ТЕХНИКАЛЫҚ СИПАТТАМА

1024501 сатып алу бойынша
Төмендету бойынша ашық тендер тәсілімен

Лот № 1 (98 У, 3743651) Менеджмент жүйесінің сертификаттауына әзірлеу, енгізу, дайындау бойынша кеңестік қызметтер

Тапсырыс беруші: АО ФНБ "Самрук-Казына"

Ұйымдастырушы: "Самрук-Қазына Бизнес Сервис" ЖШС

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	98 У
Атауы және қысқаша сипаттамасы	Менеджмент жүйесінің сертификаттауына әзірлеу, енгізу, дайындау бойынша кеңестік қызметтер, Менеджмент жүйесінің сертификаттауына әзірлеу, енгізу, дайындау бойынша кеңестік қызметтер
Қосымша сипаттама	ISO/IEC 27001:2022 сәйкес ақпараттық қауіпсіздікті басқару және сәулет жүйесін кешенді дамыту
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Астана қ., "Нұра" ауданы, ул. Сығанақ, строение 17/10
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап (қоса алғанда) 12.2024 дейін.
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 100%, Соңғы төлем - 0%

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

ТЕХНИКАЛЫҚ ЕРЕКШЕЛІК

1. ЖАЛПЫ АҚПАРАТ:

- Жобаны іске асыру мерзімі: 2024 жылғы 31 желтоқсанға дейін
- Жобаның басталу күні: [_]
- Жобаның аяқталу мерзімі: [_]

2. КІРІСПЕ

Бұл құжатта ISO/IEC 27001:2022 стандартының талаптарына сәйкес ақпараттық қауіпсіздікті басқару жүйесін (бұдан әрі – АҚБЖ) енгізу және сүйемелдеу бойынша жобалау жұмыстарын орындауға техникалық ерекшелік келтірілген.

Жобада АТ-инфрақұрылым жұмысының барлық бағыттары бойынша кешенді іс-шараларды қарастыру қажет. Ағымдағы жағдайға талдау жүргізу, кемшіліктер мен проблемалық мәселелерді анықтау, орындау үшін қажетті мақсаттарды, іс-қимылдарды айқындау, АТ және АҚ сәулетін көрсету және ұйымдастыру талап етіледі. жабдықтар, жүйелер және бағдарламалық қамтамасыз етулер бойынша талдау және ұсынымдар беру. Сонымен қатар әрбір енгізілген процесті құжатпен регламенттеу, жалпы тұжырымдаманы сипаттау талап етіледі.

3. ТАЛАПТАР

Жұмыс регламенттерін әзірлеу және олардың әрқайсысында жұмыс тәртібін, құрылыс архитектурасын, жүйелердің физикалық орналасуын айқындау, сондай-ақ ақпаратты сақтау тәртібін айқындау талап етіледі.

Анықталған кемшіліктер мен проблемаларды ескере отырып, АТ-инфрақұрылымының жұмысын ретке келтіру жөнінде талдау және ұсынымдар беру, ақпараттың қозғалу жолдарын, деректерді беру мен қабылдаудың кіру және шығу жолдарын талдау, жабдықтар мен компьютерлердің орналасуын оңтайландыру, осал жерлерді анықтау және оларды жою жөнінде шаралар әзірлеу, мынадай іс-шараларды орындау қажет:

1. Барлық бар проблемалар мен кемшіліктерді анықтау үшін ағымдағы АТ-инфрақұрылымына толық тексеру және талдау жүргізу.
2. Ағымдағы процестерді және ұйымның желісі ішінде ақпараттың қозғалу жолдарын құжаттандыру.
3. Ақпаратты беру мен қабылдаудың кіру және шығу жолдарын қоса алғанда, деректер ағынын картаға түсіру.
4. Ақпарат қозғалысының ағымдағы жолдарындағы проблемалық учаскелер мен әлеуетті іркіліс нүктелерін анықтау.
5. Серверлердің, желілік құрылғылардың және жұмыс станцияларының ағымдағы орналасуына талдау жүргізу.
6. Өнімділікті жақсарту және қызмет көрсетуді жеңілдету үшін жабдықтың оңтайлы орналасуын анықтау.
7. Аса маңызды осалдықтарды анықтау және оларды жою бойынша жоспар әзірлеу.
8. Қорғау құралдарын, басып кіруді анықтау және болдырмау жүйесін орнату және баптау бойынша талдау және ұсынымдар беру.
9. АТ-инфрақұрылымының жай-күйі мен өнімділігін қадағалау үшін мониторинг жүйелерін енгізу.
10. Барлық өзгерістер мен жаңа процестер бойынша толық құжаттама жасау.
11. Жұмыста ең аз іркілістермен АТ-инфрақұрылымының жаңа конфигурациясына біртіндеп көшуді қамтамасыз етуге талдау және ұсынымдар беру.
    1. Бұл ретте мыналарды өндіру қажет:
12. АҚ саласындағы әлемдік практикалар мен стандарттарды есепке алу (мысалы, NIST, ISO/IEC 27001).
13. Ақпараттың құпиялылығына, тұтастығына және қолжетімділігіне қойылатын талаптарды айқындау.
14. Жаңа архитектураға қойылатын техникалық және функционалдық талаптарды әзірлеу.
15. Пайдаланылатын технологиялар мен шешімдерді бағалау.
16. Шешімдерді түйінді параметрлер (қауіпсіздік, өнімділік, құн) бойынша салыстырмалы талдау.
17. Ұйымның бизнес-процестерінің ерекшелігін ескеретін желі мен жүйе архитектурасын құру бойынша оңтайлы шешімдерді таңдау.
18. Архитектура бойынша шешімдерді кезең-кезеңмен енгізу жоспарын әзірлеу.
19. Архитектура бойынша жаңа шешімдерді қолданыстағы АҚ-инфрақұрылыммен ықпалдастыруға талдау және ұсынымдар беру.
20. Енгізудің барлық кезеңдерінде бизнес-процестердің үздіксіздігін қамтамасыз ету жөнінде талдау жүргізу және ұсынымдар беру.

ISO/IEC 27001: 2022 сәйкес ақпараттық қауіпсіздікті басқару және сәулет жүйесін кешенді әзірлеу 2 кезеңде көзделеді, бұл ретте қызметтер қатар көрсетілуі мүмкін:

кезең №	**Қызметтер құрамы**	**Орындау мерзімі**	**Төлем мерзімі мен мөлшері**
1	Талаптарды орындау: 1. Желілік жабдыққа 2. Пошта қызметімен 3. Веб-сайтпен 4. Серверлік инфрақұрылым мен	2024 жылғы 15 желтоқсан	15 күнтізбелік мерзім ішінде орындалғаннан кейінгі күнде р 1 кезең 50 мөлшерінде сом аның (елу) % шарт

2	Талаптарды орындау: 1. электрондық құжат айналымы жүйесімен жұмыс 2. ақпараттық қауіпсіздік жүйелерімен жұмыс 3. интернетпен жұмыс 4. IP-телефониямен жұмыс	2024 жылғы 15 желтоқсан	15 күнтізбелік мерзім ішінде орындалғаннан кейінгі күнде р 2 кезең 50 мөлшерінде сом аның (елу) % шарт

АҚ жүйелерімен жұмыс істеу нұсқаулығы

Төменде көрсетілген кем дегенде базалық талаптарды орындау қажет:

1 КЕЗЕҢ

- ***Желілік жабдыққа қойылатын талаптар***

1. ***Жоспарлау және жобалау****:*
2. *Қауіпсіздік мақсатын анықтау және желілік ортаға қойылатын талаптар.*
3. *Трафиктің бір түріне рұқсат беру немесе тыйым салу туралы шешім.*
4. *Firewall және басқа да маңызды желілік элементтердің орналасуын ескере отырып, желілік топология жоспарын құру.*
5. ***Мониторинг және басқару:***
6. *Firewall арқылы трафик пен қауіпсіздік оқиғаларын тұрақты бақылау бойынша талдау және ұсыныстар беру.*
7. *Ауытқулар мен ықтимал қауіптерді анықтау үшін логтар мен есептерге тұрақты талдау және ұсыныстар беру.*
8. ***Қызмет көрсету және жаңарту:***
9. *Желідегі өзгерістер мен талаптарға сәйкес ережелер мен саясаттарды үнемі жаңартып отыру бойынша талдау және ұсыныстар беру.*
10. *Firewall өндірушісінен қауіпсіздік жаңартулары мен түзетулерін орнату бойынша талдау және ұсыныстар беру.*
11. ***Firewall үшін желілік ережелер:***
12. *желінің әртүрлі бөліктерін бөлу және оқшаулау үшін VLANs және аймақтық саясаттарды пайдалану бойынша талдау және ұсыныстар беру.*
13. *басқару аймақтары мен деректер сияқты ішкі желілерді қоғамдық желілерден қорғау бойынша талдау және ұсыныстар беру.*
14. ***Архитектуралық орналасуы***
15. *Орын*

Пошта сервисімен жұмыс істеу талаптары

1) Жоспарлау және жобалау:

- *Пошта қызметіне қойылатын талаптарды анықтау, соның ішінде пошта көлемі, пайдаланушылар саны, басқа қызметтермен интеграция және қауіпсіздік талаптары.*

2) Қауіпсіздікті орнату:

- *Деректерді беру үшін шифрлауды пайдалану бойынша талдау және ұсыныстар беру және сақталған поштаны шифрлау.*
- *Пайдаланушылардың аутентификациясы мен авторизациясын орнату бойынша талдау және ұсыныстар беру.*
- *Кіріс және шығыс пошта үшін спам сүзгілерін және антивирустық қорғауды пайдалану бойынша талдау және ұсыныстар беру.*
- *Пошта жәшіктеріне кіру үшін екі факторлы аутентификация бойынша талдау және ұсыныстар беру.*

3) Мониторинг және басқару:

- *Пошта серверінің және пайдаланушылардың есептік жазбаларының жұмысын мониторингілеу бойынша талдау және ұсынымдар беру.*
- *Проблемалар мен күдікті белсенділік туралы хабарлау үшін хабарлау жүйесін баптау бойынша талдау және ұсынымдар беру.*
- *Аномалияларды және хакерлік әрекеттерді анықтау үшін сервер логтарына талдау және тұрақты талдау бойынша ұсынымдар беру.*

4) Қызмет көрсету және жаңарту:

- *Пошта серверінің БҚ-сын тұрақты жаңарту және қауіпсіздік жаңартуларын қолдану бойынша талдау және ұсынымдар беру.*
- *Пошта жәшіктерінің тұрақты резервтік көшірмелерін және сервер конфигурацияларын жүзеге асыру бойынша талдау және ұсынымдар беру.*
- ***Пошта сервисінің архитектуралық орналасуында мынадай компоненттер қарастырылуы тиіс:** сыртқы Firewall, пошта шлюзінің, пошта серверінің, аутентификация серверінің жұмысы, резервтік серверлер мен репликацияларды есепке алу.*

- ***<u>Веб-сайтпен жұмыс істеу талаптары</u>***

1) Жүктемені бөлуді, мәліметтер базасын және қолданбалы серверлерді қоса алғанда, веб-сайттың архитектурасын әзірлеу.

2) Веб-сайттың архитектуралық орналасуы:

Келесі компоненттердің дұрыс орналасуын ескеру қажет:

- *Сыртқы Firewall*
- *Веб-сервер*
- *Қосымшалар сервері*
- *Мәліметтер базасы*
- *Load Balancer (Жүктемені теңестіруші)*
- *WAF (Web Application Firewall)*

3) Веб-сайттың жұмысын ұйымдастыру тәртібі, конфигурациясы.

- ***<u>Серверлік инфрақұрылыммен жұмыс істеу талаптары</u>***

1) Жоспарлау және жобалау:

- *Серверлік инфрақұрылымға қойылатын талаптарды анықтау (есептеу қуаты, сақтау көлемі, желінің өткізу қабілеті және т.б.).*
- *Әзірлеу ауқымдылықты, ақауларға төзімділікті және қауіпсіздікті ескере отырып, серверлік инфрақұрылым архитектурасы.*

2) Серверлерді орнату және конфигурациялау:

- *Серверлердің желілік қосылымдарын (LAN, SAN) баптау және аса маңызды қосылыстарды резервтеуді қамтамасыз ету бойынша талдау және ұсынымдар беру.*
- *Серверлерде операциялық жүйелер мен қажетті бағдарламалық қамтылымдарды орнату және баптау бойынша талдау және ұсынымдар беру.*

3) Логикалық конфигурация және желілік байланыстар:

- *IP-адрестеуді, VLANs және серверлер мен желілік жабдықтар үшін маршруттауды теңшеу бойынша талдау және ұсынымдар беру.*
- *Виртуализация жүйесін баптау бойынша талдау және ұсынымдар беру.*
- *Виртуализация жүйесін баптау бойынша талдау және ұсынымдар беру.*
- *Деректерді сақтау және деректерді резервтеуді қамтамасыз ету жүйесін баптау бойынша талдау және ұсынымдар беру.*

4) Қауіпсіздікті және мониторингті қамтамасыз ету:

- *Серверлік инфрақұрылымды қорғау үшін firewall және басып кіруді болдырмау жүйесін (IDS/IPS) баптау бойынша талдау және ұсынымдар беру.*
- *Транзиттегі және тыныштықтағы деректерді шифрлауды қосу бойынша талдау және ұсынымдар беру.*
- *Серверлер мен желілік жабдықтардың жай-күйін қадағалау үшін мониторинг және логинг жүйелерін баптау.*

5) Серверлік инфрақұрылымның архитектуралық орналасуы:

- ***Физикалық орналасу сипаттамасы:***
- *Өнімділікті талдауды қоса алғанда, қолданыстағы серверлік және желілік инфрақұрылымды талдау.*
- *Істен шығуға төзімділікті ескере отырып, жабдықтың қолжетімділігін қамтамасыз етуге арналған орын.*
- ***Логикалық орналасу және қосылу сипаттамасы:***

- Желілік жабдық:

- *Серверлерді қосуға және сыртқы желілермен байланыс орнатуға арналған қосқыштар мен маршрутизаторлар.*
- *Виртуалды жергілікті желілер (VLAN) трафикті сегменттеу және қауіпсіздікті жақсарту.*

- Серверлер және сақтау жүйелері:

- *Функциялары бойынша логикалық топтарға бөлінген серверлер.*
- *Деректерді орталықтандырылған сақтау және резервтеу үшін сақтау жүйелері.*
- ***Брондау және ақауларға төзімділік:***
- *Желілік ақауларға төзімділікті қамтамасыз ету үшін коммутаторлар мен маршрутизаторлардың орналасуы мен қайталануы бойынша талдау және ұсыныстар беру.*
- *Серверлердің қолжетімділігін арттыру үшін серверлерді кластерлеу және жүктемені теңестіру бойынша талдау және ұсынымдар беру.*

2 КЕЗЕҢ

- ***Электрондық құжат айналымы жүйесімен жұмыс істеу талаптары***

1) Жоспарлау және жобалау:

- *ЭҚА мақсаттары мен талаптарын, соның ішінде құжат айналымы көлемін, пайдаланушылар санын, басқа жүйелермен интеграцияны және қауіпсіздік талаптарын анықтау.*
- *Масштабталуды, ақауларға төзімділікті және қауіпсіздікті ескере отырып, ЭҚА архитектурасын әзірлеу.*

2) Физикалық және логикалық орналастыруды дайындау:

- *Қолданбалы серверлерді, дерекқорларды және деректерді сақтау жүйелерін қоса алғанда, ЭҚА орналастыру үшін серверлік инфрақұрылымды анықтау.*
- *Қамтамасыз ету жоғары қолжетімділік пен ақауларға төзімділік үшін қажетті желілік қосылыстар және резервтеу.*

3) Орнату және конфигурация:

- *ЭҚА үшін қолданбалы серверлерді, дерекқорды және деректерді сақтау жүйелерін орнату.*
- *Желілік қосылымдарды орнату және қамтамасыз ету маңызды қосылымдарды брондау.*
- *Пайдаланушыларды басқаруды, қол жеткізу құқығын және басқа жүйелермен интеграцияны қоса алғанда, ЭҚА орнату және баптау.*

4) Қауіпсіздікті баптау:

- *Транзитте және тыныштықта деректерді шифрлау.*
- *Басып кірудің алдын алу жүйелері.*

5) Басқару мен мониторингті қамтамасыз ету:

- *ЭҚА және пайдаланушы есептік жазба жұмысын бақылауды орнату.*
- *мәселелер мен күдікті әрекеттер туралы хабарлау үшін ескерту жүйесін орнату.*

6) Электрондық құжат айналымы жүйесінің архитектуралық орналасуы:

- *Физикалық және логикалық орналастыру*
- *Компоненттердің архитектуралық орналасуы: Frontend (веб-серверлер және қосымшалар серверлері); Backend (мәліметтер базасы және сақтау серверлері). Жұмысты ұйымдастыруды таратып жазу.*

<u>Ақпараттық қауіпсіздік жүйелерімен жұмыс істеу талаптары</u>

1) Жоспарлау және жобалау

- *Негізгі АҚ жүйелерінің анықтамасы: firewall, IDS/IPS, антивирус, DLP, SIEM, қол жеткізуді басқару және деректерді шифрлау жүйелері.*

2) АҚ жүйелерін конфигурациялау және баптау

- *Қауіпсіздік оқиғаларын орталықтандырылған бақылау және корреляциялау үшін SIEM орнату*
- *Маңызды оқиғалар мен қауіпсіздіктің бұзылуы туралы автоматтандырылған ескертулерді орнату.*

3) Архитектуралық орналасуы

- *Қолжетімділікті шектеу үшін қорғалған желіге орналастыру, осы процесті ұйымдастырудың сипаттамасы және іске асырылуы.*
- *Оқиғаларды орталықтандырылған басқару және корреляциялау үшін SIEM-мен барлық АҚ жүйесін біріктіру.*
- *Кешенді қорғауды қамтамасыз ету үшін желі және соңғы құрылғылар деңгейінде қауіпсіздік саясатын енгізу.*

4) Мониторинг орталығы

- *оқиғаларды бақылау, жедел әрекет ету үшін ұйым шеңберінде бірыңғай автоматтандырылған мониторинг орталығын қалыптастыру бойынша талдау және ұсынымдар беру.*

IP-телефониямен жұмыс істеу талаптары

1) Орнату және конфигурация

- *IP телефония серверлерінің тәртібі мен ұйымдастырылуы және оларды желіге қосу.*
- *SIP (Session Initiation Protocol) серверлерін қоса алғанда, IP телефония бағдарламалық қамтылымын баптау және пайдаланушы есептік жазбасын баптау.*

2) Логикалық орналастыру және өзара әрекеттесу

- *IP-телефондарды және басқа құрылғыларды желіге қосу бойынша ұсынымдарды талдау және беру, баптау және конфигурациялау тәртібі.*
- *Байланыс қауіпсіздігі мен сапасын қамтамасыз ету үшін дауыстық және трафик деректерін бөлуді ескере отырып, VLAN орнату бойынша талдау және ұсыныстар беру.*
- *Бизнес-процестерді жақсарту үшін IP-телефония жүйелерін қолданыстағы АТ-жүйелермен (CRM, ERP) интеграциялау бойынша талдау және ұсыныстар беру.*

- ***Интернетпен жұмыс істеу талаптары***

- *Барлық қажетті компоненттерді ескере отырып, желі архитектурасын әзірлеу: маршрутизаторлар, қосқыштар, кіру нүктелері, firewall және басқа қауіпсіздік жүйелері.*
- *Кіруді басқару және резервтік қуаты бар сервер бөлмесінде желілік жабдықты физикалық орналастыруды орнату.*
- *Қауіпсіз қосылымды орнатуды ескере отырып, интернет-провайдерге қосылу.*
- *Интернетке шығатын жүйелерді анықтау.*
- *Қандай порттарды пайдалану керек*

- ***Бағдарламалық қамтылыммен (БҚ) жұмыс істеу талаптары***

- *Жаңа / жаңартылған БҚ-ны қабылдау тәртібін анықтау.*
- *Ақпараттық қауіпсіздікке қойылатын талаптарды анықтау: деректердің қауіпсіздігін және рұқсатсыз кіруден қорғауды қамтамасыз ету жөніндегі шаралардың сипаттамасы, жүйенің деректердің жүктемесі мен көлемін ұлғайтуға бейімделу қабілеті, ақаулар болған жағдайда жүйенің үздіксіз жұмысын қамтамасыз ету тетіктері.*
- *Қабылдау өлшемшарттарын анықтау, тестілеудің қандай нәтижелері БҚ қабылдау үшін негіз болады, қандай жағдайда және қандай мәліметтерде тестілеу жүргізіледі.*
- *Әзірленуі тиіс құжаттама түрлерін тізімдеу (пайдаланушы құжаттамасы, техникалық құжаттама және т.б.).*

4. ҚОРЫТЫНДЫ ҚҰЖАТТАР

- **Жоғарыда көрсетілген барлық жұмыстардың аяқталуы бойынша жай-күйін белгілей отырып, АТ-инфрақұрылымының әрбір бағыты бойынша ақпараттық қауіпсіздік архитектурасын құру және қағидалары жөніндегі әдістеме.**
- **Әдістемеде осы қатерлерді қорғауды, ден қою шараларын және жоюды ескере отырып, анықталған және бар қауіптер кезең-кезеңмен нұсқаулықпен, жауапкершілікті түсіндірумен және бөлумен қамтылуға тиіс.**

Мазмұны:

Дұрыс желі архитектурасы.

Желі компоненттерін орнату.

Ақпараттық қауіпсіздік бойынша бағдарламалық шешімдерді енгізу бойынша ұсыныстар.

Барлық компоненттерді біріктіру және өзара әрекеттесу бойынша ұсыныстар.

- **Әр процесс бойынша құжаттар**

Мазмұны:

Процестердің сипаттамасы.

Саясат және рәсімдер.

Орнату және пайдалану нұсқаулары.

Оқиғаларға жауап беру жоспары.

Қызметкерлерді оқыту және хабардар ету құжаттамасы.

Қол қойған	Байзаков Тимур Еркамысович
Қол қойылған күні	28.08.2024

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1024501
способом Открытый тендер на понижение

Лот № 1 (98 У, 3743651) Услуги консультационные по разработке, внедрению, подготовке к сертификации систем менеджмента

Заказчик: Акционерное общество «Фонд национального благосостояния «Самрук-Қазына»

Организатор: Товарищество с ограниченной ответственностью "Самрук-Казына Бизнес Сервис"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	98 У
Наименование и краткая характеристика	Услуги консультационные по разработке, внедрению, подготовке к сертификации систем менеджмента, Услуги консультационные по разработке, внедрению, подготовке к сертификации систем менеджмента
Дополнительная характеристика	Комплексная разработка системы управления и архитектуры информационной безопасности в соответствии с ISO/IEC 27001:2022
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Астана, район "Нұра", ул. Сығанақ, строение 17/10
Условия поставки	-
Срок поставки	С даты подписания договора по (включительно) 12.2024
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 100%, Окончательный платеж - 0%

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

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

на оказание услуг по комплексной разработке системы управления и архитектуры информационной безопасности в соответствии с ISO/IEC 27001:2022

1. ОБЩАЯ ИНФОРМАЦИЯ:

- Срок реализации проекта: до 31.12.2024
- Дата начала проекта: [_]
- Срок завершения проекта: [_]

2. ВВЕДЕНИЕ

В данном документе приведена техническая спецификация на выполнение проектных работ по внедрению и сопровождению системы управления информационной безопасностью (далее – СУИБ) в соответствии с требованиями стандарта ISO/IEC 2700 1:2022.

В проекте необходимо предусмотреть комплексные мероприятия по всем направлениям работы ИТ-инфраструктуры. Требуется проведение анализа текущей ситуации, выявление недостатков и проблемных вопросов, определить цели, действия необходимые для исполнения, отобразить и организовать ИТ и ИБ архитектуру. провести анализ и выдачу рекомендаций по оборудованиям, системам и программным обеспечениям. Вместе с тем, требуется документально регламентировать каждый внедренный процесс, отрисовать общую концепцию.

3. ТРЕБОВАНИЯ

Требуется разработать регламенты работы и в каждом из них определить порядок работы, архитектуру построения, физическое размещение систем, а также определить порядок хранения информации.

Провести анализ и выдачу рекомендаций по налаживанию работы ИТ-инфраструктуры, учитывая выявленные недочеты и проблемы, проанализировать пути передвижения информации, входы и выходы передачи и приема данных, оптимизировать расположение оборудования и компьютеров, выявить уязвимые места и разработать меры по их устранению, выполнить мероприятия:

1. Провести полную проверку и анализ текущей ИТ-инфраструктуры для выявления всех существующих проблем и недочетов.
1. Задокументировать текущие процессы и пути передвижения информации внутри сети организации.
1. Картографировать потоки данных, включая входы и выходы передачи и приема информации.
1. Определить проблемные участки и потенциальные точки сбоя в текущих путях передвижения информации.
1. Провести анализ текущего расположения серверов, сетевых устройств и рабочих станций.
1. Определить оптимальное расположение оборудования для улучшения производительности и упрощения обслуживания.
2. Определить наиболее критические уязвимости и разработать план по их устранению.

3. Провести анализ и выдачу рекомендаций по установке и настройке средств защиты, системы обнаружения и предотвращения вторжений.
4. Внедрить системы мониторинга для отслеживания состояния и производительности ИТ-инфраструктуры.
5. Создать подробную документацию по всем изменениям и новым процессам.
6. Провести анализ и выдачу рекомендаций обеспечению плавного перехода к новой конфигурации ИТ-инфраструктуры с минимальными перебоями в работе.

При этом необходимо произвести:

1. Учет мировых практик и стандартов в области ИБ (например, NIST, ISO/IEC 27001).
2. Определение требований к конфиденциальности, целостности и доступности информации.
3. Разработку технических и функциональных требований к новой архитектуре.
4. Оценка используемых технологий и решений.
5. Проведение сравнительного анализа решений по ключевым параметрам (безопасность, производительность, стоимость).
6. Выбор оптимальных решений по построению сети и архитектуры системы, учитывающих специфику бизнес-процессов организации.
7. Разработка плана поэтапного внедрения решений по архитектуре.
8. Провести анализ и выдачу рекомендаций интеграции новых решений по архитектуре с существующей ИБ-инфраструктурой.
9. Провести анализ и выдачу рекомендаций по обеспечению непрерывности бизнес-процессов на всех этапах внедрения.

Комплексная разработка системы управления и архитектуры информационной безопасности в соответствии с ISO/IEC 27001:2022 предусматривается в 2 этапа, при этом услуги могут оказываться параллельно:

№ этапа	Состав услуг	Срок исполнения	Срок и размер оплаты
	1. К сетевому оборудованию 2. С почтовым сервисом 3. С веб-сайтом		В течение 15 календарных дней с момента выполнения

1	4. С серверной инфраструктурой Исполнение требований:	15 декабря 2024 года	Этапа 1 в размере 50 (пятидесяти) % от суммы договора
2	1. работы с системой электронного документооборота 2. работы с системами информационной безопасности 3. работы с интернетом 4. работы с IP-телефонией Исполнение требований:	31 декабря 2024 года	В течение 15 календарных дней с момента выполнения Этапа 2 в размере 50 (пятидесяти) % от суммы договора

Инструкция работы с системами ИБ

Необходимые выполнить по меньшей мере базовые требования, которые указаны ниже:

-

1 ЭТАП:

-

Требования к сетевому оборудованию

- ***Планирование и проектирование**:*
    1. *Определение цели безопасности и требования для сетевой среды.*
    2. *Решение о том, какие типы трафика должны быть разрешены или запрещены.*
    3. *Создание плана сетевой топологии с учетом местоположения firewall и других критически важных элементов сети.*
- ***Мониторинг и управление**:*
    1. *Провести анализ и выдачу рекомендаций по постоянному мониторингу трафика и событий безопасности через firewall.*
    2. *Провести анализ и выдачу рекомендаций по регулярному анализу логов и отчетов для выявления аномалий и возможных угроз.*
- ***Обслуживание и обновление**:*
    1. *Провести анализ и выдачу рекомендаций по регулярному обновлению правил и политик в соответствии с изменениями в сети и требованиями.*
    2. *Провести анализ и выдачу рекомендаций по установке обновлений безопасности и исправлений от производителя firewall.*
- ***Сетевые правила для firewall:***
    1. *Провести анализ и выдачу рекомендаций по использованию VLANs и зональных политик для разделения и изоляции разных частей сети.*
    2. *Провести анализ и выдачу рекомендаций по защите внутренних сетей, такие как зоны управления и данные, от общедоступных сетей.*

5. Архитектурное расположение

Место

Требования работы с почтовым сервисом

- ***Планирование и проектирование**:*
    1. *Определение требований к почтовому сервису, включая объем почты, количество пользователей, интеграцию с другими сервисами и требования к безопасности.*
- ***Настройка безопасности*:**
    1. *Провести анализ и выдачу рекомендаций по использованию шифрования для передачи данных и шифрование хранимой почты.*
    2. *Провести анализ и выдачу рекомендаций по настройке аутентификации и авторизации пользователей.*
    3. *Провести анализ и выдачу рекомендаций по использованию фильтров спама и антивирусную защиту для входящей и исходящей почты.*
    4. *Провести анализ и выдачу рекомендаций по двухфакторной аутентификации для доступа к почтовым ящикам.*
- ***Мониторинг и управление**:*

1. *Провести анализ и выдачу рекомендаций по мониторингу работы почтового сервера и учетных записей пользователей.*
2. *Провести анализ и выдачу рекомендаций по настройке системы оповещения для уведомления о проблемах и подозрительной активности.*
3. *Провести анализ и выдачу рекомендаций по регулярному анализу логов сервера для выявления аномалий и попыток взлома.*

- ***Обслуживание и обновление**:*
  1. *Провести анализ и выдачу рекомендаций по регулярному обновлению ПО почтового сервера и применение обновлений безопасности.*
  2. *Провести анализ и выдачу рекомендаций по осуществлению регулярных резервных копий почтовых ящиков и конфигураций сервера.*

***5. Архитектурное расположение почтового сервиса должна предусматривать следующие компоненты: внешний Firewall**, работу почтового шлюза, почтового сервера*

сервера аутентификации, учет резервных серверов и репликации.

Требования работы с веб-сайтом

1. ***Разработка архитектуры веб-сайта, включая распределение нагрузки, базы данных и серверы приложений.***
2. ***Архитектурное расположение веб-сайта:***

Необходимо учесть корректное расположение следующих компонентов:

1. *Внешний Firewall*
2. *Веб-сервер*
3. *Сервер приложений*
4. *База данных*
5. *Load Balancer (Балансировщик нагрузки)*
6. *WAF (Web Application Firewall)*

3. Порядок организации работы веб-сайта, конфигурация.

Требования работы с серверной инфраструктурой

- ***Планирование и проектирование**:*

1. *Определение требований к серверной инфраструктуре (вычислительные мощности, объем хранилища, пропускная способность сети и т.д.).*
2. *Разработка архитектуру серверной инфраструктуры с учетом масштабируемости, отказоустойчивости и безопасности.*

- ***Установка и конфигурация серверов**:*
  1. *Провести анализ и выдачу рекомендаций по настройке сетевых подключений серверов (LAN, SAN) и обеспечению резервирования критически важных соединений.*
  2. *Провести анализ и выдачу рекомендаций по установке и настройка операционных систем и необходимых программных обеспечений на серверах.*
- ***Логическая конфигурация и сетевые подключения**:*
  1. *Провести анализ и выдачу рекомендаций по настройке IP-адресации, VLANs и маршрутизации для серверов и сетевого оборудования.*
  2. *Провести анализ и выдачу рекомендаций по настройке системы виртуализации.*
  3. *Провести анализ и выдачу рекомендаций по настройке системы виртуализации.*
  4. *Провести анализ и выдачу рекомендаций по настройке системы хранения данных и обеспечения резервирования данных.*
- ***Обеспечение безопасности и мониторинга**:*
  1. *Провести анализ и выдачу рекомендаций по настройке firewall и системы предотвращения вторжений (IDS/IPS) для защиты серверной инфраструктуры*
  2. *Провести анализ и выдачу рекомендаций по включению шифрования данных в транзите и в покое.*
  3. *Настройте системы мониторинга и логирования для отслеживания состояния серверов и сетевого оборудования.*

5. Архитектурное расположение серверной инфраструктуры:

***Описание Физического расположения**:*

- *Анализ существующей серверной и сетевой инфраструктуры, включая анализ производительности.*
- *Расположение для обеспечения доступности оборудования с учетом отказоустойчивости.*

- ***Описание логического расположения и соединения**:*

***- Сетевое оборудование**:*

- *Коммутаторы и маршрутизаторы для соединения серверов и обеспечения связи с внешними сетями.*
- *Виртуальные локальные сети (VLAN) для сегментации трафика и повышения безопасности.*

***- Серверы и системы хранения**:*

- *Серверы, разделенные на логические группы по функциям.*

- *Системы хранения данных для централизованного хранения и резервирования данных.*

- ***Резервирование и отказоустойчивость:***
  1. *Провести анализ и выдачу рекомендаций по расположению и дублированию коммутаторов и маршрутизаторов для обеспечения сетевой отказоустойчивости.*
  - *Провести анализ и выдачу рекомендаций по кластеризации серверов и балансировки нагрузки для повышения доступности сервисов.*

---

2 ЭТАП

Требования работы с системой электронного документооборота

- ***Планирование и проектирование****:*
  1. *Определение целей и требований к СЭД, включая объем документооборота, количество пользователей, интеграцию с другими системами и требования к безопасности.*
  2. *Разработка архитектуры СЭД с учетом масштабируемости, отказоустойчивости и безопасности.*
- ***Подготовка физического и логического размещения****:*
  1. *Определение серверной инфраструктуры для размещения СЭД, включая серверы приложений, базы данных и системы хранения данных.*
  2. *Обеспечение необходимые сетевые соединения и резервирование для высокой доступности и отказоустойчивости.*
- ***Установка и конфигурация****:*
  1. *Настройка серверов приложений, базы данных и системы хранения данных для СЭД.*
  2. *Настройка сетевых подключений и обеспечение резервирование критически важных соединений.*
  3. *Установка и настройка СЭД, включая управление пользователями, права доступа и интеграцию с другими системами.*
- ***Настройка безопасности****:*
  1. *Шифрование данных в транзите и в покое.*
  2. *Системы предотвращения вторжений.*
- ***Обеспечение управления и мониторинга****:*
  1. *Настройка мониторинга работы СЭД и учетных записей пользователей.*
  2. *Настройка системы оповещения для уведомления о проблемах и подозрительной активности.*

6. Архитектурное расположение системы электронного документооборота:

1. *Физическое и логическое размещение*
2. *Архитектурное расположение компонентов:* ***Frontend (Веб-серверы и серверы приложений); Bac kend (Серверы баз данных и хранения данных).*** *Расписать организацию работы.*

Требования работы с системами информационной безопасности

1. ***Планирование и проектирование***
    1. *Определение ключевых систем ИБ: firewall, IDS/IPS, антивирус, DLP, SIEM, системы управления доступом и шифрования данных.*
2. ***Конфигурация и настройка систем ИБ***
    1. *Настройка SIEM для централизованного мониторинга и корреляции событий безопасности*
    2. *Настройка автоматизированных оповещений о критических инцидентах и нарушениях безопасности.*
3. ***Архитектурное расположение***
    1. *размещение в защищенной сети для ограничения доступа, описание и реалзиация организации данного процесса.*
    2. *Интеграция всех системы ИБ с SIEM для централизованного управления и корреляции событий.*
    3. *Внедрите политики безопасности на уровне сети и конечных устройств для обеспечения комплексной защиты.*

4. Мониторинговый центр

1. *Провести анализ и выдачу рекомендаций по формированию единого автоматизированного мониторинговый центр в рамках организации для отслеживания событий, моментального реагирования.*

Требования работы с IP-телефонией

1. ***Установка и конфигурация***

1. *Порядок и организация серверов IP-телефонии и подключение их к сети.*
2. *Настройка программного обеспечения IP-телефонии, включая серверы SIP (Session Initiation Protocol) и настройка учетные записи пользователей*

2) Логическое размещение и взаимодействие

1. *Провести анализ и выдачу рекомендаций по подключению IP-телефонов и других устройств к сети, порядок настройки и конфигурации.*
2. *Провести анализ и выдачу рекомендаций по настройке VLAN с учетом разделения голосового и данных трафика для обеспечения безопасности и качества связи.*
3. *Провести анализ и выдачу рекомендаций по интеграции систем IP-телефонии с существующими ИТ-системами (CRM, ERP) для улучшения бизнес-процессов.*

Требования работы с интернетом

1. *Разработка архитектуры сети с учетом всех необходимых компонентов: маршрутизаторы, коммутаторы, точки доступа, firewall и другие системы безопасности.*
2. *Настройка физического размещения сетевого оборудования в серверной комнате с контролем доступа и резервным питанием.*
3. *подключения к интернет-провайдеру, с учетом настройки безопасного подключения.*
4. *Определение систем, которые имеют выход в интернет.*

1. *Какие порты необходимо использовать*
2.

Требования работы с программным обеспечением (ПО)

1. *Определить порядок приемки нового/модернизированного ПО.*
2. *Определить требования к информационной безопасности: описание мер по обеспечению безопасности данных и защиты от несанкционированного доступа, способность системы адаптироваться к увеличению нагрузки и объема данных, механи змы обеспечения непрерывной работы системы в случае сбоев.*
3. *Определить критерии приемки, какие результаты тестирования будут являться основанием для приемки ПО, в каких условиях и на каких данных будет проводиться тестирование.*
4. *Перечислить виды документации, которые должны быть разработаны (пользовательская документация, техническая документация и т.д.).*

4. ИТОГОВЫЕ ДОКУМЕНТЫ

- **Методика по построению и правилам архитектуры информационной безопасности по каждому направлению ИТ-инфраструктуры с фиксацией состояния по завершению всех вышеуказанных работ.**
- **Методика должна содержать выявленные и имеющиеся угрозы с учетом защиты, мер реагирования и устранения данных угроз с пошаговой инструкцией, объяснением и распределением ответственности.**

Содержание:

Правильная архитектура сети.

Настройка компонентов сети.

Рекомендации по внедрению программный решений по информационной безопасности.

Рекомендации по интеграции и взаимодействию всех компонентов.

Документы по каждому процессу

Содержание:

Описания процессов.

Политики и процедуры.

Инструкции по настройке и эксплуатации.

План реагирования на инциденты.

Документация по обучению и повышению осведомленности сотрудников.

Подписал	Байзаков Тимур Еркамысович
Дата подписания	28.08.2024