



Руководство по мониторингу безопасности

Листов: 24

АННОТАЦИЯ

В настоящем документе приводятся сведения о функциональных возможностях, назначении и условиях применения программного модуля «Монитор безопасности», входящего в состав Системы планирования и проведения закупок «Е1-Закупки».

В документе приводится описание операций, которые выполняет пользователь при работе с модулем, а также действий по разрешению аварийных ситуаций, которые могут возникнуть в процессе работы.

СОДЕРЖАНИЕ

1. Глоссарий.....	4
2. Введение	5
2.1. Область применения	5
2.2. Общие сведения о мониторинге безопасности	5
3. Назначение и условия применения	6
3.1. Автоматизируемые виды деятельности и функции.....	6
3.2. Требования к аппаратно-программному обеспечению	6
3.3. Уровень подготовки пользователей	6
4. Подготовка к работе	7
4.1. Общий порядок работы в модуле «Монитор безопасности»	7
4.2. Запуск и завершение сеанса работы с модулем	7
4.3. Описание главного окна модуля.....	9
5. Описание операций.....	12
5.1. Просмотр сообщений о событиях.....	12
5.2. Настройка приема сообщений о событиях	13
5.2.1. Включение и отключение автоматического обновления списка сообщений о событиях.....	13
5.2.2. Настройка параметров приема сообщений о событиях	13
5.3. Настройка отображения списка сообщений о событиях.....	15
5.3.1. Сортировка списка сообщений о событиях.....	15
5.3.2. Группировка сообщений о событиях	15
5.3.3. Отображение списка сообщений, относящихся к определенному временному интервалу	15
5.3.4. Фильтрация сообщений о событиях.....	16
5.4. Управление подключениями пользователей	20
5.5. Формирование отчета по пользователям	21
5.6. Сохранение списка сообщений.....	22
5.7. Копирование сообщений о событиях	22
5.8. Вывод на печать списка сообщений о событиях	23
6. Аварийные ситуации	24

1. ГЛОССАРИЙ

В рамках настоящего документа использован набор сокращений и терминов, приведенных в таблицах 1 и 2 соответственно.

Таблица 1 — Сокращения

Сокращение	Расшифровка
БД	База данных
ОС	Операционная система
ПО	Программное обеспечение
Система	Система планирования и проведения закупок «Е1-Закупки»
СУБД	Система управления базами данных

Таблица 2 — Термины

Термин	Определение
Веб-клиент	Программное средство, предназначенное для работы с Системой через веб-интерфейс (с помощью интернет-обозревателя на компьютерах и мобильных устройствах)
Действие	Действие с защищаемыми объектами Системы — документами, поручениями, группами пользователей и т. п.
Событие	Результат выполнения определенного действия (например, редактирование документа, отправка документа по почте и т. д.)

2. ВВЕДЕНИЕ

2.1. Область применения

Система планирования и управления закупками «Е1-Закупки» (далее — Система) предназначена для автоматизации процессов планирования и проведения закупок товаров, работ, услуг для обеспечения удовлетворения потребностей в товарах, работах, услугах отдельных видов юридических лиц в соответствии с определенными нормативными документами.

2.2. Общие сведения о мониторинге безопасности

Средствами модуля «Монитор безопасности» обеспечивается мониторинг действий, которые были выполнены пользователями при работе с модулями Системы. Кроме того, средствами модуля обеспечивается возможность принудительного отключения от сервера Системы пользователя, работающего с одним из модулей Системы.

Модуль «Монитор безопасности» предназначен для получения информации о событиях, происходящих в Системе, в том числе попыток несанкционированного доступа. Полученная информация может быть использована для разрешения ситуаций, связанных со случайными или ошибочными действиями пользователей Системы.

В качестве *события* в Системе рассматривается результат выполнения определенного действия (например, редактирование документа, отправка документа по почте и т. д.). Под действием подразумеваются не любые манипуляции с данными, а только действия с защищаемыми объектами Системы — документами, поручениями, группами пользователей и т. п.

Информация о событиях сохраняется на сервере Системы с момента его установки. С помощью модуля «Монитор безопасности» информацию о событиях можно просматривать в виде списка сообщений о событиях, происходящих в Системе — *Журнала аудита*.

Журнал аудита доступен для просмотра и обработки. Информация, хранящаяся в Журнале аудита, недоступна для изменения и удаления.

3. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

3.1. Автоматизируемые виды деятельности и функции

Система предназначена для автоматизации процессов планирования и проведения закупок, в частности, в ходе указанных процессов пользователи регистрируют, просматривают и редактируют различные документы Системы. Модуль «Монитор безопасности» предоставляет возможности для получения информации о событиях, происходящих на сервере Системы.

3.2. Требования к аппаратно-программному обеспечению

Требования к аппаратно-программному обеспечению рабочего места пользователя, работающего с модулем «Монитор безопасности», совпадают с требованиями к программному обеспечению Системы, описанными в документе «Руководство по инсталляции».

3.3. Уровень подготовки пользователей

Настоящий документ рассчитан на пользователей, имеющих следующие знания и навыки:

- использование клавиатуры и устройства «мышь» (далее — мышь);
- работа со стандартными элементами графического интерфейса приложений, работающих под управлением операционной системы (ОС) Microsoft Windows;
- работа с программой «Проводник» и программами пакета Microsoft Office;
- составление логических условий;
- понимание бизнес-процессов, происходящих в организации, а также знание нормативных документов, которым они подчиняются;
- понимание общего принципа работы приложений на основе клиент-серверной технологии, подразумевающее понимание такого термина как «сервер».

Кроме того, пользователю следует ознакомиться с документом «Руководство администратора» и настоящим руководством.

4. ПОДГОТОВКА К РАБОТЕ

4.1. Общий порядок работы в модуле «Монитор безопасности»

Средствами модуля «Монитор безопасности» обеспечивается выполнение следующих функций:

- просмотр сообщений о событиях, происходящих в Системе;
- настройка параметров приема сообщений;
- включение и отключение автоматического обновления списка сообщений о событиях;
- сортировка и группировка сообщений о событиях по различным параметрам;
- отображение списка сообщений, относящихся к определенному временному интервалу;
- фильтрация сообщений о событиях по различным параметрам;
- управление подключениями пользователей к серверу;
- формирование отчета по пользователям;
- сохранение сообщений о событиях в файле (TXT, XLSX или CEF);
- копирование сообщения о событии в буфер обмена;
- вывод на печать сообщений о событиях.

Общий порядок работы в модуле «Монитор безопасности» со списком сообщений о событиях в Системе представлен на рисунке 1.

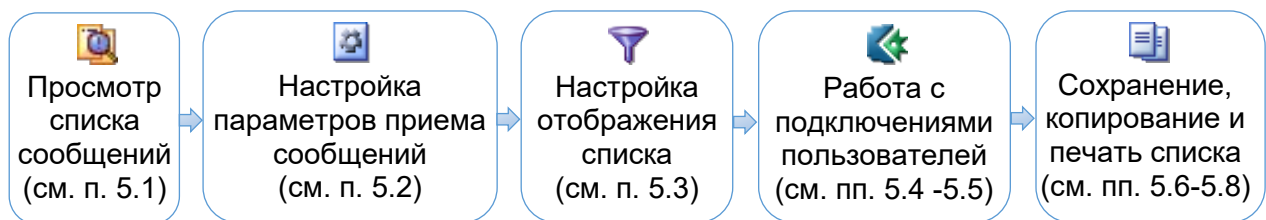


Рисунок 1

4.2. Запуск и завершение сеанса работы с модулем

Доступ к функциональным возможностям модуля «Монитор безопасности» открыт только для пользователей, обладающих правами администратора Системы (права доступа и их разграничение описаны в документе «Руководство администратора»).

Для того чтобы запустить сеанс работы с модулем «Монитор безопасности»:

1) в зависимости от версии ОС, в главном меню Microsoft Windows выберите один из следующих пунктов:

- **Пуск — Все программы — E1 Закупки — Администрирование — Монитор безопасности;**

- **Пуск — Все приложения — E1 Закупки — Монитор безопасности.**

В результате откроется окно **Подключение к серверу** (рис. 2);

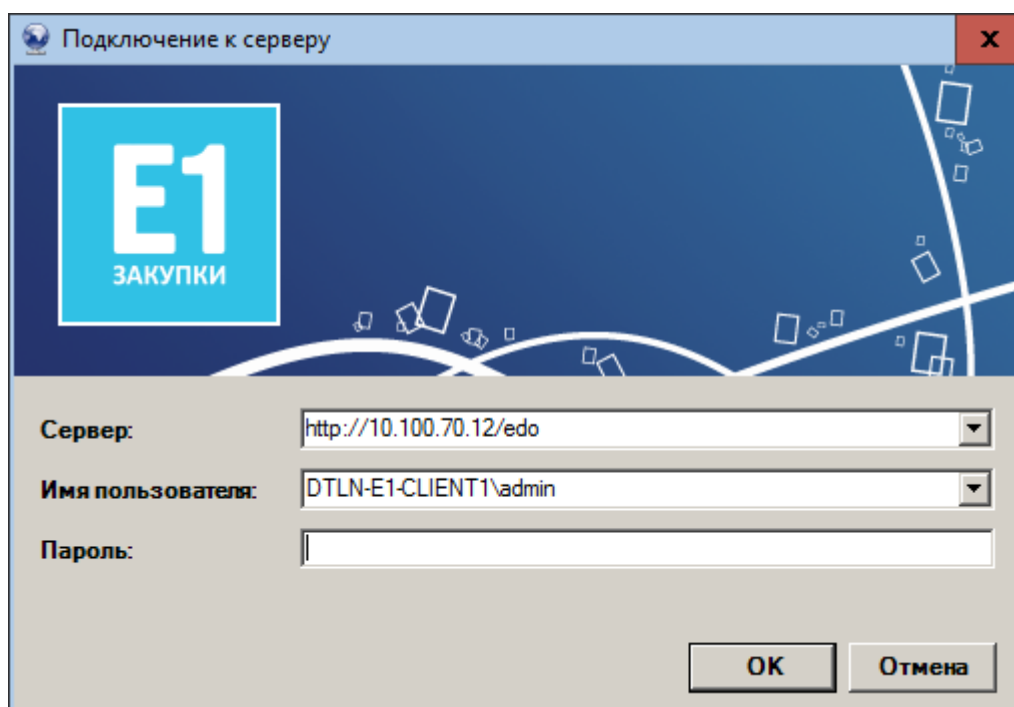


Рисунок 2

2) в поле **Сервер** укажите сетевое имя сервера приложений в формате **http://<сетевое имя сервера приложений>/edo;**

3) выполните одно из следующих действий:

- для запуска модуля «Монитор безопасности» от имени текущего пользователя Microsoft Windows, оставьте поля **Имя пользователя** и **Пароль** пустыми;

- для запуска модуля «Монитор безопасности» от имени другого пользователя, в поле **Имя пользователя** укажите логин этого пользователя в формате **<название домена>\<имя пользователя>**, а в поле **Пароль** — пароль учетной записи для входа в домен;

4) нажмите на кнопку **ОК**. В результате откроется главное окно модуля «Монитор безопасности» (см. п. 4.3).

Для того чтобы завершить сеанс работы с модулем «Монитор безопасности», в главном окне модуля (см. п. 4.3) нажмите на кнопку **Заккрыть** **✕**, расположенную в правом верхнем углу окна.

4.3. Описание главного окна модуля

Вид главного окна модуля «Монитор безопасности» представлен на рисунке 3.

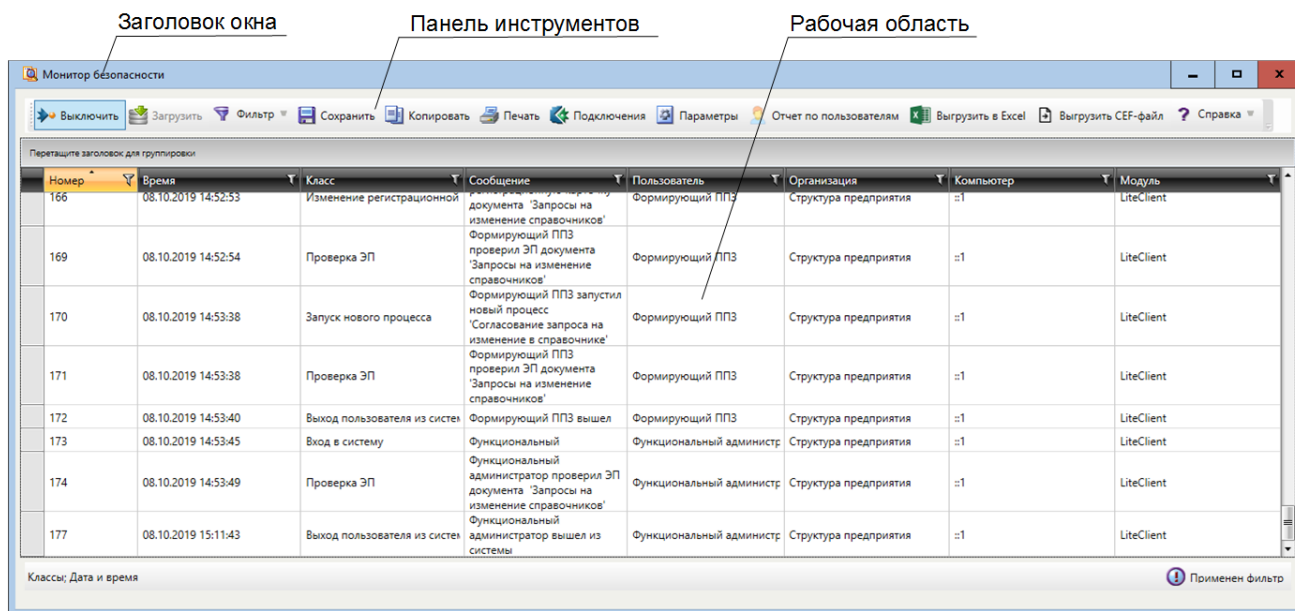





Рисунок 3















В заголовке главного окна модуля указывается название модуля.



В верхней части главного окна модуля расположена *панель инструментов*, содержащая кнопки для работы с модулем. Набор кнопок панели инструментов зависит от включенного *режима работы с модулем* (см. таблицу 3).

Большинство операций в модуле выполняется в *основном режиме*, при котором в рабочей области отображается список сообщений о событиях. Кроме того, предусмотрены следующие вспомогательные режимы: *режим настройки параметров фильтрации списка сообщений*, *режим настройки параметров приема новых сообщений* и *режим настройки параметров отчета по пользователям*. На рис. 3 главное окно имеет вид, соответствующий основному режиму работы с модулем.

Таблица 3 — Описание кнопок панели инструментов в зависимости от режима работы с модулем

Кнопка	Назначение
Основной режим работы с модулем	
Включить  (Выключить )	Включение и отключение автоматического обновления списка сообщений
Загрузить 	Просмотр списка сообщений о событиях, относящихся к определенному временному интервалу

Кнопка	Назначение
Фильтр 	Вызов меню фильтрации, содержащего следующие пункты: - Изменить . Пункт предназначен для перехода от основного режима работы с модулем к режиму настройки параметров фильтрации списка сообщений; - Очистить . Пункт предназначен для отмены фильтрации списка сообщений
Сохранить 	Сохранение списка сообщений о событиях в файле формата txt
Копировать 	Копирование выделенных сообщений о событиях в буфер обмена
Печать 	Печать списка сообщений о событиях
Подключения 	Просмотр списка системных имен пользователей и IP-адресов компьютеров, на которых в данный момент запущен сеанс работы с каким-либо модулем Системы
Параметры 	Переход к режиму настройки параметров приема новых сообщений
Отчет по пользователям 	Переход к режиму настройки параметров отчета по пользователям
Выгрузить в Excel 	Выгрузка Журнала аудита файл Excel
Выгрузить в SEF-файл 	Ручной запуск выгрузки Журнала аудита в SEF-файл
Справка ?	Вызов меню справки, содержащего следующие пункты: - Справка . Пункт предназначен для вызова справки; - О программе . Пункт предназначен для вызова окна с информацией о версии программного модуля
Режим настройки параметров фильтрации списка сообщений	
Применить 	Сохранение указанных параметров фильтрации и переход к основному режиму работы с модулем с учетом этих параметров
Отмена 	Отмена изменений, внесенных в параметры фильтрации, и переход к основному режиму работы с модулем
Параметры 	Переход к режиму настройки параметров приема новых сообщений
Справка ?	Вызов меню справки, содержащего следующие пункты: - Справка . Пункт предназначен для вызова справки; - О программе . Пункт предназначен для вызова окна с информацией о версии программного модуля
Режим настройки параметров приема новых сообщений	
Применить 	Сохранение указанных параметров приема новых сообщений и переход к предыдущему режиму работы с модулем с учетом этих параметров
Отмена 	Отмена изменений, внесенных в параметры приема новых сообщений, и переход к основному режиму работы с модулем
Справка ?	Вызов меню справки, содержащего следующие пункты: - Справка . Пункт предназначен для вызова справки; - О программе . Пункт предназначен для вызова окна с информацией о версии программного модуля
Режим настройки параметров отчета по пользователям	

Кнопка	Назначение
Выгрузить в Excel 	Выгрузка отчета по пользователям файл Excel
Вернуться 	Отмена группировки и переход к основному режиму работы

5. ОПИСАНИЕ ОПЕРАЦИЙ

5.1. Просмотр сообщений о событиях

Модуль «Монитор безопасности» обеспечивает просмотр информации о событиях, происходящих в Системе.

Список сообщений о событиях отображается в хронологическом порядке в главном окне модуля «Монитор безопасности» в табличном виде. Каждая строка сообщения содержит информацию об определенных характеристиках события. Каждой характеристике соответствует отдельный столбец таблицы. Названия столбцов и характеристик событий приводятся в таблице 4.

Таблица 4 — Названия столбцов и характеристики событий

Название столбца	Характеристика события
Номер	Уникальный идентификатор сообщения, под которым это сообщение сохранено на сервере Системы
Время	Дата и время, когда произошло событие
Класс	Класс события
Сообщение	Описание события. Кроме того, в данном столбце могут отображаться системные сообщения, которые при возникновении конфликтных ситуаций позволяют получить более подробную информацию
Пользователь	Системное имя пользователя, действия которого вызвали событие
Организация	Название организации, в которой состоит пользователь
Компьютер	Системное имя или IP-адрес компьютера, с которого выполнено подключение к серверу
Модуль	Название модуля Системы, в котором было выполнено действие, повлекшее событие

По умолчанию отображается список сообщений о последних событиях, произошедших в Системе. Сообщения обо всех событиях можно просмотреть в списке событий ОС Microsoft Windows в журнале приложений «Закупки» на компьютере, на котором установлен сервер приложений Системы.


Примечание 1. В ОС Microsoft Windows 7, Microsoft Windows Server 2008 и более поздних версиях этот журнал включен в журнал приложений «Закупки», а в более ранних версиях ОС Microsoft Windows — в список всех журналов.



5.2. Настройка приема сообщений о событиях


В модуле позволяет осуществить следующие настройки приема сообщений о событиях, происходящих в Системе:

- 1) включение/отключение автоматического обновления списка сообщений (см. п. 5.2.1);
- 2) настройка параметров приема сообщений (см. п. 5.2.2).

5.2.1. Включение и отключение автоматического обновления списка сообщений о событиях

Список сообщений о событиях обновляется автоматически с определенной периодичностью (см. п. 5.2.2). При этом на панели инструментов кнопка **Выключить**  подсвечена.

Для того чтобы отключить автоматическое обновление, на панели инструментов нажмите на кнопку **Выключить** . В результате эта кнопка не будет подсвечиваться на панели инструментов, а ее название изменится на **Включить** .


Для того чтобы вновь включить автоматическое обновление, на панели инструментов нажмите на кнопку **Включить** .

5.2.2. Настройка параметров приема сообщений о событиях

Средствами модуля «Монитор безопасности» обеспечивается возможность настройки следующих параметров приема сообщений:

- период обновления списка сообщений;
- сопровождение звуковым сигналом;
- сопровождение дополнительным системным оповещением;
- выделение цветом строк списка, соответствующих определенным классам событий.

Для того чтобы указать параметры приема сообщений:

1) на панели инструментов нажмите на кнопку **Параметры** . В результате работа с модулем будет переведена в режим настройки параметров приема новых сообщений, и в рабочей области отобразятся параметры приема сообщений (рис. 4);

2) при необходимости в поле **Обновление сообщений каждые** измените период обновления, указав значение в секундах от 1 до 100;

3) для того чтобы задать новое условие, определяющее способ оповещения о событиях, выполните двойной щелчок левой кнопкой мыши в пустой строке таблицы в столбце **Класс сообщения**. В результате в ячейке раскроется список;

4) из раскрывшегося списка выберите класс сообщения, о приеме которого следует оповещать специальным образом. В нижней части таблицы отобразится пустая строка для задания другого класса;

5) если прием сообщений, относящихся к данному классу, следует сопровождать звуковым сигналом, установите флажок в столбце **Звук**;


6) если прием сообщений, относящихся к данному классу, следует сопровождать дополнительным системным оповещением, установите флажок в столбце **Сообщение**. Пример такого сообщения представлен на рисунке 5;

7) если сообщения, относящиеся к данному классу, в списке следует выделять цветом, выполните следующие действия:

- выполните двойной щелчок левой кнопкой мыши в столбце **Цвет**;

- из раскрывшегося списка выберите цвет, которым будут выделены сообщения;

8) при необходимости повторите шаги (3) — (7) для следующего класса сообщений;

9) для того чтобы сохранить указанные параметры приема новых сообщений, на панели инструментов нажмите на кнопку **Применить** .

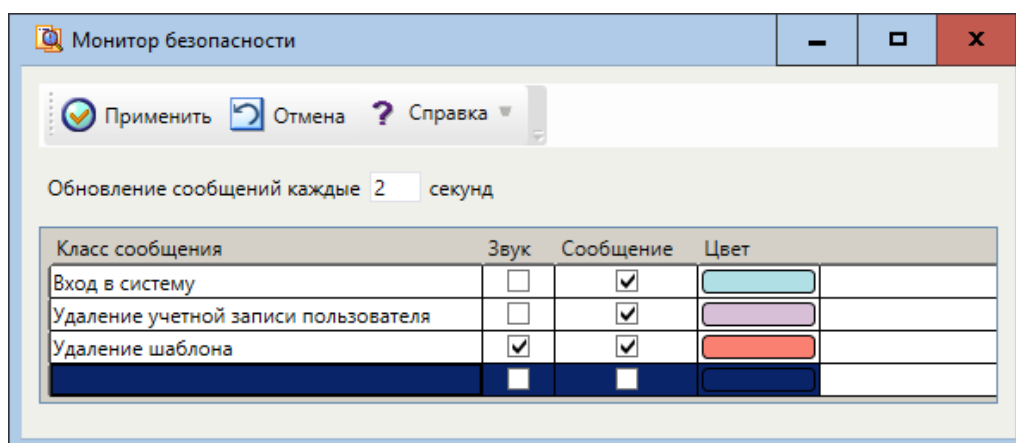


Рисунок 4

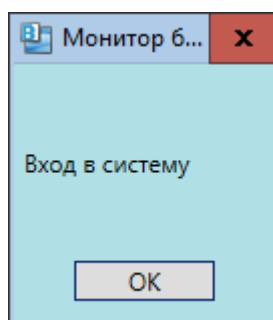



Рисунок 5

Для того чтобы отменить изменения, внесенные при настройке параметров приема новых сообщений, на панели инструментов нажмите на кнопку **Отмена** .

Для редактирования параметров приема одного из классов сообщений выполните двойной щелчок левой кнопкой мыши в строке с интересующим классом сообщений и выполните необходимую настройку.

5.3. Настройка отображения списка сообщений о событиях

5.3.1. Сортировка списка сообщений о событиях

Сортировка списка сообщений выполняется для числовых данных по возрастанию или убыванию, а для текстовых — в алфавитном или обратном алфавитном порядке.

Сообщения о событиях сортируются по названиям столбцов. Названиям столбцов соответствуют характеристики событий. Описание характеристик событий и соответствующих им столбцов приведено в таблице 4.

Для того чтобы отсортировать сообщения, выберите название столбца, соответствующее характеристике, по которой следует выполнить сортировку. В результате сообщения будут отсортированы по этой характеристике.

5.3.2. Группировка сообщений о событиях

Для того чтобы сгруппировать сообщения по одному или нескольким реквизитам:

1) в главном окне модуля «Монитор безопасности» в шапке таблицы со списком сообщений о событиях поднесите курсор мыши к заголовку столбца, по значениям которого следует сгруппировать список;

2) нажмите левую кнопку мыши и, удерживая ее, перетащите этот заголовок в область выше списка, где отображается надпись «Перетащите заголовок для группировки»;

3) отпустите левую кнопку мыши. В результате список сообщений будет сгруппирован по возрастанию значений выбранного реквизита. Чтобы сгруппировать список по убыванию значений этого реквизита, повторно щелкните левой кнопкой мыши по его названию;



4) повторите шаги (1)–(3) для каждого реквизита, по которому следует сгруппировать список.

Для того чтобы отменить группировку по выбранному реквизиту, аналогичным образом перетащите его из области над таблицей в то место шапки таблицы, куда следует вернуть соответствующий столбец.

5.3.3. Отображение списка сообщений, относящихся к определенному временному интервалу

По умолчанию в модуле «Монитор безопасности» отображается список сообщений о последних событиях, произошедших в Системе.

Для того чтобы отобразить только события, относящиеся к определенному временному интервалу:

- 1) выключите автоматическое обновление списка сообщений (см. п. 5.2.1);
- 2) на панели инструментов нажмите на кнопку **Загрузить** . В результате откроется окно **Загрузить данные** (рис. 6);
- 3) для того чтобы указать нижнюю (верхнюю) границу интересующего диапазона:
 - нажмите на кнопку , расположенную справа от соответствующего поля;
 - в отобразившемся календаре (рис. 7) выберите дату;
 - нажмите на кнопку **ОК**;
- 4) в окне **Загрузить данные** нажмите на кнопку **ОК** (рис. 6). В результате в главном окне модуля отобразятся только те события, которые произошли в указанном временном интервале.

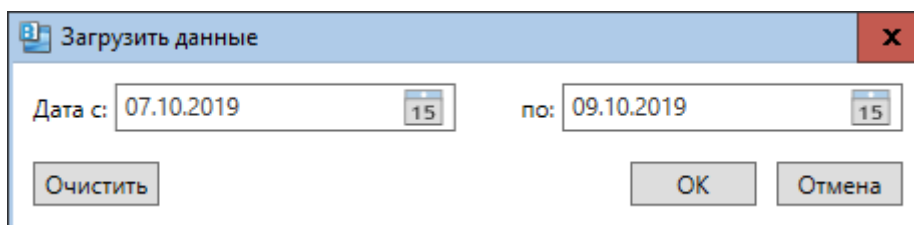


Рисунок 6

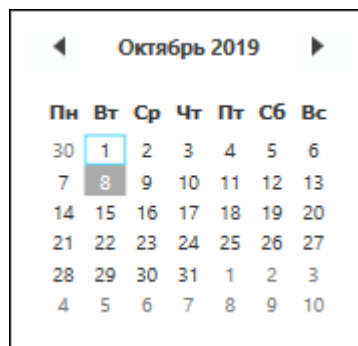



Рисунок 7

Для того чтобы очистить параметры отображения данных выполните одно из следующих действий:

- на панели инструментов нажмите на кнопку **Загрузить**  и в открывшемся окне нажмите на кнопку **Очистить**;
- включите автоматическое обновление списка сообщений (см. п. 5.2.1).


5.3.4. Фильтрация сообщений о событиях

5.3.4.1. Правила наложения условий фильтрации

Модуль «Монитор безопасности» позволяет настроить список сообщений модуль таким образом, чтобы в списке отображались не любые сообщения, а

соответствующие определенным критериям, т. е. наложить *фильтр* на список сообщений, задав *параметры фильтрации*.

Для того чтобы отобразить параметры фильтрации:

- 1) на панели инструментов нажмите на кнопку **Фильтр** ;
- 2) в отобразившемся меню выберите пункт **Изменить**. В результате работа с модулем будет переведена в режим настройки параметров фильтрации списка сообщений, и в рабочей области отобразятся параметры фильтрации (рис. 8). Описание элементов рабочей области модуля «Монитор безопасности» в режиме настройки параметров фильтрации представлено в таблице 5.

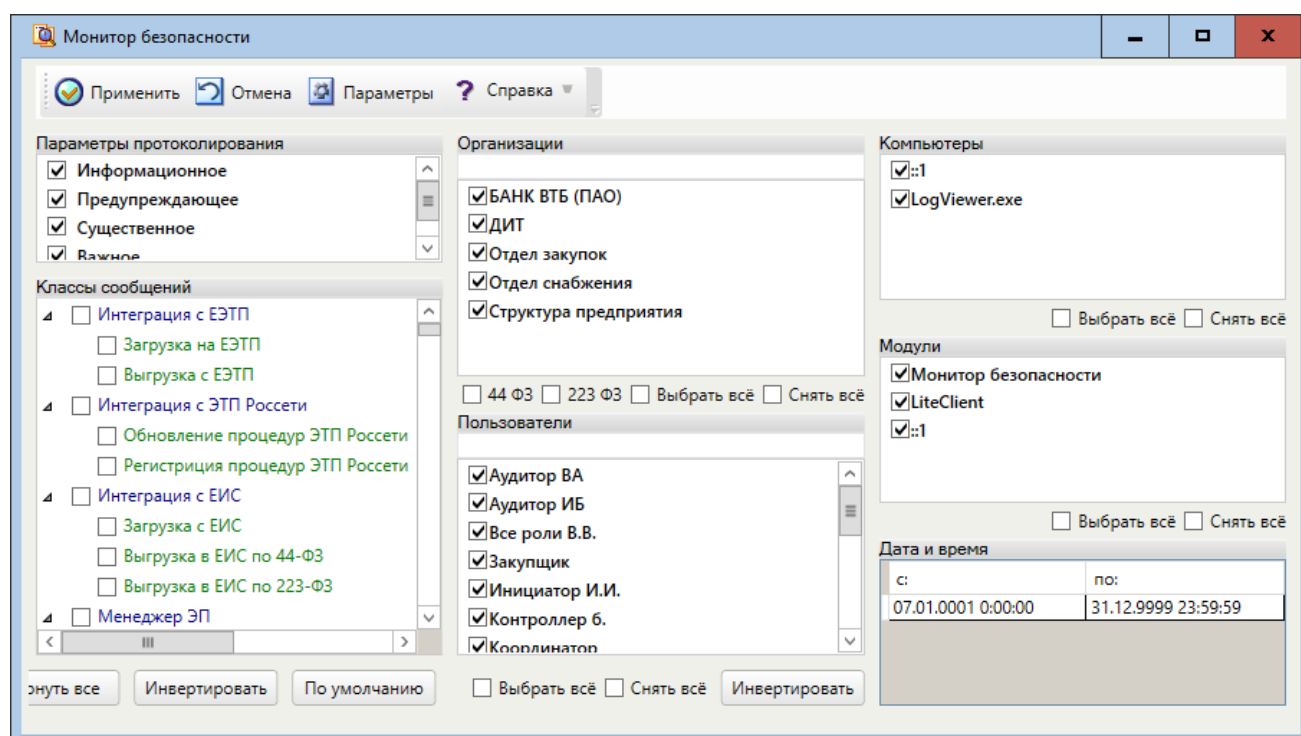


Рисунок 8

Фильтр фактически является составным логическим условием, налагаемым на множество сообщений о событиях.

Над параметрами, отмеченными в рамках одной секции, выполняется логическая операция «дизъюнкция» (логическое «ИЛИ»). Иными словами, будут отобраны сообщения о событиях, удовлетворяющие хотя бы одному из параметров, указанных в данной секции.

Если параметры фильтрации указываются в разных секциях, то над ними выполняется логическая операция «конъюнкция» (логическое «И»). Иными словами, будут отобраны сообщения о событиях, одновременно удовлетворяющие условиям, указанным в данных секциях.

Если в какой-либо секции не отмечено ни одного параметра, это означает, что фильтр по данным параметрам не налагается.

5.3.4.2. Наложение фильтра

На список сообщений накладываются параметры фильтрации, которые указываются в режиме настройки параметров фильтрации списка сообщений. Описание параметров фильтрации и правил наложения фильтра приводятся в п. 5.3.4.1.

Для того чтобы наложить фильтр на список сообщений:

1) в секциях рабочей области (см. рис. 8) укажите параметры фильтрации, установив или сняв соответствующие флажки;

Примечание 2. Для того чтобы в секции **Классы сообщений** в иерархическом списке отображались только элементы первого уровня, нажмите на кнопку **Свернуть все**.

Примечание 3. Для того чтобы в секции **Классы сообщений** установить флажки по умолчанию, нажмите на кнопку **По умолчанию**.

Примечание 4. При установке флажков в секции **Классы сообщений** или **Пользователи** существует возможность инвертировать флажки, т. е. установить в секции те флажки, которые в данный момент сняты, и снять те флажки, которые в данный момент установлены. Для того чтобы инвертировать флажки в секции **Классы сообщений** или **Пользователи**, нажмите на кнопку **Инвертировать**, расположенную ниже соответствующей секции.


2) на панели инструментов нажмите на кнопку Применить . В результате работа с модулем будет продолжена в основном режиме, и в рабочей области отобразятся сообщения, удовлетворяющие заданным параметрам фильтрации.

Таблица 5 — Описание параметров фильтрации


Секция	Параметр (название флажка)	Описание
Параметры протоколирования	Информационное	Протокол события носит информационный характер. Например, поиск документов, просмотр какого-либо маршрута и т. п.
	Предупреждающее	Протокол события носит предупреждающий характер. Например, получение сведений о пользователе и т. п.
	Существенное	Протокол значимого события. Например, изменение настройки доступа к документу и т. п.
	Важное	Протокол важного события. Например, запуск сеанса работы с каким-либо модулем Системы, переназначение контролирующего по маршруту, прерывание маршрута и т. п.

Секция	Параметр (название флажка)	Описание
Классы сообщений	В данной секции отображается иерархический список классов событий, который зависит от конфигурации Системы	Параметры позволяют отбирать сообщения о событиях, относящихся к определенным классам
Пользователи	В данной секции приводится список пользователей, работающих в данный момент с Системой	Параметр позволяет отбирать сообщения о событиях, вызванных действиями определенного пользователя (допускается указывать несколько пользователей)
Компьютеры	В данной секции приводится список системных имен или IP-адресов компьютеров (в случае удаленного доступа), пользователи которых в данный момент работают с Системой	Параметр позволяет отбирать сообщения о событиях по IP-адресу или системному имени компьютера, с которого было выполнено действие (допускается указывать несколько компьютеров)
Модули	Монитор безопасности	Параметр позволяет отбирать сообщения о событиях, являющихся результатом выполнения действий в модуле «Монитор безопасности»
	LiteClient	Параметр позволяет отбирать сообщения о событиях, являющихся результатом выполнения действий в веб-клиенте.
	Администратор	Параметр позволяет отбирать сообщения о событиях, являющихся результатом выполнения действий в модуле «Администратор»
	Менеджер журналов и отчетов	Параметр позволяет отбирать сообщения о событиях, являющихся результатом выполнения действий в модуле «Менеджер журналов и отчетов»
	Дизайнер маршрутов	Параметр позволяет отбирать сообщения о событиях, являющихся результатом выполнения действий в модуле «Дизайнер маршрутов»
	Дизайнер форм	Параметр позволяет отбирать сообщения о событиях, являющихся результатом выполнения действий в модуле «Дизайнер форм»

Секция	Параметр (название флажка)	Описание
Дата и время	с:	Параметры позволяют отбирать сообщения, относящиеся к определенному временному промежутку времени
	по:	


5.3.4.3.Отмена фильтрации

Для того чтобы отменить фильтрацию сообщений:

- 1) на панели инструментов нажмите на кнопку **Фильтр** ;
- 2) в отобразившемся меню выберите пункт **Очистить**. В результате параметры фильтрации будут сняты, и в рабочей области отобразится список сообщений обо всех событиях, произошедших в Системе.

5.4. Управление подключениями пользователей

С помощью модуля «Монитор безопасности» предоставляется возможность просматривать список системных имен пользователей и IP-адресов компьютеров, с которых запущена работа с Системой в данный момент.

Для того чтобы открыть окно со списком пользователей, на панели инструментов нажмите на кнопку **Подключения** . В результате откроется окно **Управление подключениями**, в котором отобразится список системных имен пользователей, подключенных в данный момент к серверу Системы (рис. 9). Помимо системного имени пользователя в списке отображается IP-адрес компьютера, с которого выполнено подключение, а также название модуля, с которым работает этот пользователь.

Кроме того, открыть окно **Управление подключениями** возможно, выполнив двойной щелчок левой кнопкой мыши по строке с сообщением о каком-либо событии.

Окно **Управление подключениями** служит для выполнения следующих операций:

- принудительное отключение пользователя от сервера Системы;
- обновление списка системных имен пользователей, подключенных к серверу;
- просмотр списка сообщений о событиях, вызванных действиями какого-либо из пользователей.

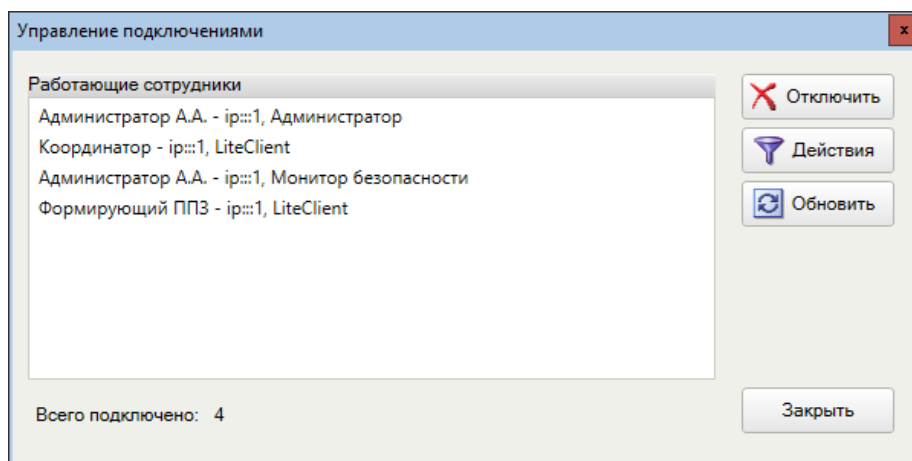





Рисунок 9

Для того чтобы принудительно отключить пользователя от сервера Системы:

- 1) выберите в списке строку с именем пользователя, которого следует отключить от сервера Системы;
- 2) нажмите на кнопку **Отключить** .



Для того чтобы просмотреть список сообщений о событиях, вызванных действиями какого-либо пользователя, который в настоящее время подключен к серверу Системы:

- 1) выберите в списке строку с именем интересующего пользователя;
- 2) нажмите на кнопку **Действия** . В результате в рабочей области отобразятся сообщения о событиях, вызванных действиями выбранного пользователя.

Для того чтобы обновить список системных имен пользователей, подключенных к серверу Системы, в окне **Управление подключениями** нажмите на кнопку **Обновить** .

5.5. Формирование отчета по пользователям


Для того чтобы сформировать отчет по пользователям:

- 1) отключите автоматическое обновление списка (см. п. 5.2.1);
- 2) на панели инструментов нажмите на кнопку **Отчет по пользователям** . В результате откроется окно формирования отчета по пользователям;
- 3) необходимым образом сгруппируйте список пользователей (см. п. 5.3.2);
- 4) для сохранения отчета по пользователям в формате XLSX на панели инструментов нажмите на кнопку **Выгрузить в Excel** .

5) в открывшемся стандартном окне сохранения файла выберите папку файловой системы Microsoft Windows, в которой следует сохранить список сообщений;

6) в соответствующем поле укажите имя файла, в котором следует сохранить список;

7) нажмите на кнопку **Сохранить**. В результате отчет по пользователям будет сохранен в файле формата XLSX.

Для того чтобы вернуться на главное окно модуля на панели инструментов нажмите на кнопку **Вернуться** .

5.6. Сохранение списка сообщений

Существует возможность сохранить список сообщений о событиях, отображающихся на текущий момент в главном окне модуля «Монитор безопасности», в файле одного из форматов: TXT, XLSX, CEF.

Для того чтобы сохранить список сообщений в файл:

1) отключите автоматическое обновление списка (см. п. 5.2);

2) выполните необходимое действие:

- для выгрузки в файл формата TXT на панели инструментов нажмите на кнопку **Сохранить** .

- для выгрузки в файл формата XLSX на панели инструментов нажмите на кнопку **Выгрузить в Excel** .

- для выгрузки в файл формата CEF на панели инструментов нажмите на кнопку **Выгрузить в CEF-файл** .

3) в открывшемся стандартном окне сохранения файла выберите папку файловой системы Microsoft Windows, в которой следует сохранить список сообщений;

4) в соответствующем поле укажите имя файла, в котором следует сохранить список;


5) нажмите на кнопку **Сохранить**. В результате список сообщений будет сохранен в файле выбранного формата.

5.7. Копирование сообщений о событиях

При работе с модулем «Монитор безопасности» предоставляется возможность копировать необходимое сообщение о событии в буфер обмена. Скопированное сообщение затем можно вставить в файл любого внешнего

приложения, поддерживающего работу с буфером обмена (например, используя комбинацию клавиш <Ctrl+V>).


Для того чтобы скопировать одно или несколько сообщений из списка в буфер обмена:

- 1) в рабочей области выберите сообщение;
- 2) на панели инструментов нажмите на кнопку **Копировать** .

5.8. Вывод на печать списка сообщений о событиях

Средствами модуля «Монитор безопасности» предоставляется возможность выводить на печать список сообщений о событиях, отображающихся на текущий момент в главном окне модуля.

Для того чтобы вывести на печать список сообщений, отображающийся в рабочей области:

- 1) на панели инструментов нажмите на кнопку **Печать** . В результате откроется стандартное окно **Печать**;
- 2) настройте параметры печати;
- 3) нажмите на кнопку **Печать**.

6. АВАРИЙНЫЕ СИТУАЦИИ

В таблице 6 приведен перечень аварийных ситуаций с соответствующими им предупреждающими сообщениями и действиями пользователя по разрешению этих ситуаций.

Таблица 6 — Аварийные ситуации и действия пользователя по их разрешению

Текст сообщения	Ситуации, при которых выдается сообщение	Действия пользователя по разрешению ситуации
Ошибка при подключении <код ошибки>	При подключении к серверу произошла ошибка. Если код ошибки 8121, 8122, 8123, 8124, то при подключении к серверу возникли проблемы с вычислительной сетью. Если код ошибки 8125, то в данный момент нет доступа к серверу. Например, администратор Системы может выполнять операции по обслуживанию сервера	Если код ошибки 8121, 8122, 8123, 8124, то проверьте работу вычислительной сети и повторите попытку подключиться к серверу. Если код ошибки 8125, то повторите попытку подключиться через небольшой промежуток времени
Недостаточно прав для запуска модуля «Монитор безопасности»	При запуске сеанса работы с модулем «Монитор безопасности» в окне Подключение к серверу указано системное имя и пароль пользователя, не обладающего правом «администрирование системы»	Обратитесь к администратору Системы с просьбой назначить права
Не удастся произвести отключение	В окне Управление подключениями при отключении пользователя от сервера возникли проблемы с вычислительной сетью	Повторите попытку отключить пользователя от сервера через небольшой промежуток времени