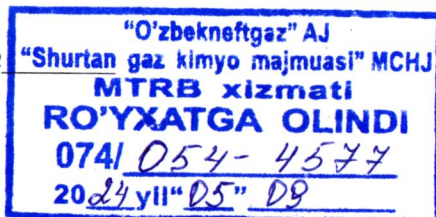


TEXNIK TOPSHIRIQ / ТЕХНИЧЕСКОЕ ЗАДАНИЕ / TECHNICAL ASSIGNMENT



Reg.No



TASDIQLAYMAN

"Sho'rtan GKM" MChJ

Bosh direktor o'rinbosari

F.Kuvatov

"5" 09 2024 yil.



TEXNIK TOPSHIRIQ "Sho'rtan gaz-kimyo majmuasi" MChJ IT infratuzilmasi uchun DLP dasturiy ta'minotini sotib olish uchun	ТЕХНИЧЕСКОЕ ЗАДАНИЕ на закупку программного обеспечения DLP для IT- инфраструктуры ШГХК	TECHNICAL ASSIGNMENT For the purchase of DLP software for the IT infrastructure of SGCC.k
1.UMUMIY MA'LUMOT	1. ОБЩИЕ СВЕДЕНИЯ	1.GENERAL INFORMATION
1.1 NOMI	1.1 Наименование	Name
SHGKMning IT infratuzilmasi uchun DLP dasturiy ta'minotini sotib olish.	Приобретение программного обеспечения для IT-инфраструктуры ШГХК.	Purchase of DLP software for the IT infrastructure of SGCC.
1.2 Tovarlarni sotib oishdan maqsad va asos	1.2 Основание и цель приобретения товара	1.2 Basis and purpose of purchasing goods
Maqsad: SHGKM IT infratuzilmasi uchun DLP dasturiy ta'minotini sotib olish. DLP tizimining asosiy vazifasi - maxfiy ma'lumotlarning tashqariga chiqishini oldini olishga qaratilgan. Sababi: Axborot xavfsizligi bo'limi boshlig'i Q.Rustamovning 054/13663 17.07.2024 dagi rasmiy xati	Цель: приобретение программного обеспечения DLP для IT-инфраструктуры ШГХК. Основная функция работы DLP системы направлена на предотвращение утечки конфиденциальных данных. Основание: служебное письмо от начальника отдела по Информационной безопасности К.Рустамова 054/13663 17.07.2024 г.	Goal: acquisition of DLP software for the IT infrastructure of SGCC. The main function of the DLP system is aimed at preventing the leakage of confidential data. Reason: official letter from the head of the Information Security Department K. Rustamov 054/13663 07/17/2024
1.3 Yangi ekanligi haqida ma'lumot	1.3 Сведения о новизне	1.3 Information about novelty
Tovar yangi (ilgari foydalanilmagan) ishlab chiqaruvchining qadoqlarida, ularning haqiqiyiligini tasdiqlovchi tegishli atributlar bilan jihozlangan, ishlab chiqaruvchi tomonidan uskunaga birlashtirilgan texnik hujjatlarga va tegishli uskunaning sertifikatlash talablariga muvofiq bo'lishi kerak. Tovarlar 2024 yildan oldin ishlab chiqarilishi kerak.	Товары должны быть новыми (не бывшим в использовании) в неповрежденной упаковке изготовителя, снабженной соответствующими атрибутами, подтверждающими их подлинность, в соответствии с технической документацией, прилагающийся к оборудованию изготовителем, и требованиями сертификации соответствующего оборудования. Товары должны быть произведены не ранее 2024 года.	The goods must be new (not previously used) in undamaged manufacturer's packaging, equipped with appropriate attributes confirming their authenticity, in accordance with the technical documentation attached to the equipment by the manufacturer, and the certification requirements of the relevant equipment. The goods must be produced no earlier than 2024.

4. TEXNIK TALABLAR	4. ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ	4. TECHNICAL REQUIREMENTS
4.1 Asosiy texnik talablar	4.1 Основные технические требования	4.1 Basic technical requirements
1. DLP dasturiy ta'minotii	1. Программное обеспечение DLP (Data Loss Prevention)	1. Software DLP (Data Loss Prevention)
<ul style="list-style-type: none"> • dona. litsenziyalar 80 dona. • Litsenziya turi doimiy 	<ul style="list-style-type: none"> • шт. лицензии 80 шт • Тип лицензии бессрочная 	<ul style="list-style-type: none"> • pcs. licenses 80 pcs • License type perpetual
<p>Shartlar va qisqartmalar</p> <ul style="list-style-type: none"> - apparat-dasturiy ta'minot kompleksi - ma'lum turdagi muammolarni hal qilish uchun birgalikda foydalaniladigan dasturiy ta'minot va texnik vositalar majmui; - ariza - mijozning xizmatlar ko'rsatish to'g'risidagi so'rovi; - AX – axborot xavfsizligi; - axborot-kommunikatsiya infratuzilmasi yoki uning alohida ob'ektlari faoliyatining bir martalik yoki ketma-ket buzilishi, ularning to'g'ri ishlashiga tahdid va (yoki) noqonuniy olish, nusxalash, tarqatish, o'zgartirish, yo'q qilish yoki blokirovka qilish shartlari. elektron axborot resurslari; - AT – axborot tizimi; - axborotlashtirish obyekti – elektron axborot resurslari, dasturiy ta'minot va axborot-kommunikatsiya infratuzilmasi; - RAM – tezkor xotirasi; - OS – operatsion tizim; - dasturiy ta'minot - dasturiy ta'minot; - AD – LDAP-mos katalog xizmatlarini amalga oshirish (Eng Active Directory); - LDAP - Yengil vaznli katalogga kirish protokoli (angl. Lightweight Directory Access Protocol); - SOC - Xavfsizlik operatsion markazi . (Security Operation Center) 	<p>Термины и сокращения</p> <ul style="list-style-type: none"> - Аппаратно-программный комплекс – совокупность программного обеспечения и технических средств, совместно применяемых для решения задач определенного типа; - Заявка – запрос Заказчика на предоставление услуг; - ИБ – информационная безопасность; - Инцидент ИБ – отдельно или серийно возникающие сбой в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов; - ИС – информационная система; - Объект информатизации – электронные информационные ресурсы, программное обеспечение и информационно-коммуникационная инфраструктура; - ОЗУ – оперативное запоминающее устройство; - ОС – операционная система; - ПО – программное обеспечение; - AD – LDAP-совместимая реализация службы каталогов (англ. Active Directory); - LDAP – облегчённый протокол доступа к каталогам (англ. Lightweight Directory Access Protocol); 	<p>Terms and abbreviations</p> <ul style="list-style-type: none"> - Hardware and software complex – a set of software and technical means that are jointly used to solve certain types of problems; - Request – the Customer's request for the provision of services. - Information security – information security. - Information security incident – separately or serially occurring failures in the operation of the information and communication infrastructure or its individual objects, creating a threat to their proper functioning and (or) conditions for illegal receipt, copying, distribution, modification, destruction or blocking of electronic information resources; - IP – information system. - Object of informatization – electronic information resources, software and information and communication infrastructure; - RAM – random access memory device. - OS – operating system. - Software; - AD-LDAP-compliant implementation of the Active Directory service. - LDAP-Lightweight Directory Access Protocol. - SOC-operational information security center (English: Security Operation Center)



Xizmat maqsadlari:

- 1) axborot xavfsizligi sohasidagi qonunchilik talablariga muvofiqligi;
 - 2) mijozning axborot aktivlarining umumiy xavfsizligini oshirish;
 - 3) tahdidlar va axborot xavfsizligi intsidentlari natijasida yuzaga keladigan xavf-xatarlar, iqtisodiy yo'qotishlar soni va darajasini kamaytirish;
 - 4) xizmatlar ko'rsatish orqali axborot xavfsizligi jarayonlarining etuklik darajasini oshirish;
 - 5) axborot xavfsizligini boshqarish jarayonini avtomatlashtirish;
 - 6) qonunchilik talablariga muvofiqligi".
1. Mahalliy vosita (ish stantsiyasini boshqarish agenti) yordamida ma'lumotlarni ushlashga qo'yiladigan talablar.
- 1.1. Umumiy talablar:
- Ish stantsiyasini boshqarish agenti tarmoqdagi ish stantsiyalariga o'rnatiladigan mustaqil dasturiy moduldir. Tizimda agentlarning ishini markazlashtirilgan tarzda o'rnatish va boshqarish tegishli sozlashlar orqali amalga oshirilishi kerak, bu agentlar ishini boshqarishning quyidagi variantlarini ta'minlashi kerak:
- 1) faol ob'ektlar bo'yicha filtrlash yordamida faqat ma'lum ish stantsiyalariga o'rnatish imkoniyati bilan agentlarni markazlashtirilgan o'rnatish Katalog va Active -dagi barcha ish stantsiyalari uchun kirish huquqlarini sozlash imkoniyati katalog ;
 - 2) Windows guruh siyosati yordamida agentlarni o'rnatish ;
 - 3) Linux bilan ishlaydigan ish stantsiyalarida agentlarni markazlashtirilgan holda o'rnatish
 - 4) keyingi qo'lda o'rnatish uchun agentlarning tarqatish paketini yaratish (agent uchun oldindan o'rnatilgan sozlamalarni tarqatish faylida saqlash

- SOC – оперативный центр информационной безопасности (англ. Security Operation Center).

Цели услуги:

- 1) соответствие требованиям законодательства в области информационной безопасности;
- 2) повышение общего уровня защищенности информационных активов Заказчика;
- 3) снижение количества и уровня рисков, экономических потерь, обусловленных угрозами и инцидентами ИБ;
- 4) повышение уровня зрелости процессов ИБ за счет предоставления услуги;
- 5) автоматизация процесса управления ИБ;
- 6) соответствие требованиям законодательства».

1. Требования к перехвату данных с помощью локального средства (агента контроля рабочей станции).

1.1. Общие требования:

Агент контроля рабочих станций - независимый программный модуль, который устанавливается на рабочие станции в сети. Централизованная установка и управление работой агентов в системе должно осуществляться путем соответствующих настроек, которые должны позволять производить следующие возможности управления работой агентов:

- 1) централизованная установка агентов, с возможностью установки только на конкретные рабочие станции с использованием фильтрации по имени компьютера и объектам Active Directory и возможностью настройки прав доступа, на все рабочие станции в Active Directory;
- 2) установка агентов при помощи групповых политик Windows;
- 3) централизованная установка агентов на рабочие станции под управлением Linux

Цели Service objectives:

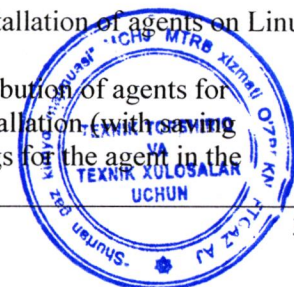
- 1) compliance with the requirements of the legislation in the field of information security;
- 2) improving the overall level of security of the Customer's information assets;
- 3) reducing the number and level of risks and economic losses caused by information security threats and incidents;
- 4) increasing the level of maturity of information security processes through the provision of services;
- 5) automation of the information security management process;
- 6) compliance with legal requirements".

1. Requirements for data interception using a local tool (workstation monitoring agent).

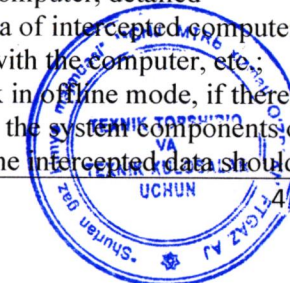
1.1. General requirements:

Workstation Monitoring Agent is an independent software module that is installed on workstations on the network. Centralized installation and management of agents in the system should be carried out by appropriate settings, which should allow you to perform the following features for managing the work of agents:

- 1) centralized installation of agents, with the ability to install only on specific workstations using filtering by computer name and Active Directory objects and the ability to configure access rights for all workstations in Active Directory;
- 2) installing agents using Windows group policies;
- 3) Centralized installation of agents on Linux workstations
- 4) creating a distribution of agents for subsequent manual installation (with saving previously made settings for the agent in the distribution file);



<p>bilan);</p> <p>5) individual ish stantsiyalarini yangilashdan istisno qilish imkoniyati bilan agentlarni avtomatik yangilash;</p> <p>6) agentlarning holatini kuzatish va har qanday oxirgi stantsiya foydalanuvchisi tomonidan agentlar yo'qligi, ishdan chiqishi yoki majburiy o'chirilishi holatlarida tegishli stantsiyada agentlarni avtomatik ravishda qayta o'rnatish.</p> <p>7) agentlarni olib tashlashdan himoya qilish;</p> <p>8) Agent jarayoni, agent fayllari va registrdagi agent ma'lumotlarini foydalanuvchi tomonidan o'zgartirishdan himoya qilish;</p> <p>9) jarayon va xizmatni, shuningdek, foydalanuvchi kompyuteridagi agent fayllari va papkalarni yashirish;</p> <p>10) Windows xavfsizlik devori qoidalari uchun maxsus nomlarni belgilash</p> <p>11) foydalanuvchi harakatlari bloklanganda sozlanishi mumkin bo'lgan bildirishnomalar;</p> <p>12) ma'lumotlarni saqlash va qayta ishlash moduliga uzatiladigan elementlarning maksimal hajmi, navbatdagi elementlarning maksimal soni, navbatni diskda ham, operativ xotirada ham saqlash imkoniyati bilan maksimal umumiy navbat hajmi bo'yicha ma'lumotlarni yuborish uchun navbatni o'rnatish;</p> <p>13) bir nechta tafsilot rejimlarini sozlash imkoniyati bilan agent hodisalarini qayd qilish: standart, ilg'or va ro'yxatga olishni butunlay o'chirish imkoniyati;</p> <p>14) agentlardan olingan va yuborilgan barcha ma'lumotlarning umumiy statistikasi;</p> <p>15) kompyuter nomi, qurilmalari va kompyuterning operatsion tizimi haqidagi umumiy ma'lumotlarni ko'rish imkoniyati bilan agentning holati va faoliyati to'g'risidagi batafsil statistik</p>	<p>4) создание дистрибутива агентов для последующей установки вручную (с сохранением в файле дистрибутива ранее выполненных настроек для агента);</p> <p>5) автоматическое обновление агентов, с возможностью исключения отдельных рабочих станций из обновления;</p> <p>6) отслеживание состояния агентов и, в случае отсутствия, сбоя или принудительного отключения агентов пользователем какой-либо конечной станции, автоматическая повторная установка агентов на соответствующей станции.</p> <p>7) защита агентов от удаления;</p> <p>8) защита процесса агента, файлов агента и данных агента в реестре от изменения пользователем;</p> <p>9) скрытие процесса и сервиса, а также файлов и папок агента на компьютере пользователя;</p> <p>10) задание пользовательских названий создаваемых правил брандмауэра Windows</p> <p>11) настраиваемые уведомления при блокировке действий пользователя;</p> <p>12) настройка очереди отправки данных в модуль хранения и обработки данных по максимальному размеру передаваемых элементов, максимальному числу элементов в очереди, максимальному общему размеру очереди с возможностью хранения очереди как на диске, так и в оперативной памяти;</p> <p>13) логирование событий агента с возможностью настройки нескольких режимов детализации: стандартный, расширенный, и возможностью полного отключения логирования;</p> <p>14) общая статистика всех принятых и отправленных данных от агентов;</p> <p>15) детализированная статистика по состоянию и активности агента с возможностями просмотра общей информации об имени компьютера, устройствах и операционной системе компьютера, детальной</p>	<p>5) automatic updating of agents, with the possibility of excluding individual workstations from the update;</p> <p>6) tracking the status of agents and, in case of absence, failure or forced disconnection of agents by the user of any end station, automatic re-installation of agents at the corresponding station.</p> <p>7) protection of agents from deletion;</p> <p>8) protecting the agent process, agent files, and agent data in the registry from user modification;</p> <p>9) hiding the process and service, as well as agent files and folders on the user's computer;</p> <p>10) setting custom names for creating Windows firewall rules</p> <p>11) custom notifications when user actions are blocked;</p> <p>12) configuring the queue for sending data to the data storage and processing module by the maximum size of transmitted elements, the maximum number of elements in the queue, the maximum total queue size with the ability to store the queue both on disk and in RAM;</p> <p>13) logging of agent events with the ability to configure several detail modes: standard, advanced, and the ability to completely disable logging;</p> <p>14) general statistics of all received and sent data from agents;</p> <p>15) detailed statistics on the state and activity of the agent with the ability to view general information about the computer name, devices and operating system of the computer, detailed information about the data of intercepted computer users, the log of actions with the computer, etc.;</p> <p>16) maintaining work in offline mode, if there is no connection between the system components or with external networks, the intercepted data should</p>
---	---	---



ma'lumotlar, ushlangan kompyuter foydalanuvchilari ma'lumotlari haqida batafsil ma'lumot, kompyuter bilan harakatlar jurnali va boshqalar. ;

16) oflayn rejimda ishlashni ta'minlash, tizim komponentlari yoki tashqi tarmoqlar o'rtasida aloqa bo'lmagan taqdirda, ushlangan ma'lumotlar mahalliy xotira hajmini va unda ma'lumotlarni saqlash muddatini cheklash imkoniyati bilan mahalliy xotirada saqlanishi kerak;

17) mahalliy saqlashning maksimal hajmini MBda ham, bo'sh disk maydonining foizi sifatida ham cheklash imkoniyati

18) interfeysda agentlarni agent serverlariga ulash oraliq'ini sozlash imkoniyati: vaqt oraliq'ini belgilash, shuningdek qabul qilingan ma'lumotlarning belgilangan miqdoriga erishilganda ulanish

19) jadvalni o'rnatish va agentlar tomonidan maksimal ma'lumotlarni uzatish tezligini cheklash orqali tarmoq resurslariga yukni optimallashtirish.

Agentlardan serverga ma'lumotlarni uzatish usuli quyidagi talablarga javob berishi kerak:

1) Tarmoq yukini optimallashtirish uchun agentlardan markaziy serverga ma'lumotlarni uzatish oraliq agent serverlari orqali amalga oshirilishi kerak.

2) tarmoq yukini muvozanatlash uchun bir nechta agent serverlarini o'rnatish imkoniyati

3) agentlar va agent serverlar o'rtasida xavfsiz tarmoq aloqa protokolidan foydalanish imkoniyati

4) agentlar va agent serverlar o'rtasidagi trafikni himoya qilish usulini tanlash qobiliyati (trafikni shifrlash yoki raqamli imzo)

5) agentlar va agent serverlar o'rtasidagi tarmoq aloqa protokoli trafikni siqishni qo'llab-quvvatlashi kerak

информацией о данных перехваченных пользователей компьютера, лога действий с компьютером и др.;

16) поддержание работы в автономном режиме, в случае отсутствия соединения между компонентами системы или с внешними сетями, перехваченные данные должны храниться в локальном хранилище с возможностями ограничения размера локального хранилища и срока хранения данных в нем;

17) возможность ограничения предельного размера локального хранилища как в Мб, так и в процентах от свободного места на диске

18) возможность настройки в интерфейсе интервала подключения агентов к серверам агентов: задание временного интервала, а также подключение по достижению заданного объема полученных данных

19) оптимизация нагрузки на сетевые ресурсы путем настройки расписания и ограничения максимальной скорости передачи данных агентами.

Способ передачи данных с агентов на сервер должен соответствовать следующим требованиям:

1) для оптимизации нагрузки на сеть передача данных от агентов на центральный сервер должна происходить через промежуточные серверы агентов.

2) возможность установки нескольких серверов агентов для балансировки нагрузки на сеть

3) возможность использования защищенного протокола сетевого взаимодействия между агентами и серверами агентов

4) возможность выбора способа защиты трафика между агентами и серверами агентов (шифрование трафика либо цифровая подпись)

5) протокол сетевого взаимодействия между агентами и серверами агентов должен поддерживать сжатие трафика

1.2. Требования к контролируемым агентами каналам передачи данных:

be stored in local storage with the ability to limit the size of local storage and the storage period of data in it;

17) the ability to limit the maximum size of local storage both in MB and as a percentage of free disk space

18) the ability to configure the interval for connecting agents to agent servers in the interface: setting a time interval, as well as connecting when the specified amount of received data is reached

19) optimize the load on network resources by configuring the schedule and limiting the maximum data transfer rate by agents.

The method of transferring data from agents to the server must meet the following requirements:

1) to optimize the network load, data transfer from agents to the central server must occur through intermediate agent servers.

2) ability to install multiple agent servers for network load balancing

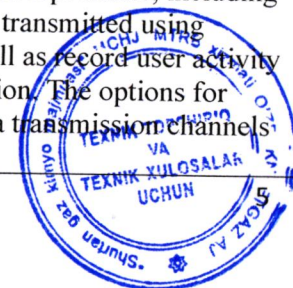
3) ability to use a secure network communication protocol between agents and agent servers

4) ability to choose how to protect traffic between agents and agent servers (traffic encryption or digital signature)

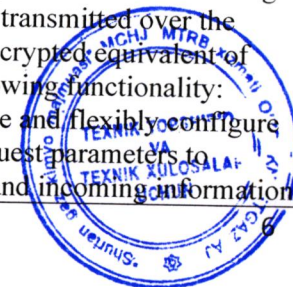
5) the network communication protocol between agents and agent servers must support traffic compression

1.2. Requirements for agent-controlled data transmission channels:

The agent module must intercept traffic, including encrypted traffic, and data transmitted using encrypted protocols, as well as record user activity on the monitored workstation. The options for configuring controlled data transmission channels should include:



<p>1.2. Agent tomonidan boshqariladigan ma'lumotlarni uzatish kanallariga qo'yiladigan talablar:</p> <p>Agent moduli trafikni, shu jumladan shifrlangan trafikni va shifrlangan protokollar orqali uzatiladigan ma'lumotlarni ushlab turishi, shuningdek, boshqariladigan ish stantsiyasida foydalanuvchi faoliyatini qayd etishi kerak. Boshqariladigan ma'lumotlarni uzatish kanallarini o'rnatish imkoniyatlari quyidagilarni o'z ichiga olishi kerak:</p> <ol style="list-style-type: none"> 1) faol guruhlar uchun individual agent sozlamalari profillari Katalog (shu jumladan domenlar, konteynerlar va tashkiliy birliklar) va Active Directory domen guruhidan tashqarida joylashgan alohida kompyuterlar uchun katalog ; 2) agent sozlamalari profilini quyidagi shartlar ostida faollashtirish: serverning bir muncha vaqt ishlamay qolishi, faol VPN ulanishi, Lua skripti yordamida belgilangan maxsus holat; 3) trafikni ushlab turish rejimlaridan birini tanlash: barcha trafik, faqat shifrlangan trafik, faqat shifrlanmagan trafik; 4) Shifrlangan trafikni ushlab turishda, foydalanuvchining SSL sertifikatidan ildiz sertifikatini sifatida foydalanish va agent tomonidan ildiz SSL sertifikatini avtomatik yaratish; 5) alohida mahalliy foydalanuvchilar ham, Active -dan individual foydalanuvchilar bundan mustasno Monitoring jarayonidagi katalog ; 6) serverlarni tarmoq trafiginini ushlab qolishdan istisno qilish; 7) alohida jarayonlarni tarmoq trafiginini ushlab qolishdan istisno qilish; 8) individual IP manzillar va diapazonlarni tarmoq trafiginini ushlab qolishdan istisno qilish. <p>1.3. Windows Agent funksional talablari</p> <p>1.3.1 HTTP/HTTPS trafiginini agent nazorati uchun talablar:</p>	<p>Агентский модуль должен выполнять перехват трафика, в том числе шифрованного, и данных, переданных по использующим шифрование протоколам, а также фиксировать активность пользователя на контролируемой рабочей станции. Возможности настройки контролируемых каналов передачи данных должны включать:</p> <ol style="list-style-type: none"> 1) индивидуальные профили настроек работы агентов как для отдельных учетных записей пользователей, компьютеров и групп Active Directory (включая домены, контейнеры и организационные единицы), так и для отдельных компьютеров, находящихся вне доменной группы Active Directory; 2) активация профиля настроек агента по следующим условиям: недоступность сервера в течении некоторого времени, активное vpn-подключение, пользовательское условие, задаваемое при помощи Lua-скрипта; 3) выбор одного из режима перехвата трафика: весь трафик, только шифрованный трафик, только нешифрованный трафик; 4) использование при перехвате шифрованного трафика как пользовательского SSL-сертификата в качестве корневого, так и автоматическая генерация агентом корневого SSL-сертификата; 5) исключение как отдельных локальных пользователей, так и отдельных пользователей из Active Directory из процесса мониторинга; 6) исключение серверов из перехвата сетевого трафика; 7) исключение отдельных процессов их перехвата сетевого трафика; 8) исключение отдельных IP-адресов и диапазонов из перехвата сетевого трафика. <p>1.3. Требования к функциональным возможностям Windows-агента</p>	<ol style="list-style-type: none"> 1) individual profiles of agent operation settings for individual user accounts, computers, and Active Directory groups (including domains, containers, and organizational units), as well as for individual computers located outside the Active Directory domain group. 2) activation of the agent settings profile based on the following conditions: server unavailability for some time, active vpn connection, custom condition set using a Lua script; 3) select one of the traffic interception modes: all traffic, encrypted traffic only, and unencrypted traffic only. 4) use of both a custom SSL certificate as the root certificate when intercepting encrypted traffic, and automatic generation of the root SSL certificate by the agent; 5) excluding both individual local users and individual Active Directory users from the monitoring process; 6) excluding servers from intercepting network traffic; 7) exclusion of individual processes of their interception of network traffic; 8) excluding individual IP addresses and ranges from network traffic interception. <p>1.3. Requirements for the functionality of the Windows Agent</p> <p>1.3.1 Requirements for the agent's control of HTTP / HTTPS traffic:</p> <p>The system should allow you to control incoming and outgoing information transmitted over the HTTP protocol and the encrypted equivalent of HTTPS and have the following functionality:</p> <ol style="list-style-type: none"> 1) the ability to create and flexibly configure filters based on HTTP request parameters to exclude certain outgoing and incoming information
---	---	--



Tizim HTTP protokoli va HTTPS ning shifrlangan analogi orqali uzatiladigan kiruvchi va chiquvchi ma'lumotlarni boshqarishga ruxsat berishi va quyidagi funksiyalarga ega bo'lishi kerak:

- 1) foydalanuvchi tomonidan yaratilgan bir qator oldindan belgilangan qoidalar va qoidalarga muvofiq ba'zi chiquvchi va kiruvchi ma'lumotlarni ushlab qolishdan istisno qilish uchun HTTP so'rov parametrlari asosida filtrlarni yaratish va moslashuvchan sozlash qobiliyati;
- 2) foydalanuvchi tomonidan yaratilgan bir qator oldindan belgilangan qoidalar va qoidalardan foydalangan holda MIME turlari bo'yicha ma'lumotlarni ushlab turishni filtrlashni sozlash imkoniyati;
- 3) uzatilgan ma'lumotlarni kuzatish uchun HTTP usullarini tanlashda GET/POST/PUT so'rovlarini ushlab turish, bloklash va filtrlash imkoniyati;
- 4) bloglar, forumlar, fayl almashish xizmatlari va boshqa veb-xizmatlarga yuborilgan xabarlar va fayllarni ushlab turish va tahlil qilish;
- 5) foydalanuvchilarning qidiruv so'rovlarini ushlab turish va tahlil qilish;
- 6) foydalanuvchi tashrif buyurgan barcha sahifalar manzillarini saqlash;
- 7) Facebook, Twitter, VKontakte, Odnoklassniki veb-resurslarida kiruvchi va chiquvchi veb-muloqot ma'lumotlarini (chat yozishmalar, nashr statuslari, sharhlar) ushlab turish;
- 8) Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex, Zimbra va boshqalar orqali uzatiladigan yoki qabul qilingan kiruvchi va chiquvchi elektron pochta xabarlari va qo'shimchalarni ushlab turish;
- 9) messenjer veb-mijozlarida uzatiladigan xabarlar va fayllarni ushlab turish: Skype, Telegram, Whatsapp, Discord, Microsoft Teams, Slack,

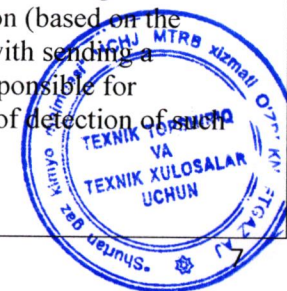
1.3.1 Требования к контролю агентом HTTP/HTTPS трафика:

Система должна позволять контролировать входящую и исходящую информацию, передаваемую по протоколу HTTP и шифрованному аналогу HTTPS и располагать следующим функционалом:

- 1) возможность создания и гибкой настройки фильтров по параметрам HTTP-запроса для исключения из перехвата определенной исходящей и входящей информации по ряду предустановленных правил и правил, созданных пользователем;
- 2) возможность настройки фильтрации перехвата данных по MIME-типам по ряду предустановленных правил и правил, созданных пользователем;
- 3) возможность перехвата, блокирования и фильтрации GET/POST/PUT запросов при выборе HTTP-методов контроля переданных данных;
- 4) перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы;
- 5) перехват и анализ поисковых запросов пользователя;
- 6) сохранение адресов всех страниц, посещенных пользователем;
- 7) перехват входящих и исходящих данных веб-коммуникаций (переписки в чатах, публикация статусов, комментарии) на веб-ресурсах: Facebook, Twitter, ВКонтакте, Одноклассники;
- 8) перехват входящих и исходящих электронных писем и вложений, переданных либо полученных через почтовые веб-сервисы (Gmail, Hotmail, Mail.ru, Rambler, Yahoo, Yandex, Zimbra и т.д.);
- 9) перехват сообщений и файлов, переданных в веб-клиентах мессенджеров: Skype, Telegram, Whatsapp, Discord, Microsoft Teams, Slack, а также перехват сообщений, переданных в веб-клиентах мессенджеров: ICQ, Google Hangouts;

from interception based on a number of preset rules and rules created by the user;

- 2) the ability to configure filtering of data interception by MIME types according to a number of preset rules and rules created by the user;
- 3) the ability to intercept, block, and filter GET/POST/PUT requests when selecting HTTP methods for controlling transmitted data;
- 4) interception and analysis of messages and files sent to blogs, forums, file-sharing services and other web services;
- 5) interception and analysis of user search queries;
- 6) saving the addresses of all pages visited by the user;
- 7) interception of incoming and outgoing data of web communications (chat conversations, posting statuses, comments) on web resources: Facebook, Twitter, VKontakte, Odnoklassniki;
- 8) interception of incoming and outgoing emails and attachments sent or received via web-based mail services (Gmail, Hotmail, etc.) Mail.ru Rambler, Yahoo, Yandex, Zimbra, etc.)
- 9) interception of messages and files transmitted in the web clients of instant messengers: Skype, Telegram, Whatsapp, Discord, Microsoft Teams, Slack, as well as interception of messages transmitted in the web clients of instant messengers: ICQ, Google Hangouts;
- 10) automatic detection of messages and files containing certain information (based on the specified security policies) with sending a notification to the person responsible for information security in case of detection of such information;



shuningdek, tezkor messenjer veb-mijozlarida uzatiladigan xabarlarni ushlar: ICQ , Google Hangouts ;

10) ma'lum ma'lumotlarni o'z ichiga olgan xabarlar va fayllarni avtomatik aniqlash (belgilangan xavfsizlik siyosati asosida), agar bunday ma'lumotlar aniqlangan bo'lsa, axborot xavfsizligi uchun mas'ul shaxsga xabarnoma yuborish;

11) HTTP(S) protokoli orqali uzatiladigan xabarlar va fayllarning matni va atributlari bo'yicha qidirish imkoniyati;

12) veb-resurslarga, chiquvchi xabarlar va fayllarga tashrif buyurishni mazmuni, atributlar to'plami, shuningdek yuborilgan fayllarning xesh miqdori bo'yicha bloklash imkoniyati;

13) HTTP(S) trafigini blokirovka qilish haqida maxsus xabarni sozlash imkoniyati.

1.3.2 Tezkor messenjerlarda yozishmalarini kuzatishga qo'yiladigan talablar:

Tizim foydalanuvchi yozishmalarini, yuborilgan fayllar va suhbatlarni ko'p havolali almashinuv dasturlarida boshqarishga imkon berishi va quyidagi funksiyalarga ega bo'lishi kerak:

1) Viber , Telegram (shu jumladan veb-versiyasi), WhatsApp (shu jumladan veb-versiyasi), Skype (shu jumladan veb-versiyasi), Microsoft-da matnli xabarlarni ushlar Lync , Microsoft Jamoalar (shu jumladan veb-versiyasi), Discord (shu jumladan veb-versiyasi), Hangouts , Slack (shu jumladan veb-versiyasi), WeChat , Signal , Express , Vk Jamoalar . Agent Mail.ru, ICQ10, ICQ, RocketChat , shuningdek SIP, OSCAR, XMPP (shu jumladan HTTP orqali XMPP), YMSG protokollaridan foydalangan holda messenjerlarda.

2) Viber , Telegram , WhatsApp (shu jumladan veb-versiyasi), Skype (shu jumladan veb-versiyasi), Microsoft messenjerlarida uzatiladigan fayllarni

10) автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

11) возможность поиска по тексту и атрибутам сообщений и файлов, переданных по протоколу HTTP(S);

12) возможность блокирования посещений веб-ресурсов, исходящих сообщений и файлов, по контенту, по набору атрибутов, а также по хеш-сумме отправляемых файлов;

13) возможность настройки пользовательского сообщения про блокировки HTTP(S) трафика.

1.3.2 Требования к контролю переписки в мессенджерах:

Система должна позволять контролировать переписку пользователей, отправляемые файлы и разговоры в программах многозвенного обмена и располагать следующим функционалом:

1) Перехват текстовых сообщений в мессенджерах Viber, Telegram (включая веб-версию), WhatsApp (включая веб-версию), Skype (включая веб-версию), Microsoft Lync, Microsoft Teams (включая веб-версию), Discord (включая веб-версию), Hangouts, Slack (включая веб-версию), WeChat, Signal, Express, Vk Teams. Агент Mail.ru, ICQ10, ICQ, RocketChat, а также в мессенджерах, использующих протоколы SIP, OSCAR, XMPP (включая XMPP по HTTP), YMSG.

2) Перехват файлов, передаваемых в мессенджерах Viber, Telegram, WhatsApp (включая веб-версию), Skype (включая веб-версию), Microsoft Lync, RocketChat, Microsoft Teams (включая веб-версию), Discord (включая веб-версию), Slack (включая веб-версию), Signal, Express, Vk Teams.

3) Перехват голосовых разговоров, осуществляемых через Skype (в том числе звонки Skype-to-Skype, Skype-to-phone), а также через Microsoft Lync, Viber, Zoom,

11) ability to search by text and attributes of messages and files transmitted over the HTTP(S) protocol;

12) the ability to block visits to web resources, outgoing messages and files, by content, by a set of attributes, as well as by the hash sum of sent files;

13) the ability to configure a custom message about blocking HTTP (S) traffic.

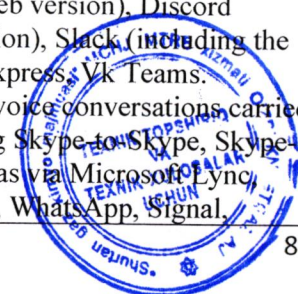
1.3.2 Requirements for monitoring correspondence in instant messengers:

The system should allow you to control user correspondence, files sent, and conversations in multi-link exchange programs and have the following functionality:

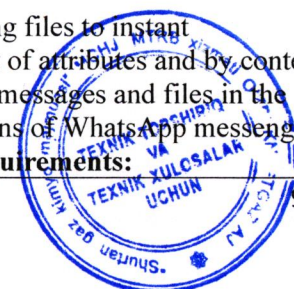
1) Interception of text messages in the messengers Viber, Telegram (including the web version), WhatsApp (including the web version), Skype (including the web version), Microsoft Lync, Microsoft Teams (including the web version), Discord (including the web version), Hangouts, Slack (including the web version).version), WeChat, Signal, Express, Vk Teams. Agent Mail.ru ICQ10, ICQ, RocketChat, as well as in instant messengers that use the SIP, OSCAR, XMPP (including XMPP over HTTP), and YMSG protocols.

2) Interception of files transmitted in the messengers Viber, Telegram, WhatsApp (including the web version), Skype (including the web version), Microsoft Lync, RocketChat, Microsoft Teams (including the web version), Discord (including the web version), Slack (including the web version), Signal, Express, Vk Teams.

3) Interception of voice conversations carried out via Skype (including Skype-to-Skype, Skype-to-phone calls), as well as via Microsoft Lync, Viber, Zoom, Telegram, WhatsApp, Signal.



<p>ushlash Lync , RocketChat , Microsoft Jamoalar (shu jumladan veb-versiyasi), Discord (shu jumladan veb-versiyasi), Slack (shu jumladan veb-versiyasi), Signal , Express , Vk Jamoalar .</p> <p>3) Skype orqali (shu jumladan Skype-dan Skype-ga , Skype-dan telefonga qo'ng'iroqlar), shuningdek Microsoft orqali amalga oshiriladigan ovozli suhbatlarni ushlab turish. Lync , Viber , Zoom , Telegram , WhatsApp , Signal , Express , Vk Jamoalar va suhbatlarni MP3 fayllarga saqlash bilan SIP protokoli orqali;</p> <p>4) ovozli suhbatlarni (muloqotlarni) tanib olish va matn formatiga tarjima qilish qobiliyati Microsoft Lync , Skype , Viber , Zoom , Telegram , WhatsApp , Signal , Express , Vk Jamoalar va SIP;</p> <p>5) Microsoft suhbatlarini o'ynash imkoniyati Lync , Skype , Viber , Zoom , Telegram , WhatsApp , Signal , Express , Vk Jamoalar va SIP;</p> <p>6) individual foydalanuvchi hisoblari tomonidan ushlashni cheklash imkoniyati;</p> <p>7) ma'lum ma'lumotlarni o'z ichiga olgan xabarlar va fayllarni avtomatik aniqlash (belgilangan xavfsizlik siyosati asosida), agar bunday ma'lumotlar aniqlangan bo'lsa, axborot xavfsizligi uchun mas'ul shaxsga xabarnoma yuborish;</p> <p>8) lahzali messenjerlar orqali yuborilgan xabarlar va fayllarning matni va atributlari bo'yicha, shu jumladan shablonlardan foydalangan holda qidirish imkoniyati .</p> <p>9) messenjer veb-mijozlarida uzatiladigan xabarlar va fayllarni ushlash: Skype , Telegram , Whatsapp , Discord , Microsoft Teams , Slack , shuningdek, tezkor messenjer veb-mijozlarida uzatiladigan xabarlarni ushlash: ICQ , Google Hangouts ;</p> <p>10) Facebook , LinkedIn dagi yozishmalar va xabarlarni nazorat qilish .</p>	<p>Telegram, WhatsApp, Signal, Express, Vk Teams и по протоколу SIP с сохранением разговоров в файлы формата MP3;</p> <p>4) возможность распознавания и перевода в текстовый формат голосовых разговоров (коммуникаций) Microsoft Lync, Skype, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams и SIP;</p> <p>5) возможность воспроизведения сохраненных разговоров Microsoft Lync, Skype, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams и SIP;</p> <p>6) возможность ограничения перехвата по отдельным учетным записям пользователей;</p> <p>7) автоматическое обнаружение сообщений и файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;</p> <p>8) возможность осуществления поиска по тексту и атрибутам сообщений и файлов, переданных через мессенджеры, в том числе с применением шаблонов.</p> <p>9) перехват сообщений и файлов, переданных в веб-клиентах мессенджеров: Skype, Telegram, Whatsapp, Discord, Microsoft Teams, Slack, а также перехват сообщений, переданных в веб-клиентах мессенджеров: ICQ, Google Hangouts;</p> <p>10) контроль переписок и постов в Facebook, LinkedIn.</p> <p>11) контроль переписок в Instagram.</p> <p>12) контроль переписок, электронной почты и файлов в CMS Bitrix24.</p> <p>13) блокировка отправки файлов в мессенджеры, как по набору атрибутов так и по содержанию</p> <p>14) перехват голосовых сообщений и файлов в web- и dekstop-версиях мессенджера WhatsApp.</p> <p>1.3.3 Требования к контролю печати:</p>	<p>Express, Vk Teams and SIP protocol with saving conversations to MP3 files;</p> <p>4) the ability to recognize and translate Microsoft Lync, Skype, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams, and SIP voice conversations (communications) into text format.</p> <p>5) ability to play saved conversations of Microsoft Lync, Skype, Viber, Zoom, Telegram, WhatsApp, Signal, Express, Vk Teams and SIP;</p> <p>6) the ability to limit interception by individual user accounts;</p> <p>7) automatic detection of messages and files containing certain information (based on the specified security policies) with sending a notification to the person responsible for information security in case of detection of such information;</p> <p>8) ability to search by text and attributes of messages and files sent via instant messengers, including using templates.</p> <p>9) interception of messages and files transmitted in the web clients of instant messengers: Skype, Telegram, Whatsapp, Discord, Microsoft Teams, Slack, as well as interception of messages transmitted in the web clients of instant messengers: ICQ, Google Hangouts;</p> <p>10) control of correspondence and posts on Facebook, LinkedIn.</p> <p>11) control your Instagram conversations.</p> <p>12) control of correspondence, email, and files in the Bitrix24 CMS.</p> <p>13) blocking sending files to instant messengers, both by set of attributes and by content</p> <p>14) intercept voice messages and files in the web and dekstop versions of WhatsApp messenger.</p> <p>1.3.3 Print control requirements:</p>
--	--	--



- 11) Instagramda yozishmalarni nazorat qilish .
- 12) CMS Bitrix24 da yozishmalar, elektron pochta va fayllarni nazorat qilish.
- 13) atributlar to'plami va mazmuni bo'yicha tezkor xabarchilarga fayllarni yuborishni bloklash
- 14) WhatsApp messenjerining veb va ish stoli versiyalarida ovozli xabarlar va fayllarni ushlab .

1.3.3 Chop etishni boshqarishga qo'yiladigan talablar:

Tizim tarmoq, mahalliy va virtual printerlarga yuborilgan hujjatlarni chop etishni nazorat qilishi va quyidagi funksiyalarga ega bo'lishi kerak:

- 1) foydalanuvchining ish stantsiyalarida o'rnatilgan agentlar tomonidan chop etish uchun yuborilgan hujjatlarni ushlab;
- 2) tarmoqqa, virtual va mahalliy printerlarga (shu jumladan COM va LPT portlariga ulangan) yuborilgan hujjatlarni tutib olish imkoniyati;
- 3) XPS formatida chop etishni to'xtatish qobiliyati;
- 4) individual printerlar uchun to'xtatib turishdan istisnolarni sozlash imkoniyati;
- 5) sahifalar soni va hujjat hajmi bo'yicha chop etishni ushlab turishni cheklash imkoniyati;
- 6) printerlarda chop etishni ushlab turish moduli uchun jarayonlarni istisno qilish imkoniyati.
- 7) chop etish uchun yuborilgan hujjatlar matnini ajratib olish va tahlil qilish;
- 8) ma'lum ma'lumotlarni o'z ichiga olgan fayllarni avtomatik ravishda aniqlash (belgilangan xavfsizlik siyosati asosida), agar bunday ma'lumotlar aniqlangan bo'lsa, axborot xavfsizligi uchun mas'ul shaxsga xabarnoma yuborish;
- 9) hujjat nomi bo'yicha chop etishni bloklash imkoniyati. hujjatning matn tarkibi va printer nomi;
- 10) chop etish uchun yuborilgan fayllarning matni va atributlari, shu jumladan shablonlardan

Система должна контролировать печать документов, отправляемых на сетевые, локальные и виртуальные принтеры, и располагать следующим функционалом:

- 1) перехват отправляемых на печать документов агентами, установленными на рабочих станциях пользователей;
- 2) возможность перехвата документов, отправляемых на сетевые, виртуальные и локальные принтеры (в том числе подключенные к COM-, LPT-портам);
- 3) возможность перехвата печати в XPS-формат;
- 4) возможность настройки исключений из перехвата по отдельным принтерам;
- 5) возможность ограничения перехвата печати по количеству страниц и по размеру документа;
- 6) возможность исключения процессов для модуля перехвата печати на принтерах.
- 7) извлечение и анализ текста отправленных на печать документов;
- 8) автоматическое обнаружение файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- 9) возможность блокировки печати по названию документа. текстовому содержимому документа и по названию принтера;
- 10) возможность поиска по тексту и атрибутам отправленных на печать файлов, в том числе с применением шаблонов;
- 11) сохранение в PDF- и XPS-формате.
- 12) возможность блокировки документов, отправляемых на печать как по набору атрибутов, так и по содержимому документа, отправляемого на печать.

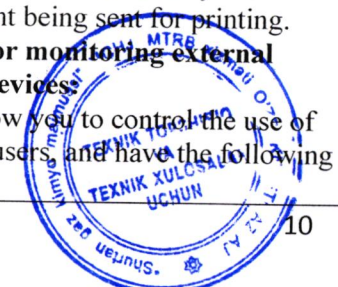
1.3.4 Требования к контролю внешних устройств и накопителей:

The system must control the printing of documents sent to network, local, and virtual printers and have the following functionality:

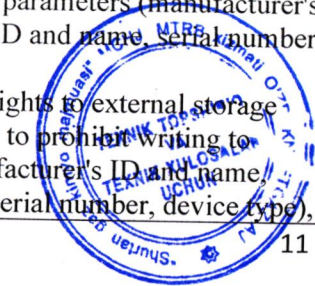
- 1) interception of documents sent for printing by agents installed on user workstations;
- 2) the ability to intercept documents sent to network, virtual and local printers (including those connected to COM and LPT ports);
- 3) the ability to intercept printing in XPS format;
- 4) the ability to configure exceptions from interception for individual printers;
- 5) the ability to limit print interception by the number of pages and document size;
- 6) the ability to exclude processes for the print interception module on printers.
- 7) extract and analyze the text of documents sent for printing;
- 8) automatic detection of files containing certain information (based on the specified security policies) with sending a notification to the person responsible for information security in case of detection of such information;
- 9) ability to block printing by document name. the text content of the document and the name of the printer.
- 10) the ability to search by text and attributes of files sent for printing, including using templates;
- 11) Save in PDF and XPS format.
- 12) the ability to block documents sent for printing both by a set of attributes and by the content of the document being sent for printing.

1.3.4 Requirements for monitoring external devices and storage devices:

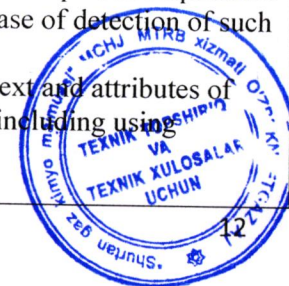
The system should allow you to control the use of drives and devices by users, and have the following functionality:



<p>foydalangan holda qidirish imkoniyati;</p> <p>11) PDF va XPS formatida saqlash.</p> <p>12) bosib chiqarish uchun yuborilgan hujjatlarni atributlar to'plami bo'yicha ham, chop etishga yuborilgan hujjatning mazmuni bo'yicha ham bloklash imkoniyati.</p> <p>1.3.4 Tashqi qurilmalar va saqlash qurilmalarini kuzatishga qo'yiladigan talablar:</p> <p>Tizim foydalanuvchilar tomonidan drayverlar va qurilmalardan foydalanishni nazorat qilish imkonini berishi va quyidagi funksiyalarga ega bo'lishi kerak:</p> <p>1) tashqi qurilma ulanishi auditi</p> <p>2) tashqi diskarga yuborilgan fayllarni soyalini nusxalash (olinadigan qattiq disklar, flesh -disklar, xotira kartalari, olinadigan disklar, CD/DVD va floppi drayvlar va boshqalar);</p> <p>3) flesh -disklar, xotira kartalari, olinadigan drayvlar, CD/DVD va floppi disklar va boshqalar) nusxalash hodisalarini tekshirish, fayl nomi, foydalanuvchi, sana, vaqt va qurilma ma'lumotlarini yozish;</p> <p>4) fayl hajmi va kengaytmasi asosida soya nusxalash va auditdan istisnolarni sozlash imkoniyati;</p> <p>5) katta fayllar uchun soya nusxasini qisman saqlashni sozlash imkoniyati (masalan, faqat birinchi 100 MBni saqlang);</p> <p>6) ma'lumotlarni serverga jo'natishdan oldin tashqi disklarda saqlangan fayllarning soya nusxalarini mahalliy ravishda boshqariladigan kompyuterlarda saqlash;</p> <p>7) boshqariladigan kompyuterlarda soyalini nusxalar uchun saqlash hajmini sozlash imkoniyati;</p> <p>8) uzatiladigan ma'lumotlarning mazmuni va boshqa atributlar asosida olinadigan tashuvchiga fayllarni yozishni bloklash imkoniyati.</p> <p>9) ba'zi tashqi xotira qurilmalari (qurilma turlari, identifikatorlar, ishlab chiqaruvchilar, nomlar, seriya</p>	<p>Система должна позволять контролировать использование накопителей и устройств пользователями, и располагать следующим функционалом:</p> <p>1) аудит подключения внешних устройств</p> <p>2) теневое копирование файлов, отправляемых на внешние накопители (съёмные жесткие диски, флеш-накопители, карты памяти, съёмные накопители, CD/DVD и флоппи-диски и т.д.);</p> <p>3) аудит событий копирования файлов на внешние накопители (съёмные жесткие диски, флеш-накопители, карты памяти, съёмные накопители, CD/DVD и флоппи-диски и т.д.), фиксируется имя файла, пользователь, дата, время и данные устройства;</p> <p>4) возможность настройки исключений из теневого копирования и аудита по размеру и расширению файлов;</p> <p>5) возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);</p> <p>6) сохранение теневых копий файлов, записанных на внешние накопители, локально на контролируемых компьютерах перед отправкой данных на сервер;</p> <p>7) возможность настройки размера хранилища для теневых копий на контролируемых компьютерах;</p> <p>8) возможность блокирования записи файлов на съёмные носители по содержанию передаваемой информации и другим атрибутам.</p> <p>9) возможность настройки исключений из теневого копирования и аудита для определенных внешних накопителей информации (по типам устройств, идентификаторам, производителям, названиям, серийным номерам);</p> <p>10) контроль доступа к внешним накопителям информации, с возможностью запрета на использование устройств с определенными параметрами (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства и др.);</p>	<p>1) audit the connection of external devices</p> <p>2) shadow copying of files sent to external storage devices (removable hard drives, flash drives, memory cards, removable drives, CD / DVD and floppy disks, etc.);</p> <p>3) audit of events of copying files to external drives (removable hard drives, flash drives, memory cards, removable drives, CD / DVD and floppy disks, etc.), the file name, user, date, time and device data are recorded;</p> <p>4) the ability to configure exceptions from shadow copying and auditing by file size and extension;</p> <p>5) the ability to configure partial shadow copy saving for large files (for example, save only the first 100 MB);</p> <p>6) saving shadow copies of files written to external drives locally on controlled computers before sending data to the server;</p> <p>7) the ability to configure the storage size for shadow copies on controlled computers;</p> <p>8) the ability to block writing files to removable media based on the content of the transmitted information and other attributes.</p> <p>9) the ability to configure exceptions from shadow copying and auditing for certain external storage devices (by device types, identifiers, manufacturers, names, serial numbers);</p> <p>10) control of access to external storage devices, with the possibility of prohibiting the use of devices with certain parameters (manufacturer's ID and name, product ID and name, serial number, device type, etc.);</p> <p>11) manage write rights to external storage devices with the ability to prohibit writing to specific devices (manufacturer's ID and name, product ID and name, serial number, device type),</p>
---	---	---



<p>raqamlari bo'yicha) uchun soyadan nusxa ko'chirish va tekshirishdan istisnolarni sozlash imkoniyati;</p> <p>10) ma'lum parametrlarga (ishlab chiqaruvchi identifikatori va nomi, mahsulot identifikatori va nomi, seriya raqami, qurilma turi va boshqalar) ega qurilmalardan foydalanishni taqiqlash imkoniyati bilan tashqi ma'lumotlarni saqlash qurilmalariga kirishni boshqarish;</p> <p>11) muayyan qurilmalarga (ishlab chiqaruvchi identifikatori va nomi, mahsulot identifikatori va nomi, seriya raqami, qurilma turi) yozishni taqiqlash, shuningdek, ma'lum kengaytmali fayllarni yozishni taqiqlash qobiliyatiga ega tashqi diskarga yozish huquqlarini boshqarish ;</p> <p>12) mahalliy va terminal foydalanuvchi seanslarida tashqi xotira qurilmalariga ma'lumotlarni nusxalashni nazorat qilish imkoniyati;</p> <p>13) alohida jarayonlarni nazorat tartibidan chiqarib tashlash, soyali nusxa ko'chirish auditi.</p> <p>14) kirishni boshqarish va qo'llab-quvvatlanadiganlar ro'yxatidan har qanday turdagi tashqi qurilmalardan foydalanishni tekshirish (USB Bus Qurilmalar (markazlar va mezbob kontrollerlar), CD\DVD, Audio , Tarmoq Adapterlar , seriyali va parallel portlar , SCSI va RAID kontrollerlari , Floppy drayvlar , kameralar va skanerlar , Windows Portativ Qurilmalar (WPD), universal kameralar), ish stantsiyasiga ulangan, parametrlar to'plami (qurilma nomi, qurilma identifikatori, ishlab chiqaruvchi identifikatori, mahsulot identifikatori, ishlab chiqaruvchi, seriya raqami, qurilma turi) filtrlangan;</p> <p>15) boshqariladigan ish stantsiyalariga ulangan qurilmalarni istisno filtriga qo'shish;</p> <p>16) belgilangan parametrlarga ega (belgilangan xavfsizlik siyosati asosida) tashqi qurilmalardan foydalanish holatlarini avtomatik aniqlash, agar bunday ma'lumotlar aniqlangan bo'lsa, axborot</p>	<p>11) управление правами записи на внешние накопители с возможностью запрета записи на определенные устройства (идентификатор и имя производителя, идентификатор и название продукта, серийный номер, тип устройства), а также запрета записи файлов с определенным расширением;</p> <p>12) возможность контроля копирования информации на внешние накопители как в локальных, так и терминальных пользовательских сессиях;</p> <p>13) исключение отдельных процессов из процедуры контроля, аудита теневого копирования.</p> <p>14) контроль доступа и аудит использования внешних устройств любого типа из списка поддерживаемых (USB Bus Devices (hubs and host controllers), CD\DVD, Audio, Network Adapters, Serial and parallel ports, SCSI and RAID controllers, Floppy drives, Cameras and scanners, Windows Portable Devices (WPD), Universal cameras), подключаемых к рабочей станции, с фильтрацией по набору параметров (название устройства, идентификатор устройства, идентификатор производителя, идентификатор продукта, производитель, серийный номер, тип устройства);</p> <p>15) добавление в фильтр исключений устройств, подключенных на контролируемых рабочих станциях;</p> <p>16) автоматическое обнаружение случаев использования внешних устройств с указанными параметрами (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;</p> <p>17) автоматическое обнаружение случаев передачи на внешние накопители файлов в целом и, в частности, содержащих определенную информацию (на основании заданных политик безопасности), с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;</p>	<p>as well as prohibit writing files with a specific extension;</p> <p>12) the ability to control copying of information to external drives in both local and terminal user sessions;</p> <p>13) exclusion of individual processes from the shadow copy control and audit procedure.</p> <p>14) access control and audit of the use of external devices of any type from the list of supported devices (USB Bus Devices (hubs and host controllers), CD\DVD, Audio, Network Adapters, Serial and parallel ports, SCSI and RAID controllers, Floppy drives, Cameras and scanners, Windows Portable Devices (WPD), Universal cameras) connected to the workstation, filtered by a set of parameters (device name, device ID, manufacturer ID, product ID, manufacturer, serial number, device type).</p> <p>15) adding devices connected on controlled workstations to the exception filter.</p> <p>16) automatic detection of cases of using external devices with the specified parameters (based on the specified security policies) with sending a notification to the person responsible for information security in case of detection of such information;</p> <p>17) automatic detection of cases when files in general and, in particular, containing certain information are transferred to external storage devices (based on the specified security policies), with sending a notification to the person responsible for information security in case of detection of such information;</p> <p>18) ability to search by text and attributes of files sent to external drives, including using templates.</p>
---	--	---



xavfsizligi uchun mas'ul shaxsga xabarnoma yuborish;

17) umumiy va, xususan, ma'lum ma'lumotlarni o'z ichiga olgan (belgilangan xavfsizlik siyosati asosida) fayllarni tashqi xotira qurilmalariga o'tkazish holatlarini avtomatik ravishda aniqlash, agar bunday ma'lumotlar aniqlangan bo'lsa, axborot xavfsizligi uchun mas'ul shaxsga xabarnoma yuborish;

18) matn va tashqi xotira qurilmalariga yuborilgan fayllarning atributlari, shu jumladan shablonlardan foydalangan holda qidirish imkoniyati.

19) drayverga yozilgan fayllarni ham atributlar to'plami, ham mazmuni bo'yicha bloklash imkoniyati

1.3.5 Bulutli saqlashni boshqarishga qo'yiladigan talablar:

Tizim ish stoli bulutli saqlash ilovalarini (iCloud , Dropbox , Google) kuzatish uchun quyidagi imkoniyatlarni taqdim etishi kerak. Drive , OneDrive , Cloud Mail.ru, Yandex.Disk):

1) fayllarni bulutli saqlashga yuborish hodisalari auditi: fayl nomi, foydalanuvchi nomi, bulutli saqlash xizmatining sanasi, vaqti va nomi qayd etiladi;

2) foydalanuvchi yoki jarayon tomonidan bulutli saqlashga yuborilgan fayllarni soyali nusxalash;

3) faqat chiquvchi, faqat kiruvchi yoki barcha fayllarni tekshirish va soyali nusxalashni sozlash;

4) katta fayllar uchun soya nusxasini qisman saqlashni sozlash imkoniyati (masalan, faqat birinchi 100 MBni saqlang);

5) serverga yuborishdan oldin bulutli xotirada saqlangan fayllarning soya nusxalarini mahalliy ravishda boshqariladigan kompyuterlarda saqlash;

6) foydalanuvchilarning mahalliy kompyuterlarida soya nusxalari uchun saqlash hajmini sozlash imkoniyati;

7) muayyan foydalanuvchilarga kirishni rad etish imkoniyati bilan alohida bulutli omborlarga

18) возможность поиска по тексту и атрибутам отправленных на внешние накопители файлов, в том числе с применением шаблонов.

19) возможность блокировки файлов, записываемых на накопитель как по набору атрибутов, так и по содержанию

1.3.5 Требования к контролю облачных хранилищ:

Система должна обеспечивать следующие возможности по контролю десктопных приложений облачных хранилищ (iCloud, Dropbox, Google Drive, OneDrive, Облако Mail.ru, Яндекс.Диск):

1) аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, имя пользователя, дата, время и имя облачного сервиса хранения;

2) теневое копирование файлов, отправляемых в облачные хранилища пользователем либо процессом;

3) настройка аудита и теневого копирования только исходящих, только входящих, либо всех файлов;

4) возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);

5) сохранение теневых копий файлов, записанных в облачное хранилище, локально на контролируемых компьютерах перед отправкой на сервер;

6) возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;

7) контроль доступа к отдельным облачным хранилищам с возможностью запрета доступа для определенных пользователей;

8) контроль доступа к отдельным облачным хранилищам с возможностью настройки режима «только чтение» для определенных пользователей;

9) управление правами передачи данных в облачные хранилища с возможностью запрета отправки файлов определенных форматов;

19) the ability to block files written to the drive both by a set of attributes and by content

1.3.5 Cloud storage monitoring requirements:

The system should provide the following capabilities for monitoring desktop cloud storage applications (iCloud, Dropbox, Google Drive, OneDrive, Cloud Mail.ru, Yandex. Disk):

1) audit of events when files are sent to cloud storage: the file name, user name, date, time, and name of the cloud storage service are recorded.

2) shadow copying of files sent to cloud storage by a user or process;

3) configure auditing and shadow copying of only outgoing, only incoming, or all files;

4) the ability to configure partial shadow copy saving for large files (for example, save only the first 100 MB);

5) saving shadow copies of files recorded in the cloud storage locally on controlled computers before sending them to the server;

6) the ability to configure the storage size for shadow copies on users ' local computers;

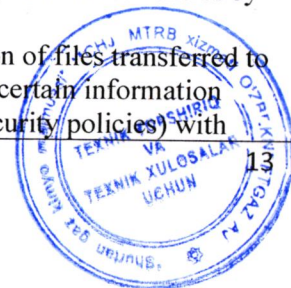
7) control of access to individual cloud storages with the ability to prohibit access for certain users;

8) access control to individual cloud storages with the ability to configure the "read-only" mode for certain users;

9) manage the rights to transfer data to cloud storage with the ability to prohibit sending files of certain formats;

10) the ability to configure exceptions from auditing, shadow copying, and access control by file extensions;

11) automatic detection of files transferred to cloud storages containing certain information (based on the specified security policies) with



kirishni boshqarish;

8) ma'lum foydalanuvchilar uchun faqat o'qish rejimini sozlash imkoniyati bilan alohida bulutli omborlarga kirishni boshqarish;

9) ma'lum formatdagi fayllarni yuborishni taqiqlash qobiliyati bilan ma'lumotlarni bulutli saqlashga o'tkazish huquqlarini boshqarish;

10) audit, soyali nusxalash va fayl kengaytmalari orqali kirishni boshqarishdan istisnolarni sozlash imkoniyati;

11) ma'lum ma'lumotlarni (belgilangan xavfsizlik siyosati asosida) o'z ichiga olgan bulutli xotiraga o'tkazilgan fayllarni avtomatik aniqlash, agar bunday ma'lumotlar aniqlangan bo'lsa, axborot xavfsizligi uchun mas'ul shaxsga xabarnoma yuborish;

12) yuborilgan fayllarning matni va atributlari, shu jumladan shablonlardan foydalangan holda qidirish imkoniyati.

Tizim bulutli saqlashning veb-versiyalarini (iCloud , Dropbox , Google) boshqarish uchun quyidagi imkoniyatlarni taqdim etishi kerak. Drive , OneDrive , Cloud Mail.ru, Yandex.Disk , ownCloud):

1) fayllarni bulutli saqlashga yuborish hodisalari auditi: fayl nomi, foydalanuvchi nomi, bulutli saqlash xizmatining sanasi, vaqti va nomi qayd etiladi;

2) foydalanuvchi yoki jarayon tomonidan bulutli saqlashga yuborilgan fayllarni soyali nusxalash;

3) serverga yuborishdan oldin bulutli xotirada saqlangan fayllarning soya nusxalarini mahalliy ravishda boshqariladigan kompyuterlarda saqlash;

4) ma'lum ma'lumotlarni (belgilangan xavfsizlik siyosati asosida) o'z ichiga olgan bulutli xotiraga o'tkazilgan fayllarni avtomatik aniqlash, agar bunday ma'lumotlar aniqlangan bo'lsa, axborot xavfsizligi uchun mas'ul shaxsga xabarnoma yuborish;

5) yuborilgan fayllarning matni va atributlari, shu jumladan shablonlardan foydalangan holda

10) возможность настройки исключений из аудита, теневого копирования и контроля доступа по расширениям файлов;

11) автоматическое обнаружение переданных в облачные хранилища файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

12) возможность поиска по тексту и атрибутам отправленных файлов, в том числе с применением шаблонов.

Система должна обеспечивать следующие возможности по контролю веб-версий облачных хранилищ (iCloud, Dropbox, Google Drive, OneDrive, Облако Mail.ru, Яндекс.Диск, ownCloud):

1) аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, имя пользователя, дата, время и имя облачного сервиса хранения;

2) теневое копирование файлов, отправляемых в облачные хранилища пользователем либо процессом;

3) сохранение теневых копий файлов, записанных в облачное хранилище, локально на контролируемых компьютерах перед отправкой на сервер;

4) автоматическое обнаружение переданных в облачные хранилища файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

5) возможность поиска по тексту и атрибутам отправленных файлов, в том числе с применением шаблонов.

1.3.6 Требования к контролю сетевых ресурсов:

Система должна позволять контролировать использование пользователями сетевых ресурсов, и располагать следующим функционалом:

sending a notification to the person responsible for information security in case of detection of such information;

12) ability to search by text and attributes of sent files, including using templates.

The system should provide the following capabilities for controlling web versions of cloud storage (iCloud, Dropbox, Google Drive, OneDrive, Cloud Mail.ru, Yandex. Disk, ownCloud):

1) audit of events when files are sent to cloud storage: the file name, user name, date, time, and name of the cloud storage service are recorded.

2) shadow copying of files sent to cloud storage by a user or process;

3) saving shadow copies of files recorded in the cloud storage locally on controlled computers before sending them to the server;

4) automatic detection of files transferred to cloud storages containing certain information (based on the specified security policies) with sending a notification to the person responsible for information security in case of detection of such information;

5) ability to search by text and attributes of sent files, including using templates.

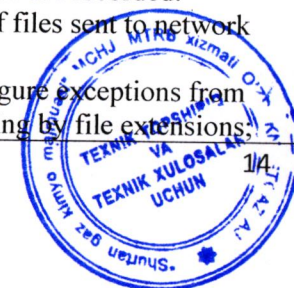
1.3.6 Requirements for monitoring network resources:

The system should allow you to control the use of network resources by users, and have the following functionality:

1) audit of file copying events to local network resources: the file name, user, date, time, and network path to the resource are recorded.

2) shadow copying of files sent to network resources;

3) the ability to configure exceptions from auditing and shadow copying by file extensions.



qidirish imkoniyati.

1.3.6 Tarmoq resurslarini monitoring qilish uchun talablar:

Tizim foydalanuvchilar tomonidan tarmoq resurslaridan foydalanishni nazorat qilish imkonini berishi va quyidagi funksiyalarga ega bo'lishi kerak:

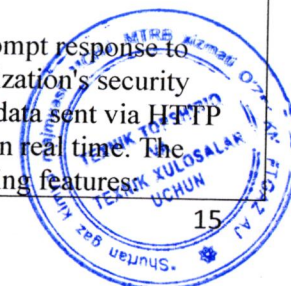
- 1) faylni mahalliy tarmoq resurslariga nusxalash hodisalari auditi: fayl nomi, foydalanuvchi, sana, vaqt va manbaga tarmoq yo'li qayd etiladi;
- 2) tarmoq resurslariga yuborilgan fayllarni soyali nusxalash;
- 3) fayl kengaytmalari asosida tekshirish va soyali nusxalashdan istisnolarni sozlash imkoniyati;
- 4) muayyan tarmoq resurslarini tekshirish va soyali tutib olishdan istisnolarni sozlash imkoniyati;
- 5) katta fayllar uchun soya nusxasini qisman saqlashni sozlash imkoniyati (masalan, faqat birinchi 100 MBni saqlang);
- 6) tarmoq resurslarida saqlangan fayllarning soya nusxalarini serverga yuborishdan oldin mahalliy ravishda boshqariladigan kompyuterlarda saqlash;
- 7) foydalanuvchilarning mahalliy kompyuterlarida soya nusxalari uchun saqlash hajmini sozlash imkoniyati;
- 8) terminal serverlarining tarmoq resurslariga o'tkaziladigan fayllarni nusxalash qobiliyati;
- 9) muayyan tarmoq resurslariga kirishni rad etish imkoniyati bilan tarmoq resurslariga kirishni boshqarish;
- 10) muayyan fayl formatlarini yozishni taqiqlash qobiliyati bilan tarmoq resurslariga yozish huquqlarini boshqarish;
- 11) alohida jarayonlarni nazorat tartibidan chiqarib tashlash, soya nusxasini tekshirish;
- 12) ma'lum ma'lumotlarni o'z ichiga olgan tarmoq resurslariga o'tkazilgan fayllarni avtomatik aniqlash (belgilangan xavfsizlik siyosati asosida), agar bunday

- 1) аудит событий копирования файлов на локальные сетевые ресурсы: фиксируется имя файла, пользователь, дата, время и сетевой путь к ресурсу;
- 2) теневое копирование файлов, отправляемых на сетевые ресурсы;
- 3) возможность настройки исключений из аудита и теневого копирования по расширениям файлов;
- 4) возможность настройки исключений из аудита и теневого перехвата определенных сетевых ресурсов;
- 5) возможность настройки частичного сохранения теневой копии для больших файлов (например, сохранять только первые 100 МБ);
- 6) сохранение теневых копий файлов, записанных на сетевые ресурсы, локально на контролируемых компьютерах перед отправкой на сервер;
- 7) возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;
- 8) возможность теневого копирования файлов, передаваемых на сетевые ресурсы терминальных серверов;
- 9) контроль доступа к сетевым ресурсам с возможностью запрета доступа на определенные сетевые ресурсы;
- 10) управление правами записи на сетевые ресурсы с возможностью запрета записи определенных форматов файлов;
- 11) исключение отдельных процессов из процедуры контроля, аудита теневого копирования;
- 12) автоматическое обнаружение переданных на сетевые ресурсы файлов, содержащих определенную информацию (на основании заданных политик безопасности) с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;

- 4) the ability to configure exceptions from auditing and shadow interception of certain network resources;
- 5) the ability to configure partial shadow copy saving for large files (for example, save only the first 100 MB);
- 6) saving shadow copies of files written to network resources locally on controlled computers before sending them to the server;
- 7) the ability to configure the storage size for shadow copies on users' local computers;
- 8) the ability to shadow copy files transferred to network resources of terminal servers;
- 9) control of access to network resources with the possibility of prohibiting access to certain network resources;
- 10) manage write rights to network resources with the ability to prohibit recording of certain file formats;
- 11) exclusion of individual processes from the shadow copy control and audit procedure;
- 12) automatic detection of files transmitted to network resources containing certain information (based on the specified security policies) with sending a notification to the person responsible for information security in case of detection of such information;
- 13) ability to search by text and attributes of files sent to network resources, including using templates.

1.3.7 Requirements for blocking data transmission:

The system should provide prompt response to cases of violation of the organization's security policies by blocking sensitive data sent via HTTP protocols, as well as printing, in real time. The system should have the following features:



ma'lumotlar aniqlangan bo'lsa, axborot xavfsizligi uchun mas'ul shaxsga xabarnoma yuborish;

13) matn va tarmoq resurslariga yuborilgan fayllarning atributlari, shu jumladan shablonlardan foydalangan holda qidirish imkoniyati.

1.3.7 Ma'lumot uzatishni blokirovka qilishga qo'yiladigan talablar:

Tizim HTTP protokollari orqali yuborilgan maxfiy ma'lumotlarni, shuningdek, bosilgan ma'lumotlarni real vaqt rejimida bloklash orqali tashkilotning xavfsizlik siyosatini buzish holatlariga tezkor javob berishi kerak. Tizim quyidagi imkoniyatlarga ega bo'lishi kerak:

1) HTTP protokoli orqali uzatiladigan ma'lumotlarni kontent tahlili (kontent tahlili) asosida quyidagi tahlil imkoniyatlaridan foydalangan holda bloklash: iboralarni qidirish, loyqa qidiruv, so'zlar orasidagi masofani hisobga olgan holda qidirish, transliteratsiya, morfologiya, hujjatdagi iboraning paydo bo'lish soni, va hokazo. Shu bilan birga, veb-pochta xizmatlari va ijtimoiy tarmoqlarda xabarlar va fayllarni yuborish, Internetda ma'lumot qidirish va boshqa ko'plab operatsiyalarni mazmuni bo'yicha blokirovka qilish imkoniyatini beradi;

2) muntazam iboralar yordamida kontent tahlili (kontent tahlili) asosida HTTP orqali uzatiladigan ma'lumotlarni bloklash

3) atributlarni tahlil qilish (kontekstli tahlil) asosida HTTP protokoli orqali uzatiladigan ma'lumotlarni blokirovka qilish: IP-manzil, port, shifrlangan ulanishdan foydalanish fakti, HTTP usuli, veb-maydon parametrlari, fayl atributlari, sayt toifasi va boshqalar.

4) HTTP protokoli orqali uzatiladigan fayllarni faylning xesh miqdori asosida bloklash, shu bilan birga bir nechta xesh miqdorini qo'lda, oldindan sozlangan xesh summolari bankidan, shuningdek,

13) возможность поиска по тексту и атрибутам отправленных на сетевые ресурсы файлов, в том числе с применением шаблонов.

1.3.7 Требования к блокировке передачи данных:

Система должна обеспечивать оперативное реагирование на случаи нарушения политик безопасности организации, путем блокировки чувствительных данных, отправляемых по протоколам HTTP, а также на печать, в режиме реального времени. Система должна располагать следующими возможностями:

1) блокировка данных, передаваемых по протоколу HTTP, на основании анализа содержимого (контентный анализ) с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология, количество вхождений фразы в документ и др. При этом обеспечивается возможность блокировать по содержимому такие операции как отправка сообщений и файлов в почтовых веб сервисах и социальных сетях, поиск информации в интернете, и многие другие;

2) блокировка данных, передаваемых по протоколу HTTP, на основании анализа содержимого (контентный анализ) с использованием регулярных выражений

3) блокировка данных, передаваемых по протоколу HTTP, на основании анализа атрибутов (контекстный анализ) с использованием таких атрибутов как: IP-адрес, порт, факт использования шифрованного соединения, HTTP-метод, параметры web-поля, атрибуты файла, категория сайта и др.

4) блокировка файлов, передаваемых по протоколу HTTP, на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы;

5) блокировка файлов, передаваемых по протоколу HTTP, на основании хеш-суммы файла, при этом может

1) blocking data transmitted over the HTTP protocol based on content analysis (content analysis) using such analysis capabilities as: phrase search, fuzzy search, search taking into account the distance between words, transliteration, morphology, number of occurrences of a phrase in a document, etc. It also provides the ability to block content-based operations such as sending messages and files in web mail services and social networks, searching for information on the Internet, and many others.

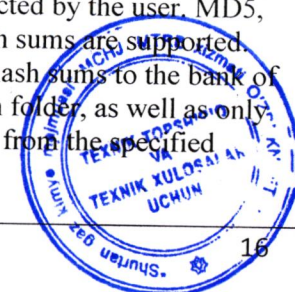
2) blocking data transmitted over the HTTP protocol based on content analysis (content analysis) using regular expressions

3) blocking data transmitted over the HTTP protocol based on attribute analysis (contextual analysis) using such attributes as: IP address, port, fact of using an encrypted connection, HTTP method, web field parameters, file attributes, site category, etc.

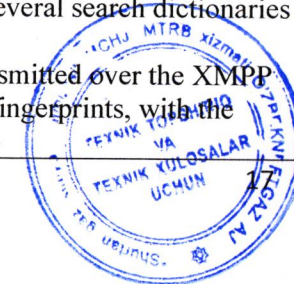
4) blocking of files transmitted over the HTTP protocol based on the hash amount of the file, and several hash amounts can be specified manually, from the pre-configured hashamount bank, or obtained from the file selected by the user. MD5, SHA-256, and SHA-1 hash sums are supported.

5) blocking of files transmitted over the HTTP protocol based on the hash amount of the file, and several hash amounts can be specified manually, from the pre-configured hash amount bank, or obtained from the file selected by the user. MD5, SHA-256, and SHA-1 hash sums are supported.

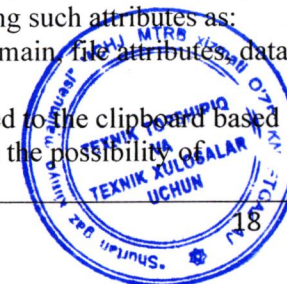
6) the ability to add hash sums to the bank of all files located in a certain folder, as well as only files of a certain extension from the specified folder;



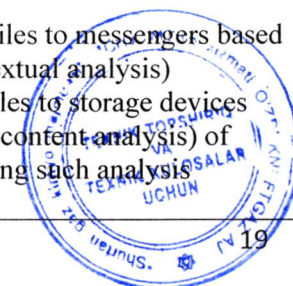
<p>foydalanuvchi tanlagan fayldan olish mumkin. MD5, SHA-256, SHA-1 xeshlari qo'llab-quvvatlanadi;</p> <p>5) HTTP protokoli orqali uzatiladigan fayllarni faylning xesh miqdori asosida bloklash, shu bilan birga bir nechta xesh miqdorini qo'lda, oldindan sozlangan xesh summalari bankidan, shuningdek, foydalanuvchi tanlagan fayldan olish mumkin. MD5, SHA-256, SHA-1 xeshlari qo'llab-quvvatlanadi;</p> <p>6) xesh-bankka ma'lum bir papkada joylashgan barcha fayllarni, shuningdek, faqat ma'lum bir papkadan ma'lum kengaytmali fayllarni qo'shish imkoniyati;</p> <p>7) qidiruv lug'atlari asosida HTTP protokoli orqali uzatiladigan ma'lumotlarni blokirovkalash, bitta blokirovka qoidasida bir nechta qidiruv lug'atlarini belgilash imkoniyati bilan;</p> <p>8) raqamli barmoq izlari asosida HTTP protokoli orqali uzatiladigan ma'lumotlarni blokirovkalash, bitta blokirovka qoidasida bir nechta raqamli barmoq izlarini belgilash imkoniyati bilan;</p> <p>9) sezgirlik yorlig'i tahlili asosida HTTP orqali yuborilgan fayllarni bloklash;</p> <p>10) XMPP protokoli orqali uzatiladigan ma'lumotlarni quyidagi tahlil imkoniyatlaridan foydalangan holda harflar va qo'shimchalar tarkibini tahlil qilish (kontent tahlili) asosida bloklash: iboralarni qidirish, loyqa qidiruv, so'zlar orasidagi masofani hisobga olgan holda qidirish, transliteratsiya, morfologiya va boshqalar;</p> <p>11) muntazam iboralar yordamida kontent tahlili (kontent tahlili) asosida XMPP protokoli orqali uzatiladigan ma'lumotlarni bloklash</p> <p>12) foydalanuvchi, kompyuter, domen, fayl atributlari va boshqalar kabi atributlardan foydalangan holda xat va qo'shimchalarning atributlarini tahlil qilish (kontekstli tahlil) asosida XMPP protokoli orqali uzatiladigan ma'lumotlarni</p>	<p>быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы;</p> <p>6) возможность добавления в банк хеш-сумм всех файлов, расположенных в определенной папке, а также только файлов определенного расширения из указанной папки;</p> <p>7) блокировка данных, передаваемых по протоколу HTTP, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки;</p> <p>8) блокировка данных, передаваемых по протоколу HTTP, на основании цифровых отпечатков, с возможностью указания нескольких цифровых отпечатков в одном правиле блокировки;</p> <p>9) блокировка файлов, отправляемых по протоколу HTTP на основании анализа меток конфиденциальности;</p> <p>10) блокировка данных, передаваемых по протоколу XMPP, на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.;</p> <p>11) блокировка данных, передаваемых по протоколу XMPP, на основании анализа содержимого (контентный анализ) с использованием регулярных выражений</p> <p>12) блокировка данных, передаваемых по протоколу XMPP, на основании анализа атрибутов (контекстный анализ) письма и вложений с использованием таких атрибутов как: пользователь, компьютер, домен, атрибуты файла и др.</p> <p>13) блокировка файлов, передаваемых по протоколу XMPP, на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из преднастроенного банка хеш-сумм, а также получена из</p>	<p>7) blocking data transmitted over the HTTP protocol based on search dictionaries, with the possibility of specifying several search dictionaries in one blocking rule;</p> <p>8) blocking of data transmitted over the HTTP protocol based on digital fingerprints, with the possibility of specifying several digital fingerprints in one blocking rule;</p> <p>9) blocking files sent over the HTTP protocol based on the analysis of privacy tags;</p> <p>10) blocking data transmitted over the XMPP protocol based on content analysis (content analysis) of emails and attachments using such analysis capabilities as phrase search, fuzzy search, word spacing search, transliteration, morphology, etc.;</p> <p>11) blocking data transmitted over the XMPP protocol based on content analysis (content analysis) using regular expressions</p> <p>12) blocking data transmitted over the XMPP protocol based on attribute analysis (contextual analysis) of emails and attachments using such attributes as: user, computer, domain, file attributes, etc.</p> <p>13) blocking files transmitted over the XMPP protocol based on the hash amount of the file, and several hash amounts can be specified manually, from a pre-configured hash amount bank, or obtained from a file selected by the user. MD5, SHA-256, and SHA-1 hash sums are supported.</p> <p>14) blocking data transmitted over the XMPP protocol based on search dictionaries, with the possibility of specifying several search dictionaries in one blocking rule;</p> <p>15) blocking data transmitted over the XMPP protocol based on digital fingerprints, with the</p>
--	--	--



<p>blokirovka qilish.</p> <p>13) XMPP protokoli orqali uzatiladigan fayllarni faylning xesh yig'indisi asosida bloklash, shu bilan birga bir nechta xesh summalarini qo'lda, oldindan tuzilgan xesh summolari bankidan, shuningdek, foydalanuvchi tanlagan fayldan olish mumkin. MD5, SHA-256, SHA-1 xeshlari qo'llab-quvvatlanadi;</p> <p>14) qidiruv lug'atlari asosida XMPP protokoli orqali uzatiladigan ma'lumotlarni blokirovkalash, bitta blokirovka qoidasida bir nechta qidiruv lug'atlarini belgilash imkoniyati bilan;</p> <p>15) raqamli barmoq izlari asosida XMPP protokoli orqali uzatiladigan ma'lumotlarni blokirovkalashning bitta qoidasida bir nechta raqamli barmoq izlarini belgilash imkoniyati bilan bloklash;</p> <p>16) sezgirlik belgilarini tahlil qilish asosida XMPP protokoli orqali uzatiladigan fayllarni bloklash;</p> <p>17) Hujjatning mazmunini tahlil qilish (kontent tahlili) asosida chop etishga yuborilgan hujjatlarni quyidagi tahlil imkoniyatlaridan foydalangan holda bloklash: iboralarni qidirish, loyqa qidiruv, so'zlar orasidagi masofani hisobga olgan holda qidirish, transliteratsiya, morfologiya va boshqalar;</p> <p>18) muntazam iboralar yordamida kontent tahlili (kontent tahlili) asosida chop etish uchun yuborilgan hujjatlarni bloklash</p> <p>19) Quyidagi kabi atributlardan foydalangan holda chop etish atributlarini tahlil qilish (kontekstli tahlil) asosida chop etishga yuborilgan hujjatlarni bloklash: kompyuter, domen, foydalanuvchi, vaqt, haftaning kuni;</p> <p>20) qidiruv lug'atlari asosida chop etish uchun yuborilgan hujjatlarni blokirovka qilish, bitta blokirovka qoidasida bir nechta qidiruv lug'atlarini ko'rsatish imkoniyati bilan;</p> <p>21) Quyidagi kabi tahlil imkoniyatlaridan</p>	<p>выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы;</p> <p>14) блокировка данных, передаваемых по протоколу XMPP, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки;</p> <p>15) блокировка данных, передаваемых по протоколу XMPP, на основании цифровых отпечатков, с возможностью указания нескольких цифровых отпечатков в одном правиле блокировки;</p> <p>16) блокировка файлов, передаваемых по протоколу XMPP, на основании анализа меток конфиденциальности;</p> <p>17) блокировка документов, отправляемых на печать, на основании анализа содержимого (контентный анализ) документа с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.;</p> <p>18) блокировка документов, отправляемых на печать, на основании анализа содержимого (контентный анализ) с использованием регулярных выражений</p> <p>19) блокировка документов, отправляемых на печать, на основании анализа атрибутов (контекстный анализ) печати с использованием таких атрибутов как: компьютер, домен, пользователь, время, день недели;</p> <p>20) блокировка документов, отправляемых на печать, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки;</p> <p>21) блокировка данных, копируемых в буфер обмена, на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.;</p>	<p>possibility of specifying several digital fingerprints in one blocking rule;</p> <p>16) blocking files transmitted over the XMPP protocol based on the analysis of privacy tags;</p> <p>17) blocking documents sent for printing based on content analysis (content analysis) of the document using such analysis capabilities as: phrase search, fuzzy search, search taking into account the distance between words, transliteration, morphology, etc.;</p> <p>18) blocking documents sent for printing based on content analysis (content analysis) using regular expressions</p> <p>19) blocking documents sent for printing based on analysis of print attributes (contextual analysis) using such attributes as: computer, domain, user, time, day of the week;</p> <p>20) blocking documents sent for printing based on search dictionaries, with the possibility of specifying several search dictionaries in one blocking rule;</p> <p>21) blocking data copied to the clipboard based on content analysis (content analysis) of emails and attachments using such analysis capabilities as phrase search, fuzzy search, word spacing search, transliteration, morphology, etc.;</p> <p>22) blocking data copied to the clipboard based on content analysis (content analysis) using regular expressions</p> <p>23) blocking data copied to the clipboard based on the analysis of attributes (contextual analysis) of emails and attachments using such attributes as: user, computer, process, domain, file attributes, data type (text, image, file), etc.</p> <p>24) blocking data copied to the clipboard based on search dictionaries, with the possibility of</p>
---	---	--



<p>foydalangan holda xat va qo'shimchalarning mazmunini tahlil qilish (kontent tahlili) asosida buferga ko'chirilgan ma'lumotlarni bloklash: iboralarni qidirish, loyqa qidiruv, so'zlar orasidagi masofani hisobga olgan holda qidirish, transliteratsiya, morfologiya va boshqalar;</p> <p>22) muntazam iboralar yordamida kontent tahlili (kontent tahlili) asosida clipboardga ko'chirilgan ma'lumotlarni bloklash</p> <p>23) foydalanuvchi, kompyuter, jarayon, domen, fayl atributlari, ma'lumotlar turi (matn, rasm, fayl) va boshqalar kabi atributlardan foydalangan holda harflar va qo'shimchalarning atributlarini tahlil qilish (kontekstli tahlil) asosida buferga ko'chirilgan ma'lumotlarni blokirovka qilish.</p> <p>24) qidiruv lug'atlari asosida buferga ko'chirilgan ma'lumotlarni blokirovka qilish, bitta blokirovka qilish qoidasida bir nechta qidiruv lug'atlarini belgilash imkoniyati bilan;</p> <p>25) Quyidagi kabi tahlil imkoniyatlaridan foydalangan holda xat va qo'shimchalarning mazmunini tahlil qilish (kontent tahlili) asosida buferdan yopishtirilgan ma'lumotlarni bloklash: iboralarni qidirish, loyqa qidiruv, so'zlar orasidagi masofani hisobga olgan holda qidirish, transliteratsiya, morfologiya va boshqalar;</p> <p>26) Muntazam iboralar yordamida kontent tahlili (kontent tahlili) asosida clipboarddan yopishtirilgan ma'lumotlarni bloklash</p> <p>27) foydalanuvchi, kompyuter, jarayon, domen, fayl atributlari, ma'lumotlar turi (matn, rasm, fayl) va boshqalar kabi atributlardan foydalangan holda harflar va qo'shimchalarning atributlarini tahlil qilish (kontekstual tahlil) asosida buferdan yopishtirilgan ma'lumotlarni bloklash.</p> <p>28) qidiruv lug'atlari asosida buferdan joylashtirilgan ma'lumotlarni bloklash, bitta</p>	<p>22) блокировка данных, копируемых в буфер обмена, на основании анализа содержимого (контентный анализ) с использованием регулярных выражений</p> <p>23) блокировка данных, копируемых в буфер обмена, на основании анализа атрибутов (контекстный анализ) письма и вложений с использованием таких атрибутов как: пользователь, компьютер, процесс, домен, атрибуты файла, тип данных (текст, изображение, файл) и др.</p> <p>24) блокировка данных, копируемых в буфер обмена, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки;</p> <p>25) блокировка данных, вставляемых из буфера обмена, на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.;</p> <p>26) блокировка данных, вставляемых из буфера обмена, на основании анализа содержимого (контентный анализ) с использованием регулярных выражений</p> <p>27) блокировка данных, вставляемых из буфера обмена, на основании анализа атрибутов (контекстный анализ) письма и вложений с использованием таких атрибутов как: пользователь, компьютер, процесс, домен, атрибуты файла, тип данных (текст, изображение, файл) и др.</p> <p>28) блокировка данных, вставляемых из буфера обмена, на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки;</p> <p>29) блокировка запуска процессов на основании анализа атрибутов (контекстный анализ) процесса с использованием таких атрибутов как: компьютер, домен, категория приложения, хеш-сумма и др.</p> <p>30) блокировка отправки файлов в мессенджеры на основании анализа содержимого (контентный анализ) с</p>	<p>specifying several search dictionaries in one blocking rule;</p> <p>25) blocking data inserted from the clipboard based on content analysis (content analysis) of emails and attachments using such analysis capabilities as phrase search, fuzzy search, word spacing search, transliteration, morphology, etc.;</p> <p>26) blocking data pasted from the clipboard based on content analysis (content analysis) using regular expressions</p> <p>27) blocking data inserted from the clipboard based on the analysis of attributes (contextual analysis) of emails and attachments using such attributes as: user, computer, process, domain, file attributes, data type (text, image, file), etc.</p> <p>28) blocking data inserted from the clipboard based on search dictionaries, with the possibility of specifying several search dictionaries in one blocking rule;</p> <p>29) blocking the launch of processes based on the analysis of attributes (contextual analysis) of the process using such attributes as: computer, domain, application category, hash sum, etc.</p> <p>30) blocking sending files to messengers based on content analysis (content analysis) using such analysis capabilities as: phrase search, fuzzy search, word spacing search, transliteration, morphology, etc.;</p> <p>31) blocking sending files to messengers based on content analysis (content analysis) using regular expressions</p> <p>32) blocking sending files to messengers based on attribute analysis (contextual analysis)</p> <p>33) blocking writing files to storage devices based on content analysis (content analysis) of emails and attachments using such analysis</p>
---	---	---

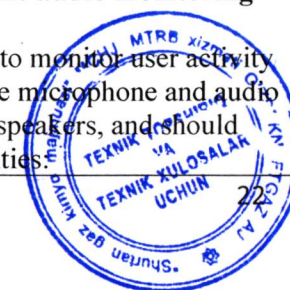


<p>blokirovka qilish qoidasida bir nechta qidiruv lug'atlarini belgilash imkoniyati;</p> <p>29) kompyuter, domen, ilovalar toifasi, xesh summasi va boshqalar kabi atributlardan foydalangan holda jarayonning atributlarini tahlil qilish (kontekstli tahlil) asosida jarayonlarni ishga tushirishni blokirovka qilish.</p> <p>30) Quyidagi kabi tahlil imkoniyatlaridan foydalangan holda kontent tahlili (kontent tahlili) asosida tezkor xabarchilarga fayllarni yuborishni bloklash: iboralarni qidirish, loyqa qidiruv, so'zlar orasidagi masofani hisobga olgan holda qidirish, transliteratsiya, morfologiya va boshqalar;</p> <p>31) muntazam iboralar yordamida kontentni tahlil qilish (kontent tahlili) asosida tezkor xabarchilarga fayllarni yuborishni bloklash</p> <p>32) atributlarni tahlil qilish (kontekstli tahlil) asosida tezkor messenjerlarga fayllarni yuborishni bloklash</p> <p>33) Quyidagi kabi tahlil imkoniyatlaridan foydalangan holda harflar va qo'shimchalarning mazmunini tahlil qilish (kontent tahlili) asosida saqlash qurilmalariga fayllarni yozishni bloklash: iboralarni qidirish, loyqa qidirish, so'zlar orasidagi masofani hisobga olgan holda qidirish, transliteratsiya, morfologiya va boshqalar;</p> <p>34) muntazam iboralar yordamida kontentni tahlil qilish (kontent tahlili) asosida fayllarni saqlash qurilmalariga yozishni bloklash</p> <p>35) foydalanuvchi, kompyuter, jarayon, domen va boshqa fayl atributlari kabi atributlar yordamida atributlarni tahlil qilish (kontekstli tahlil) asosida drayvlarga fayllarni yozishni bloklash</p> <p>36) fayllarni ma'lum drayverlarga yozishni bloklash (seriya raqami, ishlab chiqaruvchi, qurilma nomi, ishlab chiqaruvchi identifikatori va mahsulot identifikatori bo'yicha)</p>	<p>использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.;</p> <p>31) блокировка отправки файлов в мессенджеры на основании анализа содержимого (контентный анализ) с использованием регулярных выражений</p> <p>32) блокировка отправки файлов в мессенджеры на основании анализа атрибутов (контекстный анализ)</p> <p>33) блокировка записи файлов на накопители на основании анализа содержимого (контентный анализ) письма и вложений с использованием таких возможностей анализа как: фразовый поиск, нечеткий поиск, поиск с учетом расстояния между словами, транслитерация, морфология и др.;</p> <p>34) блокировка записи файлов на накопители на основании анализа содержимого (контентный анализ) с использованием регулярных выражений</p> <p>35) блокировка записи файлов на накопители на основании анализа атрибутов (контекстный анализ) с использованием таких атрибутов как: пользователь, компьютер, процесс, домен, и др. атрибуты файла</p> <p>36) блокировка записи файлов на определенные накопители (по серийному номеру, производителю, названию устройства, идентификатору производителя и идентификатору продукта)</p> <p>37) блокировка записи файлов на накопители на основании хеш-суммы файла, при этом может быть указано несколько хеш-сумм вручную, из предустановленного банка хеш-сумм, а также получена из выбранного пользователем файла. Поддерживаются MD5, SHA-256, SHA-1 хеш-суммы;</p> <p>38) блокировка записи файлов на накопители на основании поисковых словарей, с возможностью указания нескольких поисковых словарей в одном правиле блокировки;</p>	<p>capabilities as phrase search, fuzzy search, word spacing search, transliteration, morphology, etc.;</p> <p>34) blocking writing files to storage devices based on content analysis (content analysis) using regular expressions</p> <p>35) blocking writing files to storage devices based on attribute analysis (contextual analysis) using attributes such as: user, computer, process, domain, and other file attributes</p> <p>36) block writing files to specific storage devices (by serial number, manufacturer, device name, manufacturer ID, and product ID)</p> <p>37) blocking writing files to storage devices based on the hash amount of the file, and several hash amounts can be specified manually, from a pre-configured hash amount bank, or obtained from a user-selected file. MD5, SHA-256, and SHA-1 hash sums are supported.</p> <p>38) blocking writing files to storage devices based on search dictionaries, with the possibility of specifying several search dictionaries in one blocking rule;</p> <p>39) blocking the recording of files to storage devices based on digital fingerprints, with the possibility of specifying several digital fingerprints in one blocking rule;</p> <p>40) blocking the recording of files to storage devices based on the analysis of privacy labels;</p> <p>41) the ability to notify the end user when blocking, with a custom notification text;</p> <p>42) the ability to notify the security officer about the triggered blocking rule;</p> <p>43) ability to search by attributes of blocked information.</p> <p>1.3.8 Requirements for the screenshot function:</p>
---	---	--



<p>37) faylning xesh yig'indisi asosida drayvlarga fayllarni yozishni blokirovka qilish, shu bilan birga bir nechta xesh summalarini qo'lda, oldindan tuzilgan xesh summolari bankidan, shuningdek, foydalanuvchi tanlagan fayldan olish mumkin. MD5, SHA-256, SHA-1 xeshlari qo'llab-quvvatlanadi;</p> <p>38) qidiruv lug'atlari asosida fayllarni saqlash qurilmalariga yozishni blokirovka qilish, bitta blokirovkalash qoidasida bir nechta qidiruv lug'atlarini ko'rsatish imkoniyati bilan;</p> <p>39) raqamli barmoq izlari asosida fayllarni saqlash qurilmalariga yozishni blokirovkalash, bitta blokirovkalash qoidasida bir nechta raqamli barmoq izlarini belgilash imkoniyati bilan;</p> <p>40) maxfiylik belgilarini tahlil qilish asosida fayllarni saqlash qurilmalariga yozishni bloklash;</p> <p>41) maxsus bildirishnoma matni bilan bloklanganda oxirgi foydalanuvchini xabardor qilish imkoniyati;</p> <p>42) qo'zg'atilgan blokirovka qoidasi haqida xavfsizlik xodimini xabardor qilish imkoniyati;</p> <p>43) bloklangan ma'lumotlarning atributlari bo'yicha qidirish imkoniyati.</p> <p>1.3.8 Skrinshot funksiyasiga qo'yiladigan talablar:</p> <p>Tizim sizga skrinshotlar olish orqali foydalanuvchining ish stoli faoliyatini kuzatish imkonini berishi va quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) ma'lum bir oraliqda bir soniyagacha aniqlik bilan skrinshot olish qobiliyati;</p> <p>2) faol oynani o'zgartirganda ekran tasvirlarini olish imkoniyati;</p> <p>3) brauzer yorliqlarini o'zgartirganda ekran tasvirlarini olish imkoniyati;</p> <p>4) jarayon boshlanganda ekran tasvirlarini olish imkoniyati;</p>	<p>39) блокировка записи файлов на накопители на основании цифровых отпечатков, с возможностью указания нескольких цифровых отпечатков в одном правиле блокировки;</p> <p>40) блокировка записи файлов на накопители на основании анализа меток конфиденциальности;</p> <p>41) возможность уведомления конечного пользователя при блокировке, с настраиваемым текстом уведомления;</p> <p>42) возможность уведомления офицера безопасности о сработавшем правиле блокировки;</p> <p>43) возможность поиска по атрибутам заблокированной информации.</p> <p>1.3.8 Требования к функции снимков экрана:</p> <p>Система должна позволять контролировать активность рабочего стола пользователя при помощи снятия снимков экрана, и располагать следующими возможностями:</p> <p>1) возможность снятия скриншотов с заданным интервалом с точностью до секунды;</p> <p>2) возможность снятия скриншотов при смене активного окна;</p> <p>3) возможность снятия скриншотов при смене вкладки браузера;</p> <p>4) возможность снятия скриншотов при запуске процесса;</p> <p>5) возможность снятия скриншотов при срабатывании правила блокировки;</p> <p>6) возможность снятия скриншотов при нажатии клавиши Print Screen;</p> <p>7) возможность отключения снятия скриншотов при простое рабочей станции.</p> <p>8) возможность настройки качества скриншотов, в том числе сохранения в черно-белом формате;</p> <p>9) возможность настройки размера скриншотов (в процентах от оригинала);</p> <p>10) возможность настройки формата скриншотов (JPEG, PNG);</p>	<p>The system should allow you to monitor the user's desktop activity by taking screenshots, and have the following features:</p> <p>1) the ability to take screenshots at a given interval with an accuracy of up to a second;</p> <p>2) the ability to take screenshots when changing the active window;</p> <p>3) the ability to take screenshots when changing the browser tab;</p> <p>4) the ability to take screenshots when starting the process;</p> <p>5) the ability to take screenshots when the blocking rule is triggered.</p> <p>6) the ability to take screenshots by pressing the Print Screen key;</p> <p>7) ability to disable taking screenshots when the workstation is idle.</p> <p>8) the ability to adjust the quality of screenshots, including saving in black and white format;</p> <p>9) the ability to adjust the size of screenshots (as a percentage of the original);</p> <p>10) ability to customize the format of screenshots (JPEG, PNG);</p> <p>11) save a special mark if it is impossible to take a screenshot (the user's session is disabled, blocked, etc.);</p> <p>12) saving information about the active process at the time of taking the screenshot;</p> <p>13) saving information about the active browser tab at the time of taking the screenshot;</p> <p>14) the ability to disable taking screenshots when visiting specified sites in the browser;</p> <p>15) the ability to take screenshots only for the specified active processes;</p> <p>16) the ability to export screenshots to an external HTML file with support for interactivity of</p>
---	--	---

<p>5) blokirovka qoidasi ishga tushirilganda skrinshot olish imkoniyati;</p> <p>6) Chop etish tugmachasini bosganingizda ekran tasvirlarini olish qobiliyati Ekran ;</p> <p>7) ish stantsiyasi ishlamay qolganda skrinshot olishni o'chirish imkoniyati.</p> <p>8) skrinshotlar sifatini sozlash, shu jumladan qora va oq formatda saqlash imkoniyati;</p> <p>9) skrinshotlar hajmini sozlash qobiliyati (asl nusxadan foiz sifatida);</p> <p>10) skrinshot formatini sozlash qobiliyati (JPEG, PNG);</p> <p>11) skrinshotni olishning iloji bo'lmasa, maxsus belgini saqlash (foydalanuvchi seansi o'chirilgan, bloklangan va hk);</p> <p>12) skrinshotni olish vaqtida faol jarayon haqidagi ma'lumotlarni saqlash;</p> <p>13) skrinshot olingan vaqtda faol brauzer yorlig'i haqidagi ma'lumotlarni saqlash;</p> <p>14) brauzerda ko'rsatilgan saytlarga tashrif buyurganingizda skrinshotlarni olishni o'chirish imkoniyati;</p> <p>15) faqat belgilangan faol jarayonlar uchun skrinshot olish imkoniyati;</p> <p>16) strukturaviy elementlarning interaktivligini qo'llab-quvvatlash va veb-brauzer orqali ushlangan ma'lumotlarni ko'rish imkoniyati bilan skrinshotlarni tashqi HTML fayliga eksport qilish imkoniyati;</p> <p>17) individual foydalanuvchining skrinshotlarini bir kun davomida (yoki tanlangan vaqt oralig'ida) grafik fayllar to'plami sifatida yoki bitta PDF yoki video faylga birlashtirilgan holda saqlash imkoniyati.</p> <p>18) kompyuter foydalanuvchisi tomonidan skrinshotlar olishni bloklash (PrintScreen tugmachasini bosish orqali ham , uchinchi tomon vositalaridan foydalanganda ham)</p>	<p>11) сохранение специальной отметки в случае невозможности снятия скриншота (сессия пользователя отключена, заблокирована и т.п.);</p> <p>12) сохранение информации об активном процессе в момент снятия скриншота;</p> <p>13) сохранение информации об активной вкладке браузера в момент снятия скриншота;</p> <p>14) возможность отключения снятия скриншотов при посещении заданных сайтов в браузере;</p> <p>15) возможность снятия скриншотов только для заданных активных процессов;</p> <p>16) возможность экспорта скриншотов во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступом к просмотру перехваченных данных через веб-браузер;</p> <p>17) возможность сохранения скриншотов отдельного пользователя за день (или за выбранный временной интервал) в виде набора графических файлов, либо объединенных в один PDF- или видеофайл.</p> <p>18) блокировка снятия скриншотов пользователем ПК (как по нажатию клавиши PrintScreen, так и при использовании сторонних средств)</p> <p>1.3.9 Требования к функции видеомониторинга:</p> <p>Система должна позволять контролировать активность пользователя при помощи снятия видео рабочего стола, а также видео с веб-камеры, и располагать следующими возможностями:</p> <p>1) подключение к монитору компьютера пользователя и просмотр видео рабочего стола в режиме реального времени;</p> <p>2) мониторинг рабочих столов нескольких пользователей одновременно;</p> <p>3) возможность вывода окна просмотра на отдельный экран;</p> <p>4) автоматическая запись видеоизображения рабочего стола и видео с подключенной веб-камеры по расписанию;</p>	<p>structural elements and access to viewing intercepted data via a web browser;</p> <p>17) the ability to save screenshots of an individual user for a day (or for a selected time interval) as a set of graphic files, or combined into a single PDF or video file.</p> <p>18) blocking of taking screenshots by the PC user (both by pressing the PrintScreen key and by using third-party tools)</p> <p>1.3.9 Requirements for the video monitoring function:</p> <p>The system should allow you to monitor user activity by taking desktop videos, as well as webcam videos, and have the following features:</p> <p>1) connecting to the user's computer monitor and viewing desktop video in real time;</p> <p>2) monitoring the desktops of several users simultaneously;</p> <p>3) the ability to display the viewport on a separate screen;</p> <p>4) automatic recording of desktop video and video from the connected webcam on a scheduled basis;</p> <p>5) record desktop video manually;</p> <p>6) ability to adjust the recording quality;</p> <p>7) the ability to record both video in color and in black and white format;</p> <p>8) ability to save records of several users simultaneously;</p> <p>9) the ability to play the recording file using the system and in any of the media players.</p> <p>1.3.10 Requirements for the audio monitoring function:</p> <p>The system should be able to monitor user activity by recording audio from the microphone and audio coming to the workstation speakers, and should have the following capabilities:</p>
---	---	--



1.3.9 Video monitoring funksiyasiga qo'yiladigan talablar:

Tizim ish stoli videosini, shuningdek veb-kameradan videoni yozib olish orqali foydalanuvchi faoliyatini kuzatish imkonini berishi va quyidagi imkoniyatlarga ega bo'lishi kerak:

- 1) foydalanuvchining kompyuter monitoriga ulanish va ish stoli videosini real vaqtda ko'rish;
- 2) bir vaqtning o'zida bir nechta foydalanuvchilarning ish stollarini kuzatish;
- 3) ko'rish oynasini alohida ekranda ko'rsatish imkoniyati;
- 4) jadvalga muvofiq ulangan veb-kameradan ish stoli video va videoni avtomatik yozib olish;
- 5) ish stoli videosini qo'lda yozib oling;
- 6) yozish sifatini sozlash qobiliyati;
- 7) rangli yoki oq-qora formatda video yozish imkoniyati;
- 8) bir vaqtning o'zida bir nechta foydalanuvchilarning yozuvlarini saqlash imkoniyati;
- 9) tizim yordamida va istalgan media pleerda yozib olish faylini o'ynash imkoniyati.

1.3.10 Ovozni kuzatish funksiyasiga qo'yiladigan talablar :

Tizim mikrofondan ovoz yozish va ish stansiyasi karnaylariga audio chiqish orqali foydalanuvchi faoliyatini kuzatishi va quyidagi imkoniyatlarga ega bo'lishi kerak:

- 1) real vaqtda audio oqimni tinglash imkoniyati bilan boshqariladigan ish stantsiyalarining mikrofonlariga ulanish;
- 2) bir vaqtning o'zida bir nechta foydalanuvchilarning mikrofonlarini tinglash;
- 3) mikrofondan keladigan audio oqimni va kompyuterning tizim tovushlarini jadvalga muvofiq avtomatik yozib olish;
- 4) qo'lda yozib olish;

- 5) запись видео рабочего стола вручную;
- 6) возможность настройки качества записи;
- 7) возможность как записи видео в цветном, так и в черно-белом формате;
- 8) возможность сохранения записей нескольких пользователей одновременно;
- 9) возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.

1.3.10 Требования к функции аудиомониторинга:

Система должна позволять контролировать активность пользователя при помощи записи аудио с микрофона и аудио, поступающего на динамики рабочей станции, и располагать следующими возможностями:

- 1) подключение к микрофонам контролируемых рабочих станций с возможностью прослушивания аудиопотока в режиме реального времени;
- 2) прослушивание микрофонов нескольких пользователей одновременно;
- 3) автоматическая запись поступающего с микрофона аудиопотока и системных звуков компьютера по расписанию;
- 4) запись вручную;
- 5) возможность сохранения записей нескольких пользователей одновременно;
- 6) возможность воспроизведения файла записи средствами системы и в любом из медиапроигрывателей.
- 7) отображение звуковой дорожки в записанном видео-, аудиоряде

1.3.11 Требования к мониторингу пользовательской активности:

Система должна позволять контролировать активность пользователя на рабочем месте и располагать следующими возможностями:

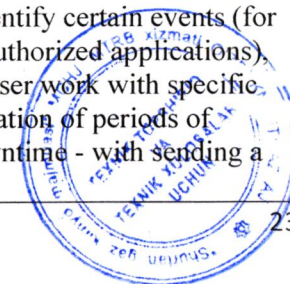
- 1) ведение статистики по активному времени работы и простоя (отсутствия действий пользователя) с возможностью настройки периода отсутствия активности до начала простоя;

- 1) connection to microphones of controlled workstations with the ability to listen to the audio stream in real time;
- 2) listening to microphones of several users at the same time;
- 3) automatic recording of the audio stream coming from the microphone and system sounds of the computer according to a schedule;
- 4) manual recording;
- 5) ability to save records of several users simultaneously;
- 6) the ability to play the recording file using the system and in any of the media players.
- 7) display the audio track in the recorded video or audio sequence

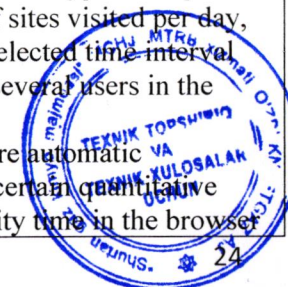
1.3.11 Requirements for monitoring user activity:

The system should allow monitoring user activity at the workplace and have the following capabilities:

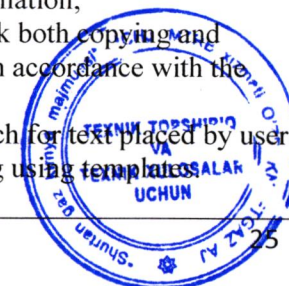
- 1) maintaining statistics on active working hours and downtime (absence of user actions) with the ability to configure the period of inactivity before the start of downtime;
- 2) maintaining statistics on the user's working time in applications with the representation of the collected information, while taking into account not all the application's working time, but the user's working time in the active window.
- 3) excluding individual processes from monitoring;
- 4) the ability to automatically analyze the collected statistics to identify certain events (for example, launching unauthorized applications), control the duration of user work with specific applications and the duration of periods of computer operation/downtime - with sending a



<p>5) bir vaqtning o'zida bir nechta foydalanuvchilarning yozuvlarini saqlash imkoniyati;</p> <p>6) tizim yordamida va istalgan media pleerda yozib olish faylini o'ynash imkoniyati.</p> <p>7) audio trekni yozib olingan video va audio ketma-ketlikda ko'rsatish</p> <p>1.3.11 Foydalanuvchi faoliyatini monitoring qilish uchun talablar:</p> <p>Tizim foydalanuvchining ish joyidagi faoliyatini kuzatish imkonini berishi va quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) faol ish vaqti va ishlamay qolish vaqti (foydalanuvchi harakatlarining yo'qligi) bo'yicha statistik ma'lumotlarni to'xtatilishdan oldin harakatsizlik davrini sozlash imkoniyati bilan yuritish;</p> <p>2) to'plangan ma'lumotlarni taqdim etgan holda ilovalarda foydalanuvchining ish vaqti statistikasini yuritish, bunda ilovaning barcha ish vaqtini emas, balki foydalanuvchining faol oynadagi ish vaqtini hisobga olish;</p> <p>3) alohida jarayonlarni monitoringdan chiqarib tashlash;</p> <p>4) ma'lum hodisalarni aniqlash (masalan, ruxsatsiz ilovalarni ishga tushirish) uchun to'plangan statistik ma'lumotlarni avtomatik ravishda tahlil qilish qobiliyati, foydalanuvchining muayyan ilovalar bilan ishlash muddatini va kompyuterning ishlash muddati / ishlamay qolish muddatini nazorat qilish - mas'ul shaxsga tegishli bildirishnoma yuborish bilan. shaxs;</p> <p>5) individual ilovalarni ishga tushirishni bloklash imkoniyati;</p> <p>6) individual foydalanuvchi yoki bir nechta foydalanuvchilar uchun tanlangan vaqt oralig'ida faoliyat (foydalanuvchining shaxsiy kompyuterdagi faoliyati, dastur faoliyati, voqealar xronologiyasi) bo'yicha alohida hisobotlarni saqlash imkoniyati.</p>	<p>2) ведение статистики по времени работы пользователя в приложениях с представлением собранной информации, при этом учитывается при этом учитывается не все время работы приложения, а время работы пользователя в активном окне;</p> <p>3) исключение отдельных процессов из мониторинга;</p> <p>4) возможность автоматического анализа собранной статистики для выявления определенных событий (например, запуск несанкционированных приложений), контроля длительности работы пользователей с конкретными приложениями и длительности периодов работы/проста компьютера – с отправкой соответствующего уведомления ответственному лицу;</p> <p>5) возможность блокировки запуска отдельных приложений;</p> <p>6) возможность сохранения отдельных отчетов по активности (активность пользователя за ПК, активность приложений, хронология событий) за выбранный временной интервал для отдельного пользователя или нескольких пользователей.</p> <p>7) автоматическая категоризация времени, проведенного в различных приложениях, на продуктивное, непродуктивное и нейтральное</p> <p>1.3.12 Требования к мониторингу браузер активности:</p> <p>Мониторинг браузер активности должен позволять вести комплексную статистику по активности контролируемых пользователей в следующих браузерах: Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Tor, Yandex браузер, Rambler, Amigo, Chromium, Microsoft Edge и располагать следующими возможностями:</p> <p>1) контроль времени посещения веб-сайтов с помощью браузера, при этом учитывается только время работы на активной вкладке, фиксируются переходы между страницами веб-сайтов и ведется комплексная статистика времени, проведенного на различных веб-ресурсах;</p>	<p>corresponding notification to the responsible person;</p> <p>5) the ability to block the launch of individual applications;</p> <p>6) the ability to save individual activity reports (user activity on the PC, application activity, event history) for the selected time interval for an individual user or several users.</p> <p>7) automatic categorization of time spent in various apps into productive, unproductive, and neutral</p> <p>1.3.12 Requirements for monitoring Internet activity:</p> <p>Browser activity monitoring should allow you to keep comprehensive statistics on the activity of monitored users in the following browsers: Internet Explorer, Google Chrome, Mozilla Firefox, Opera, Tor, Yandex Browser, Rambler, Amigo, Chromium, Microsoft Edge and have the following features:</p> <p>1) monitoring the time of visiting websites using a browser, taking into account only the working time on the active tab, recording transitions between pages of websites and maintaining comprehensive statistics of time spent on various web resources;</p> <p>2) the ability to configure the exclusion of individual sites from the browser activity monitoring process;</p> <p>3) the ability to save various types of reports on browser activity (rating of sites visited per day, chronology of events) for a selected time interval for an individual user or for several users in the form of a PDF file.</p> <p>4) the ability to configure automatic notifications about reaching certain quantitative indicators for the user's activity time in the browser</p>
--	---	---



<p>7) turli ilovalarda sarflangan vaqtni avtomatik ravishda samarali, samarasiz va neytralga ajratish</p> <p>1.3.12 Brauzer faoliyatini monitoring qilish uchun talablar:</p> <p>Brauzer faoliyati monitoringi quyidagi brauzerlarda kuzatilayotgan foydalanuvchilarning faoliyati to'g'risida to'liq statistik ma'lumotlarni olish imkonini berishi kerak: Internet Explorer , Google Chrome , Mozilla Firefox , Opera , Tor , Yandex brauzeri, Rambler , Amigo , Chromium , Microsoft Edge va quyidagi imkoniyatlarga ega:</p> <p>1) brauzer yordamida veb-saytlarga tashrif buyurish vaqtini kuzatish, faqat faol yorliqda o'tkaziladigan vaqtni hisobga olgan holda, veb-sayt sahifalari orasidagi o'tishlarni qayd etish va turli veb-resurslarga sarflangan vaqtning to'liq statistikasini yuritish;</p> <p>2) brauzer faoliyatini monitoring qilish jarayonidan alohida saytlarni istisno qilishni sozlash imkoniyati;</p> <p>3) individual foydalanuvchi yoki bir nechta foydalanuvchilar uchun PDF-fayl ko'rinishida tanlangan vaqt oralig'ida brauzer faoliyati to'g'risidagi har xil turdagi hisobotlarni (kuniga tashrif buyurilgan saytlar reytingi, voqealar xronologiyasi) saqlash imkoniyati.</p> <p>4) foydalanuvchining brauzerdagi faollik vaqtiga qarab ma'lum miqdoriy ko'rsatkichlarga erishilganda avtomatik bildirishnomalarni sozlash imkoniyati (masalan, "Foydalanuvchining brauzer orqali ma'lum bir saytda o'tkazgan vaqti kuniga 1 soatdan oshdi" va boshqalar);</p> <p>5) turli saytlarda sarflangan vaqtni samarali, samarasiz va neytralga avtomatik toifalash</p>	<p>2) возможность настройки исключения отдельных сайтов из процесса мониторинга браузер активности;</p> <p>3) возможность сохранения различных типов отчетов о браузер-активности (рейтинг посещенных сайтов за день, хронология событий) за выбранный временной интервал для отдельного пользователя или для нескольких пользователей в виде PDF-файла.</p> <p>4) возможность настройки автоматических уведомлений о достижении определенных количественных показателей по времени активности пользователя в браузере (например, «Время пребывания пользователя на определенном сайте через браузер превысило 1 час за день» и т.д.);</p> <p>5) автоматическая категоризация времени, проведенного на различных сайтах, на продуктивное, непродуктивное и нейтральное</p> <p>1.3.13 Требования к контролю буфера обмена:</p> <p>Система должна позволять контролировать использование пользователями буфера обмена, и располагать следующими возможностями:</p> <p>1) теневое копирование помещаемой в буфер обмена текстовой информации с фиксацией приложения, из которого данная информация была помещена в буфер обмена, и времени события;</p> <p>2) аудит файлов, помещаемых в буфер обмена;</p> <p>3) теневое копирование графического содержимого помещаемого в буфер обмена;</p> <p>4) теневое копирование файлов, помещаемых в буфер обмена;</p> <p>5) возможность ограничения максимального объема данных, перехватываемых из буфера обмена;</p> <p>6) возможность исключения отдельных процессов из мониторинга буфера обмена либо мониторинг только определенных процессов;</p> <p>7) возможность исключения отдельных файлов из мониторинга буфера обмена либо мониторинг только определенных файлов;</p>	<p>(for example, "The user's time spent on a certain site through the browser exceeded 1 hour per day" , etc.);</p> <p>5) automatic categorization of time spent on various sites into productive, unproductive and neutral</p> <p>1.3.13 Clipboard control requirements:</p> <p>The system should allow you to control the use of the clipboard by users, and have the following features:</p> <p>1) shadow copying of text information placed in the clipboard with fixing the application from which this information was placed in the clipboard, and the time of the event;</p> <p>2) audit of files placed on the clipboard;</p> <p>3) shadow copying of graphic content placed on the clipboard;</p> <p>4) shadow copying of files placed on the clipboard;</p> <p>5) the ability to limit the maximum amount of data intercepted from the clipboard;</p> <p>6) the ability to exclude individual processes from clipboard monitoring or monitor only certain processes;</p> <p>7) the ability to exclude individual files from clipboard monitoring or monitor only certain files;</p> <p>8) automatic detection of certain information (based on the specified security policies) placed in the clipboard, with sending a notification to the person responsible for information security in case of detection of such information;</p> <p>9) the ability to block both copying and pasting files by content, in accordance with the configured security rules.</p> <p>10) the ability to search for text placed by users in the clipboard, including using templates</p>
--	---	---



1.3.13 Buferni boshqarishga qo'yiladigan talablar:

Tizim sizga foydalanuvchilarning clipboarddan qanday foydalanishini nazorat qilish imkonini berishi va quyidagi imkoniyatlarga ega bo'lishi kerak:

- 1) buferga joylashtirilgan matnli ma'lumotlarning soyali nusxasi, bu ma'lumot almashish buferiga joylashtirilgan dastur va voqea sodir bo'lgan vaqtni yozib olish;
- 2) buferga joylashtirilgan fayllar auditi;
- 3) buferga joylashtirilgan grafik tarkibni soyali nusxalash;
- 4) buferga joylashtirilgan fayllarni soyali nusxalash;
- 5) clipboarddan ushlab olingan ma'lumotlarning maksimal miqdorini cheklash imkoniyati;
- 6) alohida jarayonlarni clipboard monitoringidan chiqarib tashlash yoki faqat ma'lum jarayonlarni kuzatish imkoniyati;
- 7) alohida fayllarni clipboard monitoringidan chiqarib tashlash yoki faqat ma'lum fayllarni kuzatish imkoniyati;
- 8) buferga joylashtirilgan ma'lum ma'lumotlarni (belgilangan xavfsizlik siyosati asosida) avtomatik aniqlash, agar bunday ma'lumotlar aniqlangan bo'lsa, axborot xavfsizligi uchun mas'ul shaxsga xabarnoma yuboriladi;
- 9) konfiguratsiya qilingan xavfsizlik qoidalariga muvofiq fayllarni kontent bo'yicha nusxalash va joylashtirishni bloklash imkoniyati.
- 10) foydalanuvchilar tomonidan buferga joylashtirilgan matnni qidirish, shu jumladan shablonlardan foydalanish imkoniyati.
- 11) almashish buferiga ko'chirilgan ma'lumotlar va buferdan alohida joylashtirilgan ma'lumotlarni aniqlashni sozlash imkoniyati;
- 12) faqat fayllarni, faqat matnni yoki faqat

- 8) автоматическое обнаружение определенной информации (на основании заданных политик безопасности), помещаемой в буфер обмена, с отправкой уведомления лицу, ответственному за информационную безопасность, в случае обнаружения такой информации;
- 9) возможность блокирования как копирования, так и вставки файлов по содержимому, в соответствии с настроенными правилами безопасности.
- 10) возможность поиска по тексту, помещаемому пользователями в буфер обмена, в том числе с применением шаблонов.
- 11) возможность настройки обнаружения отдельно информации, скопированной в буфер обмена, и информации, вставляемой из буфера обмена;
- 12) возможность настройки обнаружения в буфере обмена только файлов, только текста либо только изображений.

1.3.14 Требования к контролю ввода с клавиатуры:

Система должна позволять контролировать ввод пользователя с клавиатуры, и располагать следующими возможностями:

- 1) регистрация нажатий пользователем клавиш на клавиатуре с фиксацией приложения, в котором пользователь вводил данную информацию, и времени, возможность отображения/скрытия нажатий служебных клавиш (Shift, Enter, Backspace и т.п.);
- 2) возможность исключения перехвата клавиатуры в заданных приложениях либо осуществление перехвата только в определенных приложениях;
- 3) возможность исключения перехвата клавиатуры по адресу активной страницы в браузере либо осуществление перехвата только на определенной активной странице в браузере;
- 4) автоматическое обнаружение определенной информации (на основании заданных политик безопасности), вводимой пользователем с помощью клавиатуры, с отправкой уведомления лицу,

- 11) the ability to configure detection separately of information copied to the clipboard and information pasted from the clipboard;
- 12) the ability to configure the detection of only files, only text, or only images in the clipboard.

1.3.14 Keyboard input control requirements:

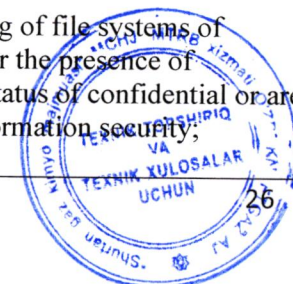
The system should allow you to control user input from the keyboard, and have the following features:

- 1) registration of user keystrokes on the keyboard with fixing the application in which the user entered this information, and time, the ability to display/hide service keystrokes (Shift, Enter, Backspace, etc.);
- 2) the ability to exclude keyboard interception in specified applications or perform interception only in certain applications;
- 3) the possibility of excluding keyboard interception at the address of the active page in the browser, or performing interception only on a specific active page in the browser;
- 4) automatic detection of certain information (based on the specified security policies) entered by the user using the keyboard, with sending a notification to the person responsible for information security in case of detection of such information;
- 5) the ability to search for text entered by users from the keyboard, including using templates.

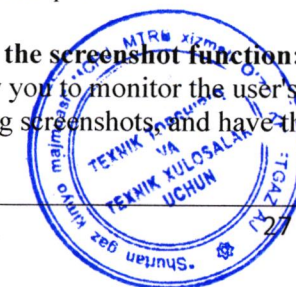
1.3.15 File system control requirements:

The system must allow you to control files stored in the workstation's file system and have the following capabilities:

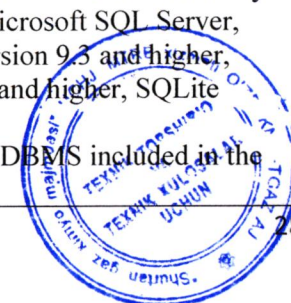
- 1) automatic scanning of file systems of controlled workstations for the presence of documents that have the status of confidential or are of interest in ensuring information security;



<p>clipboarddagi rasmlarni aniqlashni sozlash imkoniyati.</p> <p>1.3.14 Klaviaturadan kiritishni boshqarishga qo'yiladigan talablar:</p> <p>Tizim klaviaturadan foydalanuvchi kiritishini boshqarish imkonini berishi va quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) foydalanuvchi ushbu ma'lumotni va vaqtni kiritgan ilovani yozib olish bilan klaviaturada foydalanuvchi tomonidan klaviatura bosishlarini ro'yxatdan o'tkazish, xizmat tugmachalarini bosishni ko'rsatish / yashirish imkoniyati (Shift , Enter , Backspace va boshqalar);</p> <p>2) belgilangan ilovalarda klaviatura ushlab istisno qilish yoki faqat ma'lum ilovalarda ushlab istisno qilish imkoniyati;</p> <p>3) brauzerdagi faol sahifa manzilida klaviaturani ushlab turishni istisno qilish yoki faqat brauzerning ma'lum bir faol sahifasida ushlab istisno qilish imkoniyati;</p> <p>4) foydalanuvchi tomonidan klaviatura yordamida kiritilgan ma'lum ma'lumotlarni (belgilangan xavfsizlik siyosati asosida) avtomatik aniqlash, agar bunday ma'lumotlar aniqlangan bo'lsa, axborot xavfsizligi uchun mas'ul shaxsga xabarnoma yuboriladi;</p> <p>5) foydalanuvchilar tomonidan klaviaturadan kiritilgan matn bo'yicha, shu jumladan shablonlardan foydalangan holda qidirish imkoniyati.</p> <p>1.3.15 Fayl tizimini boshqarishga qo'yiladigan talablar:</p> <p>Tizim ish stantsiyasining fayl tizimida saqlangan fayllarni boshqarishga ruxsat berishi va quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) maxfiy maqomga ega bo'lgan yoki axborot xavfsizligi doirasida qiziqish uyg'otadigan hujjatlar mavjudligi uchun boshqariladigan ish</p>	<p>ответственному за информационную безопасность, в случае обнаружения такой информации;</p> <p>5) возможность поиска по тексту, вводимому пользователями с клавиатуры, в том числе с применением шаблонов.</p> <p>1.3.15 Требования к контролю файловой системы: Система должна позволять контролировать файлы, хранящиеся в файловой системе рабочей станции и располагать следующими возможностями:</p> <p>1) автоматическое сканирование файловых систем контролируемых рабочих станций на предмет наличия документов, которые носят статус конфиденциальных либо представляют интерес в рамках обеспечения информационной безопасности;</p> <p>2) формирование банков конфиденциальных документов, поиск которых должен выполняться во время сканирования;</p> <p>3) возможность автоматического импорта в банк конфиденциальных документов подготовленных хеш-функций из файлов txt- и csv-формата;</p> <p>4) возможность выбора рабочих станций и пользователей, чьи файловые системы будут контролироваться;</p> <p>5) гибкая настройка правил выбора файлов и папок, подлежащих автоматической проверке;</p> <p>6) исключение из сканирования файлов настраиваемого размера;</p> <p>7) возможность выполнения проверок файловой системы по расписанию;</p> <p>8) возможность создавать индивидуальные политики контроля за содержимым файловых систем для отдельных пользователей и рабочих станций, в том числе с применением шаблонов;</p> <p>9) возможность поиска документов в файловых системах контролируемых рабочих станций по атрибутам файлов и значениям их хеш-функций.</p>	<p>2) formation of banks of confidential documents, the search for which should be performed during scanning;</p> <p>3) the ability to automatically import prepared hash functions from txt and csv files to the bank of confidential documents;</p> <p>4) the ability to select workstations and users whose file systems will be monitored;</p> <p>5) flexible configuration of rules for selecting files and folders to be automatically checked;</p> <p>6) exclusion of files of a custom size from scanning;</p> <p>7) ability to perform scheduled file system checks;</p> <p>8) the ability to create individual policies for controlling the contents of file systems for individual users and workstations, including using templates;</p> <p>9) the ability to search for documents in the file systems of controlled workstations by file attributes and values of their hash functions.</p> <p>2.1. Requirements for the functionality of the macOS agent:</p> <p>The system must support macOS 11 (Big Sur) and later versions</p> <p>2.1.1 Requirements for monitoring user activity:</p> <p>The system should allow monitoring user activity at the workplace and have the following capabilities:</p> <p>1) audit of running processes;</p> <p>2) excluding individual processes from monitoring;</p> <p>2.1.2 Requirements for the screenshot function:</p> <p>The system should allow you to monitor the user's desktop activity by taking screenshots and have the following features:</p>
---	--	---



<p>stantsiyalarining fayl tizimlarini avtomatik skanerlash;</p> <p>2) skanerlash vaqtida izlash amalga oshirilishi kerak bo'lgan maxfiy hujjatlar banklarini shakllantirish;</p> <p>3) txt va csv fayllaridan tayyorlangan xesh-funksiyalarni maxfiy hujjatlar bankiga avtomatik ravishda import qilish imkoniyati ;</p> <p>4) fayl tizimlari nazorat qilinadigan ish stantsiyalari va foydalanuvchilarni tanlash imkoniyati;</p> <p>5) avtomatik skanerlash uchun fayl va papkalarni tanlash qoidalarining moslashuvchan konfiguratsiyasi;</p> <p>6) maxsus o'lchamdagi fayllarni skanerlashdan chiqarib tashlash;</p> <p>7) jadval bo'yicha fayl tizimini tekshirishni amalga oshirish imkoniyati;</p> <p>8) individual foydalanuvchilar va ish stantsiyalari, shu jumladan shablonlardan foydalanish uchun fayl tizimlarining mazmunini boshqarish bo'yicha individual siyosatlarini yaratish qobiliyati;</p> <p>9) fayl atributlari va ularning xesh funksiyalari qiymatlari bo'yicha boshqariladigan ish stantsiyalarining fayl tizimlarida hujjatlarni qidirish qobiliyati.</p> <p>2.1. MacOS agenti funksional talablari : Tizim MacOS 11 (Big Sur) va keyingi versiyalari</p> <p>2.1.1 Foydalanuvchi faoliyatini monitoring qilish uchun talablar: Tizim foydalanuvchining ish joyidagi faoliyatini kuzatish imkonini berishi va quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) ishlaydigan jarayonlarning auditi;</p> <p>2) alohida jarayonlarni monitoringdan chiqarib tashlash;</p>	<p>2.1. Требования к функциональным возможностям MacOS-агента: Система должна поддерживать MacOS 11(Big Sur) и более поздние версии</p> <p>2.1.1 Требования к мониторингу пользовательской активности: Система должна позволять контролировать активность пользователя на рабочем месте и располагать следующими возможностями:</p> <p>1) аудит запущенных процессов;</p> <p>2) исключение отдельных процессов из мониторинга;</p> <p>2.1.2 Требования к функции снимков экрана: Система должна позволять контролировать активность рабочего стола пользователя при помощи снятия снимков экрана, и располагать следующими возможностями:</p> <p>1) возможность снятия скриншотов с заданным интервалом с точностью до секунды;</p> <p>2) возможность снятия скриншотов при запуске процесса;</p> <p>3) возможность настройки качества скриншотов, в том числе сохранения в черно-белом формате;</p> <p>4) возможность настройки размера скриншотов (в процентах от оригинала);</p> <p>5) возможность настройки формата скриншотов (JPEG, PNG);</p> <p>6) сохранение специальной отметки в случае невозможности снятия скриншота;</p> <p>7) возможность снятия скриншотов только при запуске заданных процессов;</p> <p>8) возможность сохранения скриншотов отдельного пользователя за день (или за выбранный временной интервал) в виде набора графических файлов, либо объединенных в один PDF- или видеофайл.</p> <p>3. Требования к хранению и обработке данных:</p>	<p>1) the ability to take screenshots at a given interval with an accuracy of up to a second;</p> <p>2) the ability to take screenshots when starting the process;</p> <p>3) the ability to adjust the quality of screenshots, including saving in black and white format;</p> <p>4) the ability to adjust the size of screenshots (as a percentage of the original);</p> <p>5) the ability to configure the format of screenshots (JPEG, PNG);</p> <p>6) save a special mark if you can't take a screenshot.</p> <p>7) the ability to take screenshots only when running the specified processes;</p> <p>8) the ability to save screenshots of an individual user for a day (or for a selected time interval) as a set of graphic files, or combined into a single PDF or video file.</p> <p>3. Data storage and processing requirements: The settings should allow you to connect information repositories managed by a number of DBMS systems, manage data in geographically distributed organizations using data replication, create rules for saving certain types of data to specified repositories, and form database rotation groups. Data storage and processing should have the following functionality:</p> <p>1) the ability to store all data collected by the system in the DBMS Microsoft SQL Server, Oracle, PostgreSQL version 9.3 and higher, MySQL version 5.7.09 and higher, SQLite (optional);</p> <p>2) built-in SQLite DBMS included in the delivery package;</p>
--	--	--



2.1.2 Skrinshot funksiyasiga qo'yiladigan talablar:

Tizim sizga skrinshotlar olish orqali foydalanuvchining ish stoli faoliyatini kuzatish imkonini berishi va quyidagi imkoniyatlarga ega bo'lishi kerak:

- 1) ma'lum bir oraliqda bir soniyagacha anqlik bilan skrinshot olish qobiliyati;
- 2) jarayon boshlanganda ekran tasvirlarini olish imkoniyati;
- 3) skrinshotlar sifatini sozlash, shu jumladan qora va oq formatda saqlash imkoniyati;
- 4) skrinshotlar hajmini sozlash qobiliyati (asl nusxadan foiz sifatida);
- 5) skrinshot formatini sozlash qobiliyati (JPEG, PNG);
- 6) skrinshotni olishning iloji bo'lmasa, maxsus belgini saqlash;
- 7) faqat belgilangan jarayonlarni bajarayotganda skrinshot olish imkoniyati;
- 8) individual foydalanuvchining skrinshotlarini bir kun davomida (yoki tanlangan vaqt oralig'ida) grafik fayllar to'plami sifatida yoki bitta PDF yoki video faylga birlashtirilgan holda saqlash imkoniyati.

3. Ma'lumotlarni saqlash va qayta ishlashga qo'yiladigan talablar:

Sozlamalar bir qator ma'lumotlar bazalari tomonidan boshqariladigan ma'lumotlar omborlarini ulashga, ma'lumotlar replikasiyasidan foydalangan holda geografik taqsimlangan tashkilotlarda ma'lumotlarni boshqarishga, ma'lum turdagi ma'lumotlarni ko'rsatilgan omborlarda saqlash qoidalarini yaratishga va ma'lumotlar bazasini aylantirish guruhlarini shakllantirishga imkon berishi kerak. Ma'lumotlarni saqlash va qayta ishlash quyidagi funktsiyalarga ega bo'lishi kerak:

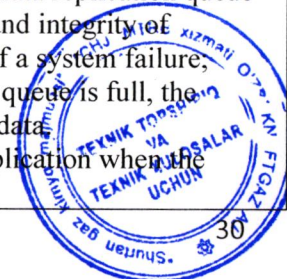
Настройки должны позволять подключать хранилища информации под управлением ряда СУБД, управлять данными в территориально распределенных организациях при помощи репликации данных, создавать правила сохранения данных определенных типов в заданные хранилища и формировать группы ротации баз данных.

Хранение и обработка данных должна обладать следующим функционалом:

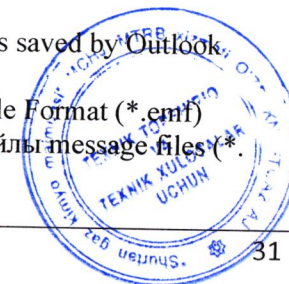
- 1) возможность хранения всех собираемых системой данных в СУБД Microsoft SQL Server, Oracle, PostgreSQL версии 9.3 и выше, MySQL версии 5.7.09 и выше, SQLite (на выбор);
- 2) встроенная СУБД SQLite в комплекте поставки;
- 3) хранение всех перехватываемых данных вне зависимости от срабатывания политик безопасности;
- 4) поддержка работы с базами данных, расположенных на разных серверах;
- 5) возможность сохранения файлов на диск сервера, а не в базу, с возможностью исключения из сохранения на диск файлов малого размера, при этом в базу данных помещаются относительные пути к файлам;
- 6) возможность включения/отключения распознавания изображений, печатей для отдельных баз данных;
- 7) возможность настройки длительности хранения информации в базе данных в группе ротации;
- 8) возможность отключения базы данных вручную через Консоль администратора, при этом содержимое базы данных сохраняется;
- 9) возможность очистки содержимого базы данных вручную через Консоль администратора;
- 10) возможность архивирования баз данных с последующим подключением к системе для осуществления ретроспективного поиска в них критичной информации;

- 3) storing all intercepted data regardless of whether security policies are triggered;
- 4) support for working with databases located on different servers;
- 5) the ability to save files to the server disk, and not to the database, with the possibility of excluding small files from saving to disk, while relative file paths are placed in the database;
- 6) ability to enable / disable image and print recognition for individual databases;
- 7) the ability to configure the duration of information storage in the database in the rotation group;
- 8) the ability to disable the database manually through the Administrator Console, while the contents of the database are saved;
- 9) the ability to clear the database contents manually through the Administrator Console;
- 10) the ability to archive databases with subsequent connection to the system for retrospective search of critical information in them;
- 11) possibility of selective deletion of intercepted information by the user;
- 12) the ability to combine single databases into groups that support circular database rotation, while search operations are performed on all databases in the group, and data is recorded only in the active one;
- 13) the ability to configure several database rotation conditions: the total amount of data, the size of the database, the size of search indexes, the size of files on disk, the time interval, the number of records, and the start of the rotation process can be configured for a specific time period;
- 14) the ability to configure the execution of scripts before the rotation process begins, after the rotation is completed, and in case of rotation error;

<p>1) tizim tomonidan to'plangan barcha ma'lumotlarni DBMSda saqlash imkoniyati Microsoft SQL Server , Oracle , PostgreSQL 9.3 va undan yuqori versiyalari, MySQL 5.7.09 va undan yuqori versiyalari, SQLite (ixtiyoriy);</p> <p>2) paketga kiritilgan o'rnatilgan SQLite DBMS ;</p> <p>3) xavfsizlik siyosatini ishga tushirishdan qat'i nazar, barcha ushlangan ma'lumotlarni saqlash;</p> <p>4) turli serverlarda joylashgan ma'lumotlar bazalari bilan ishlashni qo'llab-quvvatlash;</p> <p>5) fayllarni ma'lumotlar bazasida emas, balki server diskda saqlash imkoniyati, kichik fayllarni diskda saqlashdan istisno qilish imkoniyati, fayllarga nisbatan nisbiy yo'llar ma'lumotlar bazasiga joylashtirilgan;</p> <p>6) individual ma'lumotlar bazalari uchun rasm va muhrni aniqlashni yoqish/o'chirish imkoniyati ;</p> <p>7) aylanish guruhida ma'lumotlar bazasida ma'lumotlarni saqlash muddatini sozlash qobiliyati,</p> <p>8) ma'lumotlar bazasi tarkibi saqlanib qolgan holda ma'lumotlar bazasini Administrator konsoli orqali qo'lda o'chirish imkoniyati;</p> <p>9) Administrator konsoli orqali ma'lumotlar bazasi tarkibini qo'lda tozalash imkoniyati;</p> <p>10) ma'lumotlar bazalarini arxivlash va keyinchalik ulardagi muhim ma'lumotlarni retrospektiv qidirishni amalga oshirish uchun tizimga ulanish imkoniyati;</p> <p>11) foydalanuvchi ushlangan ma'lumotni tanlab o'chirish imkoniyati;</p> <p>12) yagona ma'lumotlar bazalarini ma'lumotlar bazasini dumaloq aylantirishni qo'llab-quvvatlaydigan guruhlariga birlashtirish imkoniyati, qidiruv operatsiyalari guruhdagi barcha ma'lumotlar bazalarida amalga oshiriladi va ma'lumotlarni yozish faqat faol bo'lganida sodir bo'ladi;</p> <p>13) ma'lumotlar bazasini aylantirish uchun bir</p>	<p>11) возможность выборочного удаления пользователем перехваченной информации;</p> <p>12) возможность объединять одиночные базы данных в группы, поддерживающие кольцевую ротацию баз, при этом поисковые операции выполняются по всем базам данных в группе, а запись данных происходит только в активную;</p> <p>13) возможность настройки нескольких условий ротации баз данных: общий объем данных, размер базы данных, размер поисковых индексов, размер файлов на диске, временной интервал, количество записей, при этом запуск процесса ротации может быть настроен на определенный временной промежуток;</p> <p>14) возможность настроить выполнение скриптов до начала процесса ротации, после завершения ротации, и при ошибке ротации, при этом поддерживаются выполнение cmd, PowerShell, Script Host, Python скриптов;</p> <p>15) возможность балансировки нагрузки по двум и более группам баз данных либо базам данных согласно алгоритму "round robin": все поступающие в систему данные записываются в базы данных поочередно;</p> <p>16) поддержка режима параллельной обработки данных, перехваченных по различным каналам передачи информации, что позволяет повысить производительность системы при выполнении операций обновления, удаления и поиска данных;</p> <p>17) возможность настройки правил записи данных в базы данных и группы ротации для регуляции, в какое хранилище записывать информацию в зависимости от часового пояса данных, типа данных, источника данных, вхождения пользователя или компьютера в домен или любой AD-контейнер по его имени, SID или GUID, IP-адреса и другой атрибутивной информации;</p> <p>18) возможность автоматической репликации поступающих данных из дочерних контролируемых сетей</p>	<p>while the execution of cmd, PowerShell, Script Host, and Python scripts is supported;</p> <p>15) the possibility of load balancing across two or more groups of databases or databases according to the "round robin" algorithm: all data entering the system is written to the databases in turn;</p> <p>16) support for parallel processing of data intercepted via various data transmission channels, which allows you to increase system performance when performing data update, delete, and search operations;</p> <p>17) ability to configure rules for writing data to databases and rotation groups to regulate which storage to write information to depending on the data time zone, data type, data source, user or computer entry into a domain or any AD container by its name, SID or GUID, IP address and other attribute information;</p> <p>18) the ability to automatically replicate incoming data from child controlled networks or offices to higher-level servers in geographically distributed organizational structures;</p> <p>19) protection against incorrect replication settings when data is returned to the replication server and then replicated again;</p> <p>20) the ability to redirect incoming data from child controlled networks or offices to higher-level servers;</p> <p>21) ability to configure a schedule for data replication;</p> <p>22) the ability to store a data replication queue on disk to ensure the safety and integrity of replicated data in the event of a system failure;</p> <p>23) when the replication queue is full, the server blocks receiving new data;</p> <p>24) the ability to skip replication when the queue is full;</p>
--	---	---



<p>nechta shartlarni sozlash qobiliyati: ma'lumotlarning umumiy hajmi, ma'lumotlar bazasi hajmi, qidiruv indekslarining o'lehami, diskdagi fayllar hajmi, vaqt oraliqi, yozuvlar soni, bunda aylanish jarayonining boshlanishi ma'lum vaqtga sozlanishi mumkin. davr;</p> <p>14) aylanish jarayoni boshlanishidan oldin, aylanish tugagandan so'ng va aylanish xatosi bo'lsa, cmd , PowerShell , skript bajarilishini qo'llab-quvvatlagan holda skriptlarning bajarilishini sozlash qobiliyati Xost , Python skriptlari;</p> <p>15) dumaloq " algoritimga muvofiq ma'lumotlar bazalari yoki ma'lumotlar bazalarining ikki yoki undan ortiq guruhlar bo'ylab balansni yuklash qobiliyati robin ": tizimga kiradigan barcha ma'lumotlar ma'lumotlar bazalariga birma-bir yoziladi;</p> <p>16) turli xil axborot uzatish kanallari orqali ushlangan ma'lumotlarni parallel qayta ishlashni qo'llab-quvvatlash, bu ma'lumotlarni yangilash, o'chirish va qidirish operatsiyalarini bajarishda tizim ish faoliyatini yaxshilaydi;</p> <p>17) ma'lumotlarning vaqt zonasi, ma'lumotlar turi, ma'lumotlar manbai, foydalanuvchi yoki kompyuter domenda yoki har qanday AD konteynerida bo'ladimi-yo'qligiga qarab ma'lumotni saqlashni tartibga solish uchun ma'lumotlar bazalari va aylanish guruhlariga ma'lumotlarni yozish qoidalarini sozlash qobiliyati. ism, SID yoki GUID, IP manzillar va boshqa atribut ma'lumotlari;</p> <p>18) boshqariladigan yordamchi tarmoqlar yoki ofislardan kelayotgan ma'lumotlarni geografik jihatdan taqsimlangan tashkiliy tuzilmalardagi yuqori darajadagi serverlarga avtomatik ravishda takrorlash imkoniyati;</p> <p>19) noto'g'ri replikatsiya sozlamalaridan himoya qilish, ma'lumotlar replikatsiya serveriga qaytarilganda va keyin yana takrorlanganda;</p>	<p>или офисов на вышестоящие сервера в территориально распределённых организационных структурах;</p> <p>19) защита от некорректной настройки репликации, когда данные возвращаются на реплицирующий сервер и далее реплицируются повторно;</p> <p>20) возможность перенаправления поступающих данных из дочерних контролируемых сетей или офисов на вышестоящие сервера;</p> <p>21) возможность настройки расписания для репликации данных;</p> <p>22) возможность хранения очереди репликации данных на диске для обеспечения сохранности и целостности реплицируемых данных в случае отказа системы;</p> <p>23) при переполнении очереди репликации сервер блокирует прием новых данных;</p> <p>24) возможность пропуска репликации при переполнении очереди;</p> <p>25) отображение статистики репликации данных;</p> <p>26) возможность хранения на диске очереди данных, поступающих от агентов, что повышает их сохранность по сравнению с хранением в оперативной памяти;</p> <p>27) возможность выбора режима очистки и обновления поисковых индексов (ручной и автоматический режимы);</p> <p>28) возможность индексации содержимого заголовков перехватываемых писем, при этом поддерживается фильтрация полей заголовков писем, значения которых будут индексироваться</p> <p>29) возможность осуществления асинхронного поиска по перехваченным данным (при проведении параллельного поиска по нескольким каналам передачи информации, отображение результатов выполняется по мере их получения);</p> <p>30) просмотр комплексной статистики по хранящимся и индексируемым данным в базах данных и группах ротации.</p>	<p>25) displaying data replication statistics.</p> <p>26) the ability to store data coming from agents on the disk queue, which increases their safety compared to storage in RAM;</p> <p>27) the ability to select the mode of cleaning and updating search indexes (manual and automatic modes);</p> <p>28) the ability to index the contents of the headers of intercepted emails, while filtering the fields of email headers whose values will be indexed is supported</p> <p>29) the ability to perform asynchronous search on intercepted data (when conducting a parallel search on several information transmission channels, the results are displayed as they are received);</p> <p>30) view comprehensive statistics on stored and indexed data in databases and rotation groups.</p> <p>The system must index files in the following formats:</p> <ol style="list-style-type: none"> 1) Adobe Acrobat (*.pdf) 2) Ami Pro (*.sam) 3) Ansi Text (*.txt) 4) ASCII Text 5) ASF (metadata) (*. asf) 6) CSV (Comma-separated values) (*.csv) 7) DBF (*.dbf) 8) DjVu 9) DWG 10) DXF 11) EBCDIC 12) EML files (emails saved by Outlook Express) (*. eml) 13) Enhanced Metafile Format (*.emf) 14) Eudora MBX файлы message files (*.mbx) 15) Flash (*.swf)
--	---	--



<p>20) boshqariladigan yordamchi tarmoqlar yoki ofislardan kiruvchi ma'lumotlarni yuqori darajadagi serverlarga yo'naltirish imkoniyati;</p> <p>21) ma'lumotlarni takrorlash uchun jadvalni sozlash qobiliyati;</p> <p>22) tizim ishlaymay qolganda takrorlangan ma'lumotlarning xavfsizligi va yaxlitligini ta'minlash uchun diskda ma'lumotlarni takrorlash navbatini saqlash imkoniyati;</p> <p>23) replikasiya navbati to'lganida, server yangi ma'lumotlarni qabul qilishni bloklaydi;</p> <p>24) navbat to'lganida replikatsiyani o'tkazib yuborish imkoniyati;</p> <p>25) ma'lumotlarni takrorlash statistikasini ko'rsatish;</p> <p>26) agentlardan olingan ma'lumotlar navbatini diskda saqlash imkoniyati, bu ularning xavfsizligini RAMda saqlashga nisbatan oshiradi;</p> <p>27) qidiruv indekslarini tozalash va yangilash rejimini tanlash imkoniyati (qo'lda va avtomatik rejimlar);</p> <p>28) qiymatlari indekslanadigan elektron pochta sarlavhalari maydonlarini filtrlashda tutib olingan xatlarning sarlavhalari tarkibini indekslash imkoniyati qo'llab-quvvatlanadi.</p> <p>29) ushlangan ma'lumotlardan foydalangan holda asinxron qidiruvni amalga oshirish qobiliyati (bir nechta ma'lumot uzatish kanallari orqali parallel qidiruvni o'tkazishda natijalar ular qabul qilinganda ko'rsatiladi);</p> <p>30) ma'lumotlar bazalari va aylanish guruhlarida saqlangan va indekslangan ma'lumotlar bo'yicha murakkab statistik ma'lumotlarni ko'rish. Tizim fayllarni quyidagi formatlarda indekslashi kerak:</p>	<p>Система должна индексировать файлы следующих форматов:</p> <ol style="list-style-type: none"> 1) Adobe Acrobat (*.pdf) 2) Ami Pro (*.sam) 3) Ansi Text (*.txt) 4) ASCII Text 5) ASF (метаданные) (*.asf) 6) CSV (Comma-separated values) (*.csv) 7) DBF (*.dbf) 8) DjVu 9) DWG 10) DXF 11) EBCDIC 12) EML files (электронные письма, сохраненные Outlook Express) (*.eml) 13) Enhanced Metafile Format (*.emf) 14) Eudora MBX файлы сообщений (*.mbx) 15) Flash (*.swf) 16) GZIP (*.gz) 17) HTML (*.htm, *.html) 18) JPEG (метаданные) (*.jpg) 19) Lotus 1-2-3 (*.wk?, *.123) 20) MBOX архивы электронных писем (включая Thunderbird) (*.mbx) 21) MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (*.mht) 22) Microsoft Access (*.mdb) 23) Microsoft Access 2007 (*.accdb) 24) Microsoft Document Imaging (*.mdi) 25) Microsoft Excel (*.xls) 26) Microsoft Excel 2003 XML (*.xml) 27) Microsoft Excel 2007 (*.xlsx) 28) Microsoft Open XML Paper Specification (*.oxps) 29) Microsoft Outlook (OST) 30) Microsoft Outlook Express 5 и 6: базы сообщений (*.dbx) 31) Microsoft PowerPoint (*.ppt) 	<ol style="list-style-type: none"> 16) GZIP (*.gz) 17) HTML (*.htm, *.html) 18) JPEG (metadata) (*.jpg) 19) Lotus 1-2-3 (*.wk?, *.123) 20) MBOX email archives (including Thunderbird) (*.mbx) 21) MHT archives (HTML archives saved by Internet Explorer) (*.mht) 22) Microsoft Access (*.mdb) 23) Microsoft Access 2007 (*.accdb) 24) Microsoft Document Imaging (*.mdi) 25) Microsoft Excel (*.xls) 26) Microsoft Excel 2003 XML (*.xml) 27) Microsoft Excel 2007 (*.xlsx) 28) Microsoft Open XML Paper Specification (*.oxps) 29) Microsoft Outlook (OST) 30) Microsoft Outlook Express 5 and 6: bases Message databases (*.dbx) 31) Microsoft PowerPoint (*.ppt) 32) Microsoft Rich Text Format (*.rtf) 33) Microsoft Searchable Tiff (*.tiff) 34) Microsoft Word 2003 XML (*.xml) 35) Microsoft Word 2007 (*.docx) 36) Microsoft Word for DOS (*.doc) 37) Microsoft Word for Windows (*.doc) 38) Microsoft Works (*.wks) 39) MIME messages 40) MP3 (metadata) (*.mp3) 41) MSG files (emails saved by Outlook) (*.msg) 42) Multimate Advantage II (*.doxx) 43) Multimate version 4 (*.doc) 44) OpenOffice versions 1, 2 and 3: documents, electronic spreadsheets and presentations (*.sx*, *.sxd, *.sxi, *.sxw, *.sxc, *.stc, *.std, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, ...)
--	---	---

3) Ansi Matn (*.txt)	32) Microsoft Rich Text Format (*.rtf)	ods, *.ots, *.odf) (including OASIS Open Document Format for office applications)
4) ASCII matni	33) Microsoft Searchable Tiff (*.tiff)	45) OST (внутренний формат Microsoft Outlook internal format)
5) ASF (metadata) (*.asf)	34) Microsoft Word 2003 XML (*.xml)	46) Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw)
6) CSV (vergul bilan ajratilgan qiymatlar) (*.csv)	35) Microsoft Word 2007 (*.docx)	47) TAR (*.tar)
7) DBF (*.dbf)	36) Microsoft Word for DOS (*.doc)	48) TIFF (*.tif)
8) DjVu	37) Microsoft Word for Windows (*.doc)	49) TNEF (winmail.dat)
9) DWG	38) Microsoft Works (*.wks)	50) Treepad HJT (*.hjt)
10) DXF	39) MIME-сообщения	51) Unicode (UCS16, порядок байтов Mac or Windows byte order, or UTF-8)
11) EBCDIC	40) MP3 (метаданные) (*.mp3)	52) Windows Metafile Format (*.wmf)
12) EML fayllari (Outlook tomonidan saqlangan elektron pochta xabarlar Ekspress) (*.eml)	41) MSG files (электронные письма, сохраненные Outlook) (*.msg)	53) WMA video (metadata) (*.wma)
13) Kengaytirilgan Metafayl Format (*.emf)	42) Multimate Advantage II (*.dox)	54) WMV video (metadata) (*.wmv)
14) Eudora MBX xabar fayllari (*.mbx)	43) Multimate version 4 (*.doc)	55) WordPerfect (5.0 and higher) (*.wpd, *.wpf)
15) Flash (*.swf)	44) OpenOffice версий 1, 2 и 3: документы, электронные таблицы и презентации (*.sxc, *.sxd, *.sxi, *.sxw, *.sxc, *.stc, *.sti, *.stw, *.stm, *.odt, *.ott, *.odg, *.otg, *.odp, *.otp, *.ods, *.ots, *.odf) (включая OASIS Open Document Format для офисных приложений)	56) WordPerfect 4.2 (*.wpd, *.wpf)
16) GZIP (*.gz)	45) OST (внутренний формат Microsoft Outlook)	57) WordStar 2000
17) HTML (*.htm, *.html)	46) Quattro Pro (*.wb1, *.wb2, *.wb3, *.qpw)	58) WordStar versions 1, 2, 3, 4, 5, 6 (*.ws)
18) JPEG (metadata) (*.jpg)	47) TAR (*.tar)	59) Write (*.wri)
19) Lotus 1-2-3 (*.wk?, *.123)	48) TIFF (*.tif)	60) xBase (including FoxPro, dBase, and other xBase-compatible formats) (*.dbf)
20) MBOX elektron pochta arxivlari (jumladan, Thunderbird) (*.mbx)	49) TNEF (winmail.dat)	61) XML Paper Specification (*.xps)
21) Internet orqali saqlangan HTML arxivlari Explorer) (*.mht)	50) Treepad HJT (*.hjt)	62) XSL
22) Microsoft Kirish (*.mdb)	51) Unicode (UCS16, порядок байтов Mac или Windows, или UTF-8)	63) XyWrite
23) Microsoft Access 2007 (*.accdb)	52) Windows Metafile Format (*.wmf)	64) ZIP (*.zip)
24) Microsoft Hujjat Tasvirlash (*.mdi)	53) WMA видео (метаданные) (*.wma)	
25) Microsoft Excel (*.xls)	54) WMV видео (метаданные) (*.wmv)	
26) Microsoft Excel 2003 XML (*.xml)	55) WordPerfect (5.0 и выше) (*.wpd, *.wpf)	
27) Microsoft Excel 2007 (*.xlsx)	56) WordPerfect 4.2 (*.wpd, *.wpf)	
28) Microsoft Open XML qog'oz spetsifikatsiyasi (*.oxps)	57) WordStar 2000	
29) Microsoft Outlook (OST)	58) WordStar версий 1, 2, 3, 4, 5, 6 (*.ws)	
30) Microsoft Outlook Express 5 va 6: asoslar xabarlar (*.dbx)	59) Write (*.wri)	
31) Microsoft PowerPoint (*.ppt)	60) XBase (включая FoxPro, dBase и другие совместимые с XBase форматы) (*.dbf)	
32) Microsoft Rich Text Format (*.rtf)	61) XML Paper Specification (*.xps)	
33) Microsoft Qidirish mumkin Tiff (*.tiff)		

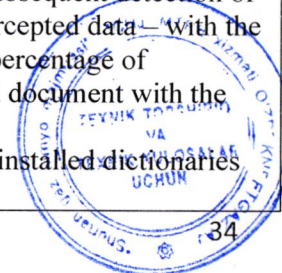
4. Requirements for data analysis.

The system should have a wide range of capabilities for analyzing intercepted data:

- 1) content analysis.
- 2) attribute analysis.
- 3) image recognition.
- 4) print recognition.
- 5) statistical analysis;
- 6) event analysis;
- 7) App categorization.
- 8) Website categorization;

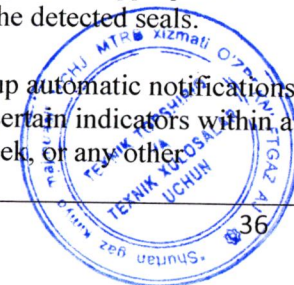


34) Microsoft Word 2003 XML (* .xml)	62) XSL	9) Accounting for the productivity of websites and applications.
35) Microsoft Word 2007 (* .docx)	63) XyWrite	4.1. Content Analysis:
36) DOS uchun Microsoft Word (* .doc)	64) ZIP (* .zip)	Content analysis of data should include:
37) Windows uchun Microsoft Word (* .doc)	4. Требования к анализу данных.	1) search by words and phrases based on morphology, with the option to disable it.
38) Microsoft Ishlar (* .wks)	Система должна располагать широким спектром возможностей анализа перехваченных данных:	2) search by words and phrases, taking into account the distance between words;
39) MIME xabarlari	1) контентный анализ;	3) search by words and phrases, taking into account the word order;
40) MP3 (metadata) (* .mp3)	2) атрибутивный анализ;	4) search by words and phrases, taking into account the transliteration of Cyrillic characters with Latin ones.
41) MSG fayllari (Outlook tomonidan saqlangan elektron pochta xabarlari) (* .msg)	3) распознавание изображений;	5) search by words and phrases with the possibility of fuzzy search, for finding keywords, including those written with errors and typos;
42) Multimate Afzallik II (* .dox)	4) распознавание печатей;	6) a regular expression search technology used to detect fixed sequences of characters, such as passport numbers, bank card numbers, etc.;
43) Multimate 4- versiya (* .doc)	5) статистический анализ;	7) the ability to use pre-installed regular expressions and create custom ones;
44) OpenOffice 1, 2 va 3 versiyalari: hujjatlar, elektron jadvallar va taqdimotlar (* .sxc , * .sxd , * .sxi , * .sxw , * .sxx , * .stc , * .sti , * .stw , * .stm , * .odt , * Hujjat Ofis ilovalari uchun format)	6) событийный анализ;	8) a mechanism for post-verification of bank card numbers based on payment systems;
45) Microsoft ichki formati Outlook)	7) Категоризация приложений;	9) search by topic dictionaries with morphology (the ability to disable it) and support for masks and regular expressions in dictionaries, with the ability to set the trigger threshold (for example, when detecting any 3 out of 10 words or expressions contained in the dictionary);
46) Quattro Pro (* .wb1, * .wb2, * .wb3, * .qpw)	8) Категоризация веб-сайтов;	10) creation of digital prints of documents or folders with documents for subsequent detection of similar documents in the intercepted data – with the possibility of specifying the percentage of compliance of the intercepted document with the original);
47) TAR (* .tar)	9) Учет продуктивности веб-сайтов и приложений.	11) the ability to use pre-installed dictionaries and create custom ones;
48) TIFF (* .tif)	4.1. Контентный анализ:	
49) TNEF (winmail.dat)	Контентный анализ данных должен включать в себя:	
50) Treepad HJT (* .hjt)	1) поиск по словам и словосочетаниям с учетом морфологии, с возможностью отключения;	
51) Unicode (UCS16, Mac yoki Windows bayt tartibi yoki UTF-8)	2) поиск по словам и словосочетаниям с учетом расстояния между словами;	
52) Windows Metafayl Format (* .wmf)	3) поиск по словам и словосочетаниям с учетом порядка слов;	
53) WMA video (metadata) (* .wma)	4) поиск по словам и словосочетаниям с учетом транслитерации кириллических символов латинскими,	
54) WMV video (metadata) (* .wmv)	5) поиск по словам и словосочетаниям с возможностью нечеткого поиска, для поиска ключевых слов, в том числе написанных с ошибками и опечатками;	
55) WordPerfect (5.0 va undan yuqori) (* .wpd , * .wpf)	6) технология поиска регулярных выражений, используемая для обнаружения фиксированных последовательностей символов, например, номеров паспортов, номеров банковских карт и т.п.;	
56) WordPerfect 4.2 (* .wpd , * .wpf)	7) возможность использования предустановленных регулярных выражений и создания пользовательских;	
57) WordStar 2000	8) механизм постпроверки номеров банковских карт по базе платежных систем;	
58) WordStar 1, 2, 3, 4, 5, 6 versiyalari (* .ws)		
59) Yozing (* .wri)		
60) XBase (shu jumladan FoxPro , dBase va boshqa XBase mos formatlari) (* .dbf)		
61) XML qog'ozlari Spetsifikatsiya (* .xps)		
62) XSL		
63) XyWrite		



<p>64) ZIP (*.zip)</p> <p>4. Ma'lumotlarni tahlil qilishga qo'yiladigan talablar.</p> <p>Tizim ushlangan ma'lumotlarni tahlil qilish uchun keng imkoniyatlarga ega bo'lishi kerak:</p> <ol style="list-style-type: none"> 1) tarkibni tahlil qilish; 2) atributlarni tahlil qilish; 3) tasvirni aniqlash; 4) muhrni tanib olish; 5) statistik tahlil; 6) hodisalarni tahlil qilish; 7) Ilova toifalari; 8) Veb-saytlarni tasniflash; 9) Veb-saytlar va ilovalarning samaradorligini nazorat qilish. <p>4.1. Kontent tahlili:</p> <p>Ma'lumotlarning mazmunini tahlil qilish quyidagilarni o'z ichiga olishi kerak:</p> <ol style="list-style-type: none"> 1) o'chirish imkoniyati bilan morfologiyani hisobga olgan holda so'zlar va iboralar bo'yicha qidirish; 2) so'zlar orasidagi masofani hisobga olgan holda so'zlar va iboralar bo'yicha qidirish; 3) so'z tartibini hisobga olgan holda so'z va iboralar bo'yicha qidirish; 4) kirill harflarining lotin harflariga transliteratsiyasini hisobga olgan holda so'z va iboralar bo'yicha qidirish; 5) kalit so'zlarni, shu jumladan xato va matn terish xatosi bilan yozilgan so'zlarni qidirish uchun loyqa qidiruv imkoniyati bilan so'zlar va iboralar bo'yicha qidirish; 6) Belgilarning qat'iy ketma-ketligini aniqlash uchun foydalaniladigan muntazam ifodalarni qidirish texnologiyasi, masalan, pasport raqamlari, bank kartalari raqamlari va boshqalar; 7) oldindan belgilangan muntazam iboralardan 	<ol style="list-style-type: none"> 9) поиск по тематическим словарям с учетом морфологии (возможность отключения) и поддержкой масок и регулярных выражений в словарях, с возможностью настройки порога срабатывания (например, при обнаружении любых 3 из 10 слов или выражений, содержащихся в словаре); 10) создание цифровых отпечатков документов или папок с документами для последующего обнаружения в перехваченных данных похожих документов – с возможностью указания процента соответствия перехваченного документа оригиналу); 11) возможность использования предустановленных словарей и создания пользовательских; 12) технология поиска по цифровым отпечаткам документов с возможностью указания процента соответствия перехваченного документа оригиналу; 13) технология поиска по цифровым отпечаткам документов с возможностью выбора прямого, обратного либо наибольшего вхождения; 14) синхронизация банка цифровых отпечатков с папками, в которых располагаются документы, с возможностью настройки интервала обновления 15) создание цифровых отпечатков CSV-файлов, с выбором полей со значимой информацией для добавления в банк данных; 16) создание цифровых отпечатков баз данных, при помощи настройки подключения системы к базе данных, для создания цифровых отпечатков определенных полей выбранных таблиц с целью последующего обнаружения утечки информации из этой базы данных (например, при одновременном обнаружении персональных данных из связки полей «ФИО + паспортные данные»); 17) создание и обновление цифровых отпечатков баз данных осуществляется без промежуточных действий, таких как выгрузка базы данных в файл-источник цифрового отпечатка. При внесении изменений в базу 	<ol style="list-style-type: none"> 12) search technology based on digital fingerprints of documents with the ability to indicate the percentage of compliance of the intercepted document with the original; 13) search technology based on digital fingerprints of documents with a choice of direct, reverse or largest occurrence; 14) synchronization of the digital fingerprint bank with folders where documents are located, with the ability to configure the update interval 15) creating digital prints of CSV files, with a choice of fields with significant information to add to the data bank; 16) creating digital fingerprints of databases, by configuring the system's connection to the database, to create digital fingerprints of certain fields of selected tables in order to subsequently detect information leakage from this database (for example, when simultaneously detecting personal data from a bunch of fields "FULL name + passport data"); 17) creation and updating of digital fingerprints of databases is performed without intermediate actions, such as uploading the database to the source file of the digital fingerprint. When changes are made to the database, the system automatically updates the corresponding digital fingerprints. <p>4.2. Attribute analysis:</p> <p>Attribute analysis of data should include:</p> <ol style="list-style-type: none"> 1) analyze document attributes such as "document name", "email recipient address", "user", "IM client account", "date", "time", "day of the week", "size", "data type", "computer, domain", "IP address", etc. 2) analysis of document attributes based on statuses, such as sending a document over a secure protocol, an encrypted or protected document
---	---	--

<p>foydalanish va moslashtirilgan iboralarni yaratish qobiliyati;</p> <p>8) to'lov tizimining ma'lumotlar bazasiga nisbatan bank kartalari raqamlarini tekshirishdan keyingi mexanizm ;</p> <p>9) morfologiyani hisobga olgan holda tematik lug'atlardan qidirish (o'chirib qo'yish mumkin) va lug'atlardagi niqoblar va oddiy iboralarni qo'llab-quvvatlash, tetik chegarasini sozlash imkoniyati (masalan, lug'atdagi 10 ta so'z yoki iboradan 3 tasi aniqlanganda).);</p> <p>10) ushlangan ma'lumotlarda shunga o'xshash hujjatlarni keyinchalik aniqlash uchun hujjatlar yoki hujjatlar bilan papkalarining raqamli barmoq izlarini yaratish - ushlangan hujjatning asl nusxaga muvofiqligi foizini ko'rsatish imkoniyati bilan);</p> <p>11) oldindan o'rnatilgan lug'atlardan foydalanish va shaxsiy lug'atlarni yaratish qobiliyati;</p> <p>12) ushlangan hujjatning asl nusxaga mos kelishi foizini ko'rsatish qobiliyatiga ega hujjatlarning raqamli barmoq izlaridan foydalangan holda qidiruv texnologiyasi;</p> <p>13) to'g'ridan-to'g'ri, teskari yoki eng katta hodisani tanlash qobiliyatiga ega hujjatlarning raqamli barmoq izlaridan foydalangan holda qidiruv texnologiyasi;</p> <p>14) raqamli barmoq izlari bankini hujjatlar joylashgan papkalar bilan sinxronlashtirish, yangilanish oralig'ini sozlash imkoniyati</p> <p>15) CSV fayllarining raqamli barmoq izlarini yaratish, ma'lumotlar bankiga qo'shish uchun muhim ma'lumotlarga ega maydonlarni tanlash;</p> <p>16) ma'lumotlar bazalarining raqamli barmoq izlarini yaratish, ma'lumotlar bazasiga tizim ulanishini o'rnatish orqali ushbu ma'lumotlar bazasidan ma'lumotlarning sizib chiqishini keyinchalik aniqlash maqsadida tanlangan jadvallarning ma'lum</p>	<p>данных система автоматически обновляет соответствующие цифровые отпечатки.</p> <p>4.2. Атрибутивный анализ: Атрибутивный анализ данных должен включать в себя:</p> <p>1) анализ атрибутов документов, таких как «имя документа», «адрес получателя электронной почты», «пользователь», «учетная запись ИМ-клиента», «дата», «время», «день недели», «размер», «тип данных», «компьютер», «домен», «IP-адрес» и др.;</p> <p>2) анализ атрибутов документа по статусам, таким как пересылка документа по защищенному протоколу, шифрованного или защищенного документа, поврежденных данных, отправка вызвавших блокирование данных либо переданных в индивидуальном порядке данных и др.;</p> <p>3) анализ атрибутов процессов, таких как: имя исполняющего файла, полный путь к файлу, заголовок окна процесса и др.;</p> <p>4) анализ атрибутов перехваченной почты, таких как: отправитель, получатель, число получатель, заголовка письма и др.;</p> <p>5) анализ атрибутов перехваченной переписки в мессенджерах, таких как: локальный идентификатор пользователя, удаленный идентификатор пользователя, число сообщений, тип данных, и др.;</p> <p>6) анализ атрибутов контролируемых устройств, таких как: название устройства, производитель, тип устройства, идентификатор производителя, идентификатор продукта, тип устройства, серийный номер и др.;</p> <p>7) анализ атрибутов печати, таких как: тип документа, название принтера, число распечатанных страниц и др.;</p> <p>4.3. Распознавание изображений: Система должна обеспечивать возможность извлечения текстовой информации из файлов графических форматов (BMP, JPEG, PNG, TIFF, GIF и другие), а также из файлов</p>	<p>damaged data, sending blocked data or individually transmitted data, etc.;</p> <p>3) analysis of process attributes, such as: executable file name, full path to the file, process window title, etc.;</p> <p>4) analysis of intercepted mail attributes, such as: sender, recipient, recipient number, email header, etc.</p> <p>5) analysis of the attributes of intercepted correspondence in instant messengers, such as: local user ID, remote user ID, number of messages, data type, etc.</p> <p>6) analysis of attributes of controlled devices, such as: device name, manufacturer, device type, manufacturer ID, product ID, device type, serial number, etc.</p> <p>7) analysis of print attributes, such as: document type, printer name, number of pages printed, etc.</p> <p>4.3. Image recognition: The system should provide the ability to extract text information from image files (BMP, JPEG, PNG, TIFF, GIF, etc.), as well as from PDF, DjVu, and OXPS files by optical character recognition (OCR). You should be able to apply all the appropriate contextual and attribute analysis tools to the extracted text.</p> <p>4.4. Print recognition: The system should provide the ability to detect seals on images based on the specified standards. You should be able to apply all the appropriate attribute analysis tools to the detected seals.</p> <p>4.5. Statistical analysis: You should be able to set up automatic notifications about the achievement of certain indicators within a certain time (hour, day, week, or any other interval):</p>
---	--	---



maydonlarining raqamli barmoq izlarini yaratish (masalan, bir vaqtning o'zida shaxsiy ma'lumotlar kombinatsiyasidan shaxsiy ma'lumotlarni aniqlashda). maydonlar "Ism + pasport ma'lumotlari");

17) ma'lumotlar bazalarining raqamli barmoq izlarini yaratish va yangilash ma'lumotlar bazasini raqamli barmoq izining manba fayliga yuklash kabi oraliq harakatlarsiz amalga oshiriladi. Ma'lumotlar bazasiga o'zgartirishlar kiritilganda tizim avtomatik ravishda tegishli raqamli barmoq izlarini yangilaydi.

4.2. Atributlarni tahlil qilish:

Atribut ma'lumotlarini tahlil qilish quyidagilarni o'z ichiga olishi kerak:

- 1) "hujjat nomi", "qabul qiluvchining elektron manzili", "foydalanuvchi", "IM mijoz hisobi", "sana", "vaqt", "hafta kuni", "hajmi", "ma'lumotlar turi" kabi hujjat atributlarini tahlil qilish. , "kompyuter", "domen", "IP manzil" va boshqalar;
- 2) hujjatni xavfsiz protokol, shifrlangan yoki himoyalangan hujjat, shikastlangan ma'lumotlar, blokirovkaga sabab bo'lgan yoki alohida uzatilgan ma'lumotlarni jo'natish va hokazolar orqali hujjatni jo'natish kabi holat bo'yicha hujjat atributlarini tahlil qilish;
- 3) jarayon atributlarini tahlil qilish, masalan: bajaruvchi fayl nomi, faylga to'liq yo'l, jarayon oynasining sarlavhasi va boshqalar;
- 4) ushlangan pochta atributlarini tahlil qilish, masalan: jo'natuvchi, qabul qiluvchi, oluvchi raqami, xat sarlavhasi va boshqalar ;
- 5) messengerlarda ushlangan yozishmalarning atributlarini tahlil qilish, masalan: mahalliy foydalanuvchi identifikatori, masofaviy foydalanuvchi identifikatori, xabarlar soni, ma'lumotlar turi va boshqalar ;
- 6) boshqariladigan qurilmalarning atributlarini

формата PDF, DjVu, OXPS путем оптического распознавания символов (OCR);

К извлеченному тексту должна быть возможность применять все соответствующие инструменты контекстного и атрибутивного анализа.

4.4. Распознавание печатей:

Система должна обеспечивать возможность обнаружения печатей на изображениях по заданным эталонам.

К обнаруженным печатям должна быть возможность применять все соответствующие инструменты атрибутивного анализа.

4.5. Статистический анализ:

Должна быть предусмотрена возможность настройки автоматических уведомлений о достижении определенных показателей в течение определенного времени (час, день, неделя, произвольный интервал):

- 1) количество отправленных/полученных пользователем электронным письмам
- 2) количество переписок/сообщений пользователя
- 3) количество/время звонков пользователя в IM-клиентах (например, «время голосовых переговоров пользователя в IM-клиентах за день превысило 1 час» или «пользователь совершил более 10 звонков за день» и т.д.);
- 4) количество посещенных веб-страниц;
- 5) количество отправленных веб-запросов;
- 6) количество распечатанных страниц/документов на принтерах;
- 7) количество отправленных/полученных файлов
- 8) продолжительность работы в браузерах, том числе на определенных сайтах (например, «Время пребывания пользователя на определенном сайте через браузер превысило 1 час за день» и т.д.);
- 9) продолжительность работы в приложениях, в т.ч. в определенных приложениях (например, «пользователь работал в Microsoft Word в течение более 5 часов за день»

- 1) the number of emails sent/received by the user
 - 2) the number of user correspondences/messages
 - 3) the number/time of user calls in IM clients (for example, "the user's voice conversation time in IM clients exceeded 1 hour per day" or "the user made more than 10 calls per day", etc.);
 - 4) the number of web pages visited;
 - 5) the number of web requests sent.
 - 6) the number of printed pages/documents on printers;
 - 7) number of files sent/received
 - 8) the duration of work in browsers, including on certain sites (for example, "The user's time spent on a certain site through the browser exceeded 1 hour per day" , etc.);
 - 9) the duration of work in applications, including in certain applications (for example, "the user worked in Microsoft Word for more than 5 hours per day" or "the user worked in the Klondike Solitaire app for more than 70% of the working time" , etc.);
 - 10) the duration of active operation/inactivity of the PC, including as a percentage of the total time (for example, "the PC was inactive for more than 3 hours per day", "the start of PC activity was recorded later than 10: 30" , etc.);
- It should be possible to set up automatic notifications about deviations from the norm of the start/end of the working day, from the norm of the duration of active work for the PC "working day duration".

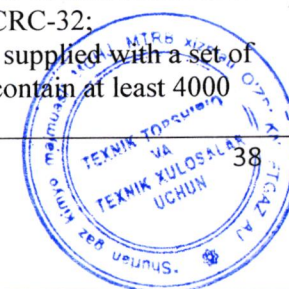
4.6. Event analysis:

Event analysis should have the following features:

- 1) registering the launch or shutdown of a specific application by the user;



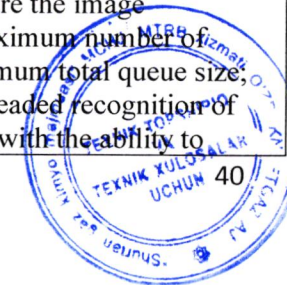
<p>tahlil qilish, masalan: qurilma nomi, ishlab chiqaruvchi, qurilma turi, ishlab chiqaruvchi identifikatori, mahsulot identifikatori, qurilma turi, seriya raqami va boshqalar ;</p> <p>7) bosma atributlarni tahlil qilish, masalan: hujjat turi, printer nomi, chop etilgan sahifalar soni va boshqalar ;</p> <p>4.3. Tasvirni aniqlash: Tizim grafik formatdagi fayllardan (BMP, JPEG, PNG, TIFF, GIF va boshqalar), shuningdek, optik belgilarni aniqlash (OCR) yordamida PDF, DjVu , OXPS formatidagi fayllardan matnli ma'lumotlarni olish imkoniyatini ta'minlashi kerak; Olingan matnga barcha tegishli kontekst va atributlarni tahlil qilish vositalarini qo'llash imkoniyati bo'lishi kerak.</p> <p>4.4. Markani tanib olish: Tizim belgilangan standartlardan foydalangan holda tasvirlardagi shtamlarni aniqlash qobiliyatini ta'minlashi kerak. Aniqlangan muhrlarga barcha tegishli atributlarni tahlil qilish vositalarini qo'llash mumkin bo'lishi kerak.</p> <p>4.5. Statistik tahlil: Muayyan ko'rsatkichlarga ma'lum vaqt ichida (soat, kun, hafta, o'zboshimchalik bilan) erishilganda avtomatik bildirishnomalarni sozlash mumkin bo'lishi kerak:</p> <p>1) foydalanuvchi tomonidan yuborilgan/qabul qilingan elektron pochta xabarlar soni 2) foydalanuvchi yozishmalari/xabarlar soni 3) IM mijozlaridagi foydalanuvchi qo'ng'iroqlari soni/vahti (masalan, "foydalanuvchining IM mijozlaridagi ovozli suhbat vahti kuniga 1 soatdan oshgan" yoki "foydalanuvchi kuniga 10 dan ortiq qo'ng'iroq qilgan" va boshqalar); 4) tashrif buyurilgan veb-sahifalar soni;</p>	<p>или «пользователь работал в приложении “Пасьянс Косынка” в течение более 70% рабочего времени» и т.д.);</p> <p>10) продолжительность активной работы/бездействия ПК, в том числе в процентах от общего времени (например, «ПК бездействовал в течение более 3 часов за день», «начало активности ПК зафиксировано позже 10:30» и т.д.);</p> <p>Должна быть предусмотрена возможность настройки автоматических уведомлений об отклонении от нормы начала/окончания рабочего, от нормы продолжительности активной работы за ПК «продолжительность рабочего дня».</p> <p>4.6. Событийный анализ: Событийный анализ должен обладать следующими возможностями:</p> <p>1) регистрация запуска, завершения работы пользователем определенного приложения;</p> <p>2) обнаружение пересылки зашифрованного вложения (например, защищенный паролем документ MS Office или архив);</p> <p>3) копирование файлов с контролируемых компьютеров на внешние накопители, облачные хранилища и сетевые диски с определенными параметрами;</p> <p>4) подключение и использования на контролируемых рабочих станциях устройств с определенными параметрами;</p> <p>5) посещение определенных web-ресурсов;</p> <p>6) блокирование пересылки данных по протоколам SMTP, HTTP, MAPI, отправки документов на печать, в том числе по дополнительным атрибутам;</p> <p>7) обнаружение конфиденциальных файлов на компьютерных дисках пользователей;</p> <p>8) выявление факта пересылки документа с измененным расширением (например, при переименовании пользователем файла .doc в .jpg и последующей отправкой, система должна быть в</p>	<p>2) detecting the transfer of an encrypted attachment (for example, a password-protected MS Office document or archive);</p> <p>3) copying files from controlled computers to external drives, cloud storage and network drives with certain parameters;</p> <p>4) connecting and using devices with certain parameters on controlled workstations;</p> <p>5) visiting certain web resources.</p> <p>6) blocking data transmission via SMTP, HTTP, MAPI protocols, sending documents for printing, including additional attributes;</p> <p>7) detection of confidential files on users ' computer disks;</p> <p>8) detection of the fact of sending a document with a modified extension (for example, when the user renames a file .doc in .The system should be able to determine the original file format and extract text from it for content analysis, additionally notifying the responsible employee about the fact of changing the extension).</p> <p>4.7. App Categorization:</p> <p>1) the system should automatically assign applications used by controlled users to categories in accordance with the system settings.</p> <p>2) categorization of applications should take into account the following attributes of applications: hash sum of the executable file, executable file name, product name, application description, application version, company name of the application developer;</p> <p>3) categorization should take into account the following types of hash sums of executable files: MD-5, SHA-1, SHA-256, CRC-32;</p> <p>4) the system must be supplied with a set of system categories (it must contain at least 4000</p>
---	---	---



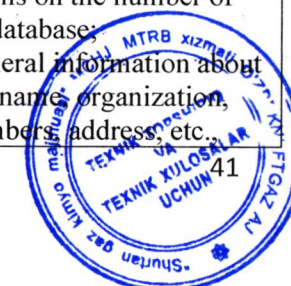
<p>5) yuborilgan veb-so'rovlar soni;</p> <p>6) printerlarda chop etilgan sahifalar/hujjatlar soni;</p> <p>7) yuborilgan/qabul qilingan fayllar soni</p> <p>8) brauzerlarda, shu jumladan ma'lum saytlarda ishlash muddati (masalan, "Foydalanuvchining brauzer orqali ma'lum bir saytda o'tkazgan vaqti kuniga 1 soatdan oshdi" va boshqalar);</p> <p>9) ilovalarda ishlash muddati, shu jumladan ba'zi ilovalarda (masalan, "foydalanuvchi Microsoft - da ishlagan Kuniga 5 soatdan ortiq Word " yoki "foydalanuvchi Solitaire Solitaire ilovasida ish vaqtining 70% dan ko'prog'ida ishlagan" va hokazo);</p> <p>10) Kompyuterning faol ish/harakatsizligi davomiyligi, shu jumladan umumiy vaqtning foiz nisbatida (masalan, "Kompyuter kuniga 3 soatdan ko'proq harakatsiz edi", "Kompyuter faoliyatining boshlanishi 10:30 dan kechroq qayd etilgan". va boshqalar);</p> <p>Ish kunining boshlanishi / tugashi uchun me'yordan yoki shaxsiy kompyuterda "ish kunining davomiyligi" faol ish vaqti uchun me'yordan chetga chiqishlar to'g'risida avtomatik bildirishnomalarni o'rnatish imkoniyati bo'lishi kerak.</p> <p>4.6. Voqea tahlili:</p> <p>Voqealarni tahlil qilish quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) ishga tushirishni ro'yxatdan o'tkazish, ma'lum bir dastur foydalanuvchisi tomonidan ishni yakunlash;</p> <p>2) shifrlangan qo'shimchani uzatilishini aniqlash (masalan, parol bilan himoyalangan MS Office hujjati yoki arxivi);</p> <p>3) fayllarni boshqariladigan kompyuterlardan tashqi diskarga, bulutli xotiraga va ma'lum parametrlarga ega tarmoq drayverlariga nusxalash;</p> <p>4) boshqariladigan ish stantsiyalarida ma'lum parametrlarga ega qurilmalarni ulash va ulardan</p>	<p>состоянии определить оригинальный формат файла и извлечь из него текст для контентного анализа, дополнительно уведомив ответственного сотрудника о самом факте изменения расширения).</p> <p>4.7. Категоризация приложений:</p> <p>1) система должна автоматически относить приложения, используемые контролируемыми пользователями, к категориям в соответствии с настройками системы;</p> <p>2) категоризация приложений должна осуществляться с учетом следующих атрибутов приложений: хеш-сумма исполняемого файла, имя исполняемого файла, имя продукта, описание приложения, версия приложения, имя компании разработчика приложения;</p> <p>3) категоризация должна осуществляться с учетом следующих видов хеш-сумм исполняемых файлов: MD-5, SHA-1, SHA-256, CRC-32;</p> <p>4) с системой должен поставляться набор системных категорий (должен содержать не менее 4000 приложений), а также предоставляться возможность создавать пользовательские категории;</p> <p>5) должен быть предусмотрен приоритет пользовательских категорий приложений над системными;</p> <p>6) должна быть предоставлена возможность отключения системных категорий приложений.</p> <p>4.8. Категоризация веб-сайтов:</p> <p>1) система должна автоматически относить сайты, посещенные контролируемыми пользователями, к категориям в соответствии с настройками системы;</p> <p>2) категоризация сайтов должна осуществляться с учетом доменной части и пути в адресе перехваченного сайта;</p> <p>3) с системой должен поставляться набор системных категорий (должен содержать не менее 20000 веб-сайтов),</p>	<p>applications), as well as the ability to create custom categories.</p> <p>5) user-defined application categories should be prioritized over system-specific ones.</p> <p>6) it should be possible to disable system categories of applications.</p> <p>4.8. Website categorization:</p> <p>1) the system should automatically assign sites visited by controlled users to categories in accordance with the system settings.</p> <p>2) site categorization should take into account the domain part and the path in the address of the intercepted site.</p> <p>3) the system must be supplied with a set of system categories (must contain at least 20,000 websites), as well as provide the ability to create custom categories;</p> <p>4) user categories of websites should be prioritized over system categories.</p> <p>5) it should be possible to disable system categories of websites.</p> <p>4.9. Productivity of websites and applications:</p> <p>1) the system should allow evaluating the productivity of employees ' working time spent on websites and applications;</p> <p>2) the system should allow you to set one of the available productivity classes for each website/application: productive, unproductive, neutral.</p> <p>3) in a situation where a user is in several groups with different productivity settings, the priority of productivity of sites and applications for this user is as follows: productive – unproductive – neutral</p> <p>4) the system should have pre-installed productivity settings templates for the main</p>
--	---	--



<p>foydalanish;</p> <p>5) muayyan veb- resurslarga tashrif buyurish;</p> <p>6) SMTP, HTTP, MAPI protokollari orqali ma'lumotlarni uzatishni blokirovka qilish, hujjatlarni chop etish uchun yuborish, shu jumladan qo'shimcha atributlar;</p> <p>7) foydalanuvchilarning kompyuter drayverlarida maxfiy fayllarni aniqlash;</p> <p>8) o'zgartirilgan kengaytmali hujjatni yuborish faktini aniqlash (masalan, foydalanuvchi .doc faylining nomini .jpg ga o'zgartirganda va keyin uni yuborganda, tizim asl fayl formatini aniqlay olishi va kontentni tahlil qilish uchun undan matn chiqarib olishi kerak. , qo'shimcha ravishda mas'ul xodimni kengaytmani o'zgartirish haqiqati haqida xabardor qilish).</p> <p>4.7. Turkumlashtirish ilovalar :</p> <p>1) tizim boshqariladigan foydalanuvchilar tomonidan ishlatiladigan ilovalarni tizim sozlamalariga muvofiq avtomatik ravishda toifalarga ajratishi kerak;</p> <p>2) Ilovalarni turkumlash quyidagi ilova atributlarini hisobga olgan holda amalga oshirilishi kerak: bajariladigan faylning xeshi, bajariladigan fayl nomi, mahsulot nomi, ilova tavsifi, ilova versiyasi, dastur ishlab chiqaruvchi kompaniya nomi;</p> <p>3) toifalarga ajratish bajariladigan fayllarning quyidagi turdagi xesh summalarini hisobga olgan holda amalga oshirilishi kerak: MD-5, SHA-1, SHA-256, CRC-32;</p> <p>4) tizim tizim toifalari to'plami bilan ta'minlangan bo'lishi kerak (kamida 4000 ta ilova bo'lishi kerak), shuningdek, maxsus toifalarni yaratish imkoniyati bilan ta'minlanishi kerak;</p> <p>5) foydalanuvchi ilovalari toifalariga tizimli ilovalardan ustunlik berilishi kerak;</p> <p>6) Tizim ilovalari toifalarini o'chirish imkoniyati</p>	<p>а также предоставлять возможность создавать пользовательские категории;</p> <p>4) должен быть предусмотрен приоритет пользовательских категорий веб-сайтов над системными;</p> <p>5) должна быть предоставлена возможность отключения системных категорий веб-сайтов.</p> <p>4.9. Продуктивность веб-сайтов и приложений:</p> <p>1) система должна позволять оценивать продуктивность использования рабочего времени сотрудниками, которое они проводят на веб-сайтах и при работе в приложениях;</p> <p>2) система должна позволять устанавливать для каждого веб-сайта/приложения один из доступных классов продуктивности: продуктивно, непродуктивно, нейтрально.</p> <p>3) в ситуации, когда пользователь находится в нескольких группах с разными настройками продуктивности приоритет продуктивности сайтов и приложений для этого пользователя следующий: продуктивно – непродуктивно – нейтрально</p> <p>4) система должна иметь предустановленные шаблоны настроек продуктивности для основных отделов/подразделений, с возможностью их дальнейшего редактирования</p> <p>5) система должна позволять создавать пользовательские шаблоны настроек продуктивности для основных отделов/подразделений, с возможностью их дальнейшего редактирования</p> <p>5. Требования к распознаванию изображений:</p> <p>Система должна иметь встроенное средство распознавания изображений: Tesseract.</p> <p>Система должна иметь модуль предварительного анализа схожести изображений с документами, который позволяет снизить нагрузку на сервер распознавания, отправляя на распознавание только файлы, похожие на документы.</p>	<p>departments/divisions, with the possibility of further editing them</p> <p>5) the system should allow you to create custom templates for productivity settings for the main departments/divisions, with the possibility of further editing them</p> <p>5. Requirements for image recognition:</p> <p>The system must have a built-in image recognition tool: Tesseract.</p> <p>The system must have a module for preliminary analysis of image similarity with documents, which can reduce the load on the speech recognition server by sending only files that are similar to documents for recognition.</p> <p>The system allows you to set a minimum threshold for image similarity with a document in the interface, before which documents are not sent to the speech recognition server.</p> <p>The system should be able to analyze the text content of graphic data using OCR technology and have the following capabilities:</p> <p>1) the ability to extract text information from image files (BMP, JPEG, PNG, TIFF, GIF, etc.), as well as from PDF, DjVu, and OXPS files by optical character recognition (OCR);</p> <p>2) the ability to detect seals on images based on specified standards;</p> <p>3) the ability to work on the extracted search text using contextual and attribute analysis tools;</p> <p>4) the ability to perform a search based on the detected seals using attribute analysis tools;</p> <p>5) the ability to configure the image recognition queue by the maximum number of items in the queue, the maximum total queue size;</p> <p>6) support for multi-threaded recognition of prints and text from images, with the ability to</p>
--	--	---



<p>ta'minlanishi kerak.</p> <p>4.8. Turkumlashtirish veb-saytlar :</p> <p>1) tizim nazorat ostidagi foydalanuvchilar tashrif buyuradigan saytlarni tizim sozlamalariga muvofiq avtomatik ravishda toifalarga ajratishi kerak;</p> <p>2) saytlarni toifalash domen qismi va ushlangan sayt manzilidagi yo'lni hisobga olgan holda amalga oshirilishi kerak;</p> <p>3) tizim toifalari to'plamiga ega bo'lishi kerak (kamida 20 000 veb-saytni o'z ichiga olishi kerak), shuningdek, maxsus toifalarni yaratish imkoniyatini ta'minlashi kerak;</p> <p>4) tizimli saytlardan foydalanuvchi toifalariga ustunlik berish kerak;</p> <p>5) Tizim veb-saytlari toifalarini o'chirish imkoniyati bo'lishi kerak.</p> <p>4.9. Veb-sayt va ilovalar samaradorligi:</p> <p>1) tizim xodimlarning veb-saytlarda va ilovalarda ishlashda sarflagan vaqtlari samaradorligini baholashga imkon berishi kerak;</p> <p>2) tizim har bir veb-sayt/ilova uchun mavjud mahsuldorlik sinflaridan birini belgilashga imkon berishi kerak: samarali, samarasiz, neytral.</p> <p>3) Agar foydalanuvchi turli xil mahsuldorlik sozlamalariga ega bo'lgan bir nechta guruhlarda bo'lsa, ushbu foydalanuvchi uchun saytlar va ilovalarning unumdorligi ustuvorligi quyidagicha: samarali - samarasiz - neytral</p> <p>4) tizimda asosiy bo'limlar/bo'limlar uchun oldindan o'rnatilgan mahsuldorlik sozlamalari shablonlari bo'lishi kerak, ularni keyinchalik tahrirlash imkoniyati mavjud.</p> <p>5) tizim sizga asosiy bo'limlar/bo'limlar uchun mahsuldorlik sozlamalari shablonlarini yaratishga imkon berishi kerak, bunda ularni keyingi tahrirlash imkoniyati mavjud.</p>	<p>Система позволяет настраивать в интерфейсе минимальный порог схожести изображения с документом, до достижения которого, документы не отправляются на сервер распознавания.</p> <p>Система должна позволять осуществлять анализ текстового содержимого графических данных при помощи технологии OCR и обладать следующими возможностями:</p> <p>1) возможность извлечения текстовой информации из файлов графических форматов (BMP, JPEG, PNG, TIFF, GIF и другие), а также из файлов формата PDF, DjVu, OXPS путем оптического распознавания символов (OCR);</p> <p>2) возможность обнаружения печатей на изображениях по заданным эталонам;</p> <p>3) возможность произведения по извлеченному тексту поиска с использованием инструментов контекстного и атрибутивного анализа;</p> <p>4) возможность произведения по обнаруженным печатям поиска с использованием инструментов атрибутивного анализа;</p> <p>5) возможность настройки очереди распознавания изображений по максимальному числу элементов в очереди, максимальному общему размеру очереди;</p> <p>6) поддержка многопоточного распознавания печатей и текста из изображений, с возможностью выбора числа потоков для обработки печатей и числа потоков для обработки текста;</p> <p>7) возможность настройки максимального времени распознавания одного документа;</p> <p>8) возможность настройки области (количество первых страниц) распознавания в многостраничных документах.</p> <p>9) отображение статистики по загрузке процессора, использованию оперативной памяти, по общему количеству обработанных документов, количеству</p>	<p>select the number of threads for printing processing and the number of threads for text processing;</p> <p>7) the ability to set the maximum recognition time for a single document.</p> <p>8) ability to configure the recognition area (number of first pages) in multi-page documents.</p> <p>9) display statistics on processor load, RAM usage, the total number of processed documents, the number of documents in processing, documents in the queue, the number of documents recognized with errors</p> <p>10) for recognizing files with image defects, it should be possible to fine-tune the recognition tools (loading images in 8-bit and 24-bit modes, the ability to automatically apply binarization depending on the degree of damage to the document, fine-tuning binarization, including choosing the binarization threshold, defect filtering settings).</p> <p>6. Management requirements for controlled users: The management of controlled users should include:</p> <p>1) creation of internal user cards containing all the identification information of controlled users;</p> <p>2) the ability to create user cards without allocating licenses for the corresponding users, for example, creating a card for an external user in order to track their communication with internal subscribers; in case of dismissal of an employee, the ability to save the user's card for monitoring their subsequent communication with the company's employees;</p> <p>3) there are no restrictions on the number of user profiles in the program database;</p> <p>4) the ability to link general information about the user to the user card: full name, organization, division, position, phone numbers, address, etc.</p>
---	---	--



5. Tasvirni tanib olish uchun talablar:

Tizimda o'rnatilgan tasvirni aniqlash vositasi bo'lishi kerak: Tesseract .

Tizimda hujjatlar bilan tasvirlarning o'xshashligini dastlabki tahlil qilish moduli bo'lishi kerak, bu faqat hujjatlarga o'xshash fayllarni tanib olish uchun yuborish orqali tanib olish serveriga yukni kamaytirish imkonini beradi.

Tizim interfeysda rasm va hujjat o'rtasidagi o'xshashlikning minimal chegarasini sozlash imkonini beradi, bunga erishgunga qadar hujjatlar tanib olish serveriga yuborilmaydi.

Tizim OCR texnologiyasidan foydalangan holda grafik ma'lumotlarning matn tarkibini tahlil qilish imkonini berishi va quyidagi imkoniyatlarga ega bo'lishi kerak:

1) grafik formatdagi fayllardan (BMP, JPEG, PNG, TIFF, GIF va boshqalar), shuningdek, belgilarni optik aniqlash (OCR) yordamida PDF, DjVu , OXPS formatidagi fayllardan matn ma'lumotlarini olish imkoniyati;

2) belgilangan standartlardan foydalangan holda tasvirlardagi shtamlarni aniqlash qobiliyati;

3) kontekst va atributlarni tahlil qilish vositalaridan foydalangan holda olingan matn bo'yicha qidiruvni amalga oshirish qobiliyati;

4) atributlarni tahlil qilish vositalaridan foydalangan holda aniqlangan shtamlarni qidirish qobiliyati;

5) tasvirni aniqlash navbatini navbatdagi elementlarning maksimal soni, maksimal umumiy navbat hajmi bo'yicha sozlash imkoniyati;

6) shtamlarni va tasvirlardan matnni ko'p bosqichli tanib olishni qo'llab-quvvatlash, shtamlarni qayta ishlash uchun iplar sonini va matnni qayta ishlash uchun iplar sonini tanlash imkoniyati bilan;

документов в обработке, документов в очереди, количеству распознанных с ошибками документов

10) для распознавания файлов с дефектами изображений должна быть предусмотрена возможность тонкой настройки средств распознавания (загрузка изображений в 8-битном и 24-битном режимах, возможность автоматического применения бинаризации в зависимости от степени повреждения документа, тонкие настройки бинаризации, в т.ч. выбор порога бинаризации, настройки фильтрации дефектов).

6. Требования к управлению контролируемых пользователей:

Управление контролируемыми пользователями должно предусматривать:

1) создание внутренних карточек пользователей, содержащих всю идентификационную информацию контролируемых пользователей;

2) возможность создания пользовательских карточек без выделения лицензий на соответствующих пользователей, например, создание карточки для внешнего пользователя с целью отслеживания его общения с внутренними абонентами; в случае увольнения сотрудника – возможность сохранения карточки пользователя для контроля его последующего общения с сотрудниками компании;

3) отсутствие ограничений по количеству профилей пользователей в базе программы;

4) возможность привязки к пользовательской карточке общей информации о пользователе: ФИО, организация, подразделение, должность, телефоны, адрес и др.,

5) возможность автоматической привязки к карточке данных пользователя из Active Directory (адреса электронной почты, названия организации, подразделения и должности пользователя, описания и фотографии пользователя);

5) the ability to automatically link user data from Active Directory to the card (email addresses, organization names, divisions and positions of the user, descriptions and photos of the user);

6) ability to display information from arbitrary fields of the corresponding Active Directory user in the user card

7) the ability to authenticate users working with the system based on internal accounts (with a request for the user's name and password when logging in);

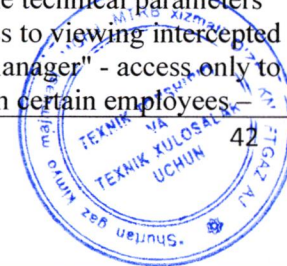
8) the ability to automatically link user identification data (used Slack IDs, ICQ numbers, Google Hangouts, Skype, Telegram, Viber, WhatsApp, Yahoo accounts, social web network IDs, SIP, email addresses, including XMPP and Microsoft Lync accounts, as well as IP addresses and photos), to the user's profile for subsequent identification.

9) the ability to select the types of contact information that will be automatically linked to the user's card

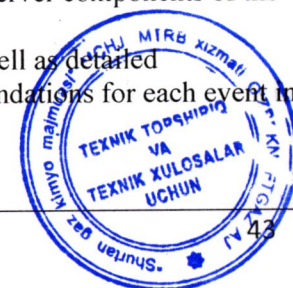
10) the ability to exclude certain users from the process of automatic binding of contact information

11) the ability to exclude certain information (IP address, email address, computer name, Skype, ICQ, Viber, Telegram, WhatsApp, MS Exchange, social network ID) from the automatic binding of contact information

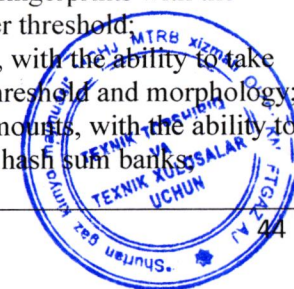
12) the ability to differentiate access rights to both individual system components and intercepted data of individual users for different groups with assigned roles (for example, "system administrator" - access only to changing the technical parameters of the system-without access to viewing intercepted information; "department manager" - access only to viewing activity information certain employees -



<p>7) bitta hujjat uchun maksimal tanib olish vaqtini sozlash imkoniyati;</p> <p>8) ko'p sahifali hujjatlarda tanib olish maydonini (birinchi sahifalar soni) sozlash qobiliyati.</p> <p>9) protsessor yuklanishi, operativ xotiradan foydalanish, qayta ishlangan hujjatlarning umumiy soni, ishlov berishdagi hujjatlar soni, navbatdagi hujjatlar, xatolik bilan tan olingan hujjatlar soni bo'yicha statistikasi ko'rsatish</p> <p>10) 24-bit rejimlarda yuklash, hujjatning shikastlanish darajasiga qarab avtomatik ravishda binarizatsiyani qo'llash qobiliyati, binarizatsiyani nozik sozlash) mumkin bo'lishi kerak. , shu jumladan binarizatsiya chegarasini tanlash , nuqsonlarni filtrlash sozlamalari).</p> <p>6. Boshqariladigan foydalanuvchilarni boshqarishga qo'yiladigan talablar:</p> <p>Boshqariladigan foydalanuvchi boshqaruvi quyidagilarni o'z ichiga olishi kerak:</p> <p>1) nazorat qilinadigan foydalanuvchilarning barcha identifikatsiya ma'lumotlarini o'z ichiga olgan ichki foydalanuvchi kartalarini yaratish;</p> <p>2) tegishli foydalanuvchilarga litsenziyalar bermasdan foydalanuvchi kartalarini yaratish imkoniyati, masalan, ichki abonentlar bilan aloqasini kuzatish uchun tashqi foydalanuvchi uchun karta yaratish; xodim ishdan bo'shatilgan taqdirda, uning kompaniya xodimlari bilan keyingi muloqotini nazorat qilish uchun foydalanuvchi kartasini saqlash imkoniyati;</p> <p>3) dastur ma'lumotlar bazasida foydalanuvchi profillari soni bo'yicha cheklovlar yo'q;</p> <p>4) foydalanuvchi haqidagi umumiy ma'lumotlarni foydalanuvchi kartasiga bog'lash imkoniyati: to'liq ism, tashkilot, bo'linma, lavozim, telefon raqamlari, manzili va boshqalar,</p> <p>5) Foydalanuvchining ma'lumotlar kartasiga</p>	<p>6) возможность отображения в карточке пользователя информации из произвольных полей соответствующего пользователя Active Directory</p> <p>7) возможность аутентификации пользователей, работающих с системой, на основании внутренних учетных записей (с запросом имени и пароля пользователя при входе в систему);</p> <p>8) возможность автоматической привязки идентификационных данных пользователя (используемые идентификаторы Slack, номера ICQ, учетные записи Google Hangouts, Skype, Telegram, Viber, WhatsApp, Yahoo, ID социальных веб-сетей, SIP, адреса электронной почты, включая учетные записи XMPP и Microsoft Lync, а также IP-адреса и фотографии), к профилю пользователя для последующей идентификации;</p> <p>9) возможность выбора типов контактной информации, которая будет автоматически привязываться к карточке пользователя</p> <p>10) возможность исключения определенных пользователей из процесса автоматической привязки контактной информации</p> <p>11) возможность исключения определенной информации (IP-адрес, адрес электронной почты, имя компьютера, учетные записи Skype, ICQ, Viber, Telegram, WhatsApp, MS Exchange, ID социальной сети) из процесса автоматической привязки контактной информации</p> <p>12) возможность разграничения прав доступа как к отдельным компонентам системы, так и к перехваченным данным отдельных пользователей для различных групп с назначением ролей (например, «системный администратор»- доступ только к изменению технических параметров системы – без доступа к просмотру перехваченной информации; «руководитель подразделения»– доступ только к просмотру информации об активности определенных сотрудников – без доступа к просмотру информации об инцидентах или об активности</p>	<p>without access to viewing information about incidents or other employees 'activity;" security officer " – access only to security policies and incidents-without access to viewing information about employee activity, etc.) using a user authentication system;</p> <p>13) the ability to integrate with Active Directory indicating the domains (domain objects) and domain controllers with which synchronization will be performed;</p> <p>14) sync Active Directory users with the ability. automatic creation and deletion of user cards, when adding and deleting records in Active Directory, with automatic creation of cards when previously unknown user information is detected;</p> <p>15) automatic synchronization of changes in user identification data in Active Directory with data in user cards with the ability to configure the synchronization schedule and synchronized data;</p> <p>16) logging of actions and authorization of users working with the system.</p> <p>7. System health monitoring requirements: Health monitoring should allow you to monitor the state of the system in real time. At the same time, provide the following features:</p> <p>1) a system health monitoring dashboard, which provides basic information about the operation of all major components of the system, as well as the use of hardware resources</p> <p>2) event logging of server components of the system;</p> <p>3) view the log, as well as detailed information and recommendations for each event in the admin console;</p>
--	--	---



<p>Active -dan avtomatik ravishda ulanish imkoniyati Katalog (elektron pochta manzillari, tashkilot nomlari, bo'limlar va foydalanuvchi pozitsiyalari, foydalanuvchi tavsiflari va fotosuratlari);</p> <p>6) faol foydalanuvchining shaxsiy maydonlaridan ma'lumotlarni ko'rsatish imkoniyati Katalog</p> <p>7) ichki hisoblar asosida tizim bilan ishlaydigan foydalanuvchilarni autentifikatsiya qilish imkoniyati (tizimga kirishda foydalanuvchi nomi va parolni so'rash bilan);</p> <p>8) foydalanuvchi identifikatsiya ma'lumotlarini avtomatik ravishda bog'lash qobiliyati (ishlatilgan Slack identifikatorlari, ICQ raqamlari, Google hisoblari Hangouts , Skype , Telegram , Viber , WhatsApp , Yahoo , ijtimoiy veb identifikatorlari, SIP, elektron pochta manzillari, shu jumladan XMPP va Microsoft hisoblari Lync , shuningdek IP manzillar va fotosuratlar), keyingi identifikatsiya qilish uchun foydalanuvchi profiliga;</p> <p>9) foydalanuvchi kartasiga avtomatik ravishda bog'lanadigan aloqa ma'lumotlari turlarini tanlash imkoniyati</p> <p>10) muayyan foydalanuvchilarni kontakt ma'lumotlarini avtomatik ravishda ulash jarayonidan chiqarib tashlash qobiliyati</p> <p>11) Skype , ICQ, Viber , Telegram , WhatsApp , MS Exchange , ijtimoiy tarmoq identifikatorlari hisoblari) kontakt ma'lumotlarini avtomatik ravishda bog'lash jarayonidan chiqarib tashlash qobiliyati</p> <p>12) Rollarni tayinlash bilan tizimning alohida komponentlariga ham, turli guruhlar uchun alohida foydalanuvchilarning ushlangan ma'lumotlariga kirish huquqlarini farqlash qobiliyati (masalan, "tizim ma'muri" - faqat tizimning texnik parametrlarini o'zgartirishga kirish - ruxsatsiz ushlangan ma'lumotlarni ko'rish "bo'lim boshlig'i" - faqat ayrim</p>	<p>других сотрудников; «офицер безопасности»— доступ только к политикам безопасности и инцидентам – без доступа к просмотру информации об активности сотрудников, и т.п.) с использованием системы аутентификации пользователей;</p> <p>13) возможность интеграции с Active Directory с указанием доменов (объектов доменов) и контроллеров доменов, с которыми будет выполняться синхронизация;</p> <p>14) синхронизацию пользователей Active Directory с возможностью автоматического создания и удаления карточек пользователей, при добавлении и удалении записей в Active Directory, с автоматическим создание карточек при обнаружении ранее неизвестной пользовательской информации;</p> <p>15) автоматическую синхронизацию изменений идентификационных данных пользователей в Active Directory с данным в карточках пользователей возможностью настройки расписания синхронизации и синхронизируемых данных;</p> <p>16) ведение журнала действий и авторизации пользователей, работающих с системой.</p> <p>7. Требования к мониторингу работоспособности системы:</p> <p>Мониторинг работоспособности должен позволять контролировать состояние системы в режиме реального времени. При этом обеспечивать следующие возможности:</p> <p>1) панель мониторинга работоспособности системы, на которой представлена основная информация о работе всех основных компонентов системы, а также использовании ресурсов оборудования</p> <p>2) ведение журнала событий серверных компонентов системы;</p> <p>3) просмотр журнала, а также детальной информации и рекомендаций по каждому событию в консоли администратора;</p>	<p>4) filtering events in the log by date, event level (information, warning, error), server component, event source;</p> <p>5) selecting specific event source servers for monitoring;</p> <p>6) automatic clearing of the log by event retention period and level;</p> <p>7) Ability to export the event log in PDF, XPS, CSV, XLS, XLSX, HTML, RTF, TXT formats</p> <p>8) ability to print the event log;</p> <p>9) automatic notification of the system administrator about new events of server components by mail;</p> <p>10) configure the rules for sending notifications by mail (selecting the destination, server component, event level, or specific events).</p> <p>8. Requirements for information retrieval:</p> <p>Information search tools should allow you to create highly detailed search queries. The system should provide the following features:</p> <p>1) search for information based on intercepted data using all available analysis tools: content analysis, attribute analysis, search by recognized images, prints, event analysis, etc.;</p> <p>2) search for information by Active Directory groups as well;</p> <p>3) search for information by site and app categories</p> <p>4) search by digital fingerprints with the ability to adjust the trigger threshold;</p> <p>5) dictionary search, with the ability to take into account the trigger threshold and morphology;</p> <p>6) search by hash amounts, with the ability to search by pre-configured hash sum banks.</p>
---	--	--



xodimlarning faoliyati to'g'risidagi ma'lumotlarni ko'rish - hodisalar yoki boshqa xodimlarning faoliyati to'g'risidagi ma'lumotlarni ko'rish imkoniyatisiz - faqat xavfsizlik siyosati va hodisalar - xodimlarning faoliyati to'g'risidagi ma'lumotlarni ko'rish imkoniyatisiz va hokazo. .) foydalanuvchi autentifikatsiya tizimidan foydalangan holda;

13) Active bilan integratsiya qilish imkoniyati Sinxronizatsiya amalga oshiriladigan domenlar (domen ob'ektlari) va domen kontrollerlari ko'rsatilgan katalog ;

14) Faol foydalanuvchi sinxronizatsiyasi Katalog c imkoniyati. Active -ga yozuvlarni qo'shish va o'chirishda foydalanuvchi kartalarini avtomatik yaratish va o'chirish Ilgari noma'lum foydalanuvchi ma'lumotlari aniqlanganda kartalarni avtomatik yaratish bilan katalog ;

15) Foydalanuvchi identifikatoridagi o'zgarishlarni Active -da avtomatik sinxronlashtirish Sinxronizatsiya jadvalini va foydalanuvchi kartalaridagi sinxronlashtirilgan ma'lumotlarni sozlash qobiliyatiga ega katalog ;

16) tizim bilan ishlaydigan foydalanuvchilarning harakatlari va ruxsatnomalari jurnalini yuritish.

7. Tizimning ishlashini monitoring qilish uchun talablar:

Salomatlik monitoringi real vaqtda tizimning sog'lig'ini kuzatish imkonini berishi kerak. Shu bilan birga, quyidagi imkoniyatlarni taqdim eting:

- 1) tizimning barcha asosiy komponentlarining ishlashi, shuningdek, asbob-uskunalar resurslaridan foydalanish haqida asosiy ma'lumotlarni taqdim etadigan tizim salomatligi monitoringi paneli
- 2) tizimning server komponentlari hodisalari jurnalini yuritish;
- 3) jurnalni ko'rish, shuningdek, administrator

- 4) фильтрация событий в журнале по дате, уровню события (информация, предупреждение, ошибка), серверному компоненту, источнику событий;
- 5) выбор определенных серверов источников событий для ведения мониторинга;
- 6) автоматическая очистка журнала по сроку хранения событий и их уровню;
- 7) возможность экспорта журнала событий в форматах PDF, XPS, CSV, XLS, XLSX, HTML, RTF, TXT
- 8) возможность печати журнала событий;
- 9) автоматическое уведомление администратора системы о новых событиях серверных компонентов по почте;
- 10) настройка правил отправки уведомлений по почте (выбор адресата, серверного компонента, уровня события или конкретных событий).

8. Требования к поиску информации:

Инструменты поиска информации должны позволять создавать поисковые запросы высокой детализации. Система должна предоставлять следующие возможности:

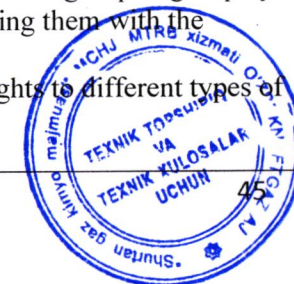
- 1) поиск информации по перехваченным данным с использованием всех доступных инструментов анализа: контентный анализ, атрибутивный анализ, поиск по распознаным изображениям, печатям, событийный анализ и др.;
- 2) поиск информации и по группам Active Directory;
- 3) поиск информации по категориям сайтов и приложений
- 4) поиск по цифровым отпечаткам с возможностью настройки порога срабатывания;
- 5) поиск по словарям, с возможностью учета порога срабатывания и морфологии;
- 6) поиск по хеш-суммам, с возможностью поиска по преднастроенным банкам хеш-сумм;
- 7) поиск информации, содержащей определенные метки конфиденциальности

- 7) search for information that contains certain privacy tags
- 8) combining several simple search terms using the logical operators "AND", "OR", "NOT", with the possibility of combining search terms into groups;
- 9) creating and using search templates – a set of search terms that can be used in other combined search queries;
- 10) add a search term to your favorites for further work;
- 11) import and export of search terms.
- 12) limit the number of search results displayed.

9. Reporting requirements:

The system's reporting module should have the following features:

- 1) creating reports based on data from randomly selected users, user groups, or Active Directory groups.
- 2) creating a report for both the entire period and a specific interval.
- 3) there is a report creation wizard with a brief description of the report's capabilities.
- 4) availability of pre-installed reports.
- 5) create groups and subgroups with at least 20 hierarchy levels.
- 6) transfer reports from group to group by simply dragging and dropping them with the mouse.
- 7) transfer subgroups from group to group by simply dragging and dropping them with the mouse.
- 8) configure access rights to different types of reports

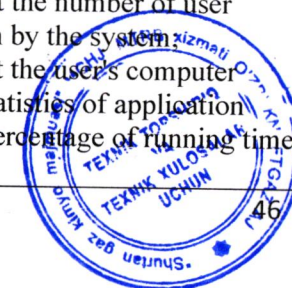


<p>konsolida har bir voqea uchun batafsil ma'lumot va tavsiyalar;</p> <p>4) jurnaldagi hodisalarni sana, hodisa darajasi (ma'lumot, ogohlantirish, xato), server komponenti, voqea manbasi bo'yicha filtrlash;</p> <p>5) monitoring uchun maxsus voqea manba serverlarini tanlash;</p> <p>6) hodisalarni saqlash muddati va ularning darajasiga qarab jurnalni avtomatik tozalash;</p> <p>7) hodisalar jurnalini PDF, XPS, CSV, XLS, XLSX, HTML, RTF, TXT formatlarida eksport qilish imkoniyati</p> <p>8) voqealar jurnalini chop etish imkoniyati;</p> <p>9) pochta orqali server komponentlarining yangi hodisalari haqida tizim ma'murini avtomatik ravishda xabardor qilish;</p> <p>10) pochta orqali bildirishnomalarni jo'natish qoidalarini o'rnatish (qabul qiluvchini, server komponentini, hodisa darajasini yoki muayyan hodisalarni tanlash).</p>	<p>8) комбинирование нескольких простых поисковых условий при помощи логических операторов «И», «ИЛИ», «НЕ», с возможностью объединения поисковых условий в группы;</p> <p>9) создание и использование шаблонов поиска – набора поисковых условий, которые можно использовать в других поисковых запросах комбинированного поиска;</p> <p>10) добавление условия поиска в избранное, для дальнейшей работы;</p> <p>11) импорт и экспорт условий поиска;</p> <p>12) ограничение количества отображаемых результатов поиска.</p> <p>9. Требования к отчетности:</p> <p>Модуль отчетности системы должен обладать следующими возможностями:</p> <p>1) построение отчетов по данным произвольно выбранных пользователей, групп пользователей либо групп Active Directory;</p> <p>2) построение отчета как за весь период, так и за определенный интервал;</p> <p>3) наличие мастера создания отчетов с кратким описанием возможностей отчета;</p> <p>4) наличие предустановленных отчетов;</p> <p>5) создание групп и подгрупп с количеством уровней иерархии не менее 20;</p> <p>6) перенос отчетов из группы в группу простым перетаскиванием «мышью»;</p> <p>7) перенос подгрупп из группы в группу простым перетаскиванием «мышью»;</p> <p>8) настройка прав доступа к различным типам отчетов</p> <p>9) настройка расписания формирования отчетов, а также выбор почтовых адресов для рассылки</p> <p>Все перехваченные данные должны представляться в форме отчетов следующих видов:</p> <p>1) отчет «Активность пользователей»;</p>	<p>9) setting up a report generation schedule, as well as selecting mailing addresses for distribution</p> <p>All intercepted data must be submitted in the form of reports of the following types:</p> <p>1) the "User Activity" report.</p> <p>2) report on users.</p> <p>3) TOP report on users.</p> <p>4) report on security policies;</p> <p>5) summary report on users.</p> <p>6) time sheet report;</p> <p>7) report on app activity.</p> <p>8) report on browser activity.</p> <p>9) report on general user activity</p> <p>9.1. Requirements for the "User activity" report:</p> <p>"User activity" should clearly represent the user's activity on a time grid in 1-hour increments and contain the following data and capabilities:</p> <p>1) information about the number of emails sent and received;</p> <p>2) information about the number of sessions of user correspondence in IM clients, indicating the duration and number of messages in each session of correspondence;</p> <p>3) information about the number of files received and sent by the user via email, IM clients, HTTP(S) and FTP(S) protocols, copied to external devices, network resources, cloud storage, or printed on local / network printers;</p> <p>4) information about the number of URLs visited and search queries sent.</p> <p>5) information about the number of user desktop screenshots taken by the system;</p> <p>6) information about the user's computer up/down time, detailed statistics of application activity and data on the percentage of running time in various applications;</p>
--	--	---

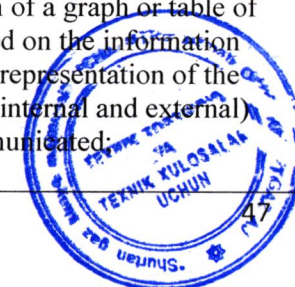
8. Axborot qidirishga qo'yiladigan talablar:

Axborot qidirish vositalari juda batafsil qidiruv so'rovlarini yaratishga imkon berishi kerak. Tizim quyidagi imkoniyatlarni ta'minlashi kerak:

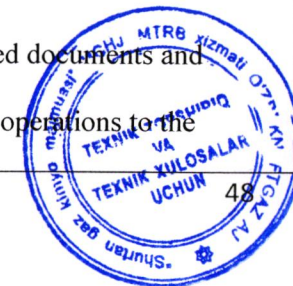
- 1) barcha mavjud tahlil vositalaridan foydalangan holda ushlangan ma'lumotlardan foydalangan holda ma'lumotni qidirish: kontentni tahlil qilish, atributlarni tahlil qilish, tan olingan tasvirlar, muhrlar, voqealar tahlili va boshqalardan foydalangan holda qidirish;
- 2) faol guruhlar bo'yicha qidirish katalog ;
- 3) saytlar va ilovalar toifalari bo'yicha ma'lumot qidirish
- 4) javob chegarasini sozlash imkoniyati bilan raqamli barmoq izlari bo'yicha qidirish;
- 5) javob chegarasi va morfologiyasini hisobga



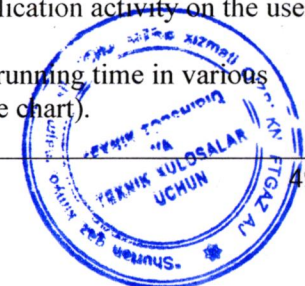
<p>olish qobiliyati bilan lug'atlardan qidirish;</p> <p>6) xesh summalarining oldindan tuzilgan banklari bo'yicha qidirish imkoniyati bilan ;</p> <p>7) maxsus sezgirlik belgilarini o'z ichiga olgan ma'lumotni qidirish</p> <p>8) qidiruv shartlarini guruhlariga birlashtirish imkoniyati bilan "VA", "YOKI", "YO'Q" mantiqiy operatorlari yordamida bir nechta oddiy qidiruv shartlarini birlashtirish;</p> <p>9) qidiruv shablonlarini yaratish va ulardan foydalanish - boshqa qo'shma qidiruv so'rovlarida ishlatilishi mumkin bo'lgan qidiruv so'zlari to'plami;</p> <p>10) keyingi ish uchun sevimlilarga qidirish shartini qo'shish;</p> <p>11) qidiruv so'zlarini import va eksport qilish;</p> <p>12) ko'rsatilgan qidiruv natijalari sonini cheklash.</p>	<p>2) отчет по пользователям;</p> <p>3) ТОП-отчет по пользователям;</p> <p>4) отчет по политикам безопасности;</p> <p>5) сводный отчет по пользователям;</p> <p>6) отчет табель рабочего времени;</p> <p>7) отчет по активности приложений;</p> <p>8) отчет по браузер-активности.</p> <p>9) отчет об общей активности пользователя</p> <p>9.1. Требования к отчету «активность пользователей»:</p> <p>«Активность пользователя» должна наглядно представлять активность пользователя на временной сетке с шагом в 1 час и содержать следующие данные и возможности:</p> <p>1) информация о количестве отправленных и полученных писем;</p> <p>2) информация о количестве сессий переписки пользователя в IM-клиентах с указанием длительности и количества сообщений в каждой сессии переписки;</p> <p>3) информация о количестве файлов, полученных и отправленных пользователем по электронной почте, через IM-клиенты, по протоколам HTTP(S) и FTP(S), скопированных на внешние устройства, сетевые ресурсы, в облачные хранилища или распечатанных на локальных/сетевых принтерах;</p> <p>4) информация о количестве посещенных URL и отправленных поисковых запросов;</p> <p>5) информация о количестве сделанных системой снимков экрана рабочего стола пользователя;</p> <p>6) информация о времени работы/простоя компьютера пользователя, детальная статистика активности приложений и данные о процентном соотношении времени работы в различных приложениях;</p> <p>7) информация о количестве документов, помещенных в буфер обмена;</p> <p>8) информация о посещении веб-сайтов с помощью веб-браузера с предоставлением комплексной и</p>	<p>7) information about the number of documents placed on the clipboard;</p> <p>8) information about visiting websites using a web browser with providing comprehensive and detailed statistics of time spent on various web resources;</p> <p>9) information about the number of characters entered by the user from the keyboard;</p> <p>10) the information should be dynamic and interactive. Clicking on links should lead directly to viewing the contents of intercepted documents or web links.</p> <p>11) it should be possible to save user activity to an external HTML file with support for interactivity of structural elements and access to intercepted data in a web browser. In the advanced save settings, you should be able to select internal storage formats for different document types and influence their display in associated viewers.</p> <p>12) it should be possible to present information in the form of graphs for individual types of information (a graph for sent / received emails, the number of sessions/messages of correspondence in IM clients, the number of files received and sent, the number of URLs visited and web requests);</p> <p>13) graphs by type of information should be interactive and dynamic, to ensure that links (points on the graph) are clicked directly to view the contents of intercepted documents;</p> <p>14) save statistics to an external PDF or XPS file.</p> <p>15) display in the form of a graph or table of the user's relationship based on the information collected on it for a visual representation of the circle of subscribers (both internal and external) with whom this user communicated;</p>
<p>9. Hisobotga qo'yiladigan talablar:</p> <p>Tizim hisoboti moduli quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) faol guruhlar ma'lumotlariga asoslangan hisobotlarni yaratish katalog ;</p> <p>2) butun davr uchun ham, ma'lum bir oralik uchun ham hisobot yaratish;</p> <p>3) hisobot imkoniyatlarining qisqacha tavsifi bilan hisobot yaratish ustasining mavjudligi;</p> <p>4) oldindan o'rnatilgan hisobotlarning mavjudligi;</p> <p>5) kamida 20 ierarxiya darajasiga ega guruhlar va kichik guruhlar yaratish;</p> <p>6) sichqoncha bilan sudrab olib tashlash orqali hisobotlarni guruhdan guruhga o'tkazish;</p> <p>7) oddiygina sichqonchani surish orqali kichik guruhlarini guruhdan guruhga o'tkazish;</p> <p>8) har xil turdagi hisobotlarga kirish huquqini o'rnatish</p> <p>9) hisobotlarni yaratish jadvalini o'rnatish,</p>		



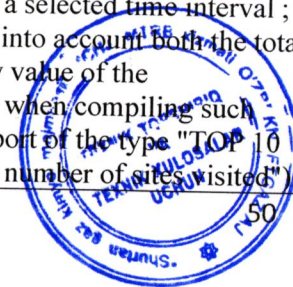
<p>shuningdek, pochta jo'natmalari uchun elektron pochta manzillarini tanlash</p> <p>Barcha ushlangan ma'lumotlar quyidagi turdagi hisobotlarda taqdim etilishi kerak:</p> <ol style="list-style-type: none"> 1) "Foydalanuvchi faoliyati" hisoboti; 2) foydalanuvchi hisoboti; 3) Foydalanuvchilarning TOP hisoboti; 4) xavfsizlik siyosati hisoboti; 5) foydalanuvchilar haqida umumiy hisobot; 6) vaqt jadvali hisoboti; 7) dastur faoliyati to'g'risidagi hisobot; 8) brauzer faoliyati hisoboti. 9) umumiy foydalanuvchi faoliyati hisoboti <p>9.1. "Foydalanuvchi faoliyati" hisobotiga qo'yiladigan talablar:</p> <p>"Foydalanuvchi faoliyati" 1 soatlik bosqichlarda vaqt jadvalidagi foydalanuvchi faoliyatini vizual tarzda aks ettirishi va quyidagi ma'lumotlar va imkoniyatlarni o'z ichiga olishi kerak:</p> <ol style="list-style-type: none"> 1) yuborilgan va qabul qilingan xatlar soni to'g'risidagi ma'lumotlar; 2) har bir yozishma sessiyasidagi xabarlarning davomiyligi va sonini ko'rsatgan holda, IM mijozlaridagi foydalanuvchi yozishmalari seanslari soni to'g'risidagi ma'lumotlar; 3) foydalanuvchi tomonidan elektron pochta orqali, IM mijozlari orqali, HTTP(S) va FTP(S) orqali qabul qilingan va yuborilgan, tashqi qurilmalarga, tarmoq resurslariga, bulutli xotiraga ko'chirilgan yoki mahalliy/tarmoq printerlarida chop etilgan fayllar soni haqidagi ma'lumotlar; 4) tashrif buyirilgan URL manzillar soni va yuborilgan qidiruv so'rovlari haqida ma'lumot; 5) tizim tomonidan olingan foydalanuvchi ish stoli ekranining skrinshotlari soni haqidagi ma'lumot; 6) foydalanuvchi kompyuterining ish vaqti/to'xtab qolish vaqti haqida ma'lumot, ilovalar 	<p>детальной статистики времени, проведенного на различных веб-ресурсах;</p> <ol style="list-style-type: none"> 9) информация о количестве символов, введенных пользователем с клавиатуры; 10) информация должна быть динамическая и интерактивная. Переход по ссылкам должен приводить непосредственно к просмотру содержимого перехваченных документов либо веб-ссылок; 11) должна обеспечиваться возможность сохранения активности пользователя во внешний HTML – файл с поддержкой интерактивности структурных элементов и доступа к перехваченным данным в веб-браузере. В расширенных настройках сохранения должна быть возможность выбора форматов внутреннего хранения разных типов документов и влиять на их отображение в ассоциированных просмотрщиках. 12) должна быть предусмотрена возможность представления информации в виде графиков по отдельным типам информации (график по отправленным/полученным письмам, по количеству сессий/сообщений переписки в IM-клиентах, по количеству полученных и отправленных файлов, количеству посещенных URL и веб-запросов); 13) графики по типам информации должны быть интерактивными и динамическими, для обеспечения перехода по ссылкам (точкам на графике) непосредственно к просмотру содержимого перехваченных документов; 14) сохранение статистики во внешний файл формата PDF или XPS; 15) отображение в виде графа или таблицы взаимосвязи пользователя на основании собранной по нему информации для наглядного представления круга абонентов (как внутренних, так и внешних), с которыми данный пользователь общался; 	<ol style="list-style-type: none"> 16) ability to build a graph of relationships based on intermediate relationships (the number of intermediate relationships is up to 5) 17) support for grouping user contacts by belonging to established and unrecognized contacts. 18) view relationships of an external subscriber with users of the organization's network after preliminary creation of an external user card. 19) selecting the scale of the report display when viewing in the client console (indicating % of the original size). 20) the ability to interactively switch from viewing the relationship diagram to the content of documents (letters, correspondence, files, etc.) that the user exchanged with a specific subscriber. 21) support for saving the relationship report as a graph to an external PNG file. <p>9.2. Requirements for the User Report:</p> <p>The user report should provide the ability to create a summary interactive report for a specific user, as well as for several users, groups of users, or Active Directory groups for the entire time of observation or for a selected time interval.</p> <p>The report should include the following information:</p> <p>Statistics of data interception, including:</p> <ol style="list-style-type: none"> 1) the amount of information transmitted and received by the user through all transmission channels, including mail and instant messengers; 2) the number of sites visited and search queries; 3) the number of files transferred/received via FTP. 4) the number of printed documents and pages; 5) the number of copy operations to the clipboard.
--	--	--



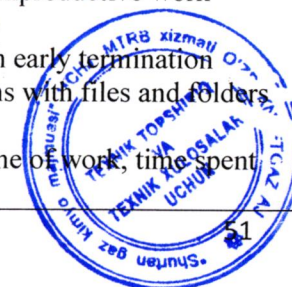
<p>faoliyati to'g'risidagi batafsil statistik ma'lumotlar va turli ilovalardagi ish vaqtining ulushi haqidagi ma'lumotlar;</p> <p>7) buferga joylashtirilgan hujjatlar soni to'g'risidagi ma'lumotlar;</p> <p>8) veb-brauzer yordamida veb-saytlarga tashrif buyurish haqida ma'lumot, turli veb-resurslarga sarflangan vaqtning to'liq va batafsil statistikasini taqdim etish;</p> <p>9) foydalanuvchi tomonidan klaviaturadan kiritilgan belgilar soni haqida ma'lumot;</p> <p>10) axborot dinamik va interaktiv bo'lishi kerak. Havolalarni bosish to'g'ridan-to'g'ri ushlangan hujjatlar yoki veb-havolalar mazmunini ko'rishga olib kelishi kerak;</p> <p>11) Tarkibiy elementlarning interaktivligini va veb-brauzerda ushlangan ma'lumotlarga kirishni qo'llab-quvvatlash bilan foydalanuvchi faoliyatini tashqi HTML fayliga saqlash imkoniyati bo'lishi kerak. Kengaytirilgan saqlash sozlamalarida har xil turdagi hujjatlar uchun ichki xotira formatlarini tanlash va ularning tegishli tomoshabinlarda ko'rinishiga ta'sir qilish imkoniyati bo'lishi kerak .</p> <p>12) ma'lumotni ma'lum turdagi ma'lumotlar uchun grafiklar ko'rinishida taqdim etish imkoniyati bo'lishi kerak (yuborilgan/qabul qilingan xatlar uchun grafik, IM mijozlaridagi yozishmalar/sessiyalar/xabarlar soni, qabul qilingan va yuborilgan fayllar soni, tashrif buyurilgan URL manzillari va veb-so'rovlar);</p> <p>13) ushlangan hujjatlar mazmunini ko'rish uchun havolalar (grafikdagi nuqtalar) to'g'ridan-to'g'ri kuzatilishini ta'minlash uchun axborot turlari bo'yicha grafiklar interaktiv va dinamik bo'lishi kerak;</p> <p>14) statistikani PDF yoki XPS formatida tashqi faylga saqlash;</p> <p>15) ushbu foydalanuvchi muloqot qilgan</p>	<p>16) возможность построения графа взаимосвязей с учетом промежуточных связей (количество промежуточных взаимосвязей до 5)</p> <p>17) поддержка группировки контактов пользователя по принадлежности к установленным и не распознанным контактам.</p> <p>18) просмотр взаимосвязей внешнего абонента с пользователями сети организации после предварительного создания карточки внешнего пользователя.</p> <p>19) выбор масштаба отображения отчета при просмотре в клиентской консоли (с указанием % размера от оригинала).</p> <p>20) возможность интерактивного перехода от просмотра схемы взаимосвязей к содержимому документов (письма, переписки, файлы и т.д.), которыми пользователь обменивался с конкретным абонентом.</p> <p>21) поддержка сохранения отчета о взаимосвязях в виде графа во внешний файл формата PNG.</p> <p>9.2. Требования к отчету по пользователям: Отчет по пользователям должен предоставлять возможность построения сводного интерактивного отчета как по определенному пользователю, так и по нескольким пользователям, групп пользователей либо групп Active Directory за все время наблюдения или за выбранный интервал времени. Отчет должен включать в себя следующую информацию: Статистика перехвата данных, в том числе:</p> <p>1) количество переданной и полученной пользователем информации по всем каналам передачи, включая почту и мессенджеры;</p> <p>2) количество посещенных сайтов и поисковых запросов;</p> <p>3) количество файлов, переданных/принятых по FTP;</p> <p>4) количество распечатанных документов и страниц;</p>	<p>6) the number of screenshots taken.</p> <p>7) the number of files transferred to external drives/network resources/cloud storage;</p> <p>8) the number of keyboard keys pressed.</p> <p>Information about the user's computer activity, including:</p> <p>1) the total time of active work of the user at the PC;</p> <p>2) the average daily time of active work of the user on the PC;</p> <p>3) total PC downtime;</p> <p>4) average daily PC downtime;</p> <p>5) the total time of the employee's presence at work;</p> <p>6) average daily time of employee's presence at work;</p> <p>7) average start time;</p> <p>8) average end-of-work time;</p> <p>9) total number of working days;</p> <p>10) calendar of employee working days accounting with indication of the start/end time of work, computer activity/downtime for each day (with color highlighting of the facts of early start of work, late start of work, early end of work, late end of work), as well as with a chart of productive/neutral/unproductive work during the day;</p> <p>11) a histogram of the user's computer activity/downtime for each day;</p> <p>12) a bar chart of the user's productive/unproductive / neutral work time for each day</p> <p>Information about application activity on the user's computer, including:</p> <p>1) percentage of running time in various applications (with a pie chart).</p>
---	---	--



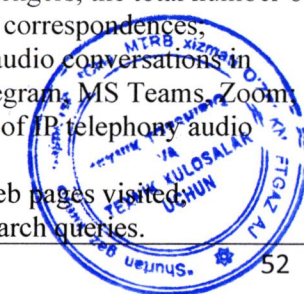
<p>abonentlar doirasini (ichki va tashqi) vizual ko'rsatish uchun foydalanuvchining o'zida to'plangan ma'lumotlarga asoslangan munosabatlarini grafik yoki jadval shaklida ko'rsatish;</p> <p>16) oraliq aloqalarni hisobga olgan holda munosabatlar grafigini qurish qobiliyati (oraliq aloqalar soni 5 tagacha).</p> <p>17) foydalanuvchi kontaktlarini aniqlangan va noma'lum kontaktlarga ko'ra guruhlashni qo'llab-quvvatlash.</p> <p>18) tashqi foydalanuvchi kartasini yaratgandan so'ng tashqi abonentning tashkilot tarmog'i foydalanuvchilari bilan munosabatlarini ko'rish.</p> <p>19) mijoz konsolida ko'rishda hisobotni ko'rsatish shkalasini tanlash (asl nusxaning % hajmini ko'rsatgan holda).</p> <p>20) foydalanuvchi ma'lum bir abonent bilan almashgan hujjatlar (xatlar, yozishmalar, fayllar va boshqalar) tarkibiga munosabatlar diagrammasini ko'rishdan interaktiv tarzda o'tish imkoniyati.</p> <p>21) munosabatlar hisobotini tashqi PNG fayliga grafik sifatida saqlashni qo'llab-quvvatlash.</p> <p>9.2. Foydalanuvchi hisobotiga qo'yiladigan talablar: faol guruhlar uchun ham umumiy interaktiv hisobotni yaratish qobiliyatini ta'minlashi kerak. Butun kuzatish davri yoki tanlangan vaqt oralig'i uchun katalog .</p> <p>Hisobot quyidagi ma'lumotlarni o'z ichiga olishi kerak:</p> <p>Ma'lumotlarni ushlab statistikasi, shu jumladan:</p> <p>1) foydalanuvchi tomonidan barcha uzatish kanallari, shu jumladan pochta va messengerlar orqali uzatiladigan va qabul qilingan axborot miqdori;</p> <p>2) tashrif buyurilgan saytlar soni va qidiruv so'rovlar;</p> <p>3) FTP orqali uzatilgan/qabul qilingan fayllar soni;</p>	<p>5) количество операций копирования в буфер обмена;</p> <p>6) количество снятых скриншотов;</p> <p>7) количество файлов, переданных на внешние накопители/сетевые ресурсы/облачные хранилища;</p> <p>8) количество нажатых клавиш клавиатуры;</p> <p>Информация об активности пользователя за компьютером, в том числе:</p> <p>1) общее время активной работы пользователя за ПК;</p> <p>2) среднесуточное время активной работы пользователя за ПК;</p> <p>3) общее время простоя ПК;</p> <p>4) среднесуточное время простоя ПК;</p> <p>5) общее время присутствия сотрудника на работе;</p> <p>6) среднесуточное время присутствия сотрудника на работе;</p> <p>7) среднее время начала работы;</p> <p>8) среднее время окончания работы;</p> <p>9) общее количество рабочих дней;</p> <p>10) календарь учета рабочих дней сотрудника с указанием времени начала/окончания работы, времени активности/простоя компьютера за каждый день (с цветовым выделением фактов раннего начала работы, начала работы с опозданием, раннего окончания работы, окончания работы с задержкой), а также с диаграммой продуктивной/нейтральной/непродуктивной работы в течение дня;</p> <p>11) гистограмму по времени активности/простоя компьютера пользователя за каждый день;</p> <p>12) гистограмму по времени продуктивной/непродуктивной/нейтральной работы пользователя за каждый день</p> <p>Информация об активности приложений на компьютере пользователя, в том числе:</p>	<p>2) a complete list of running applications with an indication of the absolute running time in each of them, indicating the number of the most popular applications displayed;</p> <p>Information about browser activity, including:</p> <p>1) rating of visited web resources;</p> <p>2) history of activity in the web browser.</p> <p>Information about the number of recorded security incidents initiated by the user and the corresponding rules with varying degrees of detail.</p> <p>Information about the number of cases under investigation that the user is involved in, including:</p> <p>1) open ones.</p> <p>2) closed ones.</p> <p>It should be possible to batch save and configure a schedule for sending reports to multiple users with pre-configuration of a single report form. At the same time, it should be allowed to send a single file to all users, or create a separate file for each user.</p> <p>9.3. Requirements for the TOP User Report:</p> <p>It should be possible to create rating interactive reports on controlled data transmission channels and statistical indicators for the entire time of observation or for a selected time interval, indicating the number of users, including:</p> <p>1) the ability to create a TOP report for randomly selected users, user groups, or Active Directory groups;</p> <p>2) the ability to configure the number of users in the TOP report ("TOP-10", "TOP-20", etc.);</p> <p>3) the ability to build top reports for the entire time of observation or for a selected time interval ;</p> <p>4) the ability to take into account both the total total and the average daily value of the corresponding parameters when compiling such reports (for example, a report of the type "TOP 10 users by the average daily number of sites visited")</p>
---	--	--



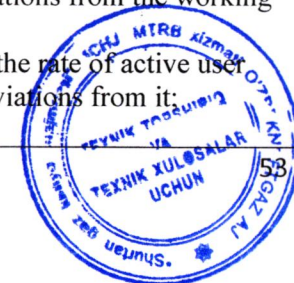
<p>4) bosilgan hujjatlar va sahifalar soni; 5) buferga nusxa ko'chirish operatsiyalari soni; 6) olingan skrinshotlar soni; 7) tashqi disklarga/tarmoq resurslariga/bulutli xotiraga o'tkazilgan fayllar soni; 8) bosilgan klaviatura tugmalari soni; Foydalanuvchining kompyuter faoliyati haqida ma'lumot, jumladan: 1) foydalanuvchi shaxsiy kompyuterda faol ishlagan umumiy vaqt; 2) shaxsiy kompyuterda faol foydalanuvchi ishini o'rtacha kunlik vaqti; 3) kompyuterning umumiy ishlamay qolish vaqti; 4) kompyuterning o'rtacha kunlik ishlamay qolish vaqti; 5) xodimning ish joyida bo'lgan umumiy vaqti; 6) xodimning ish joyida bo'lgan o'rtacha kunlik vaqti; 7) o'rtacha boshlanish vaqti; 8) ishni bajarishning o'rtacha vaqti; 9) ish kunlarining umumiy soni; 10) Ishning boshlanish/tugash vaqtini, har bir kun uchun kompyuterning ish vaqti/ish vaqtini ko'rsatuvchi xodimning ish kunlarini qayd qilish uchun kalendar (ishning erta boshlanishi, ishning kech boshlanishi, ishning erta tugashi faktlarini rang bilan ajratib ko'rsatish bilan); ishning kechikish bilan tugashi), shuningdek kun davomida samarali / neytral / samarasiz ishlarning diagrammasi bilan; 11) har bir kun uchun foydalanuvchining kompyuter faoliyati/bo'sh vaqtining gistogrammasi; 12) foydalanuvchining har bir kun uchun samarali / samarasiz / neytral ish vaqtining gistogrammasi Foydalanuvchi kompyuteridagi dastur faoliyati haqida ma'lumot, jumladan: 1) turli xil ilovalardagi ish vaqtining ulushi</p>	<p>1) процентное соотношение времени работы в различных приложениях (с построением круговой диаграммы); 2) полный список запускавшихся приложений с указанием абсолютного времени работы в каждом из них с указанием количества отображаемых наиболее популярных приложений; Информация о браузер-активности, в том числе: 1) рейтинг посещенных веб-ресурсов; 2) хронология активности в веб-браузере. Информация о количестве зафиксированных инцидентов безопасности, инициированных пользователем, и соответствующих им правил с различной степенью детализации. Информация о количестве расследуемых дел, в которые вовлечен пользователь, в том числе: 1) открытых; 2) закрытых. Должна быть предусмотрена возможность пакетного сохранения и настройки расписания рассылки отчетов для нескольких пользователей с предварительной настройкой единой формы отчета. При этом должна допускаться как отправка одним файлом по всем пользователям, так и создание отдельного файла для каждого пользователя. 9.3. Требования к ТОП-отчету по пользователям: Должна быть предоставлена возможность построения рейтинговых интерактивных отчетов по контролируемым каналам передачи данных и статистическим показателям за все время наблюдения или за выбранный интервал времени с указанием числа пользователей, в том числе: 1) возможность создания ТОП-отчета для произвольно выбранных пользователей, групп пользователей либо групп Active Directory; 2) возможность настройки количества пользователей в ТОП-отчете («ТОП-10», «ТОП-20» и т.д.);</p>	<p>You should be able to configure the rating based on various indicators, including: 1) the number of incoming / outgoing emails, the total number of emails. 2) the number of incoming / outgoing messages in instant messengers, the total number of messages, the number of correspondences; 3) number and time of audio conversations in instant messengers 4) number and size of sent / received files 5) the number/time of IP telephony audio conversations; 6) the number of web pages visited; 7) the number of search queries. 8) the number of emails/publications in web-based communications; 9) the number/size of files written to the USB drive, network resources, and cloud storage. 10) the number of files sent/received, the total number of files over the FTP protocol, the size of files sent/received, the total size of all files over the FTP protocol; 11) the number of printed pages/documents; 12) the number of operations for copying text to the clipboard. 13) the number of keys pressed. 14) the number of security incidents; 15) the number of cases involving the user. 16) the time of active operation/downtime of the PC; 17) time of productive/unproductive work 18) number of days late 19) number of days with early termination 20) number of operations with files and folders, divided by operation type 21) average start/end time of work, time spent at work.</p>
---	---	--



<p>(dumaloq diagramma tuzish bilan);</p> <p>2) ishga tushirilgan ilovalarning to'liq ro'yxati, ularning har birida mutlaq ish vaqtini ko'rsatuvchi, ko'rsatilgan eng mashhur ilovalar sonini ko'rsatuvchi; Brauzer faoliyati haqida ma'lumot, jumladan:</p> <p>1) tashrif buyurilgan veb-resurslar reytingi;</p> <p>2) veb-brauzerdagi faoliyat xronologiyasi.</p> <p>Foydalanuvchi tomonidan boshlangan qayd etilgan xavfsizlik hodisalari va turli darajadagi tafsilotlarga ega tegishli qoidalar to'g'risidagi ma'lumotlar.</p> <p>Foydalanuvchi ishtirok etgan davom etayotgan holatlar soni haqida ma'lumot, jumladan:</p> <p>1) ochiq;</p> <p>2) yopiq.</p> <p>Yagona hisobot shaklining dastlabki konfiguratsiyasi bilan bir nechta foydalanuvchilarga hisobotlarni yuborish jadvalini to'plamli saqlash va o'rnatish imkoniyati bo'lishi kerak. Bunday holda, barcha foydalanuvchilarga bitta faylni yuborish va har bir foydalanuvchi uchun alohida fayl yaratish imkoniyati bo'lishi kerak.</p> <p>9.3. Foydalanuvchilar tomonidan TOP hisobotiga qo'yiladigan talablar:</p> <p>Kuzatuvning butun davri yoki tanlangan vaqt oralig'i uchun monitoring qilinadigan ma'lumotlarni uzatish kanallari va statistik ko'rsatkichlar bo'yicha reyting interaktiv hisobotlarini yaratish imkoniyati bo'lishi kerak, shu jumladan foydalanuvchilar soni:</p> <p>1) faol guruhlar uchun TOP hisobotini yaratish imkoniyati katalog;</p> <p>2) TOP hisobotida foydalanuvchilar sonini sozlash imkoniyati ("TOP-10", "TOP-20" va boshqalar);</p> <p>3) vaqt oralig'i uchun eng yaxshi hisobotlarni yaratish qobiliyati;</p> <p>4) bunday hisobotlarni tuzishda tegishli parametrlarning umumiy umumiy va o'rtacha kunlik</p>	<p>3) возможность построения топ-отчетов за все время наблюдения или за выбранный интервал времени;</p> <p>4) возможность учета как общего суммарного, так и среднесуточного значения соответствующих параметров при составлении таких отчетов (например, отчет вида «ТОП-10 пользователей по среднесуточному количеству посещенных сайтов»).</p> <p>Должна быть предусмотрена возможность настройки рейтинга по различным показателям, в том числе:</p> <p>1) количество входящих/исходящих писем, общее количество писем;</p> <p>2) количество входящих/исходящих сообщений в мессенджерах, общее количество сообщений, количество переписок;</p> <p>3) количество и время аудио-разговоров в мессенджерах</p> <p>4) количество и размер отправленных/принятых файлов</p> <p>5) количество/время аудио-разговоров IP-телефонии;</p> <p>6) количество посещенных веб-страниц;</p> <p>7) количество поисковых запросов;</p> <p>8) количество писем/публикаций в web-коммуникациях;</p> <p>9) количество/размер файлов, записанных на USB-накопитель, сетевые ресурсы, облачные хранилища;</p> <p>10) количество отправленных/принятых файлов, общее количество файлов по протоколу FTP, размер отправленных/принятых файлов, общий размер всех файлов по протоколу FTP;</p> <p>11) количество распечатанных страниц/документов;</p> <p>12) количество операций копирования текста в буфер обмена;</p> <p>13) количество нажатых клавиш;</p> <p>14) количество инцидентов безопасности;</p> <p>15) количество дел с участием пользователя;</p> <p>16) время активной работы/простоя ПК;</p>	<p>9.4. Requirements for reporting violations:</p> <p>It should be possible to create summary interactive reports on security rule response statistics, including:</p> <p>1) view statistics for all users and groups of users, as well as for individual users.</p> <p>2) report details by day, week, month, and user</p> <p>3) creating a report for an arbitrary time period with viewing the total number of triggers for each rule separately, as well as the total number of triggers for all existing security rules.</p> <p>9.5 Requirements for the summary report for users:</p> <p>It should be possible to create summary interactive reports on the network and local activity statistics of selected users, including:</p> <p>1) the ability to select activity indicators for which the report will be built.</p> <p>2) view statistics for all users and groups of users, as well as for individual users.</p> <p>3) detailing the report by day, month, or any time period and viewing summary statistics for selected statistical indicators.</p> <p>The report should be based on the following activity indicators:</p> <p>1) the number of incoming / outgoing emails, the total number of emails.</p> <p>2) the number of incoming / outgoing messages in instant messengers, the total number of messages, the number of correspondences;</p> <p>3) number/time of audio conversations in Skype, Lync, Viber, Telegram, MS Teams, Zoom;</p> <p>4) the number/time of IP-telephony audio conversations;</p> <p>5) the number of web pages visited;</p> <p>6) the number of search queries.</p>
--	--	---



<p>qiymatini hisobga olish qobiliyati (masalan, "Kunlik tashrif buyurilgan saytlarning o'rtacha soni bo'yicha TOP 10 foydalanuvchi" kabi hisobot). Reytingni turli ko'rsatkichlar asosida sozlash mumkin bo'lishi kerak, jumladan:</p> <ol style="list-style-type: none"> 1) kiruvchi / chiquvchi xatlar soni, xatlarning umumiy soni; 2) messenjerlardagi kiruvchi/chiqish xabarlar soni, xabarlarining umumiy soni, yozishmalar soni; 3) messenjerlardagi audio suhbatlar soni va vaqti 4) yuborilgan/qabul qilingan fayllar soni va hajmi 5) IP telefoniyadagi audio suhbatlar soni/vaqti; 6) tashrif buyurilgan veb-sahifalar soni; 7) qidiruv so'rovlari soni; 8) veb- kommunikatsiyalardagi xatlar/nashrlar soni ; 9) USB diskida, tarmoq resurslarida, bulutli xotirada yozilgan fayllar soni/hajmi; 10) yuborilgan/qabul qilingan fayllar soni, FTP orqali fayllarning umumiy soni, yuborilgan/qabul qilingan fayllar hajmi, FTP orqali barcha fayllarning umumiy hajmi; 11) chop etilgan sahifalar/hujjatlar soni; 12) matnni buferga nusxalash operatsiyalari soni; 13) bosilgan tugmalar soni; 14) xavfsizlik hodisalari soni; 15) foydalanuvchi bilan bog'liq holatlar soni; 16) Kompyuterning faol/bo'sh vaqti; 17) unumli / samarasiz ish vaqti 18) kechikkan kunlar soni 19) erta tugatilgan kunlar soni 20) fayl va papkalar bilan operatsiyalar soni, operatsiya turiga bo'linadi 21) ishning o'rtacha boshlanish/tugash vaqti, ishda o'tkaziladigan vaqt. 	<ol style="list-style-type: none"> 17) время продуктивной/непродуктивной работы 18) количество дней с опозданием 19) количество дней с досрочным окончанием 20) количество операций с файлами и папками с разделением по типам операций 21) среднее время начала/окончания работы, время нахождения на работе. <p>9.4. Требования к отчету по нарушениям: Должна быть предусмотрена возможность построения сводных интерактивных отчетов о статистике срабатывания правил безопасности, в том числе:</p> <ol style="list-style-type: none"> 1) просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям; 2) детализация отчета по дням, неделям, месяцам, по пользователям 3) построение отчета за произвольный временной промежуток с просмотром итогового количества срабатываний по каждому правилу в отдельности, а также суммарного количества срабатываний по всем существующим правилам безопасности. <p>9.5 Требования к сводному отчету по пользователям: Должна быть предусмотрена возможность построения сводных интерактивных отчетов о статистических показателях сетевой и локальной активности выбранных пользователей, в том числе:</p> <ol style="list-style-type: none"> 1) возможность выбора показателей активности, по которым будет построен отчет; 2) просмотр статистики как по всем пользователям и группам пользователей, так и по отдельным пользователям; 3) детализация отчета по дням, месяцам, за произвольный временной промежуток и просмотр сводной статистики по выбранным статистическим показателям. <p>Отчет должен предусматривать построение по следующим показателям активности:</p>	<ol style="list-style-type: none"> 7) the number of emails/publications in web-based communications; 8) the number/size of files written to the USB drive, network resources, and cloud storage. 9) the number of files sent/received, the total number of files over the FTP protocol, the size of files sent/received, the total size of all files over the FTP protocol; 10) the number of printed pages/documents; 11) the number of operations of copying text to the clipboard; 12) the number of keys pressed. 13) the number of security incidents; 14) the number of cases involving the user. 15) the time of active operation/downtime of the PC; 16) time of productive/unproductive work 17) charts of productive/unproductive work, both with and without downtime 18) number of days late 19) number of days with early termination 20) number of operations with files and folders divided by operation type 21) average start/end time of work, time spent at work. <p>9.6 Requirements for the report "timesheet": The report should record the use of working hours by employees, including the time of arrival and departure from work, active working hours, and the time when employees are present at the workplace, and also have the following features:</p> <ol style="list-style-type: none"> 1) the ability to set a schedule of working hours and highlight deviations from the working schedule; 2) the ability to set the rate of active user activity and highlight deviations from it;
--	---	---



9.4. Buzilish to'g'risida hisobot berish talablari:

Xavfsizlik qoidalarini ishga tushirish statistikasi bo'yicha qisqacha interaktiv hisobotlarni yaratish mumkin bo'lishi kerak, jumladan:

1) barcha foydalanuvchilar va foydalanuvchilar guruhlarini, shuningdek, alohida foydalanuvchilar uchun statistikasi ko'rish;

2) foydalanuvchilar tomonidan kunlar, haftalar, oylar bo'yicha batafsil hisobot

3) har bir qoida uchun signallarning umumiy sonini, shuningdek, barcha mavjud xavfsizlik qoidalarini uchun signallarning umumiy sonini ko'rib chiqish bilan ixtiyoriy vaqt davri uchun hisobot yaratish.

9.5 Foydalanuvchilar tomonidan umumiy hisobotga qo'yiladigan talablar:

Tanlangan foydalanuvchilarning tarmoq va mahalliy faoliyatining statistik ko'rsatkichlari bo'yicha umumiy interaktiv hisobotlarni yaratish mumkin bo'lishi kerak, shu jumladan:

1) hisobot tuziladigan faoliyat ko'rsatkichlarini tanlash imkoniyati;

2) barcha foydalanuvchilar va foydalanuvchilar guruhlarini, shuningdek, alohida foydalanuvchilar uchun statistikasi ko'rish;

3) hisobotni kun, oy, ixtiyoriy vaqt oralig'ida batafsil bayon qilish va tanlangan statistik ko'rsatkichlar bo'yicha umumiy statistikasi ko'rish.

Hisobot quyidagi faoliyat ko'rsatkichlari asosida qurilishni o'z ichiga olishi kerak:

1) kiruvchi / chiquvchi xatlar soni, xatlarning umumiy soni;

2) messenjerlardagi kiruvchi/chiqish xabarlar soni, xabarlarining umumiy soni, yozishmalar soni;

3) Skype, Lync, Viber, Telegram, MS Teams, Zoom dagi audio suhbatlar soni/vaqt;

4) IP telefoniyadagi audio suhbatlar soni/vaqt;

1) количество входящих/исходящих писем, общее количество писем;

2) количество входящих/исходящих сообщений в мессенджерах, общее количество сообщений, количество переписок;

3) количество/время аудио-разговоров в Skype, Lync, Viber, Telegram, MS Teams, Zoom;

4) количество/время аудио-разговоров IP-телефонии;

5) количество посещенных веб-страниц;

6) количество поисковых запросов;

7) количество писем/публикаций в web-коммуникациях;

8) количество/размер файлов, записанных на USB-накопитель, сетевые ресурсы, облачные хранилища;

9) количество отправленных/принятых файлов, общее количество файлов по протоколу FTP, размер отправленных/принятых файлов, общий размер всех файлов по протоколу FTP;

10) количество распечатанных страниц/документов;

11) количество операций копирования текста в буфер обмена;

12) количество нажатых клавиш;

13) количество инцидентов безопасности;

14) количество дел с участием пользователя;

15) время активной работы/простоя ПК;

16) время продуктивной/непродуктивной работы

17) диаграммы продуктивной/непродуктивной работы как с учетом времени простоя, так и без него

18) количество дней с опозданием

19) количество дней с досрочным окончанием

20) количество операций с файлами и папками с разделением по типам операций

21) среднее время начала/окончания работы, время нахождения на работе.

9.6 Требования к отчету «табель рабочего времени»:

3) the ability to exclude a certain time period from accounting (for example, lunch time);

4) the ability to build a report for the current calendar month, as well as for the specified month.

9.7 Requirements for the App Activity report:

The report should contain information about app usage by employees and only take into account working hours in active apps. It should also have the following features:

1) the ability to build reports on applications or on categories/productivity of applications, taking into account the data of the application categorizer;

2) the report can be presented as a bar chart, bar chart, or pie chart, or as a table.

3) the ability to configure a report on the activity of work in certain applications, or exclude certain applications from the report;

4) the ability to build a report in the context of the most active users with an indication of their number.

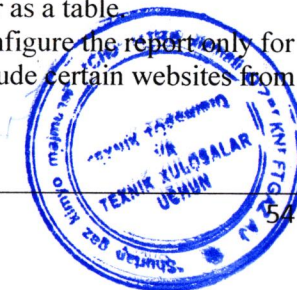
9.8 Requirements for the Browser Activity report:

The report should contain information about the use of working hours on sites and only take into account working hours on sites in the active browser tab. It should also have the following features:

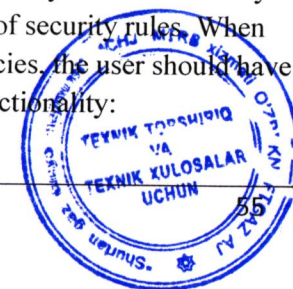
1) the ability to build reports on websites or by categories/productivity of websites, taking into account the data of the website categorizer;

2) the report can be presented as a bar chart, bar chart, or pie chart, or as a table.

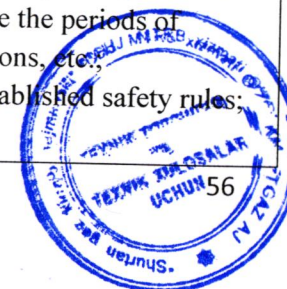
3) the ability to configure the report only for certain websites, or exclude certain websites from the report;



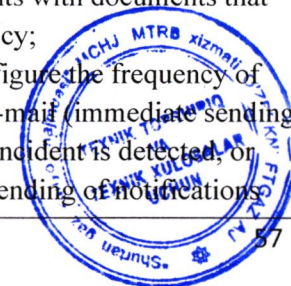
<p>5) tashrif buyurilgan veb-sahifalar soni; 6) qidiruv so'rovlari soni; 7) veb- kommunikatsiyalardagi xatlar/nashrlar soni; 8) USB diskida, tarmoq resurslarida, bulutli xotirada yozilgan fayllar soni/hajmi; 9) yuborilgan/qabul qilingan fayllar soni, FTP orqali fayllarning umumiy soni, yuborilgan/qabul qilingan fayllar hajmi, FTP orqali barcha fayllarning umumiy hajmi; 10) chop etilgan sahifalar/hujjatlar soni; 11) matnni buferga nusxalash operatsiyalari soni; 12) bosilgan tugmalar soni; 13) xavfsizlik hodisalari soni; 14) foydalanuvchi bilan bog'liq holatlar soni; 15) Kompyuterning faol/bo'sh vaqti; 16) unumli / samarasiz ish vaqti 17) bo'sh vaqtli va unumsiz ishlarning diagrammalari 18) kechikkan kunlar soni 19) erta tugatilgan kunlar soni 20) fayl va papkalar bilan operatsiyalar soni, operatsiya turiga bo'linadi 21) ishning o'rtacha boshlanish/tugash vaqti, ishda o'tkaziladigan vaqt.</p> <p>9.6 "Vaqt jadvali" hisobotiga qo'yiladigan talablar: Hisobotda xodimlarning ish vaqtidan foydalanishi, ishdan kelish va ketish vaqtlari, faol ish vaqti, xodimlarning ish joyida bo'lish vaqti qayd etilgan, shuningdek quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) ish vaqti jadvalini belgilash va ish jadvalidan chetlanishlarni ajratib ko'rsatish qobiliyati; 2) foydalanuvchining faol ishi uchun normani belgilash va undan og'ishlarni ta'kidlash qobiliyati; 3) ma'lum bir vaqtni buxgalteriya hisobidan chiqarib tashlash imkoniyati (masalan, tushlik vaqti);</p>	<p>Отчет должен регистрировать использование рабочего времени сотрудниками, с регистрацией времени прихода и ухода с работы, активного времени работы, времени присутствия сотрудников на рабочем месте, а также иметь следующие возможности:</p> <p>1) возможность задания графика рабочего времени и выделения отклонения от рабочего графика; 2) возможность задать норму активной работы пользователя и выделять отклонения от нее; 3) возможность исключать из учета определенный временной промежуток (например, время обеда); 4) возможность построения отчета за текущий календарный месяц, а также за указанный месяц.</p> <p>9.7 Требования к отчету по активности приложений: Отчет должен содержать информацию об использовании приложений сотрудниками и учитывать только время работы в активных приложениях, а также иметь следующие возможности:</p> <p>1) возможность построения отчетов по приложениям либо по категориям/продуктивности приложений с учетом данных категоризатора приложений; 2) представление отчета на выбор в виде гистограммы, линейчатой либо круговой диаграммы, в виде таблицы; 3) возможность настройки отчета по активности работы в определенных приложениях, либо исключения определенных приложений из отчета; 4) возможность построения отчета в разрезе наиболее активных пользователей с указанием их количества.</p> <p>9.8 Требования к отчету по браузер-активности: Отчет должен содержать информацию об использовании рабочего времени на сайтах и учитывать только время работы на сайтах в активной вкладке браузера а также иметь следующие возможности:</p>	<p>4) the ability to build a report in the context of the most active users with an indication of their number.</p> <p>9.9 Requirements for the General activity report: The report should contain information about the use of working hours on sites and only take into account working hours on sites in the active browser tab. It should also have the following features:</p> <p>1) the ability to build reports on applications and websites or on categories/productivity of websites, taking into account the data of the website and application categorizer; 2) the report can be presented as a bar chart, bar chart, or pie chart, or as a table. 3) the ability to configure the report only for certain websites and applications, or exclude certain websites and applications from the report; 4) the ability to build a report in the context of the most active users with an indication of their number.</p> <p>10. Requirements for creating security rules/policies: The system must have the functionality intended for setting up a system for notifying authorized persons about cases of violation of security rules. Intercepted data should be analyzed automatically based on the specified list of security rules. When working with security policies, the user should have access to the following functionality:</p>
---	--	---



<p>4) joriy kalendar oyi uchun, shuningdek, belgilangan oy uchun hisobot yaratish imkoniyati.</p> <p>9.7 Ilova faoliyati hisobotiga qo'yiladigan talablar: Hisobot xodimlar tomonidan ilovalardan foydalanish to'g'risidagi ma'lumotlarni o'z ichiga olishi va faqat faol ilovalarga sarflangan vaqtni hisobga olishi, shuningdek, quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) ilovalar toifalari ma'lumotlarini hisobga olgan holda ilovalar bo'yicha yoki ilovalar toifasi/ish unumdorligi bo'yicha hisobotlarni yaratish imkoniyati ;</p> <p>2) hisobotni gistogramma, chiziqli yoki doiraviy diagramma yoki jadval shaklida taqdim etish;</p> <p>3) ma'lum ilovalarda ish faoliyati to'g'risidagi hisobotni sozlash yoki hisobotdan ma'lum ilovalarni chiqarib tashlash imkoniyati;</p> <p>4) eng faol foydalanuvchilar kontekstida ularning sonini ko'rsatgan holda hisobot tuzish qobiliyati.</p> <p>9.8 Brauzer faoliyati hisobotiga qo'yiladigan talablar: Hisobot saytlarda ish vaqtidan foydalanish to'g'risidagi ma'lumotlarni o'z ichiga olishi va faqat faol brauzer yorlig'ida saytlarda o'tkaziladigan vaqtni hisobga olishi va quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) veb-sayt toifalari bo'yicha ma'lumotlarni hisobga olgan holda veb-saytlarning toifalari / mahsuldorligi bo'yicha hisobotlarni yaratish qobiliyati ;</p> <p>2) hisobotni gistogramma, chiziqli yoki doiraviy diagramma yoki jadval shaklida taqdim etish;</p> <p>3) ma'lum veb-saytlar uchun sozlash yoki ma'lum veb-saytlarni hisobotdan chiqarib tashlash imkoniyati ;</p> <p>4) eng faol foydalanuvchilar kontekstida ularning sonini ko'rsatgan holda hisobot tuzish</p>	<p>1) возможность построения отчетов по веб-сайтам либо по категориям/продуктивности веб-сайтов с учетом данных категоризатора веб-сайтов;</p> <p>2) представление отчета на выбор в виде гистограммы, линейчатой либо круговой диаграммы, в виде таблицы;</p> <p>3) возможность настройки отчета только по определенным веб-сайтам, либо исключения определенных веб-сайтов из отчета;</p> <p>4) возможность построения отчета в разрезе наиболее активных пользователей с указанием их количества.</p> <p>9.9 Требования к отчету по общей активности: Отчет должен содержать информацию об использовании рабочего времени на сайтах и учитывать только время работы на сайтах в активной вкладке браузера а также иметь следующие возможности:</p> <p>1) возможность построения отчетов по приложениям и веб-сайтам либо по категориям/продуктивности веб-сайтов с учетом данных категоризатора веб-сайтов и приложений;</p> <p>2) представление отчета на выбор в виде гистограммы, линейчатой либо круговой диаграммы, в виде таблицы;</p> <p>3) возможность настройки отчета только по определенным веб-сайтам и приложениям, либо исключения определенных веб-сайтов и приложений из отчета;</p> <p>4) возможность построения отчета в разрезе наиболее активных пользователей с указанием их количества.</p> <p>10. Требования к формированию правил/политик безопасности: Система должна обладать функционалом, предназначенным для настройки системы оповещения уполномоченных лиц о случаях нарушения правил безопасности. Перехваченные данные должны</p>	<p>1) configuring security rules using search conditions using all available analysis tools: content analysis, attribute analysis, search by recognized images, prints, event analysis, etc.;</p> <p>2) combining several simple search terms using the logical operators "AND", "OR", "NOT", with the possibility of combining search terms into groups;</p> <p>3) security rules for Active Directory groups;</p> <p>4) security rules by site and app categories.</p> <p>5) security rules for detecting files with certain privacy labels</p> <p>6) creating security policies using search templates – a set of search conditions that can be used when forming other security rules;</p> <p>7) safety rules for digital fingerprints with the ability to adjust the trigger threshold and choose the direction of entry (forward, reverse, or maximum);</p> <p>8) safety rules based on dictionaries, with the possibility of taking into account the trigger threshold and morphology;</p> <p>9) security rules for hash amounts, with the ability to search through pre-configured hash sum banks;</p> <p>10) statistical security rules that control the excess of quantitative indicators of user activity, for example, the number of emails, correspondence in messengers, visited sites, sent requests, printed files and pages, as well as calculate the periods of activity of users and applications, etc.;</p> <p>11) availability of pre-established safety rules;</p>
--	---	--

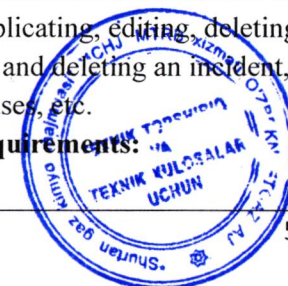


<p>qobiliyati.</p> <p>9.9 Umumiy faoliyat hisobotiga qo'yiladigan talablar: Hisobot saytlarda ish vaqtidan foydalanish to'g'risidagi ma'lumotlarni o'z ichiga olishi va faqat faol brauzer yorlig'ida saytlarda o'tkaziladigan vaqtni hisobga olishi va quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) va ilovalar toifalari ma'lumotlarini hisobga olgan holda veb-saytlarning toifalari/mahsuldorligi bo'yicha hisobotlarni yaratish qobiliyati ;</p> <p>2) hisobotni gistogramma, chiziqli yoki doiraviy diagramma yoki jadval shaklida taqdim etish;</p> <p>3) ma'lum veb-saytlar va ilovalar uchun moslashtirish yoki ma'lum veb-saytlar va ilovalarni hisobotdan chiqarib tashlash imkoniyati ;</p> <p>4) eng faol foydalanuvchilar kontekstida ularning sonini ko'rsatgan holda hisobot tuzish qobiliyati.</p> <p>10. Xavfsizlik qoidalarini/siyosatlarini shakllantirishga qo'yiladigan talablar:</p> <p>Tizim vakolatli shaxslarni xavfsizlik qoidalarini buzish holatlari haqida ogohlantirish tizimini o'rnatish uchun mo'ljallangan funktsionallikka ega bo'lishi kerak. Qabul qilingan ma'lumotlar xavfsizlik qoidalarining belgilangan ro'yxati asosida avtomatik ravishda tahlil qilinishi kerak. Xavfsizlik siyosati bilan ishlashda foydalanuvchi quyidagi funktsiyalardan foydalanishi kerak:</p> <p>1) barcha mavjud tahlil vositalaridan foydalangan holda qidiruv shartlaridan foydalangan holda xavfsizlik qoidalarini o'rnatish: kontentni tahlil qilish, atributlarni tahlil qilish, tan olingan tasvirlar, muhrlar, hodisalar tahlili va boshqalar bo'yicha qidirish;</p> <p>2) qidiruv shartlarini guruhlariga birlashtirish imkoniyati bilan "VA", "YOKI", "YO'Q" mantiqiy operatorlari yordamida bir nechta oddiy qidiruv</p>	<p>анализироваться в автоматическом режиме на основании заданного списка правил безопасности. При работе с политиками безопасности пользователю должен быть доступен следующий функционал:</p> <p>1) настройка правил безопасности при помощи поисковых условий с использованием всех доступных инструментов анализа: контентный анализ, атрибутивный анализ, поиск по распознанным изображениям, печатам, событийный анализ и др.;</p> <p>2) комбинирование нескольких простых поисковых условий при помощи логических операторов «И», «ИЛИ», «НЕ», с возможностью объединения поисковых условий в группы;</p> <p>3) правила безопасности по группам Active Directory;</p> <p>4) правила безопасности по категориям сайтов и приложений;</p> <p>5) правила безопасности на обнаружение файлов с определенными метками конфиденциальности</p> <p>6) создание политик безопасности с использованием шаблонов поиска – набора поисковых условий, которые можно использовать при формировании других правил безопасности;</p> <p>7) правила безопасности по цифровым отпечаткам с возможностью настройки порога срабатывания и выбором направления вхождения (прямое, обратное, или наибольшее);</p> <p>8) правила безопасности по словарям, с возможностью учета порога срабатывания и морфологии;</p> <p>9) правила безопасности по хеш-суммам, с возможностью поиска по преднастроенным банкам хеш-сумм;</p> <p>10) статистические правила безопасности, контролирующие превышение количественные показатели активности пользователя, например, количество электронных писем, переписок в мессенджерах, посещенных сайтов, отправленных</p>	<p>12) ability to create groups and subgroups with at least 20 hierarchy levels;</p> <p>13) ability to disable security rules</p> <p>14) filter on / off safety rules</p> <p>15) the ability to transfer security policies from group to group by simply dragging and dropping the "mouse";</p> <p>16) the ability to transfer subgroups from group to group by simply dragging and dropping with the mouse;</p> <p>17) adding or excluding Active Directory groups to which security policies can be applied;</p> <p>18) adding, excluding, and editing security server incident categories</p> <p>19) the ability to execute scripts when a security rule is triggered or an error occurs;</p> <p>20) ability to send incident data to third-party systems;</p> <p>21) automatic delivery of notifications by e-mail to the responsible person in case of triggering the security policy (detecting an incident);</p> <p>22) the incident contains general information (the name of the security policy, the user who committed the violation, the type of intercepted data, the date/time of the incident, etc.), as well as a link to opening the corresponding incident in the user console or attachments with documents that triggered the security policy;</p> <p>23) the ability to configure the frequency of sending notifications to e-mail (immediate sending of notifications when an incident is detected, or accumulation and batch sending of notifications)</p>
---	---	---

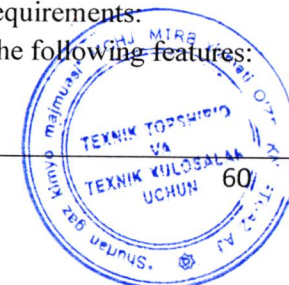


<p>shartlarini birlashtirish;</p> <p>3) Faol guruhlar tomonidan xavfsizlik qoidalari katalog ;</p> <p>4) saytlar va ilovalar toifalari bo'yicha xavfsizlik qoidalari;</p> <p>5) muayyan sezgirlik belgilariga ega fayllarni aniqlash uchun xavfsizlik qoidalari</p> <p>6) qidiruv shablonlari yordamida xavfsizlik siyosatini yaratish - boshqa xavfsizlik qoidalarini yaratishda foydalanish mumkin bo'lgan qidiruv shartlari to'plami;</p> <p>7) javob chegarasini sozlash va kirish yo'nalishini tanlash (to'g'ridan-to'g'ri, teskari yoki eng katta) qobiliyatiga ega raqamli barmoq izlari uchun xavfsizlik qoidalari;</p> <p>8) javob chegarasi va morfologiyasini hisobga olish qobiliyati bilan lug'atlarga asoslangan xavfsizlik qoidalari;</p> <p>9) oldindan tuzilgan xesh so'm banklari orqali qidirish imkoniyati bilan xesh summalariga asoslangan xavfsizlik qoidalari ;</p> <p>10) foydalanuvchi faoliyatining miqdoriy ko'rsatkichlaridan oshib ketishini nazorat qiluvchi statistik xavfsizlik qoidalari, masalan, elektron pochta xabarlari soni, messenjerlardagi yozishmalar, tashrif buyurilgan saytlar, yuborilgan so'rovlar, bosma fayllar va sahifalar, shuningdek, foydalanuvchi va ilovalar faoliyatining davrlarini hisoblash va boshqalar. .;</p> <p>11) oldindan belgilangan xavfsizlik qoidalarining mavjudligi;</p> <p>12) kamida 20 ierarxiya darajasiga ega bo'lgan guruhlar va kichik guruhlarini yaratish qobiliyati;</p> <p>13) xavfsizlik qoidalarini o'chirish qobiliyati</p> <p>14) yoqilgan/o'chirilgan xavfsizlik qoidalari uchun filtr</p> <p>15) sichqoncha bilan shunchaki sudrab, guruhdan guruhga xavfsizlik siyosatini o'tkazish imkoniyati;</p>	<p>запросов, распечатанных файлов и страниц, а также вычислять периоды активности пользователей и приложений, и др.;</p> <p>11) наличие предустановленных правил безопасности;</p> <p>12) возможность создания групп и подгрупп с количеством уровней иерархии не менее 20;</p> <p>13) возможность отключения правила безопасности</p> <p>14) фильтр включенных/выключенных правил безопасности</p> <p>15) возможность переноса политик безопасности из группы в группу простым перетаскиванием «мышью»;</p> <p>16) возможность переноса подгрупп из группы в группу простым перетаскиванием «мышью»;</p> <p>17) добавление, исключение групп Active Directory, к которым могут быть применены политики безопасности;</p> <p>18) добавление, исключение, редактирование категорий инцидентов сервера безопасности</p> <p>19) возможность выполнения скриптов при срабатывании или ошибке срабатывания правила безопасности;</p> <p>20) возможность отправки данных о инцидентах в сторонние системы;</p> <p>21) автоматическая доставка уведомлений по электронной почте ответственному лицу в случае срабатывания политики безопасности (выявления инцидента);</p> <p>22) инцидент содержит общую информацию (название политики безопасности, пользователь, допустивший нарушение, тип перехваченных данных, дата/время инцидента и др.), а также ссылку на открытие соответствующего инцидента в пользовательской консоли либо вложения с документами, вызвавшими срабатывание политики безопасности;</p> <p>23) возможность настройки периодичности отправки уведомлений на электронную почту (немедленная отправка уведомления по выявлению инцидента либо</p>	<p>with a specified frequency – once an hour, once a day, etc.);</p> <p>24) the ability to view all incidents according to the selected security policy in the client console with the ability to select viewed, unseen incidents for each security officer working with the system;</p> <p>25) when viewing information about an incident in the client console, the following information is available: the user who committed the violation, the date and time of the incident, the type of document that triggered the security policy (email, file sent for printing, etc.), the content of the document (email, correspondence in the IM client, file, etc.) which triggered the security policy, as well as other additional information.</p> <p>26) ability to assign a status for an incident (incident not investigated, incident investigation postponed, incident investigated, important incident, unimportant incident, false positive);</p> <p>27) ability to assign a color category to an incident</p> <p>28) ability to add comments to the incident</p> <p>29) the ability to flexibly selectively view incidents according to the security policy (for example, show only new or unseen incidents; show only the last 100 incidents; show incidents for the next month, but no more than the last 20; show incidents that have the "Important" status and were registered during the last week, etc.);</p> <p>30) the ability to completely or selectively delete incident records according to the security policy (for example, delete all incidents older than</p>
--	--	---

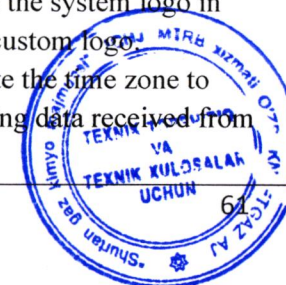
<p>16) sichqoncha bilan sudrab kichik guruhlarini guruhdan guruhga o'tkazish imkoniyati;</p> <p>17) qo'shish, faol guruhlar bundan mustasno Xavfsizlik siyosati qo'llanilishi mumkin bo'lgan katalog ;</p> <p>18) xavfsizlik serveri hodisalari toifalarini qo'shish, istisno qilish, tahrirlash</p> <p>19) xavfsizlik qoidasi ishga tushganda yoki ishlaymay qolganda skriptlarni bajarish imkoniyati;</p> <p>20) voqea ma'lumotlarini uchinchi tomon tizimlariga yuborish imkoniyati;</p> <p>21) xavfsizlik siyosati ishga tushirilganda (hodisalar aniqlanganda) mas'ul shaxsga elektron pochta orqali bildirishnomalarni avtomatik etkazib berish;</p> <p>22) hodisa umumiy ma'lumotlarni (xavfsizlik siyosatining nomi, qoidabuzarlikni sodir etgan foydalanuvchi, ushlangan ma'lumotlarning turi, voqea sodir bo'lgan sana/vaqt va boshqalar), shuningdek foydalanuvchi konsolida yoki qo'shimchalarida tegishli hodisani ochish uchun havolani o'z ichiga oladi. xavfsizlik siyosatini qo'zg'atgan hujjatlar bilan;</p> <p>23) elektron pochta orqali bildirishnomalarni yuborish chastotasini sozlash imkoniyati (hodisa aniqlanganda darhol xabarnoma yuborish yoki belgilangan chastotada bildirishnomalarni to'plash va to'plash - soatiga bir marta, kuniga bir marta va boshqalar);</p> <p>24) tizim bilan ishlaydigan har bir xavfsizlik xodimi uchun ko'rilgan va ko'rib chiqilmagan hodisalarni ajratib ko'rsatish imkoniyati bilan ko'rish imkoniyati ;</p> <p>25) Mijoz konsolida hodisa haqidagi ma'lumotlarni ko'rishda quyidagi ma'lumotlar mavjud: qoidabuzarlikni sodir etgan foydalanuvchi, voqea sanasi va vaqti, xavfsizlik siyosatini qo'zg'atgan hujjat turi (elektron pochta, chop etish uchun</p>	<p>накопление и порционная отправка уведомлений с заданной периодичностью – раз в час, раз в сутки и т.д.);</p> <p>24) возможность просмотра всех инцидентов по выбранной политике безопасности в клиентской консоли с возможностью выделения просмотренных, непросмотренных инцидентов для каждого офицера безопасности, работающего с системой;</p> <p>25) при просмотре информации об инциденте в клиентской консоли доступна следующая информация: пользователь, допустивший нарушение, дата и время инцидента, тип документа, вызвавшего срабатывание политики безопасности (электронное письмо, файл, отправленный на печать и т.д.), содержание документа (электронного письма, переписки в IM-клиенте, файла и т.д.), вызвавшего срабатывание политики безопасности, а также другая дополнительная информация.</p> <p>26) возможность назначения статуса для инцидента (инцидент не расследован, расследование инцидента отложено, инцидент расследован, важный инцидент, неважный инцидент, ложное срабатывание);</p> <p>27) возможность присвоения цветовой категории инциденту</p> <p>28) возможность добавления комментария к инциденту</p> <p>29) возможность гибкого выборочного просмотра инцидентов по политике безопасности (например, показать только новые или непросмотренные инциденты; показать только последние 100 инцидентов; показать инциденты за ближайший месяц, но не более 20 последних; показать инциденты, имеющие статус «Важный» и зарегистрированные в течение последней недели и т.д.);</p> <p>30) возможность полного или выборочного удаления записей об инцидентах по политике безопасности (например, удалить все инциденты старше 10 дней; удалить последние N инцидентов; удалить все</p>	<p>10 days; delete the last N incidents; delete all incidents with the status "Investigated"; delete incidents based on data deleted from the database, etc.);</p> <p>31) ability to sort the list of incidents by various parameters (by relevance, by date/time, by local / remote user, by type/size of intercepted data, by incident status, etc.);</p> <p>32) ability to filter the list of incidents by various parameters: by status (for example, display only important ones), by data type (for example, display only incidents caused by sending information via mail protocols), by status (for example, display only unseen ones) – and by combinations of these parameters.</p> <p>33) the ability to export the list of incidents to a CSV, MS Excel, PDF, XML file (the following information about incidents is saved – type of intercepted data, local / remote user, date/time of interception, size, incident status, and other information);</p> <p>34) the ability to export intercepted data that triggered the security policy to files of the appropriate formats;</p> <p>35) maintaining a log of the security officer's actions with the ability to export log events;</p> <p>36) the following information is recorded in the event log: creating, duplicating, editing, deleting security rules, viewing and deleting an incident, changing incident statuses, etc.</p> <p>11. System scaling requirements:</p>
---	--	---



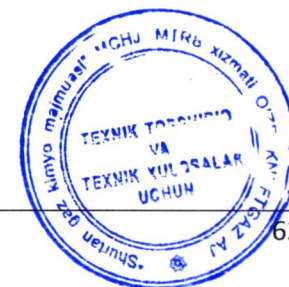
<p>yuborilgan fayl va boshqalar).), xavfsizlik siyosatini ishga tushirgan hujjatning mazmuni (elektron pochta , IM mijozidagi yozishmalar, fayl va boshqalar), shuningdek, boshqa qo'shimcha ma'lumotlar.</p> <p>26) hodisaga maqom berish qobiliyati (hodisalar tekshirilmagan, voqea tergovni kechiktirilgan, voqea tekshirilgan, muhim voqea, ahamiyatsiz hodisa, noto'g'ri ijobiy);</p> <p>27) hodisaga rang toifasini belgilash qobiliyati</p> <p>28) voqeaga sharh qo'shish qobiliyati</p> <p>29) xavfsizlik siyosatiga muvofiq intsidentlarni tanlab ko'rish qobiliyati (masalan, faqat yangi yoki ko'rib chiqilmagan hodisalarni ko'rsatish; faqat oxirgi 100 ta hodisani ko'rsatish; keyingi oydagi hodisalarni ko'rsatish, lekin oxirgi 20 dan ortiq bo'lmagan hodisalarni ko'rsatish; "Muhim" maqomi va oxirgi haftada ro'yxatdan o'tgan va hokazo);</p> <p>30) xavfsizlik siyosatiga muvofiq hodisalar yozuvlarini to'liq yoki tanlab yo'q qilish imkoniyati (masalan, 10 kundan ortiq bo'lgan barcha hodisalarni o'chirish; oxirgi N hodisani o'chirish; "Tekshirilgan" holati bilan barcha hodisalarni o'chirish; o'chirilgan ma'lumotlarga asoslangan hodisalarni o'chirish ma'lumotlar bazasi va boshqalar);</p> <p>31) hodisalar ro'yxatini turli parametrlar bo'yicha (muvofiqligi, sana/vaqt, mahalliy/masofaviy foydalanuvchi, ushlangan ma'lumotlarning turi/hajmi, hodisa holati va boshqalar bo'yicha) saralash imkoniyati;</p> <p>32) hodisalar ro'yxatini turli parametrlar bo'yicha filtrlash imkoniyati: holat bo'yicha (masalan, faqat muhimlarini ko'rsatish), ma'lumotlar turlari bo'yicha (masalan, faqat pochta protokollari orqali ma'lumot yuborish natijasida yuzaga kelgan hodisalarni ko'rsatish), holat bo'yicha (masalan, displey faqat ko'rilmaganlar) - va ushbu parametrlarning kombinatsiyasi bo'yicha;</p>	<p>инциденты, имеющие статус «Расследован»; удалить инциденты по данным, удаленным из БД, и т.д.);</p> <p>31) возможность сортировки списка инцидентов по различным параметрам (по релевантности, по дате/времени, по локальному/удаленному пользователю, по типу/размеру перехваченных данных, по статусу инцидента и т.д.);</p> <p>32) возможность фильтрации списка инцидентов по различным параметрам: по статусам (например, отобразить только важные), по типам данных (например, отобразить только инциденты, вызванные пересылкой информации по почтовым протоколам), по состоянию (например, отобразить только непросмотренные) – и по комбинациям этих параметров;</p> <p>33) возможность экспорта списка инцидентов в файл форматов CSV, MS Excel, PDF, XML (при этом сохраняется следующая информация об инцидентах – тип перехваченных данных, локальный/удаленный пользователь, дата/время перехвата, размер, статус инцидента, прочая информация);</p> <p>34) возможность экспорта перехваченных данных, вызвавших срабатывание политики безопасности, в файлы соответствующих форматов;</p> <p>35) ведение журнала (лога) действий офицера безопасности с возможностью экспорта событий журнала;</p> <p>36) в журнале событий регистрируется следующая информация создание, дублирования, редактирование, удаление правила безопасности, просмотр и удаление инцидента, изменения статусов инцидента и др.</p> <p>11. Требования к масштабированию системы:</p> <p>1) Все компоненты должны иметь возможность устанавливаться на один сервер или разнесены по разным, чтобы обеспечить нужную масштабируемость при одновременном контроле большого количества сотrudников;</p>	<p>1) All components should be able to be installed on the same server or distributed across different servers in order to provide the necessary scalability while simultaneously controlling a large number of employees;</p> <p>2) depending on the network configuration, the amount of intercepted data being processed, and other parameters, the system should scale flexibly to ensure control of a large and complex network, as well as load distribution on network and hardware resources;</p> <p>3) the ability to install multiple data interception servers - to parallelize the interception of several controlled Internet access channels;</p> <p>4) the ability to install multiple agent control servers– for monitoring different network segments or different groups of computers;</p> <p>5) ability to install multiple intermediate agent servers for network load balancing.</p> <p>6) the ability to organize a cluster for horizontal scaling of large loads across multiple servers;</p> <p>7) the ability to install multiple indexing servers - to optimize and distribute the load on the server and database;</p> <p>8) The system should provide full support for load balancing in multi-core and multiprocessor systems.</p> <p>12. System administration requirements:</p> <p>The system should include the following features:</p> <p>1) provide</p>
--	--	---



<p>33) hodisalar ro'yxatini faylga CSV, MS Excel, PDF, XML formatlarida eksport qilish imkoniyati (hodisalar haqida quyidagi ma'lumotlar saqlanadi - ushlangan ma'lumotlar turi, mahalliy/uzoq foydalanuvchi, ushlab turish sanasi/vaqti, hajmi, hodisa holati, boshqa ma'lumotlar);</p> <p>34) xavfsizlik siyosatini qo'zg'atgan ushlangan ma'lumotlarni tegishli formatdagi fayllarga eksport qilish imkoniyati;</p> <p>35) jurnal hodisalarini eksport qilish imkoniyati bilan xavfsizlik xodimlarining harakatlari jurnalini (jurnalini) yuritish;</p> <p>36) Voqealar jurnali quyidagi ma'lumotlarni qayd etadi: xavfsizlik qoidasini yaratish, takrorlash, tahrirlash, o'chirish, hodisani ko'rish va o'chirish, hodisa holatini o'zgartirish va hokazo.</p> <p>11. Tizimni masshtablashtirishga qo'yiladigan talablar:</p> <p>1) Barcha komponentlar bir serverga o'rnatilishi yoki bir vaqtning o'zida ko'p sonli xodimlarni kuzatib borishi uchun zarur miqyoslilikni ta'minlash uchun turli serverlar bo'ylab taqsimlanishi kerak;</p> <p>2) Tarmoq konfiguratsiyasiga, ushlangan ma'lumotlarning qayta ishlanishi hajmiga va boshqa parametrlarga qarab, tizim katta va murakkab tarmoqni boshqarishni, shuningdek, tarmoq va apparat resurslariga yuk taqsimotini ta'minlash uchun moslashuvchan tarzda kengaytirilishi kerak;</p> <p>3) bir nechta ma'lumotlarni ushlab turish serverlarini o'rnatish imkoniyati - bir nechta boshqariladigan Internetga kirish kanallarini tutib olishni parallellashtirish;</p> <p>4) bir nechta agent boshqaruv serverlarini o'rnatish qobiliyati - turli tarmoq segmentlarini yoki turli xil kompyuter guruhlarini boshqarish;</p> <p>5) tarmoq yukini muvozanatlash uchun bir nechta oraliq agent serverlarini o'rnatish imkoniyati.</p>	<p>2) в зависимости от конфигурации сети, от объема обрабатываемых перехваченных данных и других параметров, система должна гибко масштабироваться для обеспечения контроля большой и сложно организованной сети, а также распределения нагрузки на сетевые и аппаратные ресурсы;</p> <p>3) возможность установки нескольких серверов перехвата данных- для распараллеливания перехвата нескольких контролируемых каналов выхода в интернет;</p> <p>4) возможность установки нескольких серверов контроля агентов- для контроля разных сегментов сети или разных групп компьютеров;</p> <p>5) возможность установки нескольких промежуточных серверов агентов для балансировки нагрузки на сеть.</p> <p>6) возможность организации кластера для горизонтального масштабирования больших нагрузок по множеству серверов;</p> <p>7) возможность установки нескольких серверов индексирования- для оптимизации и распределения нагрузки на сервер и базу данных;</p> <p>8) Система должна обеспечивать полную поддержку распределения нагрузки в многоядерных и многопроцессорных системах.</p> <p>12. Требования к администрированию системы: Система должна предусматривать следующие возможности:</p> <p>1) обеспечивать</p> <p>2) централизованное управление всеми компонентами системы из двух консолей: единая консоль администратора и единая консоль пользователя (сотрудника службы ИБ);</p> <p>3) обеспечивать возможность шифрования трафика между консолями и сервером;</p> <p>4) централизованное подключение и настройка хранилищ информации для всех серверных компонентов системы;</p>	<p>2) centralized management of all system components from two consoles: a single administrator console and a single user console (an information security service employee);</p> <p>3) provide the ability to encrypt traffic between consoles and the server;</p> <p>4) centralized connection and configuration of information repositories for all server components of the system;</p> <p>5) the ability to disable automatic management of the system firewall;</p> <p>6) the ability to add a computer to the profile from the agent schema when configuring profiles for agents, as well as copy/move objects between profiles;</p> <p>7) the ability to configure automatic launch of programs and scripts when security rules are triggered;</p> <p>8) provide monitoring of the status of all server components and services of the system in real time, with the output of basic statistics for each of them, as well as managing the launch of server components and services from the system;</p> <p>9) support parallel operation of several users in the administrator console;</p> <p>10) the ability to authorize the system's servers in automatic and manual mode;</p> <p>11) the ability to replace the system logo in exported documents with a custom logo;</p> <p>12) the ability to translate the time zone to improve the quality of viewing data received from other time zones</p>
---	--	--



<p>6) bir nechta serverlar bo'ylab katta yuklarni gorizontall o'lchash uchun klasterlarni tashkil qilish imkoniyati;</p> <p>7) bir nechta indekslash serverlarini o'rnatish imkoniyati - server va ma'lumotlar bazasidagi yukni optimallashtirish va taqsimlash;</p> <p>8) Tizim ko'p yadroli va ko'p protsessorli tizimlarda yuk muvozanatini to'liq qo'llab-quvvatlashi kerak.</p> <p>12. Tizim boshqaruvida qo'yiladigan talablar: Tizim quyidagi imkoniyatlarni ta'minlashi kerak:</p> <p>1) ta'minlash</p> <p>2) ikkita konsoldan barcha tizim komponentlarini markazlashtirilgan boshqarish: bitta administrator konsoli va bitta foydalanuvchi konsoli (axborot xavfsizligi xizmati xodimi);</p> <p>3) konsollar va server o'rtasidagi trafikni shifrlash imkoniyatini ta'minlash;</p> <p>4) markazlashtirilgan ulanish va tizimning barcha server komponentlari uchun axborot omborlarini sozlash;</p> <p>5) tizim xavfsizlik devorini avtomatik boshqarishni o'chirish imkoniyati;</p> <p>6) agentlar uchun profilarni o'rnatishda agent sxemasidan profilga kompyuter qo'shish, shuningdek, ob'ektlarni profilga o'rtasida nusxalash/ko'chirish imkoniyati;</p> <p>7) xavfsizlik qoidalari ishga tushirilganda dasturlar va skriptlarni avtomatik ishga tushirishni sozlash imkoniyati;</p> <p>8) real vaqt rejimida tizimning barcha server komponentlari va xizmatlari holatini ularning har biri bo'yicha asosiy statistik ma'lumotlarni ko'rsatgan holda monitoringini ta'minlash, shuningdek tizimdan server komponentlari va xizmatlarini ishga tushirishni boshqarish;</p> <p>9) administrator konsolida bir nechta</p>	<p>5) возможность отключения автоматического управления системным брандмауэром;</p> <p>6) возможность при настройке профилей для агентов добавлять компьютер в профиль из схемы агентов, а также копировать/перемещать объекты между профилями;</p> <p>7) возможность настройки автоматического запуска программ и скриптов при срабатывании правил безопасности;</p> <p>8) обеспечивать наблюдение за состоянием всех серверных компонентов и сервисов системы в режиме реального времени, с выводом основной статистики по каждому из них, а также управление запуском серверных компонентов и сервисов из системы;</p> <p>9) поддерживать параллельную работу нескольких пользователей в консоли администратора;</p> <p>10) возможность авторизации серверов системы на в автоматическом и ручном режиме;</p> <p>11) возможность замены логотипа системы в экспортируемых документах на пользовательский логотип.</p> <p>12) возможность перевода часового пояса для улучшения качества просмотра данных полученных из других часовых поясов</p> <p>12. Требования к авторизации пользователей: Система должна предоставлять несколько вариантов авторизации</p> <p>1) на основании учетных записей Windows;</p> <p>2) на основании внутренней системы аутентификации.</p> <p>Система должна обладать следующими возможностями:</p> <p>1) возможность ограничения срока действия пароля (в днях), по истечении которого доступ к системе будет закрыт;</p> <p>2) возможность блокировки пользователя после 3-х неудачных попыток входа;</p>	<p>12. User authorization requirements: The system must provide several authorization options</p> <p>1) based on Windows accounts.</p> <p>2) based on the internal authentication system.</p> <p>The system must have the following features:</p> <p>1) the ability to limit the password validity period (in days), after which access to the system will be closed;</p> <p>2) the ability to block the user after 3 failed login attempts;</p> <p>3) the ability to save information about all authorization attempts in the log;</p> <p>4) the ability to set an additional password to change the settings of the Administrator console;</p> <p>5) the ability to automatically exit the consoles when the set idle time is exceeded;</p> <p>6) ability to automatically exit the console after the specified session duration expires.</p> <p>In the course of its operation, the system should not have a negative impact on the functioning of the Customer's application ICS.</p> <p>13. Requirements for suppliers:</p> <p>1) Authorization letter from the DLP solution manufacturer.</p> <p>2) Partner certificate, also from the manufacturer.</p>
---	--	--



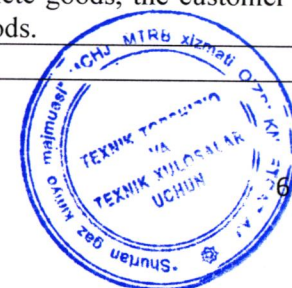
<p>foydalanuvchilarning parallel ishlashini qo'llab-quvvatlash;</p> <p>10) avtomatik va qo'lda rejimlarda tizim serverlarini avtorizatsiya qilish imkoniyati;</p> <p>11) eksport qilinadigan hujjatlarda tizim logotipini maxsus logotip bilan almashtirish imkoniyati.</p> <p>12) boshqa vaqt zonalaridan olingan ma'lumotlarni ko'rish sifatini yaxshilash uchun vaqt zonalarini tarjima qilish imkoniyati</p> <p>12. Foydalanuvchi avtorizatsiyasiga qo'yiladigan talablar:</p> <p>Tizim bir nechta avtorizatsiya imkoniyatlarini taqdim etishi kerak</p> <p>1) Windows hisoblari asosida ;</p> <p>2) ichki autentifikatsiya tizimiga asoslangan.</p> <p>Tizim quyidagi imkoniyatlarga ega bo'lishi kerak:</p> <p>1) parolning amal qilish muddatini cheklash imkoniyati (kunlarda), shundan so'ng tizimga kirish yopiladi;</p> <p>2) 3 ta muvaffaqiyatsiz kirish urinishidan keyin foydalanuvchini bloklash imkoniyati;</p> <p>3) jurnaldagi barcha avtorizatsiya urinishlari haqidagi ma'lumotlarni saqlash imkoniyati;</p> <p>4) Administrator konsoli sozlamalarini o'zgartirish uchun qo'shimcha parol o'rnatish imkoniyati;</p> <p>5) bo'sh vaqtdan oshib ketganda avtomatik ravishda konsollardan chiqish imkoniyati ;</p> <p>6) belgilangan seans davomiyligidan so'ng avtomatik ravishda konsoldan chiqish imkoniyati.</p>	<p>3) возможность сохранения информации обо всех попытках авторизации в журнале;</p> <p>4) возможность задания дополнительного пароля для изменения настроек консоли Администратора;</p> <p>5) возможность автоматического выхода из консолей при превышении заданного времени простоя;</p> <p>6) возможность автоматического выхода из консоли по истечении заданной продолжительности сеанса.</p> <p>В процессе своего функционирования система не должна оказывать негативного влияния на функционирование прикладных ИС Заказчика.</p> <p>13. Требования к поставщикам:</p> <p>1) Авторизационное письмо от производителя DLP решения.</p> <p>2) Сертификат партнера, так же от производителя.</p>	
---	--	--



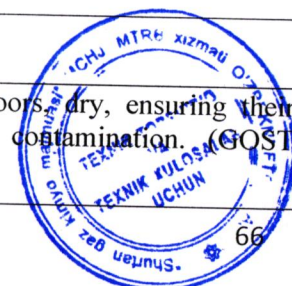
<p>Tizim o'z faoliyati davomida Buyurtmachining amaliy axborot tizimlarining ishlashiga salbiy ta'sir ko'rsatmasligi kerak.</p> <p>13. Yetkazib beruvchilarga qo'yiladigan talablar:</p> <p>1) DLP yechimini ishlab chiqaruvchidan ruxsatnoma</p> <p>2) Hamkor sertifikati, shuningdek ishlab chiqaruvchidan.</p>		
2.2 Belgilash talablari	2.2 Требования к маркировке	2.2 Labeling requirements
<p>Asosiy etiketka ma'lumotlari quyidagilarni o'z ichiga olishi kerak;</p> <ul style="list-style-type: none"> • tovar belgisi yoki ishlab chiqaruvchining nomi. • mahsulotning asosiy parametrlarining nominal qiymatlari. 	<p>Основные маркировочные данные должны содержать;</p> <ul style="list-style-type: none"> • товарный знак или наименование предприятия-изготовителя. • номинальные значения основных параметров товара. 	<p>Basic labeling data must contain;</p> <ul style="list-style-type: none"> • trademark or name of the manufacturer. • nominal values of the main parameters of the product.
2.3 Ishonchlilik talablari	2.3 Требования по надежности	2.3 Reliability requirements
<p>Texnik topshiriqning 2.1 bandi asosida har bir Tovar uchun ilova qilingan texnik hujjatlariga muvofiq kafolat muddati davomida.</p>	<p>В соответствии с технической документацией, прилагаемой к каждой единице товара в течении установленного гарантийного срока, согласно пункту 2.1 настоящего ТЗ.</p>	<p>In accordance with the technical documentation attached to each unit of goods within the established warranty period, in accordance with clause 2.1 of this technical assignment.</p>
2.4 Materiallarga bo'lgan talablar	2.4 Требования к материалам	2.4 Material requirements
<p>Har bir tovar birligiga ilova qilingan texnik hujjatlariga muvofiq, 2.1-bandga muvofiq</p>	<p>В соответствии с технической документацией, прилагаемой к каждой единице товара, согласно пункту 2.1</p>	<p>In accordance with the technical documentation attached to each unit of goods, in accordance with clause 2.1</p>
2.5 Atrof-muhit omillari ta'sirida barqarorlik va parametrlarga qo'yiladigan talablar	2.5 Требования к стабильности и параметрам при воздействии фактов внешней среды	2.5 Requirements for stability and parameters when exposed to environmental factors
<p>Har bir tovar birligiga ilova qilingan texnik hujjatlariga muvofiq, 2.1-bandga muvofiq</p>	<p>В соответствии с технической документацией, прилагаемой к каждой единице товара, согласно пункту 2.1</p>	<p>In accordance with the technical documentation attached to each unit of goods, in accordance with clause 2.1</p>
2.6 Quvvat/quvvat talablari	2.6 Требования к электропитанию/энергоснабжению	2.6 Power/Power Requirements
<p>Har bir tovar birligiga ilova qilingan texnik hujjatlariga muvofiq, 2.1-bandga muvofiq</p>	<p>В соответствии с технической документацией, прилагаемой к каждой единице товара, согласно пункту 2.1</p>	<p>In accordance with the technical documentation attached to each unit of goods, in accordance with clause 2.1</p>



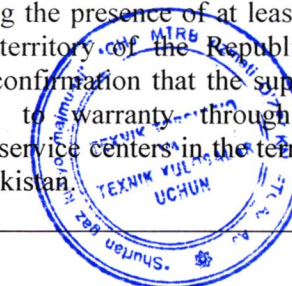
2.7 Komponentlar, dastlabki va ekspluatatsion xom ashyo / materiallar, shuningdek tayyor mahsulotlarga qo'yiladigan talablar	2.7 Требования к составным частям, исходным и эксплуатационным сырью/материалам, а также готовой продукции	2.7 Requirements for components, initial and operational raw materials/materials, as well as finished products
Har bir tovar birligiga ilova qilingan texnik hujjatlariga muvofiq, 2.1-bandga muvofiq	В соответствии с технической документацией, прилагаемой к каждой единице товара, согласно пункту 2.1	In accordance with the technical documentation attached to each unit of goods, in accordance with clause 2.1
2.8 O'lchami va qadoqlash talablari Mahsulot ishlab chiqaruvchidan standart eksport o'ramiga (yopiq, muhrlangan qadoqlangan, yaxshi holatda) qadoqlanishi kerak, bu mahsulotning uzoq muddatli saqlash va tashish paytida har qanday shikastlanishdan to'liq xavfsizligini ta'minlaydi, bunda bir nechta ortiqcha yuklarni hisobga oladi. yo'l. Qadoqlash yukni qo'lda tashish uchun mo'ljallangan bo'lishi va vaqtincha korroziyaga qarshi himoyaga ega bo'lishi kerak Sotuvchi uskunani noto'g'ri va/yoki ehtiyotsiz qadoqlash yoki himoya qilish natijasida yuzaga kelgan barcha yo'qotishlar va/yoki zararlar uchun javobgardir. Boshqa qadoqlash variantlari va o'lchamlari, ularning maqbulligini hisobga olgan holda, Buyurtmachi tomonidan qo'shimcha tasdiqlanishi kerak.	2.8 Требования к размерам и упаковке Товар должен быть упакован в экспортную стандартную упаковку (закрытая, герметичная упаковка, исправная) изготовителя, обеспечивающую полную её сохранность от всякого рода повреждений при длительном хранении и перевозке продукции с учётом нескольких перегрузок в пути. Упаковка должна быть рассчитана на обработку груза вручную, а также иметь временную антикоррозийную защиту Продавец несёт ответственность за все потери и/или убытки, возникшие из-за ненадлежащей и/или небрежной упаковки или защиты оборудования. Иные варианты и размеры упаковок подлежат дополнительному согласованию Заказчиком при условии их приемлемости.	2.8 Dimensions and packaging requirements The product must be packaged in standard export packaging (closed, sealed packaging, in good working order) from the manufacturer, ensuring its complete safety from any kind of damage during long-term storage and transportation of products, taking into account several overloads along the way. The packaging must be designed for manual handling of cargo and also have temporary anti-corrosion protection Seller is responsible for all losses and/or damages resulting from improper and/or careless packaging or protection of the equipment. Other packaging options and sizes are subject to additional approval by the Customer, subject to their acceptability.
3. QABUL QILISH VA QABUL QILISH QOIDALARIGA QO'YILADIGAN TALABLAR	3. ТРЕБОВАНИЯ ПО ПРАВИЛАМ СДАЧИ И ПРИЕМКИ	3. REQUIREMENTS FOR THE RULES OF DELIVERY AND ACCEPTANCE
3.1 Qabul qilish va qabul qilish tartibi Qabul qilish xaridorning binosida qabul komissiyasi tomonidan amalga oshiriladi. Noto'g'ri yoki to'liq bo'lmagan tovarlar yetkazib berilgan taqdirda, mijoz tovarni qaytarishga haqli.	3.1 Порядок сдачи и приемки Приемка осуществляется приемочной комиссией на территории покупателя. В случае поставки несоответствующего, некомплектного товара заказчик вправе осуществить возврат товара.	3.1 Order of delivery and acceptance Acceptance is carried out by the acceptance committee at the buyer's premises. In case of delivery of inappropriate or incomplete goods, the customer has the right to return the goods.



3.2 Tovarlarni etkazib berishda texnik va boshqa hujjatlarni buyurtmachiga topshirish talablari	3.2 Требования по передаче заказчику технических и иных документов при поставке товара	3.2 Requirements for the transfer of technical and other documents to the customer upon delivery of the goods
<p>Mahsulotga quyidagi hujjatlar ilova qilinishi kerak:</p> <ul style="list-style-type: none"> - mahsulotning muvofiqlik sertifikat; - miqdori, birlik narxi va umumiy summasi ko'rsatilgan tovar tavsifi bilan sotuvchining hisob-fakturas (schiyot-fakturas); - jo'natish stansiyasi belgisi va belgilangan manzil belgisi, Buyurtmachining nomi, amaldagi shartnomaning raqami va imzolangan sanasi ko'rsatilgan yuk oluvchi nomiga berilgan yo'l varaqasi; - faktura raqami va sanasi ko'rsatilgan tovarning kelib chiqishi to'g'risidagi sertifikat; - o'rama bo'yicha hisob-kitob hujjati; Yuk-mol hujjati; - mahsulot xavfsizligi ma'lumotlar varag'i - sertifikatlar (xalqaro standartlar ISO 9001, 14001, 45001, 50001, ishlab chiqaruvchining sifat sertifikati va/yoki xalqaro tan olingan laboratoriyalar va sinov markazlarining boshqa sertifikatlari). 	<p>Товар должен сопровождаться следующей документацией:</p> <ul style="list-style-type: none"> - сертификат соответствия товара; - счёт-фактура (инвойс) Продавца с описанием товара, указанием количества, цены единицы товара и общей суммы; - транспортная накладная, выпущенная на имя грузополучателя с отметкой станции отправления и отметкой пункта назначения, наименования Заказчика, номера и даты подписания действующего контракта; - сертификат о происхождении страны товара с указанием номера и даты инвойса; - упаковочный лист; - паспорт безопасности товара - сертификаты (международные стандарты ISO 9001, 14001, 45001, 50001, сертификат качества производителя и/или другие сертификаты международно-признанных лабораторий и центров испытаний). 	<p>The product must be accompanied by the following documentation:</p> <ul style="list-style-type: none"> - certificate of conformity of the product; - invoice (invoice) of the Seller with a description of the goods, indicating the quantity, unit price and total amount; - a waybill issued in the name of the consignee with a mark of the departure station and a mark of the destination, the name of the Customer, the number and date of signing of the current contract; - certificate of origin of the country of goods indicating the invoice number and date; - packing list; - product safety data sheet - certificates (international standards ISO 9001, 14001, 45001, 50001, manufacturer's quality certificate and/or other certificates of internationally recognized laboratories and testing centers).
4. TRANSPORT TALABLARI	4. ТРЕБОВАНИЯ К ТРАНСПОРТИРОВАНИЮ	4. TRANSPORT REQUIREMENTS
<p>Mahsulot yuqori sifatli bo'lishi kerak, sifat kafolati muddati etkazib berilgan kundan boshlab 12 oy. Yetkazib beruvchi kafolat muddati davomida nosoz mahsulotni bepul almashtirish majburiyatini oladi va bildirishnoma olingan kundan boshlab 10 kun ichida aniqlangan nosozlikni bartaraf etishi yoki nosoz mahsulotni almashtirishi shart.</p>	<p>Транспортирование товара в адрес Заказчика может осуществляться любым закрытым видом транспорта с соблюдением требований перевозки для данного вида транспорта. При транспортировке обязательно учесть манипуляционные знаки производителя.</p>	<p>The product must be of high quality, the quality guarantee period is 12 months from the date of delivery. The supplier undertakes to replace the faulty product free of charge during the warranty period and must eliminate the identified fault or replace the faulty product within 10 days from the date of receipt of the notification.</p>
	5. ТРЕБОВАНИЯ К ОБЪЕМУ И/ИЛИ СРОКУ ПРЕДОСТАВЛЕНИЯ ГАРАНТИЙ	
<p>Tovarlarni yopiq, quruq holda saqlanishi kerak, bu ularning shikastlanish va ifloslanishdan xavfsizligini ta'minlaydi. (GOST 51558-2014, GOST 15150)</p>	<p>Товары должны храниться в закрытых помещениях, сухими, с обеспечением их сохранности от повреждений и загрязнений. (ГОСТ 51558-2014, ГОСТ 15150)</p>	<p>Goods must be stored indoors dry, ensuring their safety from damage and contamination. (GOST 51558-2014, GOST 15150)</p>



	6. ТРЕБОВАНИЯ ПО РЕМОНТНО ПРИГОДНОСТИ	6. REQUIREMENTS FOR THE VOLUME AND/OR TERM OF GUARANTEES
<p>Mahsulot yuqori sifatli bo'lishi kerak, sifat kafolati muddati etkazib berilgan kundan boshlab 12 oy.</p> <p>Yetkazib beruvchi kafolat muddati davomida nosoz mahsulotni bepul almashtirish majburiyatini oladi va bildirishnoma olingan kundan boshlab 10 kun ichida aniqlangan nosozlikni bartaraf etishi yoki nosoz mahsulotni almashtirishi shart.</p>	<p>Товар должен быть качественным, срок гарантии качества – 12 месяцев с момента поставки.</p> <p>Поставщик берет на себя обязательства по бесплатной замене неисправного товара в период гарантийного срока и должен устранить выявленную неисправность или заменить неисправный товар в течение 10 дней с момента получения оповещения.</p>	<p>The product must be of high quality, the quality guarantee period is 12 months from the date of delivery.</p> <p>The supplier undertakes to replace the faulty product free of charge during the warranty period and must eliminate the identified fault or replace the faulty product within 10 days from the date of receipt of the notification.</p>
7. TA'MIRLASHGA TALABLAR	7. ТРЕБОВАНИЯ ПО РЕМОНТНО ПРИГОДНОСТИ	7. REQUIREMENTS FOR REPAIRABILITY
<p>Mahsulot dizayni ta'mirlanishi mumkin, texnik xizmat ko'rsatish xavfsiz va texnik xizmat ko'rsatish oson bo'lishi kerak.</p>	<p>Конструкция Товара должна быть ремонтно пригодной, безопасной в обслуживании и легко обслуживаемой.</p>	<p>The design of the Product must be repairable, safe to maintain and easy to maintain.</p>
11. TASNIF VA SIFATIGA QO'YILADIGAN TALABLAR	11. ТРЕБОВАНИЯ К КАЧЕСТВУ И КЛАССИФИКАЦИИ	11. REQUIREMENTS FOR QUALITY AND CLASSIFICATION
<p>Yetkazib beruvchi bu Yetkazib beruvchi rasmiy hamkor maqomiga ega ekanligi va taklif etilayotgan asbob-uskunalar va dasturiy ta'minotni xarid qilish tartibi talablariga muvofiq jo'natish huquqiga ega ekanligi to'g'risida Buyurtmachi nomiga ishlab chiqaruvchidan ruxsatnoma (MAF- manufacturer authorization form) taqdim etishi shart.</p> <p>Yetkazib beruvchi ishlab chiqaruvchidan O'zbekiston Respublikasi hududida kamida bitta xizmat ko'rsatish markazi mavjudligini tasdiqlovchi xatni, shu jumladan yetkazib beriladigan uskunaga ishlab chiqaruvchining O'zbekiston Respublikasi hududidagi rasmiy servis markazlari orqali kafolatlanishi lozimligini tasdiqlovchi xat taqdim etishi shart.</p>	<p>Поставщик должен предоставить авторизационное письмо от производителя (MAF- manufacturer authorization form) на имя Заказчика о том, что данный Поставщик имеет официальный партнерский статус и имеет право отгружать предлагаемую технику и программное обеспечение согласно требованиям закупочной процедуры.</p> <p>Поставщик должен предоставить письмо от производителя о наличии не менее одного сервисного центра на территории Республики Узбекистан, в том числе с подтверждением, что поставляемая техника подлежит гарантии через официальные сервисные центры производителя на территории Республики Узбекистан.</p>	<p>The Supplier must provide an authorization letter from the manufacturer (MAF-manufacturer authorization form) addressed to the Customer stating that this Supplier has official partner status and has the right to ship the proposed equipment and software in accordance with the requirements of the procurement procedure.</p> <p>The supplier must provide a letter from the manufacturer confirming the presence of at least one service center in the territory of the Republic of Uzbekistan, including confirmation that the supplied equipment is subject to warranty through the manufacturer's official service centers in the territory of the Republic of Uzbekistan.</p>



<p>Yetkazib beruvchida O'zbekiston Respublikasi "Kiberxavfsizlik markazi" davlat unitar korxonasi taqdim etilgan faol DLP dasturiy ta'minoti uchun ekspertiza sertifikatini bo'lishi kerak.</p> <p>DLP dasturiy ta'minoti O'zDST 2814:2024 davlat standart talablariga javob berishi kerak.</p> <p>Mahsulot yuqori sifatli bo'lishi va mo'ljallangan maqsadiga muvofiq talablarga javob berishi, zarur iste'mol xususiyatlari va texnik xususiyatlari, ekologik va sanoat xavfsizligi xususiyatlariga ega bo'lishi kerak.</p> <p>Mahsulot sifatini ishlab chiqaruvchi tomonidan berilgan sertifikat bilan tasdiqlanishi kerak.</p> <p>Yetkazib beruvchi Buyurtmachiga u tomonidan sotib olingan tovarlar ushbu uskunaning buyurtmachisi tomonidan e'lon qilingan uskunaning texnik xususiyatlariga mos kelishini kafolatlaydi.</p> <p>Sifat kafolati muddati kamida 3 yil.</p>	<p>Поставщик должен иметь сертификат экспертизы на поставляемое активное ПО DLP от ГУП «Центр кибербезопасности» РУз.</p> <p>ПО DLP должно соответствовать требованиям государственного стандарта O'zDST 2814:2024.</p> <p>Товар должен быть качественным и отвечающим предъявляемым к нему требованиям назначения, имеющим необходимые потребительские свойства и технические характеристики, характеристики экологической и промышленной безопасности.</p> <p>Качество товара должно подтверждаться сертификатом качества, выданного на заводе изготовителя.</p> <p>Поставщик гарантирует Заказчику, что приобретенный им товар соответствует техническим характеристикам оборудования, заявленным заказчиком данного оборудования.</p> <p>Срок гарантии качества не менее 3 лет.</p>	<p>The supplier must have an examination certificate for the supplied active DLP software from the State Unitary Enterprise "Cyber Security Center" of the Republic of Uzbekistan.</p> <p>DLP software must comply with the requirements of the state standard O'zDST 2814:2024.</p> <p>The product must be of high quality and meet the requirements for its intended purpose, have the necessary consumer properties and technical characteristics, environmental and industrial safety characteristics. The quality of the product must be confirmed by a quality certificate issued by the manufacturer.</p> <p>The Supplier guarantees to the Customer that the goods purchased by him correspond to the technical characteristics of the equipment declared by the customer of this equipment.</p> <p>The quality guarantee period is at least 3 years.</p>
--	---	---

12. YETKAZIB BERISH MIQDORI, JOYI VA MUDDATI UCHUN TALABLAR	12. ТРЕБОВАНИЯ К КОЛИЧЕСТВУ, КОМПЛЕКТАЦИИ, МЕСТУ И СРОКУ (ПЕРИОДИЧНОСТИ) ПОСТАВКИ	12. REQUIREMENTS TO THE QUANTITY, PACKAGING, PLACE AND TERM (FREQUENCY) OF DELIVERY
<p>Ushbu texnik spetsifikatsiyaning 2.1-bandiga muvofiq konfiguratsiya.</p> <p>Mahsulot GOST 2.601-2013 ga muvofiq operatsion hujjatlar bilan birga bo'lishi kerak. Operatsion hujjatlar texnik ma'lumotlarning kerakli miqdorini va o'rnatish va ishlatish bo'yicha ma'lumotlarni o'z ichiga olishi kerak, bunda texnik xizmat ko'rsatish hajmi va tavsiya etilgan chastotasi ko'rsatilgan.</p> <p>Yetkazib berish vaqti va joyi etkazib beruvchining taklifi va shartnoma bilan belgilanadi.</p>	<p>Комплектация согласно пункту 2.1 данного технического задания.</p> <p>К товару должна прилагаться эксплуатационная документация по ГОСТ 2.601-2013.</p> <p>Эксплуатационная документация должна содержать необходимое количество технических данных и сведений по монтажу и эксплуатации с указанием объема и рекомендуемой периодичности технического обслуживания.</p> <p>Время и место доставки определяется предложением поставщика и договором.</p>	<p>Configuration in accordance with clause 2.1 of this technical specification.</p> <p>The product must be accompanied by operational documentation in accordance with GOST 2.601-2013.</p> <p>The operational documentation must contain the required amount of technical data and information on installation and operation, indicating the scope and recommended frequency of maintenance.</p> <p>The time and place of delivery is determined by the supplier's offer and the contract.</p>



Axborot xavfsizligi bo'limi boshlig'i:

Q. Rustamov

AKT xizmati boshlig'i:

R. Normatov

Ishonchlilikni boshqarish xizmati boshlig'i:

T. Diyorov

Bosh metrolog:

X. Maxmudov

Material texnik resurslarni boshqarish guruhi muhandisi:

Sh. Nizamov

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.

