ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ ПРЕДЛАГАЕМОГО ТОВАРА

ТОО «Cloud Security» | Конкурс № 16642394-ОК1 | Лот № 81014512-ОК2

Товар: Программное обеспечение InfoWatch Traffic Monitor Standard Solution: InfoWatch Person Monitor для 3000 учётных записей

1. ТРЕБОВАНИЯ К АРХИТЕКТУРЕ И ПЛАТФОРМЕ

1.1. Архитектура клиент-сервер

1.1.1. Клиентское программное обеспечение (далее — ПО) Системы предотвращения утечки информации (далее — DLP, Система) передаёт данные на сервер DLP для их последующего сохранения в базе данных.

1.1.2. В Системе реализованы технологии искусственного интеллекта / нейронных сетей / AI для автоматизации процесса сохранения данных, оптимизации запросов и управления базой данных.

1.1.3. Клиентское ПО DLP представлено в версиях для операционных систем Windows, Linux и macOS.

1.1.4. Серверное ПО DLP представлено в версиях для ОС Windows и Linux; реализован слой программной совместимости для запуска исполняемых файлов Windows в средах POSIX.

Поддерживаемые операционные системы: сервер (Windows) — Windows Server 2008R2 и новее, Windows 8.1/10/11, 64-бит; сервер (Linux) — Ubuntu 22/24, Astra Linux 1.7/1.8; клиент (Windows) — Windows XP SP3 и новее, 32/64-бит; клиент (Linux) — Astra, CentOS, Debian, Mint, Ubuntu, Rosa, RED OS и другие совместимые дистрибутивы; клиент (macOS) — Mojave, Catalina, Big Sur, Monterey, Ventura, Sonoma, Sequoia, Tahoe.

1.2. Работа DLP в физических и виртуальных средах

1.2.1. Клиентское и серверное ПО DLP функционирует на физических и виртуальных серверах (далее — серверная машина).

1.3. Инстанцирование сервера и базы данных

1.3.1. DLP поддерживает установку сервера комплекса и базы данных DLP в нескольких экземплярах (инстанциях) на одной серверной машине.

2. СЕРВЕРНАЯ ИНФРАСТРУКТУРА И МАСШТАБИРОВАНИЕ

2.1. Поддержка нескольких серверов

2.1.1. Комплекс функционирует в режиме нескольких серверов и единой центральной базы данных. Нейросеть применяется для управления трафиком между серверами, оптимизации нагрузки, обнаружения и устранения сбоев; применяется для автоматического масштабирования системы в зависимости от нагрузки.

2.2. Дополнительный IP-адрес для связи с сервером

2.2.1. DLP поддерживает указание дополнительного внешнего IP-адреса сервера для связи (актуально при использовании ноутбуков за пределами офиса). Искусственный интеллект применяется для мониторинга трафика через дополнительный IP-адрес и обнаружения аномалий и подозрительной активности.

2.3. Работа сервера за DMZ

2.3.1. DLP поддерживает работу сервера через reverse-proxy nginx за демилитаризованной зоной (DMZ), что обеспечивает работу удалённых сотрудников. Искусственный интеллект применяется для построения интеллектуальных систем аутентификации и авторизации, обеспечивающих безопасный доступ к ресурсам сервера.

2.4. Терминальный сервер, тонкий клиент

2.4.1. Клиенты комплекса ПО реализованы по принципу «тонкого клиента»: вся обработка данных выполняется на сервере, что исключает затруднения при работе в терминальных сессиях. Искусственный интеллект применяется для оптимизации обработки данных на сервере, включая автоматическую оптимизацию запросов, управление ресурсами и балансировку нагрузки.

2.5. Поддержка двух СУБД SQL

2.5.1. Все данные мониторинга хранятся в SQL-базе на серверной машине.

2.5.2. DLP поддерживает СУБД Microsoft SQL Server и СУБД PostgreSQL.

Дополнительно поддерживаются СУБД на основе PostgreSQL: Postgres Pro, Jatoba, Tantor, Platform V Pangolin DB и совместимые.

2.6. Локальное хранение данных

2.6.1. При отсутствии связи с сервером данные наблюдений сохраняются в локальной базе данных и гарантированно передаются на сервер после восстановления соединения. Ретроспектива хранения локальных данных настраивается. В качестве локальной базы используется компактная встраиваемая реляционная СУБД с открытым исходным кодом, не требующая отдельного сервера.

2.7. Отложенное наблюдение

2.7.1. При большом числе клиентских машин реализован режим отложенного наблюдения: данные передаются на сервер DLP по запросу от выбранных машин. Искусственный интеллект определяет, когда и с каких клиентских машин запрашивать данные, на основе исторических данных и текущих трендов, увеличивая частоту запросов к машинам, генерирующим наиболее важные данные. При сравнительно небольших системных требованиях сервер комплекса и база данных обслуживают более 20 000 клиентских подключений.

2.8. Ограничение трафика

2.8.1. DLP ограничивает трафик от клиентов к серверу при больших нагрузках и множественных подключениях. Искусственный интеллект динамически регулирует лимиты с учётом текущей нагрузки, скорости сети и других параметров: снижает объём данных от клиентов с меньшим приоритетом; для клиентов, передающих важные данные, лимиты повышаются.

2.9. Шифрование трафика данных

2.9.1. Канал клиент-сервер зашифрован; реализован HTTPS-доступ к веб-интерфейсу.

2.9.2. DLP поддерживает сети IPv6.

2.9.3. DLP функционирует в сетях IPv4 и IPv6.

3. ИНТЕГРАЦИЯ И УЧЁТНЫЕ ЗАПИСИ

3.1. Вход с учётными записями Windows

3.1.1. DLP поддерживает вход в систему с текущей учётной записью ОС Windows, доменными и иными учётными записями.

3.2. Доменные пользователи

3.2.1. По доменным пользователям DLP формирует отчёты как по всем клиентским машинам, за которыми они работали суммарно, так и по конкретным клиентским машинам.

3.3. Интеграция с Active Directory

3.3.1. DLP синхронизирует данные одновременно с несколькими доменами компании.

3.3.2. Реализована автоматическая установка и удаление клиентского ПО в соответствии с группами компьютеров Active Directory (AD).

3.3.3. Данные досье сотрудника (ФИО, отдел и др.) синхронизируются с записями в AD.

3.3.4. Связь «руководитель — подчинённый» для доступа к отчётам соответствует реальной структуре организации на основе данных AD.

3.3.5. DLP поддерживает автоматическую синхронизацию организационной структуры сразу с несколькими доменами организации.

Реализована поддержка входа в СУБД PostgreSQL с учётными записями из Active Directory через протокол LDAP, включая защищённое соединение по LDAPS. Реализована передача данных о событиях в SIEM-системы по протоколу syslog (RFC 5424, UDP и TCP) с настраиваемым перечнем типов событий.

4. НАБЛЮДЕНИЕ И МОНИТОРИНГ

4.1. Удалённое веб-наблюдение

4.1.1. Все онлайн- и офлайн-наблюдения ведутся через веб-браузер независимо от местоположения.

4.2. Наблюдение за экранами

4.2.1. Реализован захват одиночных текущих скриншотов и видеопоток экрана в режиме реального времени.

4.2.2. Реализовано сохранение записи экрана в видеофайл.

4.3. Наблюдение с веб-камер

4.3.1. Реализован захват одиночных фотографий и видеопоток с веб-камеры в режиме реального времени.

4.3.2. Реализовано сохранение записи с веб-камеры в видеофайл.

4.4. Прослушивание аудио и микрофонов

4.4.1. Реализована прослушка микрофонов и аудио рабочих станций.

4.4.2. Реализовано сохранение аудиозаписи в файл.

4.4.3. Реализовано прослушивание микрофонов и аудио с применением искусственного интеллекта и нейронных сетей для анализа и классификации звуковых данных. Алгоритмы машинного обучения применяются для оптимизации качества звука и сжатия данных при сохранении аудиозаписей.

Аудиозаписи сохраняются в формате OGG. Реализована ИИ-сводка (саммари) по голосовому звонку на базе LLM-нейросети с поддержкой дополнительных пользовательских инструкций для анализа.

4.5. Преобразование голоса в текст

4.5.1. Реализована функция распознавания речи сотрудника в режиме реального времени с применением искусственного интеллекта и нейронных сетей. Реализовано сохранение разговора в текстовый файл; реализовано преобразование голоса в текст с высокой точностью и минимальной задержкой; реализованы распознавание и анализ эмоций, акцентов и иных характеристик речи.

4.6. Список процессов и окон

4.6.1. Реализовано получение списка активных процессов и открытых окон пользователя.

4.7. Пауза наблюдения

4.7.1. Реализована функция постановки наблюдения на паузу и снятия с паузы.

4.8. Реакция на подозрительные события

4.8.1. Система применяет искусственный интеллект и нейронные сети для мониторинга подозрительных событий и реагирования на них. Обеспечивается выдача уведомлений о важных событиях в системном трее и окне браузера со звуком. Реализованы получение SMS- и e-mail-уведомлений посредством алгоритмов машинного обучения, которые анализируют поведение пользователя и оптимизируют время и способ доставки уведомлений.

5. УПРАВЛЕНИЕ, УВЕДОМЛЕНИЯ И ВЗАИМОДЕЙСТВИЕ

5.1. Интеграция с мессенджером Telegram

5.1.1. Реализована отправка уведомлений о важных событиях в персональный чат мессенджера Telegram; уведомления дополняются скриншотами экрана.

5.2. Отправка сообщений

5.2.1. Реализована отправка мгновенных сообщений пользователям.

5.3. Тревожная кнопка

5.3.1. Реализованы быстрое выключение всех компьютеров, их блокировка и выполнение скрипта на сервере по команде через мессенджер Telegram.

5.4. Отправка отчётов сотрудникам организации

5.4.1. Сотрудники организации получают ежедневные отчёты о собственной работе на личный e-mail по расписанию.

5.5. Отправка отчётов администратору DLP и руководству

5.5.1. Реализована автоматическая генерация отчётов по расписанию и их отправка администратору DLP и руководству по e-mail, FTP, DropBox и иными способами — в разбивке по группам сотрудников. Применяются искусственный интеллект и нейронные сети для анализа данных, формирования отчётов и определения оптимального времени отправки. Отчёты автоматически адаптируются к предпочтениям каждого руководителя с помощью алгоритмов машинного обучения.

Реализованы следующие каналы доставки отчётов: сохранение в папку на сервере, отправка по FTP, отправка на e-mail, публикация на веб-сайте, отправка в файлообменник. Реализована отдельная рассылка отчётов руководителям и отдельная рассылка сотрудникам с показателями их собственной работы по расписанию.

6. ПОИСК И АНАЛИТИКА

6.1. Поисковый движок по файлам на клиентских машинах

6.1.1. Реализован мощный многофункциональный поисковик, применяющий искусственный интеллект и нейронные сети для индексирования содержимого файлов на клиентских машинах. Реализована поддержка многоуровневых и запароленных архивов; реализованы распознавание и анализ текста внутри документов с использованием алгоритмов глубокого обучения.

6.2. Поиск в файлах

6.2.1. Реализован мгновенный поиск слов, фраз и регулярных выражений в файлах на клиентских машинах. Применяются алгоритмы глубокого обучения для повышения точности и скорости поиска; реализовано обучение на основе предыдущих запросов для улучшения результатов.

Реализован поиск по тексту в файлах форматов документов, многоуровневых и запароленных архивах, а также распознавание и извлечение текста внутри изображений и документов с использованием встроенного OCR-движка.

6.3. Глобальный поиск

6.3.1. Реализован поиск по тегам, словам кейлоггера, заголовкам окон, приложениям и сайтам в пределах всей базы данных по всем сотрудникам с быстрым переходом к скриншотам найденного временного промежутка по сотруднику.

Для ускорения полнотекстового поиска в MS SQL Server реализована поддержка компонента Full Text Search. Реализован поиск по тегам, словам кейлоггера, заголовкам окон, именам приложений, адресам сайтов — с мгновенным переходом к снимкам экрана соответствующего временного промежутка.

6.4. Поиск по шаблонам

6.4.1. Реализовано множество критериев поиска ; реализовано создание пользовательских шаблонов.

6.5. Отчёт по категориям и отклонениям

6.5.1. Реализован сводный отчёт, показывающий статистику в разрезе используемых ресурсов, категорий и отклонений от средних значений по сотрудникам.

Аналитический модуль системы реализует три независимых метода статистической оценки сотрудников: z-преобразование (стандартизация относительно среднего), ранговое исчисление и расчёт на основе абсолютных порогов. Каждый метод даёт самостоятельную оценку уровня риска, что обеспечивает трёхкратную верификацию результата.

6.6. Сводный отчёт по сотруднику

6.6.1. Реализован удобный сводный отчёт по конкретному сотруднику в виде кликабельных круговых диаграмм ; реализован детальный анализ производительности.

6.7. Сводный упрощённый отчёт

6.7.1. Реализован сводный отчёт по группе сотрудников в табличном виде ; реализован экспорт в системы визуализации и анализа данных в табличных форматах.

6.8. Лента активности

6.8.1. Реализован графический отчёт «Лента активности», позволяющий оценить, в какие периоды времени, чем и в какой степени занимался пользователь.

6.9. Сравнение активности

6.9.1. Реализовано текстовое представление отчёта «Лента активности» с удобным интерфейсом сравнения показателей.

6.10. Отчёты мониторинга

6.10.1. Реализована аналитика «Чёрный ящик» с применением нейронных сетей и искусственного интеллекта, включая:

— постоянную запись видео с экрана и аудио с микрофона/динамиков в зашифрованном виде на машинах сотрудников для последующего детального анализа при расследовании инцидентов;

— автоматическое распознавание образов и звуков посредством искусственного интеллекта для быстрого и точного анализа записей;

— распознавание лиц с применением нейронных сетей и искусственного интеллекта.

6.10.2. Реализован периодический анализ лиц сотрудников с веб-камер на совпадение с другими сотрудниками.

6.10.3. Реализовано удобное отображение и анализ присутствия сотрудника и выявление подмены сотрудника другим лицом, непосредственно в отчёте.

6.10.4. Применяется офлайн-движок собственной разработки на основе нейронной сети для обеспечения контроля доступа, безопасности и предотвращения мошенничества на рабочем месте.

6.10.5. Реализован анализатор рисков и производительности с применением нейронных сетей и искусственного интеллекта. Настраиваемый на основе профилей и словарей анализатор использует алгоритмы машинного обучения для анализа поведения сотрудников и определения эффективной, неэффективной и опасной работы.

Для повышения точности оценки рисков администратор настраивает словари (корпоративные, сторонние, потенциально опасные ресурсы) и профили активности, привязывая «полезные» и «вредные» словари к должностям сотрудников. Одна и та же категория ресурсов классифицируется как рабочая для одних должностей и как рисковая — для других.

6.10.6. Искусственный интеллект обеспечивает выявление скрытых рисков, повышение производительности и предотвращение потенциальных инцидентов на рабочем месте.

6.11. Расчёт уровня рисков сотрудников

6.11.1. В дополнение к отчёту «Анализатор рисков» реализован математический расчёт уровня риска тремя независимыми способами.

Методы расчёта: 1) z-преобразование — нормализация значений относительно среднего по группе с выявлением значимых отклонений; 2) ранговое исчисление — ранжирование сотрудников внутри группы; 3) пороговый метод — сравнение показателей с заданными абсолютными нормами риска. Шкала результата: 0 — нет риска, 1 — значительно ниже среднего, 2–3 — ниже среднего, 4–7 — в пределах среднего, 8–9 — выше среднего, 10 — значительно выше среднего.

7. КОММУНИКАЦИИ И ПЕРЕХВАТ ДАННЫХ

7.1. Голосовые переговоры

7.1.1. Реализованы перехват и запись голосовых переговоров в следующих приложениях: Skype, Lync, Viber, Telegram, Bitrix Desktop, ICQ, Mail.ru Agent, Microsoft Teams, Zoom, Slack, Myteam, Cisco Webex Teams, WhatsApp Desktop, eXpress Desktop, VK Teams (Cloud) Desktop.

Голосовые записи сохраняются в формате OGG. Реализована ИИ-сводка (саммари) по каждому звонку на базе LLM-нейросети с поддержкой пользовательских инструкций для анализа содержания звонка.

7.1.2. Реализовано распознавание голоса и речи с применением нейронных сетей и искусственного интеллекта.

7.1.3. Реализовано преобразование перехваченных голосовых переговоров в текст; перехваченные переговоры доступны для просмотра в виде текстового файла. Искусственный интеллект обеспечивает точное преобразование голоса в текст для документирования, анализа и архивации разговоров, выявления коммуникационных трендов и настроений.

7.2. Текстовые сообщения в мессенджерах

7.2.1. Реализован перехват текстовых сообщений в следующих мессенджерах: Telegram Desktop/Web, Skype, Microsoft Teams, WebSkype, Lync, Viber, Bitrix Desktop, BitrixWeb, Slack,

Myteam, Cisco Webex Teams, WhatsApp Desktop/Web, корпоративный eXpress, VK Teams (Cloud) Desktop/Web, ICQ Desktop/Web.

7.3. Текстовые сообщения чата Битрикс24

7.3.1. Реализован перехват переписки в Битрикс24 Desktop и на сайте (облачная и корпоративная версии Битрикс).

Для корпоративной версии Битрикс24 реализована интеграция с модулем DLPS мессенджера eXpress через ICAP-протокол: сервер комплекса принимает входящие и исходящие сообщения и отображает их в отчёте «Чаты/звонки».

7.4. Электронная почта и вложения

7.4.1. Реализован перехват входящих и исходящих писем с вложениями для: Microsoft Outlook — Exchange/IMAP/POP3/SMTP (с шифрованием и без), IBM Lotus Notes — вся исходящая почта, Outlook Express, Thunderbird, Bat, Mail — POP3/SMTP (с шифрованием и без).

7.5. Отправка файлов в интернет

7.5.1. Реализован перехват файлов, отправляемых через браузер, почтовые клиенты, Skype, Lync, популярные мессенджеры, FTP/FTPS. Во всех случаях обеспечивается перехват, сохранение файлов и запрет их отправки.

7.6. Файловые операции

7.6.1. Реализован перехват операций копирования, удаления и переноса файлов.

7.6.2. При копировании файлов на флэш-накопитель реализована функция теневого копирования.

7.6.3. Реализована поддержка протокола WebDAV.

8. DLP-ВОЗМОЖНОСТИ

8.1. DLP Анти-фото

8.1.1. Реализована защита от фотографирования экрана компьютера смартфоном в момент работы с критическими приложениями и сайтами.

8.2. Голосовой DLP

8.2.1. Реализована мгновенная реакция на произнесённые сотрудником слова и фразы в голосовых переговорах через: Skype, Lync, Viber, Telegram, Bitrix Desktop, ICQ, Mail.ru Agent, Zoom, MS Teams, Slack, Myteam, Cisco Webex Teams.

8.3. Водяные знаки на изображениях

8.3.1. Реализовано нанесение скрытых водяных знаков на PrintScreen-изображения с целью их последующей идентификации после обнаружения в открытых источниках.

8.4. DLP в документах

8.4.1. Реализованы функции контроля документов с ключевыми словами и фразами: открытие, отправка в интернет, печать, копирование на флэш-накопитель, копирование в буфер обмена — с регистрацией события и возможностью блокировки операции.

Реализован DLP-контроль голоса: мгновенная реакция на произнесённые сотрудником слова и фразы из настроенных словарей в голосовых переговорах через поддерживаемые мессенджеры — с регистрацией события и уведомлением администратора.

8.4.2. Поддерживаются форматы документов: .docx, .xlsx, .odt, .ods, .sxw, .pptx, .odp, .txt, .csv, .pdf, .doc, .xls, .ppt, .rtf.

8.4.3. Реализован нечёткий поиск текста и поиск по шаблонам: кредитные карты, контакты, пользовательские регулярные выражения (RegExp PCRE).

8.5. Сканирование папок Outlook

8.5.1. Реализовано сканирование папок «Черновики», «Встречи» и «Задачи» Outlook на наличие конфиденциальных вложений с удалением найденных конфиденциальных вложений.

8.6. Маркировка документов

8.6.1. В документах реализованы скрытые метки для защиты от несанкционированной отправки; пересохранение документа и копирование его части реализованы.

8.6.2. Поддерживаются исходные форматы маркировки: pdf, docx, xlsx, pptx, ; реализовано пересохранение в форматы OpenOffice: odt, ods, sxw.

8.7. Запрет на отправку файлов

8.7.1. Реализован запрет отправки файлов через сайты-файлообменники, почтовые сайты и программы, чаты и социальные сети.

8.8. Карантин

8.8.1. Все файлы, заблокированные к передаче согласно DLP-политикам, помещаются в карантин в зашифрованном виде.

Карантин-файлы доступны для просмотра и ручного принятия решений (разрешить или удалить) непосредственно из веб-интерфейса администратора. Блокировка файла фиксируется в журнале событий.

8.9. Настройки DLP по форматам файлов

8.9.1. Реализована страница настроек «DLP по форматам файлов» для анализа файлов по типам: CAD-чертежей и иных специализированных форматов.

8.10. Цифровые отпечатки файлов

8.10.1. Реализована поддержка цифровых отпечатков файлов при операциях поиска и DLP.

Сервер комплекса выполняет периодическое автоматическое обновление цифровых отпечатков из указанных папок и файлов (раз в час), включая поддержку масок и сетевых путей UNC. Удаление оригинального файла не приводит к удалению его отпечатка из базы данных.

8.11. Распознавание текста на скриншотах (OCR)

8.11.1. Реализован запрет копирования скриншота, содержащего важные текстовые данные, в буфер обмена.

8.11.2. Реализована поддержка встроенного офлайн-движка OCR и онлайн-сервиса ABBYY OCR.

8.12. Управление буфером обмена

8.12.1. Реализованы полный запрет копирования в буфер обмена и раздельный запрет клавиши PrintScreen.

9. КОНТРОЛЬ ДОСТУПА И ОБОРУДОВАНИЯ

9.1. Запрет веб-сайтов

9.1.1. Реализован запрет посещения выбранных сайтов в браузерах.

9.2. Запрет FTP

9.2.1. Реализован полный запрет передачи и приёма файлов по протоколу FTP.

9.3. Запрет WiFi / Bluetooth / USB-модема

9.3.1. Реализован запрет сетевых подключений через WiFi, Bluetooth и USB-модем.

9.4. Запрет RDP

9.4.1. Реализована блокировка входящих удалённых подключений к компьютеру по протоколу RDP.

9.5. Запрет USB-устройств

9.5.1. Реализован запрет подключения следующих категорий USB-устройств: фотокамеры и смартфоны, съёмные диски, Bluetooth/WiFi/модем.

9.6. Чёрный и белый списки программ

9.6.1. Реализован запрет запуска программ в соответствии с чёрным и белым списками.

9.7. Запрет флэш-дисков

9.7.1. Реализован запрет записи на съёмные носители; реализован полный запрет доступа к съёмным носителям.

9.8. Запрет команд в терминале Linux

9.8.1. Реализован запрет выбранных команд в терминале Linux.

10. ГЕОЛОКАЦИЯ

10.1. Реализована геолокация местоположения ноутбуков на картах Google.

10.2. Реализовано определение внешнего IP-адреса, страны и города.

11. СКУД И УЧЁТ РАБОЧЕГО ВРЕМЕНИ

11.1. Детализация СКУД

11.1.1. В отчёте отображаются реальные входы и выходы сотрудников по данным СКУД.

11.1.2. Реализована поддержка системы СКУД.

11.2. Табель учёта рабочего времени (УРВ)

11.2.1. В форме стандартного табеля учёта рабочего времени реализовано отображение данных по активности на компьютере и по данным СКУД.

11.2.2. В отчёте отображается информация о прогулах, опозданиях, начале и конце рабочего дня, общем отработанном времени.

12. МОНИТОРИНГ АКТИВНОСТИ СОТРУДНИКОВ

12.1. Машинное время

12.1.1. Реализована функция просмотра времени активности (включения/выключения) компьютеров сотрудников.

12.2. Загрузка CPU / GPU

12.2.1. Реализован отчёт с развёрнутой во времени картиной использования ресурсов процессора и видеокарт; отчёт применяется для контроля майнинга.

12.3. Пользовательское время

12.3.1. Реализована фиксация активности пользователя за день, прогулов, опозданий на работу, популярных программ и сайтов; реализована синхронизация с календарём Outlook и СКУД.

Отчёт «Пользовательское время» содержит графическое отображение активности на временной шкале за каждый день: активное время (красный), время без активности (серый), данные из календаря Outlook (фиолетовый), данные СКУД (голубой), паузы наблюдения (оранжевый). Встречи из Outlook синхронизируются каждые 5 минут (учитываются только предстоящие встречи).

12.4. Запуск программ

12.4.1. Реализован просмотр перечня программ и времени активной работы сотрудника в них.

Для каждой программы отображается: время активной работы (мышь/клавиатура), общее время на переднем плане, заголовок окна, путь исполняемого файла, вводимый текст. Программы упорядочены по убыванию активного времени.

12.5. Мониторинг сайтов

12.5.1. Реализован отчёт по сайтам, которые посещал сотрудник.

12.5.2. Реализован мониторинг вводимого текста (кейлоггер).

Реализован «Клавиатурный почерк» — биометрический анализ динамики ввода текста (скорость набора, паузы, количество опечаток) для идентификации пользователя за рабочим местом. Система выявляет работу другого сотрудника под чужой учётной записью и формирует предупреждение с указанием вероятного реального пользователя.

12.5.3. Реализован перехват вводимого текста во всех программах и на всех сайтах.

12.6. Буфер обмена

12.6.1. Реализована фиксация текста, файлов и изображений в буфере обмена.

В отчёте «Буфер обмена» отображаются дата, время перехвата и перехваченное содержимое. Файловые операции с участием буфера обмена дополнительно отражаются в отчёте «Файловые операции».

12.7. Поисковые запросы

12.7.1. Реализован просмотр всех поисковых запросов пользователя в поисковых системах Google, Yandex и других.

13. ГОЛОСОВЫЕ И ТЕКСТОВЫЕ КОММУНИКАЦИИ

13.1. Голосовые переговоры и распознавание

13.1.1. Реализованы перехват и запись голосовых переговоров с распознаванием речи сотрудника в текстовый файл с применением нейронных сетей и искусственного интеллекта.

13.2. Текстовые сообщения

13.2.1. Реализован перехват сообщений в мессенджерах и корпоративных чатах.

14. КОНТРОЛЬ ФАЙЛОВ И ДОКУМЕНТОВ

14.1. Файловые операции

14.1.1. Реализован перехват операций копирования, удаления и переноса файлов.

14.1.2. Реализованы контроль копирования файлов на флэш-носитель и теневое копирование.

14.2. Контроль печати

14.2.1. Реализован перехват распечатанных файлов в формате спулера с расчётом стоимости в зависимости от установленного тарифа.

Перехваченные файлы сохраняются в формате спулера с привязкой к пользователю, устройству и времени события. Реализован расчёт стоимости печати на основе настраиваемого тарифа. Отчёт «Печать на принтере» отображает список распечатанных документов с возможностью просмотра сохранённой копии.

14.3. Подозрительные события

14.3.1. Реализована запись в отчёт настраиваемых пользователем событий: запуск программ, посещение сайтов, ввод текста с учётом алгоритма нечёткого сравнения слов.

14.3.2. Реализована запись видео с экрана при возникновении подозрительных событий.

15. ОТЧЁТЫ И АНАЛИТИКА

15.1. Отчёт «Контакты»

15.1.1. Реализован просмотр списка контактов сотрудника, с которыми он общался по e-mail, Skype и в чатах.

Контакты сотрудников, находящихся под мониторингом, выделяются зелёным цветом. Источниками данных служат перехваченные письма (поля «от кого» и «кому») и сообщения из мессенджеров, а также досье сотрудников.

15.2. Отчёт «Граф связей»

15.2.1. Реализовано визуальное отображение отчёта «Контакты» в виде наглядного графа связей.

В отчёте «Граф связей» реализована поддержка режима 3D-визуализации. Цветовая кодировка: синий — наблюдаемые сотрудники, серый — связанные внутренние контакты, красный — внешние контакты. Толщина линии связи пропорциональна числу контактов за период. При выборе нескольких сотрудников наглядно отображаются их общие контакты.

15.3. Отчёт «Пользователи онлайн»

15.3.1. Реализован отчёт с наглядным отображением периодов подключения пользователей к серверу.

15.4. Отчёты мониторинга и AI

15.4.1. Реализованы: аналитика «Чёрный ящик», распознавание лиц, анализатор рисков, глобальный поиск и AI-отчёты с применением нейронных сетей и искусственного интеллекта.

Реализован отчёт «Анализатор переписок» — аналог отчёта «Чаты и звонки», дополненный столбцом «Краткое содержание» с ИИ-суммаризацией переписки на базе LLM-нейросети без необходимости читать её полностью. Реализован отчёт «Классификация файлов» — отображает файлы, отправленные в интернет, на съёмные носители или на печать, с автоматической классификацией содержимого по заданным категориям (в %) на базе LLM.

15.5. Отчёт «Модуль интеллектуальной аналитики ИИ»

15.5.1. Реализован модуль генеративного искусственного интеллекта для анализа данных и формирования рекомендаций.

Отчёт «AI Оракул» передаёт накопленные данные мониторинга в LLM-нейросеть и формирует обобщённую характеристику деятельности сотрудника в нескольких аналитических разрезах: оценка продуктивности, поведенческие риски, рекомендации. Реализована настройка подключения к локальному или облачному LLM-серверу.

16. ГОЛОСОВОЙ И ЧАТ-ПОМОЩНИК

16.1. Реализован голосовой и чат-помощник для решения вопросов, связанных с работой комплекса, с применением искусственного интеллекта и нейронных сетей для предоставления

информации, поддержки пользователей, выполнения команд и управления задачами. Алгоритмы машинного обучения обеспечивают постепенное улучшение качества и точности ответов.

Голосовой и чат-помощник функционирует на базе встроенного LLM-сервера. Реализована поддержка интеграции с внешними LLM-провайдерами: Gemini, а также локальными LLM-серверами через совместимый API. Помощник поддерживает русский и другие языки.

17. ТРЕБОВАНИЕ К ТЕХНИЧЕСКОЙ ПОДДЕРЖКЕ

17.1. Система DLP обеспечивается технической поддержкой от производителя в режиме 24 часа в сутки, 7 дней в неделю, 12 месяцев.