

**Сатып алынатын қызметтердің Техникалық ерекшелігі
(тапсырыс беруші толтырады)**

Тапсырыс берушінің атауы:	Астана қаласы әкімдігінің "Қалалық мониторинг және жедел әрекет ету орталығы" шаруашылық жүргізу құқығындағы мемлекеттік коммуналдық кәсіпорны
Ұйымдастырушының атауы:	Астана қаласы әкімдігінің "Қалалық мониторинг және жедел әрекет ету орталығы" шаруашылық жүргізу құқығындағы мемлекеттік коммуналдық кәсіпорны
Конкурстың №:	№ 17856902-1
Конкурстың атауы:	Деректер жоғалуының алдын алу бағдарламалық құралын алу және орналастыру қызметі
Лоттың нөмірі:	№ 83033478-OK2
Лоттың атауы	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы:	801019.000.000010
Қызметтің атауы:	Ақпараттық қауіпсіздікті қамтамасыз ету бойынша қызметтер
Өлшем бірлігі:	Бір қызмет
Саны (көлемі):	1
Қосылған құн салығын есептемегенде бірлік бағасы:	6741181
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома:	6741181
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс:	
Қызмет көрсету мерзімі	Техникалық ерекшелікке сәйкес
Аванстық төлем мөлшері:	0

Кепілдік мерзімі (айлармен)	12
--------------------------------	----

Талап етілетін сипаттамалардың, параметрлердің және өзге де бастапқы деректердің сипаттамасы	1. Сипаттамасы және қажетті функционалы: 1.1. Бағдарламалық кешен мынадай компоненттерден тұруы тиіс: • Бақыланатын жұмыс станциялары мен серверлерге орнатылатын пайдаланушылық бөлік (агент). • Деректерді орталықтандырылған қабылдауды, өңдеуді және сақтауды қамтамасыз ететін серверлік бөлік. • Жүйе параметрлері мен агенттерді басқаруға арналған әкімшілік консолі. • Жиналған ақпаратты талдауға және инциденттерді тергеуге арналған деректерді қарау консолі. Агенттік бөлік бақыланатын компьютердегі пайдаланушылардың әрекеттері туралы ақпаратты жинауды және жинақтауды қамтамасыз етуі тиіс. Жиналған деректерді уақытша сақтау қорғалған каталогта шифрланған түрде жергілікті жүзеге асырылуы тиіс. Деректер серверге жіберілгеннен кейін жергілікті көшірмелер автоматты түрде жойылуы тиіс. Бағдарламалық кешен деректерді жинау және жіберу жиілігін баптауды қолдауы тиіс. Агент пен сервер арасындағы өзара әрекеттесу шифрлауды пайдалана отырып, қорғалған байланыс арналары арқылы жүзеге асырылуы тиіс. Агенттермен өзара әрекеттескен кезде серверлік бөлікті авторизациялау үшін пароль орнату мүмкіндігі қолдау табуы тиіс. Бағдарламалық кешеннің серверлік бөлігі Windows және Linux операциялық жүйелерінде орналастыруды қолдауы тиіс. Linux үшін Docker контейнері арқылы пайдалану мүмкіндігі қамтамасыз етілуі тиіс. Жүйенің пайдаланушылық интерфейсі Nginx веб-серверін пайдалана отырып, web-интерфейс арқылы ұсынылуы тиіс. 1.2. Пайдаланушылардың әрекеттерін мониторингілеу ішкі жүйесі Бағдарламалық кешен бақыланатын компьютерлердегі пайдаланушылардың әрекеттері туралы ақпаратты, соның ішінде мыналарды тіркеуді және сақтауды қамтамасыз етуі тиіс: • пернетақтадағы пернелердің басылуын тіркеу; • кесте бойынша және белсенді терезе ауысқан кезде экран суреттерін (скриншоттарды) жасау; • скриншоттардың сапасы мен түс режимін (түрлі-түсті/ақ-қара) баптау; • жекелеген қолданбалар үшін скриншот жасаудың жеке жиілігін баптау; • бағдарламалардың іске қосылуы мен аяқталуын тіркеу; • қолданбалардың ашылуы мен жабылуын іске қосу уақытын, бағдарлама атауын, терезе тақырыбын және орындалатын файлға дейінгі жолды белгілей отырып тіркеу; • тыйым салынған қолданбалардың іске қосылуын бұғаттау; • іздеу жүйелеріндегі іздеу сұрауларын тіркеу; • қаралған web-ресурстарды тіркеу; • браузерлердегі белсенділікті мыналарды белгілей отырып тіркеу: о қаралған ресурстың URL мекенжайы; о web-ресурстың санаты; о қарау уақыты; о терезе тақырыбы; о сеанстың ұзақтығы; о пайдаланушы аты; • пайдаланушылардың әлеуметтік желілердегі белсенділігін тіркеу; • Интернет желісіне жүктелетін файлдарды тіркеу; • компьютердің қосылу және өшу оқиғаларын тіркеу; • пайдаланушылардың операциялық жүйеге кіруін және одан шығуын тіркеу; • жұмыс станциясының бұғатталуын және пайдаланушының бос тұру кезеңдерін тіркеу. 1.3. Коммуникацияларды бақылау ішкі жүйесі Бағдарламалық кешен пайдаланушылардың коммуникациялық белсенділігін, соның ішінде Тапсырыс берушіге тиесілі қызметтік құрылғыларда (ноутбуктерде, дербес компьютерлерде,
--	--

	смартфондарда) жүзеге асырылатын коммуникациялық белсенділікті ұстап алуды және тіркеуді қамтамасыз етуі тиіс. • POP3, POP3S, SMTP, SMTPS және IMAP протоколдары бойынша электрондық поштаның кіріс және шығыс хабарламаларын ұстап алу; • электрондық пошта тіркемелерін сақтау; • мынадай мессенджерлердегі мәтіндік хат алмасуды сақтау: o WhatsApp Web; o Telegram Web; o Telegram Desktop; o Viber; o Яндекс Мессенджер Web; o AITU Web; • дауыстық хабарламаларды сақтау; • AITU мессенджерінің web-нұсқасындағы хат алмасуды ұстап алу; • әлеуметтік желілер арқылы жіберілетін хабарламаларды тіркеу; • web-пошта арқылы жүргізілетін хат алмасуды тіркеу. 1.4. Мессенджерлерді мониторингілеу ішкі жүйесі Бағдарламалық кешен қолдау көрсетілетін мессенджерлердегі хабарламаларды мынадай параметрлерді көрсете отырып тіркеуді қамтамасыз етуі тиіс: • хабарламаның күні мен уақыты; • мессенджердің атауы; • әңгімелесуші (чат, топ немесе пайдаланушы); • хабарлама түрі; • хабарлама мәтіні немесе жіберілген файлдың мазмұны; • бақыланатын компьютер пайдаланушысының аты. Ішкі жүйе хабарламалардың мынадай түрлерін тіркеуді қамтамасыз етуі тиіс: • кіріс хабарламалар (incoming); • шығыс хабарламалар (outgoing). Хабарламаларды қарау интерфейсі мыналарды қамтамасыз етуі тиіс: • деректерді кілт сөз бойынша сүзу; • журнал бағандары бойынша сүзу; • таңдалған бағанды топтау аймағына көшіру арқылы деректерді топтау; • деректерді таңдалған бағандар бойынша сұрыптау; • көрсетілетін деректерді сыртқы файлға экспорттау. Хабарламалар журналында мынадай бағандар көрсетілуі тиіс: • Уақыты; • Мессенджер; • Әңгімелесуші; • Хабарлама түрі; • Хабарлама мәтіні/файл; • Пайдаланушы аты. 1.5. Файлдық операцияларды бақылау ішкі жүйесі Бағдарламалық кешен файлдық жүйенің мониторингін мынадай оқиғаларды тіркей отырып қамтамасыз етуі тиіс: • файлдарды құру; • файлдарды өзгерту; • файлдардың атын өзгерту; • файлдарды жою. Өрбір оқиға үшін мыналар тіркелуі тиіс: • операцияның күні мен уақыты; • операция түрі; • файлға дейінгі толық жол; • файл өлшемі; • MD5 бақылау сомасы (бар болса); • пайдаланушы аты. Қосымша жүйе мыналарды қамтамасыз етуі тиіс: • желілік ресурстармен жүргізілетін операцияларды бақылау; • ортақ каталогтармен жүргізілетін операцияларды тіркеу; • бағдарламалық қамтамасыз етудің орнатылуы мен жойылуын тіркеу; • бақыланатын компьютердің аппараттық конфигурациясындағы өзгерістерді, соның ішінде процессорды, жедел жадты және жинақтауыштарды тіркеу. 1.6. Алмасу буферін бақылау ішкі жүйесі Бағдарламалық кешен алмасу буферінің мазмұнын мынадай параметрлерді тіркей отырып ұстап алуды қамтамасыз етуі тиіс: • оқиға уақыты; • белсенді терезенің тақырыбы; • деректер түрі (мәтін, файл, сурет және т.б.); • алмасу буферінің мазмұны. Жүйе ұсталған деректерді қарау консолі операторының жұмыс станциясына сақтау мүмкіндігін қамтамасыз етуі тиіс. 1.7. Басып шығаруды бақылау ішкі жүйесі Бағдарламалық кешен мыналарды қамтамасыз етуі тиіс: • құжаттарды басып шығару фактілерін тіркеу; • басып шығару параметрлерін
--	--

	тіркеу; • басып шығарылған құжаттың электрондық бейнесін PDF форматында сақтау. 1.8. Құрылғылар мен сыртқы тасымалдағыштарды бақылау ішкі жүйесі Бағдарламалық кешен мыналарды қамтамасыз етуі тиіс: • USB-жинақтауыштардың қосылуы мен ажыратылуын анықтау; • қосылатын құрылғылардың параметрлерін тіркеу; • алынбалы тасымалдағыштарға көшірілетін файлдардың көлеңкелі көшірмелерін жасау; • USB-жинақтауыштардың қосылуын бұғаттау; • мынадай сыныптағы құрылғылардың қосылуын бұғаттау: o USB Mass Storage; o CD/DVD-ROM; o Floppy Drive; • сенімді USB-құрылғылар тізімін жүргізу; • тек рұқсат етілген тізімге енгізілген құрылғылармен жұмыс істеуге рұқсат беру; • барлық басқа USB-жинақтауыштарды бұғаттау. 1.9. Бұлттық сервистерді бақылау ішкі жүйесі Бағдарламалық кешен мыналарды қамтамасыз етуі тиіс: • бұлттық сақтау орындары клиенттерінің пайдаланылуын анықтау; • бұлттық сервистер клиенттерін бұғаттау; • бұлттық сақтау орындарына жіберілетін файлдардың көлеңкелі көшірмелерін жасау. 1.10. Қашықтан басқару ішкі жүйесі Бағдарламалық кешен қашықтан әкімшілендірудің мынадай функцияларын қамтамасыз етуі тиіс: • агентті қашықтан іске қосу және тоқтату; • мониторингті қашықтан қосу және өшіру; • оқиғалар журналдарын мәжбүрлі түрде синхрондау; • іске қосылған процестер тізімін алу; • орнатылған бағдарламалық қамтамасыз ету тізімін алу; • қосылған жабдық тізімін алу; • пайдаланушыларға мәтіндік хабарламалар жіберу; • агенттерді қашықтан орнату; • агенттерді қашықтан жою; • агенттерді Active Directory топтық саясаттары арқылы MSI және EXE пакеттері көмегімен орналастыру. 1.11. Қашықтан қолжетімділік ішкі жүйесі Бағдарламалық кешен мыналарды қамтамасыз етуі тиіс: • бақыланатын компьютерлердің экрандарын нақты уақыт режимінде қарау; • жұмыс үстелін қашықтан басқару; • қашықтан сеанс кезінде жұмыс станциясының басқаруын өзіне алу мүмкіндігі. 1.12. Агенттерді диагностикалау ішкі жүйесі Бағдарламалық кешен агенттік модульдердің жай-күйін мына мүмкіндіктермен бақылауды қамтамасыз етуі тиіс: • барлық агенттерді көрсету; • байланыссыз агенттерді көрсету; • байланыстың болмаған күндер саны бойынша сүзу. Әрбір агент үшін мынадай параметрлер көрсетілуі тиіс: • компьютер атауы; • MAC-мекенжайы; • IP-мекенжайы; • серверпен соңғы байланыс уақыты; • деректердің соңғы берілу уақыты. 1.13. Хабарландыру және әрекет ету ішкі жүйесі Бағдарламалық кешен әкімшілерге мынадай оқиғалар туралы белсенді хабарлауды қамтамасыз етуі тиіс: • USB-тасымалдағыштардың қосылуы мен ажыратылуы; • бағдарламаларды орнату және жою; • файлдарды алынбалы тасымалдағыштарға көшіру; • web-пошта арқылы хабарламалар жіберу; • қауіпсіздік саясаттарын бұзу; • компьютерлердің аппараттық конфигурациясының өзгеруі. Қолдау көрсетілетін хабарландыру арналары: • деректерді қарау консолі; • электрондық пошта; • Telegram. 1.14. Желілік қолжетімділікті бақылау ішкі жүйесі Бағдарламалық кешен желілік қолжетімділік оқиғаларын мынадай параметрлерді көрсете отырып тіркеуді қамтамасыз етуі тиіс: • оқиғаның күні мен уақыты; • пайдаланушы
--	--

	аты; • компьютер атауы; • оқиға түрі. Қолдау көрсетілетін оқиға түрлері мыналарды қамтуы тиіс: • қосылымның басталуы; • қосылымның аяқталуы. Ішкі жүйе мыналарды қамтамасыз етуі тиіс: • тіркелген оқиғаларды кілт сөз бойынша сүзу; • деректерді бағандар бойынша сұрыптау; • тіркелген оқиғаларды сыртқы файлға экспорттау. 1.15. Мінез-құлықтық талдау ішкі жүйесі Бағдарламалық кешен жиналған деректерді талдау негізінде пайдаланушылардың стандартты емес белсенділігін анықтауды қамтамасыз етуі тиіс. Қосымша жүйе мыналарды анықтауды қамтамасыз етуі тиіс: • майнер-бағдарламалар; • жұмыс станцияларының есептеу ресурстарына ауытқушы жүктеме түсіретін бағдарламалар; • пайдаланушылардың әлеуетті қауіпті белсенділігінің өзге де белгілері. 1.16. Іздеу және тергеу ішкі жүйесі Бағдарламалық кешен мыналарды қамтамасыз етуі тиіс: • барлық жиналған деректер бойынша толық мәтінді іздеу; • файлдардың көлеңкелі көшірмелері бойынша іздеу; • электрондық пошта тіркемелері бойынша іздеу; • басып шығаруға жіберілген құжаттар бойынша іздеу; • тұрақты өрнектер бойынша іздеу. Жүйе деректердің мынадай түрлерін іздеуді қолдауы тиіс: • телефон нөмірлері; • паспорттық деректер; • БСН/ЖСН; • банк карталарының нөмірлері; • өзге де пайдаланушылық үлгілер. 1.17. Құпия деректерді қорғау ішкі жүйесі Бағдарламалық кешен мынадай функцияларды қолдайтын құпия каталогтарды құруды қамтамасыз етуі тиіс: • файлдармен тек белгілі бір қолданбаларда жұмыс істеуге рұқсат беру; • файлдарды құпия каталог шегінен тыс көшіруге тыйым салу; • каталог ішіндегі файлдарды өңдеуге рұқсат беру; • деректерді алмасу буферіне көшіруге тыйым салу; • құжаттарды басып шығаруға тыйым салу. 1.18. Цифрлық су таңбалары ішкі жүйесі Бағдарламалық кешен экран бейнесін алу көзін кейіннен анықтау мақсатында бақыланатын компьютерлердің экранында цифрлық су таңбаларын көрсетуді қамтамасыз етуі тиіс. Ішкі жүйе мынадай функцияларды қамтамасыз етуі тиіс: • су таңбаларын жұмыс үстелі мен қолданба терезелерінің үстінде көрсету; • су таңбаларын көрсетуді орталықтандырылған түрде қосу және өшіру; • су таңбасының түрін таңдау: о мәтіндік; о QR-код; • экран бетінде бірнеше QR-кодты бір мезгілде көрсету. «QR-код» түріндегі су таңбалары үшін бағдарламалық кешен деректерді қарау консоліне фотосуретті немесе экран суретін жүктеу арқылы QR-кодты тану мүмкіндігін қамтамасыз етуі тиіс. QR-код танылғаннан кейін мынадай ақпарат көрсетілуі тиіс: • компьютер атауы; • пайдаланушы аты; • QR-кодты қалыптастырудың уақыт аралығы. Алынған ақпарат құпия ақпаратты қамтитын фотосуреттердің немесе экран суреттерінің таратылуына байланысты ақпараттық қауіпсіздік инциденттерін тергеу кезінде бақыланатын компьютер мен пайдаланушыны анықтау үшін пайдаланылуы тиіс. 1.19. Жасанды интеллект ішкі жүйесі Бағдарламалық кешен Интернет желісіне қосылусыз және деректерді сыртқы ақпараттық жүйелерге бермей, деректерді өңдеуді және талдауды, сондай-ақ зияткерлік көмекшінің жұмысын қамтамасыз ететін жасанды интеллекттің жергілікті модельдерін қамтуы тиіс. Пайдаланушы
--	--

	сұрауларын өңдеу, тіркелген деректерді талдау және жауаптарды қалыптастыру бағдарламалық кешен серверінің есептеу ресурстарын пайдалана отырып, жасанды интеллекттің жергілікті модельдерімен орындалуы тиіс. Жасанды интеллект ішкі жүйесінің жұмысы үшінші тарап сервистерінде тіркелуді, телеметрияны жіберуді немесе өңделетін деректерді тапсырыс беруші инфрақұрылымынан тыс жерде сақтауды талап етпеуі тиіс. 1.20. Құжаттарды талдау Ішкі жүйе мәтіндік құжаттарды жасанды интеллект технологияларын пайдалана отырып талдауды қамтамасыз етуі тиіс. Талдау нәтижелері бойынша мыналарға мүмкіндік қамтамасыз етілуі тиіс: • құжат санатын автоматты түрде анықтау; • құпия ақпараттың белгілерін анықтау; • құжаттың қысқаша мазмұнын қалыптастыру; • ақпарат сезімталдығының деңгейін бағалау; • ақпараттық қауіпсіздік саясаттарын қолдану бойынша ұсынымдар қалыптастыру. 1.21. Аудиодеректерді талдау Ішкі жүйе аудиожазбалардағы сөйлеуді автоматты түрде тануды қамтамасыз етуі тиіс. Өңдеу нәтижелері бойынша мыналарға мүмкіндік қамтамасыз етілуі тиіс: • сөйлеуді мәтінге түрлендіру; • танылған мәтін бойынша іздеу; • әңгімелердің мазмұнын талдау; • кілт сөздер мен сөз тіркестерін анықтау. 1.22. Инциденттерді тергеу ішкі жүйесі Бағдарламалық кешен зияткерлік көмекшіні және табиғи тілде тұжырымдалған сұрауларды пайдалана отырып, ақпараттық қауіпсіздік оқиғаларын тергеуді жүргізуді қамтамасыз етуі тиіс. 1.23. Тергеуді басқару ішкі жүйесі Бағдарламалық кешен мыналарды қамтамасыз етуі тиіс: • бұрын құрылған тергеулер тізімін көрсету; • жаңа тергеу құру; • нәтижелерін қарау үшін бұрын құрылған тергеуді таңдау; • тергеулер тарихын жою. Әрбір тергеу үшін мыналар көрсетілуі тиіс: • пайдаланушы сұрауының мәтіні; • талдау жүргізу кезеңі; • зерттелетін компьютерлер саны; • талдау жүргізу кезінде пайдаланылған деректер көздерінің тізбесі. Деректер көздері ретінде, соның ішінде мыналарға қолдау көрсетілуі тиіс: • алмасу буфері; • компьютерлер оқиғалары; • пошта клиенттері; • жүйе тіркеген өзге де деректер көздері. 1.24. Тергеудің орындалуын бақылау ішкі жүйесі Бағдарламалық кешен тергеудің орындалу параметрлерін, соның ішінде мыналарды көрсетуді қамтамасыз етуі тиіс: • деректерге орындалған сұраулар саны; • қатемен аяқталған сұраулар саны; • тергеуді орындау ұзақтығы. 2. Тергеу нәтижелерін қалыптастыру Тергеу жүргізу нәтижелері бойынша бағдарламалық кешен түпкілікті талдамалық қорытындыны қалыптастыруды қамтамасыз етуі тиіс. Тергеу нәтижесі мыналарды қамтуы тиіс: • анықталған фактілер; • растаулардың жоқтығы туралы мәліметтер; • тергеуге қатысты анықталған оқиғалар; • қалыптастырылған нәтиженің сенімділігін бағалау. 3. Оқиғалар хронологиясын қалыптастыру Бағдарламалық кешен жүргізіліп жатқан тергеуге қатысты оқиғалар хронологиясын қалыптастыруды қамтамасыз етуі тиіс. Әрбір оқиға үшін мыналар көрсетілуі тиіс: • оқиғаның күні мен уақыты; • орындалған әрекеттің сипаттамасы; • байланысты дәлелдемелерге сілтемелер. Хронология оқиғалардың,
--	--

	соның ішінде мынадай түрлерін көрсетуді қамтамасыз етуі тиіс: • файлдарды көшіруді бұғаттау; • құжаттарды бұғаттау; • каталогтарға қолжетімділікті бұғаттау; • файлдардың көлеңкелі көшірмелерін жасау; • хабарламаларды жариялау немесе жіберу. 4. Анықталған фактілерді қалыптастыру Бағдарламалық кешен тергеу деректерін талдау нәтижелерімен расталған фактілерді бөліп көрсетуді және көрсетуді қамтамасыз етуі тиіс. Анықталған фактілер көздер санаттары бойынша, соның ішінде мыналар бойынша топтастырылуы тиіс: • web-браузерлердің белсенділігі; • мессенджерлер; • әлеуметтік желілер; • файлдық операциялар; • көшіру операциялары; • желілік ресурстар. Әрбір санат үшін жүргізілген талдау нәтижелерінің қысқаша сипаттамасы көрсетілуі тиіс. 5. Балама нұсқаларды қалыптастыру Бағдарламалық кешен анықталған оқиғалардың балама түсіндірмелерін қалыптастыруды және көрсетуді қамтамасыз етуі тиіс. Ішкі жүйе мыналарды көрсетуді қамтамасыз етуі тиіс: • тіркелген әрекеттердің ықтимал балама түсіндірмелерін; • тергеу нәтижелеріне әсер ететін белгісіздік факторларын. 6. Деректердегі олқылықтарды анықтау Бағдарламалық кешен тергеудің толықтығына әсер ететін шектеулерді анықтауды және көрсетуді қамтамасыз етуі тиіс. Тергеу нәтижелерінде, соның ішінде мыналар көрсетілуі тиіс: • жекелеген деректер көздерінің қолжетімсіздігі; • деректерді алу қателері; • оқиғалар журналдарының бір бөлігінің болмауы; • жүргізілген талдау толықтығының өзге де шектеулері. 7. Ұсынылатын тексерулер Тергеу нәтижелері бойынша бағдарламалық кешен қосымша тексерулер жүргізу бойынша ұсынымдарды қалыптастыруды қамтамасыз етуі тиіс. Ұсынымдар тергеу нәтижелерін нақтылауға немесе растауға бағытталған әрекеттер тізбесі түрінде көрсетілуі тиіс. 8. Дәлелдемелермен жұмыс Бағдарламалық кешен тергеу нәтижелерін қалыптастыру кезінде пайдаланылған дәлелдемелер санын көрсетуді қамтамасыз етуі тиіс. Тергеу нәтижелерінің мәтінінде дәлелдемелердің идентификаторларына сілтемелер арқылы тиісті дәлелдемелерге өту мүмкіндігі қамтамасыз етілуі тиіс. Дәлелдеменің идентификаторын таңдаған кезде жүйе тиісті материалға өтуді қамтамасыз етуі тиіс. 9. Тергеу нәтижелерімен жұмыс Бағдарламалық кешен мыналарды қамтамасыз етуі тиіс: • қалыптастырылған тергеу нәтижелерін көшіру; • ағымдағы тергеу нәтижелері бойынша қосымша сұрақтар енгізу; • жаңа тергеу құруды қажет етпей, ағымдағы тергеу шеңберінде талдауды жалғастыру. 10.Тергеулер жүргізу кезіндегі зияткерлік көмекшінің функциялары Зияткерлік көмекші мыналарды қамтамасыз етуі тиіс: • пайдаланушының табиғи тілде тұжырымдалған сұрауларын өңдеу; • бірнеше көзден алынған деректерді талдау; • түпкілікті талдамалық қорытындыны қалыптастыру; • байланысты оқиғалар хронологиясын қалыптастыру; • расталған фактілерді бөліп көрсету; • оқиғаларды түсіндірудің балама нұсқаларын қалыптастыру; • бастапқы деректердегі шектеулер мен олқылықтарды анықтау; • қосымша тексерулер жүргізу бойынша ұсынымдарды қалыптастыру; • пайдаланушының ағымдағы тергеу
--	---

	шеңберіндегі нақтылаушы сұрақтарын өңдеу. 10.1. AI Chat ішкі жүйесі Бағдарламалық кешен пайдаланушының зияткерлік көмекшімен табиғи тілдегі сұрауларды пайдалана отырып диалог форматында өзара әрекеттесуін, сондай-ақ жауаптарды қалыптастыру кезінде пайдаланылған материалдарды көрсетуді қамтамасыз етуі тиіс. 10.2. Чаттарды басқару ішкі жүйесі Бағдарламалық кешен мыналарды қамтамасыз етуі тиіс: • зияткерлік көмекшімен жаңа диалог құру; • бұрын құрылған диалогтар тізімін көрсету; • белсенді диалогты таңдау; • чаттар тарихын жою. Әрбір чат үшін мыналар көрсетілуі тиіс: • чаттың атауы; • құрылған күні. 10.3. Сұрауларды өңдеу ішкі жүйесі Бағдарламалық кешен пайдаланушының мониторингтің тіркелген деректеріне сұрауларын орындауды қамтамасыз етуі тиіс. Әрбір сұрау үшін оны өңдеу барысы туралы ақпарат, соның ішінде мыналар көрсетілуі тиіс: • деректерге орындалған сұраулар саны; • жауапты қалыптастыру ұзақтығы. Пайдаланушы жаңа диалог құруды қажет етпей, бір чат шеңберінде сұраулар тізбегін қалыптастыра алуы тиіс. 10.4. Зияткерлік көмекшінің жауаптарын қалыптастыру Сұрауды өңдеу нәтижелері бойынша бағдарламалық кешен зияткерлік көмекшінің жауабын қалыптастыруды қамтамасыз етуі тиіс. Жауап мыналарды көрсетуді қолдауы тиіс: • талдау нәтижелерінің мәтіндік түйіндемесін; • тізімдерді; • статистикалық көрсеткіштерді; • анықталған фактілерді; • қолжетімді деректерге байланысты шектеулерді. Зияткерлік көмекші, соның ішінде мыналарға байланысты сұрауларды орындау мүмкіндігін қамтамасыз етуі тиіс: • пайдаланушыларға; • web-ресурстарға кіруге; • web-ресурстарға кірудің ұзақтығына; • жұмыс кестесін бұзуға; • бағдарламалық кешен тіркеген өзге де деректерге. 10.5. Жауап материалдарымен жұмыс Бағдарламалық кешен зияткерлік көмекшінің жауабын қалыптастыру кезінде пайдаланылған материалдарды көрсетуді қамтамасыз етуі тиіс. Әрбір қалыптастырылған жауап үшін мыналарға мүмкіндік қамтамасыз етілуі тиіс: • жиналған материалдарды қарау; • жауап нәтижесін көшіру. 10.6. Сұрауларды енгізу өрісі Бағдарламалық кешен пайдаланушының ағымдағы диалог шеңберінде келесі сұрауларын енгізу мүмкіндігін қамтамасыз етуі тиіс. Енгізу өрісі мониторинг деректеріне табиғи тілде сұраулар қалыптастыруды қамтамасыз етуі тиіс. 10.7. Материалдар панелі Бағдарламалық кешен зияткерлік көмекшінің жауабын қалыптастыру кезінде пайдаланылған материалдар панелін көрсетуді қамтамасыз етуі тиіс. Панель мыналарды қарауды қамтамасыз етуі тиіс: • ағымдағы жауапты қалыптастыру кезінде пайдаланылған материалдарды; • барлық қолжетімді материалдарды. Көрсетілетін материалдардың әрбір санаты үшін қолжетімді нысандар саны көрсетілуі тиіс. 11. Материалдар карточкалары Әрбір материал мыналарды қамтитын жеке карточка түрінде көрсетілуі тиіс: • материал түрі; • күні мен уақыты; • нысан туралы мәліметтер; • тиісті кестелік деректер немесе параметрлер; • бастапқы дереккөзге өту мүмкіндігі. 12. Web-ресурстарға кіру туралы материалдар Бағдарламалық кешен web-ресурстарға кіру
--	---

	туралы материалдарды мынадай деректермен көрсетуді қамтамасыз етуі тиіс: • пайдаланушы аты; • кірілген ресурс; • URL; • пайдаланылатын браузер; • кіру ұзақтығы. Материал үшін мыналарға мүмкіндік қамтамасыз етілуі тиіс: • журналдағы тиісті оқиғаны ашу; • оқиғалар таспасына өту. 13. Жұмыс кестесін бұзу туралы материалдар Бағдарламалық кешен жұмыс кестесін бұзу туралы материалдарды мыналарды көрсете отырып көрсетуді қамтамасыз етуі тиіс: • қызметкерді; • кешігулер санын; • жұмыс уақытын ерте аяқтау жағдайларының санын; • қосымша сандық көрсеткіштерді. Тиісті материал үшін есепке өту мүмкіндігі қамтамасыз етілуі тиіс. 14. Өнімділік туралы материалдар Бағдарламалық кешен жұмыс өнімділігіне байланысты материалдарды мыналарды көрсете отырып көрсетуді қамтамасыз етуі тиіс: • қызметкерді; • есептік жазбаның немесе компьютердің атын. Тиісті материал үшін есепке өту мүмкіндігі қамтамасыз етілуі тиіс. 15. Web-ресурстарға кіру статистикасы Бағдарламалық кешен web-ресурстарға кіру статистикасын мыналарды көрсете отырып көрсетуді қамтамасыз етуі тиіс: • қызметкерді; • кірілген сайтты; • статистиканың қосымша параметрлерін. 16. Сұрауларды өңдеу контексті Бағдарламалық кешен зияткерлік көмекшінің сұрауды өңдеуінің ағымдағы контексті туралы ақпаратты көрсетуді қамтамасыз етуі тиіс. Мыналарды көрсету мүмкіндігі қамтамасыз етілуі тиіс: • пайдаланылатын контекстің ағымдағы көлемін; • жауапты қалыптастыру кезінде пайдаланылған материалдар санын қолжетімді материалдардың жалпы санына қатысты. 17. Зияткерлік көмекшінің функциялары Зияткерлік көмекші мыналарды қамтамасыз етуі тиіс: • пайдаланушымен табиғи тілде диалог жүргізу; • мониторинг деректеріне сұрауларды өңдеу; • талдамалық жауаптарды қалыптастыру; • түрлі көздерден алынған деректерді іздеу және талдау; • пайдаланушылар бойынша іріктеулер қалыптастыру; • web-ресурстарға кіруді талдау; • жұмыс кестесінің бұзылуын талдау; • жауаптарды қалыптастыру кезінде жиналған материалдарды пайдалану; • оқиғалар журналдары мен есептер арқылы бастапқы деректерге қолжетімділік беру; • талдау нәтижелерін көшіру; • ағымдағы чаттың алдыңғы сұраулары мен нәтижелерін ескере отырып, диалогты жалғастыру. 18. Деректерді сақтау және есептілік ішкі жүйесі Бақыланатын компьютерлерден жиналатын барлық ақпарат бағдарламалық кешеннің серверлік бөлігінің дерекқорында орталықтандырылған түрде сақталуы тиіс. Бағдарламалық кешен мыналарды қамтамасыз етуі тиіс: • жиналған деректер бойынша есептерді қалыптастыру; • есептерді кесте бойынша құру; • есептерді құжаттардың кең таралған форматтарына экспорттау. Лицензиялауға қойылатын талаптар Бағдарламалық кешенді лицензиялау бір мезгілде бақыланатын компьютерлер саны бойынша жүзеге асырылуы тиіс. Жүйе жұмыс станцияларын мониторингтен шығару және кейіннен қосымша лицензиялар сатып алуды қажет етпей, лицензияларды басқа компьютерлерге тағайындау мүмкіндігін қамтамасыз етуі тиіс. Бағдарламалық кешенге лицензия мерзімсіз негізде берілуі тиіс. 19.
--	---

	Әкімшілік консоліне қойылатын талаптар 19.1. Басқару ішкі жүйесінің жалпы параметрлері («Негізгі» панелі) Орталықтандырылған әкімшілік консолі бағдарламалық кешен жұмысының мынадай параметрлерін конфигурациялауды қамтамасыз етуі тиіс: • Жұмыс станцияларын сұрау: агенттерді сұрау жиілігін (минутпен) баптау, әдепкі агент паролін енгізу және көрсету. • Хабарландырулар: хабарландыру тапсырмаларының өмір сүру уақытын (күнмен) және хабарландыру тапсырмаларын тексеру жиілігін (секундпен) баптау. • Қауіпсіздік: мәтінді талдау кезіндегі ұқсастықтың ең аз пайызын баптау, сондай-ақ стандартты емес мінез-құлықты анықтау модулінің іске қосылуының нақты уақытын орнату. • Тарих: тарихты сақтау уақытын (күнмен) баптау. • Есептер жоспарлағышы: серверде есептерге дейінгі жолды белгілеу. • Сервис жұмысы: ағындар санын анықтау. • Прокси-сервер: мекенжайын, портын, логинін және паролін көрсете отырып, прокси-серверді пайдалануға қолдау көрсету. • Email арқылы хабарландыру параметрлері: SMTP-сервер мекенжайын, логинді, парольді, портты баптау, SSL пайдалануды белсендіру, сынақ хат жіберу, сондай-ақ хабарландыруда оқиға бойынша барлық ақпаратты көрсету опциясын қосу. • Telegram bot token: Telegram-боттың токенін енгізу өрісі. • Сервердің сыртқы IP-і: Интернет желісі арқылы сұрау үшін сыртқы IP-мекенжайын және портты баптау. • Active Directory-ден ДК тізімін алуға арналған есептік жазба: AD-да жаңа ДК мен пайдаланушылардың құрылуы туралы хабарландыруларды қосу, логинді, парольді және тексеру жиілігін (сағатпен) баптау. 19.2. Құрылғыларды қосу және түгендеу ішкі жүйесі («Агенттер» панелі) Бағдарламалық кешен клиенттік модульдерді (агенттерді) мынадай мүмкіндіктермен басқаруды қамтамасыз етуі тиіс: • Пайдаланушыларды қосу тәсілдері: IP-мекенжайлар диапазонын сканерлеу (бастапқы және соңғы IP-ді көрсете отырып), ДК-лерді Active Directory-ден импорттау, "remote" пайдаланушыларды қосу, компьютерлер тізімімен жұмыс, тізімге қолмен қосу, Active Directory-де жақында құрылған ДК-лерді таңдау. • Агенттерді басқару: агентті орнату және жою функциялары, орнатудан/жоюдан кейін ДК-ні қайта жүктеу (қолмен қайта жүктеу мүмкіндігімен), мониторинг тізіміне қосу және одан жою, сондай-ақ әкімші деректерін (аты мен паролі) енгізу. • Мәртебелерді бақылау: желілік атауды, IP-мекенжайды және мәртебелерді («Орнатылған / тізімде», «Орнатылмаған / байланыс жоқ», «Нұсқалардың сәйкес келмеуі») көрсету. 19.3. Деректерді жинау профильдері мен ережелерін баптау («Бақылау» панелі) Бағдарламалық кешен ДК мен пайдаланушылар топтары үшін (мысалы, «Basic» профилі) мынадай бақылау бөлімдерін қамтитын баптау профильдерін құруды қолдауы тиіс: • Жинаудың жалпы параметрлері: автостарт және логтар өлшемі, жинаудың негізгі параметрлері, скриншоттар, сыртқы жинақтауыштар, файлдар мен қалталар, көлеңкелі көшіру, internet логтары, жұмыс уақытын есепке алу, webcam/microphone. • Көлеңкелі көшіру параметрлері: о USB-жинақтауыштарға көшірілетін файлдардың көлеңкелі көшірмелерін құруды белсендіру; о бұлттық дискілерге
--	---

	көшірілетін файлдардың көшірмелерін құруды белсендіру; о көшірмелерді құруды «Алынбалы дискіге көшірілетін» және «Алынбалы дискіде өзгертілетін» белгілері бойынша бөле отырып баптау; о көшірілетін файлдың ең үлкен өлшемін шектеу (МБ-пен); о файлдарды сақтауға көлем бөлу (МБ-пен); о сақтау буфері толған кездегі логиканы баптау («Жаңа файлдарды жазбау» режимін таңдау). • Қауіпсіздік параметрлері (Қолданбаларды бақылау): ехе-файлдың атын, терезе тақырыбын, мақсатты әрекетті (мысалы, «Тек хабарландыру») және түсініктемені белгілей отырып, кестелік тізімдерді жүргізу. 20. Стандартты емес мінез-құлықты анықтауды баптау Жүйе деректердің мынадай санаттары бойынша ауытқушы белсенділік анықталған кезде хабарландыруларды белсендіру мүмкіндігімен мінез-құлықтық талдауды қолдауы тиіс: • құжаттарды принтерге басып шығару; • web сайттарға кіру; • файлдарды интернетке жүктеу; • файлдарды алынбалы жинақтауыштарға көшіру; • мессенджерлердегі қарым-қатынас (хабарламалар саны); • Skype-тағы хат алмасу (хабарламалар саны); • әлеуметтік желілердегі қарым-қатынас (хабарламалар саны); • пошта арқылы хат алмасу (хаттар саны); • web пошта арқылы хат алмасу (браузер арқылы); • іздеу сұраулары; • бағдарламаларды іске қосу. Талдаудың қосымша параметрлері мыналарды қамтуы тиіс: • талдауға арналған уақыт аралығын (жұмыс күндерімен) баптау; • салыстыру режимін таңдау: «Қызметкердің өзіне қатысты салыстыру» немесе «Топқа қатысты салыстыру»; • күнделікті CPU жоғары тұтыну триггерін (берілген %-дан астам) белгілеу; • әкімшілер үшін екі факторлы авторизацияны қосу, олардың Windows есептік жазбаларын, IP-мекенжайларын, E-mail, логиндері мен парольдерін баптау мүмкіндігі, хабарландыру арналарын (тікелей, Telegram арқылы, E-mail арқылы) таңдай отырып. 21. Файлдармен жұмыс ережелерін құру модулі (DLP-саясаттар) Жүйе екі түрдегі нысандық ережелерді құруды қамтамасыз етуі тиіс: • Ереже түрі: Қолжетімділікті шектеу о Дискілер түрлеріне қолдану: «Барлық түрлері» немесе «Таңдамалы» (чек-боксстармен бөлек таңдай отырып: Ішкі (қатты дискілер), Алынбалы жинақтауыштар, Желілік дискілер мен шарлар). о Каталогтар бойынша бақылау: мақсатты каталогтарды/файлдарды енгізу өрісі («жұлдызша» * таңбасын қолдай отырып). о Ерекшеліктер: ережеден шығару үшін жолдарды/файлдарды енгізу өрісі. о Адресаттылық: ережені пайдаланушыларға (ереженің инверсиясы және есептік жазбаларды domain\username форматында енгізу мүмкіндігімен) және нақты қолданбаларға байланыстыру. о Қолжетімділік құқықтары: мынадай режимдердің бірін таңдау — «Барлығына рұқсат», «Қолжетімділікке тыйым», «Тек оқу» немесе «Құпия каталог режимі» («Алмасу буферіне көшіруге тыйым салу» және «Принтерге басып шығаруға тыйым салу» қосымша опцияларымен). • Ереже түрі: Көлеңкелі көшіру о Дискілер түрлеріне (барлығы/таңдамалы), пайдаланушыларға, қолданбаларға, бақыланатын каталогтарға және ерекшеліктерге байланыстырудың ұқсас тетіктері бар. о Көлеңкелі көшірме құру шарттары: «Файлдарды жазу/өңдеу» және «Файлдарды оқу (ашу)» опцияларын бөлек белсендіру. о
--	---

	Өлшемді шектеу: көшірілетін файлдың ең үлкен өлшемін (МБ-пен) баптау. 22. Әкімшілік консоліне кіру міндетті авторизациядан кейін жүзеге асырылады. Әкімшілік консолі Windows классикалық қолданбасы ретінде іске асырылуы тиіс, браузерді пайдалануды қажет етпей. 23. Деректерді қарау консоліне қойылатын талаптар Бұл web-консоль авторизацияланған пайдаланушыларға бақыланатын компьютерлердегі белсенділікті мониторингілеудің жиналған деректерін қарауға мүмкіндік береді. Әрбір пайдаланушыға тек өзіне қолжетімділікке рұқсат етілген компьютерлер бойынша және сол компьютерлерге қатысты ақпарат ғана беріледі, оқу және өңдеу құқықтары ажыратылады. Консоль нақты уақыт режимінде мониторингті (пернетақтадан енгізу, экран скриншоттары, іске қосылған қолданбалар, файлдық операциялар, қаралған сайттар, алмасу буфері, басып шығару, USB-құрылғылар, электрондық пошта, мессенджерлер, желілік сеанстар, автожүктеме) қамтамасыз етеді және ағымдағы деректер бойынша есептерді де, бақыланатын компьютерлерді, бағдарламалық қамтамасыз етуді пайдалану, веб-сайттарға кіру, принтерлерді пайдалану, хабарламалар алмасу бағдарламалары арқылы хат алмасу, интернет-қосылымдар, микрофон жазбасы статистикасын, сондай-ақ жұмыс өнімділігінің жиынтық көрсеткіштері мен еңбек тәртібін бұзуды қамтитын талдамалық есептерді де қалыптастыруға мүмкіндік беретін есептер шеберін қамтиды. Белгіленген қауіпсіздік саясаттары бұзылған кезде бұл туралы хабарлама арнайы хабарландырулар терезесінде көрсетіледі. Жүйе сондай-ақ барлық деректер түрлері бойынша толық мәтінді іздеуді, жұмыс станцияларындағы агенттердің тапсырмаларын басқаруды, автоматты есептер жоспарлағышын және жинау параметрлерін, пайдаланушыларды, контент санаттарын және қауіпсіздік ережелерін баптауға арналған әкімші панелін қамтиды. Консольге кіру логин мен пароль бойынша міндетті аутентификациядан кейін жүзеге асырылады. 24. Хабарландыру жүйесіне қойылатын талап 24.1. Мониторинг, оқиғаларды сүзу және жедел хабарландырулар жіберу Жүйе ақпараттық қауіпсіздік оқиғаларын және пайдаланушылардың белсенділігін мынадай санаттар бойынша үздіксіз мониторингілеуді, жинауды, жіктеуді және сүзуді қамтамасыз етуі тиіс: • терілетін мәтін (пернетақта белсенділігі); • бағдарламалар (қолданбаларды пайдалану); • файлдық жүйе (файлдармен операциялар); • бағдарламаларды орнату және жою; • алмасу буфері; • қаралған сайттар; • көлеңкелі көшірме (файлдарды резервтік көшіру); • ақпарат тасымалдағыштарын қосу және ажырату; • белсенді хабарландыру; • пошта (электрондық пошта E-mail); • желі: файлдар (желілік файлдық белсенділік); • мессенджерлер; • әлеуметтік желілер; • web пошта; • жүктелетін файлдар; • принтер (басып шығару статистикасы); • мессенджерлер: файлдар (мессенджерлерде файлдар беру); • жабдықтың (аппараттық қамтамасыз етудің) өзгерістері; • AD-дан жаңа ДК (Active Directory-мен интеграция); • іздеу сұраулары; • ДК жұмысы; • өзекті деректердің болмауы (агенттердің қолжетімділігін бақылау). Жүйе басқару консолінде деректерді іріктеуді, іздеуді және сүзуді
--	--

	мынадай мүмкіндіктермен қамтамасыз етуі тиіс: • деректерді іріктеудің еркін уақыт аралығын минутқа дейінгі дәлдікпен баптау (кезеңнің басталу/аяқталу күні мен уақыты бойынша); • деректерді оқиғалар санаттары бойынша сүзу; • деректерді оқиғаларды верификациялау мәртебесі бойынша сүзу (барлық оқиғалар, тек расталған, расталмаған); • кілт сөздер бойынша контекстік іздеу; • қалыптастырылған деректер іріктеулерін сыртқы форматтарға экспорттау. Жүйе қауіпсіздік әкімшілерінің (бақылаушыларының) профильдерін мынадай параметрлерді белгілей отырып жүргізуді қамтамасыз етуі тиіс: • Windows есептік жазбасы (жергілікті немесе домендік); • әкімшінің IP-мекенжайы; • электрондық пошта мекенжайы (E-mail); • басқару консоліне кіруге арналған логин мен пароль. Жүйе екі факторлы авторизацияны қосу мүмкіндігімен әкімшінің басқару консоліне қолжетімділік қауіпсіздігін қамтамасыз етуді қолдауы тиіс. Жүйе әкімшілерге тіркелген оқиғалар мен инциденттер туралы жедел хабарландырулар жіберуді қамтамасыз етуі тиіс. Хабарландыру модулі мыналарды қолдауы тиіс: • белсенді хабарландыру функциясын қосу және өшіру; • пайдаланушылардың стандартты емес (ауытқушы) мінез-құлқы туралы хабарландыру функциясын қосу және өшіру; • әкімшінің бақыланатын оқиғалардың кез келген санаты бойынша хабарландыруларға жазылуын жеке баптау; • хабарландыруларды үш тәуелсіз арна бойынша жеткізу: о тікелей басқару консоліне (тікелей хабарландырулар); о Telegram мессенджеріне (арнайы Telegram-бот арқылы байланыстыруға қолдау көрсете отырып); о электрондық пошта мекенжайына (E-mail). 25. Белсенді әрекет ету жүйесіне қойылатын талаптар 25.1. Белсенді әрекет ету ішкі жүйесі Бағдарламалық кешен бақыланатын ақпараттық қауіпсіздік оқиғалары мен пайдаланушылардың белсенділігі туындаған кезде әрекет ету іс-қимылдарын автоматты түрде орындауды қамтамасыз етуі тиіс. Ішкі жүйе белсенді әрекет ету ережелерін құруды, өңдеуді, жоюды, қосуды және өшіруді қамтамасыз етуі тиіс. Әрбір ереже бір іске қосылу шартын және бір әрекет ету іс-қимылын қамтуы тиіс. Әрбір ереже үшін мынадай параметрлерді баптау мүмкіндігі қамтамасыз етілуі тиіс: • ереженің атауы; • ереженің белсенділік белгісі; • іс-қимылдың орындалуын бастайтын оқиға; • ереженің әрекеті қолданылатын пайдаланушылар, компьютерлер немесе пайдаланушылар топтары; • таңдалған іс-қимылды орындау параметрлері. Қолдау көрсетілетін оқиғалар мыналарды қамтуы тиіс: • USB-жинақтауыштарды қосу; • файлдарды алынбалы тасымалдағыштарға көшіру; • тыйым салынған қолданбаны іске қосу («Қауіпсіздік» ішкі жүйесінің ережелеріне сәйкес); • бақыланатын бағдарламалар тізімін көрсету мүмкіндігімен таңдалған қолданбаны іске қосу; • бақыланатын сайттар тізімін көрсету мүмкіндігімен web-сайтты ашу; • бақыланатын өрнектер тізімін қалыптастыру мүмкіндігімен пернетақтадан берілген кілт сөзді немесе сөз тіркесін енгізу; • деректерді алмасу буферіне көшіру; • пайдаланушының бақыланатын компьютерде авторизациялануы; • компьютердің бос тұру кезеңінің басталуы; • компьютердің бос тұру кезеңінің
--	---

	аяқталуы; • қолдау көрсетілетін мессенджерде хабарлама жіберу. Қолдау көрсетілетін әрекет ету іс-қимылдары мыналарды қамтуы тиіс: • түсірілім санын және олардың арасындағы аралықты баптау мүмкіндігімен бір немесе бірнеше экран суретін жасау; • хабарландырудың еркін мәтінін беру мүмкіндігімен пайдаланушыға ақпараттық хабарлама шығару; • орындалу кідірісін баптау мүмкіндігімен пайдаланушы сеансын аяқтау; • орындалу кідірісін баптау мүмкіндігімен бақыланатын компьютерді өшіру; • түсірілім санын және олардың арасындағы аралықты баптау мүмкіндігімен веб-камерадан бір немесе бірнеше сурет жасау; • жазба ұзақтығын баптау мүмкіндігімен микрофоннан аудио жазу; • жазба ұзақтығын баптау мүмкіндігімен веб-камерадан бейне жазу; • орындалатын файлды және пәрмен жолы параметрлерін көрсету мүмкіндігімен сыртқы бағдарламаны іске қосу; • PowerShell тілінде пайдаланушылық сценарийді (скриптті) орындау. Әрекет ету іс-қимылдары үшін мынадай параметрлерді баптау мүмкіндігі қамтамасыз етілуі тиіс: • жасалатын экран суреттерінің саны; • экран суреттерін жасау арасындағы аралық; • пайдаланушыға шығарылатын хабарлама мәтіні; • пайдаланушы сеансын аяқтау алдындағы кідіріс; • компьютерді өшіру алдындағы кідіріс; • жасалатын веб-камера суреттерінің саны; • веб-камерадан сурет жасау арасындағы аралық; • аудио жазу ұзақтығы; • бейне жазу ұзақтығы; • орындалатын бағдарламаға дейінгі жол және оны іске қосу параметрлері; орындалатын PowerShell-сценарийдің мәтіні. 26. Есептер ішкі жүйесіне қойылатын талаптар 26.1. Есептерді қалыптастыру, жоспарлау және жеткізу Жүйе есептерді қалыптастыруды және деректерді іріктеуді баптауға болатын уақыт кезеңдері бойынша: 1, 2, 3, 5, 7, 10, 15, 30, 45, 60, 90, 120, 182 және 365 күн, сондай-ақ тек пайдаланушының жұмыс уақыты бойынша қамтамасыз етуі тиіс. Жүйе мынадай есептер мен деректер іріктеулерін қалыптастыруды қолдауы тиіс: • компьютер мен қолданбалардың жұмыс уақыты; • файлдарды көлеңкелі көшіру; • электрондық пошта (E-mail); • алмасу буфері; • файлдарды жүктеу; • аппараттық қамтамасыз етудің өзгерістері; • мессенджерлердегі хат алмасу (егжей-тегжейлендіру мүмкіндігімен); • іздеу сұраулары; • қаралған веб-сайттар; • веб-поштамен жұмыс; • сыртқы жинақтауыштарды пайдалану; • пернетақта белсенділігі; • компьютерде жұмыс істеу; • қолданбаларды пайдалану; • принтерлерді пайдалану және басып шығару статистикасы; • әлеуметтік желілерді пайдалану; • желілік белсенділік; • скриншоттар; • орнатылған және жойылған бағдарламалар; • файлдық жүйемен операциялар; • пайдаланушылар белсенділігінің таспасы; • еңбек тәртібін бұзу; • файлдарды жүктеу бойынша есеп; • мессенджерлерді пайдалану бойынша есеп; • электрондық поштаны пайдалану бойынша есеп; • қаралған веб-сайттар бойынша есеп; • компьютердің жұмыс өнімділігі бойынша есеп; • бағдарламаларды пайдалану бойынша есеп; • жұмыс уақыты бойынша жиынтық есеп; • компьютер, өнімділік және принтерлерді пайдалану бойынша жиынтық есеп; • жұмыс уақытының табелі; • пайдаланушылар белсенділігінің жылу картасы. Жүйе
--	---

	есептерді кесте бойынша автоматты түрде қалыптастыруды мына мүмкіндіктермен қамтамасыз етуі тиіс: • есеп қалыптастырылатын пайдаланушылар мен компьютерлерді таңдау; • тапсырманың іске қосылу уақытын баптау; • орындау жиілігін таңдау (күн сайын, апта сайын немесе ай сайын); • тапсырманы орындау үшін апта күндерін таңдау; • деректерді қолданбалардың берілген тізбесі бойынша сүзу; • кесте параметрлерін сақтау және өңдеу. Жүйе қалыптастырылған есептерді PDF, XLS және RTF форматтарына экспорттауды қамтамасыз етуі тиіс. Жүйе қалыптастырылған есептерді электрондық пошта арқылы автоматты түрде жіберуді мына мүмкіндіктермен қамтамасыз етуі тиіс: • жіберу функциясын қосу немесе өшіру; • алушылардың бір немесе бірнеше электрондық пошта мекенжайын көрсету; • есептерді таңдалған форматта белгіленген кесте бойынша жіберу. 27. Жабдыққа, бағдарламалық қамтамасыз етуге және жабдықтаушыға қойылатын талаптар 27.1. Жабдық пен бағдарламалық қамтамасыз етуге қатысты ұсынылған барлық сипаттамалар осы техникалық сипаттамада көрсетілген ең төменгі техникалық сипаттамаларға сәйкес келуі немесе олардан жоғары болуы тиіс; 27.2. Қызметті көрсету үшін әлеуетті өнім беруші конкурстық өтінім құрамында өндірушіден немесе олардың ресми өкілдерінен (дилерлерден немесе дистрибьюторлардан) растайтын құжаттарды ұсынуға міндетті. 27.3. Қызмет көрсету мерзімі: 2026 жылғы 2 қарашадан 2026 жылғы 17 қарашаға дейін.
Әлеуетті өнім берушіге оның жеңімпазы анықталған және онымен Мемлекеттік сатып алу туралы шарт жасалған жағдайда қойылатын талаптар (қажет болған кезде көрсетіледі) (әлеуетті өнім берушіні көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін қабылдамауға жол берілмейді)	

**Техническая спецификация
закупаемых услуг
(заполняется заказчиком)**

Наименование заказчика	Государственное коммунальное предприятие на праве хозяйственного ведения "Городской центр мониторинга и оперативного реагирования" акимата города Астаны
Наименование организатора	Государственное коммунальное предприятие на праве хозяйственного ведения "Городской центр мониторинга и оперативного реагирования" акимата города Астаны
№ конкурса:	№ 17856902-1
Наименование конкурса:	Услуги по приобретению и развертыванию программного обеспечения для предотвращения потери данных
Номер лота:	№ 83033478-OK2
Наименование лота:	Услуги по обеспечению информационной безопасности
Наименование кода Единого номенклатурного справочника товаров, работ, услуг:	801019.000.000010
Наименование услуги:	Услуги по обеспечению информационной безопасности
Единица измерения:	Одна услуга
Количество (объем):	1
Цена за единицу, без учета налога на добавленную стоимость:	6741181
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость:	6741181
Срок оказания услуги:	Согласно технической спецификации
Размер авансового платежа* *:	0 %
Гарантийный срок (в месяцах)	12

Описание требуемых характеристик, параметров и иных исходных данных	1. Описание и требуемый функционал: 1.1. Программный комплекс должен состоять из следующих компонентов: • Пользовательская часть (агент), устанавливаемая на контролируемые рабочие станции и серверы. • Серверная часть, обеспечивающая централизованный прием, обработку и хранение данных. • Консоль администрирования для управления настройками системы и агентами. • Консоль просмотра данных для анализа собранной информации и расследования инцидентов. Агентская часть должна обеспечивать сбор и накопление информации о действиях пользователей на контролируемом компьютере. Временное хранение собранных данных должно осуществляться локально в защищенном каталоге в зашифрованном виде. После передачи данных на сервер локальные копии должны автоматически удаляться. Программный комплекс должен поддерживать настройку периодичности сбора и передачи данных. Взаимодействие между агентом и сервером должно осуществляться по защищенным каналам связи с использованием шифрования. Должна поддерживаться возможность установки пароля для авторизации серверной части при взаимодействии с агентами. Серверная часть программного комплекса должна поддерживать развертывание под операционными системами Windows и Linux. Для Linux должна обеспечиваться возможность эксплуатации посредством контейнера Docker. Пользовательский интерфейс системы должен предоставляться через web-интерфейс с использованием веб-сервера Nginx. 1.2. Подсистема мониторинга действий пользователей Программный комплекс должен обеспечивать регистрацию и хранение информации о действиях пользователей на контролируемых компьютерах, включая: • регистрацию нажатий клавиш на клавиатуре; • создание снимков экрана (скриншотов) по расписанию и при смене активного окна; • настройку качества и цветового режима скриншотов (цветной/черно-белый); • настройку индивидуальной периодичности создания скриншотов для отдельных приложений; • регистрацию запуска и завершения программ; • регистрацию открытия и закрытия приложений с фиксацией времени запуска, имени программы, заголовка окна и пути к исполняемому файлу; • блокировку запуска запрещенных приложений; • регистрацию поисковых запросов в поисковых системах; • регистрацию посещенных web-ресурсов; • регистрацию активности в браузерах с фиксацией: о URL посещенного ресурса; о категории web-ресурса; о времени посещения; о заголовка окна; о длительности сеанса; о имени пользователя; • регистрацию активности пользователей в социальных сетях; • регистрацию файлов, загружаемых в сеть Интернет; • регистрацию событий включения и выключения компьютера; • регистрацию входа и выхода пользователей из операционной системы; • регистрацию блокировки рабочей станции и периодов простоя пользователя. 1.3. Подсистема контроля коммуникаций Программный комплекс должен обеспечивать перехват и регистрацию коммуникационной активности пользователей, исключительно на служебных устройствах (ноутбуки, ПК, смартфоны), принадлежащие Заказчику включая: • перехват входящих и исходящих сообщений электронной почты
---	--

	по протоколам POP3, POP3S, SMTP, SMTPS и IMAP; • сохранение вложений электронной почты; • сохранение текстовой переписки в следующих мессенджерах: о WhatsApp Web; о Telegram Web; о Telegram Desktop; о Viber; о Яндекс Мессенджер Web; о AITU Web; • сохранение голосовых сообщений; • перехват переписки в web-версии мессенджера AITU; • регистрацию сообщений, передаваемых через социальные сети; • регистрацию переписки через web-почту. 1.4. Подсистема мониторинга мессенджеров Программный комплекс должен обеспечивать регистрацию сообщений из поддерживаемых мессенджеров с отображением следующих параметров: • дата и время сообщения; • наименование мессенджера; • собеседник (чат, группа или пользователь); • тип сообщения; • текст сообщения либо содержимое переданного файла; • имя пользователя контролируемого компьютера. Подсистема должна обеспечивать регистрацию следующих типов сообщений: • входящие сообщения (incoming); • исходящие сообщения (outgoing). Интерфейс просмотра сообщений должен обеспечивать: • фильтрацию данных по ключевому слову; • фильтрацию по столбцам журнала; • группировку данных путем переноса выбранного столбца в область группировки; • сортировку данных по выбранным столбцам; • экспорт отображаемых данных во внешний файл. В журнале сообщений должны отображаться следующие столбцы: • Время; • Мессенджер; • Собеседник; • Тип сообщения; • Текст сообщения/файл; • Имя пользователя. 1.5. Подсистема контроля файловых операций Программный комплекс должен обеспечивать мониторинг файловой системы с регистрацией следующих событий: • создание файлов; • изменение файлов; • переименование файлов; • удаление файлов. Для каждого события должны фиксироваться: • дата и время операции; • тип операции; • полный путь к файлу; • размер файла; • контрольная сумма MD5 (при наличии); • имя пользователя. Дополнительно система должна обеспечивать: • контроль операций с сетевыми ресурсами; • регистрацию операций с общими каталогами; • регистрацию установки и удаления программного обеспечения; • регистрацию изменений аппаратной конфигурации контролируемого компьютера, включая процессор, оперативную память и накопители. 1.6. Подсистема контроля буфера обмена Программный комплекс должен обеспечивать перехват содержимого буфера обмена с регистрацией следующих параметров: • время события; • заголовок активного окна; • тип данных (текст, файл, изображение и др.); • содержимое буфера обмена. Система должна обеспечивать возможность сохранения перехваченных данных на рабочую станцию оператора консоли просмотра. 1.7. Подсистема контроля печати Программный комплекс должен обеспечивать: • регистрацию фактов печати документов; • фиксацию параметров печати; • сохранение электронного образа распечатанного документа в формате PDF. 1.8. Подсистема контроля устройств и внешних носителей Программный комплекс должен обеспечивать: • обнаружение подключения и отключения USB-накопителей; • регистрацию параметров подключаемых устройств; • создание теневых копий файлов, копируемых на
--	---

	съемные носители; • блокировку подключения USB-накопителей; • блокировку подключения устройств классов: о USB Mass Storage; о CD/DVD-ROM; о Floppy Drive; • ведение списка доверенных USB-устройств; • разрешение работы только с устройствами, включенными в список разрешенных; • блокирование всех остальных USB-накопителей. 1.9. Подсистема контроля облачных сервисов Программный комплекс должен обеспечивать: • обнаружение использования клиентов облачных хранилищ; • блокировку клиентов облачных сервисов; • создание теневых копий файлов, передаваемых в облачные хранилища. 1.10. Подсистема удаленного управления Программный комплекс должен обеспечивать следующие функции удаленного администрирования: • удаленный запуск и остановку агента; • удаленное включение и отключение мониторинга; • принудительную синхронизацию журналов событий; • получение списка запущенных процессов; • получение списка установленного программного обеспечения; • получение списка подключенного оборудования; • отправку текстовых сообщений пользователям; • удаленную установку агентов; • удаленное удаление агентов; • развертывание агентов посредством MSI и EXE-пакетов через групповые политики Active Directory. 1.11. Подсистема удаленного доступа Программный комплекс должен обеспечивать: • просмотр экранов контролируемых компьютеров в режиме реального времени; • удаленное управление рабочим столом; • возможность перехвата управления рабочей станцией во время удаленного сеанса. 1.12. Подсистема диагностики агентов Программный комплекс должен обеспечивать контроль состояния агентских модулей с возможностью: • отображения всех агентов; • отображения агентов без связи; • фильтрации по количеству дней отсутствия соединения. Для каждого агента должны отображаться следующие параметры: • имя компьютера; • MAC-адрес; • IP-адрес; • время последнего соединения с сервером; • время последней передачи данных. 1.13. Подсистема оповещений и реагирования Программный комплекс должен обеспечивать активное оповещение администраторов о следующих событиях: • подключение и отключение USB-носителей; • установка и удаление программ; • копирование файлов на съемные носители; • отправка сообщений через web-почту; • нарушение политик безопасности; • изменение аппаратной конфигурации компьютеров. Поддерживаемые каналы оповещения: • консоль просмотра данных; • электронная почта; • Telegram. 1.14. Подсистема контроля сетевого доступа Программный комплекс должен обеспечивать регистрацию событий сетевого доступа с отображением следующих параметров: • дата и время события; • имя пользователя; • имя компьютера; • тип события. Поддерживаемые типы событий должны включать: • начало подключения; • окончание подключения. Подсистема должна обеспечивать: • фильтрацию зарегистрированных событий по ключевому слову; • сортировку данных по столбцам; • экспорт зарегистрированных событий во внешний файл. 1.15. Подсистема поведенческого анализа Программный комплекс должен обеспечивать обнаружение нестандартной активности пользователей на
--	--

	основе анализа накопленных данных. Дополнительно система должна обеспечивать выявление: • программ-майнеров; • программ, создающих аномальную нагрузку на вычислительные ресурсы рабочих станций; • иных признаков потенциально опасной активности пользователей. 1.16. Подсистема поиска и расследований Программный комплекс должен обеспечивать: • полнотекстовый поиск по всем собранным данным; • поиск по теневым копиям файлов; • поиск по вложениям электронной почты; • поиск по документам, отправленным на печать; • поиск по регулярным выражениям. Система должна поддерживать поиск следующих типов данных: • номера телефонов; • паспортные данные; • БИН/ИИН; • номера банковских карт; • иные пользовательские шаблоны. 1.17. Подсистема защиты конфиденциальных данных Программный комплекс должен обеспечивать создание конфиденциальных каталогов с поддержкой следующих функций: • разрешение работы с файлами только в определенных приложениях; • запрет копирования файлов за пределы конфиденциального каталога; • разрешение редактирования файлов внутри каталога; • запрет копирования данных в буфер обмена; • запрет печати документов. 1.18. Подсистема цифровых водяных знаков Программный комплекс должен обеспечивать отображение цифровых водяных знаков на экране контролируемых компьютеров с целью последующей идентификации источника получения изображения экрана. Подсистема должна обеспечивать следующие функции: • отображение водяных знаков поверх рабочего стола и окон приложений; • централизованное включение и отключение отображения водяных знаков; • выбор типа водяного знака: о текстовый; о QR-код; • отображение нескольких QR-кодов одновременно на поверхности экрана. Для водяных знаков типа «QR-код» программный комплекс должен обеспечивать возможность распознавания QR-кода путем загрузки фотографии или снимка экрана в консоль просмотра данных. После распознавания QR-кода должна отображаться следующая информация: • имя компьютера; • имя пользователя; • временной интервал формирования QR-кода. Полученная информация должна использоваться для идентификации контролируемого компьютера и пользователя при расследовании инцидентов информационной безопасности, связанных с распространением фотографий или снимков экрана, содержащих конфиденциальную информацию. 1.19. Подсистема искусственного интеллекта Программный комплекс должен включать локальные модели искусственного интеллекта, обеспечивающие обработку и анализ данных, а также работу интеллектуального помощника без подключения к сети Интернет и без передачи данных во внешние информационные системы. Обработка пользовательских запросов, анализ зарегистрированных данных и формирование ответов должны выполняться локальными моделями искусственного интеллекта с использованием вычислительных ресурсов сервера программного комплекса. Работа подсистемы искусственного интеллекта не должна требовать регистрации в сторонних сервисах, передачи телеметрии или хранения обрабатываемых данных за пределами инфраструктуры заказчика. 1.20. Анализ
--	---

	документов Подсистема должна обеспечивать анализ текстовых документов с использованием технологий искусственного интеллекта. По результатам анализа должна обеспечиваться возможность: • автоматического определения категории документа; • выявления признаков конфиденциальной информации; • формирования краткого содержания документа; • оценки уровня чувствительности информации; • формирования рекомендаций по применению политик информационной безопасности. 1.21. Анализ аудиоданных Подсистема должна обеспечивать автоматическое распознавание речи в аудиозаписях. По результатам обработки должна обеспечиваться возможность: • преобразования речи в текст; • поиска по распознанному тексту; • анализа содержания разговоров; • выявления ключевых слов и фраз. 1.22. Подсистема расследования инцидентов Программный комплекс должен обеспечивать проведение расследований событий информационной безопасности с использованием интеллектуального помощника и запросов, сформулированных на естественном языке. 1.23. Подсистема управления расследованиями Программный комплекс должен обеспечивать: • отображение списка ранее созданных расследований; • создание нового расследования; • выбор ранее созданного расследования для просмотра результатов; • удаление истории расследований. Для каждого расследования должны отображаться: • текст запроса пользователя; • период проведения анализа; • количество исследуемых компьютеров; • перечень источников данных, использованных при проведении анализа. В качестве источников данных должны поддерживаться, в том числе: • буфер обмена; • события компьютеров; • почтовые клиенты; • иные зарегистрированные системой источники данных. 1.24. Подсистема контроля выполнения расследования Программный комплекс должен обеспечивать отображение параметров выполнения расследования, включая: • количество выполненных запросов к данным; • количество запросов, завершившихся ошибкой; • продолжительность выполнения расследования. 2. Формирование результатов расследования По результатам проведения расследования программный комплекс должен обеспечивать формирование итогового аналитического вывода. Результат расследования должен содержать: • выявленные факты; • сведения об отсутствующих подтверждениях; • выявленные события, относящиеся к расследованию; • оценку уверенности сформированного результата. 3. Формирование хронологии событий Программный комплекс должен обеспечивать формирование хронологии событий, относящихся к проводимому расследованию. Для каждого события должны отображаться: • дата и время события; • описание выполненного действия; • ссылки на связанные доказательства. Хронология должна обеспечивать отображение, в том числе, следующих типов событий: • блокировка копирования файлов; • блокировка документов; • блокировка доступа к каталогам; • создание теневых копий файлов; • публикация или отправка сообщений. 4. Формирование установленных фактов Программный комплекс должен обеспечивать выделение и отображение фактов,
--	--

	подтвержденных результатами анализа данных расследования. Установленные факты должны группироваться по категориям источников, включая: • активность web-браузеров; • мессенджеры; • социальные сети; • файловые операции; • операции копирования; • сетевые ресурсы. Для каждой категории должно отображаться краткое описание результатов проведенного анализа. 5. Формирование альтернативных версий Программный комплекс должен обеспечивать формирование и отображение альтернативных интерпретаций выявленных событий. Подсистема должна обеспечивать отображение: • возможных альтернативных объяснений зафиксированных действий; • факторов неопределенности, влияющих на результаты расследования. 6. Выявление пробелов в данных Программный комплекс должен обеспечивать выявление и отображение ограничений, влияющих на полноту расследования. В результатах расследования должны отображаться, в том числе: • недоступность отдельных источников данных; • ошибки получения данных; • отсутствие части журналов событий; • иные ограничения полноты проведенного анализа. 7. Рекомендуемые проверки По результатам расследования программный комплекс должен обеспечивать формирование рекомендаций по проведению дополнительных проверок. Рекомендации должны отображаться в виде перечня действий, направленных на уточнение или подтверждение результатов расследования. 8. Работа с доказательствами Программный комплекс должен обеспечивать отображение количества доказательств, использованных при формировании результатов расследования. В тексте результатов расследования должна обеспечиваться возможность перехода к соответствующим доказательствам посредством ссылок на их идентификаторы. При выборе идентификатора доказательства система должна обеспечивать переход к соответствующему материалу. 9. Работа с результатами расследования Программный комплекс должен обеспечивать: • копирование сформированных результатов расследования; • ввод дополнительных вопросов по результатам текущего расследования; • продолжение анализа в рамках текущего расследования без необходимости создания нового расследования. 10. Функции интеллектуального помощника при проведении расследований Интеллектуальный помощник должен обеспечивать: • обработку запросов пользователя, сформулированных на естественном языке; • анализ данных из нескольких источников; • формирование итогового аналитического вывода; • формирование хронологии связанных событий; • выделение подтвержденных фактов; • формирование альтернативных версий интерпретации событий; • выявление ограничений и пробелов в исходных данных; • формирование рекомендаций по проведению дополнительных проверок; • обработку уточняющих вопросов пользователя в рамках текущего расследования. 10.1. Подсистема AI Chat Программный комплекс должен обеспечивать взаимодействие пользователя с интеллектуальным помощником в формате диалога с использованием запросов на естественном языке, а также отображение материалов, использованных при формировании ответов. 10.2. Подсистема
--	---

	управления чатами Программный комплекс должен обеспечивать: • создание нового диалога с интеллектуальным помощником; • отображение списка ранее созданных диалогов; • выбор активного диалога; • удаление истории чатов. Для каждого чата должны отображаться: • наименование чата; • дата создания. 10.3. Подсистема обработки запросов Программный комплекс должен обеспечивать выполнение запросов пользователя к зарегистрированным данным мониторинга. Для каждого запроса должна отображаться информация о ходе его обработки, включая: • количество выполненных запросов к данным; • продолжительность формирования ответа. Пользователь должен иметь возможность формировать последовательность запросов в рамках одного чата без необходимости создания нового диалога. 10.4. Формирование ответов интеллектуального помощника По результатам обработки запроса программный комплекс должен обеспечивать формирование ответа интеллектуального помощника. Ответ должен поддерживать отображение: • текстового резюме результатов анализа; • списков; • статистических показателей; • выявленных фактов; • ограничений, связанных с доступными данными. Интеллектуальный помощник должен обеспечивать возможность выполнения запросов, связанных, в том числе, с: • пользователями; • посещением web-ресурсов; • продолжительностью посещения web-ресурсов; • нарушениями рабочего графика; • иными данными, зарегистрированными программным комплексом. 10.5. Работа с материалами ответа Программный комплекс должен обеспечивать отображение материалов, использованных при формировании ответа интеллектуального помощника. Для каждого сформированного ответа должна обеспечиваться возможность: • просмотра собранных материалов; • копирования результата ответа. 10.6. Поле ввода запросов Программный комплекс должен обеспечивать возможность ввода последующих запросов пользователя в рамках текущего диалога. Поле ввода должно обеспечивать формирование запросов к данным мониторинга на естественном языке. 10.7. Панель материалов Программный комплекс должен обеспечивать отображение панели материалов, использованных при формировании ответа интеллектуального помощника. Панель должна обеспечивать просмотр: • материалов, использованных при формировании текущего ответа; • всех доступных материалов. Для каждой категории отображаемых материалов должно указываться количество доступных объектов. 11. Карточки материалов Каждый материал должен отображаться в виде отдельной карточки, содержащей: • тип материала; • дату и время; • сведения об объекте; • соответствующие табличные данные или параметры; • возможность перехода к первоисточнику. 12. Материалы о посещении web-ресурсов Программный комплекс должен обеспечивать отображение материалов о посещении web-ресурсов со следующими данными: • имя пользователя; • посещенный ресурс; • URL; • используемый браузер; • продолжительность посещения. Для материала должна обеспечиваться возможность: • открытия соответствующего события в журнале; • перехода к ленте событий.
--	---

	13. Материалы о нарушениях рабочего графика Программный комплекс должен обеспечивать отображение материалов о нарушениях рабочего графика с указанием: • сотрудника; • количества опозданий; • количества случаев раннего завершения рабочего времени; • дополнительных числовых показателей. Для соответствующего материала должна обеспечиваться возможность перехода к отчету. 14. Материалы о продуктивности Программный комплекс должен обеспечивать отображение материалов, связанных с продуктивностью работы, с указанием: • сотрудника; • имени учетной записи или компьютера. Для соответствующего материала должна обеспечиваться возможность перехода к отчету. 15. Статистика посещения web-ресурсов Программный комплекс должен обеспечивать отображение статистики посещения web-ресурсов с указанием: • сотрудника; • посещенного сайта; • дополнительных параметров статистики. 16. Контекст обработки запросов Программный комплекс должен обеспечивать отображение информации о текущем контексте обработки запроса интеллектуальным помощником. Должна обеспечиваться возможность отображения: • текущего объема используемого контекста; • количества материалов, использованных при формировании ответа, относительно общего количества доступных материалов. 17. Функции интеллектуального помощника Интеллектуальный помощник должен обеспечивать: • ведение диалога с пользователем на естественном языке; • обработку запросов к данным мониторинга; • формирование аналитических ответов; • поиск и анализ данных из различных источников; • формирование выборок по пользователям; • анализ посещения web-ресурсов; • анализ нарушений рабочего графика; • использование собранных материалов при формировании ответов; • предоставление доступа к первичным данным через журналы событий и отчеты; • копирование результатов анализа; • продолжение диалога с учетом предыдущих запросов и результатов текущего чата. 18. Подсистема хранения данных и отчетности Вся информация, собираемая с контролируемых компьютеров, должна централизованно храниться в базе данных серверной части программного комплекса. Программный комплекс должен обеспечивать: • формирование отчетов по собранным данным; • создание отчетов по расписанию; • экспорт отчетов в распространенные форматы документов. Требования к лицензированию Лицензирование программного комплекса должно осуществляться по количеству одновременно контролируемых компьютеров. Система должна обеспечивать возможность вывода рабочих станций из-под мониторинга и последующего назначения лицензий другим компьютерам без необходимости приобретения дополнительных лицензий. Лицензия на программный комплекс должна предоставляться на бессрочной основе. 19. Требования к консоли администрирования 19.1. Общие настройки подсистемы управления (Панель «Основные») Централизованная консоль администрирования должна обеспечивать конфигурирование следующих параметров функционирования программного комплекса: • Опрос рабочих станций: настройка частоты опроса агентов (в минутах), ввод
--	--

и отображение пароля агента по умолчанию. • Оповещения: настройка времени жизни задач оповещения (в днях) и частоты проверки задач оповещения (в секундах). • Безопасность: настройка минимального процента сходства при анализе текста, а также установка точного времени запуска модуля обнаружения нестандартного поведения. • История: настройка времени хранения истории (в днях). • Планировщик отчетов: задание пути к отчетам на сервере. • Работа сервиса: определение количества потоков. • Прокси-сервер: поддержка использования прокси-сервера с указанием адреса, порта, логина и пароля. • Параметры уведомления по email: настройка адреса SMTP-сервера, логина, пароля, порта, активация использования SSL, отправка тестового письма, а также включение опции отображения всей информации по событию в оповещении. • Telegram bot token: поле для ввода токена Telegram-бота. • Внешний IP сервера: настройка внешнего IP-адреса и порта для опроса через сеть Интернет. • Учетка для получения списка ПК из Active Directory: включение уведомлений о создании новых ПК и пользователей в AD, настройка логина, пароля и периодичности проверки (в часах).

19.2. Подсистема добавления устройств и инвентаризации (Панель «Агенты») Программный комплекс должен обеспечивать управление клиентскими модулями (агентами) со следующими возможностями: • Способы добавления пользователей: сканирование диапазона IP-адресов (с указанием начального и конечного IP), импорт ПК из Active Directory, добавление "remote" пользователей, работа со списком компьютеров, добавление вручную в список, выбор ПК, недавно созданных в Active Directory. • Управление агентами: функции установки и удаления агента, перезагрузка ПК после установки/удаления (с возможностью ручной перезагрузки), добавление и удаление из списка мониторинга, а также ввод данных администратора (имя и пароль). • Контроль статусов: отображение сетевого имени, IP-адреса и статусов («Установлен/ в списке», «Не установлен / нет связи», «Несовпадение версий»). 19.3. Настройки профилей и правил сбора данных (Панель «Контроль») Программный комплекс должен поддерживать создание профилей настроек для ПК и групп пользователей (например, профиль «Basic»), содержащих следующие разделы контроля: • Общие настройки сбора: автостарт и размер логов, основные настройки сбора, скриншоты, внешние накопители, файлы и папки, теневое копирование, internet логи, учет рабочего времени, webcam/microphone. • Параметры теневого копирования: о активация создания теневых копий файлов, копируемых на USB-накопители; о активация создания копий файлов, копируемых на облачные диски; о настройка создания копий файлов, разделенная по признакам: «Копируемых на съемный диск» и «Изменяемых на съемном диске»; о ограничение максимального размера копируемого файла (в МБ); о выделение объема для хранения файлов (в МБ); о настройка логики при переполнении буфера хранения (выбор режима «Не писать новые файлы»). • Настройки безопасности (Контроль приложений): ведение табличных списков с

фиксацией имени exe-файла, заголовка окна, целевого действия (например, «Только оповещение») и комментария. 20. Настройка обнаружения нестандартного поведения Система должна поддерживать поведенческий анализ с возможностью активации оповещений при обнаружении аномальной активности по следующим категориям данных:

- печать документов на принтер;
- посещение web сайтов;
- выгрузка файлов в интернет;
- копирование файлов на съемные накопители;
- общение в мессенджерах (кол-во сообщений);
- переписка в Skype (кол-во сообщений);
- общение в соц сетях (кол-во сообщений);
- переписка по почте (кол-во писем);
- переписка по web почте (через браузер);
- поисковые запросы;
- запуски программ.

Дополнительные параметры анализа должны включать:

- настройку временного интервала для анализа (в рабочих днях);
- выбор режима сравнения: «Сравнивать относительно самого сотрудника» или «Сравнивать относительно группы»;
- фиксацию триггера повышенного потребления CPU за день (более заданного %);
- возможность включения двухфакторной авторизации для администраторов, настройки их учетных записей Windows, IP-адресов, E-mail, логинов и паролей с выбором каналов уведомлений (напрямую, по Telegram, по E-mail).

21. Модуль создания правил работы с файлами (DLP-политики) Система должна обеспечивать создание объектных правил двух типов:

- Тип правила: Ограничение доступа о Применение к типам дисков: «Все типы» либо «Выборочно» (с отдельным выбором чек-боксами: Внутренние (жесткие диски), Съемные накопители, Сетевые диски и шары).
- Слежение по каталогам: поле ввода целевых каталогов/файлов (с поддержкой символа «звездочка *»). о Исключения: поле ввода путей/файлов для исключения из правила. о Адресность: привязка правила к пользователям (с возможностью инверсии правила и ввода учетных записей в формате domain\username) и к конкретным приложениям. о Права доступа: выбор одного из режимов — «Все разрешено», «Запрет доступа», «Только чтение», либо «Режим конфиденциального каталога» (с дополнительными опциями «Запретить коп-е в буфер обмена» и «Запрет печати на принтер»).
- Тип правила: Теневое копирование Обладает аналогичными механизмами привязки к типам дисков (все/выборочно), пользователям, приложениям, отслеживаемым каталогам и исключениям. о Условия создания теневой копии: отдельная активация опций «Запись/редактирование файлов» и «Чтение (открытие) файлов». о Ограничение размера: настройка максимального размера копируемого файла (в МБ).

22. Вход и в консоль администрирования осуществляется после обязательной авторизации. Консоль администрирования должна быть реализована классическим приложением Windows, без необходимости использовать браузер. 23. Требования к консоли просмотра данных Данная веб-консоль позволяет авторизованным пользователям осуществлять просмотр собранных данных мониторинга активности на контролируемых компьютерах. Каждому пользователю предоставляется только та информация и по тем компьютерам, к которым ему разрешён доступ, с разграничением прав на чтение

и редактирование. Консоль обеспечивает мониторинг в реальном времени (клавиатурный ввод, скриншоты экрана, запущенные приложения, файловые операции, посещённые сайты, буфер обмена, печать, USB-устройства, электронная почта, мессенджеры, сетевые сессии, автозагрузка) и содержит мастер отчётов, позволяющий сформировать как отчёты по текущим данным, так и аналитические отчёты, содержащие статистику использования контролируемых компьютеров, программного обеспечения, посещения веб-сайтов, использования принтеров, переписки через программы обмена сообщениями, интернет-соединений, записи микрофона, а также сводные показатели продуктивности работы и нарушения трудовой дисциплины. При нарушении заданных политик безопасности сообщение об этом отображается в специальном окне оповещений. Система также включает полнотекстовый поиск по всем типам данных, управление задачами агентов на рабочих станциях, планировщик автоматических отчётов и панель администратора для настройки параметров сбора данных, пользователей, категорий контента и правил безопасности. Вход в консоль осуществляется после обязательной аутентификации по логину и паролю.

24. Требование к системе оповещения

24.1. Мониторинг, фильтрация событий и отправка оперативных уведомлений

Система должна обеспечивать непрерывный мониторинг, сбор, классификацию и фильтрацию событий информационной безопасности и активности пользователей по следующим категориям:

- набираемый текст (активность клавиатуры);
- программы (использование приложений);
- файловая система (операции с файлами);
- установка и удаление программ;
- буфер обмена;
- посещённые сайты;
- теневая копия (резервное копирование файлов);
- подключение и отключение носителей информации;
- активное оповещение;
- почта (электронная почта E-mail);
- сеть: файлы (сетевая файловая активность);
- мессенджеры;
- социальные сети;
- web почта;
- выгружаемые файлы;
- принтер (статистика печати);
- мессенджеры: файлы (передача файлов в мессенджерах);
- изменения оборудования (аппаратного обеспечения);
- новый ПК из AD (интеграция с Active Directory);
- поисковые запросы;
- работа ПК;
- отсутствие актуальных данных (контроль доступности агентов).

Система должна обеспечивать выборку, поиск и фильтрацию данных в консоли управления со следующими возможностями:

- настройка произвольного временного интервала выборки данных с точностью до минут (по дате и времени начала/окончания периода);
- фильтрация данных по категориям событий;
- фильтрация данных по статусу верификации событий (все события, только подтвержденные, не подтвержденные);
- контекстный поиск по ключевым словам;
- экспорт сформированных выборок данных во внешние форматы.

Система должна обеспечивать ведение профилей администраторов (контроллеров) безопасности с фиксацией следующих параметров:

- учетная запись Windows (локальная или доменная);
- IP-адрес администратора;
- адрес электронной почты (E-mail);
- логин и пароль для доступа к консоли управления.

Система должна поддерживать обеспечение

	безопасности доступа к консоли управления администратора с возможностью включения двухфакторной авторизации. Система должна обеспечивать отправку оперативных уведомлений администраторам о зарегистрированных событиях и инцидентах. Модуль уведомлений должен поддерживать: • включение и отключение функции активного оповещения; • включение и отключение функции оповещения о нестандартном (аномальном) поведении пользователей; • индивидуальную настройку подписки администратора на оповещения по любой из контролируемых категорий событий; • доставку уведомлений по трем независимым каналам: о напрямую в консоль управления (прямые уведомления); о в мессенджер Telegram (с поддержкой привязки через специализированный Telegram-бот); о на адрес электронной почты (E-mail). 25. Требования к системе активного реагирования 25.1. Подсистема активного реагирования Программный комплекс должен обеспечивать автоматическое выполнение действий реагирования при возникновении контролируемых событий информационной безопасности и активности пользователей. Подсистема должна обеспечивать создание, редактирование, удаление, включение и отключение правил активного реагирования. Каждое правило должно содержать одно условие срабатывания и одно действие реагирования. Для каждого правила должна обеспечиваться настройка следующих параметров: • наименование правила; • признак активности правила; • событие, инициирующее выполнение действия; • пользователи, компьютеры или группы пользователей, на которых распространяется действие правила; • параметры выполнения выбранного действия. Поддерживаемые события должны включать: • подключение USB-накопителей; • копирование файлов на съемные носители; • запуск запрещенного приложения (в соответствии с правилами подсистемы «Безопасность»); • запуск выбранного приложения с возможностью указания списка контролируемых программ; • открытие web-сайта с возможностью указания списка контролируемых сайтов; • ввод заданного ключевого слова или фразы с клавиатуры с возможностью формирования списка контролируемых выражений; • копирование данных в буфер обмена; • авторизация пользователя на контролируемом компьютере; • начало периода простоя компьютера; • окончание периода простоя компьютера; • отправка сообщения в поддерживаемом мессенджере. Поддерживаемые действия реагирования должны включать: • создание одного или нескольких снимков экрана с возможностью настройки количества снимков и интервала между ними; • вывод информационного сообщения пользователю с возможностью задания произвольного текста уведомления; • завершение пользовательского сеанса с возможностью настройки задержки выполнения; • выключение контролируемого компьютера с возможностью настройки задержки выполнения; • создание одного или нескольких снимков с веб-камеры с возможностью настройки количества снимков и интервала между ними; • запись аудио с микрофона с возможностью настройки продолжительности записи; • запись видео с веб-камеры с возможностью настройки продолжительности записи; • запуск
--	--

	внешней программы с возможностью указания исполняемого файла и параметров командной строки; • выполнение пользовательского сценария (скрипта) на языке PowerShell. Для действий реагирования должна обеспечиваться возможность настройки следующих параметров: • количество создаваемых снимков экрана; • интервал между созданием снимков экрана; • текст выводимого пользователю сообщения; • задержка перед завершением пользовательского сеанса; • задержка перед выключением компьютера; • количество создаваемых снимков с веб-камеры; • интервал между созданием снимков с веб-камеры; • продолжительность записи аудио; • продолжительность записи видео; • путь к исполняемой программе и параметры ее запуска; • текст выполняемого PowerShell-сценария. 26. Требования к подсистеме отчетов 26.1. Формирование, планирование и доставка отчетов Система должна обеспечивать формирование отчетов и выборку данных за настраиваемые периоды времени: 1, 2, 3, 5, 7, 10, 15, 30, 45, 60, 90, 120, 182 и 365 дней, а также только за рабочее время пользователя. Система должна поддерживать формирование следующих отчетов и выборок данных: • время работы компьютера и приложений; • теневое копирование файлов; • электронная почта (E-mail); • буфер обмена; • выгрузка файлов; • изменения аппаратного обеспечения; • переписка в мессенджерах (с возможностью детализации); • поисковые запросы; • посещенные веб-сайты; • работа с веб-почтой; • использование внешних накопителей; • активность клавиатуры; • работа за компьютером; • использование приложений; • использование принтеров и статистика печати; • использование социальных сетей; • сетевая активность; • скриншоты; • установленные и удаленные программы; • операции с файловой системой; • лента активности пользователей; • нарушения трудовой дисциплины; • отчет по выгрузке файлов; • отчет по использованию мессенджеров; • отчет по использованию электронной почты; • отчет по посещенным веб-сайтам; • отчет по продуктивности работы компьютера; • отчет по использованию программ; • суммарный отчет по рабочему времени; • сводный отчет по компьютеру, продуктивности и использованию принтеров; • табель рабочего времени; • тепловая карта активности пользователей. Система должна обеспечивать автоматическое формирование отчетов по расписанию с возможностью: • выбора пользователей и компьютеров, по которым формируется отчет; • настройки времени запуска задания; • выбора периодичности выполнения (ежедневно, еженедельно или ежемесячно); • выбора дней недели для выполнения задания; • фильтрации данных по заданному перечню приложений; • сохранения и редактирования параметров расписания. Система должна обеспечивать экспорт сформированных отчетов в форматы PDF, XLS и RTF. Система должна обеспечивать автоматическую отправку сформированных отчетов по электронной почте с возможностью: • включения или отключения функции отправки; • указания одного или нескольких адресов электронной почты получателей; отправки отчетов в выбранном формате согласно установленному расписанию. 27.
--	---

	Требования к оборудованию, программному обеспечению и поставщику 27.1. Все предложенные характеристики оборудования и программного обеспечения должны соответствовать или превосходить минимальные технические характеристики, указанные в данной технической спецификации; 27.2. Для оказания Услуги потенциальный поставщик обязан предоставить подтверждающие документы от производителя или их официальных представителей (дилеров или дистрибьюторов) в составе конкурсной заявки. 27.3. Срок оказания услуги: со 2 ноября 2026 года по 17 ноября 2026 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)	