Құжат «Самұрық-Қазына» АҚ сатып алу веб-порталымен құрылған
Документ сформирован веб-порталом закупок АО «Самрук-Қазына»

ТЕХНИКАЛЫҚ СИПАТТАМА

1265154 , Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтер сатып алу бойынша Ашық тендер тәсілімен

Лот № 1 (21-1 У, 4564722) Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер

Тапсырыс беруші: ТОО «СП «Caspi Bitum»

Ұйымдастырушы: ТОО «СП «Caspi Bitum»

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	21-1 У
Атауы және қысқаша сипаттамасы	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер, Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтер
Қосымша сипаттама	Ақпараттық қауіпсіздік жедел орталығының қызметтері.
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Маңғыстау облысы, г. Актау, промышленная зона 5, здание 65
Жеткізу шарттары	-
Жеткізу мерзімі	01.2027 бастап 12.2029 дейін (қоса алғанда)
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 100%, Соңғы төлем - 0%

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

Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтерге техникалық ерекшелік (Ақпараттық қауіпсіздіктің операциялық орталығы)

Пайдаланылатын қысқартулар мен терминдер тізімі

Қысқарту / термин	Толық жазылуы
АҚ	Ақпараттық қауіпсіздік

АҚОО (SOC)	Ақпараттық қауіпсіздіктің операциялық орталығы – электрондық ақпараттық ресурстарды, ақпараттық жүйелерді, телекоммуникация желілерін және өзге де ақпараттандыру объектілерін қорғау жөніндегі қызметті жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі
АҚ инциденті	Ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген объектілерінің жұмысындағы жекелеген немесе сериялы түрде туындайтын, олардың тиісінше жұмыс істеуіне қауіп төндіретін және (немесе) электрондық ақпараттық ресурстарды заңсыз алуға, көшіруге, таратуға, түрлендіруге, жоюға немесе бұғаттауға жағдай жасайтын іркілістер
АЖ	Ақпараттық жүйе – белгілі бір технологиялық әрекеттерді ақпараттық өзара іс-қимыл арқылы іске асыратын АКТ, қызмет көрсетуші персонал мен техникалық құжаттаманың ұйымдастырушылық тұрғыдан реттелген жиынтығы
АТ / ОТ	Ақпараттық технологиялар / операциялық (технологиялық) технологиялар
ТПАБЖ	Технологиялық процесті автоматтандырылған басқару жүйесі
АКИАМО	Ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілері
АҚҰКО	Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығы

«МТҚ» АҚ	«Мемлекеттік техникалық қызмет» АҚ
ИҚБШ	Интернетке қол жеткізудің бірыңғай шлюзі
SIEM	Security Information and Event Management – АҚ оқиғаларын басқару жүйесі
IRP	Incident Response Platform – АҚ инциденттеріне ден қою платформасы
MISP	Қауіптер туралы деректермен (Threat Intelligence) алмасу платформасы
VPN (Site-to-Site)	Виртуалды жеке желі – Тапсырыс берушінің және Орындаушының АҚОО алаңдары арасындағы криптографиялық құралдармен қорғалған байланыс
Мониторинг периметрі	АҚОО-ға қосылған Тапсырыс берушінің АҚ оқиғалары көздерінің жиынтығы
АҚҚ	Ақпаратты қорғау құралдары
Орындаушы	Сатып алу туралы шартты жасасуға үміткер / жасасқан заңды тұлға немесе консорциум

2.1. Негізгі ережелер

Орындаушы Тапсырыс берушіге тәулік бойы (24×7×365) АҚОО қызметтерін көрсетеді: Тапсырыс берушінің АТ және ОТ инфрақұрылымындағы АҚ оқиғаларына мониторинг жүргізу, АҚ инциденттерін анықтау, талдау және оларға ден қою. Қызметтер «Киберқауіпсіздік туралы» Қазақстан Республикасы Заңының 7-5-бабына сәйкес көрсетіледі.

Шарт жасасқан күннен бастап 10 (он) жұмыс күні ішінде Орындаушы Тапсырыс берушімен АҚОО қызметтерін көрсету кезіндегі өзара іс-қимыл регламентін (АҚ инциденттерін анықтау және оларға ден қою, байланыс тұлғалары, байланыс арналары, есептілік мерзімдері) әзірлейді және келіседі. Дәл осы мерзімде тараптар АҚ инциденттерін жою бөлігінде рөлдер мен жауапкершілікті бөлу матрицасын ресімдейді.

Қызметтерді көрсету мерзімі. 2027 жылғы 01 қаңтардан бастап 2029 жылғы 31 желтоқсанға дейін.

2.2. Нормативтік-құқықтық база

Осы техникалық ерекшелік Қазақстан Республикасының мынадай нормативтік құқықтық актілеріне сәйкес әзірленді:

1. «Киберқауіпсіздік туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы – ақпараттандыру объектілері мен АКИАМО-ның АҚ-сын қамтамасыз етуге қойылатын талаптар, АҚОО қызметі (7-5-бап) және АҚҰКО-мен өзара іс-қимыл бөлігінде.
2. Қазақстан Республикасының 2026 жылғы 9 қаңтардағы № 255-VIII «Қазақстан Республикасының Цифрлық кодексі» Кодексі – цифрлық объектілердің киберқауіпсіздігі және аудиті талаптары бөлігінде (97–99-баптар).
3. «Ұлттық қауіпсіздік туралы» Қазақстан Республикасының 2012 жылғы 6 қаңтардағы № 527-IV Заңы – ақпараттық қауіпсіздікті ұлттық қауіпсіздіктің құрамдас бөлігі ретінде қамтамасыз ету бөлігінде.
4. «Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы – дербес деректерді Қазақстан Республикасының аумағында өңдеу және сақтау бөлігінде (12-бап).
5. «Терроризмге қарсы іс-қимыл туралы» Қазақстан Республикасының 1999 жылғы 13 шілдедегі № 416-I Заңы – терроризмге қатысты осал объектілерді және олардың ақпараттық жүйелерін қорғау бөлігінде (10-3-бап).
6. «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы.
7. Қазақстан Республикасының Үкіметі бекіткен ақпараттық-коммуникациялық инфрақұрылым объектілерін АКИАМО-ға жатқызу қағидалары мен өлшемшарттары.
8. АҚОО мен АҚҰКО арасында АҚ-ты қамтамасыз ету үшін қажетті ақпаратпен алмасу қағидалары, сондай-ақ АҚ саласындағы уәкілетті орган бекіткен АКИАМО-ның АҚ-сын қамтамасыз ету мониторингін жүргізу қағидалары.

Қызметтер сондай-ақ Орындаушыға жеткізілген Тапсырыс берушінің АҚ саласындағы ішкі нормативтік құжаттарын ескере отырып көрсетіледі. Актілердің деректемелері қызметтер көрсету күніне қолданыста болатын редакцияда қолданылады.

2.3. Қызметтерге қойылатын талаптар

АҚ инциденттерін мониторингтеу және оларға ден қою шеңберінде Орындаушы мыналарды қамтамасыз етуге міндетті:

1. Тапсырыс берушінің мониторинг периметрінде туындайтын АҚ оқиғаларын тәулік бойы (24×7×365) мониторингтеу.
2. Тіркелген АҚ инциденттерін жою жөніндегі ұсынымдарды әзірлеу және Тапсырыс берушіге беру. Қажет болған жағдайда Орындаушы инцидентті жою үшін әрекеттер орындау талап етілетін жабдық пен БҚ өндірушілерінің техникалық қолдау қызметтеріне өтінімдер (тикеттер) ашады. Өтінімдер Тапсырыс берушінің атынан жасалады.
3. Шарт жасасқан күннен бастап 45 (қырық бес) күнтізбелік күн ішінде Тапсырыс берушімен бірлесіп оқиға көздерінің толық тізбесін қалыптастыру және оларды Орындаушының АҚОО-на қосу. Тапсырыс беруші агенттер мен коллекторларды өз қуаттарында орнатады және «шикі» деректерді Site-to-Site VPN арқылы Орындаушының инфрақұрылымына береді. «Шикі» деректер коллекторларына арналған лицензиялар Орындаушының міндеттемелеріне кіреді.
4. Оқиғаларды тіркеу журналдарының тізбесін анықтау және ОЖ, ДҚБЖ, желілік жабдық, қолданбалы БҚ және АҚҚ оқиғаларын хаттамалауды баптау (көзде функционал болған кезде) мақсатында Тапсырыс беруші объектілерін (оның ішінде АКИАМО-ға жатқызылғандарын) талдау.
5. АҚ оқиғаларын үш желілі модель бойынша мониторингтеу:
    - **бірінші желі** – инциденттерді тіркеу және нақты техникалық шешімдер бойынша терең құзыреттерді қажет етпейтін негізгі ұсынымдарды беру; 24×7×365 режимі;
    - **екінші желі** – типтік АҚ инциденттерін шешу, арнайы құралдарды пайдалана отырып терең талдау, корреляция ережелерін Тапсырыс беруші инфрақұрылымының өзгерістеріне бейімдеу, келісілген инциденттерді рөлдер матрицасына сәйкес жою; 8×5 режимі;
    - **үшінші желі** – Орындаушы сарапшыларының сыни деңгейдегі АҚ инциденттерін тергеп-тексеруі, жою жөніндегі ұсынымдар, ретроспективті талдау, өзекті қауіптер, шабуылдар және оларды анықтау мен оларға қарсы тұру тәсілдері туралы мәліметтерді өзектендіру; 8×5 режимі.
6. Анықталған АҚ инциденттері туралы ақпаратты Тапсырыс берушімен келісу бойынша АҚҰКО-ға беру: хабарлама – анықталған сәттен бастап 15 минут ішінде, инцидент туралы деректер тізбесі – 24 сағат ішінде, осалдықтарды жою шаралары туралы мәліметтер – зерттеп-қарау нәтижелерін алған күннен бастап 20 күнтізбелік күн ішінде.
7. Тапсырыс берушінің жұмыс станцияларындағы, серверлеріндегі және желісіндегі қауіптер туралы ақпаратты нақты уақыт режимінде алу.
8. Орындаушының шабуылдарды анықтау сценарийлерін іске асыру және жалған іске қосылуларды барынша азайту үшін қажетті АТ/ОТ инфрақұрылымы мен активтер

туралы мәліметтерді Тапсырыс берушіден сұратуға құқығы. Сұрау салу Тапсырыс берушінің уәкілетті тұлғасына негіздемемен бірге электрондық пошта арқылы жолданады; Тапсырыс беруші 5 жұмыс күні ішінде жауап береді (мерзім түзетілуі мүмкін). Сұрау салу мыналарға қатысты болуы мүмкін, бірақ олармен шектелмейді: DNS-серверлер тізімі; қауіпсіздік сканерлерінің IP-мекенжайлары; Интернет желісінен қолжетімді ресурстар; Тапсырыс берушінің «ақ» IP-мекенжайлары; АЖ әкімшілерінің есептік жазбалары; АЖ және ресурстар иелері; IP-мекенжайлардың пайдаланушыларға немесе жүйелерге тиесілігі; ТПАБЖ желілері мен АТ сегменттері бойынша техникалық құжаттама.

9. Қажет болған жағдайда Тапсырыс берушінің ТПАБЖ, АТ жүйелері және АҚҚ өндірушілерімен өзара іс-қимыл жасау; өтінімдер Тапсырыс берушінің атынан жасалады.
10. Тапсырыс беруші іске асыратын АТ жобаларында және автоматтандыру жобаларында (оның ішінде ТПАБЖ жаңғырту кезінде) АҚ-ның ұйымдастырушылық-техникалық шараларын Тапсырыс берушінің сұрауы бойынша талап етілетін қауіпсіздік деңгейіне сәйкестігіне бағалау, шараларды жақсарту жөнінде ұсыныстар және енгізілетін жүйелер дизайнын әзірлеуге АҚ бөлігінде қатысу.
11. Тапсырыс берушіден алынатын деректерді (оқиғалар, желілік ағындар) шарттың қолданылу мерзімі ішінде тек Қазақстан Республикасының аумағында орналасқан ресурстарда сақтау.
12. Қызметтерді көрсетудің технологиялық негізі ретінде SIEM, SOAR, UEBA және Threat Intelligence сыныбындағы арнайы платформаны пайдалану. Платформа Орындаушының құралы болып табылады, тек қызметтер көрсету үшін қолданылады және Тапсырыс берушіге жеткізілмейді, берілмейді және оның меншігіне ресімделмейді. Платформа мыналарды қамтамасыз етуі тиіс:

– АҚ оқиғаларын орталықтандырылған жинауды, өңдеуді және сақтауды;

– АҚ инциденттерін анықтауды, корреляциялауды және жіктеуді;

– оқиғалар мен инциденттерге олардың сыни деңгейі бойынша автоматты түрде басымдық беруді;

– талдамалық қорытындылар мен ден қою жөніндегі ұсынымдарды қалыптастыруды;

– сценарийлерді (плейбуктарды) пайдалана отырып, ден қою процестерін автоматтандыруды;

– инциденттер хронологиясын және әрекеттер журналын жүргізуді.

1. Платформаның үздіксіз жұмысын, жаңартылуын және сүйемелденуін, оқиғаларды нақты уақытқа жақын режимде (24×7×365) өңдеуді.
2. Тапсырыс берушіге платформаның жеке кабинетіне қолжетімділік беру: АҚ оқиғалары мен инциденттерін нақты уақыт режимінде қарау, талдау нәтижелері мен ұсынымдарға қол жеткізу, инциденттер тарихы мен олар бойынша әрекеттерді қарау, есептілікті қалыптастыру және жүктеп алу мүмкіндігімен.

3. ОЖ, ДҚБЖ, қолданбалы БҚ, АҚҚ, қорғалуын талдаудың арнайы құралдарының қауіпсіздік оқиғаларын тіркеу мен есепке алудың кіріктірілген тетіктері, сондай-ақ АҚҰКО-дан алынған ақпарат негізінде АҚ оқиғаларын ықтимал қауіптер мен инциденттер тұрғысынан талдау.
4. АКИАМО объектісінің иесін және АҚҰКО-ны АҚ инциденттері туралы Орындаушының жауапты қызметкерінің (немесе ол уәкілеттік берген қызметкердің) электрондық пошта арқылы және (немесе) MISP платформасы арқылы хабардар етуі.

2.4. АҚОО қызметтерінің түрлері

Қызмет түрі	Қысқаша сипаттамасы
АҚОО-ның (SOC) бірінші желісі	АҚ оқиғаларын 24×7 режимінде талдау. Жалған іске қосылуларды тексеру, алғашқы талдау және санаттар мен ережелер негізінде АҚ инциденттерін бөліп көрсету; типтік инциденттерге ден қою жөніндегі ұсынымдар; АҚОО жүйелерінде инциденттер туралы мәліметтерді тіркеу және өзектендіру. Сыртқы периметрді қорғауға қатысты инциденттерге ден қою. Хаттар мен қоңырауларға жауап беру, АҚ инциденттері мен оқиғалары туралы ақпараттық хабарламаларды тарату
АҚОО-ның (SOC) екінші желісі	АҚ инциденттерін 8×5 режимінде өңдеу, ден қою жөніндегі ұсынымдар, инциденттерді терең талдау. Корреляция ережелерін Тапсырыс беруші инфрақұрылымының өзгерістеріне бейімдеу; Тапсырыс берушінің талап етуі бойынша корреляция ережелеріне ерекшеліктер енгізу
АҚОО-ның (SOC) үшінші желісі	Сыни АҚ инциденттеріне ден қоюды қолдау, тергеп-тексеру қорытындылары бойынша Тапсырыс беруші инфрақұрылымының қорғалуын арттыру жөніндегі ұсынымдар. Корреляция ережелерін, оның ішінде ТПАБЖ сегментіне шабуыл сценарийлері үшін әзірлеу

Қосымша сараптама	Ең сыни инциденттерді тергеп-тексеру, қатты дискілердің бейнелерін жинау және зерттеу (форензика), зиянды БҚ-ны талдау, салдарларды жоюға көмектесу. Жылына 4 рет (сыртқы және ішкі периметр, Grey Box моделі, тоқсан сайынғы негізде) ену тестілеуін жүргізу және кейіннен осалдықтардың жойылуын бақылау; бақылау әдістерін Орындаушы таңдайды. Тапсырыс берушінің сұрауы бойынша бастапқы кодқа аудит – жылына 1 рет, қосымша көлемі 500 000 жолдан аспайды, құқық иесі – Тапсырыс беруші
Сыртқы периметрді қорғау	Интернет желісінен қолжетімді Тапсырыс беруші ресурстарына бағытталған қауіптерді мониторингтеу және оларға ден қою
Осалдықтардың бар-жоғына сканерлеу	Ішкі және сыртқы периметрді, жабдық пен тораптарды қосымшалар мен ОЖ осалдықтарының бар-жоғына тоқсанына 1 рет, сондай-ақ Тапсырыс берушінің өтінімі бойынша (айына 1 реттен жиі емес) сканерлеу. Осалдықтар бойынша ұсынымдары бар толық есеп – сканерлеу аяқталғаннан кейін 15 жұмыс күні ішінде; осалдықтарды жою бойынша консультация беру
Желілік құрылғылардың конфигурацияларын талдау	Конфигурацияларды желілік жабдық өндірушілерінің ақпараттық қауіпсіздік бөлігіндегі тәжірибелері мен ұсынымдарына сәйкестігі тұрғысынан талдау жүргізу және Тапсырыс берушіге ұсынымдар беру
Фишинг-кампания	Тапсырыс берушімен келісілген фишинг-тарату жұмысын тоқсанына 1 рет жүргізу, нәтижелер мен әрекеттерге арналған ұсынымдарды беру

АҚ зерттеп-қарау және ену тестілеуі. Зерттеп-қарау объектілерінің тізбесі Тапсырыс берушімен келісіледі. Зерттеп-қарау мынадай тәртіппен жүргізіледі:

• сыртқы периметр – «осалдық сканері» сыныбындағы БҚ қолдана отырып сканерлеу; осалдықтарды валидациялау үшін барлық анықталған нәрселерді Орындаушының білікті маманы қолмен тексереді; сканерлеу аймағы – кемінде 10 объект (бірегей жария URL);

• ішкі сегмент – ішкі URL-дер VPN-қосылымды пайдалана отырып сканерленеді, ішкі ақпараттық жүйелер мен желілер – Тапсырыс берушінің жергілікті желі периметрінен; сканер анықталған хосттарды түгендеуді (АТ активтерінің картасы) орындайды, содан кейін олар осалдықтардың бар-жоғына тексеріледі;

• ену тестілеуін сертификатталған мамандар жүргізеді; сценарийлер мен әдістер Тапсырыс берушімен келісіледі;

• қорытындысы бойынша 2.11-тармаққа сәйкес есеп ұсынылады.

Ақпараттық қауіпсіздікке (киберқауіпсіздікке) аудит. Орындаушы Тапсырыс берушінің цифрлық объектілеріне киберқауіпсіздік аудитін Қазақстан Республикасы Цифрлық кодексінің 99-бабына және «Киберқауіпсіздік туралы» Қазақстан Республикасы Заңының 18 және 50-баптарына сәйкес мынадай шарттарда жүргізеді:

• Кезеңділігі. Жылына кемінде бір рет (аса маңызды цифрлық объектілер және заңмен қорғалатын құпияны қамтитын цифрлық деректерді өңдейтін объектілер үшін кезеңділік заңмен белгіленген). Жоспардан тыс аудит Тапсырыс берушінің сұрауы бойынша келісімшарттың қолданылу кезеңінде бір рет, Орындаушыға кемінде 30 күнтізбелік күн бұрын алдын ала жазбаша хабарлама жіберілген жағдайда жүргізіледі.

• Аудит объектілері. Келісілген тізбе бойынша Тапсырыс берушінің цифрлық объектілері, оның ішінде аса маңызды цифрлық объектілер мен ТПАБЖ.

• Бағалау өлшемшарттары. Цифрландыру және киберқауіпсіздікті қамтамасыз ету салаларындағы бірыңғай талаптар, қорғау профильдері, 2.2-тармақта көрсетілген нормативтік құқықтық актілер және Тапсырыс берушінің АҚ саласындағы ішкі нормативтік құжаттары; қазақстандық стандарттар болмаған жағдайда ISO/IEC 27001 қолдануға жол беріледі, аудит жүргізер алдында тараптар аудиттің нақты көлемін және аудит әдістемесінде қолданылатын нормативтік-құқықтық базаны айқындайды және келіседі.

• Кезеңдері. Бастапқы деректерді жинау; ұйымдастырушылық-өкімдік және техникалық құжаттаманы талдау; жауапты қызметкерлермен сұхбат жүргізу; техникалық тексеру (конфигурацияларды талдау, осалдықтарды сканерлеу); талаптарға сәйкестікті бағалау; есепті дайындау.

• Нәтижелері. Сыни деңгейі көрсетілген анықталған сәйкессіздіктер тізбесін, оларды жою жөніндегі ұсынымдар мен жоспарды қамтитын сәйкестікті бағалау туралы есеп; аудит нәтижелерін Тапсырыс берушіге ұсыну. Есеп аудит аяқталған күннен бастап 30 жұмыс күнінен кешіктірілмей беріледі.

• Жоюды бақылау. Анықталған сәйкессіздіктердің жойылуын Тапсырыс берушіден жою туралы хабарлама алынған күннен бастап [көрсету] мерзімде қайта тексеру.

• Аудит орындаушысына қойылатын талаптар. Киберқауіпсіздікті қамтамасыз ету саласында қызметтер көрсету үшін заңнамада талап етілетін лицензияның болуы; тексерілетін жүйелерден тәуелсіздік; біліктілігі расталған мамандар (оның ішінде ISO/IEC 27001 Lead Auditor); аудит жүргізу кезінде алынған ақпараттың құпиялылығын сақтау міндеттемесі.

• Бақылаушы органдармен өзара іс-қимыл. Тапсырыс берушінің сұрауы бойынша Орындаушы аудит материалдарын ұсынады және уәкілетті органдардың тексерулеріне дайындық кезінде консультациялық қолдау көрсетеді.

Фишинг-кампания. Орындаушы қызметкерлердің әлеуметтік инженерия шабуылдарына тұрақтылығын бағалау үшін оқыту фишинг-кампаниясын жүргізеді, ол фишинг сценарийлерін (хаттар, сілтемелер, нысандар) әзірлеуді, Тапсырыс берушімен келісілген қызметкерлер тізімі бойынша тарату жұмысын, нәтижелерді жинау мен өңдеуді қамтиды. Қорытындысы бойынша талдамасы мен ұсынымдары бар есеп ұсынылады, онда мыналар қамтылады: сілтемені басқан қызметкерлердің аты-жөні немесе идентификаторы; оқиғаның күні мен уақыты; құрылғының IP-мекенжайы; деректердің енгізілу фактісі (қолданылса); тәуекел деңгейі. Қызметкерлер енгізген парольдер мен өзге де дербес деректер сақталмайды, тек енгізу фактісі тіркеледі. Тапсырыс берушіге нәтижелерді өз бетінше бақылау үшін онлайн-панель немесе жүктеп алу беріледі. Кампания жұмыс жүйелеріне қауіп төндірместен, бақыланатын ортада жүргізіледі.

Компьютерлік криминалистика (форензика) міндеттері. Инциденттерді тергеп-тексеру кезінде Орындаушы объектіге техникалық қызмет көрсетуді жүзеге асыратын Тапсырыс беруші қызметкерлерімен бірлесіп мынадай міндеттерді шешеді:

- бұзуды іске асыру тәсілін анықтау;
- шабуыл сценарийін құру және оның хронологиясын қалпына келтіру;
- шабуылдың қалған іздерін жинау;
- осындай және мүмкіндігінше өзге де шабуылдардан қорғау шараларын әзірлеу;
- келтірілген зиянды азайту және жою.

2.5. Қызметтер көлемі және оқиға көздерінің тізбесі

Қызметтер көлемі төменде ең көп мөлшер ретінде көрсетілген мониторинг объектілерінің санымен айқындалады. Көздердің нақты тізбесін Тапсырыс беруші бастапқы зерттеп-қарау қорытындысы бойынша шарт жасасқан күннен бастап 45 күнтізбелік күн ішінде нақтылайды.

№	Мониторинг объектісі (оқиға көздерінің сыныбы)	Саны, көп емес
1	Серверлер (физикалық және виртуалды, Windows / Linux, оның ішінде ДҚБЖ серверлері мен пошта серверлері)	10
2	Желілік құрылғылар (коммутаторлар, маршрутизаторлар, қолжетімділік нүктелері)	30
3	Желіаралық экрандар	2
4	Жұмыс станциялары	200

5	ТПАБЖ сегментінің көздері (SCADA серверлері, инженерлік және операторлық станциялар, өнеркәсіптік желіні мониторингтеу құралдары)	Бастапқы зерттеп-қарау қорытындысы бойынша, 1–4-тармақтар шегінде

Оқиғаларды хаттамалауға қойылатын талаптар. Объектілерді талдау қорытындысы бойынша (2.3-тармақ) Орындаушы оқиғалардың мынадай түрлерін тіркеуді айқындайды және баптайды (көзде функционал болған кезде):

• ОЖ: пайдаланушылардың авторизациясы және шығуы, сәтті және сәтсіз кіру әрекеттері; жүйелік конфигурацияның өзгеруі; есептік жазбаларды құру, жою, түрлендіру; артықшылықты есептік жазбаларды пайдалану; қорғау құралдарын (антивирус, енуді анықтау жүйесі, ОЖ журналдарын емес, қорғау құралдарының журналдарын сұрау кезінде іске асыру мүмкін) және журнал жүргізу құралдарын іске қосу және сөндіру; қорғау параметрлерінің өзгеруі немесе өзгерту әрекеттері; кіріс-шығыс құрылғыларын қосу және ажырату; пайдаланушының сәтсіз аяқталған немесе қабылданбаған әрекеттері, оның ішінде деректер мен ресурстарға қатысты әрекеттер; процестерді іске қосу және тоқтату;

• ДҚБЖ: сессияларды бақылау (сәтті және сәтсіз авторизация, тіркелмеген есептік жазбаларды пайдалану); әкімшілік артықшылықтары бар пайдаланушылардың барлық әрекеттері; артықшылықтарды ДҚ-ның басқа пайдаланушыларына тағайындау құқығы бар пайдаланушылардың барлық әрекеттері;

• желілік жабдық: жүйені іске қосу және тоқтату; конфигурацияның өзгеруі; жергілікті есептік жазбаларды құру, жою, түрлендіру; артықшылықты есептік жазбаларды пайдалану; кіріс-шығыс құрылғыларын қосу және ажырату; пайдаланушының сәтсіз аяқталған немесе қабылданбаған әрекеттері; желілік байланыстарды іске қосу, құлау және тоқтату;

• қолданбалы БҚ: пайдаланушыларды авторизациялау (сәтті және сәтсіз); есептік жазбалар мен конфигурациялық файлдарды құру, көшіру, жылжыту, жою, түрлендіру; сәтсіз аяқталған немесе қабылданбаған әрекеттер; қолжетімділік объектілеріне қол жеткізу; пайдаланушылардың деректермен әрекеттері (қол жеткізу, өзгерту, жою);

• АҚҚ: есептік жазбалар мен конфигурациялық файлдарды құру, көшіру, жылжыту, жою, түрлендіру; қызметті іске қосу және тоқтату; жүйелік конфигурацияның өзгеруі.

Хаттамаланатын әрбір оқиға үшін кемінде мыналар жазылады: пайдаланушы идентификаторы, оқиға түрі, күні мен уақыты, нәтижесі (сәтті немесе сәтсіз), оқиға көзі, оқиға әсер еткен деректердің, компоненттің немесе ресурстың идентификаторы немесе

атауы. Оқиғалар журналы мынадай өрістерді қамтуы тиіс: күні мен уақыты (КК.АА. ЖЖЖЖ, СС:ММ:СС); оқиға көзінің атауы (сервис, қызмет); есептік жазбаның аты немесе пайдаланушы ID-і; клиенттің IP-мекенжайы; операцияның басталу және аяқталу уақыты; оқиғаның сипаттамасы.

2.6. АҚ инциденттерін тіркеу

АҚ инциденті тіркелген кезде Орындаушы өзінің есепке алу жүйесінде инцидент карточкасын жасайды және оны Тапсырыс берушіге жолдайды. Карточка мыналарды қамтиды:

- Орындаушының есепке алу жүйесіндегі АҚ инцидентінің атауы мен нөмірі;
- UTC форматындағы тіркеу уақыты және инциденттің басымдығы;
- инцидент сәтінде зардап шеккен хосттардың және олардағы белсенді есептік жазбалардың тізбесі (деректер қолжетімді болған кезде);
- инцидент негізінде анықталған АҚ оқиғаларының көзі(лері);
- анықталған компрометация индикаторлары (хэш-сомасы мен файл атауы, C&C-сервердің мекенжайы, байланысты домендік атаулар және т.б.);
- қоса берілетін файлдарға сілтемелер;
- ұсынымдар: салдарларды болдырмау немесе барынша азайту жөніндегі алғашқы әрекеттер не одан әрі талдау үшін Тапсырыс берушіден қажетті қосымша мәліметтер.

Инцидентті Тапсырыс беруші күшімен анықтаған кезде ол Орындаушыны электрондық пошта арқылы немесе Өзара іс-қимыл регламентінде көрсетілген өзге арна арқылы хабардар етеді. Орындаушы инцидентті тіркейді және Тапсырыс берушіге оның нөмірін, тіркеу уақытын, қысқаша сипаттамасын және ұсынымдарды хабарлайды.

Тапсырыс берушінің өтініштері. Инциденттерден басқа, Тапсырыс беруші Орындаушыға мынадай түрдегі өтініштерді жолдай алады:

• өзгеріс туралы сұрау – қызмет конфигурациясын өзгерту (АҚ оқиғалары көзін қосу немесе алып тастау, анықтау сценарийін бейімдеу); қажеттілігіне қарай;

• ақпараттық сұрау – қызмет пен шарт бойынша консультациялық сұрақтар; қажеттілігіне қарай;

• АҚ инциденттеріне күмән – Тапсырыс берушінің болжамды инцидент туралы өтініші; бастапқыда «шұғылдығы төмен» басымдығы беріледі, Тапсырыс беруші оны арттыруға құқылы; өңдеу 2-кестеге сәйкес жүргізіледі; өтініштер саны шектелмейді.

2.7. Инциденттерді жіктеу және қызмет көрсету стандарттары (SLA)

1-кесте. АҚ инциденттерін жіктеу

Басымдық	Сипаттамасы	Мысал
Сыни (шұғыл)	Тапсырыс берушінің қорғалатын ресурстарының 15 минуттан астам толық қолжетімсіздігі, елеулі залал келтіру мүмкіндігімен ресурстардың көп санының компрометациясы, технологиялық процестің тоқтауы немесе бұзылу қаупі не шабуылдың таргеттелген сипаты	Домен әкімшісінің есептік жазбасы компрометацияланған таргеттелген шабуыл; ТПАБЖ сегментіне рұқсатсыз қол жеткізу
Жедел	Қазіргі уақытта ресурстардың қолжетімсіздігіне әкелмейтін, бірақ неғұрлым жоғары басымдықтағы инцидентке ұласу ықтималдығы жоғары инцидент; зиянды белсенділік оқшауланған және алдын алу АҚҚ-мен бұғатталған	Хостты жұқтыру әрекетімен браузер осалдығын пайдалану, антивирустық қорғаныспен бұғатталған
Шұғылдығы төмен	Тапсырыс берушіге зиян келтірмейтін инцидент; қолда бар қолжетімділік құқықтары шеңберінде жүйе туралы ақпарат жинау	Қорғалатын периметр туралы ақпарат жинау

2-кесте. Қызмет көрсету стандарттары

Кезең	Басымдық	Орындаушының әрекет ету уақыты	Режим
Инцидентті анықтау және тіркеу	Сыни, жедел	Назар аудару – 15 минутқа дейін	24×7×365

Инцидентті анықтау және тіркеу	Шұғылдығы төмен	Назар аудару – 60 минутқа дейін	24×7×365
Тапсырыс берушіні хабардар ету (мессенджердегі топ және e-mail)	Сыни	Тіркелген сәттен бастап 30 минутқа дейін	24×7×365
Тапсырыс берушіні хабардар ету	Жедел	Тіркелген сәттен бастап 45 минутқа дейін	24×7×365
Тапсырыс берушіні хабардар ету	Шұғылдығы төмен	Тіркелген сәттен бастап 90 минутқа дейін	24×7×365
Инцидентті жою жөніндегі ұсынымдар және жою	Сыни	Назар аудару – 30 минут; жабдықты ауыстыруды немесе елеулі қайта конфигурациялауды талап етпейтін шешім – 3 сағат	24×7×365
Инцидентті жою жөніндегі ұсынымдар және жою	Жедел	Назар аудару – 4 сағат; БҚ-ны немесе жабдықты жаңартуды (ауыстыруды) талап етпейтін шешім – 6 сағат	24×7×365
Инцидентті жою жөніндегі ұсынымдар және жою	Шұғылдығы төмен	Назар аудару – 8 сағат; БҚ-ны немесе жабдықты жаңартуды (ауыстыруды) талап етпейтін шешім – 12 сағат	24×7×365

Егер АҚ инцидентін жою үшін үшінші тұлғалардың БҚ немесе жабдық өндірушісінің техникалық қолдауына жүгіну және (немесе) Тапсырыс берушіден қосымша ақпарат қажет болса, инцидентті нақты шешу мерзімі ұзартылады. Осы уақытқа инцидент «Күту» мәртебесіне ауыстырылады. Тапсырыс беруші Орындаушының сұраулары бойынша жедел жауап беру үшін 3 (үш) маманның байланыс нөмірлерін көрсетеді.

Сыни инцидент болған кезде Орындаушы Тапсырыс берушінің сұрауы бойынша жауапты маманды Тапсырыс беруші объектісіне 24 сағат ішінде жібереді. Ден қою мыналарды қамтиды: инцидентті растау немесе жоққа шығару; оны жіктеу және сыни деңгейін нақтылау; дәлелдемелерді жинау және сақтау; салдарларды барынша азайту; персоналға консультация беру; тәуекелдерді қайта бағалау және АҚ регламенттерін өзектендіру.

2.8. Жауапкершілік аймақтарын бөлу

№	Параметр	Тапсырыс беруші	Орындаушы
1	АҚ оқиғаларына 24×7 мониторинг және талдау, жалған іске қосылуларды тексеру, алғашқы талдау, инциденттерді тіркеу		+
2	АҚ оқиғаларын басқару ішкі жүйесінің (SIEM, коллекторлар) жұмысқа қабілеттілігін мониторингтеу және дұрыс жұмыс істеуі		+

3	Көздерде агенттер мен коллекторларды орнату, оқиғалар ағындарын коллекторларға бағыттау	+	+
4	Орындаушының ұсынымдары бойынша коллекторларға арналған есептеу қуаттарын беру	+	
5	Тапсырыс беруші мен Орындаушы алаңдары арасындағы қорғалған арнаның (Site-to-Site VPN) жұмысқа қабілеттілігі	+	+
6	Мониторинг периметрінің жабдығы мен АЖ-ның өзекті тізбесі, өзгерістер (жаңа құрылғылар, IP-мекенжайлау, сыртқы қосылымдар) туралы жедел хабардар ету	+	
7	Ден қою жөніндегі ұсынымдар беру және инциденттерді тергеп-тексеру		+

8	Инциденттерді оқшаулау, салдарларын жою және штаттық режимді Орындаушының ұсынымдары бойынша қалпына келтіру (оның ішінде ТПАБЖ сегментінде)	+	
9	Қайталама инциденттерді болдырмау үшін ұсынымдарды қолдану	+	
10	Тапсырыс беруші деректерін (оқиғалар, желілік ағындар) шарттың қолданылу кезеңінде ҚР аумағында сақтау		+

Рөлдердің толық бөлінуі 2.1-тармаққа сәйкес тараптар келісетін матрицада бекітіледі.

2.9. Жоспарлы және апаттық жұмыстар

Жоспарлы жұмыстар. Орындаушы қызмет көрсетілетін ішкі жүйелерге сағат 19:00-ден 08:00-ге дейін (Астана қаласының уақыты бойынша) немесе Тапсырыс берушімен келісілген кезеңде жоспарлы қызмет көрсетуді, жаңғыртуды немесе жетілдіруді жүргізе алады. Жұмыстар уақытында Орындаушы Тапсырыс берушіні АҚОО-ның резервтік алаңына ауыстырады. Орындаушы Тапсырыс берушіні кемінде 7 (жеті) күнтізбелік күн бұрын хабардар етеді, Тапсырыс берушінің сұрауы бойынша немесе мемлекеттік органдардың талабы бойынша жүргізілетін жұмыстарды қоспағанда.

Тапсырыс беруші қорғалатын ресурстардың қолжетімсіздігін туғызуы мүмкін өз жабдығындағы жоспарлы жұмыстар (оның ішінде технологиялық қондырғылардың

жоспарлы тоқтатылуы) туралы Орындаушыны кемінде 5 (бес) күн бұрын хабардар етеді. Хабарламада күні, уақыты, ұзақтығы және байланыс тұлғасы көрсетіледі. Мерзімдердің ауыстырылғаны туралы Тапсырыс беруші 1 (бір) тәуліктен кешіктірмей хабарлайды.

Апаттық жұмыстар қызмет көрсету мезгіл-мезгіл үзілген кезде немесе оның сапасы айтарлықтай нашарлаған кезде жүргізіледі. Әрбір тарап екінші тарапты өз жабдығындағы осындай жұмыстар туралы олар басталғанға дейін 24 (жиырма төрт) сағат ішінде мерзімдері мен байланыс тұлғасын көрсетіп хабардар етеді.

2.10. Орындаушыға қойылатын талаптар

Тапсырыс беруші персоналын оқыту. Орындаушы Тапсырыс берушінің кемінде 2 (екі) негізгі АҚ маманын АҚ инциденттеріне ден қою бойынша оқытуды жүргізеді: әрқайсысына киберинциденттерді тергеп-тексеру немесе талдау саласында 1 авторизацияланған курстан. Курстардың нақты атауы жұмыстарды орындау сәтінде келіседі.

Тапсырыс беруші қызметкерлерін киберқауіпсіздік бойынша оқыту. Орындаушы Тапсырыс беруші қызметкерлерін киберқауіпсіздік мәселелері бойынша оқытуды жүргізеді: ақпаратты қорғау, цифрлық гигиена, дербес деректерді қорғау, цифрлық технологиялармен жұмыс істеу кезіндегі тәуекелдерді барынша азайту. Тақырыптар тізбесі және оқытылатын қызметкерлер саны: 25 адамнан аспайтын екі топ; міндетті тақырып – «Цифрлық гигиена және киберқауіпсіздікке кіріспе». Оқыту Тапсырыс берушінің таңдауы бойынша күндізгі және (немесе) қашықтан (бейнебайланыс арқылы) қазақ және орыс тілдерінде жүргізіледі. Сабақтар презентациялық материалдарды, практикалық мысалдарды және тестілеуді қамтиды. Сабақтар саны, ұзақтығы және өткізу кестесі Тапсырыс берушімен келіседі.

Оқыту қорытындысы бойынша Орындаушы Тапсырыс берушіге оқу материалдарын және тестілеу нәтижелерінің тізімдемесін береді.

2.11. Есептілік, кепілдік және сапа

Есепті айдан кейінгі айдың 5-күнінен кешіктірмей Орындаушы мәтіндік, кестелік және графикалық ақпараты бар ай сайынғы талдамалық есепті ұсынады:

- есепті кезеңдегі АҚ сұраулары мен инциденттерінің статистикасы, SLA көрсеткіштерінің орындалуы;
- Тапсырыс берушінің АҚ инфрақұрылымы жай-күйін талдау (АТ және ТПАБЖ);
- проблемалық мәселелер және оларды шешу жөніндегі ұсынымдар;
- қызмет көрсетуге жауапты мамандардың өзекті байланыстары.

Ену тестілеуінің қорытындысы бойынша тәуекелдерді бағалауы, желіден тыс және желі ішінен болатын шабуылдар тәуекелдерін жою және төмендету жөніндегі ұсынымдары бар осалдықтар туралы толық есеп ұсынылады. Тестілеудің жалпы ұзақтығы – 45 жұмыс күнінен аспайды, кесте Тапсырыс берушімен келіседі.

Кепілдік міндеттемелер. Көрсетілетін қызметтерге кепілдік – шарттың бүкіл қолданылу мерзіміне. Кепілдік мерзімі ішінде сервистік қызмет көрсетуді пайдаланылатын шешімдер өндірушілері авторизациялаған мамандар қамтамасыз етеді.

Сапаға қойылатын талаптар. Қызметтер осы техникалық ерекшелікке және ҚР-да қолданыстағы осы түрдегі қызметтерді реттейтін нормалар мен қағидаларға сәйкес сапалы көрсетіледі.

АҚ бойынша техникалық құжаттама. Орындаушы АҚТ және АҚ-ты қамтамасыз ету саласындағы Бірыңғай талаптардың (Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы) 31-тармағына сәйкес құжаттардың төрт деңгейлі жүйесі түріндегі АҚ бойынша техникалық құжаттама жинағын әзірлейді және Тапсырыс берушіге береді:

- бірінші деңгей – ақпараттық қауіпсіздік саясаты;
- екінші деңгей – АҚ саясатын нақтылайтын құжаттар (АҚ тәуекелдерін бағалау әдістемесі, активтерді сәйкестендіру, жіктеу және таңбалау қағидалары, аутентификация және қолжетімділікті бөлу қағидалары, антивирустық бақылау қағидалары және Бірыңғай талаптарда көзделген өзге де қағидалар);
- үшінші деңгей – процестер мен рәсімдерді сипаттайтын құжаттар (АҚ қауіптері (тәуекелдері) каталогы, қауіптерді (тәуекелдерді) өңдеу жоспары, активтердің үздіксіз жұмысын қамтамасыз ету және жұмысқа қабілеттілігін қалпына келтіру жөніндегі іс-шаралар жоспары, АҚ инциденттеріне ден қою жөніндегі нұсқаулықтар мен нұсқаулар);
- төртінші деңгей – жұмыс нысандары, журналдар және хаттамалар (АҚ инциденттерін тіркеу және штаттан тыс жағдайларды есепке алу журналы, резервтік көшірмелерді есепке алу журналы, осалдықтарды бағалау туралы есептер және өзге де құжаттар).

Құжаттама қазақ және орыс тілдерінде әзірленеді, Тапсырыс берушімен келіседі және бекітуге беріледі; Орындаушы оны кемінде екі жылда бір рет, сондай-ақ заңнама талаптары, архитектура немесе қорғау объектілерінің құрамы өзгерген кезде өзектендіреді.

2.12. Қорытынды талаптар

Қызметтер «Киберқауіпсіздік туралы» ҚР Заңының 7-5-бабына, 2.2-тармақта көрсетілген өзге де актілерге, ИҚБШ пайдалануға қойылатын талаптарға және Тапсырыс берушінің

ішкі нормативтік құжаттарына сәйкес көрсетіледі. Қазақстандық стандарттар болмаған жағдайда ҚР заңнамасында белгіленген тәртіппен ISO/IEC 27001 және үздік халықаралық тәжірибелерді қолдануға жол беріледі.

Тапсырыс беруші деректері ҚР аумағында орналасқан ресурстарда сақталады («Дербес деректер және оларды қорғау туралы» ҚР Заңының 12-бабы, «Терроризмге қарсы іс-қимыл туралы» ҚР Заңы 10-3-бабы 1-тармағының 5) тармақшасы, 2016 жылғы 20 желтоқсандағы № 832 ҚР Үкіметінің қаулысы). АҚОО-ның АҚҰКО-мен өзара іс-қимылы «Ақпараттандыру туралы» ҚР Заңына сәйкес жүзеге асырылады.

Орындаушы осы техникалық ерекшеліктің талаптарына сәйкес АҚ инциденттеріне уақтылы ден қою үшін жауапты болады және қызметтер көрсету кезінде алынған мәліметтердің құпиялылығын сақтайды.

3. Нормативтік-техникалық құжаттар

№ р/с	Атауы
1	«Киберқауіпсіздік туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы
2	Қазақстан Республикасының 2026 жылғы 9 қаңтардағы № 255-VIII «Қазақстан Республикасының Цифрлық кодексі» Кодексі
3	«Ұлттық қауіпсіздік туралы» Қазақстан Республикасының 2012 жылғы 6 қаңтардағы № 527-IV Заңы
4	«Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы
5	«Терроризмге қарсы іс-қимыл туралы» Қазақстан Республикасының 1999 жылғы 13 шілдедегі № 416-I Заңы
6	«Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы
7	Қазақстан Республикасының Үкіметі бекіткен ақпараттық-коммуникациялық инфрақұрылым объектілерін АКИАМО-ға жатқызу қағидалары мен өлшемшарттары.
8	АҚОО мен АҚҰКО арасында АҚ-ты қамтамасыз ету үшін қажетті ақпаратпен алмасу қағидалары, сондай-ақ АҚ саласындағы уәкілетті орган бекіткен АКИАМО-ның АҚ-сын қамтамасыз ету мониторингін жүргізу қағидалары.

Қол қойған Тлеуберлиев Ерасыл Ержанулы

Қол қойылған күні 11.11.2026

Құжат «Самұрық-Қазына» АҚ сатып алу веб-порталымен құрылған
Документ сформирован веб-порталом закупок АО «Самрук-Қазына»

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1265154 , Услуги по обеспечению информационной безопасности
способом Открытый тендер

Лот № 1 (21-1 У, 4564722) Услуги по обеспечению информационной безопасности

Заказчик: Товарищество с ограниченной ответственностью "Совместное предприятие "CASPI BITUM"
Организатор: Товарищество с ограниченной ответственностью "Совместное предприятие "CASPI BITUM"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	21-1 У
Наименование и краткая характеристика	Услуги по обеспечению информационной безопасности, Услуги по обеспечению информационной безопасности
Наименование категории ОКТРУ	Услуги по обеспечению информационной безопасности
Дополнительная характеристика	"Услуги оперативного центра информационной безопасности"
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, Мангистауская область, г. Актау, промышленная зона 5, здание 65
Условия поставки	-
Срок поставки	с 01.2027 по 12.2029 (включительно)
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 100%, Окончательный платеж - 0%

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

Техническая спецификация на услуги по обеспечению информационной безопасности (Оперативный центр информационной безопасности)

Список используемых сокращений и терминов

Сокращение / термин	**Расшифровка**
ИБ	Информационная безопасность

ОЦИБ (SOC)	Оперативный центр информационной безопасности – юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации
Инцидент ИБ	Отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных её объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов
ИС	Информационная система – организационно упорядоченная совокупность ИКТ, обслуживающего персонала и технической документации, реализующих определённые технологические действия посредством информационного взаимодействия
ИТ / ОТ	Информационные технологии / операционные (технологические) технологии
АСУТП	Автоматизированная система управления технологическим процессом
КВОИКИ	Критически важные объекты информационно-коммуникационной инфраструктуры
НКЦИБ	Национальный координационный центр информационной безопасности

АО «ГТС»	АО «Государственная техническая служба»
ЕШДИ	Единый шлюз доступа к Интернету
SIEM	Security Information and Event Management – сис тема управления событиями ИБ
IRP	Incident Response Platform – платформа реагирования на инциденты ИБ
MISP	Платформа обмена данными об угрозах (Threat Intelligence)
VPN (Site-to-Site)	Виртуальная частная сеть – защищённое криптографическими средствами соединение между площадками Заказчика и ОЦИБ Исполни теля
Периметр мониторинга	Совокупность источников событий ИБ Заказчика, подключённых к ОЦИБ
СЗИ	Средства защиты информации
Исполнитель	Юридическое лицо или консорциум, претендующие на заключение / заключившие договор о закупках

2.1. Основные положения

Исполнитель в круглосуточном режиме (24×7×365) оказывает Заказчику услуги ОЦИБ: мониторинг событий ИБ, выявление, анализ и реагирование на инциденты ИБ в ИТ- и ОТ-инфраструктуре Заказчика. Услуги оказываются в соответствии со статьёй 7-5 Закона Республики Казахстан «О кибербезопасности».

В течение 10 (десяти) рабочих дней с даты заключения договора Исполнитель разрабатывает и согласовывает с Заказчиком Регламент взаимодействия при оказании услуг ОЦИБ (выявление и реагирование на инциденты ИБ, контактные лица, каналы связи, сроки отчётности). В тот же срок стороны оформляют матрицу распределения ролей и ответственности в части устранения инцидентов ИБ.

Срок оказания услуг. С 01.01.2027 года по 31.12.2029 года.

2.2. Нормативно-правовая база

Настоящая техническая спецификация разработана в соответствии со следующими нормативными правовыми актами Республики Казахстан:

1. Закон Республики Казахстан от 24 ноября 2015 года № 418-V «О кибербезопасности» - в части требований к обеспечению ИБ объектов информатизации и КВОИКИ, деятельности ОЦИБ (ст. 7-5) и взаимодействия с НКЦИБ.
2. Кодекс Республики Казахстан от 9 января 2026 года № 255-VIII «Цифровой кодекс Республики Казахстан» – в части требований к кибербезопасности и аудиту цифровых объектов (ст. 97–99).
3. Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности» – в части обеспечения информационной безопасности как составляющей национальной безопасности.
4. Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» – в части обработки и хранения персональных данных на территории Республики Казахстан (ст. 12).
5. Закон Республики Казахстан от 13 июля 1999 года № 416-I «О противодействии терроризму» - в части защиты объектов, уязвимых в террористическом отношении, и их информационных систем (ст. 10-3).
6. Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».
7. Правила и критерии отнесения объектов информационно-коммуникационной инфраструктуры к КВОИКИ, утверждённые Правительством Республики Казахстан.
8. Правила обмена информацией, необходимой для обеспечения ИБ, между ОЦИБ и НКЦИБ, а также правила проведения мониторинга обеспечения ИБ КВОИКИ, утверждённые уполномоченным органом в сфере обеспечения ИБ.

Услуги также оказываются с учётом внутренних нормативных документов Заказчика в области ИБ, доведённых до Исполнителя. Реквизиты актов применяются в действующей на дату оказания услуг редакции.

2.3. Требования к услугам

В рамках мониторинга и реагирования на инциденты ИБ Исполнитель обязан обеспечить:

1. Круглосуточный (24×7×365) мониторинг событий ИБ, возникающих в периметре мониторинга Заказчика.
2. Разработку и выдачу Заказчику рекомендаций по устранению зарегистрированных инцидентов ИБ. При необходимости Исполнитель открывает обращения (тикеты) в службы технической поддержки производителей оборудования и ПО, на которых требуется выполнить действия для устранения инцидента. Обращения производятся от имени Заказчика.
3. Формирование совместно с Заказчиком в течение 45 (сорока пяти) календарных дней с даты заключения договора полного перечня источников событий и подключение их к ОЦИБ Исполнителя. Заказчик устанавливает агенты и коллекторы на собственных мощностях и передаёт «сырые» данные в инфраструктуру Исполнителя по Site-to-Site VPN. Лицензии на коллекторы «сырых» данных входят в обязательства Исполнителя.
4. Анализ объектов Заказчика (в том числе отнесённых к КВОИКИ) на предмет определения перечня журналов регистрации событий и настройку протоколирования событий ОС, СУБД, сетевого оборудования, прикладного ПО и СЗИ (при наличии функционала в источнике).
5. Мониторинг событий ИБ по трёхлинейной модели:
    - **первая линия** – фиксация инцидентов и выдача базовых рекомендаций, не требующих углублённых компетенций по конкретным техническим решениям; режим 24×7×365;
    - **вторая линия** – решение типовых инцидентов ИБ, углублённая аналитика с использованием специализированных инструментов, адаптация правил корреляции под изменения инфраструктуры Заказчика, устранение согласованных инцидентов согласно матрице ролей; режим 8×5;
    - **третья линия** – расследование инцидентов ИБ критичного уровня экспертами И сполнителя, рекомендации по устранению, ретроспективная аналитика, актуализация сведений о релевантных угрозах, атаках и способах их обнаружения и противодействия; режим 8×5.
6. Передачу информации о выявленных инцидентах ИБ в НКЦИБ по согласованию с Заказчиком: уведомление – в течение 15 минут с момента выявления, перечень данных об инциденте – в течение 24 часов, сведения о мерах по устранению уязвимостей – в течение 20 календарных дней с даты получения результатов обследования.
7. Получение информации об угрозах на рабочих станциях, серверах и в сети Заказчика в режиме реального времени.
8. Право Исполнителя запрашивать у Заказчика сведения об ИТ/ОТ-инфраструктуре и активах, необходимые для реализации сценариев выявления атак и минимизации ложных срабатываний. Запрос направляется по электронной почте уполномоченному лицу Заказчика с обоснованием; Заказчик отвечает в течение 5 рабочих дней (срок может быть скорректирован). Запрос может касаться, но не ограничиваться: списка DNS-серверов; IP-адресов сканеров безопасности; ресурсов, доступных из сети Интернет; «белых» IP-адресов Заказчика; учётных записей администраторов ИС; владельцев ИС и ресурсов; принадлежности IP-адресов пользователям или системам; технической документации по сетям АСУТП и ИТ-сегментов.

9. Взаимодействие при необходимости с производителями АСУТП, ИТ-систем и СЗИ Заказчика; обращения выполняются от имени Заказчика.
10. Оценку по запросу Заказчика организационно-технических мер ИБ в реализуемых Заказчиком ИТ-проектах и проектах автоматизации (в т.ч. модернизации АСУТП) на соответствие требуемому уровню безопасности, предложения по улучшению мер и участие в разработке дизайна внедряемых систем в части ИБ.
11. Хранение данных, получаемых от Заказчика (события, сетевые потоки), в течение срока действия договора исключительно на ресурсах, расположенных на территории Республики Казахстан.
12. Использование специализированной платформы класса SIEM, SOAR, UEBA и Threat Intelligence в качестве технологической основы оказания услуг. Платформа является инструментом Исполнителя, применяется исключительно для оказания услуг и не поставляется, не передаётся и не оформляется в собственность Заказчика. Платформа должна обеспечивать:

– централизованный сбор, обработку и хранение событий ИБ;

– выявление, корреляцию и классификацию инцидентов ИБ;

– автоматическую приоритизацию событий и инцидентов по уровню критичности;

– формирование аналитических заключений и рекомендаций по реагированию;

– автоматизацию процессов реагирования с использованием сценариев (плейбуков);

– ведение хронологии инцидентов и журнала действий.

1. Бесперебойную работу, обновление и сопровождение платформы, обработку событий в режиме, близком к реальному времени (24×7×365).
2. Предоставление Заказчику доступа к личному кабинету платформы с возможностью просмотра событий и инцидентов ИБ в режиме реального времени, доступа к результатам анализа и рекомендациям, просмотра истории инцидентов и действий по ним, формирования и выгрузки отчётности.
3. Анализ событий ИБ на предмет возможных угроз и инцидентов на основе встроенных механизмов регистрации и учёта событий безопасности ОС, СУБД, прикладного ПО, СЗИ, специализированных средств анализа защищённости, а также информации, полученной от НКЦИБ.
4. Уведомление владельца объекта КВОИКИ и НКЦИБ об инцидентах ИБ ответственным работником Исполнителя (или уполномоченным им работником) по электронной почте и (или) через платформу MISP.

2.4. Виды услуг ОЦИБ

Вид услуги	**Краткое описание**

Первая линия ОЦИБ (SOC)	Анализ событий ИБ в режиме 24×7. Проверка ложных срабатываний, первичная аналитика и выделение инцидентов ИБ на основе категорий и правил; рекомендации по реагированию на типовые инциденты; регистрация и актуализация сведений об инцидентах в системах ОЦИБ. Реагирование на инциденты, относящиеся к защите внешнего периметра. Ответы на письма и звонки, рассылка информационных сообщений об инцидентах и событиях ИБ
Вторая линия ОЦИБ (SOC)	Обработка инцидентов ИБ в режиме 8×5, рекомендации по реагированию, углублённый анализ инцидентов. Адаптация правил корреляции под изменения инфраструктуры Заказчика; добавление исключений в правила корреляции по требованию Заказчика
Третья линия ОЦИБ (SOC)	Поддержка реагирования на критичные инциденты ИБ, рекомендации по повышению защищённости инфраструктуры Заказчика по итогам расследований. Разработка правил корреляции, в т.ч. для сценариев атак на сегмент АСУТП
Дополнительная экспертиза	Расследование наиболее критичных инцидентов, сбор и исследование образов жёстких дисков (форензика), анализ вредоносного ПО, помощь в устранении последствий. Тестирование на проникновение 4 раза в год (внешний и внутренний периметр, модель Grey Box, на ежеквартальной основе) с последующим контролем устранения уязвимостей; методы контроля выбирает Испол нитель. Аудит исходного кода по запросу Заказчика – 1 раз в год, объём приложения не более 500 000 строк, правообладатель – Заказчик

Защита внешнего периметра	Мониторинг и реагирование на угрозы, направленные на ресурсы Заказчика, доступные из сети Интернет
Сканирование на наличие уязвимостей	Сканирование внутреннего и внешнего периметра, оборудования и узлов на наличие уязвимостей приложений и ОС 1 раз в квартал, а также по заявке Заказчика (не чаще 1 раза в месяц). Детальный отчёт по уязвимостям с рекомендациями – в течение 15 рабочих дней после завершения сканирования; консультирование по устранению уязвимостей
Анализ конфигураций сетевых устройств	Осуществление анализа на предмет соответствия конфигураций практикам и рекомендациям производителей сетевого оборудования в части информационной безопасности и выдача рекомендаций Заказчику
Фишинг-компания	Осуществление согласованной с Заказчиком фишинг-рассылки 1 раз в квартал, с предоставлением результатов и рекомендаций к действиям

Обследование ИБ и тестирование на проникновение. Перечень объектов обследования согласуется с Заказчиком. Обследование проводится в следующем порядке:

• внешний периметр – сканирование с применением ПО класса «сканер уязвимостей»; все обнаружения проверяются вручную квалифицированным специалистом Исполнителя для валидации уязвимостей; область сканирования – не менее 10 объектов (уникальные публичные URL);

• внутренний сегмент – внутренние URL сканируются с использованием VPN-соединения, внутренние информационные системы и сети – из периметра локальной сети Заказчика; сканер выполняет инвентаризацию обнаруженных хостов (карта ИТ-активов), которые затем проверяются на наличие уязвимостей;

• тестирование на проникновение выполняется сертифицированными специалистами; сценарии и методы согласуются с Заказчиком;

- по итогам представляется отчёт в соответствии с п. 2.11.

Аудит информационной безопасности (кибербезопасности). Исполнитель проводит аудит кибербезопасности цифровых объектов Заказчика в соответствии со статьёй 99 Цифрового кодекса Республики Казахстан и статьями 18 и 50 Закона Республики Казахстан «О кибербезопасности» на следующих условиях:

- Периодичность. Не реже одного раза в год (для критически важных цифровых объектов и объектов, обрабатывающих цифровые данные, содержащие охраняемую законом тайну, периодичность установлена законом). Внеплановый аудит проводится по запросу Заказчика один раз за период действия контракта, при условии предварительного письменного уведомления Исполнителя не менее чем за 30 календарных дней.

- Объекты аудита. Цифровые объекты Заказчика по согласованному перечню, включая критически важные цифровые объекты и АСУТП.

- Критерии оценки. Единые требования в сферах цифровизации и обеспечения кибербезопасности, профили защиты, нормативные правовые акты, указанные в п. 2.2, и внутренние нормативные документы Заказчика в области ИБ; при отсутствии казахстанских стандартов допускается применение ISO/IEC 27001, перед проведением аудита сторонами определяется и согласовывается конкретный объем аудита и применяемая в методике аудита нормативно-правовая база.

- Этапы. Сбор исходных данных; анализ организационно-распорядительной и технической документации; интервьюирование ответственных работников; техническая проверка (анализ конфигураций, сканирование уязвимостей); оценка соответствия требованиям; подготовка отчёта.

- Результаты. Отчёт об оценке соответствия, содержащий перечень выявленных несоответствий с указанием уровня критичности, рекомендации и план по их устранению; представление результатов аудита Заказчику. Отчёт передаётся в срок не позднее 30 рабочих дней с даты завершения аудита.

- Контроль устранения. Повторная проверка устранения выявленных несоответствий в срок 15 календарных дней с даты получения от Заказчика уведомления об устранении.

- Требования к исполнителю аудита. Наличие лицензии, требуемой законодательством для оказания услуг в сфере обеспечения кибербезопасности; независимость от проверяемых систем; специалисты с подтверждённой квалификацией (в том числе ISO/IEC 27001 Lead Auditor); обязательство по соблюдению конфиденциальности информации, полученной при проведении аудита.

• Взаимодействие с контролирующими органами. По запросу Заказчика Исполнитель предоставляет материалы аудита и консультационную поддержку при подготовке к проверкам уполномоченных органов.

Фишинг-кампания. Исполнитель проводит обучающую фишинг-кампанию для оценки устойчивости работников к атакам социальной инженерии, включающую разработку фишинговых сценариев (письма, ссылки, формы), рассылку по согласованному с Заказчиком списку работников, сбор и обработку результатов. По итогам представляется отчёт с аналитикой и рекомендациями, содержащий: ФИО или идентификатор работников, перешедших по ссылке; дату и время события; IP-адрес устройства; факт ввода данных (если применимо); уровень риска. Пароли и иные персональные данные, введённые работниками, не сохраняются, фиксируется только факт ввода. Заказчику предоставляется онлайн-панель или выгрузка для самостоятельного контроля результатов. Кампания проводится в контролируемой среде без угрозы для рабочих систем.

Задачи компьютерной криминалистики (форензики). При расследовании инцидентов Испол нитель совместно с работниками Заказчика, осуществляющими техническое обслуживание объекта, решает следующие задачи:

• установить способ реализации взлома;

• построить сценарий атаки и восстановить её хронологию;

• собрать оставшиеся следы атаки;

• разработать меры защиты от подобных и, по возможности, иных атак;

• уменьшить и устранить нанесённый ущерб.

2.5. Объём услуг и перечень источников событий

Объём услуг определяется количеством объектов мониторинга, указанным ниже как максимальное. Точный перечень источников уточняется Заказчиком по итогам первичного обследования в течение 45 календарных дней с даты заключения договора.

№	Объект мониторинга (класс источника событий)	Количество, не более

1	Серверы (физические и виртуальные, Windows / Linux, включая серверы СУБД и почтовые серверы)	10
2	Сетевые устройства (коммутаторы, маршрутизаторы, точки доступа)	30
3	Межсетевые экраны	2
4	Рабочие станции	200
5	Источники сегмента АСУТП (серверы SCADA, инженерные и операторские станции, средства мониторинга промышленной сети)	По итогам первичного обследования, в пределах п. 1–4

Требования к протоколированию событий. По итогам анализа объектов (п. 2.3) Исполнитель определяет и настраивает регистрацию следующих типов событий (при наличии функционала в источнике):

• ОС: авторизация и выход пользователей, успешные и неуспешные попытки входа; изменение системной конфигурации; создание, удаление, модификация учётных записей; использование привилегированных учётных записей; активация и дезактивация средств защиты (антивирус, система обнаружения вторжений, возможна реализация при опросе логов средств защиты, а не логов ОС) и средств ведения журнала; изменение или попытки изменения настроек защиты; подключение и отключение устройств ввода-вывода; неудавшиеся или отвергнутые действия пользователя, в том числе затрагивающие данные и ресурсы; запуск и остановка процессов;

• СУБД: контроль сессий (успешная и неуспешная авторизация, использование незарегистрированных учётных записей); все действия пользователей с административными привилегиями; все действия пользователей, имеющих право назначать привилегии другим пользователям БД;

• сетевое оборудование: запуск и остановка системы; изменение конфигурации; создание, удаление, модификация локальных учётных записей; использование

привилегированных учётных записей; подключение и отключение устройств ввода-вывода; неудавшиеся или отвергнутые действия пользователя; запуск, падение и остановка сетевых линков;

• прикладное ПО: авторизация пользователей (успешная и неуспешная); создание, копирование, перемещение, удаление, модификация учётных записей и конфигурационных файлов; неудавшиеся или отвергнутые действия; получение доступа к объектам доступа; действия пользователей с данными (доступ, изменение, удаление);

• СЗИ: создание, копирование, перемещение, удаление, модификация учётных записей и конфигурационных файлов; запуск и остановка службы; изменение системной конфигурации.

Для каждого протоколируемого события записываются как минимум: идентификатор пользователя, тип события, дата и время, результат (успешно или неуспешно), источник события, идентификатор или название данных, компонента или ресурса, на который повлияло событие. Журнал событий должен содержать поля: дата и время (ДД.ММ.ГГГГ, ЧЧ:ММ:СС); наименование источника события (сервис, служба); имя учётной записи или ID пользователя; IP-адрес клиента; время начала и окончания операции; описание события.

2.6. Регистрация инцидентов ИБ

При фиксации инцидента ИБ Исполнитель заводит карточку инцидента в своей учётной системе и направляет её Заказчику. Карточка содержит:

- заголовок и номер инцидента ИБ в учётной системе Исполнителя;
- время регистрации в формате UTC и приоритет инцидента;
- перечень затронутых хостов и активных на них учётных записей на момент инцидента (при доступности данных);
- источник(и) событий ИБ, на основании которых выявлен инцидент;
- выявленные индикаторы компрометации (хэш-сумма и имя файла, адрес C&C-сервера, ассоциированные доменные имена и др.);
- ссылки на прилагаемые файлы;
- рекомендации: первичные действия для предотвращения или минимизации последствий либо дополнительные сведения, необходимые от Заказчика для дальнейшего анализа.

При обнаружении инцидента силами Заказчика он уведомляет Исполнителя по электронной почте или иным каналом, указанным в Регламенте взаимодействия. Исполнитель к регистрирует инцидент и сообщает Заказчику его номер, время регистрации, краткое описание и рекомендации.

Обращения Заказчика. Помимо инцидентов, Заказчик может направлять Исполнителю обра щения следующих типов:

• запрос на изменение – изменение конфигурации услуги (добавление или удаление источника событий ИБ, адаптация сценария выявления); по мере необходимости;

• информационный запрос – консультационные вопросы по услуге и договору; по мере необходимости;

• подозрение на инцидент ИБ – обращение Заказчика о предполагаемом инциденте; изначально присваивается приоритет «малой срочности», Заказчик вправе его повысить; обработка ведётся по Таблице 2; количество обращений не ограничено.

2.7. Классификация инцидентов и стандарты обслуживания (SLA)

Таблица 1. Классификация инцидентов ИБ

Приоритет	Описание	Пример
Критический (экстренный)	Полная недоступность защищаемых ресурсов Заказчика более 15 минут, компрометация большого числа ресурсов с возможностью существенного ущерба, остановка или угроза нарушения технологического процесса, либо таргетированный характер атаки	Таргетированная атака с компрометацией учётной записи администратора домена; несанкционированный доступ к сегменту АСУТП
Срочный	Инцидент, не приводящий в данный момент к недоступности ресурсов, но с высокой вероятностью перерасти в инцидент более высокого приоритета; злонамеренная активность локализована и заблокирована превентивными СЗИ	Эксплуатация уязвимости браузера с попыткой заражения хоста, заблокированной антивирусной защитой

Малой срочности	Инцидент без ущерба для Заказчика; сбор информации о системе в рамках имеющихся прав доступа	Сбор информации о защищаемом периметре

Таблица 2. Стандарты обслуживания

Этап	Приоритет	Время реакции Испол нителя	Режим
Обнаружение и регистрация инцидента	Критический, срочный	Отклик – до 15 минут	24×7×365
Обнаружение и регистрация инцидента	Малой срочности	Отклик – до 60 минут	24×7×365
Уведомление Заказчика (группа в мессенджере и e-mail)	Критический	До 30 минут с момента регистрации	24×7×365
Уведомление Заказчика	Срочный	До 45 минут с момента регистрации	24×7×365
Уведомление Заказчика	Малой срочности	До 90 минут с момента регистрации	24×7×365
Рекомендации и устранение инцидента	Критический	Отклик – 30 минут; решение, не требующее замены оборудования или значительной реконфигурации, – 3 часа	24×7×365

Рекомендации и устранение инцидента	Срочный	Отклик – 4 часа; решение, не требующее обновления (замены) ПО или оборудования, – 6 часов	24×7×365
Рекомендации и устранение инцидента	Малой срочности	Отклик – 8 часов; решение, не требующее обновления (замены) ПО или оборудования, – 12 часов	24×7×365

Срок фактического решения инцидента ИБ увеличивается, если для его устранения требуется обращение в техническую поддержку производителя ПО или оборудования третьих лиц и (или) дополнительная информация от Заказчика. На это время инцидент переводится в статус «Ожидание». Заказчик указывает контактные номера 3 (трёх) специалистов для оперативного ответа на запросы Исполнителя.

При критическом инциденте Исполнитель по запросу Заказчика направляет ответственного специалиста на объект Заказчика в течение 24 часов. Реагирование включает: подтверждение или опровержение инцидента; его классификацию и уточнение критичности; сбор и сохранение доказательств; минимизацию последствий; консультирование персонала; переоценку рисков и актуализацию регламентов ИБ.

2.8. Разграничение зон ответственности

№	Параметр	Заказчик	Исполнитель
1	Мониторинг и анализ событий ИБ 24×7, проверка ложных срабатываний, первичная аналитика, регистрация инцидентов		+
	Мониторинг работоспособности и		

2	корректное функционирование подсистемы управления событиями ИБ (SIEM, коллекторы)		+
3	Установка агентов и коллекторов на источниках, направление потоков событий в коллекторы	+	+
4	Предоставление вычислительных мощностей для коллекторов по рекомендациям Исполнителя	+	
5	Работоспособность защищённого канала (Site-to-Site VPN) между площадками Заказчика и Исполнителя	+	+
6	Актуальный перечень оборудования и ИС периметра мониторинга, оперативное информирование об изменениях (новые устройства, IP-адресация, внешние подключения)	+	
	Выдача рекомендаций по реагированию и		

7	расследование инцидентов		+
8	Локализация инцидентов, устранение последствий и восстановление штатного режима по рекомендациям Исполнителя (в т.ч. в сегменте АСУТП)	+	
9	Применение рекомендаций для исключения повторных инцидентов	+	
10	Хранение данных Заказчика (события, сетевые потоки) на территории РК в период действия договора		+

Детальное распределение ролей фиксируется в матрице, согласуемой сторонами в соответствии с п. 2.1.

2.9. Плановые и аварийные работы

Плановые работы. Исполнитель может проводить плановое обслуживание, модернизацию или усовершенствование подсистем, на базе которых оказывается услуга, с 19:00 до 08:00 (время г. Астана) или в согласованный с Заказчиком период. На время работ Исполнитель пе реключает Заказчика на резервную площадку ОЦИБ. Исполнитель уведомляет Заказчика не менее чем за 7 (семь) календарных дней, кроме работ по запросу Заказчика или по требованию государственных органов.

Заказчик уведомляет Исполнителя о плановых работах на своём оборудовании, способных вызвать недоступность защищаемых ресурсов (в т.ч. плановых остановах технологических

установок), не менее чем за 5 (пять) дней. В уведомлении указываются дата, время, продолжительность и контактное лицо. О переносе сроков Заказчик сообщает не позднее чем за 1 (одни) сутки.

Аварийные работы проводятся при периодических прерываниях услуги или существенном ухудшении её качества. Каждая сторона уведомляет другую о таких работах на своём оборудовании в течение 24 (двадцати четырёх) часов до их начала, с указанием сроков и контактного лица.

2.10. Требования к Исполнителю

Обучение персонала Заказчика. Исполнитель проводит обучение не менее 2 (двух) ключевых специалистов ИБ Заказчика по реагированию на инциденты ИБ: на каждого по 1 авторизованному курсу в области расследования или анализа киберинцидентов. Точное наименование курсов обучение согласуются в момент выполнения работ.

Обучение работников Заказчика по кибербезопасности. Исполнитель проводит обучение работников Заказчика по вопросам кибербезопасности: защита информации, цифровая гигиена, защита персональных данных, минимизация рисков при работе с цифровыми технологиями. Перечень тем и количество обучаемых работников: две группы не более 25 человек; обязательная тема – «Введение в цифровую гигиену и кибербезопасность». Обучение проводится очно и (или) дистанционно (по видеосвязи) на казахском и русском языках, по выбору Заказчика. Занятия включают презентационные материалы, практические примеры и тестирование. Количество занятий, продолжительность и график проведения согласовываются с Заказчиком.

По итогам обучения Исполнитель передаёт Заказчику учебные материалы и ведомость результатов тестирования.

2.11. Отчётность, гарантия и качество

Не позднее 5 числа месяца, следующего за отчётным, Исполнитель представляет ежемесячный аналитический отчёт с текстовой, табличной и графической информацией:

- статистика запросов и инцидентов ИБ за отчётный период, выполнение показателей SLA;
- анализ состояния инфраструктуры ИБ Заказчика (ИТ и АСУТП);
- проблемные вопросы и рекомендации по их решению;
- актуальные контакты специалистов, ответственных за оказание услуги.

По итогам тестирования на проникновение представляется полный отчёт об уязвимостях с оценкой рисков, рекомендациями по устранению и снижению рисков атак извне и изнутри сети. Общая продолжительность тестирования – не более 45 рабочих дней, график согласуется с Заказчиком.

Гарантийные обязательства. Гарантия на оказываемые услуги – на весь срок действия договора. В течение гарантийного срока сервисное обслуживание обеспечивается специалистами, авторизованными производителями используемых решений.

Требования к качеству. Услуги оказываются качественно, в соответствии с настоящей технической спецификацией и действующими в РК нормами и правилами, регламентирующими данный вид услуг.

Техническая документация по ИБ. Исполнитель разрабатывает и передаёт Заказчику комплект технической документации по ИБ в виде четырёхуровневой системы документов в соответствии с п. 31 Единых требований в области ИКТ и обеспечения ИБ (Постановление Правительства РК от 20 декабря 2016 года № 832):

- первый уровень – политика информационной безопасности;

- второй уровень – документы, детализирующие политику ИБ (методика оценки рисков ИБ, правила идентификации, классификации и маркировки активов, правила аутентификации и разграничения доступа, правила антивирусного контроля и иные правила, предусмотренные Едиными требованиями);

- третий уровень – документы, описывающие процессы и процедуры (каталог угроз (рисков) ИБ, план обработки угроз (рисков), план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, руководства и инструкции по реагированию на инциденты ИБ);

- четвёртый уровень – рабочие формы, журналы и протоколы (журнал регистрации инцидентов ИБ и учёта внештатных ситуаций, журнал учёта резервных копий, отчёты об оценке уязвимостей и иные документы).

Документация разрабатывается на казахском и русском языках, согласовывается с Заказчиком и передаётся на утверждение; актуализируется Исполнителем не реже одного раза в два года, а также при изменении требований законодательства, архитектуры или состава объектов защиты.

2.12. Заключительные требования

Услуги оказываются в соответствии со статьёй 7-5 Закона РК «О кибербезопасности», иными актами, перечисленными в п. 2.2, требованиями к использованию ЕШДИ и внутренними нормативными документами Заказчика. При отсутствии казахстанских стандартов допускается применение ISO/IEC 27001 и лучших международных практик в порядке, установленном законодательством РК.

Данные Заказчика хранятся на ресурсах, расположенных на территории РК (ст. 12 Закона РК «О персональных данных и их защите», пп. 5) п. 1 ст. 10-3 Закона РК «О

противодействии терроризму», Постановление Правительства РК № 832 от 20.12.2016). Взаимодействие ОЦИБ с НКЦИБ осуществляется в соответствии с Законом РК «Об информатизации».

Исполнитель несёт ответственность за своевременное реагирование на инциденты ИБ в соответствии с условиями настоящей технической спецификации и соблюдает конфиденциальность сведений, полученных при оказании услуг.

3. Нормативно-технические документы

№ п/п	Наименование
1	Закон Республики Казахстан от 24 ноября 2015 года № 418-V «О кибербезопасности»
2	Кодекс Республики Казахстан от 9 января 2026 года № 255-VIII «Цифровой кодекс Республики Казахстан»
3	Закон Республики Казахстан от 6 января 2012 года № 527-IV «О национальной безопасности»
4	Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите»
5	Закон Республики Казахстан от 13 июля 1999 года № 416-I «О противодействии терроризму»
6	Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»
7	Правила и критерии отнесения объектов информационно-коммуникационной инфраструктуры к КВОИКИ, утверждённые Правительством Республики Казахстан
8	Правила обмена информацией, необходимой для обеспечения ИБ, между ОЦИБ и НКЦИБ, а также правила проведения мониторинга обеспечения ИБ КВОИКИ, утверждённые уполномоченным органом в сфере обеспечения ИБ

Подписал Тлеуберлиев Ерасыл Ержанулы

Дата подписания 11.11.2026