ТЕХНИКАЛЫҚ СИПАТТАМА

1271653 сатып алу бойынша
Бағалы ұсыныстарға сұраным тәсілімен

Лот № (19 У, 4584171) Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер

Тапсырыс беруші: "Құрық Порты" ЖШС
Ұйымдастырушы: "Құрық Порты" ЖШС

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	19 У
Атауы және қысқаша сипаттамасы	Бағдарламалық жасақтама қолдану құқығына лицензия ұсыну бойынша қызмет көрсетулер, Бағдарламалық қамтамасыз етуді пайдалану құқығына лицензия беру бойынша қызметтер
Қосымша сипаттама	DLP ақ бағдарламалық жасақтамасын пайдалану құқығы 1 жыл
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Маңғыстау облысы, Қарақия ауданы, Құрық с.о., Құрық с., участок Сарша, строение 636
Жеткізу шарттары	-
Жеткізу мерзімі	01.2027 бастап 12.2027 дейін (қоса алғанда)
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

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

№ п/п	**Мазмұны**
1	Сатып алынатын қызметтердің сипаттамасы
	1.1. **153 жұмыс орнына арналған "DLP-жүйе"** бағдарламалық қамтамасыз етуді пайдалану құқығына лицензиялар беру жөніндегі қызметтер. Жазылу мерзімі-1 жыл.
2	**Сатып алынатын қызметтердің талап етілетін функционалдық, техникалық, сапалық, пайдалану сипаттамалары.**
	2.1. Жүйенің жалпы сипаттамасы, сипаттамасы.

БҚ жүйелердің корпоративтік класына (Enterprise DLP) жатуы тиіс және оның түпкі нүктелерде орнатылған агенттің көмегімен құпия деректердің ағып кетуінен түпкі нүктелерді қорғау функционалы (EndPoint DLP), сондай-ақ желілік арналар бойынша құпия деректердің ағып кетуін бақылау функционалы (Network DLP) болуы тиіс.

БҚ жұмыс станциялары мен файлдық серверлердегі құпия ақпаратты іздеу мүмкіндігін қамтамасыз етуі тиіс (табылған файлдарды карантинге ауыстыру және мұндай файлдардың орнына осылай ауыстырылу себептері туралы ақпаратты / мәтіндік файлдарды қалдыру мүмкіндігімен).

БҚ құпия ақпараттың ықтимал ағып кетуінің келесі арналарын бақылауы тиіс:

- шығыс SMTP-қосылымдары;
- шығыс HTTP-қосылымдары;
- шығыс HTTPS-қосылымдары;
- шығыс IM-қосылымдары (лездік хабарлама алмасу арналары);
- сыртқы ақпарат тасымалдаушыларға және ақпараттық ресурстарға ақпаратты көшіру;
- жергілікті / желілік принтерде ақпаратты басып шығару.

БҚ келесі функционалдық мүмкіндіктерді қамтамасыз етуі тиіс:

- корпоративтік пошта жүйесі арқылы құпия ақпараттың жария етілуінің алдын алу;
- құпия ақпаратты қамтитын шығыс хаттарды бұғаттау мүмкіндігі;
- Интернет желісіне корпоративтік қолжетімділік жүйесі арқылы құпия ақпараттың жария етілуінің алдын алу;
- HTTP- / HTTPS-трафиктен құпия ақпаратты алу (бөліп шығару) мүмкіндігі;
- HTTP- / HTTPS-трафикті бұғаттау мүмкіндігі;
- құпия ақпараттың жария етілуінің алдын алу және ағып кету арналарына мониторинг жүргізу, атап айтқанда: құпия ақпаратты желілік папкадан жергілікті қатты дискілерге көшіру, құпия ақпаратты сыртқы тасымалдаушыларға көшіру, құпия ақпаратты жергілікті және желілік басып шығаруға, сондай-ақ факс арқылы жіберу, көшіру / қою операциялары кезінде алмасу буферінің мазмұнын қорғау;
- құпия ақпараттың болуына желінің түпкі түйінінің жергілікті қатты дискілерін сканирлеу (соның ішінде белгіленген кесте бойынша) және табылған файлдарды ауыстыру мүмкіндігі;
- графикалық объектілердегі (PDF-файлдар, кескіндер және т.б.) мәтіндік ақпаратты, сондай-ақ осындай объектілердегі графикалық бейнелерді (жауапты тұлғалардың қолдарын, штамптарды, логотиптерді және т.б.) тану мүмкіндігі;
- құпия деректерді сканирлеу және олардан «цифрлық таңбалар» алу мүмкіндігі;
- ұсынылған құпия құжаттар бойынша өздігінен үйрену (өздігінен оқыту) және кейіннен ұқсас құжаттарды бұғаттау мүмкіндігі.
- түпкі түйін корпоративтік желіден ажыратылған немесе желімен байланыс үзілген жағдайда, БҚ клиенттері мен модульдерінің (анықтау серверлерінің) автономды жұмыс істеу мүмкіндігі;
- қауіпсіздік саясаттарын орталықтандырылған түрде әкімшілендіру (басқару) мүмкіндігі;
- БҚ қауіпсіздік саясатына нақты уақыт режимінде жедел өзгерістер енгізу, қолданыстағы ережелерді, баптауларды өзгерту және жаңаларын қосу мүмкіндігі;
- БҚ саясаттарының бұзылуы туралы автоматты хабарламаларды баптау;
- қауіпсіздік саясатының бұзылуына әртүрлі әрекет ету (жауап қайтару) нұсқаларын баптау;
- қауіпсіздік саясаттарының бұзылу күндері мен фактілері бойынша есептерді баптау және генерациялау (құрастыру);
- басқару консолімен орыс немесе украин тілдерінде жұмыс істеу мүмкіндігі;
- басқару консолінде аутентификация жасау үшін қолданыстағы Active Directory тіркелгілерін пайдалану мүмкіндігі;
- AD тіркелгілерінің атрибуттарын (аты-жөні, телефоны, департаменті, лауазымы және т.б.) тікелей БҚ басқару консолінен қарау мүмкіндігі.

2.2. Сервистерді ұсыну шарттары.

Операцияларды бақылау мүмкіндігі:

- құпия ақпаратты (бұдан әрі – ҚА) ауыстырмалы тасымалдаушыларға (USB, CompactFlash, SD) жазу;
- қосымша модульдерді өрбітусіз (орнатпай-ақ) кірістірілген «Device Control» функционалының болуы;
- ҚА басып шығару (желілік және жергілікті принтерлер);
- ҚА алмасу буферіне көшіру;
- ҚА CD / DVD-ге жазу;
- қолданбалардың (қолданбалы бағдарламалардың) ҚА-ға жүгінуін бақылау (соның ішінде құрамында ҚА бар файлдарды Skype және Teams арқылы беру);
- ҚА деректерін HTTP протоколы арқылы жіберу;
- ҚА деректерін HTTPS протоколы арқылы жіберу;
- пошта клиенттері деңгейінде SMTP-ні бақылау;
- ҚА файлдарын желілік ресурстарға, соның ішінде Office 365 ресурстары мен сервистеріне көшіру;
- түпкі нүктелердегі агентке оның орналасқан жері бойынша (корпоративтік желіде немесе корпоративтік желіден тыс жерде) саясаттар мен конфигурацияларды баптау және қолдану мүмкіндігі;
- сыртқы тасымалдаушыларға құжаттардың жаппай көшірілуін бақылау мүмкіндігі. Жүйе белгіленген уақыт кезеңі ішінде пайдаланушы сыртқы тасымалдаушыға көшіре алатын файлдар санын бақылауы тиіс;
- сыртқы тасымалдаушыларға көшіру кезінде құжаттарды шифрлау мүмкіндігі. Құпия сөзді пайдаланушының да, БҚ әкімшісінің де орнату мүмкіндігі;
- MTP протоколын бұғаттау мүмкіндігі.

(бақылау ұғымы сәйкесінше белгіленген саясаттарға сәйкес ҚА анықтау (детекциялау), сондай-ақ ҚА бұғаттау (беруге кедергі келтіру) мүмкіндігін білдіреді)

- қосымша модульдерді өрбітусіз (орнатпай-ақ) кірістірілген «Device Control» функционалының болуы;
- ҚА басып шығару (желілік және жергілікті принтерлер);
- ҚА алмасу буферіне көшіру;
- ҚА CD / DVD-ге жазу;
- қолданбалардың ҚА-ға жүгінуін бақылау (соның ішінде құрамында ҚА бар файлдарды Skype және Teams арқылы беру);
- ҚА деректерін HTTP протоколы арқылы жіберу;
- ҚА деректерін HTTPS протоколы арқылы жіберу;
- пошта клиенттері деңгейінде SMTP-ні бақылау;
- ҚА файлдарын желілік ресурстарға, соның ішінде Office 365 ресурстары мен сервистеріне көшіру;
- түпкі нүктелер деңгейінде орталықтандырылған бұғаттау мүмкіндігімен PrintScreen экранын скриншоттау функциясын бақылау;
- түпкі нүктелердегі агентке оның орналасқан жері бойынша (корпоративтік желіде немесе корпоративтік желіден тыс жерде) саясаттар мен конфигурацияларды баптау және қолдану мүмкіндігі;
- сыртқы тасымалдаушыларға құжаттардың жаппай көшірілуін бақылау мүмкіндігі. Жүйе белгіленген уақыт кезеңі ішінде пайдаланушы сыртқы тасымалдаушыға көшіре алатын файлдар санын бақылауы тиіс;
- сыртқы тасымалдаушыларға көшіру кезінде құжаттарды шифрлау мүмкіндігі. Құпия сөзді пайдаланушының да, БҚ әкімшісінің де орнату мүмкіндігі;
- MTP/PTP протоколын бұғаттау мүмкіндігі.

(бақылау ұғымы белгіленген саясаттарға сәйкес ҚА анықтау (детекциялау), сондай-ақ ҚА бұғаттау (беруге кедергі келтіру) мүмкіндігін білдіреді)

- жүйенің барлық анықтау модульдерін Windows және Linux ОЖ-де өрбіту (орнату) мүмкіндігі.

Инциденттерге әрекет ету (жауап қайтару) мүмкіндігі: жауапты тұлғаны немесе ақпарат иесін автоматты түрде хабарландыру, электрондық пошта арқылы жіберуді бұғаттау, веб-формалар арқылы деректерді жіберуді бұғаттау, скриптті орындау, құпия ақпаратты жою.

Инцидентті эскалациялау және қосымша әрекеттерді (ҚА шифрлау, ҚА ауыстыру және т.б. сияқты) іске қосу мүмкіндігі.

Оптикалық таңбаларды тану (OCR - Optical Character Recognition) бөгде өндірушілердің қосымша бағдарламалық қамтамасыз етуін пайдаланбай, кірістірілген технология / механизм арқылы қамтамасыз етілуі тиіс, ол агент деңгейінде болуы тиіс.

Мәтінді тану ағылшын, қазақ және орыс тілдерін қолдай отырып, латын және кириллица әліпбилерін қолдауы тиіс.

Келесі форматтардағы сканирленген бейнелерді тану және түрлендіру: PDF, BMP, JPEG, PNG, TIFF.

OCR жұмыс істеу бағыттары:

- жергілікті сканирлеу;
- ҚА сыртқы тасымалдаушыларға көшіру;
- ҚА Файлдар серверіне көшіру;
- ҚА HTTP / HTTPS арқылы жіберу;
- ҚА Webmail протоколы арқылы жіберу;
- SMTP протоколы арқылы жіберу.

Пайдаланушылардың USB-ге қолжетімділік деңгейін реттеу мүмкіндігі.

Түпкі нүктелер модулін Ubuntu және CentOS жүйелерінде келесі мүмкіндіктермен өрбіту (орнату) мүмкіндігі:

- тыныштық күйіндегі (сақтаудағы) ҚА анықтау;
- ҚА сыртқы тасымалдаушыларға ағып кетуін бақылау, соның ішінде осындай ақпаратты бұғаттау және журналға жазу (логирование);
- ҚА HTTP / HTTPS арналары арқылы ағып кетуін бақылау;
- ҚА Webmail протоколы арқылы ағып кетуін бақылау.

БҚ пайдаланушы компьютерге USB жинақтауышын қосқан кезде әкімшіні алдын ала (превентивті) ақпараттандыру мүмкіндігін қолдауы тиіс.

БҚ агенті жасырын (стелс) режимде жұмыс істеуді қолдауы тиіс, барлық процестер түпкі пайдаланушыдан жасырылуы тиіс.

2.3. Интерфейске қойылатын талаптар.

БҚ келесі интерфейс тілдерін қолдауы тиіс: ағылшын, орыс, қазақ;

БҚ жүйені және инциденттерді басқарудың біраңғай Web-интерфейсін қолдауы тиіс;

Шешім интерфейсінің көмегімен түпкі нүктелер агенттерін жою мүмкіндігі болуы тиіс;

Шешім интерфейсінің көмегімен түпкі нүктелер агенттерін жаңарту мүмкіндігі болуы тиіс.

2.4. Жіктеуге (классификациялауға) қойылатын талаптар.

БҚ Microsoft Office және Microsoft Outlook файлдарын жіктеуді қолдауы тиіс;

Жіктеу файлды жапқан кезде емес, сақтау кезінде жүзеге асырылуы тиіс;

БҚ тыныштық күйіндегі және нақты уақыт режимінде деректерді іздеу кезінде мәтіндік құжаттар мен кескіндерді жіктеуді қолдауы тиіс;

БҚ Outlook шақыруларын (шақыру қағаздарын /кездесулерді) жіктеуді қолдауы тиіс;

БҚ деректерді жіктеу кезінде құжатқа су белгісін (водяной знак) қою мүмкіндігін қолдауы тиіс;

БҚ желілік қоймаларды аудиттен өткізу мүмкіндігін қолдауы тиіс, файлдарды ашу, өзгерту, жою, атауын өзгерту әрекеттеріне мониторинг жүргізілуі тиіс;

БҚ басып шығару операциясы кезінде құжаттарды жіктеуі тиіс;

БҚ орналасқан жерін, көрінуін таңдау мүмкіндігімен, сондай-ақ бүкіл экранға су белгісін қою мүмкіндігімен пайдаланушы экранына су белгісін қою мүмкіндігіне ие болуы тиіс;

БҚ нақты уақыт режимінде тек файлдарды ғана емес, сонымен қатар папкаларды да жіктеуі тиіс;

БҚ алмасу буфері деңгейінде файлдарды көшіруді бақылауы тиіс және файлды жіктеу деңгейіне байланысты мұндай операцияны бұғаттау мүмкіндігі болуы тиіс;

БҚ Microsoft Office файлдарының экранын түсіруді (скриншот жасау) бақылауы тиіс және жіктелген файлдар үшін экранды түсіру әрекетін бұғаттауы тиіс.

2.5. Қосымша талаптар.

БҚ арнайы стандартты хаттамалардың (MTA) көмегімен үшінші тарап пошта сервистерімен интеграцияны қолдауы тиіс;

БҚ арнайы стандартты хаттамалардың (ICAP) көмегімен үшінші тарап веб-сервистерімен (шлюздерімен) интеграцияны қолдауы тиіс;

БҚ орталықтандырылған БҚ консолінде осындай ортадағы ҚА-ға байланысты инциденттерді қарау мүмкіндігімен Office 365 бұлтты ортасымен интеграцияны қолдауы тиіс. Соның ішінде OneDrive және OneDrive for Business ішіндегі файлдармен жұмыс істеу мүмкіндігі;

Қатысушы техникалық қолдау (ТҚ) аясында Тапсырыс берушіде жүйені және оның құрамдас бөліктерін пайдалану және әкімшілендіру бойынша консультациялық қолдау көрсете отырып, жүйені толық көлемде енгізуді және баптауды қамтамасыз етуге тиіс.

Жүйенің техникалық қолдауына (ТҚ) қойылатын талаптар:

	• ТҚ 24х7 режимінде қамтамасыз етілуі тиіс; • ТҚ орыс тілінде ұсынылуы тиіс; • Жүйені және оның құрамдас бөліктерін пайдалану және әкімшілендіру бойынша Тапсырыс берушінің кемінде үш маманына консультациялық қолдау көрсете отырып, Тапсырыс берушіде жүйені толық көлемде енгізу, баптау және жаңарту; • Құпия ақпараттың ағып кетуінің алдын алу (жүйесін) орнату және баптау бойынша Тапсырыс берушінің персоналына (кемінде 3 адам) техникалық консультациялар өткізу; Off Premise DLP функциясының болуы, орталық консольге қосылған кезде агент бір қорғаныс саясатын қолдануы тиіс, ал оффлайн режимінде басқа саясаттарды қолдануы тиіс; Агенттің көмегімен трафиккке интерцепция (ұстап алу) жасау пайдаланушының браузеріне плагин орнату арқылы жүзеге асырылмауы тиіс; Жүйе әрбір функция үшін жеке файлды сканирлеудің максималды уақытын белгілеу мүмкіндігіне ие болуы тиіс; Active Directory-ге тәуелсіз (байланыстырмай) өз топтарын құру мүмкіндігі болуы тиіс; БҚ белгілі một сайттар үшін пакеттерді ашпастан инспекцияны толық елемеуді қолдану мүмкіндігіне ие болуы тиіс; Өтінім құрамында Қазақстан Республикасының аумағында лицензиялық бағдарламалық қамтамасыз етуді өндіруші компаниядан тапсырыс берушінің атына жеткізу құқығына өндірушінің авторизацияланған хатын міндетти түрде ұсыну; Ұсынылып отырған бағдарламалық қамтамасыз ету мен осы техникалық спецификацияның сәйкестігін салыстыру үшін әлеуетті жеткізуші өтінім құрамында жүйенің бағдарламалық қамтамасыз ету өндірушісін және ұсынылатын жүйенің атауын, құқық иеленушінің сайтын, ұсынылатын лицензиялар мен сервистердің SKU (партномерлерін) көрсетуі тиіс.

Қол қойған Измуратов Олжас Амандыкович
Қол қойылған күні 13.11.2026

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1271653
способом Запрос ценовых предложений

Лот № (19 У, 4584171) Услуги по предоставлению лицензий на право использования программного обеспечения

Заказчик: Товарищество с ограниченной ответственностью "Порт Курык"

Организатор: Товарищество с ограниченной ответственностью "Порт Курык"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	19 У
Наименование и краткая характеристика	Услуги по предоставлению лицензий на право использования программного обеспечения, Услуги по предоставлению лицензий на право использования программного обеспечения
Дополнительная характеристика	Право использования программного обеспечения ИБ DLP 1 год
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, Мангистауская область, Каракиянский район, Курыкский с.о., с.Курык, участок Сарша, строение 636
Условия поставки	-
Срок поставки	с 01.2027 по 12.2027 (включительно)
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

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

№ п/п	
1	**Описание закупаемых услуг**
	1. Услуги по предоставлению лицензий на право использования программного обеспечения **«DLP-система» на 153 рабочих мест.** Срок подписки – 1 год.
2	**Требуемые функциональные, технические, качественные, эксплуатационные характеристики закупаемых услуг**
	2.1. Общая характеристика, описание системы.

ПО должно относиться к корпоративному классу систем (Enterprise DLP) и иметь как функционал защиты конечных точек от утечек конфиденциальных данных с помощью установленного на конечные точки агенту (EndPoint DLP), так и функционал контроля утечки конфиденциальных данных по сетевым каналам (Network DLP).

ПО должно обеспечивать возможность поиска конфиденциальной информации, находящейся на рабочих станциях и файловых серверах (с возможностью перемещения найденных файлов в карантин и оставление на месте таких файлов информации / текстовых файлов / о причинах такого перемещения).

ПО должно контролировать следующие каналы потенциального утечки конфиденциальной информации:

• исходящие SMTP-соединения;

• исходящие HTTP-соединения;

• исходящие HTTPS-соединение;

• исходящие IM-соединения;

• копирования информации на внешние носители информации и информационные ресурсы;

• печать информации на локальном \ сетевом принтере.

ПО должно обеспечивать следующие функциональные возможности:

- предотвращения разглашения конфиденциальной информации через корпоративную почтовую систему;
- возможность блокировки исходящих писем, содержащих конфиденциальную информацию;
- предотвращения разглашения конфиденциальной информации через корпоративную систему доступа в сеть Интернет;
- возможность извлечения конфиденциальной информации с HTTP- / HTTPS-трафика;
- возможность блокировки HTTP- / HTTPS-трафика;
- предотвращения разглашения конфиденциальной информации и мониторинг каналов утечки, а именно: копирование конфиденциальной информации с сетевой папки на локальные жесткие диски, копирование конфиденциальной информации на съемные носители, отправка конфиденциальной информации на локальную и сетевую печать, а также по факсу, защита содержимого буфера обмена при операциях копирования / вставки;
- возможность сканирования (в том числе - по заданному расписанию) локальных жестких дисков конечного узла сети на предмет конфиденциальной информации с возможностью перемещения найденных файлов;

- возможность распознавания текстовой информации находящейся в графических объектах (pdf-файлы, изображения и т.д.), а также графических образов в таких объектах (подписей ответственных лиц, штампов, логотипов и т.п.);
- возможность сканирования конфиденциальных данных и снятия с них «цифровых отпечатков»;
- возможность самообучения на предоставленных конфиденциальных документах, с последующим блокированием похожих документов;
- возможность автономной работы клиентов и модулей ПО (серверов детектирования), в случае отключения конечного узла от корпоративной сети или потери соединения с сетью;
- возможность централизованного администрирования политик безопасности;
- возможность оперативного внесения изменений в режиме реального времени в политике безопасности ПО, изменения существующих и добавление новых правил, настроек;
- настройка автоматических сообщений о нарушениях политик ПО;
- настройки различных вариантов реагирования на нарушения политики безопасности;
- настройка и генерацию отчетов по датам, фактам нарушения политик безопасности;
- возможность работать с консолью управления на русском или украинском языке;
- возможность использовать учетные записи существующей Active Directory для аутентификации в консоли управления;

• возможность просмотра атрибутов учетных записей AD (имя, телефон, департамент, должность и т.д.) непосредственно из консоли ПЗ.

2.2. Технические требования.

Возможность контроля операций:

• Запись конфиденциальной информации (далее - КИ) на съемные носители (USB, CompactFlash, SD);

• Встроенный функционал «Device Control», без необходимости развертывания (установки) дополнительных модулей;

• Печать КИ (сетевые и локальные принтеры);

• Копирование КИ в буфер обмена;

• Запись КИ на CD / DVD;

• Контроль обращения приложений к КИ (в том числе передача файлов, содержащих КИ через Skype, и Teams;

• Отправка КИ данных через HTTP протокол;

• Отправка КИ данных через HTTPS протокол;

• Контроль SMTP на уровне почтовых клиентов;

• Копирование КИ файлов на сетевые ресурсы, в том числе ресурсы и сервисы Office 365;

• Возможность настройки и применения политик, и конфигураций агенту на конечных точках по месту нахождения: в корпоративной сети, или за пределами корпоративной сети;

• Возможность контроля массового копирования документов на внешние носители. Система должна контролировать количество файлов пользователь может копировать на внешний носитель в течение установленного периода времени;

• Возможность шифрования документов при копировании на внешние носители. Возможность установки пароля как пользователем так и администратором ПО;

• Возможность блокировки протокола MTP.

(под контролем подразумевается возможность как детектирования КИ так и блокировки (препятствование передачи) КИ (в соответствии с заданными политик))

Возможность контроля операций:

• Запись конфиденциальной информации (далее - КИ) на съемные носители (USB, CompactFlash, SD);

• Встроенный функционал «Device Control», без необходимости развертывания (установки) дополнительных модулей;

• Печать КИ (сетевые и локальные принтеры);

• Копирование КИ в буфер обмена;

• Запись КИ на CD / DVD;

• Контроль обращения приложений к КИ (в том числе передача файлов, содержащих КИ через Skype, и Teams;

• Отправка КИ данных через HTTP протокол;

• Отправка КИ данных через HTTPS протокол;

• Контроль SMTP на уровне почтовых клиентов;

• Копирование КИ файлов на сетевые ресурсы, в том числе ресурсы и сервисы Office 365;

• Контроль функции скриншот экрана PrintScreen, с возможностью централизованной блокировки на уровне конечных точек.

• Возможность настройки и применения политик, и конфигураций агенту на конечных точках по месту нахождения: в корпоративной сети, или за пределами корпоративной сети.

• Возможность контроля массового копирования документов на внешние носители. Система должна контролировать количество файлов пользователь может копировать на внешний носитель в течение установленного периода времени.

• Возможность шифрования документов при копировании на внешние носители. Возможность установки пароля как пользователем так и администратором ПО.

• Возможность блокировки протокола MTP/PTP.

(под контролем подразумевается возможность как детектирования КИ так и блокировки (препятствование передачи) КИ (в соответствии с заданными политик))

Возможность развертывания (установки) всех модулей детектирования системой на ОС Windows и Linux.

Возможность реакции на инциденты: автоматическое сообщение ответственного лица или владельца информации, блокирование отправки по электронной почте, блокировка отправки данных через веб-формы, выполнение скрипта, удаления конфиденциальной информации.

Возможность эскалации инцидента и запуска дополнительных действия (таких как шифрование КИ, перемещения КИ и т.д.).

Распознавания (OCR - Optical Character Recognition), должно обеспечиваться встроенной технологии \ механизмом без использования дополнительного программного обеспечения сторонних производителей, он должен быть на уровне агента.

Распознавание текста должно поддерживать латинский и кириллический алфавит со поддержкой английского, казахского и русского языков.

Распознавания и преобразования отсканированных образов в следующих форматах: PDF, BMP, JPEG, PNG, TIFF.

Направления работы OCR:

• Локальное сканирование;

• Копирование КИ на внешние носители;

• Копирование КИ на Файловый сервер;

• Отправка КИ через HTTP / HTTPS;

• Отправка КИ через Webmail протокол;

• Отправка через SMTP протокол;

Возможность регулировать уровень доступа пользователей к USB.

Возможность развертывания модуля конечных точек на системах Ubuntu и Centos с возможностью:

• Выявление КИ которая находится в состоянии покоя;

• Контроль утечки КИ на сменные носители в том числе блокировку и логирования такой информации;

• Контроль утечки КИ через HTTP / HTTPS каналы;

• Контроль утечки КИ через Webmail протокол.

ПО должно поддерживать возможность превентивного информирования администратора когда пользователь вставляет USB накопитель в компьютер.

Агент ПО должно поддерживать работу в стелс режиме, все процессы должны быть скрыты от конечного пользователя.

2.3. Требования к интерфейсу.

ПО должно поддерживать следующие языки интерфейса: английский, русский, казахский;

ПО должно поддерживать единый Web-интерфейс управления системой и инцидентами;

Должна присутствовать возможность удаления агентов конечных точек с помощью интерфейса решения;

Должна присутствовать возможность обновления агентов конечных точек с помощью интерфейса решения.

2.4. Требования к классификации.

ПО должно поддерживать классификацию файлов Microsoft Office и Microsoft Outlook;

Классификация должна осуществляться при сохранении файла, а не при закрытии;

ПО должно поддерживать классификацию текстовых документов и изображений при поиске данных в состоянии покоя и в реальном времени;

ПО должно поддерживать классификацию приглашений Outlook;

ПО должно поддерживать возможность ставить водяной знак на документ при классификации данных;

ПО должно поддерживать возможность аудита сетевых хранилищ, должен производиться мониторинг открытия, изменения, удаления, переименования файлов;

ПО имеет классифицировать документы во время операции печати;

ПО должно иметь возможность ставить водяной знак на экран пользователя с возможностью выбора позиции, видимости, а также возможностью ставить водяной знак на весь экран;

ПО должно классифицировать не только файлы а и папки в режиме реального времени;

ПО должно контролировать копирование файлов на уровне буфера обмена и иметь возможность блокировать такую операцию в зависимости от уровня классификации файла;

ПО должно контролировать снимок экрана файлов Microsoft Office и блокировать попытку снимка экрана для классифицированных файлов.

2.5. Дополнительные требования.

ПО должно поддерживать интеграцию со сторонними почтовыми сервисами с помощью специализированных стандартных протоколов (MTA);

ПО должно поддерживать интеграцию с посторонними веб-сервисами (шлюзами) с помощью специализированных стандартных протоколов (ICAP);

ПО должно поддерживать интеграцию с облачным средой Office 365 с возможностью просмотра инцидентов, связанных с КИ в такой среде в централизованной консоли ПО. В том числе возможность работы с файлами внутри OneDrive и OneDrive for Business;

Участник должен иметь возможность обеспечить в рамках технической поддержки (ТП) внедрение и настройка системы у Заказчика в полном объеме с предоставлением консультационной поддержки, по эксплуатации и администрирования системы и ее составляющих.

Требования к ТП системы:

• ТП должно обеспечиваться в режиме 24х7;

• ТП должна предоставляться на русском языке;

• Внедрение, настройка и обновление системы у Заказчика в полном объеме с предоставлением консультационной поддержки не менее чем трем специалистам Заказчика, по эксплуатации и администрирования системы и ее составляющих;

• Проведение технических консультаций персонала Заказчика (не менее 3х человек) по установке и настройке (системы) предотвращение утечки конфиденциальной информации;

	Наличие функции Off Premise DLP, при подключении к центральной консоли агент должен применять одни политики защиты, при оффлайн режима применять другие политики; Перехват трафика с помощью агента должно осуществляться не с помощью установки плагина на браузер пользователя; Система должна иметь возможность задать максимальное время сканирования файла для каждой функции в отдельности; Должна присутствовать возможность создавать свои группы без привязки к Active Directory; ПО должно иметь возможность применять полное игнорирование инспекции без вскрывания пакетов для определенных сайтов; Обязательное предоставление в составе заявки авторизованного письма от производителя на право поставки на имя заказчика от компании-производителя лицензионного программного обеспечения на территории Республики Казахстан. Для сопоставления соответствия предлагаемого программного обеспечения и настоящей технической спецификации потенциальный поставщик в составе заявки должен указать производителя программного обеспечения системы и наименование предлагаемой системы, сайт правообладателя, SKU (партномеры) предлагаемых лицензии и сервисов.

Подписал Измуратов Олжас Амандыкович

Дата подписания 13.11.2026