Конкурстық құжаттамаға
15-қосымша

Құрылыс-монтаждау жұмыстарымен байланысты емес сатып алынатын жұмыстардың техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Абай облысының цифрлық технологиялар басқармасы" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Абай облысының мемлекеттік сатып алу басқармасы" мемлекеттік мекемесі
Конкурстың №:	№ 17859608-2
Конкурстың атауы:	Ақпараттық технологиялар саласында «толық аяқталған» кешендік жұмыстар
Лоттың нөмірі:	№ 88191553-ОК1
Лоттың атауы	Ақпараттық технологиялар саласында «толық аяқталған» кешендік жұмыстар
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	620920.000.000000
Жұмыстың атауы:	Ақпараттық технологиялар саласында «толық аяқталған» кешендік жұмыстар
Өлшем бірлігі:	Жұмыс
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	618572100
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	618572100
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	

Жұмыстарды орындау мерзімі	техникалық сипаттамаға сәйкес
Аванстық төлем мөлшері:	0
Кепілдік мерзімі (айлармен)	12

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	Объектінің атауы Орналасқан жері Әкімшілік ғимараты Қазақстан Республикасы, Абай облысы, Семей қаласы, Қ. Мұхамедханов көшесі, 8. 1. Жұмыстарды жүргізу мақсаттары. 1.1. Жұмыстарды сатып алудың негізгі мақсаты пайдаланушылардың тұтынушының негізгі ақпараттық жүйелеріне қосылуын біріктіруге арналған ақпараттың ағып кетуін және дұрыс конфигурацияланған белсенді және пассивті телекоммуникациялық желілік жабдықты болдырмау үшін бағдарламалық қамтамасыз етуді орнату және конфигурациялау арқылы "кілтке дейін" ақпараттық технологиялар саласындағы жұмыстарды жүргізу болып табылады. 1.2. Ғимарат Абай облысы, Семей қаласы, Қайым Мұхамедханов көшесі, 8 мекенжайында орналасқан. Ғимаратта 5 қабат және техникалық қабат бар. 2. Атқарушылық құжаттамаға қойылатын талаптар. 2.1. Жұмыстарды орындау аяқталғаннан кейін Өнім беруші Тапсырыс берушіге мынадай атқарушылық құжаттаманы ұсынуы тиіс: 2.1.1. Байланыс желілерінің құрылымдық схемасы 2.1.2. Байланыс желілерін монтаждау схемасы 2.1.3. Қосылыстардың тік магистральдық схемалары 2.1.4. Телекоммуникациялық шкафтарда жабдықтарды орналастыру схемалары 2.1.5. Оптикалық байланыс желілеріндегі рефлектограммалар; 2.1.6. Кабельдік журналдар 3. Желілік инфрақұрылымның сандық және сапалық сипаттамалары. 3.1. Қабаттағы жұмыс орындарының саны (ЖМ) : 3.1.1. Техникалық қабат-кемінде 5 РМ 3.1.2. Бірінші қабат-кемінде 15 РМ; 3.1.3. Екінші қабат-кемінде 120 РМ; 3.1.4. Үшінші қабат-кемінде 120 РМ; 3.1.5. Төртінші қабат-кемінде 120 РМ; 3.1.6. Бесінші қабат-кемінде 40 РМ; 3.2. Қажет болған жағдайда, әлеуетті өнім беруші өз бетінше және өз есебінен міндеттердің дұрыс техникалық шешімін қалыптастыру үшін қажетті деректерді жинай отырып, ғимаратқа зерттеу жүргізе алуы тиіс. 3.3. Желілік инфрақұрылым элементтерін жаңғырту белсенді, пассивті желілік жабдықты, серверлерді, үздіксіз қуат көздерін, құрылғыларды орналастыруға арналған шкафтарды, жабдықты монтаждау және баптау материалдарын, қажетті бағдарламалық қамтамасыз етуді қамтуы тиіс. 3.4. Элементтердің құрамы бойынша техникалық шешімді әзірлеу кезінде желілік инфрақұрылымды жаңғырту кезінде мынадай талаптар қамтамасыз етілуге тиіс: 3.4.1. архитектура мен өнімділік параметрлері құрылымдалған кабельдік жүйелердің (ҚКЖ) құрылысын сипаттайтын ISO/IEC 11801 стандартының талаптарына және ҚР ҚН құрылыс нормаларына сәйкес болуы тиіс 3.02-17-2011; 3.4.2. кабельдік көлік ортасы, белсенді желілік жабдық (серверлерден басқа) пайдаланушылар санын көбейту мүмкіндігін қамтамасыз ету үшін кемінде 10% порт қоры мен кабельдік сыйымдылыққа ие болуы керек. 3.4.3. желінің барлық клиенттері үшін Ieee_802.1X технологиясы бойынша Ethernet порттарында авторизация қамтамасыз етілуі тиіс. Әлеуетті өнім беруші барлық тиісті техникалық шешімдерді өрістетуге және желінің барлық клиенттік құрылғыларын жоспарлы (Тапсырыс берушімен келісім бойынша) енгізуді жүзеге асыруға тиіс. 4. Желілік инфрақұрылымды жаңғыртуға қойылатын талаптар 4.1. Желілік инфрақұрылым тәуелсіз ақпараттық желілердің екі сегментінен

	тұруы керек-Private Network және Public network. 4.1.1. Жоғарыда аталған желілерде физикалық байланыс болмауы керек. 4.2. Private Network-мемлекеттік органдардың бірыңғай телекоммуникациялық желісін (МО БНАЖ) пайдалану үшін жабық жергілікті-есептеу желісі (бұдан әрі-ЖТҚ). 4.2.1. ҚР МО БНАЖ байланыс арнасымен физикалық коммутацияны көздеу қажет. 4.2.2. Ғимаратта орналасқан мекемелер деңгейінде желіні логикалық сегменттеуді пайдалана отырып, МО БНАЖ желісіне қорғалған қолжетімділікті қамтамасыз ету үшін private желісінің инфрақұрылымын теңшеу талап етіледі. 4.2.3. Жеке желідегі барлық желілік ресурстарды басқару орталық маршрутизаторды шығаруы керек. Ол, өз кезегінде, брандмауэр - брандмауэр-брандмауэр немесе желілік экран (Тапсырыс беруші ұсынған) (берілген ережелерге сәйкес ол арқылы өтетін желілік пакеттерді бақылауды және сүзуді жүзеге асыратын аппараттық немесе бағдарламалық құралдар кешені) арқылы МО БНАЖ сыртқы желісіне қосылуы тиіс. 4.2.4. Жеке желіде орталықтандырылған аутентификация мен авторизацияны орындау үшін IEEE 802.1 x RADIUS (Remote Authentication dial-in User Service) протоколын қолдана отырып, серверде орнатылған бағдарламалық жасақтама (radius-сервер) пайдаланылуы керек. құрылғыны конфигурацияланған Ethernet қосқышының портына қосқан кезде қосылған құрылғының аутентификациясы және тиісті сегменттерге кіру құқығы берілуі керек және желі ресурстарына. Сегменттеу белгілі бір сегменттегі сегменттеу талаптарына байланысты OSI желілік моделінің екінші және үшінші деңгейлерінде орындалуы керек. 4.2.5. Желінің бас қосқышы 2 қосқыштан тұратын стекті пайдалану арқылы желінің ақауларға төзімділігін қамтамасыз етуі керек. Әрбір стек элементінен әрбір агрегация қосқышына дейін жеке оптикалық байланыс желісі қамтамасыз етілуі керек. 4.2.6. Желіні біріктіру қосқышы 2 қосқыштан тұратын стекті пайдалану арқылы желінің ақауларға төзімділігін қамтамасыз етуі керек. Әрбір стек элементінен әр қабатты қол жеткізу қосқышына дейін жеке оптикалық байланыс желісі қамтамасыз етілуі керек. 4.3. Public Network-Интернетке қосылуға арналған жалпы телекоммуникациялық желі. 4.3.1. Барлық желілік ресурстарды басқаруды орталық маршрутизатор жүзеге асыруы керек, ол өз кезегінде сыртқы желіге қорғаныс функциялары бар брандмауэр арқылы қосылады (Тапсырыс беруші ұсынады). 4.3.2. Ғимаратта орналасқан мекемелер деңгейінде желіні логикалық сегменттеуді пайдалана отырып, Интернетке қорғалған қолжетімділікті қамтамасыз ету үшін public желісінің инфрақұрылымын теңшеу қажет. 4.3.3. Орталықтандырылған аутентификация мен авторизацияны орындау үшін public Network-те radius (Remote Authentication dial-in User Service) IEEE 802.1 x протоколын қолдана отырып, серверде орнатылған бағдарламалық жасақтама (radius-сервер) пайдаланылуы керек.құрылғыны конфигурацияланған Ethernet қосқышының портына қосқан кезде қосылған құрылғының аутентификациясы және тиісті сегменттерге және желі ресурстарына. Сегменттеу желінің белгілі бір сегментіндегі сегменттеу талаптарына байланысты OSI

	желілік моделінің екінші және үшінші деңгейлерінде орындалуы керек. 4.3.4. Желінің бас қосқышы 2 қосқыштан тұратын стекті пайдалану арқылы желінің ақауларға төзімділігін қамтамасыз етуі керек. Әрбір стек элементінен әрбір агрегация қосқышына дейін жеке оптикалық байланыс желісі қамтамасыз етілуі керек. 4.3.5. Желіні біріктіру қосқышы 2 қосқыштан тұратын стекті пайдалану арқылы желінің ақауларға төзімділігін қамтамасыз етуі керек. Әрбір стек элементінен әр қабатты қол жеткізу қосқышына дейін жеке оптикалық байланыс желісі қамтамасыз етілуі керек. 4.4. Кабельдік ішкі жүйеге қойылатын техникалық талаптар 4.4.1. Жеткізуші деректерді кемінде 100 Мбит/сек жылдамдықпен құрылымдық кабельдік желілерде (СКС) беру мүмкіндігін қамтамасыз етуі тиіс; 4.4.2. Тапсырыс берушінің қызметкерінің жұмыс орнында екі Ақпараттық розеткадан тұратын кемінде бір қос Розетка (RJ45 типті қосқыштар) болуы керек. 4.4.3. Ақпараттық розеткалар кабель қорабының ішіне орнатылуы немесе арнайы қораптарға орнатылуы керек, кабельдің минималды қорының талаптары сақталуы керек. 4.4.4. Кабель қорабының қақпағы қатты және анық бекітілуі керек, Бос орындар жоқ, қораптың көрінісі эстетикалық жағынан жақсы болуы керек, кабельдік керек-жарақтарды пайдалану қажет. Қорап жануды қолдамайтын ПВХ материалынан жасалуы керек.Gorenje. 4.4.5. Scs кросс бөлігі RJ45 типті коннекторлары бар 24 немесе 48 портты патч-панельдерден, 5е-ден төмен емес санаттан, ISO 11801, TIA'568' B және EN 50173 стандарттарынан тұруы керек және бекіткіштер мен қосылыстарды қамтамасыз ету үшін ілеспе керек-жарақтары болуы керек. 4.4.6. Көлденең Ішкі жүйе кросс жабдықтары, жұмыс орнындағы ақпараттық розеткалар арасындағы байланысты қамтамасыз етуі керек. Оның құрамында кемінде 0.411 мм (24-AWG) өзек қалыңдығы бар 4 жұп "экрандалмаған бұралған жұп, UTP" кабелі болуы керек. Физикалық және электрлік сипаттамалары бойынша Кабель 5е-ден төмен емес санат стандарттарына сәйкес келуі тиіс. 4.4.7. Тік магистральдық кабельдік жүйе байланыс торабынан әрбір телекоммуникациялық қабат шкафына дейін басталуы тиіс. Тік кабельдік жүйені құру кезінде резервті жоспарлау қажет кабельдік конструкцияларды жобалау кезінде талап етілетін кабельдік трассалардың кемінде 5%. Кабельді бағыттау "жұлдыз" типті топологияға сәйкес келуі керек, оның орталығы коммутациялық шкафтың кроссы болып табылады. 4.4.8. Тік кабельдік жүйе объектінің ішінде диапазон мен өткізу қабілеттілігі талаптарына сәйкес келетін бір режимді немесе көп режимді оптикалық кабельді қолдану арқылы орындалуы керек. 4.4.9. Әрбір жұмыс орнында кемінде екі Ақпараттық коннектор орнатылуы тиіс болғандықтан, әрбір жұмыс орнына кемінде 5е санаттағы "бұралған жұп" кабельдерінің тиісті саны салынуы тиіс. Компьютерлік желіге арналған кабельдік қосылыстың әр желісінің ұзындығы (белсенді телекоммуникациялық жабдықсыз жалпы желі) 90 м-ден аспауы керек, бұл ретте әрбір кабельдік қосылым кабельдің бір сегментін пайдаланған кезде орындалуы тиіс және оның бүкіл бойында ешқандай қосылымдар болмауы

	тиіс. 4.4.10. Кабельдік өнімдерді төсеу ANSI/EIA/TIA-568 стандартының СКС монтаждау талаптарына сәйкес жүзеге асырылуы тиіс. 4.4.11. Коммутация орталығының барлық белсенді жабдықтары патч панельдері тігілген байланыс шкафында орналасуы керек. Байланыс шкафтарындағы компьютерлік, телефон желілерін кесіп өту үшін RJ45 типті коннекторлары бар қосқыш сымдар қажет. 4.4.12. Қабат аралық телекоммуникациялық шкафтардың биіктігі кемінде 42U, габариттік өлшемдері кемінде 800х1000 мм болуы тиіс. шкафтардың саны кемінде 7 дана. 4.4.13. Орталық телекоммуникациялық шкафтар еденге арналған, биіктігі кемінде 42U, габариттік өлшемдері кемінде 800х1000 мм болуы тиіс.шкафтардың Жалпы саны кемінде 2. 4.4.14. Кабельдік Ішкі жүйе даму және модернизациялау мүмкіндігін қамтамасыз етуі керек, ең аз уақытпен өзгерістер енгізуге дайын болуы керек. 4.4.15. Жеткізуші өлшеу жабдығын қолдана отырып, барлық жаңадан салынған сызықтарды тексеруі керек. 4.4.16. Кабельдерді төсеу ғимараттың өрт қауіпсіздігі талаптарын сақтай отырып, оның ішінде төсемнің биіктігі, күштік кабельдермен қиылысу, кабельдік науалар мен қораптарды пайдалану, жылу көздеріне және электромагниттік кедергілерге дейінгі жол берілетін арақашықтықтар бойынша орындалуы тиіс. 4.4.17. Кабельдік желілер күштік кабельдер мен жарық беру желілерінен ең аз рұқсат етілген арақашықтықты сақтай отырып, ал бірлескен төсеу кезінде — жекелеген арналарда немесе бітелген секцияларда, ұшқындар мен өзара кедергілерді болдырмай салынуы тиіс. 4.5. Электр ішкі жүйесін орнатуға қойылатын жалпы талаптар 4.5.1. Телекоммуникациялық шкафтар (ТК) ғимараттың электр желісіне бөлек кабельдік желілермен қосылуы тиіс. 4.5.2. Телекоммуникациялық шкафтардың электр қуатын қосу үшін қимасы орнатылған белсенді жабдықтың номиналды жүктемесіне сәйкес келетін кабельді пайдалану қажет. 4.5.3. Әрбір ТК-да үздіксіз қуат көзін (UPS)орнату қажет: 4.5.4. Орталық шкафтар үшін жалпы максималды қуаты кемінде 5000 ВА болатын UPS пайдаланыңыз; 4.5.5. Қабатаралық шкафтар үшін жалпы максималды қуаты кемінде 3000 ВА болатын тіреуішті UPS қолданыңыз. 4.5.6. Барлық телекоммуникациялық шкафтар қуатты тарату құрылғысы арқылы қосылуы және электр розеткалары орнатылған тіреуішті аспаптық корпуспен және қажетті номиналдағы Автоматты ажыратқыштармен жабдықталуы тиіс. 4.6. Кросс үй-жайларды ұйымдастыру және жарақтандыру жөніндегі талаптар 4.6.1. Ғимаратта кросс бөлмелерін ұйымдастыру және жабдықтау бойынша бірқатар міндеттерді орындау қажет. 4.6.2. Кросс бөлмелері келесідей орналастырылуы керек: ғимараттың сол қанатында — 2, 3, 4 және 5 қабаттарда орналасқан 4 бөлме; ғимараттың оң қанатында-2, 3 және 4 қабаттарда орналасқан 3 бөлме. Орналасқан жері сол жерде келісіледі. 4.6.3. Үй-жайларды ұйымдастыру 4.6.3.1. Тиісті Қанаттың әрбір кросс-үй-жайы үшін Тапсырыс беруші ауданы кемінде 6 ш. м. жеке техникалық үй-жайды ұйымдастыру үшін алаң бөледі. 4.6.3.2. Бөлімнің түсі, сыртқы түрі және конструктивті орындалуы ғимараттың қолданыстағы дизайнын ескере отырып, Тапсырыс берушімен

	алдын-ала келісіледі. Кіреберіс есікті ені кемінде 0,8 м етіп орнатыңыз. 4.6.3.3. Әрбір үй-жайда қабырғалар мен беттерге косметикалық жөндеу жүргізу, Armstrong типті аспалы төбе, антистатикалық линолеум төсеу; қолданыстағы терезе ойығын кейіннен әрлеумен гипсокартонмен тігу; қолданыстағы транзиттік құбырларды сақтай отырып, Жылыту радиаторын (бар болса) бөлшектеу. 4.6.3.4. Үй-жайлардың нақты өлшемдері мен әрлеу жұмыстарының көлемі жұмыс басталғанға дейін орны бойынша нақтылансын. 4.6.3.5. Коммутациялық үй-жайдың көлемі мен өлшемдері: дәліздің ені бойынша болжамды өлшемдері – 3 × 2 м, биіктігі – 2,9 м. Үй-жайдың ауданы – 6 м². Қолданыстағы терезенің өлшемі – 2 × 2 м. 4.6.3.6. Есік орната отырып, қалқа тұрғызу. Ұзындығы 2 м және биіктігі 2,9 м қалқаны екі нұсқаның бірі бойынша орындау: сэндвич-панельдермен тұтас толтырылған алюминий профильден немесе металл қаңқаға бекітілген гипсокартоннан, жалпы қалыңдығы 100 мм-ге дейін, ішкі кеңістігін дыбыс оқшаулағыш материалмен толтырып, екі жағын әрлеу. Қалқаға өлшемі 0,8 × 2 м, оң жаққа ашылатын, қорабы мен фурнитурасы жиынтықта қарастырылған, кіруді бақылау және басқару жүйесінің (КББЖ) жабдығын орнату мүмкіндігі бар 1 металл есік блогын орнату. Есік ойығын шегергендегі қалқаның ауданы – 4,2 м². Гипсокартоннан орындалған жағдайда екі жағынан әрленетін беттердің ауданы, ойық жиектерін есепке алмағанда – 8,4 м². 4.6.3.7. Қолданыстағы қабырғаларды дайындау. Бөлінетін үй-жай ішіндегі қолданыстағы үш қабырғаны тазалау, ақаулы жерлерін жөндеу, тегістегіш қоспамен тегістеу және астарлау жұмыстарын орындау. Терезе ауданын шегергендегі дайындалатын беттердің ауданы – 19,2 м². 4.6.3.8. Қабырғаларды бояу. Ауданы 19,2 м² болатын дайындалған қолданыстағы қабырғаларды бояу жұмыстарын орындау. 4.6.3.9. Төбені бөлшектеу. Бөлінетін үй-жай шегіндегі ауданы 6 м² болатын қолданыстағы Armstrong аспалы төбесін бөлшектеу. 4.6.3.10. Төбені орнату. Бөлінетін үй-жай шегінде ауданы 6 м² болатын Armstrong аспалы төбесін монтаждау. Төбенің жаңадан орнатылған қалқаға түйісуін қарастыру. 4.6.3.11. Терезе ойығын қаптап жабу. Өлшемі 2 × 2 м болатын қолданыстағы терезе ойығын металл қаңқаға бекітілген гипсокартонмен қаптап жабу, түйіскен жерлерін бітеу, тегістегіш қоспамен тегістеу, астарлау және бояу жұмыстарын орындау. Қаптап жабылатын аудан – 4 м². Терезе блогын бөлшектеу қарастырылмайды. 4.6.3.12. Еденді дайындау. Қолданыстағы кафель жабындысын сақтау. Антистатикалық линолеум төсеу үшін негіздің беріктігін тексеру, бетін дайындау және қажетті тегістеу жұмыстарын орындау. Ауданы – 6 м². 4.6.3.13. Еден жабындысын төсеу. Ауданы 6 м² болатын антистатикалық линолеум төсеу жұмыстарын орындау. 4.6.3.14. Еден жиегін орнату. Есік ойығын қоспағанда, үй-жайдың периметрі бойынша жанбайтын материалдан жасалған еден жиегін орнату. Жалпы ұзындығы – 9,2 қума м. 4.6.4. Кондиционерлеу 4.6.4.1. Кросс үй-жайлардың әрқайсысы өнімділігі кемінде 18 000 BTU/сағ (18-сынып) жеке кондиционерлеу жүйесімен жабдықталсын. 4.6.4.2. Кондиционер ғимараттың

	қалған үй-жайларын пайдалану режиміне қарамастан, кросс үй-жайының қажетті температуралық режимін сақтауды қамтамасыз етуі тиіс. 4.6.4.3. Кондиционерді сыртқы ауаның теріс температурасында пайдалануға арналған қысқы жиынтықпен жабдықтаңыз. Сыртқы блок қорғаныш қалқанмен және қорғаныш қаптамамен жабдықталсын (Тапсырыс берушінің келісімі бойынша). 4.6.5. Электрмен жабдықтау 4.6.5.1. Әрбір кросс үй-жайға Тапсырыс берушімен келісілген қосылу нүктесінен бөлек электрмен жабдықтау желісін орындау қажет. Кабельдің қимасы Pue сәйкес анықталады. 4.6.5.2. Әрбір кросс-бөлмеде бөлменің барлық тұтынушыларын қосу үшін модульдер саны бойынша жеткілікті және одан әрі кеңейту үшін резерві бар жеке тарату қалқаны орнатылады. 4.6.5.3. Телекоммуникациялық жабдықтар, ИБП, кондиционер, жарықтандыру, СКУД жабдықтары, бейнебақылау, өрт және күзет дабылы, мониторинг және Кросс үй-жайының басқа да тұтынушылары үшін жекелеген желілер мен тиісті қорғаныс аппаратурасын көздеу. 4.6.6. Телекоммуникациялық шкафтар 4.6.6.1. Әрбір кросс бөлмесінде биіктігі кемінде 42U және ені кемінде 800 мм еден телекоммуникациялық шкафын орнату қажет. 4.6.6.2. ТК шкафтарында оптикалық және мыс кросс жабдықтарын, коммутаторларды, патч-панельдерді, кабельді ұйымдастырушыларды, UPS және басқа да қажетті жабдықтарды орналастыруды қарастырыңыз. 4.6.6.3. Шкафтарды орналастыру жабдықты монтаждау, коммутациялау және кейіннен техникалық қызмет көрсету үшін еркін қол жетімділікті қамтамасыз ете отырып жүзеге асырылады. 4.6.7. Жерге қосу 4.6.7.1. Ғимараттың сол және оң қанаттары бойымен кросс-бөлмелердің жерге тұйықтау контурларының құрылымын орындаңыз. 4.6.7.2. Сол қанаттың контурына сол қанаттың 2, 3, 4 және 5 қабаттарының кросс бөлмелерін қосыңыз. Оң қанаттың контурына оң қанаттың 2, 3 және 4 қабаттарының кросс бөлмелерін қосыңыз. 4.6.7.3. Контурларды біріктіріп, ғимараттың қолданыстағы жерге қосу жүйесіне қосыңыз. 4.6.7.4. Қажетті магистральды және тармақталған қорғаныс өткізгіштерін төсеуді орындаңыз. Жерге тұйықтау жүйесіне телекоммуникациялық шкафтарды, тарату қалқандарын, Металл конструкцияларды, жабдық корпустарын және қорғаныш жерге тұйықталуға жататын басқа да элементтерді қосу қажет. 4.6.7.5. Қосылымды жасамас бұрын ғимараттың қолданыстағы жерге қосу жүйесінің күйі мен параметрлерін тексеріңіз. 4.6.7.6. Жұмыс аяқталғаннан кейін Тапсырыс берушіге тиісті өлшеу хаттамаларын ұсына отырып, қажетті электротехникалық өлшемдерді орындаңыз. 4.6.8. Кіруді басқару және басқару жүйесі 4.6.8.1. Әрбір кросс үй-жай кіруді бақылау және басқару жүйесімен жабдықталсын. 4.6.8.2. Бөлмеге кіруді бақылауды, электромагниттік құлыпты, оқырманды, шығу түймелерін, есіктің апаттық құлпын ашу түймелерін, жақындатқышты және есіктің күйін бақылауды қамтамасыз ету. 4.6.8.3. Кабель желілерін төсеу, монтаждау, қосу және іске қосу жұмыстарын орындау. 4.6.9. Бейнебақылау жүйесі 4.6.9.1. Әрбір кросс үй-жай кіруді бақылауды қамтамасыз ететін бейнебақылау жүйесімен жабдықталсын. 4.6.9.2. Камераларды орнатуды, кабель желілерін

	салуды, қосуды және конфигурациялауды орындаңыз. 4.6.10. Кросс-үй-жайларды бақылау 4.6.10.1. Әрбір кросс үй-жайда үй-жайдың инженерлік жай-күйіне мониторинг жүргізу жүйесін ұйымдастыру. 4.6.10.2. Температураны; ылғалдылықты; судың ағып кетуін; алдыңғы есіктің ашылуын / жабылуын бақылау қажет. Авариялық және алдын алу оқиғаларының оқиғаларды есепке алу және бақылау жүйесіне берілуін қамтамасыз ету. 4.6.11. Кабельдік және желілік инфрақұрылым 4.6.11.1. Кросс бөлмелерінің толық жұмыс істеуі үшін барлық қажетті оптикалық, мыс, қуат және төмен токты кабельдік желілерді төсеу. 4.6.11.2. Кабельдік науаларды, қораптарды, бекіту конструкцияларын, кабельдік ұңғымаларды және кабельдік инфрақұрылымның басқа да қажетті элементтерін (қолданылатын жерде) қарастыру. 4.6.11.3. Барлық кабельдік желілер терминал және екі жағынан таңбалау. Жабдықты ауыстырыңыз. 4.6.11.4. Орнату аяқталғаннан кейін мыс және оптикалық сызықтарды тексеріп, тексеріңіз. 4.7. Байланыс арналарын орталықтандырылған маршруттау, теңгерімдеу және оңтайландыру жөніндегі жұмыстарға қойылатын талаптар 4.7.1. Өнім беруші желілік инфрақұрылымның тоқтап қалуын болдырмау үшін жүктемені динамикалық бөлу және аса маңызды қызметтік трафикке (QoS) басымдық беру тетіктерін енгізе отырып, тапсырыс берушінің байланыс операторларының кіріс және шығыс трафигін орталықтандыруды және біріктіруді ұйымдастыруға міндетті. Телекоммуникациялық жабдықты және маршруттау схемасын баптау ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптардың 123, 124, 128 және 139-тармақтарына сәйкес орындалуы тиіс. Барлық коммутация және маршруттау ішкі адрестеуді (NAT) жасыратын шекаралық шлюз және брандмауэр арқылы, әр интерфейстегі пакеттерді сүзу, уақытты синхрондау арқылы қорғалған оқиғалар журналдарын жүргізу арқылы жүзеге асырылуы керек. 4.8. Пайдаланушы порттарын рұқсатсыз кіруден қорғауға қойылатын талаптар 4.8.1. Жеткізуші белсенді желілік жабдықтың физикалық және логикалық пайдаланушы порттарын қорғау бойынша ұйымдастырушылық-техникалық шаралар кешенін іске асыруға міндетті. 4.8.2. Жеткізуші құрылымдық кабельдік жүйенің барлық бос, пайдаланылмаған порттарын және белсенді желілік жабдық интерфейстерін физикалық және бағдарламалық түрде өшіруді немесе құлыптауды қамтамасыз етеді. Белсенді пайдаланушының желілік порттары үшін үшінші тарап құрылғыларының, маршрутизаторлардың, басқарылмайтын қосқыштардың және сымсыз кіру нүктелерінің рұқсатсыз қосылуын болдырмайтын қосылымдарды шектеу және басқару саясаттары (соның ішінде MAC мекенжайларын байланыстыру, IEEE 802.1 x құрылғысының аутентификация механизмдері) орнатылуы керек. 4.9. Техникалық жарақтандыруға қойылатын талаптар. 4.9.1. Жеткізуші жабдыққа тапсырыс берушінің жергілікті-есептеу желісіне физикалық орнату, базалық баптау және интеграциялау жөніндегі міндеттер кешенін (жеткізуші ұсынады) төмендегілерден төмен емес сипаттамалармен орындауы тиіс. Сервер түрі 1 сервер корпусы - Форма факторы: Rackmount, 2U -

	Процессорларды қолдау: кем дегенде 1 - Үйлесімділік: пассивті радиаторлар, фронтальды салқындату - Диск бөлімдері: 12× 3.5" дейін Hot-swap (SAS3/SATA). - Қуат көзі: резервтелген, 2x1000w, 1U, hot-swap Аналық плата −SATA қолдауы: 12× SATA3 дейін (6 Гбит / с) - Raid қолдауы: 0, 1, 5, 10 деңгейлері - Басқару порты: 1Gbps Base-T Ethernet −Жедел жад: DDR4 ecc registered қолдауы, 16 слот Процессорлар - Сәулет: x86_64, 10 нм-ден кем емес - Жиілігі: 2.4 ГГц бастап - Кэш: 24 МБ L3 бастап - Ядролар/ағындар: кем дегенде 8 ядро / 16 ағын Жедел жад - Түрі: DDR4 ECC тіркелген (RDIMM) - Жиілігі: 3200 МГц - Көлемі: кемінде 128ГБ Сақтау жүйесі −SSD (Enterprise-класс, SATA 6 Гбит/с): 2× 480 ГБ, 2× 1.92 ТБ −HDD (SATA 6 Гбит/с): кемінде 2× 10 ТБ, 7200 айн/мин, кэш ≥256 МБ - Дискілерді орнатуға арналған шаналар қосымша адаптерлерсіз 2.5" және 3,5" дискілерді орнату мүмкіндігі бар барлық дискілер үшін болуы керек. RAID контроллері - Қолдау: SATA/SAS 12 Гбит/с - Порттар: 8 ішкі - Интерфейс: PCIe 3.0 - Кэш: 2 ГБ DDR3 - RAID деңгейлерін қолдау: 0, 1, 5, 6, 10, 50, 60 Желілік адаптер - Порттар: кем дегенде 2x1Gbps Base-T Ethernet - Интерфейс: PCIe 2.0/3.0/4.0 OCP Жалпы саны кемінде 2 дана. Сервер Түрі 2 1. Сервер корпусы - Форма факторы: Rackmount, 2U - Процессорларды қолдау: кем дегенде 2 - Үйлесімділік: пассивті радиаторлар, фронтальды салқындату - Диск бөлімдері: 12× 3.5" дейін Hot-swap (SAS3/SATA) - Қуат көзі: резервтелген, 2x1000w, 1U, hot-swap 2. Аналық плата −SATA қолдауы: 12× SATA3 дейін (6 Гбит / с) - Raid қолдауы: 0, 1, 5, 10 деңгейлері - Басқару порты: 1Gbps Base-T Ethernet −Жедел жад: DDR4 ecc registered қолдауы, 32 слот 3. Процессорлар - Сәулет: x86_64 - Жиілігі: 2.4 ГГц бастап - Кэш: 24 МБ L3 бастап - Ядролар/ағындар: кем дегенде 12 ядро / 24 ағын 4. Жедел жад - Түрі: DDR4 ECC тіркелген (RDIMM) - Жиілігі: 3200 МГц - Көлемі: кемінде 256 ГБ 5. Сақтау жүйесі −SSD (Enterprise-класс, SATA 6 Гбит/с): 2× 480 ГБ, 4× 3.84 ТБ −HDD (SATA 6 Гбит/с): кемінде 4× 10 ТБ, 7200 айн / мин, кэш ≥256 МБ - Дискілерді орнатуға арналған шаналар қосымша адаптерлерсіз 2.5" және 3,5" дискілерді орнату мүмкіндігі бар барлық дискілер үшін болуы керек. 6. RAID контроллері - Қолдау: SATA/SAS 12 Гбит/с - Порттар: 8 ішкі - Интерфейс: PCIe 3.0 - Кэш: 2 ГБ DDR3 + батарея - RAID деңгейлерін қолдау: 0, 1, 5, 6, 10, 50, 60 7. Желілік адаптер - Порттар: кем дегенде 2x1Gbps Base-T Ethernet - Интерфейс: PCIe 2.0/3.0/4.0 OCP Жалпы саны кемінде 2 дана. 1 типті қосқыш Коммутаторда кемінде 48 10/100/1000Base-T Ethernet порты және 100/1000/10G жылдамдығы бар кемінде 6 SFP+ порты болуы керек. 100 Мбит/с режиміндегі SFP+ порттарының жұмысына қолдау көрсету керек. Коммутатордың өткізу қабілеті кемінде 190 Гбит/с, пакеттерді жіберу жылдамдығы секундына кемінде 150 миллион пакет болуы керек. ЖЖҚ көлемі кемінде 256 МБ, Flash жады кемінде 32 МБ болуы керек. Жұмыс температурасының диапазоны 0-ден +50 °C-қа дейін болуы керек. Бір уақытта қолдау көрсетілетін VLAN саны кемінде 4094, Multicast-топтар

	саны кемінде 4096 болуы тиіс. Коммутатор кем дегенде 12000 IPv4 маршруттарын және кем дегенде 8000 ARP жазбаларын қолдауы керек. Абоненттік портта бір уақытта қол қойылған Multicast-топтардың санын шектеу функциясы, MVR функционалы, порттардағы Drop Query және Drop Report сүзгісі, multicast Router Port динамикалық және статикалық конфигурациясы, сондай-ақ IGMP snooping және MVR функцияларына қарамастан қызметтік multicast-трафикті мөлдір беру қолдау керек. ACL ережелерінің саны кемінде 3000 болуы керек. Кем дегенде 12 000 байт Jumbo Frames қолдауы міндетті болып табылады. Коммутатор IEEE 802.1 d, IEEE 802.1 S және IEEE 802.1 w стандарттарына сәйкес Spanning Tree протоколдарын, сондай-ақ Root guard, BPDU Guard және Bpdu Forwarding функцияларын қолдауы керек. Статикалық маршруттау, қатаң SPQ басымдығы, WRR кезегін басқару саясаты, WRR+SPQ және PQ+WRR болуы міндетті. Әрбір портта кемінде төрт трафикті беру кезегі сақталуы керек, олардың біреуінде Strict Priority қызмет көрсету деңгейі болуы керек. Коммутатор басым трафик ағынының шектелуімен трафикті мәжбүрлеп таңбалауды және қайта таңбалауды қамтамасыз етуі керек, dscp өрісінің өзгеруін, IEEE 802.1 P және DSCP CoS бойынша трафиктің жіктелуін қолдауы керек. Әкімшілік қол жетімділік үшін TACACS+ және RADIUS арқылы аутентификацияға қолдау көрсету керек. Коммутаторды басқару RS-232 (RJ-45) консоль порты арқылы, сондай-ақ Telnet, SSH, SNMP және HTTPS протоколдары арқылы жүзеге асырылуы керек. Коммутатор 220 В айнымалы ток қуатын, IEEE 802.3 x Flow Control стандартын, белсенді салқындату жүйесін, VLAN Translation функционалдығын және IPv6 протоколын қолдауы керек. DHCP Option 37 және option 38 қолдауының болуы міндетті. SFP/SFP+ үшінші тарап модульдерін пайдалануға ешқандай шектеулер болмауы керек. Коммутатор конфигурацияның қашықтағы серверге автоматты түрде сақтық көшірмесін жасауы керек, dynamic ARP Inspection (DAI), порт оқшаулауын (Порт оқшаулау), орталық процессорды қорғау механизмдерін (CPU Protection), жедел жадты, Flash жадын және қашықтағы серверді қолдауы керек. MAC Authentication Bypass (MAB), Dying Gasp, ULDP, коммутатор процессорынан трафикті түсіру (Packet Capture), портты шағылыстыру және RSPAN, кірістірілген диагностика және жөндеу құралдары, Voice VLAN және MAC VLAN функцияларына қолдау көрсету керек. Құрылғыны басқаруға және бақылауға қол жеткізуді шектеу, Port Security қолдауы, PPPoE Relay/PPPoE+, DNS Client (RFC 1591), сондай-ақ VLAN менеджері үшін IEEE 802.1 p басымдылығын реттеу үшін қол жеткізуді басқару тізімдерін теңшеу мүмкіндігі болуы керек. Коммутатор кем дегенде екі кіріктірілген қуат көзімен жабдықталуы керек. Жалпы саны 19 данадан кем емес. 2 типті қосқышта кемінде 48 10GBase-R (SFP+)/1000BASE-X (SFP) Ethernet порты және кемінде 6 40g QSFP+порты болуы керек. Сыртқы дискілерді қосуға арналған арнайы 10/100/1000BASE-T RJ-45 басқару портының және USB портының болуы міндетті. Коммутация өнімділігі кем дегенде 960 Гбит/с, пакеттерді жіберу жылдамдығы кем дегенде 960 Mpps

	болуы керек. Жедел жад көлемі кемінде 2048 МБ, Flash жады кемінде 4096 МБ болуы керек. Жұмыс температурасының диапазоны 0-ден +50 °C-қа дейін болуы керек. MAC мекенжай кестесінің өлшемі кемінде 162 000 жазба болуы керек. Бір уақытта қолдау көрсетілетін VLAN саны кемінде 4000, Multicast топтарының саны кемінде 4000 болуы керек. ACL ережелерінің саны кемінде 2048 кіріс және 1024 Шығыс жазбаны құрауы керек. Кем дегенде 12000 байт Jumbo frame қолдауы міндетті болып табылады. Коммутатор стекингті қолдауы керек. Стектегі құрылғылардың ең аз саны кемінде екі болуы керек. Selective Q-in-Q (IEEE 802.1 ad), Spanning Tree IEEE 802.1 d, IEEE 802.1 s, IEEE 802.1 w протоколдарына, сондай-ақ Root guard, BPDU Guard және BPDU Tunnel мүмкіндіктеріне қолдау қажет. ITU-T G. 8032, MRPP, ULPP және ULSM сақина топологиясын қорғау хаттамаларының жұмысына қолдау көрсетілуі керек. Сондай-ақ, Dynamic ARP Inspection, ARP Guard, ARP Binding және ANTI-ARP-Scan механизмдерін қолдау қажет. ARP жазбаларының саны стандартты UFT режимінде кемінде 192 000 болуы керек. Коммутатор VRF технологиясын қолдауы керек. VFI саны кемінде 256, VRF саны кемінде 64 болуы керек. Тең ecmp маршруттарының саны кемінде 32 болуы керек. RIPv2, OSPFv2, OSPFv3, bgpv4+, PIM-SM және Pim-DM статикалық және динамикалық маршруттау протоколдарын қолдау міндетті болып табылады. IPv4 және IPv6 PIM маршруттарының саны әр хаттама үшін кемінде 4094 болуы керек. Маршруттау кестесінің өлшемі стандартты UFT режимінде кемінде 8000 маршрут және маршруттау режимінде 128000 маршрут болуы керек. Әкімшілік қол жетімділік үшін TACACS+ және RADIUS протоколдарының аутентификациясы сақталуы керек. Құрылғыны басқару RS-232 (RJ-45) консоль порты арқылы, сондай-ақ Telnet, SSH және SNMP протоколдары арқылы жүзеге асырылуы керек. Syslog қолдауы міндетті болып табылады. Коммутатор ыстық ауыстыру мүмкіндігі бар екі қуат көзін орнатуды қолдауы керек. Пакеттік буфердің өлшемі кемінде 6 МБ болуы керек. Топтардың саны кемінде 64 және бір топта кемінде 4 портты біріктіру мүмкіндігі бар LACP арналарын біріктіру хаттамасын қолдау міндетті болып табылады. DHCP server, DHCP Client және DHCP Relay жұмысына, сондай-ақ IEEE 802.1 x және MAB протоколдарының аутентификациясына қолдау көрсетілуі керек. Конфигурацияның қашықтағы серверге автоматты түрде сақтық көшірмесін жасау, MD5 және SHA-256 алгоритмдерімен парольдерді шифрлауды қолдау, сондай-ақ CLI арқылы конфигурация файлдарын салыстыру функциясы қажет. Коммутатор VLAN жүйесінде IGMP Snooping пайдалану кезінде IGMP пакеттерінде Source IP мекенжайын және source MAC мекенжайын көрсету мүмкіндігін қамтамасыз етуі керек. CPU-дан құрылғының Flash-жадына, NQA (network Quality Analysis) функционалына, сондай-ақ VLAN: Port-based VLAN, IEEE 802.1 Q, Private VLAN, Protocol VLAN, Voice VLAN, MAC VLAN, N:1 VLAN Translation және Port-Based QinQ хаттамаларына пакеттерді жазуды қолдау міндетті болып табылады. Span, RSPAN және ERSPAN трафигін шағылыстыруға қолдау көрсету керек. Қызмет көрсету сапасын

	қамтамасыз ету үшін QoS механизмдерін қолдайтын портқа кемінде 8 кезек қажет: Strict Priority, WRR, SP+WRR, DWRR және SP+DWRR. Жалпы саны кемінде 4 дана. 3 типті қосқышта кемінде 16 Ethernet 100/1000Base-X SFP порты, кемінде 8 10/100/1000Base-T немесе 100/1000Base-X SFP біріктірілген Ethernet порты және кемінде 4 10GBase-R (SFP+)/1000BASE-X (SFP) порты болуы керек. Стекті ұйымдастыру үшін кем дегенде 2 арнайы 20G QSFP+порты қарастырылуы керек. Сыртқы дискілерді қосуға арналған арнайы 10/100/1000BASE-T RJ45 басқару портының және USB портының болуы міндетті. Коммутация өнімділігі кем дегенде 208 Гбит/с, пакеттерді жіберу жылдамдығы кем дегенде 155 Mpps болуы керек. ЖЖҚ көлемі кемінде 1024 МБ болуы керек. Flash жады кемінде 32 МБ, ал NAND Flash жады кемінде 1024 МБ болуы керек. MAC мекен-жайы кестесінің өлшемі кем дегенде 64000 жазбаны құрауы керек. Бір уақытта қолдау көрсетілетін VLAN саны кемінде 4094 болуы керек. Коммутатор Port-based VLAN, IEEE 802.1 Q, Private VLAN, Protocol VLAN, Voice VLAN, MAC VLAN, selective QinQ, Port-Based QinQ және N:1 VLAN Translation қолдауы керек. Multicast топтарының саны кем дегенде 1000 болуы керек. ACL ережелерінің саны кемінде 3328 кіріс және 1024 Шығыс болуы керек. IPv4/IPv6 маршруттау кестесінің өлшемі кемінде 16382/6143 жазбаны құрауы керек. Кем дегенде 16 000 байт Jumbo frame қолдауы міндетті болып табылады. Коммутатор кем дегенде 4 құрылғыны стекке біріктіру мүмкіндігімен стекингті қолдауы керек. Стек қосылымының жалпы өткізу қабілеті кемінде 40 Гбит/с болуы керек. Selective Q-in-Q технологиясына (IEEE 802.1 ad), Spanning Tree IEEE 802.1 d, IEEE 802.1 S және IEEE 802.1 W протоколдарына, сондай-ақ Root guard, BPDU Guard және BPDU Tunnel мүмкіндіктеріне қолдау көрсету керек. ITU-T G. 8032, MRPP, ULPP және ULSM сақина топологиясын қорғау протоколдарын қолдау міндетті болып табылады. Коммутатор dynamic ARP Inspection, ARP Guard, ARP Binding және ANTI-ARP-Scan механизмдерін қолдауы керек. IPv4/IPv6 ARP жазбаларының саны кем дегенде 16400/16381 болуы керек. Тең ecmp маршруттарының саны кемінде 32 болуы керек. RIPv2, OSPFv2, OSPFv3, bgpv4+, PIM-SM және Pim-DM статикалық және динамикалық маршруттау протоколдарын қолдау міндетті болып табылады. Топтар саны кемінде 192 болатын vrrp резервтеу технологиясына қолдау көрсету керек. Коммутатор MPLS-ті, соның ішінде L2VPN және L3VPN-ді қолдауы керек, MPLS тегтерінің саны кемінде 8096. Әкімшілік қол жетімділік үшін TACACS+ және RADIUS протоколдарының аутентификациясы сақталуы керек. Құрылғыны басқару RS-232 (RJ-45) консоль порты арқылы, сондай-ақ Telnet, SSH және SNMP протоколдары арқылы жүзеге асырылуы керек. Коммутатор ыстық ауыстыру мүмкіндігі бар екі қуат көзін орнатуды, сондай-ақ кіріс кернеуі 36-72 в Тұрақты ток қуат көздерін пайдалану мүмкіндігін қолдауы керек. OAM, Dying gasp, VCT және DDM протоколдарын қолдау міндетті болып табылады. Коммутатор LACP арналарын біріктіру протоколын қолдауы керек. Агрегация топтарының саны бір топта кемінде 4 портты біріктіру

	мүмкіндігімен кемінде 128-ні құрауға тиіс. CLI арқылы конфигурация файлдарын салыстыру мүмкіндігі болуы керек. Пакеттік буфердің өлшемі кемінде 4 МБ болуы керек. Коммутатор vfi саны кемінде 256 және VRF саны кемінде 251 болатын VRF қолдауы керек. LDP тегтерін сүзуге де қолдау көрсету керек. VLAN-да IGMP Snooping пайдалану кезінде IGMP пакеттерінде Source IP Address және source MAC address-ті көрсету, MD5 және SHA-256 алгоритмдерімен парольдерді шифрлау, VFI-де MAC мекенжайларының санын көру, құрылғының Flash-жадына CPU-дан пакеттерді жазу және NQA (network Quality Analysis) функционалы міндетті болып табылады. Span, RSPAN және ERSPAN трафигін шағылыстыруға қолдау көрсету керек. Қызмет көрсету сапасын қамтамасыз ету үшін QoS механизмдерін қолдайтын портқа кемінде 8 кезек қажет: Strict Priority, WRR, strict+WRR, DWRR, sdwrr және WRED. Жалпы саны кемінде 4 дана. 4 типті Коммутатор қосқышта кемінде 48 10/100/1000Base-T Ethernet порты және 100/1000/10G жылдамдығы бар кемінде 6 SFP+ порты болуы керек. SFP+ порттарының жұмысына 100 Мбит/с қолдау көрсетілуі керек.барлық 48 мыс порттары Poe IEEE 802.3 af және IEEE 802.3 at технологияларын қолдауы керек. PoE жалпы бюджеті кем дегенде 760 Ватт болуы керек. 10/100/1000Base-T RJ-45 арнайы басқару портының болуы міндетті. Коммутатордың өткізу қабілеті кемінде 192 Гбит/с, пакеттерді жіберу жылдамдығы секундына кемінде 120 миллион пакет болуы керек. ЖЖҚ көлемі кемінде 256 МБ, Flash жады кемінде 32 МБ болуы керек. Жұмыс температурасының диапазоны 0-ден +50 °C-қа дейін болуы керек. MAC мекен-жайы кестесінің өлшемі кем дегенде 28000 жазбаны құрауы керек. Бір уақытта қолдау көрсетілетін VLAN саны кемінде 4094, Multicast-топтар саны кемінде 4096 болуы тиіс. Коммутатор кем дегенде 12000 IPv4 маршруттарын және кем дегенде 8000 ARP жазбаларын қолдауы керек. Қуат 220 В айнымалы ток желісінен берілуі керек.Коммутатор екі қуат көзімен жабдықталуы керек. Абоненттік портта бір уақытта қол қойылған Multicast-топтардың санын шектеу функциясы, MVR функционалы, порттардағы Drop Query және Drop Report сүзгісі, multicast Router Port динамикалық және статикалық конфигурациясы, сондай-ақ IGMP snooping және MVR функцияларына қарамастан қызметтік multicast-трафикті мөлдір беру қолдау керек. ACL ережелерінің саны кемінде 3840 болуы керек. Кем дегенде 12 000 байт Jumbo Frames қолдауы міндетті болып табылады. Коммутатор selective Q-in-Q (IEEE 802.1 ad), Spanning Tree IEEE 802.1 d, IEEE 802.1 S және IEEE 802.1 W протоколдарын, сондай-ақ Root guard, bpdu Guard және BPDU Forwarding мүмкіндіктерін қолдауы керек. Статикалық маршруттау, қатаң SPQ басымдығы, WRR кезегін басқару саясаты, WRR+SPQ және PQ+WRR болуы міндетті. Әрбір портта кемінде төрт трафикті беру кезегі сақталуы керек, олардың біреуінде Strict Priority қызмет көрсету деңгейі болуы керек. Коммутатор трафикті мәжбүрлеп таңбалауды және қайта таңбалауды, dscp өрісін өзгертуді және трафикті IEEE 802.1 P және DSCP CoS бойынша жіктеуді қамтамасыз етуі керек. Әкімшілік қол

	жетімділік үшін TACACS+ және RADIUS арқылы аутентификацияға қолдау көрсету керек. Коммутаторды басқару RS-232 (RJ-45) консоль порты арқылы, сондай-ақ Telnet, SSH, SNMP және HTTPS протоколдары арқылы жүзеге асырылуы керек. Коммутатор IEEE 802.3 x Flow Control, белсенді салқындату жүйесі, VLAN Translation және IPv6 қолдауы керек. DHCP Option 37 және option 38 қолдауы қажет. SFP/SFP+ үшінші тарап модульдерін пайдалануға ешқандай шектеулер болмауы керек. Коммутатор MAC Authentication Bypass (MAB), ULDP, құрылғының процессорынан трафикті түсіру (Packet Capture), rspan трафигін көрсету, кірістірілген диагностикалық құралдар, Voice VLAN және MAC VLAN қолдауы керек. Сондай-ақ, құрылғыны, Port Security функциясын және PPPoE Relay/PPPoE+функциясын басқару және бақылау үшін қол жетімділікті басқару тізімдерін конфигурациялау қажет. Жалпы саны 17 данадан кем емес. Маршрутизатор форма факторы: тірек өнімділігі (Rackmount), стандартты 19 дюймдік телекоммуникация сөресіне немесе шкафқа орнатуға арналған "құлақтарды" орнату. Аппараттық платформа: ядро саны кемінде 4 (төрт) және әр ядроның сағаттық жиілігі кемінде 1,7 ГГц болатын Процессор (архитектура 64-бит). ЖЖҚ (ЖЖҚ) көлемі — кемінде 4 ГБ. Кірістірілген тұрақты емес жад (NAND/Flash) кемінде 128 МБ құрайды. Мыс желілік интерфейстер: жергілікті трафикті бағыттауға арналған RJ-45 қосқыштары бар кемінде 16 (Он алты) 10/100/1000Base-T (Gigabit Ethernet) Ethernet порттары. Оптикалық желі интерфейстері: жоғары жылдамдықты магистральдық (Uplink) арналарды ұйымдастыруға арналған 10 Гбит/с дейінгі деректер жылдамдығын қолдайтын (сонымен қатар 1.25 Гбит/с SFP модульдерімен кері үйлесімділік) кемінде 2 (екі) SFP+ порты. Басқару және кеңейту интерфейстері: Жергілікті физикалық конфигурация үшін 1 (бір) консоль портының (RJ-45) болуы. Сыртқы дискілерді, резервтік LTE/4G-модемдерді немесе өзге де Перифериялық құрылғыларды қосуға арналған толық өлшемді USB портының (3.0 Type-A-дан төмен емес нұсқасы) болуы. Қуат талаптары: қуат ақауларына төзімділікті қолдау — кемінде 2 (екі) кіріктірілген резервтелген Автоматты коммутациялық қуат көздерінің болуы (айнымалы ток 100-240В желілерін қолдау). Функционалдылық (желілік ОЖ): Саясатқа негізделген статикалық маршруттау мен маршруттауды қолдау (Саясатқа негізделген маршруттау). Аппараттық шифрлауды жеделдетуді қолдайтын виртуалды жеке желілер мен туннельдерді (IPsec, L2TP, PPTP, OpenVPN, WireGuard немесе олардың баламалары) құруды қолдау. Қосылым күйін бақылайтын (Stateful inspection) және желілік адресті аудару механизмдерін (NAT/PAT) қолдайтын кіріктірілген брандмауэр (Firewall). Өткізу қабілеттілігі мен қызмет көрсету сапасын басқарудың икемді жүйесі (QoS / Traffic Shaping). Жалпы саны кемінде 2 дана. Брандмауэр желілік интерфейстер: WAN, DMZ, LAN рөлдерін тәуелсіз тағайындау мүмкіндігі бар кемінде 10 гигабиттік Ethernet порты (10/100/1000Base-T, RJ45). Басқару интерфейстері: кемінде 1 RJ45 консоль порты және кемінде 1 USB қызмет порты. Қуат: кернеуі 100-240 В, жиілігі 50/60

	Гц айнымалы ток желісінен сыртқы қуат көзі. Брандмауэр өткізу қабілеттілігі (Firewall Throughput): үлкен өлшемді пакеттерді тасымалдау кезінде кемінде 8 Гбит/с (1518 байт). IPS өнімділігі (кірудің алдын алу жүйелері): кемінде 1,2 Гбит / с. Келесі буын брандмауэрінің өнімділігі (NGFW): кем дегенде 900 Мбит/с. Кешенді қауіптен қорғау өнімділігі (Threat Protection): кемінде 650 Мбит/с. IPsec VPN туннельдерінің өткізу қабілеті: кемінде 5 Гбит / с. Қолдау көрсетілетін IPSec VPN туннельдерінің саны: кемінде 75 "шлюз-шлюз" (Gateway-to-Gateway) және кемінде 120 "клиент-шлюз" (client-to-Gateway). Желілік функционалдылық: статикалық және динамикалық маршруттауды қолдау, VLAN (IEEE 802.1 Q), адресті аудару механизмдерін (NAT/PAT), арналарды біріктіруді, IPv4 және IPv6 протоколдарын қолдау. Vpn технологиялары: IPsec VPN және SSL VPN қорғалған виртуалды желілерін құру протоколдарын қолдау; AES-256-дан төмен емес стандарттар бойынша шифрлауды қолдау. Трафикті бақылау және сүзу: пакеттерді терең тексеру (DPI), L7 деңгейіндегі қосымшаларды басқару, SSL/TLS шифрланған трафикті тексеру (TLS 1.3 қоса), URL санаттары бойынша веб және мазмұнды сүзу, зиянды бағдарламалар мен нақты уақыттағы желілік шабуылдардан қорғау. Басқару және бақылау: Жергілікті веб-интерфейсті (HTTPS), командалық жол интерфейсін (SSH/консоль арқылы CLI) қолдау, SNMP, Syslog, NTP протоколдарын қолдау, бір орталықтандырылған оқиғалар журналын басқару және талдау жүйесіне қосылу мүмкіндігі. Жалпы саны кемінде 2 дана. Wi-Fi кіру нүктесі орындау Түрі: Ішкі, қабырғаға немесе төбеге бекіту мүмкіндігі бар (орнату жинағы жинақта болуы керек). Сымсыз байланыс стандарттары: IEEE 802.11 a/b/g/n/ac/ax (wi-fi 6) заманауи стандарттарын қолдау. Жұмыс диапазондары: екі жиілік диапазонында бір уақытта жұмыс істеу (Dual-Band) — 2.4 ГГц және 5 ГГц. Антенналар: кіріктірілген көп бағытты антенналар. Антеннаны күшейту коэффициенті 5 ГГц диапазоны үшін кемінде 5.5 dBi және 2.4 ГГц диапазоны үшін кемінде 6 dBi. Желілік интерфейстер: кемінде 2 (екі) Ethernet порты 10/100 / 1000Base-T (Gigabit Ethernet). Қуат (PoE): бірінші портта 802.3 af/at стандартындағы power over Ethernet (PoE-In) технологиясы бойынша қуат алуды қолдау. Қосымша құрылғыларды қосу үшін екінші портта электр қуатын беру (PoE-Out) функциясының болуы. Аппараттық бөлік: кемінде 1.8 ГГц жиіліктегі 4 ядродан кем емес Процессор;кемінде 1 Гбайт жедел жады; кемінде 128 Мб ішкі флэш-жады. Қауіпсіздік және шифрлау: WPA2-PSK, WPA3-PSK, WPA2-Enterprise, WPA3-Enterprise, OW қоса алғанда, қазіргі қауіпсіздік протоколдарын қолдау. Басқару: құрылғы бағдарламалық жасақтама немесе аппараттық сымсыз желі контроллері (жіксіз роумингті қолдайтын) арқылы толық офлайн және орталықтандырылған басқару режимінде жұмыс істеуі керек. Жалпы саны кемінде 50 дана. Деректерді сақтау жүйесі орындау Түрі: Ішкі, сөреге коммутациялық шкафқа орнату мүмкіндігі бар. Процессорлардың саны 1-ден кем емес, процессордағы ядролардың саны 4-тен кем емес, процессор ағындарының саны 8-ден кем емес,

	процессордың архитектурасы 64 бит, процессордың жиілігі 2,0 ГГц-тен кем емес 32GB дейін кеңейту мүмкіндігі бар кем дегенде 4GB жүйелік жады Диск бөлімдері ыстық режимде ауыстыру мүмкіндігін қолдауы және 4 X HDD SATA 3.5" немесе 4 X 2,5" SATA SSD орнату мүмкіндігіне ие болуы тиіс, көлемі кемінде 4х дана көлемінде кемінде 12tb болатын SATA 3,5" корпоративтік HDD стандартының дискілерімен жинақталуы тиіс. RJ-45 LAN Ethernet порттары тасымалдау жылдамдығын кемінде 1Gbit/sec ұстап тұруы керек және олардың қолында кемінде 2 болуы керек 100В-240В диапазонындағы айнымалы токтың кіріс кернеуі, жиынтықтағы қуат адаптері. Жалпы саны кемінде 2 дана. Үздіксіз қуат көзі 1 ТИП орындау түрі-Қос түрлендіру және негізгі сипаттамалары бар On-line класындағы 5000ва қуаты бар тірек: Кіру: Номиналды кернеу - 380/400/415В 305-480в жүктеме кезінде батареяларға ауыспай кіріс кернеуінің диапазоны қуатты төмендетпей Кіріс жиілігі - 50/60 Гц, АВТО таңдау Жиілік диапазоны-40-70 Гц Қысқа тұйықталу тогы - 90 А Шығу: Номиналды кернеу - 200/208/220/230/240В + / - 1% On-line режимінде 90% - ға дейін, жоғары тиімді режимде 95% - ға дейін тиімділік Шығыс кернеуінің жалпы бұрмалануы < 2% Рұқсат етілген шамадан тыс жүктеме-102-110% = 120с, 110-125% = 60с Номиналды Шығыс жиілігі - 50/60 Гц, АВТО таңдау, жиілік түрлендіргіші Байланыс: RS-232 порты-бар, USB порты-бар (HID) USB және RS232 порттарын бір уақытта пайдалану мүмкін емес Жалпы саны кемінде 2 дана. Батарея модулі сыртқы батарея модулі батареяның қызмет ету мерзімін ұзарту үшін 6000ВА үздіксіз қуат көздеріне қосылуға арналған. Әрбір батарея Модулінің ішінде кернеуі 12 В және сыйымдылығы 9 Ач дейінгі қорғасын-қышқылды аккумуляторлар орнатылған. Жалпы саны кемінде 2 дана. Үздіксіз қуат көзі 2 ТИП орындау түрі-тірек, 3000ва класс класса-line Қос түрлендіру және негізгі сипаттамалары бар: Кіру: Номиналды кернеу 200/208/220/230 / 240В Жүктеме кезінде батареяларға ауыспай кіріс кернеуінің диапазоны - 176-276В Жиілік диапазоны-40-70 Гц Жиілік - 50/60 Гц, АВТО таңдау Қысқа тұйықталу тогы - 90 А Шығу: Номиналды кернеу 200/208/220/230/240В + / - 1% Крест факторы 3: 1 On-line режимінде 90% - ға дейін, жоғары тиімді режимде 95% - ға дейін тиімділік Шығыс кернеуінің жалпы бұрмалануы < 2% Рұқсат етілген шамадан тыс жүктеме - 102-110%: 120с, 110-125%: 60с Номиналды Шығыс жиілігі - 50/60 Гц, АВТО таңдау, жиілік түрлендіргіші Байланыс: RS-232 порты-бар USB порты-бар (HID) Жалпы саны кемінде 7 дана. 4.9.2. Жеткізуші келесі міндетті қадамдарды орындауы керек: 4.9.2.1. Физикалық орнату және кабельді байлау: 4.9.2.1.1. Серверлер мен коммутаторларды Тапсырыс берушінің телекоммуникациялық шкафтарына штаттық бекітпелер мен телескопиялық бағыттағыштарды пайдалана отырып орнату. 4.9.2.1.2. Жабдықтың қызып кетуіне жол бермейтін шкафтар ішіндегі ауа ағындарының дұрыс таралуын ұйымдастыру. 4.9.2.1.3. Жабдықты қуат желілерін резервтеу арқылы үздіксіз қуат көздеріне (UPS) қосу. 4.9.2.1.4. Кабельді ұйымдастырушыларды қолдана отырып, кабельдерді

	эстетикалық төсеу (кабельді басқару). 4.9.2.2. Серверлік жабдықты орнату (1 типті Сервер, 2 типті Сервер): 4.9.2.2.1. Firmware аналық платаларын, желілік адаптерлерді және RAID контроллерлерін қажет болған жағдайда өндірушінің соңғы тұрақты нұсқаларына жаңарту. 4.9.2.2.2. Қауіпсіз серверді қашықтан басқару порттарын орнату (IPMI/BMC/баламасы) оларға сәйкес IP мекенжайларын бөле отырып. 4.9.2.2.3. Диск ішкі жүйесін инициализациялау: операциялық жүйелердің ақауларға төзімділігін және қажет болған жағдайда дерекқорларды сақтауды қамтамасыз ету үшін тапсырыс берушінің архитектуралық жоспарына сәйкес қажетті деңгейдегі RAID массивтерін (RAID 1, 5, 10 және т.б.) құру және пішімдеу. 4.9.2.2.4. Қолданбалы бағдарламалық жасақтаманы орнатуға жібермес бұрын сервердің процессорлық және дискілік ішкі жүйелеріне негізгі жүктемелік тестілеу жүргізу. 4.9.2.3. Желілік жабдықты орнату (1, 2, 3, 4 типті қосқыштар, маршрутизатор): 4.9.2.3.1. Коммутаторлардың операциялық жүйелерін (микробағдарламаларын) ағымдағы тұрақты нұсқаларға жаңарту. 4.9.2.3.2. Негізгі желі параметрі: басқару интерфейстерін конфигурациялау (management VLAN), қауіпсіз қашықтан қол жеткізу протоколдарын орнату (SSH, HTTPS) және пайдаланылмаған қызметтер мен порттарды өшіру. 4.9.2.3.3. Жергілікті желіні архитектуралық баптау: виртуалды Жергілікті желілерді (VLAN) құру, статикалық және/немесе динамикалық маршруттауды, арналарды біріктіруді (LACP) және қызмет көрсету сапасы саясатын (QoS) Тапсырыс берушінің өтініші бойынша орнату. 4.9.2.3.4. Қол жеткізу қосқыштары үшін (соның ішінде 4 Тип): қажет болған жағдайда қосылатын соңғы құрылғылар үшін power over Ethernet (PoE/Poe+) қуат тарату саясатын орнату. 4.9.2.4. Ішкі кіру нүктелерін орнату және конфигурациялау. 4.9.2.4.1. "Бұралған жұп" типті кабельді пайдаланып және кіру қосқыштарынан power over Ethernet (PoE) технологиясы бойынша қуат беру арқылы жергілікті есептеу желісіне кіру нүктелерін қосу. 4.9.2.4.2. Кіру нүктелерінің микробағдарламасын (микробағдарламасын) аппараттық құрал өндірушісі ұсынған соңғы тұрақты нұсқаға жаңарту. 4.9.2.4.3. Статикалық немесе динамикалық IP мекенжайын, уақытты синхрондауды (NTP) және қашықтан қорғалған басқару параметрлерін орнату. 4.9.2.4.4. Радио интерфейстерін орнату (2.4 ГГц және 5 ГГц): біркелкі қамтуды қамтамасыз ету және көршілес нүктелер арасындағы өзара радио кедергілерді болдырмау үшін оңтайлы, бір-біріне сәйкес келмейтін жиілік арналарын таңдау және таратқыш қуатын реттеу (Tx Power). 4.9.2.4.5. Тапсырыс берушінің өтінімі бойынша трафикті виртуалды жергілікті желілер (VLAN) бойынша бөле отырып, қажетті сымсыз желілерді (SSID) құру. 4.9.2.4.6. Қажет болса, заманауи қауіпсіздік және шифрлау саясатын орнату. 4.9.2.4.7. Қажет болса, байланыс сеанстарын үзбей ғимарат бойынша жылжу кезінде клиенттік құрылғылардың кіру нүктелері арасында үздіксіз ауысуын қамтамасыз ету үшін параметрлерді реттеу. 4.9.2.5. Барлық конфигурацияланған жабдықты тұтынушының қолданыстағы желісіне қосу және желінің байланысын тексеру. 5.

	Бағдарламалық жасақтамаға қойылатын талаптар. 5.1. Бағдарламалық жасақтама 9 ай мерзімге, 2027 жылдың 1 сәуірінен 2027 жылдың 31 желтоқсанына дейін берілуі керек. 5.2. Жеткізуші төмендегілерден төмен емес сипаттамалары бар ақпараттың ағып кетуін болдырмайтын бағдарламалық қамтамасыз етуді орналастыру және іске қосу жөніндегі міндеттер кешенін орындауы тиіс: Ақпараттың ағып кетуін болдырмау жүйесіне бағдарламалық қамтамасыз етуді пайдалану құқығына Лицензия осы техникалық ерекшелікте белгіленген шарттарда Тапсырыс берушінің желілік инфрақұрылымында Қазақстан Республикасының аумағы шегінде 9 ай мерзімге көбейту тәсілін пайдалану құқығымен қарапайым айрықша емес лицензия шарттарында берілуге тиіс. Техникалық қолдау. Техникалық қолдау кезеңі лицензия іске қосылған сәттен бастап 9 айға берілуі керек. 1. Кепілдік, қолдау мерзімі және лицензиялар. Әлеуетті Жеткізуші кепілдік қолдауын ұсынады. Техникалық қолдау шеңберінде жеткізуші: * бағдарламалық өнім нұсқаларын жаңарту; * патчтар мен хотфикстерді жүктеңіз; * 24/7 режимінде қашықтықтан қолдауды қамтамасыз етіңіз. 5. Талап етілетін іс-шаралар тізбесі: * жергілікті орталықтандырылған басқару серверін орналастыру және конфигурациялау. * лицензиялар мен сервистік келісімшарттарды белсендіру. * орталықтандырылған басқару серверін Windows Active Directory жүйесімен біріктіру. * жалған позитивтерді болдырмау және алып тастау тізімдерін жасау үшін уақытша қауіпсіздік саясатын құру. 6. Қосымша талаптар. Жеткізу тапсырыс берушінің инфрақұрылымын іске қосуды және интеграциялауды қоса алғанда, Тапсырыс берушінің атына біржолғы және толық көлемде жүзеге асырылуға тиіс. 7. Ақпараттың ағып кетуін болдырмайтын бағдарламалық қамтамасыз етуге қойылатын талаптар (кем емес, кем емес): * лицензиялар саны-кеңейту мүмкіндігімен ақпараттың ағып кетуін болдырмауға арналған кемінде 280 лицензия (DLP) ; * әлеуетті өнім беруші жеткізетін бағдарламалық қамтамасыз ету отандық өндірушінің әзірлемесі болуы тиіс. 8. Жүйенің мақсатына қойылатын талаптар. Жүйе келесі міндеттерді шешуді қамтамасыз етуі керек: * келесі арналар арқылы құпия ақпаратты тұтынушының есептеу желілерінің периметрінен тыс пайдаланушылардың кездейсоқ немесе әдейі жіберуі оқиғаларының мониторингі: * электрондық пошта (POP3, SMTP, IMAP, MAPI, HTTP хаттамалары, соның ішінде шифрланған аналогтар); * электрондық пошта арқылы жіберілген электрондық пошта (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex, Zimbra және т. б.); * Facebook, Odnoklassniki, Vk, Twitter, Instagram, LinkedIn, Bitrix24 әлеуметтік медиа форумдарында чаттардағы, посттардағы және әлеуметтік медиа форумдардағы хабарламаларды екі жақты ұстау; * жедел хабар алмасу құралдары – Telegram, Skype, SIP, Viber, Microsoft Lync, Mail.Ru Агент, WhatsApp, PSI, Yahoo! Messenger, MS Teams, Discord, Slack, WeChat, XMPP, Zoom, RocketChat, Signal, eXpress, VK Teams, TrueConf және т. б., соның ішінде шифрлауды қолдану; * сыртқы дискілерге файлдарды жазу; * жергілікті желілік ресурстарға файлдарды жазу; *

	файлдарды бұлтты сақтау қызметтеріне жіберу (iCloud, Dropbox, Google Drive, OneDrive, бұлт Mail.ru, Яндекс. Диск); * файлдарды жергілікті және желілік принтерлерге басып шығаруға жіберу; * FTP және FTPS протоколдары арқылы компьютерлік желілерде файлдарды тасымалдау; - нақты уақыт режимінде бақыланатын жұмыс станциясының микрофонынан аудио ағынды бақылау арқылы ауызекі тілде құпия ақпаратты жариялау оқиғаларын бақылау; - нақты уақыт режимінде пайдаланушының компьютерінің жұмыс үстелінің бейне көрінісіне қашықтан қол жеткізуді қолдау; - бақыланатын жұмыс станциясының файлдық жүйесінде құпия құжаттардың болуын немесе пайда болуын нақты уақыт режимінде бақылау; мұрағат бойынша, оның ішінде хаттарға қосылған файлдарда толық мәтінді іздеу мүмкіндігімен барлық шығыс және кіріс электрондық хабарламаларды жинау және сақтау; - Перифериялық құрылғыларды пайдалануды бақылау (сыртқы дискілерге қол жеткізу және көшіру, қосылу аудиті және әртүрлі мақсаттағы сыртқы құрылғыларға қол жеткізу); - скриншоттарды түсіру, компьютердің жұмыс уақыты/тоқтап қалуы туралы ақпаратты жинау, қолданылатын қосымшалар (соның ішінде WinRT (Metro) және виртуалды жұмыс үстелдері), сондай-ақ ұсталған ақпаратты статистикалық және оқиғаларға талдау жасау арқылы компания қызметкерлерінің жұмыс уақыты мен ресурстарын пайдалану тиімділігін бақылау; - жеке бағдарламалық қосымшаларды іске қосуға тыйым салу; -белгілі бір веб-ресурстарға және олардың функционалдығына қол жеткізуді бұғаттау мүмкіндігі (берілген қауіпсіздік саясаты негізінде); - жеке процестердің желілік трафигін блоктау; - SMTP, HTTP және MAPI хаттамалары бойынша (оның ішінде шифрлауды пайдалана отырып) хабарламалардың мазмұны мен атрибуттық талдауы және кірістірілген деректер негізінде белгілі бір ақпаратты қамтитын Шығыс хабарламалардың берілуін бұғаттау мүмкіндігі. - Бұғатталған мазмұнды ұстап қалу мүмкіндігімен (берілген қауіпсіздік саясаты негізінде)мазмұнды және атрибуттық талдау негізінде алынбалы тасымалдағыштарға деректерді беруді бұғаттау мүмкіндігі; - Мазмұнды және атрибуттық талдау негізінде алмасу буфері арқылы деректерді беруді бұғаттау мүмкіндігі (берілген қауіпсіздік саясаты негізінде); - Контенттік және атрибуттық талдау негізінде (берілген қауіпсіздік саясаты негізінде) жергілікті немесе желілік принтерлер арқылы (агенттен іске қосылған кезде)деректерді беруді бұғаттау мүмкіндігі; - Файлды кеңейту немесе процестер бойынша сүзу мүмкіндігімен қалталармен және файлдармен (оқу, жазу, жою, атын өзгерту, кіру құқықтарын өзгерту) файлдық операцияларды тексеру мүмкіндігі. 9. Деректерді сақтау және өңдеу функциялары Деректерді сақтау және өңдеу бөлігінде жүйе мыналарды қамтамасыз етуі керек: * жүйе жинайтын барлық деректерді Microsoft SQL Server, Microsoftacle, PostgreSQL 9.3 және одан жоғары нұсқаларында, MySQL 5.7.09 және одан жоғары нұсқаларында, SQLite (таңдау үшін)ДҚБЖ-да сақтау мүмкіндігі; * SQLite кіріктірілген ДҚБЖ жеткізілім жиынтығында; * қауіпсіздік саясатының іске қосылуына қарамастан барлық

	ұсталған деректерді сақтау; * әр түрлі серверлерде орналасқан мәліметтер базасымен жұмыс істеуді қолдау; * файлдарды дерекқорға емес, сервер дискісіне сақтау мүмкіндігі, шағын көлемді файлдарды дискіге сақтаудан алып тастау мүмкіндігі, бұл ретте дерекқорға файлдарға қатысты жолдар орналастырылады; * жеке мәліметтер базасы үшін кескінді, мөрді және сөйлеуді тануды қосу/өшіру мүмкіндігі; * ротация тобындағы мәліметтер базасында ақпаратты сақтау ұзақтығын реттеу мүмкіндігі, * Дерекқордың мазмұнын сақтай отырып, әкімші консолі арқылы дерекқорды қолмен өшіру мүмкіндігі; * дерекқор мазмұнын әкімші консолі арқылы қолмен тазалау мүмкіндігі; * маңызды ақпаратты ретроспективті іздеуді жүзеге асыру үшін жүйеге қосыла отырып, мәліметтер базасын мұрағаттау мүмкіндігі; * пайдаланушының ұсталған ақпаратты іріктеп жою мүмкіндігі; * бір дерекқорды топтағы барлық дерекқорлар бойынша іздеу операциялары орындалатын және деректерді жазу тек белсенді түрде орындалатын Дерекқордың айналуын қолдайтын топтарға біріктіру мүмкіндігі; * дерекқорды айналдырудың бірнеше шарттарын теңшеу мүмкіндігі: Жалпы деректер көлемі, дерекқор өлшемі, іздеу индекстерінің өлшемі, дискідегі файл өлшемі, уақыт аралығы, жазбалар саны, айналу процесін іске қосу белгілі бір уақыт аралығына реттелуі мүмкін; * ротация процесі басталғанға дейін, ротация аяқталғаннан кейін және ротация қатесі болған кезде сценарийлердің орындалуын теңшеу мүмкіндігі, CMD, PowerShell, script host, Python сценарийлерінің орындалуына қолдау көрсетіледі; * "round robin" алгоритміне сәйкес екі және одан да көп деректер базасы немесе деректер базасы бойынша жүктемені теңестіру мүмкіндігі: жүйеге келіп түскен барлық деректер дерекқорға кезекпен жазылады; * Деректерді жаңарту, жою және іздеу операцияларын орындау кезінде жүйенің өнімділігін арттыруға мүмкіндік беретін әртүрлі ақпарат беру арналары арқылы ұсталған деректерді параллель өңдеу режимін қолдау; * деректер уақыт белдеуіне, деректер түріне, деректер көзіне, пайдаланушының немесе компьютердің доменге немесе кез келген ad контейнеріне оның аты, SID немесе GUID, IP мекенжайы және басқа атрибуттық ақпаратқа сәйкес ақпаратты қай қоймаға жазу керектігін реттеу үшін Деректер базасына және айналмалы топтарға деректерді жазу ережелерін теңшеу мүмкіндігі; * еншілес бақыланатын желілерден немесе кеңселерден келіп түскен деректерді аумақтық бөлінген ұйымдық құрылымдардағы жоғары тұрған серверлерге автоматты түрде көшіру мүмкіндігі; * деректер репликация серверіне оралып, содан кейін қайталанған кезде дұрыс емес репликация параметрінен қорғау; * еншілес бақыланатын желілерден немесе кеңселерден келіп түскен деректерді жоғары тұрған серверлерге қайта бағыттау мүмкіндігі; * деректерді репликациялау үшін кестені теңшеу мүмкіндігі; * жүйе істен шыққан жағдайда репликацияланатын деректердің сақталуы мен тұтастығын қамтамасыз ету үшін дискідегі деректердің репликация кезегін сақтау мүмкіндігі; * репликация кезегі толған кезде сервер жаңа деректерді қабылдауға тыйым салады; * кезек

	толып кеткен кезде репликацияны өткізіп жіберу мүмкіндігі; * деректерді репликациялау статистикасын көрсету; * жедел жадта сақтаумен салыстырғанда олардың сақталуын арттыратын агенттерден келетін деректердің кезегін дискіде сақтау мүмкіндігі; * іздеу индекстерін тазарту және жаңарту режимін таңдау мүмкіндігі (қолмен және автоматты режимдер); * мәндері индекстелетін электрондық пошта тақырыптарының өрістерін сүзгілеу кезінде ұсталған электрондық пошта тақырыптарының мазмұнын индекстеу мүмкіндігі; * ұсталған деректер бойынша асинхронды іздеуді жүзеге асыру мүмкіндігі (ақпаратты берудің бірнеше арналары бойынша параллельді іздеуді жүргізу кезінде нәтижелерді көрсету оларды алу шамасына қарай орындалады); * деректер базасында және ротация топтарында сақталған және индекстелген деректер бойынша кешенді статистиканы қарау. 10. Қолдау көрсетілетін файл пішімдері Жүйе келесі форматтағы файлдарды өңдеуді қолдауы керек: •Adobe Acrobat (*.pdf) •Ami Pro (*.sam) •Ansi Text (*.txt) •ASCII Text * ASF (метадеректер) (*.asf) •CSV (Comma-separated values) (*.csv) •DBF (*.dbf) •DjVu •DWG •DXF •EBCDIC * EML файлдары (Outlook Express сақтаған электрондық пошталар) (*.eml) •Enhanced Metafile Format (*.emf) * Eudora MBX хабарлама файлдары (*.mbx) •Flash (*.swf) •GZIP (*.gz) •HTML (*.htm, *.html) * JPEG (метадеректер) (*.jpg) •Lotus 1-2-3 (*.wk?, *.123) * MBOX электрондық пошта мұрағаты (Thunderbird қоса) (*.mbx) * MHT мұрағаттары (Internet Explorer сақтаған HTML мұрағаттары) (*.mht) * MIME хабарламалары * MSG файлдары (Outlook сақтаған электрондық пошталар) (*.msg) •Microsoft Access (*.mdb) •Microsoft Access 2007 (*.accdb) •Microsoft Outlook (OST) •Microsoft Document Imaging (*.mdi) •Microsoft Excel (*.xls)Microsoft Excel 2003 XML (*.xml) •Microsoft Excel 2007 (*.xlsx) * Microsoft Outlook Express 5 және 6: хабарламалар базасы (*.dbx) •Microsoft PowerPoint (*.ppt) •Microsoft Rich Text Format (*.rtf) •Microsoft Searchable Tiff (*.tiff) •Microsoft Word for DOS (*.doc) •Microsoft Word for Windows (*.doc) •Microsoft Word 2003 XML (*.xml) •Microsoft Word 2007 (*.docx) •Microsoft Works (*.wks) * MP3 (метадеректер) (*. mp3) * OpenOffice 1, 2 және 3 нұсқалары: құжаттар, электрондық кестелерпрезентациялар (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (Oasis Open document Format қоса алғанда) * OST(Microsoft Outlook ішкі форматы) •Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw) •TAR (*.tar) •TIFF (*.tif) •TNEF (winmail.dat) •Treepad HJT (*.hjt) * Unicode (Ucs16, Mac немесе Windows байттарының реті немесе UTF-8) •Windows Metafile Format (*.wmf) *WMA бейне (метадеректер) (* .wma) * WMV бейне (метадеректер) (*.wmv) •WordPerfect 4.2 (*.wpd, *.wpf) * WordPerfect (5.0 тал) (*.wpd, *.wpf) •Write (*.wri) * XBase (соның ішінде FoxPro, dBase және басқа XBase үйлесімді форматтар) (*.dbf) •XML Paper Specification (*.xps) •XSL •XyWrite •ZIP (*.zip) Сонымен қатар, жүйе графикалық форматтағы файлдардағы (BMP, JPEG,

	PNG, TIFF, GIF және басқалары) мәтіндік ақпаратты, сондай - ақ таңбаларды оптикалық тану (OCR) арқылы PDF және DjVu файлдарын тануды және талдауды қамтамасыз етуі керек. 11. Пайдаланушыларды басқару мүмкіндіктері. Жүйеде қамтамасыз етілуі керек: * бақыланатын пайдаланушылардың барлық сәйкестендіру ақпаратын қамтитын ішкі пайдаланушы карталарын жасау; * тиісті пайдаланушыларға лицензия бермей пайдаланушы карточкаларын жасау мүмкіндігі, мысалы, ішкі абоненттермен қарым-қатынасын бақылау мақсатында сыртқы пайдаланушыға карточка жасау; қызметкер жұмыстан шығарылған жағдайда-пайдаланушының карточкасын оның компания қызметкерлерімен кейінгі қарым-қатынасын бақылау үшін сақтау мүмкіндігі; * бағдарлама базасында пайдаланушы профильдерінің саны бойынша шектеулердің болмауы; * пайдаланушы туралы жалпы ақпаратты пайдаланушы картасына байланыстыру мүмкіндігі: аты-жөні, ұйымы, бөлімшесі, лауазымы, телефондары, мекен-жайы және т. б., * Active Directory-ден пайдаланушының деректер картасына автоматты түрде байланыстыру мүмкіндігі (электрондық пошта мекенжайлары, ұйымның, бөлімшенің және пайдаланушының лауазымының атаулары, пайдаланушының сипаттамалары мен фотосуреттері); * пайдаланушы картасында тиісті Active Directory пайдаланушысының ерікті өрістерінен ақпаратты көрсету мүмкіндігі * ішкі есептік жазбалар негізінде жүйемен жұмыс істейтін пайдаланушыларды аутентификациялау мүмкіндігі (кіру кезінде Пайдаланушының аты мен паролін сұрай отырып); * пайдаланушының жеке куәліктерін автоматты түрде байланыстыру мүмкіндігі (Slack идентификаторлары, ICQ нөмірлері, Google Hangouts есептік жазбалары, Skype, Telegram, Viber, WhatsApp, Yahoo, әлеуметтік медиа идентификаторы, SIP, электрондық пошта мекенжайлары, соның ішінде XMPP және Microsoft Lync есептік жазбалары, сондай-ақ IP мекенжайлары мен фотосуреттері). кейінгі сәйкестендіру үшін пайдаланушы профиліне; * пайдаланушы картасына автоматты түрде қосылатын БАЙЛАНЫС АҚПАРАТЫНЫҢ түрлерін таңдау мүмкіндігі * байланыс ақпаратын автоматты түрде байланыстыру процесінен белгілі бір пайдаланушыларды алып тастау мүмкіндігі * байланыс ақпаратын автоматты түрде байланыстыру процесінен белгілі бір ақпаратты (IP мекенжайы, электрондық пошта мекенжайы, Компьютер атауы, Skype, ICQ, Viber, Telegram, WhatsApp, MS Exchange, әлеуметтік желі идентификаторы) алып тастау мүмкіндігі * жүйенің жекелеген компоненттеріне де, жекелеген деректерге де қол жеткізу құқықтарын ажырату мүмкіндігі пайдаланушы рөлдерді тағайындайтын әр түрлі топтар үшін (мысалы, "жүйелік әкімші" - жүйенің техникалық параметрлерін өзгертуге ғана қол жеткізу-ұсталған ақпаратты қарауға қол жеткізбестен;" бөлімше басшысы " – белгілі бір функциялардың белсенділігі туралы ақпаратты қарауға ғана қол жеткізу қызметкерлер-оқиғалар туралы немесе басқа қызметкерлердің белсенділігі туралы ақпаратты қарауға рұқсатсыз; "қауіпсіздік офицері" – тек қауіпсіздік саясатына және инциденттерге қол жеткізу-қызметкерлердің белсенділігі туралы ақпаратты қарауға қол жеткізусіз және т. б.)

	пайдаланушылардың аутентификация жүйесін пайдалана отырып; * синхрондау жүргізілетін домендерді (Домен нысандарын) және домен контроллерлерін көрсете отырып, Active Directory-мен интеграциялау мүмкіндігі; * Active Directory с пайдаланушыларын синхрондау мүмкіндігі. пайдаланушы карталарын автоматты түрде құру және жою, Active Directory-ге жазбаларды қосу және жою кезінде, бұрын белгісіз пайдаланушы ақпараты анықталған кезде автоматты түрде карталар жасау; * Active Directory-дегі пайдаланушының сәйкестендіру деректерінің өзгеруін пайдаланушы карталарындағы деректермен синхрондау кестесін және синхрондалатын деректерді теңшеу мүмкіндігімен автоматты түрде синхрондау; * жүйемен жұмыс істейтін пайдаланушылардың іс-әрекеттері мен авторизация журналын жүргізу. 12. Жүйенің техникалық және функционалдық сипаттамаларына қойылатын талаптар. Жүйе бақыланатын желідегі трафикті ұстап қалудың бірнеше схемаларын, сондай-ақ олардың комбинацияларын қолдауы керек: * желілік қосқыштан деректерді орталықтандырылған ұстау; * пайдаланушылардың жұмыс станцияларынан деректерді ұстау; * пошта серверлері арқылы жіберілген электрондық поштаны ұстау; * HTTP(S)-прокси-сервер арқылы жіберілген трафикті ұстау. 13. Деректерді орталықтандырылған ұстап қалуды іске асыруға қойылатын талаптар Жүйе қамтамасыз етуі керек: * шифрлауды пайдаланбайтын хаттамалар арқылы жіберілетін деректерді орталықтандырылған ұстау (FTP, HTTP, IMAP, POP3, SMTP, MAPI, MRA (Mail.Ru Агент), OSCAR (AIM, ICQ), XMPP (Jabber), YMSG (y!M) трафикті шағылыстыру арқылы; * HTTP протоколы бойынша MIME типі бойынша және атрибуттар жиынтығы бойынша (IP-адрес, порт, HTTP-әдіс, web-өріс және т. б.), оның ішінде күрделі шарттарды ("және", "немесе", "емес")пайдалана отырып жіберілетін ұсталатын деректерді сүзу; * IP мекенжайлары (жеке және ауқым) және жеке MAC мекенжайлары, хаттамалар, есептік жазбалар және электрондық пошта мекенжайлары, жедел хабар алмасу жүйелерінің есептік жазбалары бойынша ұстап қалудан ерекшеліктерді орнату; 14. Жұмыс станцияларынан деректерді ұстап қалуға қойылатын талаптар Жүйе тәуелсіз бағдарламалық басқару модульдерін тікелей ұйым желісінің жұмыс станцияларына орнатуды қолдауы керек. Жұмыс станцияларын басқару агенті-желідегі жұмыс станцияларына Орнатылатын тәуелсіз бағдарламалық модуль. Модуль шифрланбаған желілік трафикті ұстап қалуды, сондай-ақ шифрлауды пайдаланатын хаттамалар бойынша берілген SSL-трафикті және деректерді ұстап қалуды жүзеге асыруы тиіс. Модуль пайдаланушының әрекетін бақыланатын жұмыс станциясына түсіруі керек. Жұмыс станцияларын бақылау мыналарды қамтамасыз етуі керек: * модульдерді орталықтандырылған орнату мүмкіндігі - бір басқару консолінен немесе домендік топтық саясат құралдарынан (MSI пакетін қолдана отырып) және қолмен орнату (графикалық интерфейсі бар модульдің жеке EXE инсталляторын қолдана отырып); * қолмен орнату үшін орталықтандырылған модуль дистрибутивін орнату; * шифрланбаған протоколдар арқылы жіберілетін деректерді ұстап қалу мүмкіндігі (POP3, SMTP,

	MAPI (MAPI over RPC, MAPI over RPC over HTTP, MAPI over HTTP), OSCAR, XMPP (Jabber), HTTP, FTP, MMP (Mail.Ru Агент), YIM); * шифрланған хаттамалар арқылы жіберілетін деректерді (SSL/TLS шифрлауды қолдана отырып), соның ішінде электрондық поштаны жіберу және жедел хабар алмасу хаттамаларын, HTTPS, FTPS, Skype, SIP, сондай-ақ Viber, WhatsApp, Google Hangouts, Telegram және Microsoft Lync қосымшаларында жіберілген деректерді ұстау мүмкіндігі; SSL/TLS шифрлауды қолдана отырып, хаттамалар арқылы жіберілген деректерді ұстап алу сандық сертификатты ауыстыру арқылы жүзеге асырылады. Бұл ретте жүйе құратын сертификаттарда куәландырушы орталықтың ерікті атауын көрсету мүмкіндігі, сондай-ақ әртүрлі SSL/TLS-қосылымдарды ұстап алған кезде әртүрлі сертификаттарды пайдалану үшін икемді ауыстыру баптау мүмкіндігі қолдау табуы тиіс; * S/MIME стандартына сәйкес қорғалған цифрлық қолтаңбасы бар (хаттарға салынған файлдарды қоса алғанда) Шифрланған пошта хабарламаларын ұстау және автоматты түрде шифрын ашу мүмкіндігі; * ұсталған деректердің атрибуттары мен мазмұнына негізделген трафикті сүзу және бұғаттау саясатын құру мүмкіндігі; * HTTP / HTTPS протоколы арқылы жіберілетін деректерді сүзу мүмкіндігі; * IP мекенжайлары (жеке және ауқым), хаттамалар, жүйелік пайдаланушы тіркелгілері, есептік жазбалар және электрондық пошта мекенжайлары, жедел хабар алмасу жүйелерінің тіркелгілері, процесс атрибуттары, сыртқы құрылғылар және жергілікті желі ресурстары бойынша ұстап қалудан ерекшеліктерді икемді конфигурациялау мүмкіндігі; * берілген саясаттар негізінде SMTP (s) хаттамасы бойынша Шығыс хабарламаларды жіберуді бұғаттау мүмкіндігі; * берілген саясаттар негізінде HTTP(S) протоколы бойынша Шығыс хабарламаларды жіберуді бұғаттау мүмкіндігі; * веб-ресурстарға кіруді бұғаттау мүмкіндігі; * зиянды бағдарламалар мен қызметтік бағдарламалардың паразиттік HTTP(S) трафигін бұғаттау мүмкіндігі; * алынбалы тасымалдағыштарға мазмұн немесе атрибуттар бойынша жіберуді бұғаттау мүмкіндігі; * жергілікті немесе желілік принтерлерге басып шығаруға жіберуді бұғаттау мүмкіндігі (агенттен іске қосылған кезде); * алмасу буферін мазмұн немесе атрибуттар бойынша бұғаттау мүмкіндігі; * процестердің желілік трафигін олардың атрибуттары мен атқарушы файлдардың хэш функцияларының мәні негізінде блоктау; * құрылғыларды құлыптау, процестерді іске қосу, Желілік процестер трафигі және MAPI трафигі туралы жұмыс станциясының пайдаланушы хабарландыруларын орнату; * Facebook, Odnoklassniki, Vk, Twitter, Instagram, LinkedIn, Bitrix24 әлеуметтік желілеріндегі пайдаланушылардың Web-коммуникацияларын ұстап алу. Бұл ретте: чаттардағы хабарламаларды екі бағытты ұстап алу; мәртебелерді ұстап алу; жарияланымдар мен суреттерге түсініктемелерді ұстап алу, әлеуметтік желілер форумдарындағы пікірлерді барлық пікірлер блогын бақылай отырып ұстап алу қолдауға тиіс; * кіріс және шығыс веб-поштаны ұстау (gmail, mail.ru, rambler, yandex, yahoo, hotmail); * сыртқы дискілерге, принтерлерге, бұлтты қоймаларға және

	пайдаланушылар мен терминал серверлерінің жергілікті желілік ресурстарына жіберілетін деректерді бақылау; * агенті бар компьютердегі файлдар мен қалталарды өзгерту, оқу, жою сияқты файлдық операцияларды тексеру; * файлдық операциялар аудиті, ақпараттың жазылуын бақылау және пайдаланушылардың жергілікті желі ресурстарына кіруіне тыйым салу; * веб-интерфейсті және жұмыс үстелі қосымшаларын (Dropbox, OneDrive, Google Drive, Yandex.Drive, Apple iCloud, бұлт) пайдалану кезінде файлдық операциялардың аудиті, ақпараттың берілуін бақылау және пайдаланушылардың ақпаратты сақтаудың бұлтты қызметтеріне кіруіне тыйым салу Mail.Ru); * файлдық операциялар аудиті, ақпараттың жазылуын бақылау және пайдаланушылардың параметрлерін ескере отырып, сыртқы ақпарат жинақтағыштарының әртүрлі кластарына кіруіне тыйым салу (идентификатор және өндірушінің аты, өнім идентификаторы және атауы, сериялық нөмір); * жұмыс станциясына қосылған сыртқы құрылғылар үшін пайдалану аудиті және кіруді бақылау және олардың параметрлерін ескере отырып кіруді бұғаттау (идентификатор және өндірушінің аты, өнім идентификаторы және атауы, сериялық нөмірі, Құрылғы түрі); * компьютердің жұмыс уақыты/тоқтап қалуы туралы статистиканы жинау мүмкіндігі; * пайдаланушылардың компьютерлерінде қосымшалардың іске қосылуын, сондай-ақ әр қосымшаның жұмыс ұзақтығын бақылау (мысалы, корпоративті желіде қажетсіз немесе тыйым салынған бағдарламалық жасақтаманың қолданылуын бақылау); * процесс атауы, атқарушы файл атрибуттары және хэш функциясының мәні негізінде бақыланатын жұмыс станциясында жеке бағдарламалық қосымшаларды іске қосуға тыйым салу; * берілген интервалмен, сондай-ақ оқиға бойынша пайдаланушының жұмыс үстелінің скриншоттарын түсіру мүмкіндігі (PrintScreen пернесін басу, белсенді қолданба терезесін немесе шолғыш қойындысын өзгерту, белгілі бір Қолданбаны іске қосу); * жеке процестердің белсенділігін ұстап қалудан алып тастауды қолдай отырып, алмасу буферіне орналастырылған және енгізілген деректерді ұстап алу; * жеке процестердің белсенділігін ұстап қалудан алып тастауды қолдай отырып, алмасу буферіне орналастырылған деректерді ұстап алу; * жеке процестердің белсенділігін ұстап қалудан алып тастау мүмкіндігімен пайдаланушы пернетақтадан ("кейлоггер") енгізетін деректерді бақылау; * нақты уақыт режимінде жұмыс станцияларына қосылған микрофондардан келетін аудио ағынды тыңдау; * нақты уақыт режимінде пайдаланушының жұмыс үстелінің бейне кескінін қашықтан қарау мүмкіндігі; * пайдаланушының жұмыс станциясының дискілеріндегі құпия файлдарды автоматты түрде іздеу (аты бойынша, берілген атрибуттар немесе хэш функцияларының мәндері бойынша); * әр түрлі AD нысандарына, жеке компьютерлерге (компьютер топтарына) және көрсетілген SID бар пайдаланушыларға қатысты модульдердің функционалдығын теңшеу; * модуль параметрлерін іске қосу шарттарын таңдау, мысалы, серверге қосылу, белсенді VPN қосылымының болуы, ерікті берілген шарт; * жұмыс станциясындағы модульді пайдаланушы рұқсатсыз жоюдан қорғау мүмкіндігі; *

	модульді жұмыс станциясында жасыру мүмкіндігі (процестерді, қызметтерді, орнату файлдары мен қалталарды жасыруды қоса); * бақыланатын жұмыс станциясының тапсырмалар тақтасында жүйе белгішесін қосымша көрсету; * жұмыс станциясын корпоративтік желіден тыс шығарған жағдайда модульдің функционалдық мүмкіндіктерін (офлайн режим) сақтау, ұстап қалудың барлық деректерін сақтау. Жүйенің серверлік бөлігімен байланысты автоматты түрде қалпына келтіру; * модульдің офлайн режимін орнату мүмкіндігі; Жүйе жұмыс станциясының бақылау модульдерінің күйі бойынша статистиканы қадағалап, көрсетуі керек: * әрбір модульден серверге деректер түсімі, * модульмен басқарылатын пайдаланушылар; * қосылған сыртқы құрылғылар * ұсталатын деректер түрлері (хаттамалар). Статистика деректері экспорттау үшін қолжетімді болуы тиіс. 15. Прокси арқылы жіберілген HTTP трафигін ұстауға қойылатын талаптар. Прокси-сервер арқылы HTTP және HTTPS протоколдары арқылы жіберілген деректерді ұстау ICAP протоколы арқылы прокси-сервермен біріктіру арқылы жүзеге асырылуы керек. Бұл ретте мынадай мүмкіндіктер қамтамасыз етілуі тиіс: - HTTP (S) протоколы арқылы жіберілген деректерді ұстау; -HTTP(S) протоколы бойынша атрибуттар жиынтығы бойынша (IP-адрес, порт, HTTP-әдіс, web-өріс және т. б.), оның ішінде күрделі шарттарды ("және", "немесе", "емес")пайдалана отырып ұсталатын деректерді сүзу; -HTTP(S) протоколы бойынша IP мекенжайы бойынша, оның ішінде мекенжайлар ауқымы бойынша АҚ және қара ерекшеліктер тізімін теңшеу мүмкіндігімен ұсталатын деректерді сүзу; - HTTP(S) протоколы бойынша жіберілетін хабарларды бұғаттау кезінде көрсетілетін хабарламаны теңшеу мүмкіндігімен берілетін деректердің мазмұндық және атрибуттық талдауы негізінде белгілі бір ақпаратты қамтитын жіберуді бұғаттау; - деректерді сақтау және өңдеу модуліне деректерді жіберу кезегін берілетін элементтердің максималды мөлшері, кезектегі элементтердің максималды саны, дискіде де, жедел жадта да кезекті сақтау мүмкіндігі бар кезектің максималды жалпы мөлшері бойынша конфигурациялау; - модульдің нақты уақыттағы жұмыс статистикасын көрсету; - сүзу және құлыптау ережелерін импорттау және экспорттау. 16. Пошта серверлері арқылы жіберілген электрондық поштаны ұстауға қойылатын талаптар Microsoft Exchange Server, IBM Lotus Domino, Sendmail, hMailServer және басқа да бағдарламалық қамтамасыз ету негізінде орналастырылған пошта серверлері арқылы жіберілетін поштаны ұстап алу POP3, IMAP, SMTP хаттамалары бойынша пошта серверлерімен интеграциялау жолымен, сондай-ақ MS Exchange коннекторының көмегімен жүзеге асырылуы тиіс 17. Бақыланатын ағып кету арналарының тізіміне қойылатын талаптар Электрондық поштаны бақылауға қойылатын талаптар. Жүйе келесі мүмкіндіктерді қоса алғанда, ақпаратты электрондық пошта арқылы жіберуді бақылауды қамтамасыз етуі керек: - шифрланбаған және шифрланған (SSL) протоколдар үшін пошта хабарламаларын ұстау-POP3, SMTP, IMAP, MAPI және шифрланған аналогтар; - Электрондық поштаның мазмұнын автоматты түрде транскрипциялайтын

	S/MIME қорғалған Электрондық пошта стандартын қолдайтын пошта бағдарламалары арқылы жіберілген пошта хабарламаларын ұстау; - POP3, SMTP, IMAP (таңдау үшін) хаттамалары бойынша пошта серверлерімен (Microsoft Exchange, IBM Lotus Domino, Postfix, Sendmail және т. б. негізінде)интеграциялау арқылы пошта хабарламаларын ұстап қалу; - MICROSOFT Outlook және Microsoft Exchange Server арасындағы MAPI протоколы арқылы (соның ішінде шифрлауды пайдалану арқылы) microsoft Outlook бағдарламасымен біріктіру арқылы электрондық пошта хабарларын тыңдау; - HTTP(s) протоколы (yandex, mail.ru, rambler, gmail, yahoo, hotmail және т.б.д.); - перехват и анализ файлов-вложений почтовых сообщений; - автоматическое обнаружение почтовых сообщений и почтовых вложений, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - smtp(S), HTTP(S), MAPI протоколдары арқылы шығыс пошта хабарламаларын мазмұнды және атрибуттық хабарламаларды талдауды қолдана отырып, берілген қауіпсіздік саясатына негізделген блоктау; -электрондық хаттарды HTML пішімінде және Microsoft Outlook бағдарламасымен үйлесімді пішімде сақтау мүмкіндігі; - возможность поиска по тексту и атрибутам почтовых сообщений и файлов, переданных по почте. 18. IM тұтынушыларын бақылауға қойылатын талаптар Жүйе КЕЛЕСІ мүмкіндіктерді қоса АЛҒАНДА, IM клиенттері арқылы ақпараттың жіберілуін бақылауды қамтамасыз етуі керек: - Viber, Telegram (веб-нұсқасын қоса), WhatsApp (веб-нұсқасын қоса), Skype (веб-нұсқасын қоса), Microsoft Lync, Microsoft Teams (веб-нұсқасын қоса), Discord (веб-нұсқасын қоса) мессенджерлеріндегі мәтіндік хабарларды тыңдау.), Hangouts, Slack (веб-нұсқасын қоса), WeChat, Signal, Express, Vk Teams. Агент Mail.ru, ICQ10, ICQ, RocketChat, СОНДАЙ-ақ SIP, OSCAR, XMPP (HTTP арқылы XMPP қоса алғанда), YMSG протоколдарын пайдаланатын мессенджерлерде. - Viber, Telegram, WhatsApp (веб-нұсқасын қоса), Skype (веб-нұсқасын қоса), Microsoft Lync, RocketChat, Microsoft Teams (веб-нұсқасын қоса), Discord (веб-нұсқасын қоса) мессенджерлерінде тасымалданатын файлдарды ұстап қалу.), Slack (веб-нұсқасын қоса), Signal, Express, Vk Teams. -Skype арқылы жүзеге асырылатын дауыстық сөйлесулерді (Соның ішінде Skype-Skype, Skype-to-phone қоңырауларын), Сондай-Ақ microsoft Lync, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams және sip протоколы арқылы сөйлесулерді САҚТАЙ ОТЫРЫП ТЫҢДАУ. mp3 форматындағы файлдарға; - Microsoft lync, Skype, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams және SIP дауыстық сөйлесулерін (коммуникацияларын) мәтіндік форматта тану және аудару мүмкіндігі; - Сақталған microsoft lync, Skype, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams және SIP сөйлесулерін ойнату мүмкіндігі; - возможность ограничения перехвата по отдельным учетным записям пользователей; - автоматическое обнаружение сообщений и файлов, содержащих определенную

	информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность осуществления поиска по тексту и атрибутам сообщений и файлов, переданных через мессенджеры, в том числе с применением шаблонов. - skype, Telegram, Whatsapp, Discord, Microsoft Teams, Slack мессенджерлерінің веб-клиенттерінде жіберілген хабарламалар мен файлдарды ұстап қалу, сондай-ақ мессенджерлердің ВЕБ-клиенттерінде ЖІБЕРІЛГЕН хабарламаларды ұстап ҚАЛУ: ICQ, Google Hangouts; - facebook, LinkedIn-тегі хат-хабарлар мен жазбаларды бақылау. - Instagram-дағы хат-хабарларды бақылау. - cms Bitrix24 жүйесіндегі хат алмасуды, электрондық поштаны және файлдарды бақылау. - блокировка отправки файлов в мессенджеры, как по набору атрибутов, так и по содержимому - WhatsApp мессенджерінің web және dekstop нұсқаларында дауыстық хабарлар мен файлдарды ұстап қалу. 19. HTTP протоколын басқаруға қойылатын талаптар. Жүйе HTTP протоколы арқылы ақпараттың жіберілуін бақылауды қамтамасыз етуі керек, соның ішінде: - пайдаланушы жасаған алдын ала орнатылған ережелер мен ережелер сериясы бойынша белгілі бір шығыс және кіріс ақпаратты ұстап қалудан алып тастау ҮШІН HTTP сұрау параметрлері бойынша сүзгілерді құру және икемді конфигурациялау мүмкіндігі.; - пайдаланушы жасаған бірқатар алдын ала орнатылған ережелер мен ережелерге СӘЙКЕС mime типтері бойынша деректерді ұстап қалуды сүзуді теңшеу мүмкіндігі; - жіберілген деректерді БАСҚАРУДЫҢ HTTP әдістерін таңдау кезінде GET/POST/PUT сұрауларын ұстап қалу, блоктау және сүзу мүмкіндігі; - перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы; - перехват и анализ поисковых запросов пользователя; - сохранение адресов всех страниц, посещенных пользователем; - facebook, Twitter, ВКонтакте, Одноклассники веб-ресурстарындағы кіріс және шығыс веб-байланыс деректерін (чаттардағы хат-хабарлар, мәртебелерді жариялау, түсініктемелер) ұстап қалу; - веб-пошта қызметтері (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex, Zimbra және т.б.д.); - skype, Telegram, Whatsapp, Discord, Microsoft Teams, Slack мессенджерлерінің веб-клиенттерінде жіберілген хабарламалар мен файлдарды ұстап қалу, сондай-ақ мессенджерлердің ВЕБ-клиенттерінде ЖІБЕРІЛГЕН хабарламаларды ұстап ҚАЛУ: ICQ, Google Hangouts; - автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - HTTP(s)протоколы арқылы жіберілген хабарламалар мен файлдардың мәтіні мен атрибуттары бойынша іздеу мүмкіндігі; - возможность блокирования посещений веб-ресурсов, исходящих сообщений и файлов, по контенту, по набору атрибутов, а также по хеш-сумме отправляемых файлов; - HTTP(s) трафигін бұғаттау туралы пайдаланушы хабарламасын теңшеу мүмкіндігі. 20. FTP протоколын басқаруға

	қойылатын талаптар Жүйе FTP протоколы арқылы берілетін ақпаратты бақылауды қамтамасыз етуі керек, оның ішінде: - FTP қосылымы арқылы жіберілген, сондай-АҚ ШИФРЛАНҒАН SSL қосылымы арқылы жіберілген шығыс және кіріс файлдарды ұстап қалу; - возможность настройки ограничения по размеру перехватываемых файлов; - автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - FTP(s) протоколы арқылы жіберілген файлдардың мәтіні мен атрибуттары бойынша, оның ішінде шаблондарды қолдану арқылы іздеу мүмкіндігі; - FTP протоколы арқылы файлдарды жіберуді блоктау мүмкіндігі. 21. Требования к контролю принтеров. Система должна обеспечивать контроль информации, отправляемой на печать, включая: - желілік, виртуалды және жергілікті принтерлерге (СОНЫҢ ішінде COM, LPT порттарына қосылған) жіберілетін құжаттарды ұстап қалу мүмкіндігі; - xps форматында басып шығаруды ұстап қалу мүмкіндігі; - возможность настройки исключений из перехвата по отдельным принтерам; - возможность ограничения перехвата печати по количеству страниц и по размеру документа; - возможность исключения процессов для модуля перехвата печати на принтерах. - извлечение и анализ текста отправленных на печать документов; - автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность блокировки печати по названию документа. текстовому содержимому документа и по названию принтера; - возможность поиска по тексту и атрибутам отправленных на печать файлов, в том числе с применением шаблонов; - PDF және XPS форматында сақтау. - возможность блокировки документов, отправляемых на печать как по набору атрибутов, так и по содержимому документа, отправляемого на печать. 22. Требования к контролю подключенных устройств и внешних накопителей информации. Система должна обеспечивать контроль информации, отправляемой на внешние носители, включая: - аудит подключения внешних устройств - сыртқы дискілерге жіберілген файлдардың көлеңкелі көшірмесі (алынбалы қатты дискілер, флэш-дискілер, жад карталары, алынбалы дискілер, CD/DVD және иілгіш дискілер және т.б.).д.); -файлдарды сыртқы дискілерге көшіру оқиғаларының аудиті (алынбалы қатты дискілер, флэш-дискілер, жад карталары, алынбалы дискілер, CD/DVD және иілгіш дискілер және т.б.).д.), фиксируется имя файла, пользователь, дата, время и данные устройства; - возможность настройки исключений из теневого копирования и аудита по размеру и расширению файлов; - возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ); - сохранение теневых копий файлов, записанных на внешние накопители, локально на контролируемых компьютерах перед отправкой данных на сервер; -

	возможность настройки размера хранилища для теневых копий на контролируемых компьютерах; - возможность блокирования записи файлов на съёмные носители по содержимому передаваемой информации и другим атрибутам. - возможность настройки исключений из теневого копирования и аудита для определенных внешних накопителей информации (по типам устройств, идентификаторам, производителям, названиям, серийным номерам); - контроль доступа к внешним накопителям информации, с возможностью запрета на использование устройств с определенными параметрами (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства и др.); - управление правами записи на внешние накопители с возможностью запрета записи на определенные устройства (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства), а также запрета записи файлов с определенным расширением; - возможность контроля копирования информации на внешние накопители как в локальных, так и терминальных пользовательских сессиях; - исключение отдельных процессов из процедуры контроля, аудита теневого копирования. - қолдау көрсетілетін тізімнен кез-келген түрдегі сыртқы құрылғылардың (USB Автобус Құрылғылары (хабтар және хост контроллері), CD\DVD, Аудио, Желілік Адаптерлер, Сериялық және параллель порттар, SCSI және RAID контроллері) қол жетімділігін бақылау және пайдалануды тексеру., Иілгіш дискілер, Камералар және сканерлер, Windows Portable Devices (WPD), Universal cameras) жұмыс станциясына қосылған, параметрлер жиынтығы бойынша сүзгіленген (Құрылғы атауы, құрылғы идентификаторы, өндіруші идентификаторы, өнім идентификаторы, өндіруші, сериялық нөмір, құрылғы түрі); - сүзгіге бақыланатын жұмыс станцияларында қосылған құрылғылардың ерекшеліктерін қосу; - мұндай ақпарат анықталған жағдайда ақпараттық қауіпсіздікке жауапты тұлғаға хабарлама жібере отырып, көрсетілген параметрлері бар сыртқы құрылғыларды (берілген қауіпсіздік саясаты негізінде) пайдалану жағдайларын автоматты түрде анықтау; - мұндай ақпарат табылған жағдайда ақпараттық қауіпсіздікке жауапты тұлғаға хабарлама жібере отырып, тұтастай алғанда және, атап айтқанда, белгілі бір ақпаратты (берілген қауіпсіздік саясаты негізінде) қамтитын файлдарды сыртқы жинақтағыштарға беру жағдайларын автоматты түрде анықтау; - сыртқы дискілерге жіберілген файлдардың мәтіні мен атрибуттары бойынша, оның ішінде шаблондарды қолдану арқылы іздеу мүмкіндігі. - атрибуттар жиынтығы бойынша да, мазмұны бойынша да дискіге жазылған файлдарды бұғаттау мүмкіндігі. 23. Жергілікті желілік ресурстарды бақылауға қойылатын талаптар Жүйе келесі мүмкіндіктерді қоса алғанда, жергілікті желілік ресурстарға жіберілетін ақпаратты бақылауды қамтамасыз етуі керек: - файлдарды жергілікті желілік ресурстарға көшіру оқиғаларының аудиті: Файл атауы, пайдаланушы, күн, уақыт және ресурсқа желі жолы жазылады; - желілік ресурстарға жіберілген файлдарды көлеңкелі көшіру; - файл кеңейтімдері бойынша аудиттен және көлеңкелі көшіруден

	ерекшеліктерді теңшеу мүмкіндігі; - аудиттен ерекшеліктерді теңшеу және белгілі бір желілік ресурстарды көлеңкелі ұстау мүмкіндігі; - үлкен файлдар үшін көлеңкелі көшірмені ішінара сақтауды теңшеу мүмкіндігі (мысалы, тек алғашқы 100 МБ сақтау); - серверге жібермес бұрын жергілікті басқарылатын компьютерлерде желілік ресурстарға жазылған файлдардың көлеңкелі көшірмелерін сақтау; - пайдаланушылардың жергілікті компьютерлерінде көлеңкелі көшірмелер үшін сақтау өлшемін теңшеу мүмкіндігі; - терминалдық серверлердің желілік ресурстарына берілетін файлдарды көлеңкелі көшіру мүмкіндігі; - белгілі бір желілік ресурстарға кіруге тыйым салу мүмкіндігімен желілік ресурстарға қол жеткізуді бақылау; - белгілі бір файл пішімдерін жазуға тыйым салу мүмкіндігімен желілік ресурстарға жазу құқықтарын басқару; - бақылау, көлеңкелі көшіру аудиті рәсімдерінен жекелеген процестерді алып тастау; - осындай ақпарат анықталған жағдайда ақпараттық қауіпсіздікке жауапты тұлғаға хабарлама жібере отырып, белгілі бір ақпаратты (берілген қауіпсіздік саясаты негізінде) қамтитын желілік ресурстарға берілген файлдарды автоматты түрде табу; - желілік ресурстарға жіберілген файлдардың мәтіні мен атрибуттары бойынша, оның ішінде шаблондарды қолдану арқылы іздеу мүмкіндігі. 24. Бұлтты сақтауды басқаруға қойылатын талаптар (Dropbox, OneDrive, Google Drive, Yandex. Drive, Apple iCloud, бұлт Mail.Ru). Жүйе бұлтты сақтауды пайдалануды бақылауды қамтамасыз етуі керек, соның ішінде: - файлдарды бұлтты сақтау орындарына жіберу оқиғаларының аудиті: Файл атауы, пайдаланушы аты, Күні, Уақыты және бұлтты сақтау қызметінің атауы жазылады; - пайдаланушы немесе процесс арқылы бұлтты қоймаларға жіберілген файлдарды көлеңкелі көшіру; - тек Шығыс, тек кіріс немесе барлық файлдардың аудиті мен көлеңкелі көшірмесін орнату; - үлкен файлдар үшін көлеңкелі көшірмені ішінара сақтауды теңшеу мүмкіндігі (мысалы, тек алғашқы 100 МБ сақтау); - серверге жібермес бұрын жергілікті басқарылатын компьютерлерде бұлтты сақтауға жазылған файлдардың көлеңкелі көшірмелерін сақтау; - пайдаланушылардың жергілікті компьютерлерінде көлеңкелі көшірмелер үшін сақтау өлшемін теңшеу мүмкіндігі; белгілі бір пайдаланушылар үшін кіруге тыйым салу мүмкіндігі бар жеке бұлттық қоймаларға кіруді басқару; белгілі бір пайдаланушылар үшін "тек оқу" режимін теңшеу мүмкіндігі бар жеке бұлттық қоймаларға кіруді басқару; белгілі бір форматтағы файлдарды жіберуге тыйым салу мүмкіндігімен бұлтты қоймаларға деректерді беру құқығын басқару; аудиттен ерекшеліктерді теңшеу, көлеңкелі көшіру және файл кеңейтімдері бойынша қол жетімділікті басқару мүмкіндігі; мұндай ақпарат анықталған жағдайда ақпараттық қауіпсіздікке жауапты тұлғаға хабарлама жібере отырып, белгілі бір ақпаратты (берілген қауіпсіздік саясаты негізінде) қамтитын бұлтты қоймаларға берілген файлдарды автоматты түрде анықтау; жіберілген файлдардың мәтіні мен атрибуттары бойынша, соның ішінде шаблондарды қолдану арқылы іздеу мүмкіндігі. Жүйе бұлтты сақтаудың веб-нұсқаларын (iCloud,

	Dropbox, Google Drive, OneDrive, бұлт) бақылау үшін келесі мүмкіндіктерді қамтамасыз етуі керек Mail.ru, Yandex. Disk, ownCloud): - файлдарды бұлтты сақтау орындарына жіберу оқиғаларының аудиті: Файл атауы, пайдаланушы аты, Күні, Уақыты және бұлтты сақтау қызметінің атауы жазылады; - пайдаланушы немесе процесс арқылы бұлтты қоймаларға жіберілген файлдарды көлеңкелі көшіру; - серверге жібермес бұрын жергілікті басқарылатын компьютерлерде бұлтты сақтауға жазылған файлдардың көлеңкелі көшірмелерін сақтау; - мұндай ақпарат анықталған жағдайда ақпараттық қауіпсіздікке жауапты тұлғаға хабарлама жібере отырып, белгілі бір ақпаратты (берілген қауіпсіздік саясаты негізінде) қамтитын бұлтты қоймаларға берілген файлдарды автоматты түрде анықтау; - жіберілген файлдардың мәтіні мен атрибуттары бойынша, соның ішінде шаблондарды қолдану арқылы іздеу мүмкіндігі. 25. ДК-де пайдаланушылардың іс-әрекеттерін бақылау мүмкіндіктеріне қойылатын талаптар. Скриншот функциясына қойылатын талаптар. Жүйе пайдаланушылардың жұмыс үстелінің суреттерін сақтауды және қамтамасыз етуді қамтамасыз етуі керек: * белгіленген аралықта скриншоттарды түсіру мүмкіндігі; * белсенді терезені ауыстырған кезде және шолғыш қойындысын ауыстырған кезде скриншоттарды түсіру мүмкіндігі; * PrintScreen пернесін басқан кезде скриншоттарды түсіру мүмкіндігі; * скриншоттардың сапасын реттеу мүмкіндігі (соның ішінде ақ-қара форматта сақтау); * скриншоттардың өлшемін реттеу мүмкіндігі (түпнұсқаның пайызымен); * скриншот пішімін теңшеу мүмкіндігі (JPEG, PNG) ; * скриншотты алу мүмкін болмаған жағдайда арнайы белгіні сақтау (пайдаланушының сессиясы өшірілген, бұғатталған және т. б.); * скриншоттарды құрылымдық элементтердің интерактивтілігін қолдайтын және веб – шолғыш арқылы ұсталған деректерді көруге қол жетімді сыртқы HTML файлына экспорттау мүмкіндігі; * жеке пайдаланушының скриншоттарын бір күнде (немесе таңдалған уақыт аралығы үшін) графикалық файлдар жиынтығы, web-құжат немесе бір PDF - немесе бейне файлға біріктірілген түрінде сақтау мүмкіндігі; * бірнеше пайдаланушының скриншоттарын таңдалған күн аралығы үшін графикалық файлдар жиынтығы, web - құжат немесе бір PDF немесе бейне файлға біріктірілген түрінде сақтау мүмкіндігі. 26. Деректерді беруді бұғаттауға қойылатын талаптар: Жүйе http, MAPI, SMTP хаттамалары бойынша жіберілетін сезімтал деректерді бұғаттау, сондай-ақ нақты уақыт режимінде басып шығару арқылы ұйымның қауіпсіздік саясатын бұзу жағдайларына жедел ден қоюды қамтамасыз етуі керек. Жүйе келесі мүмкіндіктерге ие болуы керек: - HTTP протоколы арқылы берілетін деректерді мазмұнды талдау негізінде бұғаттау (мазмұнды талдау): фразалық іздеу, бұлыңғыр іздеу, сөздер арасындағы қашықтықты ескере отырып іздеу, транслитерация, морфология, құжатқа фразаның пайда болу саны және т. б. сияқты талдау мүмкіндіктерін пайдалана отырып. электрондық пошта қызметтері мен әлеуметтік желілердегі файлдар, интернеттен ақпарат іздеу және басқалары; - тұрақты өрнектерді қолдана отырып, мазмұнды талдау (мазмұнды

	талдау) негізінде HTTP арқылы берілетін деректерді бұғаттау - IP мекенжайы, порт, шифрланған қосылымды пайдалану фактісі, HTTP әдісі, веб-өріс параметрлері, файл атрибуттары, сайт санаты және т. б. сияқты атрибуттарды пайдалана отырып, атрибуттарды талдау (контекстік талдау) негізінде HTTP протоколы арқылы берілетін деректерді блоктау. -файлдың хэш сомасы негізінде HTTP протоколы арқылы берілетін файлдарды бұғаттау, бұл ретте алдын ала конфигурацияланған хэш-сомалар банкінен бірнеше хэш-сомаларды қолмен көрсетуге, сондай-ақ пайдаланушы таңдаған файлдан алуға болады. MD5, SHA-256, SHA-1 хэш сомаларына қолдау көрсетіледі; - файлдың хэш сомасы негізінде HTTP протоколы арқылы берілетін файлдарды бұғаттау, бұл ретте алдын ала конфигурацияланған хэш-сомалар банкінен бірнеше хэш-сомаларды қолмен көрсетуге, сондай-ақ пайдаланушы таңдаған файлдан алуға болады. MD5, SHA-256, SHA-1 хэш сомаларына қолдау көрсетіледі; -банкке белгілі бір қалтада орналасқан барлық файлдардың хэш-сомаларын, сондай-ақ көрсетілген қалтадан белгілі бір кеңейтім файлдарын қосу мүмкіндігі; - бір құлыптау ережесінде бірнеше іздеу сөздіктерін көрсету мүмкіндігімен іздеу сөздіктері негізінде HTTP арқылы берілетін деректерді блоктау; - HTTP протоколы арқылы берілетін деректерді бір құлыптау ережесінде бірнеше цифрлық басып шығаруды көрсету мүмкіндігімен сандық басып шығару негізінде блоктау; - құпиялылық белгілерін талдау негізінде HTTP арқылы жіберілетін файлдарды бұғаттау; - SMTP хаттамасы бойынша жіберілетін поштаны Электрондық поштаның мазмұнын талдау негізінде бұғаттау (мазмұнды талдау) және мынадай талдау мүмкіндіктерін пайдалана отырып, тіркемелер: фразалық іздеу, бұлыңғыр іздеу, сөздер арасындағы қашықтықты ескере отырып іздеу, транслитерация, морфология және т. б.; - SMTP хаттамасы бойынша жіберілетін поштаны тұрақты өрнектерді қолдана отырып, мазмұнды талдау (мазмұнды талдау) негізінде бұғаттау -IP мекенжайы, порт, жіберуші, алушы, файл атрибуттары және т. б. сияқты атрибуттарды пайдалана отырып, хат пен тіркемелердің атрибуттарын талдау (контекстік талдау) негізінде SMTP протоколы арқылы жіберілетін поштаны бұғаттау. -SMTP хаттамасы бойынша берілетін тіркемелерді файлдың хэш-сомасы негізінде бұғаттау, бұл ретте бірнеше хэш-сомаларды қолмен, алдын ала конфигурацияланған хэш-сомалар банкінен көрсетуге, сондай-ақ пайдаланушы таңдаған файлдан алуға болады. MD5, SHA-256, SHA-1 хэш сомаларына қолдау көрсетіледі; - SMTP хаттамасы бойынша жіберілетін поштаны іздеу сөздіктері негізінде бір құлыптау ережесінде бірнеше іздеу сөздіктерін көрсету мүмкіндігімен бұғаттау; - SMTP хаттамасы бойынша жіберілетін поштаны бір құлыптау ережесінде бірнеше цифрлық басып шығаруды көрсету мүмкіндігімен цифрлық басып шығару негізінде бұғаттау; - құпиялылық белгілерін талдау негізінде SMTP хаттамасы бойынша жіберілетін файлдарды бұғаттау; - mapi хаттамасы бойынша жіберілетін поштаны Электрондық поштаның мазмұнын талдау негізінде бұғаттау (мазмұнды талдау) және мынадай талдау мүмкіндіктерін пайдалана

	отырып, тіркемелер: фразалық іздеу, бұлыңғыр іздеу, сөздер арасындағы қашықтықты ескере отырып іздеу, транслитерация, морфология және т. б.; - mapi хаттамасы бойынша жіберілетін поштаны тұрақты өрнектерді қолдана отырып, мазмұнды талдау (мазмұнды талдау) негізінде бұғаттау -IP мекенжайы, порт, жіберуші, алушы, файл атрибуттары және т. б. сияқты атрибуттарды пайдалана отырып, хат пен тіркемелердің атрибуттарын талдау (контекстік талдау) негізінде MAPI протоколы арқылы жіберілетін поштаны бұғаттау. -mapi хаттамасы бойынша берілетін тіркемелерді файлдың хэш-сомасы негізінде бұғаттау, бұл ретте бірнеше хэш-сомаларды қолмен, алдын ала конфигурацияланған хэш-сомалар банкінен көрсетуге, сондай-ақ пайдаланушы таңдаған файлдан алуға болады. MD5, SHA-256, SHA-1 хэш сомаларына қолдау көрсетіледі; - бір құлыптау ережесінде бірнеше іздеу сөздіктерін көрсету мүмкіндігімен іздеу сөздіктері негізінде MAPI хаттамасы бойынша жіберілетін поштаны бұғаттау; - бір құлыптау ережесінде бірнеше цифрлық басып шығаруды көрсету мүмкіндігімен сандық басып шығару негізінде MAPI хаттамасы бойынша жіберілетін поштаны бұғаттау; - құпиялылық белгілерін талдау негізінде MAPI арқылы жіберілетін файлдарды бұғаттау; -пайдаланушы, IP мекенжайы, порт, компьютер, Домен, файл атрибуттары және т. б. сияқты атрибуттарды пайдалана отырып, атрибуттарды талдау (контекстік талдау) негізінде FTP протоколы арқылы берілетін деректерді блоктау. - XMPP хаттамасы бойынша жіберілген деректерді жазу мазмұнын талдау негізінде бұғаттау (мазмұнды талдау) және мынадай талдау мүмкіндіктерін пайдалана отырып, тіркемелер: фразалық іздеу, бұлыңғыр іздеу, сөздер арасындағы қашықтықты ескере отырып іздеу, транслитерация, морфология және т. б.; - тұрақты өрнектерді қолдана отырып, мазмұнды талдау (мазмұнды талдау) негізінде XMPP протоколы арқылы берілетін деректерді бұғаттау - пайдаланушы, компьютер, домен, файл атрибуттары және т. б. сияқты атрибуттарды қолдана отырып, хаттың атрибуттарын (контекстік талдау) талдау негізінде XMPP арқылы берілетін деректерді бұғаттау. -XMPP хаттамасы бойынша берілетін файлдарды файлдың хэш сомасы негізінде бұғаттау, бұл ретте бірнеше хэш-сомаларды қолмен, алдын ала конфигурацияланған хэш-сомалар банкінен көрсетуге, сондай-ақ пайдаланушы таңдаған файлдан алуға болады. MD5, SHA-256, SHA-1 хэш сомаларына қолдау көрсетіледі; - бір құлыптау ережесінде бірнеше іздеу сөздіктерін көрсету мүмкіндігімен іздеу сөздіктері негізінде XMPP протоколы арқылы берілетін деректерді бұғаттау; - бір құлыптау ережесінде бірнеше цифрлық басып шығаруды көрсету мүмкіндігімен сандық басып шығару негізінде XMPP протоколы арқылы берілетін деректерді бұғаттау; - құпиялылық белгілерін талдау негізінде XMPP арқылы берілетін файлдарды бұғаттау; - фразалық іздеу, бұлыңғыр іздеу, сөздер арасындағы қашықтықты ескере отырып іздеу, транслитерация, морфология және т. б. сияқты талдау мүмкіндіктерін пайдалана отырып, құжаттың мазмұнын (мазмұнды талдау) талдау негізінде басып шығаруға жіберілетін құжаттарды

	бұғаттау.; - тұрақты өрнектерді пайдалана отырып, мазмұнды талдау (мазмұнды талдау) негізінде басып шығаруға жіберілетін құжаттарды бұғаттау - компьютер, домен, пайдаланушы, уақыт, Апта күні және т. б. сияқты атрибуттарды пайдалана отырып, басып шығару атрибуттарын талдау (контекстік талдау) негізінде басып шығаруға жіберілетін құжаттарды бұғаттау. - бір құлыптау ережесінде бірнеше іздеу сөздіктерін көрсету мүмкіндігімен іздеу сөздіктері негізінде басып шығаруға жіберілетін құжаттарды бұғаттау; - алмасу буферіне көшірілетін деректерді жазу мазмұнын талдау негізінде бұғаттау (мазмұнды талдау) және мынадай талдау мүмкіндіктерін пайдалана отырып, тіркемелер: фразалық іздеу, бұлыңғыр іздеу, сөздер арасындағы қашықтықты ескере отырып іздеу, транслитерация, морфология және т. б.; - тұрақты өрнектерді қолдана отырып, мазмұнды талдау (мазмұнды талдау) негізінде алмасу буферіне көшірілетін деректерді бұғаттау - пайдаланушы, компьютер, процесс, домен, файл атрибуттары, деректер түрі (мәтін, сурет, файл) және т. б. сияқты атрибуттарды қолдана отырып, хат пен тіркемелердің атрибуттарын талдау негізінде алмасу буферіне көшірілетін деректерді бұғаттау. - іздеу сөздіктері негізінде алмасу буферіне көшірілетін деректерді бір құлыптау ережесінде бірнеше іздеу сөздіктерін көрсету мүмкіндігімен бұғаттау; - алмасу буферінен енгізілген деректерді жазу мазмұнын талдау негізінде бұғаттау (мазмұнды талдау) және мынадай талдау мүмкіндіктерін пайдалана отырып, тіркемелер: фразалық іздеу, бұлыңғыр іздеу, сөздер арасындағы қашықтықты ескере отырып іздеу, транслитерация, морфология және т. б.; - тұрақты өрнектерді қолдана отырып, мазмұнды талдау (мазмұнды талдау) негізінде алмасу буферінен енгізілген деректерді бұғаттау - пайдаланушы, компьютер, процесс, домен, файл атрибуттары, деректер түрі (мәтін, сурет, файл) және т. б. сияқты атрибуттарды қолдана отырып, хат пен тіркемелердің атрибуттарын талдау (контекстік талдау) негізінде алмасу буферінен енгізілген деректерді бұғаттау. - іздеу сөздіктеріне негізделген алмасу буферінен енгізілген деректерді бір құлыптау ережесінде бірнеше іздеу сөздіктерін көрсету мүмкіндігімен бұғаттау; -компьютер, домен, қолданба санаты, хэш сомасы және т. б. сияқты атрибуттарды қолдана отырып, процестің атрибуттарын талдау (контекстік талдау) негізінде процестердің басталуын блоктау. - фразалық іздеу, бұлыңғыр іздеу, сөздер арасындағы қашықтықты ескере отырып іздеу, транслитерация, морфология және т. б. сияқты талдау мүмкіндіктерін пайдалана отырып, мазмұнды талдау (мазмұнды талдау) негізінде файлдарды мессенджерлерге жіберуді бұғаттау.; - тұрақты өрнектерді қолдана отырып, мазмұнды талдау (мазмұнды талдау) негізінде файлдарды мессенджерлерге жіберуді бұғаттау - атрибуттарды талдау негізінде файлдарды мессенджерлерге жіберуді бұғаттау (контекстік талдау) - жазу мазмұнын талдау (мазмұнды талдау) негізінде файлдарды дискілерге жазуды бұғаттау және талдау мүмкіндіктерін пайдалана отырып, тіркемелер: фразалық іздеу, бұлыңғыр іздеу, сөздер арасындағы

	қашықтықты ескере отырып іздеу, транслитерация, морфология және т. б.; -тұрақты өрнектерді қолдана отырып, мазмұнды талдау (мазмұнды талдау) негізінде файл жазбаларын бұғаттау - атрибуттарды талдауға негізделген файлдарды бұғаттау (контекстік талдау) сияқты атрибуттарды қолдана отырып: пайдаланушы, компьютер, процесс, домен, және т. б. атрибут файл - файл жазбаларын белгілі бір көрсеткіштерге (сериялық нөмірі, өндірісі, құрылғының мақсаты, өндіруші идентификаторы және өнім идентификаторы бойынша)құлыптау -файлдың хэш сомасы негізінде жазылған файлдарды бұғаттау, бұл ретте бірнеше хэш сомасын қолмен, белгіленген хэш сомасының банкінен көрсетуге болады, сондай-ақ сіз таңдаған файлдан алуға болады. MD5, SHA-256, SHA-1 хэш сомаларына қолдау көрсетіледі; - іздеу сөздіктеріне негізделген файл жазбаларын бұғаттау, бір бұғаттау құқығында бірнеше іздеу сөздіктерін көрсету мүмкіндігі бар; - бір құлыптау ережесінде бірнеше сандық жауаптарды көрсету мүмкіндігімен сандық жауаптар негізінде файл жазбаларын бұғаттау; - құпиялылық әдістерін талдау негізінде файл жазбаларын дискілерге құлыптау; - кіріспе мәтіні орнатылған құлыптау кезінде соңғы пайдаланушыны енгізу мүмкіндігі; - қауіпсіздік офицерін іске қосылатын бұғаттау құқығы туралы енгізу мүмкіндігі; - бұғатталған ақпарат атрибуттары бойынша іздеу мүмкіндігі. 26. ДК белсенділігі бойынша статистиканы жинау функцияларына қойылатын талаптар Жүйе бақыланатын жұмыс станцияларының белсенділігі және пайдаланушының жұмыс станцияларындағы активтері туралы деректерді жинауды және сақтауды қамтамасыз етуі керек: - белсенді жұмыс уақыты бойынша статистиканы жүргізу және жай ғана (пайдаланушының әрекетінің болмауы) бастамас бұрын белсенділіктің болмау кезеңін орнату мүмкіндігімен; - жиналған ақпаратты ұсына отырып, қосымшаларда пайдаланушының жұмыс уақыты бойынша статистиканы жүргізу, бұл ретте қосымшаның жұмысы, ал белсенді терезеде пайдаланушының жұмыс уақыты ескеріледі; - мониторингтен жекелеген процестерді зерттеу; - белгілі бір оқиғаларды шығару үшін жиналған статистиканы автоматты түрде талдау мүмкіндігі (мысалы, рұқсат етілмеген қосымшалардың жазбасы), пайдаланушылардың белгілі бір қосымшалармен жұмыс сапасын бақылау және жұмыс уақыты үшін/жай компьютер – жауапты адамға тиісті өтінішпен; - жеке қосымшалардың қуат құлпы мүмкіндігі; - жеке пайдаланушы немесе бірнеше пайдаланушы үшін таңдалған уақыт аралығы үшін әрекеттер туралы есептер деректерін (ДК-дегі пайдаланушы белсенділігі, қолданба белсенділігі, Оқиғалар хронологиясы) сақтау мүмкіндігі. - әр түрлі қосымшаларда өткізілетін уақытты өнімді, өнімсіз және бейтарапқа автоматты түрде санаттау 28. Жад буферінің контроллеріне қойылатын талаптар Жүйе бақыланатын жұмыс станцияларының белсенділігі және пайдаланушының жұмыс станцияларындағы активтері туралы деректерді жинауды және сақтауды қамтамасыз етуі керек: - осы ақпарат алмасу буферіне орналастырылған қосымшаны тіркей отырып, мәтіндік ақпарат алмасу буферіне орналастыру арқылы көлеңкелі көшіру және өткізу уақыты; -

	алмасу буферіне орналастырылған файлдардың аудиті; - жер иесінің графикалық мазмұнын алмасу буферіне көлеңкелі көшіру; - алмасу буферіне орналастырылған файлдарды көлеңкелі көшіру; - өтініш буферінен берілетін деректердің максималды объектісін шектеу мүмкіндігі; - алмасу буферін бақылаудан немесе тек белгілі бір процестерді бақылаудан жеке процестерді іздеу мүмкіндігі; - алмасу буферін бақылаудан немесе тек белгілі бір файлдарды бақылаудан жеке файлдарды іздеу мүмкіндігі; - алмасу буферіне орналастырылатын белгілі бір ақпаратқа автоматты түрде қызмет көрсету (берілген қауіпсіздік саясаты негізінде), мұндай ақпаратпен жұмыс істеген жағдайда, ақпараттық ақпаратқа жауапты адамның басқару анықтамасымен; - белгіленген қауіпсіздік ережелеріне сәйкес файлдарды мазмұны бойынша көшіруді де, қоюды да бұғаттау мүмкіндігі. - пайдаланушылар алмасу буферіне орналастыратын мәтін бойынша, оның ішінде шаблондарды қолдану арқылы іздеу мүмкіндігі. - ақпаратты тек алмасу буферіне көшірілген ақпаратпен және алмасу буферінен енгізілген ақпаратпен теңшеу мүмкіндігі; - буферде тек файлдарды, тек мәтінді немесе тек кескінді жасау мүмкіндігі. 29.K. M. Keylogger талаптары. Жүйе қолдау көрсетуі керек: - қажетті пайдаланушыны тіркеңіз пайдаланушы осы ақпаратты енгізген қосымшаны бекітетін пернетақтадағы перне және уақыт, қызметтік пернелерді (Shift, Enter, Backspace және т. б.) иеліктен шығару / қорғау мүмкіндігі; - берілген қосымшаларда пернетақта аудармасын іздеу немесе тек белгілі бір қосымшаларда беру мүмкіндігі; - браузердегі белсенді беттің мекен-жайы бойынша пернетақтаны ауыстыруды іздеу немесе браузердегі белгілі бір белсенді бетке өтуді қамтамасыз ету мүмкіндігі; - арнайы ақпаратқа автоматты түрде қызмет көрсету (берілген қауіпсіздік саясаты негізінде), пернетақтаның көмегімен, осындай ақпаратты пайдаланған жағдайда, ақпараттық ақпаратқа жауапты адамның өтінішінің рұқсатымен; - мәтін бойынша іздеу, пайдаланушыларды пернетақтадан енгізу, соның ішінде шаблондарды қолдану мүмкіндігі. 30. Бейне бақылау. Жүйе жұмыс үстелінің бейнелерін, сондай-ақ веб-камерадан бейнелерді түсіруге және келесі мүмкіндіктермен толықтыруға көмектесетін пайдаланушының әрекетін бақылауға мүмкіндік беруі керек: - пайдаланушының компьютер мониторына қосылу және нақты уақыт режимінде жұмыс үстелінің бейнелерін көру; - бір уақытта бірнеше пайдаланушылардың жұмыс үстелдерін бақылау; - терезеден бөлек экранға қарау мүмкіндігі; - жұмыс үстелінің бейне суретін және тарату веб-камерасы қосылған бейнені автоматты түрде жазу; - жұмыс үстелінің бейнесін қолмен жазу; - жазу сапасын реттеу мүмкіндігі; -бейнені түрлі-түсті және ақ-қара форматта жазу мүмкіндігі; - бірнеше пайдаланушылардың жазбаларын бір уақытта сақтау мүмкіндігі; - файлдарды ортаңғы жүйелерде және кез-келген медиа ойнатқыштарда жазбалармен қарау мүмкіндігі. 31. Аудио мониторинг функциясына қойылатын талаптар: Жүйе жұмыс станциясының динамиктеріне түсетін микрофоннан және аудиодан аудио жазудың көмегімен пайдаланушының белсенділігін

	бақылауға және келесі мүмкіндіктермен толықтыруға мүмкіндік беруі керек: - нақты уақыт режимінде аудио ағындарды тыңдау мүмкіндігі бар бақыланатын жұмыс станцияларының микрофондарына қосылу; - бірнеше пайдаланушылардың микрофондарын тыңдау монотонды; - микрофоннан келетін аудио ағыны мен тарату бойынша компьютердің жүйелік дыбыстарын автоматты түрде жазу; - қолмен жазу; - бірнеше пайдаланушылардың жазбаларын бір уақытта сақтау мүмкіндігі; - файлдарды ортаңғы жүйелерде және кез-келген медиа ойнатқыштарда жазбалармен қарау мүмкіндігі. - жазылған бейне, аудиодағы аудио тректердің сипаттамасы 32.Файлдық жүйе контроллеріне қойылатын талаптар. Файлдық жүйелерді басқару мүмкіндік беруі керек: - бақыланатын жұмыс станцияларының файлдық жүйелерін құпия мәртебеге ие немесе ақпараттық қауіпсіздікті қамтамасыз ету шеңберінде мүдделерін білдіретін құжаттардың болуына автоматты түрде сканерлеу; - іздеу сканерлеу кезінде орындалуы тиіс құпия құжаттардың банктерін қалыптастыру; -ТХТ файлдарынан дайындалған хэш функцияларының құпия құжаттарын банкке автоматты түрде импорттау мүмкіндігі - және csv-формат; - жұмыс станциялары мен файлдық жүйелері бақыланатын пайдаланушыларды таңдау мүмкіндігі; - автоматты түрде тексерілетін файлдар мен қалталарды таңдау ережелерін икемді түрде теңшеу; - нақты өлшемдегі файлдарды сканерлеуден іздеу; - шығу мүмкіндігі тарату бойынша файлдық жүйені тексеру; - жеке пайдаланушылар мен жұмыс станциялары үшін, оның ішінде шаблондарды қолдана отырып, қолдау көрсетілетін файлдық жүйелерді бақылаудың жеке саясатын құру мүмкіндігі; -бақыланатын жұмыс станцияларының файлдық жүйелерінде файл атрибуттары мен олардың хэш функцияларының белгілері бойынша құжаттарды іздеу мүмкіндігі. 33. Жіберілетін ақпаратты талдау әдістеріне және жүйенің қауіпсіздік инциденттеріне ден қою рәсімдеріне қойылатын талаптар Қауіпсіздік саясаттарымен жұмыс істеу кезінде мынадай функционалдық мүмкіндіктерді көздеуге тиіс: -барлық қол жетімді талдау құралдарын қолдана отырып, іздеу шарттарының көмегімен қауіпсіздік ережелері: мазмұнды талдау, атрибуттық талдау, танылған өнертабыстарды іздеу, басып шығару, танылған сөйлеу, тақырыптық талдау және т. б.; - іздеу шарттарын топтарға біріктіру мүмкіндігімен "және", "немесе", "емес" логикалық операторларының көмегімен бірнеше қарапайым іздеу шарттарын біріктіру; - Active Directory топтары бойынша қауіпсіздік ережелері; - сайттар мен қосымшалар санаттары бойынша қауіпсіздік ережелері; - белгілі бір құпиялылық белгілері бар файлдарды ұстауға арналған қауіпсіздік ережелері - іздеу үлгілерін қолдана отырып қауіпсіздік саясатын құру - басқа қауіпсіздік ережелерін қалыптастыруда қолдануға болатын іздеу шарттарының жиынтығы; - іске қосу шегі мен қозғалыс бағытын таңдау мүмкіндігі бар сандық жауаптар бойынша қауіпсіздік ережелері (тікелей, кері немесе ең үлкен); - қауіпсіздік ережелері табалдырық пен морфологияны есепке алу мүмкіндігімен; -хэш-сомалар бойынша қауіпсіздік ережелері, банктерге арналған хэш-сомаларды іздеу мүмкіндігі

	бар; -пайдаланушының белсенділігі санының, мысалы, электрондық пошта санының, хат алмасудың алдын ала қаралуын бақылайтын статистикалық қауіпсіздік ережелері мессенджерлерде, кірген сайттарда, жіберілген сұрауларда, басып шығарылған файлдар мен беттерде, сондай-ақ пайдаланушылар мен қосымшалардың белсенділік кезеңдерін жазыңыз және т. б.; - алдын ала орнатылған қауіпсіздік ережелерінің болуы; - иерархия деңгейлерінің саны кемінде 20 болатын топтар мен кіші топтарды құру мүмкіндігі; - қауіпсіздік ережесін өшіру мүмкіндігі - қауіпсіздік ережелерін қосу/өшіру сүзгісі - қауіпсіздік саясатын топтан топқа "тінтуірді" жай сүйреп апару мүмкіндігі; - "тінтуірді"жай сүйреп апару арқылы кіші топтарды топтан топқа ауыстыру мүмкіндігі; - қауіпсіздік саясаты қолданылуы мүмкін Active Directory топтарын қосу, Алып тастау; - қауіпсіздік серверінің инциденттер санаттарын қосу, Алып тастау, редакциялау - қауіпсіздік серверінің инциденттерінің тәуекел деңгейін анықтау және редакциялау - пайдаланушылардың тәуекел деңгейінің көрсеткіштерін автоматты түрде есептеу және инциденттердің тәуекел деңгейіне негізделген мінез-құлықты талдау; - қауіпсіздік ережелері іске қосылған немесе іске қосылған кезде сценарийлерді орындау мүмкіндігі; - оқиғалар туралы деректерді үшінші тарап жүйелеріне жіберу мүмкіндігі; - қауіпсіздік саясаты іске қосылған (оқиға анықталған)жағдайда жауапты тұлғаға электрондық пошта арқылы хабарламаларды автоматты түрде жеткізу; - оқиғада жалпы ақпарат (қауіпсіздік саясатының атауы, бұзушылыққа жол берген пайдаланушы, ұсталған деректер түрі, оқиғаның күні/уақыты және т. б.), сондай-ақ пайдаланушы консолінде тиісті оқиғаны ашуға сілтеме немесе қауіпсіздік саясатының іске қосылуына себеп болған құжаттары бар тіркемелер болады; - электрондық поштаға хабарламаларды жіберу мерзімділігін реттеу мүмкіндігі (оқиғаны анықтау бойынша хабарламаны дереу жіберу немесе берілген кезеңділікпен хабарламаларды жинақтау және бөлшектеп жіберу-сағатына бір рет, тәулігіне бір рет және т. б.); - жүйемен жұмыс істейтін әрбір қауіпсіздік офицері үшін қаралған, қаралмаған оқиғаларды бөлектеу мүмкіндігімен клиент консолінде таңдалған қауіпсіздік саясаты бойынша барлық оқиғаларды көру мүмкіндігі; - клиент консолінде оқиға туралы ақпаратты қарау кезінде мынадай ақпарат қолжетімді: бұзушылыққа жол берген пайдаланушы, оқиғаның күні мен уақыты, берілген тәуекел деңгейінің көрсеткіші, қауіпсіздік саясатының іске қосылуына себеп болған құжаттың түрі (электрондық пошта, басып шығаруға жіберілген файл және т.б.), құжаттың мазмұны (электрондық пошта, im-клиентке хат алмасу, және т.б.) қауіпсіздік саясатын, сондай-ақ басқа да қосымша ақпаратты тудырды. - оқиға үшін мәртебе тағайындау мүмкіндігі (оқиға зерттелмеген, оқиғаны тергеу кейінге қалдырылған, оқиға тексерілген, маңызды оқиға, маңызды емес оқиға, жалған позитив); - оқиғаға түс санатын беру мүмкіндігі - оқиғаға түсініктеме қосу мүмкіндігі - қауіпсіздік саясаты бойынша инциденттерді икемді іріктеп қарау мүмкіндігі (мысалы, тек жаңа

	немесе қаралмаған инциденттерді көрсету; тек соңғы 100 инцидентті көрсету; алдағы айдағы, бірақ соңғы 20-дан аспайтын инциденттерді көрсету; "маңызды" мәртебесі бар және соңғы апта ішінде тіркелген инциденттерді көрсету және т. б.); - қауіпсіздік саясаты бойынша инциденттер туралы жазбаларды толық немесе іріктеп жою мүмкіндігі (мысалы, 10 күннен асқан барлық инциденттерді жою; соңғы N инциденттерді жою; "тергелді" мәртебесі бар барлық инциденттерді жою; ДҚ-дан жойылған деректер бойынша инциденттерді жою және т. б.); - инциденттер тізімін әртүрлі параметрлер бойынша сұрыптау мүмкіндігі (өзектілігі бойынша, күні / уақыты бойынша, жергілікті / қашықтағы пайдаланушы бойынша, ұсталған деректердің түрі/мөлшері бойынша, инциденттің мәртебесі бойынша және т. б.); - оқиғалар тізімін әртүрлі параметрлер бойынша сүзу мүмкіндігі: күйлер бойынша (мысалы, тек маңыздыларын көрсету), деректер түрлері бойынша (мысалы, ақпаратты пошта хаттамалары арқылы жіберуден туындаған оқиғаларды ғана көрсету), жағдай бойынша (мысалы, тек қаралмағандарды көрсету) - және осы параметрлердің тіркесімдері бойынша; - оқиғалар тізімін CSV, MS Excel, PDF, XML форматтарының файлына экспорттау мүмкіндігі (бұл жағдайда оқиғалар туралы келесі ақпарат сақталады – ұсталған деректер түрі, Жергілікті / қашықтағы пайдаланушы, ұстау күні / уақыты, өлшемі, оқиға күйі, басқа ақпарат); - қауіпсіздік саясатының іске қосылуына себеп болған ұсталған деректерді тиісті форматтағы файлдарға экспорттау мүмкіндігі; - журнал оқиғаларын экспорттау мүмкіндігімен қауіпсіздік офицерінің іс-қимыл журналын (журналын) жүргізу; - оқиғалар журналында келесі ақпарат тіркеледі: қауіпсіздік ережелерін құру, қайталау, редакциялау, жою, оқиғаны қарау және жою, оқиғаның күйін өзгерту және т. б. Ақпаратты талдау кезінде орыс, қазақ және ағылшын тілдеріндегі ақпаратты талдауды қоса алғанда, талдаудың мынадай әдістері пайдаланылуы тиіс: 34. Мазмұнды талдау: - морфологияны ескере отырып, сөздерді және сөз тіркестерін іздеу, өшіру мүмкіндігі бар; - сөздер арасындағы қашықтықты ескере отырып, сөздер мен сөз тіркестерін іздеу; - сөз тәртібін ескере отырып, сөздер мен сөз тіркестерін іздеу; - латын тіліндегі кириллица таңбаларының транслитерациясын ескере отырып, сөздер мен сөз тіркестерін іздеу, - бұлыңғыр іздеу мүмкіндігі бар сөздер мен сөз тіркестерін іздеу, кілт сөздерді, соның ішінде қателер мен терулермен жазылған сөздерді іздеу; - белгіленген таңбалар тізбегін анықтау үшін қолданылатын тұрақты өрнектерді іздеу технологиясы, мысалы, төлқұжат нөмірлері, банк карталарының нөмірлері және т. б.; - алдын ала орнатылған тұрақты өрнектерді пайдалану және теңшелетін өрнектерді жасау мүмкіндігі; - төлем жүйелерінің базасы бойынша банк карталарының нөмірлерін кейінгі тексеру тетігі; - морфологияны ескере отырып, тақырыптық сөздіктерді іздеу (өшіру мүмкіндігі) және сөздіктердегі маскалар мен тұрақты өрнектерді қолдау, іске қосу шегін реттеу мүмкіндігі бар (мысалы, сөздікте қамтылған 10 сөздің немесе өрнектің кез-келгенін анықтаған

	кезде); - ұқсас құжаттардың ұсталған деректерінде кейіннен анықтау үшін құжаттардың немесе құжаттары бар қалталардың цифрлық іздерін жасау-ұсталған құжаттың түпнұсқаға сәйкестік пайызын көрсету мүмкіндігімен); - алдын ала орнатылған сөздіктерді пайдалану және теңшелетін сөздіктерді жасау мүмкіндігі; - ұсталған құжаттың түпнұсқаға сәйкестік пайызын көрсету мүмкіндігімен құжаттардың цифрлық іздері бойынша іздеу технологиясы; - Тікелей, кері немесе ең үлкен кіруді таңдау мүмкіндігі бар құжаттардың сандық іздері бойынша іздеу технологиясы; - цифрлық басып шығару банкін жаңарту аралығын теңшеу мүмкіндігімен құжаттар орналасқан қалталармен синхрондау - деректер банкіне қосу үшін маңызды ақпараты бар өрістерді таңдай отырып, CSV файлдарының сандық іздерін жасау; - осы дерекқордан ақпараттың ағып кетуін кейіннен анықтау мақсатында таңдалған кестелердің белгілі бір өрістерінің цифрлық іздерін жасау үшін жүйені дерекқорға қосуды баптау арқылы деректер базасының цифрлық іздерін жасау (мысалы, "ТАӘ + Паспорт деректері" өрістерінің байламынан дербес деректерді бір мезгілде анықтау кезінде); - деректер базасының сандық іздерін құру және жаңарту деректер базасын сандық басып шығару көзі файлына жүктеу сияқты аралық әрекеттерсіз жүзеге асырылады. Деректер базасына өзгертулер енгізген кезде жүйе тиісті цифрлық басып шығаруларды автоматты түрде жаңартады 35. Атрибуттар бойынша талдау. - "құжат атауы", "Электрондық пошта алушының мекен-жайы", "пайдаланушы", "IM клиентінің есептік жазбасы", "күні", "уақыты", "апта күні", "өлшемі", "деректер түрі", "компьютер", "домен"сияқты құжат атрибуттарын талдау, "IP-мекен-жайы" және т. б.; - қорғалған хаттама бойынша құжатты, шифрланған немесе қорғалған құжатты, бүлінген деректерді жіберу, бұғаттауға себеп болған немесе жеке тәртіппен берілген деректерді жіберу және т. б. сияқты мәртебелер бойынша құжат атрибуттарын талдау.; - процесс атрибуттарын талдау, мысалы: Орындаушы Файл атауы, файлға толық жол, процесс терезесінің тақырыбы және т. б.; - ұсталған пошта атрибуттарын талдау, мысалы: жіберуші, алушы, алушы саны, хат тақырыбы және т. б; - жергілікті пайдаланушы идентификаторы, қашықтағы пайдаланушы идентификаторы, хабарламалар саны, деректер түрі және т. б. сияқты мессенджерлерде ұсталған хат алмасу атрибуттарын талдау; - бақыланатын құрылғылардың атрибуттарын талдау, мысалы: Құрылғы атауы, өндіруші, құрылғы түрі, Өндіруші идентификаторы, өнім идентификаторы, құрылғы түрі, сериялық нөмір және т. б; - басып шығару атрибуттарын талдау, мысалы: құжат түрі, принтер атауы, басып шығарылған беттер саны және т. б; 36. Статистикалық талдау - пайдаланушы жіберген / алған электрондық хаттардың саны - пайдаланушының хат-хабарларының/хабарламаларының саны - im клиенттеріндегі пайдаланушының қоңырауларының саны/уақыты (мысалы, "IM клиенттеріндегі пайдаланушының дауыстық келіссөздері бір күнде 1 сағаттан асты" немесе "пайдаланушы бір күнде 10-нан астам қоңырау шалды" және т. б.); - кірген веб-беттер саны; - жіберілген веб-сұраулар

	саны; - принтерлерде басып шығарылған беттер/құжаттар саны; - жіберілген / алынған файлдар саны - браузерлерде, оның ішінде белгілі бір сайттарда жұмыс істеу ұзақтығы (мысалы, "браузер арқылы белгілі бір сайтта пайдаланушының болу уақыты күніне 1 сағаттан асты" және т. б.); - қосымшалардағы, оның ішінде белгілі бір қосымшалардағы жұмыс ұзақтығы (мысалы, "пайдаланушы Microsoft Word-та күніне 5 сағаттан артық жұмыс істеді" немесе "пайдаланушы "Солитер орамал" қосымшасында жұмыс уақытының 70% - дан астамы жұмыс істеді" және т. б.); - ДК-нің белсенді жұмысының/әрекетсіздігінің ұзақтығы, оның ішінде жалпы уақыттың пайызымен (мысалы, "ДК күніне 3 сағаттан артық ұйықтамады", "ДК белсенділігінің басталуы 10:30-дан кейін тіркелді" және т. б.); - "Жұмыс күнінің ұзақтығы" ДК үшін белсенді жұмыс ұзақтығының нормасынан жұмыскердің басталу/аяқталу нормасынан ауытқу туралы Автоматты хабарламаларды баптау мүмкіндігі көзделуге тиіс. 37. Оқиғаны талдау. Келесі жағдайларда Автоматты хабарландыруларды теңшеу мүмкіндігі: - пайдаланушының белгілі бір қосымшаны іске қосуын, жұмысын аяқтауын тіркеу; - шифрланған тіркемені қайта жіберуді анықтау (мысалы, құпия сөзбен қорғалған MS Office құжаты немесе мұрағат); - файлдарды басқарылатын компьютерлерден сыртқы дискілерге, бұлтты қоймаларға және белгілі бір параметрлері бар желілік дискілерге көшіру; - бақыланатын жұмыс станцияларында белгілі бір параметрлері бар құрылғыларды қосу және пайдалану; - белгілі бір веб-ресурстарға кіру; - SMTP, HTTP, MAPI хаттамалары бойынша деректерді жіберуді, Құжаттарды басып шығаруға, оның ішінде қосымша атрибуттар бойынша жіберуді бұғаттау; - пайдаланушылардың компьютерлік дискілерінде құпия файлдарды табу; - өзгертілген кеңейтімі бар құжатты жіберу фактісін анықтау (мысалы, пайдаланушы файлдың атын өзгерткен кезде .doc жылы .JPG және одан кейінгі жіберу арқылы жүйе файлдың бастапқы пішімін анықтай алуы және одан мазмұнды талдау үшін мәтінді шығарып алуы керек, бұл жауапты қызметкерге кеңейтімнің өзгеру фактісі туралы қосымша хабарлайды). 38. Есеп беру талаптары. Барлық ұсталған деректер келесі түрдегі есептер түрінде ұсынылуы керек: а) пайдаланушының жұмыс күнінің есептілігі мыналарды қамтуы тиіс: * сағат бойынша бөлінген пайдаланушы жіберген және алған хаттар саны туралы ақпарат; * әр хат алмасу сессиясындағы хабарламалардың ұзақтығы мен санын көрсете отырып, im-клиенттердегі пайдаланушының хат алмасу сессияларының саны туралы ақпарат; * пайдаланушы электрондық пошта арқылы, IM клиенттері арқылы, HTTP(S) және FTP(S) протоколдары арқылы сыртқы құрылғыларға, желілік ресурстарға, бұлтты қоймаларға көшірілген немесе жергілікті/желілік принтерлерде басып шығарылған файлдар саны туралы ақпарат-сағат бойынша бөлінген; * кірген URL мекенжайлары мен жіберілген сұраулар саны туралы ақпарат-сағат бойынша бөлінген; * жүйемен түсірілген пайдаланушының жұмыс үстелінің скриншоттарының саны туралы ақпарат-сағат бойынша бөлінген; * пайдаланушының компьютерінің жұмыс уақыты/тоқтап қалуы туралы ақпарат,

	қолданба белсенділігінің егжей-тегжейлі статистикасы және әртүрлі қолданбалардағы жұмыс уақытының пайызы туралы деректер; * алмасу буферіне орналастырылған құжаттар саны туралы ақпарат – сағат бойынша бөле отырып; * әр түрлі веб-ресурстарда өткізілген уақыттың жан-жақты және егжей-тегжейлі статистикасын ұсына отырып, сағат бойынша бөлінген веб-шолғыш арқылы веб-сайттарға кіру туралы ақпарат; * пайдаланушы пернетақтадан сағат бойынша енгізілген таңбалар саны туралы ақпарат. Пайдаланушының жұмыс күнінің фотосуреті интерактивті және Динамикалық есеп болуы керек, бұл сілтемелер бойынша ұсталған құжаттардың немесе веб-сілтемелердің мазмұнын тікелей қарауға өтуге мүмкіндік беруі керек. Жұмыс күнінің фотосуретін сыртқы HTML файлына, Outlook файлына немесе құрылымдық элементтердің интерактивтілігін қолдайтын және веб – шолғыш арқылы ұсталған деректерге қол жеткізе отырып, бастапқы форматтағы файлға экспорттау мүмкіндігі қамтамасыз етілуі керек. b) ақпарат түрлері бойынша Кестелер. Жүйе белгілі бір уақыт аралығында белгілі бір пайдаланушы бойынша жиналған деректерді ақпараттың жекелеген түрлері бойынша графиктер түрінде ұсынуы керек (Жіберілген/Алынған хаттар бойынша график, IM клиенттеріндегі хат алмасу сессиялары/хабарламалар саны, алынған және жіберілген файлдар саны, кірген URL мекенжайлары мен веб-сұраулар саны бойынша). Ақпарат түрлері бойынша графиктер интерактивтілік пен серпінділікті қолдауы, сілтемелер бойынша (графиктегі нүктелер) ұсталған құжаттардың мазмұнын тікелей қарауға өту мүмкіндігін қолдауы тиіс. c) график-пайдаланушылардың өзара байланысының анализаторы. Жүйе абоненттер шеңберін (ішкі және сыртқы) көрнекі түрде көрсету үшін жиналған ақпарат негізінде пайдаланушының өзара байланысын (баған немесе матрица түрінде) графикалық түрде көрсету мүмкіндігіне ие болуы керек, олармен осы пайдаланушы таңдалған уақыт аралығында қандай да бір ақпаратпен алмасты. Пайдаланушының контактілерін орнатылған және танылмаған контактілерге қатыстылығы бойынша топтастыруға қолдау көрсетілуі тиіс. Сыртқы пайдаланушының карточкасын алдын-ала жасағаннан кейін сыртқы абоненттің ұйым желісінің пайдаланушыларымен байланысын көру мүмкіндігі. Клиент консолінде қарау кезінде есептің дисплей масштабын таңдау мүмкіндігі(түпнұсқаның % өлшемімен). Пайдаланушы белгілі бір абонентпен алмасатын өзара байланыс схемасын көруден құжаттардың мазмұнына (хаттар, хат алмасулар, файлдар және т.б.) интерактивті өту мүмкіндігі. Қатынастар туралы есепті сыртқы PNG файлына график ретінде сақтауды қолдау. d) жиынтық есептілік Жүйе есептерді пайдаланушы қолмен қайта құруды қолдайтын есептерді күнделікті автоматты түрде жаңартуды орындауы керек. Жүйе сандық деректердің интерактивтілігін қолдауы керек-таңдалған көрсеткіш бойынша нәтижелер тізіміне тікелей өту мүмкіндігі. Көрсетілген абоненттерге электрондық пошта кестесіне сәйкес есептерді автоматты түрде жіберуді қолдау. Есептерді сыртқы файлға экспорттау. 39. Пайдаланушы туралы есеп келесі талаптарды орындауы керек: Келесі ақпаратты

	қамтитын барлық бақылау уақыты (немесе таңдалған уақыт аралығы) үшін белгілі бір пайдаланушы бойынша жиынтық интерактивті есепті құру мүмкіндігі: a) деректерді ұстау статистикасы, оның ішінде: * пошта мен мессенджерлерді қоса алғанда, барлық тарату арналары бойынша пайдаланушы берген және алған ақпараттың саны; * кірген сайттар мен іздеу сұрауларының саны; * FTP арқылы жіберілген / қабылданған файлдар саны; * басып шығарылған құжаттар мен беттер саны; * алмасу буферіне көшіру операцияларының саны; * түсірілген скриншоттар саны; * сыртқы дискілерге/желілік ресурстарға/бұлтты сақтау орындарына жіберілген файлдар саны; * пернетақта пернелерінің саны; b) пайдаланушының компьютердегі белсенділігі туралы ақпарат, оның ішінде: * ДК үшін пайдаланушының белсенді жұмысының жалпы уақыты; * ДК үшін пайдаланушының белсенді жұмысының орташа тәуліктік уақыты; * компьютердің жалпы жұмыс уақыты; * ДК-нің орташа тәуліктік тоқтау уақыты; * қызметкердің жұмысқа қатысуының жалпы уақыты; * қызметкердің жұмыста болуының орташа тәуліктік уақыты; * орташа жұмыс уақыты; * жұмыстың аяқталуының орташа уақыты; * жұмыс күндерінің жалпы саны; * жұмыстың басталу/аяқталу уақыты, әр күн үшін компьютердің жұмыс уақыты/тоқтап қалуы көрсетілген қызметкердің жұмыс күндерін есепке алу күнтізбесі (жұмыстың ерте басталу фактілерін түстермен бөле отырып, жұмыстың кешігіп басталуы, жұмыстың ерте аяқталуы, жұмыстың кідіріспен аяқталуы); * әр күн үшін пайдаланушының компьютерінің белсенділігі/тоқтап қалу уақытының гистограммасы; c) пайдаланушының компьютеріндегі қосымшалардың белсенділігі туралы ақпарат, оның ішінде: * әр түрлі қосымшалардағы жұмыс уақытының пайызы (дөңгелек диаграмма құрумен) * іске қосылған қосымшалардың толық тізімі, олардың әрқайсысында абсолютті жұмыс уақыты көрсетілген; d) браузер қызметі туралы ақпарат: * кірген веб-ресурстардың рейтингі; * веб-шолғыштағы әрекет хронологиясы. e) пайдаланушы бастамашылық жасаған тіркелген қауіпсіздік инциденттерінің саны және әртүрлі дәрежедегі егжей-тегжейлері бар оларға сәйкес ережелер туралы ақпарат. 40. Жүйе ұйымдағы барлық бақыланатын пайдаланушылар бойынша жиынтық есептер шығаруды қамтамасыз етуі керек, олар келесі талаптарды қанағаттандыруы керек: Бақыланатын деректер арналары бойынша барлық бақылау уақыттары үшін немесе осы арнаны неғұрлым белсенді пайдаланатын пайдаланушылардың 10 (немесе кез келген басқа санын) көрсете отырып, таңдалған уақыт аралығы үшін жиынтық интерактивті есептерді құру мүмкіндігі. Белсенділігі қауіпсіздік ережелерін бірнеше рет іске қосуға әкелген пайдаланушылардың 10 (немесе кез келген басқа санын) көрсете отырып, барлық бақылау уақытындағы немесе таңдалған уақыт аралығындағы қауіпсіздік оқиғаларының саны бойынша жиынтық есептерді құру мүмкіндігі. Есептерді жасау кезінде осындай есептерді жасау кезінде тиісті параметрлердің жалпы жиынтық және орташа тәуліктік мәнін есепке алу мүмкіндігі қамтамасыз етілуге тиіс. Таңдалған пайдаланушылардың желілік және жергілікті белсенділігінің статистикалық

	көрсеткіштері туралы жиынтық интерактивті есептерді құру мүмкіндігі. Жүйе қауіпсіздік ережелерінің іске қосылу статистикасы туралы жиынтық интерактивті есептерді құру мүмкіндігін қамтамасыз етуі тиіс. Бұл ретте жүйе барлық пайдаланушылар мен пайдаланушылар топтары бойынша, сондай-ақ жекелеген пайдаланушылар бойынша статистиканы күндер, айлар бойынша, ерікті уақыт аралығы бойынша егжей-тегжейлерді таңдай отырып қарауды және әрбір ереже бойынша жеке және барлық қолданыстағы қауіпсіздік ережелері бойынша іске қосулардың қорытынды санын қарауды қамтамасыз етуге тиіс. 41. Жүйе ұйымда келесі талаптарды қанағаттандыруы тиіс топ 20 пайдаланушы бойынша браузер-белсенділік бойынша есептер құруды қамтамасыз етуі тиіс: Осы арнаны белсенді пайдаланатын 10 (ең көбі 20) пайдаланушыны көрсете отырып, таңдалған уақыт аралығы үшін кірген веб-ресурстар бойынша белгілі бір қызметкерлер бойынша есеп құру мүмкіндігі. Есепті құру кезінде сайттардың санаттарын (әлеуметтік желілер, бейне хостингтер және т.б.) және өнімділік бойынша есепке алу мүмкіндігі қамтамасыз етілуі керек. Сонымен қатар, әдепкі бойынша өнімділіктің 3 санаты бар: өнімсіз, бейтарап, өнімді. Сондай-ақ, жүйе белгілі бір пайдаланушылардан таңдалған санаттар бойынша есеп құру мүмкіндігін қамтамасыз етуі керек. 42. Жүйе ұйымдағы барлық бақыланатын пайдаланушылар үшін "жұмыс уақыты табельдері" есептерін құруды қамтамасыз етуі керек, олар келесі талаптарды қанағаттандыруы керек: Есепті белгілі бір уақыт аралықтары бойынша құру мүмкіндігі, мысалы: ағымдағы күнтізбелік ай, алдыңғы күнтізбелік ай немесе белгілі бір айды таңдау. Бұл ретте жүйе жұмыс кестесінен ауытқуларды қарауды қамтамасыз етуі тиіс, оның деректері (басы мен соңы) редакциялау мүмкіндігіне ие болуы тиіс. 43. Жүйенің жұмысын бақылау. Жүйе қолдау көрсетуі керек: - жүйенің барлық негізгі компоненттерінің жұмысы, сондай-ақ жабдық ресурстарын пайдалану туралы негізгі ақпарат берілген жүйенің жұмысын бақылау тақтасы - жүйенің серверлік компоненттерінің оқиғалар журналын жүргізу; - журналды, сондай-ақ әкімші консоліндегі әрбір оқиға бойынша толық ақпарат пен ұсыныстарды қарау; - журналдағы оқиғаларды оқиға күні, деңгейі (ақпарат, ескерту, қате), серверлік компонент, оқиға көзі бойынша сүзу; - мониторинг жүргізу үшін белгілі бір оқиға көзі серверлерін таңдау; - журналды оқиғаларды сақтау мерзімі және олардың деңгейі бойынша автоматты түрде тазарту; - оқиғалар журналын PDF, XPS, CSV, XLS, XLSX, HTML, RTF, TXT форматтарында экспорттау мүмкіндігі - оқиғалар журналын басып шығару мүмкіндігі; - пошта арқылы сервер компоненттерінің жаңа оқиғалары туралы жүйе әкімшісін автоматты түрде хабардар ету; - хабарламаларды пошта арқылы жіберу ережелерін орнату (адресатты, сервер компонентін, оқиға деңгейін немесе нақты оқиғаларды таңдау). 44. Жүйелер серверлік компоненттердің жұмысындағы барлық маңызды оқиғалар туралы мәліметтерді олар орнатылған жұмыс станциясының операциялық жүйесінің журналында жазуы керек. 45. Жүйенің масштабталуы. Желінің конфигурациясына,

	өңделетін ұсталған деректердің көлеміне және басқа параметрлерге байланысты жүйе үлкен және күрделі ұйымдастырылған желіні басқаруды, сондай-ақ желілік және аппараттық ресурстарға жүктемені бөлуді қамтамасыз ету үшін икемді түрде масштабталуы керек: Жүйенің барлық компоненттерінің жұмысын көп ағынды бағытқа бағыттау Жүйе көп ядролы және көп процессорлы жүйелерде жүктеменің таралуына толық қолдау көрсетуі керек. 46. Басқарудың ыңғайлылығы. Екі консольден тұратын жүйенің компоненттерін орталықтандырылған басқару: бір әкімші консолі және бір пайдаланушы консолі (АҚ қызметінің қызметкері). Жүйе әкімші консолі арқылы сервер параметрлерін қалпына келтіруді қолдайтын барлық сервер компоненттерінің конфигурациясының сақтық көшірмесін жасау мүмкіндігін қамтамасыз етуі керек. 47. Лицензиялау саясаты. Жүйе бақыланатын пайдаланушылар санына сәйкес лицензиялануы керек. Бұл ретте лицензияның нақты жұмыс станцияларына немесе пайдаланушыларға қатаң байланысын пайдалануға жол берілмейді. Сатып алынған лицензиялардың саны тек бір уақытта бақыланатын пайдаланушылардың санын анықтауы керек, ал бақыланатын тізімнің өзі қажет болған жағдайда тез және икемді түрде өзгеруі мүмкін (мысалы, желіде 100 пайдаланушы және тек 50 лицензия болса-алдымен кейбір пайдаланушыларды, содан кейін басқаларын іріктеп бақылау мүмкіндігі; бұл ретте лицензиялық слоттарды қайта тағайындау тәулігіне кемінде 1 рет мүмкін болуы тиіс). Лицензиялау жүйесі құрамдас жеткізуді, яғни бақыланатын деректер түрлерін таңдауды және пайдаланылмаған функционалды лицензия деңгейінде өшіруді қамтамасыз етуі керек. 48. Қолдау қызметіне қол жеткізу. * 8 * 5 уақыт бойынша техникалық қолдау (аптасына 8 сағат 5 күн-жергілікті уақыт бойынша жұмыс күндері GMT +5); * Телефон және интернет-арналар арқылы қолдауға жүгіну; * Өтініштер саны-шектеусіз; * Әрекет ету уақыты 4 (төрт) сағаттан аспайды (сағаттық қамту кезеңінде). 5.3. Жеткізуші келесі міндетті қадамдарды орындауы керек: 5.3.1. Сервер компоненттері мен мәліметтер базасын орналастыру. 5.3.1.1. Жүйенің артқы жағын орнату 5.3.1.2. Толық мәтінді іздеудің жоғары жылдамдығын және ұсталған файлдар мен мұрағаттардың көлеңкелі көшірмелерін сенімді сақтауды қамтамасыз ету үшін дерекқор параметрлерін оңтайландыру. 5.3.1.3. Автоматты сақтық көшірмені орнату (сақтық көшірме) жүйе конфигурациясы және жинақталған оқиғалар журналдары. 5.3.2. Тапсырыс берушінің ат-инфрақұрылымымен Интеграция 5.3.2.1. Кешенді корпоративтік каталог қызметімен интеграциялау (бар болса). 5.3.2.2. Трафикті шағылыстыруды орнату. 5.3.3. Клиенттік модульдерді (агенттерді) орналастыру. 5.3.3.1. Пайдаланушылардың жұмыс станцияларында агенттік бағдарламалық қамтамасыз етуді орталықтандырылған (жасырын) орналастыру (сатып алынған лицензиялар санына сәйкес). 5.3.3.2. Агенттердің жасырын параметрлерін орнату және оларды рұқсатсыз жоюдан, қызметтерді тоқтатудан немесе пайдаланушылардың конфигурациясын өзгертуден қорғау. 5.3.4. Ақпараттық қауіпсіздік саясатын орнату. 5.3.4.1. Құпия ақпараттың, дербес

	деректердің, мөрлер мен қолтаңбалар сканерлерінің берілуін анықтау үшін негізгі қауіпсіздік саясаттарын (сөздіктер, тұрақты өрнектер, құжаттардың цифрлық іздері) құру және бейімдеу. 5.3.4.2. Жазылатын файлдарды көлеңкелі түрде көшіру және рұқсат етілген құрылғылардың "ақ тізімдерін" жасау мүмкіндігімен сыртқы дискілерді (USB флэш-дискілерін) пайдалануды бақылау ережелерін орнату. 5.3.4.3. Алмасу буферін басқаруды, Құжаттарды басып шығаруға шығаруды және файлдарды жалпыға ортақ мессенджерлер мен бұлтты сақтау арқылы жіберуді орнату. 5.3.4.4. Автоматты хабарландыруларды орнату. 5.3.5. Бастапқы статистиканы жинау және Тапсырыс берушінің заңды бизнес-процестерін анықтау үшін "аудит/мониторинг" режимінде жүйені іске қосу. 5.3.6. Тапсырыс берушімен келісілген деректерді беру арналары бойынша жүйені "белсенді алдын алу/бұғаттау" режиміне ауыстыру. 5.4. Жеткізуші антивирустық бағдарламалық жасақтаманы орналастыру және іске қосу бойынша бірқатар тапсырмаларды орындауы керек. 5.4.1. Өнім беруші соңғы нүктелерді орталықтандырылған вирусқа қарсы қорғаудың мамандандырылған бағдарламалық қамтамасыз етуін пайдалану құқығына ерекше емес лицензиялар қоюға және оны орнату, Тапсырыс берушінің кемінде 300 жұмыс станциясында конфигурациялау жөніндегі міндеттер кешенін орындауға міндетті. 5.4.2. Жеткізілетін бағдарламалық қамтамасыз етуде орталықтандырылған мониторинг пен қауіпсіздік саясатын басқарудың бірыңғай консолі бар клиент-сервер архитектурасы болуы тиіс, нақты уақыт режимінде қауіп-қатерді қолтаңбалық, эвристикалық және белсенді мінез-құлық талдау модульдерін, төлем бағдарламаларынан, руткиттерден, зиянды және шпиондық бағдарламалардан қорғауды, желілік шабуылдарды анықтау және алдын алу жүйесін және соңғы нүктенің желілік экранын, веб-трафикті және пошта хабарламаларын басқару, қосымшаларды іске қосуды басқару модулі, сондай-ақ сыртқы алынбалы электрондық ақпарат тасымалдағыштар мен перифериялық интерфейстердің қосылуы мен пайдаланылуын бақылау модулі. Антивирустық қорғаныс агенттерінде конфигурацияны рұқсатсыз өзгертуден, қызметтерді жүктеуден немесе жергілікті пайдаланушылардың әкімшілік артықшылықтарсыз жоюынан өзін-өзі қорғаудың кіріктірілген механизмдері болуы керек. 5.4.3. Желілік сегменттерді бөлу туралы заңнамалық талапты және контурларды тікелей жұптастыруға тыйым салуды ескере отырып, Жеткізуші Тапсырыс берушінің тиісті желілік инфрақұрылымы шеңберінде: сыртқы контурдың жергілікті желісі үшін және ішкі контурдың жергілікті желісі үшін антивирустық қорғауды басқарудың 2 (екі) дербес серверін орналастыруға міндетті. 5.5. Жеткізуші Active Directory-де екі тәуелсіз қоғамдық және жеке желілер үшін (кемінде 80 пайдаланушы) ақпаратты басқару саясатын енгізіп, конфигурациялауы керек. 5.5.1. Баптау шеңберінде пайдаланушыларды, құрылғылар мен ресурстарды орталықтандырылған басқаруды, ақпаратқа қол жеткізуді шектеуді, ақпараттық қауіпсіздік талаптарын сақтауды ұйымдастыру талап етіледі. 5.5.2. Домендік құрылымға қойылатын жалпы талаптар. 5.5.2.1. Active

	Directory Domain Services (AD DS) пайдалану. 5.5.2.2. Қоғамдық және жеке желілерде OU және GPO жиынтықтары бар екі тәуелсіз Домен. 5.5.3. Екі желіні оқшаулауға қойылатын талаптар. 5.5.3.1. Әрбір қоғамдық және жеке желі жеке қауіпсіздік контуры ретінде қарастырылуы керек. 5.5.3.2. Пайдаланушыларды, компьютерлерді, серверлерді, кіру топтарын, топтық саясаттарды міндетті түрде бөлу қажет. 5.5.3.3. Желілер арасындағы саясатты автоматты түрде мұрагерлікке тыйым салуды және берілген саясаттар мен топтар арқылы желілер арасындағы өзара әрекеттесуді қамтамасыз ету қажет. 5.5.4. Ou ұйымы (gganizational Units). Жеткізуші екі publlic және Private желілерінің әрқайсысы үшін тәуелсіз OU (gganizational Units) иерархиясын құру бойынша аналитикалық жұмыс жүргізуі керек. 5.5.5. Қауіпсіздік саясаты (Group Policy Objects). Жеткізуші ақпараттық қауіпсіздік талаптарына сәйкес publlic және Private екі желісінің әрқайсысы үшін GPO (Group Policy Objects) құру бойынша талдамалық жұмыс жүргізуі тиіс: 5.5.5.1. Аутентификация және тіркелгі саясаты. Құпия сөз саясатын орнату: ең аз ұзындық; күрделілік; жарамдылық мерзімі; құпия сөз тарихы. 5.5.5.2. Есептік жазбаны бұғаттау саясаты: сәтсіз әрекеттер саны; бұғаттау уақыты. 5.5.5.3. Пайдаланушыны басқару саясаты: жергілікті әкімші құқықтарын шектеу, кіріктірілген әкімші тіркелгісін пайдалануға тыйым салу, пайдаланушының кіруін уақыт пен құрылғы түрі бойынша басқару, user Rights Assignment орнату. 5.5.5.4. Жұмыс станциялары мен серверлерді басқару саясаты: рұқсат етілмеген Бағдарламалық жасақтамаға тыйым салу (Software Restriction Policies / AppLocker); жаңартуларды басқару (WSUS немесе Windows Update саясаты); қауіпті қызметтер мен хаттамаларды өшіру; USB құрылғылары мен алынбалы медианы басқару; BitLocker орнату (бар болса және қажет болса). 5.5.5.5. Желілік қауіпсіздік саясаттары: ішкі желілер үшін әртүрлі профильдері бар Windows Firewall орнату; ішкі желілер арасындағы желілік қосылымдарды шектеу; SMB, RDP, PowerShell Remoting басқару; IPsec орнату (қажет болса). 5.5.6. Ақпаратты басқару және қол жетімділік саясаты. Жеткізуші ақпараттық қауіпсіздік талаптарына сәйкес Publlic және Private екі желісінің әрқайсысы үшін ақпаратты басқару және қолжетімділік саясатын құру бойынша талдамалық жұмыс жүргізуі тиіс соның ішінде: 5.5.6.1. Ресурстарға қол жеткізуді шектеу: rbac (Role-Based Access Control) моделін іске асыру, қауіпсіздік топтарын пайдалану: файлдық ресурстарға қол жеткізу; қосымшаларға қол жеткізу; қызметтерге қол жеткізу, пайдаланушыларға құқықтарды тікелей тағайындауды болдырмау. 5.5.6.2. Файлдық ресурстарды басқару: NTFS рұқсаттарын минималды қол жетімділік принципі бойынша конфигурациялау, "Read / Modify / Full Control" топтарын пайдалану, ішкі желілер арасында кросс-қатынасуға тыйым салу, маңызды деректерге қол жетімділік аудитін орнату. 5.5.7. Аудит, лог. Advanced Audit Policy қосу керек: 5.5.7.1. пайдаланушыларға кіру/шығу; 5.5.7.2. есептік жазбаларды өзгерту; 5.5.7.3. нысандарға қол жеткізу; 5.5.7.4. GPO

	өзгерістері. 5.5.8. Жеткізуші жұмыс және тексерілген GPO, ad логикалық схемасын қамтитын құжаттаманы ұсынуға міндетті; ou сипаттамасы және саясат; топтар мен кіру құқықтарының тізімі; әкімшілерге арналған нұсқаулар. 5.5.9. Баптау ауқымдылықты, одан әрі кеңейту мүмкіндігін және Қазақстан Республикасының мемлекеттік органдарына қолданылатын ақпараттық қауіпсіздіктің өзгертілген талаптарына сәйкестігін қамтамасыз етуге тиіс. 6. Құпия ақпаратты жария етпеу туралы талаптар 6.1. Өнім беруші жұмыс жүргізу кезінде өзіне белгілі болған барлық ақпараттың, оның ішінде Ақпараттық жүйелер, жергілікті-есептеу желісі, желілік инфрақұрылым архитектурасы, ақпараттық қауіпсіздік құралдары мен оқиғалары, есептік жазбалар, жабдықтар мен бағдарламалық қамтамасыз етуді баптау параметрлері, желінің мекенжай кеңістігі, қосылу схемалары, пайдалану құжаттамасы, сондай-ақ өзге де қызметтік, Тапсырыс берушінің ақпаратын таратуға техникалық, ұйымдастырушылық және шектеулі. 6.2. Өнім беруші Тапсырыс берушінің жазбаша келісімінсіз Қазақстан Республикасының заңнамасында тікелей көзделген жағдайларды қоспағанда, Шартты орындау шеңберінде алынған ақпаратты жария етуге, үшінші тұлғаларға беруге, жариялауға, көшіруге, көбейтуге, жеке немесе коммерциялық мақсаттарда пайдалануға, сондай-ақ өзге де жолмен таратуға құқылы емес. 6.3. Өнім беруші көрсетілген ақпаратқа тек өз қызметкерлеріне және тартылған мамандарға ғана қол жеткізуді қамтамасыз етуге міндетті, оларға мұндай қол жеткізу шарт бойынша міндеттемелерді орындау үшін ғана қажет. 6.4. Өнім беруші құпия ақпаратты рұқсатсыз кіруден, көшіруден, өзгертуден, жоюдан, бұғаттаудан және таратудан, оның ішінде қашықтан қосылу, файлдармен алмасу, алынбалы ақпарат тасығыштарды, есепке алу деректерін және әкімшілендіру құралдарын пайдалану кезінде қорғау жөнінде қажетті ұйымдастырушылық және техникалық шараларды қабылдауға міндетті. 6.5. Тапсырыс берушіден алынған құжаттарды, электрондық файлдарды, есептік жазбаларды, резервтік көшірмелерді, конфигурацияларды, схемаларды, оқиғалар журналдарын және өзге де материалдарды өнім беруші шартты орындау мақсатында ғана пайдалануы тиіс және жұмыстар аяқталғаннан кейін, егер Шарттың талаптарында немесе Қазақстан Республикасының заңнамасында өзгеше көзделмесе, Тапсырыс берушінің талабы бойынша Тапсырыс берушіге қайтарылуға не жойылуға тиіс. 6.6. Құпия ақпараттан айырылу, жария ету, рұқсатсыз қол жеткізу не өзге де компаға келу фактісі анықталған жағдайда өнім беруші дереу, бірақ анықталған сәттен бастап 1 жұмыс күнінен кешіктірмей Тапсырыс берушіге осындай факт, оның себептері, ақпараттың көлемі және салдарларды барынша азайту жөнінде қолданылған шаралар туралы жазбаша хабарлауға міндетті. 7. Қосымша талаптар 7.1. Сатып алу нысанасы желілік инфрақұрылым мен ақпараттық қауіпсіздіктің өзара байланысты компоненттерін, соның ішінде серверлік жабдықты, маршрутизаторларды, коммутаторларды, сымсыз кіру нүктелерін, кабельдік ішкі жүйені, электрмен жабдықтауды, сондай-ақ ақпараттың ағып кетуін болдырмайтын

	бағдарламалық жасақтаманы орнатуды, орнатуды, конфигурациялауды, интеграциялауды және пайдалануға беруді қамтитындықтан, жеткізуші орталықтандырылған жобаны іске асырудың барлық кезеңдерінде тапсырмалардың орындалуын басқару. Жеткізу мерзімдерін үйлестіру, монтаждау және іске қосу-баптау жұмыстарының реттілігін ұйымдастыру, Тапсырыс берушінің қолданыстағы инфрақұрылымының тоқтап қалу Тәуекелдерін басқару, сервистерді ауыстыру кезеңдерін келісу, кестенің орындалуын бақылау, Тапсырыс берушінің жауапты өкілдерімен өзара іс-қимыл жасау, сондай-ақ өнім берушінің атқарушылық құжаттамасын уақтылы дайындауды қамтамасыз ету үшін жобалық менеджменттің халықаралық әдістемелеріне сәйкес міндеттердің орындалу барысын басқаруды ұйымдастыруға тиіс. 7.2. Жеткізуші жобаны іске асыру шеңберінде Тапсырыс берушінің әкімшілік ғимаратында орналасқан мекемелерде ақпаратты өңдеу процестерін талдау және регламенттеу жөніндегі міндеттер кешенін орындауы тиіс. 7.2.1. Жеткізуші Тапсырыс берушінің мекемелерінде ақпаратты өңдеу мен берудің ағымдағы ("as is") процестеріне талдау жүргізуі керек, соның ішінде: 7.2.1.1. электрондық поштаны, мессенджерлерді, веб-ресурстарды және бұлттық Қызметтерді пайдалану; 7.2.1.2. жергілікті жұмыс станцияларында, желілік ресурстарда және сыртқы тасымалдағыштарда файлдармен жұмыс істеу; 7.2.1.3. жергілікті және желілік принтерлерде Құжаттарды басып шығару; 7.2.1.4. бөлімшелер мен сыртқы контрагенттер арасындағы өзара әрекеттесу ерекшеліктері. 7.2.2. Жүргізілген талдау негізінде өнім беруші ақпараттық қауіпсіздік саясатына және бағдарламалық жасақтаманы одан әрі конфигурациялау үшін ақпараттың ағып кетуіне жол бермеуге қойылатын талаптарды қалыптастыруы керек, соның ішінде: 7.2.2.1. бақылауға жататын ақпарат санаттарының тізбесі (құпия, қызметтік, Дербес деректер және т. б.); 7.2.2.2. әрбір санат үшін рұқсат етілген және рұқсат етілмеген деректер арналары; 7.2.2.3. операцияларды бұғаттауға, рұқсат беруге және келісуге қойылатын талаптар (жіберу, көшіру, басып шығару, тасығыштарға жазу және т.б.). 7.3. Өнім беруші ақпараттық қауіпсіздік жөніндегі техникалық құжаттаманы әзірлеуі (өзектендіруі) тиіс. 7.3.1. Өнім беруші ақпараттық қауіпсіздік саясатын (ұйымның негізгі құжаты), ұйымның телекоммуникациялық жабдықтарын басқару және қызмет көрсету жөніндегі нұсқаулықтарды, есепке алу журналдарының нысандарын, ұйым қызметкерлерінің АҚ ережелерімен танысу парақтарын қамтитын құжаттар жиынтығын әзірлеуге тиіс. Сондай-ақ, жеткізуші ұйымның АҚ-ның басқа құжаттары мен рәсімдерін әзірлеу кезінде консультациялық көмек көрсетуі керек. 7.3.2. Келесі қадамдарды орындау қажет: 7.3.2.1. Тапсырыс берушінің ақпараттық қауіпсіздігінің ағымдағы жай-күйін талдау. 7.3.2.2. Тапсырыс берушінің бизнес-процестерінің ерекшелігін ескере отырып, құжаттардың мәтіндерін жазу. 7.3.2.3. Құжаттардың жобаларын Тапсырыс берушіге беру, ескертулер жинау және оларды пысықтау. 7.3.2.4. Құжаттардың соңғы жиынтығын электрондық (және қажет болған жағдайда баспа түрінде) дайындау. 7.3.3.

	Құжаттар орыс тілінде, өңделетін форматта (DOCX, XLSX) жасалуы керек. 7.3.4. Құжаттар ҚР АҚ саласындағы қолданыстағы нормативтік-құқықтық актілерге сәйкес болуы тиіс. 7.3.5. Егер құжат мерзімді толтыруды қажет етсе, онда жеткізуші осындай құжаттардың шаблондарын ұсынуы керек. 7.3.6. Құжаттардың ең аз тізбесі: 7.3.6.1. Ақпараттық қауіпсіздік саясаты 7.3.6.2. Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі 7.3.6.3. Ақпаратты өңдеу және оларды түгендеу құралдарымен байланысты активтерді сәйкестендіру, жіктеу, таңбалау, паспорттау қағидалары 7.3.6.4. Ақ ішкі аудитін жүргізу қағидалары 7.3.6.5. Ақпаратты криптографиялық қорғау құралдарын пайдалану ережелері 7.3.6.6. Электрондық ақпараттық ресурстарға қол жеткізу құқықтарын аутентификациялау және саралау рәсімін ұйымдастыру қағидалары 7.3.6.7. Вирусқа қарсы бақылауды ұйымдастыру, мобильді құрылғыларды, ақпарат тасығыштарды, интернет пен электрондық поштаны пайдалану қағидалары 7.3.6.8. Ақпаратты өңдеу құралдарымен байланысты активтердің физикалық қорғалуын, жұмыс істеуінің қауіпсіз ортасын ұйымдастыру және үздіксіз жұмысын қамтамасыз ету қағидалары 7.3.6.9. Ақпараттандыру объектісін сүйемелдеу, ақпараттың сақтық көшірмесін жасау және қалпына келтіру жөніндегі әкімшінің нұсқауы 7.3.6.10. Ақ инциденттеріне және штаттан тыс (дағдарыстық) жағдайларда әрекет ету бойынша пайдаланушылардың іс-қимыл тәртібі туралы Нұсқаулық 7.3.6.11. Серверлік және телекоммуникациялық жабдықтарды, деректерді сақтау жүйелерін, жұмыс станцияларын, ақпарат тасығыштарды кәдеге жарату және(немесе) қайта пайдалануға дайындау рәсімін құжаттау (мысалы, актілер, Бұйрықтар немесе басқалар) 7.3.6.12. Ұйымдағы ақ үздіксіздігін қамтамасыз ететін құжаттық стратегия немесе процесс 7.3.6.13. АҚ және бизнес-процестердің үздіксіздігін қамтамасыз ету және штаттан тыс (дағдарыстық) жағдайдан кейін қалпына келтіру жоспары (рәсімдер мен процестер) 7.3.6.14. Ақпараттың сақтық көшірмесін жасау рәсімдерінің орындалуын тіркейтін құжаттар (мысалы, актілер, хаттамалар және басқалар) 7.3.6.15. Резервтік көшірмелерді тестілеуді тіркейтін құжаттар (мысалы, актілер, хаттамалар және басқалар) 7.3.6.16. Желілік жабдықты басқару порттарының бекітілген тізбесі 7.3.6.17. Жергілікті желінің құжатталған бекітілген схемасы 7.3.6.18. Ақпаратты өңдеу құралдарымен байланысты активтердің қауіптер (тәуекелдер) каталогын құжаттау 7.3.6.19. Бекітілген тәуекелдерді өңдеу жоспарын құжаттау 7.3.6.20. Ведомстволық (корпоративтік) телекоммуникация желісінің құжатталған схемасы 7.3.6.21. Кабельдік қосылыстарды құжаттау 7.3.6.22. Құжатталған орнату (жаңарту) рәсімдері (БҚ (қолданбалы және жүйелік)) (мысалы, актілер, журналдар, тізілімдер және басқалар) 7.3.6.23. Желілік жабдықты басқару рәсімін реттеу 7.4. Конкурстық өтінім құрамында әлеуетті Өнім берушіге ҚР СТ ISO/IEC 15408-3-2017 "Ақпараттық технологиялар. Қауіпсіздік әдістері мен құралдары. Ақпараттық технологиялардың қауіпсіздігін бағалау критерийлері. 3 бөлім. Қорғауды қамтамасыз етуге қойылатын талаптар". Сенімнің

	бағалау деңгейі 5-тен төмен емес. 8. Жұмыс нәтижесі. 8.1. Жұмыстарды жүргізу қорытындылары бойынша өнім беруші ақпараттық қауіпсіздіктің бағдарламалық-аппараттық кешенін орнатуды, монтаждауды, баптауды, интеграциялауды, іске қосуды және техникалық ерекшелікте көзделген толық көлемде тапсырыс берушінің желілік инфрақұрылымын жаңғыртуды қамтамасыз етуге тиіс. Жұмыстардың нәтижесі серверлік жабдықты, маршрутизаторларды, коммутаторларды, сымсыз кіру нүктелерін, электрмен қоректендіру құралдарын, ақпараттық қауіпсіздікті бағдарламалық қамтамасыз етуді, сондай-ақ ерекшелікте көзделген өзге де компоненттерді қамтитын жұмысқа қабілетті, бапталған және пайдалануға дайын инфрақұрылымды құру болып табылады. 8.2. Жұмыстарды жүргізу нәтижесінде жабдық көзделген орналастыру орындарында физикалық түрде орнатылуы, электрмен жабдықтау және деректерді беру желілеріне қосылуы, жұмысқа қабілеттілігі тексерілуі және Тапсырыс берушінің қолданыстағы инфрақұрылымына интеграциялануы тиіс. Жеткізілім құрамына кіретін барлық серверлер, маршрутизаторлар, коммутаторлар, кіру нүктелері, үздіксіз қуат көздері және басқа құрылғылар орнатылып, өзара әрекеттесудің жалпы схемасына енгізіліп, штаттық пайдалану жағдайына ауыстырылуы керек. 8.3. Жұмыстарды жүргізу қорытындысы бойынша серверлік жабдық телекоммуникациялық шкафтарға орнатылуы, электр қуатына қосылуы, базалық жүйелік деңгейде конфигурациялануы және кешен құрамында пайдалануға дайындалуы тиіс. Дискінің ішкі жүйелерін, RAID-массивтерін, басқару интерфейстерін, желілік параметрлерді және техникалық сипаттамада көзделген өзге де параметрлерді жеткізуші серверлердің сенімді және үздіксіз жұмыс істеуі үшін жеткілікті көлемде орындауы тиіс. 8.4. Желілік жабдық желіні сегменттеуді, маршруттауды, ақауларға төзімділікті, коммутацияны, құрылғыларды авторизациялауды және соңғы тораптарды қосуды қоса алғанда, Тапсырыс берушінің жергілікті-есептеу желісінің штаттық жұмыс істеуін қамтамасыз етуі тиіс. Маршрутизаторлар мен коммутаторларда интерфейстердің, VLAN, маршруттардың, қол жеткізуді басқару тетіктерінің, қызмет көрсету сапасының саясатының, қорғалған әкімшілендірудің және техникалық ерекшелікте көзделген өзге де параметрлердің қажетті параметрлері орындалуы тиіс. 8.5. Жұмыстарды жүргізу қорытындысы бойынша сымсыз желі көзделген қамту аймақтарында орналастырылуы, бапталуы және пайдалануға берілуі тиіс. Кіру нүктелері орнатылуы, деректер желісі мен қуат көзі арқылы қосылуы, орталықтандырылған басқаруға қосылуы, радио желісі, қауіпсіздік, SSID және VLAN параметрлері бойынша конфигурациялануы, сондай-ақ көзделген қызмет көрсету аймағы шегінде пайдаланушы құрылғыларының тұрақты сымсыз қосылуын қамтамасыз етуі тиіс. 8.6. Ақпараттың ағып кетуін болдырмау және деректерді беру арналарын бақылау бағдарламалық жасақтамасы техникалық сипаттаманың функционалдық талаптарына сәйкес орнатылуы, іске қосылуы, Тапсырыс берушінің инфрақұрылымымен интеграциялануы және конфигурациялануы керек. Жұмыстарды жүргізу қорытындылары бойынша жүйенің

	серверлік бөлігінің жұмыс қабілеттілігі, желілік инфрақұрылыммен, каталог қызметімен, пошталық және өзге де ақпараттық сервистермен өзара іс-қимыл (қажет болған жағдайда), сондай-ақ ақпараттық қауіпсіздік инциденттерін мониторингтеу, тіркеу, талдау және алдын алу саясаттарының жұмыс істеуі қамтамасыз етілуге тиіс. 8.7. Жұмыстардың нәтижесін Тапсырыс берушіге берген кезде, Бар болса, логиндерді, парольдерді, кіру кілттерін, лицензиялар, сериялық нөмірлер, кепілдік міндеттемелер және техникалық қолдау туралы мәліметтерді қоса алғанда, одан әрі пайдалану үшін қажетті барлық мәліметтер мен материалдар берілуі тиіс. 8.8. Шартты орындаудың түпкілікті нәтижесі желілік өзара іс-қимылды, серверлік және сымсыз компоненттерді пайдалануды, сондай-ақ осы техникалық ерекшеліктің талаптары шегінде ақпараттық қауіпсіздік міндеттерін орындауды қамтамасыз ететін бірыңғай жұмыс істейтін инфрақұрылымды құру болып табылады. Орындалу мерзімі 2027 жылғы 31 желтоқсанға дейін.
Әлеуетті өнім беруші оны жеңімпаз деп айқындаған және онымен мемлекеттік сатып алу туралы шарт жасасқан жағдайда (қажет болған жағдайда көрсетіледі) (Әлеуетті өнім берушінің көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін бас тартуына жол берілмейді)	

Приложение 15
к конкурсной документации

Техническая спецификация
закупаемых работ, не связанных со строительно-монтажными работами
(заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Управление цифровых технологий области Абай"
Наименование организатора	Государственное учреждение "Управление государственных закупок области Абай"
№ конкурса:	№ 17859608-2
Наименование конкурса:	Комплексные работы в сфере информационных технологий «под ключ»
Номер лота:	№ 88191553-ОК1
Наименование лота:	Комплексные работы в сфере информационных технологий «под ключ»
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	620920.000.000000
Наименование работы:	Комплексные работы в сфере информационных технологий «под ключ»
Единица измерения:	Работа
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	618572100
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	618572100
Срок выполнения работы:	согласно технической спецификации
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	Наименование объекта Место расположения Административное здание Республика Казахстан, Область Абай г.Семей, ул. К.Мухамедханова, 8. 1. Цели проведения работ. 1.1. Основной целью закупки работ является проведение работ сфере информационных технологий «под ключ» с установкой и настройкой программного обеспечения для предотвращения утечек информации и корректно сконфигурированного активного и пассивного телекоммуникационного сетевого оборудования, предназначенного для агрегации подключений пользователей к основным информационным системам Заказчика. 1.2. Здание расположено по адресу область Абай, г. Семей, ул. Каюма Мухамедханова, 8. Здание имеет 5 этажей и технический этаж. 2. Требования к исполнительной документации. 2.1. После завершения выполнения работ Поставщик должен предоставить Заказчику следующую исполнительную документацию: 2.1.1. Структурная схема линий связи 2.1.2. Монтажная схема линий связи 2.1.3. Вертикальные магистральные схемы соединений 2.1.4. Схемы размещения оборудования в телекоммуникационных шкафах 2.1.5. Рефлектограммы на оптические линии связи; 2.1.6. Кабельные журналы 3. Количественные и качественные характеристики сетевой инфраструктуры. 3.1. Количество рабочих мест (РМ) на этаже: 3.1.1. Технический этаж – не менее 5 РМ 3.1.2. Первый этаж - не менее 15 РМ; 3.1.3. Второй этаж - не менее 120 РМ; 3.1.4. Третий этаж - не менее 120 РМ; 3.1.5. Четвёртый этаж - не менее 120 РМ; 3.1.6. Пятый этаж – не менее 40 РМ; 3.2. В случае необходимости, потенциальный поставщик самостоятельно и за свой счет должен иметь возможность провести обследование здания со сбором необходимых данных для формирования корректного технического решения задач. 3.3. Модернизация элементов сетевой инфраструктуры должна включать активное, пассивное сетевое оборудование, серверы, источники бесперебойного питания, шкафы для размещения устройств, материалы для монтажа и наладки оборудования, необходимое программное обеспечение. 3.4. При разработке технического решения по составу элементов при модернизации сетевой инфраструктуры должны быть обеспечены следующие требования: 3.4.1. архитектура и параметры производительности должны соответствовать требованиям стандарта ISO/IEC 11801, описывающего построение структурированных кабельных систем (СКС) и строительным нормам СН РК 3.02-17-2011; 3.4.2. кабельная транспортная среда, активное сетевое оборудование (кроме серверов), должны иметь не менее чем 10% запас портов и кабельной ёмкости для обеспечения возможности увеличения числа пользователей. 3.4.3. для всех клиентов сети должна быть обеспечена авторизация на портах Ethernet по технологии IEEE_802.1X. В составе оборудования и сопутствующего ПО должны быть предусмотрены все компоненты для организации сервисов аутентификации, авторизации и учета (AAA). Потенциальный поставщик должен развернуть все соответствующие технические решения и осуществить плановый (по согласованию с Заказчиком) ввод всех клиентских устройств сети. 4. Требования к модернизации

	сетевой инфраструктуры 4.1. Сетевая инфраструктура должна состоять из двух сегментов независимых информационных сетей - Private Network и Public Network. 4.1.1. Вышеуказанные сети не должны иметь физического соединения. 4.2. Private Network - закрытая локально-вычислительная сеть (далее ЛВС) для использования единой телекоммуникационной сети государственных органов (ЕТС ГО). 4.2.1. Необходимо предусмотреть физическую коммутацию с каналом связи ЕТС ГО РК. 4.2.2. Требуется произвести настройку инфраструктуры сети Private для обеспечения защищённого доступа в сеть ЕТС ГО с использованием логического сегментирования сети на уровне учреждений, расположенных в здании. 4.2.3. Управлением всеми сетевыми ресурсами в Private Network должен производить центральный маршрутизатор. Он, в свою очередь, должен быть подключен к внешней сети ЕТС ГО через брандмауэр - межсетевой экран или сетевой экран (предоставляется Заказчиком) (комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами). 4.2.4. Для выполнения централизованной аутентификации и авторизации в Private Network должно использоваться программное обеспечение (RADIUS-сервер) установленное на сервере, использующее протокол RADIUS (Remote Authentication Dial-In User Service) IEEE 802.1X. При подключении устройства к порту настроенного коммутатора Ethernet должна происходить аутентификация подключенного устройства и выдача прав доступа к соответствующим сегментам и ресурсам сети. Сегментирование должно быть выполнено как на втором, так и на третьем уровнях сетевой модели OSI в зависимости от требований к сегментированию в конкретном сегменте. 4.2.5. Головной коммутатор сети должен обеспечивать отказоустойчивость сети путем использования стека, состоящего из 2 коммутаторов. От каждого элемента стека должна быть предусмотрена отдельная оптическая линия связи до каждого коммутатора агрегации. 4.2.6. Коммутатор агрегации сети должен обеспечивать отказоустойчивость сети путем использования стека, состоящего из 2 коммутаторов. От каждого элемента стека должна быть предусмотрена отдельная оптическая линия связи до каждого этажного коммутатора доступа. 4.3. Public Network - общая телекоммуникационная сеть для подключения к сети Internet. 4.3.1. Управление всеми сетевыми ресурсами должен производить центральный маршрутизатор, который в свою очередь подключен к внешней сети через брандмауэр (предоставляется Заказчиком) с защитными функциями. 4.3.2. Требуется произвести настройку инфраструктуры сети Public для обеспечения защищённого доступа в сеть Интернет с использованием логического сегментирования сети на уровне учреждений, расположенных в здании. 4.3.3. Для выполнения централизованной аутентификации и авторизации в Public Network должно использоваться программное обеспечение (RADIUS-сервер) установленное на сервере использующее протокол RADIUS (Remote Authentication Dial-In User Service) IEEE 802.1X. При

	подключении устройства к порту настроенного коммутатора Ethernet должна происходить аутентификация подключённого устройства и выдача прав доступа к соответствующим сегментам и ресурсам сети. Сегментирование должно быть выполнено как на втором, так и на третьем уровнях сетевой модели OSI в зависимости от требований к сегментированию в конкретном сегменте сети. 4.3.4. Головной коммутатор сети должен обеспечивать отказоустойчивость сети путем использования стека, состоящего из 2 коммутаторов. От каждого элемента стека должна быть предусмотрена отдельная оптическая линия связи до каждого коммутатора агрегации. 4.3.5. Коммутатор агрегации сети должен обеспечивать отказоустойчивость сети путем использования стека, состоящего из 2 коммутаторов. От каждого элемента стека должна быть предусмотрена отдельная оптическая линия связи до каждого этажного коммутатора доступа. 4.4. Технические требования к кабельной подсистеме 4.4.1. Поставщик должен обеспечить возможность передачи данных в структурированных кабельных сетях (СКС) со скоростью не менее 100 Мбит/сек; 4.4.2. Рабочее место сотрудника Заказчика должно иметь в своем составе как минимум одну двойную розетку (коннекторы типа RJ45), содержащую два информационных гнезда. 4.4.3. Информационные розетки должны монтироваться внутри кабельного короба, либо устанавливаться в специальных боксах, должны быть соблюдены требования минимального запаса кабеля. 4.4.4. Крышка кабельного короба должна защелкиваться жестко и четко, без зазоров, вид короба должен быть эстетически хорошим, необходимо использование кабельных аксессуаров. Короб должен быть выполнен из материала ПВХ не поддерживающего горение. 4.4.5. Кроссовая часть СКС должна состоять из патч-панелей на 24 или 48 портов с разъемами типа RJ45, категории не ниже 5е, стандартов ISO 11801, TIA'568'B и EN 50173, и иметь сопутствующие аксессуары для обеспечения крепежа и соединений. 4.4.6. Горизонтальная подсистема должна обеспечивать соединение между кроссовым оборудованием, информационными розетками на рабочем месте. Она должна содержать кабель типа «неэкранированная витая пара, UTP», 4-х парный с толщиной жил не менее 0.411 мм (24-AWG). Кабель по физическим и электрическим характеристикам должен соответствовать стандартам категории не ниже 5е. 4.4.7. Вертикальная магистральная кабельная система должна начинаться от узла коммуникации до каждого телекоммуникационного этажного шкафа. При создании вертикальной кабельной системы необходимо запланировать резерв несущих кабель конструкций не менее 5% от требуемых на момент проектирования кабельных трасс. Прокладка кабеля должна соответствовать топологии типа «звезда», в которой центром является кросс коммутационного шкафа. 4.4.8. Вертикальная кабельная система должна быть выполнена с использованием внутри объектового одномодового или многомодового оптического кабеля, соответствующего требованиям по дальности и полосе пропускания. 4.4.9. Так как на каждом рабочем месте должно быть установлено не менее двух

	информационных коннекторов, то к каждому рабочему месту должно быть проложено соответствующее количество кабелей "витая пара" не ниже 5е категории. Длина каждой линии кабельного соединения (общей линии без активного телекоммуникационного оборудования) для компьютерной сети не должна превышать 90 м. При этом каждое кабельное соединение должно быть выполнено при использовании одного отрезка кабеля и не должно иметь никаких соединений на всем своем протяжении. 4.4.10. Прокладка кабельной продукции должна осуществляться в соответствии с требованиями по монтажу СКС стандарта ANSI/EIA/TIA-568. 4.4.11. Все активное оборудование центра коммутации должно располагаться в коммуникационном шкафу, где расшиваются патч-панели. Для кроссирования компьютерных, телефонных линий в коммуникационных шкафах требуются соединительные шнуры с коннекторами типа RJ45. 4.4.12. Межэтажные телекоммуникационные шкафы должны быть высотой не менее 42U, габаритными размерами не менее 800х1000 мм. Количество шкафов не менее 7 шт. 4.4.13. Центральные телекоммуникационные шкафы должны быть напольного исполнения, высотой не менее 42U, габаритными размерами не менее 800х1000 мм. Общее количество шкафов не менее 2. 4.4.14. Кабельная подсистема должна обеспечивать возможность развития и модернизации, быть готовой к внесению изменений с минимальными затратами времени. 4.4.15. Поставщик должен выполнить тестирование всех вновь проложенных линий с использованием измерительного оборудования. 4.4.16. Прокладка кабелей должна выполняться с соблюдением требований пожарной безопасности здания, в том числе по высоте прокладки, пересечению с силовыми кабелями, использованию кабельных лотков и коробов, допустимым расстояниям до источников тепла и электромагнитных помех. 4.4.17. Кабельные линии должны быть проложены с соблюдением минимально допустимых расстояний от силовых кабелей и линий освещения, а при совместной прокладке — в отдельных каналах или перегороженных секциях, предотвращающих наводки и взаимные помехи. 4.5. Общие требования к монтажу электрической подсистемы 4.5.1. Телекоммуникационные шкафы (ТК) должны быть подключены к электрической сети здания отдельными кабельными линиями. 4.5.2. Для подключения электропитания телекоммуникационных шкафов необходимо использовать кабель, сечение которого соответствует номинальной нагрузке установленного активного оборудования. 4.5.3. В каждый ТК необходимо установить источник бесперебойного питания (ИБП): 4.5.4. Для центральных шкафов использовать ИБП с общей максимальной выходной мощностью не менее 5000 ВА; 4.5.5. Для межэтажных шкафов использовать ИБП стоечного исполнения с общей максимальной выходной мощностью не менее 3000 ВА. 4.5.6. Все телекоммуникационные шкафы должны быть подключены через устройство распределения питания и оснащены приборным корпусом стоечного исполнения с установленными электрическими розетками, и автоматическими выключателями необходимого номинала. 4.6. Требования по организации и оснащению кроссовых помещений 4.6.1. В

	здании необходимо выполнить комплекс задач по организации и оснащению кроссовых помещений. 4.6.2. Кроссовые помещения необходимо минимально разместить следующим образом: в левом крыле здания — 4 помещения, расположенных на 2, 3, 4 и 5 этажах; в правом крыле здания — 3 помещения, расположенных на 2, 3 и 4 этажах. Места расположения согласовать на месте. 4.6.3. Организация помещений 4.6.3.1. Для каждого кроссового помещения соответствующего крыла Заказчик выделяет площадь для организации отдельного технического помещения площадью не менее 6 кв.м. 4.6.3.2. Цвет, внешний вид и конструктивное исполнение перегородки предварительно согласовать с Заказчиком с учетом существующего дизайна здания. Установить входную дверь шириной не менее 0,8 м. 4.6.3.3. В каждом помещении выполнить косметический ремонт стен и поверхностей, подвесной потолок типа Armstrong, укладку антистатического линолеума; зашивку существующего оконного проема гипсокартоном с последующей чистовой отделкой; демонтаж радиатора (при наличии) отопления с сохранением существующих транзитных трубопроводов. 4.6.3.4. Фактические размеры помещений и объем отделочных работ уточнить по месту до начала производства работ. 4.6.3.5. Объемы и размеры коммутационного помещения по ширине коридора ориентировочным размером 3 × 2 м, высотой 2,9 м. Площадь помещения – 6 м². Размер существующего окна – 2 × 2 м. 4.6.3.6. Устройство перегородки с установкой двери. Выполнить перегородку длиной 2 м и высотой 2,9 м в одном из двух вариантов: из алюминиевого профиля с глухим заполнением сэндвич-панелями либо из гипсокартона по металлическому каркасу общей толщиной до 100 мм с заполнением внутреннего пространства звукоизоляционным материалом и чистовой отделкой с обеих сторон. В перегородке установить 1 металлический дверной блок размером 0,8 × 2 м, правого открывания, в комплекте с коробкой и фурнитурой, с возможностью установки оборудования СКУД. Площадь перегородки за вычетом дверного проёма – 4,2 м². При гипсокартонном исполнении площадь отделки с двух сторон – 8,4 м², без учёта откосов. 4.6.3.7. Подготовка существующих стен. Выполнить очистку, локальный ремонт дефектов, шпатлевание и грунтование трёх существующих стен внутри выделяемого помещения. Площадь подготовки за вычетом окна – 19,2 м². 4.6.3.8. Окраска стен. Выполнить окраску подготовленных существующих стен площадью 19,2 м². 4.6.3.9. Демонтаж потолка. Демонтировать существующий подвесной потолок Armstrong в пределах выделяемого помещения площадью 6 м². 4.6.3.10. Устройство потолка. Выполнить монтаж подвесного потолка Armstrong площадью 6 м² в границах выделяемого помещения. Предусмотреть примыкание потолка к вновь установленной перегородке. 4.6.3.11. Зашивка окна. Выполнить зашивку существующего оконного проёма размером 2 × 2 м гипсокартоном по металлическому каркасу с заделкой стыков, шпатлеванием, грунтованием и окраской. Площадь зашивки – 4 м². Демонтаж оконного блока не предусматривается. 4.6.3.12. Подготовка пола. Существующее покрытие из кафеля

	сохранить. Выполнить проверку прочности основания, подготовку поверхности и необходимое выравнивание под укладку антистатического линолеума. Площадь – 6 м². 4.6.3.13. Укладка напольного покрытия. Выполнить укладку антистатического линолеума площадью 6 м². 4.6.3.14. Установка плинтуса. Установить плинтус из негорючего материала по периметру помещения за вычетом дверного проёма. Общая длина – 9,2 пог. м. 4.6.4. Кондиционирование 4.6.4.1. Каждое из кроссовых помещений оборудовать отдельной системой кондиционирования производительностью не менее 18 000 BTU/ч (класс 18). 4.6.4.2. Кондиционер должен обеспечивать поддержание требуемого температурного режима кроссового помещения независимо от режима эксплуатации остальных помещений здания. 4.6.4.3. Кондиционер оснастить зимним комплектом для эксплуатации при отрицательной температуре наружного воздуха. Наружный блок оборудовать защитным козырьком и защитным кожухом (по согласованию с Заказчиком). 4.6.5. Электроснабжение 4.6.5.1. К каждому кроссовому помещению выполнить отдельную линию электроснабжения от точки подключения, согласованной с Заказчиком. Сечение кабеля определить в соответствии с ПУЭ. 4.6.5.2. В каждом кроссовом помещении установить отдельный распределительный щит, достаточный по количеству модулей для подключения всех потребителей помещения и имеющий резерв для дальнейшего расширения. 4.6.5.3. Предусмотреть отдельные линии и соответствующую защитную аппаратуру для телекоммуникационного оборудования, ИБП, кондиционера, освещения, оборудования СКУД, видеонаблюдения, пожарной и охранной сигнализации, мониторинга и других потребителей кроссового помещения. 4.6.6. Телекоммуникационные шкафы 4.6.6.1. В каждом кроссовом помещении установить напольный телекоммуникационный шкаф высотой не менее 42U и шириной не менее 800 мм. 4.6.6.2. В ТК шкафах предусмотреть размещение оптического и медного кроссового оборудования, коммутаторов, патч-панелей, кабельных организаторов, ИБП и другого необходимого оборудования. 4.6.6.3. Размещение шкафов выполнить с обеспечением свободного доступа для монтажа, коммутации и последующего технического обслуживания оборудования. 4.6.7. Заземление 4.6.7.1. Выполнить устройство контуров заземления кроссовых помещений по левому и правому крылу здания. 4.6.7.2. К контуру левого крыла подключить кроссовые помещения 2, 3, 4 и 5 этажей левого крыла. К контуру правого крыла подключить кроссовые помещения 2, 3 и 4 этажей правого крыла. 4.6.7.3. Контуры объединить между собой и подключить к существующей системе заземления здания. 4.6.7.4. Выполнить прокладку необходимых магистральных и ответвительных защитных проводников. К системе заземления подключить телекоммуникационные шкафы, распределительные щиты, металлические конструкции, корпуса оборудования и другие элементы, подлежащие защитному заземлению. 4.6.7.5. Перед выполнением подключения провести проверку состояния и параметров существующей системы заземления здания. 4.6.7.6. После завершения работ выполнить необходимые

	электротехнические измерения с предоставлением Заказчику соответствующих протоколов измерений. 4.6.8. Система контроля и управления доступом 4.6.8.1. Каждое кроссовое помещение оборудовать системой контроля и управления доступом (СКУД). 4.6.8.2. Предусмотреть контроль доступа в помещение, установку электромагнитного замка, считывателя, кнопки выхода, кнопки аварийной разблокировки двери, доводчика и контроля состояния двери. 4.6.8.3. Выполнить прокладку кабельных линий, монтаж, подключение и пусконаладочные работы. 4.6.9. Система видеонаблюдения 4.6.9.1. Каждое кроссовое помещение оборудовать системой видеонаблюдения, обеспечивающей контроль входа. 4.6.9.2. Выполнить монтаж камер, прокладку кабельных линий, подключение и настройку. 4.6.10. Мониторинг кроссовых помещений 4.6.10.1. В каждом кроссовом помещении организовать систему мониторинга инженерного состояния помещения. 4.6.10.2. Необходимо предусмотреть контроль температуры; влажности; протечки воды; открытия/закрытия входной двери. Обеспечить передачу аварийных и предупредительных событий в систему учета и контроля событий. 4.6.11. Кабельная и сетевая инфраструктура 4.6.11.1. Выполнить прокладку всех необходимых оптических, медных, силовых и слаботочных кабельных линий для полноценного функционирования кроссовых помещений. 4.6.11.2. Предусмотреть кабельные лотки, короба, крепежные конструкции, кабельные проходки и другие необходимые элементы кабельной инфраструктуры (где применимо). 4.6.11.3. Все кабельные линии оконцевать и промаркировать с двух сторон. Выполнить коммутацию оборудования. 4.6.11.4. После завершения монтажа выполнить проверку и тестирование медных и оптических линий. 4.7. Требования к работам по централизованной маршрутизации, балансировке и оптимизации каналов связи 4.7.1. Поставщик обязан организовать централизацию и агрегацию входящего и исходящего трафика операторов связи Заказчика с внедрением механизмов динамического распределения нагрузки и приоритезации критически важного служебного трафика (QoS) для исключения простоев сетевой инфраструктуры. Настройка телекоммуникационного оборудования и схемы маршрутизации должна быть выполнена в соответствии с пунктами 123, 124, 128 и 139 Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности. Вся коммутация и маршрутизация должны осуществляться через пограничный шлюз и межсетевые экраны с сокрытием внутренней адресации (NAT), фильтрацией пакетов на каждом интерфейсе, ведением защищенных журналов событий с синхронизацией времени. 4.8. Требования к защите пользовательских портов от несанкционированного доступа 4.8.1. Поставщик обязан реализовать комплекс организационно-технических мер по защите физических и логических пользовательских портов активного сетевого оборудования. 4.8.2. Поставщик обеспечивает физическое и программное отключение либо блокировку всех свободных, неиспользуемых портов структурированной кабельной системы и интерфейсов активного сетевого оборудования.

	Для активных пользовательских сетевых портов должна быть выполнена настройка политик разграничения доступа и контроля подключений (включая привязку MAC-адресов, механизмы аутентификации устройств по стандарту IEEE 802.1X), исключающая несанкционированное подключение сторонних устройств, маршрутизаторов, неуправляемых коммутаторов и беспроводных точек доступа. 4.9. Требования к техническому оснащению. 4.9.1. Поставщик должен выполнить комплекс задач по физической установке, базовой настройке и интеграции в локально-вычислительную сеть Заказчика оборудования (предоставляется Поставщиком) с характеристиками не ниже следующих. Сервер Тип 1 Серверный корпус −Форм-фактор: Rackmount, 2U −Поддержка процессоров: не менее 1 −Совместимость: Пассивные радиаторы, фронтальное охлаждение −Отсеки накопителей: до 12× 3.5" hot-swap (SAS3/SATA). −Блок питания: Резервируемый, 2x1000 Вт, 1U, hot-swap Материнская плата −Поддержка SATA: до 12× SATA3 (6 Гбит/с) −Поддержка RAID: уровни 0, 1, 5, 10 −Порт управления: 1Gbps Base-T Ethernet −ОЗУ: Поддержка DDR4 ECC Registered, 16 слотов Процессоры −Архитектура: x86_64, не хуже 10 нм −Частота: от 2.4 ГГц −Кэш: от 24 МБ L3 −Ядра/потоки: не менее 8 ядер / 16 потоков Оперативная память −Тип: DDR4 ECC Registered (RDIMM) −Частота: 3200 МГц −Объем: не менее 128ГБ Система хранения −SSD (Enterprise-класс, SATA 6 Гбит/с): 2× по 480 ГБ, 2× по 1.92 ТБ −HDD (SATA 6 Гбит/с): не менее 2× по 10 ТБ, 7200 об/мин, кеш ≥256 МБ −Салазки для установки накопителей должны быть для всех накопителей с возможностью установки 2.5” и 3,5” накопителей без дополнительных адаптеров. RAID-контроллер − Поддержка: SATA/SAS 12 Гбит/с − Порты: 8 внутренних − Интерфейс: PCIe 3.0 − Кэш: 2 ГБ DDR3 − Поддержка уровней RAID: 0, 1, 5, 6, 10, 50, 60 Сетевой адаптер − Порты: не менее 2x1Gbps Base-T Ethernet − Интерфейс: PCIe 2.0/3.0/4.0 OCP Общее количество не менее 2 шт. Сервер Тип 2 1. Серверный корпус − Форм-фактор: Rackmount, 2U −Поддержка процессоров: не менее 2 −Совместимость: Пассивные радиаторы, фронтальное охлаждение −Отсеки накопителей: до 12× 3.5" hot-swap (SAS3/SATA) −Блок питания: Резервируемый, 2x1000 Вт, 1U, hot-swap 2. Материнская плата −Поддержка SATA: до 12× SATA3 (6 Гбит/с) −Поддержка RAID: уровни 0, 1, 5, 10 −Порт управления: 1Gbps Base-T Ethernet −ОЗУ: Поддержка DDR4 ECC Registered, 32 слота 3. Процессоры −Архитектура: x86_64 −Частота: от 2.4 ГГц −Кэш: от 24 МБ L3 −Ядра/потоки: не менее 12 ядер / 24 потока 4. Оперативная память −Тип: DDR4 ECC Registered (RDIMM) −Частота: 3200 МГц −Объем: не менее 256ГБ 5. Система хранения −SSD (Enterprise-класс, SATA 6 Гбит/с): 2× по 480 ГБ, 4× по 3.84 ТБ −HDD (SATA 6 Гбит/с):не менее 4× по 10 ТБ, 7200 об/мин, кеш ≥256 МБ −Салазки для установки накопителей должны быть для всех накопителей с возможностью установки 2.5” и 3,5” накопителей без дополнительных адаптеров. 6. RAID-контроллер −Поддержка: SATA/SAS 12 Гбит/с −Порты: 8 внутренних −Интерфейс: PCIe 3.0 −Кэш: 2 ГБ DDR3 + батарея −Поддержка уровней

	RAID: 0, 1, 5, 6, 10, 50, 60 7. Сетевой адаптер −Порты: не менее 2x1Gbps Base-T Ethernet −Интерфейс: PCIe 2.0/3.0/4.0 OCP Общее количество не менее 2 шт. Коммутатор тип 1 Коммутатор должен иметь не менее 48 портов Ethernet 10/100/1000Base-T и не менее 6 портов SFP+ со скоростью 100/1000/10G. Должна поддерживаться работа SFP+ портов в режиме 100 Мбит/с. Наличие выделенного порта управления 10/100/1000Base-T RJ-45 обязательно. Пропускная способность коммутатора должна составлять не менее 190 Гбит/с, скорость пересылки пакетов — не менее 150 млн пакетов в секунду. Объем оперативной памяти должен быть не менее 256 МБ, объем Flash-памяти — не менее 32 МБ. Диапазон рабочих температур должен составлять от 0 до +50 °C. Размер таблицы MAC-адресов должен составлять не менее 24 000 записей. Количество одновременно поддерживаемых VLAN должно быть не менее 4094, количество Multicast-групп — не менее 4096. Коммутатор должен поддерживать не менее 12 000 маршрутов IPv4 и не менее 8 000 записей ARP. Должна поддерживаться функция ограничения количества одновременно подписанных Multicast-групп на абонентском порту, функционал MVR, фильтрация Drop Query и Drop Report на портах, динамическая и статическая настройка Multicast Router Port, а также прозрачная передача служебного Multicast-трафика независимо от функций IGMP Snooping и MVR. Количество правил ACL должно составлять не менее 3000. Поддержка Jumbo Frames размером не менее 12 000 байт обязательна. Коммутатор должен поддерживать Selective Q-in-Q (IEEE 802.1ad), протоколы Spanning Tree согласно стандартам IEEE 802.1d, IEEE 802.1s и IEEE 802.1w, а также функции Root Guard, BPDU Guard и BPDU Forwarding. Обязательно наличие статической маршрутизации, строгой приоритетной очереди SPQ, политик управления очередями WRR, WRR+SPQ и PQ+WRR. На каждом порту должно поддерживаться не менее четырех очередей передачи трафика, одна из которых должна иметь уровень обслуживания Strict Priority. Коммутатор должен обеспечивать принудительную маркировку и перемаркировку трафика с ограничением потока приоритетного трафика, поддерживать изменение поля DSCP, классификацию трафика по IEEE 802.1p и DSCP CoS. Для административного доступа должна поддерживаться аутентификация через TACACS+ и RADIUS. Управление коммутатором должно осуществляться через консольный порт RS-232 (RJ-45), а также посредством протоколов Telnet, SSH, SNMP и HTTPS. Коммутатор должен поддерживать питание от сети переменного тока 220 В, стандарт IEEE 802.3x Flow Control, активную систему охлаждения, функционал VLAN Translation и протокол IPv6. Обязательно наличие поддержки DHCP Option 37 и Option 38. Не должно быть ограничений на использование SFP/SFP+ модулей сторонних производителей. Коммутатор должен обеспечивать автоматическое резервное копирование конфигурации на удаленный сервер, поддерживать Dynamic ARP Inspection (DAI), изоляцию портов (Port Isolation), механизмы защиты центрального процессора (CPU Protection), логирование на оперативную память,

	Flash-память и удаленный сервер. Должны поддерживаться функции MAC Authentication Bypass (MAB), Dying Gasp, ULDP, захват трафика с процессора коммутатора (Packet Capture), зеркалирование портов и RSPAN, встроенные средства диагностики и отладки, Voice VLAN и MAC VLAN. Необходимо наличие возможности настройки списков контроля доступа для ограничения доступа к управлению и мониторингу устройства, поддержки Port Security, PPPoE Relay/PPPoE+, DNS Client (RFC 1591), а также настройки приоритета IEEE 802.1p для управляющего VLAN. Коммутатор должен быть оснащен не менее чем двумя встроенными блоками питания. Общее количество не менее 19 шт. Коммутатор тип 2 с Коммутатор должен иметь не менее 48 портов Ethernet 10GBASE-R (SFP+)/1000BASE-X (SFP) и не менее 6 портов 40G QSFP+. Наличие выделенного порта управления 10/100/1000BASE-T RJ-45 и USB-порта для подключения внешних накопителей обязательно. Производительность коммутации должна составлять не менее 960 Гбит/с, скорость пересылки пакетов — не менее 960 Mpps. Объем оперативной памяти должен быть не менее 2048 МБ, объем Flash-памяти — не менее 4096 МБ. Диапазон рабочих температур должен составлять от 0 до +50 °C. Размер таблицы MAC-адресов должен составлять не менее 162 000 записей. Количество одновременно поддерживаемых VLAN должно быть не менее 4000, количество Multicast-групп — не менее 4000. Количество правил ACL должно составлять не менее 2048 входящих и 1024 исходящих записей. Поддержка Jumbo Frame размером не менее 12 000 байт обязательна. Коммутатор должен поддерживать стекирование. Минимальное количество устройств в стеке должно составлять не менее двух. Необходимо наличие поддержки Selective Q-in-Q (IEEE 802.1ad), протоколов Spanning Tree IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, а также функций Root Guard, BPDU Guard и BPDU Tunnel. Должна поддерживаться работа протоколов защиты кольцевых топологий ERPS ITU-T G.8032, MRPP, ULPP и ULSM. Также обязательна поддержка механизмов Dynamic ARP Inspection, ARP Guard, ARP Binding и Anti-ARP-Scan. Количество ARP-записей должно составлять не менее 192 000 в стандартном режиме UFT. Коммутатор должен поддерживать технологию VRF. Количество VFI должно быть не менее 256, количество VRF — не менее 64. Число равноценных маршрутов ECMP должно составлять не менее 32. Обязательна поддержка протоколов статической и динамической маршрутизации RIPv2, OSPFv2, OSPFv3, BGPv4+, PIM-SM и PIM-DM. Количество PIM-маршрутов IPv4 и IPv6 должно составлять не менее 4094 для каждого протокола. Размер таблицы маршрутизации должен составлять не менее 8 000 маршрутов в стандартном режиме UFT и до 128 000 маршрутов в режиме маршрутизации. Для административного доступа должна поддерживаться аутентификация по протоколам TACACS+ и RADIUS. Управление устройством должно осуществляться через консольный порт RS-232 (RJ-45), а также посредством протоколов Telnet, SSH и SNMP. Поддержка Syslog обязательна. Коммутатор должен поддерживать установку двух блоков питания с возможностью горячей

	замены. Размер пакетного буфера должен составлять не менее 6 МБ. Обязательна поддержка протокола агрегации каналов LACP с количеством групп не менее 64 и возможностью объединения не менее 4 портов в одной группе. Должна поддерживаться работа DHCP Server, DHCP Client и DHCP Relay, а также аутентификация по протоколам IEEE 802.1X и MAB. Необходимо наличие функции автоматического резервного копирования конфигурации на удаленный сервер, поддержки шифрования паролей алгоритмами MD5 и SHA-256, а также функции сравнения конфигурационных файлов через CLI. Коммутатор должен обеспечивать возможность указания Source IP Address и Source MAC Address в IGMP-пакетах при использовании IGMP Snooping во VLAN. Обязательна поддержка записи пакетов из CPU на Flash-память устройства, функционала NQA (Network Quality Analysis), а также протоколов VLAN: Port-based VLAN, IEEE 802.1Q, Private VLAN, Protocol VLAN, Voice VLAN, MAC VLAN, N:1 VLAN Translation и Port-Based QinQ. Должна поддерживаться зеркализация трафика SPAN, RSPAN и ERSPAN. Для обеспечения качества обслуживания необходимо наличие не менее 8 очередей на порт с поддержкой механизмов QoS: Strict Priority, WRR, SP+WRR, DWRR и SP+DWRR. Общее количество не менее 4 шт. Коммутатор тип 3 Коммутатор должен иметь не менее 16 портов Ethernet 100/1000Base-X SFP, не менее 8 комбинированных портов Ethernet 10/100/1000Base-T или 100/1000Base-X SFP, а также не менее 4 портов 10GBASE-R (SFP+)/1000BASE-X (SFP). Для организации стека должны быть предусмотрены не менее 2 выделенных портов 20G QSFP+. Наличие выделенного порта управления 10/100/1000BASE-T RJ45 и USB-порта для подключения внешних накопителей обязательно. Производительность коммутации должна составлять не менее 208 Гбит/с, скорость пересылки пакетов — не менее 155 Mpps. Объем оперативной памяти должен быть не менее 1024 МБ. Объем Flash-памяти должен составлять не менее 32 МБ, а объем NAND Flash-памяти — не менее 1024 МБ. Размер таблицы MAC-адресов должен составлять не менее 64 000 записей. Количество одновременно поддерживаемых VLAN должно быть не менее 4094. Коммутатор должен поддерживать Port-based VLAN, IEEE 802.1Q, Private VLAN, Protocol VLAN, Voice VLAN, MAC VLAN, Selective QinQ, Port-Based QinQ и N:1 VLAN Translation. Количество Multicast-групп должно составлять не менее 1000. Количество правил ACL должно быть не менее 3328 входящих и 1024 исходящих. Размер таблицы маршрутизации IPv4/IPv6 должен составлять не менее 16382/6143 записей. Поддержка Jumbo Frame размером не менее 16 000 байт обязательна. Коммутатор должен поддерживать стекирование с возможностью объединения не менее 4 устройств в стек. Общая пропускная способность стекового соединения должна составлять не менее 40 Гбит/с. Должна поддерживаться технология Selective Q-in-Q (IEEE 802.1ad), протоколы Spanning Tree IEEE 802.1d, IEEE 802.1s и IEEE 802.1w, а также функции Root Guard, BPDU Guard и BPDU Tunnel. Обязательна поддержка протоколов защиты кольцевых топологий ERPS ITU-T G.8032, MRPP, ULPP и

	ULSM. Коммутатор должен поддерживать механизмы Dynamic ARP Inspection, ARP Guard, ARP Binding и Anti-ARP-Scan. Количество ARP-записей IPv4/IPv6 должно составлять не менее 16400/16381. Число равноценных маршрутов ECMP должно быть не менее 32. Обязательна поддержка протоколов статической и динамической маршрутизации RIPv2, OSPFv2, OSPFv3, BGPv4+, PIM-SM и PIM-DM. Должна поддерживаться технология резервирования VRRP с количеством групп не менее 192. Коммутатор должен поддерживать MPLS, включая L2VPN и L3VPN, с количеством MPLS-меток не менее 8096. Для административного доступа должна поддерживаться аутентификация по протоколам TACACS+ и RADIUS. Управление устройством должно осуществляться через консольный порт RS-232 (RJ-45), а также посредством протоколов Telnet, SSH и SNMP. Коммутатор должен поддерживать установку двух блоков питания с возможностью горячей замены, а также возможность использования блоков питания с входным напряжением 36–72 В постоянного тока. Обязательна поддержка протоколов OAM, Dying GASP, VCT и DDM. Коммутатор должен поддерживать протокол агрегации каналов LACP. Количество групп агрегации должно составлять не менее 128, с возможностью объединения не менее 4 портов в одной группе. Необходимо наличие функции сравнения файлов конфигурации через CLI. Размер пакетного буфера должен составлять не менее 4 МБ. Коммутатор должен поддерживать VRF с количеством VFI не менее 256 и количеством VRF не менее 251. Также должна поддерживаться фильтрация LDP-меток. Обязательна возможность указания Source IP Address и Source MAC Address в IGMP-пакетах при использовании IGMP Snooping во VLAN, шифрование паролей алгоритмами MD5 и SHA-256, просмотр количества MAC-адресов в VFI, запись пакетов из CPU на Flash-память устройства и функционал NQA (Network Quality Analysis). Должна поддерживаться зеркализация трафика SPAN, RSPAN и ERSPAN. Для обеспечения качества обслуживания необходимо наличие не менее 8 очередей на порт с поддержкой механизмов QoS: Strict Priority, WRR, Strict+WRR, DWRR, SDWRR и WRED. Общее количество не менее 4 шт. Коммутатор тип 4 Коммутатор должен иметь не менее 48 портов Ethernet 10/100/1000Base-T и не менее 6 портов SFP+ со скоростью 100/1000/10G. Должна поддерживаться работа SFP+ портов в режиме 100 Мбит/с. Все 48 медных портов должны поддерживать технологии PoE IEEE 802.3af и IEEE 802.3at. Общий бюджет PoE должен составлять не менее 760 Вт. Наличие выделенного порта управления 10/100/1000Base-T RJ-45 обязательно. Пропускная способность коммутатора должна составлять не менее 192 Гбит/с, скорость пересылки пакетов — не менее 120 млн пакетов в секунду. Объем оперативной памяти должен быть не менее 256 МБ, объем Flash-памяти — не менее 32 МБ. Диапазон рабочих температур должен составлять от 0 до +50 °C. Размер таблицы MAC-адресов должен составлять не менее 28 000 записей. Количество одновременно поддерживаемых VLAN должно быть не менее 4094, количество Multicast-групп — не менее 4096. Коммутатор должен поддерживать не

	менее 12 000 маршрутов IPv4 и не менее 8 000 записей ARP. Питание должно осуществляться от сети переменного тока 220 В. Коммутатор должен комплектоваться двумя блоками питания. Должна поддерживаться функция ограничения количества одновременно подписанных Multicast-групп на абонентском порту, функционал MVR, фильтрация Drop Query и Drop Report на портах, динамическая и статическая настройка Multicast Router Port, а также прозрачная передача служебного Multicast-трафика независимо от функций IGMP Snooping и MVR. Количество правил ACL должно составлять не менее 3840. Поддержка Jumbo Frames размером не менее 12 000 байт обязательна. Коммутатор должен поддерживать Selective Q-in-Q (IEEE 802.1ad), протоколы Spanning Tree IEEE 802.1d, IEEE 802.1s и IEEE 802.1w, а также функции Root Guard, BPDU Guard и BPDU Forwarding. Обязательно наличие статической маршрутизации, строгой приоритетной очереди SPQ, политик управления очередями WRR, WRR+SPQ и PQ+WRR. На каждом порту должно поддерживаться не менее четырех очередей передачи трафика, одна из которых должна иметь уровень обслуживания Strict Priority. Коммутатор должен обеспечивать принудительную маркировку и перемаркировку трафика, изменение поля DSCP, а также классификацию трафика по IEEE 802.1p и DSCP CoS. Для административного доступа должна поддерживаться аутентификация через TACACS+ и RADIUS. Управление коммутатором должно осуществляться через консольный порт RS-232 (RJ-45), а также посредством протоколов Telnet, SSH, SNMP и HTTPS. Коммутатор должен поддерживать IEEE 802.3x Flow Control, активную систему охлаждения, VLAN Translation и IPv6. Обязательна поддержка DHCP Option 37 и Option 38. Не должно быть ограничений на использование SFP/SFP+ модулей сторонних производителей. Коммутатор должен поддерживать MAC Authentication Bypass (MAB), ULDP, захват трафика с процессора устройства (Packet Capture), зеркалирование трафика RSPAN, встроенные средства диагностики, Voice VLAN и MAC VLAN. Также должна поддерживаться настройка списков контроля доступа для управления и мониторинга устройства, функции Port Security и PPPoE Relay/PPPoE+. Общее количество не менее 17 шт. Маршрутизатор Форм-фактор: Стоечное исполнение (Rackmount), наличие монтажных «ушей» для установки в стандартную 19-дюймовую телекоммуникационную стойку или шкаф. Аппаратная платформа: Процессор (архитектура 64-бит) с количеством ядер не менее 4 (четырех) и тактовой частотой каждого ядра не менее 1.7 ГГц. Объем оперативной памяти (RAM) — не менее 4 ГБ. Объем встроенной энергонезависимой памяти (NAND/Flash) — не менее 128 МБ. Медные сетевые интерфейсы: Не менее 16 (шестнадцати) портов Ethernet 10/100/1000Base-T (Gigabit Ethernet) с разъемами RJ-45 для маршрутизации локального трафика. Оптические сетевые интерфейсы: Не менее 2 (двух) портов SFP+ с поддержкой скорости передачи данных до 10 Гбит/с (а также с обратной совместимостью с модулями 1.25 Гбит/с SFP) для организации высокоскоростных магистральных (Uplink) каналов. Интерфейсы

	управления и расширения: Наличие 1 (одного) консольного порта (RJ-45) для локального физического конфигурирования. Наличие полноразмерного порта USB (версии не ниже 3.0 Type-A) для подключения внешних накопителей, резервных LTE/4G-модемов или иных периферийных устройств. Требования к питанию: Поддержка отказоустойчивости по питанию — наличие не менее 2 (двух) встроенных резервируемых блоков питания с автоматическим переключением (поддержка сетей переменного тока AC 100-240В). Функциональные возможности (Сетевая ОС): Поддержка статической маршрутизации и маршрутизации на основе политик (Policy-Based Routing). Поддержка построения виртуальных частных сетей и туннелей (IPsec, L2TP, PPTP, OpenVPN, WireGuard или их эквивалентов) с поддержкой аппаратного ускорения шифрования. Встроенный межсетевой экран (Firewall) с отслеживанием состояний соединений (Stateful inspection) и поддержкой механизмов трансляции сетевых адресов (NAT/PAT). Гибкая система управления полосой пропускания и качеством обслуживания (QoS / Traffic Shaping). Общее количество не менее 2 шт. Межсетевой экран Сетевые интерфейсы: суммарно не менее 10 портов Gigabit Ethernet (10/100/1000Base-T, RJ45) с возможностью независимого назначения ролей WAN, DMZ, LAN. Интерфейсы управления: не менее 1 консольного порта RJ45 и не менее 1 служебного порта USB. Питание: внешний блок питания от сети переменного тока напряжением 100–240 В, частотой 50/60 Гц. Пропускная способность межсетевого экрана (Firewall Throughput): не менее 8 Гбит/с при передаче пакетов большого размера (1518 байт). Производительность IPS (системы предотвращения вторжений): не менее 1,2 Гбит/с. Производительность межсетевого экрана следующего поколения (NGFW): не менее 900 Мбит/с. Производительность комплексной защиты от угроз (Threat Protection): не менее 650 Мбит/с. Пропускная способность туннелей IPsec VPN: не менее 5 Гбит/с. Количество поддерживаемых туннелей IPsec VPN: не менее 75 типа «шлюз-шлюз» (Gateway-to-Gateway) и не менее 120 типа «клиент-шлюз» (Client-to-Gateway). Сетевой функционал: поддержка статической и динамической маршрутизации, поддержка VLAN (IEEE 802.1Q), механизмов трансляции адресов (NAT/PAT), агрегации каналов, протоколов IPv4 и IPv6. Технологии VPN: поддержка протоколов построения защищенных виртуальных сетей IPsec VPN и SSL VPN; поддержка шифрования по стандартам не ниже AES-256. Контроль и фильтрация трафика: глубокая инспекция пакетов (DPI), контроль приложений на уровне L7, инспекция шифрованного трафика SSL/TLS (включая TLS 1.3), веб- и контентная фильтрация по категориям URL, защита от вредоносного ПО и сетевых атак в реальном времени. Управление и мониторинг: поддержка локального веб-интерфейса (HTTPS), интерфейса командной строки (CLI через SSH/консоль), поддержка протоколов SNMP, Syslog, NTP, возможность подключения к единой централизованной системе управления и анализа журналов событий. Общее количество не менее 2 шт. Точка доступа Wi-Fi Тип исполнения: Внутренняя, с возможностью крепления на

	стену или потолок (монтажный комплект должен поставляться в комплекте). Стандарты беспроводной связи: Поддержка современных стандартов IEEE 802.11a/b/g/n/ac/ax (Wi-Fi 6). Рабочие диапазоны: Одновременная работа в двух частотных диапазонах (Dual-Band) — 2.4 ГГц и 5 ГГц. Антенны: Встроенные всенаправленные антенны. Коэффициент усиления антенн не менее 5.5 dBi для диапазона 5 ГГц и не менее 6 dBi для диапазона 2.4 ГГц. Сетевые интерфейсы: Не менее 2 (двух) портов Ethernet 10/100/1000Base-T (Gigabit Ethernet). Питание (PoE): Поддержка получения питания по технологии Power over Ethernet (PoE-In) стандарта 802.3af/at на первом порту. Наличие функции сквозной передачи питания (PoE-Out) на втором порту для подключения дополнительных устройств. Аппаратная часть: Процессор не менее 4 ядер с тактовой частотой не менее 1.8 ГГц; объем оперативной памяти не менее 1 ГБ; объем встроенной флеш-памяти не менее 128 МБ. Безопасность и шифрование: Поддержка актуальных протоколов безопасности, включая WPA2-PSK, WPA3-PSK, WPA2-Enterprise, WPA3-Enterprise, OWE. Управление: Устройство должно поддерживать работу как в полностью автономном режиме, так и в режиме централизованного управления через программный или аппаратный контроллер беспроводной сети (с поддержкой бесшовного роуминга). Общее количество не менее 50 шт. Система хранения данных Тип исполнения: Внутренняя, с возможностью установки на полку в коммутационный шкаф. Количество процессоров не менее 1, Количество ядер в CPU не менее 4, Количество потоков CPU не менее 8, Архитектура процессора – 64 бит, Частота CPU не менее 2,0GHz Системная память не менее 4Gb, с возможностью расширения до 32Gb Отсеки для дисков должны поддерживать возможность замены в горячем режиме и иметь возможность установки 4 x HDD SATA 3.5” или 4 x 2,5” SATA SSD, должно быть укомплектовано дисками корпоративного стандарта HDD SATA 3,5” объёмом не менее 12Tb в количестве не менее 4х шт. Порты LAN Ethernet RJ-45 должны поддерживать скорость передачи не менее 1Gbit/sec и в наличии их должно быть не менее 2 Входное напряжение переменного тока в диапазоне 100В-240В, адаптер питания в комплекте. Общее количество не менее 2 шт. Источник бесперебойного питания Тип 1 Тип исполнения – стоечный, мощностью 5000ВА класса On-line с двойным преобразованием и основными характеристиками: Вход: Номинальное напряжение - 380/400/415В Диапазон входного напряжения без перехода на батареи при нагрузке 305-480В без снижения мощности Входная частота - 50/60 Гц, автовыбор Диапазон частоты - 40-70 Гц Ток короткого замыкания - 90 А Выход: Номинальное напряжение - 200/208/220/230/240В +/– 1% КПД до 90% в режиме on-line, до 95% в высокоэффективном режиме Общие искажения выходного напряжения < 2% Допустимая перегрузка - 102–110% = 120с, 110–125% = 60с Номинальная выходная частота - 50/60 Гц, автовыбор, конвертор частоты Коммуникации: Порт RS-232 - Есть, Порт USB - Есть (HID) Порты USB и RS232 не могут использоваться одновременно Общее количество не менее 2

	шт. Батарейный модуль Внешний батарейный модуль предназначен для подключения к источникам бесперебойного питания мощностью 6000ВА с целью увеличения времени их автономной работы. Внутри каждого батарейного модуля установлены свинцово-кислотные аккумуляторы напряжением 12В и емкостью до 9 Ач. Общее количество не менее 2 шт. Источник бесперебойного питания Тип 2 Тип исполнения – стоечный, мощностью 3000ВА класса On-line с двойным преобразованием и основными характеристиками: Вход: Номинальное напряжение 200/208/220/230/240В Диапазон входного напряжения без перехода на батареи при нагрузке - 176-276В Диапазон частоты - 40-70 Гц Частота - 50/60 Гц, автовыбор Ток короткого замыкания - 90 А Выход: Номинальное напряжение 200/208/220/230/240В +/– 1% Крест-фактор 3:1 КПД до 90% в режиме on-line, до 95% в высокоэффективном режиме Общие искажения выходного напряжения < 2% Допустимая перегрузка - 102–110% : 120с, 110–125%: 60с Номинальная выходная частота - 50/60 Гц, автовыбор, конвертор частоты Коммуникации: Порт RS-232 - Есть Порт USB - Есть (HID) Общее количество не менее 7 шт. 4.9.2. Поставщик должен выполнить следующие обязательные этапы: 4.9.2.1. Физический монтаж и кабельная обвязка: 4.9.2.1.1. Установка серверов и коммутаторов в телекоммуникационные шкафы Заказчика с использованием штатных креплений и телескопических направляющих. 4.9.2.1.2. Организация правильного распределения воздушных потоков внутри шкафов, исключающая перегрев оборудования. 4.9.2.1.3. Подключение оборудования к источникам бесперебойного питания (ИБП) с резервированием линий питания. 4.9.2.1.4. Эстетичная укладка кабелей (кабель-менеджмент) с использованием кабельных организаторов. 4.9.2.2. Настройка серверного оборудования (Сервер тип 1, Сервер тип 2): 4.9.2.2.1. Обновление firmware материнских плат, сетевых адаптеров и RAID-контроллеров до последних актуальных стабильных версий от производителя при необходимости. 4.9.2.2.2. Настройка защищенных портов удаленного управления серверами (IPMI/BMC/эквивалент) с выделением им соответствующих IP-адресов. 4.9.2.2.3. Инициализация дисковой подсистемы: создание и форматирование RAID-массивов требуемого уровня (RAID 1, 5, 10 и др.) согласно архитектурному плану Заказчика для обеспечения отказоустойчивости операционных систем и хранения баз данных при необходимости. 4.9.2.2.4. Проведение базового нагрузочного тестирования процессорной и дисковой подсистем сервера перед передачей под установку прикладного программного обеспечения. 4.9.2.3. Настройка сетевого оборудования (Коммутаторы тип 1, 2, 3, 4, маршрутизатор): 4.9.2.3.1. Обновление операционных систем (прошивок) коммутаторов до актуальных стабильных версий. 4.9.2.3.2. Базовая сетевая настройка: конфигурирование интерфейсов управления (Management VLAN), настройка протоколов безопасного удаленного доступа (SSH, HTTPS) и отключение неиспользуемых служб и портов. 4.9.2.3.3. Архитектурная настройка локальной сети: создание виртуальных локальных сетей (VLAN), настройка статической

	и/или динамической маршрутизации, агрегации каналов (LACP) и политик качества обслуживания (QoS) по заявке Заказчика. 4.9.2.3.4. Для коммутаторов доступа (в том числе Тип 4): настройка политик распределения питания Power over Ethernet (PoE/PoE+) для подключаемых оконечных устройств при необходимости. 4.9.2.4. Установка и настройка внутренних точек доступа. 4.9.2.4.1. Подключение точек доступа к локальной вычислительной сети с использованием кабеля типа «витая пара» и обеспечением питания по технологии Power over Ethernet (PoE) от коммутаторов доступа. 4.9.2.4.2. Обновление микропрограммного обеспечения (прошивок) точек доступа до последней стабильной версии, рекомендованной производителем оборудования. 4.9.2.4.3. Настройка статической или динамической IP-адресации, синхронизации времени (NTP) и параметров удаленного защищенного управления. 4.9.2.4.4. Настройка радиоинтерфейсов (2.4 ГГц и 5 ГГц): выбор оптимальных непересекающихся частотных каналов и регулировка мощности передатчиков (Tx Power) для обеспечения равномерного покрытия и исключения взаимных радиопомех между соседними точками. 4.9.2.4.5. Создание необходимых беспроводных сетей (SSID) с разделением трафика по виртуальным локальным сетям (VLAN) по заявке Заказчика. 4.9.2.4.6. Настройка современных политик безопасности и шифрования, при необходимости. 4.9.2.4.7. Настройка параметров для обеспечения непрерывного переключения клиентских устройств между точками доступа при перемещении по зданию без обрыва сессий связи при необходимости. 4.9.2.5. Подключение всего настроенного оборудования к существующей сети Заказчика и проверка сквозной сетевой связности. 5. Требования к программному обеспечению. 5.1. Программное обеспечение должно быть предоставлено сроком на 9 месяцев, с 1 апреля 2027 по 31 декабря 2027 года. 5.2. Поставщик должен выполнить комплекс задач по развёртыванию и пусконаладке программного обеспечения предотвращения утечек информации с характеристиками, не ниже следующих: Лицензия на право использования программного обеспечения к Системе предотвращения утечек информации должна быть передана на условиях простой неисключительной лицензии с правом использования способом воспроизведения сроком на 9 месяцев в пределах территории Республики Казахстан, в сетевой инфраструктуре Заказчика на условиях, установленных данной Технической спецификацией. Техническая поддержка. Период технической поддержки должен быть предоставлен на 9 месяцев с момента активации лицензии. 1. Гарантия, срок поддержки и лицензий. Потенциальный Поставщик предоставляет гарантийную поддержку. Поставщик в рамках технической поддержки должен: •обновлять версии программного продукта; •загружать патчи и хотфиксы; •обеспечить дистанционную поддержку в режиме 24/7. 5. Перечень требуемых мероприятий: •развертывание и настройка локального сервера централизованного управления. •активация лицензий и сервисных контрактов. •интеграция сервера централизованного управления с Windows Active Directory. •создание временных

	политик безопасности, для исключения ложных срабатываний и составления списков исключений. 6. Дополнительные требования. Поставка должна быть осуществлена единовременно и в полном объеме в адрес Заказчика, включая запуск и интеграцию в инфраструктуру Заказчика. 7. Требования к программному обеспечению предотвращения утечек информации (не менее, не хуже): •количество лицензий – не менее 280 лицензий на предотвращения утечек информации (DLP) с возможностью расширения; •поставляемое потенциальным поставщиком программное обеспечение должно являться разработкой отечественного производителя. 8. Требования к назначению системы. Система должна обеспечивать решение следующих задач: •мониторинг событий случайной или преднамеренной пересылки пользователями за пределы периметра вычислительных сетей Заказчика конфиденциальной информации по следующим каналам: •электронная почта (протоколы POP3, SMTP, IMAP, MAPI, HTTP, в т.ч. шифрованные аналоги); •электронная почта, переданная через почтовые веб-службы (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex, Zimbra и т.д.); •двунаправленный перехват сообщений в чатах, комментариев к публикациям и на форумах социальных сетей: Facebook, Odnoklassniki, Vk, Twitter, Instagram, LinkedIn, Bitrix24; •средства мгновенного обмена сообщениями – Telegram, Skype, SIP, Viber, Microsoft Lync, Mail.Ru Агент, WhatsApp, PSI, Yahoo! Messenger, MS Teams, Discord, Slack, WeChat, XMPP, Zoom, RocketChat, Signal, eXpress, VK Teams, TrueConf и др., в т.ч. использующие шифрование; •запись файлов на внешние накопители; •запись файлов на локальные сетевые ресурсы; •отправка файлов в облачные сервисы хранения информации (iCloud, Dropbox, Google Drive, OneDrive, Облако Mail.ru, Яндекс.Диск); •отправка файлов на печать на локальные и сетевые принтеры; •передача файлов в компьютерных сетях по протоколам FTP и FTPS; - мониторинг событий разглашения конфиденциальной информации в разговорной речи путем контроля аудиопотока с микрофона контролируемой рабочей станции в режиме реального времени; - поддержка удаленного доступа к просмотру видеоизображения рабочего стола компьютера пользователя в режиме реального времени; - мониторинг в режиме реального времени наличия или появления в файловой системе контролируемой рабочей станции конфиденциальных документов; сбор и хранение всех исходящих и входящих электронных сообщений, с возможностью полнотекстового поиска по архиву, в том числе и в присоединенных к письмам файлах; - контроль использования периферийных устройств (доступ и копирование на внешние накопители, аудит подключения и доступ к внешним устройствам различного назначения); - контроль эффективности использования рабочего времени и ресурсов персоналом компании путем снятия снимков экрана, сбора информации по времени работы/простоя ПК, используемым приложениям (в том числе WinRT (Metro) и виртуальные рабочие столы), а также статистического и событийного анализа перехваченной информации; - запрет запуска отдельных программных

	приложений; - возможность блокирования доступа к определенным веб-ресурсам и их функционалу (на основании заданных политик безопасности); - блокирование сетевого трафика отдельных процессов; - возможность блокирования передачи исходящих сообщений по протоколам SMTP, HTTP и MAPI (в т.ч. с использованием шифрования), содержащих определенную информацию на основе контентного и атрибутивного анализа сообщений и вложенных данных. - Возможность блокирования передачи данных на съемные носители на основе контентного и атрибутивного анализа, с возможностью перехвата заблокированного содержимого (на основании заданных политик безопасности); - Возможность блокирования передачи данных через буфер обмена на основе контентного и атрибутивного анализа (на основании заданных политик безопасности); - Возможность блокирования передачи данных через локальные либо сетевые принтеры (при запуске с агента) на основе контентного и атрибутивного анализа (на основании заданных политик безопасности); - Возможность аудита файловых операций с папками и файлами (чтение, запись, удаление, переименование, изменение прав доступа) с возможностью фильтрации по расширению файла либо процессам. 9. Функции хранения и обработки данных В части хранения и обработки данных система должна обеспечивать: • возможность хранения всех собираемых системой данных в СУБД Microsoft SQL Server, Oracle, PostgreSQL версии 9.3 и выше, MySQL версии 5.7.09 и выше, SQLite (на выбор); • встроенная СУБД SQLite в комплекте поставки; • хранение всех перехватываемых данных вне зависимости от срабатывания политик безопасности; • поддержка работы с базами данных, расположенных на разных серверах; • возможность сохранения файлов на диск сервера, а не в базу, с возможностью исключения из сохранения на диск файлов малого размера, при этом в базу данных помещаются относительные пути к файлам; • возможность включения/отключения распознавания изображений, печатей и речи для отдельных баз данных; • возможность настройки длительности хранения информации в базе данных в группе ротации, • возможность отключения базы данных вручную через Консоль администратора, при этом содержимое базы данных сохраняется; • возможность очистки содержимого базы данных вручную через Консоль администратора; • возможность архивирования баз данных с последующим подключением к системе для осуществления ретроспективного поиска в них критичной информации; • возможность выборочного удаления пользователем перехваченной информации; • возможность объединять одиночные базы данных в группы, поддерживающие кольцевую ротацию баз, при этом поисковые операции выполняются по всем базам данных в группе, а запись данных происходит только в активную; • возможность настройки нескольких условий ротации баз данных: общий объем данных, размер базы данных, размер поисковых индексов, размер файлов на диске, временной интервал, количество записей, при этом запуск процесса ротации может быть настроен на определенный временной промежуток; • возможность настроить

	выполнение скриптов до начала процесса ротации, после завершения ротации, и при ошибке ротации, при этом поддерживаются выполнение cmd, PowerShell, Script Host, Python скриптов; • возможность балансировки нагрузки по двум и более группам баз данных либо базам данных согласно алгоритму "round robin": все поступающие в систему данные записываются в базы данных поочерёдно; • поддержка режима параллельной обработки данных, перехваченных по различным каналам передачи информации, что позволяет повысить производительность системы при выполнении операций обновления, удаления и поиска данных; • возможность настройки правил записи данных в базы данных и группы ротации для регуляции, в какое хранилище записывать информацию в зависимости от часового пояса данных, типа данных, источника данных, вхождения пользователя или компьютера в домен или любой AD-контейнер по его имени, SID или GUID, IP-адреса и другой атрибутной информации; • возможность автоматической репликации поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера в территориально распределённых организационных структурах; • защита от некорректной настройки репликации, когда данные возвращаются на реплицирующий сервер и далее реплицируются повторно; • возможность перенаправления поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера; • возможность настройки расписания для репликации данных; • возможность хранения очереди репликации данных на диске для обеспечения сохранности и целостности реплицируемых данных в случае отказа системы; • при переполнении очереди репликации сервер блокирует прием новых данных; • возможность пропуска репликации при переполнении очереди; • отображение статистики репликации данных; • возможность хранения на диске очереди данных, поступающих от агентов, что повышает их сохранность по сравнению с хранением в оперативной памяти; • возможность выбора режима очистки и обновления поисковых индексов (ручной и автоматический режимы); • возможность индексации содержимого заголовков перехватываемых писем, при этом поддерживается фильтрация полей заголовков писем, значения которых будут индексироваться; • возможность осуществления асинхронного поиска по перехваченным данным (при проведении параллельного поиска по нескольким каналам передачи информации, отображение результатов выполняется по мере их получения); • просмотр комплексной статистики по хранящимся и индексируемым данным в базах данных и группах ротации. 10. Поддерживаемые форматы файлов Система должна поддерживать обработку файлов следующих форматов: •Adobe Acrobat (*.pdf) •Ami Pro (*.sam) •Ansi Text (*.txt) •ASCII Text •ASF (метаданные) (*.asf) •CSV (Comma-separated values) (*.csv) •DBF (*.dbf) •DjVu •DWG •DXF •EBCDIC •EML files (электронные письма, сохраненные Outlook Express) (*.eml) •Enhanced Metafile Format (*.emf) •Eudora MBX файлысообщений (*.mbx) •Flash (*.swf) •GZIP (*.gz) •HTML (*.htm, *.html) •JPEG (метаданные) (*.jpg) •Lotus 1-2-3 (*.wk?,

	.123) •MBOX архивыэлектронныхписем (включая Thunderbird) (.mbx) •MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (*.mht) •MIME-сообщения •MSG files (электронные письма, сохраненные Outlook) (*.msg) •Microsoft Access (*.mdb) •Microsoft Access 2007 (*.accdb) •Microsoft Outlook (OST) •Microsoft Document Imaging (*.mdi) •Microsoft Excel (*.xls)Microsoft Excel 2003 XML (*.xml) •Microsoft Excel 2007 (*.xlsx) •Microsoft Outlook Express 5 и 6: базысообщений (*.dbx) •Microsoft PowerPoint (*.ppt) •Microsoft Rich Text Format (*.rtf) •Microsoft Searchable Tiff (*.tiff) •Microsoft Word for DOS (*.doc) •Microsoft Word for Windows (*.doc) •Microsoft Word 2003 XML (*.xml) •Microsoft Word 2007 (*.docx) •Microsoft Works (*.wks) •MP3 (метаданные) (*.mp3) •OpenOffice версий 1, 2 и 3: документы, электронныетаблицыипрезентации (*.sxc, *.sxd, *.sxi, *.sxw, *.sxg, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (включая OASIS Open Document Format дляофисныхприложений) •OST(внутреннийформат Microsoft Outlook) •Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw) •TAR (*.tar) •TIFF (*.tif) •TNEF (winmail.dat) •Treepad HJT (*.hjt) •Unicode (UCS16, порядокбайтов Mac или Windows, или UTF-8) •Windows Metafile Format (*.wmf) •WMA видео (метаданные) (*.wma) •WMV видео (метаданные) (*.wmv) •WordPerfect 4.2 (*.wpd, *.wpf) •WordPerfect (5.0 ивыше) (*.wpd, *.wpf) •Write (*.wri) •XBase (включая FoxPro, dBase и другие совместимые с XBase форматы) (*.dbf) •XML Paper Specification (*.xps) •XSL •XyWrite •ZIP (*.zip) Кроме того, система должна обеспечивать распознавание и анализ текстовой информации в файлах графических форматов (BMP, JPEG, PNG, TIFF, GIF и другие), а также PDF- и DjVu-файлов путем оптического распознавания символов (OCR). 11. Возможности управления пользователями. В системе должно обеспечиваться: • создание внутренних карточек пользователей, содержащих всю идентификационную информацию контролируемых пользователей; • возможность создания пользовательских карточек без выделения лицензий на соответствующих пользователей, например, создание карточки для внешнего пользователя с целью отслеживания его общения с внутренними абонентами; в случае увольнения сотрудника – возможность сохранения карточки пользователя для контроля его последующего общения с сотрудниками компании; • отсутствие ограничений по количеству профилей пользователей в базе программы; • возможность привязки к пользовательской карточке общей информации о пользователе: ФИО, организация, подразделение, должность, телефоны, адрес и др., • возможность автоматической привязки к карточке данных пользователя из Active Directory (адреса электронной почты, названия организации, подразделения и должности пользователя, описания и фотографии пользователя); • возможность отображения в карточке пользователя информации из произвольных полей соответствующего пользователя Active Directory • возможность аутентификации пользователей, работающих с системой, на основании внутренних

	учетных записей (с запросом имени и пароля пользователя при входе в систему); • возможность автоматической привязки идентификационных данных пользователя (используемые идентификаторы Slack, номера ICQ, учетные записи Google Hangouts, Skype, Telegram, Viber, WhatsApp, Yahoo, ID социальных веб-сетей, SIP, адреса электронной почты, включая учетные записи XMPP и Microsoft Lync, а также IP-адреса и фотографии), к профилю пользователя для последующей идентификации; • возможность выбора типов контактной информации, которая будет автоматически привязываться к карточке пользователя • возможность исключения определенных пользователей из процесса автоматической привязки контактной информации • возможность исключения определенной информации (IP-адрес, адрес электронной почты, имя компьютера, учетные записи Skype, ICQ, Viber, Telegram, WhatsApp, MS Exchange, ID социальной сети) из процесса автоматической привязки контактной информации • возможность разграничения прав доступа как к отдельным компонентам системы, так и к перехваченным данным отдельных пользователь для различных групп с назначением ролей (например, «системный администратор»- доступ только к изменению технических параметров системы – без доступа к просмотру перехваченной информации; «руководитель подразделения»– доступ только к просмотру информации об активности определенных сотрудников – без доступа к просмотру информации об инцидентах или об активности других сотрудников; «офицер безопасности»– доступ только к политикам безопасности и инцидентам – без доступа к просмотру информации об активности сотрудников, и т.п.) с использованием системы аутентификации пользователей; • возможность интеграции с Active Directory с указанием доменов (объектов доменов) и контроллеров доменов, с которыми будет выполняться синхронизация; • синхронизацию пользователей Active Directory с возможность. автоматического создания и удаления карточек пользователей, при добавлении и удалении записей в Active Directory, с автоматическим создание карточек при обнаружении ранее неизвестной пользовательской информации; • автоматическую синхронизацию изменений идентификационных данных пользователей в Active Directory с данным в карточках пользователей возможностью настройки расписания синхронизации и синхронизируемых данных; • ведение журнала действий и авторизации пользователей, работающих с системой. 12. Требования к техническим и функциональным характеристикам системы. Система должна поддерживать несколько схем перехвата трафика в контролируемой сети, а также их комбинации: •централизованный перехват данных с сетевого коммутатора; •перехват данных с рабочих станций пользователей; •перехват электронной почты, переданной через почтовые сервера; •перехват HTTP(S)-трафика, переданного через прокси-сервер. 13. Требования к реализации централизованного перехвата данных Система должна обеспечивать: • централизованный перехват данных, отправляемых по протоколам, не использующим шифрование (FTP, HTTP, IMAP, POP3, SMTP, MAPI, MRA

	(Mail.Ru Агент), OSCAR (AIM, ICQ), XMPP (Jabber), YMSG (Y!M) посредством зеркалирования трафика; • фильтрация перехватываемых данных, отправляемых по протоколу HTTP по MIME типу, и по набору атрибутов (IP-адрес, порт, HTTP-метод, web-поле и др.), в том числе с использованием сложных условий («И», «Или», «Не»); • настройка исключений из перехвата по IP-адресам (отдельным и диапазону) и отдельным MAC-адресам, протоколам, учетным записям и адресам электронной почты, учетным записям систем мгновенного обмена сообщениями; 14. Требования к перехвату данных с рабочих станций Система должна поддерживать установку независимых программных модулей контроля непосредственно на рабочие станции сети организации. Агент контроля рабочих станций - независимый программный модуль, который устанавливается на рабочие станции в сети. Модуль должен осуществлять перехват нешифрованного сетевого трафика, а также выполнять перехват SSL-трафика и данных, переданных по использующим шифрование протоколам. Модуль должен фиксировать активность пользователя на контролируемой рабочей станции. Контроль рабочих станций должен обеспечивать следующее: • возможность как централизованной установки модулей - из единой консоли управления либо средствами групповых политик домена (с использованием MSI-пакета), так и установки вручную (с использованием отдельного EXE-инсталлятора модуля с графическим интерфейсом); • централизованная настройка дистрибутива модуля для установки вручную; • возможность перехвата данных, отправляемых по нешифрованным протоколам (POP3, SMTP, MAPI (MAPI over RPC, MAPI over RPC over HTTP, MAPI over HTTP), OSCAR, XMPP (Jabber), HTTP, FTP, MMP (Mail.Ru Агент), YIM); • возможность перехвата данных, отправляемых по шифрованным протоколам (с использованием SSL/TLS-шифрования), включая шифрованные протоколы передачи электронной почты и мгновенного обмена сообщениями, HTTPS, FTPS, Skype, SIP, а также данные, переданные в приложении Viber, WhatsApp, Google Hangouts, Telegram и Microsoft Lync; перехват данных, отправляемых по протоколам с использованием SSL/TLS-шифрования, осуществляется путем подмены цифрового сертификата. При этом должна поддерживаться возможность указания произвольного имени удостоверяющего центра в генерируемых системой сертификатах, а также возможность гибкой настройки подмены для использования различных сертификатов при перехвате различных SSL/TLS-соединений; • возможность перехвата и автоматического дешифрования зашифрованных почтовых сообщений, содержащих цифровую подпись (включая вложенные в письма файлы), защищенных по стандарту S/MIME; • возможность создания политик фильтрации и блокирования трафика на основании атрибутов и содержимого перехватываемых данных; • возможность фильтрации данных, отправляемых по протоколу HTTP/ HTTPS; • возможность гибкой настройки исключений из перехвата по IP-адресам (отдельным и диапазону), протоколам, системным учетным записям пользователей, учетным записям и адресам электронной почты, учетным записям систем

	мгновенного обмена сообщениями, атрибутам процессов, вешним устройствам и локальным сетевым ресурсам; • возможность блокирования передачи исходящих сообщений по протоколу SMTP(S) на основании заданных политик; • возможность блокирования передачи исходящих сообщений по протоколу HTTP(S) на основании заданных политик; • возможность блокирования посещения веб-ресурсов; • возможность блокирования паразитного HTTP(S) трафика вредоносных и служебных программ; • возможность блокирования отправки на съемные носители по содержимому, либо атрибутам; • возможность блокирования отправки на печать на локальные либо сетевые принтеры (при запуске с агента); • возможность блокирования буфера обмена по содержимому, либо атрибутам; • блокирование сетевого трафика процессов на основании их атрибутов и значения хеш-функций исполнительных файлов; • настройка уведомлений пользователя рабочей станции о блокировке устройств, запуска процессов, сетевого трафика процессов и MAPI-трафика; • перехват Web-коммуникаций пользователей в социальных сетях Facebook, Odnoklassniki, Vk, Twitter, Instagram, LinkedIn, Bitrix24. При этом должны поддерживаться: двунаправленный перехват сообщений в чатах; перехват статусов; перехват комментариев к публикациям и изображениям, перехват комментариев на форумах социальных сетей с контролем всего блока комментариев; • перехват входящей и исходящей web-почты (gmail, mail.ru, rambler, yandex, yahoo, hotmail); • контроль данных, отправляемых на внешние накопители, принтеры, облачные хранилища и локальные сетевые ресурсы пользователей и терминальных серверов; • аудит файловых операций, таких как изменение, чтение, удаление файлов и папок на компьютере с агентом; • аудит файловых операций, контроль записи информации и блокирование доступа пользователей к локальным сетевым ресурсам; • аудит файловых операций, контроль передачи информации и блокирование доступа пользователей к облачным сервисам хранения информации при использовании веб-интерфейса и десктоп- приложений (Dropbox, OneDrive, Google Drive, Яндекс.Диск, Apple iCloud, облако Mail.Ru); • аудит файловых операций, контроль записи информации и блокирование доступа пользователей к различным классам внешних накопителей информации с учетом их параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер); • аудит использования и контроль доступа для внешних устройств, подключенных к рабочей станции, и блокирование доступа с учетом их параметров (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства); • возможность сбора статистики по времени работы/простоя компьютера; • контроль запуска приложений на компьютерах пользователей, а также длительность работы в каждом приложении (например, контроль использования нежелательного или запрещенного программного обеспечения в корпоративной сети); • запрет запуска отдельных программных приложений на контролируемой рабочей станции на основании имени процесса, атрибутов

	исполнительного файла и значения хеш-функции; • возможность снятия снимков экрана рабочего стола пользователя с заданным интервалом, а также по событию (нажатие клавиши PrintScreen, смена окна активного приложения либо вкладки браузера, запуск определенного приложения); • перехват данных, помещаемых и вставляемых в буфер обмена с поддержкой исключения активности отдельных процессов из перехвата; • перехват данных, помещаемых в буфер обмена с поддержкой исключения активности отдельных процессов из перехвата; • контроль данных, вводимых пользователем с клавиатуры («кейлоггер») с возможностью исключения активности отдельных процессов из перехвата; • прослушивание аудиопотока, поступающего с микрофонов, подключенных к рабочим станциям в режиме реального времени; • возможность удаленного просмотра видеоизображения рабочего стола пользователя в режиме реального времени; • автоматический поиск конфиденциальных файлов на дисках рабочей станции пользователя (по имени, по заданным атрибутам или значениям хеш-функций); • настройка функциональных возможностей модулей применительно к различным объектам AD, отдельным компьютерам (группам компьютеров) и пользователям с указанным SID; • выбор условий активации настроек модулей, например, наличие соединения с сервером, наличие активного VPN-подключения, произвольное заданное условие; • возможность защиты модуля на рабочей станции от несанкционированного удаления пользователем; • возможность скрытия модуля на рабочей станции (включая скрытие процессов, служб, установочных файлов и папок); • опциональное отображение иконки системы в панели задач контролируемой рабочей станции; • сохранение функциональных возможностей модуля (автономный режим) в случае выноса рабочей станции за пределы корпоративной сети, сохранение всех данных перехвата. Автоматическое восстановление связи с серверной частью системы; • возможность настройки автономного режима работы модуля; Система должна отслеживать и отображать статистику по состоянию модулей контроля рабочих станций: • поступление данных на сервер от каждого модуля, • пользователей, контролируемых модулем; • подключенные внешние устройства • типы перехватываемых данных (протоколов). Данные статистики должны быть доступны для экспорта. 15. Требования к перехвату HTTP-трафика, переданного через прокси-сервера. Перехват данных, переданных по протоколам HTTP и HTTPS через прокси-сервер, должен выполняться путем интеграции с прокси-сервером по ICAP-протоколу. При этом должны обеспечиваться следующие возможности: - перехват данных, отправляемых по протоколу HTTP(S); - фильтрация данных, перехватываемых по протоколу HTTP(S) по набору атрибутов (IP-адрес, порт, HTTP-метод, web-поле и др.), в том числе с использованием сложных условий («И», «Или», «Не»); - фильтрация данных, перехватываемых по протоколу HTTP(S) по IP-адресу, в том числе по диапазону адресов, с возможностью настройки белого и черного списка исключений; - блокировка передачи исходящих сообщений по протоколу HTTP(S),

	содержащих определенную информацию на основании контентного и атрибутивного анализа передаваемых данных с возможностью настройки сообщения, отображаемого при блокировке; - настройка очереди отправки данных в модуль хранения и обработки данных по максимальному размеру передаваемых элементов, максимальному числу элементов в очереди, максимальному общему размеру очереди с возможностью хранения очереди как на диске, так и в оперативной памяти; - отображение статистики по работе модуля в реальном времени; - импорт и экспорт правил фильтрации и блокировки. 16. Требования к перехвату электронной почты, переданной через почтовые сервера Перехват почты, отправляемой через почтовые сервера, развернутые на базе Microsoft Exchange Server, IBM Lotus Domino, Sendmail, hMailServer и другого программного обеспечения, должен осуществляться путем интеграции с почтовыми серверами по протоколам POP3, IMAP, SMTP, а также при помощи коннектора MS Exchange 17. Требования к перечню контролируемых каналов утечки Требования к контролю электронной почты. Система должна обеспечивать контроль отправки информации посредством электронной почты, включая следующие возможности: - перехват почтовых сообщений для нешифрованных и шифрованных (SSL) протоколов – POP3, SMTP, IMAP, MAPI плюс шифрованные аналоги; - перехват почтовых сообщений, переданных посредством почтовых программ с поддержкой стандарта защищённой электронной почты S/MIME с автоматической расшифровкой содержимого письма; - перехват почтовых сообщений путем интеграции с почтовыми серверами (на базе Microsoft Exchange, IBM Lotus Domino, Postfix, Sendmail и др.) по протоколам POP3, SMTP, IMAP (на выбор); - перехват почтовых сообщений между Microsoft Outlook и Microsoft Exchange Server по протоколу MAPI (в том числе с использованием шифрования) путем интеграции с Microsoft Outlook; - перехват и анализ почтовых сообщений, отправленных либо полученных при помощи почтовых веб-сервисов по протоколу HTTP(S) (yandex, mail.ru, rambler, gmail, yahoo, hotmail и т.д.); - перехват и анализ файлов-вложений почтовых сообщений; - автоматическое обнаружение почтовых сообщений и почтовых вложений, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - блокировка исходящих почтовых сообщений по протоколу SMTP(S), HTTP(S), MAPI на основании заданных политик безопасности с использованием контентного и атрибутивного анализа сообщений; - возможность сохранения электронных писем в HTML-формате и в формате, совместимом с Microsoft Outlook; - возможность поиска по тексту и атрибутам почтовых сообщений и файлов, переданных по почте. 18. Требования к контролю IM-клиентов Система должна обеспечивать контроль отправки информации посредством IM-клиентов, включая следующие возможности: - Перехват текстовых сообщений в мессенджерах Viber, Telegram (включая веб-версию), WhatsApp (включая веб-версию), Skype

	(включая веб-версию), Microsoft Lync, Microsoft Teams (включая веб-версию), Discord (включая веб-версию), Hangouts, Slack (включая веб-версию), WeChat, Signal, Express, Vk Teams. Агент Mail.ru, ICQ10, ICQ, RocketChat, а также в мессенджерах, использующих протоколы SIP, OSCAR, XMPP (включая XMPP по HTTP), YMSG. - Перехват файлов, передаваемых в мессенджерах Viber, Telegram, WhatsApp (включая веб-версию), Skype (включая веб-версию), Microsoft Lync, RocketChat, Microsoft Teams (включая веб-версию), Discord (включая веб-версию), Slack (включая веб-версию), Signal, Express, Vk Teams. - Перехват голосовых разговоров, осуществляемых через Skype (в том числе звонки Skype-to-Skype, Skype-to-phone), а также через Microsoft Lync, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams и по протоколу SIP с сохранением разговоров в файлы формата MP3; - возможность распознавания и перевода в текстовый формат голосовых разговоров (коммуникаций) Microsoft Lync, Skype, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams и SIP; - возможность воспроизведения сохраненных разговоров Microsoft Lync, Skype, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams и SIP; - возможность ограничения перехвата по отдельным учетным записям пользователей; - автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность осуществления поиска по тексту и атрибутам сообщений и файлов, переданных через мессенджеры, в том числе с применением шаблонов. - перехват сообщений и файлов, переданных в веб-клиентах мессенджеров: Skype, Telegram, Whatsapp, Discord, Microsoft Teams, Slack, а также перехват сообщений, переданных в веб-клиентах мессенджеров: ICQ, Google Hangouts; - контроль переписок и постов в Facebook, LinkedIn. - контроль переписок в Instagram. - контроль переписок, электронной почты и файлов в CMS Bitrix24. - блокировка отправки файлов в мессенджеры, как по набору атрибутов так и по содержимому - перехват голосовых сообщений и файлов в web- и dekstop-версиях мессенджера WhatsApp. 19. Требования к контролю HTTP-протокола. Система должна обеспечивать контроль отправки информации по HTTP-протоколу, включая: - возможность создания и гибкой настройки фильтров по параметрам HTTP-запроса для исключения из перехвата определенной исходящей и входящей информации по ряду предустановленных правил и правил, созданных пользователе; - возможность настройки фильтрации перехвата данных по MIME-типам по ряду предустановленных правил и правил, созданных пользователе; - возможность перехвата, блокирования и фильтрации GET/POST/PUT запросов при выборе HTTP-методов контроля переданных данных; - перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы; - перехват и анализ поисковых запросов пользователя; - сохранение адресов всех страниц,

	посещенных пользователем; - перехват входящих и исходящих данных веб-коммуникаций (переписки в чатах, публикация статусов, комментарии) на веб-ресурсах: Facebook, Twitter, ВКонтакте, Одноклассники; - перехват входящих и исходящих электронных писем и вложений, переданных либо полученных через почтовые веб-сервисы (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex, Zimbra и т.д.); - перехват сообщений и файлов, переданных в веб-клиентах мессенджеров: Skype, Telegram, Whatsapp, Discord, Microsoft Teams, Slack, а также перехват сообщений, переданных в веб-клиентах мессенджеров: ICQ, Google Hangouts; - автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность поиска по тексту и атрибутам сообщений и файлов, переданных по протоколу HTTP(S); - возможность блокирования посещений веб-ресурсов, исходящих сообщений и файлов, по контенту, по набору атрибутов, а также по хеш-сумме отправляемых файлов; - возможность настройки пользовательского сообщения про блокировки HTTP(S) трафика. 20. Требования к контролю FTP-протокола Система должна обеспечивать контроль информации, передаваемой по протоколу FTP, включая: - Перехват исходящих и входящих файлов, переданных по FTP-соединению, а также переданных по зашифрованному SSL-соединению; - возможность настройки ограничения по размеру перехватываемых файлов; - автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность поиска по тексту и атрибутам файлов, переданных по протоколу FTP(S), в том числе с применением шаблонов; - возможность блокирования отправки файлов по протоколу FTP. 21. Требования к контролю принтеров. Система должна обеспечивать контроль информации, отправляемой на печать, включая: - возможность перехвата документов, отправляемых на сетевые, виртуальные и локальные принтеры (в том числе подключенные к COM-, LPT-портам); - возможность перехвата печати в XPS-формат; - возможность настройки исключений из перехвата по отдельным принтерам; - возможность ограничения перехвата печати по количеству страниц и по размеру документа; - возможность исключения процессов для модуля перехвата печати на принтерах. - извлечение и анализ текста отправленных на печать документов; - автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность блокировки печати по названию документа. текстовому содержимому документа и по названию принтера; - возможность поиска по тексту и атрибутам отправленных на печать файлов, в том числе с применением шаблонов; - сохранение в

	PDF- и XPS-формате. - возможность блокировки документов, отправляемых на печать как по набору атрибутов, так и по содержимому документа, отправляемого на печать. 22. Требования к контролю подключенных устройств и внешних накопителей информации. Система должна обеспечивать контроль информации, отправляемой на внешние носители, включая: - аудит подключения внешних устройств - теневое копирование файлов, отправляемых на внешние накопители (съемные жесткие диски, флеш-накопители, карты памяти, съемные накопители, CD/DVD и флоппи-диски и т.д.); - аудит событий копирования файлов на внешние накопители (съемные жесткие диски, флеш-накопители, карты памяти, съемные накопители, CD/DVD и флоппи-диски и т.д.), фиксируется имя файла, пользователь, дата, время и данные устройства; - возможность настройки исключений из теневого копирования и аудита по размеру и расширению файлов; - возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ); - сохранение теневых копий файлов, записанных на внешние накопители, локально на контролируемых компьютерах перед отправкой данных на сервер; - возможность настройки размера хранилища для теневых копий на контролируемых компьютерах; - возможность блокирования записи файлов на съёмные носители по содержимому передаваемой информации и другим атрибутам. - возможность настройки исключений из теневого копирования и аудита для определенных внешних накопителей информации (по типам устройств, идентификаторам, производителям, названиям, серийным номерам); - контроль доступа к внешним накопителям информации, с возможностью запрета на использование устройств с определенными параметрами (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства и др.); - управление правами записи на внешние накопители с возможностью запрета записи на определенные устройства (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства), а также запрета записи файлов с определенным расширением; - возможность контроля копирования информации на внешние накопители как в локальных, так и терминальных пользовательских сессиях; - исключение отдельных процессов из процедуры контроля, аудита теневого копирования. - контроль доступа и аудит использования внешних устройств любого типа из списка поддерживаемых (USB Bus Devices (hubs and host controllers), CD\DVD, Audio, Network Adapters, Serial and parallel ports, SCSI and RAID controllers, Floppy drives, Cameras and scanners, Windows Portable Devices (WPD), Universal cameras), подключаемых к рабочей станции, с фильтрацией по набору параметров (название устройства, идентификатор устройства, идентификатор производителя, идентификатор продукта, производитель, серийный номер, тип устройства); - добавление в фильтр исключений устройств, подключенных на контролируемых рабочих станциях; - автоматическое обнаружение случаев использования внешних устройств с указанными

	параметрами (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - автоматическое обнаружение случаев передачи на внешние накопители файлов в целом и, в частности, содержащих определенную информацию (на основании заданных политик безопасности), с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность поиска по тексту и атрибутам отправленных на внешние накопители файлов, в том числе с применением шаблонов. - возможность блокировки файлов, записываемых на накопитель как по набору атрибутов, так и по содержимому. 23. Требования к контролю локальных сетевых ресурсов Система должна обеспечивать контроль информации, отправляемой на локальные сетевые ресурсы, включая следующие возможности: - аудит событий копирования файлов на локальные сетевые ресурсы: фиксируется имя файла, пользователь, дата, время и сетевой путь к ресурсу; - теневое копирование файлов, отправляемых на сетевые ресурсы; - возможность настройки исключений из аудита и теневого копирования по расширениям файлов; - возможность настройки исключений из аудита и теневого перехвата определенных сетевых ресурсов; - возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ); - сохранение теневых копий файлов, записанных на сетевые ресурсы, локально на контролируемых компьютерах перед отправкой на сервер; - возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей; - возможность теневого копирования файлов, передаваемых на сетевые ресурсы терминальных серверов; - контроль доступа к сетевым ресурсам с возможностью запрета доступа на определенные сетевые ресурсы; - управление правами записи на сетевые ресурсы с возможностью запрета записи определенных форматов файлов; - исключение отдельных процессов из процедуры контроля, аудита теневого копирования; - автоматическое обнаружение переданных на сетевые ресурсы файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность поиска по тексту и атрибутам отправленных на сетевые ресурсы файлов, в том числе с применением шаблонов. 24. Требования к контролю облачных хранилищ (Dropbox, OneDrive, Google Drive, Яндекс.Диск, Apple iCloud, облако Mail.Ru). Система должна обеспечивать контроль использования облачных хранилищ, в том числе: - аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, имя пользователя, дата, время и имя облачного сервиса хранения; - теневое копирование файлов, отправляемых в облачные хранилища пользователем либо процессом; - настройка аудита и теневого копирования только исходящих, только входящих, либо всех файлов; - возможность настройки частичного сохранения теневой копии для больших

	файлов (например, сохранять только первые 100 МБ); - сохранение теневых копий файлов, записанных в облачное хранилище, локально на контролируемых компьютерах перед отправкой на сервер; - возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей; контроль доступа к отдельным облачным хранилищам с возможностью запрета доступа для определенных пользователей; контроль доступа к отдельным облачным хранилищам с возможностью настройки режима «только чтение» для определенных пользователей; управление правами передачи данных в облачные хранилища с возможностью запрета отправки файлов определенных форматов; возможность настройки исключений из аудита, теневого копирования и контроля доступа по расширениям файлов; автоматическое обнаружение переданных в облачные хранилища файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; возможность поиска по тексту и атрибутам отправленных файлов, в том числе с применением шаблонов. Система должна обеспечивать следующие возможности по контролю веб-версий облачных хранилищ (iCloud, Dropbox, Google Drive, OneDrive, Облако Mail.ru, Яндекс.Диск, ownCloud): - аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, имя пользователя, дата, время и имя облачного сервиса хранения; - теневое копирование файлов, отправляемых в облачные хранилища пользователем либо процессом; - сохранение теневых копий файлов, записанных в облачное хранилище, локально на контролируемых компьютерах перед отправкой на сервер; - автоматическое обнаружение переданных в облачные хранилища файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность поиска по тексту и атрибутам отправленных файлов, в том числе с применением шаблонов. 25. Требования к возможностям мониторинга действий пользователей на ПК. Требования к функции снятия скриншотов. Система должна выполнять сохранение снимков рабочего стола пользователей и обеспечивать: •возможность снятия скриншотов с заданным интервалом; •возможность снятия скриншотов при смене активного окна и смене вкладки браузера; •возможность снятия скриншотов при нажатии клавиши PrintScreen; •возможность настройки качества скриншотов (в т.ч. сохранения в черно-белом формате); •возможность настройки размера скриншотов (в процентах от оригинала); •возможность настройки формата скриншотов (JPEG, PNG); •сохранение специальной отметки в случае невозможности снятия скриншота (сессия пользователя отключена, заблокирована и т.п.); •возможность экспорта снимков экранов во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к просмотру перехваченных данных через веб-браузер; •возможность сохранения скриншотов отдельного пользователя за день

	(или за выбранный временной интервал) в виде набора графических файлов, web- документа либо объединенных в один PDF- или видеофайл; •возможность сохранения скриншотов нескольких пользователей за выбранный интервал дат в виде набора графических файлов, web-документа либо объединенных в один PDF- или видеофайл. 26. Требования к блокировке передачи данных: Система должна обеспечивать оперативное реагирование на случаи нарушения политик безопасности организации, путем блокировки чувствительных данных, отправляемых по протоколам HTTP, MAPI, SMTP, а также на печать, в режиме реального времени. Система должна располагать следующими возможностями: - блокировка данных, передаваемых по протоколу HTTP, на основании анализа содержимого (контентный анализ) с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология, количество вхождений фразы в документ и др. При этом обеспечивается возможность блокировать по содержимому такие операции как отправка сообщений и файлов в почтовых веб сервисах и социальных сетях, поиск информации в интернете, и многие другие; - блокировка данных, передаваемых по протоколу HTTP, на основании анализа содержимого (контентный анализ) с использованием регулярных выражений - блокировка данных, передаваемых по протоколу HTTP, на основании анализа атрибутов (контекстный анализ) с использованием таких атрибутов как: IP-адрес, порт, факт использования шифрованного соединения, HTTP-метод, параметры web-поля, атрибуты файла, категория сайта и др. - блокировка файлов, передаваемых по протоколу HTTP, на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы; - блокировка файлов, передаваемых по протоколу HTTP, на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы; - возможность добавления в банк хеш-сумм всех файлов, расположенных в определенной папке, а также только файлов определенного расширения из указанной папки; - блокировка данных, передаваемых по протоколу HTTP, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки; - блокировка данных, передаваемых по протоколу HTTP, на основании цифровых отпечатков, с возможностью указания нескольких цифровых отпечатков в одном правиле блокировки; - блокировка файлов, отправляемых по протоколу HTTP на основании анализа меток конфиденциальности; - блокировка почты, отправляемой по протоколу SMTP, на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.; - блокировка

	почты, отправляемой по протоколу SMTP, на основании анализа содержимого (контентный анализ) с использованием регулярных выражений - блокировка почты, отправляемой по протоколу SMTP, на основании анализа атрибутов (контекстный анализ) письма и вложений с использованием таких атрибутов как: IP-адрес, порт, отправитель, получатель, атрибуты файла и др. - блокировка вложений, передаваемых по протоколу SMTP, на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы; - блокировка почты, отправляемой по протоколу SMTP, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки; - блокировка почты, отправляемой по протоколу SMTP, на основании цифровых отпечатков, с возможностью указания нескольких цифровых отпечатков в одном правиле блокировки; - блокировка файлов, отправляемых по протоколу SMTP на основании анализа меток конфиденциальности; - блокировка почты, отправляемой по протоколу MAPI, на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.; - блокировка почты, отправляемой по протоколу MAPI, на основании анализа содержимого (контентный анализ) с использованием регулярных выражений - блокировка почты, отправляемой по протоколу MAPI, на основании анализа атрибутов (контекстный анализ) письма и вложений с использованием таких атрибутов как: IP-адрес, порт, отправитель, получатель, атрибуты файла и др. - блокировка вложений, передаваемых по протоколу MAPI, на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы; - блокировка почты, отправляемой по протоколу MAPI, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки; - блокировка почты, отправляемой по протоколу MAPI, на основании цифровых отпечатков, с возможностью указания нескольких цифровых отпечатков в одном правиле блокировки; - блокировка файлов, отправляемых по протоколу MAPI, на основании анализа меток конфиденциальности; - блокировка данных, передаваемых по протоколу FTP, на основании анализа атрибутов (контекстный анализ) с использованием таких атрибутов как: пользователь, IP-адрес, порт, компьютер, домен, атрибуты файла и др. - блокировка данных, передаваемых по протоколу XMPP, на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.; - блокировка данных, передаваемых по протоколу XMPP, на основании анализа содержимого

	(контентный анализ) с использованием регулярных выражений - блокировка данных, передаваемых по протоколу XMPP, на основании анализа атрибутов (контекстный анализ) письма и вложений с использованием таких атрибутов как: пользователь, компьютер, домен, атрибуты файла и др. - блокировка файлов, передаваемых по протоколу XMPP, на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы; - блокировка данных, передаваемых по протоколу XMPP, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки; - блокировка данных, передаваемых по протоколу XMPP, на основании цифровых отпечатков, с возможностью указания нескольких цифровых отпечатков в одном правиле блокировки; - блокировка файлов, передаваемых по протоколу XMPP, на основании анализа меток конфиденциальности; - блокировка документов, отправляемых на печать, на основании анализа содержимого (контентный анализ) документа с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.; - блокировка документов, отправляемых на печать, на основании анализа содержимого (контентный анализ) с использованием регулярных выражений - блокировка документов, отправляемых на печать, на основании анализа атрибутов (контекстный анализ) печати с использованием таких атрибутов как: компьютер, домен, пользователь, время, день недели и др. - блокировка документов, отправляемых на печать, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки; - блокировка данных, копируемых в буфер обмена, на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.; - блокировка данных, копируемых в буфер обмена, на основании анализа содержимого (контентный анализ) с использованием регулярных выражений - блокировка данных, копируемых в буфер обмена, на основании анализа атрибутов (контекстный анализ) письма и вложений с использованием таких атрибутов как: пользователь, компьютер, процесс, домен, атрибуты файла, тип данных (текст, изображение, файл) и др. - блокировка данных, копируемых в буфер обмена, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки; - блокировка данных, вставляемых из буфера обмена, на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.; - блокировка данных, вставляемых из буфера обмена, на основании анализа содержимого (контентный анализ) с использованием

	регулярных выражений - блокировка данных, вставляемых из буфера обмена, на основании анализа атрибутов (контекстный анализ) письма и вложений с использованием таких атрибутов как: пользователь, компьютер, процесс, домен, атрибуты файла, тип данных (текст, изображение, файл) и др. - блокировка данных, вставляемых из буфера обмена, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки; - блокировка запуска процессов на основании анализа атрибутов (контекстный анализ) процесса с использованием таких атрибутов как: компьютер, домен, категория приложения, хеш-сумма и др. - блокировка отправки файлов в мессенджеры на основании анализа содержимого (контентный анализ) с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.; - блокировка отправки файлов в мессенджеры на основании анализа содержимого (контентный анализ) с использованием регулярных выражений - блокировка отправки файлов в мессенджеры на основании анализа атрибутов (контекстный анализ) - блокировка записи файлов на накопители на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.; - блокировка записи файлов на накопители на основании анализа содержимого (контентный анализ) с использованием регулярных выражений - блокировка записи файлов на накопители на основании анализа атрибутов (контекстный анализ) с использованием таких атрибутов как: пользователь, компьютер, процесс, домен, и др. атрибуты файла - блокировка записи файлов на определенные накопители (по серийному номеру, производителю, названию устройства, идентификатору производителя и идентификатору продукта) - блокировка записи файлов на накопители на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы; - блокировка записи файлов на накопители на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки; - блокировка записи файлов на накопители на основании цифровых отпечатков, с возможностью указания нескольких цифровых отпечатков в одном правиле блокировки; - блокировка записи файлов на накопители на основании анализа меток конфиденциальности; - возможность уведомления конечного пользователя при блокировке, с настраиваемым текстом уведомления; - возможность уведомления офицера безопасности о сработавшем правиле блокировки; - возможность поиска по атрибутам заблокированной информации. 27. Требования к функции сбора статистики по активности ПК Система должна обеспечивать сбор и хранение данных об активности контролируемых рабочих станций и активности пользователя на рабочей станции: - ведение

	статистики по активному времени работы и простоя (отсутствия действий пользователя) с возможностью настройки периода отсутствия активности до начала простоя; - ведение статистики по времени работы пользователя в приложениях с представлением собранной информации, при этом учитывается при этом учитывается не все время работы приложения, а время работы пользователя в активном окне; - исключение отдельных процессов из мониторинга; - возможность автоматического анализа собранной статистики для выявления определенных событий (например, запуск несанкционированных приложений), контроля длительности работы пользователей с конкретными приложениями и длительности периодов работы/простоя компьютера – с отправкой соответствующего уведомления ответственному лицу; - возможность блокировки запуска отдельных приложений; - возможность сохранения отдельных отчетов по активности (активность пользователя за ПК, активность приложений, хронология событий) за выбранный временной интервал для отдельного пользователя или нескольких пользователей. - автоматическая категоризация времени, проведенного в различных приложениях, на продуктивное, непродуктивное и нейтральное 28. Требования к контролю буфера обмена Система должна обеспечивать сбор и хранение данных об активности контролируемых рабочих станций и активности пользователя на рабочей станции: - теневое копирование помещаемой в буфер обмена текстовой информации с фиксацией приложения, из которого данная информация была помещена в буфер обмена, и времени события; - аудит файлов, помещаемых в буфер обмена; - теневое копирование графического содержимого помещаемого в буфер обмена; - теневое копирование файлов, помещаемых в буфер обмена; - возможность ограничения максимального объема данных, перехватываемых из буфера обмена; - возможность исключения отдельных процессов из мониторинга буфера обмена либо мониторинг только определенных процессов; - возможность исключения отдельных файлов из мониторинга буфера обмена либо мониторинг только определенных файлов; - автоматическое обнаружение определенной информации (на основании заданных политик безопасности), помещаемой в буфер обмена, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность блокирования как копирования, так и вставки файлов по содержимому, в соответствии с настроенными правилами безопасности. - возможность поиска по тексту, помещаемому пользователями в буфер обмена, в том числе с применением шаблонов. - возможность настройки обнаружения отдельно информации, скопированной в буфер обмена, и информации, вставляемой из буфера обмена; - возможность настройки обнаружения в буфере обмена только файлов, только текста либо только изображений. 29. Требования к функциям кейлоггера. Система должна поддерживать: - регистрация нажатий пользователем клавиш на клавиатуре с фиксацией приложения, в котором пользователь вводил данную информацию, и времени, возможность отображения/скрытия нажатий служебных

	клавиш (Shift, Enter, Backspace и т.п.); - возможность исключения перехвата клавиатуры в заданных приложениях либо осуществление перехвата только в определенных приложениях; - возможность исключения перехвата клавиатуры по адресу активной страницы в браузере либо осуществление перехвата только на определенной активной странице в браузере; - автоматическое обнаружение определенной информации (на основании заданных политик безопасности), вводимой пользователем с помощью клавиатуры, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации; - возможность поиска по тексту, вводимому пользователями с клавиатуры, в том числе с применением шаблонов. 30. Видеомониторинг. Система должна позволять контролировать активность пользователя при помощи снятия видео рабочего стола, а также видео с веб-камеры, и располагать следующими возможностями: - подключение к монитору компьютера пользователя и просмотр видео рабочего стола в режиме реального времени; - мониторинг рабочих столов нескольких пользователей одновременно; - возможность вывода окна просмотра на отдельный экран; - автоматическая запись видеоизображения рабочего стола и видео с подключенной веб-камеры по расписанию; - запись видео рабочего стола вручную; - возможность настройки качества записи; - возможность как записи видео в цветном, так и в черно-белом формате; - возможность сохранения записей нескольких пользователей одновременно; - возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей. 31. Требования к функции аудиомониторинга: Система должна позволять контролировать активность пользователя при помощи записи аудио с микрофона и аудио, поступающего на динамики рабочей станции, и располагать следующими возможностями: - подключение к микрофонам контролируемых рабочих станций с возможностью прослушивания аудиопотока в режиме реального времени; - прослушивание микрофонов нескольких пользователей одновременно; - автоматическая запись поступающего с микрофона аудиопотока и системных звуков компьютера по расписанию; - запись вручную; - возможность сохранения записей нескольких пользователей одновременно; - возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей. - отображение звуковой дорожки в записанном видео-, аудио 32. Требования к контролю файловых систем. Контроль файловых систем должен позволять: - автоматическое сканирование файловых систем контролируемых рабочих станций на предмет наличия документов, которые носят статус конфиденциальных либо представляют интерес в рамках обеспечения информационной безопасности; - формирование банков конфиденциальных документов, поиск которых должен выполняться во время сканирования; - возможность автоматического импорта в банк конфиденциальных документов подготовленных хеш-функций из файлов txt- и csv-формата; - возможность выбора рабочих станций и пользователей, чьи файловые системы будут контролироваться; - гибкая настройка

	правил выбора файлов и папок, подлежащих автоматической проверке; - исключение из сканирования файлов настраиваемого размера; - возможность выполнения проверок файловой системы по расписанию; - возможность создавать индивидуальные политики контроля за содержимым файловых систем для отдельных пользователей и рабочих станций, в том числе с применением шаблонов; - возможность поиска документов в файловых системах контролируемых рабочих станций по атрибутам файлов и значениям их хеш-функций. 33. Требования к методам анализа перехваченной информации и процедурам реагирования на инциденты безопасности Система должна обеспечивать следующие функциональные возможности при работе с политиками безопасности: - настройка правил безопасности при помощи поисковых условий с использованием всех доступных инструментов анализа: контентный анализ, атрибутивный анализ, поиск по распознанным изображениям, печатям, распознанной речи, событийный анализ и др.; - комбинирование нескольких простых поисковых условий при помощи логических операторов «И», «ИЛИ», «НЕ», с возможностью объединения поисковых условий в группы; - правила безопасности по группам Active Directory; - правила безопасности по категориям сайтов и приложений; - правила безопасности на обнаружение файлов с определенными метками конфиденциальности - создание политик безопасности с использованием шаблонов поиска – набора поисковых условий, которые можно использовать при формировании других правил безопасности; - правила безопасности по цифровым отпечаткам с возможностью настройки порога срабатывания и выбором направления вхождения (прямое, обратное, или наибольшее); - правила безопасности по словарям, с возможностью учета порога срабатывания и морфологии; - правила безопасности по хеш-суммам, с возможностью поиска по преднастроенным банкам хеш-сумм; - статистические правила безопасности, контролирующие превышение количественные показатели активности пользователя, например, количество электронных писем, переписок в мессенджерах, посещенных сайтов, отправленных запросов, распечатанных файлов и страниц, а также вычислять периоды активности пользователей и приложений, и др.; - наличие предустановленных правил безопасности; - возможность создания групп и подгрупп с количество уровней иерархии не менее 20; - возможность отключения правила безопасности - фильтр включенных/выключенных правил безопасности - возможность переноса политик безопасности из группы в группу простым перетаскиванием «мышью»; - возможность переноса подгрупп из группы в группу простым перетаскиванием «мышью»; - добавление, исключение групп Active Directory, к которым могут быть применены политики безопасности; - добавление, исключение, редактирование категорий инцидентов сервера безопасности - задание и редактирование уровня риска инцидентов сервера безопасности - автоматический расчёт показателей уровней риска пользователей и поведенческого анализ на основании уровней риска инцидентов; - возможность выполнения скриптов при срабатывании или

	ошибке срабатывания правила безопасности; - возможность отправки данных о инцидентах в сторонние системы; - автоматическая доставка уведомлений по электронной почте ответственному лицу в случае срабатывания политики безопасности (выявления инцидента); - инцидент содержит общую информацию (название политики безопасности, пользователь, допустивший нарушение, тип перехваченных данных, дата/время инцидента и др.), а также ссылку на открытие соответствующего инцидента в пользовательской консоли либо вложения с документами, вызвавшими срабатывание политики безопасности; - возможность настройки периодичности отправки уведомлений на электронную почту (немедленная отправка уведомления по выявлению инцидента либо накопление и порционная отправка уведомлений с заданной периодичностью – раз в час, раз в сутки и т.д.); - возможность просмотра всех инцидентов по выбранной политике безопасности в клиентской консоли с возможностью выделения просмотренных, непросмотренных инцидентов для каждого офицера безопасности, работающего с системой; - при просмотре информации об инциденте в клиентской консоли доступна следующая информация: пользователь, допустивший нарушение, дата и время инцидента, показатель присвоенного уровня риска, тип документа, вызвавшего срабатывание политики безопасности (электронное письмо, файл, отправленный на печать и т.д.), содержание документа (электронного письма, переписки в IM-клиенте, файла и т.д.), вызвавшего срабатывание политики безопасности, а также другая дополнительная информация. - возможность назначения статуса для инцидента (инцидент не расследован, расследование инцидента отложено, инцидент расследован, важный инцидент, неважный инцидент, ложное срабатывание); - возможность присвоения цветовой категории инциденту - возможность добавления комментария к инциденту - возможность гибкого выборочного просмотра инцидентов по политике безопасности (например, показать только новые или непросмотренные инциденты; показать только последние 100 инцидентов; показать инциденты за ближайший месяц, но не более 20 последних; показать инциденты, имеющие статус «Важный» и зарегистрированные в течение последней недели и т.д.); - возможность полного или выборочного удаления записей об инцидентах по политике безопасности (например, удалить все инциденты старше 10 дней; удалить последние N инцидентов; удалить все инциденты, имеющие статус «Расследован»; удалить инциденты по данным, удаленным из БД, и т.д.); - возможность сортировки списка инцидентов по различным параметрам (по релевантности, по дате/времени, по локальному/удаленному пользователю, по типу/размеру перехваченных данных, по статусу инцидента и т.д.); - возможность фильтрации списка инцидентов по различным параметрам: по статусам (например, отобразить только важные), по типам данных (например, отобразить только инциденты, вызванные пересылкой информации по почтовым протоколам), по состоянию (например, отобразить только непросмотренные) – и по комбинациям этих параметров; - возможность

	экспорта списка инцидентов в файл форматов CSV, MS Excel, PDF, XML (при этом сохраняется следующая информация об инцидентах – тип перехваченных данных, локальный/удаленный пользователь, дата/время перехвата, размер, статус инцидента, прочая информация); - возможность экспорта перехваченных данных, вызвавших срабатывание политики безопасности, в файлы соответствующих форматов; - ведение журнала (лога) действий офицера безопасности с возможностью экспорта событий журнала; - в журнале событий регистрируется следующая информация создание, дублирования, редактирование, удаление правила безопасности, просмотр и удаление инцидента, изменения статусов инцидента и др. При анализе информации должны быть использованы следующие методы анализа, включая анализ информации на русском, казахском и английском языке: 34. Контентный анализ: - поиск по словам и словосочетаниям с учетом морфологии, с возможностью отключения; - поиск по словам и словосочетаниям с учетом расстояния между словами; - поиск по словам и словосочетаниям с учетом порядка слов; - поиск по словам и словосочетаниям с учетом транслитерации кириллических символов латинскими, - поиск по словам и словосочетаниям с возможностью нечеткого поиска, для поиска ключевых слов, в том числе написанных с ошибками и опечатками; - технология поиска регулярных выражений, используемая для обнаружения фиксированных последовательностей символов, например, номеров паспортов, номеров банковских карт и т.п.; - возможность использования предустановленных регулярных выражений и создания пользовательских; - механизм постпроверки номеров банковских карт по базе платежных систем; - поиск по тематическим словарям с учетом морфологии (возможность отключения) и поддержкой масок и регулярных выражений в словарях, с возможностью настройки порога срабатывания (например, при обнаружении любых 3 из 10 слов или выражений, содержащихся в словаре); - создание цифровых отпечатков документов или папок с документами для последующего обнаружения в перехваченных данных похожих документов – с возможностью указания процента соответствия перехваченного документа оригиналу); - возможность использования предустановленных словарей и создания пользовательских; - технология поиска по цифровым отпечаткам документов с возможностью указания процента соответствия перехваченного документа оригиналу; - технология поиска по цифровым отпечаткам документов с возможностью выбора прямого, обратного либо наибольшего вхождения; - синхронизация банка цифровых отпечатков с папками, в которых располагаются документы, с возможностью настройки интервала обновления - создание цифровых отпечатков CSV-файлов, с выбором полей со значимой информацией для добавления в банк данных; - создание цифровых отпечатков баз данных, при помощи настройки подключения системы к базе данных, для создания цифровых отпечатков определенных полей выбранных таблиц с целью последующего обнаружения утечки информации из этой базы данных (например, при одновременном обнаружении персональных

	данных из связки полей «ФИО + паспортные данные»); - создание и обновление цифровых отпечатков баз данных осуществляется без промежуточных действий, таких как выгрузка базы данных в файл-источник цифрового отпечатка. При внесении изменений в базу данных система автоматически обновляет соответствующие цифровые отпечатки 35. Анализ по атрибутам. - анализ атрибутов документов, таких как «имя документа», «адрес получателя электронной почты», «пользователь», «учетная запись IM-клиента», «дата», «время», «день недели», «размер», «тип данных», «компьютер», «домен», «IP-адрес» и др.; - анализ атрибутов документа по статусам, таким как пересылка документа по защищенному протоколу, шифрованного или защищенного документа, поврежденных данных, отправка вызвавших блокирование данных либо переданных в индивидуальном порядке данных и др.; - анализ атрибутов процессов, таких как: имя исполняющего файла, полный путь к файлу, заголовок окна процесса и др.; - анализ атрибутов перехваченной почты, таких как: отправитель, получатель, число получатель, заголовка письма и др; - анализ атрибутов перехваченной переписки в мессенджерах, таких как: локальный идентификатор пользователя, удаленный идентификатор пользователя, число сообщений, тип данных, и др; - анализ атрибутов контролируемых устройств, таких как: название устройства, производитель, тип устройства, идентификатор производителя, идентификатор продукта, тип устройства, серийный номер и др; - анализ атрибутов печати, таких как: тип документа, название принтера, число распечатанных страниц и др; 36. Статистический анализ - количество отправленных/полученных пользователем электронным письмам - количество переписок/сообщений пользователя - количество/время звонков пользователя в IM-клиентах (например, «время голосовых переговоров пользователя в IM-клиентах за день превысило 1 час» или «пользователь совершил более 10 звонков за день» и т.д.); - количество посещенных веб-страниц; - количество отправленных веб-запросов; - количество распечатанных страниц/документов на принтерах; - количество отправленных/полученных файлов - продолжительность работы в браузерах, том числе на определенных сайтах (например, «Время пребывания пользователя на определенном сайте через браузер превысило 1 час за день» и т.д.); - продолжительность работы в приложениях, в т.ч. в определенных приложениях (например, «пользователь работал в Microsoft Word в течение более 5 часов за день» или «пользователь работал в приложении “Пасьянс Косынка” в течение более 70% рабочего времени» и т.д.); - продолжительность активной работы/бездействия ПК, в том числе в процентах от общего времени (например, «ПК бездействовал в течение более 3 часов за день», «начало активности ПК зафиксировано позже 10:30» и т.д.); - Должна быть предусмотрена возможность настройки автоматических уведомлений об отклонении от нормы начала/окончания рабочего, от нормы продолжительности активной работы за ПК «продолжительность рабочего дня». 37. Событийный анализ. Возможность

	настройки автоматических уведомлений в следующих случаях: - регистрация запуска, завершения работы пользователем определенного приложения; - обнаружение пересылки зашифрованного вложения (например, защищенный паролем документ MS Office или архив); - копирование файлов с контролируемых компьютеров на внешние накопители, облачные хранилища и сетевые диски с определенными параметрами; - подключение и использования на контролируемых рабочих станциях устройств с определенными параметрами; - посещение определенных web-ресурсов; - блокирование пересылки данных по протоколам SMTP, HTTP, MAPI, отправки документов на печать, в том числе по дополнительным атрибутам; - обнаружение конфиденциальных файлов на компьютерных дисках пользователей; - выявление факта пересылки документа с измененным расширением (например, при переименовании пользователем файла .doc в .jpg и последующей отправкой, система должна быть в состоянии определить оригинальный формат файла и извлечь из него текст для контентного анализа, дополнительно уведомив ответственного сотрудника о самом факте изменения расширения). 38. Требования к отчетности. Все перехваченные данные должны представляться в форме отчетов следующих видов: а) Отчётность рабочего дня пользователя должна содержать: •информацию о количестве отправленных и полученных пользователем писем с разбивкой по часам; •информацию о количестве сессий переписки пользователя в IM-клиентах с указанием длительности и количества сообщений в каждой сессии переписки; •информацию о количестве файлов, полученных и отправленных пользователем по электронной почте, через IM-клиенты, по протоколам HTTP(S) и FTP(S), скопированных на внешние устройства, сетевые ресурсы, в облачные хранилища или распечатанных на локальных/сетевых принтерах – с разбивкой по часам; •информацию о количестве посещенных URL и отправленных запросов – с разбивкой по часам; •информацию о количестве сделанных системой снимков экрана рабочего стола пользователя – с разбивкой по часам; •информацию о времени работы/простоя компьютера пользователя, детальную статистику активности приложений и данные о процентном соотношении времени работы в различных приложениях; • информацию о количестве документов, помещенных в буфер обмена – с разбивкой по часам; •информацию о посещении веб-сайтов с помощью веб-браузера с разбивкой по часам с предоставлением комплексной и детальной статистики времени, проведенного на различных веб-ресурсах; •информацию о количестве символов, введенных пользователем с клавиатуры с разбивкой по часам. Фотография рабочего дня пользователя должна являться интерактивным и динамическим отчетом, что должно позволять осуществлять переход по ссылкам непосредственно к просмотру содержимого перехваченных документов либо веб-ссылок. Должна быть обеспечена возможность экспорта фотографии рабочего дня во внешний HTML – файл, Outlook-файл либо в файл исходного формата с поддержкой интерактивности структурных элементов и доступом к перехваченным данным через

	веб-браузер. b) Графики по типам информации. Система должна представлять данные, собранные по определенному пользователю за конкретный интервал времени, в виде графиков по отдельным типам информации (график по отправленным/полученным письмам, по количеству сессий/сообщений переписок в IM-клиентах, по количеству полученных и отправленных файлов, количеству посещенных URL и веб-запросов). Графики по типам информации должны поддерживать интерактивность и динамичность, поддерживать возможность перехода по ссылкам (точкам на графике) непосредственно к просмотру содержимого перехваченных документов. c) Граф-анализатор взаимосвязей пользователей. Система должна обладать возможностью графического отображения взаимосвязей пользователя (в виде графа либо матрицы) на основании собранной по нему информации для наглядного представления круга абонентов (как внутренних, так и внешних), с которыми данный пользователь обменивался какой-либо информацией в течение выбранного интервала времени. Должна быть обеспечена поддержка группировки контактов пользователя по принадлежности к установленным и не распознанным контактам. Возможность просмотра взаимосвязей внешнего абонента с пользователями сети организации после предварительного создания карточки внешнего пользователя. Возможность выбора масштаба отображения отчета при просмотре в клиентской консоли (с указанием % размера от оригинала). Возможность интерактивного перехода от просмотра схемы взаимосвязей к содержимому документов (письма, переписки, файлы и т.д.), которыми пользователь обменивался с конкретным абонентом. Поддержка сохранения отчета о взаимосвязях в виде графа во внешний файл формата PNG. d) Сводная отчетность Система должна выполнять ежедневное автоматическое обновление отчетов с поддержкой перестроения отчетов вручную пользователем. Система должна поддерживать интерактивность количественных данных - возможность прямого перехода к списку результатов по выбранному показателю. Поддержка автоматической рассылки отчетов согласно расписанию на электронную почту указанным подписчикам. Экспорт отчетов во внешний файл. 39. Отчет по пользователю должен реализовывать следующие требования: Возможность построения сводного интерактивного отчета по определенному пользователю за все время наблюдения (или за выбранный интервал времени), включающего следующую информацию: a) статистику перехвата данных, в т.ч.: •количество переданной и полученной пользователем информации по всем каналам передачи, включая почту и мессенджеры; •количество посещенных сайтов и поисковых запросов; •количество файлов, переданных/принятых по FTP; •количество распечатанных документов и страниц; •количество операций копирования в буфер обмена; •количество снятых скриншотов; •количество файлов, переданных на внешние накопители/сетевые ресурсы/облачные хранилища; •количество нажатых клавиш клавиатуры; b) информацию об активности пользователя за компьютером, в т.ч.: •общее время активной работы пользователя за ПК; •среднесуточное время активной

	работы пользователя за ПК; •общее время простоя ПК; •среднесуточное время простоя ПК; •общее время присутствия сотрудника на работе; •среднесуточное время присутствия сотрудника на работе; •среднее время начала работы; •среднее время окончания работы; •общее количество рабочих дней; •календарь учета рабочих дней сотрудника с указанием времени начала/окончания работы, времени активности/простоя компьютера за каждый день (с цветовым выделением фактов раннего начала работы, начала работы с опозданием, раннего окончания работы, окончания работы с задержкой); •гистограмму по времени активности/простоя компьютера пользователя за каждый день; c) информацию об активности приложений на компьютере пользователя, в т.ч.: •процентное соотношение времени работы в различных приложениях (с построением круговой диаграммы) •полный список запускавшихся приложений с указанием абсолютного времени работы в каждом из них; d) информацию о браузер-активности: •рейтинг посещенных веб-ресурсов; •хронология активности в веб-браузере. e) информацию о количестве зафиксированных инцидентов безопасности, инициированных пользователем, и соответствующих им правилах с различной степенью детализации. 40. Система должна обеспечивать создание сводных отчетов по всем контролируемым пользователям в организации, которые должны удовлетворять следующим требованиям: Возможность построения сводных интерактивных отчетов по контролируемым каналам передачи данных за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, наиболее активно использующих этот канал. Возможность построения сводных отчетов по количеству инцидентов безопасности за все время наблюдения или за выбранный интервал времени с указанием 10 (или любого другого количества) пользователей, активность которых привела к срабатыванию правил безопасности большее количество раз. При создании отчетов должна быть обеспечена возможность учета как общего суммарного, так и среднесуточного значения соответствующих параметров при составлении таких отчетов. Возможность построения сводных интерактивных отчетов о статистических показателях сетевой и локальной активности выбранных пользователей. Система должна обеспечивать возможность построения сводных интерактивных отчетов о статистике срабатывания правил безопасности. При этом система должна обеспечивать просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям с выбором детализации по дням, месяцам, за произвольный временной промежуток и просмотр итогового количества срабатываний по каждому правилу в отдельности и по всем существующим правилам безопасности. 41. Система должна обеспечивать создание отчетов по браузер-активности по топ 20 пользователям в организации, которые должны удовлетворять следующим требованиям: Возможность построения отчета по определенным сотрудникам по посещенным веб-ресурсам за за выбранный интервал времени с указанием 10 (максимум 20) пользователей,

	наиболее активно использующих этот канал. При создании отчета должна быть обеспечена возможность учета как категорий сайтов (социальные сети, видеохостинги и т.д.) так и по продуктивности. При этом, по умолчанию имеется 3 категории продуктивности: непродуктивно, нейтрально, продуктивно. Также система должна обеспечивать возможность создания отчета по выбранным категориям у определенных пользователей. 42. Система должна обеспечивать создание отчетов «табелей рабочего времени», по всем контролируемым пользователям в организации, которые должны удовлетворять следующим требованиям: Возможность построения отчета по определенным временным промежуткам, таким как: текущий календарный месяц, предыдущий календарный месяц либо выбирать конкретный месяц. При этом система должна обеспечивать просмотр отклонений от рабочего графика, данные которого (начало и конец) должны иметь возможность редактирования. 43. Мониторинг работоспособности системы. Система должна поддерживать: - панель мониторинга работоспособности системы, на которой представлена основная информация о работе всех основных компонентов системы, а также использовании ресурсов оборудования - ведение журнала событий серверных компонентов системы; - просмотр журнала, а также детальной информации и рекомендаций по каждому событию в консоли администратора; - фильтрация событий в журнале по дате, уровню события (информация, предупреждение, ошибка), серверному компоненту, источнику событий; - выбор определенных серверов источников событий для ведения мониторинга; - автоматическая очистка журнала по сроку хранения событий и их уровню; - возможность экспорта журнала событий в форматах PDF, XPS, CSV, XLS, XLSX, HTML, RTF, TXT - возможность печати журнала событий; - автоматическое уведомление администратора системы о новых событиях серверных компонентов по почте; - настройка правил отправки уведомлений по почте (выбор адресата, серверного компонента, уровня события или конкретных событий). 44. Систем должна фиксировать сведения о всех наиболее существенных событиях в работе серверных компонентов в журнале операционной системы рабочей станции, на которой они установлены. 45. Масштабируемость системы. В зависимости от конфигурации сети, от объема обрабатываемых перехваченных данных и других параметров, система должна гибко масштабироваться для обеспечения контроля большой и сложно организованной сети, а также распределения нагрузки на сетевые и аппаратные ресурсы: Ориентация работы всех компонентов системы на многопоточность Система должна обеспечивать полную поддержку распределения нагрузки в многоядерных и многопроцессорных системах. 46. Удобство администрирования. Централизованное управление компонентами системы из двух консолей: единая консоль администратора и единая консоль пользователя (сотрудника службы ИБ). Система должна обеспечивать возможность создания резервной копии конфигурации всех серверных компонентов с поддержкой последующего восстановления настроек серверов через консоль

	администратора. 47. Политика лицензирования ПО. Система должна лицензироваться в соответствии с количеством контролируемых пользователей. При этом недопустимо использование жесткой привязки лицензии к конкретным рабочим станциям или пользователям. Количество приобретенных лицензий должно определять только количество одновременно контролируемых пользователей, при этом сам список контролируемых может быстро и гибко изменяться в случае необходимости (например, при наличии 100 пользователей в сети и только 50 лицензий – возможность контролировать выборочно сначала одних пользователей, затем других; при этом переназначение лицензионных слотов должно быть возможно не реже 1 раза в сутки). Система лицензирования должна предусматривать возможность покомпонентной поставки, т.е. выбора типов контролируемых данных и отключения неиспользуемого функционала на уровне лицензии. 48. Доступ к службе поддержки. •Техническая поддержка по времени 8*5 (8 часов 5 дней в неделю – в рабочее время по рабочим дням по местному времени GMT +5); •Обращение на поддержку через телефон и интернет-каналы; •Количество обращений – неограниченное; •Время реагирования не более 4 (четырех) часов (в период часового покрытия). 5.3. Поставщик должен выполнить следующие обязательные этапы: 5.3.1. Развертывание серверных компонентов и баз данных. 5.3.1.1. Установка серверной части системы 5.3.1.2. Оптимизация параметров баз данных для обеспечения высокой скорости полнотекстового поиска и надежного хранения теневых копий перехваченных файлов и архивов. 5.3.1.3. Настройка автоматического резервного копирования (backup) конфигурации системы и накопленных журналов событий. 5.3.2. Интеграция с ИТ-инфраструктурой Заказчика 5.3.2.1. Интеграция комплекса с корпоративной службой каталогов (при наличии). 5.3.2.2. Настройка зеркалирования трафика. 5.3.3. Развертывание клиентских модулей (агентов). 5.3.3.1. Централизованное (скрытое) развертывание агентского программного обеспечения на рабочих станциях пользователей (согласно количеству закупленных лицензий). 5.3.3.2. Настройка параметров скрытности агентов и защиты их от несанкционированного удаления, остановки служб или изменения конфигурации пользователями. 5.3.4. Настройка политик информационной безопасности. 5.3.4.1. Создание и адаптация базовых политик безопасности (словари, регулярные выражения, цифровые отпечатки документов) для выявления передачи конфиденциальной информации, персональных данных, сканов печатей и подписей. 5.3.4.2. Настройка правил контроля использования внешних накопителей (USB-флешек) с возможностью теневого копирования записываемых файлов и создания «белых списков» разрешенных устройств. 5.3.4.3. Настройка контроля буфера обмена, вывода документов на печать и передачи файлов через публичные мессенджеры и облачные хранилища. 5.3.4.4. Настройка автоматических уведомлений. 5.3.5. Запуск системы в режиме «аудита/мониторинга» для сбора первоначальной статистики и выявления легитимных бизнес-процессов Заказчика. 5.3.6. Перевод

	системы в режим «активного предотвращения/блокировки» по согласованным с Заказчиком каналам передачи данных. 5.4. Поставщик должен выполнить комплекс задач по развёртыванию и пусконаладке антивирусного программного обеспечения. 5.4.1. Поставщик обязан поставить неисключительные лицензии на право использования специализированного программного обеспечения централизованной антивирусной защиты конечных точек и выполнить комплекс задач по его установке, конфигурации не менее чем на 300 рабочих станциях Заказчика. 5.4.2. Поставляемое программное обеспечение должно обладать клиент-серверной архитектурой с единой консолью централизованного мониторинга и управления политиками безопасности, включать модули сигнатурного, эвристического и проактивного поведенческого анализа угроз в режиме реального времени, защиту от программ-вымогателей, руткитов, вредоносного и шпионского ПО, систему обнаружения и предотвращения сетевых атак и сетевой экран конечной точки, средства контроля веб-трафика и почтовых сообщений, модуль контроля запуска приложений, а также модуль контроля подключения и использования внешних съемных электронных носителей информации и периферийных интерфейсов. Агенты антивирусной защиты должны обладать встроенными механизмами самозащиты от несанкционированного изменения конфигурации, выгрузки служб или удаления локальными пользователями без административных привилегий. 5.4.3. С учетом законодательного требования о разделении сетевых сегментов и запрета прямого сопряжения контуров, Поставщик обязан развернуть 2 (два) автономных сервера управления антивирусной защитой в рамках соответствующей сетевой инфраструктуры Заказчика: для локальной сети внешнего контура и для локальной сети внутреннего контура. 5.5. Поставщик должен внедрить и настроить политики управления информацией в Active Directory для двух независимых сетей Public и Private (не менее 80 пользователей). 5.5.1. В рамках настройки требуется организация централизованного управления пользователями, устройствами и ресурсами, разграничения доступа к информации, соблюдения требований информационной безопасности. 5.5.2. Общие требования к доменной структуре. 5.5.2.1. Использование Active Directory Domain Services (AD DS). 5.5.2.2. Два независимых домена со своими наборами OU и GPO в сетях Public и Private. 5.5.3. Требования к изоляции двух сетей. 5.5.3.1. Каждая сеть Public и Private должна рассматриваться как отдельный контур безопасности. 5.5.3.2. Необходимо провести обязательное разделение пользователей, компьютеров, серверов, групп доступа, групповых политик. 5.5.3.3. Необходимо обеспечить запрет автоматического наследования политик между сетями, и взаимодействие между сетями через заданные политики и группы. 5.5.4. Организация OU (Organizational Units). Поставщик должен провести аналитическую работу по созданию независимой иерархии OU (Organizational Units) для каждой из двух сетей Publlic и Private. 5.5.5. Политики безопасности (Group Policy Objects). Поставщик должен провести

	аналитическую работу по созданию GPO (Group Policy Objects) для каждой из двух сетей Publlic и Private согласно требованиям информационной безопасности включающее: 5.5.5.1. Политики аутентификации и учетных записей. Настройка политик паролей: минимальная длина; сложность; срок действия; история паролей. 5.5.5.2. Политики блокировки учетных записей: количество неудачных попыток; время блокировок. 5.5.5.3. Политики управления пользователями: ограничение прав локальных администраторов, запрет использования встроенной учетной записи Administrator, контроль входа пользователей по времени и типу устройств, настройка User Rights Assignment. 5.5.5.4. Политики управления рабочими станциями и серверами: запрет несанкционированного ПО (Software Restriction Policies / AppLocker); управление обновлениями (WSUS или политики Windows Update); отключение небезопасных служб и протоколов; управление USB-устройствами и съемными носителями; настройка BitLocker (при наличии и необходимости). 5.5.5.5. Политики сетевой безопасности: настройка Windows Firewall с разными профилями для подсетей; ограничение сетевых соединений между подсетями; контроль SMB, RDP, PowerShell Remoting; настройка IPsec (при необходимости). 5.5.6. Политики управления информацией и доступом. Поставщиком должна быть проведена аналитическая работа по созданию политик управления информаций и доступом для каждой из двух сетей Publlic и Private согласно требованиям информационной безопасности включающее: 5.5.6.1. Разграничение доступа к ресурсам: реализация модели RBAC (Role-Based Access Control), использование групп безопасности: доступ к файловым ресурсам; доступ к приложениям; доступ к сервисам, исключение прямых назначений прав пользователям. 5.5.6.2. Управление файловыми ресурсами: настройка NTFS-разрешений по принципу минимально необходимого доступа, использование групп «Read / Modify / Full Control», запрет перекрестного доступа между подсетями, настройка аудита доступа к критичным данным. 5.5.7. Аудит, логирование. Необходимо включить Advanced Audit Policy: 5.5.7.1. вход/выход пользователей; 5.5.7.2. изменения учетных записей; 5.5.7.3. доступ к объектам; 5.5.7.4. изменения GPO. 5.5.8. Поставщик обязан предоставить рабочие и протестированные GPO, документацию, включающую логическую схему AD; описание OU и политик; перечень групп и прав доступа; инструкции для администраторов. 5.5.9. Настройка должна обеспечивать масштабируемость, возможность дальнейшего расширения и соответствие изменённым требованиям информационной безопасности, применимым к государственным органам Республики Казахстан. 6. Требования о неразглашении конфиденциальной информации 6.1. Поставщик обязан обеспечивать конфиденциальность всей информации, ставшей ему известной при проведении работ, включая сведения об информационных системах, локально-вычислительной сети, архитектуре сетевой инфраструктуры, средствах и событиях информационной безопасности, учетных записях, параметрах настройки оборудования и программного обеспечения,

	адресном пространстве сети, схемах подключения, эксплуатационной документации, а также иной служебной, технической, организационной и ограниченной к распространению информации Заказчика. 6.2. Поставщик не вправе без письменного согласия Заказчика разглашать, передавать третьим лицам, публиковать, копировать, тиражировать, использовать в личных или коммерческих целях, а также иным образом распространять полученную в рамках исполнения договора информацию, за исключением случаев, прямо предусмотренных законодательством Республики Казахстан. 6.3. Поставщик обязан обеспечить доступ к указанной информации только тем своим работникам и привлеченным специалистам, которым такой доступ необходим исключительно для исполнения обязательств по договору. 6.4. Поставщик обязан принимать необходимые организационные и технические меры по защите конфиденциальной информации от несанкционированного доступа, копирования, изменения, уничтожения, блокирования и распространения, в том числе при удаленном подключении, обмене файлами, использовании съемных носителей информации, учетных данных и средств администрирования. 6.5. Полученные от Заказчика документы, электронные файлы, учетные записи, резервные копии, конфигурации, схемы, журналы событий и иные материалы должны использоваться Поставщиком исключительно в целях исполнения договора и по завершении работ подлежат возврату Заказчику либо уничтожению по требованию Заказчика, если иное не предусмотрено условиями договора или законодательством Республики Казахстан. 6.6. В случае выявления факта утраты, разглашения, несанкционированного доступа либо иной компрометации конфиденциальной информации Поставщик обязан незамедлительно, но не позднее 1 рабочего дня с момента выявления, письменно уведомить Заказчика о таком факте, его причинах, затронутом объеме информации и принятых мерах по минимизации последствий. 7. Дополнительные требования 7.1. В связи с тем, что предмет закупки включает установку, монтаж, настройку, интеграцию и ввод в эксплуатацию взаимосвязанных компонентов сетевой инфраструктуры и информационной безопасности, в том числе серверного оборудования, маршрутизаторов, коммутаторов, беспроводных точек доступа, кабельной подсистемы, средств электропитания, а также программного обеспечения предотвращения утечек информации, Поставщик должен обеспечить централизованное управление выполнением задач на всех этапах реализации проекта. Для координации сроков поставки, организации последовательности монтажных и пусконаладочных работ, управления рисками простоев действующей инфраструктуры Заказчика, согласования этапов переключения сервисов, контроля исполнения графика, взаимодействия с ответственными представителями Заказчика, а также обеспечения своевременной подготовки исполнительной документации Поставщика должен организовать управление ходом выполнения задач в соответствии с международными методологиями проектного менеджмента. 7.2. Поставщик в рамках реализации проекта должен выполнить комплекс задач по анализу и

	регламентации процессов обработки информации в учреждениях, расположенных в административном здании Заказчика. 7.2.1. Поставщик должен провести анализ текущих («as is») процессов обработки и передачи информации в учреждениях Заказчика, включая: 7.2.1.1. использование электронной почты, мессенджеров, веб ресурсов и облачных сервисов; 7.2.1.2. работу с файлами на локальных рабочих станциях, сетевых ресурсах и внешних носителях; 7.2.1.3. печать документов на локальных и сетевых принтерах; 7.2.1.4. особенности взаимодействия между подразделениями и внешними контрагентами. 7.2.2. На основании проведённого анализа Поставщик должен сформировать требования к политике информационной безопасности и предотвращения утечек информации для дальнейшей настройки программного обеспечения, включая: 7.2.2.1. перечень категорий информации (конфиденциальная, служебная, персональные данные и др.), подлежащих контролю; 7.2.2.2. допустимые и недопустимые каналы передачи данных для каждой категории; 7.2.2.3. требования к блокированию, разрешению и согласованию операций (отправка, копирование, печать, запись на носители и т.п.). 7.3. Поставщик должен разработать (актуализировать) техническую документацию по информационной безопасности. 7.3.1. Поставщик должен разработать комплект документов, который включает Политику информационной безопасности (основной документ организации), Инструкции по администрированию и обслуживанию телекоммуникационного оборудования организации, формы журналов учета, листов ознакомления сотрудников организации с правилами ИБ. Также Поставщик должен оказывать консультативную помощь при разработке прочих документов и процедур ИБ организации. 7.3.2. Необходимо провести следующие этапы: 7.3.2.1. Анализ текущего состояния информационной безопасности Заказчика. 7.3.2.2. Написание текстов документов с учетом специфики бизнес-процессов Заказчика. 7.3.2.3. Передача черновиков документов Заказчику, сбор замечаний и их доработка. 7.3.2.4. Подготовка финального комплекта документов в электронном (и при необходимости печатном) виде. 7.3.3. Документы должны быть разработаны на русском языке, в редактируемом формате (DOCX, XLSX). 7.3.4. Документы должны соответствовать действующим нормативно-правовым актам в сфере ИБ РК. 7.3.5. Если документ требует периодического заполнения, то Поставщик должен предоставить шаблоны таких документов. 7.3.6. Минимальный перечень документов: 7.3.6.1. Политика информационной безопасности 7.3.6.2. Методика оценки рисков информационной безопасности 7.3.6.3. Правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации 7.3.6.4. Правила проведения внутреннего аудита ИБ 7.3.6.5. Правила использования средств криптографической защиты информации 7.3.6.6. Правила организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам 7.3.6.7. Правила организации антивирусного контроля, использования мобильных устройств, носителей

	информации, Интернета и электронной почты 7.3.6.8. Правила организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации 7.3.6.9. Руководство администратора по сопровождению объекта информатизации, резервному копированию и восстановлению информации 7.3.6.10. Инструкцию о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях 7.3.6.11. Документирование процедуры утилизации и(или) подготовки к повторному использованию серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций, носителей информации (например, акты, приказы или другое) 7.3.6.12. Документальная стратегия или процесс, обеспечивающий непрерывность ИБ в организации 7.3.6.13. План (процедур и процессов) обеспечения непрерывности ИБ и бизнес-процессов и восстановления после внештатной (кризисной) ситуации 7.3.6.14. Документы фиксирующие выполнение процедур резервного копирования информации (например, акты, протоколы и прочее) 7.3.6.15. Документы фиксирующие тестирование резервных копий (например, акты, протоколы и прочее) 7.3.6.16. Утвержденный перечень портов управления сетевого оборудования 7.3.6.17. Документированная утвержденная схема локальной сети 7.3.6.18. Документирование каталога угроз (рисков) активов, связанных со средствами обработки информации 7.3.6.19. Документирование утвержденного плана обработки рисков 7.3.6.20. Документированная схема ведомственной (корпоративной) сети телекоммуникаций 7.3.6.21. Документирование кабельных соединений 7.3.6.22. Документированные процедуры установки (обновления) (ПО (прикладного и системного)) (например, акты, журналы, реестры и прочее) 7.3.6.23. Регламентирование процедуры управления сетевым оборудованием 7.4. В составе конкурсной заявки Потенциальному Поставщику необходимо предоставить сертификат соответствия программного продукта «Программное обеспечение предотвращения утечек информации» требованиям СТ РК ISO/IEC 15408-3-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты». Оценочный уровень доверия не ниже 5. 8. Результат проведения работ. 8.1. По итогам проведения работ Поставщик должен обеспечить установку, монтаж, настройку, интеграцию, пусконаладку программно-аппаратного комплекса информационной безопасности и модернизацию сетевой инфраструктуры Заказчика в полном объеме, предусмотренном технической спецификацией. Результатом работ должно являться создание работоспособной, настроенной и готовой к эксплуатации инфраструктуры, включающей серверное оборудование, маршрутизаторы, коммутаторы, беспроводные точки доступа, средства электропитания, программное обеспечение информационной безопасности, а также иные предусмотренные спецификацией компоненты. 8.2. В результате проведения работ оборудование должно быть физически установлено в предусмотренных местах

	размещения, подключено к линиям электропитания и передачи данных, проверено на работоспособность и интегрировано в действующую инфраструктуру Заказчика. Все серверы, маршрутизаторы, коммутаторы, точки доступа, источники бесперебойного питания и иные устройства, входящие в состав поставки, должны быть смонтированы, включены в общую схему взаимодействия и переведены в состояние штатной эксплуатации. 8.3. Серверное оборудование по итогам проведения работ должно быть установлено в телекоммуникационные шкафы, подключено к электропитанию, настроено на базовом системном уровне и подготовлено к эксплуатации в составе комплекса. Дисковые подсистемы, RAID-массивы, интерфейсы управления, сетевые параметры и иные предусмотренные технической спецификацией настройки должны быть выполнены Поставщиком в объеме, достаточном для надежной и бесперебойной работы серверов. 8.4. Сетевое оборудование должно обеспечивать штатное функционирование локально-вычислительной сети Заказчика, включая сегментацию сети, маршрутизацию, отказоустойчивость, коммутацию, авторизацию устройств и подключение оконечных узлов. На маршрутизаторах и коммутаторах должны быть выполнены необходимые настройки интерфейсов, VLAN, маршрутов, механизмов управления доступом, политик качества обслуживания, защищенного администрирования и иных параметров, предусмотренных технической спецификацией. 8.5. Беспроводная сеть по итогам проведения работ должна быть развернута, настроена и введена в эксплуатацию в предусмотренных зонах покрытия. Точки доступа должны быть смонтированы, подключены по сети передачи данных и электропитанию, включены в централизованное управление, настроены по параметрам радиосети, безопасности, SSID и VLAN, а также обеспечивать устойчивое беспроводное подключение пользовательских устройств в пределах предусмотренной зоны обслуживания. 8.6. Программное обеспечение предотвращения утечек информации и контроля каналов передачи данных должно быть установлено, активировано, интегрировано с инфраструктурой Заказчика и настроено в соответствии с функциональными требованиями технической спецификации. По итогам проведения работ должна быть обеспечена работоспособность серверной части системы, взаимодействие с сетевой инфраструктурой, службой каталогов, почтовыми и иными информационными сервисами (при необходимости), а также функционирование политик мониторинга, регистрации, анализа и предотвращения инцидентов информационной безопасности. 8.7. При передаче результата работ Заказчику при наличии должны быть переданы все необходимые для дальнейшей эксплуатации сведения и материалы, включая логины, пароли, ключи доступа, сведения о лицензиях, серийных номерах, гарантийных обязательствах и технической поддержке. 8.8. Окончательным результатом исполнения договора должно являться создание единой функционирующей инфраструктуры, обеспечивающей сетевое взаимодействие, эксплуатацию серверных и беспроводных компонентов, а также выполнение задач информационной безопасности в пределах требований

	настоящей технической спецификации. Срок исполнения до 31 декабря 2027 года.
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	