ТЕХНИКАЛЫҚ СИПАТТАМА

1271384 сатып алу бойынша
Төмендету бойынша ашық тендер тәсілімен

Лот № 1 (31-2 У, 4583333) Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер

Тапсырыс беруші: "МұнайТас "Солтүстік-Батыс құбыр компаниясы" жауапкершілігі шектеулі серіктестігі
Ұйымдастырушы: "МұнайТас "Солтүстік-Батыс құбыр компаниясы" жауапкершілігі шектеулі серіктестігі

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	31-2 У
Атауы және қысқаша сипаттамасы	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер, Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызметтер
Қосымша сипаттама	Ақпараттық қауіпсіздік инциденттерінің мониторингі мен анықталуын қамтамасыз ету және оларға ден қою
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Алматы қ., Бостандық ауданы, ул. Тимирязева, 26/29
Жеткізу шарттары	-
Жеткізу мерзімі	01.2027 бастап 12.2027 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

ҚОЛДАНЫЛАТЫН ҚЫСҚАРТУЛАР МЕН ТЕРМИНДЕР ТІЗІМІ

АҚ	Ақпараттық қауіпсіздік
ККЕО	киберқауіпсіздікті қамтамасыз ету орталығы – шетелдік заңды және жеке тұлғалардың қатысуынсыз Қазақстан Республикасының резиденті болып табылатын, цифрлық объектілерді қорғау жөніндегі қызметті жүзеге асыратын заңды тұлға немесе заңды тұлғаның құрылымдық бөлімшесі
АҚ инфрақұрылымы	АҚ сервистерін қамтамасыз ету үшін қолданылатын бағдарламалық және аппараттық құралдар, электрондық түрде ұсынылған мәліметтер

АҚ инциденті	Ақпараттық-коммуникациялық инфрақұрылымның немесе оның жекелеген нысандарының жұмысында туындайтын ақаулар, олар жұмысқа қауіп төндіреді немесе электрондық ақпараттық ресурстарға заңсыз қол жеткізу, көшірме жасау, тарату, өзгерту, жою немесе бұғаттау жағдайларын туғызады
АЖ	Ақпараттық жүйе – ақпараттық-коммуникациялық технологиялардың, техникалық құжаттаманың, қызмет көрсетуші персоналдың реттелген жиынтығы, ол ақпараттық өзара әрекеттесу арқылы белгілі бір функционалдық міндеттерді орындауға арналған
АТ	Ақпараттық технологиялар
ҰКҰО	Ұлттық киберқауіпсіздікті үйлестіру орталығы
КМ	МСН киберқауіпсіздік мониторингі
IP-мекен-жайы	Интернеттегі немесе жергілікті желідегі құрылғыны анықтайтын бірегей мекен-жай
SIEM	(Security information and event management) ақпараттық қауіпсіздік оқиғаларын басқару жүйесі
VPN	(Virtual Private Network) – криптография құралдары (шифрлау, аутентификация, ашық кілттер инфрақұрылымы, логикалық желі арқылы берілетін хабарламалардың қайталануынан және өзгеруінен қорғау құралдары) бойынша басқа желінің үстінен бір немесе бірнеше желілік қосылыстарды қамтамасыз етуге мүмкіндік беретін «виртуалды жеке желі»

ОЖ	Операциялық жүйе
МСН	маңызды сандық Нысандар
«МТҚ» АҚ	«Мемлекеттік техникалық қызмет» АҚ
ИКБШ	Интернетке кірудің бірыңғай шлюзі
MISP	Threat Intelligence АҚЖО платформасы

1. **Негізгі ережелер**

1.1. Жедел ден қоюды және ақпараттық қауіпсіздік инциденттерін (бұдан әрі – АҚ) пысықтауды қамтамасыз ету мақсатында Орындаушы Тапсырыс берушінің аумағында сұраныс бойынша техникалық маманның болуын қамтамасыз етуге міндетті. Оқыс оқиға (жоғары сыни) анықталған жағдайда, ОАО қызметкерлері 60 минут ішінде Тапсырыс берушінің аумағына физикалық түрде келеді (қашықтықтан алып жүруге тыйым салынады) және АҚ инциденттерін толық тергеумен және жоюмен айналысады және т. б.

1.2. ККЕО қызметінің өзара әрекеттесуі Тапсырыс берушімен, құқық қорғау және арнайы органдармен, ақпараттық жүйені әзірлеушімен жүзеге асырылады.

1. **ҚЫЗМЕТТЕРГЕ КІРЕТІН СЕРВИСТЕРДІҢ ТІЗІМІ**

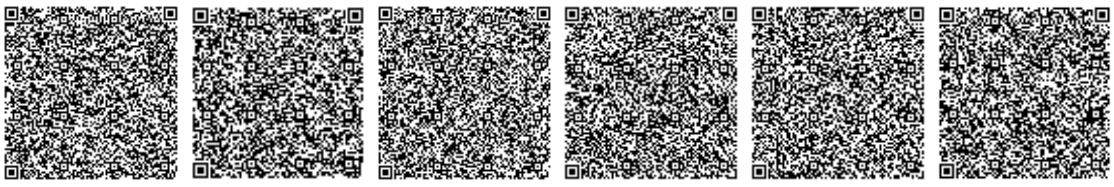
№	Сипаттама	Арнайы шарттар	
1	Ақпараттық қауіпсіздік жедел орталық (ККЕО) қызметін ұсыну	Тәулік бойы	

Міндетті түрде орындалатын сервистер				
№	**Сипаттама**	**Параметрлер**	**Орындаушының жауапты қызметкерлері**	
1	**Ішкі инфрақұрылымға ену тесттерін жүргізу (тоқсанына 1 рет) ****	Енуге тестілеу бойынша сертификатталған қызметкерлердің Тапсырыс берушінің инфрақұрылымына (Тапсырыс берушінің жергілікті желісінің периметрінен) енуіне тесттер өткізу. Тестілеуді өткізу сценарийлері мен қолданылатын әдістер Тапсырыс берушімен келісіледі. Қорытындысы бойынша өнім беруші есеп береді (қашықтан алып жүруге тыйым салынады).	Екінші желі талдаушылары	

2	**Сыртқы инфрақұрылымға ену тесттерін жүргізу (тоқсанына 1 рет) ****	Тапсырыс берушінің интернет желісінен тест өткізу. Тест жүргізу сценарийлері мен әдістері тапсырыс берушімен келісім бойынша жүзеге асырылады. Нәтижесінде Орындаушы есеп ұсынады.	Екінші желі талдаушылары	
		Әлеуметтік инженерия (психологиялық манипуляция жасау арқылы әрекеттерге итермелеу немесе құпия ақпаратты алу)	Екінші желі талдаушылары	
		60 минут ішінде Тапсырыс берушінің аумағында физикалық түрде болады (қашықтықтан алып жүруге тыйым салынады) және АҚ инциденттерін толық тергеумен және жоюмен айналысады.		

		Шарттың қолданылу кезеңіне Тапсырыс берушінің өтінімдер саны шектеусіз. Компьютерлік криминалистика саласындағы қызметтерге мыналар жатады: 1. Әртүрлі тасымалдаушылардан деректерді қалпына келтіру, соның ішінде зақымдалған немесе шифрланған құрылғылардан;			

		2. Компьютерлік технологияларды тергеу, соның ішінде зиянды бағдарламаларды, желілік шабуылдарды және бұзушылардың әрекеттерін талдау; 3. ақпараттандыру объектісін сараптау, атап айтқанда: 3.1. Инциденттің ауқымы мен ықтимал салдарын бағалау, болашақта осындай инциденттерді болдырмау бойынша ұсыныстар әзірлеу; 3.2. Уақыт белгілері мен жүйелік артефактілерді талдау арқылы			



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

			оқиғалардың хронологиясын қалпына келтіру; 3.3. Инцидентті ң көзін анықтау (ішкі немесе сыртқы бұзушы) және заңды маңызды дәлелдерді жинау; 3.4. Жасырын немесе жойылған деректерді іздеу үшін файлдық жүйелерді зерттеу; 3.5. Кілт сөздер бойынша іздеу, бұл шектеулі бастапқы деректер болған кезде де қажетті ақпаратты анықтауға мүмкіндік береді;			
3	**Инциденттерді талдау (компьютерлік криминалистика) ***			2, 3 желі талдаушылары		

		4. OSINT барлауын жүргізу — ашық көздерден ақпарат іздеу, жинау және талдау; 5. Мобильді құрылғыларды талдау, соның ішінде құлыпты ашу, жойылған деректерді алу және орнатылған қолданбаларды талдау; 6. Желілік журналдарды және белсенділікті талдау, кіріп кетулерді анықтау және олардың алдын алу;		

		7. Қылмыстық және әкімшілік істерді сүйемелдеу, құқық қорғау органдары үшін сараптамалық қорытындылар мен кеңестер беру; 8. Арнайы сараптамалар жүргізу, соның ішінде фишингтік шабуылдарды, деректердің тарап кетуін және тіркелгілердің бұзылуын талдау;			

		9. Тергеу іс-шараларына қатысу үшін маманды оқиға орнына шақыру, деректерді бекіту және хаттама жасау, бұл істің сәтті ашылу ықтималдығын арттырады.		
		Бір объектіні зерттеу мыналарды қамтиды:		

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

4	**Зиянды бағдарламалық жасақтаманы талдау бойынша кеңейтілген сараптама**	1. зиянды бағдарламаларды бастапқы талдау; 2. компьютерлік технологиялар құралдарын зиянды бағдарламаны анықтау тұрғысынан зерттеу бағдарламалық қамтамасыз ету; 3. объектіге динамикалық және статикалық талдау жүргізу; 4. жұқтыру алгоритмін талдау, жұқтыру индикаторларын анықтау, жою бойынша ұсынымдар беру; 5. талдамалық есепті құрастыру.	2, 3 желі талдаушылары	

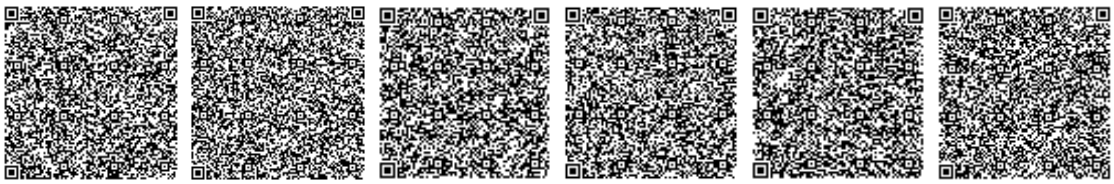
5	**Сыни инциденттерді тергеу бойынша кеңейтілген сараптама**	Сыни инциденттерді тергеу бойынша сараптама (Тапсырыс берушінің алаңында ақпараттық қауіпсіздік инциденттеріне жауап беру іс-шараларын жүргізу, қатқыл дисклердің кескіндерін жинау және зерттеу, зиянды бағдарламаларды талдау, инциденттердің салдарын жоюға көмек көрсету).	1, 2, 3 желі талдаушылары	

6	**Периметрді осалдықтар бойынша сканерлеу (сыртқы)**	300 IP-мекенжайдан аспайды. Интернет желісі арқылы Тапсырыс берушінің периметріндегі тораптар мен ақпараттық жүйелерді қосымшалар мен операциялық жүйелердегі осалдықтарды анықтау үшін құралдық сканерлеу жүргізу, осалдықтар туралы егжей-тегжейлі есеп пен оларды жою бойынша ұсыныстарды ұсыну.	2 желі талдаушылары	

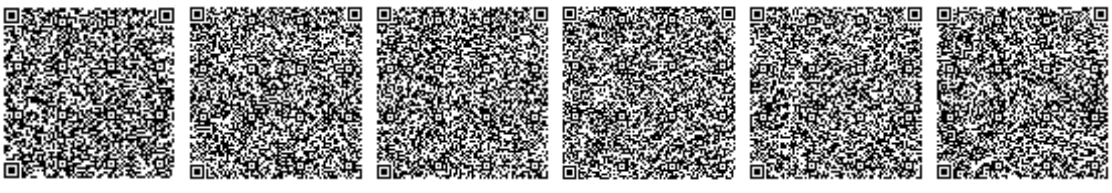
7	**Мониторинг аймағын осалдықтардың бар-жоғына сканерлеу (бір реттік жұмыстар)**	300 IP-мекенжайдан аспайды. Мониторинг аймағына кіретін тораптар мен ақпараттық жүйелерді қосымшалар мен операциялық жүйелердегі осалдықтарды анықтау үшін құралдық сканерлеу жүргізу, осалдықтар туралы егжей-тегжейлі есеп пен оларды жою бойынша ұсыныстарды ұсыну.	2 желі талдаушылары	
8	**Ақпараттық қауіпсіздік жағдайына кешенді техникалық тексеру жүргізу.**	• Периметрді осалдықтар бойынша сканерлеу (сыртқы); • Сыртқы ену тестілеуі; • Ішкі ену тестілеуі; • Әлеуметтік инженерия; • WEB-қосымшалардың қорғалуын талдау.	2, 3 желі талдаушылары	

9	**Мақсатты кибершабуылдарды имитациялау (Red Teaming).**	Ақпараттық жүйелердің қорғаныс деңгейін арттыру бойынша талдау жүргізу және Тапсырыс берушіге ұсыныстар беру арқылы мақсатты кибершабуылдарды имитациялау. Ену тестілеуінен айырмашылығы, бұл процесте Орындаушының мақсаты – белгілі бір уақыт ішінде максималды осалдықтарды анықтау емес, Тапсырыс берушіге бағытталған шабуылдарды имитациялау арқылы олардың шабуылдарды анықтау және алдын алу қабілеттерін бағалау.	2 желі талдаушылары	

		Қосымшаның күрделілігіне және қорғаныс деңгейін талдау әдісіне (қара жәшік/сұр жәшік /ақ жәшік) байланысты (талдаудан кейін 3 ай ішінде осалдықтарды жоюды бір рет тексеру кіреді). Мобильді немесе WEB-қосымшаның осалдықтарын анықтау үшін мамандандырылған бағдарламалық жасақтама қолданылады, сондай-ақ тиісті біліктілігі бар сарапшылар қолмен талдау жүргізеді.			
10	**Қосымшаларды қорғаныс деңгейін талдау**		2 желі талдаушылары		



		Қызмет түрлеріне байланысты (қара жәшік, сұр жәшік немесе ақ жәшік), талдау қосымша туралы техникалық ақпаратсыз немесе оған қолжетімділіксіз жүргізіледі (қара жәшік), аналитикке қосымшаға қолданушылардың қолжетімділіктеріне ұқсас қолжетімділік беріледі (сұр жәшік), аналитик қосымшаның бастапқы кодын қолдана отырып қорғаныс деңгейін талдайды (ақ жәшік).		
11	**Шабуылдарды анықтаудың бейстандарт сценарийін әзірлеу**	Тапсырыс берушінің өтініші бойынша	2, 3 желі талдаушылары	



		Ақпараттық қауіпсіздік деңгейін арттыру және дайындықты жақсарту мақсатында, Тапсырыс берушінің өтініші бойынша Орындаушы Тапсырыс берушінің қызметкерлеріне ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша оқыту өткізуі керек. Оқыту білім беру орталықтарына арналған әзірленген және бекітілген оқу бағдарламасы бойынша жүргізілуі тиіс. Оқыту тест тапсырмаларымен бекітілуі және тестілеу нәтижесін беруі қажет. Оқу барысында тарату материалдары мен әдістемелік құралдар қолданылуы тиіс.		

12	**Тапсырыс берушінің қызметкерлерін оқыту талаптары**	Орындаушы келесі тақырыптар бойынша оқыту жүргізуі тиіс: 1) ақпараттық қауіпсіздік және ақпаратты қорғау. 2) ақпаратты қорғау әдістері мен құралдары. 3) Цифрлық гигиена және киберқауіпсіздік негіздері. 4) Мәліметтер базасының негіздері. 5) Компьютерлік желілердің негіздері. 6) Компьютерлік криминалистика негіздері. Оқыту қызметтерін ұсынушы оқу аяқталған күннен бастап бір жыл ішінде оқушыларға консультациялық қолдау көрсетуге міндетті. *Киберқауіпсіздік бойынша онлайн-оқыту платформасы.*	2, 3 желі талдаушылары		

		Орындаушы киберқауіпсіздікке арналған платформаға қолжетімділікті қамтамасыз етуі тиіс. Платформада киберқауіпсіздік бойынша базалық курстар жиынтығы және оларды аяқтағаннан кейін тестілеу қарастырылуы қажет. Сондай-ақ, платформада оқыту нәтижелерін, тестілеуді бақылау панелі және ақпараттық ағымдар туралы есеп болуы тиіс.		

13	**Фишинг-кампания жүргізу**	Орындаушы әлеуметтік инженерия шабуылдарын еліктейтін оқыту мақсатындағы фишинг-кампанияны жүргізуі тиіс. Сілтемеге өткен қызметкерлерді IP-мекенжайы, уақыты және басқа деректермен бірге сәйкестендіру міндетті. Кампания аяқталғаннан кейін талдауы мен ұсынымдары бар есеп беріледі. Тапсырыс берушіге нәтижелерді тексеру мүмкіндігі ұсынылуы тиіс.	2, 3 желі талдаушылары	

14	**DDoS шабуылдарынан қорғау қызметі**	Орындаушы желіге кірмей тұрып трафикті сүзгіден өткізу арқылы провайдер деңгейінде DoS/DDoS шабуылдарынан автоматты түрде қорғауды қамтамасыз етуі тиіс. Шабуылдар туралы (көзі, көлемі, жылдамдығы) есептері бар жеке кабинет және шабуыл анықталған жағдайда e-mail немесе басқа арна арқылы жедел хабарлама жіберу мүмкіндігі міндетті.	1, 2, 3 желі талдаушылары	
15	Purple Team Exercise — жылына кемінде 1 рет.	Орындаушы инц иденттерді анықтау және оларға әрекет ету процестерін тексеру мен жетілдіру жұмыстарын жүргізуі тиіс. Бұл жұмыстар кемінде жылына бір рет өткізіліп, нәтижелері құжат түрінде рәсімделеді..	1, 2, 3 желі талдаушылары	

** соның ішінде ақпараттық қауіпсіздік инциденттерінің пайда болу көздері мен себептерін анықтау, сондай-ақ олардың салдарын бағалауды* ККЕО *қызметкері ақпараттандыру объектісіне техникалық қызмет көрсететін қызметкерлермен немесе* МСН-*мен бірлесіп жүзеге асырады.*

Компьютерлік криминалистика бойынша жұмыстарды жүргізу аясында келесі міндеттер қойылады:

- *бұзудың жүзеге асырылу әдісін анықтау;*
- *шабуыл сценарийін құрастыру;*
- *шабуылдың хронологиясын қалпына келтіру;*
- *шабуылдан қалған іздерді жинау;*
- *осындай шабуылдың алдын алуға және мүмкіндігінше басқа шабуылдардан қорғауға қажетті қорғаныс шараларын әзірлеу, ақпараттық қауіпсіздікті қамтамасыз ету процесін жетілдіру;*
- *келтірілген шығынды азайту және қалпына келтіру.*

*** Сыртқы желі сегментіне ішінара немесе шамамен тақырыптық ақпаратты пайдаланып ену тестілеуі (Grey Box):*

- *кАҚершабуылдарды модельдеу арқылы инфрақұрылымның қауіпсіздігін сыртқы пайдаланушы (қызметкер емес) тұрғысынан бағалау, оның ұйым қызметкерінің есептік жазбасына қол жеткізуге тырысуын ескеру;*
- *кАҚершабуылдарды модельдеу арқылы ұйым қызметкері ретінде әрекет етіп, артықшылықтарды арттыруға, сервер жағына қол жеткізуге немесе ақпараттық қауіпсіздік құралдарының басқа әлсіз тұстарын анықтауға тырысып инфрақұрылым қауіпсіздігін қолмен бағалау.*

Нәтижелер:

1. *анықталған осалдықтар туралы толық есеп, соның ішінде тәуекел мен маңыздылық сипаттамасы;*
2. *оларды жою және қауіпсіздік деңгейін арттыру бойынша ұсыныстар есебі;*
3. *жалпы желілер мен ішкі желілер тарапынан шабуылдар қаупін азайту бойынша ұсыныстар;*

АЖ аудитін (пентест) жүргізу кестесі қызмет көрсету шартының қолданылу мерзімінде әлеуетті Ор ындаушымен қосымша келісіледі. АЖ аудитінің жалпы ұзақтығы 45 жұмыс күнінен аспауы тиіс.

Ену тестілеуі үшін келесі стандарттар қолданылуы тиіс:

- *PTES (Penetration Testing Execution Standard);*
- *OWASP Top 10 (OWASP Testing Guide);*
- *ISECOM OSSTMM;*
- *NIST SP 800-15.*

Жұмыстар тестіленетін жүйе әкімшілері мен пайдаланушыларын хабардар ете отырып жүргізіледі. Тестілеу барысында құрал-жабдықтар мен қолмен қауіпсіздік талдау әдістері де қолданылады.

2. Қызметке қойылатын талаптар:

2.1. Ақпараттық қауіпсіздік инциденттерін мониторингтеу және әрекет ету шеңберінде Орындаушы қамтамасыз етуі тиіс:

2.1.1. МСН объектісін ақпараттық қауіпсіздік оқиғаларын басқару жүйесіне (ҰҚҰО) беру үшін қажетті оқиғаларды тіркеу журналдары тізімін анықтау мақсатында талдау;

2.1.2. МСН объектісінің оқиғаларды тіркеу журналдарын жинау жүйесіне және қажет болған жағдайда, МСН объектісінің меншік иесі немесе иесіне тиесілі басқа да ақпараттық-коммуникациялық инфрақұрылым объектілеріне ақпараттық қауіпсіздік оқиғаларын басқару жүйесі агенттерін орнату;

2.1.3. МСН объектісінің және оған қатысты ақпаратты қорғау құралдарының оқиғаларды тіркеу журналдарын ақпараттық қауіпсіздік оқиғаларын басқару жүйесінде (ҰҚҰО) жинау, өңдеу және талдау арқылы ақпараттық қауіпсіздік оқиғалары мен инциденттерін анықтау;

2.1.4. МСН объектісінде анықталған ақпараттық қауіпсіздік оқиғаларын немесе инциденттерін бастапқы талдау;

2.1.5. қорғаныс және аэроғарыш өнеркәсібі министрінің 2018 жылғы 28 наурыздағы №52 /НҚ "цифрлық үкімет және аса маңызды цифрлық объектілер" цифрлық объектілерінің киберқауіпсіздігін қамтамасыз ету мониторингін жүргізу қағидаларын бекіту туралы" бұйрығына (бұдан әрі – мониторинг қағидалары)2-қосымшаға сәйкес АҚ инциденті туралы деректер тізбесін ұсына отырып, МСН объектісінің АҚ қамтамасыз етуіне жауапты тұлғаларды хабардар ету. АҚ оқиғасы немесе ақ оқиғасы анықталған сәттен бастап 30 минут ішінде, ҚР ҰҚК-24 сағат ішінде;

2.1.6. МСН объектісінің меншік иесі немесе иесіне ақпараттық қауіпсіздік инцидентінің таралуын тоқтату бойынша бастапқы ұсынымдар беру;

2.1.7. МСН объектілерін осалдықтардың бар-жоғына тексеру (бұдан әрі – осалдыққа тексеру);

2.1.8. Осалдықтарға тексеру нәтижелері мен осалдықтарды жою бойынша ұсынымдарды МСН объектілерінің меншік иелеріне немесе иелеріне жұмыстарды аяқтағаннан кейін 10 жұмыс күні ішінде ұсыну;

2.1.9. Осалдықтарды жою мәселелері бойынша МСН объектілерінің меншік иелеріне немесе иелеріне кеңес беру;

2.1.10. МСН объектісін ақпараттық қауіпсіздік бойынша техникалық құжаттама талаптарының орындалуы тұрғысынан тексеру (бұдан әрі – ТҚ бойынша АҚ), МСН объектісінің ТҚ бойынша талаптарын орындау нәтижелері мен анықталған бұзушылықтарды жою бойынша ұсынымдарды тексеру күнінен бастап 10 жұмыс күні ішінде ұсыну;

2.1.11. МСН объектісінің және оған қатысты ақпаратты қорғау құралдарының оқиғаларын журналға енгізуді ұйымдастыру, оқиғаларды тіркеу журналдарының форматтары мен типтеріне сәйкес;

2.1.12. МСН объектісі жұмыс істейтін телекоммуникациялық желі аясында оқиғаларды тіркеу журналдарын жинау жүйесін ұйымдастыру;

2.1.13. МСН объектісінің және оған қатысты ақпаратты қорғау құралдарының оқиғаларды тіркеу журналдарын МСН объектісінің оқиғаларды тіркеу журналдарын жинау жүйесіне беруін ұйымдастыру;

2.1.14. МСН объектісінің оқиғаларды журналға енгізу бойынша жоспарланған өзгерістер туралы ҰКҰО-ті өзгерістер енгізу күнінен 5 жұмыс күні бұрын хабардар ету. Хабарламаға өзгертілетін оқиғаларды тіркеу журналдарының үлгілері мен олардың сипаттамасы қоса беріледі;

2.1.15. МСН объектісінің оқиғаларды тіркеу журналдарын МСН объектісінің оқиғаларды тіркеу журналдарын жинау жүйесінен ҰКҰО ақпараттық қауіпсіздік оқиғаларын басқару жүйесіне беру үшін ҰКҰО-пен келісілген шарттарды қамтамасыз ету;

2.1.16. МСН объектісіндегі ақпараттық қауіпсіздік инцидентін өздігінен анықтаған кезде ҰКҰО-ке 15 минут ішінде хабарлау;

2.1.17. Ақпараттық қауіпсіздік инциденті анықталған сәттен бастап 24 сағат ішінде ҰКҰО-ке деректер тізімін ұсыну;

2.1.18. Осалдықтарды тексеру нәтижелерін алған күннен бастап 20 күнтізбелік күн ішінде МСН объектісінің осалдықтарын жою бойынша қабылданған шаралар туралы ақпаратты ҰКҰО-ке жіберу;

2.1.19. ҰКҰО объектісінің осалдығы өз бетінше анықталған жағдайда, ҰКҰО объектісінің осалдығы анықталған кезден бастап 24 сағат ішінде мониторинг қағидаларының 5-қосымшасына сәйкес нысан бойынша ЭҮ АИ осалдығы туралы деректер тізбесін ҰКҰО-ға ұсыну;

2.1.20. МСН объектісінің осалдығын жою мүмкін болмаған жағдайда, осалдыққа белгілі бір санат (өндірістік қажеттілік, нөлдік күн осалдығы, жалған іске қосу) бере отырып, оны жоюдың себептерін және негіздемесін ҰКҰО-ке ұсыну.

2.1.21. 1.1-тармаққа сәйкес Тапсырыс берушінің объектілерінде АҚ бойынша өз мамандарының физикалық қатысуы. Тапсырыс берушінің ақ оқиғалары мен оқиғаларын жедел пысықтау үшін. Мамандардың болу мерзімдері мен шарттары шартқа қол қойылғаннан кейін Тапсырыс берушімен келісіледі.

3. Мониторингке қойылатын талаптар

3.1. Ақпараттандыру объектісінің оқиғаларын мониторингтеу АҚ оқиғаларын басқару жүйесі (SIEM) арқ044Влы тұрақты негізде жүзеге асырылады.

3.2. ККЕО-ке қосылу шеңберінде Орындаушы:

- Тапсырыс берушінің ақпараттандыру объектісіне жүйе-дереккөздерден оқиғаларды жинау үшін коллекторды орналастырады, оларды әрі қарай өңдеу үшін қорғалған/шифрланған байланыс арнасы арқылы Орындаушы серверлеріне жібереді;
- Тапсырыс беруші қызметкерлерімен бірге ақпараттық қауіпсіздік инциденттерін анықтау процесін бейімдейді, оған мыналар кіреді:
- инциденттерді анықтау сценарийін анықтайтын корреляциялық ережелер;
- бір сценарий аясында бір/әртүрлі инциденттерге қатысты оқиғаларды анықтау логикасы.

* Жалған позитивтерді азайту үшін тапсырыс берушінің қызметкерлерімен желілік және хосттық белсенділікті талдауды жүргізеді.

3.3. Жаңа дереккөздерді қосу:

Тапсырыс беруші Орындаушыға жаңа оқиғалар дереккөздерін қосуға сұраныс жібереді (дереккөз – ақпараттық жүйеге қатысты оқиға немесе оқиғалар тудыратын объект), келесі ақпаратты ұсынады:

- дереккөздердің түрі;
- дереккөздерден деректер алу туралы ақпарат (IP-мекенжайы, қол жеткізу деректері).

Орындаушы сұранысты алғаннан кейін екі жұмыс күні ішінде жаңа дереккөзді ККЕО-ке қосады.

3.4. Дереккөздерді ажырату:

Тапсырыс беруші Орындаушыға дереккөздерді ажырату туралы сұраныс жібереді, келесі ақпаратты ұсынады:

- дереккөздердің түрі;
- дереккөздердің идентификаторы (IP-мекенжайы, қосымша).

Орындаушы Тапсырыс берушінің сұранысын алған күннен бастап 10 (он) жұмыс күні ішінде қолданыстағы инциденттерді анықтау сценарийлерін талдап, дереккөзді ККЕО-ден ажыратады.

3.5. ККЕО-ке қосылған әрбір МСН үшін оқиғаларды хаттамалау механизмі бапталады (егер МСН-де бұл функция болса).

Операциялық жүйе (бұдан әрі – ОЖ) оқиғаларының түрлері:

- жүйені іске қосу/тоқтату;
- ОЖ объектілерімен жұмыс (ашу, сақтау, қайта атау, жою, жасау, көшіру);
- бағдарламалық қамтамасыз етуді (бұдан әрі – БҚ) орнату және жою;
- пайдаланушылардың ОЖ-ге кіруі мен шығуы, авторизацияның сәтті және сәтсіз әрекеттері;
- жүйелік конфигурацияны өзгерту;
- тіркелгі жазбаларын жасау, жою, өзгерту;
- қорғау жүйелерін, мысалы, антивирустық жүйелер мен шабуылдарды анықтау жүйелерін және оқиғаларды тіркеу журналын іске қосу/өшіру;
- жүйе қауіпсіздігін басқару параметрлерін өзгерту немесе өзгертуге әрекет жасау;
- артықшылықты тіркелгі жазбаларын пайдалану;
- енгізу/шығару құрылғыларын қосу/ажырату;
- пайдаланушының сәтсіз немесе қабылданбаған әрекеттері;
- деректер мен басқа ресурстарға әсер ететін сәтсіз немесе қабылданбаған әрекеттер;
- ОЖ-де процестерді іске қосу, тоқтату.

Деректер базасын басқару жүйесінің оқиғаларының түрлері:

- сессияларды басқару (сәтті/сәтсіз авторизация, тіркелмеген тіркелгілерді пайдалану);
- әкімшілік артықшылықтары бар деректер базасы (бұдан әрі – ДБ) пайдаланушыларының барлық әрекеттері (select, create, alter, drop, truncate, rename, insert, update, delete, call (execute), lock командалары);
- басқа пайдаланушыларға артықшылықтарды беру құқығы бар пайдаланушылардың барлық әрекеттері (grant, revoke, deny).

Телекоммуникациялық жабдықтың оқиғаларының түрлері:

- жүйені іске қосу/тоқтату;
- жүйелік конфигурацияны өзгерту;
- жергілікті тіркелгі жазбаларын жасау, жою, өзгерту;
- артықшылықты тіркелгі жазбаларын пайдалану;
- енгізу/шығару құрылғыларын қосу/ажырату;
- пайдаланушының сәтсіз немесе қабылданбаған әрекеттері;
- желілік байланыстарды (коннектерді) іске қосу, үзілуі, тоқтауы.

Бағдарламалық жасақтама оқиғаларының түрлері:

- пайдаланушылардың авторизациясы (кіру және шығу), авторизацияның сәтті және сәтсіз әрекеттері;
- жергілікті тіркелгі жазбалары мен конфигурациялық файлдарды жасау, көшіру, жылжыту, жою, өзгерту;
- пайдаланушының сәтсіз немесе қабылданбаған әрекеттері;
- пайдаланушының қолжетімділік объектілеріне кіруі;
- қолданбалы БҚ пайдаланушыларының әрекеттері (объектіге (деректерге) қол жеткізу, объектіні (деректерді) өзгерту, объектіні (деректерді) жою).

Ақпараттық қауіпсіздік құралдарымен анықталатын оқиғалар түрлері:

- жергілікті тіркелгі жазбаларын және конфигурациялық файлдарды жасау, көшіру, жылжыту, жою, өзгерту;
- қызметті іске қосу/тоқтату;
- жүйелік конфигурацияны өзгерту;

Әрбір хаттамаланатын оқиға үшін ақпараттық жүйелер немесе олардың компоненттері бойынша ең аз дегенде келесі параметрлер жазылады: пайдаланушы идентификаторы, оқиға түрі, күні мен уақыты, оқиғаның сәтті немесе сәтсіз болғаны, оқиға көзі, оқиға әсер еткен деректердің, жүйелік компоненттің немесе ресурстың идентификаторы немесе атауы.

Оқиғаларды тіркеу журналы келесі өрістерді қамтуы керек:

- күн мен уақыт (күн форматы: КК:АА:ЖЖЖЖ, уақыт форматы: СС:ММ:СС);
- оқиға көзі атауы (қызмет/сервис);
- есептік жазба атауы/пайдаланушы ID;
- пайдаланушының IP-мекенжайы;
- операцияның басталу уақыты;
- операцияның аяқталу уақыты;
- оқиғаның сипаттамасы.

3.6. Оқиғаларды тіркеу журналдарындағы жазбалар мәтіндік форматта сақталады. Тіркеу журналдарының өріс мәндері бөлгіш таңбалармен ажыратылады. Егер өріс ұзын форматта болса және оның мазмұнында бөлгіш таңба болса, өріс шектеуші таңбалары қолданылады. Оқиғаларды тіркеу журналдары үшін UTF-8 кодтамасы қолданылады. Бір оқиғаларды тіркеу журналы файлына әртүрлі деректер форматындағы оқиғаларды жазуға болмайды. Оқиғаларды тіркеу журналдары ақпараттық қауіпсіздік оқиғаларын басқару жүйесінің серверінде кемінде бір жыл сақталады.

3.7. АҚ инциденттері анықталған жағдайда, АҚ инциденттерін басқару жүйесі ККЕО қызметкерлеріне электрондық пошта арқылы автоматты түрде хабарлама жібереді.

3.8. Ақпараттық қауіпсіздік инциденті туралы ақпарат алынғаннан кейін ККЕО оны шұғыл түрде бастапқы деректерді талдайды. Талдау барысында ККЕО қызметкері анықталған деректерде бұзушылықтардың бар-жоғын тексереді.

3.9. Ақпараттық қауіпсіздік инцидентінің сындылығы ақпараттық активтердің құндылығы (маңыздылығы) және/немесе қамтылатын ақпараттық активтердің ауқымы, сондай-ақ инциденттердің қайталануы негізінде бағаланады:

сындарлы (5-деңгей) – қызмет көрсетудің мүмкін еместігіне, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникациялық желілер және басқа да ақпараттандыру объектілері үшін елеулі теріс салдарға әкелетін сөзсіз инциденттер;

маңызды (4-деңгей) – қызмет көрсетудің мүмкін еместігіне, электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникациялық желілер және басқа да ақпараттандыру объектілері үшін елеулі теріс салдарға әкелуі мүмкін инциденттер;

жоғары (3-деңгей) – қызмет көрсетуді айтарлықтай шектеуге, жағдайдың айтарлықтай нашарлауына немесе электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникациялық желілер және басқа да ақпараттандыру объектілері үшін айтарлықтай теріс салдарға әкелуі мүмкін инциденттер;

орташа (2-деңгей) – қызмет көрсетуді шектеуге, жағдайдың нашарлауына немесе электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникациялық желілер және басқа да ақпараттандыру объектілері үшін теріс салдарға әкелуі мүмкін ықтимал инциденттер;

төмен (1-деңгей) – қызмет көрсетуді шектеуге, жағдайдың нашарлауына немесе электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникациялық желілер және басқа да ақпараттандыру объектілері үшін теріс салдарға әкелуі мүмкін ықтимал инциденттер;

сындарлы емес (0-деңгей) – электрондық ақпараттық ресурстар, ақпараттық жүйелер, телекоммуникациялық желілер және басқа да ақпараттандыру объектілері үшін әсер етпейтін шамалы инциденттер.

3.10. Ақпараттық қауіпсіздік инциденті туралы мәліметтер ККЕО қызметкерлері инциденттерді тіркеу жүйесінде тіркеледі.

Инцидентті тіркеу кезінде келесі мәліметтер көрсетіледі:

- инциденттің ағымдағы мәртебесі;
- инциденттің санаты мен түрі;
- инциденттің сипаттамасы (сыртқы көріністері мен алдын ала тергеу нәтижелері);
- инцидентті жою үшін қабылданған шаралар;
- инцидентті тергеу нәтижелері, тергеуге қатысқан қызметкерлердің байланыс деректері.

3.11. Инциденттің санаты мен түрін анықтау ККЕО қызметкерлеріне жүктеледі.

3.12. Қауіптерді мониторингтеу және анықтау бойынша күшейтілген талаптар.

Орындаушы қауіптерді анықтау үшін біріктірілген тәсілді қолдануға міндетті:

- Сигнатуралық ережелер — Sigma, YARA форматында;

- Мінез-құлыққа негізделген ережелер мен модельдер — MITRE ATT&CK, өзіндік корреляциялар, UEBA негізінде;

- Оқиғаларды байыту — MISP және ұқсас Threat Intelligence платформалары арқылы.

3.13. Қызмет көрсетудің алғашқы айында Тапсырыс берушінің саласына тән қауіптерге арналған кемінде 20 теңшелген анықтау ережесін әзірлеу және енгізу.

3.14. Ережелердің өзектілігін үздіксіз қамтамасыз ету — кемінде айына 1 рет, олардың тиімділігін міндетті түрде тексерумен бірге.

3.15. Қызметкерлердің резервін қамтамасыз ету — тәулік бойы (24/7) жұмыс үшін кемінде екі ауысым болуы шарт.

3.16. Шартқа қол қойылғанға дейін тестілік әрекет ету рәсімін міндетті түрде көрсету.

3.17. ККЕО ең маңызды оқиға көздері бойынша апаттық өзара іс-қимылды қамтамасыз ету үшін резервтік байланыс арнасы.

Орындаушы резервтік байланыс арнасын ұйымдастыру және пайдалану кезінде, тек ең маңызды оқиға көздерімен апаттық өзара іс-қимылды қамтамасыз ету мақсатында, кеңес беру және техникалық қолдау көрсетуге, сондай-ақ ККЕО жауапкершілік аймағында оның мониторингін жүргізуге міндетті. Маңызды оқиға көздерінің тізімі шартқа қол қойылғаннан кейін 10 жұмыс күні ішінде қалыптастырылып, Тапсырыс берушімен келісуге жатады және кемінде тоқсанына бір рет өзектендіріледі.

3.18. Өнім беруші шартқа қол қойылған сәттен бастап күнтізбелік 5 (бес) күн ішінде техникалық ерекшелікке 1-қосымшада санамаланған ақпараттық қауіпсіздік оқиғаларының барлық көздерінің толық қосылуын қамтамасыз етуге міндетті. ККЕО-не дереккөздерді уақтылы қосу оқиғаларды үздіксіз бақылауды, анықтауды және корреляциялауды қамтамасыз ету үшін өте маңызды.

3.19. Қызметкерлер резервінің міндетті түрде болуы (24/7 жұмыс үшін кемінде екі ауысым).

4. Инциденттерді хабарлау және оларға жауап беру

4.1. Ақпараттық қауіпсіздікке қатерлер/инциденттер анықталған және олардың деректері расталған жағдайда, ККЕО оларды анықтаған сәттен бастап 15 минут ішінде ақпараттық қауіпсіздік инциденттері туралы ККЕО басшысын, МСН объектісінің иесін және ҰКҰО -ті хабардар етеді.

4.2. МСН объектісінің иесін және ҰКҰО -ті ақпараттық қауіпсіздік инциденттері туралы хабарлау ККЕО-тің «МТҚ» АҚ-мен өзара әрекеттесуге жауапты қызметкері (немесе оның өкілетті қызметкері) электрондық пошта және/немесе MISP арқылы жүзеге асырылады.

4.3. АҚ инциденттерін талдау операциялық жүйелер, деректер базасын басқару жүйелері, қолданбалы бағдарламалық қамтамасыз ету, ақпаратты қорғау құралдары, ақпараттық жүйелердің қорғанысын талдау үшін арнайы құралдардың қауіпсіздік оқиғаларын тіркеу және есепке алу кіріктірілген механизмдері, сондай-ақ ҰКҰО -тен алынған ақпарат негізінде ККЕО қызметкеріме н жүргізіледі.

4.4. Ақ инцидентіне ден қоюдың басталу уақыты ол анықталған сәттен бастап және уәкілетті қызметкерлерді хабардар еткен сәттен бастап техникалық ерекшелікке №1 қосымшаның №1 кестесіне сәйкес айқындалады.

4.5. Сыни оқиғаны оқшаулау және жою ол анықталғаннан кейін 15 минут ішінде, қажет болған жағдайда (Орындаушының орнында) МСН объектісі қызметкерлерінің көмегімен басталады. Ақпараттық қауіпсіздік инцидентіне жауап беру келесі кезеңдерден тұрады:

а) ақпараттық қауіпсіздік инцидентінің орын алғанын растау/терістеу;

б) ақпараттық қауіпсіздік инцидентін жіктеу;

в) ақпараттық қауіпсіздік инцидентінің сыни деңгейін растау/түзету;

г) ақпараттық қауіпсіздік инцидентінің қосымша жағдайларын (детальдарын) нақтылау;

д) ақпараттық қауіпсіздік инцидентінің пайда болу дәлелдерін алу (жинау), олардың сақталуын және тұтастығын қамтамасыз ету;

е) ақпараттық қауіпсіздік инцидентінің салдарын азайту;

ж) ақпараттық қауіпсіздік инцидентін анықтау, салдарын жою және алдын алу бойынша қызметкерлерді ақпараттандыру және кеңес беру;

з) инциденттің пайда болуына әкелген тәуекелдерді қайта бағалау, қажетті ережелерді, регламенттерді және ақпараттық қауіпсіздік қағидаларын жаңарту.

4.6. АҚ инциденттерін талдау (форензика), оның ішінде ақпараттық қауіпсіздік инциденттерінің пайда болу көздері мен себептерін анықтау, сондай-ақ олардың салдарын бағалау, ККЕО қызметкерімен және ақпараттандыру объектісіне техникалық қызмет көрсететін қызметкерлермен бірлесе отырып жүргізіледі.

4.7. Техникалық ерекшелікке №1 қосымшаның №2 кестесіне сәйкес ОӘБ көрсету кезеңіне жауапкершілік аймақтарын бөлу.

1. **АҚЖО қызметтерінің көлемі және есептілік талаптары**

5.1. Орындаушы ККЕО қызметтерін Тапсырыс берушінің сұранысы негізінде қажетті техникалық сипаттамаларды көрсете отырып ұсынады.

Техникалық ерекшелікке №1 қосымшаның №3 кестесіне сәйкес ККЕО-на қосылу жөніндегі көздердің саны мен техникалық сипаттамалары.

5.2. Шартқа қол қойылғаннан кейін, 15 күн ішінде, Тапсырыс берушімен бірлесіп, Орындаушы ин циденттерге жауап беру бойынша өзара іс-қимыл Регламентін әзірлейді және келіседі, сондай-ақ ақпараттандыру нысанына немесе МСН (Тапсырыс берушінің сұрауы бойынша) бастапқы аудит жүргізеді.

5.3. Бастапқы аудиттің нәтижесі ақпараттандыру нысанының / МСН ағымдағы жағдайын және 5.1-кестеде көрсетілген нақты деректерді сипаттайтын есеп болуы тиіс.

5.4. Орындаушы айдың 15-інен кешіктірмей мәтіндік, кестелік және графикалық (диаграммалар, графиктер) ақпаратпен Ай сайынғы аналитикалық есепті ұсынады, ол шартты орындау бойынша төмендегі мәліметтерді қамтиды:

- есепті кезеңдегі сұраулар мен инциденттер бойынша статистикалық мәліметтер;
- ақпараттық қауіпсіздік инфрақұрылымының жағдайын талдау;
- проблемалық мәселелердің тізімі және оларды шешу мен ақпараттық қауіпсіздік инфрақұрылымын жақсарту бойынша ұсынымдар;
- Қызмет көрсетуді жүзеге асыратын мамандардың өзекті байланыс деректері.

6. АҚ аудитін жүргізуге қойылатын талаптар

6.1. Орындаушы шартқа қол қойылғаннан кейін 15 күн ішінде ақпараттандыру нысанына барып, ақпараттық қауіпсіздік аудитін (қорғауды талдау) жүргізуді қамтамасыз етеді. **Ақпараттық қауіпсіздік аудитін жүргізу кезінде Орындаушының қызметкерлері Тапсырыс берушінің аумағында болуы тиіс.**

6.2. Тексеру объектілерінің тізбесі осы техникалық ерекшеліктің №1 Қосымшасының №3 кестесінде көрсетілген.

6.3. Сыртқы желі сегментінің осалдықтарын талдау

- желілік инфрақұрылымның сыртқы периметрін осалдықтарды сканерлеу бағдарламалық құралын қолдану арқылы сканерлеу;
- сканердің барлық табылған осалдықтарын Орындаушының білікті маманы қолмен тексеріп, оларды валидациялауы тиіс;
- сыртқы сканерлеу аймағы – кемінде 10 нысан (қоғамдық URL мекенжайлары).

6.4. Ішкі желі сегментінің осалдықтарын талдау

Ішкі желі сегментінің осалдықтарын анықтау Тапсырыс берушінің жергілікті желісінің периметрінен жүзеге асырылады және келесілерді қамтиды:

- ішкі URL мекенжайларын VPN байланысы арқылы сканерлеу;
- ішкі ақпараттық жүйелер мен желілерді Тапсырыс берушінің аумағынан сканерлеу;
- сканер барлық табылған хосттарды түгендеуді (АТ-активтердің картасын құру) қамтамасыз етуі тиіс;
- табылған хосттар мен URL мекенжайлар ашық осалдықтарға тексерілуі тиіс.

7. Фишинг-кампания жүргізу талаптары.

Орындаушы қызметкерлердің әлеуметтік инженерия шабуылдарына төзімділігін бағалау мақсатында оқыту фишинг-кампаниясын жүргізуді қамтамасыз етуі тиіс. Қызмет келесілерді қамтуы қажет:

- фишинг сценарийлерін әзірлеу (хаттар, сілтемелер, формалар),

- келісілген қызметкерлер тізімі бойынша тарату,

- нәтижелерді жинау және өңдеу (сілтемеге өту, деректерді енгізу және т.б.).

Фишинг-акция нәтижелері бойынша Орындаушы келесі мәліметтерді қамтитын толық есепті ұсынуға міндетті:

- сілтемеге өткен қызметкерлердің ТАӘ немесе идентификаторы;

- оқиға күні мен уақыты;

- құрылғының IP-мекенжайы;

-енгізілген деректер туралы ақпарат (қолданылған жағдайда);

- қауіп деңгейі.

Сондай-ақ, тапсырыс берушіге кампания нәтижелерін нақты уақыт режимінде немесе аяқталғаннан кейін өз бетінше бақылауға мүмкіндік беретін онлайн-панель немесе жүктеу нұсқасы қарастырылуы тиіс. Барлық әрекеттер жұмыс жүйелеріне қауіп төндірмейтін бақыланатын ортада жүргізілуі тиіс.

8. DDoS-шабуылдардан қорғау қызметіне қойылатын талаптар.

Орындаушы телекоммуникациялық провайдер деңгейінде — трафик Тапсырыс берушінің желісіне түскенге дейін — DoS/DDoS-шабуылдарын анықтауды және автоматты түрде сүзгіден өткізуді қамтамасыз етуі тиіс. Шешім келесілерді қамтуы қажет:

- Зиянды трафикті инфрақұрылымға кірмей тұрып автоматты түрде тазарту;

- Белсенділік шегінен асқан аномалияларды тәулік бойы бақылау және оларға әрекет ету;

- Тапсырыс берушінің барлық тіркелген шабуылдары көрсетілетін жеке кабинеті: күні, уақыты, дереккөздердің географиясы, көлемі (Gbps), қарқындылығы (pps), векторы (SYN Flood, UDP Flood және т.б.);

- Шабуыл фактісі туралы нақты уақыт режимінде e-mail және/немесе баламалы арналар (мессенджер және т.б.) арқылы хабарлама жіберу;

- Инциденттер бойынша толық статистикасы бар есептерді қалыптастыру (PDF/Excel форматтарында экспорттауды қоса алғанда);

- Ақпараттық қауіпсіздік инциденттері санатына жататын оқиғалар анықталған жағдайда ҚР Ұлттық ақпараттық қауіпсіздік үйлестіру орталығына тәулік бойы ақпарат беру міндетті.

Жүйе тұрақты жұмыс істеуі және заңды трафикке әсері барынша аз болуы тиіс.

9. қосымша қызметтер көрсету:

9.1. Орындаушы жылына 1 рет тиісті бағдарламалық құралды қолданып, «Тапсырыс берушінің» ақпараттық жүйесінің бастапқы кодына талдау жүргізеді және ықтимал осалдықтарды, қателерді жою бойынша ұсыныстар мен есеп ұсынады. Бұл қателер жүйе жұмысының бұзылуына, деректердің жоғалуына немесе рұқсатсыз қол жеткізуге әкелуі мүмкін.

9.2. Бастапқы кодты талдауға арналған бағдарламалық құрал ақпараттық жүйенің қауіпсіздігін талдаудың келесі әдістерін жүзеге асырады: статикалық (Static Application Security Testing, SAST); динамикалық (Dynamic Application Security Testing, DAST, «қара жәшік» әдісі); үшінші тарап компоненттерін талдау; ақпараттық жүйенің конфигурациялық файлдарын талдау.

9.3. Бастапқы кодты талдауға арналған бағдарламалық құрал ақпараттық жүйенің алдыңғы талдау нәтижелерін ескереді және ең алдымен, соңғы талдаудан бері өзгертілген код бөліктерін талдайды, ал қалған код өзгеріске әсер еткен жағдайда ғана талданады.

9.4. Бастапқы кодты талдауға арналған бағдарламалық құрал кіріктірілген үлгілер негізінде есептер жасау мүмкіндігін қамтамасыз етеді, соның ішінде келесі есеп түрлері: автотексеру есебі; OWASP Top 10 2021 есебі; OWASP Mobile Top 10 2024 Final Release есебі; SANS Top 25 есебі; PCI DSS 4.0.1 есебі; NIST 800-53 (revision 5) есебі.

9.5. Бастапқы кодты талдауға арналған бағдарламалық құрал осалдық сигнатураларының пайдаланушы базасын редакциялау мүмкіндігін қамтамасыз етеді.

10.Қазақстан Республикасының заңнамасын сақтауға қойылатын талаптар

10.1.Қызметтер «Киберқауіпсіздік туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңының (бұдан әрі – Заң) 7-5-бабына, сондай-ақ «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» ҚР Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысына және басқаларға сәйкес көрсетілуі тиіс Қазақстан Республикасының қолданыстағы стандарттарымен. Қазақстандық стандарттар болмаған жағдайда Қазақстан Республикасының заңнамасында белгіленген тәртіппен ақпараттық қауіпсіздікте - ISO/IEC 27001-өзге де стандарттар мен үздік халықаралық тәжірибелерді пайдалануға жол беріледі. Сондай-ақ, Қызметтер интернетке қол жеткізудің бірыңғай шлюзін пайдалануға қойылатын талаптарға сәйкес, сонымен қатар, Тапсырыс берушінің ішкі нормативтік құжаттарына сай көрсетілуі тиіс.

10.2. Тапсырыс берушінің деректерін сақтау Қазақстан Республикасының аумағында орналасқан ресурстарда жүзеге асырылады («Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңының талаптары, «Ақпаратқа қол жеткізу туралы» Қазақстан Республикасының 2015 жылғы 16 қарашадағы № 401-V Заңы, «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» ҚР Үкіметінің 20.12.2016 жылғы № 832 Қаулысы).

10.3. Ақпараттық қауіпсіздіктің ұлттық үйлестіру орталығымен ККО өзара іс-қимылы Заңға сәйкес жүзеге асырылады.

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 27001-2015	384044	Қазақстан Республикасының ұлттық стандарты	Информационная технология методы и средства обеспечения безопасности системы менеджмента информационной безопасностью требования	Настоящий стандарт устанавливает требования к разработке, внедрению, поддержанию в рабочем состоянии и непрерывному совершенствованию системы менеджмента информационной безопасностью организации в контексте существующих бизнес рисков организации.	Нет ()	68	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	

Қосымша

Приложение 1 к ТС каз .docx
Приложение 1 к ТС.docx

Қол қойған Дубовая Юлия Анатольевна
Қол қойылған күні 20.11.2026

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

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1271384
способом Открытый тендер на понижение

Лот № 1 (31-2 У, 4583333) Услуги по обеспечению информационной безопасности

Заказчик: Товарищество с ограниченной ответственностью "Северо-Западная трубопроводная компания "МунайТас"

Организатор: Товарищество с ограниченной ответственностью "Северо-Западная трубопроводная компания "МунайТас"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	31-2 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	Обеспечение мониторинга и обнаружения инцидентов информационной безопасности и реагирование на них
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Алматы, Бостандыкский район, ул. Тимирязева, 26/29
Условия поставки	-
Срок поставки	с 01.2027 по 12.2027 (включительно)
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 100%, Окончательный платеж - 0%

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

СПИСОК ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ И ТЕРМИНОВ

ИБ	Информационная безопасность

ЦОК	Центр обеспечения кибербезопасности - юридическое лицо или структурное подразделение юридического лица, являющееся резидентом Республики Казахстан без участия иностранных юридических и физических лиц, осуществляющее деятельность по защите цифровых объектов
Инфраструктура ИБ	Программные и аппаратные средства, данные в электронном виде, обеспечивающие работу сервисов ИБ. используемых Заказчиком
Инцидент ИБ	Инцидент информационной безопасности - отдельно или серийно возникающие сбои в работе информационно- коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов
ИС	Информационная система - организационно упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач

ИТ	Информационные технологии
НКЦКБ	Национальный координационный центр кибербезопасности
МОКБ	мониторинг обеспечения кибербезопасности К ВЦО
IP-адрес	уникальный адрес, идентифицирующий устройство в интернете или локальной сети
SIEM	(Security information and event management) система управления событиями информационной безопасности
VPN	(Virtual Private Network) - «виртуальная частная сеть», позволяющих обеспечить одно или несколько сетевых соединений поверх другой сети по средствам криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств защиты от повторов и изменений передаваемых по логической сети сообщений)
ОС	операционная система

КВЦО	Критически важные цифровые объекты
АО «ГТС»	АО "Государственная техническая служба"
ЕШДИ	Единый шлюз доступа к Интернету
MISP	платформа Threat Intelligence ОЦИБ

1. **Основные положения:**
    1. В целях обеспечения оперативного реагирования и отработки инцидентов информаци онной безопасности (далее – ИБ) Исполнитель обязан обеспечить присутствие техни ческого специалиста на территории Заказчика по запросу. В случае обнаружения инцидента (высокой критичности), сотрудники ОЦИБ в течении 60 минут физически пребывают на территорию Заказчика (удаленное сопровождение запрещено) и занимаются полным расследованием и устранением инцидентов ИБ и т.д.
    2. Взаимодействие ЦОК осуществляется с Заказчиком, правоохранительными и специальными органами.
        1. **ПЕРЕЧЕНЬ СЕРВИСОВ ВХОДЯЩИХ В УСЛУГУ**

№	Описание	Особые условия
1	Предоставление услуги оперативного центра информационной безопасности (ЦОК)	Круглосуточный режим
Обязательные к исполнению сервисы		

№	Описание	Параметры	Ответственные сотрудники Исполнителя
1	**Проведение внешних и внутренних тестов на проникновение (1 раз в квартал) ****	Проведение тестов на проникновение в инфраструктуру Заказчика *(из периметра локальной сети Заказчика)* сертифицированными сотрудниками по тестированию на проникновение. Сценарии проведения тестирования и используемые методы согласовываются с Заказчиком. По итогам Исполнитель предоставляет отчет (удаленное сопровождение запрещено).	Аналитики 2 линий
		Проведение тестов на проникновение в инфраструктуру Заказчика из сети Интернет. Сценарии проведения тестирования и используемые методы согласовываются с Заказчиком. По итогам Исполнитель предоставляет отчет.	Аналитики 2 линий

2	**Проведение внешних тестов на проникновение (1 раз в квартал) ****	Социальная инженерия (вид тестирования: психологическое манипулирование с целью совершения определённых действий или разглашения конфиденциальной информации)	Аналитики 2 линий
		В течении 60 минут физически пребывают на территорию Заказчика (удаленное сопровождение запрещено) и обеспечивают полное расследование и устранение инцидентов ИБ. Без ограничений на количество заявок Заказчика на период действия договора. Услуги в области компьютерной криминалистики включают: • 1. восстановление данных с различных носителей, включая повреждённые или зашифрованные устройства;	

- 2. расследование компьютерных технологий, включая анализ вредоносного ПО, сетевых атак и действий злоумышленников;
- 3. экспертиза объекта информатизации, а именно:
  - 3.1. оценка масштабов инцидента и возможных последствий, разработку рекомендаций по предотвращению аналогичных событий в будущем;
  - 3.2. восстановление хронологии событий с использованием анализа временных меток и системных артефактов;

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

3	**Анализ инцидентов (компьютерная криминалистика) ***	• 3.3. установление источника инцидента (внутренний или внешний нарушитель) и сбор юридически значимых доказательств; • 3.4. исследование файловых систем для поиска скрытых или удалённых данных; • 3.5. поиск, по ключевым словам, что позволяет выявить необходимую информацию даже при ограниченных исходных данных; • 4. проведение OSINT-разведки — поиск, сбор и анализ информации из открытых источников;	Аналитики 2,3 линий

		• 5. анализ мобильных устройств, включая разблокировку, извлечение удалённых данных и анализ установленных приложений; • 6. анализ сетевых логов и активности для выявления проникновений, а также предотвращения их в будущем; • 7. сопровождение уголовных и административных дел, предоставление экспертных заключений и консультаций для правоохранительных органов; • 8. проведение специализированных экспертиз, включая анализ фишинговых атак, утечек данных и компрометации учётных записей;		

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

		выезд специалиста на место для участия в следственных действиях, фиксации и протоколирования данных, что увеличивает шансы успешного раскрытия дела.	
4	**Расширенная экспертиза по анализу зловредного программного обеспечения**	Исследование одного объекта включает в себя: 1. первичный анализ вредоносных программ; 2. исследование средств компьютерных технологий на предмет выявления вредоносного ПО; 3. проведение динамического и статического анализа объекта; 4. анализ алгоритма заражения, определение индикаторов заражения, выдача рекомендаций по устранению; 5. составление аналитического отчета.	Аналитики 2,3 линий

5	**Расширенная экспертиза по расследованию критичных инцидентов**	Экспертиза по расследованию критичных инцидентов (проведение мероприятий по реагированию на инциденты ИБ на площадке Заказчика, сбору и исследованию образов жестких дисков, анализ вредоносного ПО, оказания помощи в устранении последствий инцидентов).	Аналитики 1,2,3 линий
6	**Сканирование периметра на уязвимости (внешнее)**	Не более 300 IP-адресов. Инструментальное сканирование из сети Интернет узлов и информационных систем периметра Заказчика на выявление наличия уязвимостей в приложениях и ОС, с предоставлением детального отчета по уязвимостям и рекомендациям по их устранению.	Аналитики 2 линий

7	**Сканирование Зоны мониторинга на наличие уязвимостей (единовременные работы)**	Не более 300 IP-адресов. Инструментальное сканирование узлов и информационных систем, входящих в Зону мониторинга, на выявление наличия уязвимостей в приложениях и ОС, с предоставлением детального отчета по уязвимостям и рекомендациям по их устранению.	Аналитики 2 линий
8	**Проведение комплексного технического обследования состояния информационной безопасности**	• Сканирование периметра на уязвимости (внешнее); • внешнее тестирование на проникновение; • внутреннее тестирование на проникновение; • социальная инженерия; анализ защищенности WEB приложений.	Аналитики 2, 3 линий

9	**Имитация целевых кибератак (Red Teaming).**	Проведение имитаций целевых кибератак с последующим анализом и предоставлением Заказчика рекомендаций по повышению уровня защищенности информационных систем. В отличие от тестирования на проникновение, у Исполнителя не стоит задача выявить максимальное количество уязвимостей за определенный промежуток времени, а, посредством проведения имитации направленных на Заказчика атак, оценить возможности Заказчика по выявлению и предотвращению вторжения.	Аналитики 2 линий

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

		В зависимости от сложности приложения и применяемого метода анализа защищенности (черный/серый /белый ящик) (включая одну проверку устранения уязвимостей в течение 3-х месяцев после проведения анализа защищенности).	
10	**Анализ защищенности приложений**		Аналитики 2 линий

		Анализ мобильного или WEB приложения на предмет наличия уязвимостей с применение специализированного ПО, а также ручной анализ, проводимый экспертами, имеющими соответствующую квалификацию. В зависимости от типов услуги (черный, серый или белый ящик), анализ проводится без получения какой-либо технической информации или доступов к приложению (черный ящик), с наличием у аналитика доступов к приложению, аналогичных доступам пользователей (серый ящик), с использованием аналитиком исходного кода приложения в процессе проведения анализа защищенности.	
11	**Разработка нетипового сценария выявления атак**	По заявке клиента	Аналитики 2, 3 линий

12	**Требования к обучению работников Заказчика**	В целях повышения уровня знаний и готовности по информационной безопасности, Исполнитель по заявке Заказчика должен провести обучение сотрудников Заказчика по информационной безопасности. Обучение должно быть закреплено тестовыми заданиями с выдачей результата тестирования. В курсе обучения должны применяться раздаточные материалы и методические пособия. Исполнитель обязан провести обучение по следующим темам: 1) Основы Информационной безопасности и защиты информации; 2) Методы и средства защиты информации; 3) Введение в цифровую гигиену и кибербезопасность. 4) Основы Базы данных; 5) Основы Компьютерных сетей;	Аналитики 2,3 линий

		6) Основы Компьютерной криминалистики. Исполнитель услуг оказывает консультационную поддержку в течение действия договора. *Онлайн-платформа для обучения кибербезопасности.* Исполнитель должен предоставить доступ к платформе по кибербезопасности. Платформа должна включать в себя набор базовых курсов по кибербезопасности и тестирование после их прохождения. Платформа должна иметь панель для отслеживания результатов прохождения обучения, тестирования и отчет об утечках.	

13	**Проведение фишинг-кампании**	Исполнитель должен провести обучающую фишинг-кампанию с имитацией атак социальной инженерии. Обязательна идентификация сотрудников, перешедших по ссылке, с указанием IP-адреса, времени и других данных. По завершении предоставляется отчёт с аналитикой и рекомендациями. Должна быть возможность проверки результатов Заказчиком.	Аналитики 2,3 линий
14	**Услуга защиты от DDoS-атак**	Исполнитель должен обеспечить автоматическую защиту от DoS/DDoS-атак на уровне провайдера с фильтрацией трафика до входа в сеть. Обязателен личный кабинет с отчётами об атаках (источник, объём, скорость), а также мгновенные уведомления о факте атаки через e-mail или другой канал.	Аналитики 1, 2, 3 линий

15	**Purple Team Exercise — не реже 1 раза в год.**	Исполнитель должен провести работу для проверки и улучшения процессов обнаружения и реагирования на инциденты. Проводится минимум 1 раз в год с документированием результатов.	Аналитики 1, 2, 3 линий

* в том числе определение источников и причин возникновения инцидентов ИБ, а также оценку их последствий осуществляет работник ЦОК совместно с сотрудниками, осуществляющими техническое обслуживание КВЦО.

В рамках проведения работ по компьютерной криминалистике ставятся следующие задачи:

- определение способа реализации взлома;

- построение сценария атаки;

- восстановление хронологии атаки;

- сбор оставшихся следов атаки;

- разработка необходимых мер защиты для предотвращения от подобной атаки и, по возможности от других атак, улучшая процесс обеспечения ИБ в целом;

- уменьшение и восстановление нанесенного ущерба.

** Тестирование на проникновение внешнего сегмента сети с частичной или приблизительной информацией о предмете тестирования (Grey Box):

- путем эмуляции кибератак, вручную оценить безопасность инфраструктуры с точки зрения внешнего пользователя (не сотрудника), пытающегося получить доступ к учетной

записи сотрудника организации

- путем эмуляции кибератак, вручную оценить безопасность инфраструктуры в качестве сотрудника организации, пытающегося увеличить привилегии, получить доступ к серверной части или обнаружить другие слабости средств информационной безопасности.

Результаты:

1) полный отчет о найденных уязвимостях, включая описание риска и важности находки;

2) отчет с рекомендациями по их устранению и повышению уровня защищенности;

3) рекомендации для снижения рисков от атак со стороны сетей общего пользования и со

стороны внутренней сети;

График проведения обследования ИС (Пентест) согласовывается с Исполнителем дополнительно в течение действия договора услуги. Общая продолжительность обследования ИС не должна превышать 45 рабочих дней.

Должны использоваться следующие стандарты для тестирования на проникновение:

- PTES (Penetration Testing Execution Standard);

- OWASP Top 10 (OWASP Testing Guide);

- ISECOM OSSTMM.

Работы проводятся с уведомлением администраторов (и пользователей) тестируемой системы. В процессе тестирования используются *как инструментальные средства, так и ручные методы анализа защищенности.*

1. **Требования к услуге:**

1. В рамках мониторинга и реагирования на инциденты ИБ Исполнитель должен обеспечить:

2.1.1 анализ объекта КВЦО на предмет определения перечня журналов регистрации событий, необходимых для передачи в систему управления событиями ИБ НКЦКБ;

2.1.2. установку агентов системы управления событиями ИБ на систему сбора журналов регистрации событий объекта КВЦО и, при необходимости, на иные объекты информационно-коммуникационной инфраструктуры собственника или владельца объекта КВЦО;

2.1.3. сбор журналов регистрации событий объекта КВЦО и относящихся к нему средств защиты информации, в системе управления событиями ИБ НКЦКБ, их обработку и анализ с целью выявления событий ИБ и инцидентов ИБ;

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

2.1.4. первичный анализ событий ИБ или инцидентов ИБ, выявленных на объекте КВЦО;

2.1.5. уведомление ответственных лиц за обеспечение ИБ объекта КВЦО с предоставлением перечня данных об инциденте ИБ, согласно приложению 2 к Приказу Министра оборонной и аэрокосмической промышленности от 28 марта 2018 года №52/НК «Об утверждении Правил проведения мониторинга обеспечения кибербезопасности цифровых объектов» цифрового правительства и критически важных цифровых объектов» (далее – Правила мониторинга), в течение 30 минут с момента выявления события ИБ или инцидента ИБ, КНБ РК – в течение 24 часов;

2.1.6. выдачу первичных рекомендаций по приостановлению распространения инцидента ИБ собственнику или владельцу объекта КВЦО;

2.1.7. обследование объектов КВЦО на предмет наличия уязвимостей (далее – обследование на уязвимости);

2.1.8. предоставление результатов обследования на уязвимости и рекомендаций по устранению уязвимостей объектов КВЦО собственникам или владельцам объектов КВЦО в течение 10 рабочих дней после завершения работ по обследованию на уязвимости;

2.1.9. консультирование собственников или владельцев объектов КВЦО по вопросам устранения уязвимостей объектов КВЦО, выявленных в рамках обследования на уязвимости ИС;

2.1.10. обследование объекта КВЦО на предмет исполнения требований технической документации по информационной безопасности (далее – ТД по ИБ) предоставление результатов обследования объекта КВЦО на предмет исполнения требований ТД по ИБ и рекомендаций по устранению выявленных нарушений ТД по ИБ собственникам или владельцам объектов КВЦО в течение 10 рабочих дней со дня завершения данного обследования.

2.1.11. организацию журналирование событий объекта КВЦО и относящихся к нему средств защиты информации, в соответствии с форматами и типами записей журналов регистрации событий.

2.1.12. организацию систему сбора журналов регистрации событий в контуре телекоммуникационной сети, в котором функционирует объект КВЦО;

2.1.13. организацию передачу журналов регистрации событий объекта КВЦО и относящихся к нему средств защиты информации, в систему сбора журналов регистрации событий объекта КВЦО;

2.1.14. уведомление НКЦИБ о планируемых работах по внесению изменений в журналирование событий объекта КВЦО за 5 рабочих дней до внесения изменений. К уведомлению прикладываются образцы изменяемых журналов регистрации событий и их описание;

2.1.15. обеспечение условия, согласованные с НКЦКБ, для передачи журналов регистрации событий объекта КВЦО из системы сбора журналов регистрации событий объекта КВЦО в систему управления событиями ИБ НКЦКБ;

2.1.16. уведомление НКЦКБ о самостоятельно выявленном инциденте ИБ на объекте КВЦО в течение 15 минут с момента выявления;

2.1.17. предоставление в НКЦКБ Перечень данных в течение 24 часов с момента обнаружения инцидента ИБ.

2.1.18. направление в НКЦКБ информацию о мерах, принятых для устранения уязвимостей объекта КВЦО, в течение двадцати календарных дней со дня получения результатов обследования на наличие уязвимостей;

2.1.19. в случае самостоятельного обнаружения уязвимости объекта КВЦО, предоставлен ие в НКЦИБ перечень данных об уязвимости ОИ ЭП по форме согласно приложению 5 Правил мониторинга в течение 24 часов с момента выявления уязвимости объекта КВЦО;

2.1.20. в случае не устранения уязвимости объекта КВЦО может обеспечить присвоение уя звимости одну из категорий (производственная необходимость, уязвимость нулевого дня, ложное срабатывание) и предоставляет в НКЦКБ категории причин не устранения уязвимости и обоснование причины не устранения.

2.1.21. физическое присутствие своих специалистов по ИБ на объектах Заказчика, согласно п.1.1. для оперативного обрабатывания инцидентов и событий ИБ Заказчика. Сроки и условия нахождения специалистов согласовываются с Заказчиком после подписания договора.

3. Требования к мониторингу:

3.1. Мониторинг событий осуществляется на постоянной основе, с использованием системы управления событиями ИБ (SIEM). В рамках оказываемой услуги Исполнитель проводит мониторинг событий с подключенных источников.

3.2. В рамках подключения к ЦОК Исполнитель:

- Размещает на территории Заказчика коллектор для сбора событий с систем-источников для дальнейшей отправки по защищенному/зашифрованному каналу связи на сервера Исполнителя для дальнейшей обработки;
- Совместно с работниками Заказчика адаптирует выявление инцидентов ИБ, включающий в себя:

- корреляционные правила, позволяющие выявлять соответствующий сценарий обнаружения инцидентов;
- логику определения событий, относящихся к одному/разным инцидентам, в рамках одного сценария.

- Проводит совместно с работниками Заказчика сетевой и хостовой анализ активности для минимизации ложных срабатываний.

3.3. Подключение новых источников. Заказчик направляет запрос на подключение новых источников событий (источник - объект, создающий событие или события, которые имеют отношение к информационной системе) Исполнителю, предоставляя следующую информацию:

- тип источников;
- информация по получению данных с источников (ip-адрес, данные доступа).

Исполнитель в течение двух рабочих дней подключает к ЦОК новый источник.

3.4. Отключение источников. Заказчик направляет запрос на отключение источников, предоставляя следующую информацию:

- тип источников;
- идентификатор источников (IP-адрес, приложение).

Исполнитель в течение 10 (десяти) рабочих дней с даты получения запроса Заказчика, проводит анализ существующих сценариев обнаружения инцидентов и проводит отключение источника от ОЦИБ.

3.5. Для каждого критически важного объекта информационно-коммуникационной инфраструктуры, подключенных к ЦОК настраивается механизм протоколирования событий (при условии наличия данного функционала в КВЦО). Перечень событий, подлежащих протоколированию

Типы событий операционной системы (далее – ОС):

- запуск/остановка системы;

- работа с объектами ОС (открытие, сохранение, переименование, удаление, создание, копирование);

- установка и удаление программного обеспечения (далее – ПО);

- авторизация (вход и выход) пользователей в ОС, успешные и неуспешные попытки авторизации;

- изменение системной конфигурации;

- создание, удаление, модификация учетных записей;

- активация/дезактивация систем защиты, таких как антивирусные системы и системы обнаружения вторжения, и средств ведения журнала регистрации событий;

- изменение или попытки изменения настроек и средств управления защитой системы;

- использование привилегированных учетных записей;

- подключение/отключение устройства ввода/вывода;

- неудавшиеся или отвергнутые действия пользователя;

- неудавшиеся или отвергнутые действия, затрагивающие данные и другие ресурсы;

- запуск, остановка процессов в ОС.

Типы событий системы управления базами данных:

- контроль сессий (успешная/неуспешная авторизация, регистрация использования незарегистрированных учетных записей);
- все действия пользователей базы данных (далее – БД) имеющих административные привилегии (включая команды select, create, alter, drop, truncate, rename, insert, update, delete, call (execute), lock);
- все действия пользователей имеющих права на присвоение привилегий другим пользователям БД (grant, revoke, deny).

Типы событий телекоммуникационного оборудования:

- запуск/остановка системы;
- изменение системной конфигурации;
- создание, удаление, модификация локальных учетных записей;
- использование привилегированных учетных записей;
- подключение/отключение устройства ввода/вывода;
- неудавшиеся или отвергнутые действия пользователя;
- запуск, падение, остановка сетевых линков (коннектов).

Типы событий ПО:

- авторизация (вход и выход) пользователей, успешные и неуспешные попытки авторизации;
- создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;
- неудавшиеся или отвергнутые действия пользователя;
- получение пользователем доступа к объектам доступа;
- действия пользователей прикладного ПО (доступ к объекту (данным), изменения объекта (данных), удаления объекта (данных))

Типы событий, выявляемые средствами защиты информации:

- создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;
- запуск/остановка службы;
- изменение системной конфигурации;

Для каждого протоколируемого события информационных систем или их компонентов записываются как минимум следующие параметры: идентификатор пользователя, тип события,

дата и время, успешным или неуспешным было событие, источник события, идентификатор или название данных, системного компонента или ресурса, на которые повлияло событие.

Журнал регистрации событий должен содержать следующие поля:

- дата и время (формат даты: ДД: ММ: ГГГГ, формат времени: ЧЧ: ММ: СС);

- наименование источника события (сервис/служба);

- имя учетной записи/ID пользователя;

- IP-адрес пользователя;

- время начала операции;

- время окончания операции;

- описание события.

3.6. Записи в журналах регистрации событий хранятся в текстовом формате. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей. Для журналов регистрации событий используется кодировка UTF-8. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных. Журналы регистрации событий хранятся на сервере системы управления событиями ИБ не менее одного года.

3.7. В случае выявления инцидентов информационной безопасности система управления событиями ИБ автоматически направляет работникам ЦОК уведомление по электронной почте.

3.8. ЦОК, после получения информации о предполагаемом инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа Работник ЦОК проводит проверку наличия в выявленном факте нарушений.

3.9. Уровень критичности инцидента информационной безопасности оценивается с точки зрения ценности (критичности) информационных активов и/или масштабов затрагиваемых информационных активов, а также от повторяемости инцидентов.

критичный (уровень 5) – неизбежные инциденты, которые приведут к невозможности предоставления услуг, значительным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации;

серьезный (уровень 4) – возможные инциденты, которые приведут к невозможности предоставления услуг, значительным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации;

высокий (уровень 3) – возможные инциденты, которые приведут к существенному ограничению предоставления услуг, существенному ухудшению ситуации или существенным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации;

средний (уровень 2) – вероятные инциденты, которые приведут к ограничению предоставления услуг, ухудшению ситуации или негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации;

низкий (уровень 1) – вероятные инциденты, которые приведут к ограничению предоставления услуг, ухудшению ситуации или негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации;

не критичный (уровень 0) – несущественные инциденты, не оказывающие влияние на электронные информационные ресурсы, информационные системы, сетей телекоммуникаций и других объектов информатизации.

3.10. Информация об обнаруженном инциденте ИБ регистрируется работниками ЦОК в системе регистрации инцидентов.

При регистрации инцидента ИБ указывается следующая информация:

- текущий статус инцидента;
- категория и тип инцидента;
- описание инцидента (внешние проявления и результаты предварительного расследования);
- действия, предпринятые для ликвидации инцидента;
- результаты расследования инцидента, контактная информация работников, участвовавших в расследовании;

3.11. Определение категории и типа инцидента возлагается на работников ЦОК.

3.12. Усиленные требования к мониторингу и выявлению угроз.

Исполнитель обязан использовать комбинированный подход к обнаружению угроз:

- Сигнатурные правила — в формате Sigma, YARA;

- Поведенческие правила и модели — на основе MITRE ATT&CK, собственных корреляций, UEBA;

- Обогащение событий через MISP и аналогичные платформы Threat Intelligence.

3.13. Разработать и внедрить не менее 20 кастомных правил обнаружения под угрозы, характерные для отрасли Заказчика, в первый месяц оказания услуг.

3.14. Обеспечить непрерывную актуализацию правил не реже 1 раза в месяц с обязательной проверкой их эффективности.

3.15. Обязательное наличие резерва сотрудников (не менее двух смен для 24/7 работы).

3.16. Обязательная демонстрация тестового реагирования до подписания договора.

3.17. Резервный канал связи с ЦОК для аварийного взаимодействия с наиболее критичными источниками.

Исполнитель обязан оказывать консультационную и техническую поддержку при организации и использовании резервного канала связи для обеспечения аварийного взаимодействия исключительно с наиболее критичными источниками событий, а также осуществляет его мониторинг в рамках зоны ответственности ЦОК. Перечень критичных источников формируется и согласуется с Заказчиком в течение 10 рабочих дней после подписания договора и подлежит актуализации не реже одного раза в квартал.

3.18 Исполнитель должен в срок не более 5 (дней) календарных дней с даты подписания Договора произвести установку, подключение и настройку технических средств ЦОК к объектам информатизации, информационно-коммуникационной инфраструктуры Заказчика. Факт установки, подключения и настройки оформляется письменным актом между Заказчиком и Исполнителем. Датой начала оказания Услуг ЦОК является следующий день после подписания Акта о подключении услуг между Заказчиком и Исполнителем. Исполнитель вправе досрочно произвести установку, подключение и настройку технических средств ЦОК для оказания Услуг.

3.19. Обязательное наличие резерва сотрудников (не менее двух смен для 24/7 работы).

1. **Уведомление и реагирование на инциденты:**
    1. При обнаружении угроз/инцидентов ИБ и проверки достоверности фактов, ЦОК в течение 15 минут с момента его обнаружения уведомляет об инцидентах информационной безопасности руководителя ЦОК, владельца объекта КВЦО и НКЦ КБ.
    2. Уведомление владельца объекта КВЦО и НКЦКБ об инцидентах ИБ осуществляет ответственный за взаимодействие с АО «ГТС» работник ЦОК (или уполномоченный им работник) по электронной почте и/или через MISP.
    3. Проводить анализ событий ИБ на предмет возможных угроз/инцидентов ИБ посредством встроенных механизмов регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения, средств защиты информации, специализированных средств анализа защищенности информационных систем, а также на основании полученной информации от НКЦКБ осуществляется работником ЦОК.
    4. Время начала реагирования на инцидент ИБ с момента его обнаружения и уведомления уполномоченных работников определяется согласно таблице №1 Приложения №1 к технической спецификации.
    5. Локализация и устранение критичного инцидента начинается в течение 15 минут после его обнаружения, при содействии работников Объекта КВЦО в случае необходимости (на месте исполнителя).

Реагирование на Инцидента ИБ, состоит из следующих этапов:

а) подтверждение/опровержение факта возникновения Инцидента ИБ;

б) классификация инцидента ИБ;

в) подтверждение/корректировка уровня критичности Инцидента ИБ;

г) уточнение дополнительных обстоятельств (деталей) Инцидента ИБ;

д) получение (сбор) доказательств возникновения Инцидента ИБ, обеспечение их сохранности и целостности;

е) минимизация последствий Инцидента ИБ;

ж) информирование и консультирование сотрудников по действиям обнаружения, устранения последствий и предотвращения инцидентов ИБ;

з) переоценка рисков, повлекших возникновение инцидента, актуализация необходимых положений, регламентов, правил ИБ.

4.6. Анализ инцидентов (форензика), в том числе определение источников и причин возникновения инцидентов ИБ, а также оценку их последствий осуществляет работник ЦОК совместно с сотрудниками, осуществляющими техническое обслуживание объекта КВЦО.

4.7. Разграничение зон ответственности на период оказания ЦОК согласно таблице №2 Пр иложения №1 к технической спецификации.

1. **Объем услуг ОЦИБ и требования к отчётности:**
    1. Исполнитель предоставляет услуги ЦОК на основе запроса Заказчика с указанием требуемых технических характеристик.

Количество и технические характеристики источников по подключению к ЦОК согласно таблице №3 Приложения №1 к технической спецификации.

5.2. Исполнитель после подписания Договора, в течении 15 дней совместно с Заказчиком разрабатывают и согласовывают Регламент взаимодействия по реагированию на инциденты и проводит первичное обследование.

Результатом первичного обследования должен являться отчёт, описывающий текущее состояние объектов КВЦО и уточнённые данные.

1. Исполнитель не позднее 15 числа месяца, следующего за отчётным, предоставляет Ежемесячный аналитический отчет с текстовой, табличной и графической (диаграммы, графики) информацией по исполнению Договора, а именно:

- статистические данные по запросам и инцидентам за отчетный период;

- анализ состояния инфраструктуры ИБ;

- перечень проблемных вопросов и рекомендации по их решению и улучшению работы инфраструктуры ИБ;

- актуальные контактные данные специалистов, ответственных за оказание Услуги

1. **Требования к проведению обследования информационной безопасности:**

6.1 Исполнитель в течение 15 дней после подписания договора проводит обследование информационной безопасности (анализ защищенности). **При проведении анализа защищенности сотрудники Исполнителя должны находится на территории Заказчика**.

6.2. Перечень объектов обследования указано в таблице №3 Приложения №1 настоящей технической спецификации.

6.3. **Анализ уязвимостей внешнего сегмента сети.**

- сканирование внешнего периметра сетевой инфраструктуры посредством сертифицированного /специализированного ПО класса сканеры уязвимостей;
- все обнаружения сканера должны быть вручную проверены квалифицированным специалистом Исполнителя с целью валидации уязвимостей;
- внешняя область сканирования - не менее чем 10 объектов (уникальные публичные URL).

6.4. **Анализ уязвимостей внутреннего сегмента сети**.

Выявление уязвимостей внутреннего сегмента сети проводится с периметра локальной сети Заказчика и включает в себя:

- Внутренние URL-адреса должны быть просканированы с использованием VPN-соединения;

- Внутренние информационные системы и сети должны быть просканированы с территории Заказчика;

- Сканер должен произвести инвентаризацию всех обнаруженных хостов (создание карты ИТ-активов);

- Обнаруженные хосты и URL-адреса должны быть проверены в соответствии с картой ИТ активов на предмет открытых уязвимостей.

7. Требования к проведению фишинг-кампании.

Исполнитель должен обеспечить проведение обучающей фишинг-кампании для оценки устойчивости сотрудников к атакам социальной инженерии. Услуга должна включать:

- разработку фишинговых сценариев (письма, ссылки, формы),

- рассылку по согласованному списку сотрудников,

- сбор и обработку результатов (переходы по ссылке, ввод данных и др.).

По итогам фишинг-акции Исполнитель обязан предоставить подробный отчёт, включающий:

- ФИО или идентификатор сотрудников, совершивших переход по ссылке;

- дату и время события;

- IP-адрес устройства;

- информацию о введённых данных (если применимо);

- уровень риска.

Также должна быть предусмотрена онлайн-панель или выгрузка, позволяющая Заказчику самостоятельно отслеживать результаты кампании в реальном времени или по завершении. Все действия проводятся в контролируемой среде без угрозы для рабочих систем.

8. Требования к услуге защиты от DDoS-атак.

Исполнитель обязан обеспечить выявление и автоматическую фильтрацию DoS/DDoS-атак на уровне телекоммуникационного провайдера — до поступления трафика в сеть Заказчика. Решение должно включать:

- Автоматическую очистку вредоносного трафика до точки входа в инфраструктуру;
- Круглосуточный мониторинг и реагирование на аномалии, превышающие порог активности;
- Личный кабинет Заказчика с отображением всех зафиксированных атак: дата, время, география источников, объём (Gbps), интенсивность (pps), вектор (SYN Flood, UDP Flood и т.д.);
- Уведомление в режиме реального времени о факте атаки через e-mail и/или альтернативные каналы (мессенджер и т.д.);
- Формирование отчётов с полной статистикой по инцидентам за произвольный период (включая экспорт в формате PDF/Excel);
- Обязательная передача сведений об инцидентах в Национальный координационный центр информационной безопасности РК в круглосуточном режиме, при выявлении событий, относящихся к категории ИБ-инцидентов.

Система должна обеспечивать отказоустойчивость и минимальное влияние на легитимный трафик.

9. Дополнительные услуги

9.1. Исполнитель 1 раз в год с соответствующим программным обеспечением проводит анализ исходного кода информационной системы «Заказчика» с предоставлением рекомендации и отчета по исправлению потенциальных уязвимостей, ошибок, которые могут стать причиной сбоев, потери данных или несанкционированного доступа к системе.

9.2. Программное обеспечение для анализа исходного кода реализует следующие методы анализа защищенности информационной системы: статический (Static Application Security Testing, SAST); динамический (Dynamic Application Security Testing, DAST, метод черного ящика); анализ сторонних компонентов; анализ конфигурационных файлов информационной системы.

9.3. Программное обеспечение для анализа исходного кода учитывает результаты предыдущих анализов информационной системы и выполняет анализ в первую очередь для фрагментов кода, которые были изменены с момента последнего анализа, остальной код анализируется, если на него влияет изменение.

9.4. Программное обеспечение для анализа исходного кода обеспечивает возможность создания отчетов на основе встроенных шаблонов, включая следующие типы отчетов: отчет автопроверки; отчет OWASP Top 10 2021; отчет OWASP Mobile Top 10 2024 Final Release; отчет SANS Top 25; отчет PCI DSS 4.0.1; отчет NIST 800-53 (revision 5).

9.5. Программное обеспечение для анализа исходного кода обеспечивает возможность редактирования базы пользовательских сигнатур уязвимостей.

10. Требования к соблюдению законодательства Республики Казахстан

10.1 Услуги должны оказываться в соответствии со статьей 7-5 Закона Республики Казахстан «О кибербезопасности» от 24 ноября 2015 года № 418-V (далее – Закон), а также Постановлением Правительства РК от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» и другими действующими стандартами Республики Казахстан. В случае отсутствия казахстанских стандартов допускается использование иных стандартов и лучших международных практик в информационной безопасности - ISO/IEC 27001 в порядке установленным законодательством Республики Казахстан. Также услуги должны оказываться в соответствии с требованиями к использованию единого шлюза доступа к интернету. а также в соответствии с внутренними нормативными документами Заказчика.

10.2. Хранение данных Заказчика осуществляется на ресурсах, которые располагаются на территории Республики Казахстан (требования Закона Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V, Закон Республики Казахстан «О доступе к информации» от 16 ноября 2015 года № 401-V, Постановления Правительства РК № 832 от 20.12.2016 года «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»).

10.3. Взаимодействие ЦОК с Национальным координационным центром кибербезопасности осуществляется в соответствии с Законом.

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 27001-2015	384044	Национальный стандарт Республики Казахстан	Информационная технология методы и средства обеспечения безопасности системы менеджмента информационной безопасностью требования	Настоящий стандарт устанавливает требования к разработке, внедрению, поддержанию в рабочем состоянии и непрерывному совершенствованию системы менеджмента информационной безопасностью организации в контексте существующих бизнес рисков организации.	Нет ()	68	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

Приложение

Приложение 1 к ТС каз .docx

Приложение 1 к ТС.docx

Подписал Дубовая Юлия Анатольевна

Дата подписания 20.11.2026