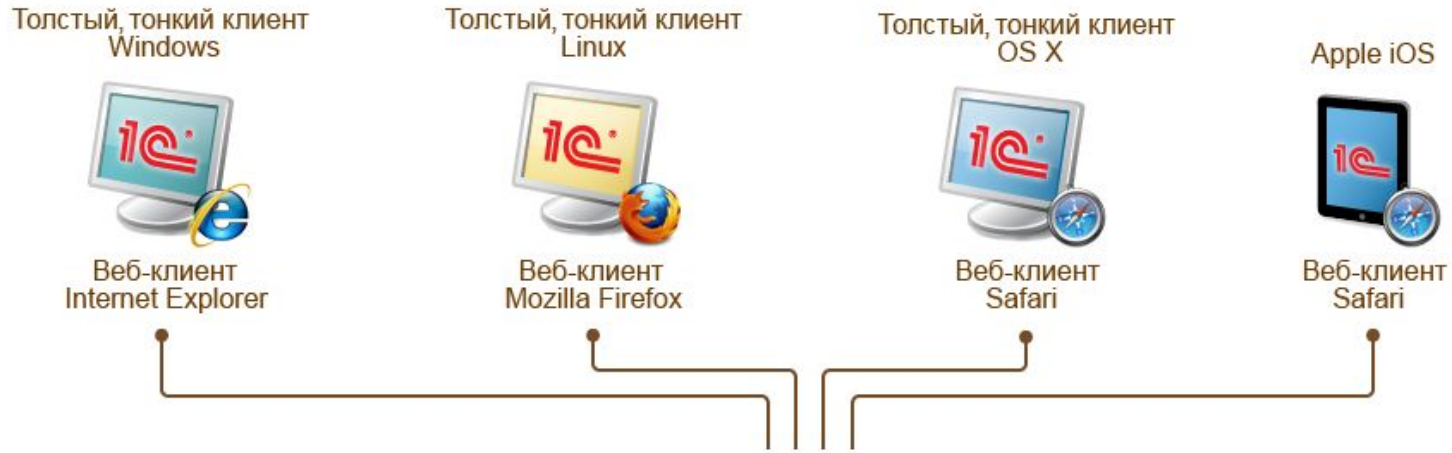
Архитектура 1С

1. Многоплатформенность

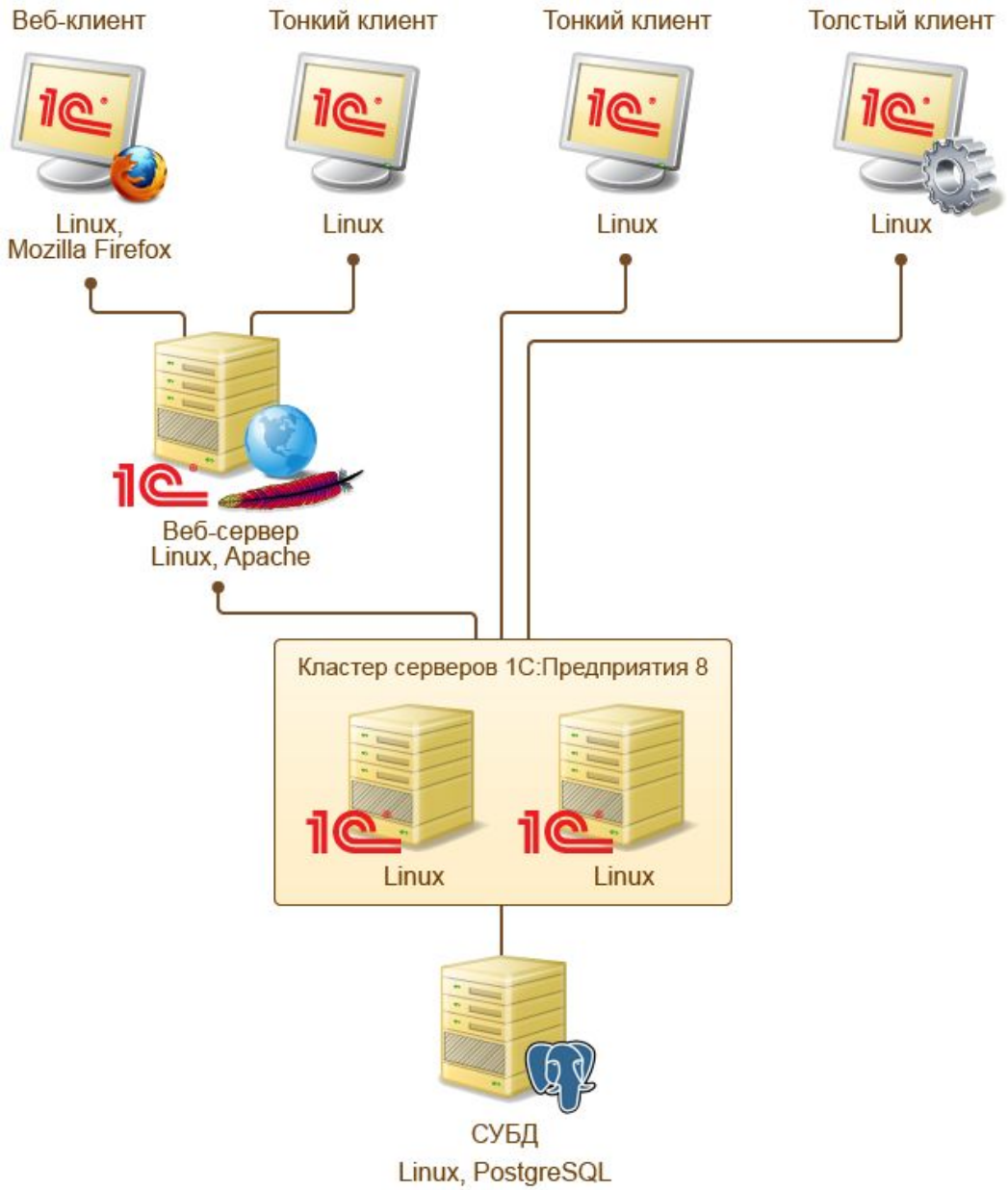
Многоплатформенность - это способность системы работать под управлением различных операционных систем. Основные компоненты системы могут работать как под управлением операционной системы Windows, так и под управлением операционной системы Linux. Кроме этого клиентская часть 1С:Предприятия может быть запущена и на компьютерах с операционными системами OS X и Apple iOS.

2. Клиентские приложения на различных платформах

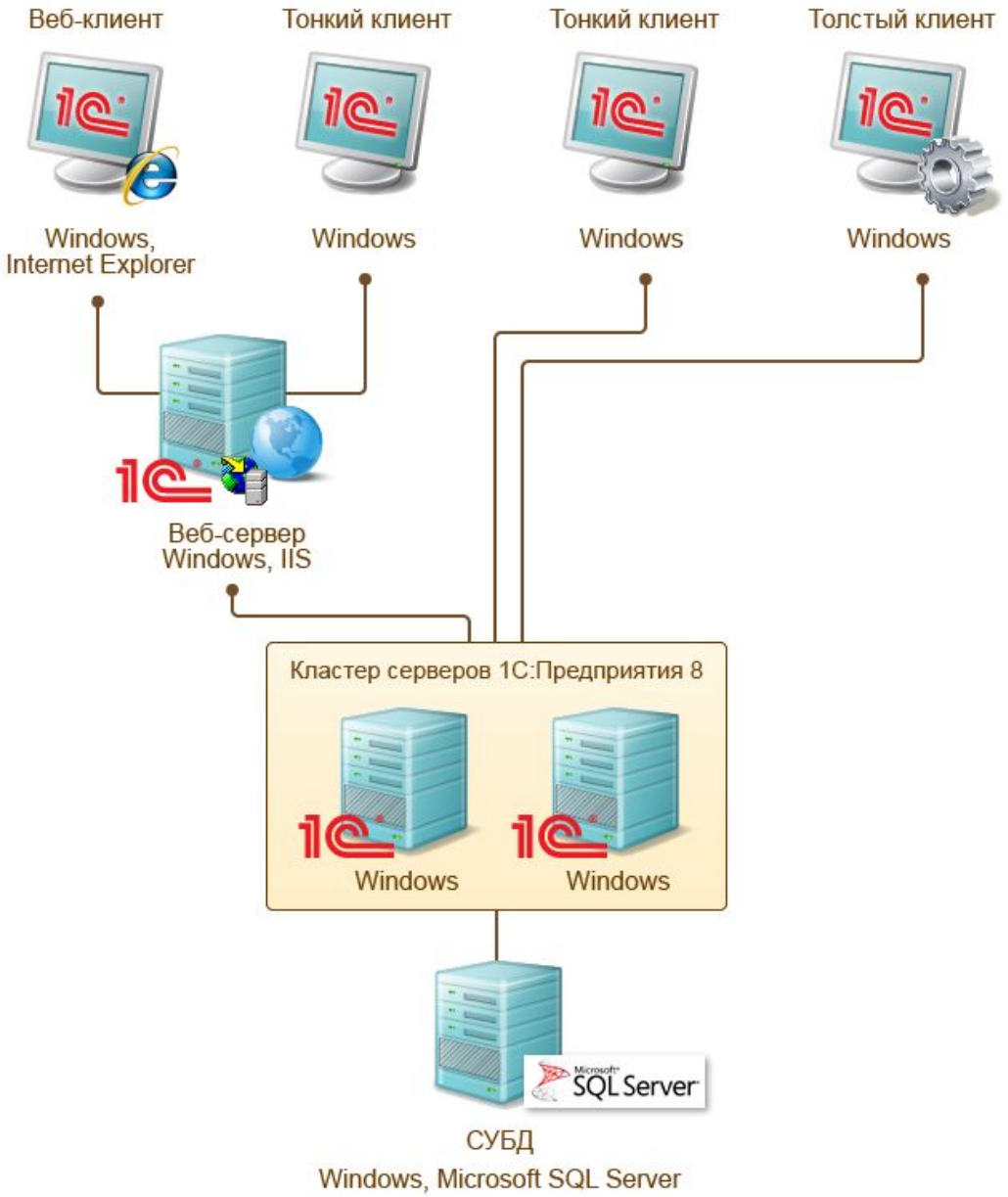
Пользователи различных устройств на разных операционных системах могут работать с информационными базами 1С: Предприятия с помощью любого из клиентских приложений. Толстый и тонкий клиенты реализованы для Windows, Linux и OS X. А веб-клиент исполняется в среде интернет-браузера и адаптирован для работы с популярными браузерами.



3. Многоплатформенность системы. Linux.



3. Многоплатфор-менность системы. Windows.



4. Многоплатформенность кластера.

Компьютеры, входящие в состав кластера, могут работать под управлением операционных систем Windows или Linux. Допускается включение в состав одного кластера рабочих серверов, функционирующих под разными операционными системами.

4. Многоплатформенность кластера.

Кластер серверов 1С:Предприятия 8 - основной компонент платформы, обеспечивающий взаимодействие между пользователями и системой управления базами данных в клиент-серверном варианте работы. Наличие кластера позволяет обеспечить бесперебойную, отказоустойчивую, конкурентную работу большого количества пользователей с крупными информационными базами.

Кластер серверов 1С:Предприятия 8 является логическим понятием и представляет собой совокупность рабочих процессов, обслуживающих один и тот же набор информационных баз.

5. Клиентское приложение

Клиентское приложение - это программа, работающая на компьютере пользователя и обеспечивающая интерактивное взаимодействие системы 1С:Предприятие 8 с пользователем, в отличие от других компонент системы (программ и рабочих процессов), предназначенных исключительно для программного взаимодействия с другими частями системы или с другими программными объектами.

В системе 1С:Предприятие 8 существует 4 клиентских приложения:

- Толстый клиент,
- Тонкий клиент,
- Веб-клиент,
- Конфигуратор.

5. Возможности клиентских приложений

	Толстый клиент	Тонкий клиент	Веб-клиент	Конфигуратор
Разработка прикладных решений	Нет	Нет	Нет	Да
Работа в локальной сети	Да	Да	Да	Да
Работа через интернет	Нет	Да	Да	Нет
Необходимость предварительной установки	Да, большой дистрибутив	Да, маленький дистрибутив	Нет	Да, большой дистрибутив

Толстый клиент

Толстый клиент позволяет реализовывать полные возможности 1С:Предприятия 8 в плане исполнения прикладного кода. Однако он не поддерживает работу с информационными базами через интернет, требует предварительной установки на компьютер пользователя и имеет довольно внушительный объем дистрибутива.

Тонкий клиент

Тонкий клиент может работать с информационными базами через интернет. Он также требует предварительной установки на компьютер пользователя, но имеет значительно меньший размер дистрибутива, чем толстый клиент

Веб-клиент

Веб-клиент не требует какой-либо предварительной установки на компьютер. В отличие от толстого и тонкого клиентов, он исполняется не в среде операционной системы компьютера, а в среде интернет-браузера (Internet Explorer, Mozilla Firefox, Google Chrome или Safari). Поэтому пользователю достаточно всего лишь запустить свой браузер, ввести адрес веб-сервера, на котором опубликована информационная база – и веб-клиент «сам приедет» к нему на компьютер и начнет исполняться.

Конфигуратор

Конфигуратор позволяет выполнять разработку и администрирование информационных баз.

6. Толстый клиент

Толстый клиент - это одно из клиентских приложений системы 1С: Предприятие 8. В операционной системе Windows исполняемый файл этого приложения - 1cv8.exe. В операционной системе Linux - 1cv8.

«Толстым» клиент называется потому, что может исполнять практически всю функциональность, предоставляемую встроенным языком, в том числе умеет работать с прикладными типами данных, такими как **СправочникОбъект.<имя>**, **ДокументОбъект.<имя>** и т.д.

Но, по этой же причине, он требует значительного количества аппаратных ресурсов на компьютере пользователя и может «общаться» с базой данных или с кластером серверов 1С: Предприятия 8 только посредством файлового доступа или по

6. Толстый клиент

Клиент-серверный вариант

Если система 1С:Предприятие 8 работает в клиент-серверном варианте, то толстый клиент подключается к кластеру серверов 1С:Предприятия 8. А кластер взаимодействует с одной из систем управления базами данных. Подключение выполняется по протоколу TCP/IP по локальной сети. Это наиболее распространенный сценарий работы. Менее распространенным, но возможным, является вариант, когда толстый клиент работает на том же компьютере, на котором находится кластер. Такой вариант может использоваться при разработке, в тестовых целях или для выполнения каких-то административных действий.

6. Толстый клиент

Клиент-серверный вариант работы предназначен для использования в рабочих группах или в масштабе предприятия. Он реализован на основе трехуровневой архитектуры «клиент-сервер».

6. Толстый клиент

Файловый вариант работы

Если система 1С:Предприятие работает в файловом варианте, то толстый клиент взаимодействует непосредственно с файловой базой данных. В этом варианте работы толстому клиенту требуется непосредственный файловый доступ к базе данных, например, через общий сетевой ресурс. При этом возможен и такой вариант, когда толстый клиент работает на том же компьютере, на котором находится файловая база данных. Толстый клиент самостоятельно реализует всю функциональность файловой СУБД.

6. Толстый клиент

Работа в обычном режиме

Толстый клиент поддерживает работу приложения в обычном режиме. Поэтому толстого клиента можно использовать для работы с прикладными решениями, созданными в старых версиях платформы, - 8.0 и 8.1, - которые не использовали управляемый интерфейс и управляемые формы.

7.Тонкий клиент

Тонкий клиент - это одно из клиентских приложений системы 1С: Предприятие 8. В операционной системе Windows исполняемый файл этого приложения - 1cv8c.exe. В операционной системе Linux - 1cv8c.

«Тонким» клиент называется потому, что умеет исполнять ограниченный набор функциональности встроенного языка. В частности на тонком клиенте недоступны все прикладные типы данных. Вместо этого тонкий клиент оперирует ограниченным набором типов встроенного языка, предназначенным лишь для отображения и изменения данных в памяти. Вся работа с базой данных, объектными данными, исполнение запросов – выполняется на стороне сервера. Тонкий клиент только получает готовые данные, подготовленные для отображения.

7.Тонкий клиент

Подключение через Интернет

Тонкий клиент позволяет работать с интерфейсом 1С: Предприятия через Интернет. Для этого используется веб-сервер, настроенный для работы с 1С:Предприятием 8.

Тонкий клиент взаимодействует с веб-сервером по протоколу HTTP или HTTPS. Веб-сервер, в свою очередь, взаимодействует с 1С:Предприятием 8 в файловом или клиент-серверном варианте работы.

7.Тонкий клиент

В качестве веб-сервера используется Apache или IIS.

7.Тонкий клиент

Клиент-серверный вариант работы

В клиент-серверном варианте работы тонкий клиент взаимодействует с кластером серверов напрямую, по протоколу TCP/IP.

7.Тонкий клиент

Файловый вариант работы

Если система 1С:Предприятие работает в файловом варианте, то тонкий клиент взаимодействует непосредственно с файловой базой данных. В этом варианте работы толстому клиенту требуется непосредственный файловый доступ к базе данных, например, через общий сетевой ресурс.

При работе тонкого клиента в файловом варианте работы на компьютере, где запущен сам тонкий клиент, организуется специализированная среда. В рамках этой специализированной среды выполняются:

- загрузка необходимых для работы системы серверных компонентов,

- загрузка прикладной конфигурации,

- другие действия, необходимые для организации нормальной работы системы с информационной базой.

7.Тонкий клиент

С точки зрения тонкого клиента, данная среда выступает в роли сервера. С точки зрения операционной системы, данная специализированная среда не выделена в отдельный процесс и выполняется в рамках процесса тонкого клиента.

8. Веб-клиент

Веб-клиент - это одно из клиентских приложений системы 1С: Предприятие 8. В отличие от "привычных" клиентских приложений (толстого клиента и тонкого клиента), его не нужно предварительно устанавливать на компьютер пользователя. У веб-клиента нет исполняемого файла. Веб-клиента вы не найдете ни в меню, ни среди исполняемых файлов. Потому он и веб-клиент, что ему для начала работы не нужно иметь никаких файлов на компьютере пользователя.

Веб-клиент, в отличие от толстого и тонкого клиентов, исполняется не в среде операционной системы компьютера, а в среде интернет-браузера (Windows Internet Explorer, Mozilla Firefox, Google Chrome или Safari). Поэтому любому пользователю достаточно всего лишь запустить свой браузер, ввести адрес веб-сервера, на котором опубликована информационная база, – и веб-клиент сам "приедет" к нему на компьютер и начнет исполняться.

8. Веб-клиент

Веб-клиент использует технологии DHTML и HTTPRequest. При работе веб-клиента клиентские модули, разработанные в конфигурации, компилируются автоматически из встроенного языка 1С:Предприятия 8 и непосредственно исполняются на стороне веб-клиента.

Таким образом, независимо от клиентского приложения (толстый, тонкий, веб-клиент), вся разработка прикладного решения ведется полностью в конфигураторе 1С: Предприятия, серверный и клиентский код пишется на встроенном языке 1С:Предприятия.

8. Работа Интернет-браузере без установки системы на компьютер пользователя

Для работы в режиме веб-клиента требуется веб-сервер, настроенный на работу с 1С:Предприятием 8. Браузер клиента взаимодействует с веб-сервером по протоколу HTTP или HTTPS. Веб-сервер, в свою очередь, взаимодействует с 1С: Предприятием 8 в файловом или клиент-серверном варианте работы.

8. Веб-клиент

В качестве веб-сервера используется Apache или IIS.

9. Сервер баз данных

- В качестве сервера баз данных могут использоваться:
- Microsoft SQL Server,
- PostgreSQL,
- IBM DB2,
- Oracle Database.

9. Сервер баз данных

Администрирование кластера серверов

В поставку платформы входит набор различных инструментов, позволяющих администратору управлять составом кластера, информационными базами и подключением пользователей.

9. Сервер баз данных

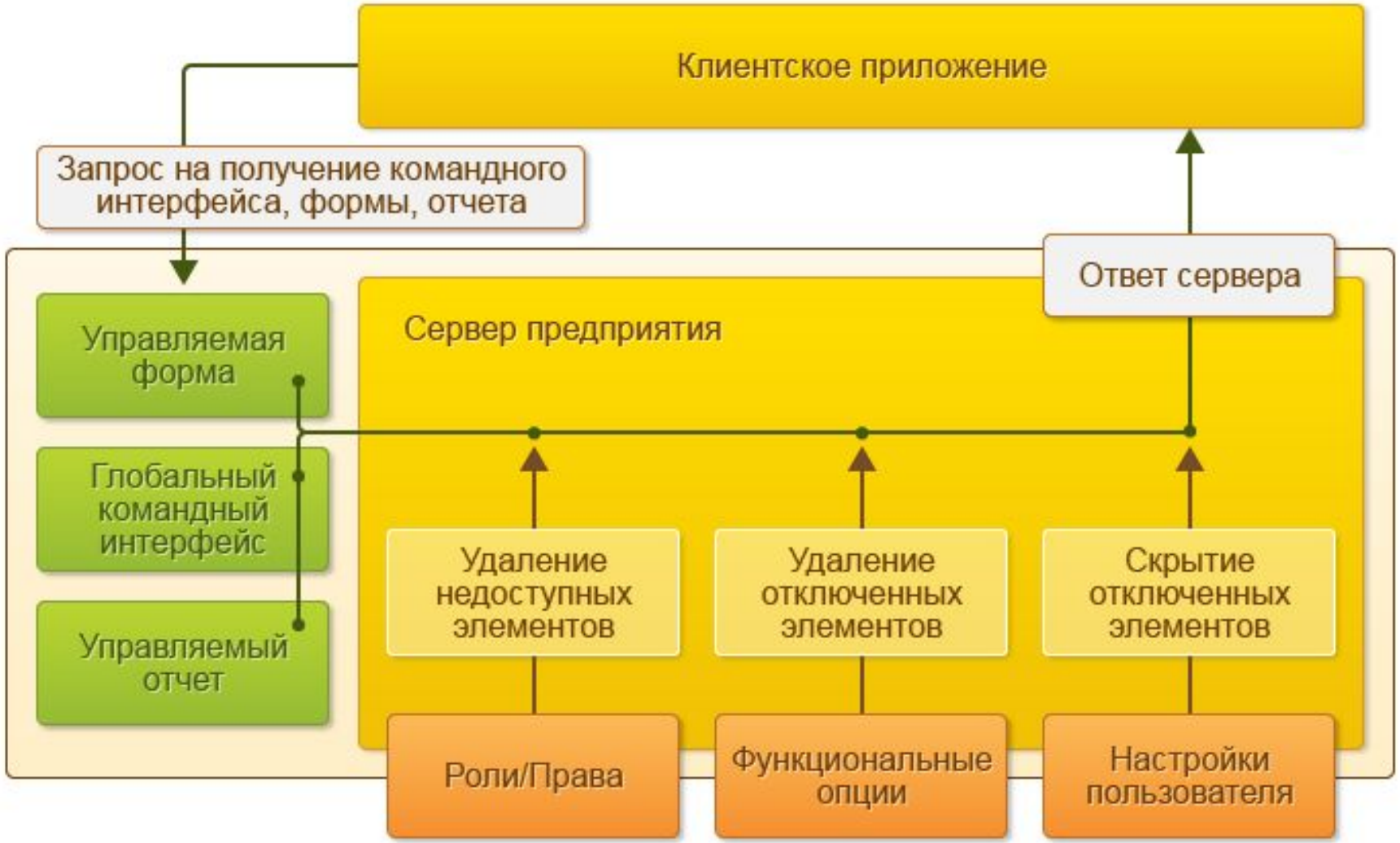
Выполнение основной функциональности на сервере

Вся работа с прикладными объектами, чтение и запись базы данных выполняется только на сервере. Функциональность форм и командного интерфейса также реализована на сервере.

На сервере выполняется подготовка данных форм, расположение элементов, запись данных форм после изменения. На клиенте отображается уже подготовленная на сервере форма, выполняется ввод данных и вызовы сервера для записи введенных данных и других необходимых действий.

Аналогично командный интерфейс формируется на сервере и отображается на клиенте. Также и отчеты формируются полностью на сервере и отображаются на клиенте.

9. Сервер баз данных



9. Сервер баз данных

На сервере выполняются:

- Запросы к базе данных,
- Запись данных,
- Проведение документов,
- Различные расчеты,
- Выполнение обработок,
- Формирование отчетов,
- Подготовка форм к отображению.

9. Сервер баз данных

На клиенте выполняется:

- Получение и открытие форм,
- Отображение форм,
- «Общение» с пользователем (предупреждения, вопросы…),
- Небольшие расчеты в формах, требующие быстрой реакции (например, умножение цены на количество),
- Работа с локальными файлами,
- Работа с торговым оборудованием.

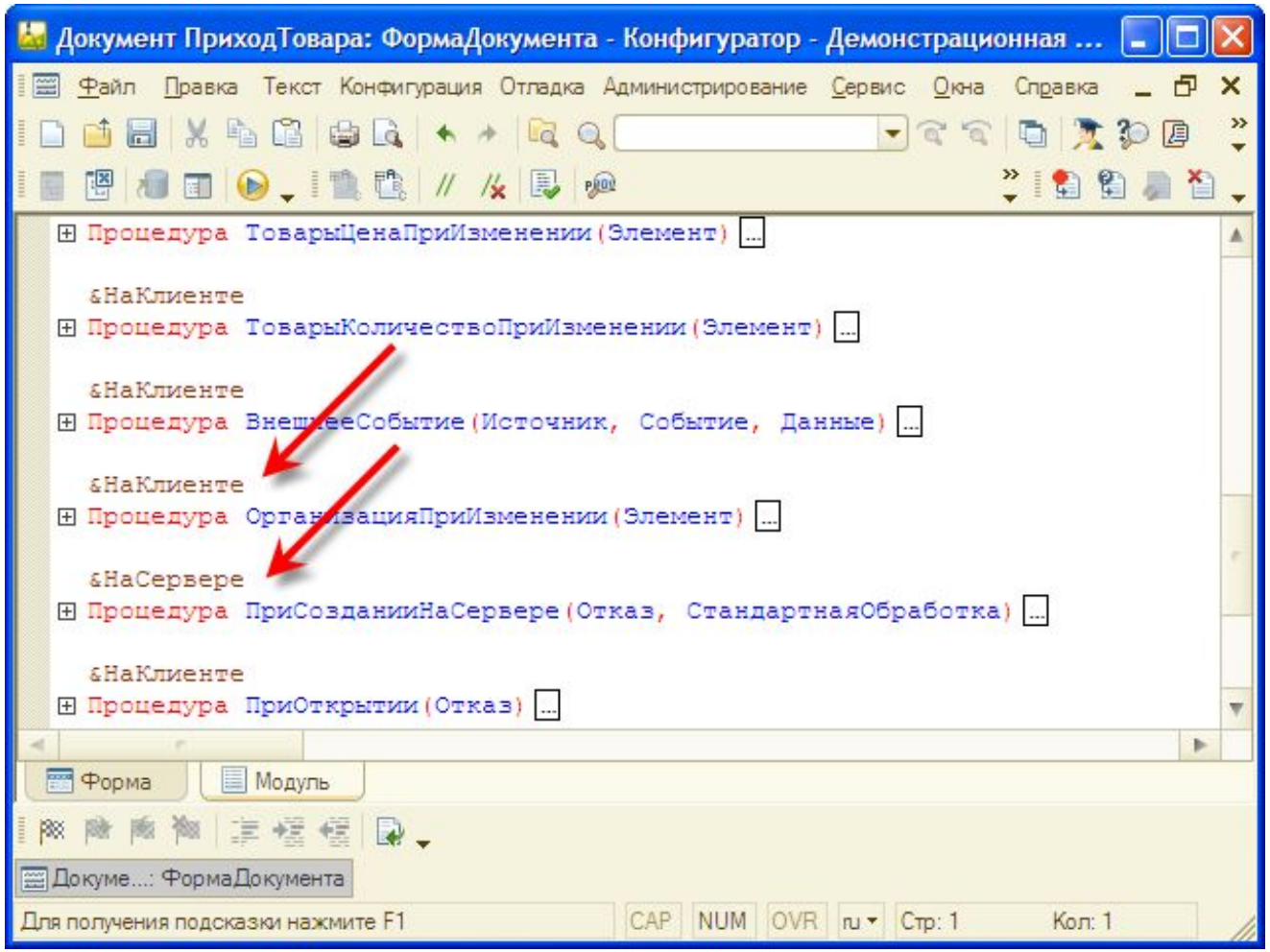
9. Сервер баз данных

Использование встроенного языка на клиенте

Управлять функциональностью форм можно не только на сервере, но и на клиенте. На клиенте поддерживается работа встроенного языка. Он используется в тех случаях, когда необходимо провести расчеты, связанные с отображенной на экране формой, например, быстро (без обращения к серверу) подсчитать сумму строки документа на основе цены и количества; задать пользователю вопрос и обработать ответ; прочитать файл из файловой системы компьютера и отправить его на сервер.

9. Сервер баз данных

Однако работа встроенного языка на клиенте поддерживается в строго ограниченном объеме. Клиентские процедуры в модулях в явном виде отделяются от серверных, и в них используется ограниченный состав объектной модели встроенного языка.



10. Отказоустойчивость

Отказоустойчивость системы обеспечивается при работе в клиент-серверном варианте с использованием кластера серверов. Система обеспечивает бесперебойную работу пользователей при программных и аппаратных сбоях в кластере серверов.

Такие события, как выход из строя рабочего сервера (в том числе и центрального сервера), аварийное (или плановое) завершение рабочего процесса или менеджера кластера не влияют на работу пользователей. Пользователи продолжают работать так, как будто ничего не произошло.

В случае физического разрыва соединения пользователя с кластером и последующего его восстановления пользователь может продолжить работу без повторного соединения с информационной базой и без потери своих текущих данных.

10. Отказоустойчивость

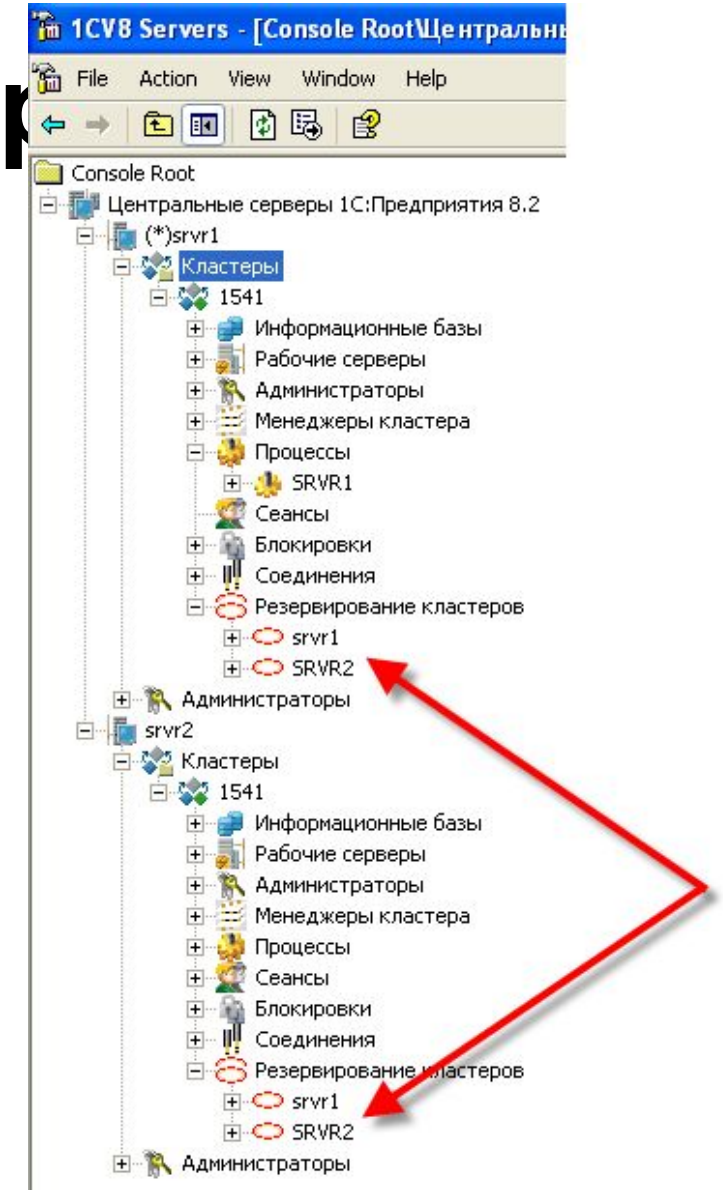
Отказоустойчивость кластера обеспечивается в трех направлениях:

- резервированием самого кластера,
- резервированием рабочих серверов,
- резервированием рабочих процессов,
- устойчивостью к обрыву канала связи.

10. Резервирование кластер

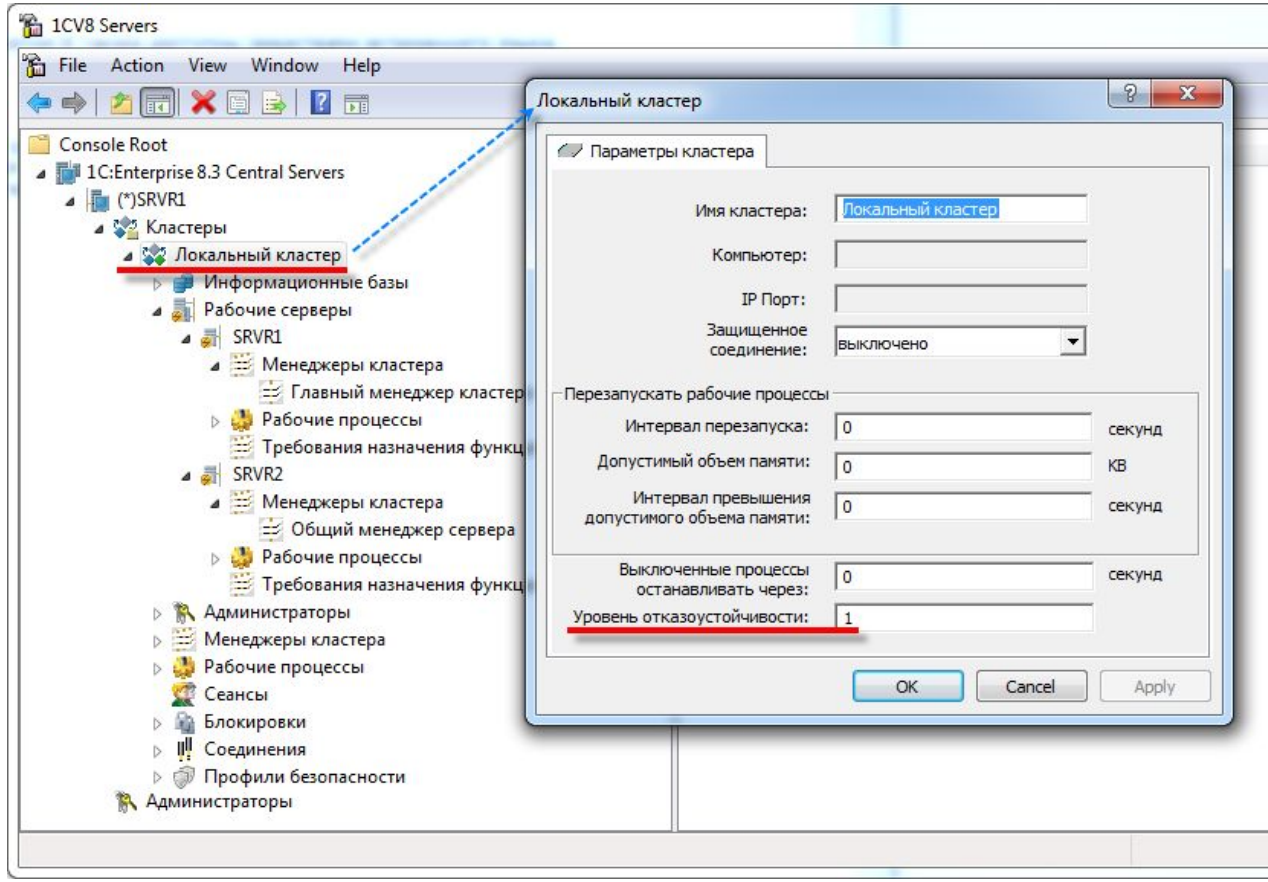
Несколько кластеров могут быть объединены в группу резервирования. Кластеры, находящиеся в одной группе резервирования синхронизируются автоматически.

При выходе из строя активного кластера активным становится следующий работоспособный кластер группы. При восстановлении работоспособности кластера, который находится в группе раньше активного, активность передается ему после автоматической синхронизации данных.



10. Резервирование рабочих серверов

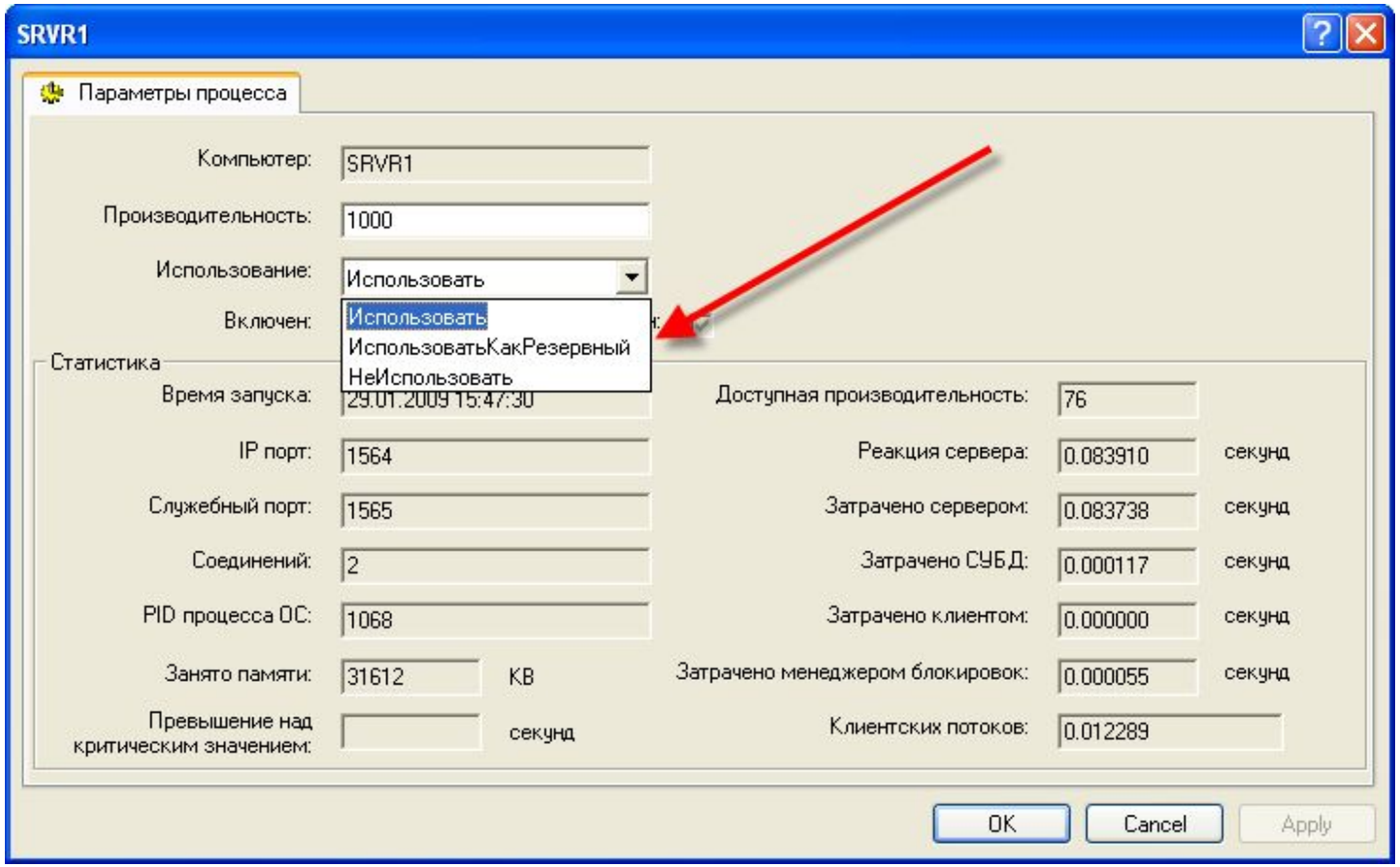
Можно задавать уровень отказоустойчивости кластера как количество рабочих серверов, которые могут одновременно выйти из строя, и это не приведет к аварийному завершению работы пользователей. Резервные сервисы запускаются автоматически в количестве, необходимом для обеспечения заданной отказоустойчивости; в реальном режиме времени выполняется репликация активного сервиса на резервные.



10. Резервирование рабочих серверов

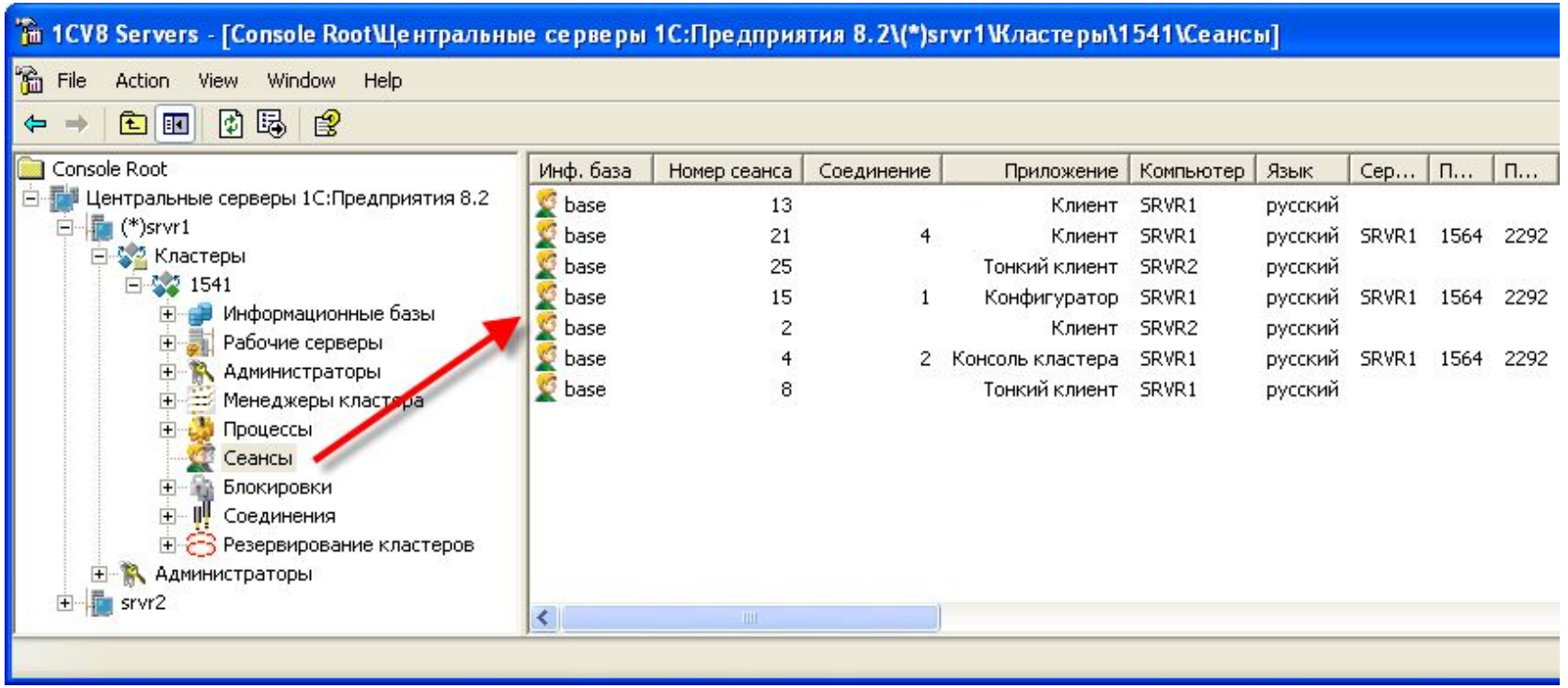
Резервирование рабочих процессов

Каждому рабочему процессу можно указать вариант его использования: Использовать, Использовать как резервный, Не использовать.



10. Устойчивость к обрыву канала связи

Кластер «запоминает» подключившихся пользователей и состояние выполняемых ими действий благодаря тому, что для каждого пользователя создается собственный сеанс.



10. Устойчивость к обрыву канала связи

В случае потери физического соединения кластер будет ожидать восстановления соединения с этим пользователем. В подавляющем большинстве случаев после восстановления соединения пользователь сможет продолжить работу с того «места», на котором она была прекращена. При этом не потребуется повторное подключение к информационной базе.

Система прав доступа 1С

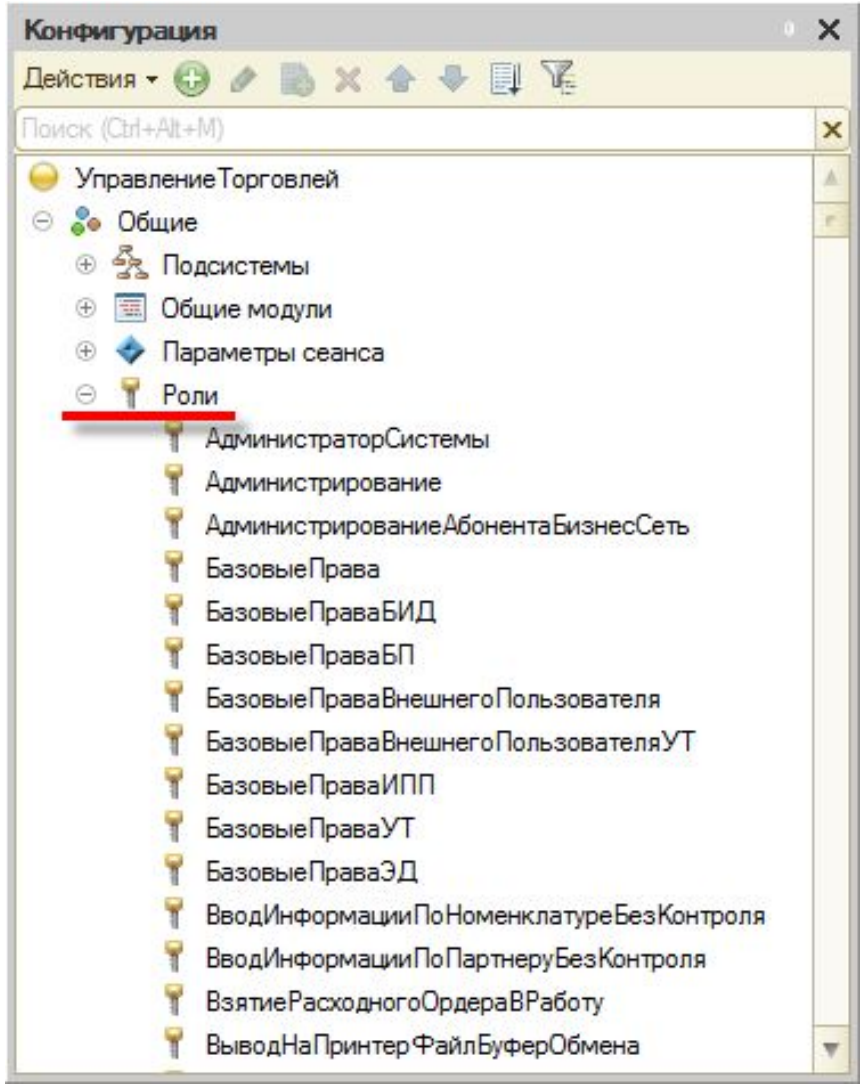
1. Общие сведения

Система прав доступа позволяет описывать наборы прав, соответствующие должностям пользователей или виду деятельности. Структура прав определяется конкретным прикладным решением.

Кроме этого, для объектов, хранящихся в базе данных (справочники, документы, регистры и т.д.) могут быть определены права доступа к отдельным полям и записям. Например, пользователь может оперировать документами (накладными, счетами и т.д.) определенных контрагентов и не иметь доступа к аналогичным документам других контрагентов.

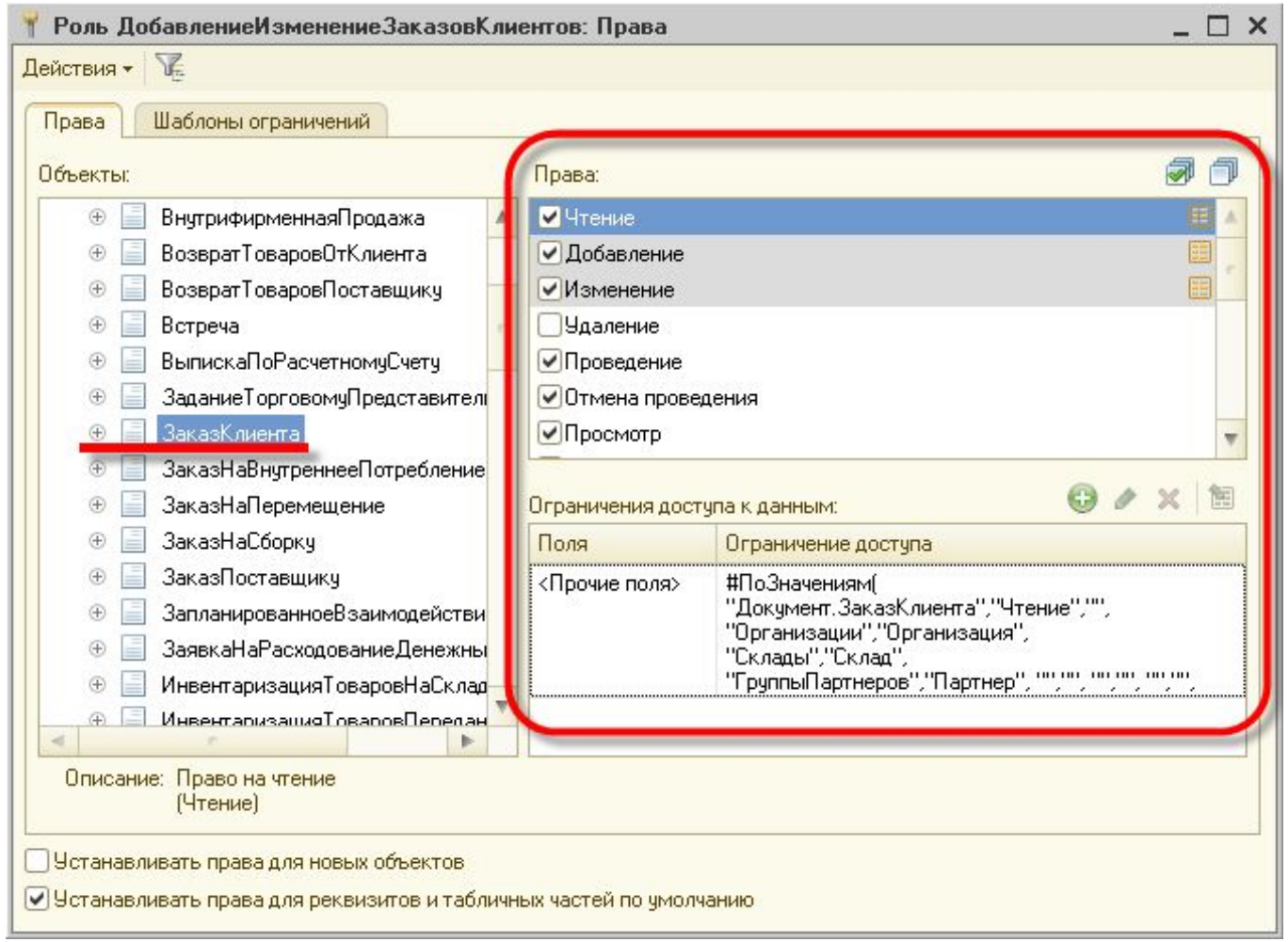
2. Роли

Роли - это общие объекты конфигурации. Они предназначены для реализации ограничения прав доступа в прикладных решениях. Роль в конфигурации может соответствовать должностям или видам деятельности различных групп пользователей, для работы которых предназначена данная конфигурация:



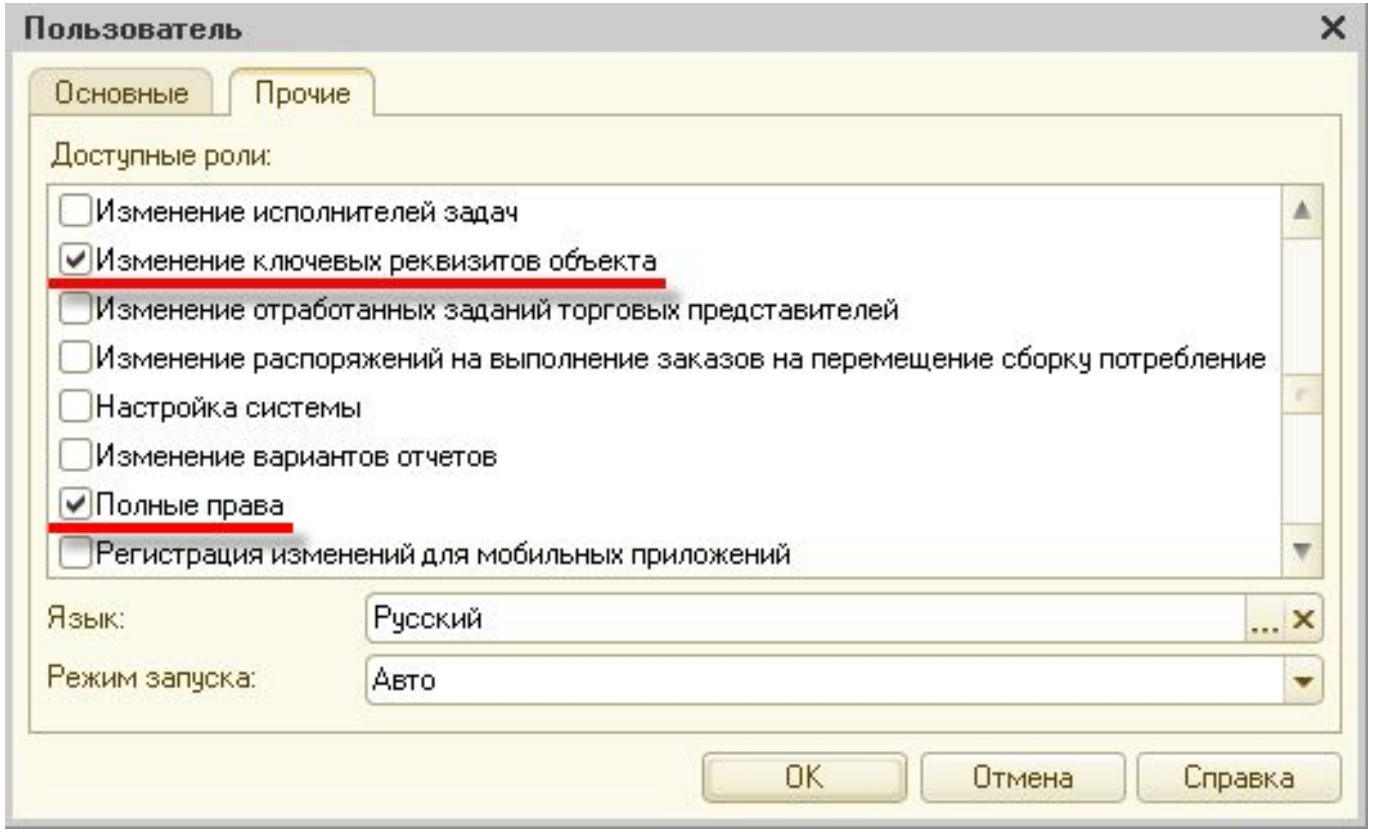
2. Роли

Роль определяет, какие действия, над какими объектами метаданных может выполнять пользователь, выступающий в этой роли:



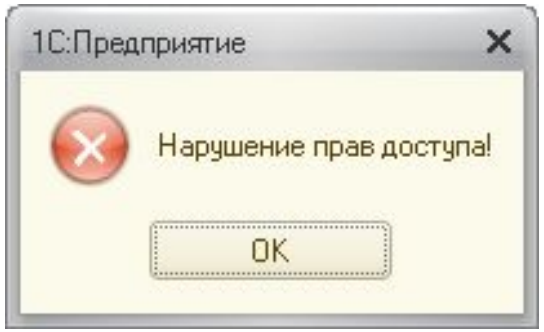
2. Роли

В процессе ведения списка пользователей прикладного решения каждому пользователю ставится в соответствие одна или несколько ролей.



2. Роли

При попытке пользователя выполнить действие, на которое у него нет разрешения, действие выполнено не будет, а система выдаст окно предупреждения:



3. Редакторы ролей

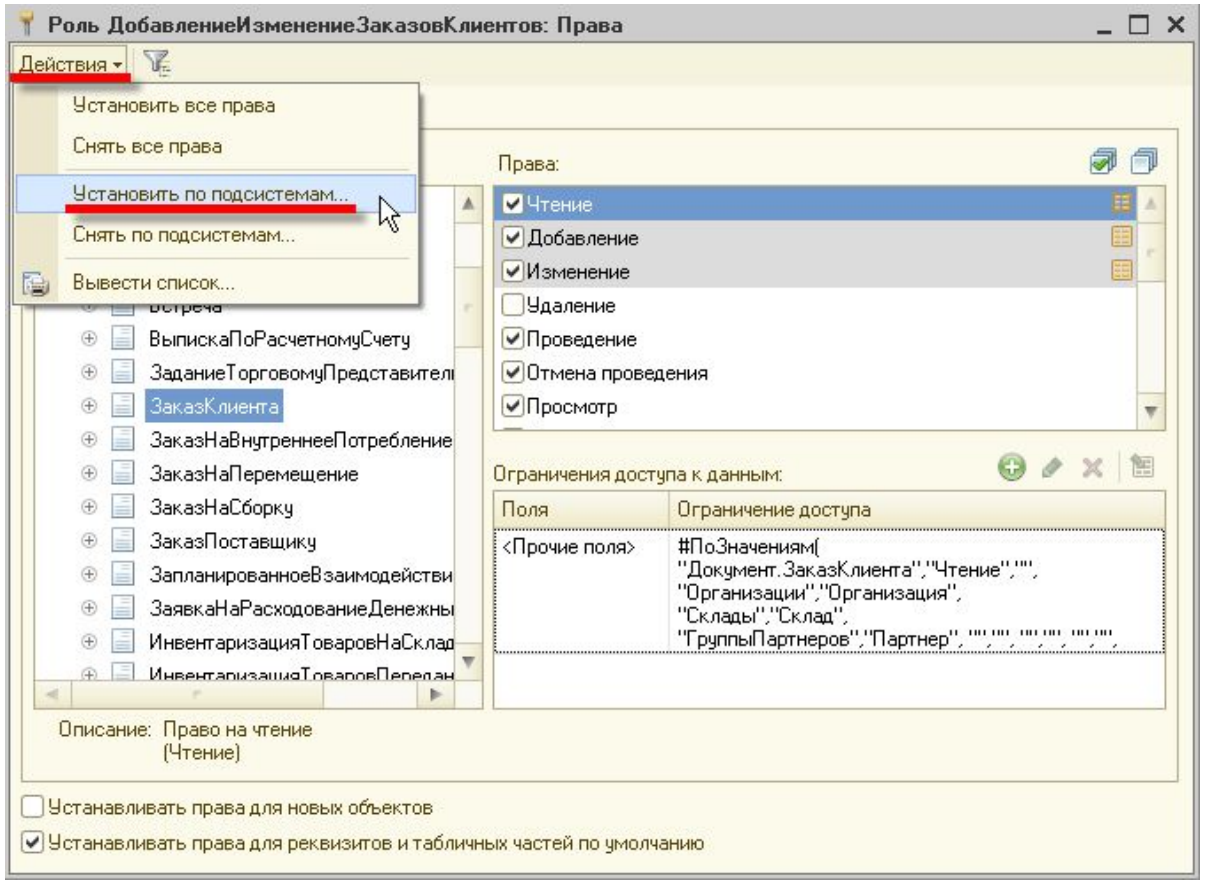
Для редактирования состава ролей платформа содержит два редактора:

1. **Редактор роли**
2. **Редактор "Все роли"**

3.1. Редактор роли

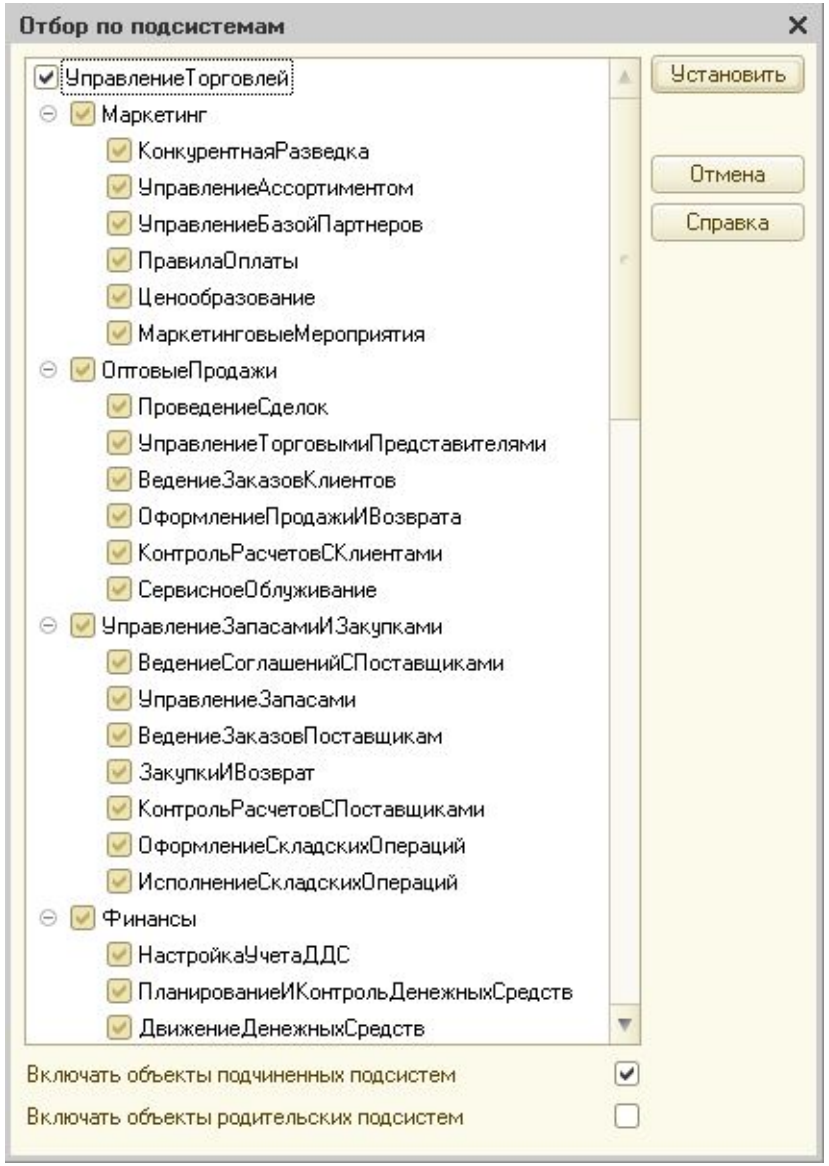
Редактор роли - это один из инструментов разработки. Он позволяет изменять состав прав для одной выбранной роли прикладного решения.

Разработчик имеет возможность устанавливать разрешения как вручную, так и используя механизм подсистем:



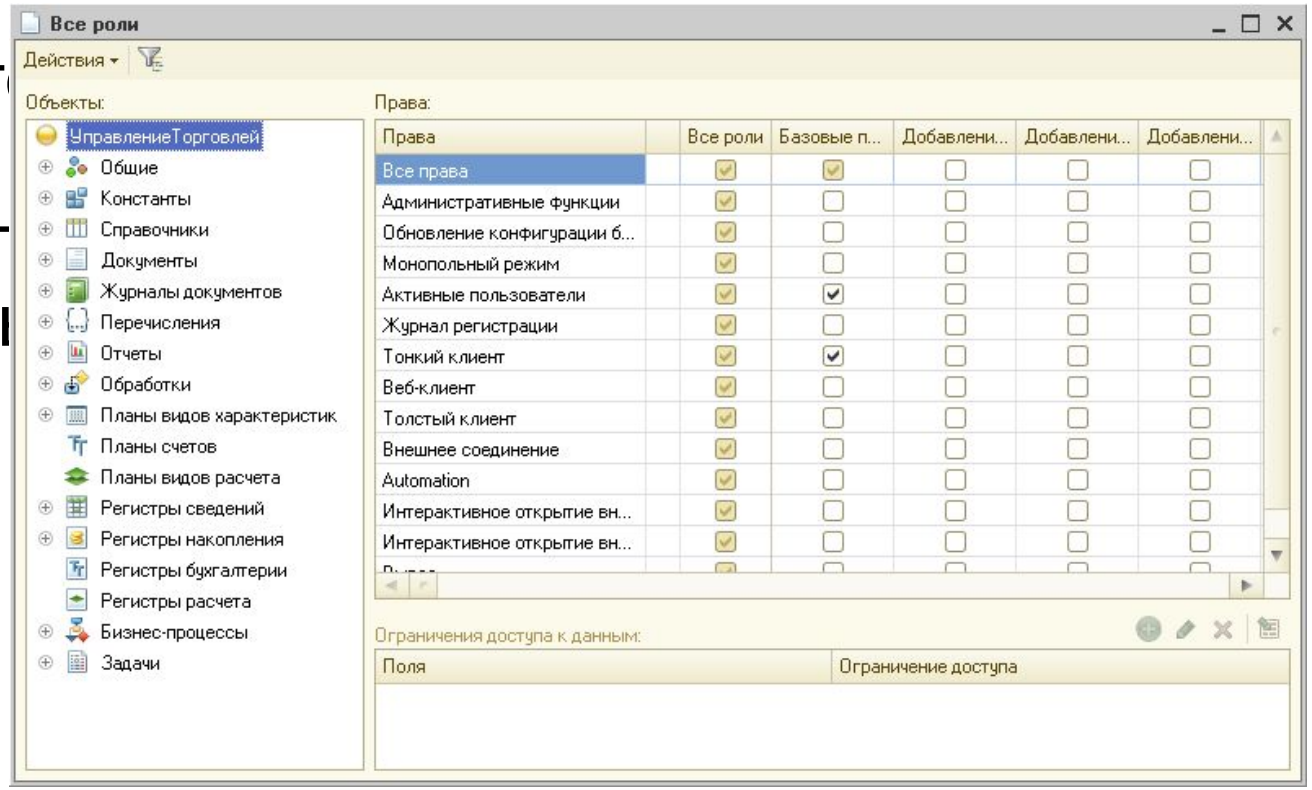
3.1. Редактор роли

Выбрав некоторый набор подсистем, он может установить или снять все права для всех объектов, принадлежащих указанным подсистемам:



3.2. Редактор "Все роли"

Редактор "Все роли" - эт
один из инструментов
разработки. Он позволяет
изменять и анализироват
состав прав сразу для
нескольких или для всех
ролей, существующих в
прикладном решении.



3.2. Редактор "Все роли"

Этим редактором удобно пользоваться в тех случаях, когда нужно одновременно установить или снять одно право для всех ролей. Или когда нужно визуально сравнить и изменить сразу несколько ролей.

Если для какого-нибудь права требуется установить или снять его разрешение во всех ролях, то достаточно в первой колонке установить или снять флажок разрешения.

4. Интерактивные и основные права

Все права, поддерживаемые системой 1С:Предприятие, можно разделить на две большие группы: основные и интерактивные. Основные права описывают действия, выполняемые над элементами данных системы или над всей системой в целом, и проверяются всегда, независимо от способа обращения к данным. Интерактивные права описывают действия, которые могут быть выполнены пользователем интерактивно. Соответственно проверяются они только при выполнении интерактивных операций стандартными способами, причем в клиент-серверном варианте все проверки прав (кроме интерактивных) выполняются на сервере.

4. Интерактивные и основные права

Основные и интерактивные права взаимосвязаны. Например, существует основное право Удаление, которому соответствуют два интерактивных права: Интерактивное удаление и Интерактивное удаление помеченных. Если пользователю запрещено Удаление, то и все интерактивные "удаления" также будут запрещены для него. В то же время, если пользователю разрешено Интерактивное удаление помеченных, это значит, что Удаление ему также разрешается.

Кроме того, основные права могут зависеть друг от друга. В результате образуются довольно сложные цепочки взаимосвязей, которые отслеживаются системой автоматически: как только разработчик снимает разрешение на какое-либо право, система сама снимает разрешения на все права, которые зависят от этого права. И наоборот, при установке какого-либо права разработчиком, система сама устанавливает все права, от которых это право зависит.

4. Интерактивные и основные права

Например, для того, чтобы пользователь имел право **Итерактивное удаление помеченных**, ему необходимо обладать интерактивными правом **Редактирование**. Это право, в свою очередь, требует наличия интерактивного права **Просмотр**:

4. Интерактивные и основные права

Право **Интерактивное удаление помеченных** требует наличия основного права **Удаление**. Интерактивное право **Редактирование** требует наличия основного права **Изменение**. Интерактивное право **Просмотр** требует наличия основного права **Чтение**.

Кроме этого основные права **Изменение** и **Удаление** требуют наличия основного права **Чтение.**

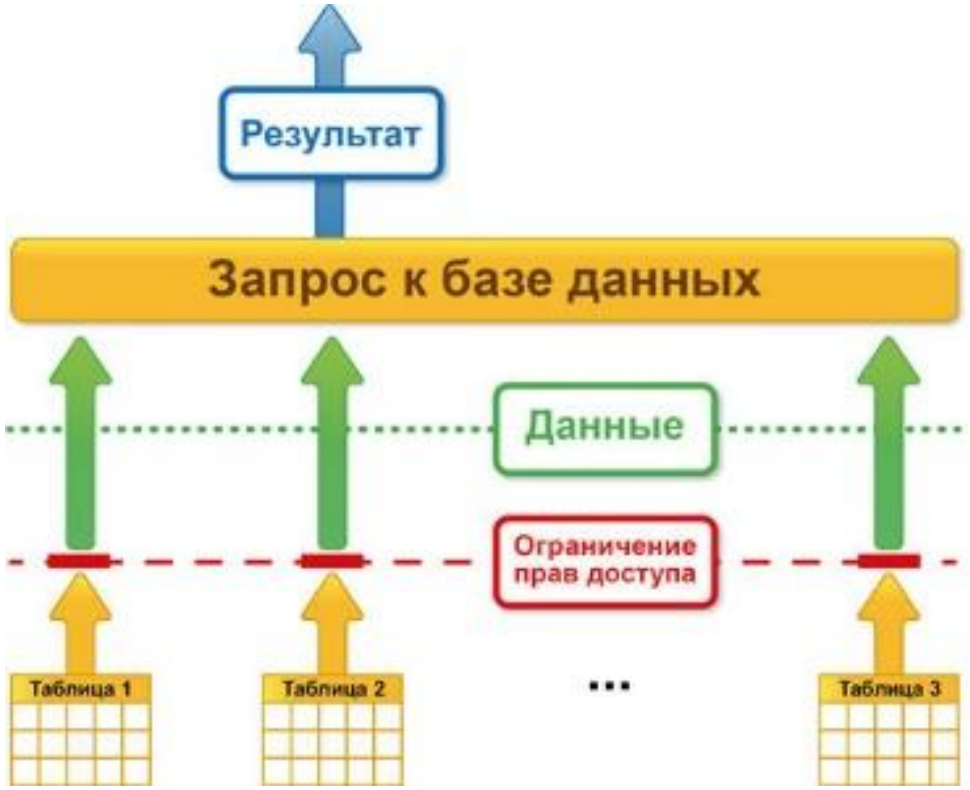
5. Ограничение доступа к данным на уровне записей и полей

Среди действий над объектами, хранящимися в базе данных (справочниками, документами и т.д.), есть действия, отвечающие за чтение или изменение информации, хранящейся в базе данных. К таким действиям относятся:

- чтение - получение записей или их фрагментов из таблицы базы данных;
- добавление - добавление новых записей без изменения существующих;
- изменение - изменение существующих записей;
- удаление - удаление некоторых записей без внесения изменений в оставшиеся.

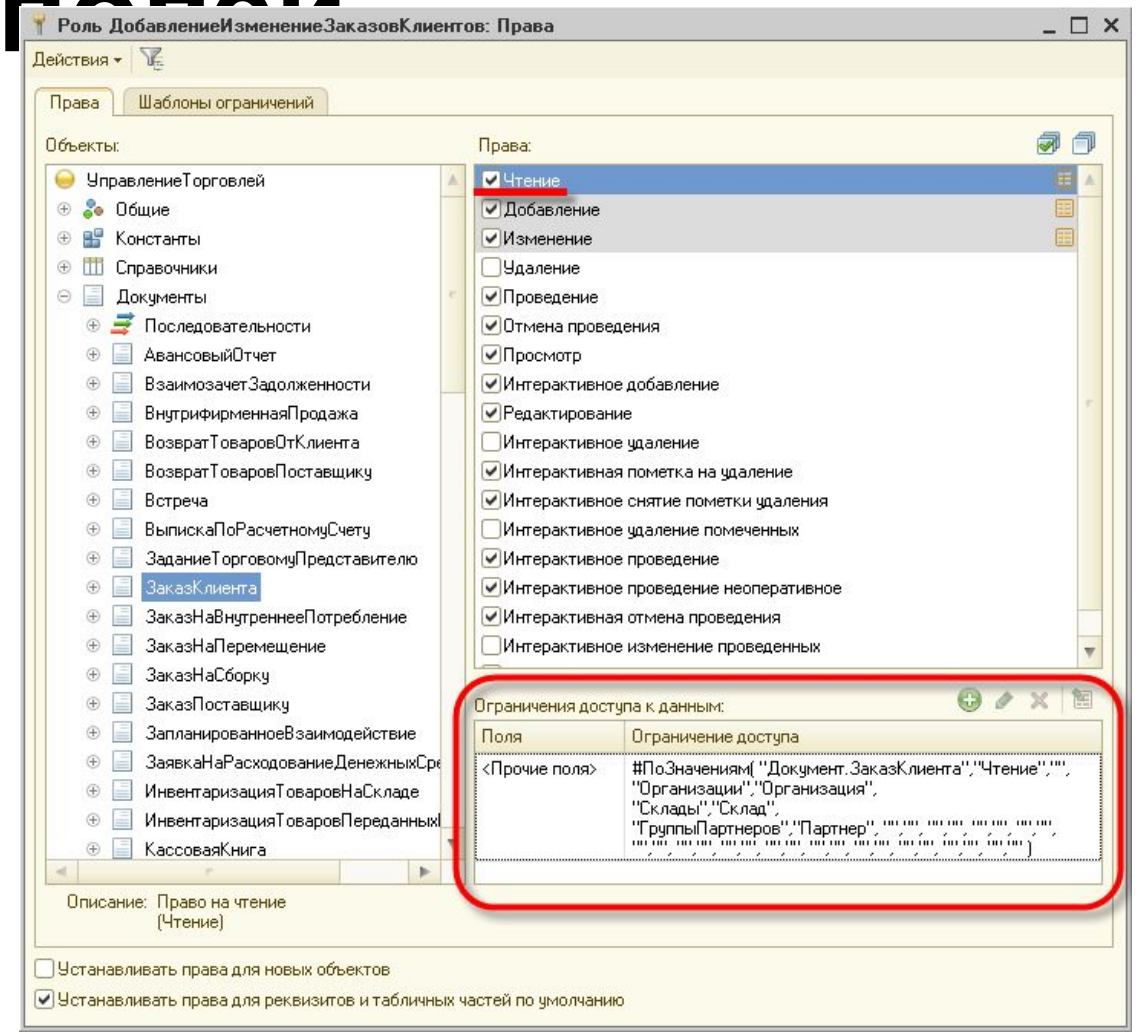
5. Ограничение доступа к данным на уровне записей и полей

Для этих действий в процессе настройки ролей могут быть заданы дополнительные условия на данные (ограничение доступа к данным). В этом случае над конкретным объектом, хранимым в базе данных, может быть выполнено запрошенное действие только в том случае, если ограничение доступа к данным для данных этого объекта принимает значение "истина". Аналогичные условия могут быть заданы и для таблиц базы данных, не имеющих объектной природы (регистров).



5. Ограничение доступа к данным на уровне записей и полей

Для объектных таблиц и регистров сведений могут быть заданы разные ограничения для различных полей таблицы, что позволяет определять ограничения не только на уровне записей базы данных, но и на уровне отдельных ее полей:



5. Ограничение доступа к данным на уровне записей и полей

Ограничение доступа к данным представляет собой условие, описанное на языке, который является подмножеством языка запросов. Это условие применяется для каждой записи таблицы базы данных, над которой выполняется операция. Если условие принимает значение "истина", то операция выполняется, а если нет, то не выполняется. Условие ограничения доступа может быть уточнено с помощью инструкций препроцессора(#ЕСЛИ <условие>, #ТОГДА.. и др.), что сделает его более эффективным. При просмотре списков и формировании отчетов существует возможность обеспечить отображение только тех данных, доступ к которым пользователю разрешен.

6. Параметры сеанса

Параметры сеанса представляют собой объекты прикладного решения, которые предназначены для использования в ограничениях доступа к данным для текущего сеанса (но могут применяться и для других целей). Их значения сохраняются в течение данного сеанса 1С:Предприятия. Использование параметров сеанса позволяет снизить время доступа к данным при ограничении доступа на уровне записей и полей.

6. Параметры сеанса

Параметры сеанса - это общие объекты конфигурации. Они предназначены для использования в ограничениях доступа к данным для текущего сеанса (но могут применяться и для других целей). Их значения сохраняются в течение данного сеанса 1С:Предприятия. Использование параметров сеанса позволяет снизить время доступа к данным при ограничении доступа на уровне записей и полей.

7. Выполнение на сервере без проверки прав

Привилегированные модули

Существует возможность назначения привилегированных модулей. В такие модули могут быть перенесены операции, использующие данные, на которые у текущего пользователя нет прав.

Например, пользователю могут быть назначены права, позволяющие создавать новый документ. Однако никаких прав на регистр, в котором этот документ создает движения при проведении, пользователю не дано. В такой ситуации процедура проведения документа может быть вынесена в привилегированный модуль, который выполняется на сервере без проверки прав. В результате, несмотря на то, что соответствующий регистр для пользователя недоступен, пользователь все же сможет проводить созданные им документы.

7. Выполнение на сервере без проверки прав

Привилегированный режим исполнения программного кода

Привилегированный режим исполнения кода, аналогичный режиму работы кода привилегированных модулей, можно включить/выключить средствами встроенного языка. Для этого в глобальном контексте предусмотрена процедура **УстановитьПривилегированныйРежим()**, а также функция **ПривилегированныйРежим()**, которая позволяет определить, включен привилегированный режим, или нет.

7. Выполнение на сервере без проверки прав

Использование привилегированного режима позволяет, во-первых, ускорить работу, так как не будут накладываться ограничения на доступ к данным, а во-вторых, позволяет выполнять операции с данными от лица пользователей, которым эти данные недоступны.

Привилегированный режим рекомендуется использовать тогда, когда с логической точки зрения нужно отключить проверку прав, или когда можно отключить проверку прав, чтобы ускорить работу. Допустимо использовать привилегированный режим тогда, когда работа с данными от лица некоторого пользователя не нарушает установленные для этого пользователя права доступа.

Обеспечение информационной безопасности

1. Криптография, механизм

Механизм криптографии позволяет прикладным решениям использовать криптографические операции для обработки данных, хранящихся в информационной базе.

Механизм криптографии не содержит реализации собственно алгоритмов криптографии. Он обеспечивает набор объектов, позволяющих взаимодействовать с внешними модулями криптографии сторонних производителей - криптопровайдерами.

1. Криптография, механизм

Для взаимодействия с криптопровайдерами в операционной системе Windows используется интерфейс CryptoAPI. Таким образом прикладные решения могут взаимодействовать с любыми криптопровайдерами, поддерживающими этот криптографический интерфейс.

1. Криптография, механизм

2. Аутентификация, механизмы

Механизм аутентификации - это один из инструментов администрирования. Он позволяет определить, кто именно из пользователей, перечисленных в списке пользователей системы, подключается к прикладному решению в данный момент.

Система поддерживает три вида аутентификации, которые могут использоваться в зависимости от конкретных задач, стоящих перед администратором информационной базы:

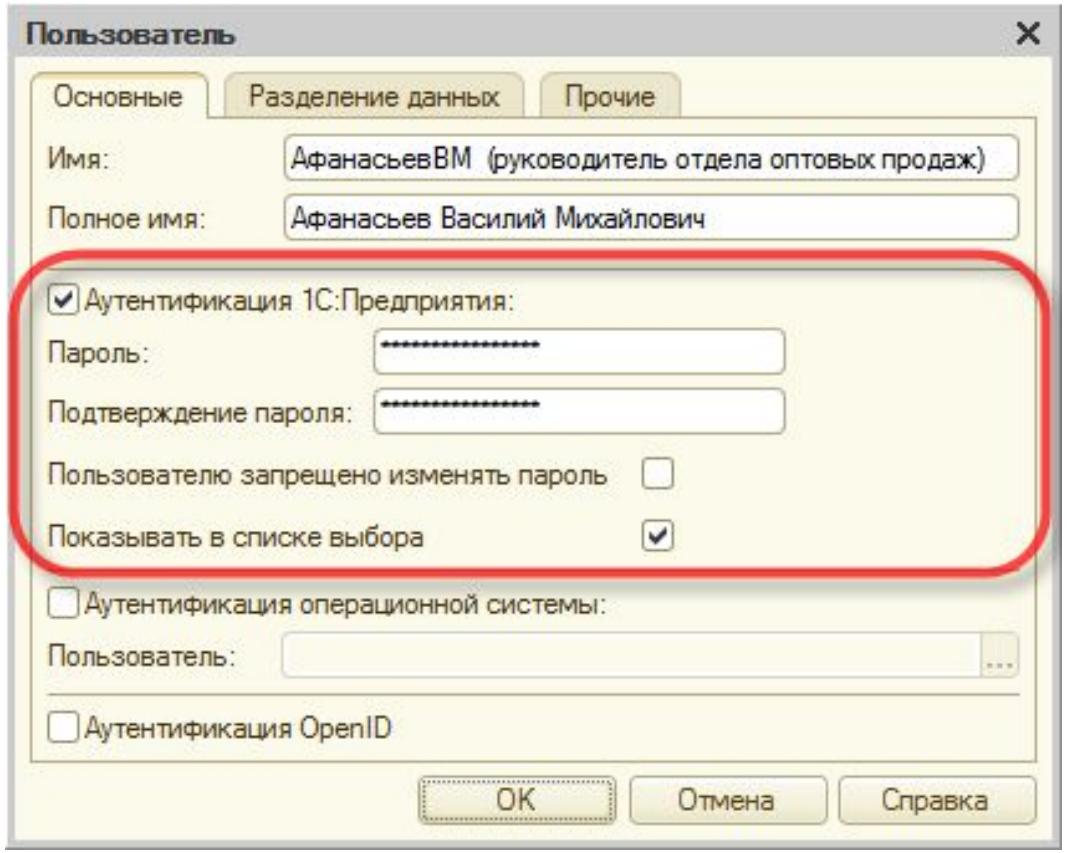
- аутентификация 1С:Предприятия;
- аутентификация операционной системы;
- OpenID-аутентификация.

Если для пользователя не указан ни один из видов аутентификации, - такому пользователю доступ к прикладному решению закрыт.

2. Аутентификация, механизмы

Аутентификация 1С: Предприятия - это один из видов аутентификации, поддерживаемых механизмом аутентификации 1С: Предприятия.

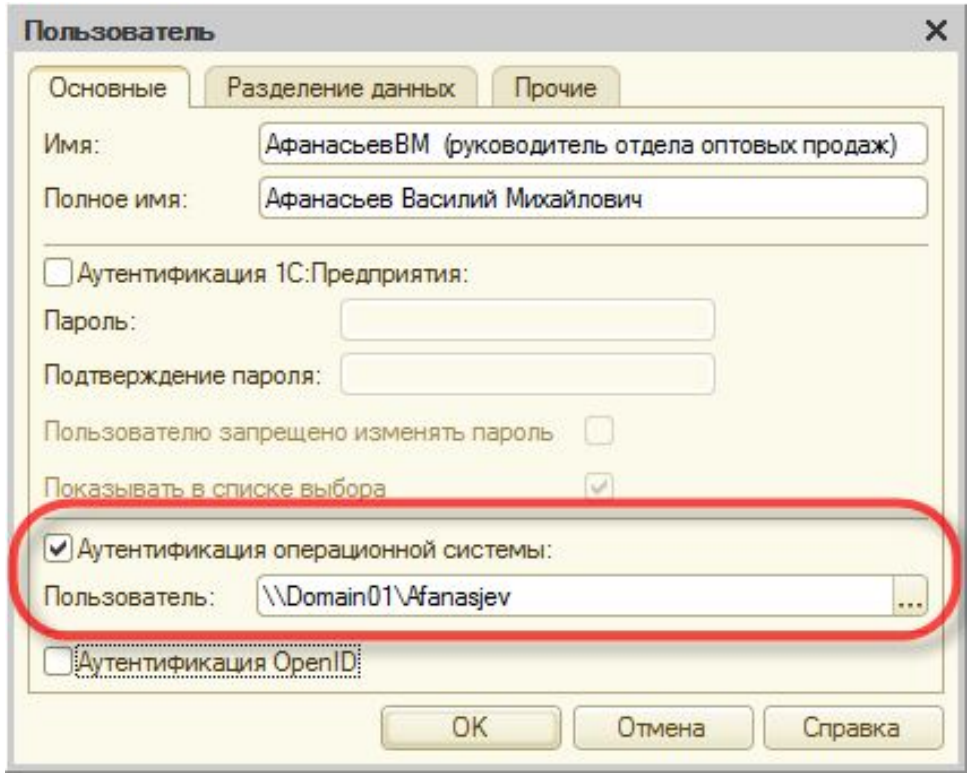
При использовании этого вида аутентификации средствами 1С:Предприятия в конфигураторе для пользователя задается пароль:



2. Аутентификация, механизмы

Аутентификация операционной системы - это один из видов аутентификации, поддерживаемых механизмом аутентификации 1С: Предприятия.

В случае аутентификации средствами операционной системы в конфигураторе для пользователя выбирается один из пользователей операционной системы:



2. Аутентификация, механизмы

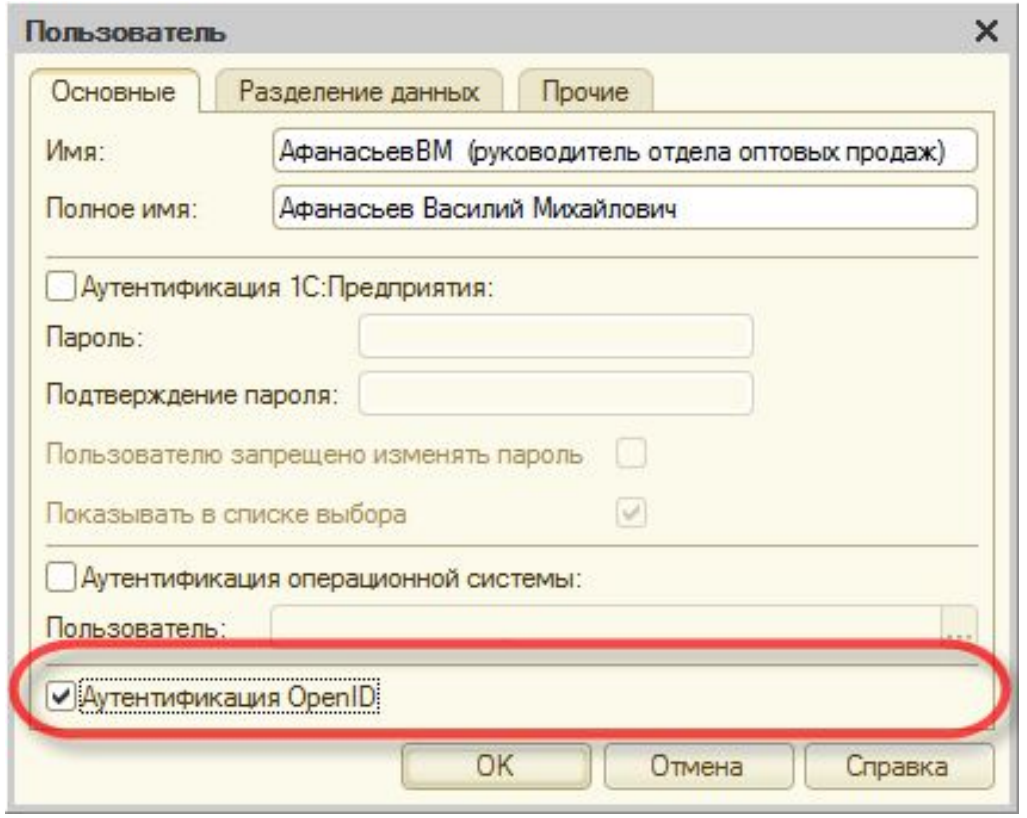
При выполнении аутентификации средствами операционной системы, от пользователя не требуется каких-либо действий по вводу логина и пароля. Система анализирует, от имени какого пользователя операционной системы выполняется подключение к прикладному решению, и на основании этого определяет соответствующего пользователя 1С:Предприятия 8. При этом диалог аутентификации 1С:Предприятия не отображается, если не указан специальный параметр командной строки.

Если для пользователя не указан ни один из видов аутентификации, - такому пользователю доступ к прикладному решению закрыт.

2. Аутентификация, механизмы

OpenID-аутентификация - это один из видов аутентификации, поддерживаемых механизмом аутентификации 1С:Предприятия.

В этом случае аутентификацию пользователя выполняет не конкретная информационная база, к которой пытается подключиться пользователь, а внешний OpenID-провайдер, хранящий список пользователей.



2. Аутентификация, механизмы

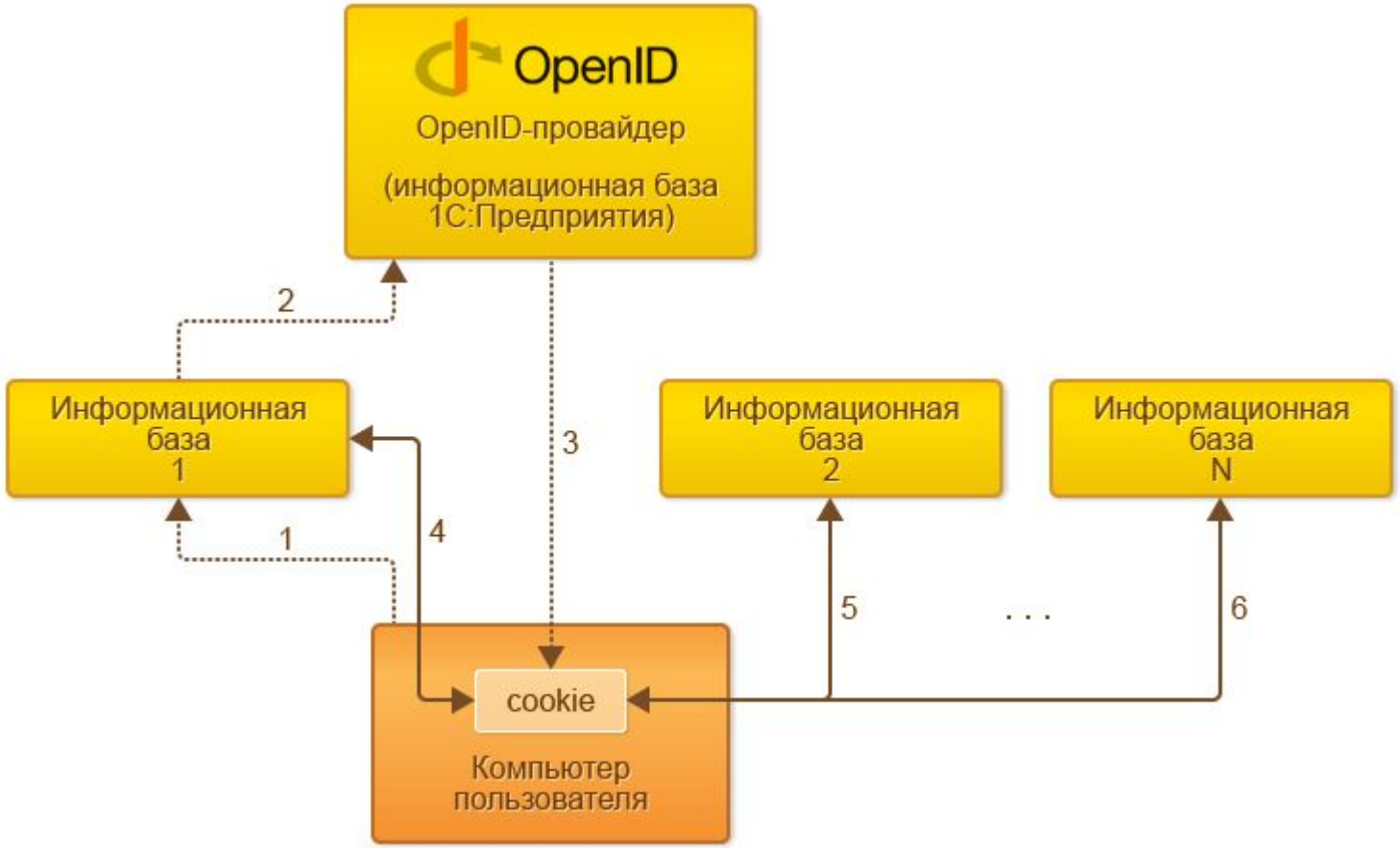
Преимущество этого вида аутентификации проявляется тогда, когда пользователь работает с большим количеством разных информационных баз.

Если используется аутентификация 1С:Предприятия, то каждый раз, при подключении к информационной базе, пользователь будет должен вводить логин и пароль.

Если же используется OpenID-аутентификация, то однажды выполнив процедуру аутентификации при подключении к одной из баз, во все остальные базы пользователь будет заходить без запроса логина и пароля. OpenID-провайдер будет автоматически аутентифицировать пользователя на основе имеющейся у него информации.

2. Аутентификация, механизмы

Последовательность действий, выполняемых при подключении пользователя, можно рассмотреть на следующе



2. Аутентификация, механизмы

В качестве OpenID-провайдера используется информационная база 1С: Предприятия. Для этого она публикуется на веб-сервере с указанием специальных параметров.

1- клиентское приложение обращается к информационной базе 1,

2 - информационная база 1 обращается к OpenId-провайдеру с тем, чтобы он аутентифицировал пользователя,

3 - OpenID-провайдер выполняет процедуру аутентификации: пользователь вводит логин и пароль; в случае успешной аутентификации на компьютере пользователя в cookie сохраняется признак того, что провайдер аутентифицировал пользователя,

4 - используя признак аутентификации, сохраненный в cookie, пользователь подключается к информационной базе 1 и начинает работу,

5, 6 - при обращении к другой информационной базе, пользователю не нужно снова вводить логин и пароль; на основании признака аутентификации, сохраненного ранее в cookie, OpenID-провайдер выполняет аутентификацию незаметно для пользователя.

3. Взлом пароля 1С

Для 1С:Предприятие 7.7

В версии 7.7 данные о пользователях и паролях хранится в папке **usrdef** информационной базы. Чтобы просто получить доступ к базе не зная пароля, достаточно переместить папку **usrdef** из папки информационной базы и тогда при следующем входе не потребуется вводить пароль. Некоторые конфигурации могут ругаться, что "*пользователь системы не определен*", в таком случае нужно в режиме "Конфигуратор" добавить нового пользователя.

Если необходимо узнать пароль пользователя, то нужно воспользоваться программой **Crash passowrd 2.0**.

3. Взлом пароля 1С

Для 1С:Предприятие 8.0 - 8.1

Файловая версия

С 8-й версией 1С:Предприятие все не так просто как с 7.7, т.к. информация о пользователях и паролях хранится в едином файле базы - 1Cv8.1CD

Что потребуется:

- Собственно сам файл базы.

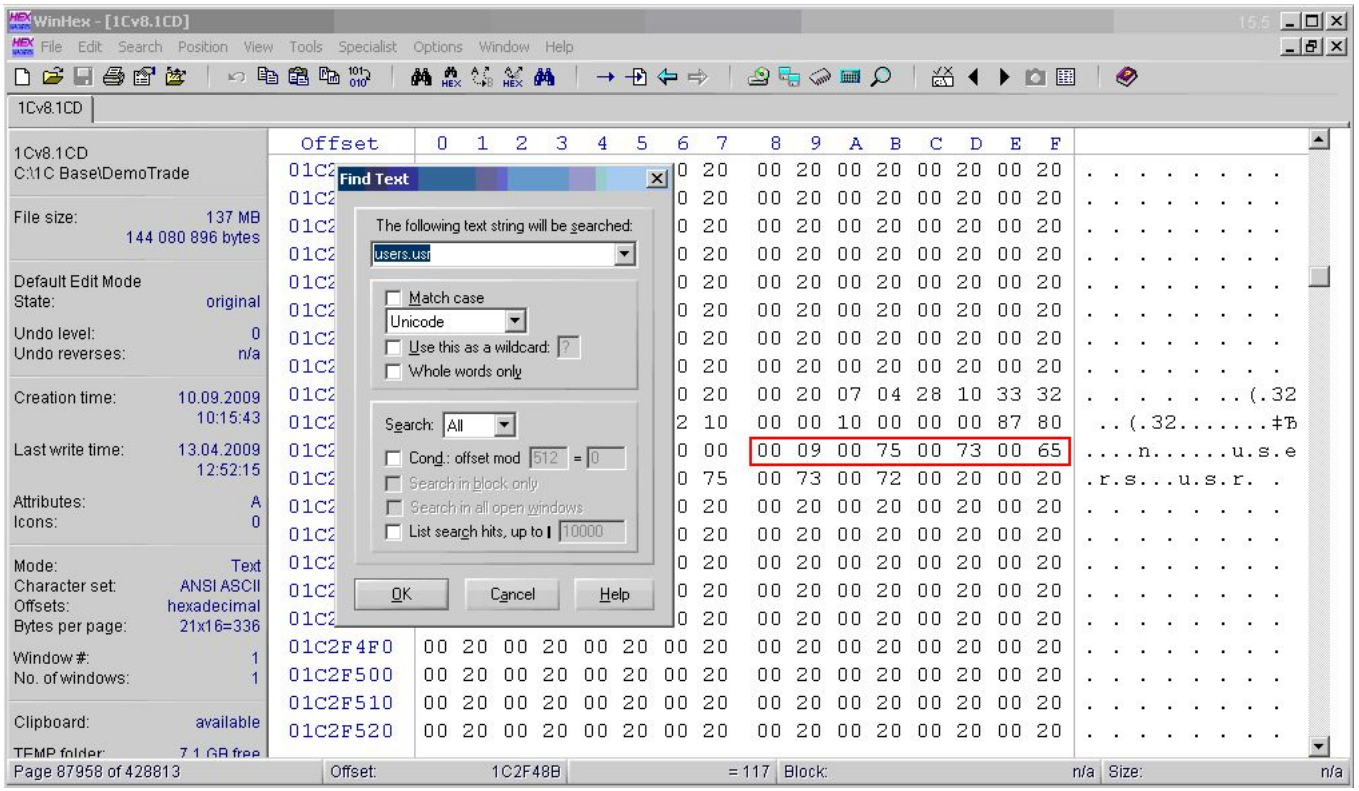
- HEX-редактор (Некоторые hex-редакторы не позволяют работать с файлами больших размеров, поэтому я предпочитаю использовать для этих целей программу WinHex).

3. Взлом пароля 1С

Для 1С:Предприятие 8.0 - 8.1

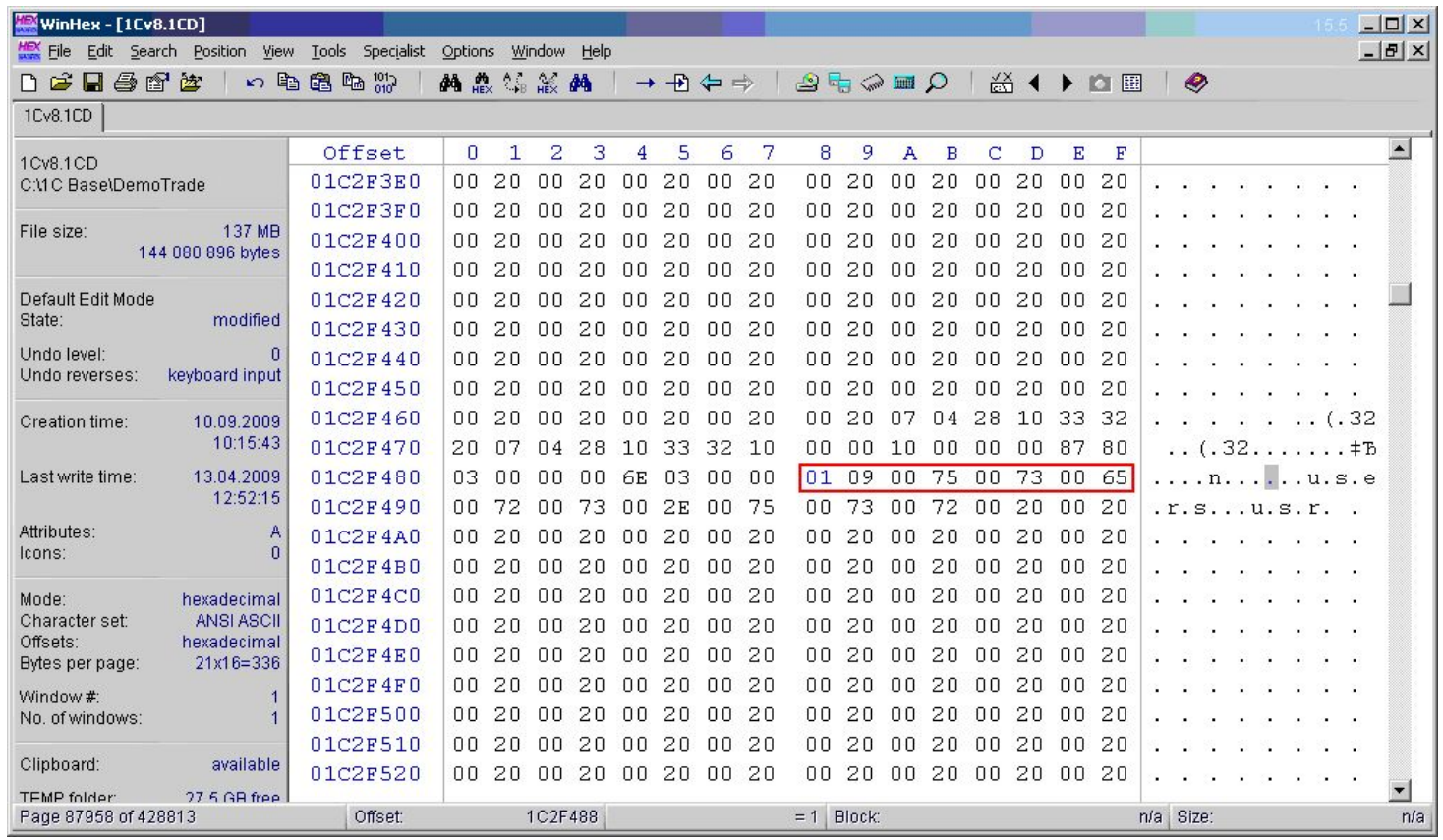
Открываем (*File -> Open*) в hex-редакторе файл базы 1Cv8.1CD

Находим строку (Unicode) вида:**00 09 00 75 00 73 00 65**



3. Взлом пароля 1С

Исправляем байт, стоящий перед **09**, в найденной строке на **01**



3. Взлом пароля 1С

После исправления, сохраняем файл в hex-редакторе (*File -> Save*). Открываем его в Конфигураторе 1С, не закрывая hex-редактор. Открываем в конфигураторе список пользователей (*Администрирование -> Пользователи*). В hex-редакторе меняем исправленное значение обратно и сохраняемся, не закрывая конфигуратор. Теперь в 1С можно обновить список пользователей – должны появиться все существующие пользователи (правда не всегда срабатывает), либо добавляем нового пользователя, устанавливаем необходимые роли, пароли и т.д.

3. Взлом пароля 1С

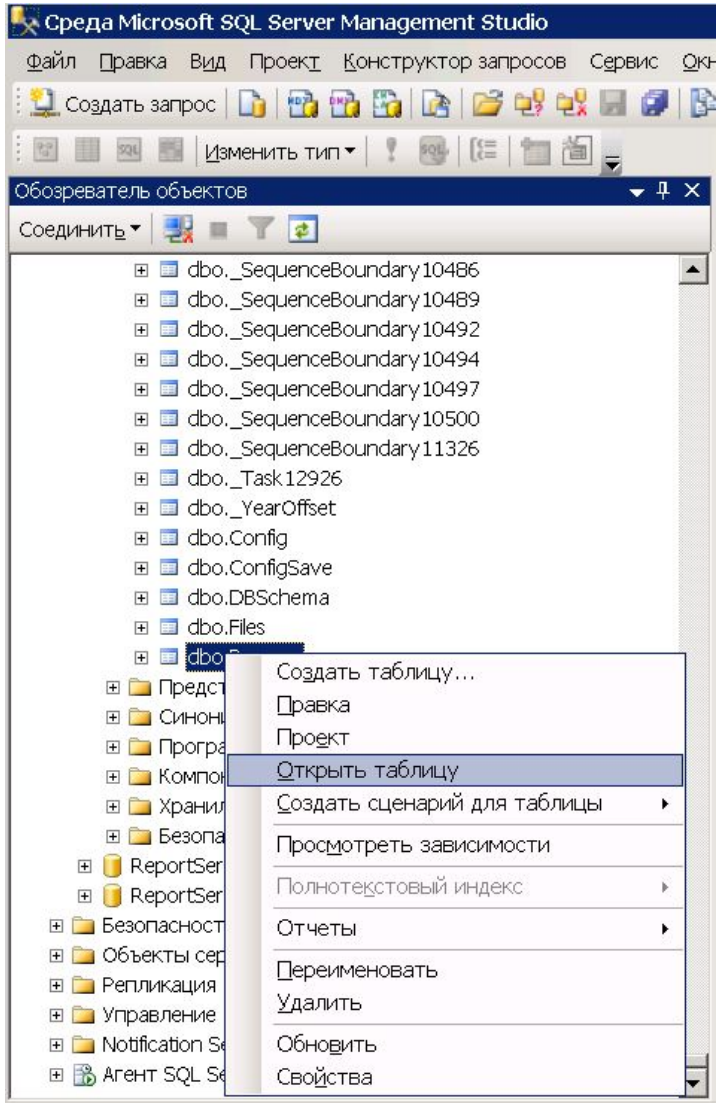
Для 1С: Предприятие 8.3 (8.3.5.1383)
В найденной строке users.usr меняем число не в столбце № 6, а ищем в этой строке число «09» и слева от него меняем «00» на «01»
Далее ищем строку «v8users».(Если не находит снимаем галочку «Match case» и повторяем поиск).
В найденной строке меняем букву «V» на «H» так, чтобы получилось «h8users» (H 8 U S E R S).

3. Взлом пароля 1С

Клиент-серверная версия

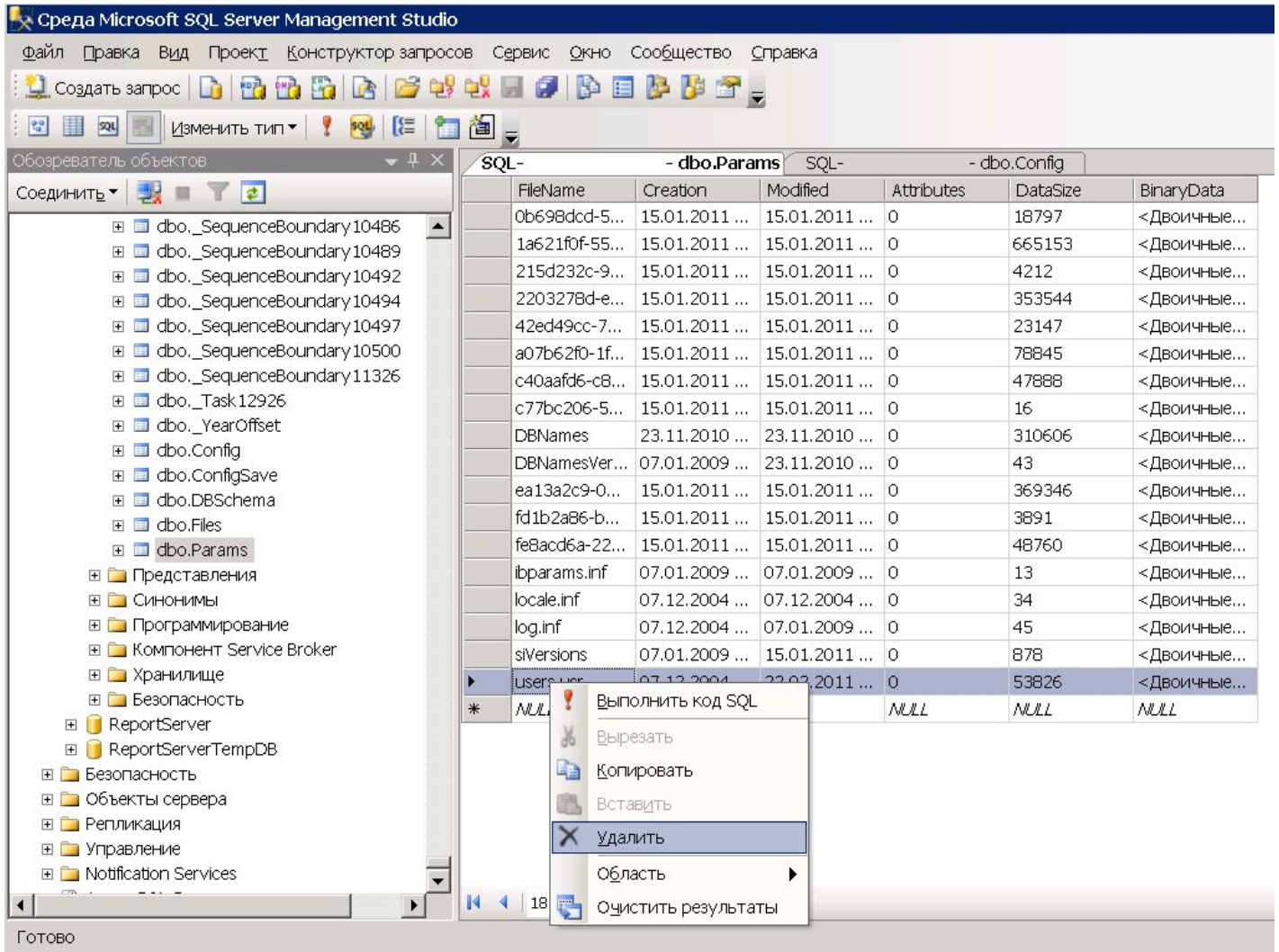
Если база размещена на SQL-сервере тогда делаем так:

- Выгоняем всех пользователей из базы
- Запускаем утилиту управления SQL-сервером (Microsoft SQL Server Menegment Studio)
- В обозревателе объектов (Object Explorer) находим в списке таблиц таблицу dbo.Params



3. Взлом пароля 1С

- Удаляем строку users.usr.
- Заходим в Конфигуратор без пароля и создаем пользователя с правами администратора.



4. Потенциальные угрозы безопасности при использовании программы 1С

Использование 1С с базами в файловом формате.

Файловые базы 1С являются наиболее уязвимые к физическому воздействию. Связано это с особенностями архитектуры такого типа баз – необходимостью держать открытыми (с полным доступом) все файлы конфигурации и самих файловых баз для всех пользователей операционной системы. В результате, любой пользователь, имеющий право работать в файловой базе 1С, теоретически может скопировать или даже удалить информационную базу 1С двумя кликами мышки.

4. Потенциальные угрозы безопасности при использовании программы 1С

Использование 1С с базами в СУБД формате. Данный тип проблем возникает, если в качестве хранилища баз 1С используется СУБД (PosgreSQL, MS SQL), а в качестве промежуточной службы связи 1С и СУБД используется сервер 1С предприятия. Такой пример – во многих компаниях практикуется доработка конфигураций 1С под свои нужды. В процессе доработки, в условиях проектной «суеты», постоянных испытаний нового доработанного функционала – ответственные специалисты зачастую пренебрегают правилами сетевой безопасности.
В результате, некоторые личности, которые имеют прямой доступ к базе данных СУБД или имеют права администратора на сервере 1С Предприятие, пусть даже на временный тестовый период – могут либо сделать резервную копию на внешние ресурсы, либо вовсе удалить базу данных в СУБД.

4. Потенциальные угрозы безопасности при использовании программы 1С

Открытость и доступность серверного оборудования. При наличии несанкционированного доступа к серверному оборудованию сотрудники компании или третьи лица могут использовать этот доступ для кражи или порчи информации. Проще говоря – если злоумышленник получает доступ непосредственно к корпусу и консоли сервера 1с – круг его возможностей расширяется в десятки раз.

4. **Потенциальные угрозы безопасности при использовании программы 1С**

Риски кражи, утечки персональных данных. Под актуальными угрозами безопасности персональных данных здесь понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, например, ответственными сотрудниками, операторами ПК, бухгалтерией и т.д.

Результатом этого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия ответственных лиц.

4. **Потенциальные угрозы безопасности при использовании программы 1С**

Сетевая безопасность. Информационная система предприятия, построенная с нарушением ГОСТ, требований к безопасности, рекомендаций, либо не имеющая надлежащей ИТ-поддержки – изобилует дырами, вирусным и шпионским программным обеспечением, множеством бэкдоров (несанкционированных доступов во внутреннюю сеть), что напрямую влияет на сохранность корпоративных данных в 1С. Это приводит к легкому доступу злоумышленника к коммерчески значимой информации. К примеру, свободный доступ к резервным копиям, отсутствие пароля на архивы с резервными копиями злоумышленник может использовать в корыстных целях. Не говоря уже об элементарном повреждении базы 1С вирусной активностью.

4. **Потенциальные угрозы безопасности при использовании программы 1С**

Взаимосвязь 1С с внешними объектами. Еще одной потенциальной угрозой является необходимость (а иногда и специальная маркетинговая особенность) учетной базы 1С связываться с «внешним миром». Выгрузки/загрузки клиент-банков, обмен информацией с филиалами, регулярная синхронизация с корпоративными сайтами, порталами, другими программами сдачи отчетности, управления клиентами и продажами и многое другое. Поскольку в данной области 1С не приветствуются соблюдения стандартов безопасности и унифицированности сетевого обмена информации – утечка вполне реальна на любом отрезке пути ее следования.

5. Обеспечение ИБ в 1С.

1. При работе с файловыми базами 1С обязательно внедрить ряд мер по обеспечению безопасности баз:

Используя разграничения доступа NTFS, дать необходимые права только тем пользователям, которые работают с этой базой, тем самым обезопасив базу от кражи или порчи недобросовестными сотрудниками или злоумышленником;

Всегда использовать авторизацию Windows для входа на рабочие станции пользователей и доступ к сетевым ресурсам;

Использовать шифрованные диски или шифрованные папки, которые позволят сохранить конфиденциальную информацию даже при выносе базы 1С;

Установить политику автоматической блокировки экрана, а также провести обучение пользователей для разъяснения необходимости блокировки профиля;

Разграничение прав доступа на уровне 1С позволит пользователям получать доступ только к той информации, на которую они имеют соответствующие права;

Необходимо разрешить запуск конфигуратора 1С только тем сотрудникам, которым он необходим.

5. Обеспечение ИБ в 1С.

2. При работе с СУБД базами 1С требуется обратить внимание на следующие рекомендации:

Учетные данные для подключения к СУБД не должны иметь административных прав;

Необходимо разграничивать права доступа к базам СУБД, например, создавать для каждой информационной базы свою учетную запись, что позволит минимизировать потерю данных при взломе одной из учетных записей;

Рекомендуется ограничить физический и удаленный доступ к серверам баз данных и 1С предприятия;

Рекомендуется использовать шифрование для баз данных, это позволит сохранить конфиденциальные данные, даже если злоумышленник получит физический доступ к файлам СУБД;

Также одним из важных решений является шифрование либо установка пароля на резервные копии данных;

Обязательным является создание администраторов кластера 1С, а также сервера 1С, так как по умолчанию если не созданы пользователи, полный доступ к информационным базам абсолютно все пользователи системы.

5. Обеспечение ИБ в 1С.

3. Требования к обеспечению физической безопасности серверного оборудования:

(согласно ГОСТ Р ИСО/МЭК ТО – 13335)

Доступ к зонам, где обрабатывается или хранится важная информация, должен управляться и быть ограничен только полномочными лицами;

Средства управления аутентификацией, например, карточка управления доступом плюс персональный идентификационный номер [PIN], должны использоваться, чтобы разрешать и подтверждать любой доступ;

Контрольный журнал всего доступа должен содержаться в надежном месте;

Персоналу вспомогательных служб третьей стороны должен быть предоставлен ограниченный доступ в зоны безопасности или к средствам обработки важной информации только тогда, когда требуется;

этот доступ должен быть разрешен и должен постоянно контролироваться;

5. Обеспечение ИБ в 1С.

3. Требования к обеспечению физической безопасности серверного оборудования:

(согласно ГОСТ Р ИСО/МЭК ТО – 13335)

Права доступа в зоны безопасности должны регулярно анализироваться и обновляться, и отменяться, если необходимо;

Должны быть учтены соответствующие нормы и стандарты по технике безопасности и охране труда;

Ключевые средства должны быть расположены так, чтобы избежать доступа к ним широкой публики;

Там, где это применимо, здания и комнаты должны быть скромными и должны давать минимальное указание на их цель, без ярких надписей, снаружи здания или внутри него, указывающих на наличие видов деятельности по обработке информации;

Указатели и внутренние телефонные книги, указывающие на местоположения средств обработки важной информации, не должны быть легко доступны широкой публике.

5. Обеспечение ИБ в 1С.

4. Конфиденциальность персональных данных. Основной целью при организации защиты персональных данных является нейтрализация актуальных угроз в информационной системе, определенных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», перечнем государственных стандартов и требований международных сертификаций по ИТ-безопасности (ГОСТ Р ИСО/МЭК 13335 2-5, ISO 27001). Достигается это путем ограничения доступа к информации по ее типам, разграничение доступа к информации по ролям пользователей, структурирование процесса обработки и хранения информации.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей;

Согласие на обработку персональных данных должно быть конкретным, информированным и сознательным;

Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;

Обработке подлежат только персональные данные, которые отвечают целям их обработки;

Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом;

5. Обеспечение ИБ в 1С.

4. Конфиденциальность персональных данных. Основной целью при организации защиты персональных данных является нейтрализация актуальных угроз в информационной системе, определенных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», перечнем государственных стандартов и требований международных сертификаций по ИТ-безопасности (ГОСТ Р ИСО/МЭК 13335 2-5, ISO 27001). Достигается это путем ограничения доступа к информации по ее типам, разграничение доступа к информации по ролям пользователей, структурирование процесса обработки и хранения информации.

Фотографическое, видео, аудио или другое записывающее оборудование, такое как камеры на мобильных устройствах, не должны допускаться, если только не разрешено;

Накопители со сменным носителем должны быть разрешены только в том случае, если для этого есть производственная необходимость;

Чтобы исключить злонамеренные действия в отношении конфиденциальной информации, требуется бумажные и электронные носители информации, когда они не используются, хранить в надлежащих запирающихся шкафах и/или в других защищенных предметах мебели, особенно в нерабочее время;

Носители с важной или критичной служебной информацией, когда они не требуются, следует убирать и запирать (например, в несгораемом сейфе или шкафу), особенно когда помещение пустует.

5. Обеспечение ИБ в 1С.

5. Сетевая безопасность - это набор требований, предъявляемых к инфраструктуре компьютерной сети предприятии и политикам работы в ней, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа. В рамках рекомендуемых действий по организации и обеспечению сетевой безопасности, помимо базовых, можно рассмотреть следующие особенности:

В первую очередь, в компании должен быть внедрен единый регламент информационной безопасности с соответствующими инструкциями;

Пользователям должен быть максимально закрыт доступ к нежелательным сайтам, в том числе файлообменникам;

Из внешней сети должны быть открыты только те порты, которые необходимы для корректной работы пользователей;

Должна присутствовать система комплексного мониторинга действий пользователей и оперативного оповещения нарушения нормального состояния всех общедоступных ресурсов, работа которых важна для Компании;

Наличие централизованной антивирусной системы и политик очистки и удаления вредоносных программ;

Наличие централизованной системы управления и обновления антивирусным ПО, а также политик регулярных обновлений ОС;

5. Обеспечение ИБ в 1С.

5. Сетевая безопасность - это набор требований, предъявляемых к инфраструктуре компьютерной сети предприятии и политикам работы в ней, при выполнении которых обеспечивается защита сетевых ресурсов от несанкционированного доступа. В рамках рекомендуемых действий по организации и обеспечению сетевой безопасности, помимо базовых, можно рассмотреть следующие особенности:

Возможность запуска съемных флэш носителей должна быть максимально ограничена;

Пароль должен быть не менее 8 символов, содержать цифры, а также буквы верхнего и нижнего регистров;

Должна быть защита и шифрование ключевых папок обмена информацией, в частности файлов обмена 1с и системы клиент-банк;

Силовые линии и линии дальней связи, входящие в средства обработки информации, должны быть подземными там, где это возможно, или должны подлежать адекватной альтернативной защите;

Сетевые кабели должны быть защищены от неразрешенного перехвата или повреждения, например, путем использования кабельного канала или избегания маршрутов, пролегающих через общедоступные зоны.