Опция «Протоколирование событий»

Опция «Протоколирование событий»предназначена для ведения протокола событий системы «ДЕЛО». Данное системное протоколирование ведется параллельно функциональному протоколированию, встроенному в различные функции системы «ДЕЛО» и не связано с ним.

Далее в тексте, для краткости, вместо термина «Опция «Протоколирование событий» возможно употребление термина «подсистема».

Подсистема ведет протокол следующих операций:

- Вход в систему;
- Завершение сеанса;
- Просмотр данных;
- Изменение данных;
- Создание объекта;
- Удаление объекта;
- Печать;
- Поиск;
- Выполнение.

1. Основные понятия подсистемы

Для того чтобы дальнейшее описание подсистемы было более понятным, следует определить основные понятия.

- Субъект доступа – некто, предъявивший аутентифицирующий идентификатор (логин), имеющий или не имеющий функционального отображения в системе – то есть либо зарегистрированный пользователь ДЕЛА, либо

кто-то, пытающийся авторизироваться в форме аутентификации ДЕЛА.

- Объект доступа – логически (функционально) локализованный набор данных системы, имеющий определённую функциональную задачу. Может быть как самостоятельным набором данных, так и контейнером для других объектов доступа.
- Идентификатор субъекта доступа – имя пользователя системы либо имя, предъявленное в процедуре аутентификации в системе.
- Идентификатор объекта доступа – логическое имя объекта в системе – регистрационная карточка №N, поручение, прикреплённый файл и т.д.
- Полномочия субъекта доступа – набор прав субъекта по отношению к объектам доступа системы.
- Статус объекта доступа – состояние объекта, определяющее возможность произведения действий над ним (например «доступный для чтения», «изменяемый» и т.д.). Может быть как общим, так и по отношению к субъекту доступа.
- Попытка доступа – запрос на выполнение функции или доступа к данным. Может быть удачной – функция отработала, данные получены, или неудачной – неправильное имя/пароль при входе, нарушение прав доступа, отсутствие/недоступность объекта доступа и т.д.

2. Точки протоколирования

Подсистема ведёт протокол следующих событий:

1. Попытки входа и выхода пользователя в/из системы. В случае, когда выход осуществляется аварийно, выход пользователя фиксируется в момент повторного входа этого пользователя при прерывании «висящей» сессии. Неудачные попытки входа протоколируются через технологический логин (пустое имя пользователя).
2. Попытки создания, просмотра, редактирования и удаления РК и РКПД, включая допреквизиты.

3. Попытки создания, просмотра, редактирования и удаления элементов справочников.
4. Попытки создания, просмотра, редактирования и удаления поручений и проектов поручений.
5. Попытки создания, просмотра, редактирования и удаления отчётов об исполнении поручений.
6. Попытки прикрепления, просмотра, редактирования и удаления файлов (РК, РКПД).
7. Попытки вызова поисковых запросов.
8. Попытки печати документов.
    - Для системы «ДЕЛО» – протоколируется факт вызова приложения;
    - Для подсистемы «ДЕЛО-WEB» – протоколируется формирование страницы для печати;
    - Для EAPI (модуль «Отчетные формы», внешние приложения) протоколируется несколько событий EAPI.
9. Попытки создания и удаления пользователей.
10. Попытки блокирования и разблокирования учетных записей пользователей.
11. Попытки модификации прав пользователей, в том числе и через копирование прав от другого пользователя.
12. Попытки очистки протокола.
13. Попытки выгрузки протокола в файл.
14. Удаление сообщений «СЭВ» из каталога «СЭВ» для ручной регистрации документов / проектов документов, выполненное пользователем вручную, или осуществленное автоматически при выполнении пользователем операции отказа в регистрации.

3. Запуск опции

Замечание. Работать с Опцией протоколирования может только пользователь, имеющий право **Системный технолог** с доступом в справочниках к опции «Зачистка протоколов».

- **Запуск Опции протоколирования:**

1. Щелкните на кнопке **Пуск** и выберите раскрывающееся меню **Программы**.
2. В открывшемся списке выберите раскрывающееся меню **Дело**, которое содержит команды запуска модулей и дополнительных опций системы.
3. В списке команд этого меню выберите команду **Опция протоколирования**. На экране появится окно **Вход в систему ДЕЛО** (см. Рис. Ошибка! **Текст указанного стиля в документе отсутствует.**-1).

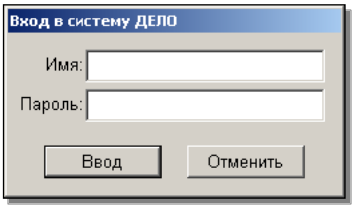

Рис. **Ошибка! Текст указанного стиля в документе отсутствует.**-1. Окно **Вход в систему** ДЕЛО

Внимание. Окно **Вход в систему ДЕЛО** не формируется, если в учетной записи пользователя, запускающего модуль, установлено проводить его аутентификацию с помощью операционной системы. В этом случае при загрузке модуля «Пользователи» пользователь идентифицируется по тем личным параметрам, которые он указал при входе в ОС Windows (см. раздел 12).

4. В поле **Имя** ведите имя (логин) технолога системы и нажмите клавишу **Tab**. Курсор перейдет в поле **Пароль**.
5. Введите с клавиатуры пароль технолога системы и щелкните на кнопке **Ввод** или нажмите клавишу **Enter**.

Внимание. При первом входе в систему в качестве имени и пароля используются имя и пароль владельца базы, которые задаются при установке серверной части (при создании базы данных) системы «ДЕЛО» (см. Руководство администратора).

Если имя и/или пароль введено неверно, на экране появится сообщение, показанное на Рис. Ошибка! **Текст указанного стиля в документе отсутствует.**-2.

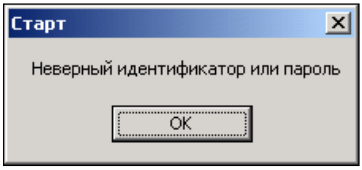

Рис. **Ошибка! Текст указанного стиля в документе отсутствует.**-2. Сообщение при неверном вводе имени и/или пароля

Щелкните кнопку **ОК**, а затем повторите ввод имени и пароля.

4. Главная страница приложения

При запуске приложения «Опция протоколирования» откроется окно **Протокол** с установленным по умолчанию фильтром на текущую дату (см. Рис. Ошибка! **Текст указанного стиля в документе отсутствует.**-3).

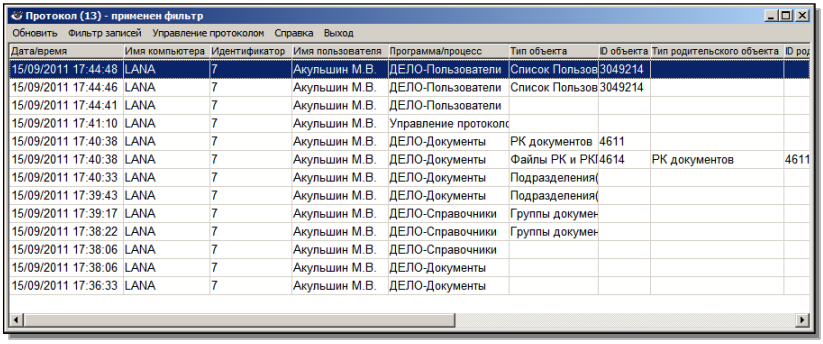

Рис. **Ошибка! Текст указанного стиля в документе отсутствует.**-3. Окно **Протокол**

Рабочая область окна содержит таблицу запротоколированных событий. Таблица отсортирована по дате, последнее событие вверху.

Таблица событий состоит из следующих столбцов:

- **Дата/время** – дата и время события;
- **Имя компьютера** – имя компьютера, с которого было вызвано событие;
- **Идентификатор** – идентификатор субъекта доступа;
- **Имя пользователя** – имя пользователя, вызвавшего событие;
- **Программа/процесс** – имя приложения или подсистемы, в которой произошло событие;
- **Тип объекта** – тип объекта доступа;
- **ID объекта** – системный идентификатор объекта доступа;
- **Тип родительского объекта** – тип объекта, являющегося родителем объекта доступа;
- **ID родительского объекта** – системный идентификатор родительского объекта;
- **Операция** – название операции, вызвавшей событие;
- **Результат** – результат выполнения операции (*Успешно* или *Не успешно*);
- **Комментарий** – текстовый комментарий (например, причина отказа в доступе).

Строка меню окна **Протокол** содержит пункты:

- **Обновить** – считывание данных протокола в рабочую область окна и пересчет их количества (при превышении допустимого количества записей выдается сообщение о необходимости экспорта и очистки протокола);
- **Фильтр записей** – вызов функции установки фильтров отображения протокола в рабочей области;
- **Управление протоколом** – вызов функции управления протоколом;

- **Выход** – завершение работы с приложением.

В заголовке окна в скобках указано количество отображаемых записей. Если в окне применен фильтр записей, то в заголовке окна будет отображаться текст «применен фильтр».

Внимание. По умолчанию при открытии окна в нем применен фильтр по дате/времени – задан отбор записей за текущую дату с начала суток по текущее время.

5. Фильтр записей

Окно функции представлено на Рис. Ошибка! **Текст указанного стиля в документе отсутствует.**-4. Окно содержит поля ввода значений для фильтрации. Пустые текстовые поля означают, что фильтрация по этим полям не производится.

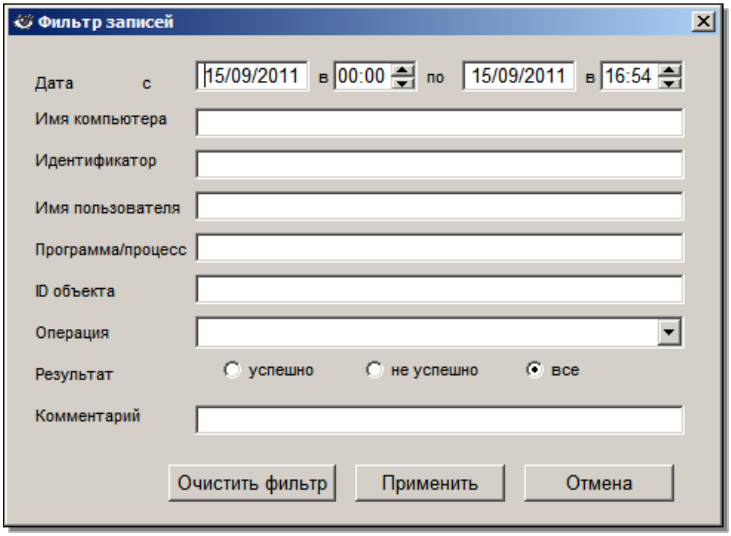

Рис. **Ошибка! Текст указанного стиля в документе отсутствует.**-4 Окно Фильтр записей

Ниже приведено описание полей фильтрации:

- **Дата.** Указывается временной промежуток, за который нужно отображать события. Дата и время указывается включительно, причём если не указана какая-либо граница

интервала, то интервал не будет ограничен. По умолчанию при открытии окна протокола в данных полях задан интервал – текущая дата с начала суток по текущее время.

- **Имя компьютера.** Текстовое поле – указывается имя компьютера.
- **Идентификатор.** Текстовое поле – указывается идентификатор субъекта доступа.
- **Имя пользователя.** Текстовое поле – указывается имя пользователя.
- **Программа/процесс.** Текстовое поле – указывается название программы или процесса, в которой произошли события.
- **ID объекта.** Текстовое поле – указывается системный идентификатор объекта доступа. Поле является обязательным.
- **Операция.** Тип операции, вызвавшей событие, выбирается из выпадающего списка доступных операции.
- **Результат.** Результат выполнения операции, устанавливается установкой переключателя в нужное положение («успешно», «не успешно» или «все»).
- **Комментарий.** Текстовое поле – указывается комментарий.

Поля фильтров **Идентификатор**, **Имя пользователя**, **Программа/процесс**, **Объект** и **Комментарий** - текстовые, неформатированные. Выводятся записи, содержащие в соответствующих полях блоки текста, указанные в фильтрах. Разделение блоков текста в поле фильтра – символом «;», заглавные буквы приравниваются к строчным. Например, фильтр «Имя пользователя», содержащий «Иванов; Петров» выводит все записи, в поле «Имя пользователя» которых содержится значение «Иванов» или «Петров» - «Иванов И.И.», «Петров П.П.», «Петровский В. В.», «Диванов Д.Д.» и т.д.

Кнопка **Очистить фильтр** служит для очистки всех введенных значений фильтра.

При нажатии кнопки **Применить** к таблице событий применяется фильтр с указанными значениями, окно закрывается, а информация в рабочей области главного окна обновляется.

Чтобы снять фильтр, нужно нажать кнопку **Отмена**. При этом окно закрывается, а в рабочей области главного окна отображаются неотфильтрованные записи.

Значение применённых фильтров сохраняется в течение сеанса работы приложения. Запуск приложения происходит с установленным фильтром по дате/времени – отбором записей за текущую дату с начала суток по текущее время.

6. Управление протоколом

Функция **Управление протоколом** служит для настройки параметров протоколирования событий в системе, таких как количество записей в протоколе и периодичность обновления, а также позволяет включать и отключать протоколирование и производить выгрузку протокола.

Окно функции показано на Рис. Ошибка! **Текст указанного стиля в документе отсутствует.**-5.

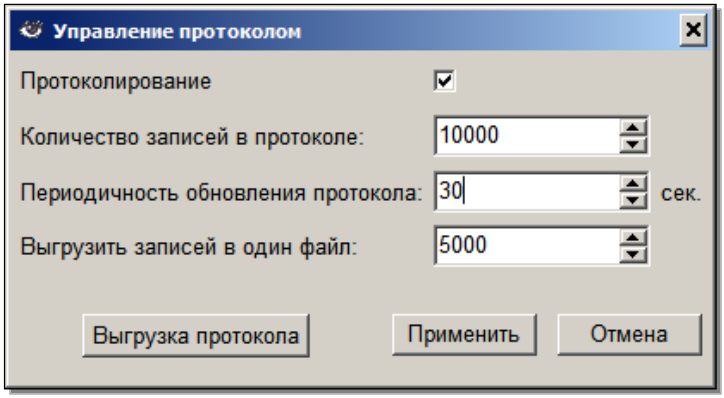

Рис. **Ошибка! Текст указанного стиля в документе отсутствует.**-5 Окно **Управление протоколом**.

В поле **Количество записей в протоколе** указывается допустимое количество записей. При достижении количества записей этого значения, подсистема выдает соответствующее предупреждение (см. Рис. Ошибка! **Текст указанного стиля в документе отсутствует.**-6):

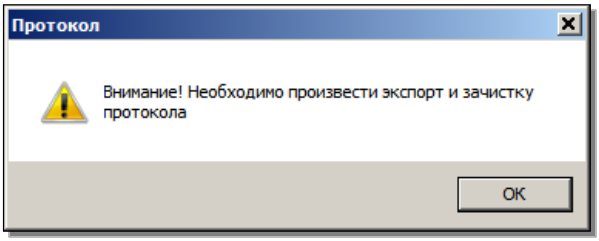

Рис. **Ошибка! Текст указанного стиля в документе отсутствует.**-6. Системное предупреждение

В поле **Периодичность обновления протокола** вводится временной интервал, через который обновляется таблица в рабочей части окна.

В поле **Выгрузить записей в один файл** указывается максимальное количество записей, выгружаемое в один файл при выгрузке протокола. Данный параметр применяется при выполнении операции выгрузки протокола (см. подпункт «Выгрузка и очистка протокола» настоящего пункта). По умолчанию установлено значение «5000». Отметим, что в параметре значение «0» недопустимо, поэтому если его установить, то при сохранении оно будет автоматически заменено на умолчательное значение «5000».

Для того чтобы включить протоколирование, следует установить флажок **Протоколирование**.

Отметим, что даже при отключенном протоколировании ведется протоколирование следующих событий:

- Попытки входа и выхода пользователя в/из системы;
- Попытки создания и удаления учетных записей пользователей;
- Попытки блокировки/разблокирования учетных записей пользователей;
- Попытки модификации прав пользователей (в том числе и через копирование прав от другого пользователя), а также изменение пароля пользователя;
- Попытки очистки протокола;
- Попытки выгрузки протокола в файл.

7. Выгрузка и очистка протокола

Для того, чтобы выгрузить информацию из протокола в окне функции **Управление протоколом** (см Рис. Ошибка! **Текст указанного стиля в документе отсутствует.**-5) нужно щелкнуть кнопку **Выгрузка протокола**.

В появившемся диалоговом окне укажите каталог выгрузки и имя файла, в который следует выгрузить протокол. По умолчанию задано имя файла, соответствующее текущей дате в формате ГГГГ-ММ-ДД.

Щелкните кнопку **Сохранить**. После этого опция произведет выгрузку протокола и выдаст запрос на очистку протокола (см. Рис. Ошибка! **Текст указанного стиля в документе отсутствует.**-7):

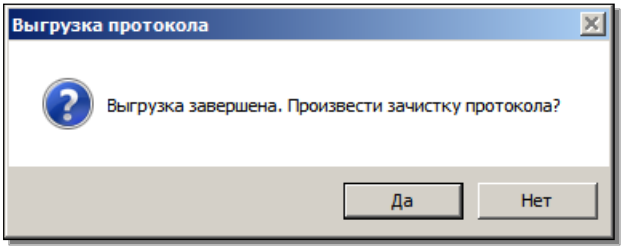

Рис. **Ошибка! Текст указанного стиля в документе отсутствует.**-7. Запрос подтверждения очистки протокола

При щелчке на кнопке **Да**, протокол событий будет очищен, и в нем останутся только записи о выгрузке протокола и об очистке протокола.

При щелчке на кнопке **Нет** очистка протокола не производится, в протокол добавляется запись о выгрузке протокола.

Замечание. Отметим, что если в окне применен установленный по умолчанию фильтр по дате/времени, то новые записи (о выгрузке и об очистке протокола) не будет видно, т.к. они сформированы позже времени открытия окна протокола. Чтобы эти записи отобразились, измените в фильтре значение текущего времени, или отмените фильтр.

Протокол выгружается в текстовый файл или несколько файлов, размещенных в указанном каталоге выгрузки. На количество создаваемых файлов выгрузки влияют количество записей в протоколе и значение параметра **Выгрузить записей в один файл**, установленного в окне «Управление протоколом». Если создается несколько файлов выгрузки, то к имени каждого файла прибавляется через нижнее подчеркивание порядковый номер файла (см. Рис. Ошибка! **Текст указанного стиля в документе отсутствует.**-8).

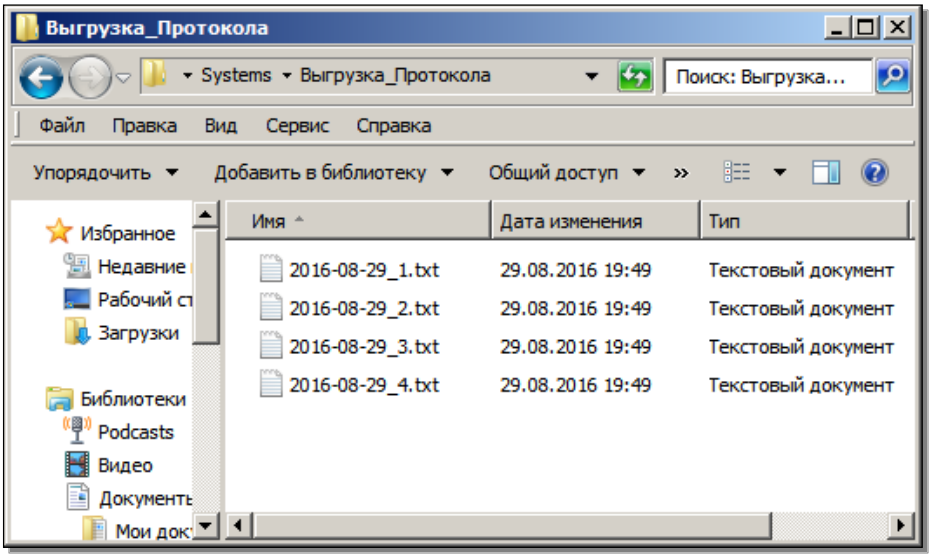

Рис. **Ошибка! Текст указанного стиля в документе отсутствует.**-8 – Файлы выгрузки протокола