Приложение 1

к извещению об осуществлении закупки

**Описание объекта закупки**

**1.** **Предмет муниципального контракта**: оказание услуг по передаче неисключительных прав на использование программного обеспечения для расследования инцидентов внутренней информационной безопасности (код ОКПД2 63.11.13.000).

**2.** **Перечень предоставляемых услуг:**

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование услуг | Характеристика предоставляемых услуг | Кол-во |
| 1 | Передача неисключительных прав на использование программного обеспечения для расследования инцидентов внутренней информационной безопасности | Передача неисключительных прав на использование программного обеспечения для расследования инцидентов внутренней информационной безопасности, бессрочно.Основные функции программного обеспечения: • предотвращение утечки или потери конфиденциальных данных; • контроль действий пользователей ПК; • учёт рабочего времени пользователей; • анализ сотрудников на лояльность компании; • анализ возникающих угроз в автоматическом режиме. | 20 штук |

**3. Общие требования к программному обеспечению:**

• Программное обеспечение должно поддерживать работу в сетях любой конфигурации и сложности;

• Программное обеспечение должно поддерживать подключение агентов к серверу через сеть Интернет, в том числе в случаях организации подключения через VPN;

• В целях импортозамещения серверная и агентская части должны поддерживать возможность установки на отечественные операционные системы (семейство Linux). Должны использоваться базы данных либо свободного распространения, либо включённые в Единый реестр отечественных программ;

• Серверная часть программного обеспечения, реализующая функционал управления агентами, хранения собираемой информации и формирования отчётов должна поддерживать возможность установки всех необходимых компонентов на одном сервере;

• Должна быть возможность предоставления серверных компонентов в едином установочном ISO-образе;

• Должна предоставляться возможность установки серверных компонентов на ОС Ubuntu 18.04, 20.04 без установки дополнительных зависимостей;

• Для сбора информации должен устанавливаться только один агент (модуль) мониторинга на один ПК;

• Агент должен быть унифицирован для рабочих станций и терминальных серверов;

• В процессе своего функционирования, система (её агенты) не должна оказывать значимого (существенного) негативного влияния на функционирование защищаемых рабочих станций и серверов;

• Для доступа к собранной информации, управления политиками безопасности, настройки конфигурации агента должна использоваться единая консоль администратора с возможностью гибкого разграничения полномочий;

• Система должна иметь возможность вертикального и горизонтального масштабирования, устанавливаться и выполнять свои функции на современных системах виртуализации;

• Задержка обновления отчётов не должна превышать 15 минут при максимальной загрузке системы на рекомендованной аппаратной конфигурации.

**4. Требования к лицензированию:**

• Лицензирование должно производиться по количеству одновременно активных рабочих станций и/или пользователей;

• Должна присутствовать возможность гибкого лицензирования с переустановкой лицензии с одной рабочей станции или пользователя на другую рабочую станцию или пользователя неограниченное количество раз;

• Серверные компоненты не должны требовать обязательного наличия у заказчика дополнительных платных лицензий на программное обеспечение;

• Назначенные и отозванные лицензии, должны наглядно и визуально отображаться в консоли сервера.

**5. Требования к поддерживаемые операционным системам для агента.**

• Агент для Windows в 32-х или 64-х битном варианте с поддержкой следующих операционных систем – Windows Vista SP2, Windows 7 SP2, Windows 8, Windows 8.1 SP1, Windows 10. Агент так же должен поддерживать работу терминальных серверов в следующих операционных системах: Windows 2008, Windows 2008 R2, Windows 2012 R2, Windows 2016;

• Агент для Linux с поддержкой следующих операционных систем: CentOS, Ubuntu Dekstop, Debian, Gentoo linux, Astra linux, Arch linux, Rosa linux, AltLinux и другие Linux-like дистрибутивы;

• Агент для MacOS с обязательной поддержкой операционных систем: macOS 10.13, 10.14, 10.15, 11.х(Bigsur), 12.x(Montray), 13.x(Ventura);

• Поддержка операционных систем утилитой удалённой установки: Windows Vista SP2, Windows 7 SP2, Windows 8, Windows1 SP1, Windows 10.

**6. Требования к архитектуре программного обеспечения.**

• Должно обеспечиваться выполнение OLAP запросов в реальном режиме времени;

• Для высокоскоростного исполнения аналитических запросов в реальном режиме времени система должна иметь возможность переключения на использование дополнительной базы данных типа columnar store, в частности, включённую в Единый реестр отечественных программ БД ClickHouse;

• Метаданные должны храниться в БД, а файлы в отдельном файловом хранилище;

• Хранение файлов должно обеспечиваться в режиме ротации типа «кольцевой буфер» с возможностью автоматического перемещения на долговременное хранилище;

• Протокол обмена между агентом и сервером, а также доступ в панель администратора должен быть защищён шифрованием семейства TLS (на основе клиентских сертификатов);

• Должна обеспечиваться возможность получения информации от сервера сбора данных посредством формирования API-запросов (REST API, Database API и взаимодействие с моделью данных);

• Должна существовать возможность передачи данных в SIEM-системы;

• Должна иметься возможность передачи данных со СКУД в БД с возможностью анализировать собранные данные в системе на основе событий и отчётов;

• Должна иметься возможность импорта табеля по отсутствию сотрудников из 1С для формирования календаря;

• Интерфейс администратора должен обеспечивать вывод суммарной (агрегированной) информации на основе больших массивов данных, структурированных по многомерному принципу;

• Агент должен уметь отправлять собранные данные не менее, чем на два различных адреса сервера как по доменному имени, так и по адресам IPv4 и IPv6;

• Агент должен иметь возможность настройки правил мониторинга, по которым необходимые события не будут индексироваться;

• Агент должен иметь возможность получения пароля от сервера, для защиты от привилегированного пользователя с правами администратора;

• Должна быть возможность использовать Rust для обработки данных;

• Должна быть возможность использовать парсер контента на основе Apache Tika;

• Должна присутствовать возможность настройки сбора данных посредством фильтрации трафика на ICAP-сервере;

• Должно быть предусмотрено горизонтальное масштабирование сервера за счёт использования кластерной архитектуры, единая консоль для работы с данными на всех кластерах и единая точка распространения политик.

**7. Требования к администрированию системы:**

 Должна присутствовать панель управления администратора внутри web-интерфейса сервера со следующими возможностями:

• Интерфейс администратора должен поддерживать распределение полномочий, основанных на ролях, в том числе заданных в Active Directory;

• Должен быть интерфейс настройки подключения Active Directory;

• Авторизация пользователей или администраторов в веб-интерфейсе консоли, распределение ролей, назначение прав доступа к данным и конфигураций мониторинга должны быть возможны с учётом пользователей и групп из Active Directory;

• Предоставление доступа администраторам для доступа к данным как к группам пользователей, на основе данных из Active Directory, так и к конкретным аккаунтам;

• Возможность ограничения доступа администраторам к конкретным данным и событиям на основе их атрибутов;

• Установка и удаление агентов должны производиться как централизовано с помощью групповых политик Active Directory с помощью инсталлятора модуля агента, так и локально, путём запуска инсталлятора на машине пользователя;

• Должна быть возможность мониторинга состояния агента;

• Возможность настройки контроля пользователей по параметрам OU;

• Возможность синхронизации данных с Active Directory по нескольким OU;

• Поддержка нескольких доменов Active Directory в рамках единой системы;

• Должна быть возможность планировки установки агентов в локальной сети по расписанию;

• Должны быть возможность исключения IP - адресов в рамках сканирования локальной сети для удалённой установки агента;

• Должна иметься возможность установки агентов контроля на VDI с возможностью генерации уникального идентификатора машины в базе данных сервера;

• Должна быть возможность просмотра активных или готовых к установке компьютеров, с возможностью выбора конкретного или нескольких рабочих мест с выполнением следующих действий: выбор всех компьютеров, освобождение лицензии, назначение лицензии, автоматическое назначение лицензии, вызов деинсталляции агента, отмена деинсталляции агента, заблокировать или разблокировать ПК, обновить агента до последней версии, отменить текущее обновление, установить агента, проверить агента, назначить свойства (выбор конфигурации и группы);

• Должна быть возможность взаимосвязи рабочих станций и сотрудников, которые на них работали;

• Должны быть возможны выбор и установка согласно списку ПК из Active Directory путём подключения инсталлятора агентов к контроллеру домена для выбора компьютеров, назначенных на установку;

• Должен присутствовать автоматический отзыв лицензии с отключённых в AD пользователей;

• Должна существовать возможность после подтверждения администратором системы проводить централизованное обновление агентов автоматически;

• Должна присутствовать возможность удаления всех неустановленных агентов;

• Должна обеспечиваться возможность настройки длительности хранения информации в базе данных, в том числе возможность автоочистки файлового хранилища без удаления данных из базы данных;

• Должна иметься возможность шифрования локальной базы данных агента;

• Должна иметься возможность сохранить локальную базу данных агента после его удаления;

• Должна присутствовать возможность назначения агентам резервного адреса для передачи данных;

• Должно формироваться предупреждение о заполнении дисков БД, дополнительной БД и файлового хранилища;

• Должны создаваться уведомления администратору системы о системных событиях (системные ошибки, предупреждения, срабатывания политик безопасности и т.д.);

• Должна обеспечиваться настройка передачи на сервер максимального размера единовременного объёма перехваченных данных от агента;

• Должна быть возможность ограничения скорости передачи данных от агента серверу;

• Должен вестись журнал действий администраторов системы непосредственно в консоли администратора;

• Должна происходить автосмена имени агента, при смене названия компьютера;

• Должна быть возможность сменить IP-адрес и порт сервера на агенте без его переустановки;

• Должна быть поддержка работы агента и сервера на одном порту и IP-адресе, но с разными SNI в сертификате;

• Должна обеспечиваться возможность скачать из интерфейса администрирования агенты версии Windows, Linux и MacOS, а также утилиту удалённой установки;

• В веб-консоли должны указываться версии агентов, которые будут использоваться при установке;

• Управление сбором данных должно осуществляться путём назначения конфигураций пользователей и компьютеров с возможностью их добавления, изменения и удаления;

• Для предустановленных (стандартных) конфигураций должна быть возможность сброса на изначальные параметры (значения по умолчанию);

• Конфигурации пользователей должны назначаться для определяемых в ней пользователей и иметь настройки правил использования USB/CD устройств: полную блокировку, разрешать только чтение и задавать перечень таких устройств по их идентификаторам;

• Должна присутствовать глобальная конфигурация с возможностью настройки модулей мониторинга для всех пользователей, независимо от назначенной им конфигурации;

• Должна быть возможность настройки параметров отправки почты в настройках сервера, которая используется для отправки всех отчётов, дашбордов и уведомлений;

• Должна быть возможность указывать точное время отправки отчёта или дашборда на почту;

• Должна быть реализована возможность отправки отчётов, дашбордов и уведомлений в форматах PDF, HTML и EXCEL;

• Должно быть организовано хранилище паролей, использующихся при установке агентов через веб-интерфейс, с возможностью сохранения и редактирования паролей;

• Должна быть возможность разбиения базы данных по месяцам (шардирование) и функционал удаления данных за выбранный месяц из интерфейса администратора;

• Должны фиксировать и быть доступными для просмотра изменения в настройках и конфигурациях, производимые администраторами в веб-консоли;

• Должны фиксироваться в консоли действия администратора по просмотру определённой информации и отчётов;

• Должна предоставляться возможность выгрузки и фильтрации «последних действий администраторов системы»;

• Должен быть доступен просмотр количества событий в очереди на обработку сервером с указанием названия политик и парсеров;

• Должна быть возможность выгрузки логов сервера, конфигураций агентов, правил мониторинга, фильтров и политик;

• Должна быть доступна информация о лицензии, сроках её активации и истечения, количестве компьютеров, которые могут подключаться к серверу и количестве подключённых компьютеров;

• Должна быть возможность просмотра собранных данных при истекшей лицензии;

• Должна быть функция ручного запуска пересчёта всех отчётов;

• Должна присутствовать возможность удаления всех пользовательских настроек, с возвращением сервера к первоначальным настройкам;

• Должна быть возможность перезапуска всех служб, связанных с программным обеспечением для расследования инцидентов внутренней информационной безопасности;

• Должен быть выбора языка веб-интерфейса (русский или английский);

• Должен быть выбор визуальной темы веб-интерфейса;

• Должна выводиться информация о версии сервера, версии Windows, Linux и MacOS агента;

• Должен быть интерфейс смены пароля администратора и функция завершения работы с интерфейсом (завершения сеанса текущего пользователя системы);

• Возможность точечного удаления данных из БД, согласно заданным параметрам данных, напрямую из консоли администрирования;

• Единое поле контроля и настройки уведомлений по инцидентам и регулярным рассылкам;

• Использование клавиш для прокрутки событий;

• Должны отображаться удачные и неудачные попытки входа в систему;

• Должен отображаться выход администратора из системы;

• Должен логироваться факт выгрузки данных из системы с детализацией выгруженных данных;

• Должна логироваться смена пароля администратора системы;

• Должна завершаться сессия, при изменении пароля администратора системы;

• Должны отключаться отсутствующие администраторы при синхронизации с AD;

• При неверном вводе пароля должен ограничиваться доступ с адреса, с которого была неуспешная авторизация;

• Должны фиксироваться и логироваться операции снятия и назначения лицензий для мониторинга как для пользователя, так и для агента с детализацией причины отзыва;

• Должна иметься возможность включить автоматическое освобождение или отзыв лицензии мониторинга неактивных пользователей с логированием данной операции;

• Возможность уведомления при появлении новой машины под мониторингом;

• Возможность просмотра и контроля правил, применяемых к работе агента в его профиле;

• Возможность настройки времени выхода из сессии администратора, при отсутствии активности;

• Обозначение активных элементов обработки данных в веб-консоли;

• Проверка пароля на сложность при создании пароля администратора, не позволяющая использовать слабые пароли;

• Должны иметься возможность управления сервером из веб консоли, в том числе и в рамках планового выполнения заданных команд;

• Должна иметься возможность на стороне сервера изменить агенту адрес для передачи данных;

• Должна иметься возможность выгрузки информации по контролируемым агентам, пользователям и их статусом в формате CSV;

• Должна иметься возможность отправки уведомления на почту администратора системы при невозможности получения лицензии агентом\пользователем;

• Должна иметься возможность подключения сервиса Graphana для мониторинга состояния системы.

**8. Требования к функциональным возможностям системы.**

Должны фиксироваться следующие типы событий действий пользователя:

• вход/выход из системы;

• удаленный вход/выход из системы;

• активность пользователя в приложениях и на сайтах;

• подключение к удаленному рабочему столу, перехват управления;

• запись видео рабочего стола;

• снимок экрана;

• снимок с веб-камеры;

• операции с файлами;

• теневые копии перехваченных файлов;

• печать документов;

• буфер обмена;

• ввод с клавиатуры;

• реестр оборудования;

• реестр установленных программ;

• запись с микрофона;

• посещение веб-ресурсов;

• сетевые подключения;

• интернет-мессенджеры;

• почта;

• установка ПО;

• запуск и завершение приложения;

• внешние диски и устройства;

• присутствие на рабочем месте;

• Подключение к беспроводным сетям;

• Операции по протоколу FTP;

• Действия администратора;

• Данные веб-форм;

• Линукс лог;

• Системный лог;

• СКУД;

• Терминал Linux;

• Файловый сканер.

Должны фиксироваться следующие атрибуты логируемой информации:

• агент;

• Назначенная конфигурация;

• IP-адрес;

• дополнительная метка;

• название ПК;

• статус;

• версия OS;

• версия агента;

• учётная запись пользователя;

• комментарий;

• отдел;

• тип сессии;

• организация;

• телефон;

• полное имя;

• Группа AD;

• почта;

• должность;

• домен;

• руководитель;

• пользователь;

• пропуск;

• приложение;

• полный путь;

• заголовок;

• название;

• описание;

• сайт;

• полный домен;

• протокол;

• URL;

• основной домен;

• тип контента;

• сетевая активность;

• IP адрес;

• сетевой порт;

• файл;

• хеш файла;

• операции;

• имя файла;

• удалённый пользователь;

• имя файла источника;

• расширение источника;

• контент извлечён;

• путь источника;

• метка;

• тип контента;

• тип устройства;

• канал перехвата;

• тип устройства источника;

• расширение;

• расширение источника;

• путь;

• устройства;

• ID устройства;

• Маркер;

• Тип устройства;

• класс устройства;

• тип устройства;

• серийный номер;

• производитель;

• переписка;

• домен получателя;

• отправитель;

• все получатели;

• формат сообщения;

• направление;

• домен отправителя;

• получатель;

• чаты;

• канал общения;

• дата;

• час суток

• часовой пояс;

• день недели;

• по годам;

• по месяцам;

• по дням;

• по часам;

• по минутам;

• инсталляции;

• операция;

• версия;

• поставщик;

• обновление;

• продукт.

Должны индексироваться системой файлы следующих форматов:

• Adobe Acrobat (\*.pdf);

• Ansi Text (\*.txt);

• ASCII Text;

• CSV (Comma-separated values) (\*.csv);

• EML files (электронные письма, сохраненные Outlook Express) (\*.eml);

• HTML (\*.htm, \*.html);

• JPEG (метаданные) (\*.jpg);

• MHT-архивы (HTML-архивы, сохраненные Internet Explorer) (\*.mht);

• MSG files (электронные письма, сохраненные Outlook) (\*.msg);

• Microsoft Excel (\*.xls) Microsoft Excel 2003 XML (\*.xml);

• Microsoft Excel 2007 и выше(\*.xlsx);

• Microsoft Outlook Express 5 и 6: базы сообщений (\*.dbx);

• Microsoft PowerPoint (\*.ppt);

• Microsoft Rich Text Format (\*.rtf);

• Microsoft Word for DOS (\*.doc);

• Microsoft Word for Windows (\*.doc);

• Microsoft Word 2003 XML (\*.xml);

• Microsoft Word 2007 и выше(\*.docx);

• Multimate version 4 (\*.doc);

• OpenOffice версий 1, 2 и 3: документы, электронные таблицы и презентации (\*.sxc, \*.sxd, \*.sxi, \*.sxw, \*.sxg, \*.stc, \*.sti, \*.stw, \*.stm, \*.odt, \*.ott, \*.odg, \*.otg, \*.odp, \*.otp, \*.ods, \*.ots, \*.odf) (включая OASIS Open Document Format для офисных приложений).

**9. Требования к перехвату в контролируемых каналах.**

Должна обеспечиваться возможность контроля электронной почты, в частности:

• Перехват почтовых сообщений по протоколам – SMTP/SMTPs, POP3/POP3s, IMAP/IMAPs, MAPI;

• Возможность перехватывать почтовые сообщения IBM Lotus Notes посредством сбора почты из IMAP-почтового ящика;

• Должна присутствовать связь между сообщениями полученными посредством IMAP и доменными пользователями в системе;

• Перехват и анализ файлов-вложений почтовых сообщений;

• Мониторинг почтовых сообщений и вложений с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Возможность перехватывать неотправленные сообщения сохранённые в виде черновиков;

• Поиск по заданным параметрам текста и атрибутам почтовых сообщений, и тексту их вложений;

• Возможность выгрузки писем в следующих видах: документ Excel, HTML, CSV, изображение в формате PNG;

• Возможность скачать переписку целиком в ZIP архиве или распечатать на принтере;

• Возможность построения графа переписки, с ручной настройкой параметров отображаемой информации.

Должна обеспечиваться возможность мониторинга обмена информацией посредством мессенджеров (IM-клиентов):

• Должен происходить перехват текстовых сообщений по протоколам (Skype, Telegram, WhatsApp, ICQ/QIP, Jabber, Mail.ru Агент, MS Teams, Bitrix 24 Desktop, Express, VKTeams);

• Должен происходить перехват отправляемых файлов для (Skype, Telegram, WhatsApp, Bitrix24 Desktop, Express, VKTeams);

• Должна быть возможность задания особых критериев мониторинга и организация мониторинга текстовых сообщений и файлов;

• В случае обнаружения передачи информации по заданным критериям мониторинга в сообщениях и файлах должна быть возможность организовать отправку уведомления одному или нескольким ответственным за информационную безопасность лицам;

• Должен осуществляться поиск по заданным параметрам текста и атрибута сообщений и (содержимого) файлов, переданных через IM-клиенты.

Должен осуществляться контроль информации по протоколам HTTP/HTTPs, в частности:

• Перехват данных по протоколам HTTP/HTTPS;

• Перехват и анализ сообщений и файлов, отправляемых в блоги, форумы, файлообменные сервисы и иные веб-службы;

• Перехват исходящих сообщений VK;

• Перехват исходящих электронных писем и вложений, переданных или полученных через почтовые веб-сервисы (как минимум, mail.yandex.ru, mail.google.com, mail.rambler.ru, e.mail.ru, outlook.com);

• Перехват и мониторинг поисковых запросов пользователя;

• Сохранение адресов всех страниц (URL), посещённых пользователем;

• Мониторинг сообщений и файлов с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Поиск по тексту и атрибутам сообщений и файлов, переданных и перехваченных по протоколу HTTP(S);

• Возможность блокировки посещения веб-ресурсов;

• Исключение мониторинга сайтов по чёрным и белым спискам;

• Мониторинг всех посещённых сайтов и времени, проведённого на веб-страницах;

• Возможность формирования различных отчётов по времени активности пользователя за ПК. Рейтинг посещённых сайтов за день, хронология событий за выбранный временной интервал для отдельного пользователя или для групп пользователей или всей организации в следующих видах: документ Excel, HTML, CSV, формат PNG;

• Возможность скачать отчёты целиком в ZIP архиве или распечатать на принтере.

Должен быть возможен контроль информации, передаваемой по протоколу FTP, в частности:

• Перехват файлов, загруженных или переданных по FTP-протоколу, а также переданных по зашифрованному FTP-протоколу (FTPs);

• Мониторинг файлов с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Мониторинг и перехват файлов и паролей по протоколу FTP/FTPs с последующим контекстным анализом перехваченных файлов.

Должна быть возможность контроля информации, отправляемой на печать, а именно:

• Перехват документов, отправляемых на печать;

• Извлечение и анализ текста отправленных на печать документов;

• Мониторинг документов, отправленных на печать с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Поиск по заданным параметрам текста и атрибута отправленных на печать файлов;

• Возможность выгрузки в виде документа Excel, HTML, CSV, в формате PNG;

• Возможностью скачать в ZIP архиве или распечатать на принтере.

Должен происходить контроль внешних накопителей со следующими возможностями:

• Теневое копирование файлов, отправляемых на внешние носители, в том числе, жёсткие диски, карты памяти и другие съёмные накопители, подключённые, как USB-устройства, CD/DVD;

• Контроль подключений и отключений USB-устройств;

• Контроль подключения, отключения и операций с RuToken с фиксацией уникального ID;

• Возможность настройки правил доступа для USB-устройств по их уникальным идентификаторам, в том числе с разрешением только для чтения;

• Возможность блокировки CD-накопителей;

• Возможность настройки правил блокировки USB-устройств по чёрным или белым спискам, по классам устройств и по группе;

• Перехват листинга и теневое копирование файлов при подключении внешних носителей, с возможностью настройки правила для перехвата по указанным расширениям файлов;

• Мониторинг случаев передачи файлов на внешние носители с содержанием информации, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Мониторинг случаев использования внешних устройств с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Аудит событий копирования файлов на внешние накопители: фиксируется имя файла, пользователь, дата, время, приложение, полный путь и данные устройства;

• Возможность поиска по тексту и атрибутам перехваченных файлов, отправленных на внешние носители.

• Возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей;

• Возможность блокировки накопителей при передаче данных, объемом превышающие заданное пороговое значение;

• Возможность контроля файловых операций при работе пользователя с CD/DVD с возможностью создания теневых копий.

• Возможность управлять доступом к внешним устройствам посредством выделенным менеджером внешних носителей информации.

• Возможность присваивать каждому внешнему накопителю метку и ответственного сотрудника.

Должны присутствовать следующие возможности контроля информации, передаваемой в облачные хранилища (файловый канал):

• Возможность осуществления контроля по следующим облачным хранилищам – Dropbox, Яндекс.Диск, Google Drive, Nextcloud, ownCloud, OneDrive;

• Теневое копирование файлов, отправляемых в облачные хранилища с рабочей станции сотрудника с установленным агентом;

• Мониторинг случаев передачи файлов в облачные хранилища с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Аудит событий отправки файлов в облачные хранилища: фиксируется имя файла, пользователь, дата, время и имя облачного сервиса;

• Возможность поиска по тексту и атрибутам перехваченных файлов, отправленных в облачные хранилища;

• Возможность настройки размера хранилища для теневых копий на локальных компьютерах пользователей.

Должен осуществляться контроль файлов и файловой активности, а именно:

• Контроль файловых операций (Запись, Копирование, Оглавление диска, Отключение, Очистка корзины, Перезапись, Переименование, Перемещение, Переименование и перемещение, Подключение, Создание, Удаление, Чтение);

• Перехват файлов и/или списка файлов со съёмных носителей, включая CD/DVD-диски при их подключении по заданным шаблонам расширений файлов;

• Сохранять теневые копии файлов, отправленных за информационный периметр контролируемой рабочей станцией;

• Последующий поиск по тексту и атрибутам перехваченных файлов;

• Мониторинг случаев использования файлов с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Создание индивидуальных политик контроля за файловой активностью, в том числе с возможностью копирования из предустановленных;

• Возможность определять пути и файлы для особого контроля с созданием теневых копий при любых файловых операциях.

• Детектирование файлов, зашифрованных крипто-про.

Должна быть возможность осуществления контроля и обработки информации, отправляемой на локальные сетевые ресурсы, следующими способами:

• Теневое копирование файлов, отправляемых на сетевые ресурсы с рабочей станции пользователя с установленным агентом;

• Мониторинг случаев передачи файлов на сетевые диски с указанными параметрами, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Аудит событий отправки файлов на сетевые диски: фиксируется имя файла, пользователь, дата, время и сетевой путь к ресурсу, приложение;

• Возможность поиска по тексту и атрибутам перехваченных файлов, отправленных на сетевые ресурсы;

• Возможность создавать индивидуальные политики контроля информации для отдельных пользователей и рабочих станций.

**10. Требования к методам мониторинга действий пользователей на ПК:**

ПО должно позволять создавать скриншоты (снимки, кадры экрана рабочего стола сотрудника) для любого количества экранов и управлять процессом съёмки следующими способами:

• Снятие скриншотов с заданным интервалом;

• Снятие скриншотов по переключению активного окна;

• Снятие скриншотов во время удалённого подключения при просмотре рабочего стола или удалённом управлении рабочим столом;

• Настройка для определённых приложений и сайтов более частых интервалов снятия скриншотов;

• Создание пакета скриншотов, сохраняющего скриншоты за определённый период в один файл с возможностью настройки сжатия и цветности скриншотов в пакетах;

• Выполнение настройки качества получаемых скриншотов в процентах;

• Использование формата скриншотов JPEG;

• Возможность увеличения снимков экрана в рамках веб-консоли для возможности анализа снимков экрана большого размера;

• Выгрузка в следующих форматах: файл Excel, HTML, CSV, формат PNG;

• Скачивание в ZIP архиве или печать на принтере.

ПО должно обеспечивать формирование и обработку статистики активностей пользователя и компьютера следующими способами:

• Ведение статистики по времени работы и простоя (отсутствия действий сотрудника) ПК с представлением собранной информации в виде различных графиков;

• Ведение статистики по времени работы пользователя в приложениях с представлением собранной информации в виде графика (при этом учитывается время не от запуска до завершения процессов, а время работы пользователя в активном окне);

• Возможность настройки периода неактивности, после которого рабочее время сотрудника будет считаться простоем;

• Возможность настройки исключений отдельных процессов из мониторинга;

• Возможность автоматического анализа собранной статистики для выявления определённых событий (например, запуск несанкционированных приложений), контроля длительности работы пользователей с конкретными приложениями и длительности периодов работы/простоя компьютера – с отправкой соответствующего уведомления ответственному лицу;

• Возможность сохранения отдельных отчётов по активности (активность пользователя за ПК, активность приложений) за выбранный временной интервал для отдельного пользователя или нескольких пользователей в формате HTML;

• Предустановленные наборы приложений и сайтов, для классификации активной деятельности за ПК;

• Разделение деятельности на продуктивную/непродуктивную/нейтральную;

• Наличие отчётов для различных представлений и анализа накопленных данных по активности пользователей;

• Общий и групповые отчёты по активности пользователей;

• Перехват активности в терминальных linux-сессиях и последующая детализированная запись терминального ввода и вывода в виде GIF;

• Перехват и логирование действий пользователей на Linux системах;

• Возможность управлением сбора статистики пользователем, посредством иконки в трее системы.

Должен осуществляться контроль буфера обмена, и реализованы следующие возможности:

• Копирование помещаемой в буфер обмена текстовой информации с фиксацией идентификатора процесса, из которого данная информация была помещена в буфер обмена, и времени события;

• Поиск по тексту, помещаемому пользователями в буфер обмена;

• Мониторинг определённой информации, помещённой в буфер обмена, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Копирование графической информации, помещаемой в буфер обмена, включая скриншоты посредством нажатия Print Screen;

• Возможность блокировки передачи данных посредством буфера обмена из одного приложения в другое.

Должен быть реализован кейлоггер (перехват нажатий клавиш на клавиатуре), имеющий следующие особенности:

• Регистрация нажатий сотрудником клавиш на клавиатуре с фиксацией приложения, в котором пользователь вводил данную информацию и времени;

• Мониторинг информации, вводимой на клавиатуре, и дальнейшей отправкой уведомления одному или нескольким ответственным лицам за информационную безопасность, в случае обнаружения информации по заданным критериям;

• Возможность создавать индивидуальные политики контроля перехвата нажатий клавиш для отдельных пользователей и рабочих станций;

• Возможность дополнять политики данными напрямую из отчётов;

• Возможность поиска по тексту, вводимому пользователями с клавиатуры;

• Возможность перехвата паролей в диалоговых окнах Windows;

• Возможность запрета/разрешения отслеживания при помощи кейлоггера по чёрным или белым спискам приложений;

• Возможность перехвата пароля в момент разблокировки рабочего стола Windows (низкоуровневый кейллоггер);

• Возможность скрывать и отображать спецсимволы полученные кейлоггером.

Должна быть функция ведения аудиомониторинга, в частности:

• Возможность вести запись с обнаруженных микрофонов на локальной станции сотрудника с установленным агентом, независимо от используемого им приложения;

• Возможность записи звука, выводимого на аудиоустройства на локальной станции сотрудника с установленным агентом;

• Возможность настройки длительности записываемых отрывков записи звука;

• Возможность настройки качества записи;

• Возможность настройки шумового порога, при котором будут игнорироваться звуки;

• Возможность настройки интервала тишины, после которого запись звука будет приостановлена;

• Возможность настройки записи звука по децибелам;

• Возможность воспроизведения файла записи средствами системы веб-интерфейса;

• Возможность скачать записанные записи;

• Отображаться осциллограмма записанных записей для визуального определения моментов разговоров.

Должна быть возможность активировать видеомониторинг, имеющий следующие ключевые особенности:

• Возможность подключения к монитору компьютера сотрудника и просмотра изображения в режиме реального времени;

• Возможность мониторинга рабочих столов нескольких пользователей одновременно;

• Возможность вывода окна просмотра на отдельный экран;

• Возможность записи потокового видео с рабочих столов сотрудников при удалённом подключении;

• Возможность записи видео рабочего стола в режиме недоступности подключения к серверу;

• Возможность настройки длительности отрывка для записи видео;

• Возможность сохранения записей нескольких пользователей одновременно;

• Возможность воспроизведения файла записи средствами системы;

• Возможность фильтрации пользователей, к которым возможно удалённое подключение.

Должна присутствовать возможность контролировать пользователей, работающих за компьютером:

• Возможность создания снимков с веб-камеры по заданному интервалу;

• Настройка для определённых приложений и сайтов более частых интервалов снятия снимков с веб-камеры;

• Возможность производить видеозапись с веб-камеры;

• Возможность делать снимки с веб-камеры при отсутствии запущенной сессии или активности за компьютером;

• Возможность удалённого подключения к веб-камере для просмотра в реальном времени.

Должен присутствовать модуль, сканирующий файлы, который:

• Позволяет блокировать несанкционированный доступ к файлам по заданным параметрам;

• Имеет возможности управления доступом пользователей и приложений к файлам согласно задаваемому набору правил;

• Обладает утилитой добавления меток к файлам основных типов офисных приложений: .docx, .xlsx, .pptx, .odt, .ods, .odp;

• Имеет возможность анализировать текстовый контент файлов и ограничивать доступ к ним по набору правил;

• Имеет возможность запрещать передавать файлы на или со съёмных носителей информации;

• Имеет возможность запрещать определённые операции, производимые с файлами: копирование, перемещение, удаление, переименование, чтение;

• Имеет возможность ограничивать доступ к шифрованным архивам по набору правил;

• Имеет возможность отслеживания работы над помеченными файлами;

• Имеет настройки собственных параметров через управление в WEB-консоли и обладает возможностями выставления правил использования и блокировок для помеченных файлов;

• Сканирует локальные файловые системы и сохраняет найденные результаты;

• Поддерживает при настройке правил операторы: not, or, and, xor, eq, matches, in;

• Использует при настройке правил атрибуты: tag, tag\_value, computer\_name, user\_name, user\_domain, file\_path, file\_name, file\_ext, exe\_name, mine.

Должна быть карточка сотрудника, агрегирующая в себе информацию о пользователе, а именно:

• данные о сотруднике из Active Directory (имя, подразделение, руководитель, почта);

• компьютеры, к которым привязан сотрудник;

• данные о последней активности сотрудника;

• зарегистрированные события;

• информация об активности сотрудника;

• инциденты, в которых сотрудник выступает фигурантом.

**11. Требования к возможностям отображения собранной информации.**

Должен присутствовать просмотр информации по типам событий, а именно:

• Поисковые запросы, информация выводится в следующем виде: время, компьютер, пользователь, приложение, домен, текст;

• Время активности, информация выводится в следующем виде: время, тип события, компьютер, пользователь, длительность (в формате 00 ч 00 м 00 с), приложение, сайт, заголовок;

• Снимок экрана, информация выводится в следующем виде: время, компьютер, пользователь, заголовок, снимок;

• Запись звука, информация выводится в следующем виде: время, компьютер, пользователь, устройство, контент (аудиофайл);

• Перехваченный файл, информация выводится в следующем виде: время, компьютер, пользователь, приложение, контент (файл, изображение и т.д.), связь с событием, страницы (перехват печати отображает количество страниц), получатели;

• Устройства, информация выводится в следующем виде: время, компьютер, пользователь, тип устройства, устройство, ID;

• Завершение приложений, информация выводится в следующем виде: время, компьютер, пользователь, приложение, ID процесса, ID пользовательской сессии;

• Системный лог, информация выводится в следующем виде: время, тип события, компьютер, текст, контент (с возможностью скачать сам лог из web-интерфейса);

• Беспроводное подключение, информация выводится в следующем виде: время, компьютер, SSID;

• Снимок с веб-камеры, информация выводится в следующем виде: время, компьютер, пользователь, приложение, снимок;

• Буфер обмена, информация выводится в следующем виде: время, компьютер, пользователь, приложение, текст, формат буфера обмена (текст или изображение);

• FTP, информация выводится в следующем виде: время, компьютер, пользователь, приложение, событие;

• Почта, информация выводится в следующем виде: время, компьютер, пользователь, отправитель, получатели, заголовок, контент (файлы, изображение и т.д. с нумерацией по номеру вложения);

• Посещение сайтов, выводится в следующем виде: время, компьютер, пользователь, приложение, ссылка;

• Ввод с клавиатуры, информация выводится в следующем виде: время, компьютер, пользователь, приложение, заголовок окна, текст;

• Сеть, информация выводится в следующем виде: время, компьютер, пользователь, приложение, сокет;

• Алерт (вычисленное сервером событие), информация выводится в следующем виде: время, тип, компьютер, пользователь, время, алерт, текст. При обнаружении алерта должна быть возможность автоматически сформировать и отправить уведомление по e-mail;

• Запуск приложения, информация выводится в следующем виде: время, компьютер, пользователь, приложение, ID процесса, ID пользовательской сессии;

• Операция с файлами, информация выводится в следующем виде: время, компьютер, пользователь, приложение, операция, имя файла, устройство, тип диска;

• Внешние диски, информация выводится следующем виде – время, компьютер, пользователь, тип, устройство, ID;

• Установка ПО, информация выводится в следующем виде: время, компьютер, операция, продукт, поставщик, версия;

• Установка и удаление пакетов на Linux системах;

• Инвентаризация установленных пакетов на Linux системах;

• Видео рабочего стола, информация выводится в следующем виде: время, компьютер, пользователь, приложение;

• Вход/выход из системы, информация выводится в следующем виде: время, компьютер, пользователь, событие (вход в систему, выход из системы и т.д.);

• Удалённый вход/выход из системы, информация выводится в следующем виде: время, компьютер, пользователь, событие (вход в систему, выход из системы и т.д.);

• Данные формы, информация выводится в следующем виде: время, компьютер, пользователь, приложение, сайт;

• Реестр оборудования, информация выводится в следующем виде: время, компьютер, тип устройства, устройство, ID;

• Реестр софта, информация выводится в следующем виде: время, компьютер, операция, продукт поставщик, версия;

• Печать документов, выводится в следующем виде: время, компьютер, пользователь, страницы (количество распечатанных страниц), текст;

• Интернет-пейджер, информация выводится в следующем виде: время, компьютер, пользователь, отправитель, получатели, сообщение;

• Отображение логотипа приложения по которому были перехвачены события.;

• Возможность изменять формат отображения детализированной информации по событиям на горизонтальный или вертикальный;

• Возможность производить фильтрацию данных на основе элемента список.

Должен быть организован просмотр собранной информации как по отдельным измерениям, так и по их комбинациям с типами событий и произвольным набором измерений:

• Измерение Агент, выбор предоставляется по следующим параметрам: IP адрес, группа (к которому относится агент), сотрудник, компьютер, статус, версия OS, версия агента;

• Измерение пользователь, выбор предоставляется по следующим параметрам: отдел, организация, телефон, полное имя, почта, должность, домен, пользователь, комментарий, (информация задаётся в профиле пользователя);

• Измерение приложение, выбор предоставляется по следующим параметрам: полный путь, заголовок окна, название, описание;

• Измерение сайт, выбор предоставляется по следующим параметрам: полный домен, протокол, URL, основной домен, тип контента;

• Измерение сетевая активность, выбор предоставляется по следующим параметрам – IP-адрес, сетевой порт;

• Измерение файл, выбор предоставляется по следующим параметрам: хеш файла, операция, имя файла, контент извлечен (true или false), метка, тип контента, тип диска, расширение, путь, имя файла источника, путь источника, расширение источника;

• Измерение устройство, выбор предоставляется по следующим параметрам: устройство, ID устройства, маркер, тип диска, класс устройства, тип устройства;

• Измерение переписка, выбор предоставляется по следующим параметрам: домен получателя, отправитель, все получатели, формат сообщения, направление, домен отправителя, получатель, чаты, канал общения. В случае большого объёма данных должно присутствовать постраничное отображение переписки;

• Измерение дата, выбор предоставляется по следующим параметрам: час суток, часовой пояс, день недели, по годам, по месяцам, по дням, по часам, по минутам;

• Измерение инсталляции, выбор предоставляется по следующим параметрам: поставщик, обновление, версия, операция, продукт;

• Измерение сработавшие фильтры, выбор предоставляется по следующим параметрам: категория, название.

Должна быть возможность смены режимов предоставления отчётов с отображением данных по следующим критериям:

• Таблица, выводящая информацию определённых типов события и типов измерения, с возможностью их комбинирования;

• Список, предоставляет информацию общим списком определённых типов события и типов измерения, с возможностью их комбинирования;

• Снимки, режим отображения для удобства предоставления информации по типам события снимков с веб-камеры и снимков с экрана, с возможностью выбора типов измерения;

• Активность, выводит информацию в виде тепловой диаграммы, с возможностью выбора отображения информации по типам события и измерениям;

• Переписка, режим отображения для удобства предоставления информации по типам события почта и интернет-пейджер, с возможностью выбора дополнительных типов измерения.

Должна присутствовать возможность наблюдать и анализировать статистику по собранным данным (строить фильтры внутри фильтров), тем самым, получая дополнительный срез информации при помощи следующих способов её отображения:

• Таблица с возможностью отображения в табличном виде события по выбранным ПК и фильтру;

• Линейный график с возможностью отображения количества событий по выбранным фильтрам в виде столбцов графика, а также возможность переключения графика между: линейным, гистограммой, с накоплением и без накопления;

• Круговая диаграмма с возможностью отображения количества событий в виде круговой диаграммы с поддержкой вложенных фильтров;

• Возможность построения графа в виде диаграммы связей;

• Возможность построения дерева взаимосвязей, которое возможно выгрузить на печать, и возможностью провалиться в события, кликнув на элемент дерева;

• Дополнительные возможности отображения данных в следующих видах: радар, река событий, статистика;

• Возможность отображать информацию по количественным измерениям: время разговора, число страниц, время активности, количество событий, размер файла.

Должен присутствовать раздел фильтров (например, в виде вкладки), включающий в себя сгруппированные измерения, политики, дашборды и словари:

• Наличие фильтров, создаваемые пользователем самостоятельно;

• Наличие фильтров, предустановленных и обновляемых разработчиком;

• Наличие возможности представления информации как в отчётах, так и конкретных событиях;

• Наличие подразделов эффективности, безопасности и инцидентов;

• Возможность маркировки приложений и сайтов по категориям продуктивности: продуктивная деятельность, непродуктивная деятельность, нейтральная деятельность, премиальная деятельность, инцидент. В любую из категорий можно добавить/удалить любое количество имён исполняемых файлов или сайтов;

• Наличие системных политик, являющимся скриптами для запуска внутренних обработчиков информации и возможность их изменения;

• Возможность создание новых фильтров или удаление уже имеющихся;

• Возможность задать любое имя созданному фильтру или дашборду, с возможностью его последующего изменения;

• Возможность добавить описание к созданному фильтру;

• Возможность регулярной рассылки настраиваемых консолидированных отчётов в html формате, позволяющими работать с отчётами из консоли без доступа к серверу.

При работе с фильтрами и политиками безопасности, пользователю должен быть доступен следующий функционал:

• Возможность настройки индивидуальных фильтров и политик безопасности, с последующим комбинированием их в дашборды, позволяющие просматривать необходимую выводимую информацию в едином месте;

• Возможность создавать копию фильтра из существующего, редактировать на лету;

• Возможность настройки уведомлений на почту ответственным лицам за информационную безопасность, с настройкой интервалов отправки (при срабатывании, ежедневно, еженедельно, ежемесячно) и возможностью настройки получаемой информации об инциденте;

• Возможность настройки уведомлений в мессенджер telegram ответственным лицам за информационную безопасность, с настройкой интервалов отправки (при срабатывании, ежедневно, еженедельно, ежемесячно) и возможностью настройки получаемой информации об инциденте;

• Наличие встроенных политик безопасности, а именно словарь ненормативной лексики, словарь наркоманского сленга, словарь откатной тематики, словарь поиска работы, поиск кредитных карт, шифрованных архивов и т.д.;

• Возможность просмотра информации и сработавших фильтров за любой промежуток времени;

• Возможность просмотра статистки с указанием количества сработавших инцидентов по определённому фильтру или типу события;

• Возможность изменения встроенных политик безопасности, с настройкой отправки уведомлений на почту ответственному лицу за информационную безопасность и возможности изменения категорий по следующим параметрам: инцидент, непродуктивно, нейтрально, продуктивно, премиально;

• Возможность автоматического изменения конфигурации, как следствие реакции на обнаруженный посредством созданной политики, словаря и политики срабатывания по пороговому значению;

• Возможность одновременного редактирование настроек уведомлений для группы фильтров и политик безопасности;

• Возможность получения уведомлений по изменению конфигурации оборудования;

• Возможность перейти из анализа к фактам по выбранным измерениям.

Должно присутствовать средство формирования инцидентов из событий (консоль инцидентов). При просмотре информации об инциденте в web-интерфейсе должна быть доступна следующая информация:

• Пользователь, допустивший нарушение;

• Дата и время инцидента;

• Тип файла, вызывающего срабатывания фильтра или политики безопасности (электронное письмо, документ, отправленный на печать и т.д.);

• Содержание файла, породившего инцидент (электронного письма, документа, отправленного на печать и т.д.);

• Участник – фигурант инцидента;

• Другая дополнительная информация (с возможностью исключения/добавления необходимых пунктов вывода);

• У инцидента должна присутствовать и предустанавливаться критичность;

• Должно присутствовать средство ежедневной генерации комплексной группы отчётов по учёту рабочего времени с возможностью детального анализа данных без доступа к веб-консоли сервера;

• Должна быть возможность объединения инцидентов;

• Должна быть возможность предпросмотра снимков экрана из консоли инцидентов;

• Должна быть возможность сортировка и фильтрация инцидентов по дате последнего изменения;

• Должен быть архив удалённых инцидентов.

С целью гибкой настройки учёта рабочего времени должны присутствовать:

• Возможность настройки рабочего расписания сотрудников, по следующим критериям: день недели, начало рабочего дня, конец рабочего дня, начало перерыва, конец перерыва, рабочее время;

• Календарь с возможностью проставления рабочих часов, праздников, больничных, отгулов и отпусков;

• Возможность назначения расписаний по компьютерам, группам, отделам, пользователям, полным именам пользователей и организации;

• Возможность отправки уведомлений ответственным лицам на почту, при превышении времени активности или разговора, размеру файла, количеству срабатываний в определённых приложениях, сайтах и других типах событий - срабатывание по порогу.

Должны присутствовать встроенные отчёты для учёта рабочего времени, а именно:

• Комбинированный отчёт, содержащий информацию за выбранный период по выбранным пользователям, разбитый на дни и выводящий следующую информацию: даты выбранного периода, пользователь, шкала активностей пользователя по часам, начало и окончание каждого рабочего дня, общее время работы, активное время, время простоя, информацию по опозданию и сверхурочным, продуктивное время, непродуктивное время и нейтральное время, расписание. Поля должны быть сгруппированы по типу измерения с возможностью выбора. Возможность включения в отображении в отчёте неактивных сотрудников. В случае выбор одного определённого пользователя отчёт дополняется комбинированной статистикой в долях по времени и процентам для продуктивности, топу используемых приложений и топу посещаемых сайтов, отображаемых на временных шкалах по каждому из дней. При этом становится возможным отфильтровать активности и перейти к фактам по этим активностям;

• Ленточный график, отчёт, содержащий информацию за выбранный период по выбранным пользователям, разбитый на дни и выводящий шкалы активностей пользователя по часам. В случае выбора одного определённого пользователя отчёт дополняется комбинированной статистикой по продуктивности, топу используемых приложений и топу посещаемых сайтов, отображаемых на временных шкалах по каждому из дней, долями этих активностей;

• Таблица - отчёт, содержащий информацию за выбранный период по выбранным пользователям, разбитый на дни и выводящий следующую информацию: даты выбранного периода, пользователь, начало и окончание каждого рабочего дня, общее время работы, активное время, время простоя, информацию по опозданию и сверхурочным, продуктивное время, непродуктивное время и нейтральное время. В случае выбора одного определённого пользователя отчёт дополняется комбинированной статистикой по продуктивности, топу используемых приложений и топу посещаемых сайтов по каждому из дней;

• Отчёт по активности за период, содержащий суммарную информацию за выбранный период, по выбранным пользователям: пользователь, общее время работы, активное время работы, время простоя, информацию по опозданию, сверхурочные, продуктивное время, нейтральное и непродуктивное время. Отчёт дополнен комбинированной статистикой в долях по времени и процентам для продуктивности, топу используемых приложений и топу посещаемых сайтов, отображаемых по каждому из дней в виде графика. При этом отчёт можно отфильтровать по выбранным типам активностей, приложений или сайтов;

• Отчёт по простоям за период, содержащий поделённую простоями на интервалы следующую информацию по выбранным пользователям: сотрудник, дата, начало и окончание интервала, совершённые действия, учтённые часы работы и часы простоя;

• Продуктивное время по отделам, отчёт, содержащий суммарное продуктивное/непродуктивное и нейтральное время пользователей на рабочих местах за выбранный период времени на шкале общего отработанного времени и отдельно по каждому из них в виде суммарного времени и его проценте от общего;

• Активное время по отделам, отчёт, содержащий на индивидуальных и общей шкалах отработанного времени суммарное активное время, переработку, суммарную недоработку, отсутствие пользователей на рабочих местах за выбранный период времени, в том числе по отношению к плановому времени в процентах;

• Топ непродуктивности по отделам, отчёт, содержащий информацию за выбранный период и сортирующий непродуктивных сотрудников по отделу, отображая следующее: компьютер, пользователь, должность, отдел, название типа активности, время активности;

• Сводный отчёт, содержащий как обобщённую статистику об опоздавших пользователях, времени опозданий, активных и неактивных, продуктивных и непродуктивных пользователях, так и сводную суммарную информацию за выбранный период по выбранным пользователям в следующем виде: пользователь, общее время, активное время, время простоя, продуктивное время, нейтральное непродуктивное время, количество опозданий, общее время опозданий и сверхурочные;

• Сводный отчёт по группам, содержащий следующую информацию по каждому сотруднику с разбиением по организационным единицам: пользователь, общее время, активное время, время простоя, продуктивное время, нейтральное и непродуктивное время, количество опозданий, общее время опозданий и сверхурочные. Вычисляются суммы по каждой группе сотрудников;

• Сводный статистический отчёт, содержащий следующий набор информации по всем выбранным сотрудникам: пользователь, активные дни, рабочие часы, общее время, активное время, продуктивное время, нейтральное время, продуктивное корректированное время, продуктивное корректированное время в день, отношение продуктивного корректированного времени к 8 часам, непродуктивное время, непродуктивное время в день, время простоя, время простоя в день;

• Отчёт по опозданиям, содержащий следующую информацию за выбранный период, по выбранным пользователям: период времени, пользователь, количество опозданий, общее время опозданий, общее время, активное время и время простоя – если выбран один пользователь, и дополнительную статистическую информацию для нескольких: отношение общего времени опозданий к общему времени, топ опоздавших и топ по времени опозданий;

• Учёт ранних уходов и приходов, отчёт, разделённый датами и содержащий следующую информацию за выбранный период по выбранным пользователям: период времени, пользователь, длительность опоздания, ранний уход на обед и опоздания с обеда, ранний уход с работы, задержание на работе и ранний приход на работу;

• Учёт ранних уходов и приходов по группам, отчёт, разделённый датами и организационными единицами, содержащий следующую информацию за выбранный период по выбранным пользователям: период времени, пользователь, длительность опоздания, ранний уход на обед и опоздания с обеда, ранний уход с работы, задержание на работе и ранний приход на работу;

• Расширенный табель учёта рабочего времени, отчёт, который представляет собой совокупность ежемесячных отчётов по всем выбранным пользователям, где для каждого пользователя предусмотрены следующие заполненные поля: организация, отделение, должность, сотрудник и рабочее время. При этом рабочее время учитывается в следующих измерениях для каждого дня: вход, выход, время нахождения в офисе, время работы в разрешённом ПО, время работы в запрещённом ПО, простой. По итогам каждого месяца по каждому измерению подводятся итоги: дни и часы в рабочие и выходные дни;

• Табели по форме Т13 (отчёты "как в 1С "): рабочего времени, активного времени, отсутствия на рабочем месте, использования принтера;

• Отчёт по входу, выходу и пребыванию в помещении на основе данных собранных со СКУД;

• Отчёт по отсутствию событий за период, содержащий в себе информацию по машинам, которые за выбранный период не присылали данных на сервер;

• Наличие возможности для редактирования отображаемой информации в отчётах;

• Возможность изменения и фиксации периода анализируемых данных;

• Возможность изменения объекта анализа в отчётах: компьютеры, пользователи, полные имена пользователей, сотрудники;

• Возможность установки минимального времени активности для анализа начала и окончания рабочего дня в рамках отчёта;

• Возможность отображения данных в отчёте по времени удалённой сессии.

**12. Требования к возможностям инвентаризации установленного ПО и оборудования:**

• Должен присутствовать встроенный отчёт инвентаризации устройств рабочей станции со следующими выводимыми параметрами: статус (в наличии или нет), компьютер (имя рабочей станции), производитель, тип устройства, HWID и дата последней проверки на наличие, с возможностью группировки по компьютерам и выгрузки отчёта в html, pdf и excel форматах;

• Должен присутствовать встроенный отчёт по инвентаризации приложений рабочей станции со следующими выводимыми данными: статус (в наличии или нет), компьютер (имя рабочей станции), продукт, поставщик, версия и дата последней проверки на наличие, с возможностью группировки по компьютерам и выгрузки отчёта в html, pdf и excel форматах;

• Должен присутствовать встроенный отчёт по приложениям на рабочих станциях организации со следующими выводимыми данными: Название приложения, список станций на которых обнаружено данное ПО, с информацией по статусу, поставщику, версии и дате наличия. Должна присутствовать возможность выгрузки отчёта в html, pdf и excel форматах.

**13. Требования к возможностям анализа и распознавания.**

В программном обеспечении должны быть предусмотрены расширенные возможности аналитики собираемой информации посредством контентного анализа, имеющего:

• Возможность поиска, по ключевым словам, и словосочетаниям;

• Возможность добавления слов или словосочетаний в фильтр для их обнаружения в перехваченных файлах или документах;

• Возможность составления собственных словарей;

• Возможность подсветки разными цветами найденных совпадений из разных словарей;

• Возможность поиска контента посредством конструктора регулярных выражений с возможностью проверки запроса, сформированного конструктором;

• Детальная информация по все политикам, среагировавшим на инцидент.

Программное обеспечение должно обладать функционалом распознавания изображений и документов, которые обеспечивает:

• Наличие собственного бесплатного встроенного модуля OCR не старее Tesseract4;

• Возможность использования 2х и более серверов распознавания;

• Возможность распознавания перевёрнутых изображений;

• Возможность выбора следующих языков - русский и английский;

• Возможность распознавания следующих форматов - PDF, JPEG, PNG;

• Возможность подключения облачного ABBYY Cloud OCR SDK;

• Возможность распознавать Паспорта и Штампы печатей через нейронные сети с использованием машинного обучения;

• Возможность распознавания лиц через снимки с веб-камеры с использованием машинного обучения.

Согласовано:

Контрактная служба: О.В. Дергилев