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 №:	№ 17835520-1
Конкурстың атауы:	2027 жылға арналған Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтерді сатып алу бойынша конкурс
Лоттың нөмірі:	№ 88115490-ОК1
Лоттың атауы	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	801019.000.000010
Қызметтің атауы:	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	12590517.24
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	12590517.24
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	Ақпараттық қауіпсіздік жедел орталығына қосылу қызметі/ 1. Қызмет көрсетудің мақсаты ККП АЖ Тапсырыс берушінің ақпараттық-коммуникациялық инфрақұрылымы объектілерінің ақпараттық қауіпсіздігін қамтамасыз ету мониторингін жүргізу болып табылады. Қызметті көрсетудің негізгі мақсаты ККП АЖ инфрақұрылымының «Ақпараттандыру туралы» Қазақстан Республикасы Заңының және «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысының талаптарына сәйкестігін қамтамасыз ету болып табылады. 2. Қызмет көрсету мерзімі: Шарт жасалған күннен бастап 2027 жылғы 31 желтоқсанға дейін. 3. ККП АЖ-ны ақпараттық қауіпсіздіктің жедел орталығына қосу мерзімі: Шарт жасалған күннен бастап 10 жұмыс күні. 4. Терминдер мен анықтамалар: 1) ақпараттық қауіпсіздік (АҚ) – электрондық ақпараттық ресурстардың, ақпараттық жүйелер мен ақпараттық-коммуникациялық инфрақұрылымның сыртқы және ішкі қатерлерден қорғалу жағдайы; 2) АҚ инциденті – ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысында олардың тиісінше жұмыс істеуіне қауіп төндіретін жеке немесе сериялық туындайтын іркілістер және (немесе) электрондық ақпараттық ресурстарды заңсыз алу, көшіру, тарату, өзгерту, жою немесе бұғаттау үшін жағдайлар; 3) ақпараттық-коммуникациялық инфрақұрылым объектілері – ақпараттық жүйелер, технологиялық платформалар, аппараттық-бағдарламалық кешендер, серверлік үй-жайлар (деректерді өңдеу орталықтары), телекоммуникациялар желілері, сондай-ақ ақпараттық қауіпсіздікті және техникалық құралдардың үздіксіз жұмыс істеуін қамтамасыз ету жүйелері; 4) оқиғаларды тіркеу журналдарын жинау жүйесі (жүйе, SIEM) - ақпараттандыру объектілерінің оқиғаларды тіркеу журналдарын орталықтандырылған жинауды, оларды сақтауды және ақпараттық қауіпсіздік оқиғаларын басқару жүйесіне одан әрі беруді қамтамасыз ететін аппараттық-бағдарламалық кешен; 5) НҚА – нормативтік құқықтық актілер; 6) АҚҰҰО – Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы; 7) АҚЖО – Ақпараттық қауіпсіздіктің жедел орталықтары; 8) АҚ үшін жауапты – ақпараттық қауіпсіздікті қамтамасыз етуге, белгіленген әкімшілік қорғау шараларын іске асыруға және үздіксіздігіне жауапты және қолданылатын физикалық және техникалық қорғау құралдарының жұмыс істеуіне тұрақты ұйымдастырушылық қолдауды жүзеге асыратын Тапсырыс берушінің қызметкері; 9) EPS (events per second) – секундына оқиғалар саны; 10) АҚ оқиғасы-ақпараттық ресурстармен байланысты күтпеген, алдын ала белгіленбеген (саясаттармен, регламенттермен, нұсқаулықтармен, техникалық параметрлермен құжатталмаған) немесе қауіпсіздікке қатысы болуы мүмкін бұрын белгісіз жағдайдың туындауы болып табылатын кез келген оқиға; 11) Ақпараттық қауіпсіздікті қамтамасыз ету мониторингі – АҚ қатерлері мен инциденттерін анықтау арқылы іс-шараларды іске асырудың толықтығы мен сапасын қадағалау. 12) ККП АЖ–

	Көші-қон полициясының ақпараттық жүйесі. 5. Бұл қызмет мыналарды қамтамасыз етеді: - телекоммуникациялық жабдықтан, серверлер мен жұмыс станцияларының жүйелік және қолданбалы бағдарламалық қамтамасыз етуінен оқиғаларды (журналдарды) жинау; - АҚ ықтимал оқиғаларын анықтау үшін оқиғаларды талдау. 1. Қызметтке мыналар кіреді: - тапсырыс беруші мен Өнім берушінің жауапты тұлғаларымен келісілген Автоматты анықтау сценарийлері бойынша (Тапсырыс берушінің бес қызметкерінен аспайтын санда) тәулік бойы режимде мониторинг аймағында тіркелген оқиғалар/инциденттер туралы Тапсырыс берушінің жауапты қызметкерлеріне автоматты мониторинг, анықтау және хабарлау; - тапсырыс беруші мен Жеткізушінің жауапты тұлғаларымен келісілген Анықтау Сценарийлері бойынша (Тапсырыс берушінің бес қызметкерінен аспайтын санда) тәулік бойы режимде БҚАЖ талдаушылары мониторинг аймағында тіркелген оқиғалар/инциденттер туралы Тапсырыс берушінің жауапты қызметкерлеріне мониторинг, анықтау және хабарлау; - Қазақстан Республикасы заңнамасының талаптарына сәйкес Ақпараттық қауіпсіздік жөніндегі ұлттық үйлестіру орталығына оқыс оқиғалар туралы хабарламалар жіберу; - ақпараттық қауіпсіздіктің жинақталған оқиғаларын жедел қолжетімділікте кемінде 62 (алпыс екі) күнтізбелік күн және мұрағат нысанында кемінде 1096 (бір мың тоқсан алты) күнтізбелік күнді құрайтын кемінде 3 (үш) жыл бойы сақтау. Сақтау мерзімі өткеннен кейін жиналған ақпаратты қорғау оқиғалары одан әрі сақтау үшін Тапсырыс берушіге беріледі; - артықшылықты шоттармен әрекеттерді автоматтандырылған тексеру; - ақпараттық қауіпсіздік оқиғаларын автоматтандырылған тексеру; - оқиғаларды жеткізу жүйесін құру бойынша ұсыныстар мен ұсынымдар енгізу; - тапсырыс берушінің қызметкерлерімен бірлесе отырып, Тапсырыс берушінің сайты мен Жеткізушінің сайты арасындағы ақпарат беру арнасының жұмыс істеуін қамтамасыз ету; - мониторинг аймағында орын алған ақпараттық қауіпсіздік инциденттерін анықтау; - тапсырыс берушіге анықталған инциденттер және оларға ден қою әдістері туралы ақпаратты жіберу, оларды жою бойынша ұсыныстар беру; - нормативтік емес жағдайлар тізбесі негізінде SIEM-де оқиғалар мен дабылдардың өзара байланысы ережелерін әзірлеу - SIEM-де оқиғалар мен дабылдардың корреляциясы ережелерін әзірлеу; - тұтынушының KVOIKI инфрақұрылымындағы өзгерістерге сәйкес корреляция ережелерін бейімдеу; Тұтынушының талабы бойынша корреляция ережелеріне ерекшеліктерді қосу. Толтыру формасы – есеп. - KZ-CERT Оқиғаларға ден қою орталығына маңыздылығы бойынша хабарлама жіберу - Ақпараттық қауіпсіздік инциденттері кезінде KZ-CERT Оқиғаларға ден қою орталығына хабарлама жіберу. Толтыру нысаны – есеп; - тапсырыс беруші мен Мердігер арасында бекітілген кестеге сәйкес сыртқы периметрді осалдықтарға сканерлеу; - тапсырыс берушінің жауапты қызметкерлерін мамандандырылған SIEM клиенттік консоліне – ақпараттық қауіпсіздік оқиғалары мен инциденттерін іздеуге және талдауға арналған интерактивті құралға оқыту және қолжетімділігін қамтамасыз ету; - ақпараттық

	қауіпсіздік оқиғалары/инциденттері туралы автоматтандырылған есепті енгізу және оған Тапсырыс берушінің жауапты қызметкерлеріне қолжетімділікті қамтамасыз ету; - компьютерлік криминалистика және Тапсырыс беруші жүйесінде ақпараттық қауіпсіздік инциденттері кезінде ақпаратты қорғау саласында консультациялық қызметтерді көрсету. - тұтынушының өтініші бойынша (әдіс Тапсырыс берушімен талқыланады) толық егжей-тегжейлі тестілеу есебін ұсына отырып, қызмет көрсетудің бүкіл мерзімі ішінде 2 реттен артық емес ену сынамасын жүргізу: Қолданбалар, желілер, жүйелер және инфрақұрылым деңгейінде пентесттерді өткізу; Әртүрлі құралдар мен әдістерді қолдану арқылы осалдықтарды пайдалану; Қауіпсіздік жүйелерін айналып өту үшін стандартты емес әдістерді әзірлеу және пайдалану; Практикалық шабуылдар арқылы жүйені қорғау және ену деңгейін бағалау; Стратегиялық көзқарас және Red Teaming-ге назар аудара отырып, нақты шабуылдаушылардың әрекеттерін еліктейтін көп деңгейлі шабуылдар; - толық есеп пен орындалған жұмыс актісін ұсына отырып, ақпараттық қауіпсіздіктің осалдығына Тапсырыс берушінің қызметтеріне талдау жүргізу, Тапсырыс беруші мен Мердігер арасында бекітілген кестеге сәйкес. Жұмыс шабуыл векторлары мен осалдықтардың соңғы классификациясына сәйкес жүзеге асырылады: A1: қол жеткізуді басқару бұзылған; A2: Криптографиялық ақаулар; A3: Инъекция; A4: Қауіпсіз дизайн; A5: Қауіпсіздік конфигурациясы қате; A6: осал және ескірген компоненттер; A7: Сәйкестендіру және аутентификация қателері; A8: Бағдарламалық қамтамасыз ету және деректер тұтастығындағы ақаулар; A9: Қауіпсіздікті тіркеу және бақылау қателері; A10: серверлік сұрау сұрауы. Жүргізілген қауіпсіздік талдауы туралы есепте анықталған осалдықтарды пайдалану процесінің сипаттамасымен, растаулармен және осалдықтың осы түрін жою бойынша ұсынымдармен бірге векторлар мен шабуылдардың жіктелуі тұрғысынан анықталған осалдықтар туралы ақпарат ұсынылуы тиіс; - ұйымда киберинциденттер анықталған/анықталған кезде Жеткізуші OCIB қызметі аясында уәкілетті маманмен тергеу жүргізеді, ол нақты инциденттер жағдайларына қарамастан тұрақты негізде тергеу жүргізуге дайын; - желілік қорғау құралдарын баптау және сүйемелдеу бойынша сараптамалық-консультациялық жәрдем: фаерволдардың қауіпсіздік саясатын, шабуылдарды анықтау және болдырмау жүйелерін (IDS/IPS) конфигурациялау және ұдайы жаңарту бойынша ұсынымдар беру; ағымдағы параметрлердің тиімділігін талдау, желілік инфрақұрылымдағы осалдықтарды анықтау және жою; желілік қауіпсіздік құрылғыларын орталықтандырылған бақылау жүйесіне біріктіру (SIEM, NOC және т.б.). - кибер барлау және қауіп-қатер талдауы: ашық (OSINT) және жабық көздерден, соның ішінде Dark Web-тен киберқауіптер туралы ақпаратты жинау, өңдеу және талдау; ақпараттық жүйенің ішкі оқиғаларымен алынған мәліметтердің байланысы; қауіпсіздік оқиғасы деректерін ымыраға келу (IOC) және қарсылас ТТП (тактикалар, әдістер және процедуралар) көрсеткіштерімен байыту; - криминалистика және инциденттерге ден қою: ақпараттық қауіпсіздік

	инциденттері кезінде цифрлық зерттеулер жүргізу; цифрлық сот сараптамасының әдістеріне сәйкес дәлелдемелерді жинау, талдау және сақтау; оқиғалардың қайталануын болдырмау үшін есептер мен ұсыныстарды дайындау. - жүйе қауіпсіздігін бағалау және жетілдіру: кибершабуыл модельдеулерін жүргізу (Red Team / Adversary Simulation), содан кейін қорғаныс жүйелерінің тиімділігін талдау (Blue Team); қауіпсіздік кедергілерін анықтау, инциденттерді анықтау және әрекет ету механизмдерін жетілдіру бойынша ұсыныстар беру; жауап оқулықтары мен TTP әрекет процедураларын бірлесіп әзірлеу, тестілеу және оңтайландыру. - зиянды бағдарламаны талдау: күдікті файлдар мен объектілердің статикалық және динамикалық талдауын орындау; зиянды бағдарламаның логикасын, мінез-құлқын және мүмкіндіктерін түсіну үшін кері инженерия; талдау нәтижелері бойынша ымыраға келу көрсеткіштерін (МОК) анықтау және ресімдеу; SIEM, антивирустық бағдарламалық қамтамасыз ету және қауіптерді анықтау жүйелеріне кейіннен біріктіру үшін қолтаңбалар мен анықтау ережелерін (YARA, Snort, Suricata және т.б.) әзірлеу. 2. Көрсетілетін қызметтердің техникалық параметрлері: - Оқиға көздерінің келесі түрлері (бақылау аймағы) қызметтерге қосылған: Серверлер; Желілік құрылғылар; IDS/IPS; Тұтынушы маңызды деп анықтаған басқа көздер (жеке жұмыс станцияларын қоса); - АҚЖО қосылуға арналған ақпараттық технологиялар объектілері: Көші-қон полициясының ақпараттық жүйесі; - қызмет көрсету деңгейі келісімі (SLA): Қызметтерді көрсету мерзімі: 24/7 автоматтандырылған режимде; 24/7 қызметтердің қолжетімділігі (тәулік бойы): Бір реттік үзіліс 4 сағаттан артық емес; Тоқсандағы қолжетімділік 95% кем емес; - тапсырыс беруші оқиға көздерінен Жеткізушінің бақылау жүйесіне қажетті оқиғалар журналдарын тасымалдауды қамтамасыз етеді. Жабдықтаушы көздерді қашықтан қосу бойынша консультациялық көмек көрсетеді; - Оқиғаның жаңа көздерін қосу Тараптардың келісімі бойынша жүзеге асырылады; - SIEM жүйесіне арналған аппараттық құралдарды, бағдарламалық қамтамасыз ету лицензияларын және Қызметтерді көрсету шеңберінде пайдаланылатын басқа да кибермониторинг инфрақұрылымының бағдарламалық қамтамасыз етуін Жеткізуші өз тарапынан ұсынады; - тараптар Тапсырыс берушінің жабдығының және/немесе бағдарламалық қамтамасыз етуінің (оқиға көздерін қоса алғанда) техникалық немесе басқа ақауы, көзден мониторинг жүйесіне жіберу кезінде оқиғалар журналының жоғалуы, оның ішінде осындай жабдықтың және/немесе Тапсырыс берушінің бағдарламалық құралының жұмысын тоқтату (тоқтата тұру), сондай-ақ үшінші тұлғалар ұсынатын байланыс арналарындағы ақаулар Қызметтерді көрсету кезеңінің кез келген уақытында бір немесе басқа қызмет көрсету көлеміне әсер етуі мүмкін екенін растайды. Қызметтерді толық емес/сапасыз көрсеткені үшін талап қоюға және/немесе сыйақының төленген сомасын (соманың бір бөлігін) қайтару туралы талап қоюға негіз бола алмайды; - жабдықтаушы Қызметтерді тек SIEM жүйесінде оған қолжетімді Тұтынушының оқиғалар журналдары шеңберінде ұсынады; - тұтынушы

	оқиғалар журналдарын қауіпсіз VPN туннелі арқылы Жеткізушінің кибербақылау инфрақұрылымына тасымалдау мүмкіндігін қамтамасыз етуі тиіс; - тұтынушы ақпараттық қауіпсіздік оқиғаларының көздеріне қажетті аудит деңгейін конфигурациялауды (Жеткізушінің ұсыныстарына сәйкес) және оқиғаларды кибермониторинг инфрақұрылымының элементтеріне қайта бағыттауды қамтамасыз етеді; - тараптар Қызметтердің орындалуына әсер ететін ақпараттық жүйелердегі және инфрақұрылымдағы барлық өзгерістер туралы бір-бірін хабардар етеді. - тараптар Қызметтерді орындау үшін қажетті ақпараттық жүйелерді және Қызметтер қолданылатын жүйелерді жұмыс жағдайында ұстайды. - Шартқа қол қойылғаннан кейін Өнім беруші Тапсырыс берушімен бірлесіп 10 жұмыс күні ішінде Өзара әрекеттесу ережесін әзірлейді және келіседі. 3. Зерттеушінің өзара әрекеттесу бағдарламасына қосылу Пайдаланылатын өзара іс-қимыл бағдарламасына қойылатын функционалдық талаптар (Қазақстан Республикасының Bug Bounty ресми ұлттық платформасымен интеграция шеңберінде) 3.1 Қатысу бағдарламасы келесі функцияларды орындауы тиіс: • Табылған осалдық туралы есептерді үнемі қабылдау, растау және қарау; • Бағдарламаға ресми түрде қатысатын бағдарламалар бойынша осалдық туралы есептерді сұрыптау; • Зерттеуші сәйкестендіру деректерін ұсыну арқылы сыйақы алу үшін өзінің жеке басын растауы керек; • Деректердің қауіпсіздігін қамтамасыз ету үшін дерекқордың үнемі сақтық көшірмелерін жасау; • Деректерді шифрлау: Барлық деректер (транзиттегі және демалыстағы деректерді қоса алғанда) AES-256 сияқты стандарттарға сәйкес келетін алгоритмдерді пайдаланып шифрлануы тиіс. Аутентификация: Барлық пайдаланушылар үшін екі факторлы аутентификация (2FA). • Оқиға журналдары: Деректерді кемінде 12 ай сақтау мүмкіндігімен қауіпсіздік талдауы үшін пайдаланушының барлық әрекеттерін тіркеу. • SAST/DAST тексерулері: Платформаның жаңа нұсқасының әрбір шығарылымы алдында статикалық (SAST) және динамикалық (DAST) қауіпсіздік талдауы жүргізілуі тиіс. Жаңарту шығарылғанға дейін анықталған барлық маңызды осалдықтарды түзету қажет. 3.2. Зерттеушілерден алынған есептер келесі талаптарға сай болуы керек: • Зерттеуші осалдықты пайдалану қадамдарын егжей-тегжейлі сипаттауы керек. • Есепте анықталған осалдықтың егжей-тегжейлі сипаттамасы, оны жоюдың қысқаша қадамдары немесе оны түзетудің жұмыс тұжырымдамасы болуы керек. Бейнелер мен скриншоттар осалдық туралы хабарламаны көрсетуі мүмкін, бірақ есепті алмастыра алмайды. • Бағдарлама есептің күйлері туралы ақпаратты көрсетуі керек (сұрыпталған, қаралуда, қайталанатын, ақпараттық, ресурс иесінің растауын күтіп тұрған, қабылданған, қабылданған және төленген, қабылданбаған). Бағдарламада Тапсырыс берушінің қызметкерлері үшін ИС иесінің тіркелгісі бар: Әкімшінің тіркелгісінде «Есептер» бөлімі көрсетілуі керек, онда мыналар көрсетіледі: идентификатор, атау, бағдарлама атаулары, осалдық түрлері, ауырлық деңгейі, тапсыру күні, қарау күйі; басқа әрекеттерді жасау мүмкіндігімен. Қосымша әрекеттер қажет: сүзгілеу, күйді орнату,

	есепті егжей-тегжейлі қарау, түсініктемелер жазу мүмкіндігімен. 3.3. Пайдаланушы панелі: Бағдарламада жүйенің негізгі функцияларына жылдам қол жеткізу мүмкіндігі бар веб-интерфейс болуы керек. Бағдарлама зерттеушілерге тіркелуге және тіркелгі жасауға мүмкіндік беруі керек. Бағдарламада екі тіркелгі түрі болуы керек: әкімшілер және зерттеушілер үшін. Бағдарламада авторизациялау үшін oAuth 2.0 авторизациялау хаттамасы қолданылуы керек. Бағдарламада аутентификациялау үшін OpenID аутентификация жүйесінің стандарты қолданылады. Зерттеушіні авторизациялау үшін RBAC (рөлге негізделген қол жеткізуді басқару) және/немесе ABAC (атрибутқа негізделген қол жеткізуді басқару) саясаттарын пайдаланып қол жеткізуді басқару қолданылады. Бағдарламада екі факторлы аутентификация болуы керек. Бағдарламада қатысуға болатын бағдарламалардың тізімі және осы бағдарламалар бойынша ұсынылған есептердің саны көрсетілуі керек. Қатысушы бағдарламалардың сипаттамасы және осы бағдарлама бойынша есептерді қабылдау шарттары міндетті түрде болуы керек. Бағдарлама зерттеушінің профилін келесі деректермен көрсетуі керек: - Зерттеушінің рейтингі; - Шешілген есептер; - Зерттеушінің есептері (есептер ұсынылған бағдарламалардың атауы, тапсырылған күні және өтінім мәртебесі); - Жабық бағдарламаға қатысуға шақыру Зерттеушінің жеке деректері (байланыс және төлем ақпараты, құпия сөзді өзгерту, құпия ақпарат (жабық жобаларға қатысу үшін) Бағдарлама қолдау қызметіне (Қолдау) хабарласу үшін функционалдылықты қамтамасыз етуі керек. Бағдарлама пайдаланушы деректерінің және осалдық туралы есептердің қауіпсіздігі мен құпиялылығын қамтамасыз етуі керек, мысалы, құпия деректерді шифрлауды пайдалануы, қауіпсіз аутентификация механизмдерін енгізуі және стандартты қауіпсіздік тәжірибелерін ұстануы керек. 3.4. Бағдарлама келесілерді көрсететін есептерді жіберу мүмкіндігін қамтамасыз етуі керек: • тізімнен осалдық түрін таңдау; • мақсатты доменді таңдау; • сындарлылық деңгейін таңдау; • есептің сипаттамасы (есепті файлдарға тіркеу мүмкіндігімен). 3.5. Бағдарламада осалдық туралы есептерді жасау бойынша нұсқаулар көрсетілуі керек: Егер осалдық жеткілікті түрде егжей-тегжейлі сипатталмаса, оны анықтау және түзету процесі айтарлықтай кешіктіріледі, бұл сайып келгенде пайдасыз болуы мүмкін; Есепте анықталған осалдықтың егжей-тегжейлі сипаттамасы, оны жоюдың қысқаша қадамдары немесе оны түзетудің жұмыс тұжырымдамасы болуы керек; 3.6. Сараптамалық сүйемелдеу шеңберінде Өнім беруші АҚЖО білікті модераторлары мен талдаушыларының күшімен ККП АЖ осалдықтары туралы келіп түсетін есептерді бастапқы өңдеуді, верификациялауды, сындарлылығын бағалауды (валидациялауды) жүзеге асыруға және оларды жабу бойынша Тапсырыс берушіге дайын ұсынымдарды ұсынуға міндеттенеді. 3.7. Жеткізуші Келісімге қол қойылған күннен бастап 15 күнтізбелік күн ішінде Жоба менеджерін және жауапты модераторларды (қызмет көрсету, жұмыс және ресми хат алмасу мәселелері бойынша ақпарат сұраулары жіберілетін электрондық пошта мекенжайын көрсете

	отырып, Тапсырыс берушіге ресми хат ұсыну) бекітеді. 4. Интернет-ресурстарды бақылау қызметі Интернет-ресурстарды бақылау жүйесіне қойылатын функционалдық талаптар 4.1. Мониторинг веб-сайттың қауіпсіздік күйіндегі өзгерістерді автоматты түрде анықтау арқылы тәулік бойы (24/7) жүргізілуі тиіс. Жүйені қолдайтын серверлер мен деректерді сақтау құралдары Қазақстан Республикасының аумағында орналасуы тиіс. 4.2. Жүйе интернет-ресурстарды бақылау нәтижелерін, хабарландыруларды және есептерді қарау үшін мемлекеттік және орыс тілдерінде қауіпсіз веб-интерфейсті, сондай-ақ Тапсырыс берушінің жауапты қызметкерлеріне қолжетімділік беру мүмкіндігін қамтамасыз етуі тиіс. 4.3. Функционалдық мүмкіндіктер: − Үздіксіз сыртқы аудит және мониторинг; − Жеткізуші қауіпсіздік оқиғаларын анықтау үшін ішкі инфрақұрылымға әсер етпей, Тапсырыс берушінің интернет-ресурстарын үнемі автоматтандырылған сканерлеуді қамтамасыз етуі тиіс. Тексеру Жалпы осалдық және қауіп-қатер (CVE) дерекқорын пайдалана отырып, келісілген әдіснамаға сәйкес жүзеге асырылады. Нәтижелер бірыңғай басқару панелінде жазылуы тиіс. Бақылау жүйесі Тапсырыс берушінің интернет-ресурстарын қауіпсіз емес ашық жолдарға (каталогтарға, файлдарға және т.б.) автоматты түрде тексереді. − Егер қауіпсіз емес ашық жолдар анықталса, қауіпсіздік оқиғасы жасалады. Жүйе Тапсырыс берушінің серверлерінің қолайлы ашық порттар тізіміне сәйкестігін тексереді; − Егер қолайлы порттар тізіміне кірмейтін порттар анықталса, қауіпсіздік оқиғасы жасалады. Жүйе TLS сертификаттарының дұрыстығы мен өзектілігін, олардың жарамдылық мерзімін, сенім тізбегін және заманауи криптографиялық стандарттарға сәйкестігін тексереді. Мерзімі өткен немесе осал сертификаттар анықталса, қауіпсіздік оқиғасы жасалады. Жеткізуші Тапсырыс берушінің халықаралық бедел дерекқорларындағы IP мекенжайлары мен домендерін үнемі тексеруді қамтамасыз етуі тиіс. Егер бұғаттау немесе қара тізімге қосу анықталса, жүйе қауіпсіздік оқиғасын тудыруы тиіс. 4.4. Есеп беру және талдау: - Жүйе интерфейсте Тапсырыс берушінің интернет-ресурстарының қауіпсіздік күйін және сканерлеу нәтижелерін көрсететін біріктірілген басқару тақтасын қамтамасыз етуі тиіс. 4.5. Оқиға және қауіпсіздік саясатын басқару: - Барлық анықталған бұзушылықтар интернет-ресурстың атауын, бұзушылық түрін, анықталған уақытын және жою бойынша ұсыныстарды көрсететін оқиғаларды автоматты түрде тудыруы тиіс. 3. Өнім беруші талаптар - штаттан тыс жағдайлар кезінде техникалық ерекшелікке сәйкес жұмыстар шеңберінде АҚЖО жабдығының тоқтап тұру уақыты тоқсанына бір рет 4 сағаттан және жиынтық 12 сағаттан аспайды (Тапсырыс беруші тарапынан профилактикалық жұмыстарды қоспағанда). - Қызметті көрсету шеңберінде туындауы мүмкін оқиғалардың сыни деңгейі: Мониторинг аймағында орналасқан инфрақұрылымда орын алған оқиғалар оларды шешудің жеделдігі дәрежесіне қарай келесі басымдықтарға бөлінеді: «Сыни»— Оқиға: ұзақтығы 15 минуттан асатын KVOIKI инфрақұрылымының толық немесе ішінара қолжетімсіздігіне әкелуі мүмкін;

	тұтынушы ресурстарының толық немесе ішінара ымыраға келуіне әкелуі мүмкін; «Жоғары»— Оқиға:ұзақтығы 15 минуттан аспайтын, 1 сағат сайын бір реттен жиі емес болатын Тұтынушы ресурстарының ішінара қолжетімсіздігіне әкелуі мүмкін; тапсырыс берушінің ресурстарына зиян келтіру үшін жағдай жасауға әкелуі мүмкін; KVOIKI инфрақұрылымында Тапсырыс беруші пайдаланатын ақпараттық қауіпсіздік жүйесі кедергі жасамаса; «Орташа»— Қазіргі уақытта Тапсырыс беруші ресурстарының қолжетімсіздігіне әкелмейтін, бірақ болашақта басымдығы жоғары оқиғаға әкелу ықтималдығы жоғары оқиға. - ұсынылатын қызметтер ISO/IEC 27000 стандарттарының әдістемелері мен серияларына, сондай-ақ ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздік саласындағы Қазақстан Республикасының қолданыстағы нормативтік құқықтық актілері мен мемлекеттік стандарттарына негізделуі тиіс; - Жеткізуші Тапсырыс берушіге өз ресурстарының ақпараттық қауіпсіздік деңгейін тиісті тәртіппен арттыру бөлігінде кеңес беруге міндетті. Өнім берушінің қызметтерді көрсету процесінде Тапсырыс берушінің негізгі ресурсының қауіпсіздік баллы мемлекеттік органдардың веб-сайттарының жыл сайынғы қауіпсіздік рейтингі шегінде кемінде 70%-ды құрауы тиіс; - Өнім беруші Тапсырыс берушінің сыртқы және ішкі желілерінің алдын алу және қорғау үшін мониторингті қамтамасыз етуге, трафикті талдауға және күдікті әрекеттерді сәйкестендіруге, Тапсырыс берушінің желілеріндегі әлсіз жерлерді анықтау және жою жөнінде ұсынымдар беруге міндетті; - «Ақпараттандыру туралы» 2015 жылғы 24 қарашадағы № 418-V ҚРЗ Заңының 54-бабының 2-1-тармағына сәйкес. Мемлекеттік органдардың ақпараттық технологиялар объектілерінің меншік иелері немесе иелері мыналарды қамтамасыз ету бойынша шаралар қабылдауға міндетті: 1) Интернет желісіне қолжетімділігі жоқ ақпараттық технологиялар объектілерін қоспағанда, ақпараттық технологиялар объектілерін өзара іс-қимыл бағдарламасына қосу; 2) мемлекеттік органдардың ақпараттық технологиялар объектілері бойынша өзара іс-қимыл бағдарламасында тіркелген анықталған осалдықтарды жою; 3) Ақпараттық қауіпсіздіктің мемлекеттік жедел орталығының немесе Ақпараттық қауіпсіздіктің жедел орталығының қызметіне қосылу. Қызметтер көрсету шеңберінде Өнім беруші Қазақстан Республикасының Ұлттық өзара іс-қимыл бағдарламасымен (Bug Bounty) өзара іс-қимыл жасауы және платформаның мынадай бағыттары мен функционалдық мүмкіндіктері бойынша Тапсырыс берушіні қолдауды қамтамасыз етуі керек: a. Осалдық туралы есептерді жүйелі түрде қабылдау, растау және қарау; b. Ресми түрде қатысатын бағдарламалар бойынша осалдық есептерін сұрыптаубағдарлама; c. Осалдықты, пайдалану әдістерін, тәуекелдерді және жою бойынша ұсыныстарды егжей-тегжейлі сипаттайтын есептерді жасау; d. Анықталған осалдықтарды жою үшін жүйе иелерімен жедел әрекеттесу; e. Дәл осалдық туралы есептерді алу үшін зерттеушілермен жедел әрекеттесу; f. Зерттеуші сәйкестендіру деректерін ұсыну арқылы сыйақы алу үшін оның жеке басын тексеруі керек; g. Бағдарламада зерттеушілердің

	жеке деректерін сенімді қорғауды қамтамасыз ету үшін екі факторлы аутентификация болуы керек. h. Зерттеушілерді осалдықтар туралы хабарлағаны үшін марапаттау және үздік зерттеушілерді жеке бағдарламаларға шақыру; i. Зерттеушілердің есептерінде ұсынылған барлық осалдықтарды қауіпсіз сақтау: Сервер қауіпсіз шифрланған қосылыммен қорғалған; деректердің сақталуын қамтамасыз ету үшін деректер қорының резервтік көшірмесін жүйелі түрде жасау; жеке деректерді шифрлау; пайдаланушының тіркелгі деректерінің екі факторлы аутентификациясы; j. Тапсырыс берушінің қызметкерлеріне арналған әкімші кеңсесі. 4. Қызметтерді төлеуге қойылатын талаптар Жеткізуші веб-портал арқылы көрсетілген қызметтер актісін рәсімдейді, бұл ретте жеткізуші және тапсырыс берушінің салалық қызметі қол қойған шығындар мен қызметтер толық жазылған қосымшаның электрондық көшірмесін ұсынады. Актілер тоқсан сайын есептік мерзімнен кейін айдың 15- күнінен кешіктірілмей веб-портал арқылы ұсынылады..
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:	№ 17835520-1
Наименование конкурса:	Конкурс по приобретению услуг по подключению к оперативному центру информационной безопасности на 2027 год
Номер лота:	№ 88115490-ОК1
Наименование лота:	Услуги по обеспечению информационной безопасности
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	801019.000.000010
Наименование услуги:	Услуги по обеспечению информационной безопасности
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	12590517.24
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	12590517.24
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	Услуги по подключению к оперативному центру информационной безопасности/ 1. Целью оказания Услуги является проведение мониторинга обеспечения информационной безопасности объектов информационно-коммуникационной инфраструктуры ИС МП. Основная задача оказания Услуги – соответствие инфраструктуры ИС МП требованиям Закона Республики Казахстан «Об информатизации» и Постановлению Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности». 2. Срок оказания услуги: с даты заключения Договора до 31 декабря 2027 года. 3. Срок подключения ИС МП к оперативному центру информационной безопасности: 10 рабочих дней с момента заключения Договора. 4. Термины и определения: 1) информационная безопасность (ИБ) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз; 2) инцидент ИБ – отдельно или серийно возникающие сбои в работе информационно¬коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов; 3) объекты информационно-коммуникационной инфраструктуры – информационные системы, технологические платформы, аппаратно-программные комплексы, серверные помещения (центры обработки данных), сети телекоммуникаций, а также системы обеспечения информационной безопасности и бесперебойного функционирования технических средств; 4) система сбора журналов регистрации событий (SIEM система) – аппаратно-программный комплекс, обеспечивающий централизованный сбор журналов регистрации событий объектов информатизации, их хранение и дальнейшую передачу в систему управления событиями информационной безопасности; 5) НПА – нормативно правовые акты; 6) НКЦИБ – Национальный координационный центр информационной безопасности; 7) ОЦИБ – Оперативный центр информационной безопасности; 8) ответственный за ИБ – работник Заказчика, ответственный за обеспечение информационной безопасности, реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты; 9) EPS (events per second) — количество событий в секунду; 10) событие ИБ – любое событие, связанное с информационными ресурсами, которое является непредвиденным, не предопределённым (не документированным политиками, регламентами, инструкциями, техническими настройками) или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности; 11) мониторинг обеспечения информационной безопасности – отслеживание полноты и качества реализации мероприятий посредством выявления угроз и инцидентов ИБ; 12) ИС МП – информационная система миграционной полиции. 5.

	Данная Услуга обеспечивает: - сбор событий (логов) с телекоммуникационного оборудования, системного и прикладного программного обеспечения серверов, и рабочих станций; - анализ событий с целью выявления потенциальных инцидентов ИБ. 1. Услуги включают в себя: - автоматический мониторинг, обнаружение и уведомление ответственных работников Заказчика о событиях/инцидентах, зарегистрированных в зоне мониторинга, в режиме 24/7, по Сценариям автоматического обнаружения (в количестве, не более пяти работников Заказчика), согласованным ответственными лицами Заказчика и Поставщика; - мониторинг, обнаружение и уведомление ответственных работников Заказчика о событиях/инцидентах, зарегистрированных в зоне мониторинга, аналитиками ОЦИБ, в режиме 24/7, по Сценариям обнаружения (в количестве, не более пяти работников Заказчика), согласованным ответственными лицами Заказчика и Поставщика; - отправка уведомлений об инцидентах в Национальный координационный центр информационной безопасности, в соответствии с требованиями законодательства Республики Казахстан; - хранение собираемых событий ИБ в течение не менее 62 (шестидесяти двух) календарных дней в оперативном доступе и в течение не менее 3 (трех) лет, что составляет не менее 1096 (одна тысяча девяносто шесть) календарных дней в архивном виде. По истечению срока хранения, собираемые события ИБ передаются Заказчику для дальнейшего хранения; - автоматизированная верификация действий с привилегированными учетными записями; - автоматизированная верификация событий информационной безопасности; - внесение предложений и рекомендаций по настройке системы доставки событий; - обеспечение, совместно с работниками Заказчика, работоспособности канала передачи информации между площадкой Заказчика и площадкой Поставщика; - выявление инцидентов ИБ, произошедших в Зоне мониторинга; - направление Заказчику информации о выявленных инцидентах и методах реагирования на них, предоставление рекомендаций по их устранению; - разработка правил корреляции событий и алармов в SIEM на основе перечня не регламентных ситуаций - Разработка правил корреляции событий и алармов в SIEM; - адаптация правил корреляции в соответствии с изменениями в инфраструктуре КВОИКИ Заказчика; добавление исключений в правила корреляции по требованию Заказчика. Форма завершения – отчет; - направление уведомления в центр реагирования на инциденты KZ-CERT АО «ГТС» согласно критичности - Направление уведомления в центр реагирования на инциденты KZ-CERT АО «ГТС» при возникновении инцидентов ИБ. Форма завершения – отчет; - сканирование внешнего периметра на наличие уязвимостей согласно плану-графику, утвержденному между Заказчиком и Исполнителем; - обучение и предоставление доступа ответственным работникам Заказчика к специализированной клиентской консоли SIEM – интерактивному инструменту для поиска и анализа событий ИБ, инцидентов; - реализация автоматизированного отчета по событиям/ инцидентам ИБ и предоставления к нему доступа ответственным работникам Заказчика; -

	оказание консультационных услуг в области компьютерной криминалистики и информационной безопасности в случае возникновения инцидента информационной безопасности в системе Заказчика; - проведение тестирования на проникновение по запросу Заказчика (Метод обсуждается с Заказчиком), не более 2-х раз за весь период оказания услуги с предоставлением полного развернутого отчета о тестировании: проведение пентестов на уровне приложений, сетей, систем и инфраструктуры; эксплуатация уязвимостей с использованием различных инструментов и техник; разработка и использование нестандартных техник для обхода систем безопасности; оценка уровня защиты и пробиваемости системы через практические атаки; стратегический подход и многоуровневые атаки, имитирующие действия реальных злоумышленников, с фокусом на Red Teaming; - проведение анализа сервисов Заказчика на предмет наличия уязвимостей информационной безопасности с предоставлением полноценного отчета и справки о проделанной работе, согласно плану-графику, утвержденному между Заказчиком и Исполнителем. Работы проводятся в соответствии с последней классификацией векторов атак и уязвимостей: A1: Broken access control; A2: Cryptographic failures; A3: Injection; A4: Insecure design; A5: Security misconfiguration; A6: Vulnerable and outdated components; A7: Identification and authentication failures; A8: Software and data integrity failures; A9: Security logging and monitoring failures; A10: Server-side request forgery. В отчете о проведенном анализе защищенности необходимо предоставить информацию об обнаруженных уязвимостях в разрезе классификации векторов и атак с описанием процесса эксплуатации обнаруженных уязвимостей, с приложением подтверждений, предоставлением рекомендаций по устранению данного типа уязвимости; - при обнаружении/выявлении кибер-инцидентов внутри организации Поставщик должен произвести расследование, уполномоченным специалистом в рамках услуги ОЦИБ, который должен быть доступен для постоянного проведения расследований независимо от конкретных случаев инцидентов; - экспертно-консультационное содействие по настройке и сопровождению сетевых средств защиты: выдача рекомендаций по конфигурированию и регулярному обновлению политик безопасности фаерволов, систем обнаружения и предотвращения атак (IDS/IPS); Анализ эффективности текущих настроек, выявление и устранение уязвимостей в сетевой инфраструктуре; - интеграция сетевых устройств безопасности в централизованную систему мониторинга (SIEM, NOC и др.); - кибер разведка и аналитика угроз (Threat Intelligence): сбор, обработка и анализ информации о киберугрозах из открытых (OSINT) и закрытых источников, включая Dark Web; корреляция полученных данных с внутренними событиями информационной системы; обогащение данных о событиях безопасности индикаторами компрометации (IOCs) и TTP противников (тактики, техники и процедуры); - форензика и реагирование на инциденты: проведение цифровых расследований в случае инцидентов информационной безопасности; сбор, анализ

	и сохранение доказательств в соответствии с методиками цифровой криминалистики; подготовка отчетов и рекомендаций по предотвращению повторных инцидентов; - оценка и улучшение защищенности систем: проведение симуляций кибератак (Red Team / Adversary Simulation) с последующим анализом эффективности действий защитных систем (Blue Team); идентификация узких мест в защите, предоставление предложений по улучшению механизмов обнаружения и реагирования на инциденты; совместная разработка, тестирование и оптимизация плейбуков (playbooks) реагирования и процедур действия по TTP. - исследование вредоносного ПО (Malware Analysis): выполнение статического и динамического анализа подозрительных файлов и объектов; обратная разработка (reverse engineering) вредоносных программ с целью понимания их логики, поведения и возможностей; выделение и формализация индикаторов компрометации (IOCs) по результатам анализа; разработка сигнатур и правил обнаружения (YARA, Snort, Suricata и пр.) для последующей интеграции в SIEM, антивирусное ПО и системы обнаружения угроз. 2. Технические параметры оказываемых Услуг: - к Услугам подключаются следующие типы источников событий (зона мониторинга): Сервера; Сетевые устройства; IDS/IPS; Прочие источники, определенные Заказчиком как критичные (включая отдельные рабочие станции); - объекты информатизации для подключения к ОЦИБ: Информационная система миграционной полиции. - параметры оказания услуг (SLA): Период предоставления Услуг: 24/7 в автоматизированном режиме; Доступность Услуг в режиме 24/7 (круглосуточно): Разовый простой не более 4 часов; Доступность за квартал не менее 95%; - Заказчик обеспечивает передачу необходимых журналов событий с источников событий в систему мониторинга Поставщика. Поставщик оказывает консультационную помощь по подключению источников в удаленном режиме; - подключение новых источников событий производится по согласованию Сторон; - аппаратное обеспечение, лицензии на ПО для SIEM-системы и другое ПО инфраструктуры кибермониторинга, используемое в рамках предоставления Услуг, обеспечивается Поставщиком на его стороне; - стороны подтверждают, что техническая или иная неисправность оборудования и/или программного обеспечения Заказчика (в том числе источников событий), потеря журналов событий при передаче от источника до системы мониторинга, в том числе прекращение (приостановка) работы такого оборудования и/или программного обеспечения Заказчика, а также сбои на каналах связи, предоставленных третьими сторонами, в любое время в период оказания Услуг, которые в той или иной степени может повлиять на объем оказываемых Поставщиком Услуг, не может являться причиной для выставления претензии о неполном/ некачественном оказании Услуг и/или требования о возврате уплаченной суммы (части суммы) вознаграждения; - Поставщик оказывает Услуги только в рамках доступных ему в системе SIEM журналов событий Заказчика; - Заказчик обеспечивает возможность передачи журналов событий на инфраструктуру кибермониторинга

	Поставщика посредством защищенного VPN – туннеля; - Заказчик обеспечивает настройку необходимого уровня аудита на источниках событий ИБ (согласно рекомендациям Поставщика) и перенаправление событий на элементы инфраструктуры кибермониторинга; - стороны уведомляют друг друга обо всех изменениях в информационных системах и инфраструктуре, влияющих на исполнение Услуг; - стороны поддерживают информационные системы, необходимые для исполнения Услуг, и системы, на которые распространяются Услуги в работоспособном состоянии; - Поставщик после подписания Договора, в течение 10 рабочих дней совместно с Заказчиком разрабатывают и согласовывают Регламент взаимодействия. 3. Подключение к программе взаимодействия с исследователями Функциональные требования к используемой Программе взаимодействия (в рамках интеграции с официальной Национальной платформой Bug Bounty Республики Казахстан 3.1. Программа взаимодействия должна иметь следующие функциональные возможности: - Регулярное принятие, подтверждение и рассмотрение отчетов о найденных уязвимостях; - Сортировка отчетов об уязвимостях по программам, официально участвующим на Программе; - Исследователь должен подтвердить свою личность для начисления вознаграждения, предоставив данные, удостоверяющие личность; - Регулярное резервное копирование базы данных, для обеспечения сохранности данных; - Шифрование данных: Все данные (в том числе передаваемые и хранящиеся) должны быть зашифрованы с использованием алгоритмов, соответствующих стандартам, таким как AES-256. Аутентификация: двухфакторная аутентификация (2FA) для всех пользователей. - Журналы событий: Логирование всех действий пользователей для анализа безопасности с возможностью хранения данных не менее 12 месяцев. - SAST/DAST проверки: Статический (SAST) и динамический (DAST) анализ безопасности должны проводиться перед каждым релизом новой версии платформы. Все выявленные критические уязвимости должны быть устранены до выпуска обновления. 3.2. Отчеты, получаемые от исследователей, должны соответствовать следующим требованиям: - Исследователь должен подробно описать шаги эксплуатации уязвимости. - Отчет должен содержать подробное описание обнаруженной уязвимости, краткие шаги по ее устранению или работающую концепцию ее исправления. Видео и скриншоты могут демонстрировать сообщение об уязвимости, но не могут заменить отчет. - Программа должна отображать информацию о статусах отчетов (отсортирован, на рассмотрении, дубликат, информативный, на подтверждении у владельца ресурса, принят, принят-оплачен, отклонен) Программа имеет кабинет владельца ИС для сотрудников Заказчика: Кабинет администратора должна отображать раздел «Отчеты» (Reports) с указанием: ID, заголовок, наименований программ, типов уязвимости, уровня критичности, даты отправки, статуса рассмотрений; с дополнительной возможностью других действий. Обязательное наличие дополнительных действий: фильтр, выставление статуса, детальное ознакомление с отчетом, с возможностью

	написания комментариев. 3.3. Панель пользователя: Программа должна иметь веб-интерфейс с возможностью быстрого доступа к основному функционалу системы.; Программа должна позволять исследователям регистрироваться и создавать учетную запись; Программа должна обладать двумя видами учетной записи для администраторов и исследователей; Для авторизации в Программе должен использоваться протокол авторизации oAuth 2.0. Для аутентификации в Программе используется стандарт системы аутентификации OpenID. Для авторизации исследователь в Программе применяется управление доступом с использованием политики RBAC (role based access control) и/или ABAC (attribute based access control). Программа должна иметь двухфакторную аутентификацию Программа должна отображать перечень доступных программ для участия и количество отправленных отчетов по данным программам Обязательное наличие описания участвующих программ с условиями принятия отчетов по данной программе. Программа должна отображать профиль исследователя со следующими данными: - Рейтинг исследователя; - Решенные отчеты; - Отчеты исследователя (название программ, по которым подавались отчеты, дата подачи и статус заявки); - Приглашение к участию в закрытой программе Личные данные исследователя (контактная и платежная информация, смена пароля, конфиденциальная информация (для участия в закрытых проектах) Программа должна предусматривать функционал для обращения в службу поддержки (Support). Программа должна обеспечивать безопасность и конфиденциальность пользовательских данных и отчетов об уязвимостях, например, использовать шифрование конфиденциальных данных, внедрять безопасные механизмы аутентификации и придерживаться стандартных методов обеспечения безопасности. 3.4. Программа должна обеспечить возможность отправки отчетов с указанием: - выбора типа уязвимости из списка; - выбора целевого домена; - выбора уровня критичности; - описания отчета (с возможностью прикрепления отчета в файлах). 3.5. Программа должна отображать инструкцию по формированию отчетов об уязвимостях: Если уязвимость не будет описана достаточно подробно, процесс ее обнаружения и исправления значительно затянется, что может в итоге не принести пользы; Отчет должен содержать подробное описание обнаруженной уязвимости, краткие шаги по ее устранению или работающую концепцию ее исправления; 3.6. В рамках экспертного сопровождения Поставщик обязуется силами квалифицированных модераторов и аналитиков ОЦИБ осуществлять первичную обработку, верификацию, оценку критичности (валидацию) поступающих отчетов об уязвимостях ИС МП и предоставлять Заказчику готовые рекомендации по их закрытию. 3.7. В целях обеспечения информационной безопасности Поставщик несет ответственность за соблюдение и обеспечение норм законодательства РК в сферах информатизации и информационной безопасности, а также политики информационной безопасности Заказчика. Поставщик в течение 15 календарных дней со дня подписания Договора утверждает Руководителя проекта и

	ответственных модераторов (предоставление официального письма Заказчику с указанием электронной почты, через которую будут осуществляться запросы информации по вопросам предоставления услуг, рабочая и служебная переписка). 4. Услуга мониторинга интернет-ресурсов Функциональные требования к системе мониторинга интернет-ресурсов 4.1. Мониторинг должен проводиться в круглосуточном режиме (24/7) с автоматическим обнаружением изменений в состоянии безопасности сайтов. Серверы и хранилища данных, обеспечивающие функционирование системы, должны располагаться на территории Республики Казахстан. 4.2. Система должна обеспечивать защищённый веб-интерфейс на государственном и русском языках для просмотра результатов мониторинга интернет-ресурсов, уведомлений и отчетов, а также возможность предоставления доступа ответственным сотрудникам Заказчика. 4.3. Функциональные возможности: − Непрерывный внешний аудит и мониторинг; − Поставщик должен обеспечить регулярное автоматизированное сканирование интернет-ресурсов Заказчика, без воздействия на внутреннюю инфраструктуру с целью выявления инцидентов безопасности. Проверка должна осуществляться по согласованной методологии с использованием базы известных уязвимостей (CVE). Результаты должны фиксироваться в единой панели управления. Система мониторинга должна осуществлять автоматическую проверку интернет-ресурсов Заказчика на наличие небезопасных открытых путей (директорий, файлов и т.п.). − В случае выявления небезопасных открытых путей, должен создаваться инцидент безопасности. Система должна выполнять проверку серверов Заказчика на предмет соответствия перечню допустимых открытых портов; − В случае выявления портов, не входящих в перечень допустимых, должен создаваться инцидент безопасности. Система должна проверять корректность и актуальность TLS сертификатов, их срок действия, цепочку доверия и соответствие современным криптографическим стандартам. В случае выявления просроченных или уязвимых сертификатов должен создаться инцидент безопасности. Поставщик должен обеспечивать регулярную проверку IP-адресов и доменов Заказчика в международных базах репутации. В случае выявления фактов блокировок или включения в «черные списки» система должна создавать инцидент безопасности. 4.4. Отчетность и аналитика: − Система должна предоставлять сводный дашборд в интерфейсе системы, отражающий состояние безопасности интернет- ресурсов Заказчика и результаты сканирований. 4.5. Управление инцидентами и политиками безопасности: − Все выявленные нарушения должны автоматически формировать инциденты с указанием названия интернет-ресурса, тип нарушения, времени обнаружения и рекомендации по устранению. 5. Требования к Поставщику - время простоя оборудования ОЦИБ, в рамках работ согласно технической спецификации, при нештатных ситуациях не более 4 часов разово и суммарно не более 12 часов в квартал (без учета профилактических работ на стороне Заказчика). - уровень критичности инцидентов, которые могут возникнуть

	в рамках оказания Услуги: Инциденты, произошедшие в инфраструктуре, находящейся в Зоне мониторинга, подразделяются на следующие приоритеты по степени срочности их решения: «Критический» — Инцидент, который: может привести к полной, либо частичной недоступности инфраструктуры КВОИКИ, продолжительностью более 15 минут; может привести к полной, либо частичной компрометации ресурсов Заказчика; «Высокий» — Инцидент, который: может привести к частичной недоступности ресурсов Заказчика, продолжительностью не более 15 минут, возникающие с периодичностью не более 1 раза в 1 час; может привести к созданию условий для компрометации ресурсов Заказчика; не предотвращен СЗИ, используемыми Заказчиком на инфраструктуре КВОИКИ; «Средний» — Инцидент, не приводящий в данный момент к недоступности ресурсов Заказчика, но имеющий высокую вероятность привести в будущем к инциденту с более высоким приоритетом. - предоставляемые услуги должны основываться на методологиях и сериях стандартов ISO/IEC 27000, а также действующим нормативным актам и государственным стандартам РК в области информационно-коммуникационных технологий и информационной безопасности. - Поставщик обязан консультировать Заказчика в части повышения уровня информационной безопасности его ресурсов должным образом. В процессе оказания услуг поставщиком, скоринг безопасности главного ресурса Заказчика должен составить не менее 70% в рамках ежегодного рейтинга защищенности сайтов государственных органов. - Поставщик обязан обеспечивать мониторинг для предотвращения и защиты внешних и внутренних сетей Заказчика, анализировать трафик и идентифицировать подозрительные действия, выявлять и предоставлять рекомендации по устранению слабых мест в сетях заказчика. - Согласно пункту 2-1 статьи 54 закона «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК. Собственники или владельцы объектов информатизации государственных органов обязаны принимать меры, обеспечивающие: 1) подключение объектов информатизации к программе взаимодействия, за исключением объектов информатизации, не имеющих доступ к Интернету; 2) устранение выявленных уязвимостей, зарегистрированных в программе взаимодействия по объектам информатизации государственных органов; 3) подключение к услуге Государственного оперативного центра информационной безопасности или оперативного центра информационной безопасности. В рамках оказания услуг Поставщик взаимодействует с Национальной программой взаимодействия (Bug Bounty) Республики Казахстан и обеспечивает поддержку Заказчика по следующим направлениям и функциональным возможностям платформы: a. Регулярное принятие, подтверждение и рассмотрение отчетов о найденных уязвимостях; b. Сортировка отчетов об уязвимостях по программам, официально участвующим на Программе; c. Генерация отчетов с подробным описанием уязвимости, методов эксплуатации, рисков и рекомендаций по устранению; d. Оперативное взаимодействие с владельцами системы для устранения найденных уязвимостей; e. Оперативное взаимодействие с

	исследователями для получения корректных отчетов об уязвимостях; f. Исследователь должен подтвердить свою личность для начисления вознаграждения, предоставив данные, удостоверяющие личность; g. Программа должна иметь двухфакторную аутентификацию для обеспечения надежной защиты персональных данных исследователей h. Награждение исследователей за отчёты о найденных уязвимостях и приглашение лучших исследователей в приватные программы; i. Надежное хранение всех уязвимостей, представленных в отчетах исследователей: Сервер защищён безопасным зашифрованным подключением; Регулярное резервное копирование базы данных, для обеспечения сохранности данных; Шифрование персональных данных; Двухфакторная аутентификация учетных данных пользователей; j. Кабинет администратора для сотрудников Заказчика. 6. Требования к оплате Услуг/ 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. Акты посредством веб-портала предоставляются 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)	-