

Reg.No

"O'zbekneftgaz" AJ
 "Shurtan gaz kimyo majmuasi" MChJ
 MTRB xizmati
RO'YXATGA OLINDI
 0741054-4604
 2024 yil "19" 09

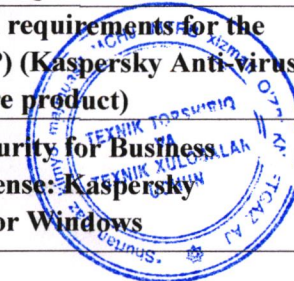
TASDIQLAYMAN
 "Sho'rtan GKM" MChJ
 Bosh direktor o'rinbosari

F. Kuvatov
 "19" 09 2024 yil.

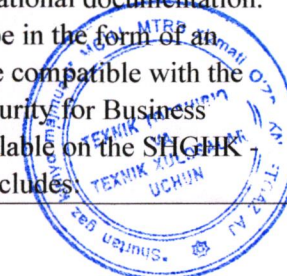
<p>TEKNIK TOPSHIRIQ "Sho'rtan gaz-kimyo majmuasi" MChJ IT infratuzilmasi uchun Kaspersky dasturiy ta'minotini xarid qilish</p>	<p>ТЕХНИЧЕСКОЕ ЗАДАНИЕ на закупку программного обеспечения Kaspersky для IT-инфраструктуры ООО "ШГХК"</p>	<p>TECHNICAL ASSIGNMENT For the purchase of Kaspersky for the IT infrastructure of SGCC.</p>
<p>1. UMUMIY MA'LUMOT</p>	<p>1. ОБЩИЕ СВЕДЕНИЯ</p>	<p>1. GENERAL INFORMATION</p>
<p>1.1 NOMI</p>	<p>1.1 Наименование</p>	<p>Name</p>
<p>Kaspersky virusga qarshi dasturiy mahsulotini yangilash va xarid qilish</p>	<p>Продление и закуп антивирусного программного продукта (ПП) Kaspersky</p>	<p>Renewal and purchase of Kaspersky anti-virus software product</p>
<p>1.2 Tovarlarni sotib oishdan maqsad va asos</p>	<p>1.2 Основание и цель приобретения товара</p>	<p>1.2 Basis and purpose of purchasing goods</p>
<p>Asos: 2024-yil uchun yillik buyurtma. Maqsad: "SHGHK" MChJda 700 ta kompyuter uchun dasturiy ta'minot litsenziyasining amal qilish muddatini uzaytirish va 1 ta korporativ pochta foydalanuvchilari uchun 300 ta dasturiy ta'minot litsenziyasining 1 qismini 1 (bir) yilga sotib olish." Ushbu ekish ostida sotib olingan antivirus dasturiy mahsuloti quyidagi vazifalarni hal qilish uchun mo'ljallangan: * Kompyuterlarni, fayl serverlarini va ma'lumotlarni viruslardan va boshqa tahdidlardan himoya qiladi. * Litsenziyaning yillik yangilanishi murakkab axborot tizimlarining doimiy himoyasini ta'minlash, * Oyna kompyuterlarida zararli dasturlardan, veb-kameralarni kuzatishdan, firibgarlardan va boshqa tahdidlardan himoya qilish. * Nafaqat viruslar va troyanlarni aniqlash va yo'q qilish, balki kompyuterda ishlaydigan har qanday dasturiy</p>	<p>Основание: годовая заявка на 2024 год Цель: Продление срока действия лицензии ПП на 700 компьютеров и закуп 1 штуки лицензии ПП для 300 пользователей корпоративной почты на 1 (один) год в ООО «ШГХК». Антивирусный программный продукт, закупаемое в рамках настоящего ТЗ, предназначено для решения следующих задач: • Защита компьютеров, файловых серверов и данных от вирусов и других угроз. • Продление годовой лицензии обеспечивает непрерывную защиту информационных систем комплекса. • Защитить от вредоносного ПО, слежки через веб-камеру, мошенников и других угроз на компьютерах Windows.</p>	<p>Basis: 2024 annual application Purpose: Extension of the validity period of the software license for 700 computers and purchase of 1 piece of the software license for 300 corporate mail users for 1 (one) year in LLC "SGCC." The anti-virus software product purchased under this SOW is designed to solve the following tasks: • Protect computers, file servers, and data from viruses and other threats. • Annual license renewal ensures continuous protection of complex information systems. • Protect against malware, webcam surveillance, scammers, and other threats on Windows computers. • The ability not only to detect and destroy viruses and Trojans, but also to monitor and suppress potentially dangerous actions of any software running on the computer.</p>

<p>ta'minotning potentsial xavfli harakatlarini kuzatish va bostirish qobiliyatiga ega bo'lish. * Zamonaviy tahdidlardan ishonchli himoyalash uchun moslashtirilgan xabar va ogohlantirishlarga ega bo'lish.</p>	<ul style="list-style-type: none"> Способность не только выявлять и уничтожать вирусные и троянские программы, но и отслеживать и пресекать потенциально опасные действия любого запущенного на компьютере программного обеспечения. Персонализированные уведомления и предупреждения для надежной защиты от современных угроз 	<ul style="list-style-type: none"> Personalized alerts and alerts to protect against today's threats
<p>1.3 Yangi ekanligi haqida ma'lumot</p>	<p>1.3 Сведения о новизне</p>	<p>1.3 Information about novelty</p>
<p>Dasturiy mahsulotning amal qilish muddati: (yillik litsenziya) 2024 yil 19 yil dekabr sanasidan boshlanishi kerak. Dasturiy mahsulotning versiyasi eng dolzarb bo'lishi hamda litsenziya "SHGKM"MCHJ nomiga berilishi kerak</p>	<p>Срок действие программного продукта: (годовая лицензия) должна начинаться с 19 декабря 2024 года. Версия программного продукта должна быть наиболее актуальной, лицензия должны быть выдана на имя: ООО «Шуртанский ГХК»</p>	<p>Software product validity period: (annual license) must begin on December 19, 2024. The version of the software product should be the most up-to-date, the license should be issued in the name of: LLC "SGCC"</p>
<p>2. Qo'llash sohasi</p>	<p>2. Область применения</p>	<p>2. 3. Scope of application</p>
<p>"SHGKM"MCHJ kompyuterlari, fayl serverlari va ma'lumotlarni viruslar va boshqa tahdidlardan ofis sharoitida uzluksiz ishlash rejimida himoya qilish uchun</p>	<p>Для защита компьютеров, файловых серверов и данных от вирусов и других угроз в непрерывном режиме работы в офисных условиях ООО "ШГХК"</p>	<p>To protect computers, file servers, and data from viruses and other threats while they are continuously operating in the office environment at SGCC LLC.</p>
<p>3. Foydalanish shartlari</p>	<p>3. Условия эксплуатации</p>	<p>3. Operating conditions</p>
<p>Dasturiy mahsulot barcha SHGKM ob'ektlaridagi kompyuterlar, serverlar va ma'lumotlarni viruslar va boshqa turdagi tahdidlardan himoya qilish uchun mo'ljallangan. U bino ichida foydalanish uchun mo'ljallangan va yil davomida ishlatilishi mumkin.</p>	<p>Программный продукт применяется для защита компьютеров, серверов и данных всех объектов ШГХК от вирусов и других угроз предназначается для эксплуатации внутри помещений в режиме круглогодичного пользования</p>	<p>The software product is designed to protect computers, servers, and data at all SGCC facilities from viruses and other types of threats. It is intended for use indoors and can be operated year-round.</p>

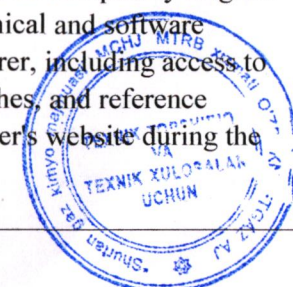
<p>4. TEXNIK TALABLAR</p>	<p>4. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ</p>	<p>4. TECHNICAL REQUIREMENTS</p>
<p>4.1 dasturiy mahsulotga (PP) asosiy texnik talablar (Kasperskiy Antivirus dasturiy mahsuloti)</p>	<p>4.1 Основные технические требования к программному продукту (ПП) (Антивирусный программный продукт Kaspersky)</p>	<p>4.1 4.1 Basic technical requirements for the software product (PP) (Kasperskiy Anti-virus software product)</p>
<p>Kasperskiy Endpoint Security for Business (Kengaytirilgan) - yangilash litsenziyasi: Kasperskiy Endpoint Security 12.Windows</p>	<p><u>Kasperskiy Endpoint Security for Business (Расширенный) – Renewal license: Kasperskiy Endpoint</u></p>	<p>Kasperskiy Endpoint Security for Business Advanced - Renewal License: Kasperskiy Endpoint Security 12.x for Windows</p>

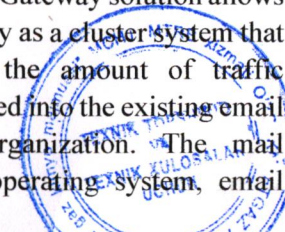


<p>uchun x (ish stantsiyalari va fayl serverlari uchun) va Kaspersky Security 11.x Windows Server uchun -700 ta kompyuter uchun 1 dona kalit Kasperskiy xavfsizlik markazi (ma'muriy konsol) – 700 ta kompyuterni boshqarish uchun 1 dona kalit</p>	<p>Security 12.x для Windows (для рабочих станций и файловых серверов) и Kaspersky Security 11.x для Windows Server – 1 штук ключа на 700 компьютеров Kaspersky security center (консоль администрирования) – 1 штук ключ для управления 700 компьютеров</p>	<p>(workstations and file servers), and Kaspersky Security 11.x for Windows Server - 1 license per 700 computers. Kaspersky Security Center (administration console) - 1 key to manage 700 computers.</p>
<p>Dasturiy ta'minot mahsuloti xalqaro standartlarga asoslangan bo'lishi va quyidagi tamoyillarga rioya qilishi kerak:</p> <ul style="list-style-type: none"> - Barcha komponentlar dizaynining modulligi - dasturiy ta'minot va ma'lumotlar ierarxiyasi - samaradorlik (ishlab chiqish va texnik xizmat ko'rsatish uchun minimal resurs xarajatlari) - Oson integratsiya (kengaytirish va o'zgartirish qobiliyati) - Moslashuvchanlik (o'zgartirishlar kiritish va sozlash qobiliyati) - Ishonchlilik (belgilangan algoritmgga muvofiqligi, noto'g'ri pozitivlarning yo'qligi, ruqsatsiz kirish va ma'lumotlarni yo'qotishdan himoya qilish) - omon qolish qobiliyati (to'liq yoki qisman muvaffaqiyatsizlikka uchragan taqdirda tayinlangan funktsiyalarni bajarish, muvaffaqiyatsizlikdan keyin tiklanish qobiliyati) - Yechimlarni birlashtirish - Dastur tarkibi, tuzilishi va manba kodining soddaligi va ravshanligi <p>Amaliy dasturiy ta'minotga o'zgartirishlar kiritishda parollarni o'rnatish va ruqsat etilgan kirish darajalarini aniqlash imkoniyati bo'lishi kerak. Litsenziyalangan mahsulotga operatsion hujjatlar ilova qilinishi kerak.</p>	<p>Программное продукт (ПП) должно базироваться на международных стандартах и отвечать следующим принципам:</p> <ul style="list-style-type: none"> - модульность построения всех составляющих; - иерархичность собственно ПО и данных; - эффективность (минимальные затраты ресурсов на создание и обслуживание ПО); - простота интеграции (возможность расширения и модификации); - гибкость (возможность внесения изменений и перенастройки); - надежность (соответствие заданному алгоритму, отсутствие ложных срабатываний), защита от несанкционированного доступа и разрушения как программ, так и данных; - живучесть (выполнение возложенных функций в полном или частичном объемах при сбоях и отказах, восстановление после сбоев); - унификация решений; - простота и наглядность состава, структуры и исходных текстов программ; <p>Должна иметься возможность задания паролей и установления границ санкционированного доступа при внесении изменений в прикладное ПО.</p>	<p>The software product should be based on international standards and adhere to the following principles:</p> <ul style="list-style-type: none"> - Modularity of the design of all components - Hierarchy of the software and data - Efficiency (minimum resource costs for development and maintenance) - Easy integration (ability to expand and modify) - Flexibility (ability to make changes and configure) - Reliability (compliance with specified algorithm, lack of false positives, protection against unauthorized access and data loss) - Survivability (ability to perform assigned functions fully or partially in case of failure, recovery after failure) - Unification of solutions - Simplicity and clarity of program composition, structure, and source code <p>It should be possible to set passwords and define authorized access levels when making changes to the application software. The licensed product must be accompanied by operational documentation. The license key should be in the form of an electronic file. It must be compatible with the Kaspersky Endpoint Security for Business (Advanced) version available on the SHGKH Renewal license. This includes:</p>



<p>Litsenziya kaliti elektron fayl shaklida bo'lishi kerak. U SHGHK - Renewal litsenziyasida mavjud Kaspersky Endpoint Security for Business (Advanced) versiyasiga mos kelishi kerak. Bunga quyidagilar kiradi:</p> <ul style="list-style-type: none"> - Ish stantsiyalari va fayl serverlarida Windows uchun Kaspersky Endpoint Security 12.x - Windows Serverda Kaspersky Security 11.x - ma'muriyat uchun Kasperskiy xavfsizlik markazi <p>Qo'llab-quvvatlanadigan operatsion tizimlar qatoriga Windows 7, 10, 11 va Windows Server 2008, 2012, 2016 va 2019 kiradi. Himoya Windows, Linux, Mac, Android va iOS qurilmalari uchun taqdim etiladi. Ilovani ishga tushirishni boshqarish Windows serverlarida mavjud. Mobil qurilma xavfsizligi ham o'z ichiga oladi. Ish stantsiyalari uchun dasturni boshqarish, veb-nazorat va qurilmalarni boshqarish mavjud. Xulq-atvorni tahlil qilish va zararli harakatlarni qaytarish ham qo'llab-quvvatlanadi.</p> <ul style="list-style-type: none"> - zaifliklarni tahlil qilish va ekspluatatsiyalardan himoya qilish - Atrof-muhitni almashtirish uchun ruxsatnomalar va hujumni oldini olish tizimi - AMSI, Microsoft AD, Syslog, RMM, PSA, EMM bilan integratsiya - Pochta va veb-tahdidlardan himoya qilish va serverlarni boshqarish vositalari - Moslashuvchan anomalialarni boshqarish va yamoqlarni o'rnatishni boshqarish - shifrlashni boshqarish, shu jumladan operatsion tizimga integratsiya - SIEM tizimlari bilan ilg'or integratsiya va OT va uchinchi tomon dasturlarini o'rnatish 	<p>Фирменное ПП должно сопровождаться эксплуатационной документацией.</p> <p>Лицензионный ключ в виде электронного файла ключа</p> <p>Лицензионный ключ должен быть совместим с имеющимся в ШГХК программным обеспечением <u>Kaspersky Endpoint Security for Business (Расширенный) – Renewal license:</u></p> <ul style="list-style-type: none"> • <u>Kaspersky Endpoint Security 12.x для Windows</u> (для рабочих станций и файловых серверов) • <u>Kaspersky Security 11.x для Windows Server</u> • <u>Kaspersky security center (консоль администрирования)</u> <p>Поддерживаемые операционные системы для рабочих станций и серверов: Windows 7, Windows 10, Windows 11, Windows Server 2008/2012/2016/2019</p> <ul style="list-style-type: none"> - Защита Windows, Linux, Mac, Android и iOS - Контроль запуска приложений на серверах Windows - Безопасность мобильных устройств - Контроль программ, веб-контроль и контроль устройств на рабочих станциях - Поведенческий анализ, Откат вредоносных действий - Анализ уязвимостей и защита от эксплойтов - Разрешения на переключение среды и система предотвращения вторжений - Интеграция с AMSI, Microsoft AD, Syslog, RMM, PSA, EMM 	<ul style="list-style-type: none"> - Kaspersky Endpoint Security 12.x for Windows on workstations and file servers - Kaspersky Security 11.x on Windows Server - Kaspersky security center for administration <p>Supported operating systems include Windows 7, 10, 11 and Windows Server 2008, 2012, 2016, and 2019. Protection is provided for Windows, Linux, Mac, Android, and iOS devices. Application launch control is available on Windows servers. Mobile device security is also included. Program control, web control, and device control are available for workstations. Behavioral analysis and rollback of malicious activities are also supported.</p> <ul style="list-style-type: none"> - Vulnerability analysis and protection against exploits - Environment switching permissions and intrusion prevention system - Integration with AMSI, Microsoft AD, Syslog, RMM, PSA, EMM - Protection against mail and web threats and control tools for servers - Adaptive anomaly control and patch installation management - Encryption management, including integration into the operating system - Advanced integration with SIEM systems and installation of OS and third-party software <p>The software product should be completely original and have all necessary technical and software support from the manufacturer, including access to updates, fixes, security patches, and reference materials on the manufacturer's website during the license period.</p>
--	---	--



<p>Dasturiy ta'minot mahsuloti to'liq original bo'lishi va ishlab chiqaruvchidan barcha zarur texnik va dasturiy ta'minotga ega bo'lishi kerak, jumladan, litsenziya muddati davomida ishlab chiqaruvchining veb-saytidagi yangilanishlar, tuzatishlar, xavfsizlik yamoqlari va ma'lumotnoma materiallariga kirish.</p>	<ul style="list-style-type: none"> - Защита от почтовых и веб-угроз и инструменты контроля для серверов - Адаптивный контроль аномалий и Управление установкой исправлений - Управление шифрованием, в том числе встроенным в операционную систему - Продвинутая интеграция с SIEM-системами, установка ОС и стороннего ПО <p>Программный продукт должен быть полностью оригинальным, иметь всю соответствующую техническую и программную поддержку со стороны его изготовителя, включая, но не ограничиваясь: доступом ко всем обновлениям, исправлениям, патчам безопасности и производительности, справочным материалам и руководствам на сайте изготовителя в течение всего срока действия лицензии</p>	
<p>2. Kasperskiy xavfsiz pochta shlyuzi (korporativ pochta himoya qilish uchun) - 300 foydalanuvchi uchun 1 dona litsenziya</p>	<p><u>2. Kaspersky Secure Mail Gateway</u> (для защиты корпоративной почты) – <u>1 штука лицензии на 300 пользователей</u></p>	<p>2. Kaspersky Secure Mail Gateway (to protect corporate mail) – 1 piece of license for 300 users</p>
<p>Dasturiy mahsulot (PP) * Foydalanishga tayyor virtual qurilma VMware ESXi va Microsoft Hyper-V kabi eng mashhur platformalar uchun virtual qurilmaning oldindan sozlangan versiyalari. Kasperskiy Secure Mail Gateway yechimi pochta shlyuzini qayta ishlangan trafik hajmiga qarab kengaytiriladigan Klaster tizimi sifatida joylashtirish va uni tashkilotning mavjud pochta infratuzilmasiga integratsiya qilish imkonini beradi. Pochta Shlyuzida operatsion tizim, pochta serveri va</p>	<p>Программный продукт (ПП) Готовое к использованию виртуальное устройство Предварительно настроенные версии виртуального устройства для большинства наиболее популярных платформ, включая VMware ESXi и Microsoft Hyper-V. Решение Kaspersky Secure Mail Gateway позволяет развернуть почтовый шлюз в виде кластерной системы, масштабируемой в зависимости от объема обрабатываемого трафика, и интегрировать ее в существующую почтовую инфраструктуру организации. На почтовом шлюзе предустановлена</p>	<p>Software Product (PP) • A ready-to-use virtual device Pre-configured versions of the virtual device are available for most popular platforms, including VMware ESXi and Microsoft Hyper-V. The Kaspersky Secure Mail Gateway solution allows you to deploy a mail gateway as a cluster system that can scale depending on the amount of traffic processed. It can be integrated into the existing email infrastructure of your organization. The mail gateway comes with an operating system, email</p> 

Kasperskiy laboratoriyasining antivirus dasturi oldindan o'rnatilgan.

Kasperskiy Secure Mail Gateway kiruvchi va chiquvchi pochta xabarlarini zararli ob'ektlardan, spam va fishingdan himoya qiladi, xabarlarni tarkibni filtrlaydi.

Kasperskiy xavfsiz pochta shlyuzi quyidagilarga imkon beradi:

Antivirus xabarlarini tekshirishni amalga oshiring:

- Xabarlarni viruslar va zararli dasturlar, makrolar (masalan, makrosli Microsoft Office formatidagi fayllar) uchun tekshiring; shifrlangan ob'ektlar, arxivlar (shu jumladan arxivlar va kompozit ob'ektlar ichidagi fayl turlarini tanib olish).
- Yangi tahdidlarga javob berish tezligini oshirish uchun Kasperskiy xavfsizlik tarmog'idagi ma'lumotlardan foydalaning.
- Internetga kirish ichki qoidalar va siyosatlar bilan cheklangan tashkilotlar uchun Kasperskiy Private Security Network (keyingi o'rinlarda KPSN deb yuritiladi) bilan integratsiya.
- Masalan, nol kunlik hujumlar, maqsadli hujumlar va advanced persistent threats (APT) ning murakkab maqsadli hujumlari kabi tahdidlarni aniqlash uchun Kasperskiy Anti Targeted Attack Platform (keyingi o'rinlarda KATA deb yuritiladi) bilan integratsiya.

Anti-spam moduli bilan xabarlarni tekshirishni amalga oshiring:

- Spam, taxmin qilingan spam, ommaviy pochta xabarlari uchun xabarlarni tekshiring (shu jumladan soxta domenlarni aniqlash va ip-manzillarning

операционная система, почтовый сервер и антивирусная программа "Лаборатории Касперского".

Kaspersky Secure Mail Gateway обеспечивает защиту входящей и исходящей почты от вредоносных объектов, спама и фишинга, выполняет контентную фильтрацию сообщений.

Kaspersky Secure Mail Gateway позволяет:

Выполнять Антивирусную проверку сообщений:

- Проверять сообщения на наличие вирусов и вредоносных программ, макросов (например, файлов форматов Microsoft Office с макросами); зашифрованных объектов, архивов (в том числе распознавать типы файлов внутри архивов и составных объектов).
- Использовать информацию из Kaspersky Security Network, чтобы увеличить скорость реакции на новые угрозы.
- Интегрироваться с Kaspersky Private Security Network (далее также KPSN) для тех организаций, в которых доступ в интернет ограничен внутренними правилами и политиками.
- Интегрироваться с Kaspersky Anti Targeted Attack Platform (далее также KATA) для обнаружения таких угроз, как, например, атаки "нулевого дня", целевые атаки и сложные целевые атаки advanced persistent threats (APT).

Выполнять проверку сообщений модулем Анти-Спам:

- Проверять сообщения на наличие спама, предполагаемого спама, массовых рассылок (в том числе с использованием технологии распознавания поддельных доменов и проверки репутации IP-адресов).

server, and Kaspersky Lab anti-virus software pre-installed.

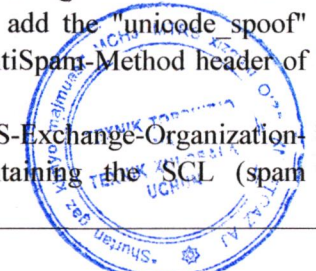
Kaspersky Secure Mail Gateways protect incoming and outgoing email from malicious objects, spam, and phishing. They also perform content filtering of emails.

With Kaspersky Secure Mail Gateway, you can:

- Perform an antivirus scan on messages to check for viruses, malware, and encrypted objects. This includes files with macros (e.g., Microsoft Office files) and archives. It also recognizes file types within archives and composite objects.
- Use information from the Kaspersky Security Network to improve the speed of response to new threats.
- Integrate with the Kaspersky Private Security Network for organizations where internet access is restricted by internal rules and policies.
- Collaborate with the Kaspersky Anti-Targeted Attack Platform to detect threats such as zero-day attacks, targeted attacks, and advanced persistent threats.

To filter messages with the anti-spam module:

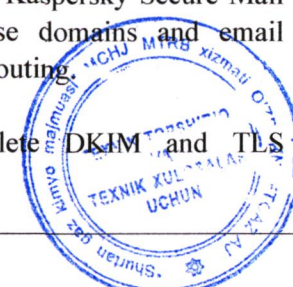
- Filter messages for spam and suspected spam, as well as mass mailings using technology to recognize fake domains and check the reputation of IP addresses.
- Detect Unicode spoofing in messages. If Unicode spoofing is detected, the message will be considered spam. The program will add the "unicode spoof" label to the X-KSMG-AntiSpam-Method header of the message.
- Add X-headers "X-MS-Exchange-Organization-SCL" to messages containing the SCL (spam



<p>obro'sini tekshirish texnologiyasidan foydalangan holda).</p> <p>-Unicode firibgarligi bilan xabarlarini aniqlang. Agar Unicode firibgarligi aniqlansa, xabar spam deb hisoblanadi. Dastur X-KSMG-AntiSpam-Method xabar sarlavhasiga unicode_spoof yorlig'ini qo'shadi.</p> <p>-Spam-tekshiruv natijalariga ko'ra x-MS-Exchange-Organization-SCL sarlavhalarini o'z ichiga olgan xabarlariga qo'shing.</p> <p>-Anti-spam karantiniga xabarlarini joylashtirish, veb-interfeysda anti-spam karantinini boshqarish.</p> <p>-Anti-Fishing moduli bilan xabarlarini tekshirishni amalga oshiring.</p> <p>- Xabarlarini zararli yoki reklama havolalari, shuningdek qonuniy dasturiy ta'minot bilan bog'liq havolalarni tekshirishni amalga oshiring.</p> <p>- Xabarlarini tarkibni filtrlashni amalga oshiring: nomi bo'yicha; hajmi bo'yicha; qo'shimchalar turi bo'yicha (Kasperskiy Secure Mail Gateway kengaytmasidan qat'i nazar, qo'shimchani haqiqiy formati va turini aniqlashga imkon beradi).</p> <p>- SPF, DKIM va DMARC texnologiyalaridan foydalangan holda xabar yuboruvchilarning haqiqiylikini tekshirish.</p> <p>- Domen foydalanuvchilari haqida ma'lumot olish uchun Active Directory integratsiyasini sozlang.</p> <p>- Dastur ishida voqealar to'g'risida ma'lumot olish: voqealarni qulay qidirish uchun filtrlash imkoniyati bilan pochta trafigini qayta ishlash hodisalarini, shuningdek dasturning tizim voqealarini jurnalga yozib olish; voqealarni CSV formatiga eksport qilish.</p> <p>-Syslog protokoli bo'yicha tashkilotda ishlatiladigan SIEM tizimida dastur ishlayotganda sodir bo'ladigan</p>	<ul style="list-style-type: none"> - Обнаруживать сообщения с Юникод-спуфингом. В случае обнаружения Юникод-спуфинга сообщение считается спамом. Программа добавляет метку unicode_spoof к заголовку сообщения X-KSMG-AntiSpam-Method. - Добавлять в сообщения X-заголовки X-MS-Exchange-Organization-SCL, содержащие SCL-оценку, по результатам проверки на спам. - Помещать сообщения в Анти-Спам карантин, управлять Анти-Спам карантином в веб-интерфейсе. - Выполнять проверку сообщений модулем Анти-Фишинг. - Выполнять проверку сообщений на наличие вредоносных или рекламных ссылок, а также ссылок, относящихся к легальному ПО. - Выполнять контентную фильтрацию сообщений: по имени; по размеру; по типу вложений (Kaspersky Secure Mail Gateway позволяет определять истинный формат и тип вложения, независимо от его расширения). - Осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC. - Настраивать интеграцию с Active Directory для получения информации о пользователях домена. - Получать информацию о событиях в работе программы: записывать события обработки почтового трафика, а также системные события работы программы в журнал, с возможностью фильтрации для удобного поиска событий; экспортировать события в формат CSV. 	<p>confidence level) score based on the results of spam checks.</p> <ul style="list-style-type: none"> - Place spam-quarantined messages in the Anti-Spam folder, manage the Anti-Spam quarantine folder in the web interface. - Verify messages using the Anti-Phishing module. - Check for malicious or promotional links, as well as legitimate software links in messages. - Filter message content: by name, size, attachment type (Kaspersky Secure Mail Gateway can determine the true format and attachment type, regardless of the extension). - Verify the authenticity of sender domains using SPF, DKIM, and DMARC. - Integrate with Active Directory for user information. - View program events: record mail traffic and system events in a log with easy search and export to CSV. - Publish events that occur during the operation of the program to the SIEM (Security Information and Event Management) system used in the organization, using the Syslog protocol. Each program event is sent as a separate Syslog message in CEF (Common Event Format) format. - Configure settings and manage the operation of the program via the web interface. - Monitor mail traffic, system resource usage, and view lists of recent threats in the program's web interface. - Limit user access to program features using a role-based system. - Enable single sign-on authentication.
---	---	---



<p>voqealarni nashr etish. Dasturning har bir hodisasi to'g'risidagi ma'lumotlar cef formatidagi alohida syslog xabari sifatida uzatiladi.</p> <ul style="list-style-type: none"> - Sozlamalarni sozlash va veb-interfeys orqali dasturning ishlashini boshqarish. -Pochta trafigi holatini va tizim resurslaridan foydalanishni kuzatib boring, dasturning veb-interfeysida topilgan so'nggi tahdidlar ro'yxatini ko'ring. - Rolli tizim yordamida foydalanuvchilarning dastur funktsiyalariga kirishini farqlash. - Yagona kirish texnologiyasi yordamida autentifikatsiyani sozlang. -Dasturning veb-interfeysi orqali klasterdagi barcha serverlarni markazlashtirilgan boshqarish qobiliyatiga ega bo'lgan echimni (gorizontal va vertikal ravishda) masshtablash uchun Klaster yarating. - Saqlashni boshqarish: tekshirish natijalari bo'yicha xabarlarning zaxira nusxalarini saqlash; xabarlarni xotiradan faylga saqlash; xabarlarni qabul qiluvchilarga yuborish; turli domenlardan foydalanuvchi ma'lumotlarini olish va foydalanuvchilarga shaxsiy xotiraga kirish huquqini berish. - Pochta tizimining ma'lum manzillardagi xabarlarga javobini aniqroq sozlash imkonini beradigan taqiqlangan va ruxsat etilgan manzillar ro'yxatini yarating. - Dastur bazalarini Kasperskiy laboratoriyasining yangilanish serverlaridan va foydalanuvchi resurslaridan jadval va talab bo'yicha yangilang. 	<ul style="list-style-type: none"> - Публиковать события, происходящие во время работы программы, в SIEM-систему, используемую в организации, по протоколу Syslog. Информация о каждом событии программы передается как отдельное syslog-сообщение формата CEF. - Настраивать параметры и управлять работой программы через веб-интерфейс. - Осуществлять мониторинг состояния почтового трафика и использования ресурсов системы, просматривать списки последних обнаруженных угроз в веб-интерфейсе программы. - Разграничивать доступ пользователей к функциям программы с помощью ролевой системы. - Настраивать аутентификацию с помощью технологии единого входа. - Создавать кластер для масштабирования решения (как горизонтально, так и вертикально), с возможностью централизованного управления всеми серверами из кластера через веб-интерфейс программы. - Управлять Хранилищем: сохранять резервные копии сообщений в Хранилище по результатам проверки; Сохранять сообщения из Хранилища в файл; Пересылать сообщения получателям; Получать информацию о пользователях из разных доменов и предоставлять пользователям доступ к персональному хранилищу. - Создавать списки запрещенных и разрешенных адресов, позволяющие более точно настроить реакцию почтовой системы на сообщения с определенных адресов. 	<ul style="list-style-type: none"> - Create a scalable solution cluster (both horizontally and vertically) with centralized management of all cluster servers through the program's web interface. - Manage the Repository: Save backup copies of messages in the repository based on the verification results. Save messages from the repository to a file. Forward messages to recipients. Receive information about users from different domains and provide users with access to personal storage. - Create lists of prohibited and permitted addresses to allow you to more accurately adjust the response of the mail system to messages from certain addresses. - Update program databases from Kaspersky Lab update servers and user resources on schedule and on demand. <p>Configure email notifications: Notify the sender, recipients, and other recipients about objects found in the message. Send notifications to users about system events in the program.</p> <p>Add notes to outgoing and incoming messages and warnings about unsafe messages. Create and view reports on message processing results and program events.</p> <ul style="list-style-type: none"> - Process email messages according to the rules set for groups of senders and recipients. - Add, change, or delete information about domains (including the organization's local domains) and email addresses. Configure Kaspersky Secure Mail Gateway settings for these domains and email addresses as well as email routing. - Configure the MTA. - Add, modify, and delete DKIM and TLS encryption keys.
--	--	--



- Pochta xabarnomalarini sozlash: jo'natuvchini, qabul qiluvchilarni va boshqa qabul qiluvchilarni xabarda topilgan narsalar to'g'risida xabardor qilish; dastur ishida tizim hodisalari to'g'risida foydalanuvchilarga xabarnoma yuborish.

- Chiquvchi va kiruvchi xabarlarga eslatmalar qo'shish va xavfli xabar haqida ogohlantirishlar qo'shish.

- Xabarlarni qayta ishlash natijalari va dastur voqealari to'g'risida hisobotlarni yaratish va ko'rish.

- Elektron pochta xabarlarini jo'natuvchilar va qabul qiluvchilar guruhlari uchun belgilangan qoidalarga muvofiq qayta ishlash.

- Domenlar (shu jumladan tashkilotning mahalliy domenlari) va elektron pochta manzillari to'g'risidagi ma'lumotlarni qo'shish, o'zgartirish yoki o'chirish, ushbu domenlar va elektron pochta manzillari uchun Kasperskiy Secure Mail Gateway sozlamalarini sozlash va elektron pochmani yo'naltirish.

- MTA-ni sozlash.

- Dkim-va TLS-shifrlash kalitlarini qo'shish, o'zgartirish va o'chirish.

- SNMP protokoli yordamida dastur statistikasini oling, SNMP tuzoqlarini yuborishni yoqing va o'chiring.

Kasperskiy Secure Mail Gateway VMware ESXi yoki Microsoft Hyper-V gipervizorida joylashtirish uchun mo'ljallangan virtual mashinaning ISO tasvir formatida tarqatiladi.

Tasvirni joylashtirish natijasida oldindan o'rnatilgan operatsion tizim, pochta serveri va Kasperskiy Secure Mail Gateway dasturi bilan virtual mashina

- Обновлять базы программы с серверов обновлений "Лаборатории Касперского" и пользовательских ресурсов по расписанию и по требованию.

- Настраивать почтовые уведомления: Уведомлять отправителя, получателей и других адресатов об обнаруженных в сообщении объектах; отправлять уведомления пользователям о системных событиях в работе программы.

- Добавлять примечания к исходящим и входящим сообщениям, а также добавлять предупреждения о небезопасном сообщении.

- Создавать и просматривать отчеты о результатах обработки сообщений и событиях работы программы.

- Обработать сообщения электронной почты согласно правилам, заданным для групп отправителей и получателей.

- Добавлять, изменять или удалять информацию о доменах (в том числе локальных доменах организации) и адресах электронной почты, настраивать параметры Kaspersky Secure Mail Gateway для этих доменов и адресов электронной почты, а также маршрутизацию электронной почты.

- Осуществлять настройку MTA.

- Добавлять, изменять и удалять DKIM- и TLS-ключи шифрования.

- Получать статистику работы программы по протоколу SNMP, включать и отключать отправку SNMP-ловушек.

- Receive program operation statistics using the SNMP protocol. Enable and disable sending SNMP traps.

Kaspersky Secure Mail Gateway is distributed as an ISO image of a virtual machine designed for deployment on VMware ESXi or Microsoft Hyper-V.

After image deployment, a virtual machine with a pre-installed operating system, mail server, and Kaspersky Secure Mail Gateway will be created. After deployment, the virtual machine can be configured using the Initial Configuration Wizard.

MULTI-LEVEL PROTECTION AGAINST MALWARE

- Multi-layered threat protection with cloud-based Kaspersky Security Network support

- Reputation filtering of malicious URLs and IP addresses through Kaspersky Security Network network

- Detection of malicious macros and ActiveX controls in Office files

- Urgent Detection System 2 for enhanced spam blocking

ANTISPAM AND CONTENT FILTERING

- Anti-spam engine

- Cloud anti-phishing

- Mass mailing detection

- Anti-spam quarantine

- Spam Confidence Level assessment

- Extended character support

- Object detection inside nested archives

INTEGRATION CAPABILITIES

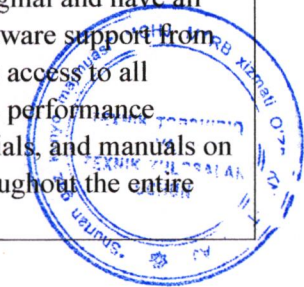
- Integration with Kaspersky Anti-Targeted Attack

- Integration with Kaspersky Private Security

Network



<p>yaratiladi. Joylashtirilgandan so'ng, dastlabki sozlash ustasi yordamida virtual mashinani sozlash imkoniyati bo'lishi kerak.</p> <p>KO'P DARAJALI ZARARLI DASTURLARDAN HIMOYA QILISH</p> <ul style="list-style-type: none"> * Kasperskiy xavfsizlik tarmog'ini qo'llab-quvvatlaydigan ko'p darajali tahdidlardan himoya qilish * Kasperskiy xavfsizlik tarmog'ining bulutli tarmog'idan foydalangan holda zararli URL va IP - manzillarning obro'li filtri * Office fayllarida zararli macros / ActiveX boshqaruvini aniqlash * Spamni yanada samarali blokirovka qilish uchun Urgent Detection System 2 tezkor aniqlash tizimi <p>ANTISPAM VA KONTENTNI FILTRLASH</p> <ul style="list-style-type: none"> * Antispam yadrosi * Bulutga asoslangan antifishing * Ommaviy axborot vositalarini aniqlash * Antispam karantini * Keraksiz pochta ehtimoli darajasini baholash (Spam ishonch darajasi) * Kengaytirilgan belgilarni qo'llab-quvvatlash * Ichki arxivlar ichidagi ob'ektlarni aniqlash <p>INTEGRATSIYA IMKONIYATLARI</p> <ul style="list-style-type: none"> * Kasperskiy maqsadli hujumga qarshi integratsiya * Kasperskiy xususiy xavfsizlik tarmog'i bilan integratsiya <p>QULAY MONITORING VA MOSLASHUVCHAN HISOBOT TIZIMI</p> <ul style="list-style-type: none"> * Texnik yordam mutaxassislari uchun qulay foydalanish * Boshqaruv paneli * SNMP-ni to'liq qo'llab-quvvatlash (Simple Network Management Protocol) 	<p>Kaspersky Secure Mail Gateway распространяется в формате ISO-образа виртуальной машины, предназначенного для развертывания в гипервизоре VMware ESXi или Microsoft Hyper-V.</p> <p>В результате развертывания образа создается виртуальная машина с предустановленной операционной системой, почтовым сервером и программой Kaspersky Secure Mail Gateway. После развертывания должна быть возможность настройки виртуальной машины с помощью мастера первоначальной настройки.</p> <p>МНОГОУРОВНЕВАЯ ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО</p> <p>Многоуровневая защита от угроз с поддержкой облачной сети Kaspersky Security Network</p> <p>Репутационный фильтр вредоносных URL- и IP-адресов с использованием облачной сети Kaspersky Security Network</p> <p>Обнаружение вредоносных макросов / элементов управления ActiveX в файлах Office</p> <p>Система быстрого обнаружения Urgent Detection System 2 для более эффективного блокирования спама</p> <p>АНТИСПАМ И ФИЛЬТРАЦИЯ КОНТЕНТА</p> <p>Антиспам-ядро</p> <p>Облачный антифишинг</p> <p>Обнаружение массовых рассылок</p> <p>Карантин антиспама</p> <p>Оценка уровня вероятности нежелательной почты (Spam Confidence Level)</p> <p>Расширенная поддержка символов</p> <p>Обнаружение объектов внутри вложенных архивов</p>	<p>USER-FRIENDLY MONITORING AND REPORTING SYSTEM</p> <ul style="list-style-type: none"> • Convenient access for technical support specialists • Information panel • Full support for SNMP (Simple Network Management Protocol) • Web-based management • Detailed flexible reports in PDF format • Notification system • Event logs • Advanced features for technical support • Features for advanced notification systems • Integration with SIEM <p>CONVENIENT INSTALLATION AND MAINTENANCE</p> <ul style="list-style-type: none"> • Easy installation • Active Directory and OpenLDAP integration • Rules for managing email traffic • IPv6 support • Scalable architecture • Upgrade <p>LICENSE AND SUBSCRIPTION MANAGEMENT</p> <ul style="list-style-type: none"> • Licensing options • Activation using a code • Software <p>Deploy a virtual image</p> <p>License key in the form of a file</p> <p>The software product must be completely original and have all the necessary technical and software support from the manufacturer. This includes access to all updates, fixes, security patches, performance improvements, reference materials, and manuals on the manufacturer's website throughout the entire validity period.</p>
--	--	--



- * Veb-interfeys orqali boshqarish
- * PDF formatida batafsil moslashuvchan hisobotlar
- * Bildirishnomalar tizimi
- * Batafsil voqealar jurnallari
- * Kengaytirilgan texnik qo'llab-quvvatlash imkoniyatlari
- * Xabarnoma tizimining kengaytirilgan xususiyatlari
- * SIEM bilan integratsiya

QULAY O'RNATISH VA TEXNIK XIZMAT KO'RSATISH

- * Oson o'rnatish
- * Active Directory va OpenLDAP integratsiyasi
- * Elektron pochta trafikini boshqarish bo'yicha keng qoidalar to'plami
- * IPv6-Ni Qo'llab-Quvvatlash
- * Kengaytiriladigan arxitektura
- * Oddiy yangilanish

LITSENZIYALAR VA OBUNALARNI BOSHQARISH

- * Kengaytirilgan litsenziyalash imkoniyatlari
- Kod bilan faollashtirish qobiliyati
- * Dasturiy ta'minot

Virtual tasvirni joylashtirish uchun
Litsenziya kaliti kalit fayli sifatida.

Dasturiy ta'minot mahsuloti to'liq original bo'lishi kerak, uning ishlab chiqaruvchisi tomonidan barcha tegishli texnik va dasturiy ta'minotga ega bo'lishi kerak, shu jumladan, lekin ular bilan cheklanmagan holda: ishlab chiqaruvchining veb-saytidagi barcha yangilanishlar, tuzatishlar, xavfsizlik va ishlash yamoqlari, ma'lumotnomalar va qo'llanmalarga amal qilish muddati davomida kirish

ВОЗМОЖНОСТИ ИНТЕГРАЦИИ

Интеграция с Kaspersky Anti Targeted Attack
Интеграция с Kaspersky Private Security Network
УДОБНЫЙ МОНИТОРИНГ И ГИБКАЯ СИСТЕМА ОТЧЕТОВ

Удобный доступ для специалистов техподдержки
Информационная панель
Полная поддержка SNMP (Simple Network Management Protocol)

Управление через веб-интерфейс
Подробные гибкие отчеты в формате PDF
Система уведомлений

Подробные журналы событий
Расширенные возможности технической поддержки
Расширенные возможности системы уведомлений
Интеграция с SIEM

УДОБНАЯ УСТАНОВКА И ОБСЛУЖИВАНИЕ

Простая установка
Active Directory и интеграция с OpenLDAP
Широкий набор правил для управления трафиком электронной почты
Поддержка IPv6
Масштабируемая архитектура
Простое обновление

УПРАВЛЕНИЕ ЛИЦЕНЗИЯМИ И ПОДПИСКОЙ

Расширенные возможности лицензирования
Возможность активировать с помощью кода

Программное обеспечение

Для развертывания образа виртуального
Лицензионный ключ в виде файла ключа.



	Программный продукт должен быть полностью оригинальным, иметь всю соответствующую техническую и программную поддержку со стороны его изготовителя, включая, но не ограничиваясь: доступом ко всем обновлениям, исправлениям, патчам безопасности и производительности, справочным материалам и руководствам на сайте изготовителя в течение всего срока действия лицензии	
4.2 Ishonchlilik talablari	4.2 Требования по надежности	4.2 Reliability requirements
Litsenziyalangan dasturiy ta'minot mijozning kompyuter uskunasining apparat va dasturiy ta'minot qismiga to'liq mos kelishi kerak. Litsenziyalangan dasturiy ta'minotdan foydalanish mijozning kompyuter va server uskunalarida nosozliklar, nosozliklar, ma'lumotlarning yo'qolishi yoki ishlashning pasayishi holatlariga olib kelmasligi kerak.	Лицензируемое программное обеспечение должно быть полностью совместимо с аппаратной и программной частью компьютерного оборудования Заказчика. Использование лицензируемого программного обеспечения не должно приводить с сбоям, отказам, к ситуациям потери данных или снижения производительности на компьютерном и серверном оборудовании Заказчика.	The licensed software must be fully compatible with the hardware and operating system of the customer's computer. The use of licensed software should not cause any issues, such as crashes, data loss, or decreased performance on the customer's computer or server.
4.3 tarkibiy qismlarga, boshlang'ich va operatsion xom ashyo/materiallarga, shuningdek tayyor mahsulotlarga qo'yiladigan talablar	4.3 Требования к составным частям, исходным и эксплуатационным сырью/материалам, а также готовой продукции	4.3 Requirements for components, initial and operational raw materials/materials, as well as finished products
Barcha manba foydalanuvchi dasturlari va ma'lumotlarini alohida olinadigan ommaviy axborot vositalarida saqlash va agar kerak bo'lsa, mijoz tomonidan ishlab chiqaruvchini jalb qilmasdan to'liq hajmda qayta o'rnatish imkoniyati ta'minlanishi kerak.	Должна предусматриваться возможность сохранения всех исходных пользовательских программ и данных на отдельных съемных носителях и при необходимости - в случае повторной инсталляции заказчиком в полном объеме без привлечения Разработчика.	It should be possible for the customer to save all their original user programs and data on removable media, and if necessary, to reinstall the system without the involvement of the developer.
4.4 Belgilash talablari	4.4 Требования к маркировке	4.4 Labeling requirements
Markirovka o 'zbekiston Respublikasida amalda bo'lgan normativ hujjatlarga to 'liq muvofiq amalga	Маркировка должна быть выполнена в полном соответствии с действующими в Республики Узбекистан нормативными документами, а также содержать:	The marking must be done in full compliance with the relevant regulations in force in the Republic of Uzbekistan and should include:



<p>oshirilishi, shuningdek quyidagilarni o'z ichiga olishi kerak:</p> <ul style="list-style-type: none"> * tovar belgisi va (yoki) ishlab chiqaruvchining boshqa tafsilotlari; * belgi; * seriya raqami; * ishlab chiqarilgan sana; * muvofiqlik sertifikatini belgisi (agar mavjud bo'lsa). 	<ul style="list-style-type: none"> • товарный знак и(или) другие реквизиты предприятия-изготовителя; • условное обозначение; • серийный номер; • дату изготовления; • знак сертификата соответствия (при его наличии). 	<ul style="list-style-type: none"> - the trademark and/or other details of the manufacturer; - a symbol; - serial number; - date of manufacture; - the mark of the certificate of conformity (if applicable).
---	---	--

4.5 Qadoqlash talablari	4.5 Требования упаковке	4.5 Packaging requirements
<p>Mahsulot bo'lishi kerak qadoqlangan va to'ldirilgan mualliflik huquqi egasining talablariga muvofiq dasturiy ta'minot nusxasi kerakli hujjatlar, litsenziya shartnomasi, asosiy fayl va faollashtirish kodi bilan.</p>	<p>Продукт должен быть упакованный и укомплектованный в соответствии с требованиями Правообладателя экземпляра ПО с необходимой документацией, лицензионным соглашением, ключевым файлом и кодом активации.</p>	<p>The product must be packaged and delivered in accordance with the requirements of the copyright holder. This includes a copy of the software, the necessary documentation, a license agreement, key file, and activation code.</p>

5. QABUL QILISH VA QABUL QILISH QOIDALARIGA QO'YILADIGAN TALABLAR	5. ТРЕБОВАНИЯ ПО ПРАВИЛАМ СДАЧИ И ПРИЕМКИ	5. REQUIREMENTS FOR THE RULES OF DELIVERY AND ACCEPTANCE
<p>5.1 Qabul qilish va qabul qilish tartibi</p>	<p>5.1 Порядок сдачи и приемки</p>	<p>5.1 Delivery and acceptance procedure</p>
<p>Mahsulot 48 soat ichida sinovdan o'tkaziladi, shundan keyin ish rejimida muammolar mavjud bo'lsa, mahsulot sotuvchi yoki etkazib beruvchi hisobidan yangisiga almashtirilishi kerak. Uskunani o'rnatgandan va ishga tushirish va ishga tushirish ishlarini bajargandan so'ng, buyurtmachi bajarilgan ishlarning dalolatnomasini tuzgan holda tovarlarni qabul qiladi.</p>	<p>ПО апробируется в течении 48 часов, после этого времени если наблюдается неполадки в рабочем режиме, ПО должно быть заменено на новый за счёт продавца или поставщика. После проведения установки ключей на рабочие станции Заказчик подписывает акт выполненных работ.</p>	<p>The product is tested for 48 hours. If there is any malfunction after that time, the product will be replaced by the seller or supplier at their expense. After installing the equipment and commissioning it, the customer will accept the goods and prepare an act of completed work.</p>

5.2 Uskunani etkazib berishda texnik va boshqa hujjatlarni buyurtmachiga topshirish talablari	5.2 Требования по передаче заказчику технических и иным документов при поставке оборудования	5.2 Requirements for the Transfer of Technical and Other Documents to the Customer during Equipment Delivery
<p>Y etkazib beruvchi taqdim etilgan dasturiy mahsulot uchun texnik pasport, foydalanish bo'yicha</p>	<p>Поставщик должен предоставить технический паспорт на поставляемый программный продукт, руководство по</p>	<p>The supplier must provide technical documentation for the software product, including a technical data</p>

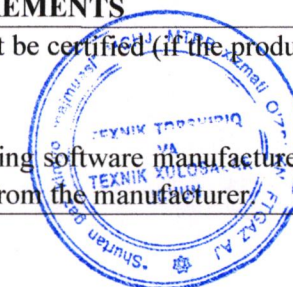


<p>qo'llanma, texnik qo'llab-quvvatlash saytlariga hisobga olish ma'lumotlarini taqdim etishi kerak. Taqdim etilgan texnik hujjatlar davlat yoki rus tillarida bo'lishi va ingliz tilida takrorlanishi kerak (iloji bo'lsa, elektron axborot vositalarida nusxalari taqdim etilishi kerak). Tavsiya etilgan dasturiy mahsulot foydalanuvchilari ro'yxatini taqdim etish kerak. Ishlab chiqaruvchi kompaniya (kompaniyaning veb-sayti va boshqalar) haqida ommaviy ma'lumotlarni ko'rsatish kerak.</p>	<p>эксплуатации, учетные данные к сайтам технической поддержки. Представляемые технические документы должны быть на государственном или на русском языках и продублировано на английском языке (по возможности, должны быть предоставлены копии на электронных носителях информации). Необходимо представить список пользователей предлагаемого программного продукта. Необходимо указать общедоступную информацию о компании производителе (сайт компании и т.д.)</p>	<p>sheet and operating manual. The documentation must be in Russian or English, and if possible, it should be duplicated on electronic media. Additionally, the supplier must provide credentials for technical support. It is also necessary to provide information about users of the software and publicly available information about the manufacturer, such as the company's website.</p>
---	--	--

6. KAFOLATLAR BERISH HAJMI VA/YOKI MUDDATIGA QO'YILADIGAN TALABLAR	6. ТРЕБОВАНИЯ К ОБЪЕМУ И/ИЛИ СРОКУ ПРЕДОСТАВЛЕНИЯ ГАРАНТИЙ	6. REQUIREMENTS FOR THE SCOPE AND/OR DURATION OF GUARANTEES
<p>Qabul qilish xaridor hududida qabul komissiyasi tomonidan amalga oshiriladi. Agar mos kelmaydigan, to'liq bo'lmagan tovarlar etkazib berilsa, mijoz tovarlarni qaytarib berishga haqlidir.</p>	<p>Приемка осуществляется приемочной комиссией на территории покупателя. В случае поставки несоответствующего, некомплектного товара заказчик вправе осуществить возврат товара.</p>	<p>Acceptance is carried out by the acceptance committee on the territory of the seller. If defective or incomplete goods are delivered, the buyer has the right to return them.</p>

7. Xizmat ko'rsatish talablari	7. Требования к сервисному обслуживанию	7. Service requirements
<p>Yetkazib beruvchi tovarlarga xizmat ko'rsatishni ta'minlashi yoki sotib olingan pddan foydalanish paytida texnik nosozliklar yuzaga kelgan taqdirda, buyurtmachining iltimosiga binoan xizmat ko'rsatish markazlari to'g'risida ishonchli ma'lumotlarni taqdim etishi kerak.</p>	<p>Поставщик должен обеспечить сервисное обслуживание товара или предоставить достоверные сведения о сервисных центрах по проведению сервисного обслуживания по заявкам Заказчика, в случае возникновения технических неисправностей в период эксплуатации закупаемого ПП.</p>	<p>The supplier must provide after-sales support for the product, or provide reliable information on service centers that can carry out after-sales services, at the request of the customer, in the event of technical issues during the operation of the purchased item.</p>

8. SIFAT VA TASNIFLASH TALABLARI	8. ТРЕБОВАНИЯ К КАЧЕСТВУ И КЛАССИФИКАЦИИ	8. QUALITY AND CLASSIFICATION REQUIREMENTS
<p>Dasturiy mahsulot sertifikatlangan bo'lishi kerak (agar mahsulot sertifikatlash uchun majburiy bo'lsa). Dasturiy mahsulot kerak:</p>	<p>Программный продукт должен быть сертифицирован (если товар является обязательным к сертификации). Программный продукт должен:</p>	<p>The software product must be certified (if the product requires certification). The software must: - Be produced by the leading software manufacturers with an official warranty from the manufacturer.</p>



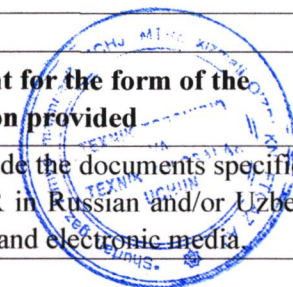
TEKNIK TOPSHIRIQ / ТЕХНИЧЕСКОЕ ЗАДАНИЕ / TECHNICAL ASSIGNMENT



<p>* dunyoning yetakchi dasturiy mahsulot ishlab chiqaruvchilari tomonidan ishlab chiqarilgan dasturiy mahsulot ishlab chiqaruvchisining rasmiy kafolati; * * sotib olingan dasturiy mahsulot tomonidan ishlab chiqarilgan yangi, ilgari ishlatilmagan bo'lishi kerak dasturiy mahsulot taxmin qilingan muddatning 2023 yilidan oldin emas. * ushbu texnik topshiriqning 4,1-bandlarida ko'rsatilgan texnik talablarga javob berish yoki undan yaxshiroq bo'lish; * o'ziga xoslikning barcha belgilarini o'z ichiga oladi. Tegishli bo'lmagan dasturiy mahsulot qabul qilinmaydi</p>	<ul style="list-style-type: none"> • быть произведен ведущими мировыми производителями программного продукта официальной гарантией от производителя программного продукта; • закупаемый программный продукт должен быть новыми, ранее не использованными, произведенными программный продукт не ранее 2024 года предполагаемого срока. • соответствовать или быть лучше технических требований, указанных в пунктах 4,1 настоящего технического задания; • содержать все признаки оригинальности. Несоответствующий программный продукт не принимаются 	<ul style="list-style-type: none"> - Be a new, unused software product manufactured no earlier than the expected date of 2023. - Meet or exceed the technical requirements in paragraphs 4.1 of this specification. - Have all the signs of originality. <p>Inappropriate products will not be accepted.</p>
---	--	---

<p>9. YETKAZIB BERISH MIQDORI, KONFIGURATSIYASI, JOYI VA MUDDATI (CHASTOTASI) UCHUN TALABLAR</p>	<p>9. ТРЕБОВАНИЯ К КОЛИЧЕСТВУ, КОМПЛЕКТАЦИИ, МЕСТУ И СРОКУ (ПЕРИОДИЧНОСТИ) ПОСТАВКИ</p>	<p>9. REQUIREMENTS FOR QUANTITY, CONFIGURATION, PLACE AND TIME (PERIODICITY) OF DELIVERY</p>
<p>Yetkazib berish muddati: 2024 yil 18 dekabr dan kechiktirmay. Miqdor va to'liqlikka bo'lgan talab: ushbu TKning 4.1-bandiga muvofiq. Yetkazib berish joyi: 180300, O'zbekiston Respublikasi. Qashqadaryo viloyati, G'uzor tumani, Shurtan posyolkasi. Telefon: +99875 552-41-75, +99890 008-41-43. E-mail: sgcc@sgcc.uz O'rnatish joyi: Qashqadaryo viloyati, G'uzor tumani, SHGKM</p>	<p>Срок поставки: не позднее 18 декабря 2024 года. Требование к количеству и комплектности: в соответствии с пунктом 4.1 настоящего ТЗ. Место поставки: 180300, Республика Узбекистан. Кашкадарьинская область, Гузарский район, посёлок Шуртан. Тел.: +99875 552-41-75, +99890 008-41-43 E-mail: sgcc@sgcc.uz Место установки: Кашкадарьинская область, Гузарский район, ШГХК</p>	<p>Delivery time: no later than December 18, 2024. Quantity and completeness requirements: in accordance with paragraph 4.1 of this TOR. Place of delivery: 180300, Republic of Uzbekistan. Kashkadarya region, Guzar district, Shurtan village. Tel.: +99875 552-41-75, +99890 008-41-43. E-mail: sgcc@sgcc.uz Installation location: Kashkadarya region, Guzar district, SGCC</p>

<p>10. Taqdim etilgan ma'lumotlar shakliga talab</p>	<p>10. Требование к форме представляемой информации</p>	<p>10. The requirement for the form of the information provided</p>
<p>Pudratchi 5.2-bandda ko'rsatilgan hujjatlarni taqdim etishi kerak. 1 (bir) nusxada qog'oz shaklida va</p>	<p>Исполнитель должен предоставить документы, приведённый в п. 5.2. настоящего ТЗ, на русском и/или</p>	<p>The Contractor must provide the documents specified in clause 5.2. of this TOR in Russian and/or Uzbek, one (1) copy in hard copy and electronic media.</p>



TEKNIK TOPSHIRIQ / ТЕХНИЧЕСКОЕ ЗАДАНИЕ / TECHNICAL ASSIGNMENT



elektron vositada rus va/yoki o'zbek tillarida mavjud bo'lsa.	узбекском языке, по 1 (один) экземпляру в бумажном виде и электронном носителе.	
---	---	--

11. QABUL QILINGAN QISQARTMALAR RO'YXATI	11. ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ	11. LIST OF ACCEPTED ABBREVIATIONS
1. TT: texnik topshiriq 2. O'z: O'zbekiston Respublikasi 3. SHGKM: "Shurtan gaz-kimyoy majmuasi" MCHJ 4. DM: dasturiy mahsulot 5. DT: dasturiy ta'minot	1. ТЗ: Технической задание 2. РУз: Республика Узбекистан 3. ШГХК: Шуртанский газохимический комплекс 4. ПП: Программный продукт 5. ПО: Программное обеспечение	1. TOR: Terms of Reference 2. Republic of Uzbekistan: Republic of Uzbekistan 3. SGCC: Shurtan gas chemical complex 4. PP: Software product 5. Software: Software

Axborot xavfsizligi bo'limi boshlig'i:

AKT xizmati boshlig'i:

Ishonchlilikni boshqarish xizmati boshlig'i:

Material texnik resurslarni boshqarish guruhi muhandisi:

Q. Rustamov

R. Normatov

T. Diyorov

B. Boybachchayev

Ushbu texnik topshiriq o'zbek, rus va ingliz tillarida tuzilgan. Agar rus va ingliz tillari o'rtasida farqlar bo'lsa, rus tilidagi matn ustunlik qiladi.

Настоящее техническое задание составлено на узбекском, русском и английском языках. При наличии разногласий между русским и английским языками, текст на русском языке будет превалировать.

This technical assignment is drafted in Uzbek, Russian and English languages. In case of discrepancies between the Russian and English languages, the Russian language shall prevail.

