Построение системы защиты данных на базе СУБД Постгрес.

Целесообразность, решаемые задачи.

Леонид Чуриков

Ведущий аналитик

SEARCHINFORM

INFORMATION SECURITY

Почему стоит использовать отечественную СУБД

- **По закону**.
- Для защиты данных по закону годятся только отечественные СУБД
- 2015 ПП №1236 (нет доступа к закупкам)
- 2016 РП №1588 (план перехода)
- 2019 Приказ Минцифры №184 (методичка по переходу)
- 2022 Указы Президента №250 и №166

(запрет закупки и с 2025г - использования)

Почему стоит использовать отечественную СУБД

- **По оформлению**.
- Легально купить иностранные СУБД (например MS SQL) в России сейчас нельзя

Почему стоит использовать отечественную СУБД

- **По карману**.
- Лицензирование иностранных СУБД таково, что сильно удорожает защиту
- (Стоимость ИБ-проекта возрастает в разы или на порядки)

Почему стоит использовать отечественную СУБД

- **По быстродействию**.
- Оно зависит от оптимизации СЗИ, а их разрабатывают сегодня под отечественные СУБД

- (Почему? По закону!)

Почему стоит использовать отечественную СУБД

- **По жизни**
- В конце прошлого года мы перенесли ИБ-решения на отечественные СУБД и…
- Все работает! Все, что в жизни нужно безопаснику!

- *Поиск*
- *Перехват*
- *Блокировки*
- *Аналитика*

Внутренний нарушитель

SEARCHINFORM
INFORMATION SECURITY

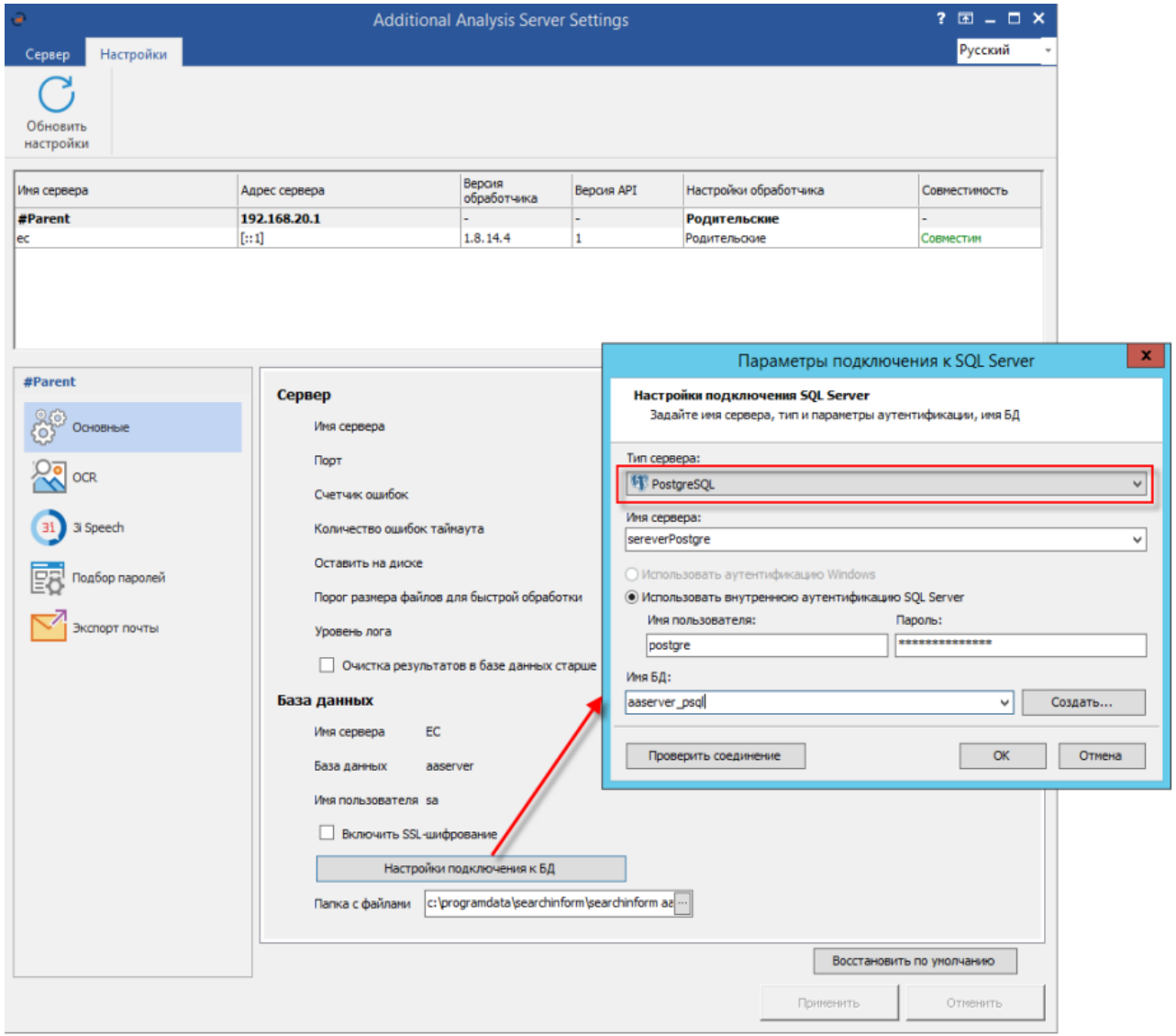
Механика инцидента

Данные могут быть выгружены из базы

Скопированы и сохранены в виде файла

Файл может быть отправлен за пределы организации

Право выбора

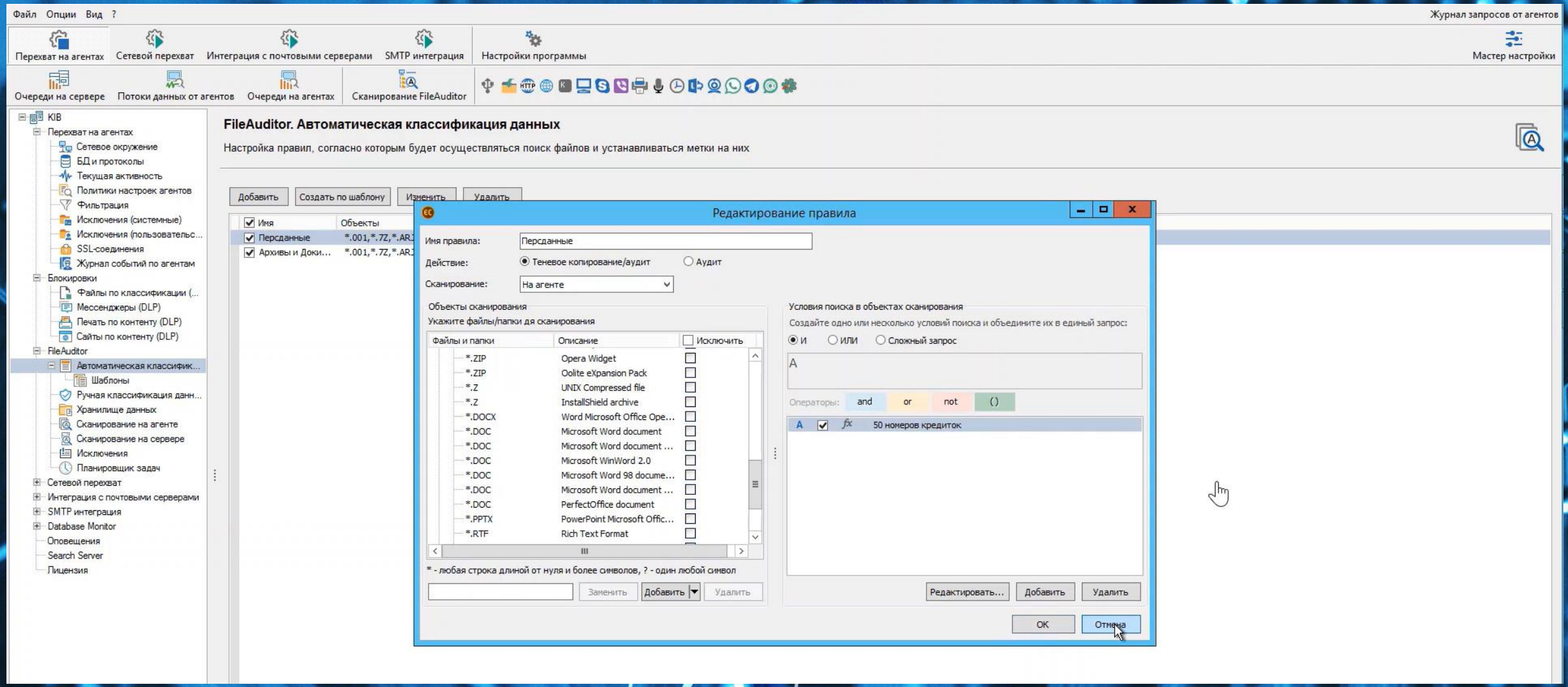


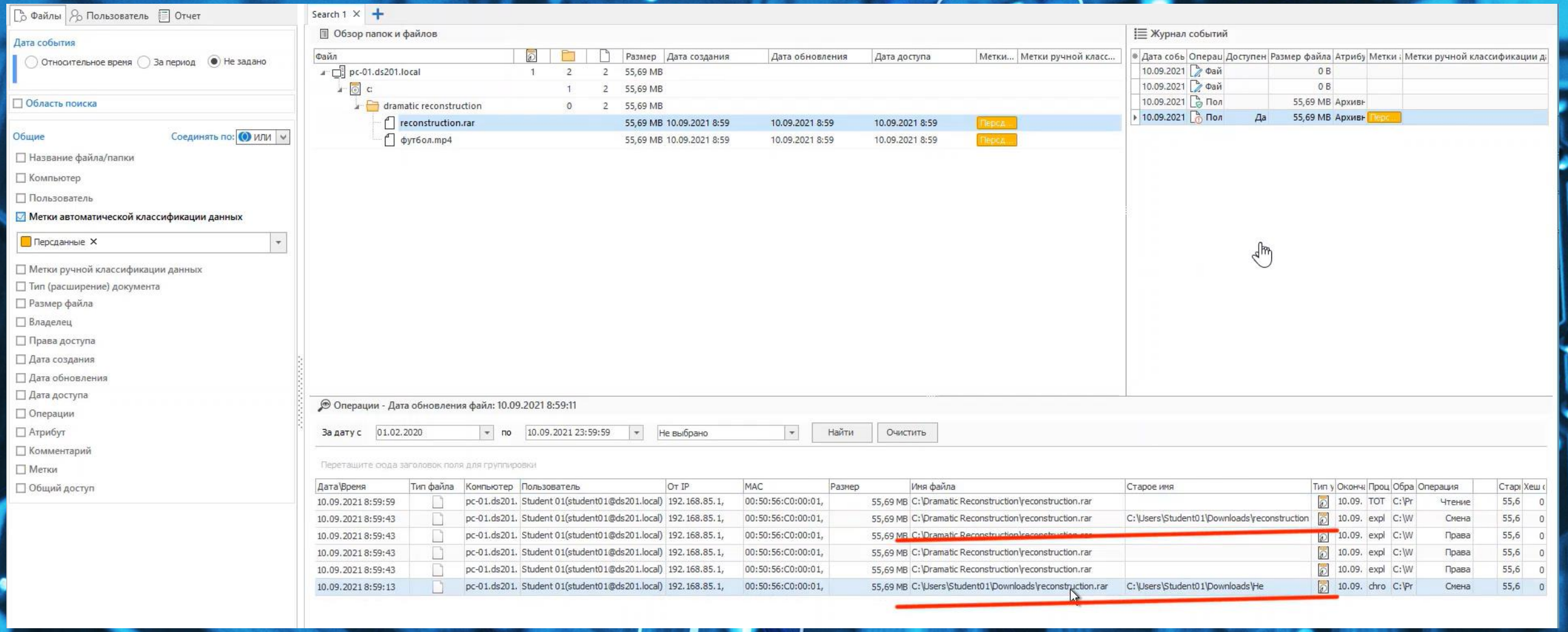
Поиск

- Для модуля FileAuditor (DCAP) реализована возможность осуществлять поиск по базам данных под управлением PostgreSQL.
- Индексация данных из баз PostgreSQL: Поддержана индексация данных, хранящихся в БД под управлением СУБД PostgreSQL, следующих источников: Облако; HTTP POST; FileAuditor; Почта; Монитор; Мессенджеры.

Перехват

- Запись перехваченных данных в базы данных под управлением СУБД PostgreSQL для следующих модулей:
- FileAuditor; CloudController; FTPController; HTTPController; IMController; MailController; сетевого перехвата; а также данных, полученных при почтовой и SMTP-интеграциях.
- Возможность создавать БД под управлением СУБД PostgreSQL для любого модуля перехвата в окне Мастер настройки EndpointController.


Файл Опции Вид ?
Журнал запросов от агентов
Перехват на агентах
Сетевой перехват
Интеграция с почтовыми серверами
SMTP интеграция
Настройки программы
Мастер настройки
Очереди на сервере
Потоки данных от агентов
Очереди на агентах
Сканирование FileAuditor
KIB
Перехват на агентах
Сетевое окружение
БД и протоколы
Текущая активность
Политики настроек агентов
Фильтрация
Исключения (системные)
Исключения (пользовательс...
SSL-соединения
Журнал событий по агентам
Блокировки
Файлы по классификации (...
Мессенджеры (DLP)
Печать по контенту (DLP)
Сайты по контенту (DLP)
FileAuditor
Автоматическая классифик...
Шаблоны
Ручная классификация данн...
Хранилище данных
Сканирование на агенте
Сканирование на сервере
Исключения
Планировщик задач
Сетевой перехват
Интеграция с почтовыми серверами
SMTP интеграция
Database Monitor
Оповещения
Search Server
Лицензия
FileAuditor. Автоматическая классификация данных
Настройка правил, согласно которым будет осуществляться поиск файлов и устанавливаться метки на них
Добавить
Создать по шаблону
Изменить
Удалить
Имя
Объекты
Персданные
.001,.7Z,*.AR
Архивы и Доки...
.001,.7Z,*.AR
Редактирование правила
Имя правила:
Персданные
Действие:
Теневое копирование/аудит
Аудит
Сканирование:
На агенте
Объекты сканирования
Укажите файлы/папки дя сканирования
Файлы и папки
Описание
Исключить
*.ZIP
Opera Widget
*.ZIP
Oolite eXpansion Pack
*.Z
UNIX Compressed file
*.Z
InstallShield archive
*.DOCX
Word Microsoft Office Ope...
*.DOC
Microsoft Word document
*.DOC
Microsoft Word document ...
*.DOC
Microsoft WinWord 2.0
*.DOC
Microsoft Word 98 docume...
*.DOC
Microsoft Word document ...
*.DOC
PerfectOffice document
*.PPTX
PowerPoint Microsoft Offic...
*.RTF
Rich Text Format
* - любая строка длиной от нуля и более символов, ? - один любой символ
Заменить
Добавить
Удалить
Условия поиска в объектах сканирования
Создайте одно или несколько условий поиска и объедините их в единый запрос:
И
ИЛИ
Сложный запрос
A
Операторы:
and
or
not
()
A
50 номеров кредиток
Редактировать...
Добавить
Удалить
OK
Отмена


Файлы
Пользователь
Отчет
Search 1
Дата события
Относительное время
За период
Не задано
Область поиска
Общие
Соединять по: ИЛИ
Название файла/папки
Компьютер
Пользователь
Метки автоматической классификации данных
Персданные
Метки ручной классификации данных
Тип (расширение) документа
Размер файла
Владелец
Права доступа
Дата создания
Дата обновления
Дата доступа
Операции
Атрибут
Комментарий
Метки
Общий доступ
Обзор папок и файлов
Файл
Размер
Дата создания
Дата обновления
Дата доступа
Метки...
Метки ручной класс...
pc-01.ds201.local
c:
dramatic reconstruction
reconstruction.rar
55,69 MB 10.09.2021 8:59 10.09.2021 8:59 10.09.2021 8:59
футбол.mp4
55,69 MB 10.09.2021 8:59 10.09.2021 8:59 10.09.2021 8:59
Журнал событий
Дата собь
Операц
Доступен
Размер файла
Атрибу
Метки
Метки ручной классификации да
10.09.2021 0 B
10.09.2021 0 B
10.09.2021 55,69 MB
10.09.2021 Да 55,69 MB
Операции - Дата обновления файл: 10.09.2021 8:59:11
За дату с 01.02.2020 по 10.09.2021 23:59:59 Не выбрано Найти Очистить
Перетащите сюда заголовок поля для группировки
Дата\Время
Тип файла
Компьютер
Пользователь
От IP
MAC
Размер
Имя файла
Старое имя
Операция
10.09.2021 8:59:59 pc-01.ds201. Student 01(student01@ds201.local) 192.168.85.1, 00:50:56:C0:00:01, 55,69 MB C:\Dramatic Reconstruction\reconstruction.rar Чтение
10.09.2021 8:59:43 pc-01.ds201. Student 01(student01@ds201.local) 192.168.85.1, 00:50:56:C0:00:01, 55,69 MB C:\Dramatic Reconstruction\reconstruction.rar C:\Users\Student01\Downloads\reconstruction Смена
10.09.2021 8:59:43 pc-01.ds201. Student 01(student01@ds201.local) 192.168.85.1, 00:50:56:C0:00:01, 55,69 MB Права
10.09.2021 8:59:43 pc-01.ds201. Student 01(student01@ds201.local) 192.168.85.1, 00:50:56:C0:00:01, 55,69 MB C:\Dramatic Reconstruction\reconstruction.rar Права
10.09.2021 8:59:43 pc-01.ds201. Student 01(student01@ds201.local) 192.168.85.1, 00:50:56:C0:00:01, 55,69 MB C:\Dramatic Reconstruction\reconstruction.rar Права
10.09.2021 8:59:13 pc-01.ds201. Student 01(student01@ds201.local) 192.168.85.1, 00:50:56:C0:00:01, 55,69 MB C:\Users\Student01\Downloads\reconstruction.rar C:\Users\Student01\Downloads\Не Смена

Файлы | Пользователь | Отчет

Search 1

Дата события

Относительное время | За период | Не задано

Область поиска

Общие — Соединять по: ИЛИ

- Название файла/папки
- Компьютер
- Пользователь
- Метки автоматической классификации данных

Архивы и Доки под паролем

- Метки ручной классификации данных
- Тип (расширение) документа
- Размер файла
- Владелец
- Права доступа
- Дата создания
- Дата обновления
- Дата доступа
- Операции
- Атрибут
- Комментарий
- Метки
- Общий доступ

Обзор папок и файлов

Файл				Размер	Дата создания	Дата обновления	Дата доступа	Метки...	Метки ручной класс...
pc-01.ds201.local	1	2	6	35,69 MB					
c:		1	6	35,69 MB					
dramatic reconstruction		0	6	35,69 MB					
футбол.part1.rar				10 MB	10.09.2021 9:00	10.09.2021 9:00	10.09.2021 9:00	Архив...	
футбол.part2.rar				0 B	10.09.2021 9:00	10.09.2021 9:00	10.09.2021 9:00	Архив...	
футбол.part3.rar				10 MB	10.09.2021 9:00	10.09.2021 9:00	10.09.2021 9:00	Архив...	
футбол.part4.rar				10 MB	10.09.2021 9:00	10.09.2021 9:00	10.09.2021 9:00	Архив...	
футбол.part5.rar				10 MB	10.09.2021 9:00	10.09.2021 9:00	10.09.2021 9:00	Архив...	
футбол.part6.rar				5,69 MB	10.09.2021 9:00	10.09.2021 9:00	10.09.2021 9:00	Архив...	

Журнал событий

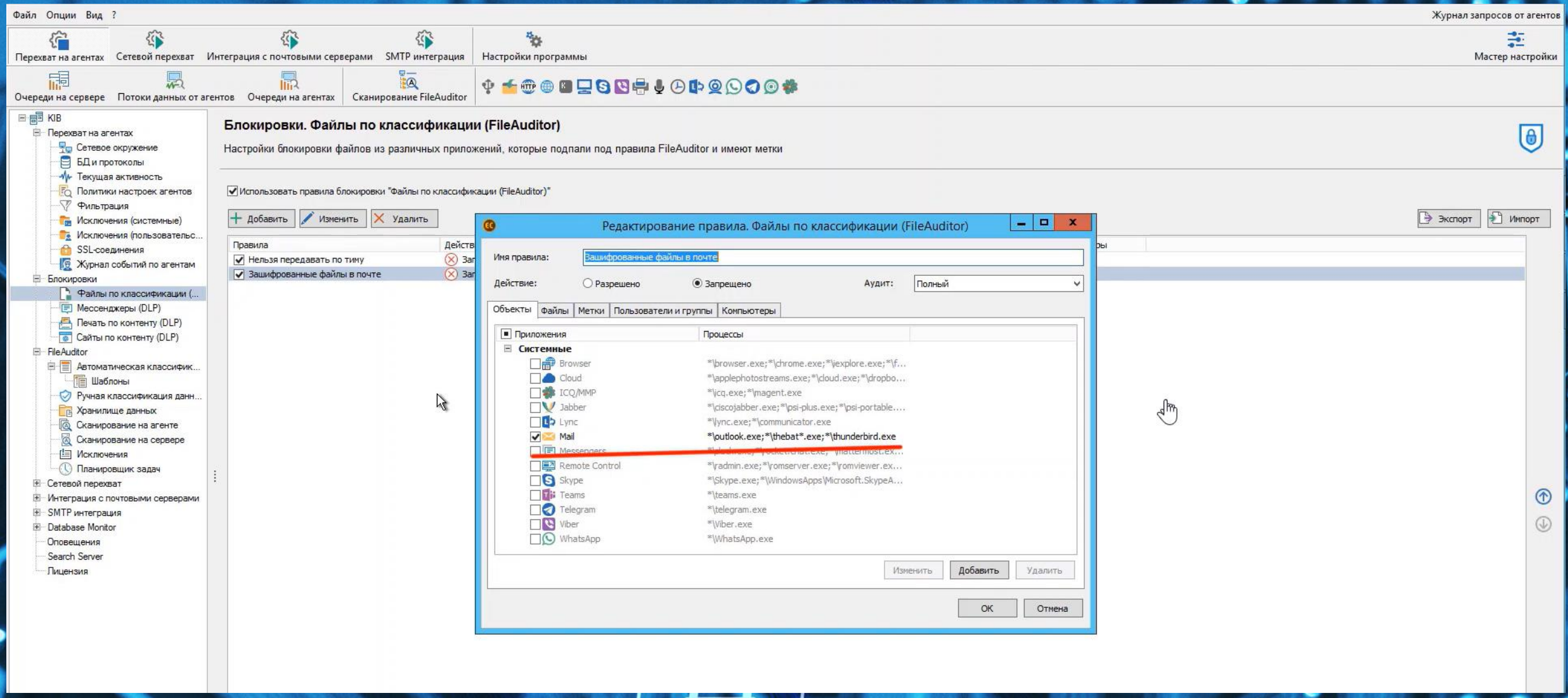
Дата собь	Операц	Доступен	Размер файла	Атрибу	Метки	Метки ручной классификации да
10.09.2021	Фай		0 B			
10.09.2021	Пол	Да	10 MB	Архивн	Архи...	

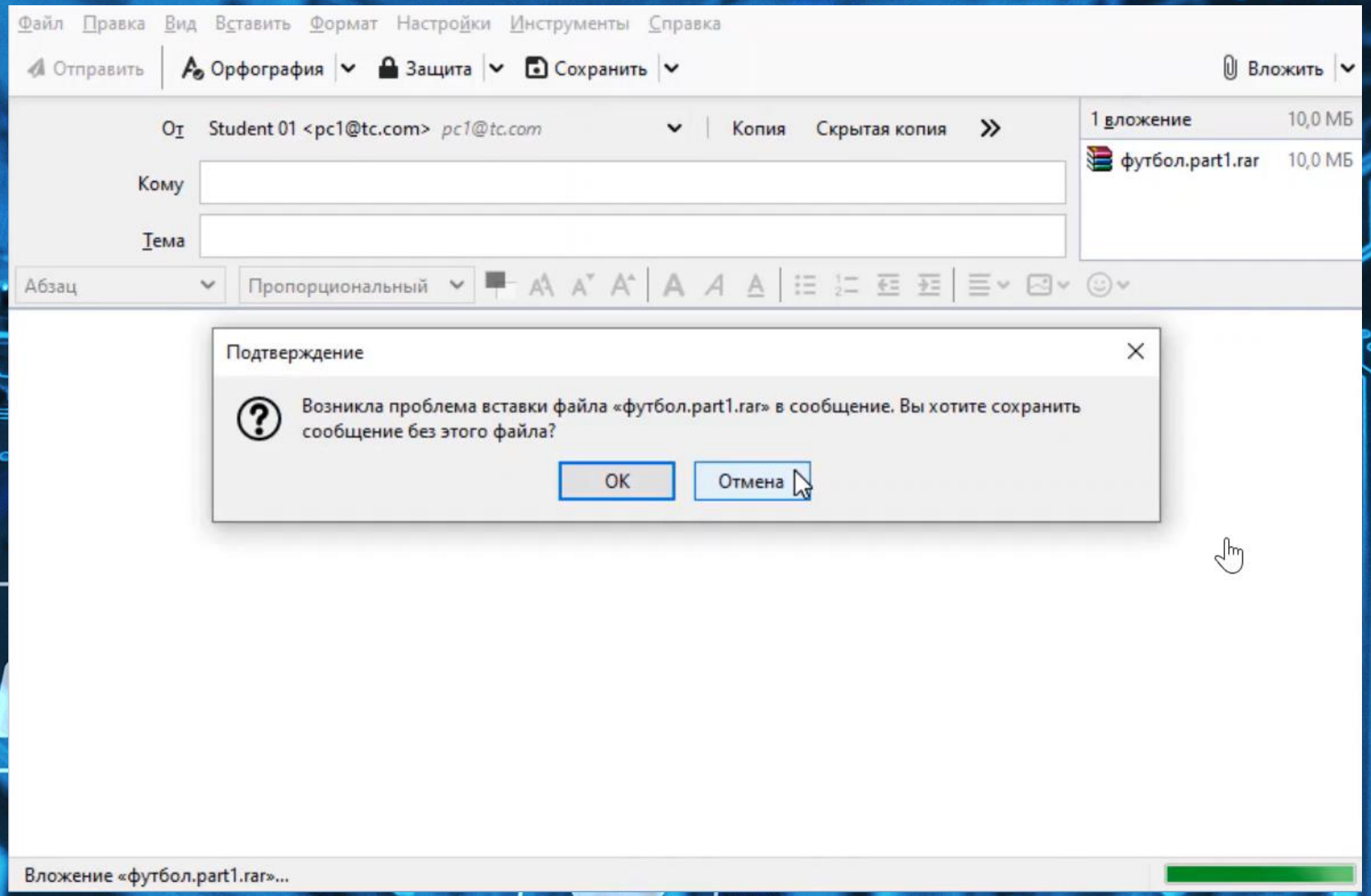
Просмотр файлов - Дата обновления файл: 10.09.2021 9:00:40

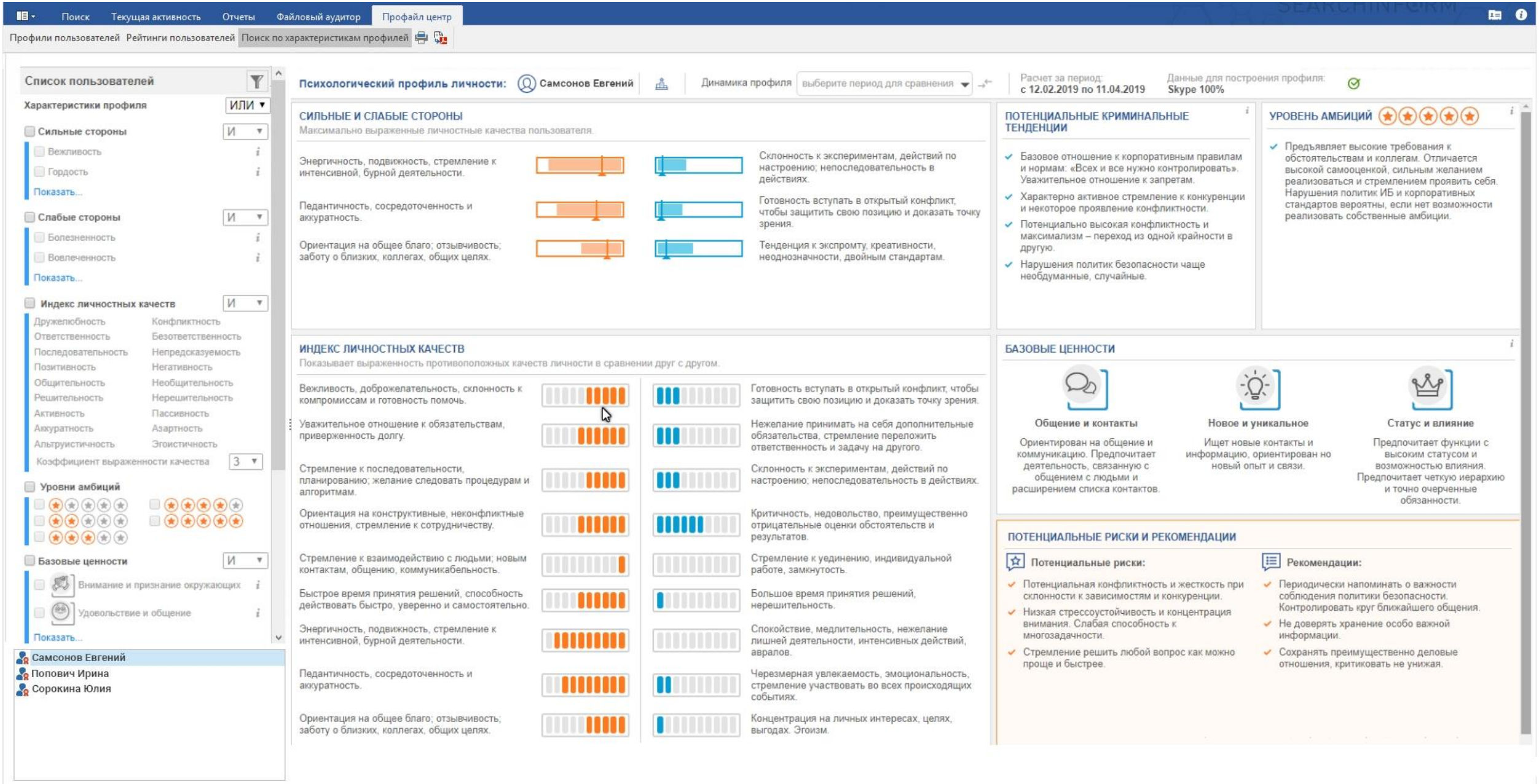
Статистика архива

Всего файлов:	0
Всего папок:	0
Общий размер:	55,69 MB
Размер в архиве:	10 MB
Степень сжатия:	18 %
Пароль:	Нет
Комментарий:	Нет
Пользователь:	-
Скорость чтения:	203 мс

Файл | Размер | Запоковано | И


Файл Опции Вид ?
Журнал запросов от агентов
Перехват на агентах
Сетевой перехват
Интеграция с почтовыми серверами
SMTP интеграция
Настройки программы
Мастер настройки
Очереди на сервере
Потоки данных от агентов
Очереди на агентах
Сканирование FileAuditor
KIB
Перехват на агентах
Сетевое окружение
БД и протоколы
Текущая активность
Политики настроек агентов
Фильтрация
Исключения (системные)
Исключения (пользовательс...
SSL-соединения
Журнал событий по агентам
Блокировки
Файлы по классификации (...
Мессенджеры (DLP)
Печать по контенту (DLP)
Сайты по контенту (DLP)
FileAuditor
Автоматическая классифик...
Шаблоны
Ручная классификация данн...
Хранилище данных
Сканирование на агенте
Сканирование на сервере
Исключения
Планировщик задач
Сетевой перехват
Интеграция с почтовыми серверами
SMTP интеграция
Database Monitor
Оповещения
Search Server
Лицензия
Блокировки. Файлы по классификации (FileAuditor)
Настройки блокировки файлов из различных приложений, которые подпали под правила FileAuditor и имеют метки
Использовать правила блокировки "Файлы по классификации (FileAuditor)"
Добавить
Изменить
Удалить
Экспорт
Импорт
Правила
Нельзя передавать по тиму
Зашифрованные файлы в почте
Редактирование правила. Файлы по классификации (FileAuditor)
Имя правила:
Зашифрованные файлы в почте
Действие:
Разрешено
Запрещено
Аудит:
Полный
Объекты
Файлы
Метки
Пользователи и группы
Компьютеры
Приложения
Процессы
Системные
Browser
\browser.exe;\chrome.exe;*\iexplore.exe;*\f...
Cloud
\applephotostreams.exe;\cloud.exe;*\dropbo...
ICQ/MMP
\icq.exe;\magent.exe
Jabber
\ciscojabber.exe;\psi-plus.exe;*\psi-portable....
Lync
\lync.exe;\communicator.exe
Mail
\outlook.exe;\thebat*.exe;*\thunderbird.exe
Remote Control
\radmin.exe;\romserver.exe;*\romviewer.ex...
Skype
\Skype.exe;\WindowsApps\Microsoft.SkypeA...
Teams
*\teams.exe
Telegram
*\telegram.exe
Viber
*\Viber.exe
WhatsApp
*\WhatsApp.exe
Изменить
Добавить
Удалить
OK
Отмена


Файл Правка Вид Вставить Формат Настройки Инструменты Справка
Отправить
Орфография
Защита
Сохранить
Вложить
От Student 01 <pc1@tc.com> pc1@tc.com
Копия
Скрытая копия
1 вложение 10,0 МБ
футбол.part1.rar 10,0 МБ
Кому
Тема
Абзац
Пропорциональный
Подтверждение
Возникла проблема вставки файла «футбол.part1.rar» в сообщение. Вы хотите сохранить сообщение без этого файла?
OK
Отмена
Вложение «футбол.part1.rar»...


Поиск
Текущая активность
Отчеты
Файловый аудитор
Профайл центр
Профили пользователей
Рейтинги пользователей
Поиск по характеристикам профилей
Список пользователей
Характеристики профиля
ИЛИ
Сильные стороны
И
Вежливость
Гордость
Показать...
Слабые стороны
И
Болезненность
Вовлеченность
Показать...
Индекс личностных качеств
И
Дружелюбность
Конфликтность
Ответственность
Безответственность
Последовательность
Непредсказуемость
Позитивность
Негативность
Общительность
Необщительность
Решительность
Нерешительность
Активность
Пассивность
Аккуратность
Азартность
Альтруистичность
Эгоистичность
Коэффициент выраженности качества
3
Уровни амбиций
Базовые ценности
И
Внимание и признание окружающих
Удовольствие и общение
Показать...
Самсонов Евгений
Попович Ирина
Сорокина Юлия
Психологический профиль личности:
Самсонов Евгений
Динамика профиля
выберите период для сравнения
Расчет за период:
с 12.02.2019 по 11.04.2019
Данные для построения профиля:
Skype 100%
СИЛЬНЫЕ И СЛАБЫЕ СТОРОНЫ
Максимально выраженные личностные качества пользователя.
Энергичность, подвижность, стремление к интенсивной, бурной деятельности.
Склонность к экспериментам, действий по настроению; непоследовательность в действиях.
Педантичность, сосредоточенность и аккуратность.
Готовность вступать в открытый конфликт, чтобы защитить свою позицию и доказать точку зрения.
Ориентация на общее благо; отзывчивость; заботу о близких, коллегах, общих целях.
Тенденция к экспромту, креативности, неоднозначности, двойным стандартам.
ПОТЕНЦИАЛЬНЫЕ КРИМИНАЛЬНЫЕ ТЕНДЕНЦИИ
Базовое отношение к корпоративным правилам и нормам: «Всех и все нужно контролировать». Уважительное отношение к запретам.
Характерно активное стремление к конкуренции и некоторое проявление конфликтности.
Потенциально высокая конфликтность и максимализм – переход из одной крайности в другую.
Нарушения политик безопасности чаще необдуманные, случайные.
УРОВЕНЬ АМБИЦИЙ
Предъявляет высокие требования к обстоятельствам и коллегам. Отличается высокой самооценкой, сильным желанием реализоваться и стремлением проявить себя. Нарушения политик ИБ и корпоративных стандартов вероятны, если нет возможности реализовать собственные амбиции.
ИНДЕКС ЛИЧНОСТНЫХ КАЧЕСТВ
Показывает выраженность противоположных качеств личности в сравнении друг с другом.
Вежливость, доброжелательность, склонность к компромиссам и готовность помочь.
Готовность вступать в открытый конфликт, чтобы защитить свою позицию и доказать точку зрения.
Уважительное отношение к обязательствам, приверженность долгу.
Нежелание принимать на себя дополнительные обязательства, стремление переложить ответственность и задачу на другого.
Стремление к последовательности, планированию; желание следовать процедурам и алгоритмам.
Склонность к экспериментам, действий по настроению; непоследовательность в действиях.
Ориентация на конструктивные, неконфликтные отношения, стремление к сотрудничеству.
Критичность, недовольство, преимущественно отрицательные оценки обстоятельств и результатов.
Стремление к взаимодействию с людьми; новым контактам, общению, коммуникабельность.
Стремление к уединению, индивидуальной работе, замкнутость.
Быстрое время принятия решений, способность действовать быстро, уверенно и самостоятельно.
Большое время принятия решений, нерешительность.
Энергичность, подвижность, стремление к интенсивной, бурной деятельности.
Спокойствие, медлительность, нежелание лишней деятельности, интенсивных действий, авралов.
Педантичность, сосредоточенность и аккуратность.
Черезмерная увлекаемость, эмоциональность, стремление участвовать во всех происходящих событиях.
Ориентация на общее благо; отзывчивость; заботу о близких, коллегах, общих целях.
Концентрация на личных интересах, целях, выгодах. Эгоизм.
БАЗОВЫЕ ЦЕННОСТИ
Общение и контакты
Ориентирован на общение и коммуникацию. Предпочитает деятельность, связанную с общением с людьми и расширением списка контактов.
Новое и уникальное
Ищет новые контакты и информацию, ориентирован но новый опыт и связи.
Статус и влияние
Предпочитает функции с высоким статусом и возможностью влияния. Предпочитает четкую иерархию и точно очерченные обязанности.
ПОТЕНЦИАЛЬНЫЕ РИСКИ И РЕКОМЕНДАЦИИ
Потенциальные риски:
Потенциальная конфликтность и жесткость при склонности к зависимостям и конкуренции.
Низкая стрессоустойчивость и концентрация внимания. Слабая способность к многозадачности.
Стремление решить любой вопрос как можно проще и быстрее.
Рекомендации:
Периодически напоминать о важности соблюдения политики безопасности. Контролировать круг ближайшего общения.
Не доверять хранение особо важной информации.
Сохранять преимущественно деловые отношения, критиковать не унижая.