Конкурстық құжаттамаға
16-қосымша

Сатып алынатың қызметтердің Техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Жасыл даму" акционерлік қоғамы
Ұйымдастырушының атауы:	"Жасыл даму" акционерлік қоғамы
Конкурстың №:	№ 17980059-1
Конкурстың атауы:	Ақпараттық қауіпсіздік жедел орталығына қосылу қызметтері (2027 ж.)
Лоттың нөмірі:	№ 88476600-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:	61396439
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	61396439
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 2027 жылғы 31 желтоқсанға дейін
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы Киберқауіпсіздікті қамтамасыз ету қызметтері бойынша техникалық сипаттама (Киберқауіпсіздік операциялық орталығына қосылу қызметі (ЦОҚҚ)) 1. Тапсырыс беруші «Жасыл Даму» АҚ. 2. Жеткізуші қызмет жеткізуші. 3. ЦЖ цифрлық жүйе. 4. ОЖ операциялық жүйе. 5. ДКБЖ деректер қорын басқару жүйесі. 6. ППО қолданбалы бағдарламалық қамтамасыз ету. 7. ДҚ деректер қоры. 8. ЛС жергілікті желі. 9. ҚҚҚО Киберқауіпсіздікті қамтамасыз ету орталығы (бұрын – ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталығы) – шетелдік заңды және жеке тұлғалардың қатысуынсыз Қазақстан Республикасының резиденті болып табылатын, цифрлық объектілерді қорғау жөніндегі қызметті жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі. 10. Тапсырыс берушінің цифрлық объектісі цифрлық технологиялар арқылы құрылған, пайдаланылатын немесе берілетін, бірегей цифрлық сипаттамаларға ие және цифрлық орта субъектілеріне Қазақстан Республикасының заңнамасында белгіленген көлемде иелену, пайдалану немесе билік ету құқықтарын жүзеге асыруға мүмкіндік беретін цифрлық ортаның оқшауланған элементі. Цифрлық объектілерге: цифрлық жазбалар, цифрлық активтер, цифрлық ресурстар, бағдарламалық қамтамасыз ету, цифрлық жүйелер, цифрлық платформалар, цифрлық инфрақұрылым объектілері, цифрлық деректер өнімдері, Қазақстан Республикасының заңдарында көзделген өзге де цифрлық объектілер жатады. 11. Цифрлық инфрақұрылым объектілері цифрлық объектілерді орналастыруды және олардың жұмыс істеу ортасын қамтамасыз ететін материалдық, техникалық және технологиялық құралдардың жиынтығы. Цифрлық инфрақұрылым объектілеріне: деректерді өңдеу орталықтары, телекоммуникация желілері, байланыс құралдары және өзге де инфрақұрылымдық объектілер жатады. 12. ҚҚ киберқауіпсіздік. 13. АТ ақпараттық технологиялар. 14. ПО бағдарламалық қамтамасыз ету. 15. КМЦО критикалық маңызды цифрлық объектілер – жұмысының бұзылуы немесе тоқтатылуы шектеулі қол жеткізімі бар жеке деректерді және заңмен қорғалатын құпияны қамтитын өзге де мәліметтерді заңсыз жинау мен өңдеуге, әлеуметтік және (немесе) техногендік сипаттағы төтенше жағдайға немесе қорғаныс, қауіпсіздік, халықаралық қатынастар, экономика, шаруашылықтың жекелеген салалары немесе тиісті аумақта тұратын халықтың тыныс-тіршілігі үшін елеулі теріс салдарларға әкеп соғатын цифрлық объектілер, оның ішінде мына инфрақұрылым: жылумен жабдықтау, электрмен жабдықтау, газбен жабдықтау, сумен жабдықтау, өнеркәсіп, денсаулық сақтау, байланыс, банк саласы, көлік, гидротехникалық құрылыстар, құқық қорғау қызметі, «цифрлық үкімет». 16. ҚҚҰО Киберқауіпсіздікті ұлттық үйлестіру орталығы – «Мемлекеттік техникалық қызмет» АҚ құрылымдық бөлімшесі. 17. SIEM киберқауіпсіздік оқиғаларын басқару жүйесі. 18. MISP киберқауіпсіздік мәселелері бойынша қатерлерді талдау және ақпарат алмасу платформасы (Threat Intelligence). 19. Киберқатерлерді мониторингілеу және оларға әрекет ету орталығы (бұдан әріSOC)

	Қызмет жеткізушінің КБ оқиғаларын алу мен өңдеуге жауапты бөлімшесі, ол 1-ші желі аналитиктері күшімен КБ инциденттерін тәулік бойы мониторингілеуді, 2-ші желі аналитиктері күшімен КБ инциденттерін талдауды, КБ инциденттерін тергеуді, оның ішінде ретроспективті аналитика жүргізуді және 3-ші сараптамалық желі күшімен қатерлер мен шабуылдар, оларды анықтау және қарсы тұру тәсілдері туралы ақпаратты өзектілендіруді қамтамасыз етеді. Орталық құрамына сондай-ақ ақпаратты қорғау құралдары кіреді, олардың көмегімен КБ оқиғаларын жинау, оларды кейіннен корреляциялау және КБ инциденттерін анықтау жүзеге асырылады. 20. КБ инциденті цифрлық объектінің киберқауіпсіздігіне теріс әсер ететін оқиға немесе оқиғалар жиынтығы. 21. КБ оқиғасы киберқауіпсіздіктің ықтимал бұзылуын немесе киберқауіпсіздікті қамтамасыз етуге қатысы болуы мүмкін бұрын белгісіз жағдайды көрсететін цифрлық объектінің жай-күйінің анықталған туындауы. 22. КБ қатері киберқауіпсіздік инцидентінің туындауына алғышарттар жасайтын шарттар мен факторлардың жиынтығы. 23. Алаң Тапсырыс берушінің КБ оқиғаларын басқару қосалқы жүйесінің компоненттері орналастырылатын инфрақұрылымы. 24. SLA (Service Level Agreement Қызмет көрсету деңгейі туралы келісім) – көрсетілетін қызметтің құжатталған параметрлері. Қызмет параметрлері – уақыт факторын ескере отырып, сандық және/немесе сапалық іс-әрекеттердің (қызмет(тер)дің кепілдік берілген жай-күйінің) сипаттамасы. 25. SOC Web-интерфейсі Қызмет көрсету шеңберінде анықталған инциденттер туралы ақпаратты автоматтандырылған жинауға және БҚ WEB-интерфейсіндегі жеке кабинет арқылы Тапсырыс берушінің уәкілетті мамандарына оған қол жеткізуді ұсынуға арналған бағдарламалық қамтамасыз ету (бұдан әрі – БҚ). 26. Корреляция екі және одан да көп КБ оқиғаларындағы деректер арасындағы өзара байланысты анықтау. 27. Агрегациялау бірдей ақпаратты қамтитын КБ оқиғаларын біріктіру. 28. Шабуылды анықтау сценарийі (бұдан әріuse-case; сценарий) бұл ақпараттың бүтіндігіне, құпиялылығына және қолжетімділігіне теріс әсерді ескере отырып, критикалық жүйелер, желі сегменттері, қызметкерлер топтары сияқты Тапсырыс беруші үшін маңызды салаларға қатысты КБ қатерін іске асырудың ықтимал сценарийі. Сценарий байқауды, қадағалауды және анықталған жағдайда белгілі бір іс-әрекеттерді қабылдауды талап ететін жағдайды сипаттауды білдіреді. 29. Типтік дереккөз Тапсырыс берушінің КБ оқиғаларының көзі, оларды қосу кезінде Жеткізуші өзінің білім базасын басшылыққа ала алады. 30. Типтік емес дереккөз Тапсырыс берушінің өз әзірлемесі жүйелеріне жататын және/немесе Жеткізуші тарапынан оқиғалар журналдарын қосымша талдау және парсер (өңдеуші) әзірлеу қажет етілетін КБ оқиғаларының көзі. 31. Өзгертуге сұраныс БҚ конфигурациясын және (немесе) баптауларын өзгертуге сұраныстармен байланысты өтініш. 32. Дашборд (ағылш.dashboard) әртүрлі трендтер мен көрсеткіштерді әртүрлі диаграммалар, графиктер, жаңартылатын кестелер немесе виджеттері бар консоль немесе басқару панелі түрінде визуализациялауға мүмкіндік беретін

	утилиталар. 33. Тапсырыс берушінің жеке кабинеті КБ инциденттерінің мәртебесі бойынша өзекті ақпаратты ұсынуға, есептілікті және Тапсырыс берушіге өзге де ақпаратты ұсынуға арналған жүйе. № р/с АтауыАтауы ТалаптарТалаптар 1. Жалпы мәліметтер 2026 жылы енгізілген Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V ҚРЗ «Киберқауіпсіздік туралы» Заңының нормаларына сәйкес Тапсырыс берушінің цифрлық объектісін ККҚО-қа қосу қызметі болып табылады. Ол Тапсырыс берушінің цифрлық объектілері мен цифрлық инфрақұрылым объектілерінің «КБ оқиғаларын мониторингілеу және талдау» қызметін қамтиды. Қызмет көрсету шеңберінде келесі міндеттер шешілуі тиіс: Киберқауіпсіздік оқиғаларын мониторингтеу және АҚ инциденттерін өңдеуді ұйымдастыру (бұдан әрі – АҚ инциденттерін мониторингтеуді ұйымдастыру), оның ішінде Тапсырыс берушінің инфрақұрылымында қызметті көрсету үшін қажетті компоненттерді орналастыру (бұдан әрі – Мониторинг аймағы); Мониторинг аймағында және сыртқы периметрді қорғау жүйелерінде тіркелген АҚ оқиғаларын тәулік бойы бақылау; Тапсырыс берушінің серверлік жабдықтары мен желілік құрылғыларында тіркелген АҚ оқиғаларын тәуілік бойы мониторингтеу; Клиентке анықталған инциденттер, оларға әрекет ету тәсілдері туралы ақпаратты жолдау және оларды жою бойынша ұсынымдар беру; Киберқауіпсіздік инциденттері туындаған жағдайда, тапсырыс берушімен келісу арқылы KZ-CERT АҚҰУО (Киберқауіпсіздікті ұлттық үйлестіру орталығына) хабарламалар жолдау; АҚ инциденттеріне әрекет ету процесінде сараптамалық қолдау көрсету; АҚ инциденттерін тергеуге көмек көрсету. Алайда, егер Мониторинг аймағында мониторинг аймағына кірмейтін жүйелерге қатысты күдікті оқиға анықталса, бұл оқиға туралы Тапсырыс берушіге хабарланады. Бұдан кейінгі тергеуді Тапсырыс беруші өз бетінше жүзеге асырады, ал Қызмет жеткізуші қажет болған жағдайда инциденттің сыни деңгейін анықтау және қосымша талдау жүргізу бойынша консультациялар береді, мәселенің қайнар көзін анықтауда және Тапсырыс берушінің мамандарына инцидентті жоюда жәрдем көрсету үшін консультациялар береді. 2. Қызмет көрсету шекаралары және АҚЖО-ға қосылу Объектілер: Тапсырыс берушінің цифрлық объектілері мен цифрлық инфрақұрылым объектілері Орналасқан жері: Қазақстан Республикасы, Астана қаласы Қызмет көрсету мерзімі: 12 ай Қызмет көрсету кезеңі: 01.01.2027 — 31.12.2027 Қажет болған жағдайда Қызмет жеткізушінің қызметкерлері Тапсырыс берушінің аумағына барып қызметтерді көрсете алады (жабдықты монтаждау, баптау және т.б.). Тапсырыс беруші Қызмет жеткізушінің қызметкерлеріне қажетті қолжетімділікті қамтамасыз етуі тиіс, бұл шарттар келісімшарт жасалғаннан кейін айқындалады. Қосылу жұмыстарының құрамына қойылатын талаптар 4 кезеңге бөлінеді, әр кезеңнің мақсаты анықталып, оған жету үшін міндеттер қойылады. 1-кезең. Зерттеу: Кезеңнің мақсаты: Қызмет көрсетудің мақсатты архитектурасын анықтау және дереккөздер тізімін белгілеу. Міндеттері: Тапсырыс беруші тарапынан толтырылған сауалнама парағына және Тапсырыс берушінің өкілдерімен сұхбатқа

	сүйене отырып, Қызмет жеткізуші Тапсырыс берушінің информатизация объектісін талдайды, соның негізінде: Қосылатын АҚ оқиғалары көздерінің құрамын және басымдылығын анықтау бойынша ұсыныстар беру; Тапсырыс берушінің бұрын бар сценарийлерді қосу және жаңа шабуылдарды анықтау сценарийлерін әзірлеу қажеттілігін анықтау (Тапсырыс берушіге аналитикалық сауалнама парағы жіберіледі); Қызмет көрсету мақсатты архитектурасы және компоненттерді орналастыру тәртібі бойынша ұйымдастырушылық-техникалық шешімдерді әзірлеу; Тапсырыс берушінің алаңында және Киберқауіптерге мониторинг және әрекет ету орталығында қызмет компоненттерінің желілік өзара әрекеттесу тәртібін ұйымдастыру. Осы кезеңде кем дегенде келесі мәліметтер жиналуы тиіс: дереккөз атауы; дереккөз функционалының сипаттамасы (тапсырыс берушінің цифрлық объектілері мен цифрық инфрақұрылым объектілеріне жататындығы); орналастыру алаңы; өндіруші/бренд/модель; ОЖ типі/нұсқасы; БҚ типі/нұсқасы; Толық домен аты (Fully Qualified Domain Name); IP-мекенжайы. 2-кезең. Енгізу: Кезеңнің мақсаты: Қызмет компоненттерін Тапсырыс берушінің алаңында орналастыру және Тапсырыс беруші мен Қызмет жеткізуші арасында VPN-туннель құру Міндеттері: L3 байланыс болмаған жағдайда, Қызмет жеткізуші мен Тапсырыс беруші арасында VPN-туннель ұйымдастырылады: Байланыс кезінде қолданылатын транспорт протоколын блоктаумен трафикті сүзу жүргізілмейді; Қызмет компоненттері мен АҚ оқиғалары дереккөздері арасындағы желілік қолжетімділікті ұйымдастыру, Қызмет жеткізушінің сұранысы бойынша; Қызмет жеткізуші Тапсырыс берушімен бірлесіп компоненттерді енгізу бойынша орнату жұмыстарын жүргізеді. 3-кезең. Қосылу: Кезеңнің мақсаты: АҚ оқиғалары дереккөздерін қосу, SIEM жүйесіне оқиғалардың дұрыс түсуін тексеру, сондай-ақ Тапсырыс берушінің сұранысы бойынша жаңа бұзушылықтар мен АҚ инциденттерін анықтау сценарийлерін әзірлеу. Міндеттері: 1-кезең және дереккөздер тізіміне сәйкес, Қызмет жеткізуші қосылу нұсқаулықтарын ұсынады; Қызмет жеткізуші типтік емес дереккөздерге жеке коннекторлар әзірлейді; Дереккөздер қосылғаннан кейін, Қызмет жеткізуші индекстелетін оқиғалардың толықтығын тексереді және қажет болса оңтайландырады; Қызмет жеткізуші Тапсырыс берушінің толтырған аналитикалық сауалнама парағына сәйкес SIEM жүйесін ақпараттық-коммуникациялық инфрақұрылымға баптайды және профилдейді; бұл бұзушылықтар мен АҚ инциденттерін анықтау сценарийлерінің жұмыс істеуін қамтамасыз етеді; Қызмет жеткізуші Тапсырыс берушінің арнайы сұраныстары және осалдықтарды талдау нәтижелеріне негізделе отырып жаңа сценарийлер әзірлейді; Қызмет жеткізуші Қызмет компоненттерін мониторингілеу үшін Тапсырыс берушінің уәкілетті өкілдеріне Дашборд арқылы қолжетімділікті қамтамасыз етеді; Тапсырыс беруші АҚ инциденттері туралы ақпарат жіберілетін қызметкерлер тізімін береді, содан кейін Қызмет жеткізуші тиісті хабарландыру топтарын баптайды. 4-кезең. Операциялық жұмыс: Кезеңнің мақсаты: Тапсырыс берушінің SIEM-жүйесіне қосылған цифрлық объектілері мен цифрлық инфрақұрылым

	объектілерін есепке алуға мүмкіндік береді. Міндеттері: Қызмет көрсетудің негізінде Киберқауіптерге мониторинг және әрекет ету орталығында Қызмет жеткізуші келесі жұмыстарды атқаруы тиіс: 24/7 режимінде 1-ші деңгей аналитиктерінің күштерімен АҚ оқиғаларын талдау, бірінші кіріс нүктесі ретінде әрекет ету, АҚ инциденттерін өңдеу, жалған ескертулерді тексеру, бастапқы аналитика жүргізу, инциденттерді категориялау және тіркеу, ITIL стандарттарына сәйкес инцидентке қызмет көрсету (категориялау, приоритизация, SLA және т.б.), АҚ инциденттері бойынша хабарландыру режимін қамтамасыз ету; 2-ші деңгей аналитиктерінің күштерімен 8х5 режимінде терең аналитика жүргізу, корреляция ережелерін Тапсырыс берушінің инфрақұрылымындағы өзгерістерге сәйкес бейімдеу; Тапсырыс берушінің сұранысы бойынша немесе өздігінен талдау нәтижесі бойынша ерекшеліктерді қосу; Тапсырыс беруші инцидентті растаса, инцидент 2 және 3 деңгей аналитиктері арқылы толық талдауға өтеді, өткен оқиғаларды зерттеу жүргізіледі. АҚ инцидентін бастапқы тексеру келесі әрекеттер арқылы жүзеге асырылады: ұсыныстар беру, инцидентке әрекет етуге арналған нұсқаулықтарды дайындау, соның ішінде оқиғаларды жинауға арналған конфигурациялық файлдар. Қызмет көрсету барысында АҚ инциденттері бойынша аналитикалық ақпаратты виджеттер және/немесе Дашборд (Жеке кабинет) арқылы визуализациялау мүмкіндігі қамтамасыз етіледі. Тапсырыс берушіге қолжетімді функциялар: әрбір АҚ инцидентінің картасын көру, инцидент статусын басқару мүмкіндігімен; АҚ инциденттері туралы статистиканы қарау; АҚ инциденттерін тіркеу және олардың мәртебесін нақты уақытта бақылау; әрбір АҚ инциденті бойынша анықталған шабуыл техникасының сипаттамасын көру; стандартты шаблон бойынша АҚ инциденті картасын ұсыну; қосылған дереккөздерді, қосылу күнін Дашборд арқылы қарау; ТОП-5 пайдаланушы топтарының күдікті әрекеттері туралы консолидирленген ақпаратты қарау; Жеке кабинеттен стандартты есептерді шығару. 3. Киберқауіпсіздік бойынша Қызмет көрсету талаптары (АҚЖО) Қызмет көрсету талаптарын орындау шеңберінде Қызмет жеткізуші АҚ оқыс оқиғаларының негізгі санаттарын анықтай білуі тиіс: Unauthorized Access/Compromised. Қорғалатын желіге/жүйеге/қосымшаға/деректерге физикалық/логикалық қолжетімділікті рұқсатсыз алумен байланысты инциденттер; Scans/Probes/Attempted Access. Қол жетімді хосттар, ашық порттар, БҚ белгілеген осалдықтар немесе бұзушы шабуылды одан әрі жоспарлау және дамыту үшін пайдалануы мүмкін нысаналы объект туралы өзге де мәліметтер алуға бағытталған белсенділікке байланысты тосын оқиғалар; Brute Force. Қорғалған жүйелерге парольдерді іріктеудің табысты және сәтсіз әрекеттеріне байланысты инциденттер; Vulnerability. Осалдықтарды табысты пайдалануға, сондай-ақ пайдаланылуы Киберқауіпсіздікке қатерлерді іске асыруға әкеп соғуы мүмкін сындарлы осалдықтарды (іске асыру осалдықтарын) анықтауға (сканерлерді пайдалануға) байланысты тосын оқиғалар; Malware. Зиянды бағдарламалық қамтамасыз етудің белсенділігіне байланысты инциденттер (мысалы,

	шифрлаушыны іске қосу, троянды автожүктеуге жазу және т.б.); Malware C&C Communication. Қорғалатын инфрақұрылым хосттарының белгілі командалық орталықтармен өзара іс-қимылын анықтауға байланысты инциденттер; • Malicious Host. Зиянды БҚ таратуды орындайтын ресурстарға қол жеткізумен байланысты (белгілі командалық желілер ботнеті орталықтарын қоспағанда) немесе Интернет желісінде осындай ресурстарды орналастырумен тікелей байланысты тосын оқиғалар; • Spam. Ақпараттық/жарнамалық сипаттағы сұралмайтын электрондық поштаны таратуға байланысты тосын оқиғалар; • Fraud. Қорғалатын ақпараттық жүйені пайдаланушылардың алаяқтық әрекеттеріне байланысты тосын оқиғалар; • Social Engineering. Қорғалатын ақпараттық жүйені пайдаланушыларды тәртіп бұзушының мақсаттарына қол жеткізуге бағытталған іс-әрекеттер жасауға (алдау немесе сенімге қиянат жасау жолымен) ынталандыруға байланысты тосын оқиғалар (ақша қаражатын аудару бойынша операцияларды жүзеге асыру, зиянды сілтеме бойынша өту, парольдік ақпаратты жария ету және т.б.); • Improper Usage. АҚ саясатының/регламенттерінің/нұсқауларының талаптарын бұзумен байланысты тосын оқиғалар (мысалы, ргоху-ны айналып өтіп Интернетке қосылу, көпшілік Wi-Fi желілеріне қосылу, тыйым салынған хосттағы домен әкімшісінің тіркелгілерін пайдалану және т.б.); • Suspicious Process Activity. Заңды процестердің аномалды мінез-құлқымен байланысты тосын оқиғалар. 4. Инциденттер туралы хабарлау және оларға ден қою ККҚО ҚҚҰҮО-мен киберқауіпсіздік саласындағы өздеріне жүктелген міндеттер мен функцияларды орындау үшін ақпарат алмасуды жүзеге асырады. ККҚО ҚҚҰҮО-дан алынған ақпаратты Тапсырыс берушіге жеткізуді қамтамасыз етеді. ККҚО ҚҚҰҮО-мен мыналарға бағытталған міндеттерді шешу мүддесінде өзара іс-қимылды жүзеге асырады: киберқауіпсіздік бұзушылықтарының алдын алу тетіктерін жетілдіру; ККҚО қызметін жақсарту; ККҚО мен ҚҚҰҮО арасындағы іс-қимылдың жеделдігі мен үйлесімділігін арттыру; цифрлық объектілердің киберқауіпсіздік деңгейін арттыру бойынша бірлескен шешімдер әзірлеу. Киберқауіпсіздікті қамтамасыз ету үшін қажетті ақпарат құпия цифрлық деректер санатына жатады, оны алу, өңдеу және пайдалану ол жиналатын мақсаттармен шектеледі. ҚҚҰҮО-дан ҚҚҚО-қа және ҚҚҚО-тан ҚҚҰҮО-ға мәліметтерді ұсыну Қазақстан Республикасы Жасанды интеллект және цифрлық даму министрінің міндетін атқарушының 2026 жылғы 25 маусымдағы № 354/НҚ «Ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті ақпаратты ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталықтары мен Ақпараттық қауіпсіздікті ұлттық үйлестіру орталығы арасында алмасу қағидаларын бекіту туралы» Қазақстан Республикасы Қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 19 наурыздағы № 48/НҚ бұйрығына өзгерістер енгізу туралы» бұйрығының (бұдан әрі – №354 бұйрық) шеңберінде жүзеге асырылады. Киберқауіпсіздік инциденті анықталған кезде ҚҚҚО: киберқауіпсіздік инциденті расталған сәттен бастап 15 (он бес) минут ішінде ҚҚҰҮО-ны және КВЦО меншік иесін немесе иесін хабардар етеді; киберқауіпсіздік

	инциденті расталған сәттен бастап 72 (жетпіс екі) сағат ішінде ҚҚҰО-ға №354 бұйрыққа қосымшаға сәйкес нысан бойынша киберқауіпсіздік инцидентінің карточкасын жібереді. ҚҚҰО-дан киберқауіпсіздік инциденті туралы хабарлама келіп түскен кезде КҚҚО хабарлама сәтінен бастап 72 (жетпіс екі) сағат ішінде ҚҚҰО-ға мыналарды жібереді: киберқауіпсіздік қатерін талдау нәтижелерін; киберқауіпсіздік оқиғасы расталған кезде киберқауіпсіздік оқиғасын талдау нәтижелерін; киберқауіпсіздік инциденті расталған кезде №354 бұйрыққа қосымшаға сәйкес нысан бойынша киберқауіпсіздік инцидентінің карточкасын. Деректерді жинау мына жағдайларда жүзеге асырылады: туындаған қатерлер, осалдықтар және киберқауіпсіздік инциденттері бойынша мәліметтерді талдау кезінде; киберқауіпсіздік инциденті цифрлық ресурстардың, цифрлық жүйелердің, телекоммуникация желілерінің және басқа да цифрлық объектілердің жұмыс қабілеттілігіне әсер етуі мүмкін деп пайымдауға негіз болған кезде; киберқауіпсіздік қатері, осалдығы және инциденті таралған кезде; ұлттық қауіпсіздік органының, уәкілетті органның және ҚҚҰО-ның киберқауіпсіздік қатерлері, осалдықтары, оқиғалары мен инциденттері туралы сұрауы бойынша; киберқауіпсіздік инциденттерінің салдарларын жоюға көмек көрсету кезінде. КҚҚО ҚҚҰО-ның сұрауы бойынша ҚҚҰО-ға киберқауіпсіздікті қамтамасыз етудің қолданыстағы мониторинг жүйелеріне қол жеткізуді қамтамасыз етеді. Ақпараттық алмасу мына тәсілдермен жүзеге асырылады: деректерді кеңейтілген таңбалау тілі (eXtensible Markup Language – XML) немесе мәтіндік деректер алмасу форматы (JavaScript Object Notation – JSON) форматтарында шифрлауды пайдалана отырып электрондық хабарлама арқылы жіберу; деректерді XML немесе JSON форматтарында ақпарат алмасуға арналған бағдарламалық қамтамасыз етуді пайдалана отырып жіберу; шифрланған деректерді HTTPS (HyperText Transfer Protocol Secure) протоколын пайдалана отырып жіберу; деректерді уәкілетті органмен пайдалануға келісілген протоколдарды пайдалана отырып жіберу. Хабарламалармен алмасу КҚҚО мен ҚҚҰО арасында ҚҚҰО платформасын және отандық шифрлау сертификатын пайдалана отырып жүзеге асырылады. КҚҚО байланыс деректерін (электрондық пошта мекенжайы, 24/7/365 режимінде қолжетімді телефон) ұсынады, сондай-ақ тоқсан сайын, тоқсанның бірінші айының 10-күнінен кешіктірмей, байланыс деректерін растайды, жаңартады және ҚҚҰО-ға жібереді. Байланыс деректері өзгерген жағдайда, ҚҚҰО-ны жедел хабардар етеді. КҚҚО тоқсан сайын, есепті тоқсаннан кейінгі айдың 10-күніне дейінгі мерзімде ҚҚҰО-ға есепті тоқсанда тіркелген киберқауіпсіздік инциденттері және олардың туындау себептерін жою үшін қабылданған шаралар туралы ақпаратты ұсынады. Инциденттің деңгейі №354 бұйрыққа сәйкес келесі қағидаттар бойынша айқындалады: Жоғары, 4-деңгей. Қызметтерді ұсынудың/жұмыстарды орындаудың мүмкін болмауына, және (немесе) критиктілі деректердің жоғалуына/өзгертілуіне, және (немесе) критиктілі деректерді өңдейтін ақпараттандыру объектісінің құпиялылығының бұзылуына әкеп соғатын киберқауіпсіздік

	инциденттері. Орташа, 3-деңгей. Қызметтерді ұсынуды/жұмыстарды орындауды едәуір шектеуге, және (немесе) критиктілі болып табылмайтын деректердің жоғалуына/өзгертілуіне, және (немесе) критиктілі болып табылмайтын деректерді өңдейтін ақпараттандыру объектісінің құпиялылығының бұзылуына әкеп соғатын киберқауіпсіздік инциденттері. Төмен, 2-деңгей. Қызметтерді ұсынуға/жұмыстарды орындауға әсер етпейтін киберқауіпсіздік инциденттері. шабуылдың қалған іздерін жинау; ұқсас және мүмкіндігінше басқа шабуылдардың алдын алу үшін қажетті қорғау шараларын әзірлеу, жалпы КБ қамтамасыз ету процесін жақсарту; келтірілген зиянды азайту және қалпына келтіру. Жеткізуші Шартқа қол қойылғаннан кейін 60 күн ішінде Тапсырыс берушімен бірлесіп инциденттерге әрекет ету жөніндегі өзара іс-қимыл регламентін әзірлейді және келіседі. 5 Киберқауіпсіздік аудитін (Pentest) жүргізуге қойылатын талаптар 1. Желінің сыртқы сегментіндегі осалдықтарды талдау: Желілік инфрақұрылымның сыртқы периметрін жетекші сканерлік бағдарламалық қамтамасыз ету арқылы сканерлеу; Сканер анықтаған барлық осалдықтар білікті маман тарапынан қолмен тексеріліп, валидациялануы тиіс; Сыртқы сканерлеу аумағы – кемінде 200 объект (бірегей қоғамдық URL). 2. Желінің ішкі сегментіндегі осалдықтарды талдау: Ішкі URL-мекенжайлар VPN байланысы арқылы сканерленуі тиіс; Сканер анықтаған барлық хосттарды инвентаризациялап, ИТ-активтер картасын жасау; Анықталған хосттар мен URL-мекенжайлар ИТ-активтер картасына сәйкес ашық осалдықтарға тексерілуі тиіс. 3. Сыртқы сегментке кіруді тестілеу (Grey Box): Кибершабуылдарды имитациялау ар
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)	Өнім беруші Қазақстан Республикасы Ұлттық қауіпсіздік комитеті Төрағасының 2015 жылғы 30 қаңтардағы № 4 (1-тармақтың 3) тармақшасы, 3-қосымша) бұйрығымен бекітілген киберқауіпсіздікті қамтамасыз ету орталығының (КБО) қызметіне қойылатын талаптарға сәйкес келуі тиіс.

Приложение 16
к конкурсной документации

Техническая спецификация закупаемых услуг (заполняется заказчиком)

Наименование заказчика	Акционерное общество "Жасыл даму"
Наименование организатора	Акционерное общество "Жасыл даму"
№ конкурса:	№ 17980059-1
Наименование конкурса:	Услуги подключения к оперативному центру информационной безопасности (2027 г.)
Номер лота:	№ 88476600-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:	61396439
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	61396439
Срок оказания услуги:	по истечению 15 календарных дней с даты заключения договора по 31 декабря 2027 года
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Описание требуемых характеристик, параметров и иных исходных данных: Техническая спецификация на услуги по обеспечению информационной безопасности. Услуга по подключению к оперативному центру информационной безопасности (услуга по подключению к Центру обеспечения кибербезопасности) СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ И ТЕРМИНОВ 1. Заказчик АО "Жасыл Даму". 2. Поставщик Поставщик услуг. 3. ЦС Цифровая система. 4. ОС Операционная система. 5. СУБД Система управления базами данных. 6. ППО Прикладное программное обеспечение. 7. БД База данных. 8. ЛС Локальная сеть. 9. ЦОК Центр обеспечения кибербезопасности (ранее – оперативный центр обеспечения информационной безопасности) - юридическое лицо или структурное подразделение юридического лица, являющееся резидентом Республики Казахстан без участия иностранных юридических и физических лиц, осуществляющее деятельность по защите цифровых объектов. 10. Цифровой объект Заказчика Обособленный элемент цифровой среды, созданный, используемый или передаваемый посредством цифровых технологий, обладающий уникальными цифровыми характеристиками и позволяющий субъектам цифровой среды осуществлять правомочия владения, пользования либо распоряжения в объеме, установленном законодательством Республики Казахстан Заказчика. К цифровым объектам относятся: цифровые записи, цифровые активы, цифровые ресурсы, программное обеспечение, цифровые системы, цифровые платформы, объекты цифровой инфраструктуры, продукты цифровых данных, иные цифровые объекты, предусмотренные законами Республики Казахстан. 11. Объекты цифровой инфраструктуры Объектом цифровой инфраструктуры признается совокупность материальных, технических и технологических средств, обеспечивающих размещение и среду функционирования цифровых объектов. К объектам цифровой инфраструктуры относятся: центры обработки данных, сети телекоммуникаций, средства связи и иные инфраструктурные объекты. 12. КБ Кибербезопасность. 13. ИТ Информационные технологии. 14. ПО Программное обеспечение. 15. КВЦО Критически важные цифровые объекты - цифровые объекты, нарушение или прекращение функционирования которых приводит к незаконному сбору и обработке персональных данных ограниченного доступа и иных сведений, содержащих охраняемую законом тайну, чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или для жизнедеятельности населения, проживающего на соответствующей территории, в том числе инфраструктуры: теплоснабжения, электроснабжения, газоснабжения, водоснабжения, промышленности, здравоохранения, связи, банковской сферы, транспорта, гидротехнических сооружений, правоохранительной деятельности, "цифрового правительства". 16. НКЦКБ Национальный координационный центр кибербезопасности - структурное подразделение АО «Государственная техническая служба». 17. SIEM Система управления событиями кибербезопасности. 18. MISP Платформа для анализа угроз и

	обмена информацией по вопросам кибербезопасности (Threat Intelligence) 19. Центр мониторинга и реагирования на киберугрозы (далее – SOC) Подразделение Поставщика услуг, отвечающее за получение и обработку событий КБ, которое обеспечивает круглосуточный мониторинг инцидентов КБ силами аналитиков 1-ой линии, анализ инцидентов КБ силами аналитиков 2-ой линии, расследование инцидентов КБ, в том числе проведение ретроспективной аналитики и актуализация информации об угрозах и атаках, способах их детектирования и противодействия силами 3-ей экспертной линии. В состав Центра также входят средства защиты информации, с помощью которых происходит сбор событий КБ, их последующая корреляция и детектирование инцидентов КБ. 20. Инцидент КБ Событие или совокупность событий, негативно влияющих на кибербезопасность цифрового объекта. 21. Событие КБ Идентифицированное возникновение состояния цифрового объекта, указывающее на возможное нарушение кибербезопасности или ранее неизвестную ситуацию, которая может иметь отношение к обеспечению кибербезопасности. 22. Угроза КБ Совокупность условий и факторов, создающих предпосылки к возникновению инцидента кибербезопасности. 23. Площадка Инфраструктура Заказчика на которой размещаются компоненты Подсистемы по управлению событиями КБ 24. SLA (Service Level Agreement (Соглашение об уровне обслуживания)) Документированные параметры предоставляемой услуги. Параметры услуги - описание количественных и / или качественных действий (гарантированного состояния услуг(и)) с учетом фактора времени. 25. Web-интерфейс SOC Программное обеспечение (далее — ПО), предназначенное для автоматизированного сбора информации о выявляемых в рамках оказания Услуги инцидентах и предоставления доступа к ней уполномоченным специалистам Заказчика через личный кабинет в WEB-Интерфейсе ПО. 26. Корреляция Определение взаимосвязи между данными, содержащимися в двух и более событиях КБ. 27. Агрегирование Объединение событий КБ, содержащих одинаковую информацию. 28. Сценарий выявления атаки (далее — use – case; сценарий) Это возможный сценарий реализации угрозы КБ в отношении важных для Заказчика областей, таких как критичные системы, сегменты сети, группы сотрудников с учетом негативного влияния на целостность, конфиденциальность и доступность информации. Сценарий представляет собой описание ситуации, которую требуется наблюдать, отслеживать и предпринимать определенные действия в случае обнаружения 29. Типовой источник Источник событий КБ Заказчика, при подключении которых Поставщик может руководствоваться собственной базой знаний. 30. Нетиповой источник Источник событий КБ, который относится к системам собственной разработки Заказчика и/или требуется дополнительный анализ журналов событий и разработка парсера (обработчика) со стороны Поставщика. 31. Запрос на изменение Обращение, связанное с запросами на изменение конфигурации и (или) настроек ПО. 32. Дашборд (англ. – dashboard) Утилиты, позволяющие визуализировать различные тренды и показатели в виде

	консоли или панели управления с различными диаграммами, графиками, обновляемыми таблицами или виджетами. 33. Личный кабинет Заказчика Система, предназначенная для предоставления актуальной информации по статусу инцидентов КБ, предоставления отчётности и иной информации Заказчику. № п/п Наименование Требования 1. Общие данные Настоящая техническая спецификация содержит в себе требования на закупку услуг по обеспечению информационной безопасности, услуга по подключению к оперативному центру информационной безопасности. В соответствии с введенными в 2026 году нормами Закона Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «О кибербезопасности» является услугой по подключению к ЦОК цифрового объекта Заказчика. Включает в себя «Мониторинг и анализ событий КБ» цифровых объектов и объектов цифровой инфраструктуры Заказчика и помощь в реагировании на события и инциденты КБ. В рамках услуги должны быть решены следующие задачи: - организация и осуществление мониторинга событий и обработки инцидентов КБ, включая развёртывание в инфраструктуре Заказчика компонентов, необходимых для оказания Услуги (далее – Зона мониторинга); - круглосуточный мониторинг событий КБ, зафиксированных системами мониторинга и управления событиями кибербезопасности в Зоне мониторинга и системами защиты внешнего периметра; - круглосуточный мониторинг событий КБ, зафиксированных на серверном оборудовании и сетевых устройствах Заказчика; - направление Клиенту информации о выявленных инцидентах и методах реагирования на них и предоставление рекомендаций по их устранению; - направление уведомлений в центр реагирования на инциденты KZ-CERT НКЦКБ при возникновении инцидентов КБ по согласованию с заказчиком; - предоставление экспертной поддержки в процессе реагирования на инциденты КБ; - оказание помощи в проведении расследования инцидентов КБ, однако в случае если в Зоне мониторинга будет выявлено подозрительное событие, касающееся цифровых объектов и объектов цифровой инфраструктуры, не входящих в Зону мониторинга, о данном событии уведомляется Заказчик. Дальнейшее расследование Заказчик осуществляет самостоятельно, Поставщик при необходимости оказывает консультации для определения степени критичности и дополнительного анализа, с целью выявления источника проблемы и помощи в устранении инцидента специалистами Заказчика. 2. Границы оказания Услуги и подключение к ЦОК Объекты - цифровые объекты и объекты цифровой инфраструктуры Заказчика Местонахождение - Республика Казахстан, г. Астана Срок оказания услуги - 12 месяцев Период оказания услуги - 01.01.2027 – 31.12.2027 В случае необходимости работники Поставщика могут оказывать Услуги с выездом на территорию Заказчика (монтаж оборудования, настройка оборудования и др.). Заказчик должен обеспечить необходимый доступ работникам Поставщика, который обговаривается после заключения договора. Требования к составу работ по подключению, можно разделить на 4 этапа, в рамках каждого этапа определена цель и поставлены задачи для ее достижения.

	Этап 1. Обследование: Цель этапа – определить целевую архитектуру оказания услуги и определить список источников. Задачи, которые должны быть решены для достижения цели. На основании опросного листа, заполненного со стороны Заказчика, и интервьюирования представителей Заказчика, Поставщик проводит анализ цифрового объекта Заказчика, на основании которого производится: • выдача рекомендаций по составу и приоритезации подключаемых источников событий КБ (далее – источников); • определение потребностей Заказчика в части подключения уже существующих и разработки новых сценариев выявления атак. Для этого Заказчику направляется аналитический опросный лист для заполнения; • выработка организационно-технических решений по целевой архитектуре предоставления услуги и порядку развертывания компонентов; • определение порядка и организации межсетевого взаимодействия компонентов Услуги на площадке Заказчика и Центра мониторинга и реагирования на киберугрозы. В рамках данного этапа должны быть собраны, как минимум следующие сведения: - название источника; - описание функционала источника (принадлежность к цифровым объектам и объектам цифровой инфраструктуры Заказчика); - площадка размещения; - производитель/марка/модель; - тип/версия операционной системы; - тип/версия программного обеспечения; - Fully Qualified Domain Name; - IP-адрес. Этап 2. Внедрение: Цель этапа – развернуть компоненты услуги на площадке Заказчика и построить VPN-туннель между площадкой Заказчика и Поставщика: Задачи, которые должны быть решены для достижения цели: В случае отсутствия L3 связности между распределенными площадками, Поставщик и Заказчик выполняют организацию VPN-туннеля между площадкой Заказчика и Поставщика. * При взаимодействии не должна осуществляться фильтрация трафика путём блокирования используемого транспортного протокола; * Организация сетевых доступов между компонентами услуги и источниками событий, согласно запросу Поставщика; * Поставщик совместно с Заказчиком выполняют инсталляционные работы по внедрению компонентов Услуги в ИТ-инфраструктуре Заказчика. Этап 3. Подключение: Цель данного этапа – подключить источники событий и убедиться, что события в SIEM-систему поступают корректно, а также разработать новые сценарии выявления нарушений и инцидентов КБ на основании запроса Заказчика (при необходимости): Задачи, которые должны быть решенны для достижения цели: * Согласно этапу №1 и перечню источников, Поставщик предоставляет инструкции по их подключению; * Поставщик разрабатывает индивидуальные коннекторы для нетиповых источников; * после подключения источников Поставщик проверяет полноту индексируемых событий и, при необходимости, оптимизирует их; * Поставщик выполняет конфигурирование и профилирование SIEM-системы под цифровую инфраструктуру цифровых объектов Заказчика на основании заполненного Заказчиком аналитического опросного листа. Данные работы гарантируют работоспособность сценариев выявления нарушений и инцидентов КБ; * Поставщик разрабатывает новые

	сценарии, а именно расширение категорий инцидентов и правил корреляции на основании специфичных запросов Заказчика и/или основываясь на результатах анализа уязвимостей; * Поставщик предоставляет доступ уполномоченным представителям Заказчика в Дашборде компонентов Услуги для мониторинга услуги; * Заказчик предоставляет Поставщику список сотрудников, которым необходимо направлять информацию по инцидентам КБ, после чего Поставщик настраивает соответствующие группы уведомлений. Этап 4. Операционная работа: Цель этапа - адаптировать SIEM-систему под цифровую инфраструктуру Заказчика, настроить отправку уведомлений об инцидентах КБ в соответствии с SLA. Задачи, которые должны быть решены для достижения цели. В рамках оказания Услуги на базе Центра мониторинга и реагирования на киберугрозы Поставщик должен выполнять: * анализ событий КБ в режиме 24х7 силами аналитиков 1-ой линии Поставщика, которая является единой «точкой входа», поступающих от различных источников событий. Аналитики 1-ой линии должны обеспечивать обработку инцидентов КБ, проверку ложного срабатывания, проведение первичной аналитики и выделение инцидентов КБ на основе категорий инцидентов и правил, регистрацию и последующее сопровождение инцидента КБ в соответствии со стандартами ITIL (категорирование, приоритизация, SLA и т.д.). Режим оповещения по инцидентам КБ; * обработку инцидентов КБ силами аналитиков 2-ой линии Поставщика в режиме 8х5, проведение углублённой аналитики при решении инцидентов КБ с использованием различных специализированных инструментов; адаптацию правил корреляции в соответствии с изменениями в цифровой инфраструктуре Заказчика; добавление исключений в правила корреляции как по требованию Заказчика, так и на основании самостоятельного анализа профиля Заказчика; * при подтверждении Заказчиком, что данное событие является инцидентом КБ, инцидент переводится в статус и дальнейшая работа по инциденту ведется аналитиками 2 и 3 линии. Аналитики проводят углубленный анализ, ретроспективных событий, которые привели к инциденту КБ. Проведение первичного расследования инцидента КБ происходит путем выдачи рекомендаций, подготовки инструкций по реагированию на инцидент КБ, которые могут включать в себя также конфигурационные файлы для сбора событий непосредственно с источника. В рамках услуг должна быть реализована возможность визуализации аналитической информации по инцидентам КБ с помощью виджетов и/или Дашбордов (Личный кабинет), в котором Заказчику доступны следующие функции: * просмотр карточки инцидента по каждому инциденту КБ, с возможностью самостоятельного управления статусом инцидента; * просмотр статистики о произошедших инцидентах КБ; * регистрация обращений/инцидентов КБ и отслеживание их статуса в режиме реального времени; * просмотр информации по каждому инциденту КБ, который снабжен описанием выявленных техник атак; * предоставление в унифицированном шаблоне карточки инцидента по каждому выявленному инциденту КБ; * предоставление доступа через Дашборд для

	просмотра информации по подключенным источникам событий, дате подключения источника, что позволяет учитывать цифровые объекты и объекты цифровой инфраструктуры Заказчика, подключенные в SIEM-систему; * просмотр сводной информации о подозрительных действиях ТОП-5 выделенных групп пользователей; * выгрузка унифицированных отчетов из Личного кабинета. 3. Требования к оказанию услуг в части ЦОК В рамках исполнения требовании услуги Поставщик должен уметь выявлять основные категории инцидентов КБ: Unauthorized Access/Compromised. Инциденты, связанные с неавторизованным получением физического/логического доступа к защищаемой сети/системе/приложению/данным; Scans/Probes/Attempted Access. Инциденты, связанные с активностью, направленной на получение сведений о доступных хостах, открытых портах, уязвимостях, установленном ПО или иных сведений о целевом объекте, которые могут быть использованы нарушителем для дальнейшего планирования и развития атаки; Brute Force. Инциденты, связанные с успешными и неуспешными попытками подбора паролей в защищаемые системы; Vulnerability. Инциденты, связанные с успешной эксплуатацией уязвимостей, а также выявлением (с использованием сканеров) критичных уязвимостей (уязвимостей реализации), эксплуатация которых может привести к реализации угроз кибербезопасности; Malware. Инциденты, связанные с активностью вредоносного программного обеспечения (например, запуск шифровальщика, прописывание в автозагрузку трояна и т.п.); Malware C&C Communication. Инциденты, связанные с выявлением взаимодействия хостов защищаемой инфраструктуры с известными командными центрами; Malicious Host. Инциденты, связанные с доступом к ресурсам, выполняющим распространение вредоносного ПО (исключая известные командные центры ботнет сетей), либо связанные непосредственно с размещением в сети Интернет таковых ресурсов; Spam. Инциденты, связанные с распространением незапрашиваемой электронной почты, носящей информативный/рекламный характер; Fraud. Инциденты, связанные с мошенническими действиями пользователей защищаемой информационной системы; Social Engineering. Инциденты, связанные с побуждением пользователей защищаемой информационной системы к совершению действий (путём обмана или злоупотребления доверием), направленных на достижение целей нарушителя (осуществление операций по переводу денежных средств, переход по вредоносной ссылке, разглашение парольной информации и т.п.); Improper Usage. Инциденты, связанные с нарушениями требований политик/регламентов/инструкций КБ (например, доступ в Интернет в обход proxy, подключение к публичным Wi-Fi сетям, использование учётных записей доменного администратора на запрещённом хосте и т.п.); Suspicious Process Activity. Инциденты, связанные с аномальным поведением легитимных процессов. 4. Уведомление и реагирование на инциденты 1. ЦОК осуществляют обмен информацией с НКЦКБ, для выполнения возложенных на них задач и функций в сфере кибербезопасности 2. ЦОК обеспечивает доведение полученной от НКЦКБ информации до

	Заказчика. 3. ЦОК осуществляет взаимодействие с НКЦКБ в интересах решения задач, направленных на: 1) совершенствование механизмов предотвращения нарушений кибербезопасности; 2) улучшение деятельности ЦОК; 3) повышение оперативности и согласованности действий между ЦОК и НКЦКБ; 4) выработку совместных решений по повышению уровня кибербезопасности цифровых объектов. 4. Информация, необходимая для обеспечения кибербезопасности, относится к категории конфиденциальных цифровых данных, получение, обработка и использование которых ограничивается целями, для которых она собирается. Представление сведений от НКЦКБ в ЦОК и от ЦОК в НКЦКБ осуществляется в рамках Приказа и.о. Министра искусственного интеллекта и цифрового развития Республики Казахстан от 25 июня 2026 года № 354/НК «О внесении изменений в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 19 марта 2018 года № 48/НК «Об утверждении Правил обмена информацией, необходимой для обеспечения информационной безопасности, между оперативными центрами обеспечения информационной безопасности и Национальным координационным центром информационной безопасности» (далее – Приказ №354). 5. При обнаружении инцидента кибербезопасности ЦОК: - уведомляет НКЦКБ и собственника или владельца КВЦО в течение 15 (пятнадцати) минут с момента подтверждения инцидента кибербезопасности; - направляет в НКЦКБ карточку инцидента кибербезопасности по форме, согласно приложению к Приказу №354 в течение 72 (семидесяти двух) часов с момента подтверждения инцидента кибербезопасности. 6. При поступлении уведомления от НКЦКБ об инциденте кибербезопасности, ЦОК в течение 72 (семидесяти двух) часов с момента уведомления направляет в НКЦКБ: - результаты анализа угрозы кибербезопасности; - результаты анализа события кибербезопасности при подтверждении события кибербезопасности; - карточку инцидента кибербезопасности по форме, согласно приложению к Приказу №354 при подтверждении инцидента кибербезопасности. 7. Сбор данных осуществляется: 1) при проведении анализа сведений по возникшим угрозам, уязвимостям и инцидентам кибербезопасности; 2) при наличии оснований полагать, что инцидент кибербезопасности способен повлиять на работоспособность цифровых ресурсов, цифровых систем, сетей телекоммуникаций и других цифровых объектов; 3) при распространении угрозы, уязвимости и инцидента кибербезопасности; 4) по запросу органа национальной безопасности, уполномоченного органа и НКЦКБ об угрозах, уязвимостях, событиях и инцидентах кибербезопасности; 5) при оказании помощи при устранении последствий инцидентов кибербезопасности. 8. ЦОК по запросу НКЦКБ обеспечивает доступ НКЦКБ к имеющимся системам мониторинга обеспечения кибербезопасности. 9. Информационный обмен осуществляется следующими способами: 1) отправка данных в форматах расширенного языка разметки (eXtensible Markup Language - XML) или текстового формата обмена данными (JavaScript Object Notation - JSON) с помощью электронного сообщения с использованием

	шифрования; 2) отправка данных в форматах XML или JSON с использованием программного обеспечения для обмена информацией; 3) отправка зашифрованных данных с использованием протокола HTTPS (HyperText Transfer Protocol Secure); 4) отправка данных с использованием протоколов, согласованных к использованию уполномоченным органом. 10. Обмен сообщениями осуществляется между ЦОК и НКЦКБ с использованием платформы НКЦКБ и отечественного сертификата шифрования. 11. ЦОК предоставляет контактные данные (адрес электронной почты, телефон доступный в режиме 24/7/365), а также ежеквартально, не позднее 10 числа первого месяца квартала, подтверждает, обновляет и направляет контактные данные в НКЦКБ. В случае изменения контактных данных, оперативно информирует НКЦКБ. 12. ЦОК ежеквартально, в срок до 10 числа месяца, следующего за отчетным кварталом, предоставляет в НКЦКБ информацию об инцидентах кибербезопасности, зарегистрированных за отчетный квартал, и о мерах, принятых для устранения причин их возникновения. 13. Уровень инцидента определяется по следующим принципам, согласно Приказу №354: - Высокий, уровень 4. инциденты кибербезопасности, которые приводят к невозможности предоставления услуг/выполнения работ, и (или) потере/модификации критичных данных, и (или) нарушению конфиденциальности объекта информатизации, обрабатывающего критичные данные.; - Средний, уровень 3. инциденты кибербезопасности, которые приводят к существенному ограничению предоставления услуг/выполнения работ, и (или) потере/модификации данных, не являющихся критичными, и (или) нарушению конфиденциальности объекта информатизации, обрабатывающего данные, не являющихся критичными; - Низкий, уровень 2. инциденты кибербезопасности, не влияющие на предоставление услуг/выполнение работ; - Не определено, уровень 1. инциденты кибербезопасности, не влияющие на предоставление услуг/выполнение работ. 14. Устранение инцидента начинается с момента после его обнаружения, при содействии Заказчика в случае необходимости. Реагирование на Инцидент КБ состоит из следующих этапов: а) подтверждение/опровержение факта возникновения Инцидента КБ; б) классификация инцидента КБ; в) подтверждение/корректировка уровня критичности Инцидента КБ; г) уточнение дополнительных обстоятельств (деталей) Инцидента КБ; д) получение (сбор) доказательств возникновения Инцидента КБ, обеспечение их сохранности и целостности; е) минимизация последствий Инцидента КБ; ж) информирование и консультирование сотрудников по действиям обнаружения, устранения последствий и предотвращения инцидентов КБ; з) переоценка рисков, повлекших возникновение инцидента, актуализация необходимых положений, регламентов, правил КБ. 15. Анализ инцидентов (форензика), в том числе определение источников и причин возникновения инцидентов КБ, а также оценку их последствий осуществляет работник ЦОК совместно с сотрудниками, осуществляющими техническое обслуживание цифрового объекта и объектов цифровой инфраструктуры Заказчика. 16. В рамках проведения работ по

	компьютерной криминалистике ставятся следующие задачи: - разобраться в способе реализации взлома; - построить сценарий атаки; - восстановить хронологию атаки; - собрать оставшиеся следы атаки; - разработать необходимые меры защиты для предотвращения от подобной и по возможности от других атак, улучшая процесс обеспечения КБ в целом; - уменьшить и восстановить нанесенный ущерб. 17. Поставщик после подписания Договора, в течение 60 дней совместно с Заказчиком разрабатывают и согласовывают Регламент взаимодействия по реагированию на инциденты. 5. Требования к проведению аудита кибербезопасности (Pentest) 1. Анализ уязвимостей внешнего сегмента сети: - сканирование внешнего периметра сетевой инфраструктуры посредством лидирующего ПО класса сканеры уязвимостей; - все обнаружения сканера должны быть вручную проверены квалифицированным специалистом с целью валидации уязвимостей; - внешняя область сканирования - не менее чем 200 объектов (уникальные публичные URL). 2. Анализ уязвимостей внутреннего сегмента сети: - внутренние URL-адреса должны быть просканированы с использованием VPN-соединения; - сканер должен произвести инвентаризацию всех обнаруженных хостов; - обнаруженные хосты и URL-адреса должны быть проверены на предмет открытых уязвимостей. 3. Тестирование на проникновение внешнего сегмента сети с частичной или приблизительной информацией о предмете тестирования (Grey Box): - путем эмуляции кибератак, вручную оценить безопасность объектов цифровой инфраструктуры Заказчика с точки зрения внешнего пользователя (не работника), пытающегося получить доступ к учетной записи работника организации. - путем эмуляции кибератак, вручную оценить безопасность инфраструктуры в качестве работника организации, пытающегося увеличить привилегии, получить доступ к серверной части или обнаружить другие слабости средств кибербезопасности. 4. Результаты: - отчет о найденных уязвимостях, включая описание риска и важности находки; - отчет с рекомендациями по их устранению и повышению уровня защищенности; - рекомендации для снижения рисков от атак со стороны сетей общего пользования и со стороны внутренней сети; График проведения аудита (Pentest) согласовывается Поставщиком с Заказчиком дополнительно, в течение действия договора услуги. Периодичность проведения аудита – 6 (шесть) раз в течение действия договора услуги. Должны использоваться следующие стандарты для тестирования на проникновение: - PTES (Penetration Testing Execution Standard); - OWASP Top 10 (OWASP Testing Guide); - ISECOM OSSTMM. Процесс оказания услуги по проведению аудита (Pentest): Фаза Описание Результат 0. Подготовка и правила взаимодействия Kick-off, согласование Scope (внешний/внутренний периметр, AD, Wi-Fi, соц.инженерия, прод), выбор модели доступа (Black/Grey/White Box), окна вне рабочего времени, контактные лица, обмен техническими данными (диапазоны IP/доменов, VPN/jump-host, allowlist сканеров), создание тест-учёток при необходимости. Подтверждённые правила (RoE), финальный Scope, чек-лист

	предусловий. 1. Внешняя рекогносцировка OSINT, перечисление поддоменов/хостов/портов/сервисов, картирование точек аутентификации и возможных API Карта поверхности атаки. 2. Автоматизированное покрытие (внешний периметр) Профильные сканеры по веб-ресурсам и внешней инфраструктуре, базовый SCA зависимостей. Черновой список потенциальных находок. 3. Ручная проверка веб-приложений По OWASP WSTG/Top 10/ASVS: authN/authZ, бизнес-логика, инъекции (SQLi и пр.), XSS, SSRF, IDOR, конфигурации; тщательная проверка входа с учётом MFA/SSO. Подтверждённые веб-уязвимости (PoC/скрины). 4. Оценка внешней инфраструктуры Версии сервисов, экспонированные админ-панели, ошибки TLS/почтовой инфраструктуры, безопасная эксплуатация без DoS (вне РВ при риске). Подтверждённые инфраструктурные риски. 5. Внутренняя сеть и Active Directory Через VPN/jump-host: обзор сети, обнаружение уязвимых хостов, AD-misconfig (Kerberoasting/AS-REP, LAPS/LDAP, GPO), сегментация, привилегии; эскалации и латеральное движение - только безопасные техники, без влияния на бизнес. Карта угроз внутреннего периметра и AD, подтверждённые векторы. 6. Wi-Fi Аудит корпоративных/гостевых SSID, проверки аутентификации/шифрования, изоляции клиентов, captive-порталов Отчёт по Wi-Fi-рискам и рекомендации. 7. Соц. инженерия (по согласованию) Таргетированная фишинговая рассылка и/или vishing с безопасными payload, метрики: доставляемость/клики/ввод учётных данных; уведомление и обучение персонала. Метрики кампании, уроки и план повышения осведомлённости. 8. Аналитика и отчётность Агрегация результатов, CVSS v3.1, приоритизация (High/Medium/Low), рекомендации и roadmap; два формата — техотчёт + управленческое резюме. Комбинированный отчёт, артефакты (сканы/логи/PoC). 6. Зоны ответственности на период оказания услуги ЦОК Зоны ответственности: № Параметр Заказчик ЦОК Оказание услуги Мониторинг и анализ событий КБ 1.1 Мониторинг и анализ событий КБ (включая предоставление рекомендаций по реагированию на инциденты), зарегистрированных и касающихся элементов инфраструктуры Клиентов, входящих в Зону мониторинга. + 1.2 Мониторинг состояния компонентов подсистемы управления событиями КБ, установленных как на площадке Заказчика, так и на площадке Поставщика + 1.3 Обеспечение корректного функционирования подсистемы управления событиями КБ + 1.4 Установка агентов на источниках для отправки логов + 1.5 Направление сетевых потоков с источников в коллекторы + 1.6 Реагирование на инциденты КБ, их локализация, устранение последствий и восстановление штатного режима работы, согласно рекомендациям, предоставленным ЦОК + 1.7 Обеспечение работоспособности защищенных каналов передачи информации между площадками Заказчика и Поставщика + 1.8 Выполнение рекомендаций ЦОК и своевременное реагирование на инциденты КБ + 1.9 Предоставление актуального перечня серверного, коммуникационного и компьютерного оборудования, а также цифровых систем, входящих в Зону мониторинга + 7. Требования к системе мониторинга событий КБ (SIEM) Система

	должна быть единым платформенным решением; Система должна иметь возможность из коробки получать стандартные (syslog, SNMP, Netflow), структурированные, а также нестандартные логи; Система должна иметь встроенные механизмы сбора данных из СУБД АС (Oracle, MS SQL, PostgreSQL, IBM DB2 forLinux, Informix, Spark SQL, Sybase (SA, ASE, IQ), Teradata); Система должна обладать интерфейсом для загрузки данных из файлов (csv, txt, xml, xlsx), web сервисов (REST), по протоколам взаимодействия (http, https); Система должна обеспечивать автоматизированный агентный или безагентный сбор журналов регистрации с поддержкой протоколов: - Syslog; - Протоколы общего доступа SMB/CIFS, NFS, FTP/SFTP; - Сбор событий, хранящихся в журналах WindowsEventLog; - SNMP. Система должна предоставлять гибкий механизм для разбора текстовых данных любого (не предустановленного) формата из журналов регистрации и log-файлов. Система должна обладать инструментами для интеллектуального анализа текстовых данных; Система должна иметь возможность быть реализованной в распределенной архитектуре с возможностью горизонтального масштабирования на всех ее компонентах; Система должна иметь собственное хранилище данных без использования реляционной схемы; Система должна поддерживать возможность бесплатной установки приложений с официального магазина приложений от производителя программного обеспечения; Система должна поддерживать REST API для возможности интеграции с другими системами; Система должна предоставлять фреймворк для разработки приложений, поддерживаемый производителем, основанный на веб технологиях; Система должна обеспечивать поддержкой ролевой моделью доступа для разграничения доступа к определенным источникам данных, приложениям, отчётов или информационных панелей; Система должна поддерживать интеграцию и авторизацию с Active Directory, LDAP, SAML, RADIUS; Система должна обеспечивать построение высоконадежной (с доступностью 99.99%) архитектуры без единой точки отказа с использованием только штатных компонентов системы; Система должна поддерживать интеграцию и авторизацию со сторонними системами для осуществления двухфакторной аутентификации; Система должна иметь возможность шифровать коммуникации между компонентами; В системе в режиме реального времени должно быть реализованы следующие механизмы: - нормализация (приведение журналов регистрации к единому формату); - обогащение событий дополнительным данными и полями непосредственно в процессе сбора (например, присвоение событиям степени критичности, присвоение категории и пр.); - предобработка событий с использованием регулярных выражений (например, выделение требуемых полей, скрытие конфиденциальной информации и пр.); Система должна обеспечивать обработку не менее 50 ГБ данных ежесуточно (с резервом +20%); Система должна обеспечивать сбор данных с минимальными задержками, максимальная величина допустимой задержки для непрерывного потока событий не более 5 минутам; Система должна поддерживать возможность неограниченного количества

	обрабатываемых событий в секунду, лимитированное только аппаратными ограничениями; Система должна осуществлять долгосрочное хранение событий за период не менее 1 года; Система должна предоставлять инструмент для поиска и анализа данных по всем источникам данных по всему объему собранных данных. В системе должна быть возможность поиска по присвоенным информационным меткам и дополнительным полям; В системе должно быть реализовано механизм создания графических отчетов (диаграммы, графики). Система должна предоставлять механизм быстрой разработки визуляционных дашбордов через тонкий клиент силами конечных пользователей без необходимости программирования; Система должна обеспечивать выгрузку отчетов в открытых форматах (PDF, CSV, XML), отправку отчетов по электронной почте и выгрузку отчетов в сетевой каталог; Система должна обеспечивать следующие возможности поиска: - поиск по заданным критериям и значениям полей; - группировка событий; - сортировка событий по любому полю; - соединение событий разных журналов регистрации по ключевым полям; - скорость выполнения поисковых запросов не более 10 минут; - поддержка языка регулярных выражений в процессе поиска событий. Система должна предоставлять возможность самостоятельного создания новых поисковых запросов администраторам и пользователям системы без привлечения программистов заказчика; В системе должно быть реализован механизм гранулированного разграничения доступа к функциям и информации, хранимой в системе; Взаимодействие между частями системы должно вестись по защищенным протоколам (TLS). Управление системой должно производиться по защищенным протоколам (https, ssh); Система должна предоставлять функционал разработки отчетов с автоматической выгрузкой по заданному интервалу времени; Система должна обеспечивать выгрузку отчетов большого объема (до 5Гб); В системе должен быть реализован аудит действий администраторов и пользователей системы; В системе должен быть реализован механизм оповещений определенных пользователей при срабатывании определенных триггеров (наступлении критичных событий); Система должна обеспечивать возможность линейного масштабирования путем наращивания числа функциональных модулей (горизонтальное масштабирование); Система должна обеспечивать возможность выполнения ключевого функционала при условии отказа любого из компонентов системы; Система должна обеспечивать построение распределенной неиерархической базы данных с управляемыми уровнями репликации и поддержкой алгоритма Map-Reduce. При этом информация в каждой из частей хранилища должна храниться в сжатом виде; Архитектура системы должна позволять построение геораспределенного кластера, внутри которого каждый из сайтов должен быть полностью автономен, с возможностью репликации данных между сайтами с указанием количества и местоположения копий, создаваемых на каждом сайте; Система должна обеспечивать инструментами машинного обучения для прогнозирования определенных событий; Система должна предоставлять функционал расширения языка

	поисковых запросов силами конечного пользователя путем создания модулей на таких языках, как Python, C#, Java, JavaScript; Система должна поддерживать расширенную таксономию событий и полей. Пользователь должен иметь возможность добавлять свои собственные уникальные названия событий; Система должна обеспечивать возможность хранения как нормализованного, так и исходного необработанного формата журнала событий для проведения качественной форензики; Система должна обеспечивать возможность корреляции событий в реальном времени со значением статистических функций в событиях предыдущего периода; Система должна обеспечивать возможность создать любой кастомизированный отчет по потребностям заказчика; Система должна иметь возможность восстановления после сбоев; Система должна обеспечивать корреляцию информации с различных источников, которые никак не взаимодействуют между собой; Система должна иметь возможность обеспечивать следующие типы действий, как результат срабатывания правила: - отправка электронного письма; - создание инцидента; - запуск скрипта (с возможностью передачи параметров из события в скрипт и возможностью написания скрипта на распространенных скриптовых языках: bash, perl, python); - создание оповещения в веб консоли управления; - отправка snmptrap; - запуск сканирования (при наличии сканера уязвимостей); - отправка Syslog сообщения. Система должна поддерживать правила для обнаружения аномалий и отклонений от пороговых значений, а также поведенческий анализ; Система должна предоставлять графический мастер настройки правил для упрощения процесса их создания, а также улучшения точности результатов и уменьшения количества ложных срабатываний; Система должна иметь возможность ограничивать число одинаковых действий вследствие срабатывания правила на единицу времени (например, ограничить количество отправленных писем на почту вследствие срабатывания правила, чтобы не заполнять почтовый ящик администратора); Система должна обеспечивать возможность коррелировать дополнительные данные безопасности (географическое расположение, известный ботнет, уязвимость, каналы распространения, атакующие IP адреса и т.п.) Эти данные автоматически собираются этим же решением, без подключения дополнительных систем; Система централизованного сбора, хранения, обработки и анализа событий должна иметь возможность учета абонентов и первичных данных по предоставленным телекоммуникационным услугам сервисов IP телефонии (сетевое оборудование и сервера); Система должна обеспечивать приоритезацию инцидентов в зависимости от требований пользователя, а также критичности активов; Система должна обеспечивать корреляцию по определенным последовательностям событий и правил. (Например, сервис остановился и не возобновляется на протяжении 10 (десяти) минут. Либо одно правило сработало после другого в течение 10 (десяти) минут для одного и того же пользователя); Система должна обеспечивать сбор и нормализацию конфигураций свичей, маршрутизаторов; Система должна обеспечивать

	сравнение конфигураций устройств и выявление их изменений; Система должна обеспечивать выявление и сообщение об изменениях конфигурации, если эти изменения выходят за рамки дозволенных границ и политик; Система должна обеспечивать экспорт отчетности в Excel с самостоятельным заданием для пользователя необходимого шаблона формата XLS со временем генерации не более 10 секунд. Для генерации отчетности в Excel ПО должно обеспечивать возможность добавления нужных заголовков (полей); Система должна в реальном времени контекстно связывать выявленные события безопасности со знаниями об активах в сети; Система должна в реальном времени поддерживать search-based корреляцию или корреляцию, построенную на базе поисковых запросов; Система должна иметь возможность импортировать информацию с систем сканирования уязвимостей сторонних производителей; Система должна иметь возможность оперативного реагирования на действия администраторов цифровых систем (ИС); Формирование и рассылка отчетов по расписанию/по критерию; Возможность использования алгоритмов машинного обучения; Система должна иметь встроенный язык поисковых запросов с расширенными функциями (статистические, математические, текстовые и др.); Система должна поддерживать применение методов машинного обучения для обнаружения аномалий и потенциальных атак в сетевом трафике, включая распределённые атаки (DDoS); Система должна обеспечивать автоматическую интеграцию результатов анализа моделей машинного обучения в механизм корреляции SIEM и Risk-Based Alerting с возможностью формирования инцидентов и уведомлений при выявлении отклонений от нормального поведения; Система должна предоставлять пользователям возможность использования встроенной модели машинного обучения, разработанной для выявления распределённых атак (DDoS) с использованием ансамблевого метода Double Random Forest. Модель должна обеспечивать анализ сетевого трафика и автоматическое выявление аномалий, характерных для DDoS-активности с визуализацией результатов анализа моделей машинного обучения в панели мониторинга и с формированием аналитических отчётов, отображающих тенденции и выявленные аномалии; Для обеспечения сбора событий Поставщик, при наличии технической возможности, устанавливает агенты на сервера и рабочие станции. При отсутствии технической возможности установки агентов Заказчик обеспечивает отправку событий (логов) на SIEM по протоколу syslog. 8. Требования к системе обнаружения вторжений с расширенным функционалом, использующей механизмы сетевых ловушек и выявления аномального поведения на конечных устройствах. Требования к архитектуре 1. Решение должно развертываться без реорганизации, существующей L2/L3-топологии; сенсоры должны устанавливаться в целевые сетевые сегменты и принимать входящие подключения. 2. Состав должен включать: a) узел центрального управления (координация, локальное хранение логов/артефактов, обратный прокси, экспорт событий); b) узел ловушек (сенсор), запускающий контейнерные приманки. 3. Развертывание в

	виртуальной/облачной среде должно поддерживаться при наличии Linux и контейнерной платформы (включая VMware vSphere, Microsoft Hyper-V, KVM/Proxmox/OpenStack, Microsoft Azure). 4. Архитектура должна быть полностью контейнерной, обеспечивая изоляцию сервисов и обновление/перезапуск отдельных ловушек без простоя узла. 5. Масштабирование должно выполняться без повторной установки: добавление сенсоров и изменение набора ловушек – конфигурационно. 6. Архитектура с множеством сенсоров и выделенным узлом управления/сбора должна поддерживаться. 7. Размещение ловушек в разных сетевых сегментах должно обеспечиваться установкой дополнительных сенсоров. 8. Работа должна осуществляться без подачи NetFlow/sFlow/jFlow или сырых копий IP-трафика на вход; телеметрию должны формировать сами ловушки/службы узлов. 9. Системные требования полного развертывания должны составлять ориентировочно: a) узел управления - 16 ГБ ОЗУ, 4 vCPU, 256–500 ГБ SSD; b) сенсор - 8–36 ГБ ОЗУ, 4–8 vCPU, 128–300 ГБ SSD (в зависимости от профиля ловушек и сроков хранения артефактов). Требования к управлению 10. Решение должно предоставлять базовый веб-интерфейс (лендинг/страницы статуса); эксплуатация должна не требовать значительных затрат. 11. Веб-консоль должна быть доступна из актуальных версий Mozilla Firefox, Safari, Google Chrome. 12. Формирование офлайн-архивов логов и артефактов (включая PCAP) для автономного разбора/DFIR должно поддерживаться. Функциональные требования 13. Каждая ловушка должна конфигурироваться как уникальная: имя/описание, набор эмулируемых служб и их параметры (порты, баннеры, поведение). 14. Масштабирование на основе IP-алиасов не должно применяться; для разных IP-адресов должны использоваться дополнительные сенсоры и/или сетевые интерфейсы. 15. Периодическая активность ловушек должна настраиваться: a) обращения к внешним веб-ресурсам; b) разрешение имён через DNS/mDNS/LLMNR/NetBIOS; c) SMB-броузинг (получение списка общих ресурсов) по расписанию. 16. Обнаружение сетевых вторжений (brute force, попытки подключения к эмуляциям, обмен данными) должно фиксироваться; для шифрованных и нешифрованных протоколов должны сохраняться доступные рукопожатия/метаданные. 17. История взаимодействий должна отображаться и содержать: a) IP-адрес источника; b) использованные учётные данные (при наличии); c) протоколы/порты и временные метки. 18. Полностью автоматическое создание ловушек по профилям/шаблонам должно поддерживаться. 19. Набор типов ловушек должен включать как минимум: a) сервер RDP (баннер/рукопожатие); b) файловый сервер SMB; c) ловушка MS RPC (детект попыток подключения); d) SSH/Telnet-сервисы с записью сессий; e) веб-ловушки (HTTP/HTTPS), включая эмуляции административных веб-панелей; f) эмуляции страниц веб-аутентификации корпоративных сервисов; g) SCADA/HMI/PLC; h) сервер DNS (приманка); i) серверы БД MySQL и PostgreSQL; j) FTP-сервер; k) Samba; l) брокер MQTT. 20. Создание собственных типов сетевых ловушек на базе базовых через стандартизованные конфигурации

	(YAML/JSON), должно поддерживаться массовое автосоздание. 21. Уровень взаимодействия должен быть средним/низким: ответы на сканирование, запросы учётных данных, веб/текст-интерфейсы; использование Full-OS-ловушек не должно применяться. 22. Методика детектирования должна опираться на факт взаимодействия с эмуляторами сервисов и не должна требовать обязательного применения сигнатур. 23. Дамп сетевого трафика, связанный с уведомлениями о безопасности, должен формироваться в формате PCAP с привязкой по времени/порту. 24. Параллельная эмуляция нескольких протоколов на одном IP (мультисервис) должна поддерживаться. 25. Гибкая подмена баннеров/метаданных (версии ПО, заголовки, приветствия) должна обеспечиваться. 26. Профили развертывания (минимальный/стандартный/sensor-only) и массовое включение/отключение групп ловушек должны быть доступны. 27. Запись интерактивных сессий SSH/Telnet с возможностью воспроизведения и извлечения введённых учётных данных должна обеспечиваться. 28. Сбор артефактов атак (загрузки/пейлоады, команды нарушителя, протокольные ошибки) в структурированной файловой иерархии должен выполняться. 29. Конфигурации должны вестись в текстовом виде (YAML/ENV) и подходить для хранения в VCS (контроль изменений/откаты). 30. Исходящие соединения ловушек должны ограничиваться политиками хоста (allow-list) для снижения операционных рисков. 31. Параметры веб-ловушек должны поддерживать: a) настройку заголовка сервера; b) ограничение скорости (rate-limit); c) перечень допустимых HTTP-методов; d) настраиваемые пути/файлы и ответы; e) произвольные HTTP-заголовки; f) установку TLS-сертификата. Требования к интеграции 32. Переадресация системных и журналов безопасности через защищённый транспорт 33. На узлах Системы должен быть установлен агент сбора журналов, выполняющий файловый мониторинг каталогов журналов Системы: 34. Для корректной обработки ротации и исключения дубликатов должна применяться устойчивая идентификация файла (аналог соли для контрольной суммы по полному пути). 35. Доставка событий в платформу аналитики должна выполняться по одному или нескольким из следующих протоколов: - Syslog over TLS (RFC 5425); - HTTPS с телом запроса JSON (HTTP POST); - Сбор событий с помощью агента SIEM. 36. Семантика доставки - at-least-once; на стороне агента должны быть включены устойчивые очереди и подтверждения приёма (ACK/эквивалент), с экспоненциальным повтором (backoff) при недоступности приёмника, отправка данных в SIEM систему с использованием шифрования. Требования к обучению персонала Заказчика 37. Поставщик должен предоставить пакет документации (админ-гайд, runbook инцидентов, чек-листы запуска/обновления) и провести вводное обучение администраторов (не менее 4 часов), включающее: - развертывание и обновление; - создание/изменение профилей ловушек; - сбор «инцидент-пакета» (логи, PCAP, записи сессий); - интеграцию с SIEM и настройку уведомлений. 38. Подсистема аналитики должна обеспечивать приём структурированных событий от Системы ловушек,

	их категоризацию, визуализацию и оповещение о значимых инцидентах. Решение должно предоставлять аналитические панели (дашборды), средства фильтрации/дрила и экспорт отчётности. Формат и состав событий: 39. События должны передаваться в формате JSON/эквивалент с кодировкой UTF-8. Минимальный состав полей должен включать: - @timestamp - время события в UTC (ISO-8601 или Unix-epoch); - src.ip - IP-адрес источника; - dest.ip - IP-адрес целевого узла (сенсора/ловушки); - network.protocol - протокол (tcp/udp/http/ssh/rdp и др.); - network.transport и/или dest.port - транспорт/порт; - event.type - тип события (например: connection_attempt, auth_success, data_transfer); - event.category - категория атаки - meta.* - дополнительная метаинформация (учётные данные, хэши файлов, команды, URL, user-agent и др.). Нормализация времени: при отсутствии поля времени должно использоваться время приёма; часовой пояс по умолчанию - UTC. Поля должны быть пригодны для агрегаций (типизированы: IP, число, строка, дата). Категоризация событий 40. Каждое событие должно иметь одну или более категорий из следующего перечня (минимум): Network, Passwords, SSH/console, RDP, Service, Webpage, E-Mail, Industrial. Категория должна использоваться для визуализации и построения сводных метрик. Возможность расширения перечня категорий должна поддерживаться конфигурационно. Визуальные представления (дашборды) 41. Обзор атак (Overview) - общий счётчик событий за выбранный интервал (не менее: 60 секунд, 1 час, 24 часа) и график интенсивности по времени. 42. Географическое распределение - карта с агрегацией по странам источников и/или по целевым сегментам. Распределение по типам атак - диаграммы/гистограммы по event.category. Распределение по портам - графики активности для наиболее частых портов (в т.ч. 22/tcp, 23/tcp, 445/tcp, 1433/tcp, 3389/tcp). Распределение по URL - статистика обращений к эмулированным веб-страницам (например, /, /index.php, /robots.txt). Тренды - графики средней активности на одну ловушку за день/неделю/месяц. Панели должны поддерживать сохранение преднастроенных представлений (presets). Оповещения и каналы доставки 43. Для событий уровня предупреждения и критических инцидентов должна поддерживаться система уведомлений. Фильтрация, агрегация и drill-down 44. Фильтрация должна поддерживаться по: IP-адресам/странам источников, типам ловушек, категориям атак, портам/протоколам, временным интервалам. Переход от агрегатов к первичным записям (drill-down) должен быть доступен из любого графика/таблицы. Детализированные журналы должны отображать первичные поля события и предоставлять экспорт. Графический стиль 45. Графическая визуализация должна быть выдержана в едином стиле. Категории атак должны иметь различимые цвета; рекомендуется следующая палитра по умолчанию: Network - синий; Passwords - жёлтый; SSH/console - оранжевый; RDP - фиолетовый; Service - бирюзовый; Webpage - зелёный; E-Mail - красный; Industrial - серый. Цвета должны быть настраиваемыми. Отчётность и

	экспорт 46. Должно поддерживаться формирование отчётов в форматах PDF и/или CSV с ключевыми метриками за заданный период. Экспорт агрегированной статистики должен поддерживать форматы JSON и CSV. Планирование периодических отчётов (например, ежедневно/еженедельно) должно поддерживаться с указанием получателей/каналов. 9. Требования к устройству защиты электронной почты Защита корпоративной электронной почты: оборудование должно быть предоставлено во временное пользование на период договора оказания услуг и функционировать в качестве шлюза между почтовым сервером и внешней средой и соответствовать следующим требованиям: Наименование Требования Архитектура и форм-фактор • Rack mount, 1U Количество • 1 шт Всего интерфейсов • не менее 4x GE RJ45. Консольный порт: RJ45 Возможность настройки доменов • не менее 70 Политики получателей входящие или исходящие (на домен/систему): • не менее 400/1500 Почтовые ящики в режиме сервера • не менее 400 Профили Анти спам, Анти вирус, Аутентификация и Контент (на домен/систему) • не менее 50/200 Производительность маршрутизации почты (сообщения в час) • не менее 250K Производительность Антиспама + Антивирус (сообщений в час) • не менее 200K Объем хранилища • не менее 2TB Источник питания переменного тока • не менее 100–240V AC, 50–60 Hz Максимальная требуемая мощность (средняя) • не менее 77 W Рабочая температура • от 0 до 40 C Влажность без конденсации • от 5 до 90% Системные особенности • Режимы развертывания Прозрачный, Шлюз и Сервер. • Гибкая настройка интерфейсов включая VLAN и поддержку резервных интерфейсов. • Инспекция входящего и исходящего трафика. • Поддержка многих доменов электронной почты с настройкой уровня домена. • Поддержка работы с почтовыми системами Exchange и iRedMail и др. • Поддержка IPv4 и IPv6 • Виртуальный хостинг с использованием пулов IP адресов источника и получателя. • Архивирование почты на основе политик с опцией удаленного хранения. • Поддержка аутентификации SMTP через LDAP, RADIUS, POP3 и IMAP. • Маршрутизация почты на основе LDAP. Инспекция по пользователям с применением LDAP атрибутов на основе политик (доменов). • Общий интерфейс web-почты для серверного режима и управления карантином. Управление почтовой очереди. • Соответствие RFC электронной почты. • Поддержка репутационной базы локальных отправителей, на основе: -Sender Policy Framework (SPF) - Domain Keys Identified Mail (DKIM) Управление, журналирование и отчетность • Административные аккаунты для доменов на основе ролей. • Общее журналирование и отчетность активностей и инцидентов. • Встроенный модуль отчетности. • Централизованный карантин для развертывания крупных масштабов. • Поддержка SNMP с использованием стандартных и частных MIB. • Поддержка локального и внешнего сервера хранения, включая поддержку iSCSI. • Поддержка внешних Syslog. Резервирование системы • Поддержка во всех режимах развертывания. • Активное / Пассивное резервирования. • Режим синхронизации конфигурации. • Синхронизация карантина и почтовой

	очереди. • Определение и уведомление об отказе устройств. • Поддержка функций интерфейсов: статус, восстановление, избыток. Антиспам профили • Анти спам: -Глобальная репутационная база отправителей -Фишинг, спам URL и электронные адреса -Контрольные суммы спам объектов -Динамические эвристические правила Защита от вспышек (outbreak). • Серые списки для IPv4, IPv6 и аккаунтов электронной почты. • Поведенческий анализ. • Глубокая инспекция заголовка электронного письма. • Гибкие профили действий и сообщений. • Спам URI третьей стороны и черные списки в реальном времени (SURBL / RBL). • Карантин, пометка и отчетность о конечном пользователе. • Сканирование PDF и анализ изображений. • Черные / белые списки на глобальном, доменном и пользовательском уровнях. • Статистическая фильтрация по Байесу. Антивирус • Антивирусная служба. • Карантин, переупаковка, замена и мониторинг. • Сканирование вложенных архивов. • Выявление вредоносного программного обеспечения. • Эмуляция кода на борту. Защита на основе контента • Фильтрация на основе словаря для входящего и исходящего направлений. • Предварительно определены HIPAA, SOX, и GLBA словари. • Фильтр по типу вложенного файла. • Фильтрация по запрещенным словом. Требование защита от DoS • Ограничение скорости входящих и исходящих сообщений. • Защита от атак в адрес получателя. • Проверка обратного DNS (анти-спуфинг). Требования к шифрованию • Шифрование на основе личности для Push / Pull доставки зашифрованных сообщений. • Поддержка S-MIME для Gateway-to-Gateway шифрования. • Поддержка протоколов HTTPS, SMTPS, SSH, IMAPS и POP3S Требования особенности режима сервер • Сервисы электронной почты: SMTP, IMAP и POP3. • Поддержка SMTP через SSL. • Поддержка квотирования дискового пространства для аккаунтов пользователей. • Поддержка доступа через защищенный клиент. • Поддержка пользователей, групп и псевдонимов. • Аутентификация локальная и через LDAP. • Календарь. • Автоответ и перенаправления. • Синхронизация адресной книги с LDAP. Требования к технической поддержке • Оборудование должно обеспечиваться гарантией от производителя сроком не меньше 1 года. • Условия гарантии должны включать в себя возможность обращения запросов в техническую поддержку производителя, регистрации сервисных случаев, замены оборудования в случае его выхода из строя, обновления микрокода системы и версии установленного ПО. • Обновление сигнатур систем антивируса, доступ онлайн антиспама и Virus Outbreak Service не менее 1 года • Постоянный авторизованный доступ к сайту производителя Требования к поставке • В целях исключения поставки контрафактного оборудования поставщик обязан предоставить в адрес заказчика авторизационное письмо от официального производителя, подтверждающее право поставщика на поставку указанного оборудования на территории Республики Казахстан • Срок поставки: в течение 5 рабочих дней с момента подписания договора Поддержка платформ виртуализации для развертывания • VMware ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0, Microsoft

	Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure Сетевые виртуальные интерфейсы (минимум/максимум) • 1/4 Количество устройств для централизованного сбора логов • Не менее 10 Допустимый объём обработки логов в день • Не менее 5 Gb/день (неограниченный в режиме collector) Допустимый объём хранилища • Не менее 3500 GB Инструменты отчетности и визуализации • Генерирование графиков для конкретного случая с возможностью фильтрации по топ пользователям, приложениям, направлениям, веб-сайтам, угрозам, использованию VPN и другим. • Встроенные шаблоны отчетов. Использование или модификация PDF-шаблонов для отображения цветных, комплексных, графических отчетов по использованию и функциям безопасности сети. • Регулярный анализ профилей безопасности и характера трафика/ пропускной способности в отчетах. • Контроль важных событий для отчетности перед администратором о потенциально аномальном поведении устройств Отображение журналов • Отображение исторических логов или в реальном времени. • Выборка из логов трафика, логов событий и логов безопасности. • Поиск по устройству, ADOM или в совокупности. • Фильтрация логов и функции поиска. • Гранулированный обзор с панелью деталей лога • Интуитивно понятный интерфейс. Управление событиями • Конфигуратор комплексных предупреждений. • Триггеры для всех уровней "severity" журналов, конкретных событий, действий и направлений. • Установка порогов по количеству событий для конкретного промежутка времени. • Просмотр или поиск исторических предупреждений. • Сообщение по электронной почте / SNMP или syslog. Архивирование DLP • Исследование архивов DLP контента. • Поддержка источников архивов: электронная почта, HTTP, FTP, IM. • Просмотр архивов текста или загруженных файлов. Взаимодействие соборудование других вендоров • Да, JSON и XML API Гарантия и сервисная поддержка • Оборудование должно обеспечиваться гарантией на весь срок договора оказания услуг. • Получение всех необходимых обновлений. • Получение основных и промежуточных релизов. программного обеспечения через сайт или поддержка программных кодов в актуальном состоянии в соответствии с рекомендациями производителя, в том числе микрокодов устройств. • Предоставление консультаций по телефону, электронной почте и на сайте поддержки производителя с понедельника по воскресенье с 00.00 до 24.00 часов круглосуточно; • Постоянный (24 часа х 7 дней) авторизованный доступ к сайту производителя. Подписки • Оборудование должно быть оснащено подпиской на службу автоматизации безопасности VM на 1 год, включающая в себя автоматизацию безопасности, включая премиум-отчеты, обработчики событий, правила корреляции SIEM для расширенного обнаружения угроз и сценарии SOAR. (1-6 ГБ журналов в день) • Оборудование должно быть оснащено подпиской на службу VM IOC и службу обнаружения вспышек вирусов (1-6 ГБ журналов в день) сроком на 1 год. 10. Требования к сопровождению средств защиты внешнего периметра и сетевой

	безопасности Поставщик должен обеспечить настройку политик безопасности, мониторинг, анализ и защиту внешнего периметра – межсетевого экранирования (NGFW / Proxy / IPS / IDS), активного сетевого оборудования объектов цифровой инфраструктуры Заказчика. Оказывать содействие в процессах логического и физического сегментирования локальной сети и управления сетевыми соединениями, в рамках обеспечения сетевой безопасности. Поставщик должен обеспечить содействие в защите веб-приложений от кибератак и уязвимостей, путем настройки политик безопасности, фильтрации трафика, мониторинга и обновления правил безопасности. 11. Требования к платформе для обучения по вопросам кибергиены В рамках оказания услуг Поставщик обязан предоставить Заказчику доступ к облачной платформе обучения кибергигиене (далее – Платформа), обеспечивающей: прохождение работниками Общества обучающих курсов по вопросам кибергигиены на казахском и русском языках; - прохождение работниками Общества тестирования по вопросам кибергиены, а также возможность повторного прохождения тестирования при неудовлетворительном результате; - выдачу сертификатов работниками Общества, успешно прошедшим тестирование. Доступ к Платформе предоставляется Поставщиком по заявке Заказчика для работников Общества для создания учётных записей. Поставщик обязан обеспечить Заказчику доступ к административной панели Платформы для просмотра и выгрузки следующих данных: - ФИО работника; - дата и время прохождения тестирования; - результат (количество правильных ответов / процент); - статус (пройден / не пройден); - наличие выданного сертификата. Данные о результатах обучения должны храниться на Платформе и быть доступны Заказчику в режиме реального времени. По запросу Заказчика, Поставщик обязан предоставить выгрузку результатов в формате XLSX/CSV. 12. Требования к анализу защищённости исходного кода Поставщик должен обеспечить проведение анализа защищённости ПО цифровых систем или разработанного прикладного ПО Заказчика. В рамках оказания услуг Поставщик должен обеспечить: 1. Статический анализ (SAST) исходного кода, байт-кода и бинарных файлов без выполнения приложения, направленный на выявление уязвимостей, ошибок программирования и потенциально небезопасных конструкций программного кода. 2. Применение средств SAST, поддерживающих не менее 15 языков программирования, включая Java, C#, C/C++, Python, PHP, JavaScript, TypeScript, Go, Rust, Kotlin, PL/SQL, Delphi, Scala и другие. 3. Динамический анализ (DAST) функционирующих веб-приложений и API с выявлением уязвимостей, проявляющихся при эксплуатации программного обеспечения, и корреляцией результатов SAST и DAST при анализе одного объекта. 4. Классификацию выявленных уязвимостей по применимым категориям OWASP Top 10, CWE/SANS Top 25, OWASP ASVS/MASVS, PCI DSS и HIPAA с учётом актуальных редакций указанных стандартов и классификаторов. 5. Формирование отчётов по результатам проверок с возможностью выгрузки в форматах PDF, HTML, CSV и SARIF, а также сравнения

	результатов первичных и последующих проверок. 6. Предоставление отчёта по каждой проверке с указанием выявленных уязвимостей, уровня их критичности, мест обнаружения, подтверждающих материалов и рекомендаций по устранению. Количество проверок — не менее 12 (двенадцати). Методы проведения проверок (SAST и/или DAST), перечень проверяемых информационных систем, компонентов и сроки проведения определяются Заказчиком в рамках оказания услуг. Под одной проверкой понимается проведение анализа защищённости одного согласованного объекта проверки выбранным Заказчиком методом (SAST или DAST) с предоставлением соответствующего отчёта. Поставщик обязан обеспечить конфиденциальность полученных исходных кодов, результатов анализа и иной информации Заказчика, а также исключить их передачу третьим лицам без письменного согласования с Заказчиком. 13. Требования к качеству оказания услуг Поставщиком 1. Поставщик обязан обеспечить качественное и своевременное оказание услуг в соответствии с требованиями действующего законодательства Республики Казахстан, в том числе: Цифрового кодекса Республики Казахстан от 9 января 2026 года № 255-VIII ЗРК; Закона Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «О кибербезопасности»; Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»; постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» в действующей редакции; приказа Министра оборонной и аэрокосмической промышленности Республики Казахстан от 19 марта 2018 года № 48/НҚ «Об утверждении Правил обмена информацией, необходимой для обеспечения кибербезопасности, между центрами обеспечения кибербезопасности, отраслевыми центрами кибербезопасности и Национальным координационным центром кибербезопасности» в редакции приказа исполняющего обязанности Министра искусственного интеллекта и цифрового развития Республики Казахстан от 25 июня 2026 года № 354/НҚ; приказа Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ Об утверждении Правил проведения мониторинга обеспечения кибербезопасности цифровых объектов «цифрового правительства» и критически важных цифровых объектов Приказа и.о. Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 февраля 2018 года № 33/НҚ «Об утверждении Правил проведения мониторинга выполнения единых требований в сферах цифровизации и обеспечения кибербезопасности» иных нормативных правовых актов Республики Казахстан, регулирующих деятельность центров обеспечения кибербезопасности, мониторинг и реагирование на инциденты кибербезопасности, в части, применимой к оказываемым услугам. При оказании услуг Поставщик должен учитывать применимые положения международного стандарта ISO/IEC 27001:2022 «Information security, cybersecurity and privacy protection — Information security management systems —

	Requirements». 2. Поставщик должен иметь действующую лицензию на осуществление деятельности по выявлению технических каналов утечки информации и специальных технических средств, предназначенных для проведения оперативно-розыскных мероприятий, с соответствующим подвидом деятельности, необходимым для оказания услуг Центра обеспечения кибербезопасности. В подтверждение соответствия указанному требованию Поставщик предоставляет копию действующей лицензии с соответствующим приложением либо сведения, позволяющие проверить наличие лицензии в государственной информационной системе «Е-лицензирование». 3. Заказчик вправе в течение всего срока действия договора осуществлять контроль качества, полноты и своевременности оказываемых услуг, проверять соблюдение Поставщиком требований технической спецификации, запрашивать отчёты, подтверждающие материалы и иную документацию, относящуюся к исполнению договорных обязательств. Поставщик обязан предоставлять запрашиваемые сведения и документацию в согласованные с Заказчиком сроки. 4. Поставщик обязан обеспечивать сохранность и конфиденциальность информации Заказчика, полученной в ходе оказания услуг, включая сведения из цифровых систем, цифровых ресурсов, баз данных, журналов событий кибербезопасности, а также взаимодействующих с ними внешних цифровых систем. Поставщику запрещается разглашать, передавать третьим лицам и использовать в собственных целях полученную информацию без предварительного письменного согласия Заказчика, за исключением случаев, предусмотренных законодательством Республики Казахстан. Обязательства по обеспечению конфиденциальности распространяются на работников Поставщика и привлечённых им лиц и сохраняются после завершения оказания услуг. 5. Хранение и обработка информации Заказчика, включая персональные данные, журналы событий кибербезопасности, сведения об инцидентах и отчётные материалы, должны осуществляться с использованием технической инфраструктуры и информационных ресурсов, расположенных на территории Республики Казахстан. Хранение персональных данных должно соответствовать требованиям статьи 12 Закона Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите». Передача информации Заказчика за пределы Республики Казахстан допускается исключительно при наличии предусмотренных законодательством оснований и предварительного письменного согласования с Заказчиком. 6. Поставщик обязан обеспечить взаимодействие с Национальным координационным центром кибербезопасности в соответствии с Правилами, утверждёнными приказом от 19 марта 2018 года № 48/НҚ в редакции приказа от 25 июня 2026 года № 354/НҚ, включая своевременное информирование о подтверждённых инцидентах кибербезопасности, обмен информацией об угрозах и инцидентах, предоставление установленных отчётных сведений и использование предусмотренных нормативными правовыми актами защищённых способов информационного взаимодействия. 7. Поставщик несёт ответственность за качество, полноту и своевременность оказания услуг,

	соблюдение требований кибербезопасности и конфиденциальности информации в соответствии с законодательством Республики Казахстан и условиями договора. 14. Место оказания услуг г. Астана район Нұра, ул. Проспект Кабанбай батыра, д. 11/5 15. Конфиденциальность Поставщик обязуется не разглашать и не передавать третьим лицам конфиденциальную информацию, полученную в ходе исполнения договорных обязательств, за исключением государственных органов в порядке, предусмотренном законодательством РК.
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)	Поставщик должен соответствовать требованиям к деятельности центра обеспечения кибербезопасности (ЦОК), утверждённым приказом Председателя Комитета национальной безопасности Республики Казахстан от 30 января 2015 года № 4 (подпункт 3) пункта 1, приложение 3).