РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

(Руководство пользо

Дата выпуска: 07.06.2022
Статус документа: Released
Версия ПО: 2.6

Содержание

1. Информация о документе 4
1.1. Назначение 4
1.2. Область применения 4
1.3. Целевая аудитория 4
1.4. Связанные документы 4
1.5. Термины, определения и сокращения 4
2. Обзор 6
2.1. Назначение системы 6
3. Интерфейс системы 7
3.1. Обзор интерфейса системы 7
4. Работа с Системой 11
4.1. Авторизация пользователя Системы 11
4.2. Просмотр сводной информации 12
4.3. Работа со структурой данных и правами сотрудн 18
4.3.1. Работа с деревом структуры организации 19
4.3.1.1. Параметры безопасности 21
4.3.1.2. Структура организации 22
4.3.1.3. Пользователи и группы 23
4.3.2. Работа с структурой защищаемых хранилищ 24

1. Информация о документе

1.1. Назначение

Цель данного документа – описать возможности, предоставляемые ПО Гарда Файлы (далее Система).
Документ покрывает основные настройки и не затрагивает специфические настройки, а также элементы интерфейса, который предоставляет единую точку доступа для всех системы.

1.2. Область применения

Документ предназначен для ПО “Гарда Файлы” версии

1.3. Целевая аудитория

Документ предназначен для сотрудников отдела информационной безопасности организации.

1.4. Связанные документы

При работе с “Гарда Файлы” Руководство администратора эксплуатационной документации “Гарда Файлы” необходимо руководствоваться “Руководство по установке и настройке Гарда Файлы” Функциональная спецификация”.

1.5. Термины, определения и сокращения

ПО	Программное обеспечение
Администратор Системы	Сотрудник, обладающий учетной записью административными привилегиями для установки и поддержание в рабочем состоянии Гарда Файлы
Пользователь	Сотрудник, занимающийся мониторингом хранилищам неструктурированных данных, также структуры организации, в
Файловый сервер	Хранилище неструктурированных данных ОС Windows/Linux
Почтовый сервер	Сервер пересылки и хранения эл сообщений
ОС	Операционная система – комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия

Браузер	Программное средство навигации интернет
ИТ / IT	Информационные технологии
ИБ	Информационная безопасность
SIEM-система	Система предназначенная для анализа и обр поступающей из различных источ отклонений по заданным критери
Syslog	Стандарт отправки и регистраци в системе событиях (то есть со использующийся в компьютерных протоколу IP.
TCP	Один из основных протоколов пе предназначенный для управления переда
UDP	Один из ключевых элементов наб Интернета. С UDP компьютерные сообщения (в данном случае наз другим хостам без IP необходимост предварительного сообщения для уст каналов передачи или путей дан
HTTP	(HyperText Transfer Protocol) передачи данных
JSON	Текстовый формат обмена данным стандарте ECMA-262 1999 года.

2. Обзор

2.1. Назначение системы

ПК "Гарда Файлы" — система класса DAG (Data Access Governan
осуществлять мониторинг операций пользователей с д
серверах и почтовых серверах под управлением ОС Wi
сервера). Система также позволяет сканировать и к
которыми она контролирует, получать структуру ка
уровнем вложенности, получать права доступа польз
защищаемых серверах и выявлять подозрительную акт
Комплекс предназначен для решения задач предо
безопасности и IT подразделений организаций.

3. Интерфейс системы

3.1. Обзор интерфейса

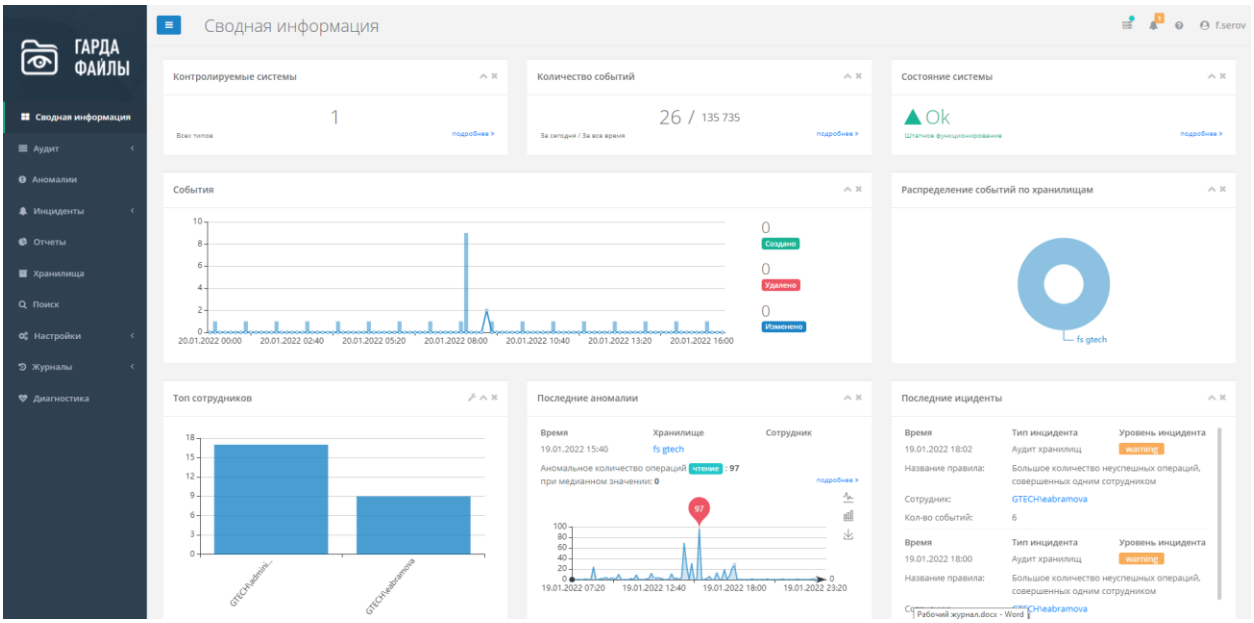

Рис.: Стартовая страница интерфейса

Интерфейс системы Гарда Файлы состоит из нескольких разделов, предлагает определенный набор функций.
В левой части интерфейса расположена панель навигации, позволяющая раз

- Сводная информация - стартовый экран системы. Он содержи информацию о функционировании системы, а также наиболее важной статистической информацией.

- Аудит
  - Хранилища - раздел содержит информацию о всех зас операциях с файлами (такими как, например, прав доступа и др.) и предоставляет инструм различным критериям, а также инструменты по
  - ActiveDirectory - раздел содержит информацию об зафиксированных MS ActiveDirectory (таких учетной записи, Факты неуспешной авторизаци

- Аномалии - раздел содержит информацию о всех зафикс аномальных активностях на хранилищах данных и н сотрудников.

- Инциденты
  - Список инцидентов в разделе содержит инструменты создания обнаружения инцидентов и способов уведомления, предоставляет историю всех зафиксированных инцидентов.
  - Активные реакции содержит список всех действующих, отмененных / завершенных активных реакций Системы и инструменты управления ими.

- Отчеты в данном разделе представлены все доступные инструменты работы с ними.

- Хранилища раздел содержит инструменты для работы с архивами информации, управления агентами контроля событий, просмотра детальной информации о хранилищах: состояние пользовательских прав, рисков и др.

- Поиск раздел предоставляет интерфейс для осуществления быстрого поиска файлов по их содержимому.

- Настройки состоит из нескольких подразделов, предоставляющих возможности создания и управления учетными записями, ролями и правами доступа, настройки интеграции системы с внешними источниками и приемниками событий, управления категоризацией документов и др.

- Журналы раздел для отображения системных событий и событий безопасности Системы

- Диагностика содержит информацию, предназначенную для диагностики работы системы: текущие функциональные параметры и настройки мониторинга, внутренние метрики и диагностическую информацию.

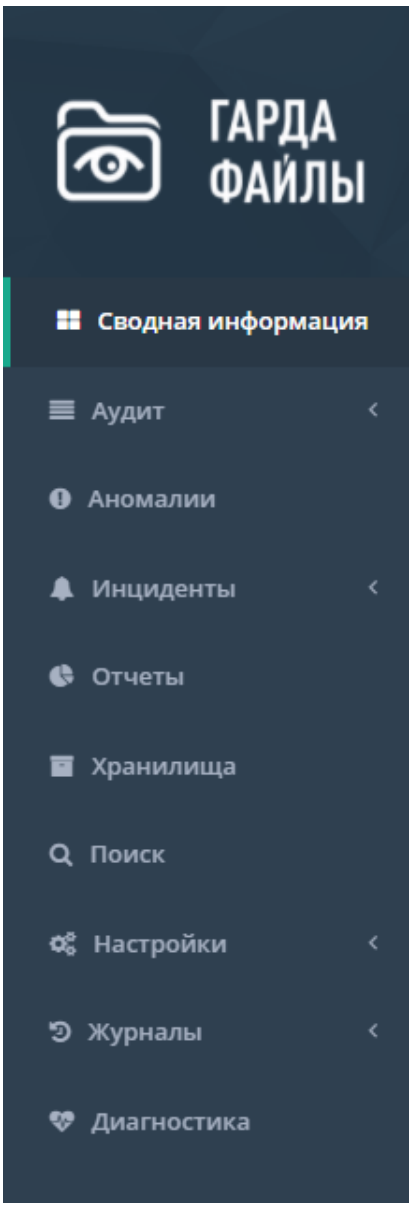

Рис.: Главное меню интерфейса

В центральной части интерфейса располагаются данн
соответствующие выбранному разделу.

В правом верхнем углу интерфейса рас
- Индикатор состояния системы
- Количество сообщений в системном журнале, на к
внимание пользователю Системы
- Ссылки на справку, документацию и описание сис
- Кнопка выхода из системы (процедура деавториза

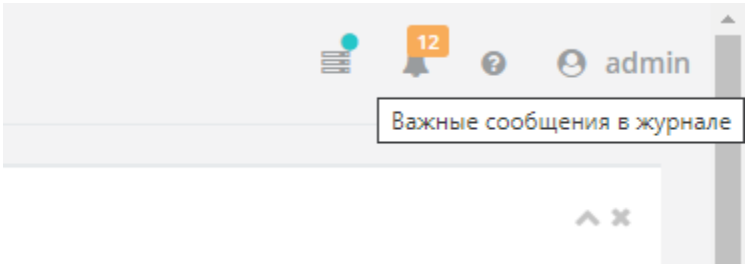

Рис.: Элементы в правом верхнем углу интерфейса

4. Работа с системой

4.1. Авторизация пользователя

Доступ к интерфейсу системы предоставляется только
Системы. Для прохождения процедуры авторизации необ

- Открыть в браузере интерфейс Системы (адрес: <server IP-address> - IP-адрес, назначенный на этапе установки)
- Заполнить поля “логин” и “пароль”
- Нажать “Вход”

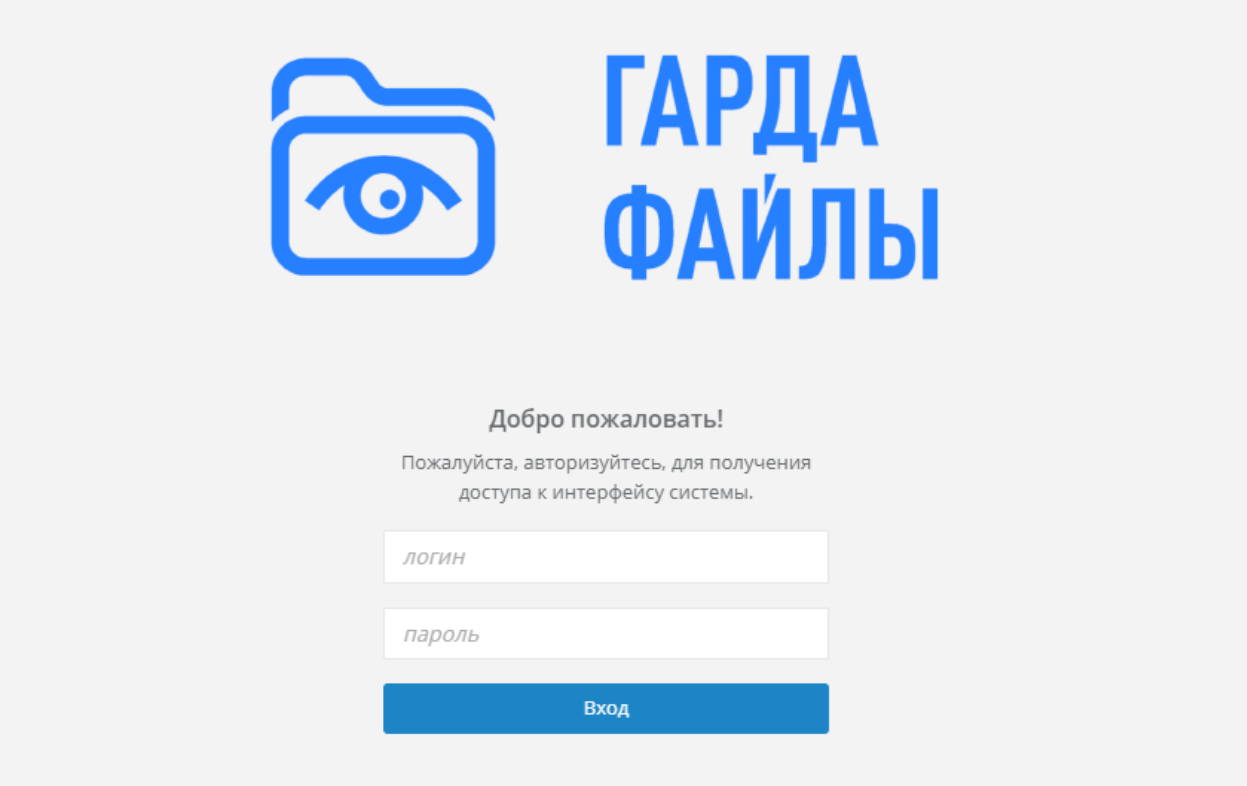

Рис.: Экран авторизации в Системе

Если логин и пароль были введены корректно, перед вами откроется
Если - нет, будет отображено сообщение с ошибкой.

Для выхода из системы (процедуры деавторизации) и
кнопку “Выйти”, которая доступна в выпадающем меню
пользователя в верхнем правом углу интерфейса:

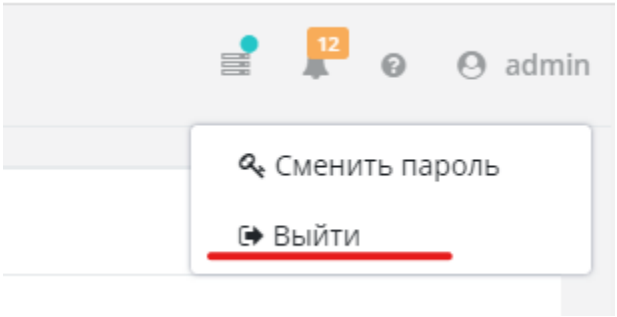

Рис.: Кнопка выхода из Системы

Также процесс деавторизации (logout) по умолчанию пользователя из Системы в течение заданного промежутка времени.

4.2. Просмотр сводной информации

Раздел "Сводная информация" - это экран авторизованного Системой пользователя. На нем представлена следующая информация:

Блок "Контролируемые системы" содержит информацию о хранилищах информации всех типов, а также ссылку "Подробнее" - раздел "Хранилища":

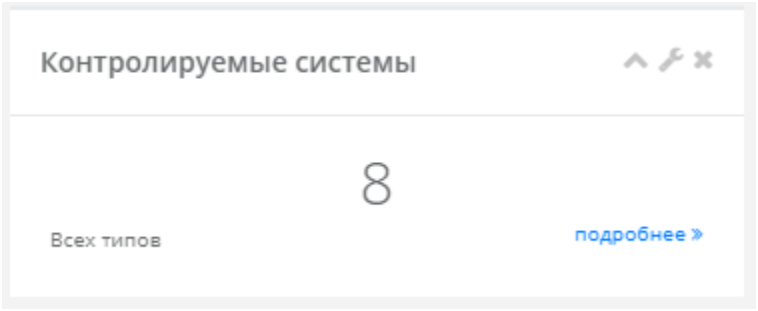

Рис.: Сводная информация. Контролируемые системы

Блок "Количество событий" отображает суммарное Системой действий, с учетом файловых сообщениями и каталога хранилищах информации за текущие сутки и общее информация о которых находится в базе данных Сис раздел "Аудит".

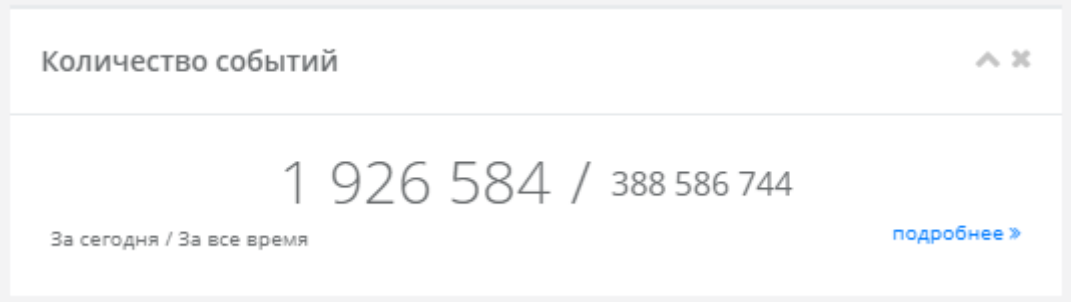

Рис.: Сводная информация. Количество событий

Блок “Состояние системы” показывает текущий стату
возможны три статуса:

- Ok - штатное функционирование Системы
- Problem - необходимо обратить внимание на параметры Системы. Данный статус отображается, когда имеются ошибки
- Critical - Система не функционирует. Требуется вмешат

Ссылка “подробнее” ведет в раздел “Диагностика”.

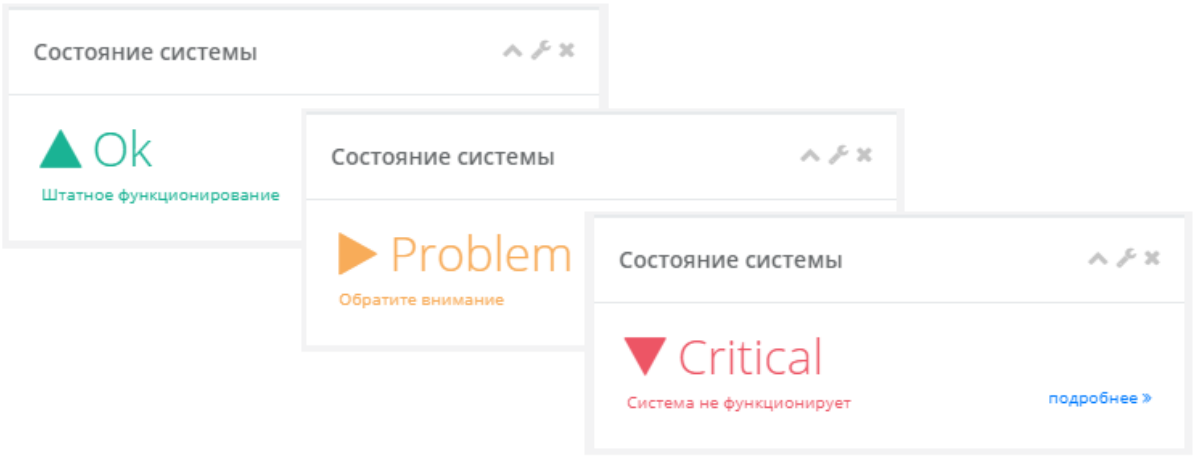

Рис.: Сводная информация. Состояние системы

Блок “События” сподержит диаграмму распределения коли
файлами, почтовыми сообщениями и каталогами сумм
времени: по времени, по суммарному количеству операций
отображается с начала текущего часа. Вторая диаграмма
диаграмме отображает количество зафиксированных де
на прошлой неделе. Также в данном блоке указано ч
сколько файлов создано, сколько удалено и т.д.

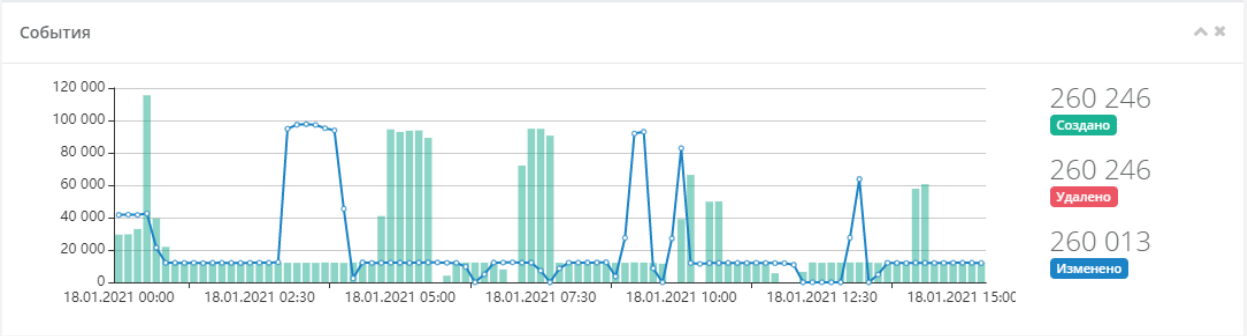

Рис.: Сводная информация. События

Блок “Топ пользователей” отображает учетные записи организации, совершивших наибольшее количество действий с сообщениями и каталогами на контролируемых хостах, а также детализацию по типам совершенных действий.

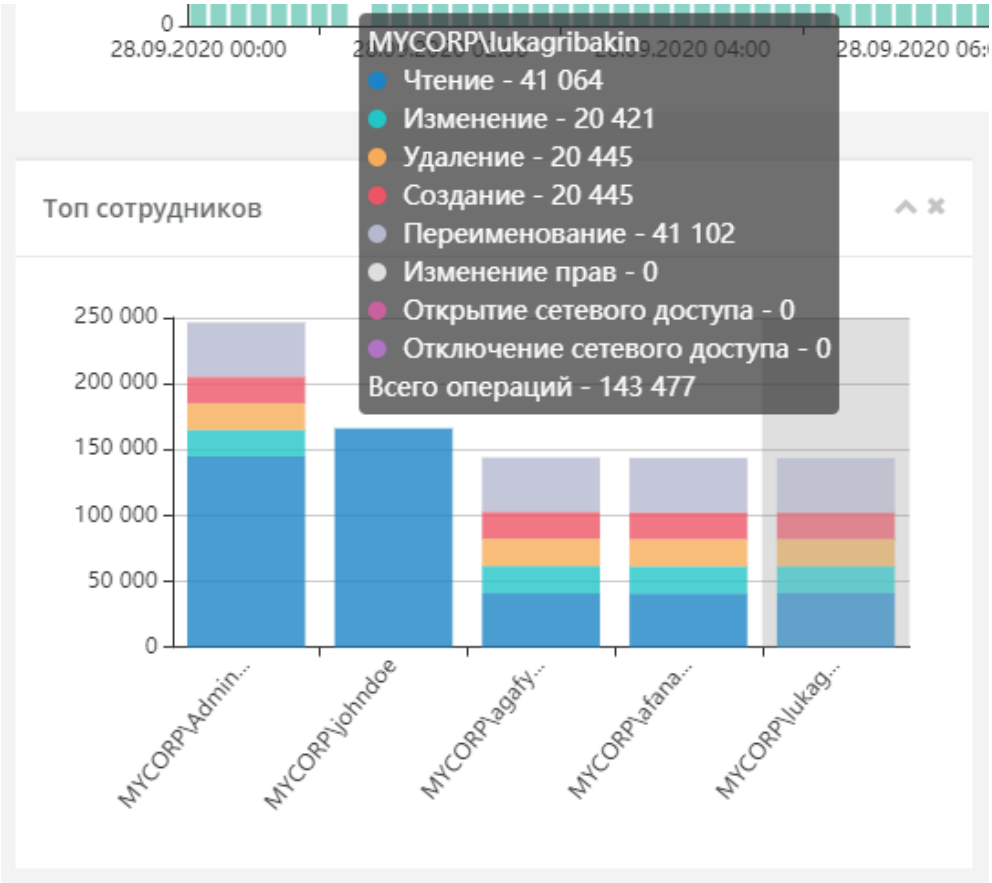

Рис.: Сводная информация. Топ пользователей

Блок “Распределение событий по хранилищам” предст
отображающую контролируемые хранилища и количество зафиксированных
действий с файлами, почтовыми сообщениями и катал

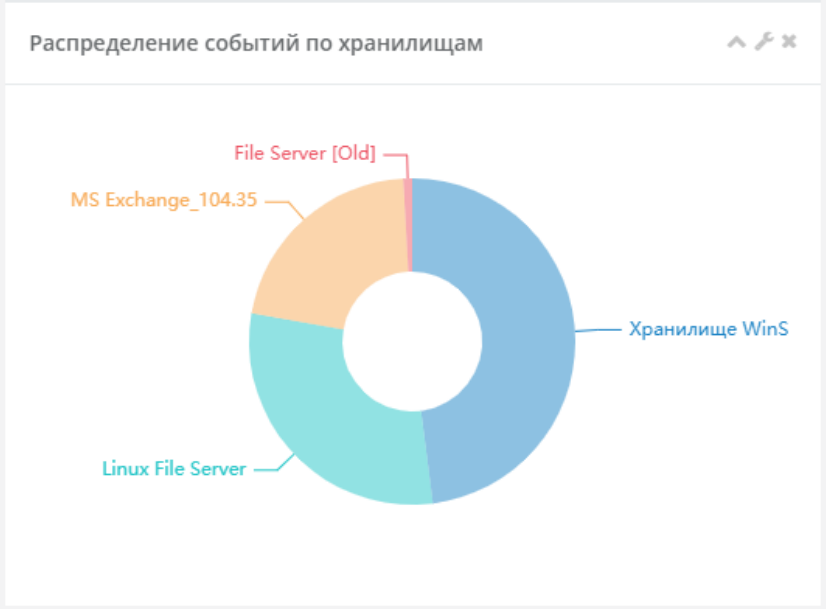

Рис.: Сводная информация. Распределение событий по хранилищам

Блок “Последние аномалии” отображает последнюю
Системой аномалию и цикличную диаграмму. Это
связанная с нетипичной активностью на хранилищах,
сотрудника организации.

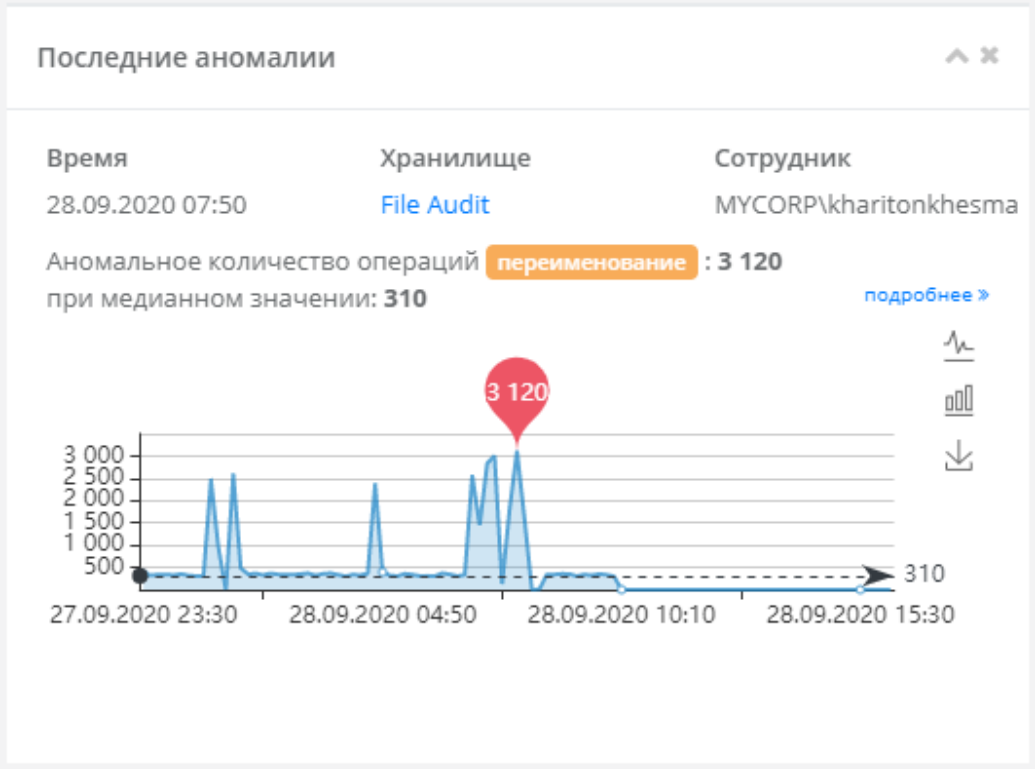

Рис.: Сводная информация. Последние аномалии

Блок “Последние инциденты” содержит графическую информацию о работе Системой инцидентов с кратким их описанием, време

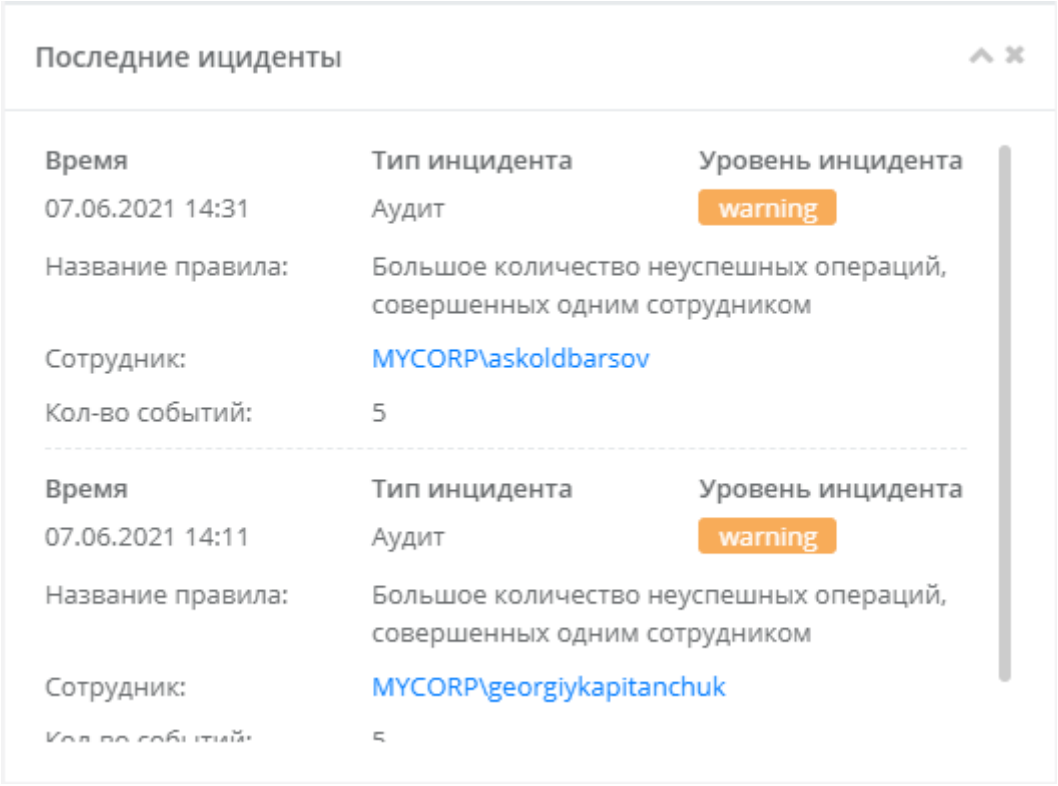

Рис.: Сводная информация. Последние инциденты

4.3. Работа со структурой данных и сотрудников

Система Гарда Файлы обладает возможностью получения ст
систем хранения неструктурированных данных, стр
безопасности, получаемых средствами интеграции с
информации о правах доступа пользователей к за
информация позволит текущие права, выявлять факт
доступа и других, связанных с ними рисков.

Для просмотра структуры конкретного защищаемого
организации с информацией о сотрудниках, получаем
следующие действия:

- Перейдите в раздел “Хранилища”
- Выберите среди перечня хранилищ тот, со структ
  работать
- Нажмите кнопку “Перейти к структуре”

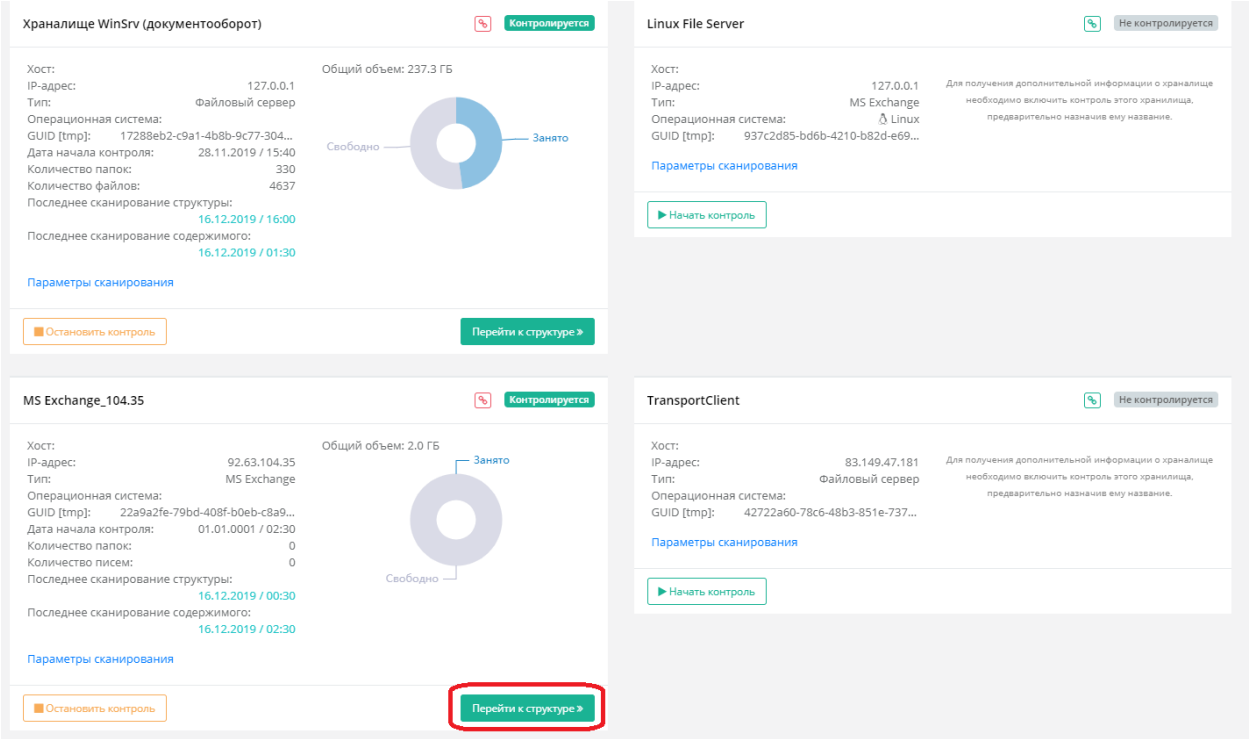

Рис.: Настройки защищаемых хранилищ неструктурированных данных

Данная возможность доступна только для хранилищ сканирования структуры и наличием результатов его сканирование серверов" Работа с данными".

Общий вид интерфейса системы для работы со структ серверов, а также структуры контроллера домена по

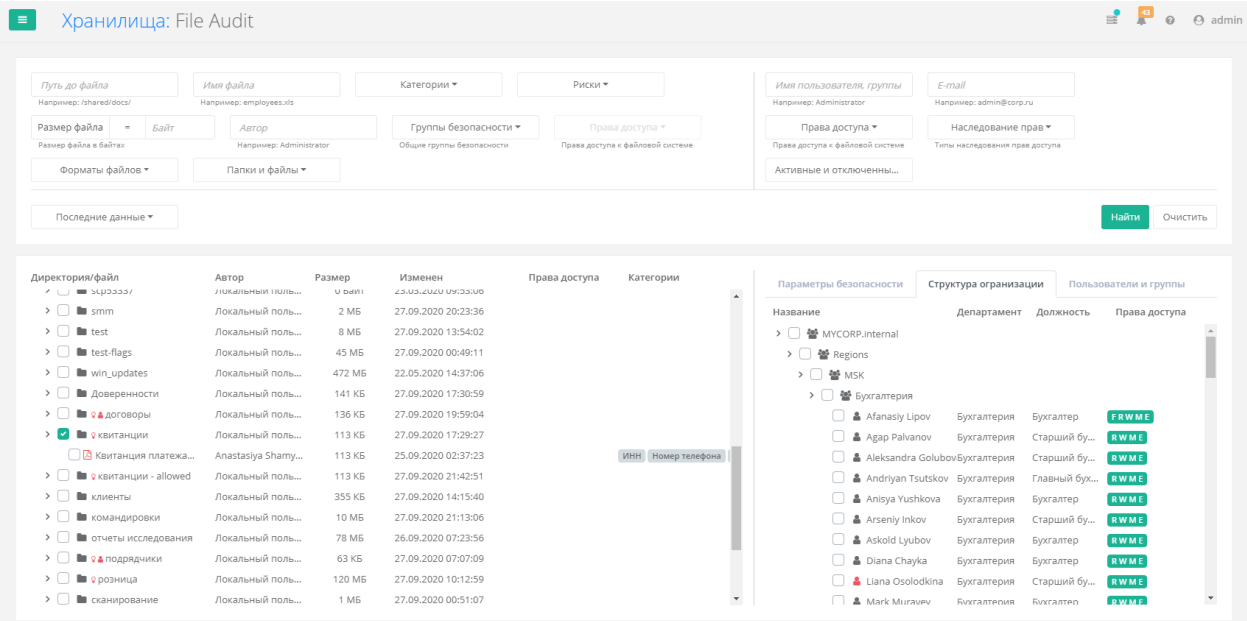

Рис.: Структура защищаемых хранилищ и структура пользователей организации

Данный интерфейс визуально разделен на две части:

- Левая: отображает дерево каталогов и файлов, д инструменты работы с ним, включая различные фи
- Правая: отображает параметры безопасности выбр структуру организации (OU и сотрудники), группы безоп также доступны инструменты фильтрации.

4.3.1. Работа с деревом структуры орга

В правой части интерфейса раздела просмотра инфо расположена структура полученная из контроллера доме себя три варианта отображения:

- Параметры безопасности отображаются только при вы файле в дереве структуры. Показывает, какие группы какие сотрудники имеют доступ на интересующую папку
- Структура организации отображает текущую ст организационных/административных единиц в доме файле отображает текущие “эффективные” права иерархического дерева, при этом элементами организационные/административные единицы и уче
- Пользователи - отображает текущую структуру гру выбранной папке или файле отображает текущие выбранный ресурс в виде иерархического дерева, п являются группы и учетные записи в них.

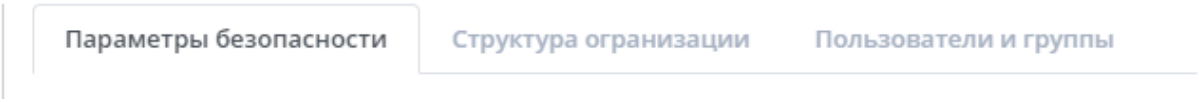

Рис.: Варианты отображения информации о сотрудниках и их правах

Информация о структуре организации, сотрудниках, автоматически в ночное время (по умолчанию), нах состоянии.

Для всех вариантов представления доступна следу сотрудника:

- Доменная учетная запись сотрудника
- E-mail адрес
- Департамент
- Должность
- Права доступа на файлы/каталоги доступные конк

Для удобства работы со структурой организации фильтрация сотрудников по следующим параметрам:

- Имя пользователя, группы
- E-mail адрес

Рис.: Поиск по структуре организации

Для поиска можно указывать как слово целиком, так нажать кнопку “Найти”.

В режиме, когда выбран конкретный файл или катало отфильтровано таким образом, что в нем остались сотрудники, име выбранному файлу/каталогу, также доступны следующ

- Права доступа: позволяет фильтровать список со доступа определенного типа
- Наследование прав: позволяет отфильтровать список со получения прав (прямое назначение или наследов

Рис.: Фильтры “Права доступа” и “Наследование прав”

4.3.1.1. Параметры безопасности

В данном варианте представления отображается инф
сотрудника на различных ресурсах на интересующую папку или ф
унаследованы те или иные разрешения от родительск

Информация доступна только при выбранной в левой части экрана папке или файле в дереве структуры хранилища.

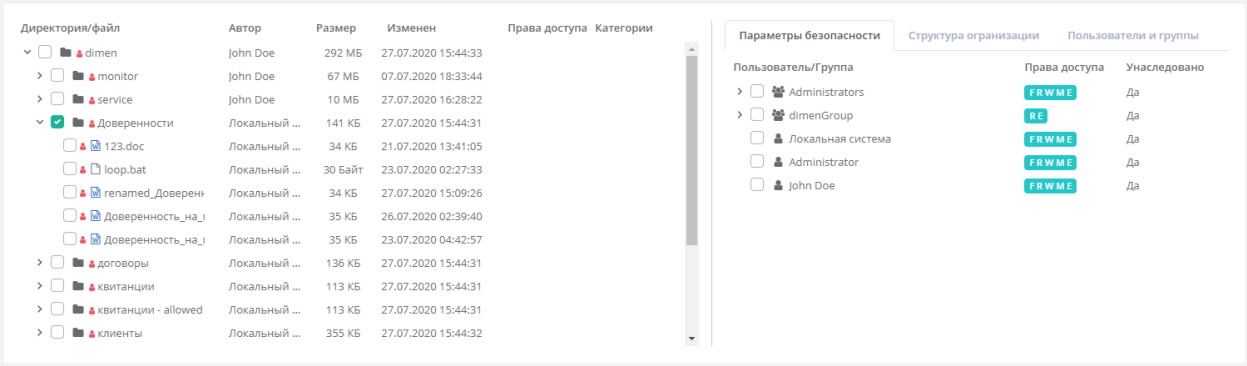

Рис.: Отображения параметров безопасности для выбранной папки

Полученную информацию можно экспортировать в виде
нажать на кнопку “Экспортировать отчет” и указать
дополнительные опции).

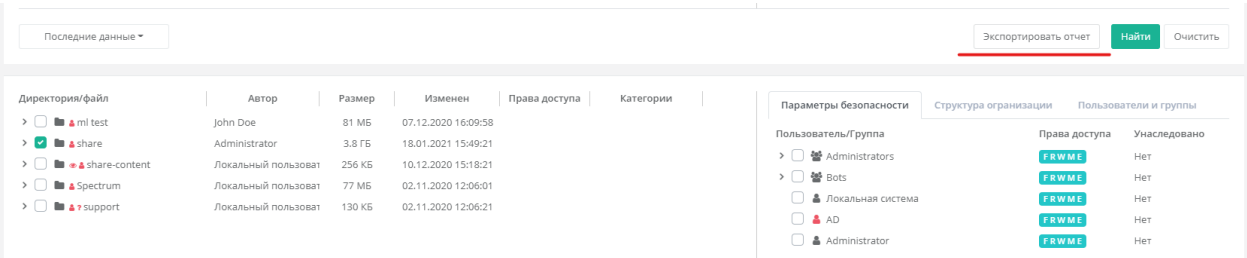

Рис.: Кнопка экспорта параметров безопасности для выбранной папки

4.3.1.2. Структура организации

В данном варианте представления отображается стру
родительскими элементами в котором являются Organ

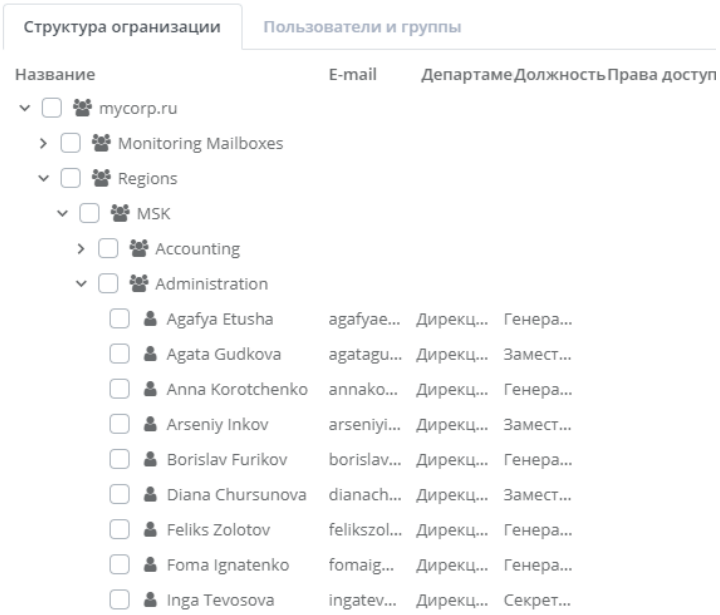

Рис.: Представление структуры организации

Если в левой части интерфейса выбрана папка или файл
то дерево структуры организации будет отфильтрован
которые имеют блокировка доступа к интересующие пи
родительские Organizational Units (OU):

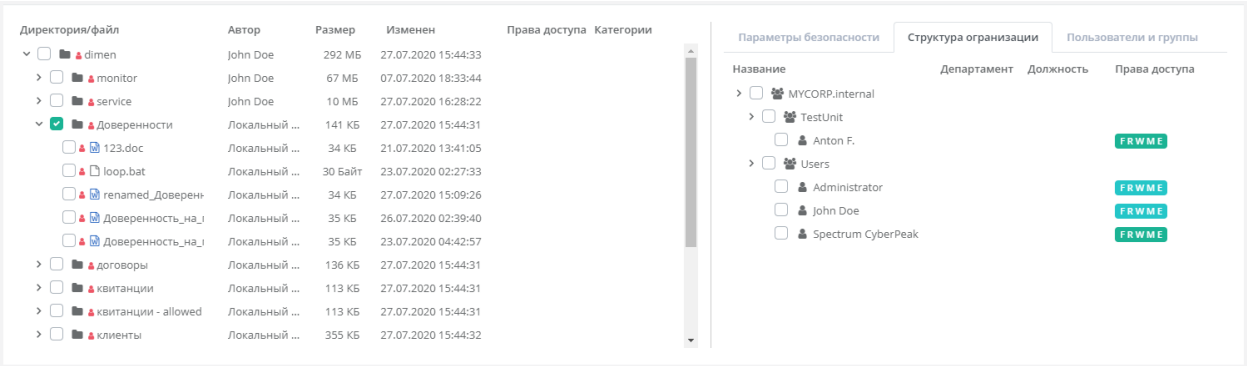

Рис.: Отображение структуры организации с учетом прав на выбранную папку

При этом для каждого сотрудника организации будут
папку (“эффективные” права).
Зеленый блокировка с правами означает получение прав п
сотрудника в группе безопасности:

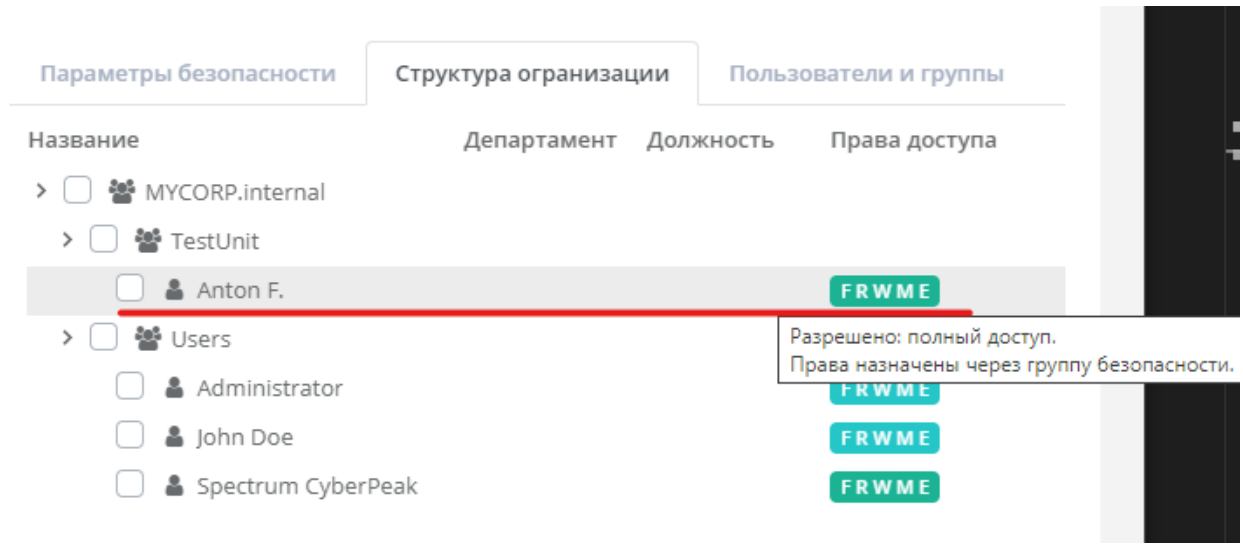

Рис.: Отображение прав сотрудника на конкретную папку, назначенных через группу безопасности

Для просмотра информации о том, от чего унаследованы права доступа, назначены, нужно кликнуть на блок с правами FRWME

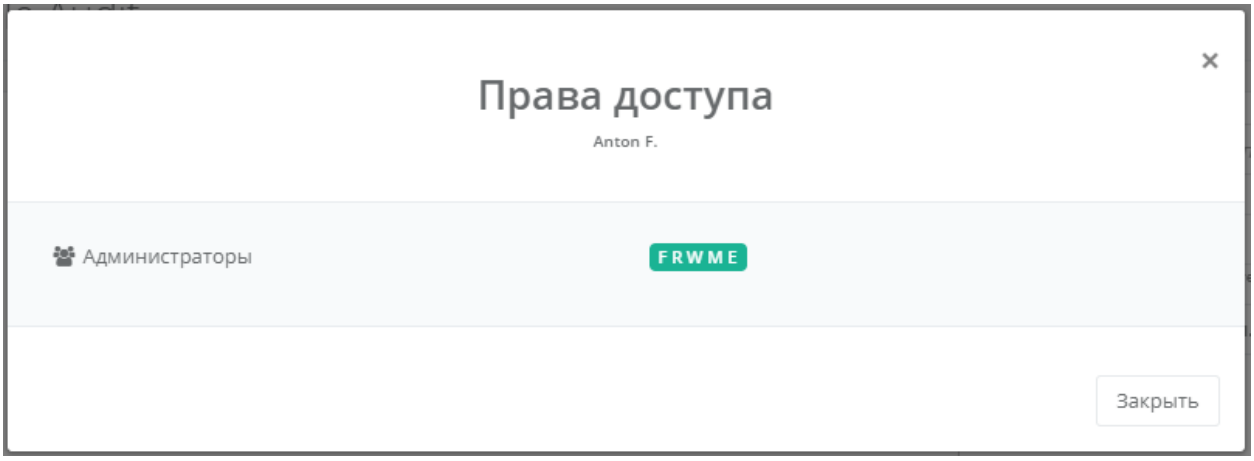

Рис.: Отображение группы безопасности, через разрешения которой интересующий сотрудник получил права доступа к папке

Светло-зеленый цвет блока с FRWME (начальными правами доступа) означает, что выбранной папке/файлу были выданы сотруднику напр

4.3.1.3. Пользователи и группы

В данном варианте представления отображается стру родительскими элементами в котором являются домен

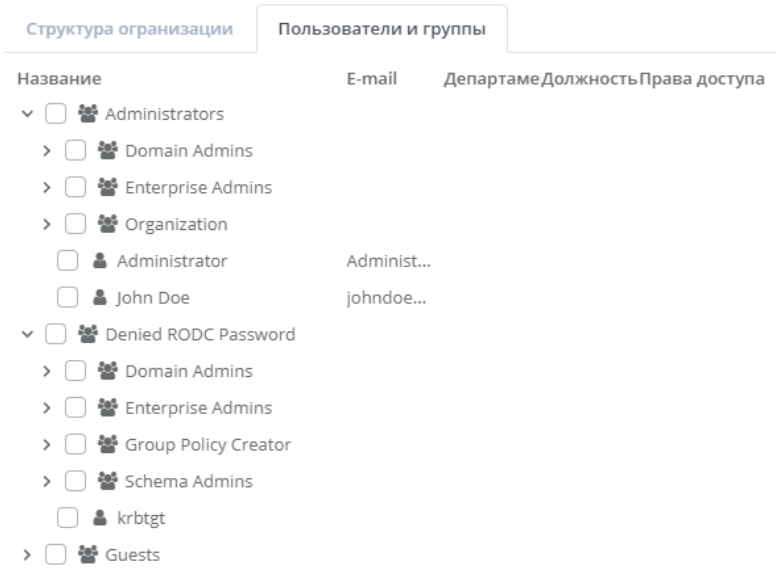

Рис.: Группы безопасности

Если в левой части интерфейса выбрана папка или файл то дерево групп безопасности будет отфильтровано: которые имеют блокировка доступа к интерфейсу, содержащей также родительские группы безопасности.
Поведение и отображаемые данные аналогичны предыд

4.3.2. Работа с структурой защищаемых

Система обладает возможностью получения всей защищаемых файлов серверов, а также Exchange. папок серве Сканирование происходит в соответствии с заданн структуры файлов/каталогов требуемого защищаемо следующие действия:

- Перейдите в раздел “Хранилища”
- Выберите среди перечня файловых серверов с уст структурой которого необходимо работать.
- Нажмите кнопку “Перейти к структуре”

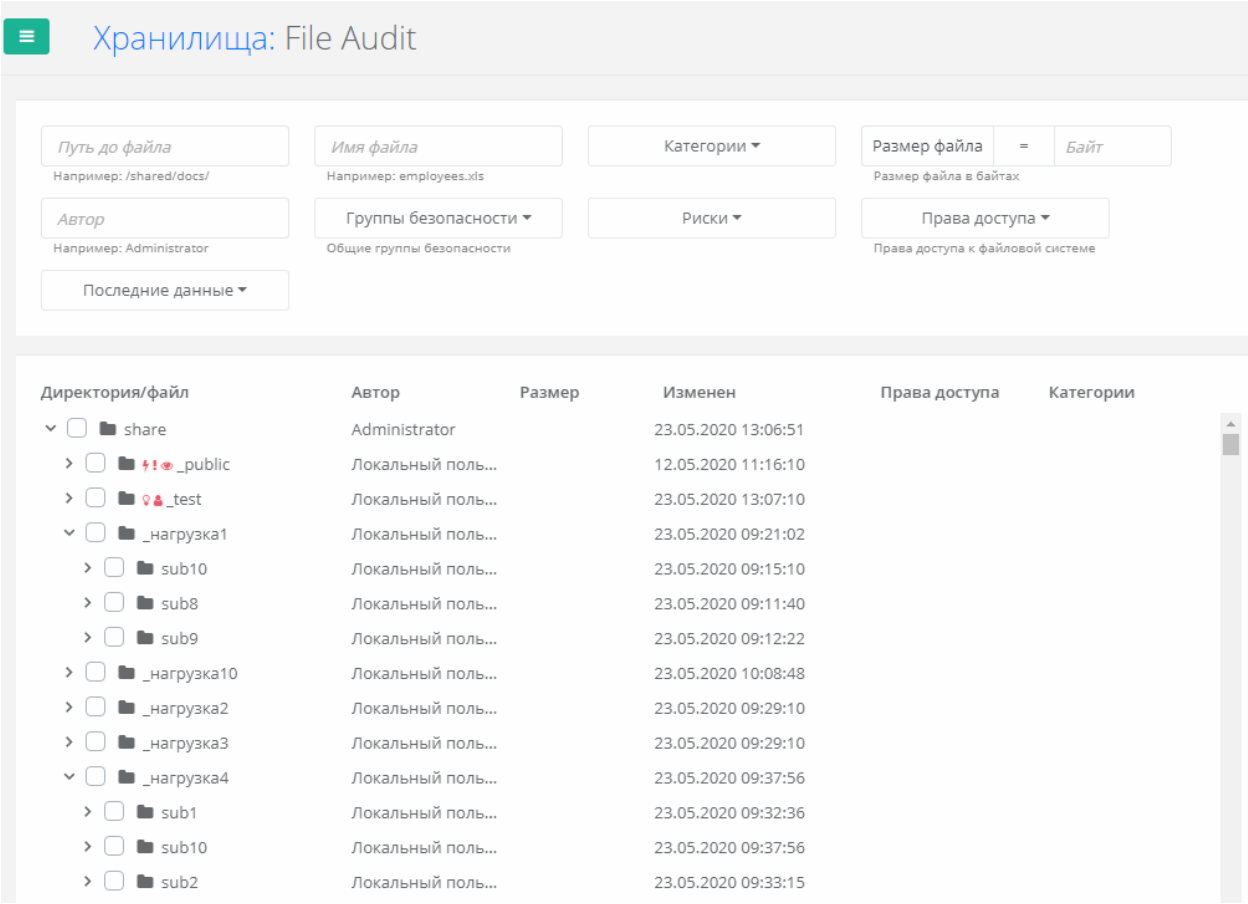

Рис.: Структура файлов/каталогов

В левой части экрана отображается дерево файлов / каталогов с их структурой. Уровень вложенности не ограничен и полностью соответствует структуре хранилища. Для каждого элемента древовидной структуры следующая информация

- Название директории / файла
- Размер
- Автор (владелец согласно ACL)
- Время создания
- Время последнего изменения
- Категории (подробнее об управлении категориями сканирования неструктурированных данных)
- Права доступа (Права файла/каталога для выбранных с

Для удобства работы со списком документов в ве фильтрация каталогов / документов по следующим пара

- Путь до директории / файла

- Название директории/файла
- Категории
- Размер (в байтах)
- Автор
- Риски
- Группы безопасности

Все полученные после применения фильтров папки и отчета в формате Excel, PDF, CSV, HTML. Для этого необходимо “Экспортировать отчет” в нижней части экрана.

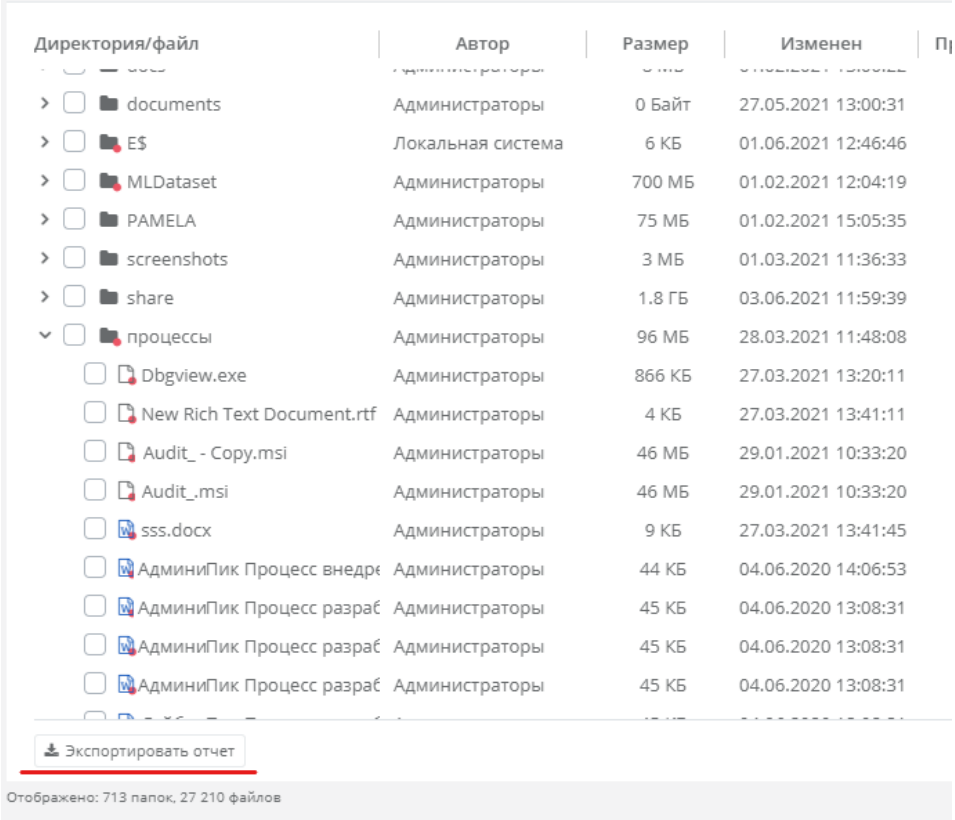

Рис.: Хранилища. Экспорт информации о файлах и директориях