Программный комплекс

«Серчинформ ДЛП»

Руководство пользователя

на 114 листах

2023

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин		Определение
Атрибутный поиск	–	поиск по атрибутам перехваченных документов (дата и время отправки сообщения, имя пользователя локальной сети, IP-/MAC-адрес рабочей станции, с которой осуществлялся перехват и т.п.)
Дело	–	централизованная информация о фактах, деталях и участниках нарушений политик безопасности компании.
Защита информации	–	деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
Поиск похожих	–	поиск текстовых документов, похожих по содержанию. В ходе поиска похожих, запрашиваемый текст сопоставляется каждому документу индекса. Документы, похожие по содержанию на запрос, фильтруются по степени сходства или «релевантности»
Программный продукт	–	программное обеспечение как результат человеческой деятельности, выставленный на рынке массового покупателя в качестве товара и имеющий ненулевую потребительную стоимость
Система	–	автоматизированная система защиты информации, разработанная ООО «ИБ-Сервис»
Текстовый поиск	–	поиск по ключевым словам и выражениям с учетом морфологии и синонимов
Фигурант	–	пользователь, имеющий отношение к нарушениям политик безопасности компании. Например, отправитель файла по протоколам электронной почты и т.п.
Фразовый поиск	–	частный случай текстового поиска, при котором можно зафиксировать порядок следования слов и выражений запроса

СОКРАЩЕНИЯ

Сокращение		Расшифровка
АРМ	–	Автоматизированное Рабочее Место
ИБ	–	Информационная Безопасность
ТПЛВС	–	Локальная Вычислительная Сеть
ОС	–	Операционная Система
ПО	–	Программное Обеспечение
РС	–	Рабочая Станция
ТП	–	Служба Технической Поддержки

1 ВВЕДЕНИЕ

Настоящее руководство содержит сведения, необходимые для работы с системой «Серчинформ ДЛП».

1.1 НАЗНАЧЕНИЕ СИСТЕМЫ

Программное решение «Серчинформ ДЛП» предназначено для выявления и предотвращения утечек конфиденциальной информации и персональных данных в ЛВС организаций, а также контроля данных, уходящих в Интернет.

1.2 ВОЗМОЖНОСТИ СИСТЕМЫ

Серчинформ ДЛП позволяет выявлять утечки конфиденциальной информации и персональных данных через электронную почту; ICQ; голосовые и текстовые сообщения Skype, Lync, Telegram, WhatsApp и Viber; посты на форумах или комментарии в блогах; внешние устройства (USB/CD); FTP; файл-серверы; ноутбуки, в том числе отключенные от корпоративной сети; документы, отправляемые на печать; а также появление конфиденциальной информации на компьютерах пользователей. Ответственные сотрудники оперативно оповещаются о нарушениях политики безопасности. Расширенные поисковые возможности позволяют эффективно защищать конфиденциальные данные при минимальных трудозатратах на анализ информационных потоков.

1.3 ТРЕБОВАНИЯ К ЧИСЛЕННОСТИ И КВАЛИФИКАЦИИ ПЕРСОНАЛА СИСТЕМЫ

Для обслуживания Системы является достаточным наличие 2 сотрудников службы информационной безопасности.

Аудиторы должны пройти обучение у сотрудников компании-разработчика программного обеспечения или у авторизованного им провайдера услуг. Также подготовка аудиторов проводится во время опытной эксплуатации Системы сотрудниками компании-разработчика.

В Таблица 1 представлен ролевой состав, функции и требования к квалификации персонала, осуществляющего сопровождение Системы.

Таблица 1 – Требования к функциям и квалификации персонала Системы

Роль	**Функции**	**Уровень квалификации**
Администратор Системы (программного обеспечения)	Модернизация, настройка и мониторинг работоспособности Системы Установка, модернизация, настройка и мониторинг работоспособности системного и базового ПО Установка, настройка и мониторинг прикладного ПО Управление базами данных Ведение учетных записей пользователей Системы	Профильное высшее образование Сертификаты компании-производителя ОС
Администратор аппаратного обеспечения	Сопровождение аппаратного обеспечения	Стандартные требования Компании
Сетевой администратор	Сопровождение сетевых коммуникаций	Стандартные требования Компании
Инженер технической поддержки[1]	Установка и настройка всех компонентов Системы Сопровождение при неполадках компонентов Серчинформ ДЛП	Стандартные требования Компании Знания инструкций по установке Системы
Сотрудник службы безопасности (аудитор)	Поиск (отслеживание) конфиденциальной информации в общем потоке контролируемого документооборота: – формализация анализа текстовых документов посредством настройки списка поисковых запросов; – настройка расписания проверок; – предварительный просмотр документа, идентифицированного как конфиденциальный, и принятие решения о целесообразности дальнейшей проверки.	Стандартные требования Компании Знания инструкции аудитора Системы

[1] Инженер технической поддержки предоставляется Компанией.

1.4 ПЕРЕЧЕНЬ ЭКСПЛУАТАЦИОННОЙ ДОКУМЕНТАЦИИ

Перечень эксплуатационных документов, с которыми необходимо ознакомиться:

- Серчинформ ДЛП. «Руководство администратора»;
- Серчинформ ДЛП. «Руководство пользователя».

2 ОБЩИЕ СВЕДЕНИЯ

2.1 НАЗНАЧЕНИЕ СИСТЕМЫ

Серчинформ ДЛП предназначен для выявления и предотвращения утечек конфиденциальной информации и персональных данных в локальных вычислительных сетях (далее – ЛВС) организаций.

Система позволяет:

- контролировать входящий и исходящий почтовый трафик на уровне рабочих станций (далее – РС) и/или сетевых протоколов (SMTP, POP3, NNTP, IMAP, MAPI, Web mail);
- блокировать на уровне РС исходящий SMTP-трафик для отдельных пользователей;
- интегрироваться с распространенными почтовыми и прокси-серверами;
- контролировать сообщения и файлы, переданные с помощью различных IM-клиентов (ICQ/QIP, Mail.ru Agent, Jabber, Google Hangouts, MS Lync, Viber, Telegram), а также переписку в популярных социальных сетях (Facebook, LinkedIn, В Контакте, Мой Мир@Mail.ru, Одноклассники, Google+, Мамба, Imo, Meebo);
- контролировать трафик Skype: сеансы текстовой и голосовой связи, файлы и SMS-сообщения;
- контролировать и ограничивать доступ пользователей или групп пользователей к устройствам (дисководам, CD/DVD-приводам, сменным накопителям, жестким дискам, мобильным устройствам типа iPod) и портов ввода-вывода (USB, FireWire, COM, LPT, IrDA);
- хранить для каждого пользователя точную копию данных, переданных на внешние устройства (теневое копирование);
- протоколировать все действия пользователей с файлами, расположенными в общих сетевых папках и/или файловых серверах;
- контролировать отправку документов на печать;
- перехватывать GET-/POST-запросы и файлы, передаваемые по HTTP(S)-протоколу;
- контролировать FTP-трафик;
- контролировать данные облачных сервисов (Evernote, Google Drive, OneDrive, Dropbox, Yandex Disk, MailRuCloud, SharePoint, ICloud, DropMeFiles, Amazon S3, OwnCloud, Pcloud, OziBox, MediaFire, OpenDrive, 4shared, Box, Syncplicity, CloudMe, MiMedia, My-Files.ru);
- фиксировать нажатия клавиш пользователями;
- осуществлять звукозапись разговоров пользователей;

- перехватывать информацию, отображаемую на мониторах РС;
- отслеживать посредством веб-камеры личность пользователя, авторизовавшегося в системе, наличие пользователя на рабочем месте, а также его действия в течение рабочего дня;
- контролировать активность пользователей в запускаемых ими приложениях;
- контролировать критичные события (вход/выход из системы, создание/удаление учетной записи, изменения в учетной записи и др.) журналов контроллера домена;
- собирать документы, хранящиеся на жестких дисках станций ЛВС, индексировать и просматривать данные документы (поддерживается около 100 файловых форматов);
- контролировать действия сотрудников службы ИБ в консолях компонентов Серчинформ ДЛП;
- контролировать данные, отправляемые с ноутбука, когда сотрудник находится вне корпоративной сети;
- однозначно идентифицировать пользователя, отправившего информацию, благодаря интеграции с доменной структурой Windows;
- исключать из перехвата трафика отдельных пользователей, пользующихся доверием;
- фильтровать перехваченную информацию и сохранять в базу данных лишь те данные, которые представляют интерес;
- управлять всеми возможными функциями агента с АРМ сотрудника службы безопасности с помощью консоли управления;
- разграничить права доступа к перехваченной информации;
- контролировать работу компонентов Серчинформ ДЛП и условий, необходимых для их корректной работы;
- автоматизировать управление индексами и базами данных компонентов Системы;
- анализировать передаваемые и принимаемые данные согласно настроенным политикам безопасности и уведомлять сотрудников службы безопасности о фактах их нарушения по электронной почте;
- собирать статистику и составлять отчеты по активности пользователей и инцидентам, связанным с нарушениями политик безопасности;
- контролировать SQL-запросы пользователей к базам данных и ответы на них.

2.2 АРХИТЕКТУРА СИСТЕМЫ

Серчинформ ДЛП базируется на клиент-серверной архитектуре.

Серверные компоненты Серчинформ EndpointController и Серчинформ NetworkController представляют собой платформы, на которых работают модули перехвата данных. Компонент Серчинформ EndpointController осуществляет перехват данных на уровне PC пользователей с помощью специально устанавливаемых агентов, в то время как сервер Серчинформ NetworkController осуществляет перехват данных на уровне сетевых шлюзов методом зеркалирования трафика.

Каждый модуль перехвата выступает в роли анализатора трафика и контролирует свои каналы передачи данных. Для текущей версии Системы предусмотрены следующие модули перехвата:

- модуль перехвата CameraController;
- модуль перехвата CloudController;
- модуль перехвата Database Monitor;
- модуль перехвата DeviceController;
- модуль перехвата FileAuditor;
- модуль перехвата FileController;
- модуль перехвата FTPController;
- модуль перехвата HTTPController;
- модуль перехвата IMController;
- модуль перехвата Индексация рабочих станций;
- модуль перехвата Keylogger;
- модуль перехвата LyncController;
- модуль перехвата MailController;
- модуль перехвата MicrophoneController;
- модуль перехвата MonitorController;
- модуль перехвата PrintController;
- модуль перехвата ProgramController;
- модуль перехвата SkypeController;
- модуль перехвата TelegramController;
- модуль перехвата ViberController;
- модуль перехвата WhatsAppController.

Search Server индексирует документы, перехваченные посредством зеркалирования трафика на сетевых шлюзах либо с помощью установленных на PC агентов, и обеспечивает поддержание индекса в постоянно актуальном состоянии.

Сервер Серчинформ AlertCenter обеспечивает проверку индексов по настроенным политикам безопасности на предмет их нарушения.

Сервер Серчинформ DataCenter предназначен для мониторинга состояния компонентов Серчинформ ДЛП и управления всеми базами данных и индексами, созданными этими компонентами. В своем составе также содержит сервер Серчинформ ReportCenter, который, в свою очередь, получает статистику по перехваченным документам и инцидентам, и записывает ее в собственную базу данных. На основании этих данных формируются отчеты, содержащие сводную информацию по результатам перехвата.

Консоли серверных компонентов Серчинформ EndpointController, Серчинформ NetworkController и Search Server позволяют управлять процессами настройки перехвата и индексирования данных.

В качестве клиентской части выступают:

- клиентское приложение Серчинформ AnalyticConsole, предназначенное для работы с индексами и базами данных, содержащими перехваченную информацию, а также для формирования и просмотра отчетов;
- клиентское приложение Серчинформ AlertCenter, предоставляющее возможность создания и настройки политик безопасности (набора правил, в соответствии с которыми фиксируются инциденты) и просмотра нарушений для текущего набора правил проверки.

2.3 КОНТРОЛИРУЕМЫЕ ПРОТОКОЛЫ

Система контролирует следующие протоколы и веб-приложения:

- SMTP – сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP. Также поддерживается Extended SMTP (ESMTP). Поддерживаются незащищенные и защищенные (SSL, TLS) соединения;
- POP3 – интернет-протокол прикладного уровня, используемый клиентами электронной почты для извлечения электронного сообщения с удаленного сервера по TCP/IP-соединению;
- NNTP – сетевой протокол распространения, запрашивания, размещения и получения групп новостей при взаимодействии между сервером групп новостей и клиентом;
- IMAP (в том числе IMAP Compressed) – протокол прикладного уровня для доступа к электронной почте, предоставляющий пользователю обширные возможности для работы с почтовыми ящиками, находящимися на центральном сервере. Является альтернативой протокола POP3;
- MAPI (в том числе RPC over HTTP) – программный интерфейс, позволяющий приложениям работать с различными системами передачи электронных сообщений. Позволяет получать, читать, создавать, отправлять сообщения, присоединять к ним файлы, получать доступ к присоединенным файлам и т.д.;

- FTP (протокол передачи файлов) – стандартный протокол для передачи файлов с одного компьютера на другой через сеть Internet. Поддерживаются активный и пассивный режимы FTP-соединений. Также поддерживается FTPS (FTP + SSL);
- HTTP (протокол передачи гипертекста) – протокол прикладного уровня для распределенных и объединенных информационных систем. Также поддерживается HTTPS (SSL + HTTP);
- Social Networks – контроль сайтов социальных сетей. Поддерживаются следующие сайты социальных сетей: Facebook, LinkedIn, Odnoklassniki, Vkontakte, Мой Мир@Mail.Ru, Google+, Mamba, Imo, Meebo;
- Cloud & SharePoint – контроль данных облачных сервисов и файлов, передаваемых при помощи MS SharePoint. Модуль позволяет отслеживать следующие облачные хранилища данных: Google Drive, OneDrive, Office 365, Dropbox, Evernote, Яндекс Диск, cloud.mail.ru, DropMeFiles, Amazon S3, ownCloud;
- Web Mail – контроль почтовых веб-служб:
    - Exchange Web Services;
    - Kerio Outlook Connect;
    - Outlook Web App и Outlook Web App light;
    - Zimbra Web Client;
    - исходящая и входящая корреспонденция с почтовых веб-серверов: Gmail, Hotmail, mail.ru, tut.by, open.by, freemail.ru, yandex.ru, rambler.ru и других. Поддерживаются незащищенные и защищенные (SSL) соединения;
- Skype – популярная бесплатная программа видео- и аудиособщения в режиме реального времени;
- ICQ/QIP – открытый сетевой протокол OSCAR, обеспечивает обмен сообщениями в реальном времени. Поддерживаются незащищенные и защищенные (SSL) соединения;
- XMPP – основанный на XML, открытый протокол для мгновенного обмена сообщениями. Поддерживаются незащищенные и защищенные (SSL) соединения;
- Mail.ru Agent – программа для быстрого обмена сообщениями через Интернет, разработанная компанией Mail.ru;
- SIP – протокол передачи данных, описывающий способ установления и завершения пользовательского интернет-сеанса, включающего обмен мультимедийным содержимым (видео- и аудиоконференция, мгновенные сообщения);

- Viber, Telegram – кроссплатформенное приложение для бесплатных сообщений, файлов и звонков, которое интегрируется в адресную книгу и авторизует по номеру телефона. Desktop-версия Viber осуществляет синхронизацию с мобильной версией приложения.

Перехват шифрованного SSL-трафика возможен с помощью агентов Серчинформ EndpointController либо путем зеркалирования в случае, когда в сети установлен прокси-сервер, способный производить мониторинг шифрованного трафика.

2.3.1 Контроль других каналов передачи данных

Агенты Серчинформ EndpointController позволяют также:

- осуществлять перехват данных, отправленных на печать;
- контролировать доступ пользователей к внешним устройствам (CD-/DVD-приводы, съемные накопители USB и FireWire, USB-устройствам WiFi и Bluetooth) и портам (USB, FireWire, COM, LPT, IRDA, Windows Mobile, Palm), а также осуществлять теневое копирование всех сохраняемых на внешние устройства данных в специальное файловое хранилище;
- протоколировать файлы, статически хранящиеся, создаваемые, изменяемые на PC пользователей;
- перехватывать информацию, отображаемую на одном или нескольких мониторах PC, включая список запущенных процессов, а также предоставляют возможность просмотра активности экрана одного или нескольких пользователей в режиме реального времени;
- фиксировать активность пользователей и запускаемых ими приложений в течение рабочего дня;
- осуществлять звукозапись разговоров пользователей, находящихся как внутри офиса, так и за его пределами (в командировках);
- создавать снимки и видеозаписи происходящего перед монитором посредством подключенной к рабочей станции веб-камеры;
- фиксировать нажатия клавиш пользователями (включая системные клавиши);
- перехватывать данные облачных сервисов: DropBox, YandexDisk, OneDrive, CMIS, OneDrive, а также библиотеки SharePoint;
- осуществлять чтение дерева файлов и каталогов на рабочих станциях пользователей, серверах, сетевых ресурсах;
- контролировать SQL-запросы к базам данных и ответы на них.

3 ОБЯЗАННОСТИ И ЗАДАЧИ АУДИТОРА

В круг типовых задач сотрудника службы информационной безопасности относительно Системы входят:

- защита Серчинформ ДЛП встроенными средствами;
- создание политик безопасности;
- создание политик карантина;
- мониторинг каналов передачи данных;
- контроль содержимого мониторов рабочих станций пользователей;
- оперативное реагирование в случае нарушений заданных политик;
- документирование всех произведенных действий.

В организациях с большим штатом сотрудников, вышеупомянутые обязанности могут делиться между несколькими аудиторами безопасности, например, сотрудниками, закрепленными за разными отделами организации.

4 НАСТРОЙКА И ЭКСПЛУАТАЦИЯ СИСТЕМЫ

4.1 СПРАВОЧНАЯ ИНФОРМАЦИЯ

Для получения дополнительной информации о настройках и возможностях Системы используйте встроенную справку, которой оснащены все компоненты Серчинформ ДЛП. Для вызова используйте клавишу «F1».

4.2 ЗАЩИТА ДАННЫХ СЕРЧИНФОРМ ДЛП ВСТРОЕННЫМИ СРЕДСТВАМИ

Если компоненты Серчинформ ДЛП включены в общую локальную сеть, то нужно использовать встроенные средства защиты. Сразу после установки и настройки компонентов Серчинформ ДЛП произведите следующие операции:

- Измените пароль доступа к консоли сервера NetworkController. После изменения пароля к серверной консоли доступом сможет воспользоваться только аудитор СБ, и только он сможет изменять настройки перехвата данных. Подробные инструкции в п. 4.2.1.
- Настройте права аудиторов относительно консолей компонентов Search Server, EndpointController, ReportCenter, AlertCenter, AnalyticConsole. Также ограничьте права доступа аудиторов к источникам данных, хранящим перехваченную информацию. Подробные инструкции в п. 4.2.2.
- Настройте доступ аудиторов СБ к политикам безопасности, меткам и спискам исключений пользователей из проверки AlertCenter. Подробные инструкции в п. 4.2.3.

Защита Серчинформ ДЛП встроенными средствами имеет ограничения. Она не позволяет:

- Ограничить доступ к базам перехваченных документов при помощи встроенных инструментов СУБД. Например, администратор корпоративной СУБД сможет удалить базы перехваченных документов.
- Обеспечить защиту от пользователей, имеющих права администратора на серверах Серчинформ ДЛП, например, от системных администраторов компании.

4.2.1 Ограничение доступа к консоли NetworkController

Первая задача, которую Вы должны выполнить как сотрудник службы безопасности, это сменить пароль доступа к консоли серверного модуля Серчинформ NetworkController.

Пароль, установленный по умолчанию, – *Admin.* Новый пароль должен содержать от шести и более символов.

Диалоговое окно смены пароля вызывается из главного меню консоли (см. Рисунок 4.1).

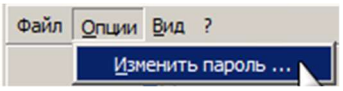


Рисунок 4.1

Введите старый пароль (значение по умолчанию – *Admin*), введите и повторите новый пароль, затем щелкните кнопку «ОК».

При следующем вызове консоли вводится новый пароль.

Авторизация доступа к консоли нужна для того, чтобы посторонние лица, в том числе администратор пользовательской сети, не могли управлять перехватом информации, а также:

- запускать/останавливать перехват информации;
- изменять настройки перехвата;
- исключать пользователей из перехвата.

4.2.2 Разграничение прав с помощью модуля DataCenter

DataCenter позволяет создать список сотрудников службы безопасности и сформировать для каждого из них права на просмотр данных по тем или иным пользователям, компьютерам либо их группам. Под данными подразумеваются инциденты, зафиксированные компонентом Серчинформ AlertCenter, а также содержимое документов при просмотре в Серчинформ AnalyticConsole.

Перейдите на вкладку «Настройки» и щелкните кнопку «Права доступа». Установите флажок «Включить ограничение прав доступа для просмотра результатов поиска и инцидентов».

В левой части окна («Аудиторы») с помощью кнопки «Добавить/Удалить» формируется список сотрудников службы безопасности (см. Рисунок 4.2).

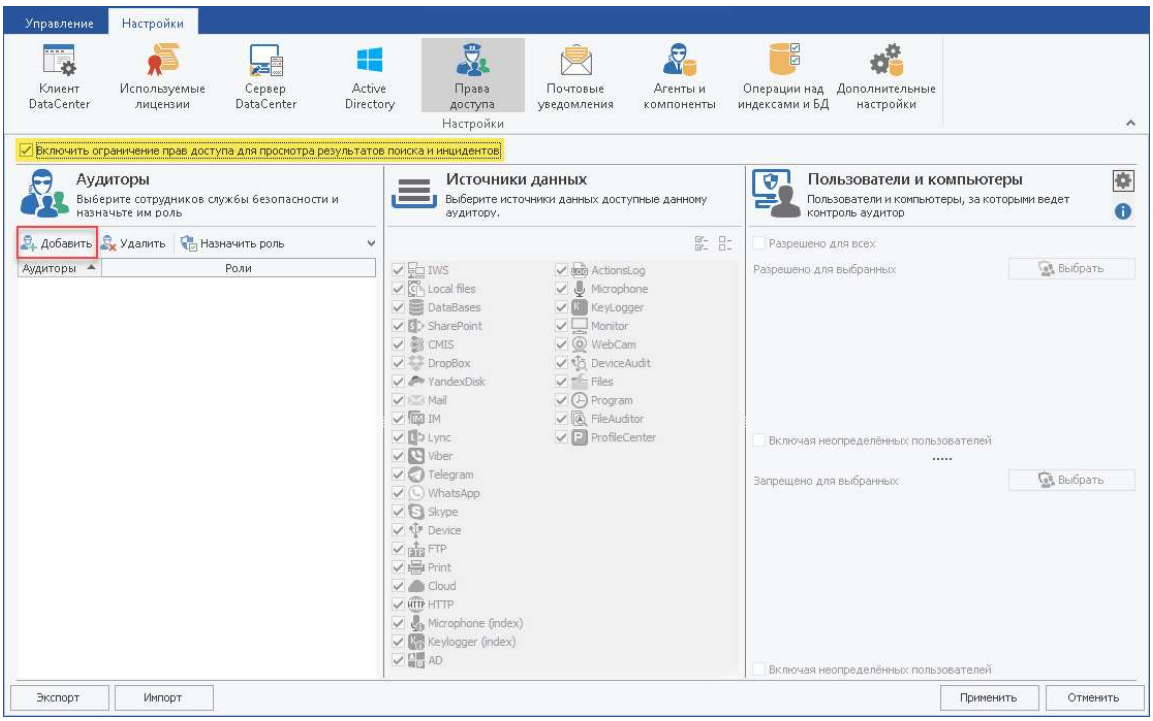


Рисунок 4.2

По умолчанию в системе предустановлены роли **Admin**, **Viewer и DirectReports**[2]. Каждому добавленному аудитору присваивается роль **Viewer**, которая, при необходимости, может быть изменена. Выбранных ролей может быть несколько. Если имеющихся по умолчанию ролей/прав недостаточно, воспользуйтесь редактором ролей.

В центральной части окна отметьте флажками продукты, данные которых разрешено отслеживать выбранному сотруднику службы безопасности. Для руководителя отдела ИБ может быть разрешен также просмотр журнала действий (**ActionsLog**) остальных аудиторов (см. Рисунок 4.3).

[2] Роль DirectReports назначается руководителям отделов. Она предоставляет доступ к просмотру Web-отчетов по подчиненным своего отдела.

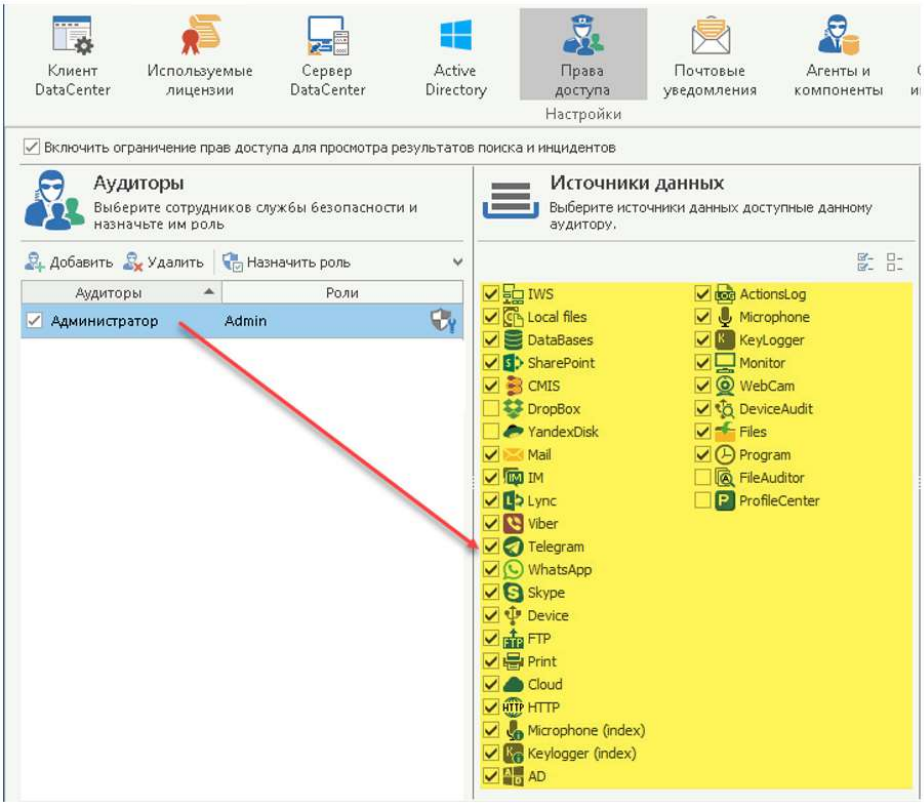


Рисунок 4.3

По умолчанию, каждому аудитору разрешен просмотр данных по всем пользователям. Настройте режим доступа для выбранного сотрудника службы безопасности:

- При установленном флажке **«Разрешено для всех»** аудитор имеет доступ к данным всех пользователей/компьютеров, кроме тех, что указаны в области **«Запрещено для выбранных»** (см. Рисунок 4.4).

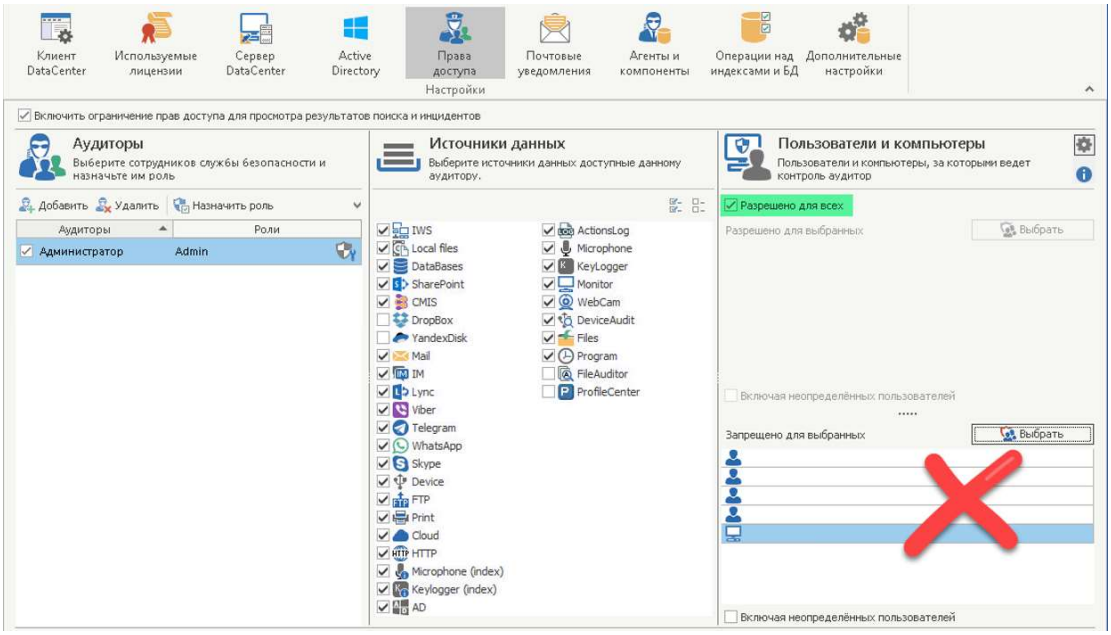


Рисунок 4.4

- При снятом флажке **«Разрешено для всех»** аудитор имеет доступ к данным только тех пользователей/компьютеров, которые будут выбраны из списка. Флажок «Включая неопределенных пользователей» предоставляет возможность просматривать документы пользователей, доменное имя которых системе не удалось определить и помечено как «unknown» (см. Рисунок 4.5).

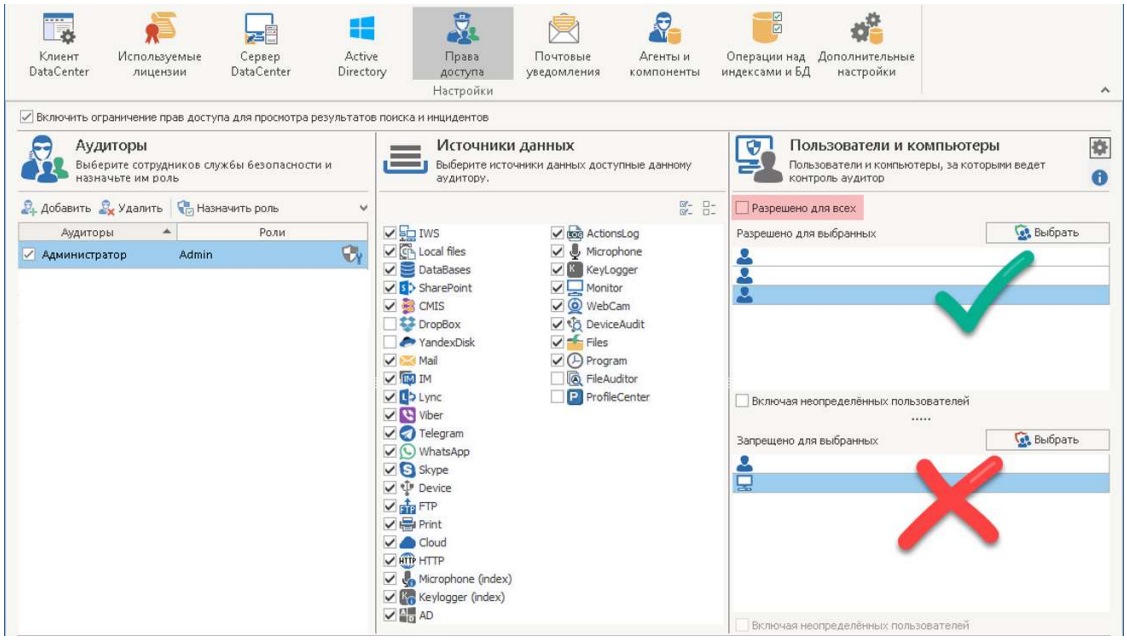


Рисунок 4.5

Для добавленных в список **имен компьютеров** ограничения будут применены только в отношении документов, проиндексированных на рабочих станциях пользователей, и отчетов по EndpointController, доступных в клиентской консоли AnalyticConsole (отчеты по установленному ПО, истории установки ПО, истории установки агентов на рабочие станции).

4.2.3 Разграничение прав с помощью модуля AlertCenter

Каждому пользователю, работающему с модулем AlertCenter, могут быть присвоены особые права, и он может быть допущен только к определенной информации.

Настройка общего списка пользователей производится на вкладке «Пользователи» клиентской консоли AlertCenter (см. Рисунок 4.6).

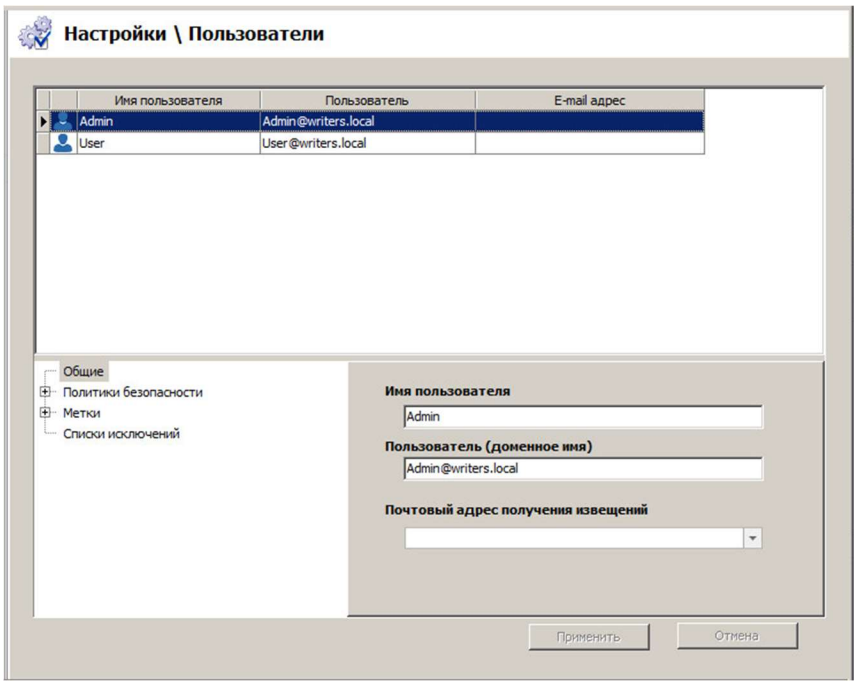


Рисунок 4.6

Для каждого пользователя можно задать четыре группы параметров:

- Общие;
- Политики безопасности;
- Метки;
- Списки исключений.

На вкладке «Общие» можно задать/изменить имя пользователя и почтовый адрес, на который будут приходить уведомления (см. Рисунок 4.7).

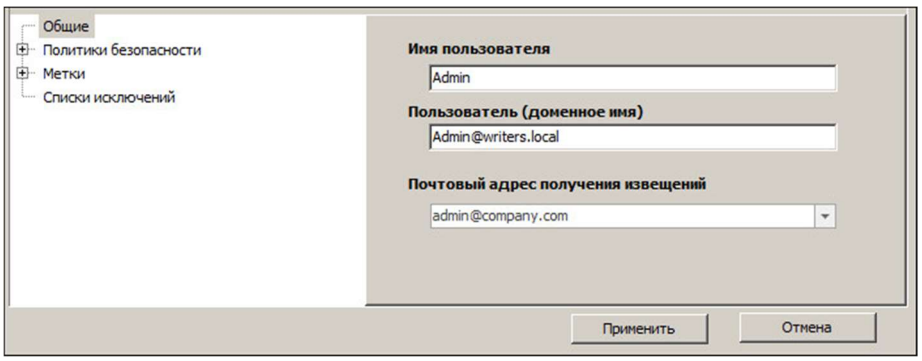


Рисунок 4.7

На вкладке «Политики безопасности» для каждой из политик индивидуально можно задать права доступа (см. Рисунок 4.8):

- Запрещено – пользователю недоступны как сама политика, так и результаты проверки по ней;
- Только просмотр – пользователь имеет доступ к политике без права ее изменения;

- Изменить – доступ с правом редактирования.

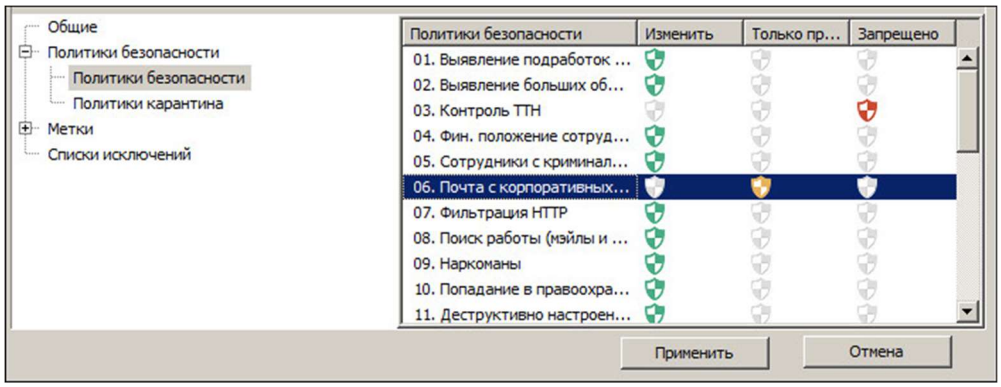


Рисунок 4.8

На вкладке «Метки» задаются права доступа к инцидентам с метками. Редактировать права доступа к меткам может только пользователь с установленным флагом «Администрирование разрешено».

На вкладке «Списки исключений» задаются права доступа к «белым» и «черным» спискам пользователей.

4.3 НАСТРОЙКА И ЭКСПЛУАТАЦИЯ АНАЛИТИЧЕСКОГО МОДУЛЯ ALERTCENTER[3]

4.3.1 Создание политик безопасности

Для добавления политики выделите узел «Политики безопасности», щелкните кнопку «Новая политика» и введите название политики (см. Рисунок 4.9).

[3] Помощь в создании политик безопасности, политик карантина, работы с цифровыми отпечатками и регулярными выражениями могут оказать инженеры ТП Компании.

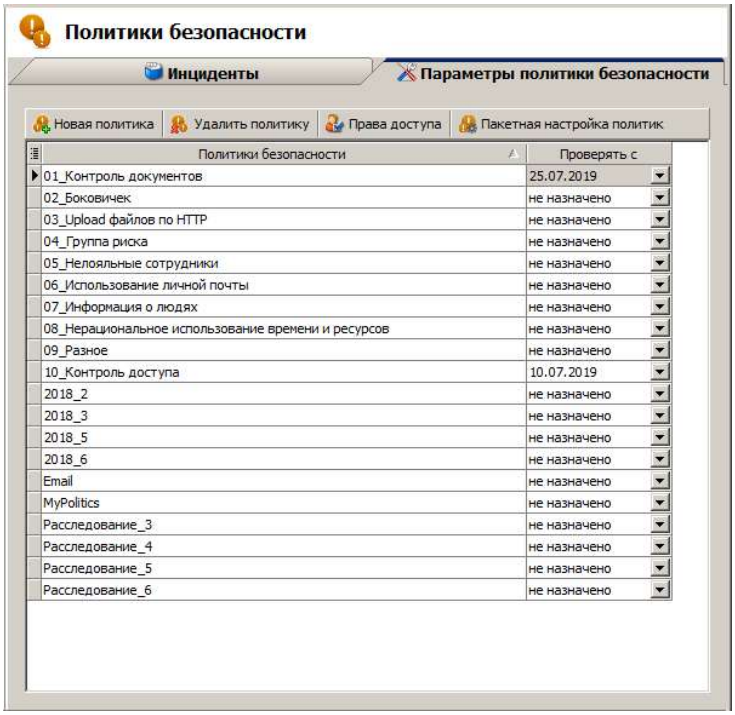


Рисунок 4.9

Для каждой политики можно задать правила доступа к ней пользователей используя кнопку «Права доступа» (см. Рисунок 4.10):

- *Запрещено* – пользователю недоступны как сама политика, так и результаты проверки по ней;
- *Только просмотр* – пользователь имеет доступ к политике, но без права ее изменения;
- *Изменить* – доступ с правом редактирования.

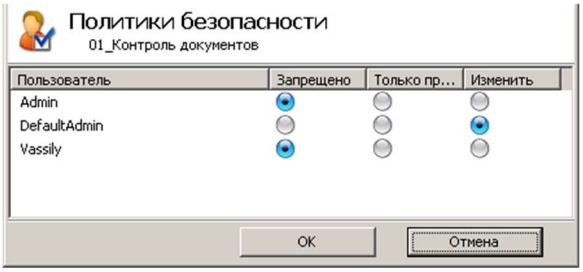


Рисунок 4.10

Созданную политику необходимо настроить: задать основные условия критерия поиска (поискового запроса) или нескольких критериев, а также задать дополнительные условия критерия поиска: индексы для анализа, расписание проверки, получатели уведомлений, списки исключений (см. Рисунок 4.11).

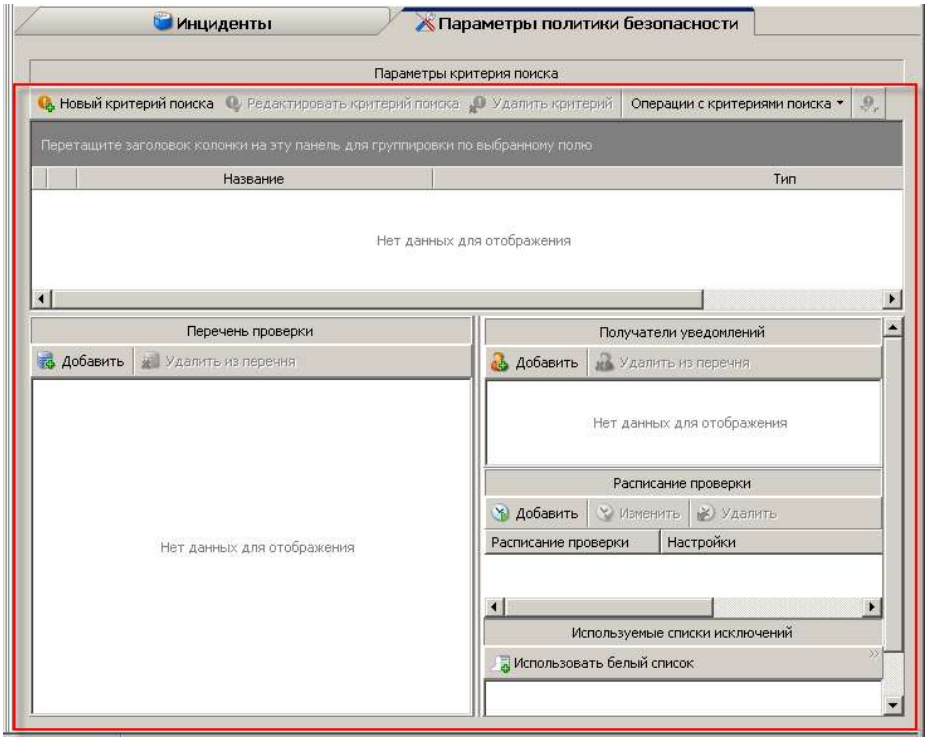


Рисунок 4.11

4.3.1.1 Настройка критериев поиска

Для нахождения документов, содержащих критичную информацию, задаются критерии поиска. Для добавления запроса щелкните кнопку «Новый критерий поиска» (см. Рисунок 4.12).

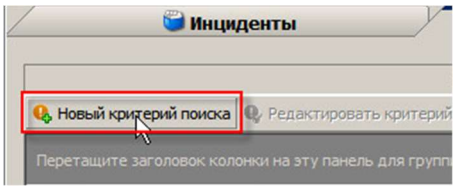


Рисунок 4.12

1. В верхней части окна введите название критерия поиска и (если необходимо) комментарий к нему.
2. Если требуется, ограничьте период времени для документов по данному критерию поиска, установив флажок «Искать в документах не старше N дней», где N – количество дней до текущей даты (см. Рисунок 4.13).

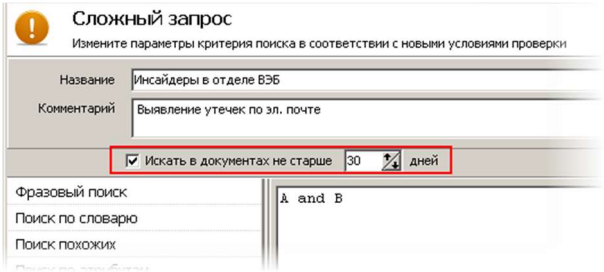


Рисунок 4.13

3. В левой части открывшегося окна выберите тип поиска:
   - сложный запрос – комбинирование нескольких простых запросов (предлагается первым по умолчанию),
   - фразовый поиск,
   - поиск по словарю,
   - поиск похожих,
   - поиск по атрибутам (имеются общие атрибуты и специальные – в зависимости от способа перехвата данных),
   - поиск нераспознанных,
   - поиск по регулярным,
   - поиск по цифровым отпечаткам,
   - поиск по базам данных,
   - статистические запросы;
   - запросы Active Directory.
4. После этого задайте другие параметры критерия поиска (в зависимости от выбранного типа). Например, для фразового поиска требуется ввести слово или несколько слов поискового запроса и обозначить целый ряд других параметров поиска (см. Рисунок 4.14).

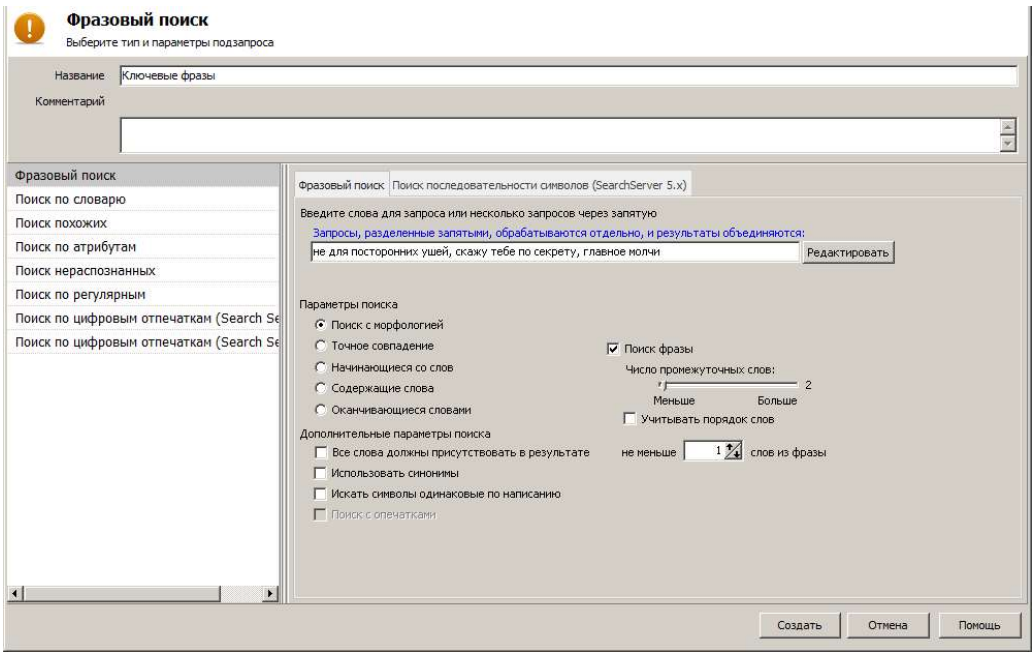


Рисунок 4.14

При необходимости произвести поиск по целому ряду условий применяется комбинирование нескольких простых запросов в одном: создайте «Сложный запрос», после чего добавьте подзапрос сложного критерия (см. Рисунок 4.15).

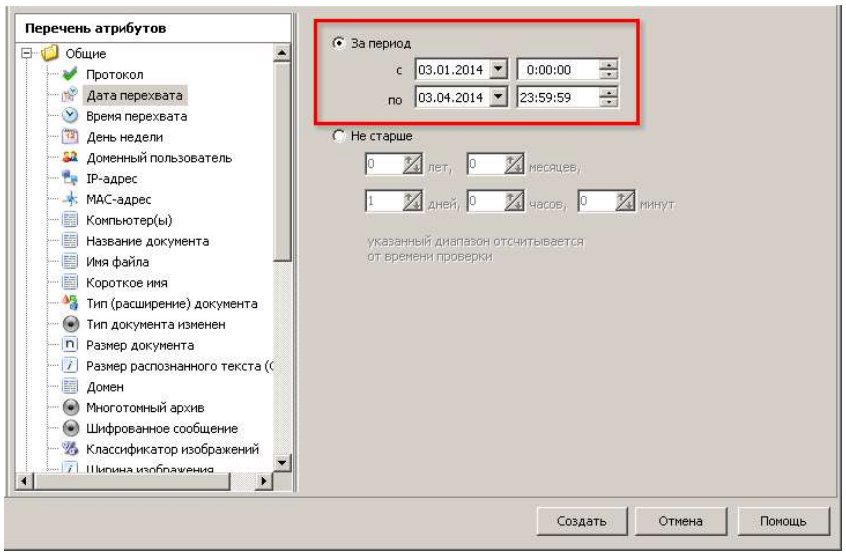


Рисунок 4.15

5. Задайте формулу объединения запросов (в примере – A and B). После задания всех необходимых параметров в основном запросе щелкните кнопку «Создать» (см. Рисунок 4.16).

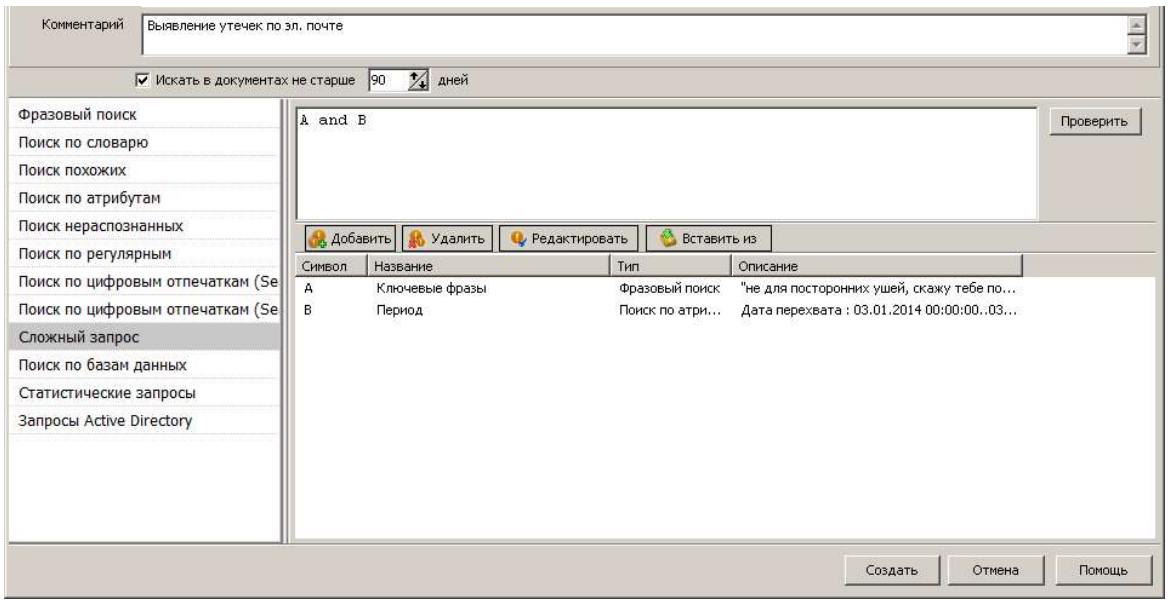


Рисунок 4.16

Добавленный запрос будет отображен в клиенте.

6. После задания основных условий критерия поиска для политики информационной безопасности задайте *дополнительные* условия:
   - перечень проверки;
   - расписание проверок;
   - список получателей уведомлений;
   - списки исключений пользователей.

4.3.1.2 Настройка перечня проверки

Для добавления перечня индексов (баз данных), по которым будет производиться проверка, щелкните кнопку «Добавить» (см. Рисунок 4.17).

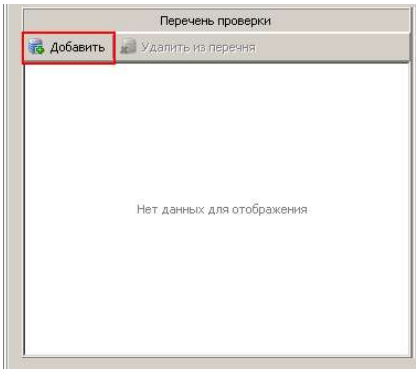


Рисунок 4.17

В появившемся диалоговом окне флажками выберите один или более индексов/баз данных (см. Рисунок 4.18).

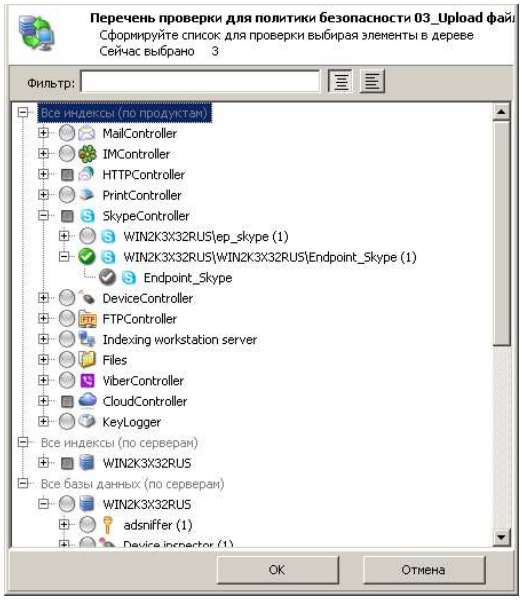


Рисунок 4.18

Щелкните «ОК», выбранные индексы будут добавлены в перечень проверки.

Для удаления индекса из политики выделите его и воспользуйтесь кнопкой «Удалить из перечня».

4.3.1.3 Настройка расписания проверок

Расписание проверок определяет, с какой частотой происходит проверка индексов перехваченных документов. Настройка производится в разделе «Дополнительные настройки» для выбранной политики безопасности (см. Рисунок 4.19).

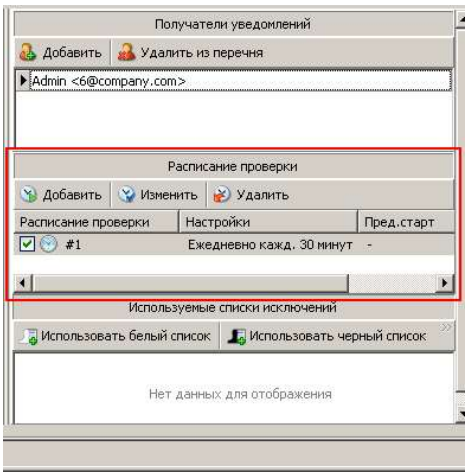


Рисунок 4.19

Для настройки расписания, воспользуйтесь кнопкой «Добавить» в разделе «Дополнительные настройки». Следуйте шагам мастера настройки расписания для задания требующегося расписания проверок (см. Рисунок 4.20).

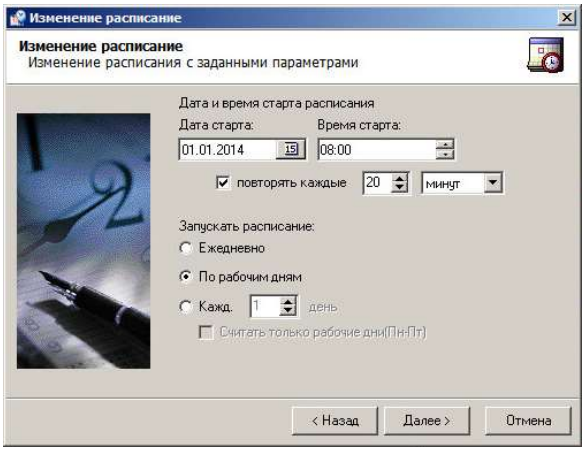


Рисунок 4.20

4.3.1.4 Настройка получателей уведомлений

В группу получателей уведомлений можно добавить только предварительно зарегистрированных пользователей.

Настройка списка производится в группе «Получатели уведомлений» дополнительных настроек политики безопасности (см. Рисунок 4.21).

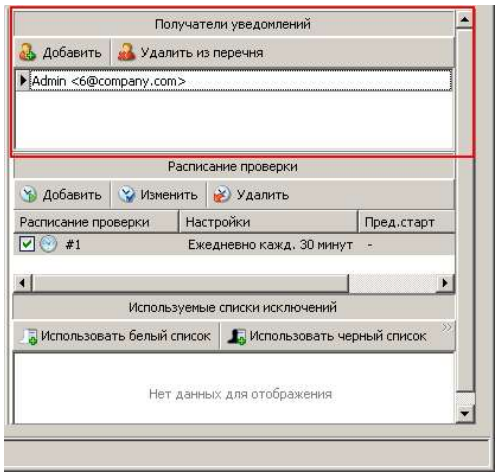


Рисунок 4.21

Щелкните кнопку «Добавить» и выберите зарегистрированного пользователя (см. Рисунок 4.22).

Рисунок 4.22

Пользователь будет добавлен в список получателей.

4.3.1.5 Настройка списков исключений пользователей

В зависимости от типа списка по документам пользователей либо не будут фиксироваться инциденты и отправляться уведомления («белый список»), либо напротив только по документам заданных пользователей будут фиксироваться инциденты и отправляться уведомления («черный список»).

Настройка списков производится в группе «Используемые списки исключений» дополнительных настроек политики безопасности (см. Рисунок 4.23).

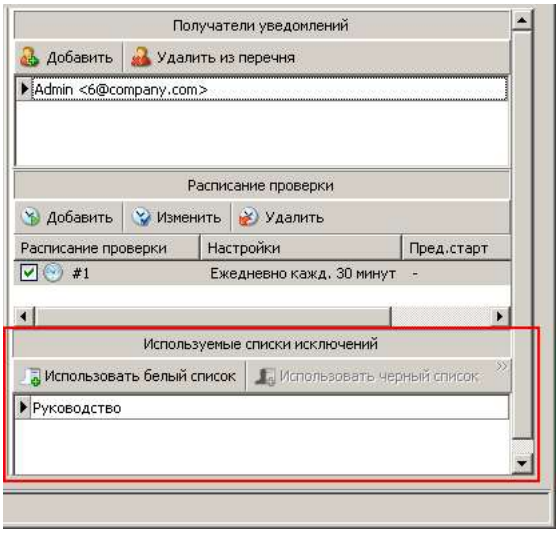


Рисунок 4.23

В список исключений можно добавить только включенных в общий список исключений пользователей.

Щелкните кнопку «Использовать белый список» или «Использовать черный список» и выберите требуемые группы пользователей из общего списка (см. Рисунок 4.24).

Примечание. *Для каждой политики можно выбрать один из типов – либо «белый список», либо «черный список». Например, если уже выбран «белый», то к нему можно добавить другие «белые», а вот «черные» добавить уже не получится.*

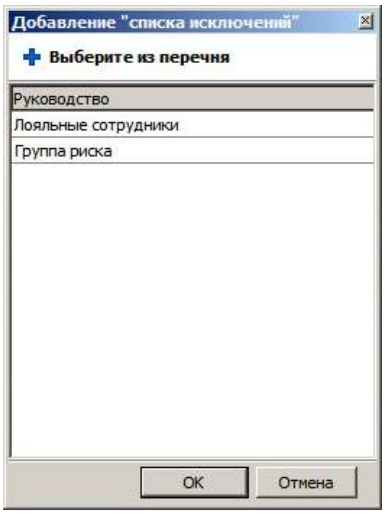


Рисунок 4.24

Для удаления списка выделите его и щелкните кнопку «Удалить из перечня».

По завершении всех настроек процедуру проверки политики безопасности можно запустить вручную из контекстного меню (см. Рисунок 4.25).

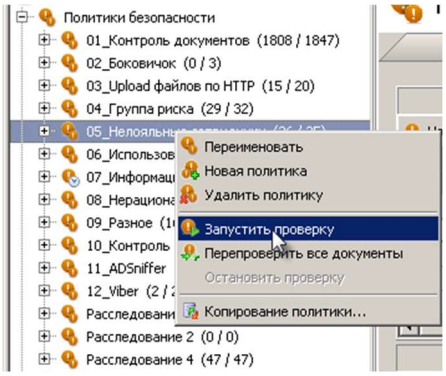


Рисунок 4.25

Для того, чтобы задать/перенастроить/отключить параметры («расписание проверки», «получатели уведомлений» и «используемые списки уведомлений») для всех политик и критериев поиска выделите узел «Политики безопасности» и нажмите кнопку «Пакетная настройка политик». В открывшемся окне можно перенастроить расписание проверок политик, отредактировать получателей уведомлений, списки исключений.

После создания политик безопасности, при необходимости, осуществляется настройка политик карантина.

4.3.2 Создание политик карантина

Политики карантина позволяют задать правила для блокирования исходящих сообщений электронной почты, передаваемых по протоколу SMTP (а также MAPI/IMAP при использовании плагина Outlook – подробнее см. в справке по продукту EndpointController). Блокированные сообщения помещаются в карантин, откуда они могут быть разблокированы и переданы по адресу назначения (в случае ложной сработки по заданной политике) либо окончательно заблокированы.

Настройка политик карантина производится при помощи клиентской части AlertCenter и аналогична настройке политик безопасности.

Для добавления политики выделите узел «Карантин» в левой части окна клиента. Щелкните кнопку «Новая политика» и введите имя политики (см. Рисунок 4.26).

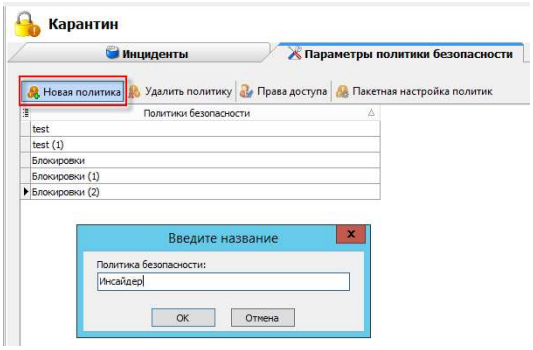


Рисунок 4.26

Выделите созданную группу. В группе нужно настроить следующие позиции (см. Рисунок 4.27):

- список критериев поиска;
- перечень проверки (список индексов для анализа);
- расписание проверки;
- список получателей уведомлений;
- списки исключений.

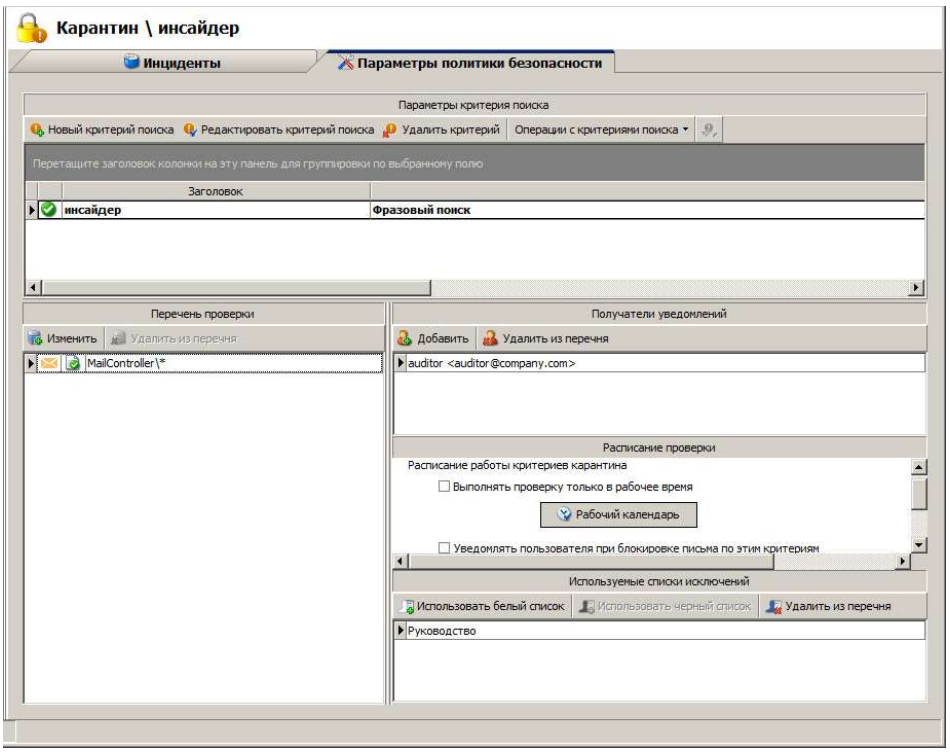


Рисунок 4.27

К числу общих настроек для карантина относятся расписание работы критериев карантина (см. Рисунок 4.28). Установите флаг для выполнения проверок только в рабочее время и настройте рабочий календарь.

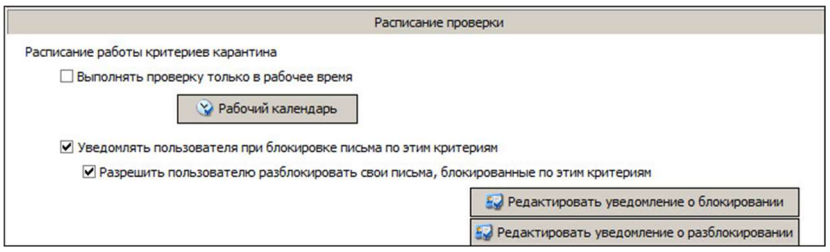


Рисунок 4.28

Сконфигурируйте график работы согласно регламенту:

- Укажите тип выбранного дня недели: рабочий либо выходной.
- Настройте начало и окончание рабочего дня в выбранный день недели.
- Настройте список перерывов в течение выбранного рабочего дня.

Также настройте:

- параметр «Уведомлять пользователя при блокировке письма по этим критериям» позволяет отправлять уведомление пользователю, письмо которого было заблокировано. Такому пользователю придет информационное письмо, содержащее сообщение о блокировке и идентификационный номер. Если письмо будет одобрено офицером

безопасности, то пользователю придет еще одно уведомление о снятии блокировки и успешной отправке его письма.

- параметр «Разрешить пользователю разблокировать свои письма, блокированные по этим критериям» позволяет пользователям, чьи письма попали в карантин, разблокировать их отправку.

При необходимости отредактируйте шаблоны уведомлений при помощи соответствующих кнопок.

Остальные дополнительные настройки политик карантина аналогичны дополнительным настройкам политик безопасности. Смотрите пункты: «Настройка критериев поиска» (п. 4.3.1.1), «Настройка перечня проверки» (п. 4.3.1.2), «Настройка списка получателей уведомлений» (п. 4.3.1.4), «Настройка списка исключений пользователей» (п. 4.3.1.5).

4.3.2.1 Настройка почты с остановкой. Модуль EndpointController

Сервер EndpointController позволяет включать/выключать режим остановки исходящих сообщений электронной почты, передаваемых по протоколу SMTP (а также MAPI/IMAP при использовании плагина Outlook). Блокированные сообщения помещаются в карантин, откуда они могут быть разблокированы и отправлены по адресу назначения.

Для настройки остановки сообщений электронной почты используются интерфейсы как клиентского модуля AlertCenter, так и консоли EndpointController. Остановка исходящих сообщений электронной почты должна быть первоначально проверена на компьютерах тестовой группы.

Перед включением режима остановки исходящих почтовых сообщений необходимо настроить политики карантина AlertCenter.

Включение режима остановки исходящих почтовых сообщений производится в консоли администрирования серверного модуля EndpointController. Последовательность действий (см. Рисунок 4.29):

1. Убедитесь, что политики карантина в AlertCenter настроены.
2. На вкладке «Агенты» консоли двойным щелчком по позиции SMTP вызовите диалог «Редактирование 'SMTP' агента» (варианты: нажмите кнопку 

или кнопку «Дополнительно» в нижней части окна).

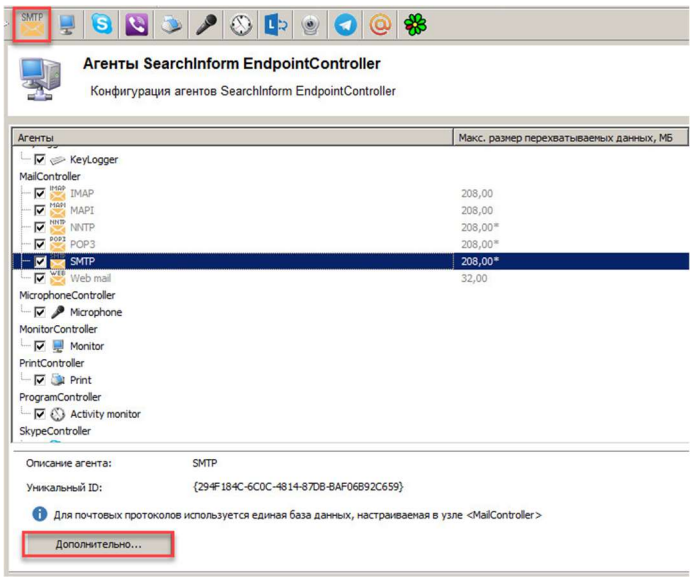


Рисунок 4.29

3. Установите флажок «Блокировать SMTP».
4. Нажмите ОК (см. Рисунок 4.30).

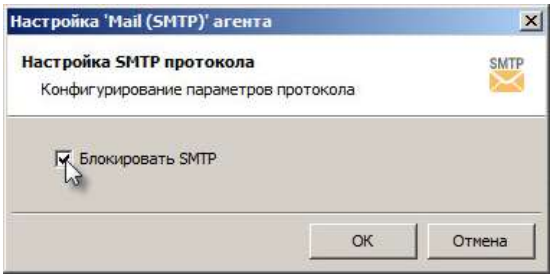


Рисунок 4.30

Для включения блокировки почтового трафика протоколов MAPI и IMAP включите также плагин интеграции Outlook («Настройки агентов» → «Почтовый перехват», см. Рисунок 4.31).

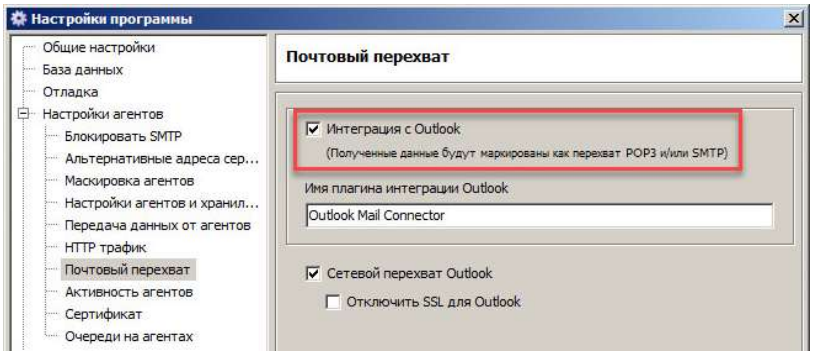


Рисунок 4.31

5. Удостоверьтесь, что остановка исходящей почты работает корректно.

Режим остановки исходящих сообщений электронной почты будет включен.

4.3.3 Настройка списков исключений пользователей

Настройка списков исключений производится при помощи клиентского модуля AlertCenter.

В список исключений должны быть добавлены группы пользователей, которые в зависимости от типа списка будут либо исключены из зоны применения политик безопасности («белый список» – пользователи, по документам которых не будут фиксироваться инциденты и отправляться уведомления) либо напротив включены в них («черный список» – только по документам заданных пользователей будут фиксироваться инциденты и отправляться уведомления).

Перейдите на вкладку «Списки исключений» узла «Настройки». Для добавления списка щелкните кнопку «Создать новый список» и введите имя списка (см. Рисунок 4.32).

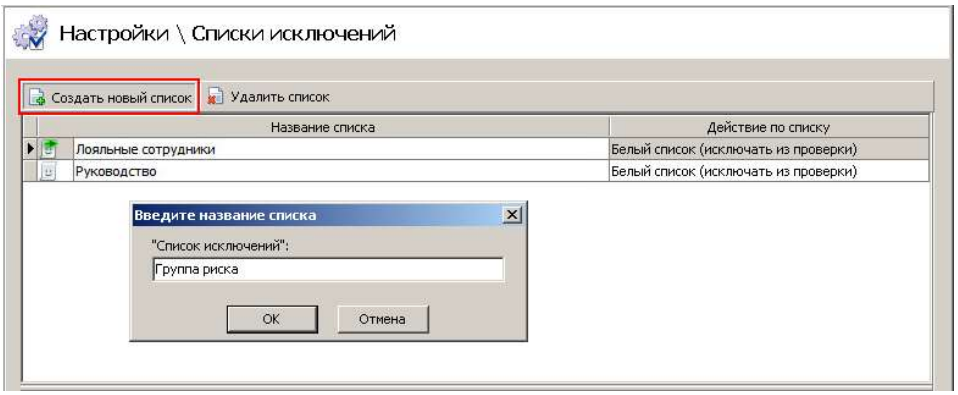


Рисунок 4.32

Имя списка будет добавлено в базу данных. Далее в столбце «Действие по списку» выбираем тип списка – «белый» либо «черный» (см. Рисунок 4.33).

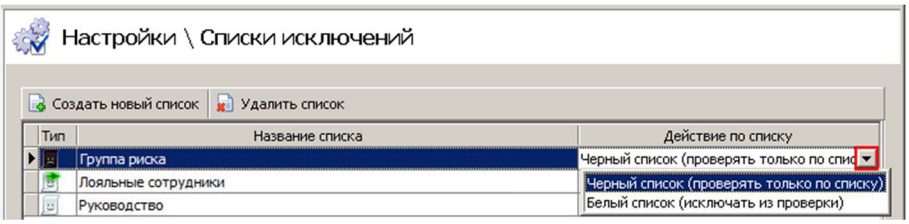


Рисунок 4.33

После добавления списка необходимо ввести параметры исключения пользователей из проверки. Исключение пользователей производится по любому из четырех атрибутов: пользователю домена, IP-адресу, MAC-адресу и адресу электронной почты (см. Рисунок 4.34).

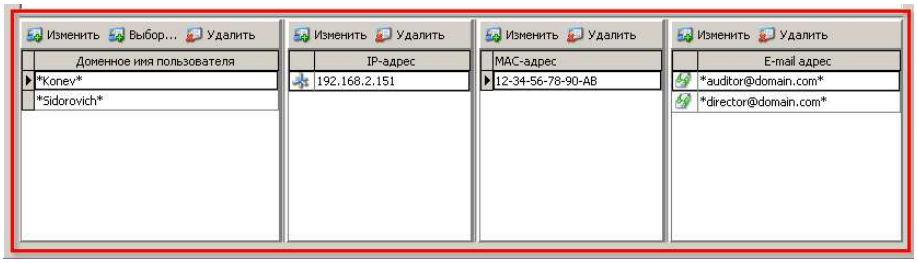


Рисунок 4.34

4.3.4 Настройка словаря синонимов

Словарь синонимов удобно использовать для мониторинга неформального общения сотрудников.

Синонимы позволяют задавать максимально широкую область поиска.

Пример поставленной задачи – поиск прямых или закамуфлированных требований взятки, условно «хочу взятку». Для решения задачи, может быть создано два синонимических ряда. Для «хочу» – дай, нужна, требуется, потребуется…. Для «взятка» - бакшиш, бонус, гонорар…. Синонимы позволят по запросу «хочу взятку» найти все возможные сочетания слов, например, «нужен бакшиш». Т.е., если ряд 1 включает в себя 3 слова, а ряд 2 – 5 синонимов, то поисковая система проверит все возможные 15 (3х5) вариантов сочетаний слов.

Управление синонимами производится на вкладке «Словарь синонимов» узла «Настройки».

Для добавления синонимического ряда используется кнопка «Новая группа» (см. Рисунок 4.35).

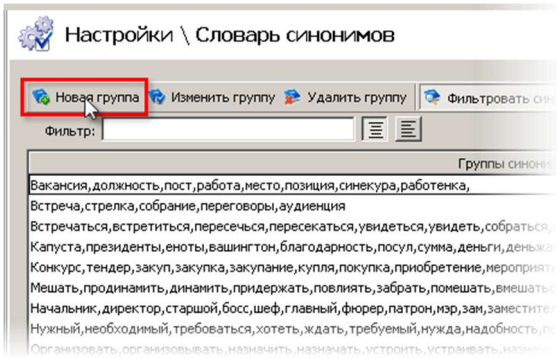


Рисунок 4.35

Ввод синонимов осуществляется через запятую, пробел или с новой строки (см. Рисунок 4.36).

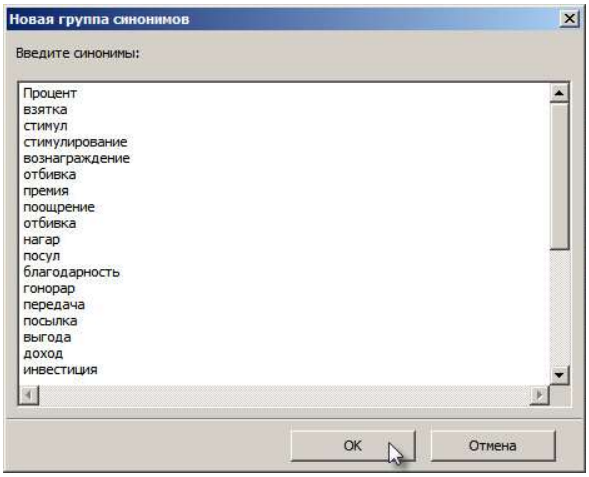


Рисунок 4.36

По нажатии «ОК» синонимический ряд будет добавлен в словарь (см. Рисунок 4.37).

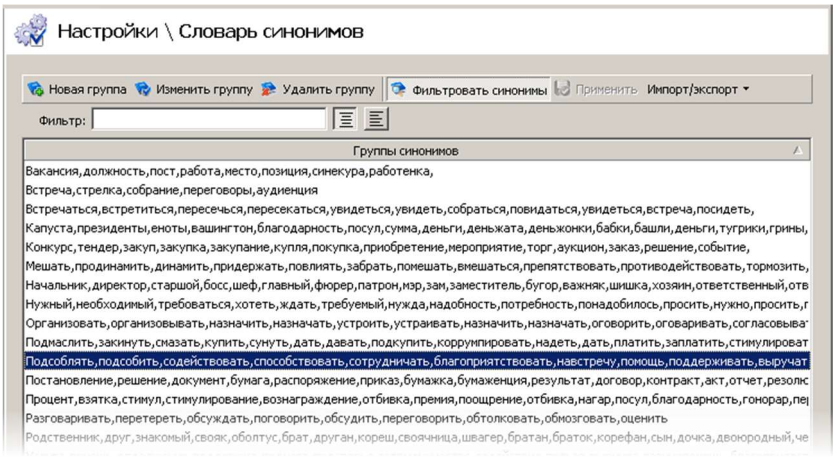


Рисунок 4.37

4.3.5 Настройка библиотеки регулярных выражений

Настройка библиотеки регулярных выражений производится на вкладке «Библиотека регулярных выражений» узла «Настройки».

Проверьте наличие необходимого регулярного выражения среди предустановленных шаблонов (группа «Стандартные выражения»). Предустановленные регулярные шаблоны поставляются с дистрибутивом, в их число входят наиболее популярные: *Фамилия И.О., IP-адрес, номер телефона, номер банковской карточки* и т.п. (см. Рисунок 4.38).

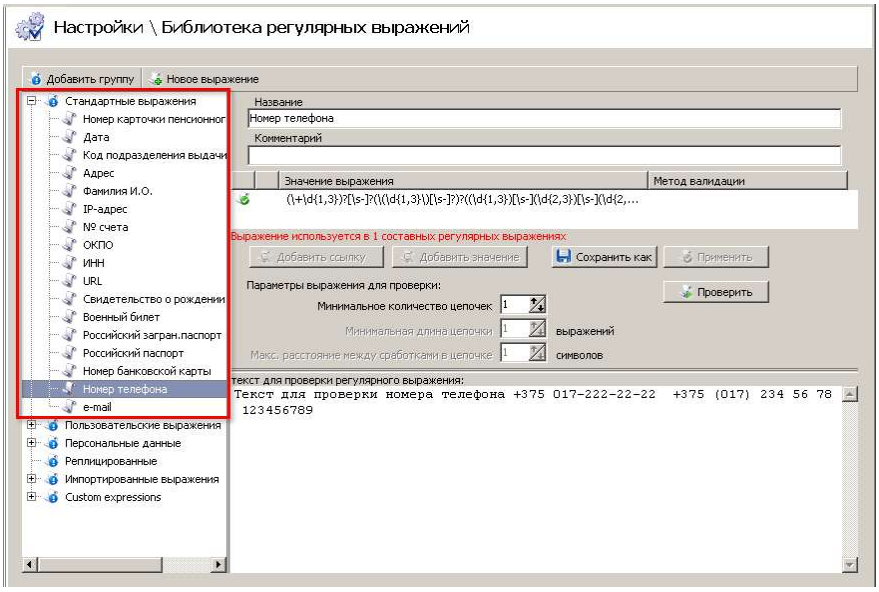


Рисунок 4.38

При отсутствии регулярного выражения среди предустановленных шаблонов создайте собственный (пользовательский) шаблон регулярного выражения:

1. Определите группу, в которую будет входить шаблон. При отсутствии подходящей группы создайте новую: щелкните кнопку «Добавить группу» и введите имя группы.
2. Щелкните кнопку «Новое выражение», введите имя регулярного выражения (см. Рисунок 4.39).

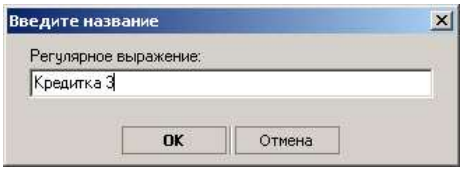


Рисунок 4.39

3. Введите значение регулярного выражения в редактируемом поле колонки «Значение выражения» (см. Рисунок 4.40).

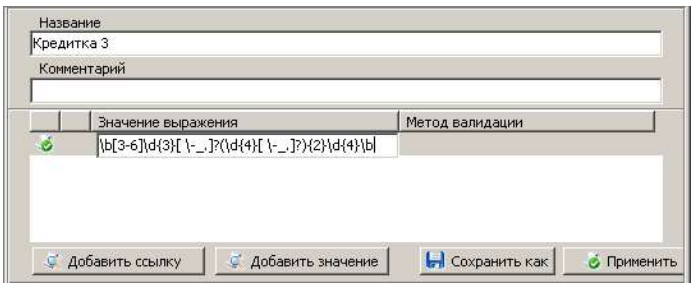


Рисунок 4.40

4. Выберите необходимый метод валидации. Методы валидации встроены в программу и не могут редактироваться (см. Рисунок 4.41).

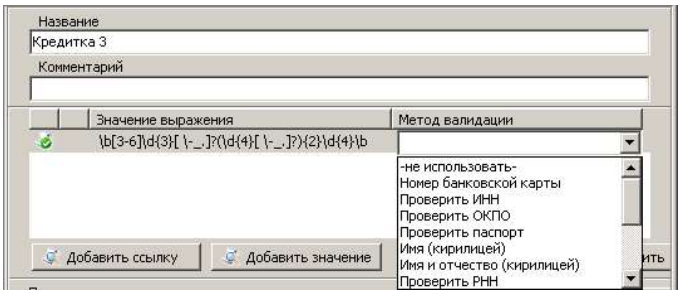


Рисунок 4.41

5. Для сохранения созданного шаблона регулярного выражения щелкните «Применить».
6. Для проверки правильности составленного регулярного выражения введите текст, по которому будет проверяться выражение, в поле, расположенное в нижней части клиента AlertCenter, и щелкните кнопку «Проверить». Справа появится всплывающее окно с информацией о времени проверки и количестве цепочек в проверочном выражении. При срабатывании регулярного выражения на тестовом фрагменте, текст будет подсвечен (см. Рисунок 4.42).

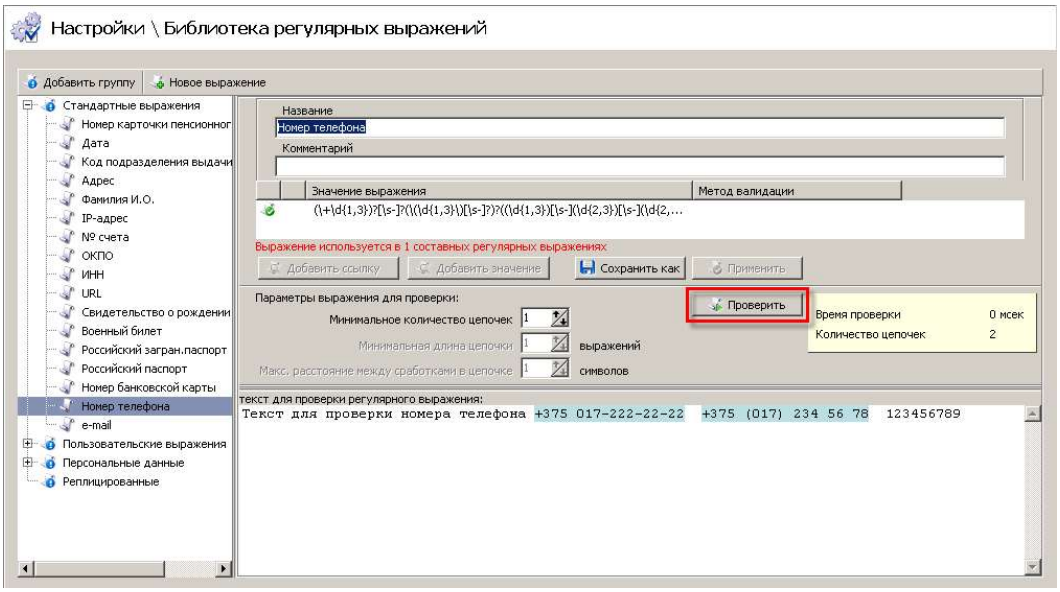


Рисунок 4.42

Несколько шаблонов регулярного выражения могут быть скомбинированы в одно составное регулярное выражение, или цепочку. **Пример:** *найти документы, содержащие значения «ФИО», «дата рождения», «номер счета», «номер карточки».*

Использование составного выражения может быть удобным при составлении различных списков, например, списка заказчиков, когда требуется объединить в одно целое несколько регулярных выражений.

Для создания составного регулярного выражения к простому шаблону регулярного выражения добавляются ссылки на имеющийся шаблон либо дополнительные значения (см. Рисунок 4.43):

- Щелкните «Добавить ссылку» и выберите регулярное выражение из предложенного списка. В данном случае изменения оригинального шаблона будут унаследованы в составном регулярном выражении.
- Щелкните «Добавить значение» и выберите регулярное выражение из предложенного списка. В данном случае изменения оригинального шаблона не отразятся на конечном регулярном выражении.

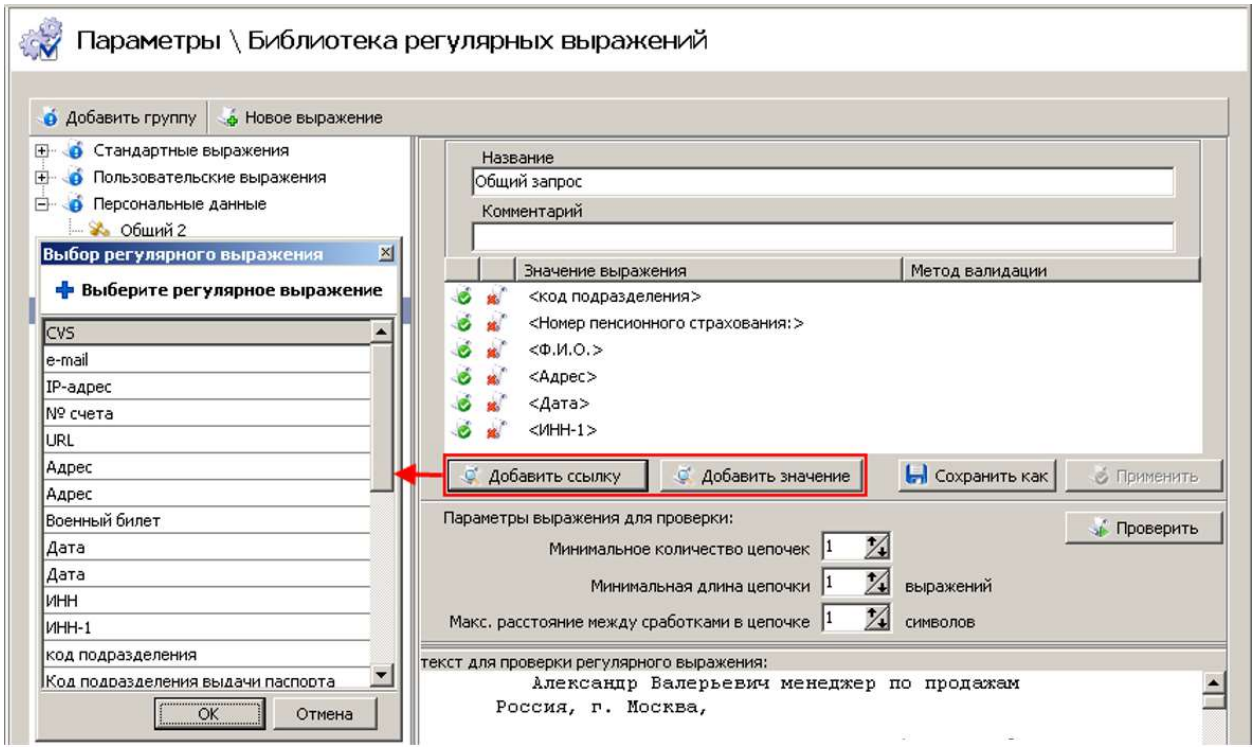


Рисунок 4.43

При проверке правильности шаблона составного регулярного выражения к числу настраиваемых параметров помимо минимального количества цепочек добавляются также следующие:

- минимальная длина цепочки,
- максимальное расстояние между сработками в цепочке.

Шаблоны регулярных выражений обозначаются в списке шаблонов значком  , составные регулярные выражения – значком  .

4.3.6 Настройки просмотра

На вкладке «Настройки просмотра» задаются параметры просмотра инцидентов: цвет подсветки найденных слов запроса, шрифт, цвет и размер текста документов,

формат вывода документа и др. Заданные настройки применяются при просмотре инцидентов в окне предварительного просмотра.

В блоке «Подсветка» настройте следующие параметры шрифта и фона:

- цвет текста;
- название и размер шрифта;
- стиль форматирования текста: жирный/курсив/подчеркнутый;
- цвет фона и подсветки, с помощью которых выделяются слова поискового запроса в найденном документе (см. Рисунок 4.44).

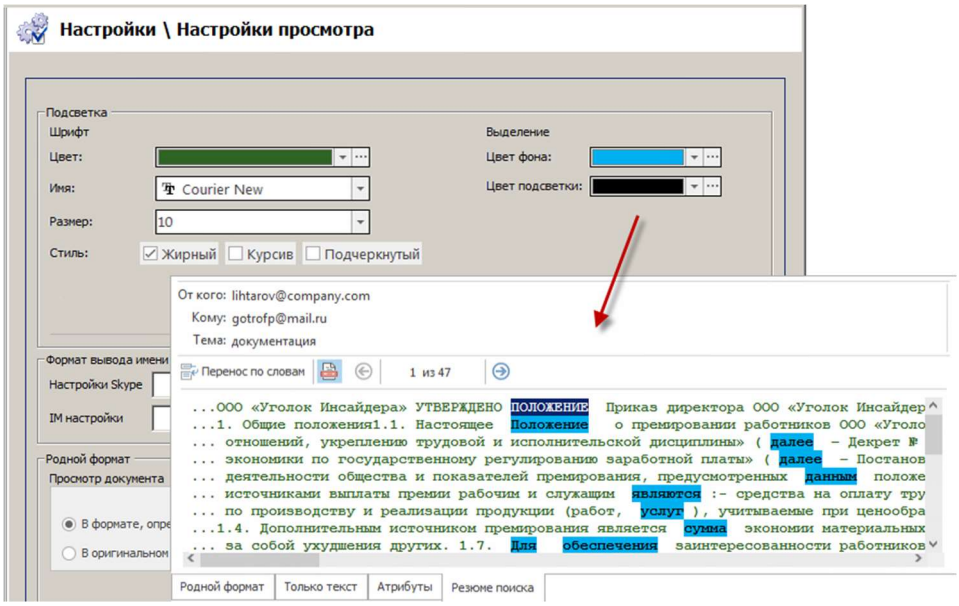


Рисунок 4.44

В блоке «Формат вывода имени» задается формат отображения имени отправителей/получателей сообщений, переданных посредством Skype или IM-клиентов. Выберите из выпадающего списка требуемый формат имени пользователей, который будет отображаться при просмотре журнала инцидентов (см. Рисунок 4.45).

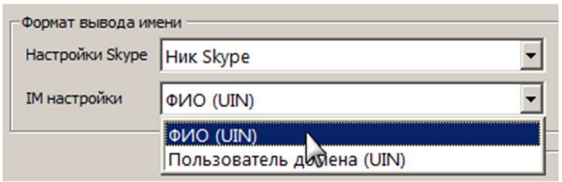


Рисунок 4.45

В блоке «Родной формат» указывается формат отображения документов ***при просмотре только в режиме «Родной формат».*** Доступные варианты просмотра:

- в формате, определенном сервером индексации;

- в оригинальном формате документа.

Для **html-файлов** можно задать число растровых потоков, а также активировать опции, обеспечивающие увеличение скорости загрузки файлов при просмотре:

- асинхронная обработка графики;
- ускоренная прокрутка (см. Рисунок 4.46).

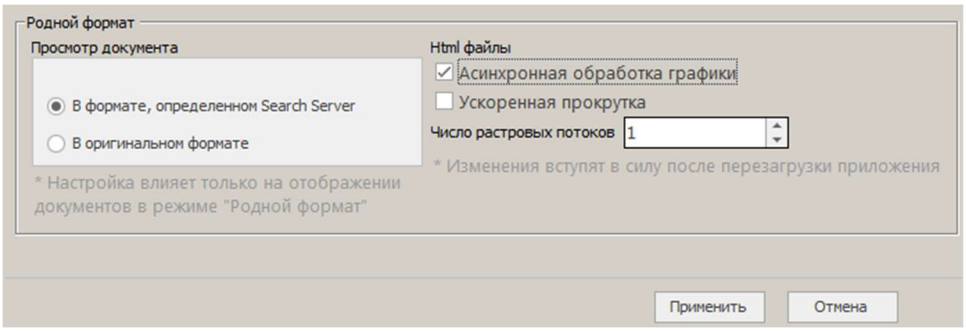


Рисунок 4.46

Изменения настроенных параметров вступят в силу после перезагрузки приложения!

4.3.7 Работа с журналом инцидентов

Журнал инцидентов включает в себя документы, по которым сработали поисковые запросы текущей базы AlertCenter.

Для просмотра журнала инцидентов выделите узел «Политики безопасности» и перейдите на вкладку «Инциденты».

Журнал инцидентов группируется по политикам и критериям поиска (поисковым запросам). Выберите требуемый список инцидентов по политике безопасности или конкретному критерию поиска.

Документы, по которым сработали критерии поиска, отображаются в виде списка в правой верхней части окна (см. Рисунок 4.47).

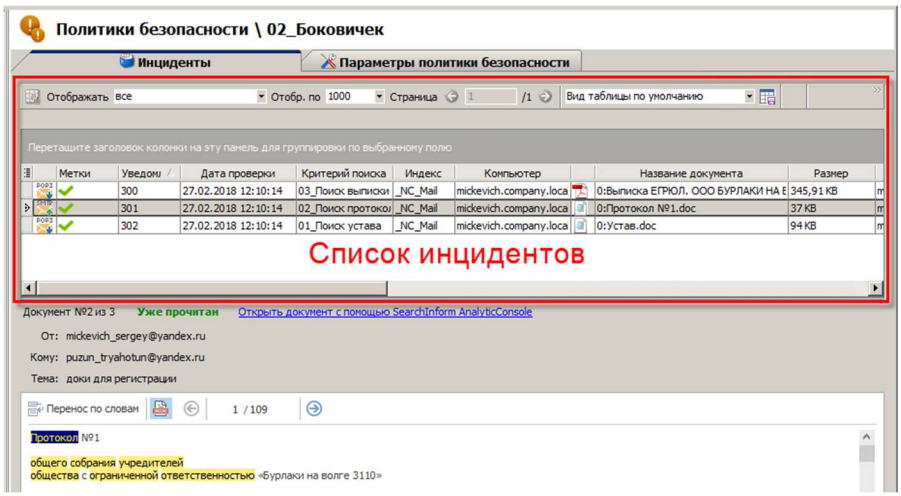


Рисунок 4.47

С помощью кнопок, расположенных на панели инструментов, можно производить операции по фильтрации документов, задавать ограничения по количеству отображаемых в списке документов, отображать только непрочитанные сообщения.

Если в результате проверок произошло множество срабатываний, журнал инцидентов будет содержать огромное число записей. Поэтому список инцидентов можно фильтровать.

Для вызова окна настройки фильтра используется кнопка «Установить параметры фильтра» (см. Рисунок 4.48).

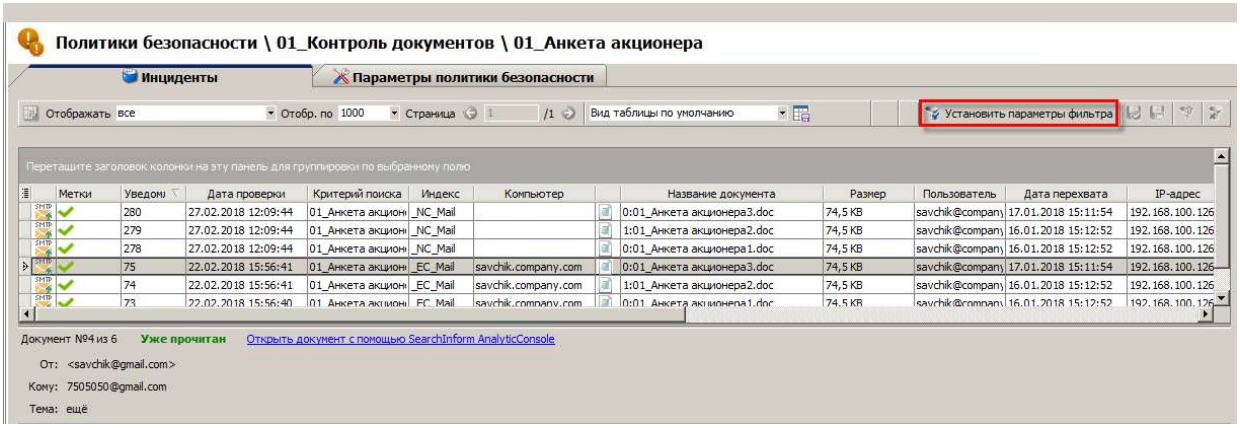


Рисунок 4.48

Записи можно фильтровать:

- по дате и времени фиксации инцидента;
- по дате и времени перехвата;
- по атрибутам.

Настроенные фильтры можно сохранять под заданным именем, загружать и удалять. Для этого используются соответствующие кнопки-значки со всплывающими подсказками. Последний сохраненный фильтр отображается в виде строки под панелью

инструментов фильтров. Для включения/отключения данного фильтра установите/ снимите флажок в начале строки фильтра (см. Рисунок 4.49).

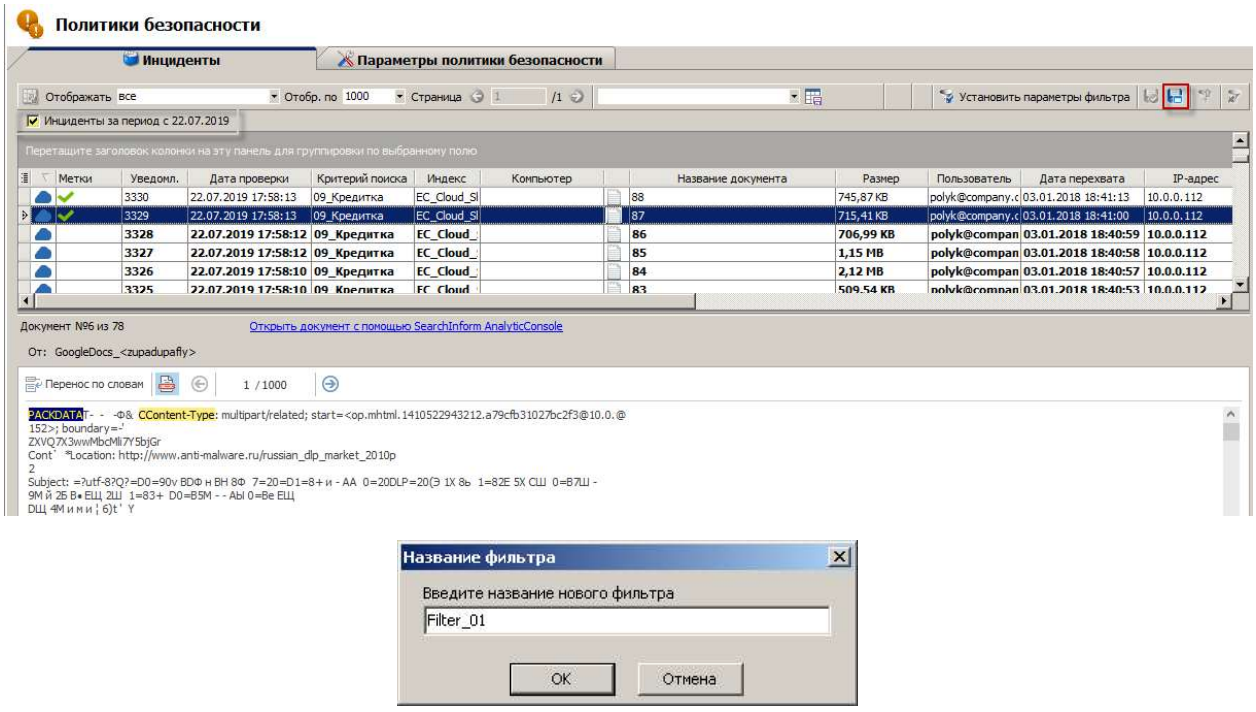


Рисунок 4.49

Сохраненные фильтры можно загрузить при помощи кнопки  и удалить при помощи кнопки  (см. Рисунок 4.50).

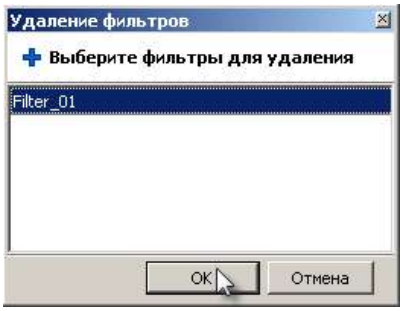


Рисунок 4.50

Для изменения количества отображаемых на странице документов воспользуйтесь выпадающим списком «Отобр. по». Для выбора режима отображения сообщений воспользуйтесь выпадающим списком «отображать». Для отображения в списке только непрочитанных сообщений установите флажок «Только непрочитанные» (см. Рисунок 4.51).

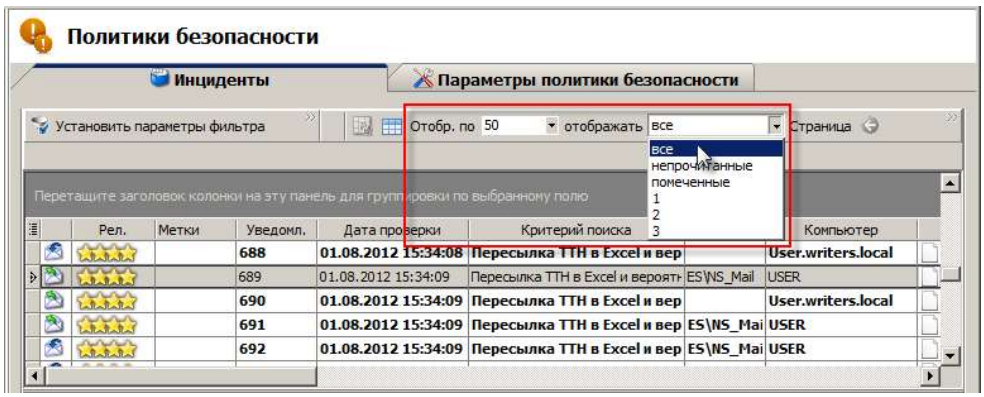


Рисунок 4.51

Если при передаче документа использовалась защита шифрованием и/или цифровой подписью, то при просмотре в режиме «Родной формат» письмо маркируется иконками:

- документ защищен электронной цифровой подписью;

- документ зашифрован (см. Рисунок 4.52).

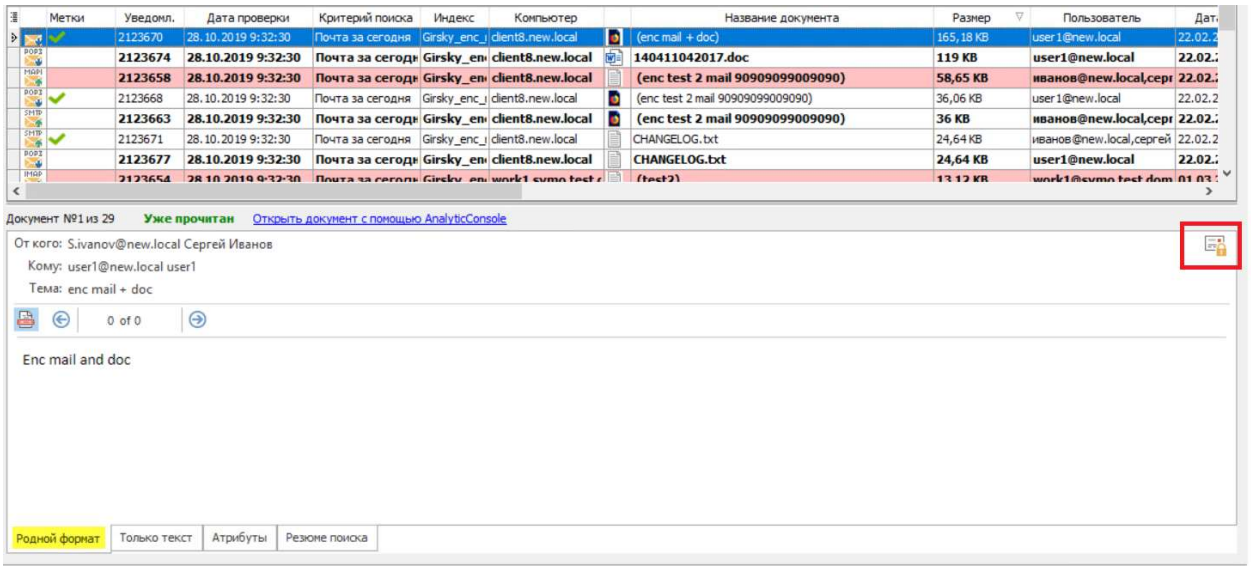


Рисунок 4.52

4.3.8 Просмотр карантина

Для просмотра результата, выделите узел «Карантин» в левой части окна клиента. В правой части окна отобразится перечень всех перемещенных в карантин сообщений (см. Рисунок 4.53).

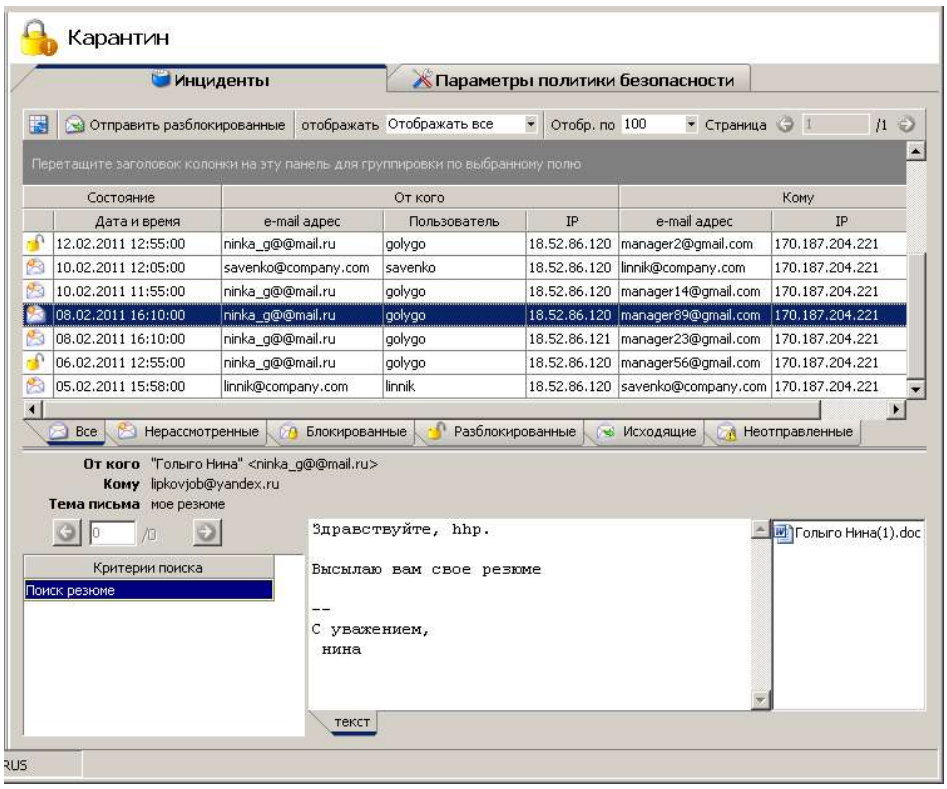


Рисунок 4.53

В панели со списком помещенных в карантин сообщений отображаются следующие данные:

- категория сообщения (обозначается пиктограммой, см. ниже);
- дата и время отправки письма;
- эл. адрес отправителя сообщения;
- учетная запись отправителя;
- IP-адрес отправителя;
- эл. адрес получателя сообщения;
- IP-адрес получателя;
- номер порта, через который отправлялось сообщение.

Имеется возможность фильтрации помещенных в карантин сообщений по хронологическому критерию (см. Рисунок 4.54):

- за указанный период времени;
- за весь период;
- за сегодня;
- за эту неделю;
- за этот месяц;
- за этот год.

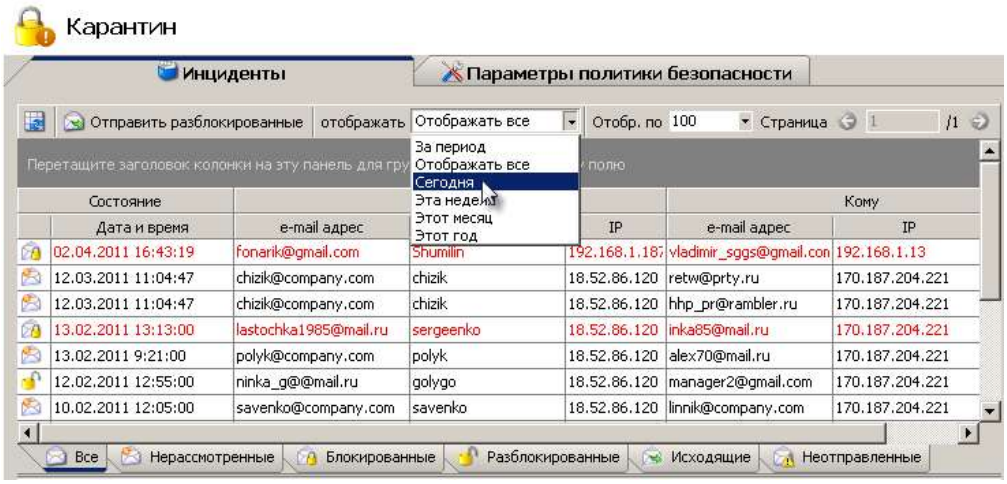


Рисунок 4.54

Отображаемая в первой колонке списка пиктограмма указывает на отнесенность сообщения к одной из пяти категорий:

– нерассмотренные (отображаются черным шрифтом);

– блокированные (отображаются красным шрифтом);

– разблокированные (отображаются жирным зеленым шрифтом);

– исходящие (отображаются обычным зеленым шрифтом);

– отправленные (отображаются черным шрифтом).

Сгруппированные по вышеуказанным категориям сообщения можно просмотреть с помощью расположенных в нижней части панели вкладок.

Под панелью с перечнем помещенных в карантин сообщений располагается панель просмотра сообщения (наряду с вложенными в него файлами). Сообщение отображается при его выделении в списке верхней панели (см. Рисунок 4.55).

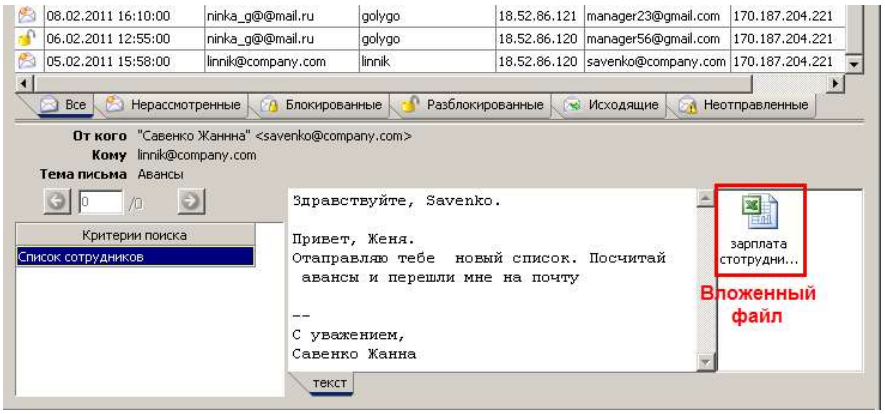


Рисунок 4.55

По находящимся в карантине сообщениям может быть принято решение: либо блокировать выбранное сообщение, либо разблокировать, либо отправить разблокированное сообщение на указанный адрес.

Для блокировки-разблокировки выбранных сообщений служат соответствующие команды контекстного меню либо комбинации клавиш (см. Рисунок 4.56):

- **Ctrl+B** – блокировать сообщение;
- **Ctrl+U** – разблокировать сообщение.

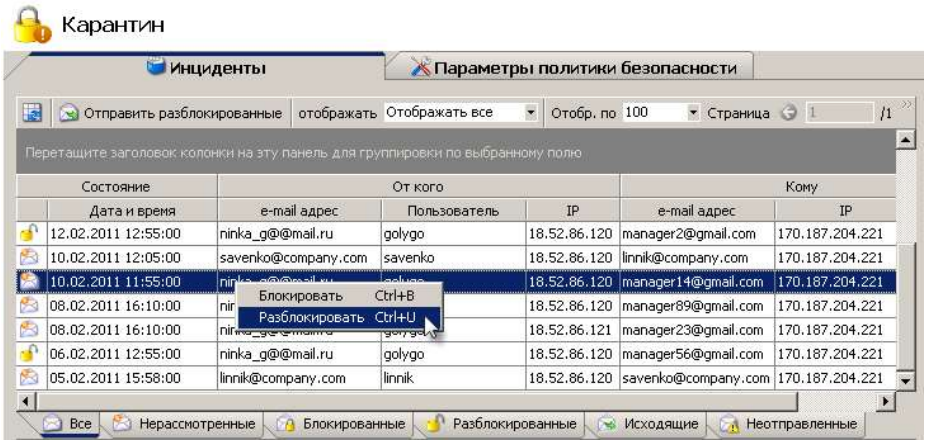


Рисунок 4.56

Отправка разблокированных сообщений производится по нажатию кнопки «Отправить разблокированные». Данное действие носит необратимый характер: все разблокированные сообщения на период отправки будут перемещены на вкладку «Исходящие» и в случае успешной отправки покинут карантин.

Письма, находящиеся на вкладке «Неотправленные», можно попробовать отправить повторно (см. Рисунок 4.57).

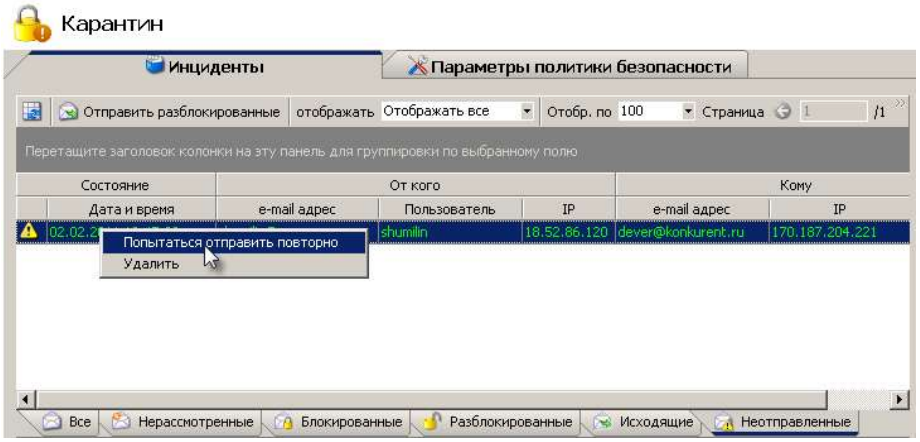


Рисунок 4.57

4.3.9 Проверка срабатывания AlertCenter

Запустите проверку по созданным политикам или дождитесь запуска по настроенному расписанию (см. Рисунок 4.58).

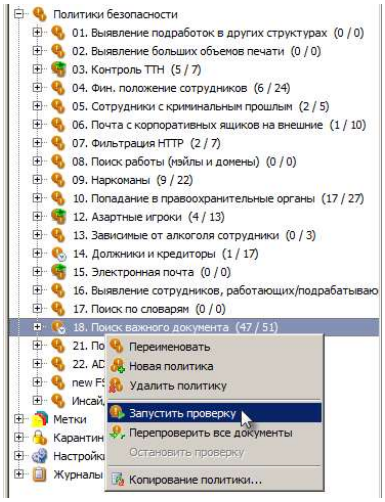


Рисунок 4.58

Получите почту. Должны быть доставлены уведомления (см. Рисунок 4.59), включающие в себя ссылки на:

- просмотр инцидентов в клиенте AlertCenter;
- просмотр сработавших критериев поиска в клиенте AlertCenter;
- просмотр найденных документов в поисковом клиенте AnalyticConsole.

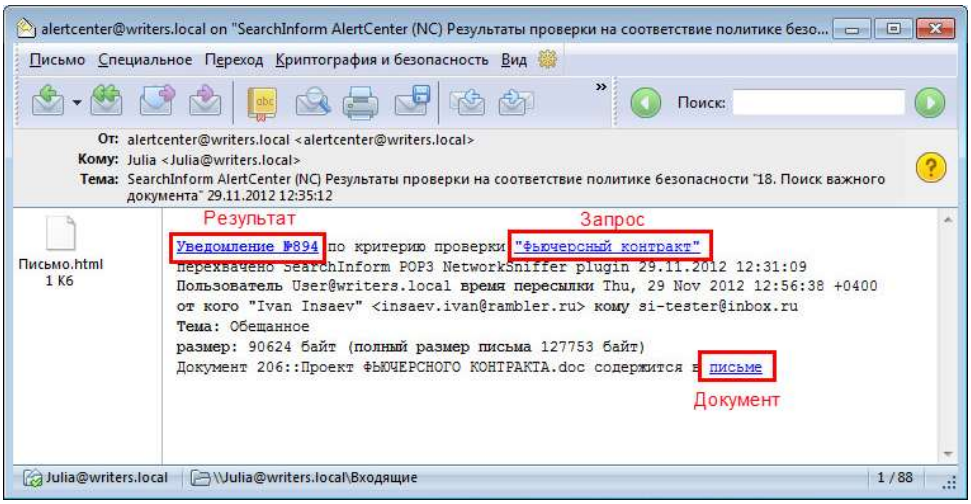


Рисунок 4.59

Вне зависимости от того, отправлено уведомление по инциденту на электронную почту или нет, все срабатывания сервера сохраняются в журнал инцидентов AlertCenter. Поэтому работу с инцидентами можно производить как по ссылкам в почтовых уведомлениях, так и в клиентской консоли AlertCenter.

Ссылка на просмотр результата открывается на вкладке «Инциденты» клиента AlertCenter (см. Рисунок 4.60).

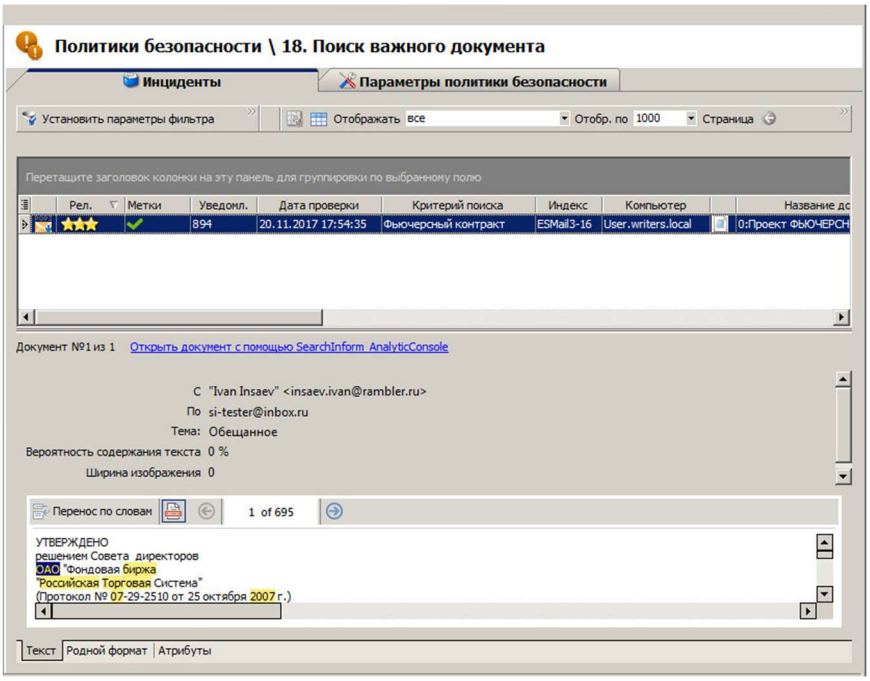


Рисунок 4.60

Ссылка на просмотр критерия поиска открывается в окне настройки запроса клиента AlertCenter (см. Рисунок 4.61).

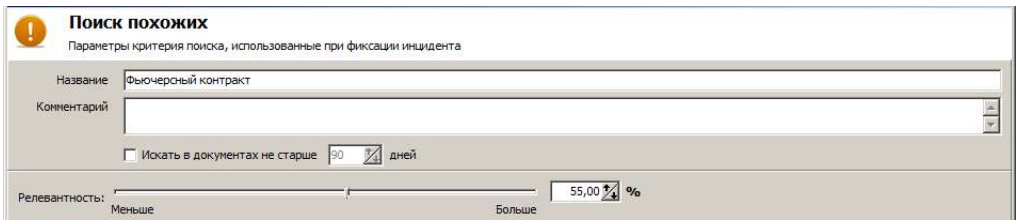


Рисунок 4.61

Ссылка на просмотр найденного документа открывается в поисковом клиенте AnalyticConsole. Документ может быть во вложении (см. Рисунок 4.62).

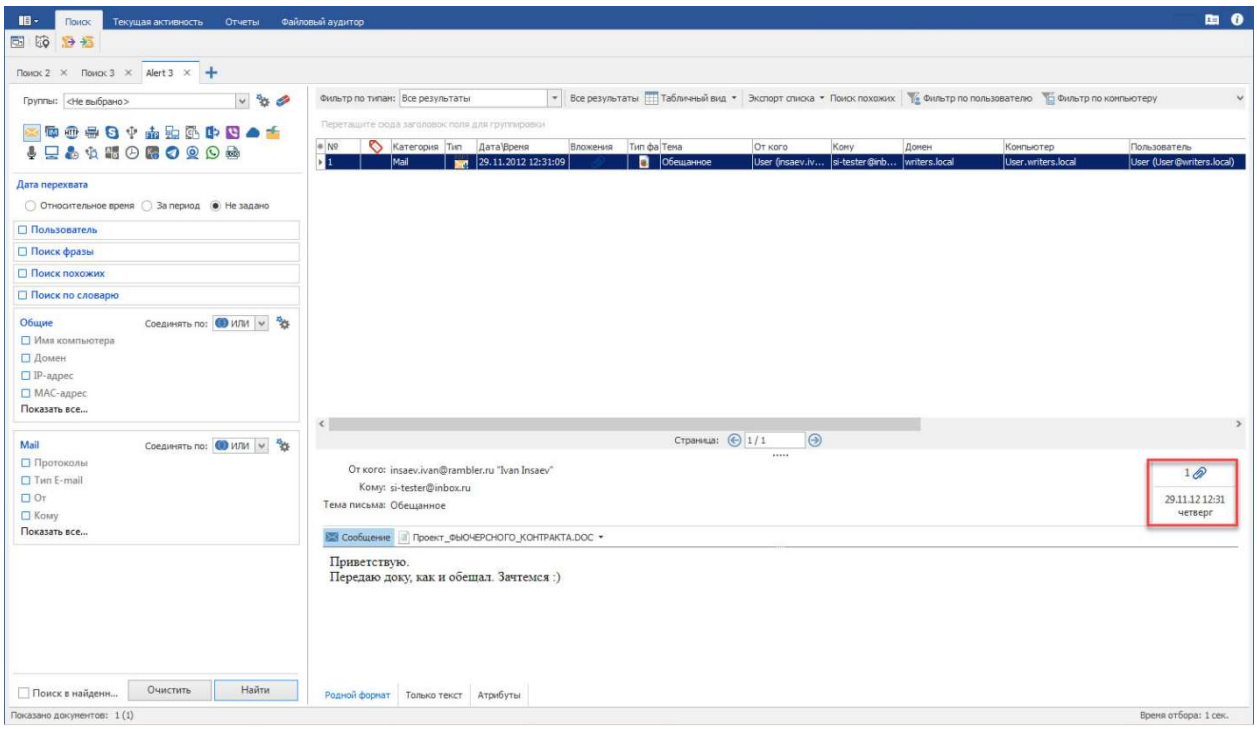


Рисунок 4.62

Вложенные файлы можно открыть в сопоставленном операционной системой приложении.

4.3.10 Поиск по цифровым отпечаткам

Цифровые отпечатки позволяют отслеживать утечку конфиденциальной информации на основании сформированного набора эталонных документов (образцов), содержащих текстовую информацию, например, устава компании, реестра держателей акций, финансовых отчётов и т.п. Перехваченные данные сопоставляются с содержанием документов-образцов.

Для работы с цифровыми отпечатками должен быть предварительно создан каталог образцов документов (либо использоваться уже имеющийся) в консоли клиента Серчинформ DataCenter. Процедура настройки библиотеки цифровых отпечатков описана в Руководстве администратора Системы.

Настройка запроса цифровых отпечатков производится при создании нового критерия поиска в клиенте Серчинформ AlertCenter на вкладке «Поиск по цифровым отпечаткам».

Выберите критерий поиска и произведите следующие настройки:

1. Установите требуемый уровень релевантности.
2. Выберите опцию:
   - при совпадении с любым образцом – поиск совпадений с любым из образцов в библиотеке цифровых отпечатков.

- при совпадении с … – поиск совпадений с указанным образцом/директорией. Введите название необходимого образца или директории (см. Рисунок 4.63).

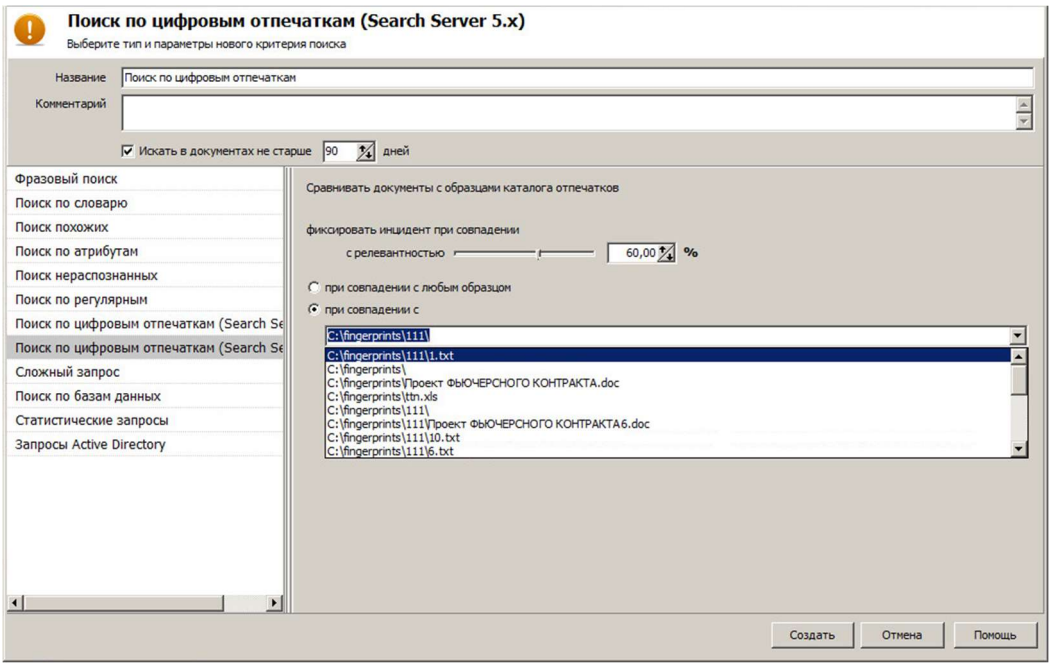


Рисунок 4.63

4.4 НАСТРОЙКА И ЭКСПЛУАТАЦИЯ СЕРЧИНФОРМ ANALYTICCONSOLE

Программный продукт Серчинформ AnalyticConsole предназначен для отслеживания утечек конфиденциальной информации через электронную почту, Skype, IM-клиенты, FTP-серверы, принтеры, подключаемые внешние устройства, контроля активности пользователя в браузере и др., подключения к базам и индексам компонентов системы безопасности, обработки информации по статистике инцидентов, активности пользователей, генерации отчетов в удобной для сотрудников службы безопасности форме, просмотре контролируемых файлов сотрудников.

4.4.1 Вкладка «Поиск»

Вкладка «Поиск» используется для формирования запроса, отображения списка результатов и просмотра выделенных документов.

Основные поисковые возможности:

- Быстрый поиск по тексту перехваченных сообщений и вложенных файлов по словам/фразам как по точному совпадению, так и с учетом морфологии.
- Поиск по тексту перехваченных сообщений и вложенных файлов по произвольным словарям.

- Поиск по тексту перехваченных сообщений и вложенных файлов с использованием запатентованной технологии «поиск похожих».
- Специальные возможности текстового поиска (поиск с учетом символов, одинаковых по написанию, поиск с учетом опечаток).
- Поиск по атрибутам перехваченных данных.
- Возможность фильтрации (группировки) результатов поиска по различным атрибутам.
- Формирование и отображение «Карточек пользователей».

Окно программы функционально разделено на несколько областей (см. Рисунок 4.64):

1. **Панель подключения источников данных** используется для подключения к индексам и базам данных, содержащим перехваченную информацию.
2. **Панель поиска** предназначена для формирования запросов.
3. **Панель результатов** показывает список результатов поиска.
4. **Окно предпросмотра** отображает подробную информацию о выбранном перехваченном документе.
5. **Строка состояния** отображает общее количество результатов поиска и количество результатов поиска, отображаемых в окне предпросмотра.

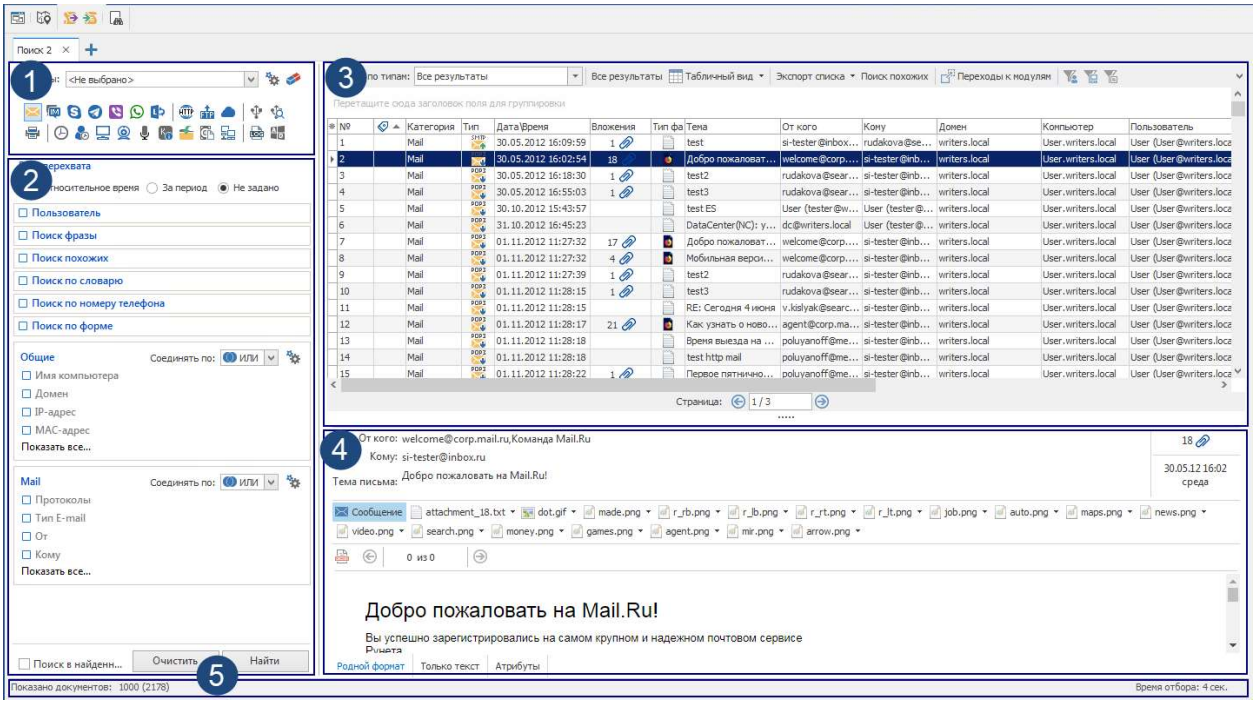


Рисунок 4.64

Приложение предоставляет возможность ввода поисковых запросов и ограничения поиска по целому ряду параметров.

На панели результатов приложения отображаются результаты выполненного поиска с учетом подключенных индексов и баз данных. Содержание выделенного в списке результатов документа отображается в окне предпросмотра.

Для анализа поискового запроса необходимо выбрать из доступного перечня иконки требуемых источников данных (см. Рисунок 4.65).

Рисунок 4.65

Щелкните по иконкам продуктов, источники данных которых необходимо задействовать при поиске.

Панель поиска включает в себя следующие элементы управления:

- Панель ограничений результатов поиска (позволяет сузить результаты поисковой выдачи за счет указания даты и времени перехвата документа, диапазона его размера).
- Блок выбора пользователя.
- Блоки поиска по тексту, включающие:
  - Вкладку поиска по пользователям;
  - Вкладку текстового поиска;
  - Вкладку поиска похожих;
  - Вкладку поиска по словарю;
  - Вкладку поиска по номеру телефона;
  - Вкладку поиска по форме.
- Блок атрибутного поиска, включающий:
  - Вкладку поиска по общим параметрам (имя компьютера, тип файла и т.д.) Тут же расположен флаг SSL (поиск данных, переданных с использованием шифрования).
  - Вкладки поиска по атрибутам отдельных каналов перехвата. Список отображаемых вкладок зависит от выбранной группы индексов.
- Кнопки «Найти» и «Очистить» (см. Рисунок 4.66).

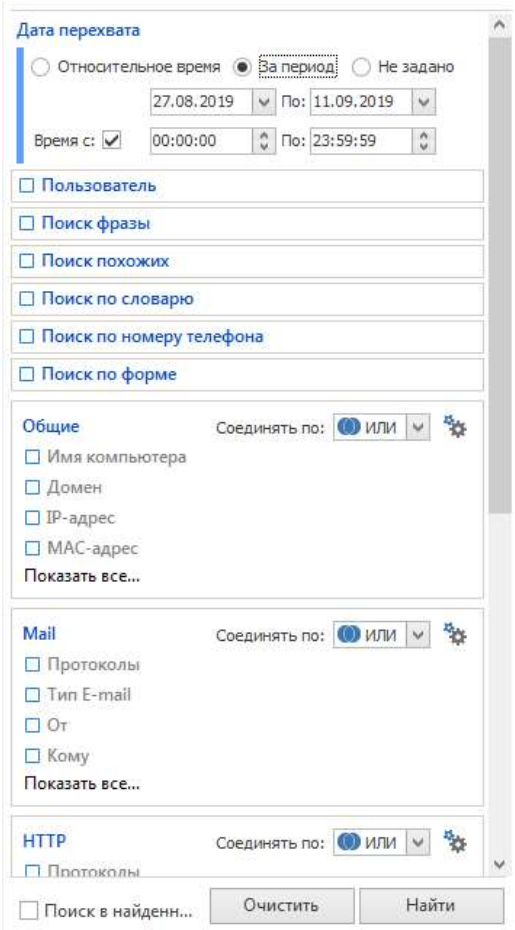


Рисунок 4.66

При нажатии кнопки «Найти» происходит выполнение поискового запроса. Результаты поиска будут отображены на панели результатов (см. Рисунок 4.67).

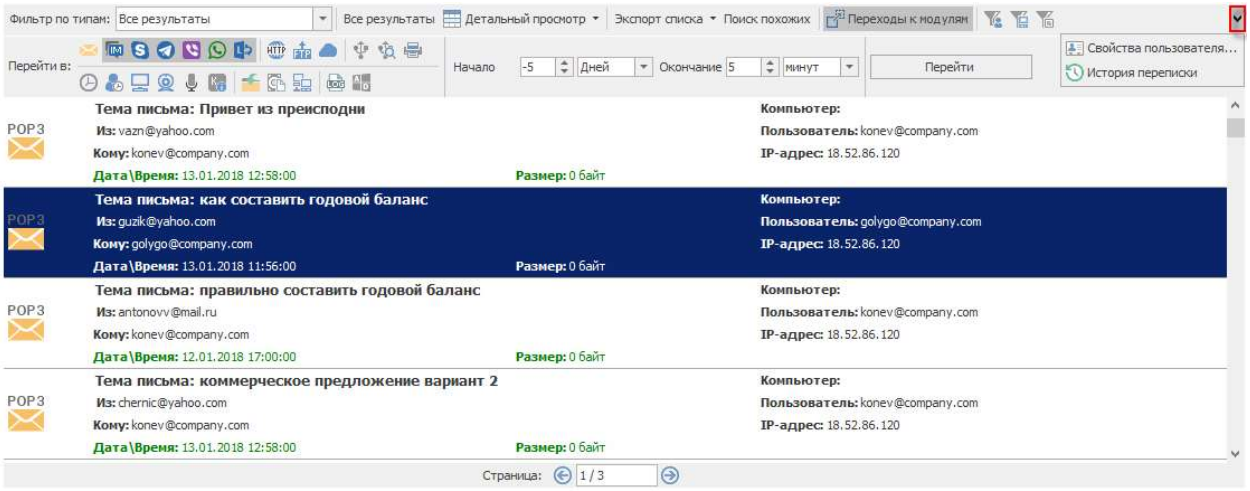


Рисунок 4.67

Панель результатов включает в себя следующие элементы управления:

- Выпадающий список «Фильтр по типам» - выбор результатов поиска по отдельному индексу либо по всем индексам в целом (опция «Все результаты»).
- Кнопка «Все результаты» - отображает полный список результатов, вне зависимости от настройки числа отображаемых документов.
- Кнопка «Табличный вид/Детальный просмотр/Эскизы» - выбор режима просмотра результатов поиска. В табличном режиме просмотра данные по свойствам каждого найденного сообщения имеют более компактный вид. «Эскизы» удобны для быстрого просмотра за счет отображения результатов поиска в виде миниатюрных иконок.
- Кнопка «Экспорт списка» - экспортирует список результатов в файлы форматов XLS, XML, HTML, TXT. Также доступен экспорт в режиме «Документы». При котором выгружается не только таблица с отображением результатов поиска, но и сами перехваченные документы (с группировкой по пользователя или продуктам), а также документов с ID. Функция может быть использована при подготовке отчетов по материалам расследований. Есть возможность экспорта файлов Microsoft Outlook в формат PST, экспорта документов с UDL, сохранения списка белых устройств для DeviceController, экспорт изображений выбранных документов PrintController в формат PDF, формирование сводного отчета по документам выбранных пользователей.
- Кнопка «Поиск похожих» - поиск документов, похожих по содержанию на выделенный объект из результатов поиска.
- Кнопка «Переходы к модулям» - отображение/скрытие панели переходов к данным, имеющимся в перехвате до/после указанного количества минут/часов/дней относительно выделенного в списке документа.
- Кнопка «Фильтр по пользователю» - фильтрация результатов поиска по значениям столбца «Пользователь».
- Кнопка «Фильтр по компьютеру» - фильтрация результатов поиска по значениям столбца «Компьютер».
- Кнопка «Свойства пользователя» - открывает окно свойств пользователя.
- Кнопка «История переписки» - отображает все сообщения, входящие в историю переписки двух пользователей (см. Рисунок 4.68).

Рисунок 4.68

Документы в результатах выдачи могут маркироваться разными цветами:

- Зеленым – если при передаче данных использовалось шифрование соединения (протокол SSL).
- Светло-красным – в случае, когда из файла не удалось извлечь текст (см. Рисунок 4.69);

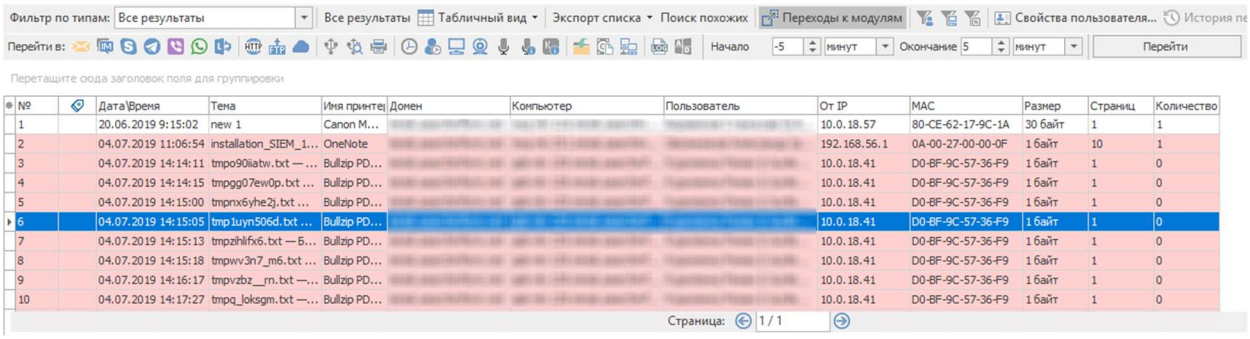


Рисунок 4.69

Количество и состав заголовков столбцов на панели результатов в табличном режиме просмотра могут изменяться в зависимости от выбранной группы индексов для поиска. Также пользователь может просмотреть только интересующие его столбцы из таблицы при помощи специального меню (вызывается нажатием левой кнопки мыши по крайнему левому заголовку из таблицы) (см. Рисунок 4.70).

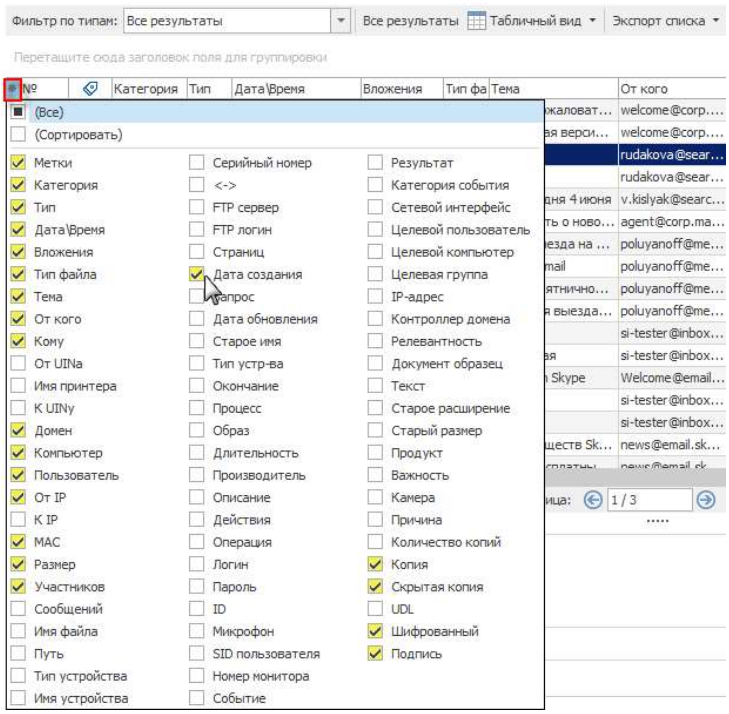


Рисунок 4.70

При работе с результатами поиска пользователю доступна функция сортировки (вызывается щелчком по заголовку столбца, результаты поиска сортируются в прямом либо обратном порядке по данному параметру).

Очередность следования столбцов можно также менять «перетаскиванием» ячеек с названием столбца в самой таблице с помощью мыши.

Результаты поиска можно «группировать» по заголовкам столбцов. Для этого с помощью мыши нужно перетащить одну или несколько ячеек с заголовком столбца в область с надписью «Перетащите сюда заголовок столбца для группировки по нему». В таблице сгруппированные результаты будут отображены с соблюдением указанной иерархии (см. Рисунок 4.71).

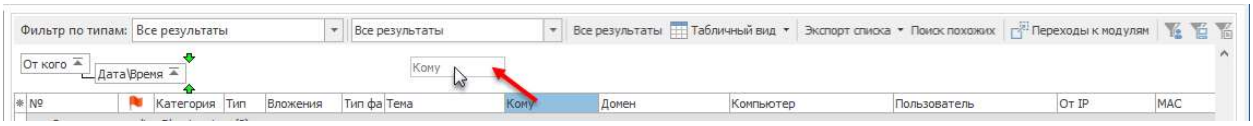


Рисунок 4.71

При выделении документа из результатов поиска его содержимое отображается в окне предпросмотра, расположенном в правом нижнем углу главного окна программы.

В нижней части окна доступны режимы отображения окна предпросмотра: «Атрибуты», «Только текст» или «'Родной' формат».

- В режиме «Только текст» содержимое документа будет отображаться как простой текст (без разметки).

- В режиме «’Родной’ формат» будут сохраняться элементы формата исходного письма (таблицы, фон, шрифт, выделение и т.п.).
- Режим «Атрибуты» предусмотрен для просмотра списка атрибутов и значений для выбранного документа.

Если в результате проведения поискового запроса были найдены совпадения внутри прикрепленного файла, то при условии включения подсветки найденных слов, он будет взят в цветную рамку для акцентирования внимания. В режиме просмотра «Только текст» будет отображена дополнительная вкладка для просмотра и перемещения по подсвеченным словам вложенного файла (см. Рисунок 4.72).

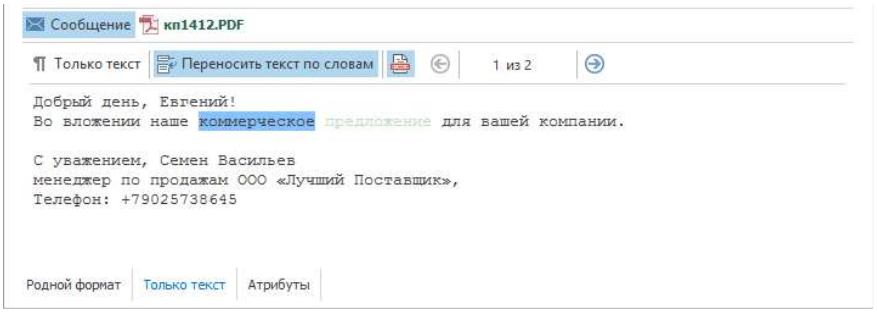


Рисунок 4.72

4.4.1.1 Выбор пользователей

Ограничение поиска по пользователям производится на вкладке Пользователь панели поиска (см. Рисунок 4.73).

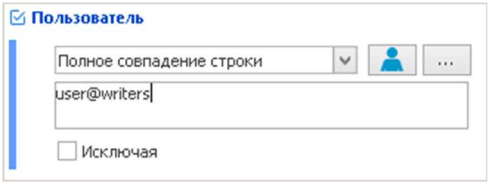


Рисунок 4.73

Для выбора пользователя необходимо установить флаг напротив параметра «Пользователь» и в открывшемся поле ввести список пользователей, по которым будет производиться поиск. Список можно создать вручную либо выбрать доменных пользователей, имеющихся в Active Directory, щелкнув по кнопке  (см. Рисунок 4.74).

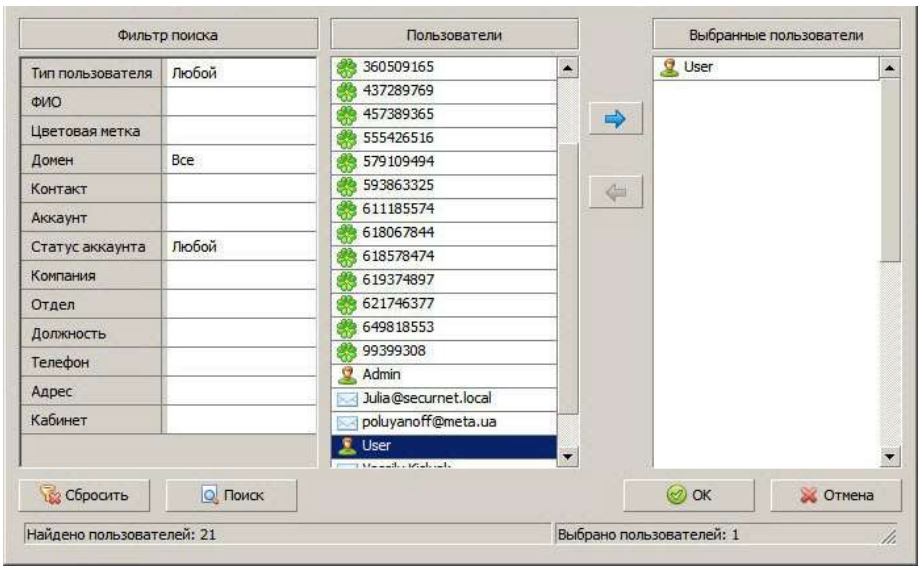


Рисунок 4.74

Необходимых пользователей перенесите в правую часть окна при помощи кнопки  или двойного клика по строке с его именем. Для удаления из выбранных воспользуйтесь кнопкой  или двойным кликом левой кнопкой мыши.

4.4.1.2 Текстовый поиск

Цель текстового поиска – обнаружение документов, содержащих ключевые слова, фразы.

Приложение позволяет производить гибкую настройку условий проверки по ключевым словам. Настройки текстового поиска задаются на вкладке **Поиск фразы** панели поиска (см. Рисунок 4.75).

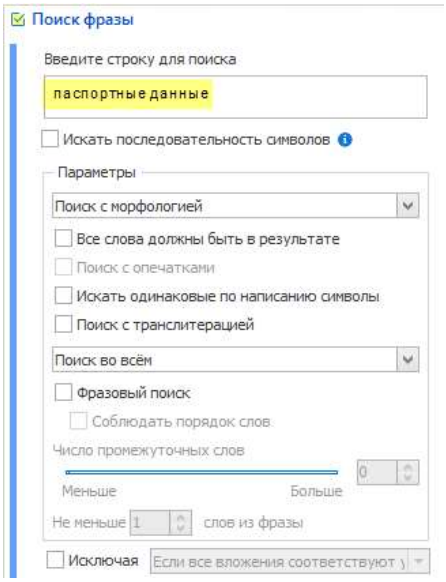


Рисунок 4.75

Опция ***Искать последовательность символов*** позволяет найти заданные символы в точном порядке. При установленном флажке нижеследующие параметры поиска становятся неактивными.

Ниже приводится описание опций для настройки текстового поиска (выбор первых пяти опций производится с помощью выпадающего списка).

- Поиск с морфологией – система идентифицирует различные словоформы при помощи специального аналитического блока. Например, при запросе «автомобиль» производится поиск всех возможных словоформ – «автомобиль», «автомобили», «автомобилей» и т.д.
- Точное совпадение – обнаруживаются только заданные пользователем словоформы.
- Начинающиеся со слов – обнаруживаются словоформы, начинающиеся с заданной пользователем комбинации символов. При запросе «автомобиль», будет идентифицирована как словоформа «автомобиль», так и иные слова, начинающиеся с «автомобиль-», например, «автомобильный».
- Содержащие слова – идентифицирует слова, содержащие сочетание символов запроса. Удобно использовать для нахождения документов, содержащих однокоренные слова. При запросе «рабо» идентифицируются такие словоформы, как «работа», «обработка», «работать».
- Оканчивающиеся на слова – поиск всех словоформ, оканчивающихся на заданное пользователем сочетание символов. При запросе «электростанция» обнаруживаются документы, содержащие словоформы «теплоэлектростанция», «гидроэлектростанция».
- «Все слова должны быть в результате» – флаг устанавливается для ограничения результатов документами, содержащими все слова запроса (в противном случае, каждое слово запроса будет обнаруживаться по отдельности).
- Поиск с опечатками – флаг устанавливается для поиска слов в документе, которые могут отличаться от слов запроса одним или двумя подряд идущими символами. При запросе «молоко» будут идентифицированы словоформы «молако» и «малоко». Документы с написанием «малако» обнаружены не будут. Поиск с опечатками недоступен при выбранных опциях Поиск с морфологией и Содержащие слова.
- Искать символы одинаковые по написанию – флаг устанавливается для идентификации слов, в которых использованы совпадающие по написанию буквы русского и латинского алфавитов. При запросе «ABC» идентифицируются все возможные сочетания кириллических и латинских букв.

- Поиск с транслитерацией - поиск русскоязычных слов, для написания которых использовались буквы латинского алфавита.
- Поиск во всем/Искать во вложениях/Поиск без вложений – для выбора, в какой части сообщения искать введенный текст. Поиск может производиться исключительно по вложенным файлам, по тексту самих сообщений, исключая вложения, либо по обоим источникам данных.
- Фразовый поиск – поиск внутри одного предложения. Частный случай текстового поиска, при котором можно зафиксировать порядок следования слов и выражений запроса, а также максимальное расстояние между отдельными словами фразы.
  - Соблюдать порядок слов – частный случай фразового поиска, при котором строго учитывается порядок слов.
  - Число промежуточных слов – с помощью ползунка регулируется количество промежуточных слов, которые не учитываются при фразовом поиске.

Активация опции ***Исключая*** скрывает в результатах поиска документы, соответствующие запросу.

Для поиска сообщений по ключевым словам на вкладке «Поиск фразы» панели поиска введите запрос в поле «Введите строку для поиска» и щелкните кнопку «Найти».

4.4.1.3 Поиск по словарю

Поиск по тематическим словарям позволяет найти документы, относящиеся к определенной тематике. В редактор параметров поиска вводится некоторое количество слов, относящихся к заданной теме (например, бухгалтерии, техническим терминам, теме денежных долгов и т.д.), и по данному словарю опрашиваются выбранные индексы.

Ниже приводится описание некоторых опций доступных при использовании поиска по словарю:

- Поиск с морфологией – система идентифицирует различные словоформы при помощи специального аналитического блока. Например, при запросе «автомобиль» производится поиск всех возможных словоформ – «автомобиль», «автомобили», «автомобилей» и т.д.
- Точное совпадение – обнаруживаются только заданные пользователем словоформы.
- Не менее указанного числа – в результаты поисковой выдачи попадут только те документы, в которых количество слов из тематического словаря больше или равно указанному числу.
- Занимающие в тексте от (%) – в результаты поисковой выдачи попадут только те документы, в которых процент содержания слов из тематического словаря больше или равен указанному числу.

Для поиска по словарю на вкладке «Поиск по словарю» панели поиска введите слова (вручную или вставьте из буфера обмена). Вы можете использовать готовый набор слов из внешнего .txt-документа, щелкнув по кнопке «Вставить словарь из файла». Настройте дополнительные параметры поиска и щелкните кнопку «Найти».

При наличии в документе указанного количества слов (или заданного процентного содержания слов) из тематического словаря, он будет отображен на панели результатов.

4.4.1.4 Поиск похожих

Данный вид поиска основывается на запатентованном алгоритме «Поиск похожих» и позволяет отслеживать данные даже в том случае, если текст документа был предварительно отредактирован. В качестве поискового запроса можно использовать наборы ключевых фраз, фрагменты текста или документы целиком.

При использовании данного вида поиска доступна опция – уровень «Релевантности» – процентный показатель соответствия найденного документа запросу. Настройка уровня релевантности проводится при помощи регулятора, расположенного в нижней части вкладки «Поиск похожих». Уровень требуемой релевантности может быть задан в пределах 1-100%, где 1% – наименьшее возможное соответствие документа условиям поиска, а 100% - полное совпадение.

Для использования поиска похожих на вкладке «Поиск похожих» панели поиска введите текст запроса вручную или вставьте из буфера обмена (для выполнения операции необходимо ввести не менее 20 символов). Установите уровень релевантности и щелкните кнопку «Найти».

4.4.1.5 Поиск по номеру телефона

Данный вид поиска позволяет искать среди перехваченных данных номера телефонов.

Ниже приводится описание некоторых опций, доступных при использовании этого вида поиска:

- Поиск во всем/Искать во вложениях/Поиск без вложений – определяет, в какой части сообщения искать введенный номер телефона. Поиск может производиться исключительно по вложенным файлам, по тексту самих сообщений, исключая вложения, либо по обоим источникам данных.
- Начинающиеся с цифр - обнаруживаются телефоны, начинающиеся с заданной пользователем комбинации цифр.
- Точное совпадение – обнаруживаются только заданные пользователем номера.
- Оканчивающийся на цифры – поиск всех номеров, оканчивающихся на заданный пользователем ряд цифр.

Также можно выбрать используемый шаблон(-ы) телефонного номера.

4.4.1.6 Поиск по форме

Данный вид поиска позволяет производить поиск по заполненным формам (например, анкеты со стандартными полями данных: ФИО, дата рождения, место жительства и т.д.).

Поиск названия поля осуществляется по критерию «точное совпадение». При подсчете слов в значении поля не учитываются знаки препинания, предлоги, союзы и частицы. Чтобы снять ограничение по количеству слов, установите значение «0». Минимальное количество полей для поиска - 3.

4.4.1.7 Особенности поиска по атрибутам

Поиск можно ограничивать по различным атрибутам документа: общим (доменный пользователь, дата перехвата, имя компьютера и т.д.) и специфические (по протоколу, имени принтера, различным идентификаторам или почтовым ящиками т.п.) Набор атрибутов зависит от типа подключенного источника данных: HTTP, Mail, Skype, IM и др.

Ограничение по атрибутам производится на панели поиска, на одноименных выбранным источникам данных вкладках – HTTP, Mail, Skype, Device, Print, IM, FTP, File, IWS и др. Значения атрибутов вводятся вручную либо выбираются из выпадающего списка после нажатия кнопки  (см. Рисунок 4.76).

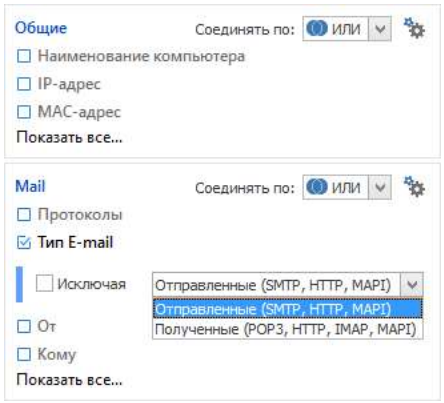


Рисунок 4.76

При выполнении поиска атрибуты могут объединяться, выступая как единое целое, либо обрабатываться отдельно, безотносительно друг к другу. Настройка производится в выпадающем списке «Объединение параметров поиска», включающем две позиции:

- Логическое ИЛИ - каждый из параметров поиска по атрибутам документа обрабатывается отдельно, безотносительно к другим параметрам.
- Логическое И - различные параметры поиска по атрибутам документа объединяются и обрабатываются как единое целое.

Любой атрибут может заполняться вручную или путем выбора значений из выпадающих списков (вызываются кнопкой ).

4.4.1.8 Экспорт данных

Результаты поиска и сами найденные документы можно экспортировать в файл как с помощью кнопки «Экспорт списка» на панели результатов поиска, так и с помощью команды из контекстного меню.

Способ 1. Выделите документы, данные по которым требуется экспортировать. Щелкните направляющую стрелку на кнопке «Экспорт списка» и выберите формат документа – XLS, XML, HTML или TXT (см. Рисунок 4.77).

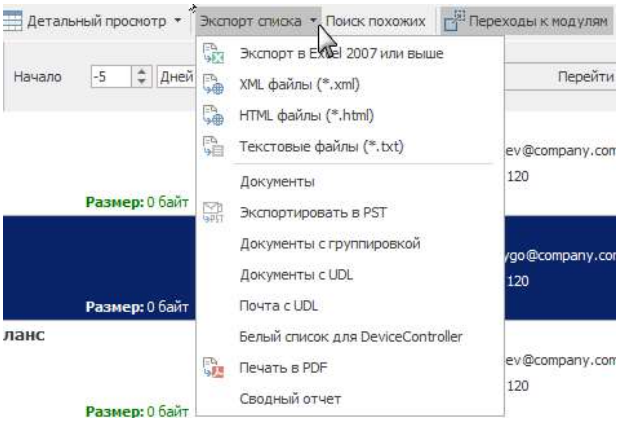


Рисунок 4.77

При выборе параметра «Документы» выделенные документы будут экспортированы в указанную папку вместе со списком формата HTML, содержащим в себе ссылки на данные документы. Клик по ссылке позволяет загрузить и просмотреть содержимое документа.

Способ 2. Выделите документы, данные по которым требуется экспортировать. Нажмите правую кнопку мыши для вызова контекстного меню и выберите команду «Экспорт списка» (см. Рисунок 4.78).

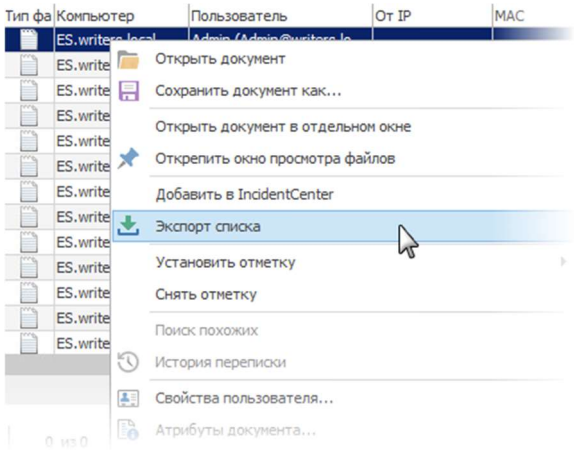


Рисунок 4.78

С помощью обозревателя выберите папку, в которую необходимо сохранить экспортируемый файл. Нажмите «ОК».

По завершении экспорта файлы появятся в выбранной папке.

4.4.1.9 Карточка пользователя

Карточки пользователей предназначены для централизованного хранения данных о пользователях и их контактах.

Для настройки карточек пользователей щелкните кнопку в правой верхней части окна  .

Консоль редактирования пользователей позволяет добавлять/удалять пользователей, редактировать информацию о пользователях, производить фильтрацию по различным критериям и др.

Для добавления нового пользователя кликните меню «Редактировать» → «Новый пользователь» либо по кнопке «Новый пользователь» (см. Рисунок 4.79).

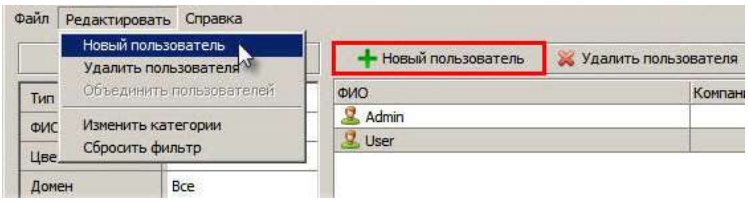


Рисунок 4.79

На вкладке «Основные» выберите тип пользователя: внутренний (пользователь Active Directory) либо внешний (пользователь почты, IM, Skype и т.д.). Задайте необходимую информацию о пользователе. С помощью вызова контекстного меню можно загрузить фотографию пользователя (см. Рисунок 4.80).

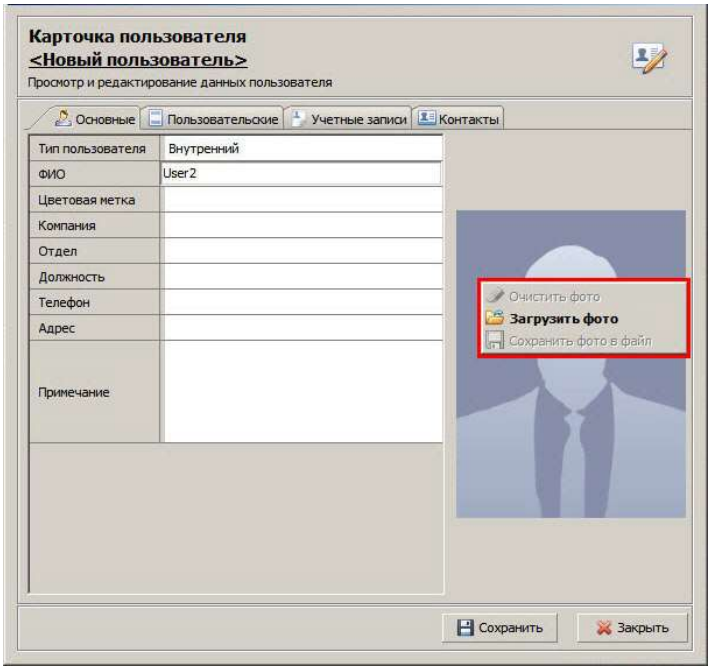


Рисунок 4.80

На вкладке «Пользовательские» при необходимости добавьте новые поля 

.

На вкладке «Учетные записи» можно привязать к пользователю учетную запись Active Directory. Щелкните «Добавить учетную запись», задайте имя пользователя и домен (см. Рисунок 4.81) и нажмите кнопку «Сохранить».

Вкладка «Учетные записи» доступна только при создании/редактировании ***внутренних*** *пользователей.*

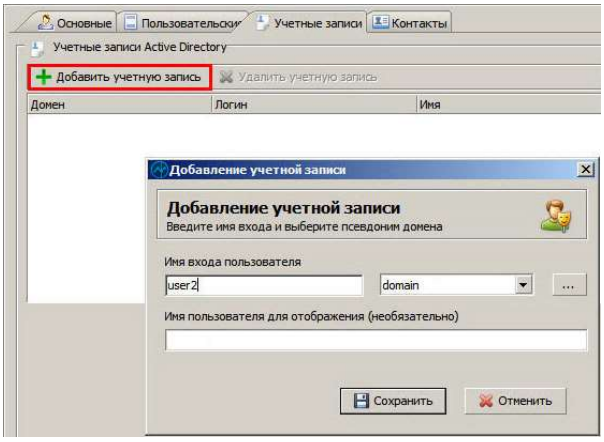


Рисунок 4.81

На вкладке «Контакты» заполните контактные данные пользователя. Щелкните «Добавить контакт», выберите тип (e-mail, логин Skype и др.) и введите необходимые данные (см. Рисунок 4.82).

Щелкните «Сохранить». Затем кликните «Закрыть».

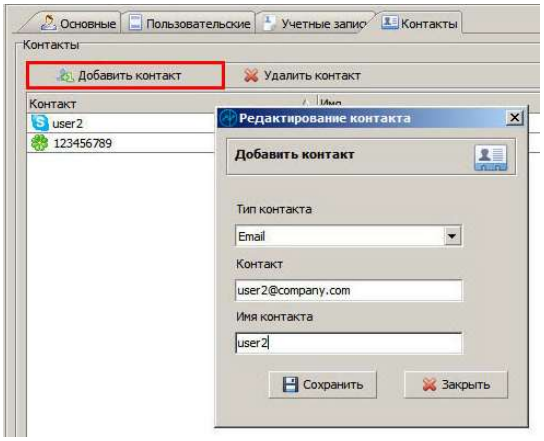


Рисунок 4.82

Нажмите «Обновить».

Пользователь будет добавлен (см. Рисунок 4.83).

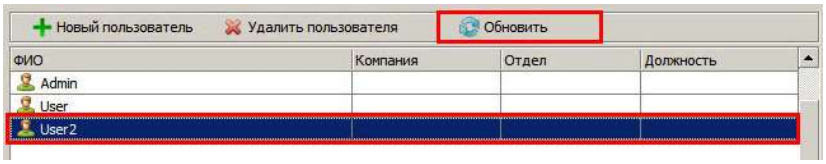


Рисунок 4.83

Для редактирования параметров пользователя используйте вкладки в нижней части экрана: «Основные», «Пользовательские», «Учетные записи» (только для внутренних пользователей) и «Контакты».

На вкладке «Связи» отображаются данные о сообщениях между пользователями. Активные связи можно фильтровать по временному периоду (за весь период, за указанный период) и количеству сообщений (> заданного в параметре).

Для открытия карточки пользователя из перечня на вкладке «Связи» используйте двойной клик или контекстное меню (см. Рисунок 4.84).

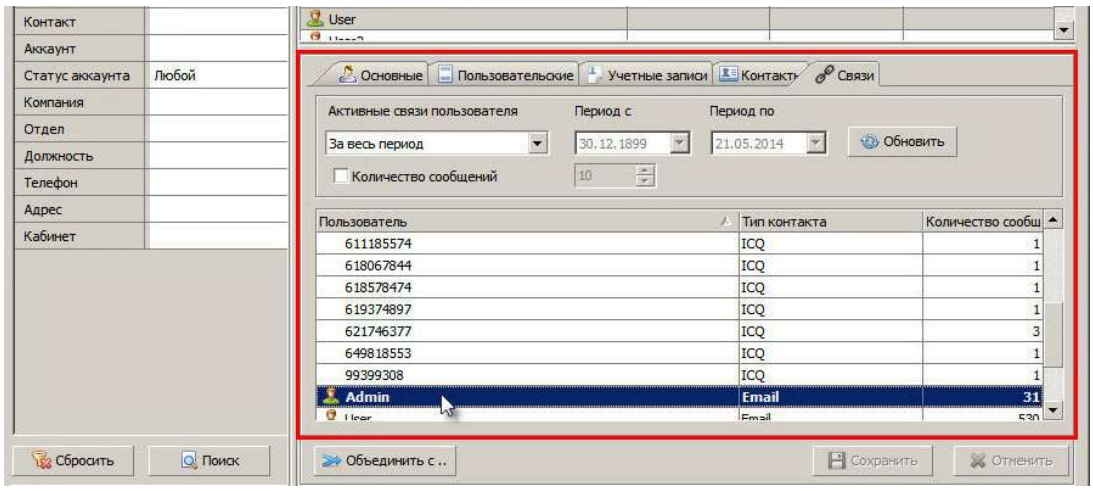


Рисунок 4.84

Для перехода к сообщениям выбранной связи используйте команду контекстного меню «Открыть переписку» (см. Рисунок 4.85).

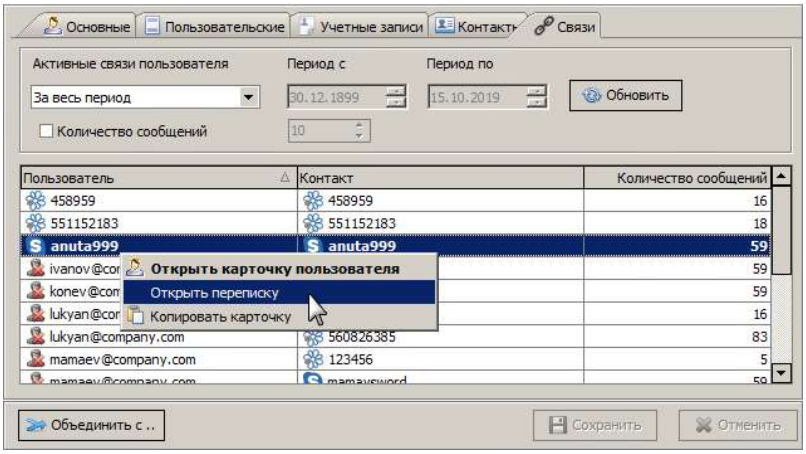


Рисунок 4.85

Для ограничения количества пользователей в результатах поиска используется фильтр (см. Рисунок 4.86).

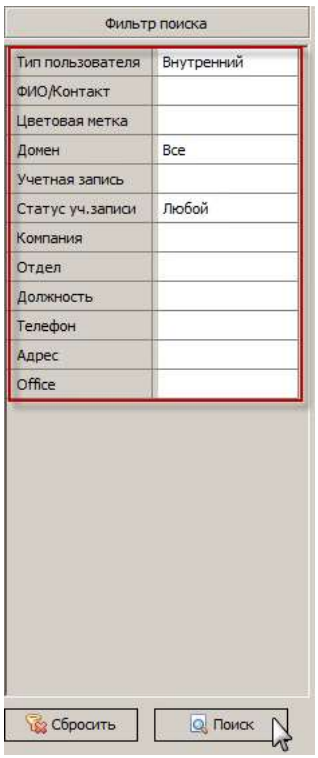


Рисунок 4.86

В Таблица 2 – Параметры фильтра и их значение представлено описание параметров фильтра с описанием каждого поля.

Таблица 2 – Параметры фильтра и их значение

Параметр фильтра	**Описание**
Тип пользователя	Выберите тип пользователя. Доступны типы: • Любой – поиск производится по всем типам пользователей; • Внутренний; • Внешний.
ФИО	Задайте имя пользователя. Поиск осуществляется по неполному совпадению строки. Например, при заданном *user* будут найдены и *user123*, и *12user3*.
Цветовая метка	Выберите цветовую метку из выпадающего меню.
Домен	Задайте имя домена. Поиск осуществляется по неполному совпадению строки. Например, при заданном *domain* будут найдены и *domain123*, и *12domain3*.

Параметр фильтра	Описание
Контакт	Введите адрес электронной почты, логин Skype и др. Поиск осуществляется по неполному совпадению строки. Например, при заданном *user* будут найдены и *user123*, и *12user3*.
Аккаунт	Введите имя учетной записи Active Directory. Поиск осуществляется по неполному совпадению строки. Например, при заданном *user* будут найдены и *user123*, и *12user3*.
Статус аккаунта	Выберите статус учетной записи Active Directory. Доступны типы: Любой - поиск производится по всем типам; • Удален; • Активный; • Заблокирован.
Компания	Введите название компании. Поиск осуществляется по неполному совпадению строки. Например, при заданном *company* будут найдены и *company123*, и *12company3*.
Отдел	Выберите отдел из выпадающего списка доступных.
Должность	Выберите должность из выпадающего списка доступных.
Телефон	Введите номер телефона. Поиск осуществляется по неполному совпадению строки.
Адрес	Введите адрес. Поиск осуществляется по неполному совпадению строки.

Задайте необходимые данные и нажмите Поиск в нижней части окна. Для сброса параметров фильтра нажмите Сбросить (см. Рисунок 4.86).

В консоли редактирования пользователей предусмотрена возможность редактирования полей, а также добавления новых.

Для редактирования полей и их типов используйте меню «Редактировать» → «Изменить категории» (см. Рисунок 4.87).

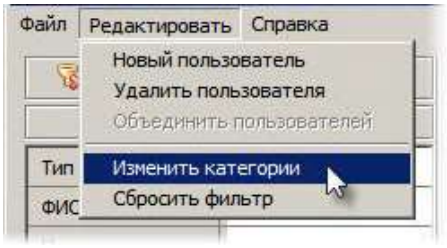


Рисунок 4.87

При создании нового пользователя либо просмотре/редактировании существующего используйте кнопку «Добавить или изменить дополнительные поля» на вкладке «Пользовательские» 

.

Щелкните «Добавить» для создания дополнительного поля (см. Рисунок 4.88).

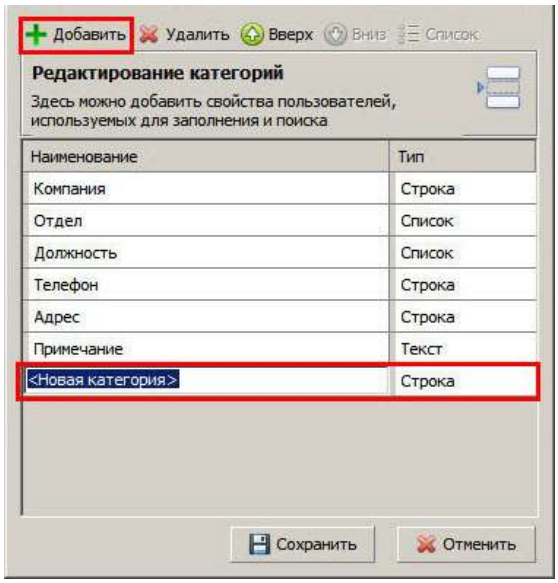


Рисунок 4.88

Введите название и выберите тип (см. Рисунок 4.89).

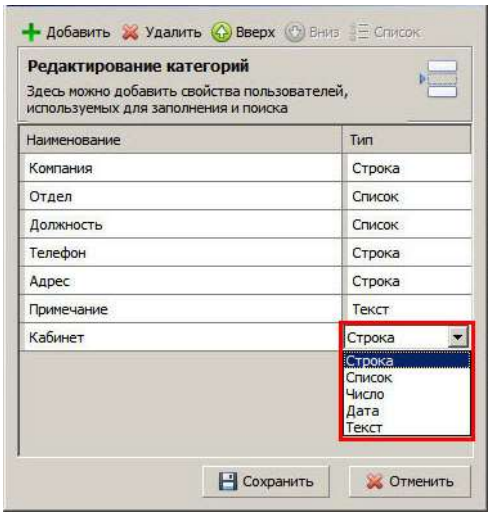
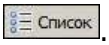


Рисунок 4.89

Для удаления категорий используйте кнопку «Удалить». Для изменения порядка расположения категорий используйте кнопки «Вверх» и «Вниз».

Для категорий с типом «Список» доступна дополнительная настройка. Выберите категорию и щелкните кнопку 

.

Для добавления значений в список нажмите «Добавить» (см. Рисунок 4.90), для удаления – «Удалить».

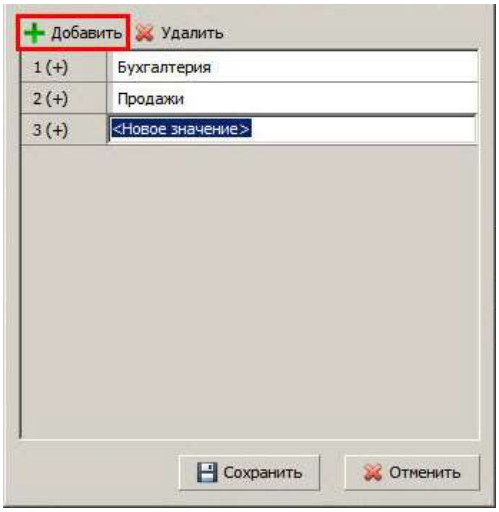


Рисунок 4.90

По завершении настройки списка нажмите «Сохранить». Введенные значения будут доступны в выпадающем списке при добавлении информации о пользователе.

По окончании всех настроек нажмите «Сохранить».

Также для добавления новых значений в категории типа «Список» можно использовать вкладку «Основные». Выберите нужное поле, а затем используйте кнопку «…» (информация о работе со списком значений представлена выше) или команду «Добавить» из выпадающего меню (см. Рисунок 4.91).

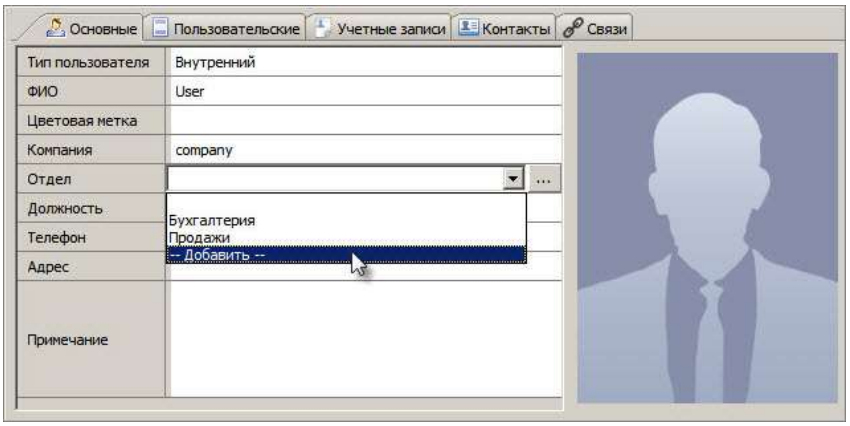


Рисунок 4.91

Введите названия и нажмите «Сохранить» (см. Рисунок 4.92).

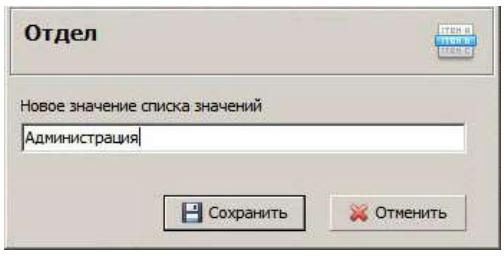


Рисунок 4.92

Для объединения пользователей выделите нескольких пользователей и выберите меню «Редактировать» → «Объединение пользователей» (см. Рисунок 4.93).

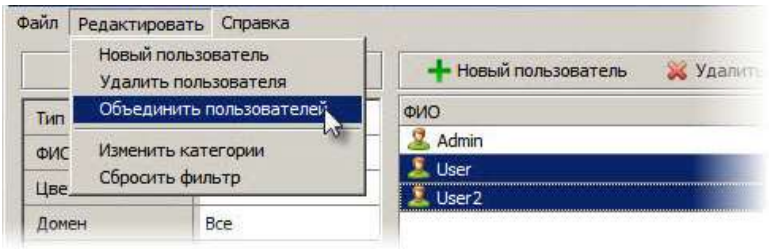


Рисунок 4.93

Либо выделите одного пользователя и нажмите 

. А затем выберите пользователя, с которым будет происходить объединение (см. Рисунок 4.94). Нажмите «ОК».

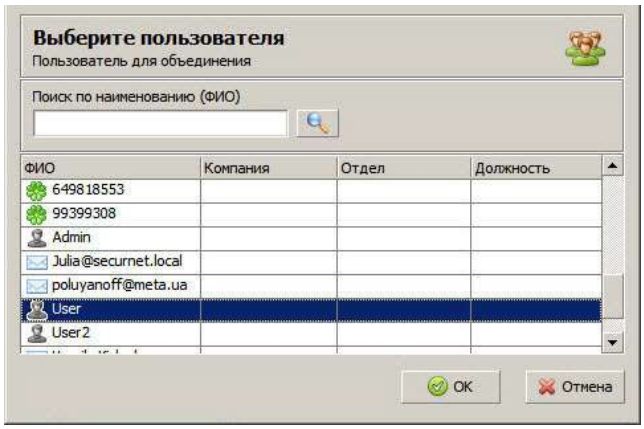


Рисунок 4.94

Отметьте необходимые контакты и нажмите «Далее» (см. Рисунок 4.95).

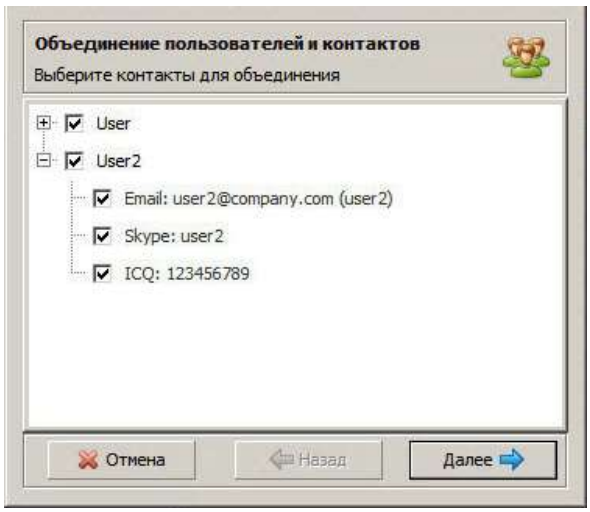


Рисунок 4.95

Выберите пользователя, для которого будут добавлены данные объединяемых пользователей (см. Рисунок 4.96).

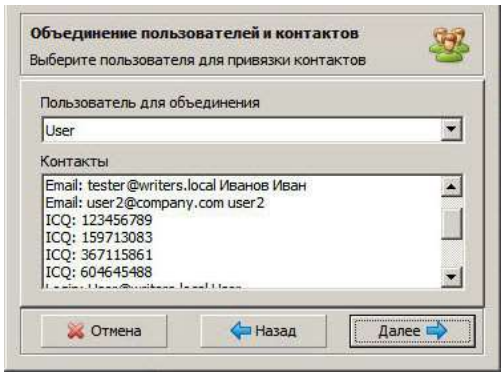


Рисунок 4.96

Нажмите «Выполнить».

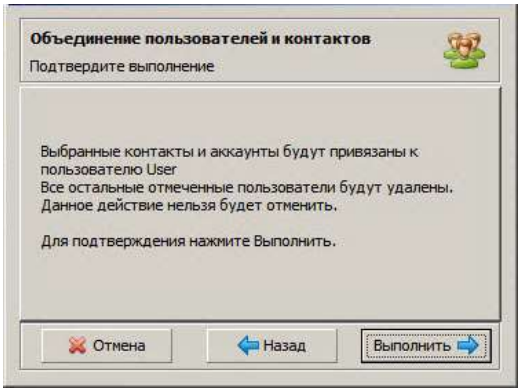


Рисунок 4.97

Пользователи будут объединены.

Чтобы экспортировать карточку выбранного пользователя, вызовите из контекстного меню команду «Экспорт» (см. Рисунок 4.98).

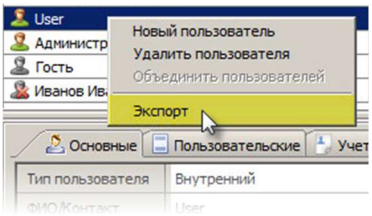


Рисунок 4.98

В диалоговом окне «Экспорт карточки пользователя» задайте необходимые настройки для экспорта (см. Рисунок 4.99):

- содержимое каких полей должно быть включено в файл,

- за какой период времени (можно ограничить экспорт связей пользователя, указав минимальное количество сообщений),
- формат файла, в который будут экспортированы данные (.RTF либо .PDF),
- директорию расположения файла,
- имя файла.

Щелкните кнопку «Экспорт» для создания файла либо кнопку «Печать» для отправки данных на принтер.

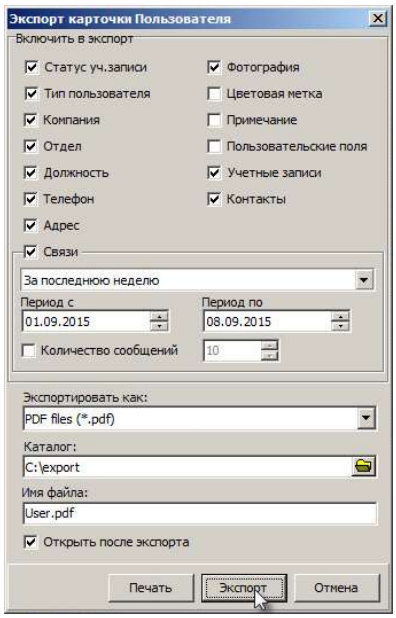


Рисунок 4.99

Если был установлен соответствующий флажок, файл будет открыт автоматически после создания.

4.4.1.10 Контентный маршрут

Контентный маршрут отображает пути передачи документа от отправителя к получателю по тому или иному каналу связи.

Для перехода к просмотру маршрута воспользуйтесь кнопкой  в левом верхнем углу вкладки или командой «Контентный маршрут», вызываемой из контекстного меню выбранного документа/письма.

Если для построения маршрута использовалась кнопка  , то в открывшемся окне выберите документ, контентный маршрут которого необходимо отобразить.

Дополнительно может быть ограничен временной диапазон, а также выбраны определенные источники данных.

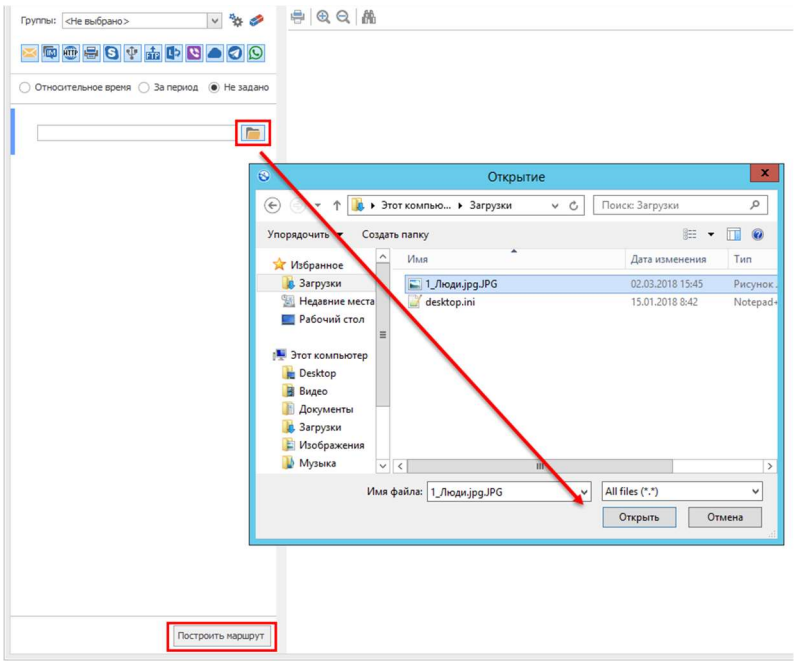


Рисунок 4.100

При переходе из контекстного меню маршрут будет построен автоматически (см. Рисунок 4.101).

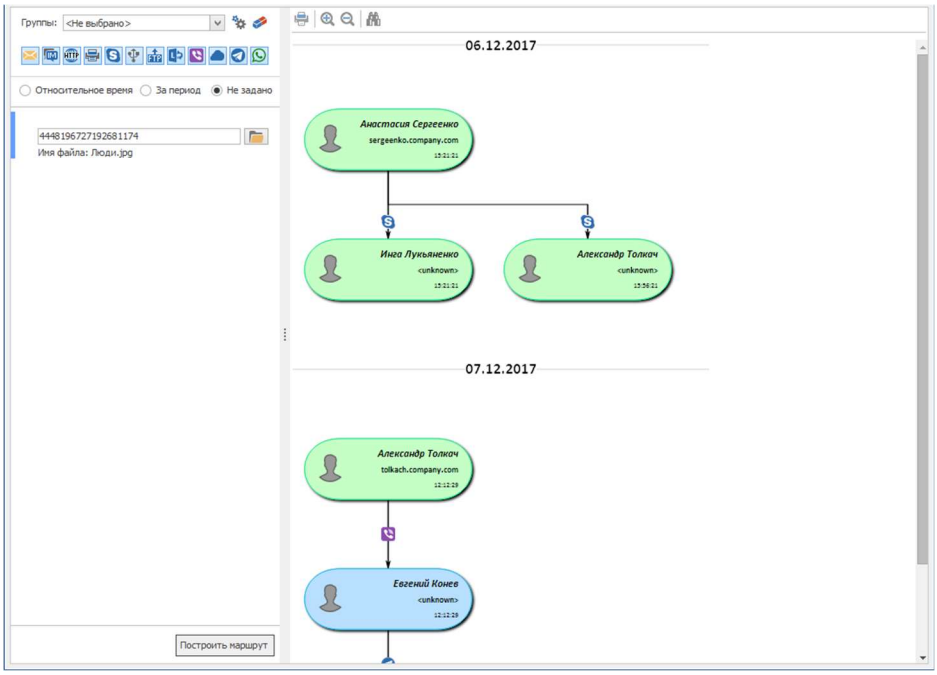


Рисунок 4.101

4.4.2 Текущая активность

4.4.2.1 Онлайн активность

Режим «Онлайн активность пользователей» позволяет просматривать информацию об активности сотрудников в режиме реального времени.

Для перехода к онлайн активности пользователей воспользуйтесь вкладкой «Текущая активность» -> «Онлайн активность пользователей». В открывшемся окне отображается список сотрудников, фильтры по категориям активности, параметры настроек списка сотрудников, временная шкала активности пользователя, статистика активности пользователя за месяц, а также график его приходов/уходов (см. Рисунок 4.102).

На панели инструментов можно задать параметры просмотра активности пользователя:

Периоды активности – время начала и окончания рабочего дня (формат времени ЧЧ:ММ).

Дата – выбор даты, за который необходимо проверить активность.

Поиск – поле ввода имени пользователя/компьютера для поиска в заданном списке сотрудников.

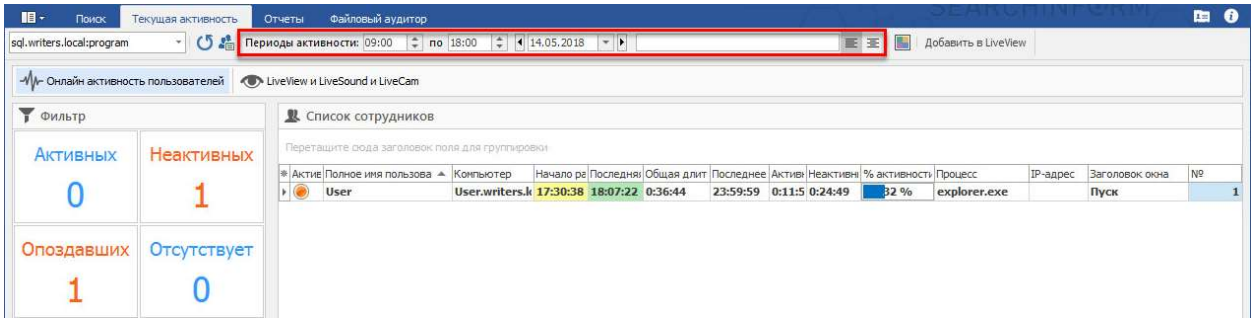


Рисунок 4.102

Цвета маркировки некоторых колонок и графиков начала/окончания работы можно изменить в настройках программы. Ниже представлены обозначения по умолчанию:

- Значок в колонке «Активность» означает:
  - - сотрудник активен в данный момент;
  - - сотрудник неактивен в данный момент;
  - - сотрудник отсутствует.
- Информация о сотрудниках может маркироваться разными цветами.
  - Все колонки:

    Серым – сотрудник отсутствует (активности сегодня не было).
  - Колонка «Начало работы»:

Зеленым – сотрудник начал работу вовремя (активность началась раньше указанного в параметре «Начало работы»);

Желтым – сотрудник опоздал (активность началась позже указанного в параметре «Начало работы»).

- Колонка «Последнее сообщение»:

  Красным – прошедший с последнего сообщения от агента промежуток времени превысил 10 минут.

Для выбора сотрудников используйте кнопку  . В открывшемся окне отметьте требуемых пользователей и кликните «ОК».

Доступны 4 фильтра для отображаемого списка сотрудников:

- **Активных** – сотрудники, на рабочих станциях которых производятся действия (нажатия клавиш, движение мыши, разговор в Skype и т.п.) в данный момент времени;
- **Неактивных** – сотрудники, на рабочих станциях которых не производятся активные действия (нажатия клавиш, движение мыши, разговор в Skype и т.п.) в данный момент времени;
- **Опоздавших** – сотрудники, активные действия на рабочих станциях которых начались позже времени, указанного в параметре «Начало работы»;
- **Отсутствуют** – сотрудники, на рабочих станциях которых активных действий сегодня не было.

Фильтры можно комбинировать:

- «**Активных**», «**Неактивных**» и «**Отсутствуют**» при комбинировании с другими объединяются по логическому «ИЛИ»;
- «**Опоздавших**» объединяется с остальными по логическому «И».

Фильтры «Неактивных», «Опоздавших» и «Отсутствуют» выделяются цветом:

- **Синий** – нет неактивных, опоздавших, отсутствующих сотрудников;
- **Красный** – есть неактивные, опоздавшие, отсутствующие сотрудники.

Для включения/отключения фильтра кликните по необходимой плитке. Например, при включении «Неактивных» будут выводиться только неактивные пользователи.

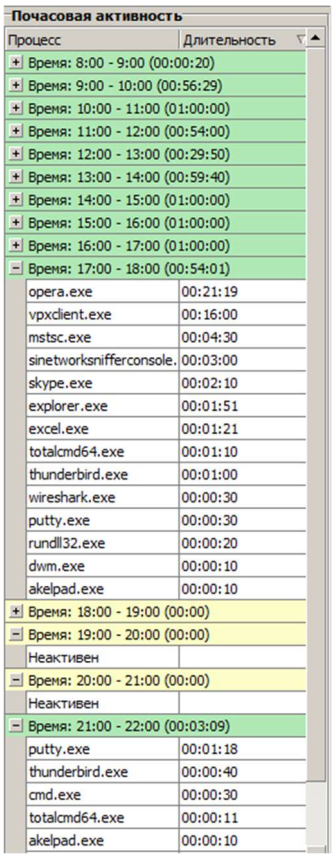
В таблице «**Информация о пользователе**» представлены статистические данные об активности сотрудника за месяц (см. Рисунок 4.103). Для просмотра данных за предыдущие месяцы воспользуйтесь настройкой «Дата».

Информация о пользователе

Месяц	Апрель
Опозданий	1
Ранних уходов	0
Отсутствий	5
Отработал (дни)	7
Работа в выходные	0
Отработал	64:14
Активность	54:47
% активности	85 %

Рисунок 4.103

В таблице «**Почасовая активность**» представлена информация об активности за каждый час в течении рабочего дня (см. Рисунок 4.104). Для просмотра активных процессов в течении выбранного часа нажмите «**+**». Часы, в течении которых не было активности, отмечаются желтым.



Почасовая активность

Процесс	Длительность
⊞ Время: 8:00 - 9:00 (00:00:20)	
⊞ Время: 9:00 - 10:00 (00:56:29)	
⊞ Время: 10:00 - 11:00 (01:00:00)	
⊞ Время: 11:00 - 12:00 (00:54:00)	
⊞ Время: 12:00 - 13:00 (00:29:50)	
⊞ Время: 13:00 - 14:00 (00:59:40)	
⊞ Время: 14:00 - 15:00 (01:00:00)	
⊞ Время: 15:00 - 16:00 (01:00:00)	
⊞ Время: 16:00 - 17:00 (01:00:00)	
⊟ Время: 17:00 - 18:00 (00:54:01)	
opera.exe	00:21:19
vpxclient.exe	00:16:00
mstsc.exe	00:04:30
sinetworksnifferconsole.	00:03:00
skype.exe	00:02:10
explorer.exe	00:01:51
excel.exe	00:01:21
totalcmd64.exe	00:01:10
thunderbird.exe	00:01:00
wireshark.exe	00:00:30
putty.exe	00:00:30
rundll32.exe	00:00:20
dwm.exe	00:00:10
akelpad.exe	00:00:10
⊞ Время: 18:00 - 19:00 (00:00)	
⊟ Время: 19:00 - 20:00 (00:00)	
Неактивен	
⊟ Время: 20:00 - 21:00 (00:00)	
Неактивен	
⊟ Время: 21:00 - 22:00 (00:03:09)	
putty.exe	00:01:18
thunderbird.exe	00:00:40
cmd.exe	00:00:30
totalcmd64.exe	00:00:11
akelpad.exe	00:00:10

Рисунок 4.104

На графике «**Приходы/Уходы**» отображена информация о начале/окончании рабочего дня за отработанные дни месяца (см. Рисунок 4.105). Для просмотра данных за предыдущие месяцы воспользуйтесь настройкой «Дата».

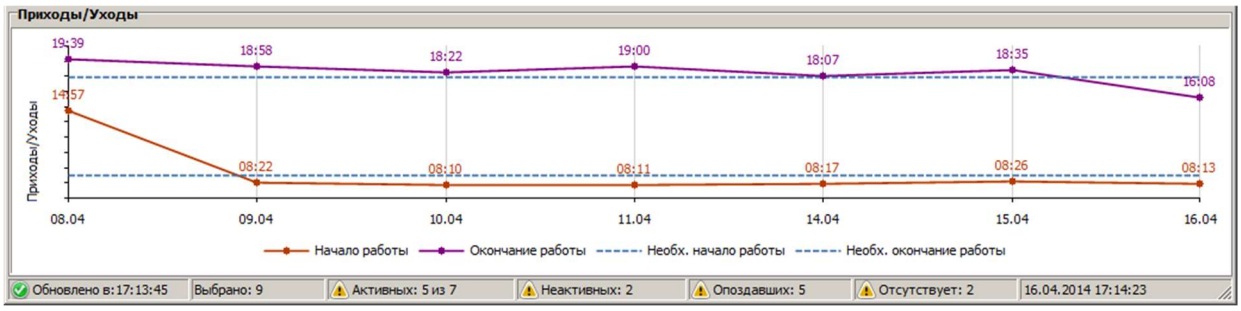


Рисунок 4.105

С помощью контекстного меню можно добавить выбранного пользователя в режимы LiveView и LiveSound (см. Рисунок 4.106).

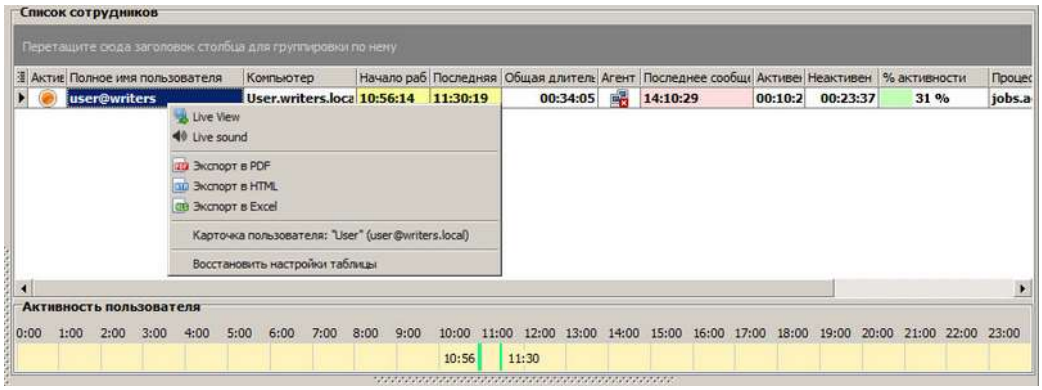


Рисунок 4.106

Для обновления данных (например, после изменения настроек) используйте кнопку 

.

4.4.2.2 LiveView, LiveSound и LiveCam

Для оперативного контроля за происходящим на рабочих местах пользователей предусмотрены специальные режимы, работающие в режиме реального времени:

- **LiveView** - просмотр содержимого экранов мониторов;
- **LiveSound** - прослушивание речи сотрудников;
- **LiveCam** - мониторинг происходящего за компьютером посредством подключенной веб-камеры.

Для перехода к режимам оперативного контроля воспользуйтесь вкладкой «Текущая активность» → «LiveView и LiveSound и LiveCam».

С помощью раскрывающегося списка «Фильтр» выберите один из трех видов отображения сетевого окружения:

- **Все** – простой список всех компьютеров.
- **Только компьютеры с агентами** – простой список компьютеров, на которые установлены агенты.

- **Только ноутбуки** – простой список всех ноутбуков.

Имена выключенных компьютеров либо не имеющих установленного агента, отображаются серым цветом. Выберите компьютер, за которым нужно установить оперативный контроль, и дважды щелкните по нему мышью (см. Рисунок 4.107).

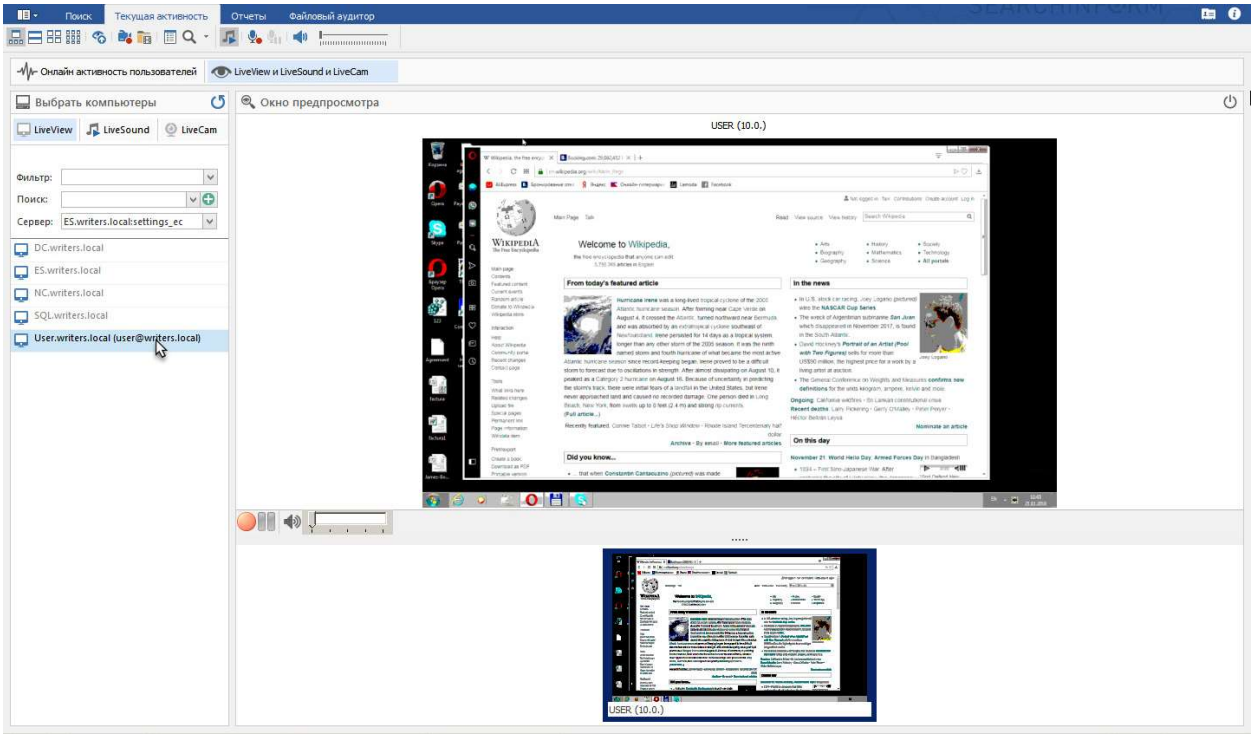


Рисунок 4.107

В правой части вкладки, спустя некоторое время, необходимое на соединение, будет отображен экран выбранного компьютера с происходящей на нем в настоящее время активностью. Над отображаемым экраном будет выводиться доменное имя компьютера и/или его IP-адрес.

Для быстрого поиска компьютера и добавления его в режим LiveView введите имя компьютера в поле «Поиск», а затем щелкните кнопку  .

В режиме оперативного контроля возможно одновременное отслеживание работы до 16 пользователей. При наблюдении за несколькими компьютерами будет удобным настроить режим просмотра экранов. Возможно 4 варианта:

-  основной режим – область просмотра разделена на 2 части: в верхней находится экран основного подключения, а в нижней - миниатюры экранов остальных подключений;
-  режим двух экранов – попарное вертикальное отображение экранов двух компьютеров;
-  режим четырех экранов – в области просмотра отображаются 4 экрана;

-  режим сетки 4x4 – одновременное наблюдение за 16 экранами.

Если рабочие станции выбранных мониторов отключены от сети, то аудитору будет выводиться оповещение о разрыве соединения.

Помимо просмотра содержимого экранов мониторов в режиме реального времени, поддерживается видеозапись всего происходящего. Файл видео именуется по шаблону *<PC_дата_время>* и сохраняется в директории, указанной в настройках программы. Для начала записи вызовите контекстное меню в окне LiveView и выберите команду «Записать» (см. Рисунок 4.108).

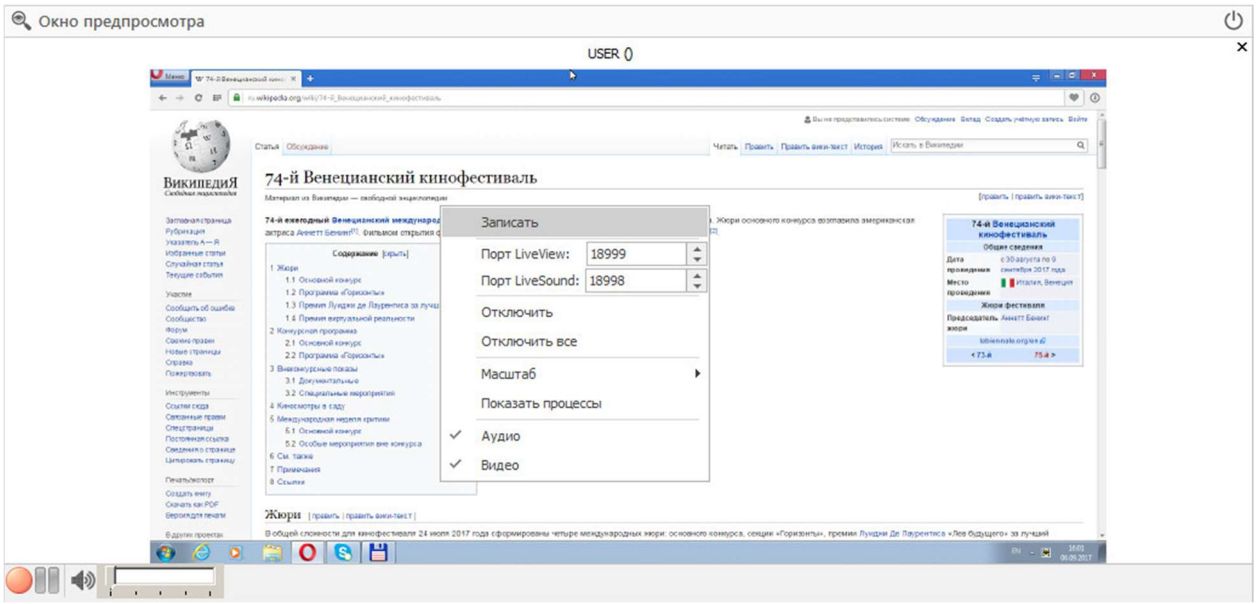


Рисунок 4.108

В верхнем левом углу окна появится надпись «Rec», сигнализирующая о длящейся видеозаписи.

Для прекращения записи выберите в контекстном меню команду «Остановить запись» (см. Рисунок 4.109).

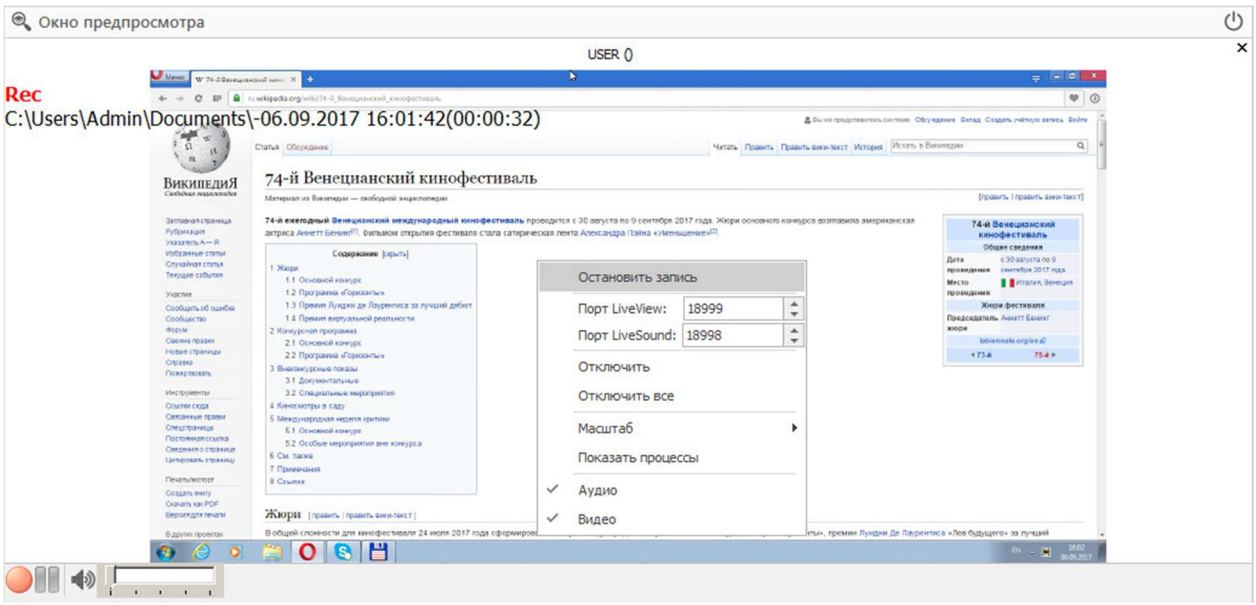


Рисунок 4.109

Для прекращения наблюдения за одной или несколькими рабочими станциями вызовите контекстное меню и выберите команду «Отключить» или «Отключить все».

Пункт контекстного меню «Масштаб» позволяет выбрать одно из предложенных соотношений размера окна.

При выборе из контекстного меню команды «Показать процессы» в правой части вкладки появится панель, отображающая запущенные в данный момент на выбранном компьютере процессы. Панель появляется и скрывается по клику курсором мыши на разделяющем сплиттере.

Режим LiveSound, предназначенный для прослушивания разговоров сотрудников, по умолчанию всегда активирован (в контекстном меню напротив команды «аудио» установлен флажок). Снятие флажка прекращает работу режима. На протяжении всего времени работы режима LiveSound будет осуществляться трансляция звука (при наличии на заданной рабочей станции аудиокарты и подключенного микрофона).

Использование кнопок  и  позволяет отключать/включать звук. Для настройки уровня звука используется регулятор громкости.

Помимо прослушивания сотрудников в режиме реального времени можно произвести запись перехватываемого звука. Нажмите кнопку  для начала записи. Директория, в которую по умолчанию осуществляется сохранение файла, может быть изменена в настройках программы.

С помощью кнопки  можно приостановить/возобновить запись в текущий файл. Для прекращения записи нажмите  .

Функционал вкладки LiveCam аналогичен функционалу режима LiveView (см. Рисунок 4.110).

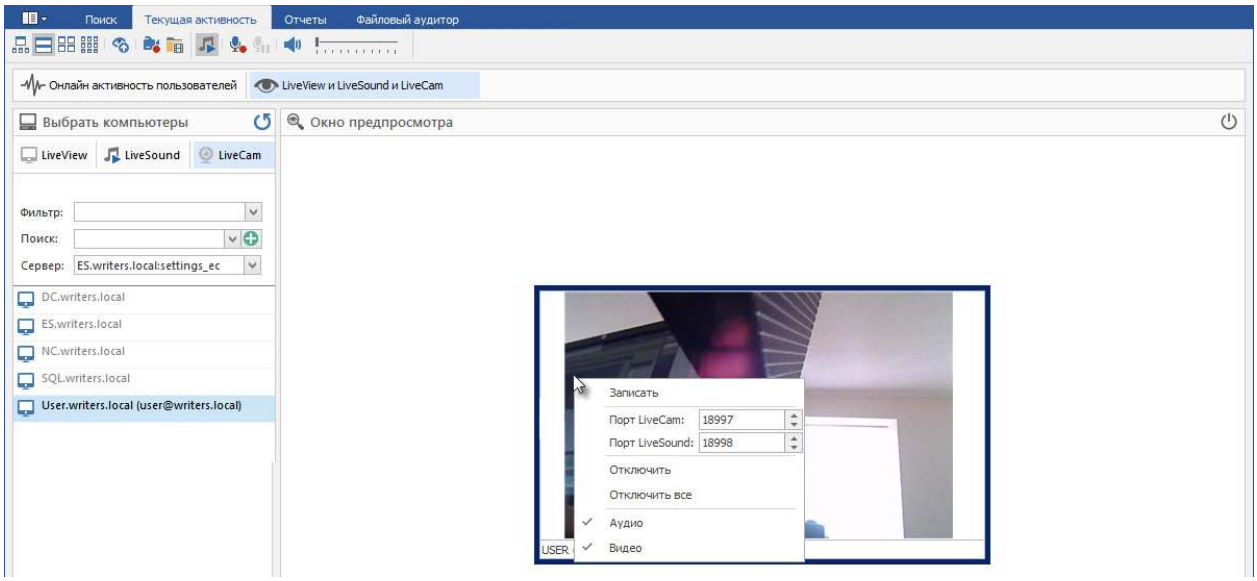


Рисунок 4.110

4.4.3 Отчеты

Вкладка «Отчеты» используется для настройки, генерирования и отображения отчетов. Вкладка функционально разделена на несколько областей (см. Рисунок 4.111):

1. ***Панель выбора шаблонов отчета*** отображает список шаблонов, на основании которых генерируются отчеты. С помощью расположенных в верхней части кнопок-иконок предусмотрена возможность создания новых шаблонов отчетов, редактирования либо удаления уже существующих (если они были созданы пользователем).
2. ***Панель выбора периода и пользователей*** позволяет задать временной период отчета, количество отображаемых в отчетах пользователей и непосредственно произвести выборку пользователей.
3. В ***окне просмотра отчетов*** отображается сгенерированный отчет. С помощью кнопок-иконок возможна навигация по отчетам, их детализация, экспорт отчета в различные форматы файлов, настройки параметров страницы и вывода отчета на печать. Окно просмотра позволяет также сохранить сгенерированный отчет в виде отдельного (пользовательского) шаблона.

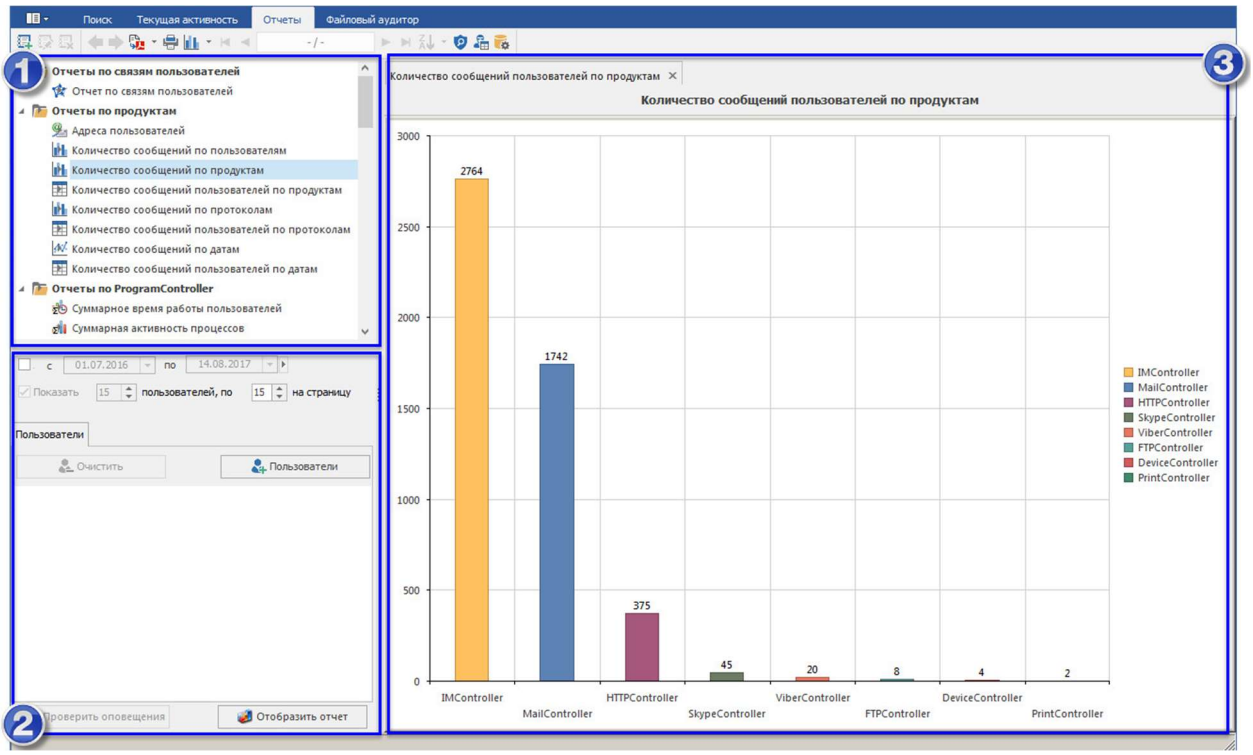


Рисунок 4.111

4.4.3.1 Генерация отчетов

Генерация отчетов производится на панели выбора шаблонов отчетов (см. Рисунок 4.112).

Выберите тип отчета и выполните любую из перечисленных операций для его отображения:

- щелкните кнопку «Отобразить отчет» в нижней части консоли;
- сделайте двойной щелчок по типу отчета;
- вызовите контекстное меню и выберите команду «Отобразить отчет».

Для некоторых отчетов требуется предварительная настройка параметров, согласно которым он будет сформирован и отображен.

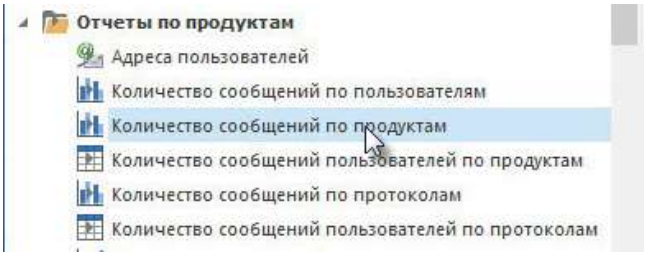


Рисунок 4.112

В окне просмотра отчетов будет отображен сгенерированный отчет (см. Рисунок 4.113).

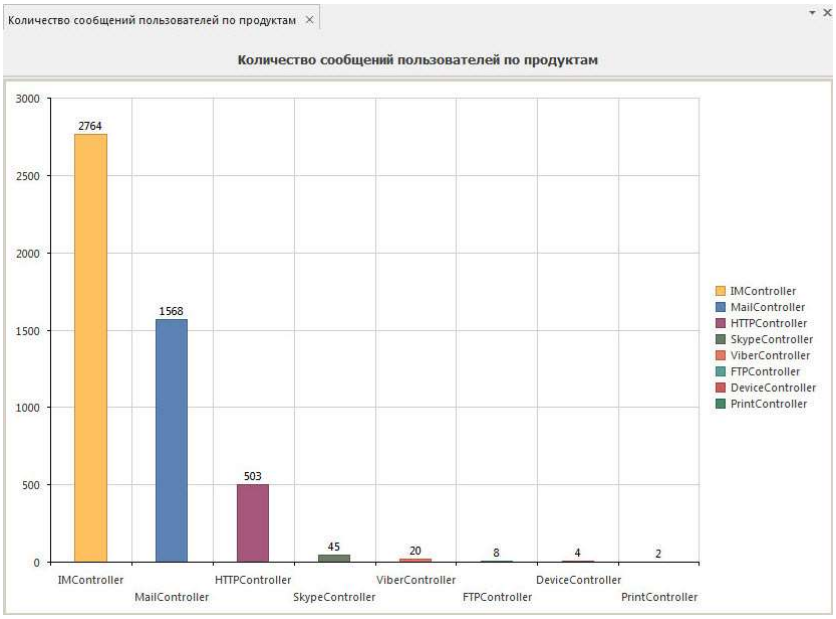


Рисунок 4.113

4.4.3.2 Выбор пользователей

Отчеты можно генерировать как по всем, так и по отдельным пользователям.

Под строкой настройки периода времени расположена строка выбора количества отображаемых пользователей, позволяющая задать следующие настройки:

- количество выбранных пользователей, отображаемых в отчете;
- число пользователей, которое будет отображаться на каждой странице отчета.

По умолчанию первая настройка отключена. Это означает, что в отчете отображаются все выбранные пользователи. Для ограничения числа отражаемых в отчете пользователей установите соответствующий флажок (перед словом «Показать») и задайте необходимое значение. По нажатии кнопки «Отобразить отчет» в графе отношений будут отображены наиболее активные выбранные пользователи (т.е. те, кто за указанный период времени имел наибольшее количество сообщений) в количестве, равному выставленному значению.

Другая настройка всегда находится в активном состоянии, позволяя указать количество отображаемых на каждой странице пользователей при представлении отчета в виде диаграммы.

Для открытия списка всех доступных пользователей домена щелкните кнопку «Пользователи» (см. Рисунок 4.114).

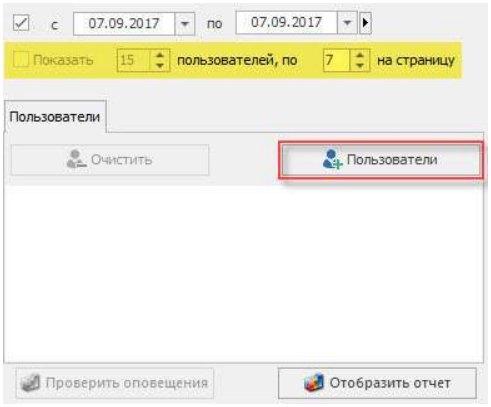


Рисунок 4.114

Выбор пользователей производится при помощи кнопок:

-  – для отдельных выделенных пользователей и групп,
-  – для пользователей и групп, входящих в состав выделенной группы.

Удаление пользователей из списка выбранных производится при помощи кнопок:

-  – для выделенных пользователей и групп,
-  – для всех добавленных в выборку пользователей и групп.

Также выбор и удаление пользователей можно производить двойным щелчком мыши по строке с именем необходимого пользователя. Подтверждение выбора производится с помощью кнопки «Применить» (см. Рисунок 4.115).

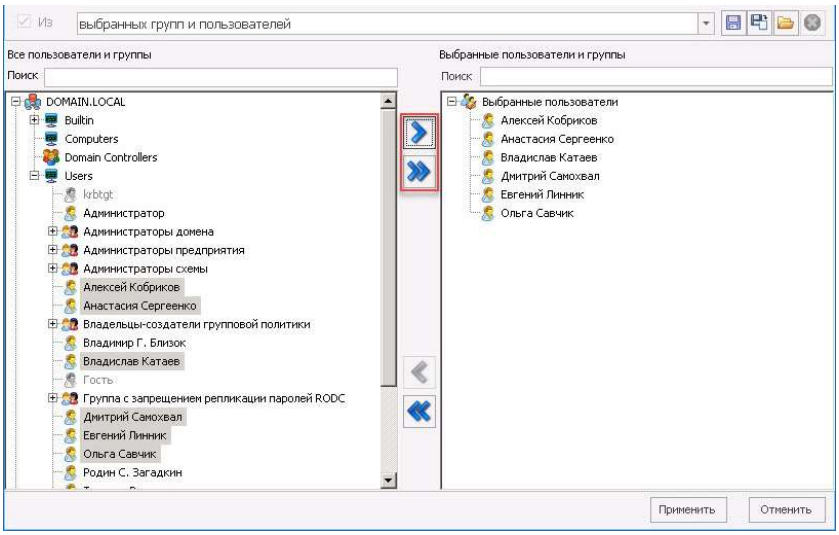


Рисунок 4.115

Для быстрого поиска по списку пользователей предусмотрено текстовое поле «Поиск». По мере ввода поискового запроса или комбинации букв совпадения, найденные в полях «имя», «фамилия» или «логин», отображаются в формате **<domain\user>**.

4.4.3.3 Выбор временного периода

AnalyticConsole позволят выбрать период времени, за который будет сгенерирован тот или иной отчет. По умолчанию отчеты формируются за все время; элементы настройки периода неактивны. Поэтому для указания конкретного временного периода нужно установить соответствующий флажок (см. Рисунок 4.116).

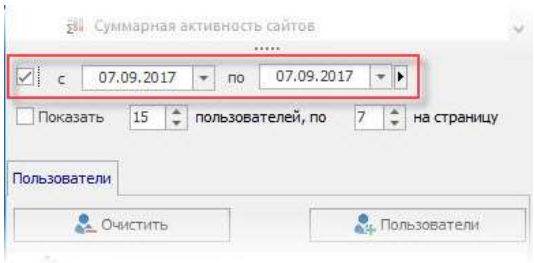


Рисунок 4.116

Кнопка служит для генерации отчета за предустановленный период (за предыдущие сутки, неделю, месяц, год) (см. Рисунок 4.117).

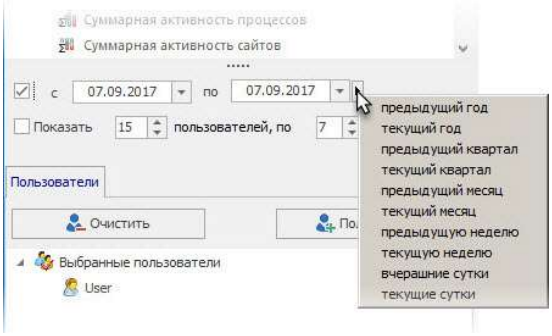


Рисунок 4.117

Для ввода произвольного периода времени введите начальную и конечную даты в формате (ДД-ММ-ГГГГ) или нажмите кнопку для вызова календаря (см. Рисунок 4.118).

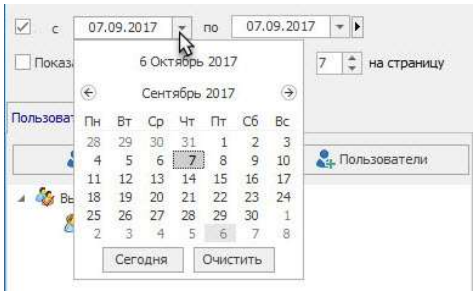


Рисунок 4.118

Отчет за указанный временной период будет отображен в окне просмотра при нажатии кнопки «Отобразить отчет» в нижней части консоли.

4.4.3.4 Отображение отчетов в окне просмотра

Переключение между режимами отображения

Отчет можно отобразить как таблицу (см. Рисунок 4.119), как диаграмму (см. Рисунок 4.120) и в виде графика (см. Рисунок 4.121). Для переключения между режимами воспользуйтесь выпадающим списком.


Количество сообщений пользователей по дням

Количество сообщений пользователей по дням за период с 11.12.2017 по 15.12.2017

	IMController		HTTPController		MailController		DeviceController	
	Объём	Кол-во	Объём	Кол-во	Объём	Кол-во	Объём	Кол-во
11.12.2017	15103	12	1256	2				
12.12.2017	5530	6	629	1	296567	2		
13.12.2017	15969	15	628	1				
14.12.2017					295506	1		
15.12.2017	5010	4					17920	
Итого:	41612	37	2513	4	592073	3	17920	

Рисунок 4.119

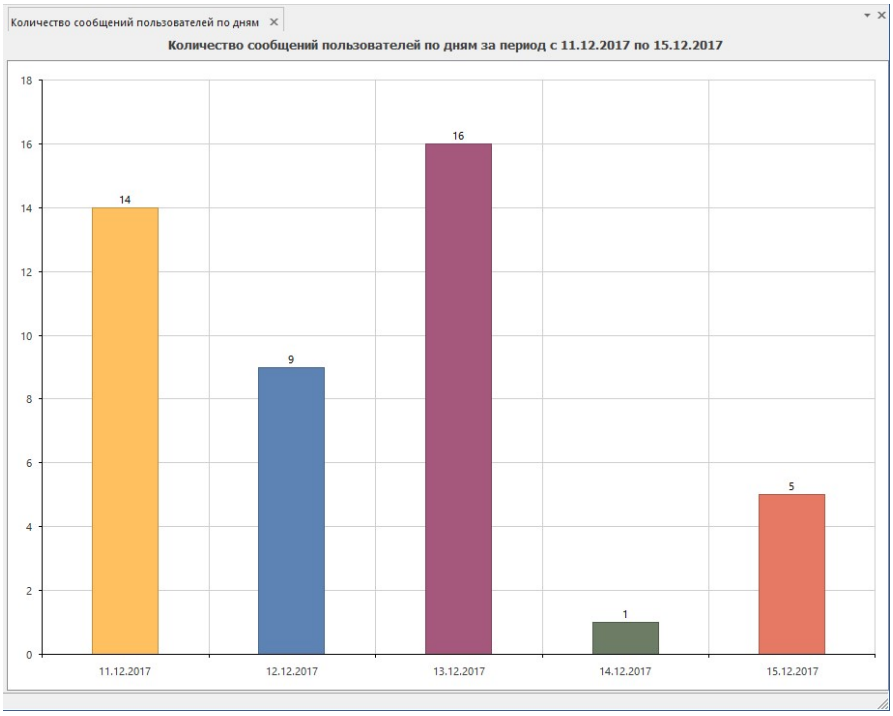


Рисунок 4.120

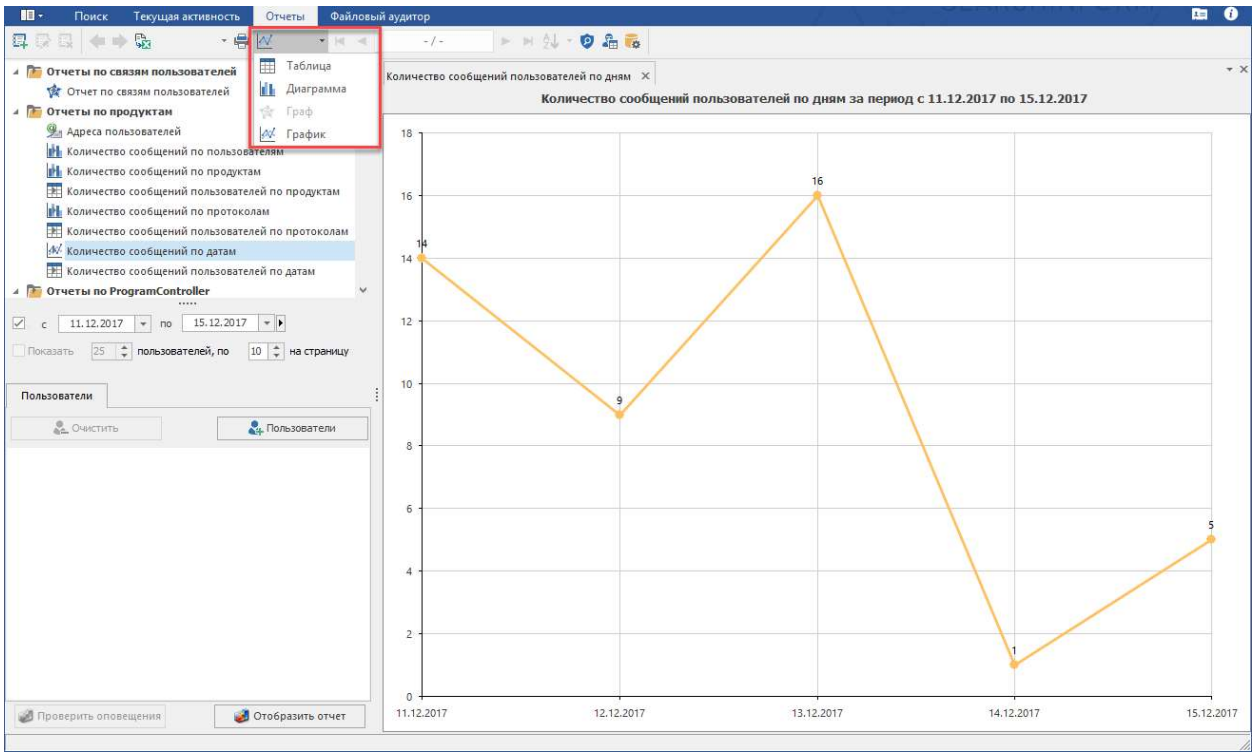


Рисунок 4.121

4.4.3.5 Представление данных в виде графа отношений

Отчет по связям пользователей может быть представлен в виде графа отношений, обладающего свойствами интерактивности. Для проверки отображения отчета в виде графа дважды щелкните типовой шаблон «Отчет по связям пользователей».

В окне просмотра отобразится отчет в виде графа отношений (см. Рисунок 4.122).

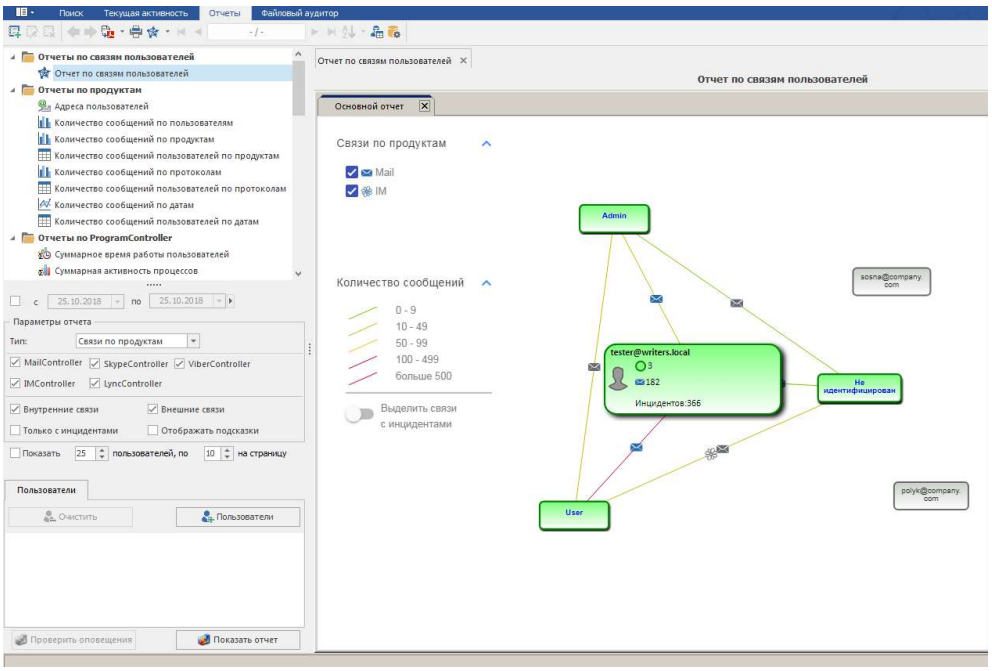


Рисунок 4.122

Расположение узлов и ребер графа отношений в окне просмотра отчетов изменяется с помощью мыши. При наведении указателя мыши на элементы графа отображается дополнительная информация в виде всплывающих подсказок.

4.4.3.6 Отображение отчетов ProgramController

Перечень стандартных отчетов по ProgramController:

- Отчет, отражающий суммарное время работы пользователей.
- Отчет по суммарной активности процессов, запускаемых пользователями.
- Отчет по суммарной активности сайтов (групп сайтов), посещаемых пользователями.
- Отчет по суммарной активности процессов (сайтов), запускаемых пользователями. Могут быть отображены как группы процессов, так и отдельные процессы или программы.
- Отчет по средней продолжительности рабочего дня пользователей.
- Отчет по среднесуточной активности процессов, запускаемых пользователями.
- Отчет по средней суточной активности сайтов (групп сайтов), посещаемых пользователями.
- Отчет по средней суточной активности процессов (сайтов), запускаемых пользователями.
- Отчет, представляющий собой детальную информацию по пользователям.
- Отчет «Продуктивность пользователей», позволяющий без детализаций и анализа оценить, насколько продуктивно работает тот или иной сотрудник.
- Отчет «Детальная продуктивность пользователей», отражающая продуктивность работы пользователей в развернутом виде.
- Отчет «Отсутствовавшие пользователи», позволяющий просматривать данные об отсутствовавших на работе пользователях за указанный период времени.
- Отчет «Опоздания сотрудников», представляющий собой отчет по поздним приходам пользователей на работу в течение заданного временного промежутка.
- Отчет «Ранние уходы», представляющий собой отчет по ранним уходам пользователей с работы в течение заданного промежутка времени.
- Отчет «Отсутствие перехвата», предназначенный для выявления отсутствия сбора данных продуктов ProgramController, Keylogger и MonitorController.

- Отчет «Промежутки неактивности», позволяющий увидеть, кто из пользователей и на протяжении которого времени в течение заданного рабочего дня не проявлял активность.
- Отчет, отображающий активность в приложениях и на веб-сайтах, соответствующих заданному заголовку программы.
- Отчет, представляющий собой оповещения, связанные с длительной работой пользователей в приложениях (нахождение на веб-сайтах), не связанных с рабочей деятельностью.
- Отчет «Журнал рабочего времени», позволяющий просматривать статистические данные рабочего времени выбранных пользователей за заданный период.
- Отчет, отображающий полную сводку активности пользователей в табличном виде.
- Отчет, отображающий информацию, связанную с недостаточной активностью пользователей в рабочее время.
- Отчет «Эффективность пользователей» включает в себя данные по нескольким отчетам ProgramController одновременно и на основании всех приведенных данных осуществляет подсчет эффективности работы пользователей в рамках заданного периода времени.
- Отчет «Показатель продуктивности пользователей», позволяющий отобразить пользователей, активность которых удовлетворяет заданным критериям продуктивности.
- Отчет «Сводная информация по пользователю» отображает информацию о процессах/сайтах, запускаемых/посещаемых пользователями в течение каждых суток, а также продолжительность работы в них.
- Отчет «Нарушения рабочего режима», позволяющий просматривать данные о нарушениях рабочего режима, таких как опоздания и низкая активность.
- Отчет «Посещения сотрудников», представляющий собой отчет по приходам и уходам пользователей в течение заданного промежутка времени.
- Отчет «Табель рабочего времени», представляющий собой свод информации по приходам, уходам и отработанном пользователями временем с работы в течение заданного временного промежутка.

Генерирование и рассылка оповещений по стандартным шаблонам не предусмотрена: для этого потребуется создать пользовательский шаблон отчета.

Настройка пользовательского шаблона отчета.

Зайдите в настройки программы (см. Рисунок 4.123).

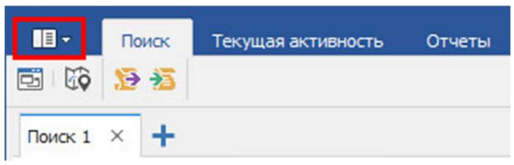


Рисунок 4.123

Перейдите на вкладку «Оповещения». Введите настройки SMTP-сервера: адрес отправителя, адрес сервера, номер SMTP-порта, имя пользователя и пароль. При необходимости шифровать отправляемые уведомления установите флажок «Использовать TLS соединение».

Корректность введенных параметров может быть проверена кнопкой «Проверить настройки». Сохраните изменения (см. Рисунок 4.124).

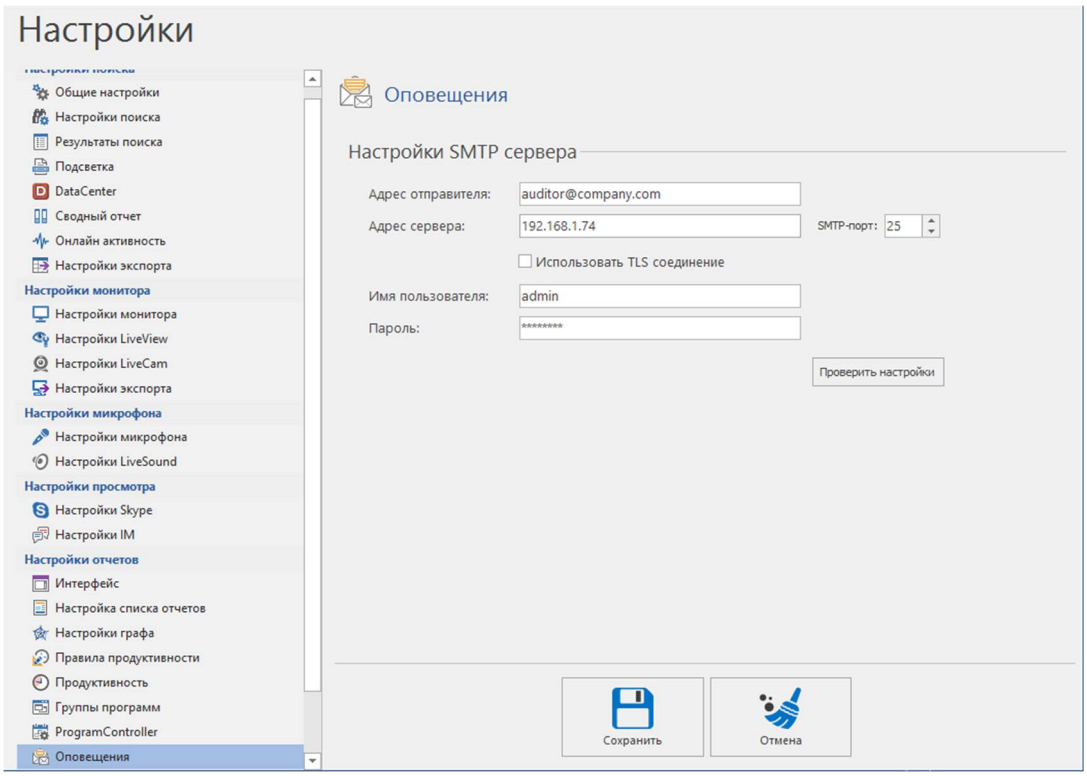


Рисунок 4.124

Для создания нового отчета щелкните кнопку «Создать» либо выберите команду «Создать отчет» из контекстного меню (см. Рисунок 4.125).

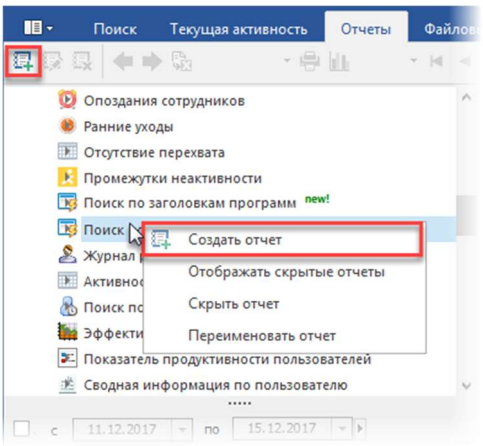


Рисунок 4.125

В окне Мастера отчетов выберите из перечня тип отчета, на основании которого будет создан новый шаблон отчета с функцией отправки оповещений. Переход к каждому последующему шагу настроек осуществляется нажатием кнопки «Далее».

На вкладке «Фильтры» укажите параметры фильтрации, которые будут использованы при построении отчета.

Выберите дополнительные параметры отображения отчета на соответствующей вкладке.

На вкладке «Вид отчета» для учета только рабочих часов отметьте соответствующий параметр.

Настройка оповещений пользовательских отчетов производится на вкладке «Параметры формирования». Отметьте флажком опцию «Автоматическая отправка по почте» и укажите критерии оповещения (см. Рисунок 4.126):

- название отчета;
- период формирования отчета;
- расписание рассылки оповещений;
- электронный адрес получателя оповещений, на который будут отправляться оповещения по данному отчету;
- для отправки оповещений даже в том случае, когда нарушений не было, отметьте соответствующий параметр флажком;
- выберите формат вложения, в котором отчет будет отправлен на указанный почтовый адрес.

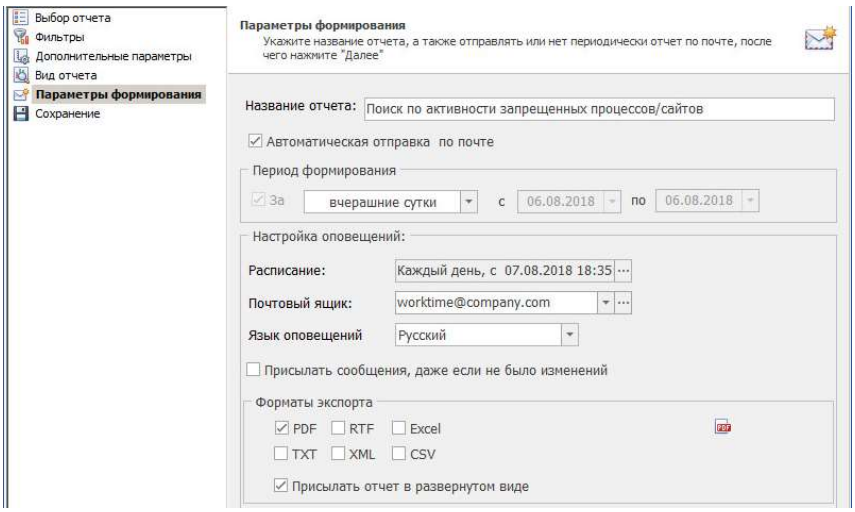


Рисунок 4.126

На вкладке «Сохранение» проверьте корректность заданных настроек и щелкните кнопку «Сохранить».

Созданный в данном примере отчет *Поиск по активности запрещенных процессов/сайтов* будет сохранен в группе отчетов «Оповещения».

Для просмотра оповещений по пользовательским отчетам сделайте двойной клик по требуемому отчету. Область просмотра отчетов будет разделена горизонтально на две части: в верхней части окна просмотра отображаются оповещения за определенный период времени, в нижней области – просмотр информации по выбранному оповещению (см. Рисунок 4.127).

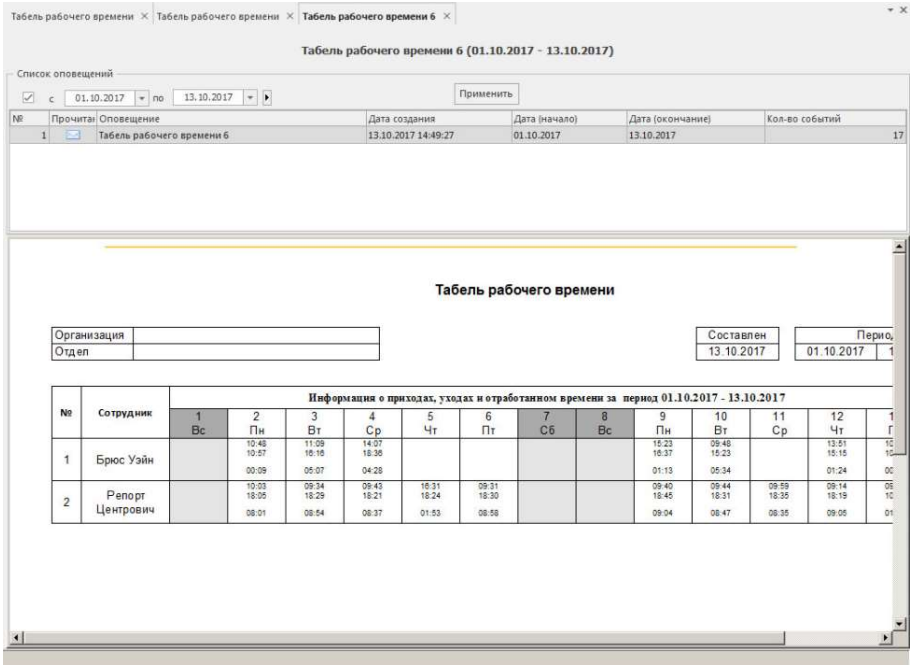


Рисунок 4.127

Оповещение, отправленное на электронную почту сотрудника службы безопасности, выглядит следующим образом (см. Рисунок 4.128):

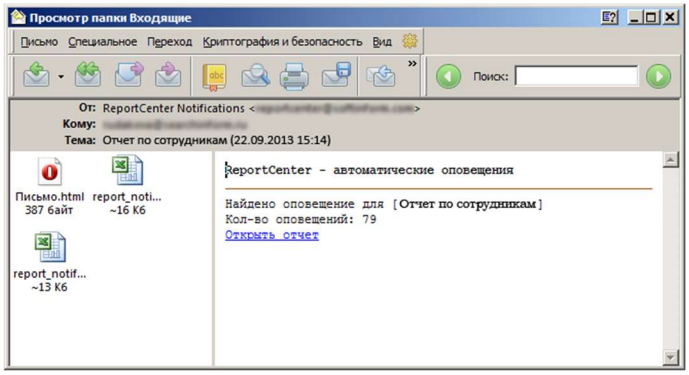


Рисунок 4.128

Содержимое вложенного файла см. Рисунок 4.129.

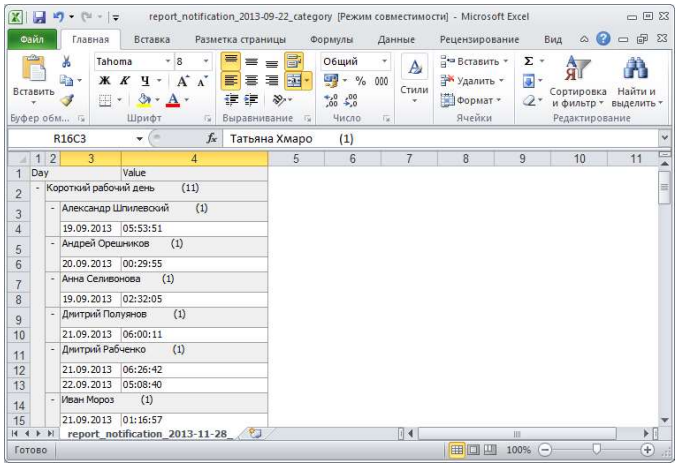


Рисунок 4.129

4.4.4 Файловый аудитор

Вкладка используется для просмотра файлов, полученных с помощью программного модуля FileAuditor[4], осуществляющего сканирование и анализ файлов на рабочих станциях, серверах, сетевых ресурсах.

Основные поисковые возможности:

- Поиск файлов по различным атрибутам: название файла/папки, размер, права доступа к файлу/папке, дата создания файла, дата перехвата и др.;
- Обзор дерева папок и файлов, хранящихся на рабочих станциях пользователей и общих сетевых ресурсах;

[4] Для использования FileAuditor не требуется установки дополнительного ПО, т.к. продукт является опциональной составляющей EndpoitController.

- Фильтрация результатов поиска по атрибутам файлов и/или пользователям;
- Возможность отследить историю изменений файлов, благодаря сохранению его последних редактируемых версий;
- Предпросмотр выбранного файла, прав доступа к файлу, операций с файлом.

Функционально окно вкладки **Файловый аудитор** разделено на несколько областей (см. Рисунок 4.130):

1. Панель фильтров используется для ограничения круга отображаемых файлов согласно заданным параметрам.

2. Панель результатов сканирования отображает дерево каталогов и файлов контролируемых рабочих станций и файловых серверов.

3. Панель журнала событий предоставляет информацию о последних сохраненных версиях выбранного файла, а также об операциях, производимых с ним.

4. Панель просмотра отображает содержимое выбранного файла, права доступа к файлу, операции с файлом.

5. Строка состояния содержит сведения об общем количестве загруженных элементов, время отображения дерева каталогов, количество элементов в дереве. Также позволяет изменить масштаб и режим просмотра файлов.

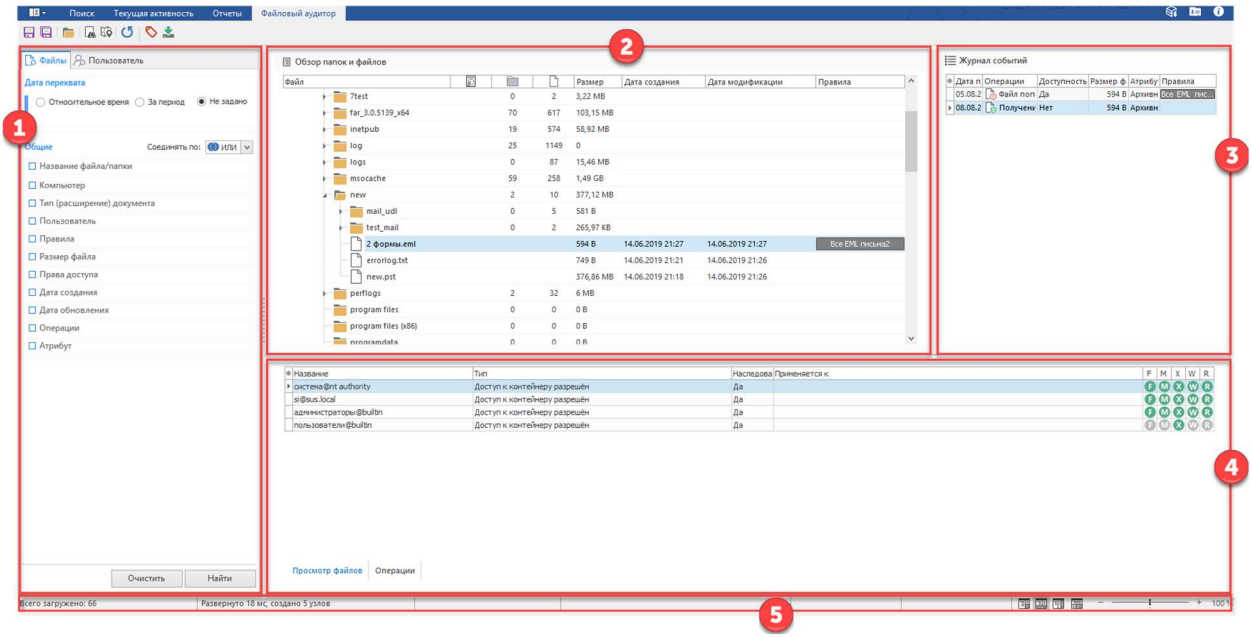


Рисунок 4.130

4.4.4.1 Вкладка «Файлы»

Панель фильтров содержит вкладки «Файлы» и «Пользователь».

Вкладка «**Файлы»** позволяет установить временной диапазон сканирования, а также настроить фильтры по следующим параметрам файлов (см. Рисунок 4.131):

- Название файла/папки;
- Имя компьютера/пользователя;
- Расширение документа;
- Название правила аудита;
- Размер файла;
- Права доступа к файлу/каталогу;
- Дата создания/обновления файла;
- Операции с файлом;
- Атрибуты файла.

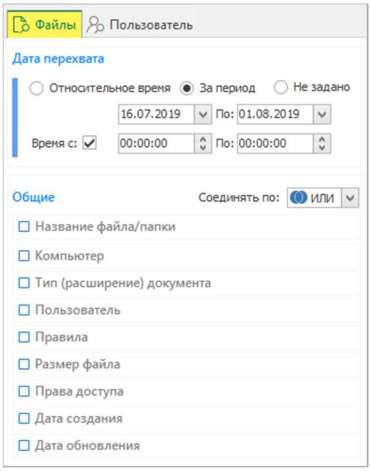


Рисунок 4.131

Для формирования условий фильтрации установите флажки перед наименованием параметров и задайте индивидуальные настройки в соответствии со значением того или иного параметра.

Значения параметров группы **Общие** могут быть объединены логическим оператором И/ИЛИ.

Ниже приведено описание некоторых параметров, при использовании которых следует иметь в виду их функциональные особенности. Настройка остальных фильтров производится в обычном порядке.

Параметр **Правила** предполагает ввод в текстовом поле наименования правила, сработавшего при сканировании документов[5] (см. Рисунок 4.132).

[5] Правила должны быть заданы в настройках FileAuditor в консоли EndpointController.

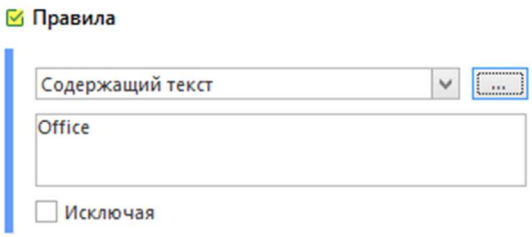


Рисунок 4.132

Установленный флаг «Исключая» означает, что файлы, относящиеся к указанному правилу, будут исключены из результатов фильтрации.

При активации параметра **Размер файла** есть возможность задать как диапазон, так и максимальное/минимальное или равное указанному значение, а также выбрать единицу измерения размера файла (см. Рисунок 4.133).

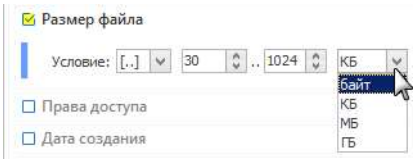


Рисунок 4.133

Параметр **Права доступа** содержит перечень прав доступа пользователя к файлу/каталогу (см. Рисунок 4.134). Одновременно может быть отмечено несколько значений.

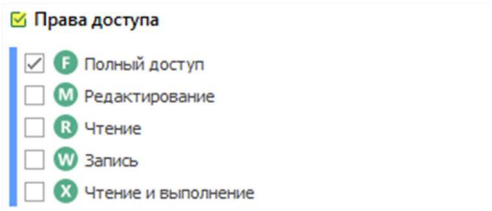


Рисунок 4.134

Параметр **Операции** содержит перечень операций, которые осуществлялись с файлом (см. Рисунок 4.135).

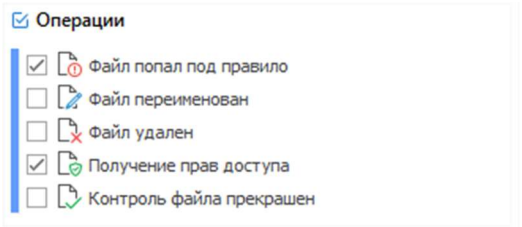


Рисунок 4.135

Параметр **Арибут** включает дополнительные атрибуты файла, относящие его к определенной категории: архивный, системный, скрытый, временный и др. (см. Рисунок 4.136).

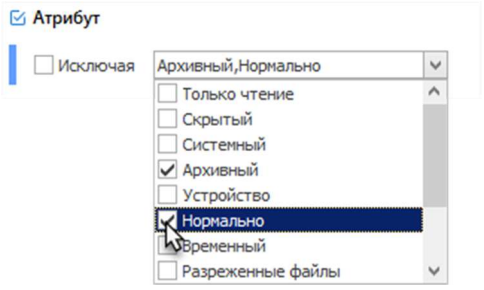


Рисунок 4.136

Установленный флаг «Исключая» означает, что файлы, относящиеся с выбранными атрибутами, будут исключены из результатов фильтрации.

4.4.4.2 Вкладка «Пользователь»

Фильтрацию можно осуществлять также по пользователям, которые работали с файлами.

На вкладке отображается список пользователей Active Directory. Выберите из списка необходимое имя пользователя. Если список достаточно длинный, то имя искомого пользователя можно указать вручную в текстовом поле «Введите текст для поиска» (см. Рисунок 4.137).

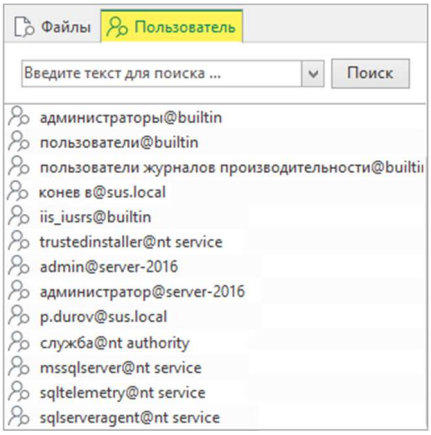


Рисунок 4.137

Важно! Фильтры разных вкладок не объединяются. Поэтому отображаются результаты с учетом фильтров только одной из вкладок: либо фильтры «Файлы» либо фильтры «Пользователь».

Установив необходимые для поиска фильтры, нажмите кнопку «Найти», расположенную в нижней части окна программы. Результаты поиска отобразятся на *Панели результатов* (см.Рисунок 4.138).

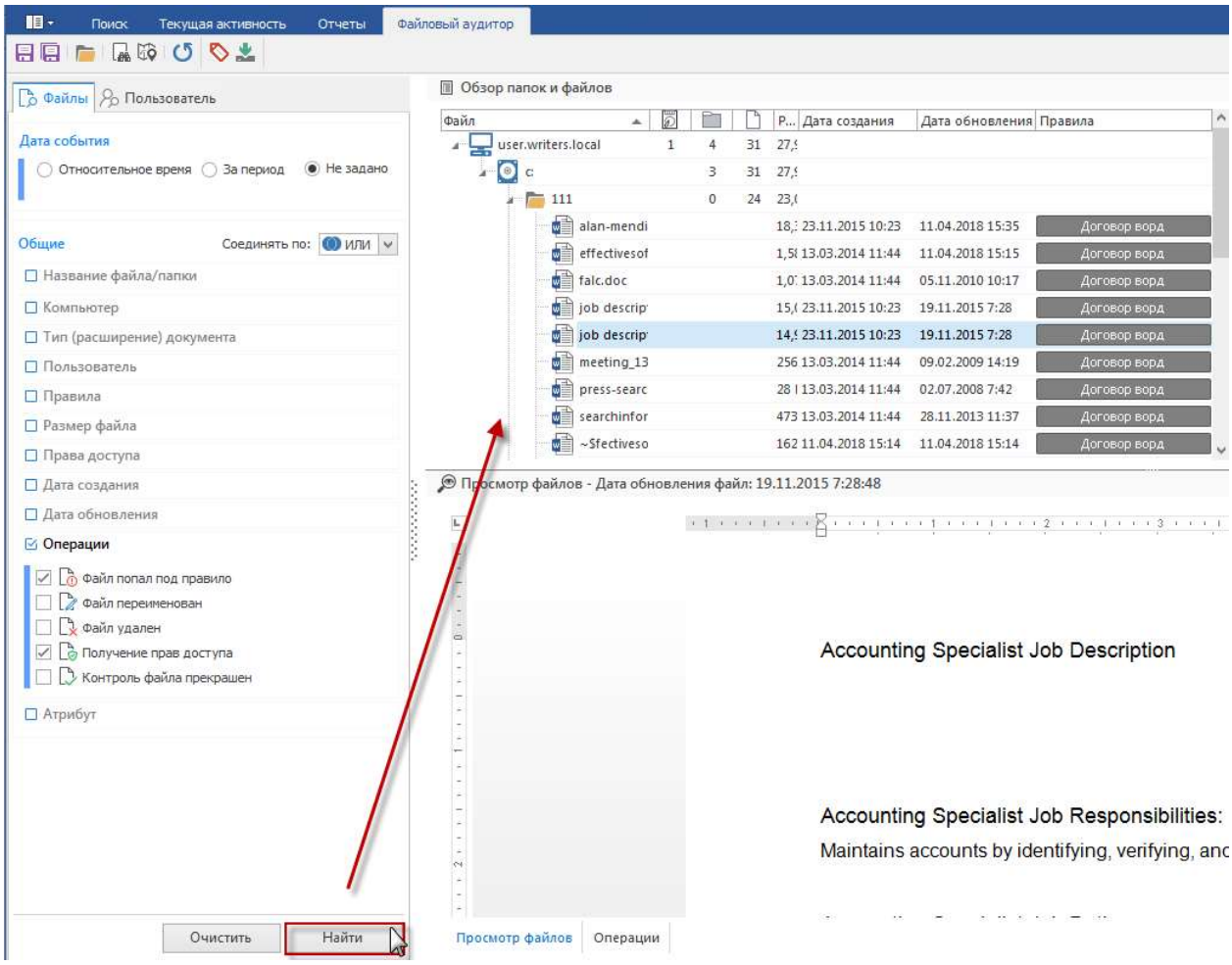


Рисунок 4.138

4.4.4.3 Панель результатов сканирования

Отображает структуру файловой системы: папки и файлы, обнаруженные в результате сканирования компьютеров пользователей и файловых серверов и удовлетворяющих условиям фильтрации.

Панель результатов содержит сведения о размере файлов; количестве вложенных в выбранную папку файлов; размер файла; дату его создания/модификации; правила, под которое попал файл (см. Рисунок 4.139).

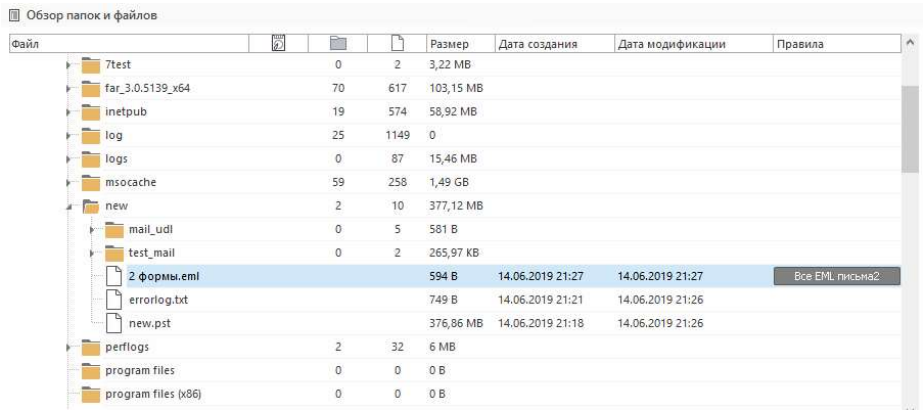


Рисунок 4.139

К выделенным файлам можно применить различные операции, используя функциональные кнопки, расположенные на панели инструментов (см. Рисунок 4.140).

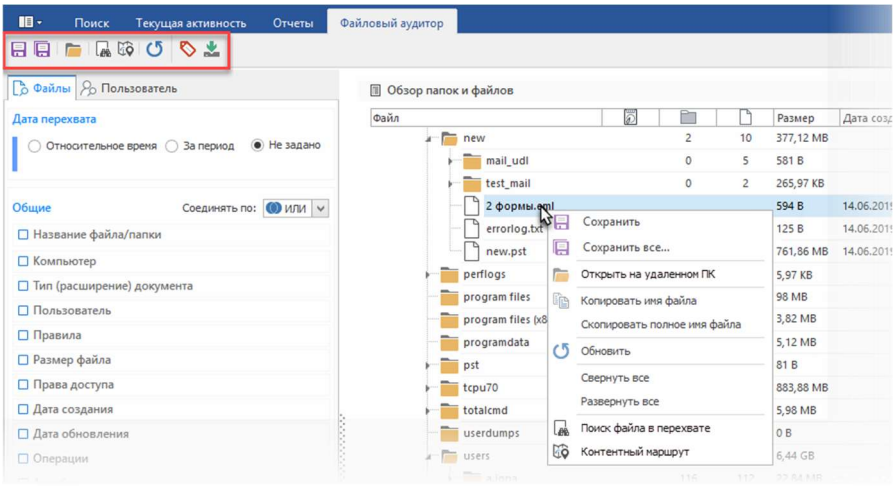


Рисунок 4.140

- сохранение выбранного файла в папку;
- сохранение всех файлов в папку;
- открытие выделенного документа на удаленном компьютере;
- поиск выбранного файла в перехвате (переход на вкладку «Поиск»);
- отображение контентного маршрута документа;
- обновление списка файлов;
- редактирование правил аудита (переход к «Настройкам» правил);
- экспорт результатов сканирования.

Некоторые операции из данного перечня могут быть вызваны также из контекстного меню файла.

4.4.4.3.1 Маркировка правил аудита

При выводе результатов аудита в столбце **Правила** событиям соответствует определенный цвет. Это удобно использовать для разграничения событий в зависимости от степени критичности информации, обнаруженной при сканировании файловой системы.

При необходимости цвет метки для каждого правила можно изменить в настройках AnalyticConsole.

Для этого нажмите кнопку редактирования правил аудита . Откроется окно настройки правил. Щелкните по цветной области в столбце «Цвет». Выберите новый цвет метки из списка стандартных цветов, кликнув , или воспользуйтесь редактором цветов, кликнув (см. Рисунок 4.141).

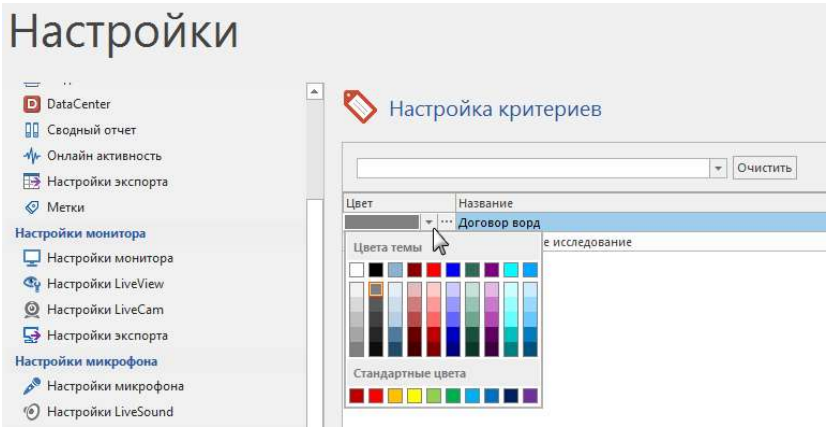


Рисунок 4.141

Сохраните изменения.

4.4.4.3.2 Экспорт данных

Результаты сканирования рабочих станций и файловых серверов, а также копии найденных документов можно экспортировать в файл с помощью кнопки «Экспорт» на панели инструментов (см. Рисунок 4.142).

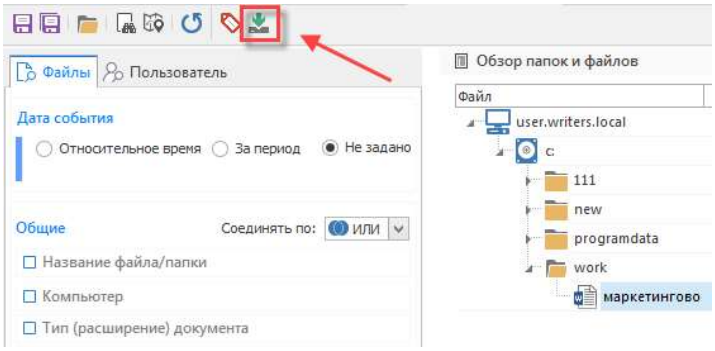


Рисунок 4.142

При экспорте файлов и документов укажите путь к папке, в которую будет помещен экспортируемый файл (в текстовом поле или с помощью обозревателя папок), введите имя экспортируемого файла и выберите его тип из выпадающего списка (см. Рисунок 4.143).

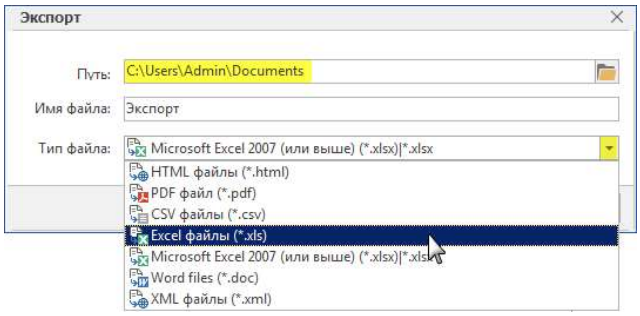


Рисунок 4.143

Кликните «ОК».

По завершении экспорта в нижней части окна появится сообщение «'Экспорт завершен». Для просмотра документа в сопоставленном операционной системой приложении выберите команду «Открыть документ» (см. Рисунок 4.144).

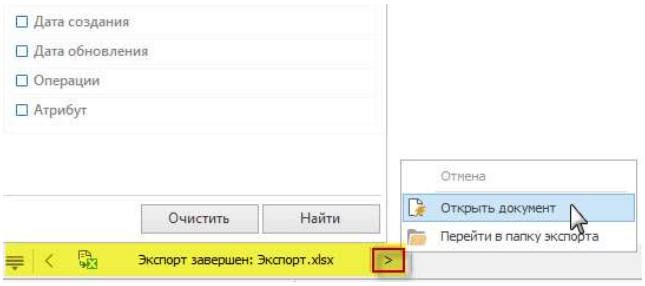


Рисунок 4.144

4.4.4.4 Панель журнала событий

Журнал событий содержит список последних зарегистрированных версий файла, выбранного на панели результатов, а также операции с этим файлом.

С помощью журнала событий возможно отследить изменения и операции, которые происходили с файлом в разные временные периоды; установить, менялся ли его размер, атрибуты и правила, согласно которым файл был обнаружен (см. Рисунок 4.145).

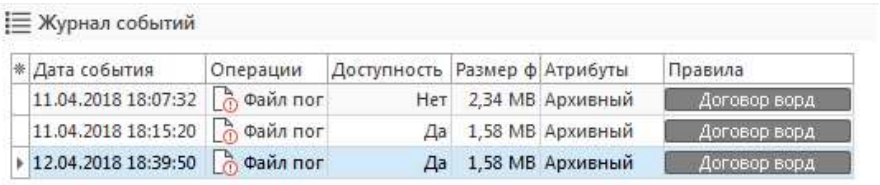


Рисунок 4.145

Перечень отображаемых операций[6]:

- Файл попал под правило;
- Файл переименован;
- Файл удален;
- Получение прав доступа;
- Контроль файла прекращен.

Количество и состав заголовков столбцов на панели журнала событий опционально может меняться с помощью вызова специального меню. Для этого щелкните заголовок крайнего левого столбца и отметьте необходимые для отображения столбцы (см. Рисунок 4.146).

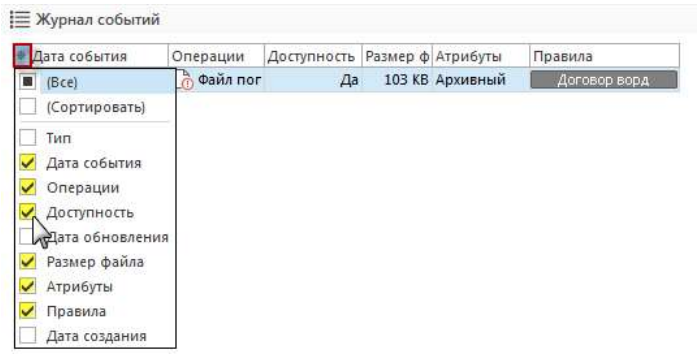


Рисунок 4.146

Очередность следования столбцов также можно изменить, перетаскивая ячейки с названиями столбцов между собой (см. Рисунок 4.147).

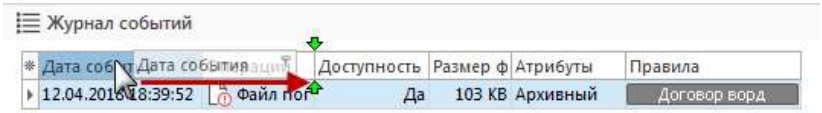


Рисунок 4.147

Из контекстного меню для файла могут быть вызваны следующие операции (см. Рисунок 4.148):

- **Сохранить** – сохраняет выбранную версию файла в папку;
- **Поиск файла в перехвате** – осуществляется переход на вкладку «Поиск» для просмотра детальной информации по файлу;
- **Контентный маршрут** – позволяет отобразить контентный маршрут выбранной версии документа;

[6] Полный перечень операций, производимых с файлом, доступен на панели предварительного просмотра.

- **Вписать таблицу в размер окна** – позволяет автоматически выровнять ширину столбцов согласно размеру панели журнала событий.

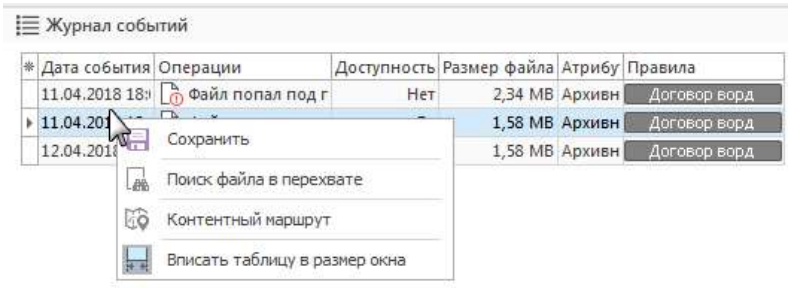


Рисунок 4.148

4.4.4.5 Панель просмотра

Позволяет просмотреть содержимое документа в родном формате, а также операции, совершенные с файлом.

На вкладке «Просмотр файлов» отображается содержимое документа, выбранного из списка результатов поиска (см. Рисунок 4.149):

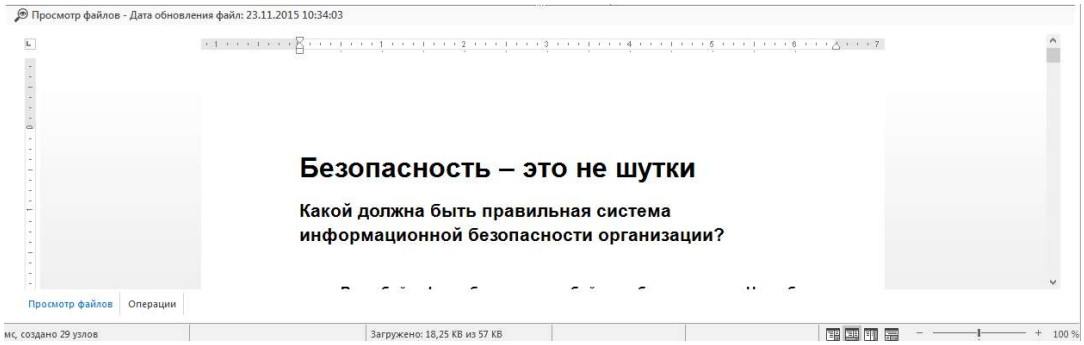


Рисунок 4.149

В случае получения прав доступа к файлу, будет отображаться также перечень выданных прав (см. Рисунок 4.150).

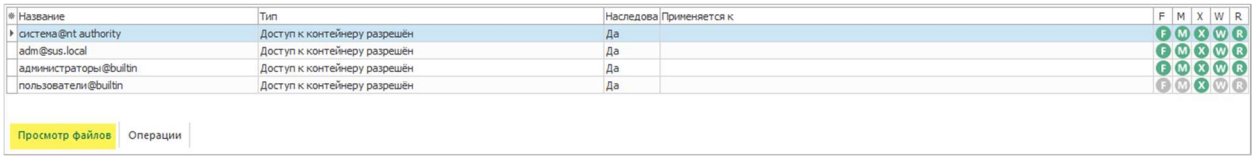


Рисунок 4.150

На вкладке «Операции» отображается ***полный перечень операций,*** которые совершали пользователи с файлами (чтение, создание, изменение, удаление, переименование и др.).

Просмотр операций и атрибутов с файлом возможен благодаря вычитке информации из базы данных модуля FileController (см. Рисунок 4.151).

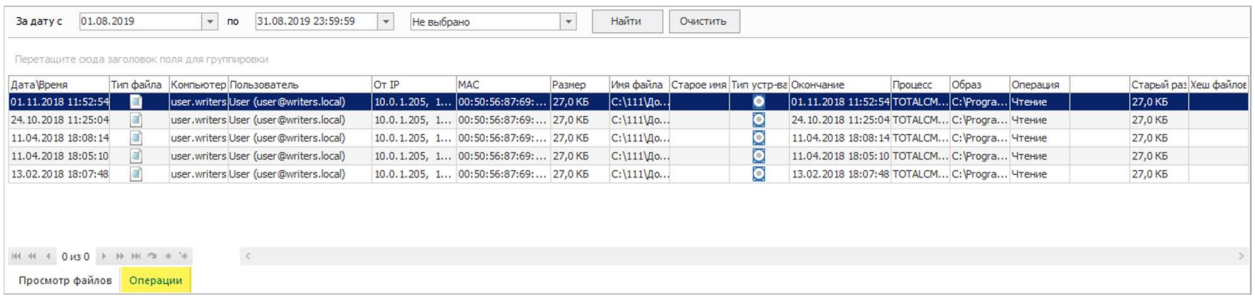


Рисунок 4.151

4.4.4.6 Режим просмотра

В зависимости от того, какой режим просмотра выбран, можно поменять расположение панелей окна «Файловый аудитор» относительно друг друга.

Для изменения режима просмотра щелкните одну из иконок в строке состояния (см. Рисунок 4.152):

- - компактный режим просмотра (панель просмотра файлов расположена в правом нижнем углу);
- - панель просмотра файлов расположена снизу;
- - панель просмотра файлов расположена справа;
- - панель просмотра файлов и панель журнала событий расположены снизу.

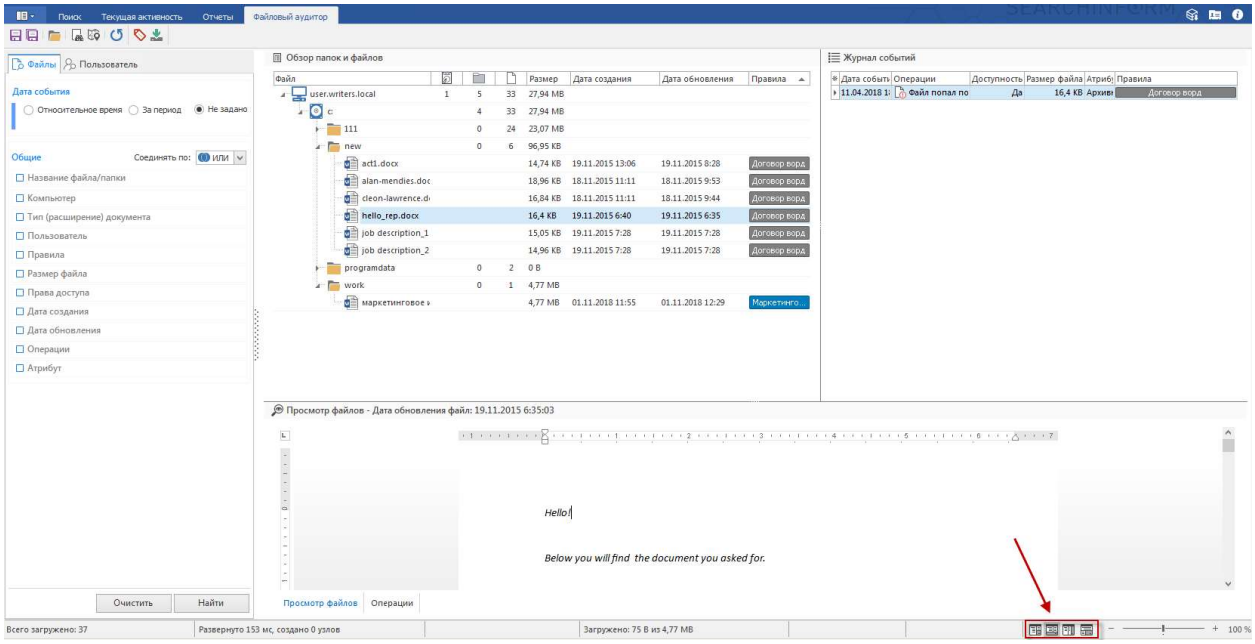


Рисунок 4.152

Также в строке состояния отображается:

- общее количество загруженных с сервера документов;
- время, затраченное системой на отрисовку дерева каталогов;
- размер загруженных файлов относительно общего объема загрузки;

- шкала изменения масштаба при отображении панелей.

4.4.5 Вкладка «Database Monitor»

Вкладка предназначена для просмотра запросов пользователей к базам данных SQL и ответам на них. Статистическая информация по SQL-запросам, перехваченным модулем «Database Monitor», представлена в виде 6 виджетов:

- Объем запросов;
- ТОП-10 по количеству запросов;
- Количество строк;
- Типы операций;
- Время выполнения запросов;
- Запросы к БД (успешные/неуспешные).

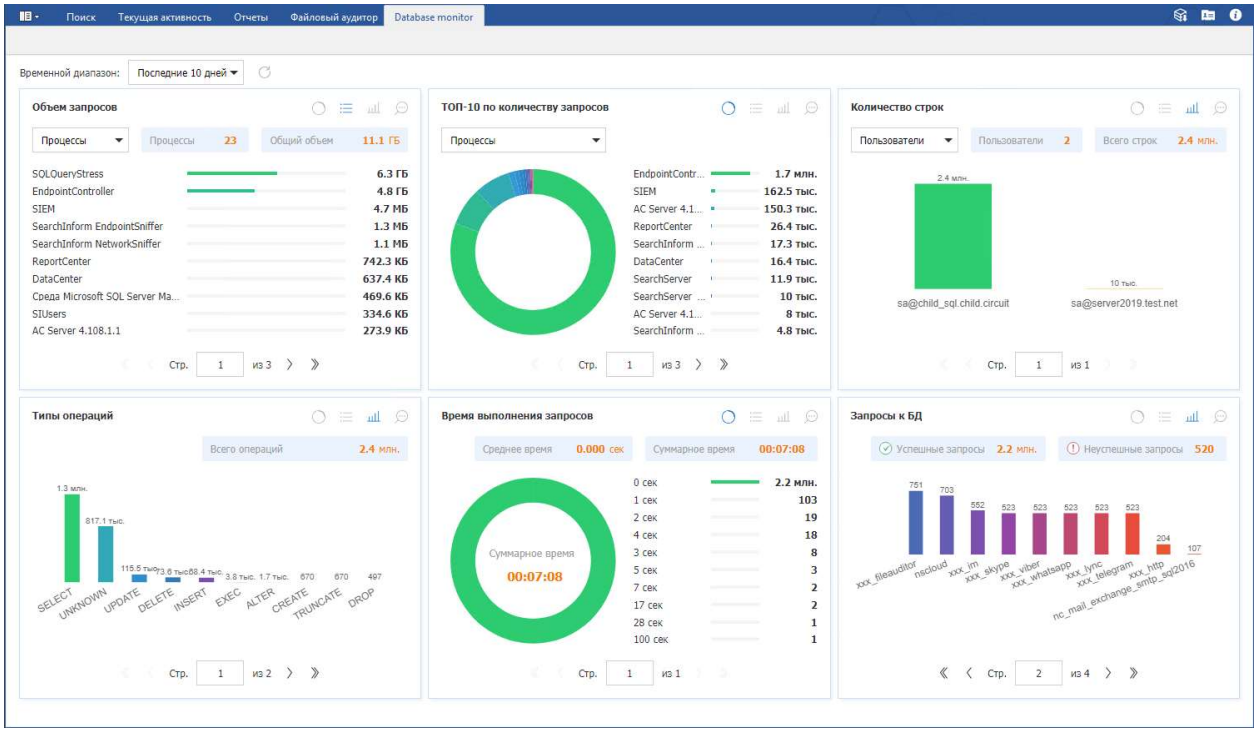


Рисунок 4.153

Параметр «Временной диапазон» позволяет выбрать период, за который будет выведена информация в виджетах (см. Рисунок 4.154).

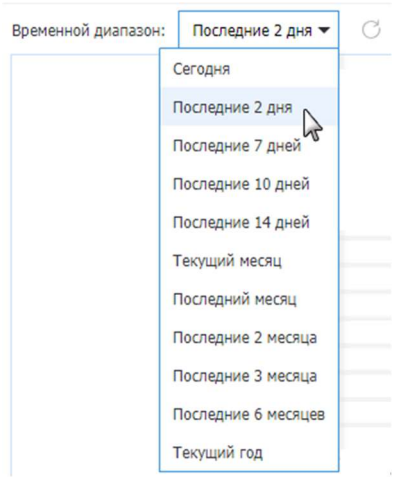


Рисунок 4.154

Есть возможность изменять способ представления данных в виджетах. Для этого используйте кнопки, расположенные справа от названия виджета:

- круговая диаграмма (см. Рисунок 4.155);

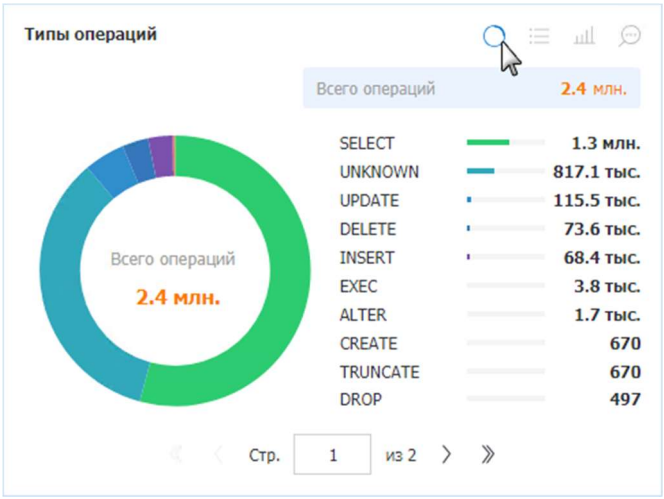


Рисунок 4.155

- строковая диаграмма (см. Рисунок 4.156);

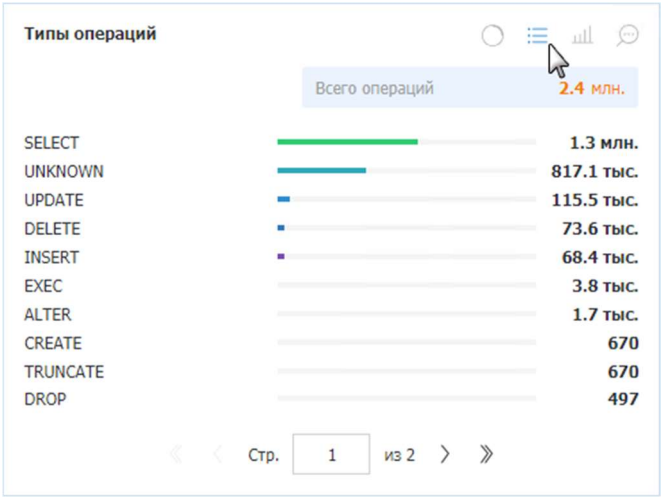


Рисунок 4.156

- гистограмма (см. Рисунок 4.157).

Рисунок 4.157

5 ИСТОЧНИКИ РАЗРАБОТКИ

Документы, на основании которых разработано данное руководство, а также на основании которых должно производиться выполнение работ:

1. РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов.
2. ГОСТ 2.503-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Правила внесения изменений.
3. ГОСТ 2.105-95 Общие требования к текстовым документам.
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».