

# Методы и средства обеспечения информационной безопасности в системе 1С: Предприятие 8.1

П.Б.Хорев  
доцент кафедры информационной  
безопасности РГСУ

# Основные методы защиты информационных систем

- Идентификация и аутентификация субъектов.
- Авторизация субъектов.
- Аудит событий, имеющих отношение к безопасности.

# Идентификация и аутентификация пользователей

- Создание и редактирование списка пользователей.
- Выбор способа аутентификации пользователей.

# Способы аутентификации

- Средствами системы 1С:Предприятие (по имени и паролю).
- Средствами ОС Microsoft Windows (по имени и паролю или с помощью смарт-карт).

# Создание учетной записи пользователя

Пользователь ✕

Основные Прочие

Имя: Сидорова

Полное имя: Сидорова Надежда Петровна

---

Аутентификация 1С:Предприятия:

Пароль: xxxxxxxxxxxxxxxx

Подтверждение пароля: xxxxxxxxxxxxxxxx

Показывать в списке выбора

---

Аутентификация Windows:

Пользователь:  ...

OK Отмена Справка

# Повышение достоверности аутентификации средствами 1С: Предприятие

- Установка минимальной длины паролей пользователей.
- Включение проверки сложности паролей.
- Удаление имени пользователя из списка выбора при входе в систему.

# Повышение достоверности аутентификации средствами ОС Windows

- Установка минимальной длины и сложности паролей.
- Ограничение максимального срока действия паролей.
- Включение требования неповторяемости паролей и их минимального срока действия.
- Неотображение последнего имени пользователя, входившего в систему.
- Вход в систему с использованием смарт-карт.

# Объединение аутентификации средствами 1С:Предприятие и средствами Windows

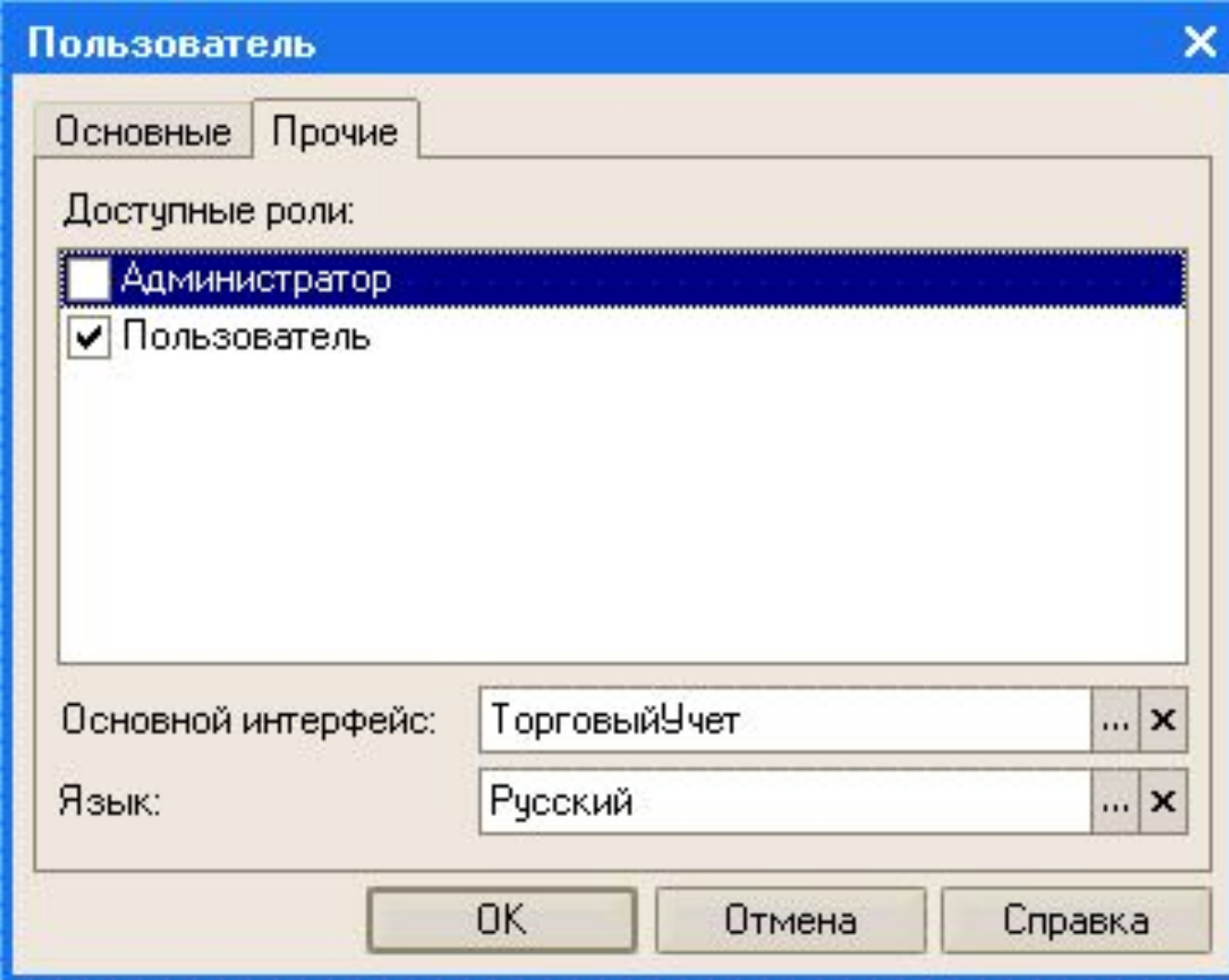
- Наиболее безопасный способ аутентификации пользователей.
- Требуется принудительное отображение диалога аутентификации пользователя средствами 1С:Предприятие (параметр командной строки /WA+).



# Авторизация пользователя в системе 1С:Предприятие

- Назначение роли.
- Назначение интерфейса.

# Назначение пользователю роли и интерфейса



Пользователь

Основные Прочие

Доступные роли:

- Администратор
- Пользователь

Основной интерфейс: ТорговыйУчет ... X

Язык: Русский ... X

OK Отмена Справка

# Создание и назначение роли


- Роли создаются для отдельных должностных обязанностей.
- Каждому пользователю системы может быть назначена одна или несколько ролей.

# Создание и редактирование роли



























- Выбор объекта (объектов) конфигурации.
- Выбор прав доступа, разрешенных для выбранного объекта.
- Учет наследования (иерархии) прав доступа.



# Создание и редактирование роли

- Возможность автоматической установки прав доступа к новым объектам.
- Возможность ограничения доступа к данным на уровне отдельных полей и записей.
- Ограничение доступа к данным может быть определено с помощью конструктора или путем создания и редактирования именованных шаблонов ограничения доступа.




Действия ▾ 

Объекты:

-  Управление Торговлей
-   Общие
-   Константы
-   Справочники
-   Документы
  -   Последовательности
    -  **Авансовый Отчет**
    -  Аккредитив
    -  Внутренний Заказ
    -  Возврат Товаров От Покупателя
    -  Возврат Товаров Поставщику
    -  Доверенность
    -  Заказ Покупателя
    -  Заказ Поставщику
    -  Закрывание Заказов Покупателя
    -  Закрывание Заказов Поставщика
    -  Изменение Лимитов Возврата
    -  Изменение Скидок Компании
    -  Изменение Цен Компании
    -  Инвентаризация Товаров
    -  Инвентаризация Товаров

Права:  

- Чтение
- Добавление
- Изменение
- Удаление
- Проведение
- Отмена проведения
- Просмотр
- Интерактивное добавление
- Редактирование

Ограничения доступа к данным:   

Поля	Ограничение доступа

Описание: Право на чтение  
(Чтение, Read)

Действия

Объекты:

- ВычетНДСПоПриобре
- ВычетНДССАванса
- ГТДИмпорт
- ДенежныйЧек
- Доверенность**
- ЗаказПокупателя
- ЗаказПоставщику
- ЗакрытиеЗаказовПок
- ЗакрытиеЗаказовПос
- ЗакрытиеЗаявокНаРа
- ЗакрытиеПланируемы
- ЗаявкаНаРасходовани
- ИзменениеЛимитовВс
- ИнвентаризацияТовар
- ИнвентаризацияТовар
- ИнкассовоеПоручение
- ИнкассовоеПорччение

Права:

- Чтение
- Добавление**
- Изменение
- Удаление
- Проведение
- Отмена проведения
- Просмотр
- И...

Ограничения доступа к данным:

Поля	Ограничение доступа
<Прочие поля>	Доверенность ИЗ Документ. Доверенность КАК Доверенность ЛЕВОЕ СОЕДИНЕНИЕ РегистрСведений. ГраницыЗапретаИИзмененияДанных КАК ГраницыЗапретаИИзмененияДанных ПО Доверенность. Организация =...

Описание: Право на добавление (Добавление, Insert)

# Конструктор ограничений доступа к данным

Таблицы и поля    Связи    Условия



База данных

- Изменение Скидок Компании
- Изменение Цен Компании**
- Инвентаризация Товаров На Склад
- Инвентаризация Товаров Отданные
- Комплектация Номенклатуры
- Контакт
- Корректировка Долга
- Корректировка Заказа Покупателя

Таблицы

- Изменение Цен Компании**
- Контакт

Запрос

< Назад

Далее >

OK

Отмена

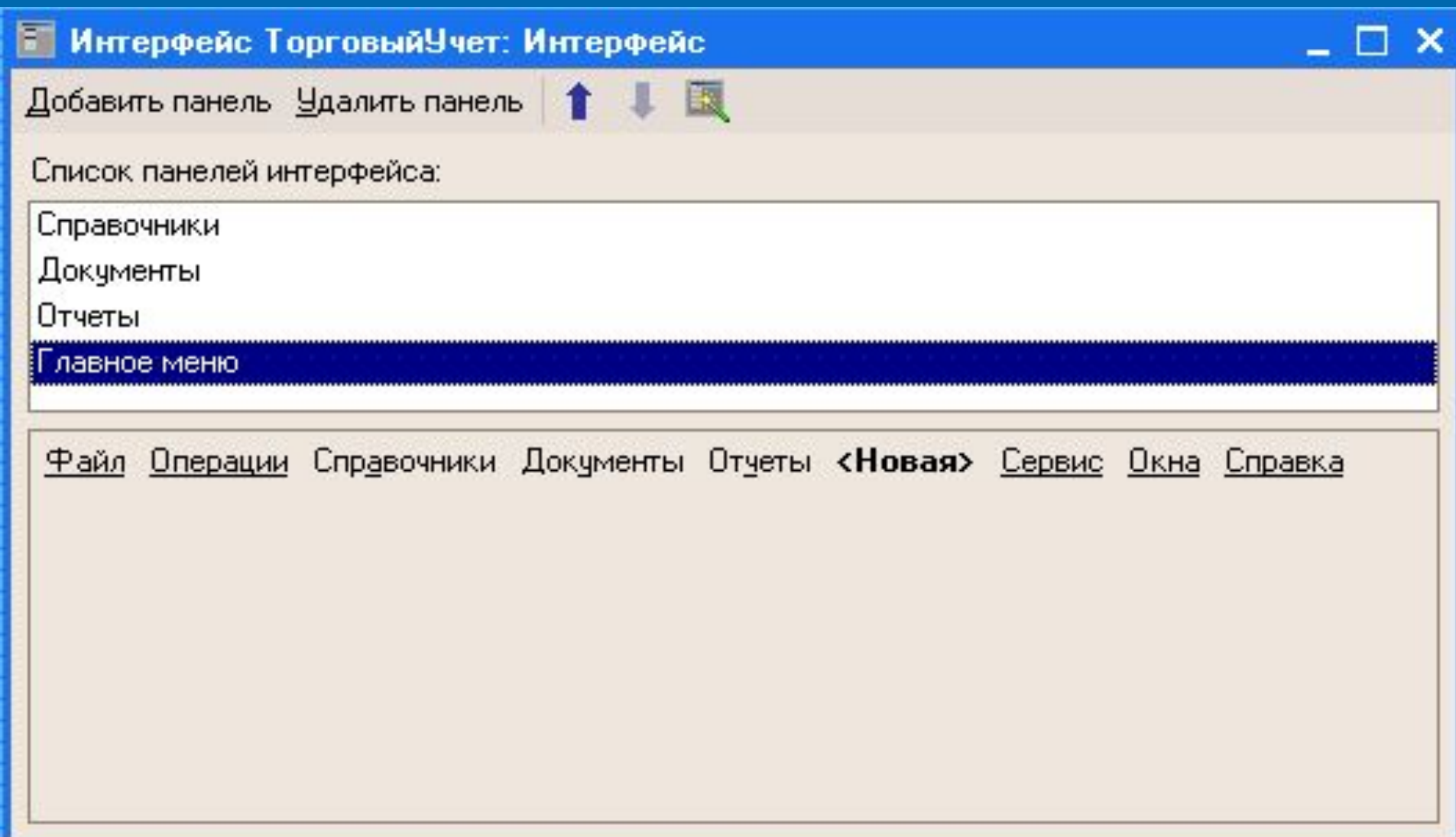
Справка



# Механизм интерфейсов

- Создание наборов команд главного меню и элементов панели инструментов, доступных для пользователя.
- Возможность дополнительного ограничения полномочий конкретного пользователя.

# Создание пользовательского интерфейса



# Интерфейс ТорговыйУчет: Интерфейс

Добавить панель   Удалить панель   ↑   ↓   [иконка]

Список панелей интерфейса:

- Справочники
- Документы
- Отчеты**
- Главное меню



### Свойства: Панель

↑   ×

A ↓   Z ↓   [иконка]   ×   ✓

Заголовок	Отчеты
Показывать	<input checked="" type="checkbox"/>
Расположение	Сверху ▼
С новой строки	<input type="checkbox"/>
Тип	Панель инструментов ▼

# Обновление конфигурации базы данных

- Необходимо после создания ролей и интерфейсов, чтобы новым пользователям информационной системы могли быть назначены созданные роли и интерфейсы.

# Настройка журнала регистрации системы 1С:Предприятие

- Определение событий, которые должны регистрироваться в журнале.
- Выбор периода времени, по истечении которого журнал регистрации будет сохраняться в новом файле.
- Возможность сокращения записей журнала до истечения указанного периода путем их удаления и, при необходимости, сохранения в файле.

# Настройка журнала регистрации системы 1С:Предприятие

- Возможность сохранения разделения журнала по периодам и его объединения с ранее сохраненным журналом.
- Возможность автоматического обновления после заданного интервала времени при просмотре журнала регистрации.

# Настройка журнала регистрации

**Настройка журнала регистрации** [X]

Регистрировать в журнале события

- Не регистрировать
- Регистрировать ошибки
- Регистрировать ошибки, предупреждения
- Регистрировать ошибки, предупреждения, информацию
- Регистрировать ошибки, предупреждения, информацию, примечания

OK  
Отмена  
Справка  
Сократить

**Сократить журнал регистрации** [X]

Текущий диапазон событий: 11.03.2004 - 01.09.2004

Удалить события до:  [календарь]

Сохранение

Записать удаляемые события в файл:

[...]

OK  
Отмена  
Справка

# Информация о событии в журнале регистрации

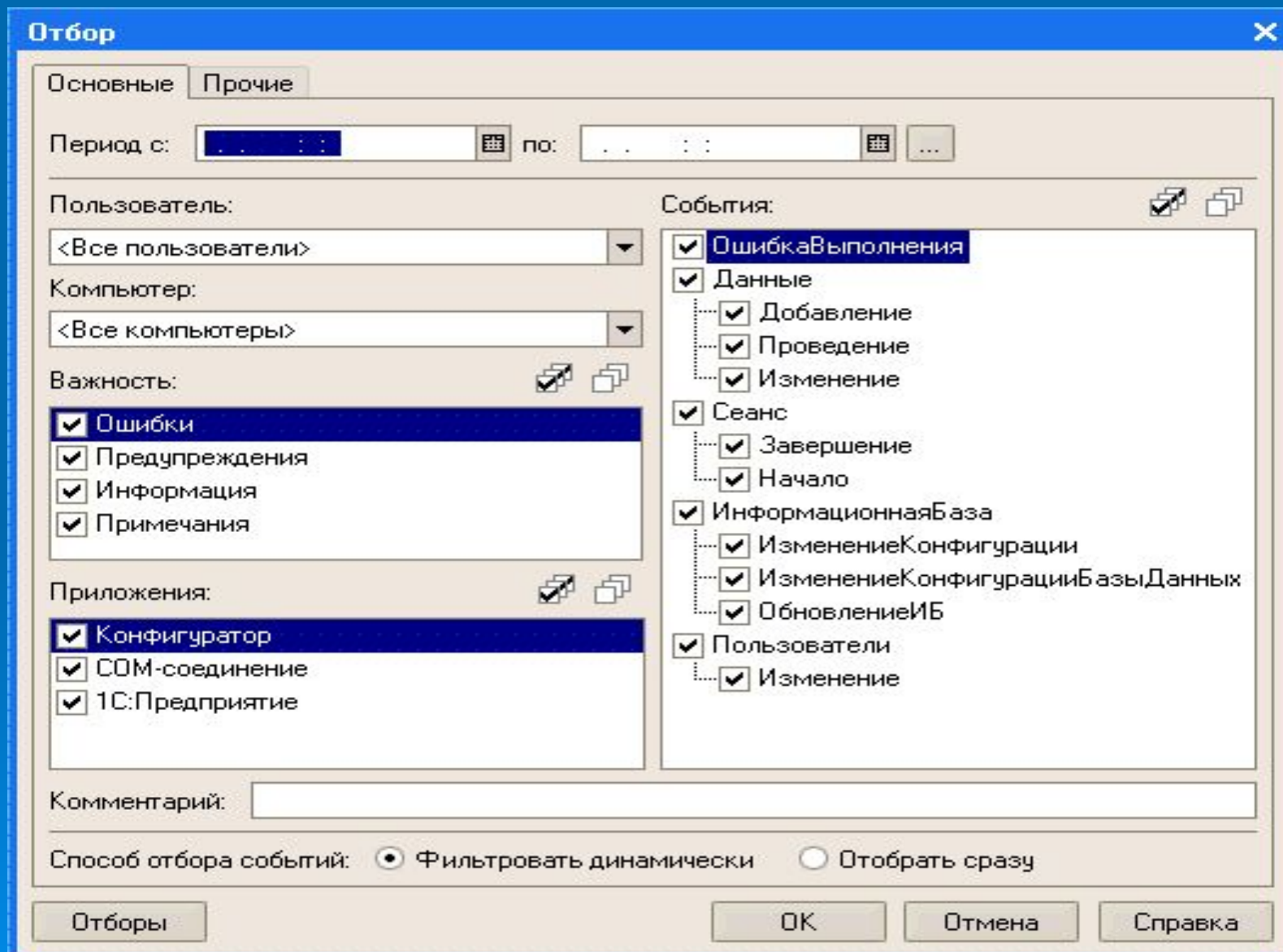
- Уровень события (ошибка, предупреждение, информация, примечание).
- Дата и время события.
- Имя и представление приложения, вызвавшего событие.
- Имя и представление события.
- Глобальный идентификатор и имя пользователя.
- Данные события и др.



Действия ▾         

	Дата, время	Пользователь	Событие	Метаданные
		Приложение	Комментарий	Данные
				Представление данных
<b>i</b>	27.04.2004 11:23:36	Иванов 1С:Предприятие	Данные.Проведение	Документ РеализацияТоваров  Реализация товаров ТК000028 от 16.06.2003 12:00:00
<b>i</b>	27.04.2004 11:23:37	Иванов 1С:Предприятие	Данные.Изменение	Регистр накопления ПартииТоваровКомпании
<b>i</b>	27.04.2004 11:23:37	Иванов 1С:Предприятие	Данные.Изменение	Регистр накопления ПартииТоваровКомпании
<b>i</b>	27.04.2004 11:23:37	Иванов 1С:Предприятие	Данные.Изменение	Регистр накопления ПродажиКомпании
<b>i</b>	27.04.2004 11:23:37	Иванов 1С:Предприятие	Данные.Изменение	Регистр накопления ПартииТоваровКомпании
<b>i</b>	27.04.2004 11:23:37	Иванов 1С:Предприятие	Данные.Изменение	Регистр накопления ПродажиКомпании
<b>i</b>	27.04.2004 11:23:37	Иванов 1С:Предприятие	Данные.Изменение	Документ ПроведениеПоПартиям  Проведение по партиям 00014 от 30.06.2003 16:33:53
<b>i</b>	27.04.2004 11:23:37	Иванов 1С:Предприятие	Данные.Проведение	Документ ПроведениеПоПартиям  Проведение по партиям 00014 от 30.06.2003 16:33:53
<b>i</b>	27.04.2004 11:23:47	Иванов 1С:Предприятие	Сеанс.Завершение	
<b>i</b>	27.04.2004 19:56:25	Иванов Конфигуратор	Сеанс.Завершение	

# Отбор записей в журнале регистрации



# Сохранение журнала регистрации

- В формате 1С:Предприятие (\*.elf).
- В формате XML.

# Выводы

- В системе 1С:Предприятие 8.1 реализованы все необходимые методы обеспечения безопасности информационных систем.
- В механизме парольной аутентификации предусмотрены возможности ее усиления и объединения с механизмом аутентификации пользователей ОС Windows.
- При авторизации пользователей используется гибкий и мощный механизм ролевого разграничения доступа к объектам информационной системы.

# Выводы

- Для дополнительного разграничения прав пользователей в системе может применяться механизм интерфейсов.
- Средства ведения, настройки, просмотра и сохранения журнала регистрации событий позволяют вести регулярный аудит безопасности системы.

# Замечания

- В эксплуатационной документации отсутствуют сведения об алгоритме хеширования паролей, что не позволяет точно оценить сложность их подбора.
- При назначении роли (ролей) пользователям целесообразно ввести средства ограничений на совмещение разных ролей одним пользователем и количество пользователей, которым может быть одновременно назначена некоторая роль.

# Замечания

- В эксплуатационной документации отсутствуют сведения о защите журнала регистрации событий от его удаления или подмены с целью скрывания совершенных несанкционированных действий. Неясно также, фиксируется ли в журнале событие, связанное с сокращением (удалением) записей в журнале до истечения заданного периода.