, компонентов защиты и стороннего ПО, формирование установочных пакетов с предустановленной конфигурацией (в том числе для изолированных сетей); статические и динамические группы с автоматическим назначением политик и задач, импорт структуры компьютеров, пользователей и групп из Active Directory;
--	---

	встроенные и пользовательские политики с экспортом и импортом; ролевое разграничение прав администраторов, аутентификация через группы Active Directory, двухфакторная аутентификация администраторов; журнал аудита всех действий и изменений конфигурации; панель мониторинга и настраиваемые отчёты (PDF, CSV) с отправкой по расписанию на электронную почту; интеграция с SIEM через syslog и REST API; локальное зеркало обновлений для сетей без доступа в Интернет; независимый агент управления с механизмами самозащиты, автоматическим обновлением и управлением из командной строки; поддержка сред VDI; поддержка актуальных версий Windows, Linux и macOS, находящихся в жизненном цикле поддержки производителей ОС. 6.16.3. Защита рабочих станций: защита от вирусов, троянских, шпионских и рекламных программ, фишинга, потенциально нежелательных и опасных программ, руткитов — в режиме реального времени, по требованию и по расписанию, включая сканирование при запуске ОС, загрузочных секторов и UEFI, реестра и WMI, оперативной памяти; сочетание сигнатурного анализа, эвристики и машинного обучения; защита от эксплойтов, поведенческая защита от программ-вымогателей, система предотвращения вторжений на хосте (HIPS) с пользовательскими правилами, проверка репутации процессов в облачной базе производителя; контроль внешних устройств по типу, производителю, модели и серийному номеру с привязкой к пользователям и группам домена и временным интервалам; проверка почтового трафика (POP3/POP3S, SMTP, IMAP/IMAPS) и вложений; проверка HTTP/HTTPS-трафика с контролем SSL-сертификатов, блокировкой фишинговых ресурсов, серверов ботнетов и управляющих серверов, списками URL; персональный брандмауэр с профилями сетей, модулем обнаружения сетевых атак (IDS) и защитой от эксплуатации уязвимостей сетевых протоколов (SMB, RPC, RDP) с указанием CVE; веб-контроль по категориям для пользователей и групп домена; обновление баз не реже 24 раз в сутки, из локального зеркала и резервных источников, с возможностью отката; защита настроек паролем; удалённая установка; поддержка Windows 10/11 и распространённых дистрибутивов Linux. 6.16.4. Защита серверов: автоматическое определение ролей сервера с созданием соответствующих исключений; защита в реальном времени, по требованию и по расписанию с теми же механизмами обнаружения, что для рабочих станций (пункт 6.16.3), включая защиту от эксплойтов и программ-вымогателей, HIPS, сканирование UEFI и оперативной памяти; сканирование виртуальных машин Hyper-V без установки агентов; контроль внешних устройств; проверка почтового и веб-трафика; работа в кластерах домена и рабочей группы; настройка числа потоков сканирования; режим без графического интерфейса для терминальных серверов; защита паролем от изменения параметров и удаления; удалённая установка; поддержка Windows Server 2016–2025 и распространённых серверных дистрибутивов Linux (Red Hat Enterprise Linux, Ubuntu, Debian, SUSE Linux Enterprise Server, Oracle Linux, Rocky/Alma Linux). 6.16.5. Модуль
--	---

	выявления и реагирования (EDR) — выявление: сбор телеметрии с конечных точек через коннектор (агент), управляемый сервером EDR, с локальным хранением данных; выявление аномального поведения на основе правил (набор правил по умолчанию и собственные правила, редактируемые в XML), а не только сигнатурного обнаружения; автоматическая классификация предупреждений по уровню критичности, приоритизация и группировка (по типу, компьютеру, правилу, процессу, файлу); карточка обнаружения со сводной информацией (время, компьютер, пользователь, исполняемый файл, инициировавший процесс), описанием события, возможными причинами, рисками и рекомендациями; сопоставление с техниками MITRE ATT&CK; анализ первопричин и полное дерево процессов с детализацией изменений файловой системы, реестра, сетевых соединений и URL; автоматическая классификация исполняемых файлов (EXE/DLL) и скриптов по критичности; фильтры по репутации, распространённости, цифровой подписи и поведению для выявления целенаправленных атак; инвентаризация всех исполняемых файлов и скриптов на конечных точках; поиск по всей базе телеметрии по любым параметрам (включая фрагменты командной строки) с сохранением поисковых задач; панель мониторинга аномальных событий. 6.16.6. Модуль выявления и реагирования (EDR) — реагирование: блокировка исполняемых файлов по контрольной сумме на всех конечных точках, чёрные и белые списки, детализированные исключения (контрольная сумма, путь, цифровая подпись); удалённое удаление и помещение файлов в карантин; изоляция скомпрометированного устройства от сети и вывод из изоляции в один клик; удалённая перезагрузка и выключение; запуск углублённого сканирования; создание снимка состояния ОС (процессы, сетевые соединения, реестр, планировщик, пользователи и привилегии, критичные файлы); загрузка подозрительных файлов и скриптов с конечных точек для анализа и их проверка на внешних репутационных сервисах из консоли; назначение тегов объектам для фильтрации; программный интерфейс (API) для интеграции с SIEM, SOAR и системами обработки задач; двухфакторная аутентификация администраторов; поддержка коннектором Windows 10/11, распространённых дистрибутивов Linux и macOS. 6.16.7. Расширенный анализ в облаке (при наличии в составе поставляемых лицензий): автоматическая и ручная отправка подозрительных файлов с рабочих станций и серверов на анализ в облачную песочницу производителя с применением машинного обучения; блокировка угроз нулевого дня по результатам первичного анализа (от нескольких секунд до 6 минут) и при длительном наблюдении; настраиваемые политики отправки и хранения образцов; отчёты о результатах анализа. 6.16.8. Оценочный уровень доверия: программный продукт системы EDR должен иметь оценочный уровень доверия (ОУД) не ниже 4 по СТ РК ISO/IEC 15408-3-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты». Заказчик вправе потребовать от
--	--

	Потенциального поставщика в течение 3 (трёх) рабочих дней с даты запроса сертификат соответствия (документ, подтверждающий соответствие) программного продукта требованиям СТ РК ISO/IEC 15408-3-2017 с указанием оценочного уровня доверия не ниже 4. 6.16.9. Потенциальный поставщик в составе конкурсной заявки должен приложить авторизационное письмо производителя (правообладателя) системы EDR, оформленное на имя Заказчика, с указанием наименования и версии программного продукта, количества и срока действия лицензий, а также подтверждением права Потенциального поставщика на передачу прав использования (поставку лицензий) и оказание технической поддержки на территории Республики Казахстан. В случае текста письма на иностранном языке письмо должно быть нотариально заверено и переведено на казахский или русский языки; 6.16.10. Передаваемые документы: по результатам развёртывания Потенциальный поставщик передаёт Заказчику лицензионные документы (ключи/сертификаты активации) с указанием количества и срока действия лицензий, эксплуатационную документацию и акт установки и настройки системы EDR с перечнем защищённых конечных точек. 6.17. Оказание содействия Заказчику при ведении переписки с государственными органами, Лабораторией и разработчиком Системы по вопросам подготовки к испытаниям, в том числе подготовка проектов заявки на проведение испытаний и комплекта прилагаемых документов в соответствии с Методикой и Правилами испытаний — для последующего представления Заказчиком в Лабораторию. 7. Требования к результатам и отчётным документам 7.1. По результатам оказания услуг Потенциальный поставщик представляет Заказчику следующие отчётные документы: № Документ Требования к содержанию / срок 1 План-график оказания услуг Этапы, сроки, ответственные, перечень необходимых от Заказчика данных и доступов. В течение 10 рабочих дней с даты заключения договора 2 Отчёт об обследовании КБ Системы Описание архитектуры и периметра обследования; результаты анализа по пунктам 6.1, 6.3, 6.5, 6.7, 6.9; оценка соответствия требованиям раздела 3 3 Перечень несоответствий и план мероприятий по их устранению Каждое несоответствие: описание, ссылка на требование НПА/стандарта, уровень критичности, рекомендация, ответственная сторона, ориентировочный срок 4 Отчёты по сканированию на уязвимости (первичный и повторный) Периметр, режимы, перечень уязвимостей с оценкой CVSS, рекомендации; сравнение результатов первичного и повторного сканирования; экспорт из средства сканирования 5 Отчёты по нагрузочному тестированию (первичный и повторный) Методика, сценарии, полученные показатели, определённая пиковая нагрузка, рекомендации, сравнение результатов 6 Отчёты о сканировании исходного кода (первичный и повторный) Периметр (перечень модулей, ветка/версия кода, контрольные суммы переданных архивов), средство анализа и его версия, выявленные уязвимости и НДВ с классификацией и степенью критичности, рекомендации по устранению, сравнение результатов первичного и повторного сканирования;
--	--

	выгрузка из средства анализа в формате PDF и SARIF/CSV 7 Отчёт о проверке физической защиты серверного помещения Результаты проверки по пункту 6.9, фотофиксация по согласованию с Заказчиком, несоответствия и рекомендации 8 Заключение по документации по КБ Перечень имеющихся и недостающих документов, замечания, рекомендации по актуализации, проекты документов 9 Документы по системе EDR (при оснащении по запросу Заказчика, пункт 6.16) Лицензионные документы (ключи/сертификаты активации) с указанием количества и срока действия лицензий; эксплуатационная документация; акт установки и настройки с перечнем защищённых конечных точек (пункт 6.16.10); по запросу Заказчика — сертификат соответствия СТ РК ISO/IEC 15408-3-2017 с ОУД не ниже 4 и авторизационное письмо производителя (пункты 6.16.8, 6.16.9) 10 Итоговый отчёт о готовности Системы к испытаниям Сводные результаты, статус устранения несоответствий, перечень принятых рисков, комплект документов для представления в Лабораторию 7.2. Отчётные документы представляются на русском языке или на казахском языке по требованию Заказчика в электронном виде (в формате PDF и в редактируемом формате) и, по требованию Заказчика, на бумажном носителе в 1 (одном) экземпляре. Отчётные документы, содержащие сведения об уязвимостях и конфигурациях, передаются по защищённым каналам либо на носителе под роспись. 8. Условия оказания услуг 8.1. Заказчик в согласованные планом-графиком сроки предоставляет Потенциальному поставщику: техническую документацию на Систему, схемы сети, перечень компонентов, учётные записи и доступы, необходимые для выполнения работ, доступ в серверное помещение в сопровождении представителя Заказчика, а также контактные лица со стороны Заказчика и разработчика Системы. 8.2. Работы, способные повлиять на доступность Системы (инструментальное сканирование, нагрузочное тестирование), выполняются только в согласованные с Заказчиком временные окна, после письменного уведомления и при условии наличия у Заказчика актуальной резервной копии Системы. Нагрузочное тестирование проводится на тестовом стенде / в промышленной среде вне часов пиковой нагрузки. 8.3. При проведении работ не допускается эксплуатация уязвимостей с деструктивным воздействием, изменение или удаление данных Заказчика, внесение изменений в конфигурацию Системы без согласования с Заказчиком. Все изменения выполняются Заказчиком (разработчиком Системы) на основании рекомендаций Потенциального поставщика либо Потенциальным поставщиком по письменному поручению Заказчика. 8.4. Потенциальный поставщик обеспечивает конфиденциальность всей информации, полученной в ходе оказания услуг, в том числе сведений об уязвимостях, конфигурациях и персональных данных, в соответствии с законодательством Республики Казахстан; до начала работ стороны подписывают соглашение о неразглашении. Результаты оказания услуг являются собственностью Заказчика; по завершении оказания услуг Потенциальный поставщик уничтожает копии данных Заказчика, полученных в ходе
--	---

	работ, с подтверждением. 8.5. Используемые Потенциальным поставщиком средства анализа защищённости, нагрузочного тестирования и анализа исходного кода должны применяться на законных основаниях (лицензионные либо свободно распространяемые), иметь актуальные базы уязвимостей/правил и обеспечивать формирование отчётов в электронном виде. Требования к средству статического анализа исходного кода и порядок подтверждения правомерности его использования установлены пунктами 6.14.1-6.14.10. 8.6. Услуги оказываются квалифицированным персоналом Потенциального поставщика. Квалификационные и иные требования к потенциальному поставщику устанавливаются конкурсной документацией. 8.7. Взаимодействие сторон осуществляется через назначенных ответственных представителей; рабочие вопросы фиксируются протоколами совещаний или официальной перепиской (в том числе по электронной почте). 9. Порядок сдачи-приёмки услуг 9.1. Сдача-приёмка услуг осуществляется по завершении оказания услуг в целом на основании представленных отчётных документов (раздел 7) и акта оказанных услуг, оформляемого в порядке, установленном законодательством Республики Казахстан о государственных закупках. 9.2. Потенциальный поставщик устраняет замечания в течение 10 (десяти) рабочих дней с даты их получения. 9.3. Услуги считаются оказанными надлежащим образом при представлении полного комплекта отчётных документов, соответствующих требованиям раздела 7, и выполнении критериев, установленных пунктами 6.12, 6.13 и 6.14. 10. Срок и место оказания услуг 10.1. Срок оказания услуг: с даты заключения договора до 20 декабря 2026 года. 10.2. Место оказания услуг: Казахстан, г. Астана, район Есиль, ул. Сыганак, зд. 70. Работы, требующие присутствия (проверка физической защиты, обучение персонала, работы в сети Заказчика без удалённого доступа), выполняются по месту размещения Системы (Заказчика); остальные работы могут выполняться дистанционно
--	---

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)	11. Обязательства Потенциального поставщика по результатам оказания услуг 11.1. Потенциальный поставщик в пределах срока оказания услуг обеспечивает консультационное сопровождение Заказчика по вопросам устранения выявленных несоответствий, включая повторные проверки их устранения. 11.2. Потенциальный поставщик несёт ответственность за полноту и достоверность отчётных документов и обоснованность выданных рекомендаций. Замечания Заказчика к отчётным документам, выявленные в течение 30 (тридцати) календарных дней после подписания акта оказанных услуг, устраняются Потенциальным поставщиком без дополнительной оплаты. 11.3. Обязательства Потенциального поставщика считаются исполненными в полном объёме с момента подписания акта оказанных услуг по итоговому отчёту о готовности Системы к испытаниям (пункт 10 раздела 7). Потенциальный поставщик не несёт ответственности за несоответствия, возникшие вследствие неустранения Заказчиком (разработчиком Системы) выданных рекомендаций, изменений состава или конфигурации Системы после завершения оказания услуг, а также неполноты предоставленных Потенциальному поставщику данных и доступов. 11.4. Гарантийные обязательства Потенциального поставщика В случае если до окончания срока оказания услуг, установленного пунктом 10.1 настоящей технической спецификации, отдельные мероприятия, предусмотренные настоящей технической спецификацией, не могут быть завершены по причинам, не зависящим от Заказчика, в том числе в связи с необходимостью устранения выявленных несоответствий, уязвимостей, доработки Системы, проведения повторных проверок, сканирований и тестирований, Потенциальный поставщик в рамках гарантийных обязательств обеспечивает их дальнейшее сопровождение и выполнение без взимания дополнительной платы с Заказчика до 1 ноября 2027 года включительно. 11.5. Гарантийные обязательства распространяются на консультационное сопровождение устранения выявленных несоответствий и уязвимостей, проведение предусмотренных настоящей технической спецификацией повторных проверок, сканирований и тестирований, актуализацию ранее подготовленных Потенциальным поставщиком отчётных материалов, а также устранение замечаний, относящихся к результатам оказанных услуг. 11.6. Выполнение указанных мероприятий в течение гарантийного периода осуществляется Потенциальным поставщиком за счёт стоимости услуг по заключённому договору и не влечёт увеличения стоимости договора, заключения дополнительного договора либо возникновения у Заказчика иных финансовых обязательств.
---	---