

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

Тапсырыс берушінің атауы:	"Нұрсұлтан Назарбаев халықаралық әуежайы" акционерлік қоғамы
Ұйымдастырушының атауы:	"Нұрсұлтан Назарбаев халықаралық әуежайы" акционерлік қоғамы
Конкурстың №:	№ 17791876-1
Конкурстың атауы:	Ақпараттық қауіпсіздік аудитін жүргізу жөніндегі қызмет. Тел.: 8 (7172) 777-377, 777-177
Лоттың нөмірі:	№ 88073656-OK1
Лоттың атауы	Ішкі тексеру жүйесінің сыртқы бақылауын жүргізу бойынша қызмет көрсетулер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	749020.000.000004
Қызметтің атауы:	Ішкі тексеру жүйесінің сыртқы бақылауын жүргізу бойынша қызмет көрсетулер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	15690431.03
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	15690431.03
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	шартқа қол қойылған күннен бастап 15 күнтізбелік күн өткен соң, 30 күнтізбелік күн ішінде

Аванстық төлем мөлшері:	0
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Терминдер мен қысқартулар АҚ - Ақпараттық қауіпсіздік; АТ - Ақпараттық технологиялар; АКТ - ақпараттық-коммуникациялық технологиялар; ДБЖ - деректерді беру желісі; ІНҚ - ішкі нормативтік құжаттама; Қызметтер / жоба - ақпараттық қауіпсіздік аудиті. 1. Сатып алынатын қызметтердің мақсаттары мен міндеттері Қызмет көрсетудің негізгі мақсаттары: - Тапсырыс берушінің ақпараттық қауіпсіздігінің (АҚ) ағымдағы жай-күйі туралы объективті және анық ақпарат беру; - Тапсырыс берушінің бизнес-қызметі үшін тәуекелдерді барынша азайтуға бағытталған АҚ басқару саласындағы ішкі бақылау жүйесін жетілдіру; - Тапсырыс берушінің ақпараттық активтерінің сенімділігін, қолжетімділігін және қауіпсіздігін арттыру; - ақпараттық қауіпсіздік жүйелерінің Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысының талаптарына сәйкестігін қамтамасыз ету-ақпараттық – коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптар (бұдан әрі-бірыңғай талаптар). Тапсырмалар: - Тапсырыс берушінің ақпараттық жүйелерінің функционалдық мүмкіндіктеріне талдау жүргізу және олардың АҚ саласындағы әлемдік стандартқа сәйкестігіне шолу жүргізу; - бірыңғай талаптарға сәйкес Ақ бағытында Тапсырыс берушінің ақпараттық жүйелерін одан әрі дамыту бойынша ұсынымдар дайындау; - желілік инфрақұрылымды, серверлік және телекоммуникациялық жабдықты қоса алғанда, акт-инфрақұрылымына шолу жүргізу; - ақпараттық қауіпсіздікті бірыңғай талаптарға сәйкестігін қамтитын ақпараттық жүйелерде Қағидаларға ревизия жүргізу; - ақпараттық активтердің сенімділігін, қолжетімділігін және қауіпсіздігін арттыру бойынша ұсынымдар дайындау; - АҚ аудитінің нәтижелері бойынша талдамалық есепті, Тапсырыс берушінің басшылығына ұсыну. 2. Іс-шаралар тізбесі және көрсетілетін қызметтердің нәтижелері Қойылған мақсаттарды іске асыру мынадай кезеңдер шеңберінде жүзеге асырылуы қажет: 1. Қолданыстағы ЖҰӨ және АҚ қызметінің процестерін талдау. 2. Ақпараттық жүйелердің функционалдық мүмкіндіктерін және бірыңғай талаптарға сәйкестігін талдау. 3. Акт инфрақұрылымына шолу, атап айтқанда желілік инфрақұрылымды құру қауіпсіздігін талдау. 4. Осалдықтарды сканерлеуді және енуге сыртқы тестілеуді қоса алғанда ақпараттық активтердің қорғалуын тексеру. 5. Есепті қалыптастыру және презентация өткізу. Аудит қызметтерінің сипаттамасы 1 кезең. Аудит мақсаттарына сәйкес жоба шеңберін айқындау 1. Жұмыстардың тізімін, оларды іске асырудың реттілігін келісу және АҚ аудиті кезінде ұсыну үшін талап етілетін құжаттар тізімін сипаттау. Нәтижесі: келісілген жұмыс жоспары, Тапсырыс беруші тарапынан құжаттар мен жауапты тұлғаларды ұсыну кестесі. 2 кезең. АҚ инфрақұрылымының ағымдағы жай-күйін бағалау, олардың бірыңғай талаптар критерийлеріне сәйкестігіне шолу жүргізу 1. Ағымдағы ақ процестерінің ҚР СТ ISO/IEC 27001-2015 бірыңғай талаптары мен талаптарына сәйкестігін талдау. 2. ҚР СТ ИСО27001 бірыңғай талаптары мен әдіснамасына сәйкес іске асырылған ақ процестерінің тиімділігін бағалау. 3. АҚ
--	---

	бойынша қолданылатын шешімдердің тиімділігін талдау (қолданылатын саясаттар, параметрлер). 4. Қолданылатын құралдардың бірыңғай талаптарға сәйкестігін бағалау. 3 кезең. Желілік инфрақұрылымды, серверлік және телекоммуникациялық жабдықты қоса алғанда, акт инфрақұрылымына шолу 1. Акт-инфрақұрылым объектілерінің (СПД, серверлік және телекоммуникациялық жабдық) конфигурациялық параметрлері мен параметрлеріне мынадай талаптар бойынша технологиялық бағалау жүргізу: - өнімділік; - қол жетімділік; - қауіпсіздік. 2. Ақауларға төзімділікті қамтамасыз ету бойынша қолданылатын іс-шаралардың тиімділігіне талдау жүргізу. Атап айтқанда, сақтық көшірме жасау және резервтік көшірмелерді қалпына келтіру процесіне егжей-тегжейлі талдау жүргізу. Ұсыныстармен акт инфрақұрылымының параметрлері мен параметрлерін бағалау нәтижелері 1. АКТ-инфрақұрылымын ҚР СТ ISO/IEC 27001-2015 бірыңғай талаптары мен талаптарына сәйкес келтіру үшін ұсынымдар дайындау. 4 кезең. АҚ саласындағы ішкі нормативтік құжаттарды талдау 1. АҚ саласындағы қолданыстағы ішкі нормативтік құжаттардың әдіснамасын бағалау және талдау, оларды жетілдіру бойынша ұсынымдар әзірлеу. 5 кезең. Жоба есебін қалыптастыру 1. Жоба барысында алынған бақылауларды, анықтауларды және ұсынымдарды келісу және талқылау. 2. Техникалық ерекшеліктің міндеттері мен талаптарына сәйкес жасалған түзету іс-қимылдары жоспарының жобасын дайындау. Ену тестілеу: В "қара жәшік" әдісімен желінің сыртқы периметрінің енуіне тестілеу жүргізу үшін Тапсырыс беруші туралы бастапқы деректердің сапасы пайдаланылады: - Тапсырыс берушінің мекенжайларының жария ауқымының тізбесі; - жалпы пайдаланымдағы желілер тарапынан қолжетімді Тапсырыс берушінің информационі мекенжайларының, домендерінің және ақпараттық жүйелер ресурстарының (бұдан әрі - АЖ) тізбесі: қолданбалы АЖ сервистері, web/Mail/DNS/NTP корпоративтік желілік сервистері, пошта мекенжайларының тізімі және т. б. В ішкі желілік сегменттердің енуіне тестілеу жүргізу үшін Тапсырыс беруші туралы бастапқы деректердің сапасы пайдаланылады: - енуге арналған сыртқы тестілеу барысында алынған есептік деректер. Енуге тестілеуді өткізу міндеттері: №1 тапсырма. Домен контроллері әкімшісінің және/немесе өзге де маңызды есептік жазбалардың құқықтарын алу, дерекқорларға, АЖ-ға, құпия және өзге де ақпаратқа қол жеткізу және т.б. Ең аз ақпаратпен шабуылдаушының әрекеттерін эмуляциялау. Бұл тапсырмаға келесі кезеңдер кіреді: - Тапсырыс беруші компанияның сыртқы ақпараттық ресурстарын зерттеу: желіде ақпарат жинау, веб-ресурстарды зерттеу, Wi-Fi желілерін зерттеу. Жалпы пайдаланымдағы желілерді қосу кезінде деректерді белсенді жинау нәтижесінде тек бастапқы деректерден және ашық көздерден ақпаратты пайдалана отырып, Тапсырыс берушінің АЖ туралы түсінік алу; - Осал қызметтерді анықтау. Ақпараттық ресурстарды дұрыс орнатпауға, әкімшілендіруге немесе пайдалануға байланысты осалдықтарды қоса алғанда, Тапсырыс берушінің АЖ ақпараттық ресурстарының және жалпы пайдаланымдағы желілер тарапынан қолжетімді белсенді
--	---

	желілік жабдықтың ықтимал бар осалдықтарын анықтау; - Ену осалдықтарын пайдалану. Тапсырыс берушінің АЖ туралы жиналған ақпаратты пайдалана отырып, сыртқы шабуылдаушының Тапсырыс берушінің ақпараттық қауіпсіздігін бұзуға және веб-қосымшалардың серверлерін компаға келтіруге (АЖ басқаруын басып алуға немесе құпия деректерді алуға) бағытталған әрекеттерін модельдеу. №2 тапсырма. Сыни АЖ қауіпсіздік деңгейін тексеру ("INSIS", " фронтальды операциялар", "1С Кәсіпорын"). Желінің ішкі периметрінің енуіне тестілеу. Active Directory-да пайдаланушы тіркелгісін бере отырып. Бұл тапсырмаға келесі кезеңдер кіреді: - Ішкі жүйелерге шолу жасау (Active Directory, LDAP, RADIUS және т.б.). Ішкі жүйелердің осалдығын анықтаңыз. Тапсырыс берушінің АЖ ақпараттық ресурстарының және ақпараттық ресурстарды дұрыс конфигурацияламауға, әкімшілендіруге немесе пайдалануға байланысты осалдықтарды қоса алғанда, ішкі желі сегменті тарапынан қолжетімді белсенді желілік жабдықтың ықтимал бар осалдықтарын анықтау; - Әкімшілік құқықтарды алуға тырысу (осалдықтарды пайдалану немесе парольдерді таңдау) маңызды ресурстарды бақылау / құпия ақпаратты алу). Тапсырыс берушінің АЖ туралы жиналған ақпаратты пайдалана отырып, тапсырыс берушінің ақпараттық қауіпсіздігін бұзуға және Тапсырыс берушінің ішкі желілік сегментінен деректерді бұзуға бағытталған шабуылдаушының әрекеттерін модельдеу. Бұзушы модельдері Ықтимал бұзушы ретінде қасақана іс-әрекеттер нәтижесінде қасақана ниетпен немесе онсыз Тапсырыс берушінің қабылдаған ақпараттық қауіпсіздік саясатын бұзуға, қызметтік және құпия ақпаратты алуға бағытталған ақпараттық қауіпсіздікке түрлі қатерлерді іске асыра алатын, сондай-ақ Тапсырыс берушінің АЖ жұмысына теріс әсер ететін адам немесе тұлғалар тобы қаралады. Ортақ пайдаланылатын желілерден желілік қауіпсіздікке талдау жүргізу кезінде бұзушы Тапсырыс берушінің АЖ-нің уәкілетті пайдаланушысы болып табылмайды, Тапсырыс берушінің АЖ туралы бастапқы ақпараты болады және Интернет желісіне және жергілікті есептеу желілеріне қосылған АЖ-ға түрлі шабуылдар жүргізудің практикалық тәжірибесі болады. Желінің ішкі сегментіне талдау жүргізу барысында бұзушы үшін ол өзінің жабдығын (дербес компьютерін) Тапсырыс берушінің АЖ желісінің кейбір аса маңызды пайдаланушы сегменттеріне қосуға, өзінің шабуыл платформасын Тапсырыс берушіде пайдаланылатын жұмыс станциясы ретінде беруге мүмкіндік алатын жағдай эмуляцияланады, бұл ретте ол да уәкілетті пайдаланушы болып табылмайды. Шабуыл түрлері Құпия ақпараттың ағып кетуінің ықтимал тәуекелдерін іздеу үшін ақпараттың тұтастығын бұзуға және Тапсырыс берушінің АЖ қолжетімділігін бұзуға бағытталған шабуылдар қаралатын болады. Құқық бұзушының орналасқан жері бойынша шабуылдар имитацияланатын болады, олар жалпы пайдалану желілері тарапынан және Тапсырыс беруші желісінің ішкі сегментінен жүзеге асырылуы мүмкін. Әсер ету объектісі бойынша Тапсырыс берушінің АЖ-нің мынадай ақпараттық ресурстарына бағытталған шабуылдар еліктелетін болады: - белсенді желілік жабдық; -
--	---

қауіпсіздікті қамтамасыз етудің бағдарламалық-аппараттық кешендері, - АЖ серверлері; - серверлер мен жұмыс орындарын виртуалдандыру платформалары; - ұсынылатын қызметтер. Қызмет көрсету қорытындысы бойынша Орындаушы Тапсырыс берушіге жүргізілетін шабуылдардың кезең-кезеңімен сипатталуын, жүргізілген шабуылдардың нәтижесін және Тапсырыс берушінің АТ-инфрақұрылымының ішкі және сыртқы периметрінде анықталған осалдықтар мен кемшіліктердің шоғырландырылған тізімін қамтитын егжей-тегжейлі есепті ұсынады. Сондай-ақ анықталған осалдықтарды/кемшіліктерді жою жөніндегі іс-шаралардың егжей-тегжейлі жоспарында жәрдем көрсете отырып, АЖ қауіпсіздік деңгейін арттыру бойынша егжей-тегжейлі ұсынымдар ұсынылатын болады. Сақтық көшірме жасау Пенетерациялық тестілеу барысында деректердің жоғалу, зақымдану немесе қате қалпына келтірілу қаупін болдырмау мақсатында, Жеткізуші жұмысты орындау алдында да, орындау барысында да маңызды жүйелердің сақтық көшірмесін жасауға міндетті. Сақтық көшірме жүйесі бағдарламалық жасақтаманы жаңартумен байланысты оқиғалар, ақаулар немесе қателер жағдайында пайдаланушы деректерін және сервер конфигурацияларын қалпына келтіруді қамтамасыз етуі керек. Мердігерге қауіпсіздік мақсатында ашық бастапқы кодты бағдарламалық жасақтаманы пайдалануға рұқсат етілмейді. Резервтік көшіруді және қалпына келтіруді Орындаушы тек қана көші-қон/Microsoft бойынша өзекті нұсқаларға жаңарту кезеңінде қолданылатын уақытша (шұғыл) лицензияларды қоса алғанда, қызмет көрсету кезеңіне ұсынылатын өз қаражатынан қамтамасыз етуі тиіс. Сақтық көшірме жасау функциясы келесі талаптардың орындалуын қамтамасыз етуі керек: 1. Платформа және лицензиялау (Endpoint) Пішім: қолдау көрсетілетін Мәңгілік лицензиялар (Perpetual). Қорғау нысаны: Ноутбуктер және жұмысшылардың дербес компьютерлері. Масштабтау: компоненттерді көлденең масштабтау арқылы өнімділікті арттыру мүмкіндігі. 2. БҚ-ға қойылатын жалпы талаптар БҚ мыналарды қамтамасыз етуі тиіс: Операциялық жүйелерді қолдау: Windows, macOS және Linux. Орталықтандырылған басқару: Windows немесе Linux жүйесінде басқару серверін орнату. Тасымалдау тиімділігі: тұрақсыз байланыс арналарында (Wi-Fi/4G) жұмыс істеу үшін тек өзгертілген блоктарды көшіру (қосымша көшіру). Сақтауды оңтайландыру: сақталған деректердің көлемін азайту үшін ғаламдық қайталану және бастапқы қысу. 3. Соңғы құрылғылардың функционалдығы Автоматтандыру: кесте бойынша немесе файлдардағы өзгерістер анықталған кезде сақтық көшірме жасау. Өзіне-өзі қызмет көрсету: әкімшінің қатысуынсыз пайдаланушылардың файлдарды өз бетінше іздеуі және қалпына келтіруі үшін порталдың болуы. Файлдық жүйелерді қолдау: FAT, NTFS, ReFS, APFS (macOS), EXT, XFS және т.б. файлдық жүйелермен жұмыс. Қалпына келтіру: жеке файлдарды да, жүйенің немесе дискілердің бүкіл конфигурациясын қалпына келтіру мүмкіндігі. Деректер қауіпсіздігі: қорғалған арналар арқылы сақтау және беру кезінде сақтық көшірмелерді міндетті түрде шифрлау. 4. Желілік мүмкіндіктер және ұтқырлық Интернет арқылы жұмыс

	істеу: орталық серверден 1000 км-ден астам қашықтықта бэкап пен қалпына келтірудің жұмыс қабілеттілігін қамтамасыз ету. Трафикті басқару: сығымдау механизмдері және өткізу қабілеттілігін шектеу (throttling), сондықтан сақтық көшірме пайдаланушының жұмысына кедергі келтірмейді. Синтетикалық сақтық көшірме: серверде синтездеу арқылы пайдаланушының құрылғысына жүктемесіз толық көшірмелерді жасауды қолдау. 3. Қызмет көрсету нәтижесі Жобаның талаптары мен міндеттеріне сәйкес орындалған, анықталған тәуекелдерді төмендету бойынша анықталған және ұсынымдары бар, АҚ-ны одан әрі дамыту перспективаларын бағалай отырып, орыс тіліндегі аудит нәтижелері бойынша есеп. Есеп электронды нұсқаларда ұсынылуы керек ("pdf" форматы, сондай-ақ "xls" және/немесе "doc"). Сатып алынатын қызметтер шеңберінде әзірленген барлық құжаттар Тапсырыс берушімен жазбаша келісілуге, сондай-ақ уәкілетті басшының қолымен және Орындаушының мөр бедерімен куәландырылуға тиіс. Есепте АҚ саласындағы ішкі бақылау жүйесінің тиімділігі, АҚ-ны корпоративтік басқарудың тиімділігі, процестер мен АҚ-ның заңнама талаптарына сәйкестігі, сондай-ақ Тапсырыс берушінің АҚ процестерінің жетілуін бағалау туралы пікір қамтылуға тиіс. Тапсырыс берушінің бизнес-мақсаттарына сәйкес АҚ-да қолданыстағы әдістемелер мен рәсімдерді жетілдіру бойынша ұсынымдар Ұсынымдар әрбір анықтауға қатысты әзірленуі тиіс, ұсынымның тұжырымы берілген ұсынымның толықтығы мен мағынасын аша отырып, егжей-тегжейлі сипатта болады. Сондай-ақ, анықтаудың пайда болу себебін және оның Тапсырыс берушінің қызметі үшін салдарын ашу қажет. Аудит бойынша қызметтер көрсету тек Тапсырыс берушінің аумағында жүргізілуі тиіс. Ақпарат жинауды, инфрақұрылымды тексеруді және техникалық ерекшелікте көрсетілген өзге де жұмыстарды өнім берушінің мамандары техникалық ерекшелікте көрсетілген әрбір объектіде тікелей жүзеге асыруы тиіс. Аудит барысында алынған ақпарат, атап айтқанда нормативтік құжаттама құпия болып табылады, осыған байланысты оны өңдеу және талдау Тапсырыс берушінің аумағында орындалуы тиіс. 4. Әлеуетті өнім берушіге қойылатын талаптар Әлеуетті өнім беруші конкурсқа өтінім құрамында аудит шеңберінде қызмет көрсететін мамандардың толық тізбесін ұсынуы тиіс. Аудит бойынша қызмет көрсету барысында ауыстырылатын маманға ұқсас осындай маманның біліктілігін растай отырып бір маманнан артық емес ауыстыруға жол беріледі. 5. Орындаушыға қойылатын талаптар Орындаушы Тапсырыс берушімен конкурсқа өтінім шеңберінде мәлімделген барлық мамандар қатысуға тиіс кемінде бір орнату кездесуін өткізуге міндетті. Қызмет көрсетуді конкурсқа өтінім құрамында мәлімделген команда жүзеге асыруы тиіс.
--	--

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)	Орындаушы Тапсырыс берушімен конкурсқа өтінім шеңберінде мәлімделген барлық мамандар қатысуға тиіс кемінде бір орнату кездесуін өткізуге міндетті. Қызмет көрсетуді конкурсқа өтінім құрамында мәлімделген команда жүзеге асыруы тиіс.
--	---

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

Наименование заказчика	Акционерное общество "Международный аэропорт Нурсултан Назарбаев"
Наименование организатора	Акционерное общество "Международный аэропорт Нурсултан Назарбаев"
№ конкурса:	№ 17791876-1
Наименование конкурса:	Услуга по проведению аудита информационной безопасности. Тел.: 8 (7172) 777-377, 777-177
Номер лота:	№ 88073656-OK1
Наименование лота:	Услуги по проведению внешней оценки системы внутреннего аудита
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	749020.000.000004
Наименование услуги:	Услуги по проведению внешней оценки системы внутреннего аудита
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	15690431.03
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	15690431.03
Срок оказания услуги:	по истечении 15 календарных дней со дня подписания договора, в течение 30 календарных дней
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Термины и сокращения ИБ – информационная безопасность; ИТ – информационные технологии; ИКТ – информационно-коммуникационные технологии; СПД – сеть передачи данных; ВНД – внутренняя нормативная документация; Услуги/Проект – аудит информационной безопасности. 1. Цели и задачи закупаемых Услуг Ключевыми целями оказания Услуг являются: - предоставление объективной и достоверной информации о текущем состоянии информационной безопасности (ИБ) Заказчика; - совершенствование системы внутреннего контроля в области управления ИБ, направленной на минимизацию рисков для бизнес-деятельности Заказчика; - повышение надежности, доступности и безопасности информационных активов Заказчика; - обеспечение соответствия систем информационной безопасности требованиям Постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 - Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности (далее – Единые требования). Задачи: - провести анализ функциональных возможностей информационных систем Заказчика и провести обзор их соответствия мировым стандартом в области ИБ; - подготовить рекомендации по дальнейшему развитию информационных систем Заказчика в направлении ИБ в соответствии с Едиными требованиями; - провести обзор ИКТ-инфраструктуры, включая сетевую инфраструктуру, серверное и телекоммуникационное оборудование; - проведение ревизии правил в информационных системах охватывающие информационную безопасность на соответствие Единым Требованиям; - подготовить рекомендации по повышению надежности, доступности и безопасности информационных активов; - презентовать аналитический отчет по результатам аудита ИБ, руководству Заказчика. 2. Перечень мероприятий и результаты оказываемых Услуг Реализацию поставленных целей необходимо осуществить в рамках следующих этапов: 1. Анализ действующих ВНД и процессов деятельности ИБ. 2. Анализ функциональных возможностей информационных систем и соответствия Единым Требованиям. 3. Обзор ИКТ-инфраструктуры, в частности анализ безопасности построения сетевой инфраструктуры. 4. Обследование защищенности информационных активов включая сканирование на уязвимости и проведение внешнего тестирования на проникновение. 5. Формирование отчета и проведение презентации. Описание услуг аудита Этап 1. Определение рамок проекта в соответствии с целями Аудита 1. Согласование списка работ, последовательности их реализации и описание списка документов, требуемых для предоставления во время Аудита ИБ. Результат: Согласованный план работ, график предоставления документов и ответственных лиц со стороны Заказчика. Этап 2. Оценка текущего состояния ИБ инфраструктуры, проведение обзора их соответствия критериям Единых требований 1. Анализ текущих ИБ процессов на соответствие Единым Требованиям и требованиям СТ РК ISO/IEC 27001-2015. 2. Оценка эффективности реализованных ИБ процессов в соответствии с Едиными требованиями и методологией СТ РК ИСО27001. 3. Анализ эффективности используемых
---	--

	решений по ИБ (используемые политики, настройки). 4. Оценка соответствия используемых инструментов Единым Требованиям. Этап 3. Обзор ИКТ-инфраструктуры, включая сетевую инфраструктуру, серверное и телекоммуникационное оборудование 1. Проведение технологической оценки конфигурационных параметров и настроек объектов ИКТ-инфраструктуры (СПД, серверное и телекоммуникационное оборудование) по следующим требованиям: - производительность; - доступность; - безопасность. 2. Проведение анализа эффективности применяемых мероприятий по обеспечению отказоустойчивости. В частности, провести детальный анализ процесса проведения резервного копирования и восстановления резервных копий. Результаты оценки параметров и настроек ИКТ-инфраструктуры с рекомендациями 1. Подготовка рекомендаций для приведения ИКТ - инфраструктуры в соответствие с Едиными требованиями и требованиями СТ РК ISO/IEC 27001-2015. Этап 4. Анализ внутренних нормативных документов в области ИБ 1. Оценка методологии и анализ действующих внутренних нормативных документов в области ИБ, выработка рекомендаций по их усовершенствованию. Этап 5. Формирование Отчета по Проекту 1. Согласование и обсуждение полученных в ходе проекта наблюдений, обнаружений и рекомендаций. 2. Подготовка проекта плана корректирующих действий, составленного в соответствии с задачами и требованиями Технической спецификации. Тестирование на проникновение: В качестве исходных данных о Заказчике, для проведения тестирования на проникновение внешнего периметра сети методом «черный ящик», используются: - перечень публичного диапазона адресов Заказчика; - перечень URL-адресов, доменов и ресурсов информационных систем (далее - ИС) Заказчика, доступных со стороны сетей общего пользования: сервисы прикладных ИС, корпоративные сетевые сервисы Web/Mail/DNS/NTP, список почтовых адресов и т.п. В качестве исходных данных о Заказчике для проведения тестирования на проникновение внутренних сетевых сегментов, используются: - учетные данные, полученные в ходе внешнего тестирования на проникновение. Задачи проведения тестирования на проникновение: Задача №1. Захват прав администратора контроллера домена и/или иных критичных учетных записей, получение доступа к базам данных, к ИС, к конфиденциальной и иной информации, прочее. Эмуляция действий злоумышленника при минимуме информации. В данную задачу входят следующие этапы: - Изучение внешних информационных ресурсов Заказчика: сбор информации в сети, обследование веб-ресурсов, изучение wi-fi сетей. Получение представления об ИС Заказчика, используя информацию только из исходных данных и открытых источников в результате активного сбора данных при подключении сетей общего пользования; - Обнаружение уязвимых сервисов. Выявить возможные существующие уязвимости информационных ресурсов ИС Заказчика и активного сетевого оборудования, доступных со стороны сетей общего пользования, включая уязвимости, связанные с неправильной настройкой, администрированием или использованием информационных ресурсов; -
--	---

	Эксплуатация уязвимостей для проникновения. Используя собранную информацию об ИС Заказчика, симитировать действия внешнего злоумышленника, направленные на нарушение информационной безопасности Заказчика и компрометацию (захват управления ИС или получение конфиденциальных данных) серверов веб приложений. Задача №2. Проверка уровня безопасности критичных ИС («INSIS», «Фронтальные операции», «1С Предприятие»). Тестирование на проникновение внутреннего периметра сети. С предоставлением пользовательской учетной записи в Active Directory. В данную задачу входят следующие этапы: - Провести обзор внутренних систем (Active Directory, LDAP, RADIUS и т.п.). Обнаружить уязвимости внутренних систем. Выявить возможные существующие уязвимости информационных ресурсов ИС Заказчика и активного сетевого оборудования, доступных со стороны внутреннего сетевого сегмента, включая уязвимости, связанные с неправильной настройкой, администрированием или использованием информационных ресурсов; - Попытка получить административные права (эксплуатация уязвимостей либо подбор паролей) контроль над критически важными ресурсами/получение конфиденциальной информации). Используя собранную информацию об ИС Заказчика, симитировать действия злоумышленника, направленные на нарушение информационной безопасности Заказчика и компрометацию данных из внутреннего сетевого сегмента Заказчика. Модели нарушителя В качестве потенциального нарушителя рассматривается лицо или группа лиц, которые в результате умышленных действий, со злым умыслом или без такового могут реализовать различные угрозы информационной безопасности, направленные на нарушение принятых Заказчика политик информационной безопасности, получение служебной и конфиденциальной информации, а также оказывают негативное воздействие на работу ИС Заказчика. При проведении анализа сетевой безопасности из сетей общего пользования, нарушитель не является авторизованным пользователем ИС Заказчика, имеет первоначальную Информацию об ИС Заказчика и обладает практическим опытом проведения различных атак на ИС, подключенным к сети Интернет и локальным вычислительным сетям. В ходе проведения анализа внутреннего сегмента сети, для нарушителя эмулируется ситуация, при которой он получает возможность подключения своего оборудования (персональный компьютер) к некоторым наиболее критичным пользовательским сегментам сети ИС Заказчика, выдавая свою атакующую платформу за используемую у Заказчика рабочую станцию, при этом он также не является авторизованным пользователем. Виды атак Будут рассмотрены атаки направленные на нарушение целостности информации и нарушение доступности ИС Заказчика для поиска потенциальных рисков утечки конфиденциальной информации. По месторасположению нарушителя будут симитированы атаки, которые могут быть реализованы со стороны сетей общего пользования и из внутреннего сегмента сети Заказчика. По объекту воздействия будут симитированы атаки, направленные на следующие информационные ресурсы ИС Заказчика: - активное сетевое
--	--

	оборудование; - программно-аппаратные комплексы обеспечения безопасности, - сервера ИС; - платформы виртуализации серверов и рабочих мест; - предоставляемые сервисы. По итогу оказания услуг Исполнитель предоставляет Заказчику детальный отчет, содержащий пошаговое описание проводимых атак, результат проведенных атак и консолидированный список выявленных уязвимостей и недостатков во внутреннем и внешнем периметре ИТ-инфраструктуры Заказчика. Так же будут предоставлены подробные рекомендации по повышению уровня безопасности ИС с оказанием содействия в детальном плане мероприятий по устранению выявленных уязвимостей/недостатков. Резервное копирование В целях исключения рисков утраты, повреждения либо некорректного восстановления информации при проведении тестирования на проникновение Поставщик обязан провести резервное копирование критичных систем до начала и в процессе проведения работ. Система резервного копирования должна обеспечивать возможность восстановления пользовательских данных и конфигураций серверов в случае возникновения инцидентов, сбоев либо ошибок, связанных с обновлением ПО. Исполнитель не имеет право использовать ПО с открытым исходным кодом с целью обеспечения безопасности. Резервное копирование и восстановление должны быть обеспечены Исполнителем из собственных средств, предоставляемых на период оказания услуги, включая временные (срочные) лицензии, действующие исключительно на этапе миграции/обновления до актуальных версий ПО Microsoft. Функционал резервного копирования должен обеспечивать соблюдение следующих требований: 1. Платформа и лицензирование (Endpoint) Формат: Бессрочные лицензии (Perpetual) с поддержкой. Объект защиты: Ноутбуки и персональные компьютеры работников. Масштабируемость: Возможность увеличения производительности путем горизонтального масштабирования компонентов. 2. Общие требования к ПО ПО должно обеспечивать: Поддержку операционных систем: Windows, macOS и Linux. Централизованное управление: Установка сервера управления на Windows или Linux. Эффективность передачи: Копирование только изменившихся блоков (инкрементальное копирование) для работы на нестабильных каналах связи (Wi-Fi/4G). Оптимизацию хранения: Глобальная дедупликация и сжатие на стороне источника для минимизации объема хранимых данных. 3. Функциональные возможности для конечных устройств Автоматизация: Резервное копирование по расписанию или при обнаружении изменений в файлах. Самообслуживание: Наличие портала для самостоятельного поиска и восстановления файлов пользователями без участия администратора. Поддержка файловых систем: Работа с файловыми системами FAT, NTFS, ReFS, APFS (macOS), EXT, XFS и другими. Восстановление: Возможность восстановления как отдельных файлов, так и всей конфигурации системы или дисков. Безопасность данных: Обязательное шифрование бэкапов при хранении и передаче по защищенным каналам. 4. Сетевые возможности и мобильность Работа через интернет: Обеспечение работоспособности бэкапа и восстановления на удалении
--	--

	более 1000 км от центрального сервера. Управление трафиком: Механизмы сжатия и ограничения полосы пропускания (throttling), чтобы бэкап не мешал работе пользователя. Синтетический бэкап: Поддержка создания полных копий без нагрузки на устройство пользователя за счет синтеза на сервере. 3. Результат оказания услуги Отчет по результатам аудита на русском языке, выполненный в соответствии с требованиями и задачами проекта, с обнаружениями и рекомендациями по снижению выявленных рисков, с оценкой перспектив дальнейшего развития ИБ. Отчет должен быть предоставлен в электронных версиях (формат «pdf», а также «xls» и/или «doc»). Все документы, разработанные в рамках закупаемых услуг, должны быть письменно согласованы с Заказчиком, а также заверены подписью уполномоченного руководителя и оттиском печати Исполнителя. Отчет должен содержать мнение об эффективности системы внутреннего контроля в области ИБ, эффективности корпоративного управления ИБ, соответствии процессов ИБ требованиям законодательства, а также оценку зрелости процессов ИБ Заказчика. Рекомендации по совершенствованию действующих методик и процедур в ИБ в соответствии с бизнес-целями заказчика Рекомендации должны быть выработаны в отношении каждого обнаружения, формулировка рекомендации будет носить детализированный характер, раскрывая полноту и смысл выданной рекомендации. Также необходимо раскрыть причину возникновения обнаружения и его последствия для деятельности Заказчика. Оказание услуг по аудиту должно проводиться исключительно на территории Заказчика. Сбор информации, обследование инфраструктуры и прочие работы, указанные в технической спецификации, должны быть осуществлены специалистами Поставщика непосредственно на каждом объекте, указанном в технической спецификации. Информация, получаемая в ходе аудита, в частности, нормативная документация, является конфиденциальной, в связи с чем ее обработка и анализ должны быть выполнены на территории Заказчика. 4. Требования к потенциальному поставщику Потенциальный поставщик в составе заявки на конкурс должен предоставить полный перечень специалистов, которые будут оказывать услуги в рамках аудита. В ходе оказания услуг по аудиту допускается замена не более одного специалиста с подтверждением квалификации такого специалиста аналогично заменяемому. 5. Требования к Исполнителю Исполнитель обязан провести не менее одной установочной встречи с Заказчиком, на которой должны присутствовать все специалисты, заявленные в рамках заявки на конкурс. Оказание услуги должно осуществляться командой, заявленной в составе заявки на конкурс.
--	---

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)	Исполнитель обязан провести не менее одной установочной встречи с Заказчиком, на которой должны присутствовать все специалисты, заявленные в рамках заявки на конкурс. Оказание услуги должно осуществляться командой, заявленной в составе заявки на конкурс.
---	---