ИБ на результат: Solar Dozor новинки релиза и не только

российский разработчик продуктов и сервисов для целевого мониторинга и управления информационной безопасностью

МОСКВА 28 июня, 2018

Что нового?

- ✓ Аудит облачных хранилищ данных
- ✓ Управление правами доступа пользователей Системы
- ✓ Аудит действий пользователей Системы
- ✓ Контекстная справка

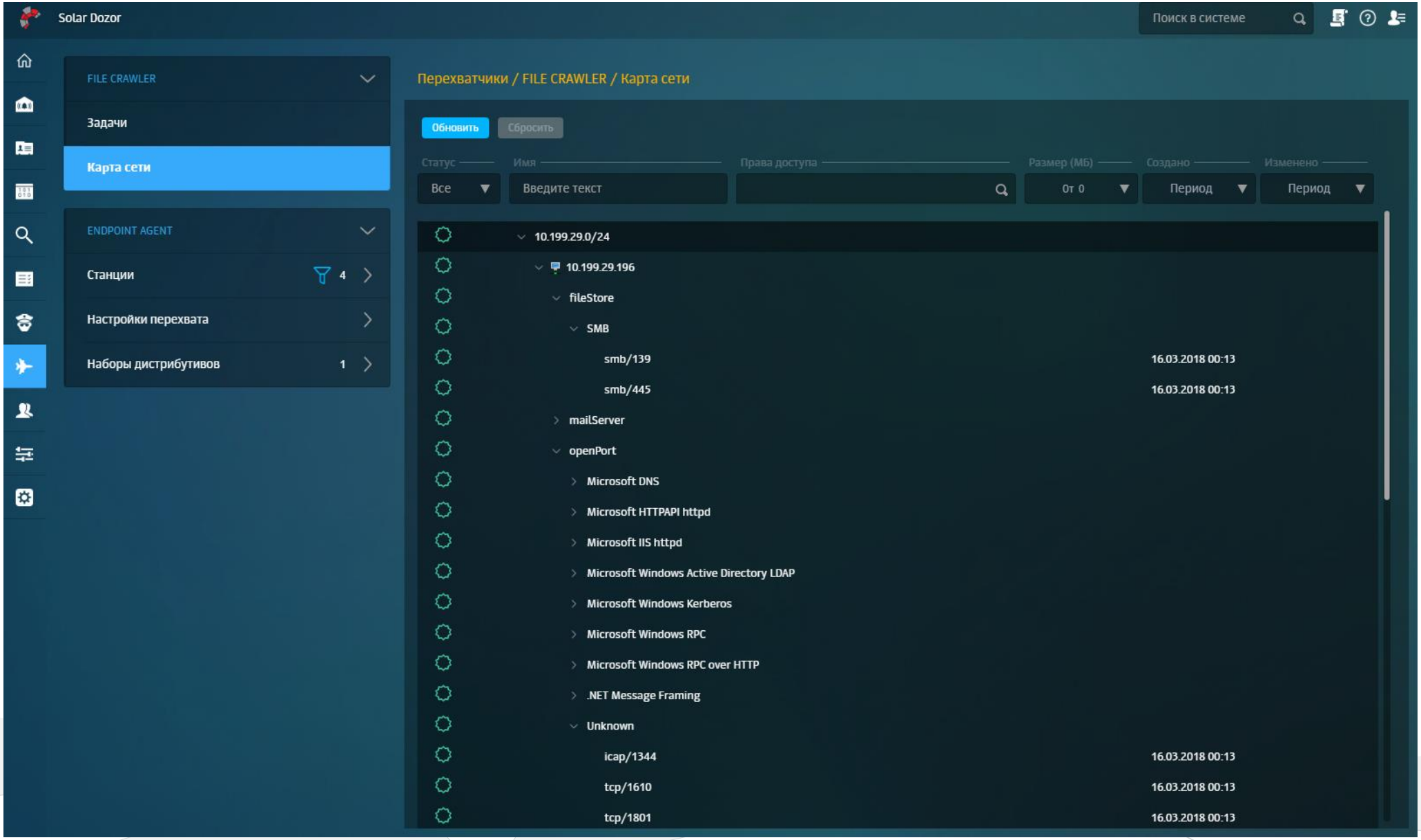
Аудит облачных хранилищ

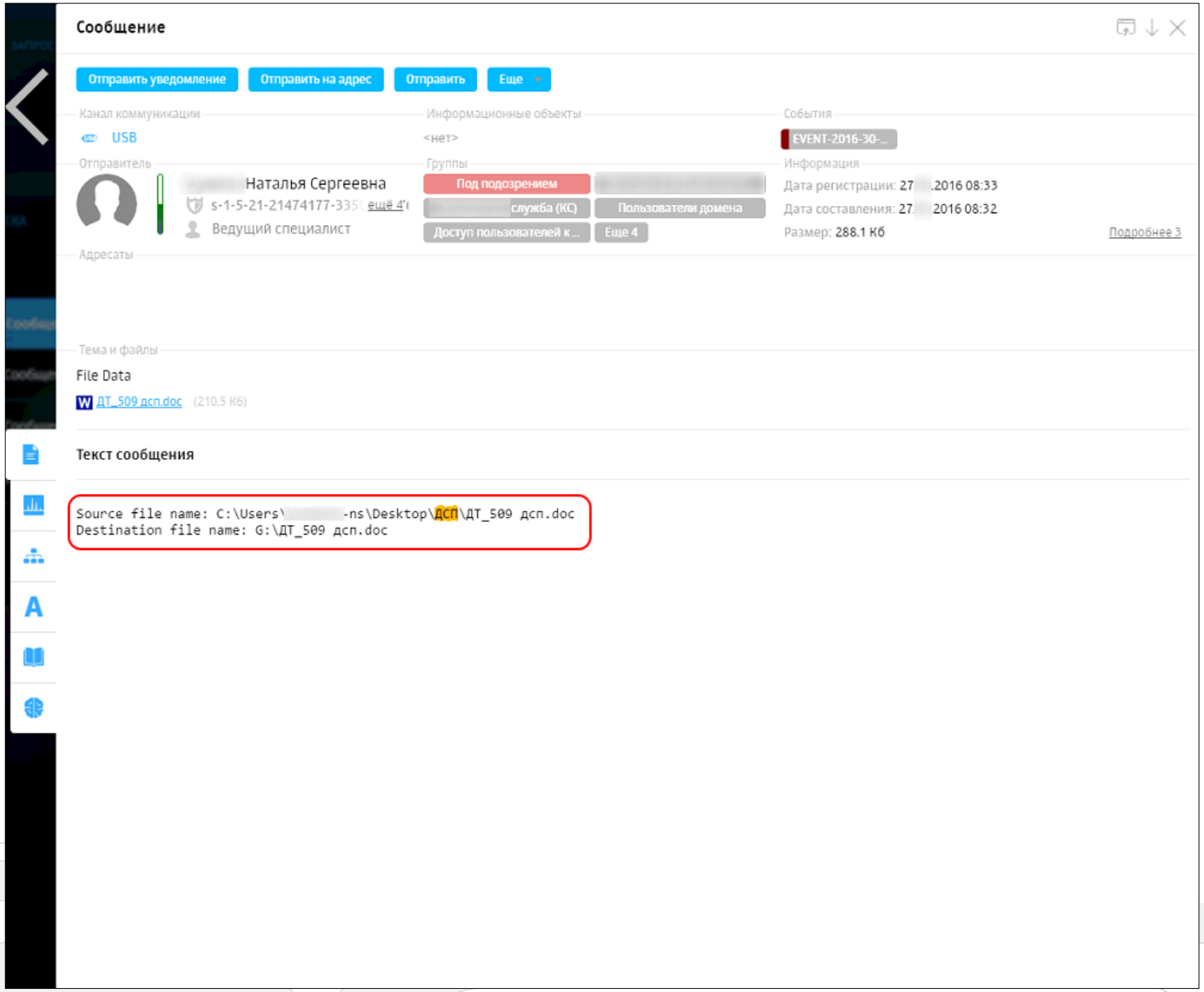
Проблема любого проекта по ИБ…

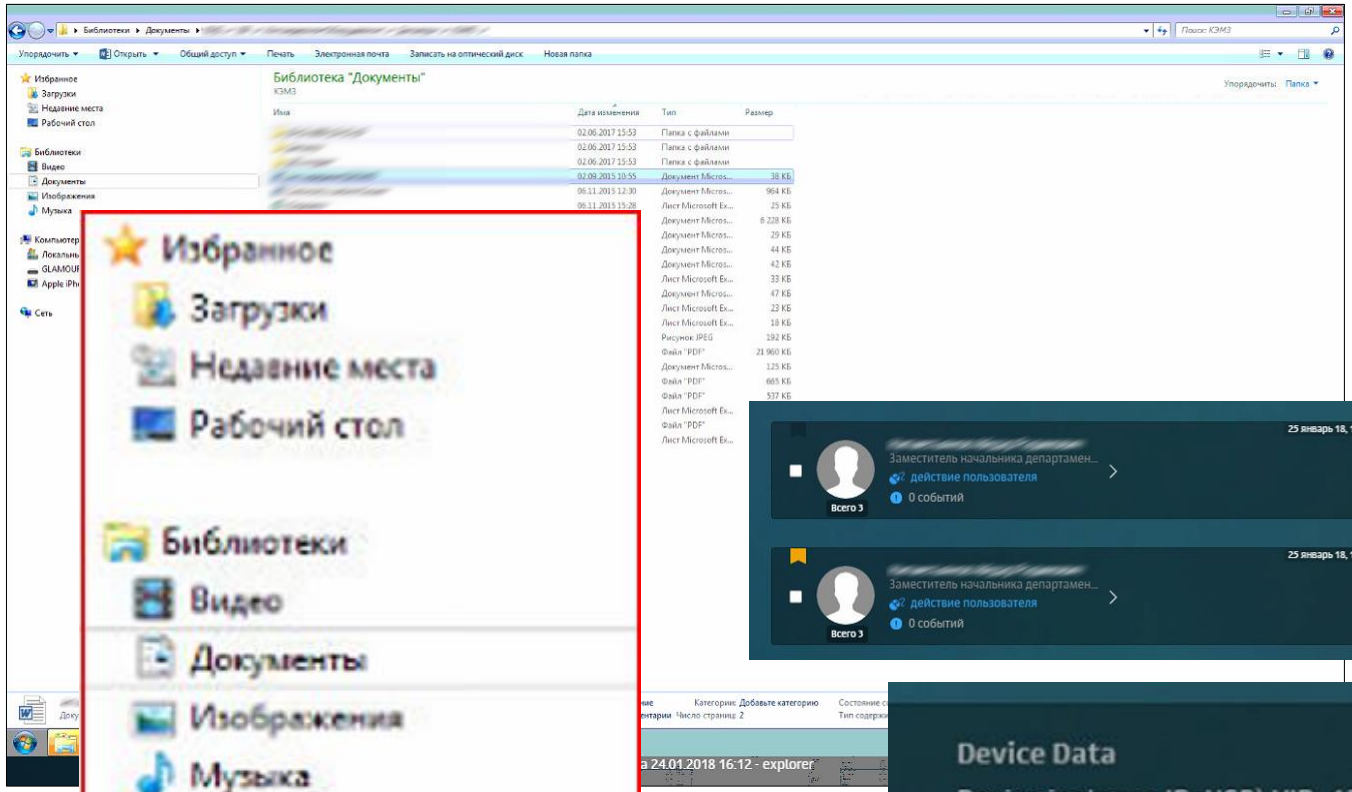
- ✓ Где **реально** хранится информация?
- ✓ **Какая** информация хранится на ПК сотрудников и файловых хранилищах?
- ✓ **Легитимно** ли хранение?

Dozor File Crawler. Основные сценарии использования:

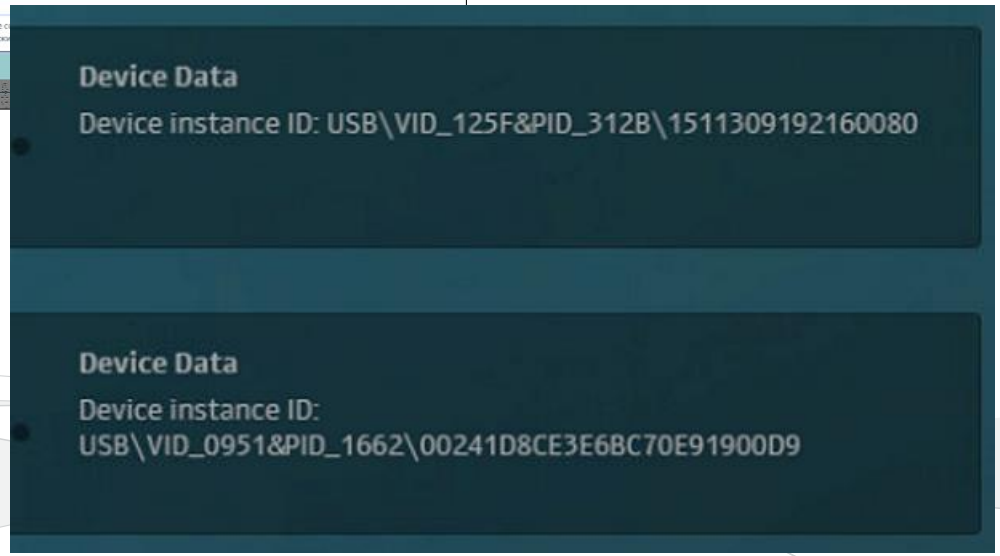
- ✓ поиск **файловых ресурсов с общим доступом**, в том числе неизвестных администратору
- ✓ контроль хранимых данных на предмет **нелегитимного содержимого**
- ✓ контроль содержимого данных **архивов теневого копирования**
- ✓ сканирование почтового сервера по протоколу IMAP с целью **ретроспективного анализа электронной почты** сотрудников
- ✓ поиск новых ресурсов в локальной сети, а также поиск **неизвестных администратору** данных на ресурсах


Solar Dozor
Поиск в системе
FILE CRAWLER
Задачи
Карта сети
ENDPOINT AGENT
Станции 4
Настройки перехвата
Наборы дистрибутивов 1
Перехватчики / FILE CRAWLER / Карта сети
Обновить
Сбросить
Статус
Имя
Права доступа
Размер (МБ)
Создано
Изменено
Все
Введите текст
От 0
Период
Период
10.199.29.0/24
10.199.29.196
fileStore
SMB
smb/139 16.03.2018 00:13
smb/445 16.03.2018 00:13
mailServer
openPort
Microsoft DNS
Microsoft HTTPAPI httpd
Microsoft IIS httpd
Microsoft Windows Active Directory LDAP
Microsoft Windows Kerberos
Microsoft Windows RPC
Microsoft Windows RPC over HTTP
.NET Message Framing
Unknown
icap/1344 16.03.2018 00:13
tcp/1610 16.03.2018 00:13
tcp/1801 16.03.2018 00:13


Сообщение
Отправить уведомление
Отправить на адрес
Отправить
Еще
Канал коммуникации
USB
Информационные объекты
<нет>
События
EVENT-2016-30-...
Отправитель
Наталья Сергеевна
s-1-5-21-21474177-335
ещё 4
Ведущий специалист
Группы
Под подозрением
служба (КС)
Пользователи домена
Доступ пользователей к ...
Еще 4
Информация
Дата регистрации: 27 .2016 08:33
Дата составления: 27 2016 08:32
Размер: 288.1 Кб
Подробнее 3
Адресаты
Тема и файлы
File Data
ДТ_509 дсп.doc (210.5 Кб)
Текст сообщения
Source file name: C:\Users\ -ns\Desktop\ДСП\ДТ_509 дсп.doc
Destination file name: G:\ДТ_509 дсп.doc

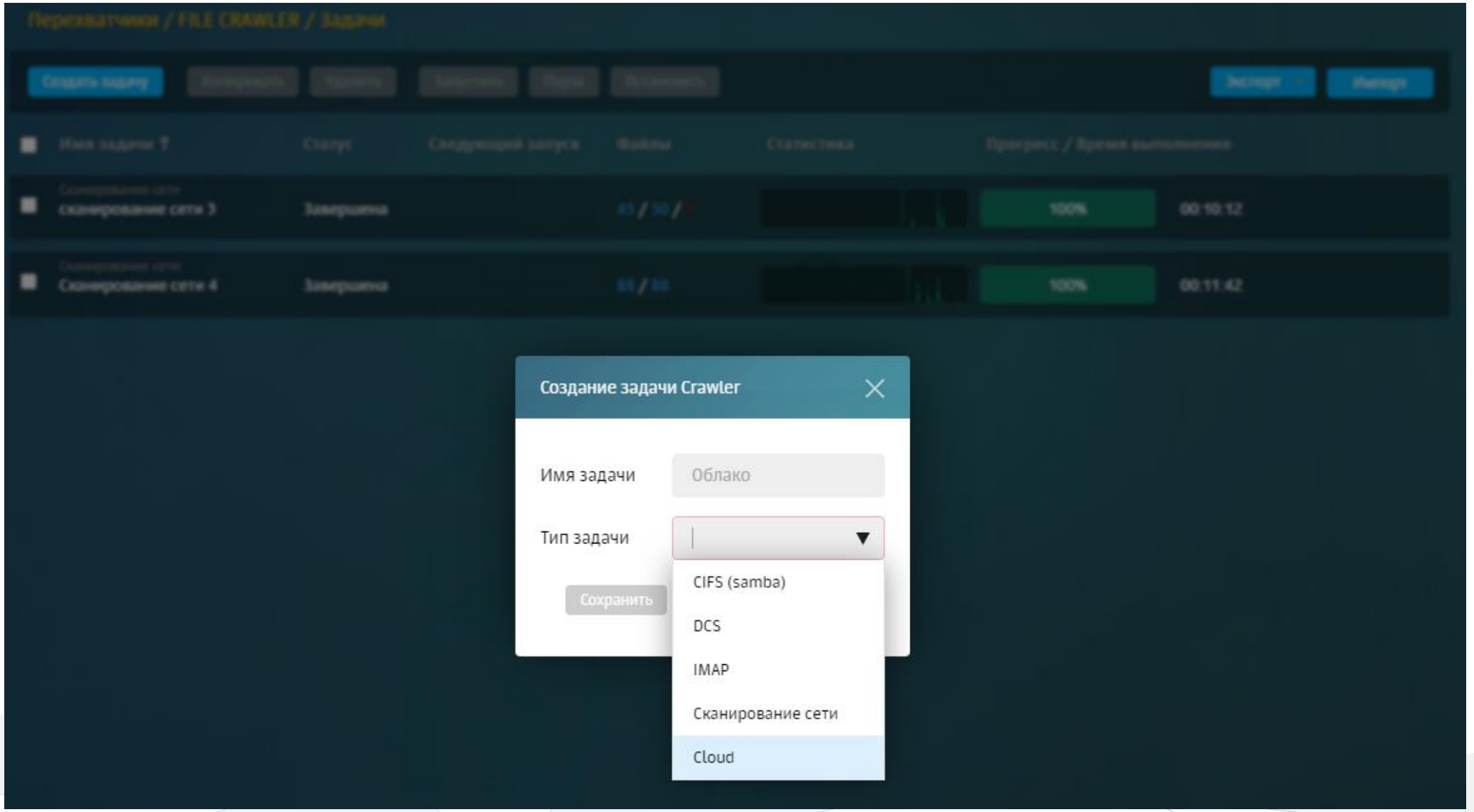

Избранное
Загрузки
Недавние места
Рабочий стол
Библиотеки
Видео
Документы
Изображения
Музыка
Компьютер
Локальный диск (C:)
GLAMOUR (E:)
Apple iPhone
Сеть

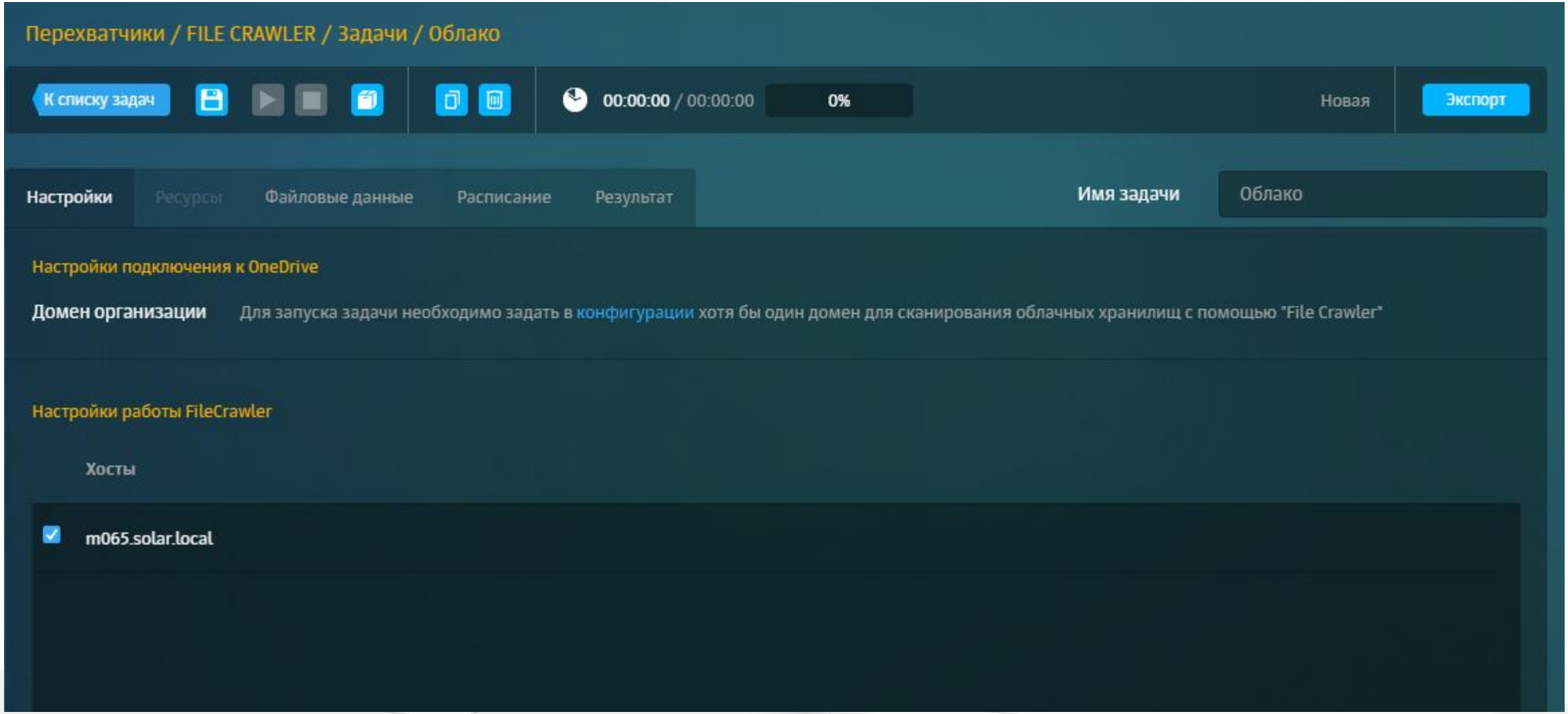
25 января 18, 17:31
Заместитель начальника департамен...
действие пользователя
0 событий
Всего 3
Device Data
Device instance ID: USB\VID_125F&PID_312B\1511309192160080
25 января 18, 17:31
Заместитель начальника департамен...
действие пользователя
0 событий
Всего 3
Device Data
Device instance ID:
USB\VID_0951&PID_1662\00241D8CE3E6BC70E91900D9

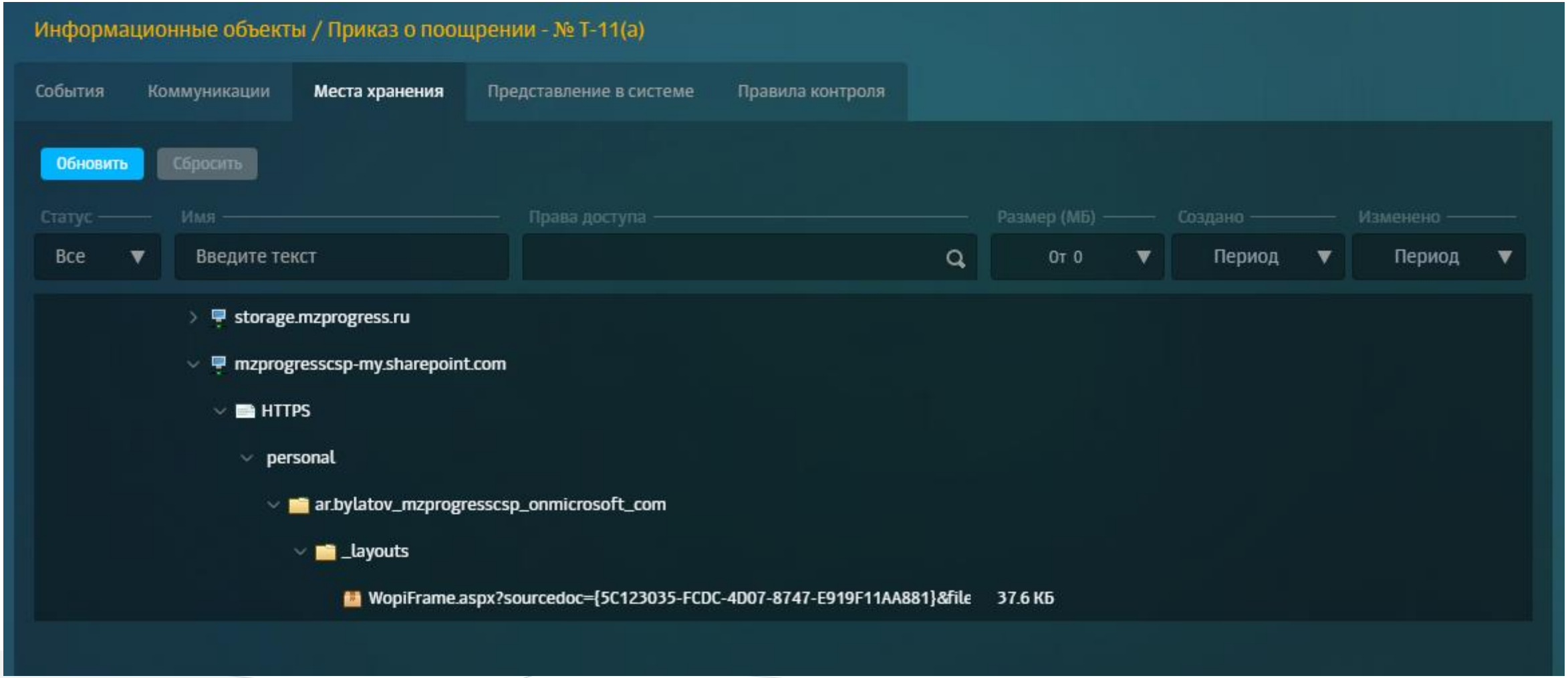

Device Data
Device instance ID: USB\VID_125F&PID_312B\1511309192160080
Device Data
Device instance ID:
USB\VID_0951&PID_1662\00241D8CE3E6BC70E91900D9

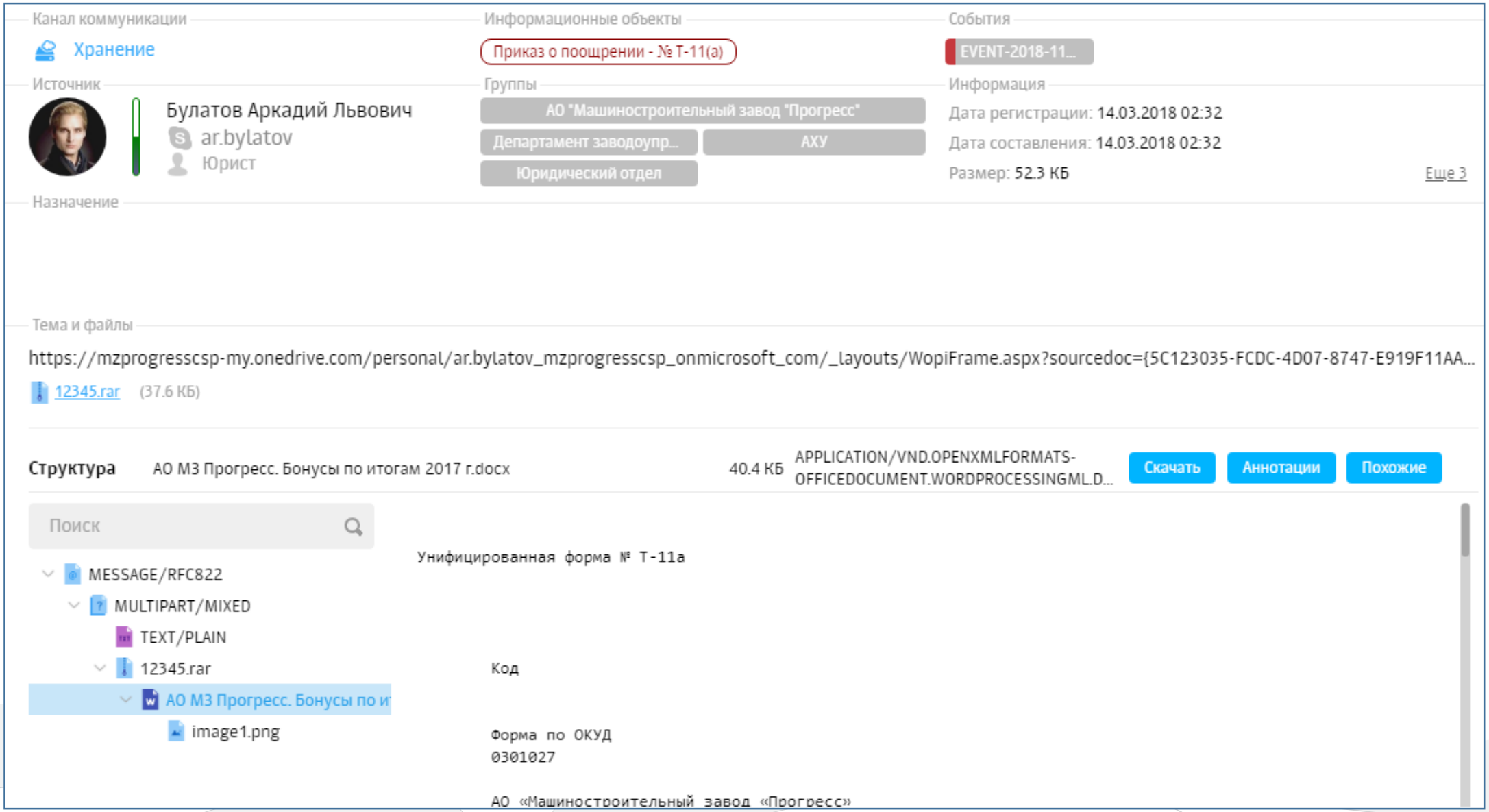
Dozor File Crawler. Мониторинг «облачных» хранилищ.

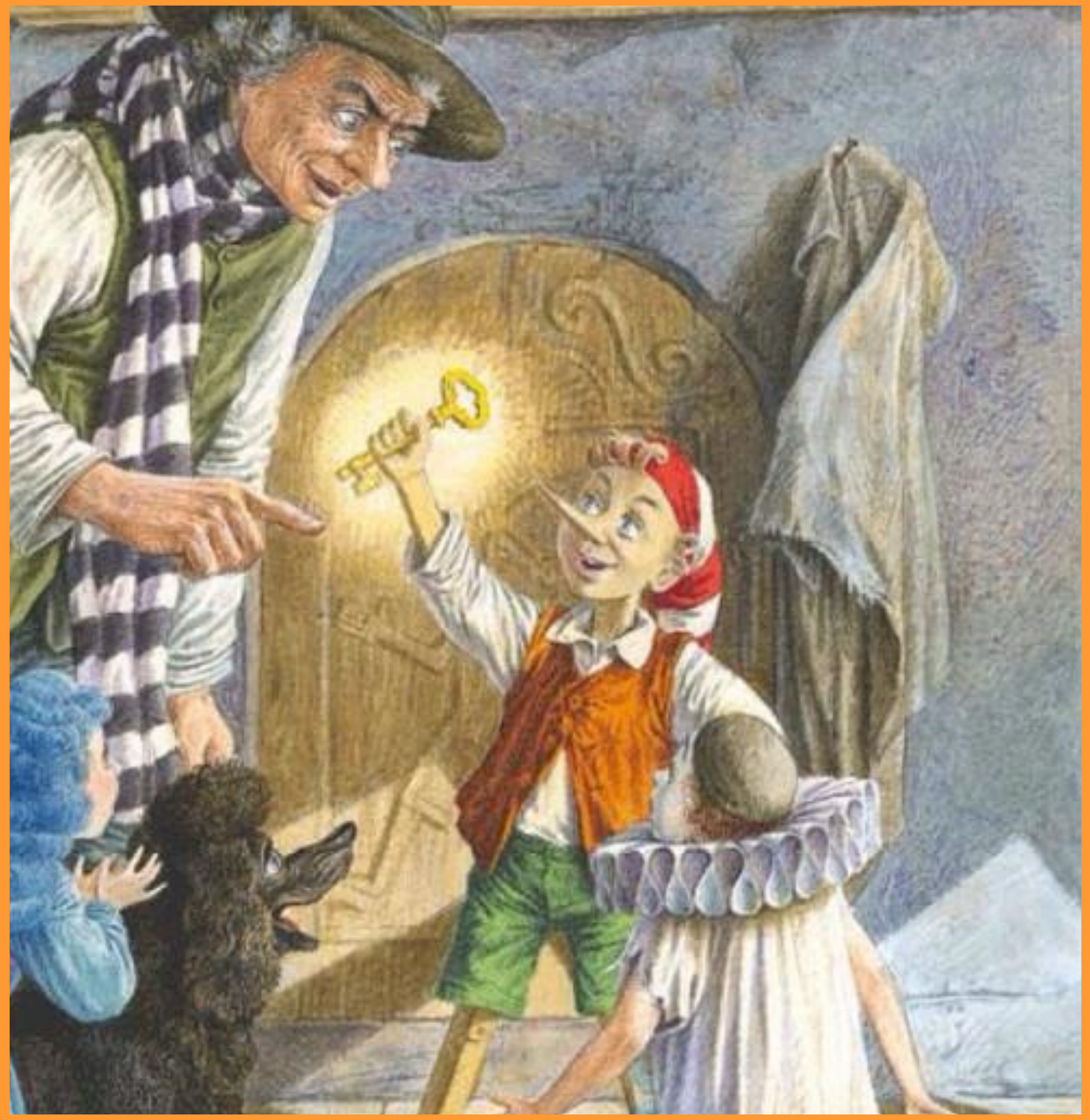
- ✓ Microsoft OneDrive
- ✓ Контроль корпоративного хранилища файлов
- ✓ Возможность интеграции с «Досье» пользователей


Создание задачи Crawler
Имя задачи
Облако
Тип задачи
Сохранить
CIFS (samba)
DCS
IMAP
Сканирование сети
Cloud


Перехватчики / FILE CRAWLER / Задачи / Облако
К списку задач
00:00:00 / 00:00:00
0%
Новая
Экспорт
Настройки
Ресурсы
Файловые данные
Расписание
Результат
Имя задачи
Облако
Настройки подключения к OneDrive
Домен организации
Для запуска задачи необходимо задать в конфигурации хотя бы один домен для сканирования облачных хранилищ с помощью "File Crawler"
Настройки работы FileCrawler
Хосты
m065.solar.local

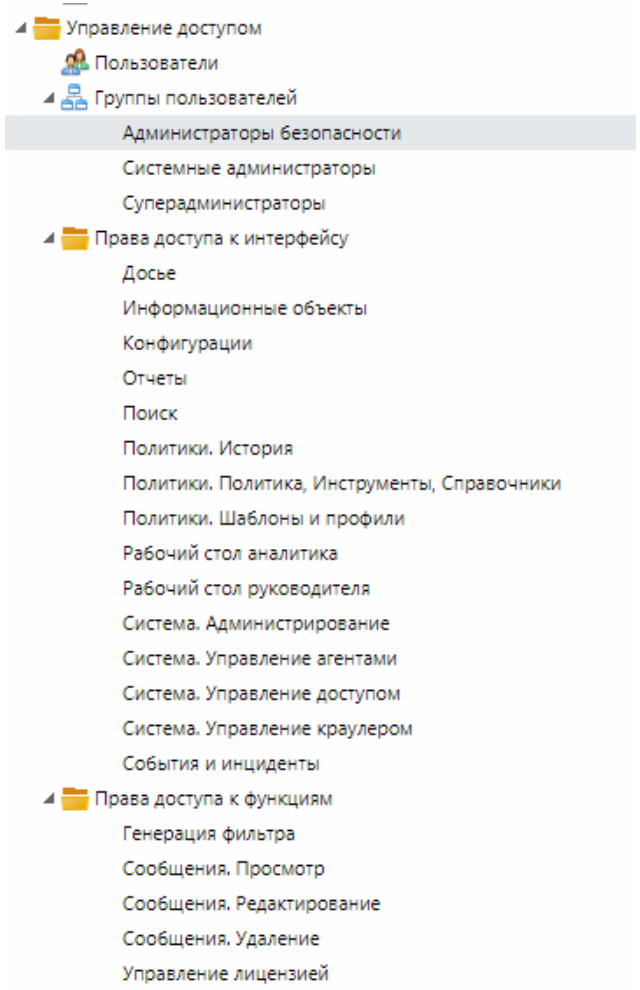

Информационные объекты / Приказ о поощрении - № Т-11(а)
События
Коммуникации
Места хранения
Представление в системе
Правила контроля
Обновить
Сбросить
Статус
Имя
Права доступа
Размер (МБ)
Создано
Изменено
Все
Введите текст
От 0
Период
Период
storage.mzprogress.ru
mzprogresscsp-my.sharepoint.com
HTTPS
personal
ar.bylatov_mzprogresscsp_onmicrosoft_com
_layouts
WopiFrame.aspx?sourcedoc={5C123035-FCDC-4D07-8747-E919F11AA881}&file
37.6 КБ


Канал коммуникации
Хранение
Информационные объекты
Приказ о поощрении - № Т-11(а)
События
EVENT-2018-11...
Источник
Булатов Аркадий Львович
ar.bylatov
Юрист
Группы
АО "Машиностроительный завод "Прогресс"
Департамент заводоупр...
АХУ
Юридический отдел
Информация
Дата регистрации: 14.03.2018 02:32
Дата составления: 14.03.2018 02:32
Размер: 52.3 КБ
Еще 3
Назначение
Тема и файлы
https://mzprogresscsp-my.onedrive.com/personal/ar.bylatov_mzprogresscsp_onmicrosoft_com/_layouts/WopiFrame.aspx?sourcedoc={5C123035-FCDC-4D07-8747-E919F11AA...
12345.rar (37.6 КБ)
Структура
АО М3 Прогресс. Бонусы по итогам 2017 г.docx
40.4 КБ
APPLICATION/VND.OPENXMLFORMATS-OFFICEDOCUMENT.WORDPROCESSINGML.D...
Скачать
Аннотации
Похожие
Поиск
MESSAGE/RFC822
MULTIPART/MIXED
TEXT/PLAIN
12345.rar
АО М3 Прогресс. Бонусы по и
image1.png
Унифицированная форма № Т-11а
Код
Форма по ОКУД
0301027
АО «Машиностроительный завод «Прогресс»

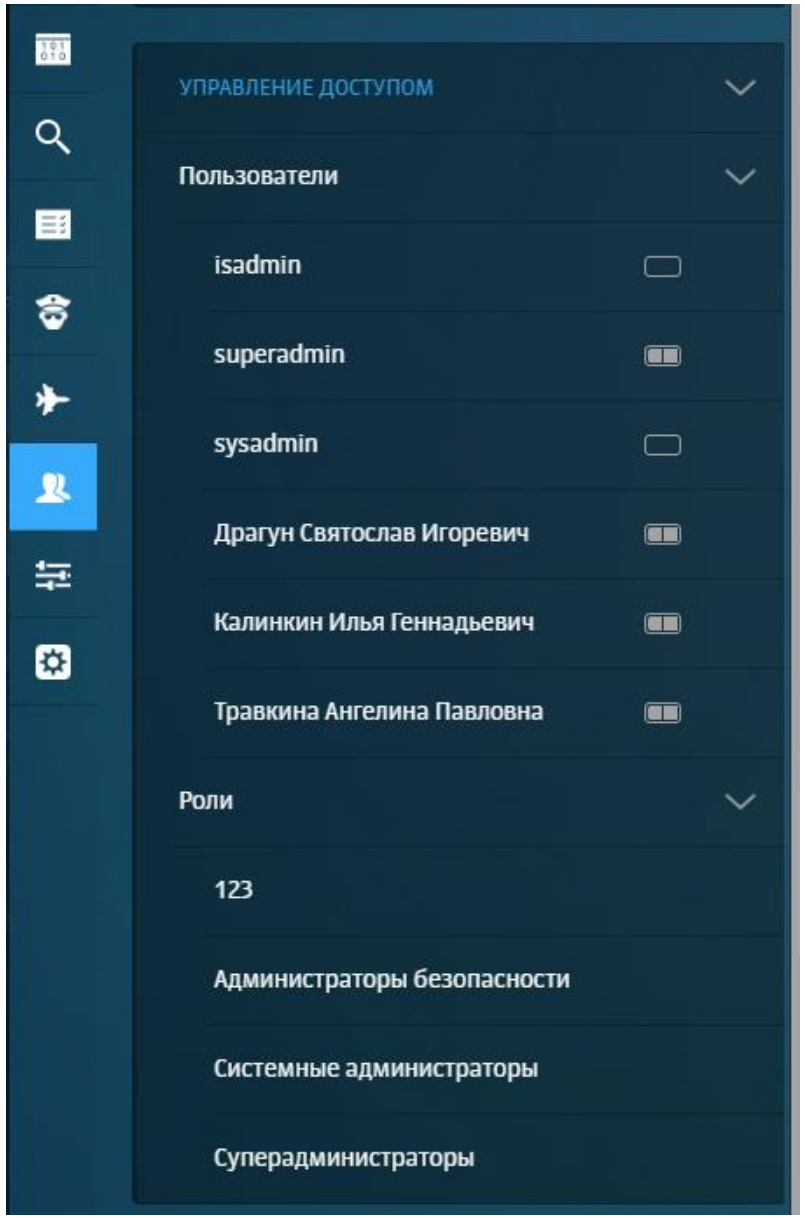


Управление правами доступа пользователей Системы

С чего мы начинали...

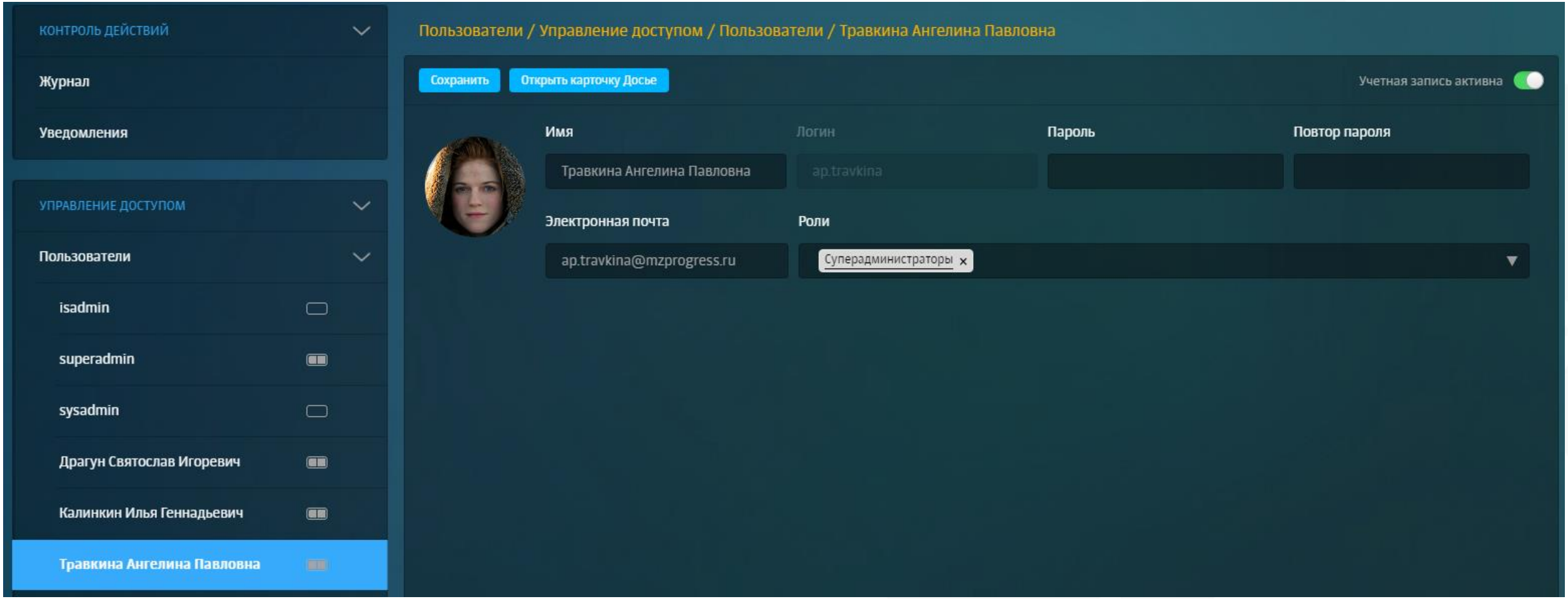


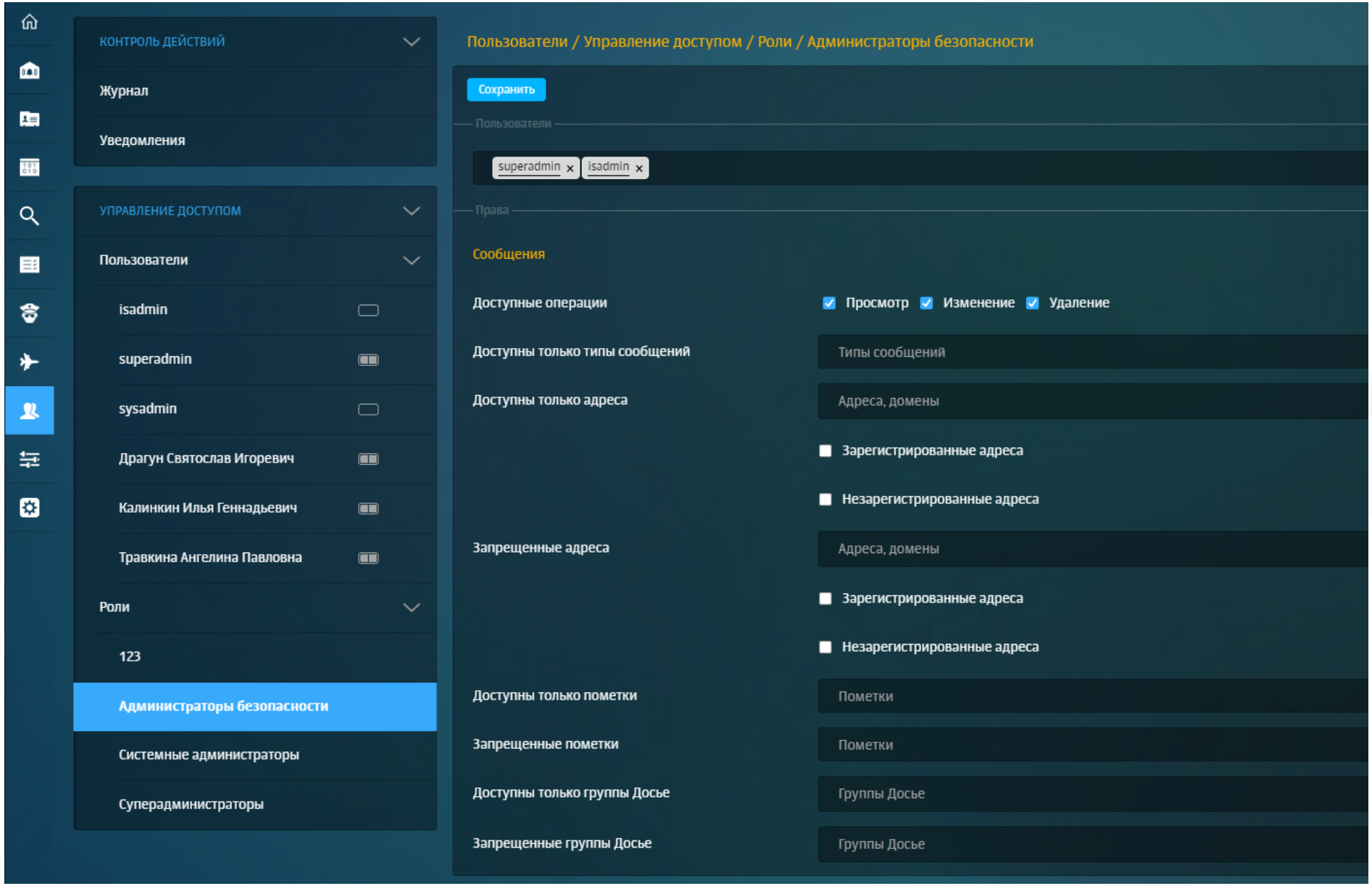
- ✓ Раздел по настройке прав доступа был спрятан в «Настройках».
- ✓ Интерфейс Системы «айфонизирован» в 2016 году, но данный процесс прошел мимо функции управления доступом...



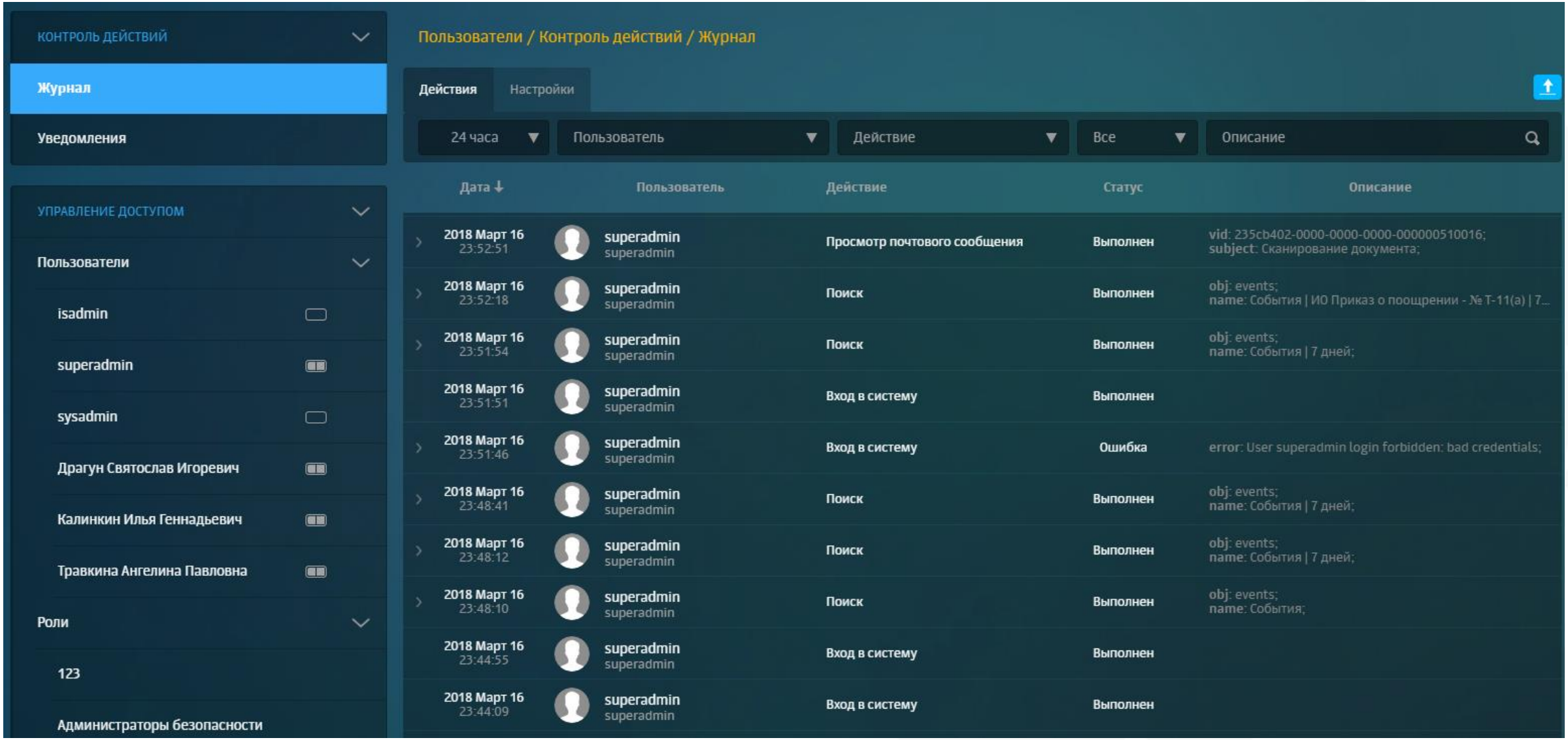
What's new?

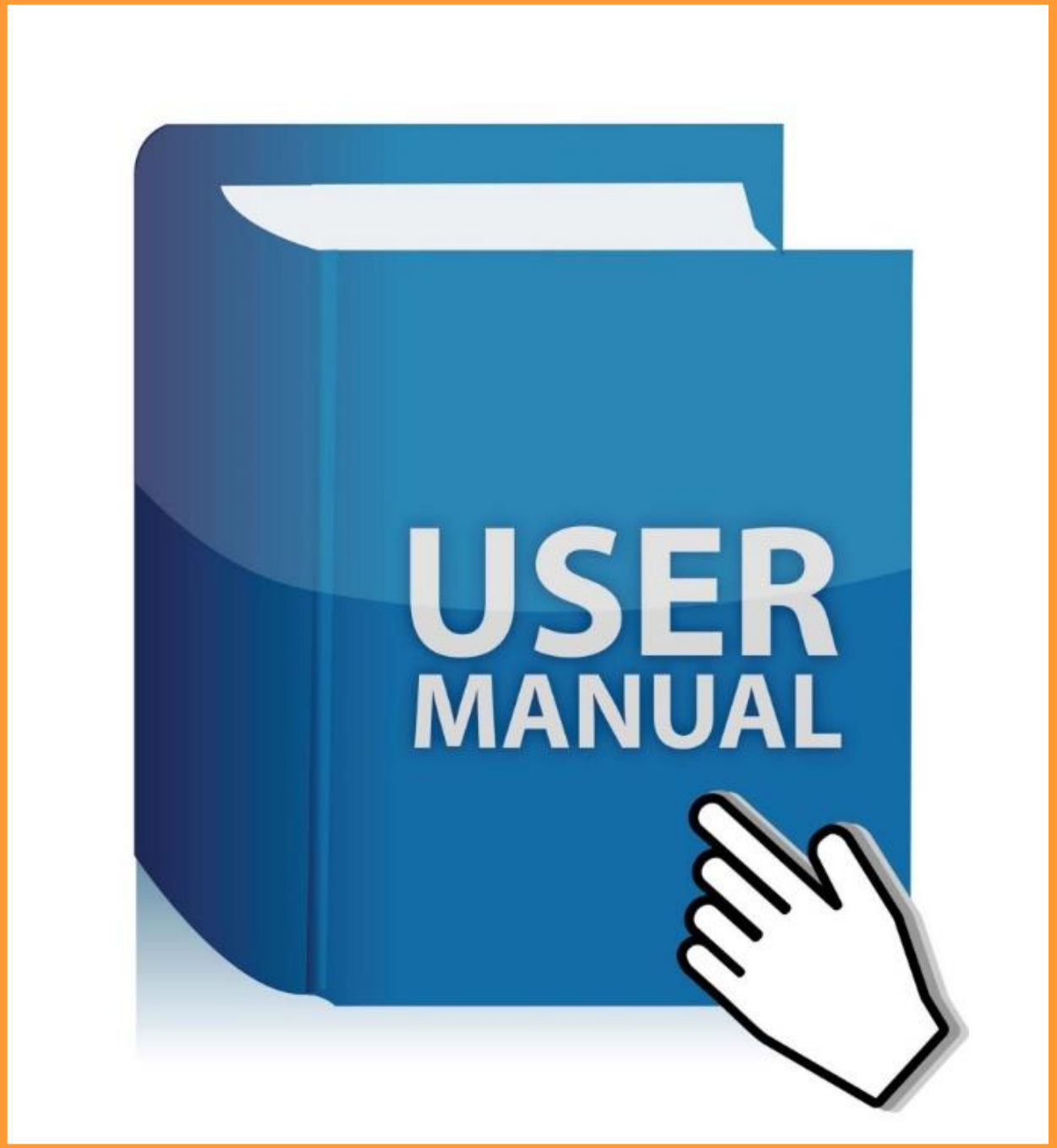
- ✓ Сократилось количество разделов
- ✓ Упростилась логика
- ✓ Действия интуитивны


КОНТРОЛЬ ДЕЙСТВИЙ
Журнал
Уведомления
УПРАВЛЕНИЕ ДОСТУПОМ
Пользователи
isadmin
superadmin
sysadmin
Драгун Святослав Игоревич
Калинкин Илья Геннадьевич
Травкина Ангелина Павловна
Пользователи / Управление доступом / Пользователи / Травкина Ангелина Павловна
Сохранить
Открыть карточку Досье
Учетная запись активна
Имя
Травкина Ангелина Павловна
Логин
ap.travkina
Пароль
Повтор пароля
Электронная почта
ap.travkina@mzprogress.ru
Роли
Суперадминистраторы


КОНТРОЛЬ ДЕЙСТВИЙ
Журнал
Уведомления
УПРАВЛЕНИЕ ДОСТУПОМ
Пользователи
isadmin
superadmin
sysadmin
Драгун Святослав Игоревич
Калинкин Илья Геннадьевич
Травкина Ангелина Павловна
Роли
123
Администраторы безопасности
Системные администраторы
Суперадминистраторы
Пользователи / Управление доступом / Роли / Администраторы безопасности
Сохранить
Пользователи
superadmin
isadmin
Права
Сообщения
Доступные операции
Просмотр
Изменение
Удаление
Доступны только типы сообщений
Типы сообщений
Доступны только адреса
Адреса, домены
Зарегистрированные адреса
Незарегистрированные адреса
Запрещенные адреса
Адреса, домены
Зарегистрированные адреса
Незарегистрированные адреса
Доступны только пометки
Пометки
Запрещенные пометки
Пометки
Доступны только группы Досье
Группы Досье
Запрещенные группы Досье
Группы Досье

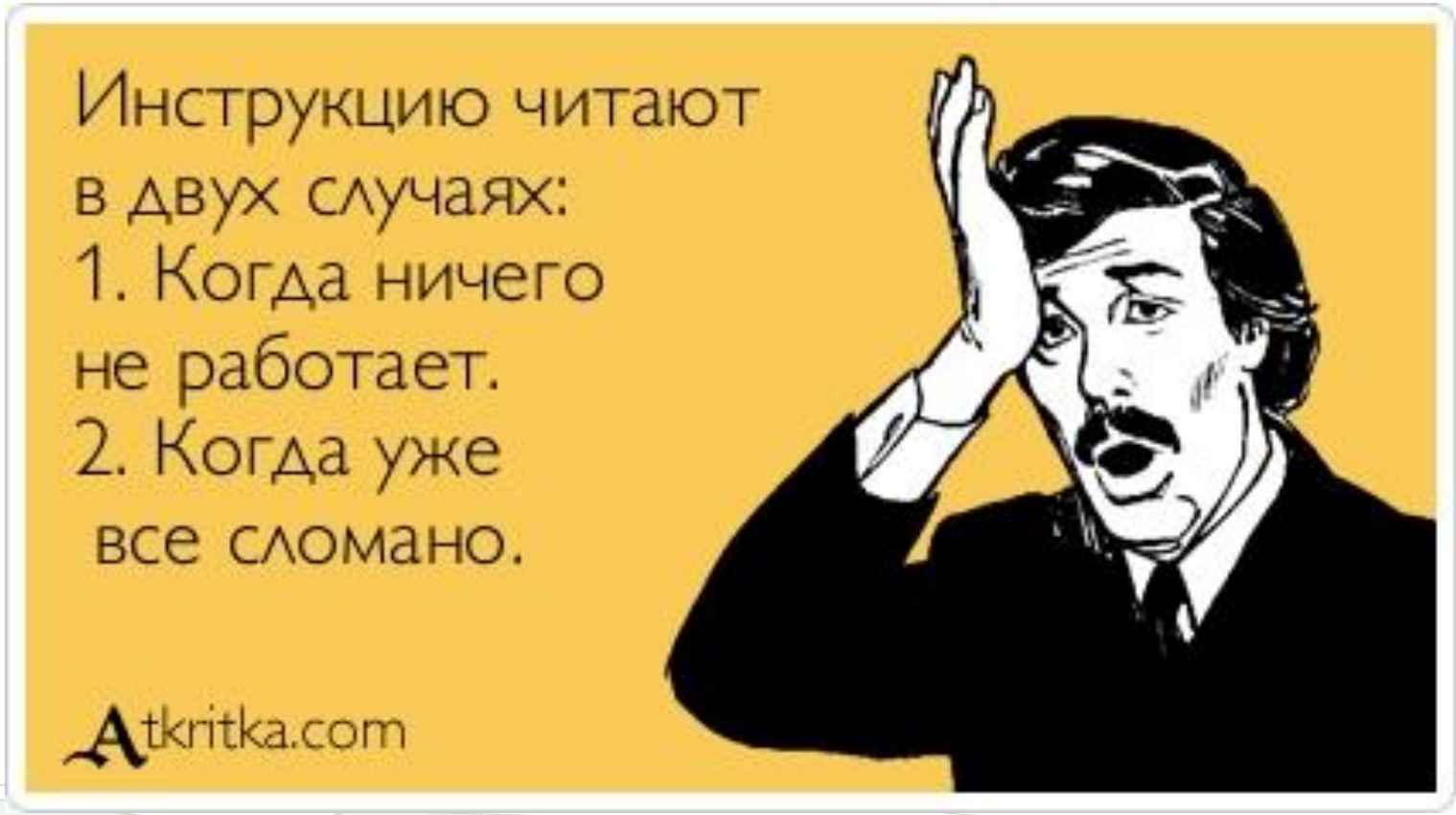
Аудит действий пользователей Системы


КОНТРОЛЬ ДЕЙСТВИЙ
Журнал
Уведомления
УПРАВЛЕНИЕ ДОСТУПОМ
Пользователи
isadmin
superadmin
sysadmin
Драгун Святослав Игоревич
Калинкин Илья Геннадьевич
Травкина Ангелина Павловна
Роли
123
Администраторы безопасности
Пользователи / Контроль действий / Журнал
Действия
Настройки
24 часа
Пользователь
Действие
Все
Описание
Дата
Пользователь
Действие
Статус
Описание
2018 Март 16 23:52:51 superadmin superadmin Просмотр почтового сообщения Выполнен vid: 235cb402-0000-0000-0000-000000510016; subject: Сканирование документа;
2018 Март 16 23:52:18 superadmin superadmin Поиск Выполнен obj: events; name: События | ИО Приказ о поощрении - № Т-11(а) | 7...
2018 Март 16 23:51:54 superadmin superadmin Поиск Выполнен obj: events; name: События | 7 дней;
2018 Март 16 23:51:51 superadmin superadmin Вход в систему Выполнен
2018 Март 16 23:51:46 superadmin superadmin Вход в систему Ошибка error: User superadmin login forbidden: bad credentials;
2018 Март 16 23:48:41 superadmin superadmin Поиск Выполнен obj: events; name: События | 7 дней;
2018 Март 16 23:48:12 superadmin superadmin Поиск Выполнен obj: events; name: События | 7 дней;
2018 Март 16 23:48:10 superadmin superadmin Поиск Выполнен obj: events; name: События;
2018 Март 16 23:44:55 superadmin superadmin Вход в систему Выполнен
2018 Март 16 23:44:09 superadmin superadmin Вход в систему Выполнен



Контекстная справка

Это так по-русски!

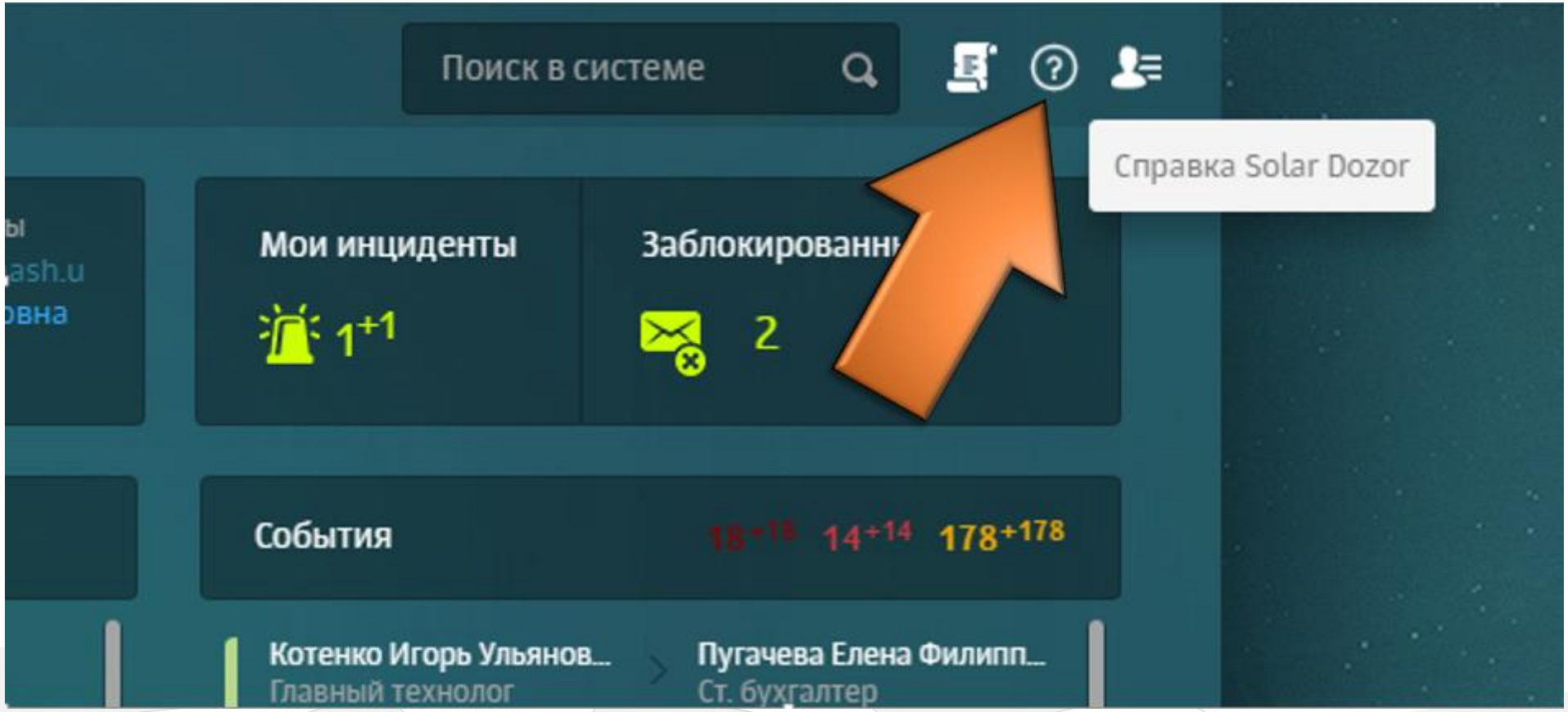


И мы тоже так работали.

- ✓ Руководство пользователя
- ✓ Справочник пользователя
- ✓ Руководство по поиску данных в Solar Dozor
- ✓ Руководство по работе с модулями

И еще огромное множество мануалов!

Спроси меня!


Поиск в системе
Справка Solar Dozor
Мои инциденты
1+1
2
События
18+18
14+14
178+178
Котенко Игорь Ульянов...
Главный технолог
Пугачева Елена Филипп...
Ст. бухгалтер

Справка Solar Dozor

Поиск по справке

РАБОЧИЙ СТОЛ > элементы и функции > общие сведения

ЭЛЕМЕНТЫ И ФУНКЦИИ

Общие сведения

Задание периода времени

Рабочий стол аналитика

Рабочий стол руководителя

ПОЛЕЗНЫЕ СТАТЬИ

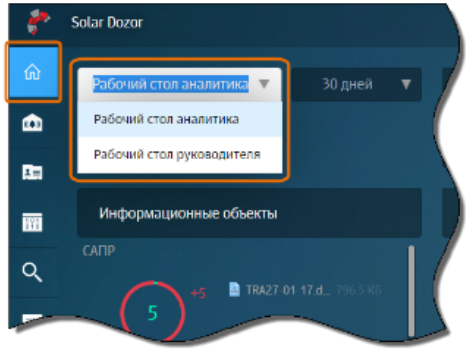
Примеры использования виджетов

Общие сведения

На **Рабочем столе** отображается вся важная информация о зарегистрированных системой текущих событиях ИБ и других объектах контроля службы безопасности.

В специальных виджетах/информерах выводится наиболее важная информация о зафиксированных системой событиях, сгруппированная в соответствии с основными фокусами внимания конкретного специалиста службы безопасности. То есть набор виджетов и информеров на **Рабочем столе** различается в зависимости от того, какой **Рабочий стол** выбран. При условии доступа вы можете выбрать:

- **Рабочий стол аналитика** (РСА): предназначен для офицера безопасности, в обязанности которого входит мониторинг нарушений политики ИБ и своевременное реагирование на них;
- **Рабочий стол руководителя** (РСР): предназначен для руководителя службы ИБ, имеющего в подчинении группу офицеров безопасности, которые используют Solar Dozor в своей деятельности. РСР предоставляет руководителю СИБ возможность быстро получить всю необходимую информацию для анализа оперативной обстановки и принятия решения.



Все данные на РСА и РСР отображаются за указанный период времени.

Еще статьи по теме:

Главное меню

Рабочий стол аналитика

Благодарю за внимание!

Solar Security

127 015 г. Москва, ул. Вятская 35/4, БЦ «Вятка»

Телефон офиса: +7 499 755 07 70

Техническая поддержка: +7 499 755 02 20

Email: info@solarsecurity.ru