ТЕХНИКАЛЫҚ СИПАТТАМА

1268491 сатып алу бойынша
Төмендету бойынша ашық тендер тәсілімен

Лот № 1 (114 У, 4575975) Ақпараттық технологиялар тексеруін жүргізу бойынша қызмет көрсетулер

Тапсырыс беруші: «Тау-Кен Самұрық» ұлттық тау-кен компаниясы» акционерлік қоғамы
Ұйымдастырушы: «Тау-Кен Самұрық» ұлттық тау-кен компаниясы» акционерлік қоғамы

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	114 У
Атауы және қысқаша сипаттамасы	Ақпараттық технологиялар тексеруін жүргізу бойынша қызмет көрсетулер, Ақпараттыө технология аудиттерін жүргізу бойынша қызметтер
Қосымша сипаттама	Ақпараттық қауіпсіздікке сыртқы аудит жүргізу қызметтері
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Астана қ., район Нұра, ул. Сыганак, строение 17/10
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 30 күнтізбелік күні
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

Ақпараттық қауіпсіздіктің кешенді аудитін жүргізу қызметін көрсетуге арналған ТЕХНИКАЛЫҚ ЕРЕКШЕЛІК

Сипаттамасы және көрсетілетін қызметтің талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары.

1. ҚҰЖАТТЫҢ МАҚСАТЫ

Осы Техникалық ерекшелік (бұдан әрі – Те) «Тау-Кен Самұрық» ҰТК» АҚ ақпараттық қауіпсіздік (АҚ) жағдайына кешенді сараптама жүргізу үшін қажетті құрамды, құрылымды, мазмұнды, функционалдық, техникалық, ұйымдастырушылық және әдістемелік талаптарды айқындайды.

Құжат міндеттер тізбесін, күтілетін нәтижелерді, мамандардың құзыреттеріне қойылатын талаптарды, өзара іс-қимыл ережелері мен қызметтірдің көрсетуін бақылау тетіктерін белгілейді.

2. ГЛОССАРИЙ

Тапсырыс беруші – «Тау-Кен Самұрық» ҰТК» АҚ.

Аудит объектісі – «Тау-Кен Самұрық» ҰТК» АҚ.

Орындаушы – аудит қызметтерін көрсететін мердігер ұйым.

АҚ – Ақпараттық қауіпсіздік.

Әдіснама – бизнес-процестерді орындау тәсілін, АҚ жағдайын талдау мен бағалауды регламенттейтін құжаттардың, әдістер мен ережелердің жиынтығы.

ТЕ – Техникалық ерекшелік.

АЖ – Ақпараттық жүйе: деректерді сақтауды, өңдеуді және беруді қамтамасыз ететін бағдарламалық-аппараттық кешен.

БҚ – Бағдарламалық қамтылым.

ЛБҚ – Лицензияланған бағдарламалық қамтылым.

3. КӨРСЕТІЛГЕН ҚЫЗМЕТТЕР ТУРАЛЫ

МӘЛІМЕТТЕР

3.1. Жобаның мақсаты

Жоба ақпараттық қауіпсіздікті (АҚ) қамтамасыз ету процестерінің, шаралары мен құралдарының ағымдағы жағдайына объективті, тәуелсіз және жан-жақты баға алуға, сондай-ақ оларды жетілдіру бойынша ұсынымдар әзірлеуге бағытталған.

Негізгі мақсаты:

– Ақпараттық қауіпсіздікті (АҚ) қамтамасыз ету процестерінің ағымдағы жағдайына кешенді бағалау жүргізу, оның ішінде ақпаратты қолданыстағы ұйымдастырушылық және техникалық қорғау шараларын бағалау.

– Ақпараттық қауіпсіздік саласындағы осалдықтарды, кемшіліктерді және әлеуетті тәуекелдерді анықтау, сондай-ақ олардың Тапсырыс берушінің ақпараттық жүйелері мен инфрақұрылымының қорғалғандығына әсерін айқындау.

– Анықталған кемшіліктерді жоюға, тәуекелдер деңгейін төмендетуге және ақпаратты қорғау бойынша қолданылатын шаралардың тиімділігін арттыруға бағытталған АҚ қамтамасыз ету процестерін жетілдіру және оңтайландыру бойынша ұсынымдар мен ұсыныстар әзірлеу.

– АҚ қамтамасыз ету процестерінің, ақпараттық инфрақұрылым баптауларының және ішкі құжаттаманың Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамасының талаптарына және қолданылатын нормативтік талаптарға сәйкестігін бағалау.

– Кибергигиена, ақпараттық ресурстармен қауіпсіз жұмыс істеу және тараған киберқатерлерге қарсы іс-қимыл мәселелері бойынша оқыту жүргізу арқылы Тапсырыс беруші қызметкерлерінің ақпараттық қауіпсіздік саласындағы хабардар болу деңгейін арттыру.

– Анықталған кемшіліктерді жою және ақпаратты қорғаудың қолданыстағы процестері мен құралдарын жетілдіру жөніндегі іс-шараларды іске асыру есебінен Тапсырыс берушінің ақпараттық қауіпсіздігінің жалпы деңгейін көтеру.

3.2. Жобаның міндеті

3.2.1. Ақпараттық қауіпсіздікті қамтамасыз етудің ағымдағы жағдайын зерттеп-тексеру

Орындаушы:

– Тапсырыс берушінің ақпараттық қауіпсіздігін қамтамасыз етудің ұйымдастырушылық, техникалық және бағдарламалық шаралары туралы мәліметтерді жинау мен талдауды;

– Ақпараттық қауіпсіздік саласындағы қолданыстағы құжаттамаға Қазақстан Республикасының АҚ саласындағы заңнамасының талаптарына сәйкестігі тұрғысынан талдау жүргізуді;

– Қолданыстағы процестер мен құжаттардың Қазақстан Республикасы заңнамасының талаптарына сәйкестігін талдауды;

– Тапсырыс беруші ұсынған мәліметтер мен қолжетімділіктер бөлігінде пайдаланылатын ақпараттық жүйелер мен ақпаратты қорғау құралдарының қауіпсіздік параметрлерінің баптауларын талдауды;

– Ақпаратты қорғаудың ұйымдастырушылық және техникалық шараларының ағымдағы тиімділігін бағалау, сондай-ақ әлеуетті сәйкессіздіктер мен жетілдіру аймақтарын анықтауды;

– Тапсырыс беруші қызметкерлерінің ақпараттық қауіпсіздік және кибергигиена саласындағы хабардар болу деңгейін арттыруды;

– Анықталған сәйкессіздіктерді жою және ақпараттық қауіпсіздікті қамтамасыз ету жүйесін жетілдіру бойынша ұсынымдар дайындауды қамтитын зерттеп-тексеру іс-шараларының кешенін орындауға міндетті.

3.2.2. Ақпараттық қауіпсіздік тәуекелдерін анықтау және талдау

Орындаушы:

– Ақпараттық қауіпсіздіктің ағымдағы жағдайын зерттеп-тексеру нәтижелері мен Тапсырыс беруші ұсынған ақпарат негізінде ақпараттық қауіпсіздік тәуекелдерін анықтау мен талдауды;

– Анықталған тәуекелдердің ықтималдығын, әлеуетті әсерін және критикалық (сыни) деңгейін бағалай отырып, олардың тізбесін қалыптастыру мен өзектендіруді;

– Анықталған тәуекелдерді өңдеу бойынша ұсынымдар дайындау, оның ішінде оларды жою, төмендету, басқа біреуге беру немесе қабылдау бойынша ықтимал шараларды қамтуды;

– Тәуекелдердің критикалық деңгейін және Тапсырыс берушінің қызметіне тигізетін әлеуетті әсерін ескере отырып, тәуекелдер мен оларды өңдеу жөніндегі ұсынымдардың басымдығын айқындауды жүзеге асырады.

3.2.3. Қолданбалы бағдарламалық қамтылымын қорғалуын талдау

Қызметтерді көрсету үшін Орындаушы мамандандырылған коммерциялық бағдарламалық қамтамасыз етуді (статикалық /динамикалық талдау құралдарын – SAST/DAST) пайдалануға тиіс.

Негізгі талдау құралы ретінде Open Source (ашық бастапқы коды бар) лицензиялары бойынша таратылатын бағдарламалық қамтамасыз етуді пайдалануға жол берілмейді. Орындаушы шарт жасалғаннан кейін 3 жұмыс күні ішінде аудитті өткізудің бүкіл кезеңінде қолданыста болатын көрсетілген БҚ-ны пайдаланудың заңдылығын растайтын құжаттарды (лицензияларды, жазылымдарды немесе сублицензиялық келісімдерді) ұсынады.

Бастапқы кодтағы осалдықтар мен құжатталмаған мүмкіндіктердің белгілерін іздеуге арналған және Java, C#, VB.NET, PHP, JavaScript, Python, Objective-C, Swift, C/C++, Go, SQL (PL/SQL, T-SQL, MySQL) тілдерін қолдайтын бастапқы кодтың қауіпсіздік анализаторы.

Осалдықтар туралы есепті алғаннан кейін күнтізбелік 30 күн ішінде Орындаушы Тапсырыс берушінің сұрау салуы бойынша қайта талдау шарт сомасына кіретін түзетілген бағдарламалық қамтылымды қайта талдауды жүргізеді. Қызметтер аяқталғаннан кейін Тапсырыс беруші берген барлық материалдар Орындаушының құралдарынан жойылады, бұл туралы акт жасалады.

3.2.4. Ақпараттық инфрақұрылым компоненттерінің баптауларын тексеру

Орындаушы Тапсырыс берушінің ақпараттық инфрақұрылымы компоненттерінің баптауларын тексеруді жүзеге асырады. Қызметтердің негізгі мақсаты – ақпараттық қауіпсіздік талаптарына сәйкестігі тұрғысынан ақпараттық инфрақұрылымның құрамдас бөліктері конфигурациясының дұрыстығы мен қорғалғандығын бағалау, сондай-ақ дұрыс емес баптауларға байланысты әлеуетті тәуекелдерді анықтау.

3.2.5. Киберқауіпсіздік және цифрлық гигиена саласындағы хабардарлық деңгейін арттыру бойынша оқыту.

Орындаушы Тапсырыс берушінің 10 қызметкерін киберқауіпсіздік және цифрлық гигиена саласындағы хабардарлық деңгейін арттыру мәселелері бойынша оқытуды қамтамасыз етуге тиіс. Оқыту киберқауіпсіздіктің негізгі қатерлерін, ақпараттық жүйелермен қауіпсіз жұмыс істеу және дербес деректерді қорғау қағидаларын зерделеуді қамтуы тиіс. Оқыту қорытындысы бойынша қорытынды тестілеу өткізу көзделуі тиіс. Қорытынды тестілеуден сәтті өткен немесе белгіленген талаптарға сәйкес курсты аяқтаған пайдаланушыларға оқудан өткенін растайтын атаулы электрондық сертификаттар беріледі.

3.2.6. Тапсырыс берушінің сырттан қолжетімді цифрлық активтерін сканерлеу

Орындаушы ұйымның сырттан қолжетімді цифрлық активтерін сканерлеуді жүргізуге міндетті. Сканерлеу шеңберінде Орындаушы ықтимал осалдықтарды анықтауды, активтерді автоматтандырылған есепке алуды, корпоративтік сегмент шегінде деректердің ықтимал таралып кету фактілерін анықтау мақсатында даркнет ресурстары мен хакерлік форумдарды

тексеруді, сондай-ақ тәуекелдерді басымдықтары бойынша саралауды жүзеге асыруға тиіс. Сканерлеу үздіксіз және рекурсивті түрде жүргізілуі тиіс. Қорғалу деңгейін бағалау жасанды интеллект технологияларын пайдалана отырып жүргізілуі тиіс.

Көрсетілген жұмыстар мамандандырылған жүйеде автоматтандырылған түрде орындалады. Орындаушы жүйенің жеке кабинетіне қолжетімділікті ұсынуға тиіс. Жүйе сканерлеу есептерін экспорттау, енгізу және сақтау функцияларын қолдауы тиіс. Ашық бастапқы кодпен (Open Source) таратылатын бағдарламалық қамтылымды пайдалануға жол берілмейді. Шарт жасалғаннан кейін Орындаушы 3 (үш) жұмыс күні ішінде көрсетілген бағдарламалық қамтылымды пайдаланудың заңдылығын растайтын, аудит жүргізудің бүкіл кезеңінде қолданыста болатын құжаттарды (лицензияларды, жазылымдарды немесе сублицензиялық келісімдерді) ұсынуға тиіс.

3.2.7. Қорытынды ұсынымдар

Тапсырыс берушінің ақпараттық жүйелері мен деректерінің қорғалу деңгейін арттыру бойынша ұйымдастырушылық, техникалық және рәсімдік шараларды қамтитын кешенді ұсынымдарды әзірлеу.

3.3. Тапсырыс беруші тарапынан бақылауға қойылатын талаптар

Орындаушы:

- Шарт жасалғаннан кейін 10 жұмыс күні ішінде мыналарды ұсынуға:

– қажетті ақпараттың тізбесін;

– аудит жүргізудің жоспар-кестесін.

- Аптасына кемінде 1 рет статус-сессияларды өткізуге.

- Әрбір кезең бойынша егжей-тегжейлі жоспарларды, есептерді, нормативтік актілерге сілтемелерді, стандарттар мен бұзушылықтарды жою бойынша ұсынымдарды ұсынуға.

- Тапсырыс берушінің деректерінің толық құпиялылығын қамтамасыз етуге және шарт жасалған сәттен бастап 10 жұмыс күні ішінде ақпаратты жария етпеу туралы міндеттемелердің түпнұсқаларын ұсынуға міндетті.

3.4. Жобаның әдіснамасы

Қызметтер кезең-кезеңімен көрсетіледі:

Кезең 1. Деректерді жинау және талдау

- АҚ бойынша ұйымдастырушылық-өкімдік құжаттаманы (саясаттар, регламенттер, нұсқаулықтар, қолжетімділік матрицалары, мердігерлермен жасалған шарттар) жинау және талдау.

- ақпараттық жүйелерді, қолданбалы БҚ-ны, лицензиялар мен жүйе иелерін түгендеу.

- Тапсырыс берушінің АҚ қамтамасыз ету процестеріне жауапты қызметкерлерімен сұхбат жүргізу.

- қолжетімділікті басқару, тіркелгі жазбалары мен пайдаланушы құқықтарын басқарудың нақты тәжірибесіне талдау жасау.

Кезең 2. Қолданбалы бағдарламалық қамтылымның қорғалғанын талдау

- талданатын бағдарламалық қамтылым тізбесін және берілетін материалдардың құрамын келісу;

- бастапқы кодты, сондай-ақ бастапқы код болмаған жағдайда орындалатын файлдарды талдау;

- үшінші тараптың және еркін таратылатын компоненттерді және олардың белгілі осалдықтарын анықтау;

- анықталған ақауларды жалған іске қосылуларға қатысты қолмен тексеру;

- көрсетілген қызметтердің нәтижелері бойынша есеп қалыптастыру.

Кезең 3. Ақпараттық қауіпсіздікті қамтамасыз ету процестеріне аудит жүргізу

Жүргізілген талдау нәтижелері бойынша Орындаушы:

- ақпараттық қауіпсіздікті қамтамасыз етудің қолданыстағы процестері мен тәжірибесіне бағалау жүргізеді;

- Тапсырыс берушіде бар АҚ саласындағы ұйымдастырушылық-өкімдік, нормативтік және әдістемелік құжаттамаға талдау жасайды;

- сәйкессіздіктерді, олқылықтарды және жетілдіруді талап ететін аймақтарды анықтайды; ақпараттық қауіпсіздікті қамтамасыз ету процестерін жетілдіру бойынша ұсынымдар береді;

- жүргізілген талдау нәтижелерін және қолданылатын талаптарды ескере отырып, ақпараттық қауіпсіздік бойынша қажетті ұйымдастырушылық-өкімдік, нормативтік және әдістемелік құжаттардың жобаларын пысықтайды және Тапсырыс берушіге ұсынады;

- әзірленген құжаттар жиынтығын кейіннен қарау, келісу және бекіту үшін Тапсырыс берушіге береді.

Құжаттарды талдау және пысықтау Тапсырыс берушімен келісілген тізбе шеңберінде жүзеге асырылады. Құжаттарды бекіту, оларды енгізу және белгіленген талаптардың орындалуын одан әрі қамтамасыз ету Тапсырыс берушімен дербес жүзеге асырылады.

4-кезең. Ақпараттық инфрақұрылым компоненттерінің баптауларын тексеру

Көрсетілетін қызметтер шегінде Орындаушы:

- серверлік инфрақұрылым және операциялық жүйелерді;

- жетаралық экрандар (межсетевые экраны) және ақпаратты қорғаудың өзге де желілік құралдарын;

- желілік жабдықты;

- виртуалдау орталарын;

- басқару және әкімшілендіру жүйелерін;

- ДҚБЖ-ны;

- қашықтан қолжетімділік құралдарын;

- SIEM жүйелерін;

- келісілген тізбеге енгізілген инфрақұрылымның өзге де құрамдастарын қоса алғанда инфрақұрылымның ұсынылған құрамдастардың теңшелуін тексеруді жүзеге асырады.

Тексеру:

- аутентификация және пароль саясаты баптауларын талдауды;

- қолжетімділік құқықтары мен артықшылықты тіркелгі жазбаларын ажыратуды тексеруді;

- қашықтағы және әкімшілік қолжетімділік баптауларын тексеруді;

- рұқсат етілген желілік қосылымдарды, порттар мен сервистерді талдауды;

- жетаралық экрандау ережелерін тексеруді;
- ақпараттық қауіпсіздік оқиғаларын журналға тіркеу және мониторинг жасау баптауларын талдауды;
- пайдаланылатын нұсқалар мен қауіпсіздік баптауларының өзектілігін тексеруді;
- ұсынылған параметрлер бөлігінде сақтық көшірме жасау және қалпына келтіру баптауларын талдауды;
- қолданылатын талаптар мен келісілген әдістемеге сәйкес қауіпсіздіктің өзге де параметрлерін тексеруді қамтиды.

Тексеру нәтижелері бойынша Орындаушы анықталған кемшіліктер мен сәйкессіздіктердің тізбесін, оларға байланысты тәуекелдерді бағалауды және оларды жою бойынша ұсынымдарды береді.

5-кезең. Киберқауіпсіздік және цифрлық гигиена саласындағы хабардарлық деңгейін арттыру бойынша оқыту.

Орындаушы киберқауіпсіздік және цифрлық гигиена саласындағы хабардарлық деңгейін арттыру мәселелері бойынша оқытуды жүргізуді қамтамасыз етуге тиіс. Оқыту қорытындысы бойынша қорытынды тестілеу өткізу көзделуі тиіс. Қорытынды тестілеуден сәтті өткен немесе белгіленген талаптарға сәйкес курсты аяқтаған пайдаланушыларға оқудан өткенін растайтын атаулы электрондық сертификаттар беріледі.

3.5. Міндеттерді бөлу

- Орындаушы тексеру, талдау, тестілеу жұмыстарын орындайды, есептер ұсынады.
- Тапсырыс беруші ақпаратты, қолжетімділіктерді беруді, кездесулерді ұйымдастыруды қамтамасыз етеді.
- Өзара іс-қимыл Тапсырыс берушімен келісілген байланыс арналары (e-mail, файлообменниктер және т.б.) арқылы жүзеге асырылады.

3.6. Нәтижелерге қойылатын талаптар

Орындаушы:

1. Мыналарды:

- барлық талдау түрлерінің нәтижелерін;
- жұмыс кезеңдері бойынша есептерді;
- анықталған сәйкессіздіктер мен тәуекелдер туралы ақпаратты;
- қорғалғандық деңгейін арттыру бойынша ұсынымдарды қамтитын қорытынды есепті ұсынуы тиіс.

2. Барлық бастапқы құжаттаманы қоса алғанда, аралық есептер аудитті өткізудің жоспар-кестесіне сәйкес қызмет көрсетудің жекелеген кезеңдері аяқталған сайын, сондай-ақ Тапсырыс берушінің сұрауы бойынша, сұрау алынғаннан кейін 10 (он) жұмыс күннен кешіктірілмейтін мерзімде ұсынылады.

3. Ұсынылатын құжаттар пакетінің құрылымы мен форматы Тапсырыс берушімен алдын ала келісілуі тиіс.

3. Техникалық стандарттар

№ р/с	ҚР тіркелген	Белгіленуі	Құжат нөмірі	Санаты	Атауы	Қолдану саласы	Әзірлеуші	Беттер	МКС	Мәртебесі	Бұйрық	Енгізу күні бастап	К б

1	Иә	СТ РК ISO /IEC 27002-2015	384046	Қазақстан Республикасының ұлттық стандарты	Информационная технология методы и средства обеспечения безопасности свод правил по средствам управления защитой информации	Настоящий стандарт содержит руководство для организационных стандартов по информационной безопасности и управлению информационной безопасностью, включая отбор, внедрение и управления системами и управления, принимая во внимание организационную среду информационного риска.	Нет ()	178	Наборы знаков и кодирование информации	Действует	Приказом Председателя Комитета технического регулирования и метрологии Министерства по инвестициям и развитию Республики Казахстан от 24 ноября 2015 г. № 236-од	01.01.2017

Қол қойған Карменова Лэйла Нуралиевна

Қол қойылған күні 03.11.2026

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1268491
способом Открытый тендер на понижение

Лот № 1 (114 У, 4575975) Услуги по проведению аудита информационных технологий

Заказчик: Акционерное общество "Национальная горнорудная компания "Тау-Кен Самрук"
Организатор: Акционерное общество "Национальная горнорудная компания "Тау-Кен Самрук"

1. Краткое описание ТРУ

Наименование	Значение
Номер строки	114 У
Наименование и краткая характеристика	Услуги по проведению аудита информационных технологий, Услуги по проведению аудита информационных технологий
Дополнительная характеристика	Услуги по проведению внешнего аудита информационной безопасности
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Астана, район Нұра, ул. Сыганак, строение 17/10
Условия поставки	-
Срок поставки	С даты подписания договора в течение 30 календарных дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ на оказание услуг по проведению комплексного аудита информационной безопасности

Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики услуги.

1. ЦЕЛЬ ДОКУМЕНТА

Настоящая Техническая спецификация (далее – ТС) определяет состав, структуру, содержание, функциональные, технические, организационные и методологические требования, необходимые для проведения комплексной экспертизы состояния информационной безопасности (ИБ) АО «НГК «Тау-Кен Самрук»

Документ устанавливает перечень задач, ожидаемые результаты, требования к компетенциям специалистов, правила взаимодействия и механизмы контроля оказания услуг.

2. ГЛОССАРИЙ

Заказчик – АО «НГК «Тау-Кен Самрук»

Объект аудита – АО «НГК «Тау-Кен Самрук»

Исполнитель – подрядная организация, оказывающая услуги по аудиту.

ИБ – Информационная безопасность.

Методология – совокупность документов, методов и правил, регламентирующих подход к выполнению бизнес-процессов, анализу и оценке состояния ИБ.

ТС – Техническая спецификация.

ИС – Информационная система: программно-аппаратный комплекс, обеспечивающий хранение, обработку и передачу данных.

ПО – программное обеспечение.

ЛПО – лицензионное программное обеспечение.

3. СВЕДЕНИЯ ОБ ОКАЗЫВАЕМЫХ УСЛУГАХ

3.1. Цели проекта

Проект направлен на получение объективной, независимой и всесторонней оценки текущего состояния процессов, мер и средств обеспечения ИБ, а также на разработку рекомендаций по их улучшению.

Основными целями являются:

- Комплексная оценка текущего состояния процессов обеспечения информационной безопасности (ИБ), включая оценку применяемых организационных и технических мер защиты информации.

- Выявление уязвимостей, недостатков и потенциальных рисков в области информационной безопасности, а также определение их влияния на защищенность информационных систем и инфраструктуры Заказчика.

- Разработка рекомендаций и предложений по совершенствованию и оптимизации процессов обеспечения ИБ, направленных на устранение выявленных недостатков, снижение уровня рисков и повышение эффективности применяемых мер защиты информации.

- Оценка соответствия процессов обеспечения ИБ, настроек информационной инфраструктуры и внутренней документации требованиям законодательства Республики Казахстан в области информационной безопасности, а также применимым нормативным требованиям.

- Повышение уровня осведомленности сотрудников Заказчика в области информационной безопасности посредством проведения обучения по вопросам кибергигиены, безопасной работы с информационными ресурсами и противодействия распространенным киберугрозам.

- Повышение общего уровня информационной безопасности Заказчика за счет реализации мероприятий по устранению выявленных недостатков и совершенствованию действующих процессов и средств защиты информации.

3.2. Задачи проекта

3.2.1. Обследование текущего состояния обеспечения информационной безопасности

Исполнитель обязан выполнить комплекс обследовательских мероприятий, включающий:

- Сбор и анализ сведений об организационных, технических и программных мерах обеспечения информационной безопасности Заказчика.

- Анализ действующей документации в области информационной безопасности на предмет соответствия требованиям законодательства Республики Казахстан в сфере ИБ.

- Анализ соответствия действующих процессов и документов требованиям законодательства Республики Казахстан.

- Анализ настроек параметров безопасности используемых информационных систем и средств защиты информации в части предоставленных Заказчиком сведений и доступов.

- Оценку текущей эффективности организационных и технических мер защиты информации и выявление потенциальных несоответствий и зон для улучшения.

- Повышение уровня осведомленности сотрудников Заказчика в области информационной безопасности и кибергигиены.

- Подготовку рекомендаций по устранению выявленных несоответствий и совершенствованию системы обеспечения информационной безопасности.

3.2.2. Выявление и анализ рисков информационной безопасности

Исполнитель осуществляет:

Выявление и анализ рисков информационной безопасности на основании результатов обследования текущего состояния ИБ и предоставленной Заказчиком информации.

Формирование и актуализацию перечня выявленных рисков с оценкой их вероятности, потенциального воздействия и уровня критичности.

Подготовку рекомендаций по обработке выявленных рисков, включая возможные меры по их устранению, снижению, передаче или принятию.

Определение приоритетности рисков и рекомендаций по их обработке с учетом уровня критичности и потенциального воздействия на деятельность Заказчика.

3.2.3. Анализ защищенности прикладного программного обеспечения

Для оказания Услуг Исполнитель должен использовать специализированное коммерческое программное обеспечение (инструменты статического/динамического анализа — SAST/DAST). Использование программного обеспечения, распространяемого по лицензиям Open Source (с открытым исходным кодом), в качестве основного инструмента анализа не допускается. Исполнитель после заключения договора в течении 3 рабочих дней предоставляет документы, подтверждающие правомерность использования (лицензии, подписки или сублицензионные соглашения) указанного ПО, действующие на весь период проведения аудита.

Анализатор защищенности исходного кода, предназначенный для поиска уязвимостей и подозрений на недокументированные возможности в исходном коде и поддерживающий следующие языки Java, C#, VB.NET, PHP, JavaScript, Python, Objective-C, Swift, C/C++, Go, SQL (PL/SQL, T-SQL, MySQL).

В течение 30 календарных дней после получения отчета уязвимостей Исполнитель по запросу Заказчика проводит повторный анализ исправленного программного обеспечения; повторный анализ входит в стоимость договора. По завершении Услуг все переданные Заказчиком материалы удаляются со средств Исполнителя, о чем составляется акт.

3.2.4. Проверка настроек компонентов информационной инфраструктуры

Исполнитель проводит проверку настроек компонентов информационной инфраструктуры Заказчика. Основной целью услуг является оценка корректности и защищенности конфигурации компонентов информационной инфраструктуры на предмет соответствия требованиям информационной безопасности и выявление потенциальных рисков, связанных с некорректными настройками.

3.2.5. Обучение повышения уровня осведомленности в области кибербезопасности и цифровой гигиены.

Исполнитель должен обеспечить проведение обучения 10-ти сотрудников Заказчика по вопросам повышения уровня осведомленности в области кибербезопасности и цифровой гигиены. Обучение должно включать изучение основных угроз кибербезопасности, правил безопасной работы с информационными системами и защиты персональных данных. По итогам обучения должно быть предусмотрено итоговое тестирование. Пользователям, успешно прошедшим итоговое тестирование или завершившим курс в соответствии с установленными условиями, выдаются именные электронные сертификаты, подтверждающие прохождение обучения.

3.2.6. Сканирование доступных извне цифровых активов Заказчика

Исполнитель обязан проводить сканирование доступных извне цифровых активов организации. В рамках сканирования Ис полнитель должен осуществлять выявление потенциальных уязвимостей, автоматизированный учет активов, проверку ресурсов даркнета и хакерских форумов на предмет возможных утечек данных в пределах корпоративного сегмента, а также приоритизацию рисков. Сканирование должно осуществляться непрерывно и рекурсивно. Оценка защищенности должна проводиться с использованием технологий искусственного интеллекта.

Указанные работы выполняются автоматизировано в специализированной системе. Исполнитель должен предоставить доступ к личному кабинету системы. Система должна поддерживать функции выгрузки, записи и сохранения отчетов

сканирования. Использование программного обеспечения, распространяемого по лицензиям Open Source (с открытым исходным кодом), не допускается. Исполнитель после заключения договора в течении 3 рабочих дней предоставляет документы, подтверждающие правомерность использования (лицензии, подписки или сублицензионные соглашения) указанного ПО, действующие на весь период проведения аудита.

3.2.7. Заключительные рекомендации

Подготовка комплексных рекомендаций по повышению уровня защищенности информационных систем и данных Заказчика, включая организационные, технические и процедурные меры.

3.3. Требования к контролю со стороны Заказчика

Исполнитель обязан:

- В течение 10 рабочих дней после подписания договора предоставить:
- перечень необходимой информации;
- план-график проведения аудита;
- Проводить статус-сессии не реже 1 раза в две недели.
- По каждому этапу предоставлять подробные планы, отчеты, ссылки на нормативные акты, стандарты и рекомендации по устранению нарушений.
- Обеспечить полную конфиденциальность данных Заказчика и предоставить оригиналы обязательств о неразглашении в течение 10 рабочих дней с момента подписания договора.

3.4. Методология проекта

Услуги оказываются поэтапно:

Этап 1. Сбор и анализ данных

- Сбор и анализ организационно-распорядительной документации по ИБ (политики, регламенты, инструкции, матрицы доступа, договоры с подрядчиками).
- Инвентаризация информационных систем, прикладного ПО, лицензий и владельцев систем.
- Проведение интервью с ответственными сотрудниками Заказчика по процессам обеспечения ИБ.
- Анализ фактических практик управления доступом, учетными записями и правами пользователей.

Этап 2. Анализ защищенности прикладного программного обеспечения

- согласование перечня анализируемого программного обеспечения и состава передаваемых материалов;
- анализ исходного кода, а также исполняемых файлов при отсутствии исходного кода;
- выявление сторонних и свободно распространяемых компонентов и их известных уязвимостей;
- ручная проверка выявленных дефектов на предмет ложных срабатываний;
- формирование отчета по результатам оказанных Услуг.

Этап 3. Аудит процессов обеспечения информационной безопасности

По результатам проведенного анализа Исполнитель:

- проводит оценку действующих процессов и практик обеспечения информационной безопасности;

- анализирует имеющуюся у Заказчика организационно-распорядительную, нормативную и методическую документацию в области ИБ;

- выявляет несоответствия, пробелы и области, требующие совершенствования; предоставляет рекомендации по совершенствованию процессов обеспечения информационной безопасности;

- дорабатывает и предоставляет Заказчику проекты необходимых организационно-распорядительных, нормативных и методических документов по информационной безопасности с учетом результатов проведенного анализа и применимых требований;

- передает разработанный комплект документов Заказчику для последующего рассмотрения, согласования и утверждения.

Анализ и доработка документов осуществляется в рамках согласованного с Заказчиком перечня. Утверждение документов, их внедрение и дальнейшее обеспечение выполнения установленных требований осуществляются Заказчиком самостоятельно.

Этап 4. Проверка настроек компонентов информационной инфраструктуры

В рамках оказываемых услуг Исполнитель осуществляет проверку настроек предоставленных компонентов инфраструктуры, включая:

- серверную инфраструктуру и операционные системы;

- межсетевые экраны и иные сетевые средства защиты информации;

- сетевое оборудование;

- среды виртуализации;

- системы управления и администрирования;

- СУБД;

- средства удаленного доступа;

- SIEM-системы;

- иные компоненты инфраструктуры, включенные в согласованный перечень.

Проверка включает:

- анализ настроек аутентификации и парольной политики;

- проверку разграничения прав доступа и привилегированных учетных записей;

- проверку настроек удаленного и административного доступа;

- анализ разрешенных сетевых соединений, портов и сервисов;

- проверку правил межсетевого экранирования;

- анализ настроек журналирования и мониторинга событий информационной безопасности;

- проверку актуальности используемых версий и настроек безопасности;

- анализ настроек резервного копирования и восстановления в части предоставленных параметров;
- проверку иных параметров безопасности в соответствии с применимыми требованиями и согласованной методикой.

По результатам проверки Исполнитель предоставляет перечень выявленных недостатков и несоответствий, оценку связанных с ними рисков и рекомендации по их устранению.

Этап 5. Обучение повышения уровня осведомленности в области кибербезопасности и цифровой гигиены.

Исполнитель должен обеспечить проведение обучения по вопросам повышения уровня осведомленности в области кибербезопасности и цифровой гигиены. По итогам обучения должно быть предусмотрено итоговое тестирование. Пользователям, успешно прошедшим итоговое тестирование или завершившим курс в соответствии с установленными условиями, выдаются именные электронные сертификаты, подтверждающие прохождение обучения.

3.5. Распределение задач

- Исполнитель выполняет обследование, анализ, тестирование, предоставляет отчеты.
- Заказчик обеспечивает предоставление информации, доступов, организацию встреч.
- Взаимодействие осуществляется через утвержденные каналы связи с Заказчиком (e-mail, файлообменники и др.).

3.6. Требования к результатам

Исполнитель должен предоставить:

1. Финальный отчет, содержащий:

- результаты всех видов анализа;
- отчеты по этапам работ;
- информацию о выявленных несоответствиях и рисках;
- рекомендации по повышению уровня защищенности.

2. Промежуточные отчеты, включая всю исходную документацию, предоставляются по мере завершения отдельных этапов оказания услуг в соответствии с план-графиком проведения аудита, а также по запросу Заказчика в срок не позднее 10-и рабочих дней после получения запроса.

3. Структура и формат предоставляемого пакета документов должны быть предварительно согласованы с Заказчиком.

3. Технические стандарты

№ п/п	Зарегистрирован в РК	Обозначение	Номер документа	Категория	Наименование	Область применения	Разработчик	Страницы	МКС	Статус	Приказ	Дата введения с

1	Да	СТ РК ISO /IEC 27002-2015	384046	Национальный стандарт Республики Казахстан	Информационная технология методы и средства обеспечения безопасности и свод правил по средствам управления защитой информации	Настоящий стандарт содержит руководство для организационных стандартов по информационной безопасности и управлению информационной безопасностью, включая отбор, внедрение и управления системами управления, принимая во внимание организационную среду информационного риска.	Нет ()	178	Наборы знаков и кодирование информации	Действует	Приказом Председателя Комитета технического регулирования и метрологии Министерства по инвестициям и развитию Республики Казахстан от 24 ноября 2015 г. № 236-од	01.01.2017

Подписал Карменова Лэйла Нуралиевна

Дата подписания 03.11.2026