ТКБ МОНИТОРИНГ

ПРОДУКТ КОМПАНИИ "ТЕХНОЛОГИИ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ"

Pointlane
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Система мониторинга и анализа информации в корпоративных сетях

ТКБ-Мониторинг

Краткое описание продукта

Сфера применения продукта

Программно-аппаратный комплекс «ТКБ-Мониторинг» предназначен для анализа и онлайн-мониторинга информационных потоков и пользовательской активности в корпоративных информационных системах.

Продукт предназначен для решения следующих задач:

- комплексная оценка эффективности работы персонала;
- анализ внутренних и внешних коммуникаций сотрудников;
- проведение служебных расследований с целью выявления инсайдеров и нелояльных к организации сотрудников;
- пресечение неэффективных и вредоносных действий, случаев мошенничества и распространения конфиденциальной информации.

Конкурентная среда

Решение "ТКБ-Мониторинг" находится на пересечении двух рынков: DLP-решений и решений по анализу эффективности работы сотрудников.

Рынок Data Leak Prevention - системы защиты от утечек данных
Представители: InfoWatch, PacketMotion, Symantec DLP, McAfee DLP

Основная особенность систем такого рода - высокие требования к корпоративным политикам безопасности, необходимость постоянной доработки правил фильтрации и наличие в штате отдельного специалиста, ответственного за эффективное использование системы. Внедрение таких систем - серьезная и затратная организационная процедура.

ТКБ не ставит перед собой задачу блокирования информации. Наш комплекс анализирует потоки данных в организации и позволяет получать отчеты и автоматические уведомления по потенциально «проблемным» ситуациям. Таким образом, он также оказывает помощь в борьбе с утечками, но требует меньше усилий при внедрении.

За пределами сферы компетенции решений DLP остаются внутренние угрозы, на выявление которых нацелен "ТКБ-Мониторинг": эффективность использования рабочего времени, текучка кадров и злоупотребления на рабочих местах.

Рынок решений удаленного мониторинга действий за компьютером.
Представители: LanAgent, Maxapt QuickEye, StaffCop, Internet Access Monitor.

В целом, эти решения нацелены на небольшие организации, продаются в "коробочном" исполнении и не предусматривают адаптации к информационной среде заказчика. Большинство продуктов использует один канал сбора информации: внедрение программ-агентов на рабочее место. Недостатком таких решений является отсутствие возможностей контент-анализа и протоколирования информации, что исключает ретроспективный анализ коммуникаций.

Установкой и технической поддержкой данных продуктов занимаются внутренние технические службы, что может приводить к искажению информации, получаемой руководителями, и значительно ограничивает сферу применения таких программ.

Комплекс ТКБ-Мониторинг обладает гораздо более широкими возможностями, при этом пользователями системы являются непосредственно руководители. Внедрение осуществляется внешними специалистами, что полностью исключает искажение данных заинтересованными лицами.

Отличительные особенности комплекса

Анализ трафика и извлечение из него фактов

Наше решение отличает особое внимание к содержательной части веб-трафика. Модуль анализа извлекает из потока данных факты, такие как "поисковый запрос", "отправленное сообщение", "полученное сообщение", "публикация резюме". Список сайтов, активность на которых детально обрабатывается, постоянно расширяется и включается в пакеты бесплатных обновлений.

Каналы сбора информации

"ТКБ-Мониторинг" использует два канала сбора информации: программы-агенты и монитор сетевого потока. Часто невозможно внедрить программы-агенты на все рабочие места. Наше решение снимает максимум информации с сетевого потока данных, а программы-агенты используются для получения дополнительной информации о работе с локальными приложениями и файлами.

Информирование, а не блокирование

Принципиальный отказ от блокирования информации дал решению "ТКБ-Мониторинг" сразу несколько ценных преимуществ:

- сделал решение более легким и дешевым при внедрении;
- снизил до минимума требования к сетевой инфраструктуре компании;
- существенно повысил надежность сети: внедрение не требует установки модулей мониторинга "в разрыв" сетевого канала.

Минимальное участие it-специалистов заказчика

Для заказчика часто необходимо скрыть факт внедрения продукта. Типичная установка продукта занимает не более часа и при необходимости может быть представлена сотрудникам, как система учета трафика. IT-отдел не имеет доступа к содержимому сервера и веб-интерфейсу. По требованию заказчика может быть создано несколько учетных записей с ограниченным доступом к интерфейсу.

Протоколирование и широкие возможности ретроспективного анализа

Информация, полученная в результате анализа, сохраняется в масштабируемом хранилище. Таким образом, доступен ретроспективный анализ архива с полнотекстовым поиском по сообщениям и с расширенными возможностями поиска по таким критериям как “отправитель”, “получатель”, “тип сообщения”, “канал коммуникации”, “лингвистический анализ содержания”.

Интеграция со смежными системами

ТКБ-Мониторинг может быть интегрирован с такими офисными системами, как СКУД и телефония. Это позволяет объединить "на одном экране" статистику посещения офиса, телефонных и сетевых коммуникаций и вести перекрестный анализ, выявляя проблемные ситуации (например, действия на компьютере отсутствующего сотрудника).

Адаптация и масштабируемость

Система легко масштабируема: для небольших компаний возможна установка одного блока, отвечающего за весь функционал (“маленькая черная коробка”). Внедрение в крупных компаниях и организациях с филиальной сетью требует установки дополнительных аппаратных модулей, но при этом настройка комплекса остается такой же простой.

Практика использования комплекса

Заказчик: Группа компаний "Восход-СК"*
Направления деятельности: девелопмент, строительство.
Количество сотрудников: 300

По результатам 4-х месяцев эксплуатации комплекса:

- службой режима выявлены нарушения трудовых договоров;
- в трех отделах изменены бизнес-процессы на основе анализа деловых внутрикорпоративных коммуникаций;
- два сотрудника уволены в связи с деятельностью, несовместимой с занимаемыми должностями;
- пресечено распространение информации, вредившей имиджу группы компаний;
- по результатам оценки целесообразности использования офисного интернета, значительно сокращены расходы на трафик.

Заказчик: Группа компаний "GBR-Networks"
Направления деятельности: Интернет-маркетинг, создание и продвижение сайтов, поисковая оптимизация.
Количество сотрудников: 330

По результатам 3-х месяцев эксплуатации комплекса:

- установлено, что некоторые сотрудники недовольны условиями работы и денежными компенсациями;
- изменения мотивационной политики позволили сохранить ряд ценных сотрудников;
- оценка эффективности работы департаментов позволила существенно оптимизировать расходы;

Заказчик: ООО "Аполлон"
Направление деятельности: логистика.
Количество сотрудников: 50

По результатам 10-ти месяцев эксплуатации комплекса:

- неоднократно выявлялись факты нарушения корпоративной этики;
- предотвращена утечка данных, представляющих коммерческую тайну;
- пресечены недружественные действия конкурентов.

* Названия компаний изменены

Заказчик: ЗАО “Южный Бриз-Телеком”
Направление деятельности: телекоммуникации.
Количество сотрудников: 3100

По результатам тестовой эксплуатации комплекса:

- выявлены многочисленные факты посещения развлекательных ресурсов;
- службой информационной безопасности выявлены факты нарушения трудового договора;
- согласованы сроки ввода комплекса в промышленную эксплуатацию.

Краткое описание архитектуры и функционала продукта

Функционал комплекса можно разделить на три составляющих:

- мониторинг информационных потоков сети и активности рабочих станций персонала;
- протоколирование получаемой информации;
- анализ и наглядное отображение информации для принятия решений.

Мониторинг информационных потоков и активности рабочих станций

Мониторинг осуществляется двумя способами: с использованием сетевых фильтров и программ-агентов на рабочих местах пользователей. Информация, поступающая от этих двух типов источников, проходит первичный анализ и попадает в хранилище в виде фактов.

Текущая версия комплекса распознает в информационном потоке следующие факты:

Веб-активность

- Посещение сайтов
- Поиск работы (ресурсы Job.ru, hh.ru, Superjob.ru, Rabota.ru, Rabota@Mail.ru).
- Поисковые системы (Rambler.ru, Yandex.ru, Google.com, поиск Mail.ru).

Коммуникации

- Блоги (livejournal.com, liveinternet.ru, Моймир.ру, ya.ru)
- Социальные сети (Odnoklassniki.ru, VKontakte.ru, Moikrug.ru, FaceBook)
- Сайты знакомств (Love.Mail.Ru, Love.Rambler.Ru, 24Open.ru, Mamba.ru)
- Корпоративная почта
- Веб-почта (Rambler-почта, Mail.ru, Yandex-почта, Gmail.com)
- Мгновенные сообщения (ICQ, Mail.ru-Агент)
- Отправка SMS (MTS, BeeLine, Megafon)

Активность на компьютере

- Общее время работы компьютера
- Реальная активность пользователя на компьютере
- Запуск приложений, классификация приложений по группам (офисные, игры и т.п.)
- Время работы пользователя в приложении
- Копирование файлов на внешние носители
- Снимки экранов пользователей

Протоколирование получаемой информации

Внедрение решения «ТКБ-Мониторинг» позволяет вести подробное протоколирование информации, пересылаемой по корпоративной сети. Срок хранения данных в стандартной комплектации составляет 6 месяцев от текущей даты, однако может быть легко увеличен с помощью изменения аппаратной конфигурации комплекса.

В настройках системы предусмотрена возможность запрещения мониторинга определенных сотрудников.

Анализ и наглядное отображение информации

Веб-интерфейс системы обеспечивает следующий функционал:

- Отображение статуса деятельности сотрудников (последняя активность, оценка эффективности работы на основании данных об используемых приложениях)
- Отображение всех авторизаций сотрудника (в корпоративной почте, в веб-почте, в социальных сетях, на сайтах вакансий, в системах обмена мгновенными сообщениями)
- Отображение круга общения и интенсивности общения сотрудника (по всем каналам)
- Отображения «ленты фактов» - полного протокола деятельности и коммуникаций в офисе.
- Возможность полнотекстового поиска по «ленте фактов» за произвольный период времени
- Гибкие возможности комбинированной фильтрации по структурным блокам фактов (сотрудники, временные интервалы, типы фактов, адресаты, тематики сайтов, содержание сообщений и пр.)
- Возможности поиска и фильтрации фактов по тематическим словарям с учетом морфологии русского языка.
- Конструктор фильтров, позволяющий формировать и сохранять собственные фильтры фактов.

- Отображение наглядных статистических отчетов
    - Учет общего рабочего времени за компьютером
    - Учет работы в группах приложений – офисные, веб, игры и т.п.
    - Учет активности работы с веб-ресурсами, в том числе по тематикам
    - Учет наиболее посещаемых сотрудниками сайтов
    - Учет активности общения по разным каналам коммуникаций

Данные статистические отчеты могут быть получены по отдельному сотруднику или группе, за любой временной отрезок.

Есть возможность экспорта статистических отчетов в формат Microsoft Excel

В интерфейсе предусмотрена настройка автоматических уведомлений (оповещений) при срабатывании набора заданных правил.

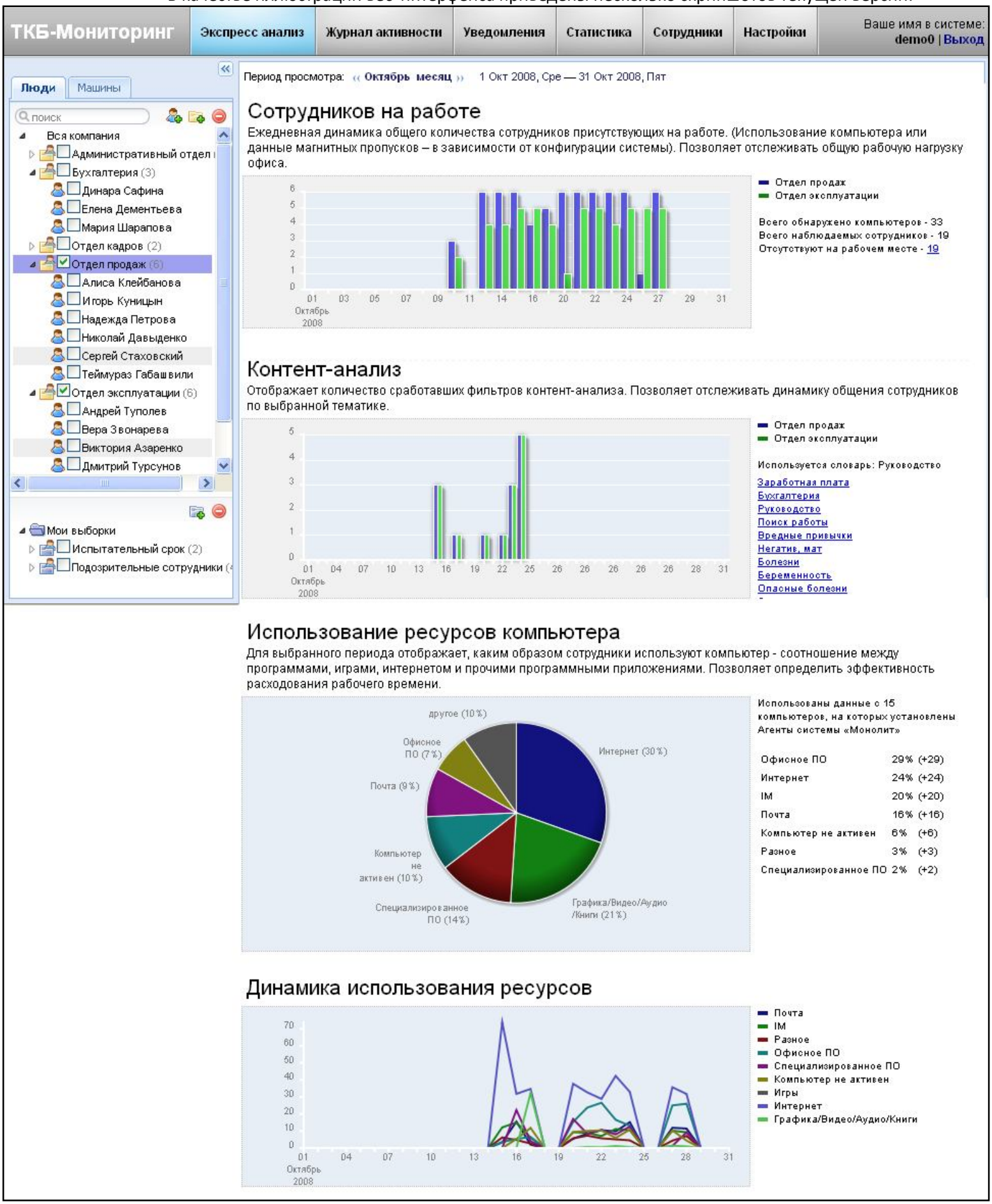
Автоматические уведомления отображаются в веб-интерфейсе системы, обозначая наличие факта, соответствующего критерию указанному критерию.

Уведомления могут быть настроены по любой комбинации критериев аналогично настройке фильтров.

ТКБ МОНИТОРИНГ
ПРОДУКТ КОМПАНИИ "ТЕХНОЛОГИИ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ"

Pointlane
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

В качестве иллюстрации веб-интерфейса приведены несколько скриншотов текущей версии:



В компоненте “Экспресс анализ” осуществляется обзор статистических данных о работе персонала (рис. 1).

В системе доступен ряд отчетов, а на странице "Экспресс-анализ" отображается графическое представление самых важных из них.

Сотрудников на работе - количество сотрудников, присутствующих на рабочих местах. Используется методика, аналогичная отчету “Время работы за компьютером”.

Контент анализ - количество сообщений (данные от Агента, анализ почтового и ICQ трафика, данные социальных сетей), соответствующее выбранной тематике. Дополнительная информация о настройке словарей представлена в разделе “Лингвистические справочники”.

Использование ресурсов компьютера - распределение времени работы за компьютером между различными видами деятельности. Данные предоставляются агентами на рабочих станциях сотрудников и классифицируются по типам приложений (офисное ПО, почта, игры).

Динамика использования ресурсов - динамика изменений показателей предыдущего отчета.

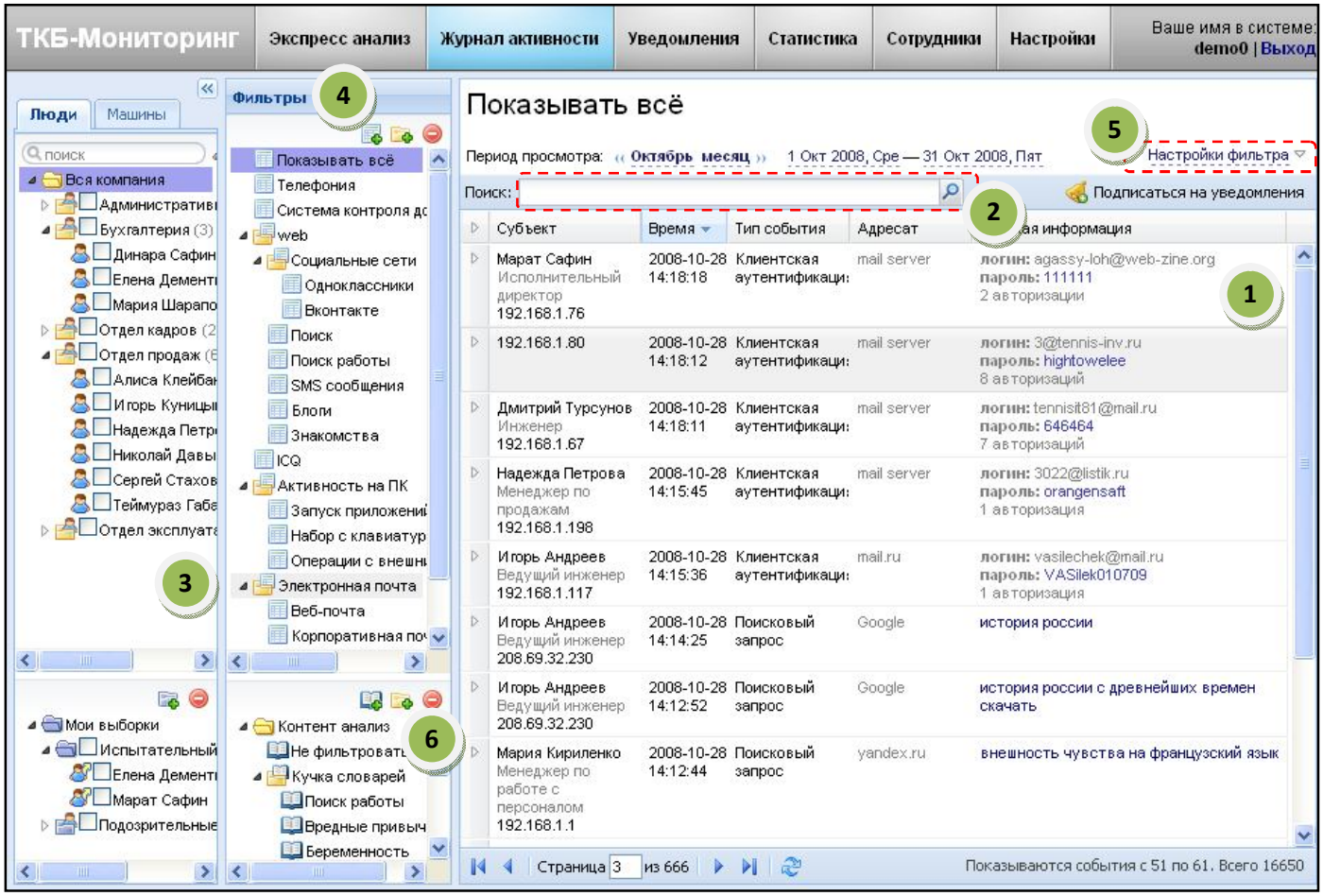


рис 2. Журнал активности

“Журнал активности” (рис. 2) - основной рабочий модуль системы. Он позволяет просматривать все **факты,** зафиксированные системой.

Страница “Журнала активности” состоит из следующих функциональных блоков:

Список фактов (1) – основной рабочий экран раздела “Журнал активности”. На данном экране пользователь может постранично просматривать список фактов, отобранных с помощью фильтров.

Факты представлены в виде таблицы, где каждая строка – это отдельный факт или группа однотипных фактов, например, множественные авторизации одного и того же пользователя в течение дня.

Форма поискового запроса (2) позволяет выполнять поиск по полям таблицы фактов.

Поиск осуществляется с учетом текущих настроек фильтров, включая выбранных сотрудников, тип фактов и лингвистические словари.

Панель Люди/Машины (3)

Данная вкладка является стандартной для всех компонентов системы. Использования фильтров организационной структуры (Люди) или списка рабочих станций (Машины) позволяет быстро получить информацию об активности конкретного сотрудника или отдела.

Панель Фильтры (4) позволяет фильтровать факты по их типу. Например, факты от агента на рабочей станции, активность в социальных сетях, сообщения ICQ, только авторизации.

С помощью панели **Настройки Фильтра (5)** можно изменять текущие фильтры и создавать новые.

Панель Контент-анализ (6) позволяет отбирать факты, относящиеся к определенной тематике. Определение тематики происходит по поиску соответствия между поисковым запросом фильтра и информационными полями факта. Например, к тематике “Поиск работы” будут отнесены факты содержащие информацию о резюме, вакансиях, рабочих отношениях.

Детально ознакомиться с пользовательским интерфейсом можно, запросив доступ к демонстрационному стенду у компании-разработчика или ее партнеров.

Процесс внедрения комплекса

Установка комплекса включает в себя в общем случае:

- установку точек сборки в сегментах сети;
- установку центрального аналитического сервера (опционально);
- настройку почтового сервера для доступа комплекса к корпоративной почте (опционально);
- настройку подключения к LDAP-серверу (опционально);
- установку Агентов на рабочие станции под управлением ОС Windows (опционально).

В зависимости от топологии сети и количества рабочих станций точка сборки может быть единственной и выполнять функцию аналитического сервера.

Точки сборки могут ставиться как "в разрыв" перед свичем/хабом/концентратором, так и "параллельно" (SPAN port).

При установке "в разрыв" надежность работы сети зависит от работоспособности оборудования, но не от программного комплекса. При выходе из строя программного обеспечения трафик продолжает пропускаться прозрачно.

При параллельной установке надежность сети не снижается, но требуется дополнительная настройка сетевых концентраторов для зеркалирования трафика на точку сборки.

Каждая точка сборки обрабатывает информацию из своего сегмента и передает ее на аналитический сервер.

Так как на сервер передается только фактографическая информация, то нагрузка на сеть минимальна.

Установка точек сборки в каждый сегмент сети необходима для того, чтобы анализировать трафик в неизменном состоянии - с исходными MAC и IP адресами (до их прохождения через NAT).

Системная консоль

На каждом сервере комплекса установлена "Системная консоль" - консольный интерфейс для управления настройками сервера. Все необходимые настройки производятся у заказчика и не требуют участия компании-разработчика.

ТКБ МОНИТОРИНГ
ПРОДУКТ КОМПАНИИ "ТЕХНОЛОГИИ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ"

Pointlane
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Информация о компаниях

Компания «Pointlane» – Российский системный интегратор в области информационной безопасности.

Направления деятельности **«Pointlane»:**

- Аудит информационной безопасности;
- Разработка и внедрение процессов управления информационной безопасностью;
- Внедрение систем и средств защиты информации;
- Управление непрерывностью бизнеса;
- Защита персональных данных.

Контакты:
http://www.pointlane.ru
Тел.: +7 (495)233-6508
E-mail: consult@pointlane.ru
109202, г.Москва, ул.Басовская д.16 стр.1

Компания **“Технологии Корпоративной Информации”** основана в 2007 году. Направление деятельности компании – разработка программного обеспечения в области защиты и анализа информации. ТКБ с особой ответственностью подходит к качеству разработки программного обеспечения, ориентируясь при этом на тесное взаимодействие с клиентами и партнерами.

Контакты:
http://tkb-monitoring.ru
Email: cst@cstech.ru
Телефон: +7 (495) 937-4075