Утверждён
643.БПВА.10002-02 32 ЛУ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

СТАРТ-2ПС

РУКОВОДСТВО СИСТЕМНОГО АДМИНИСТРАТОРА

643.БПВА.10002-02 32

ЛИСТОВ 108

2012

ЛИТЕРА

Подп. и дата	
Инв.№ дубл.	
Взам. инв. №	
Подп. и дата	
Инв.№ подл	

Аннотация

Данный документ описывает механизмы работы системного администратора с программой «СТАРТ-2ПС», устанавливает правила и ограничения на применение программы

Содержание

Раздел 1 Назначение программы 4

Раздел 2 Описание программы 5

1 Архитектура программного обеспечения 5

Общие положения 5

Организация информационного обмена 6

Организационные группы 7

Состав и взаимодействие компонентов узла 8

2 Назначение компонентов системы Старт-2 ПС 8

Программа оперативного контроля 8

Хранилище 9

Сервер терминалов РЗА (ROPC) 9

Служба сетевого информатора 10

Шаблоны (файлы описания конфигурации устройств) 10

Служба аварийного контроля 10

3 Взаимодействие компонентов системы Старт-2 ПС 10

Раздел 3 Условия выполнения программы 13

1 Технические требования к оборудованию 13

2 Технические требования к локальной сети 15

Рекомендации по выбору параметров сети 15

Раздел 4 Выполнение программы 17

1 Подготовка компьютера для установки системы 17

Типы установки 17

Операционная система Windows XP SP3 18

Основная и локальная установка 18

Основная установка 21

Операционная система Windows Vista Business / Ultimate SP2 28

Основная и локальная установка 28

Основная установка 32

Операционная система Windows 7 Professional/Ultimate 39

Основная и локальная установка 39

Основная установка 44

Операционная система Windows Server 2003 Std SP2 50

Основная и локальная установка 50

Основная установка 55

Операционная система Windows Server 2008 Std SP2 (2008 R2) 62

Основная и локальная установка 62

Основная установка 69

2 Установка и удаление системы 76

Установка Старт-2ПС 76

Установка системы поверх существующей 82

Удаление системы или её компонентов 83

3 Конфигурирование программного обеспечения 83

Раздел 5 Административные настройки 84

1 Особенности развёртывания системы в домене 84

2 Настройка компонентов ПО 85

Общие сведения о настройке компонентов ПО 85

Структура файла конфигурации 87

Настройки уровня операционной системы 88

Примеры настройки уровня операционной системы ... 92
Пример настройки организационных групп ... 92
Пример настройки статически заданных узлов ... 93
Настройка службы сетевого информатора ... 93
Настройка компонента "Хранилище" ... 94

Раздел 6 Устранение неполадок 98

1 Контрольный лист настройки компьютера ... 98

Раздел 7 Часто задаваемые вопросы 100

1 Что такое демо-режим? ... 100
2 Как узнать версию системы? ... 101
3 Как убрать окно приветствия при запуске Windows XP? ... 102
4 Где найти диагностические сообщения системы? ... 103
5 Как управлять службами Windows? ... 104

Раздел 8 Приложения 105

1 Приложение А. Архитектура АСУТП ... 105
2 Приложение Б. Взаимодействие с внешними сетями ... 105
3 Приложение В. Организационные группы ... 106
4 Приложение Г. Взаимодействие компонентов узла ... 106

Раздел 9 Лист сводки параметров 107

1 Назначение программы

ПО «СТАРТ-2ПС» представляет собой комплекс программ предназначенных для создания АСУТП ПС. ПО «СТАРТ-2ПС» может быть использовано как сервер сбора данных, АРМ РЗА, АРМ дежурного оператора, АРМ диспетчера и т.п. Компоненты ПО могут работать как на одном компьютере, так и удаленно

2 Описание программы

2.1 Архитектура программного обеспечения

2.1.1 Общие положения

ПО «СТАРТ-2ПС» построена на основе объединённых в локальную вычислительную сеть (ЛВС) персональных и промышленных ЭВМ, к каждой из которых могут быть подключены терминалы РЗА и другое промышленное оборудование (Приложение А). Каждая ЭВМ с комплектом подключенного к ней оборудования в рамках данного документа именуется узлом.

Узел может быть построен на основе персональной ЭВМ в настольном, серверном или промышленном исполнении в соответствии с назначением узла и условиями эксплуатации ЭВМ. На ЭВМ используется программное обеспечение, работающее под управлением операционной системы Microsoft Windows, не ниже версии XP SP3.

Терминалы РЗА и другое промышленное оборудование подключается к ЭВМ узла посредством штатных интерфейсов USB, RS-232, RS-485. При необходимости узел доукомплектовывается дополнительными интерфейсными устройствами. В качестве интерфейсных устройств могут применяться как простые, так и более сложные устройства, например такие, как изображённый на рисунке сервер последовательных устройств, представляющий собой мост Ethernet - RS485. С удалённым оборудованием возможна организация связи по телефонным линиям, с помощью модемов. Целесообразность применения тех или иных интерфейсных устройств определяется проектом.

Локальная вычислительная сеть строится на основе стандартного оборудования Ethernet 100/1000. Топология сети определяется проектом, индивидуально для каждой подстанции. В качестве сетевого протокола нижнего уровня используется протокол TCP/IP; все узлы системы СТАРТ-2ПС должны быть членами одной подсети (использовать одинаковую маску подсети).

Защита от несанкционированного доступа к функциям системы СТАРТ-2ПС обеспечивается встроенными в операционную систему Microsoft Windows механизмами. В соответствии с выданными Microsoft сертификатами Российской Федерации, в операционных системах Windows XP и Windows 7 возможна обработка информации с максимальным грифом «Для служебного пользования», а при применении дополнительных (покупных) средств защиты – «Секретно».

Наилучшая защита от несанкционированного доступа обеспечивается при организации сети на основе домена Windows. При организации сети на основе рабочих групп обеспечивается более низкий уровень защиты, однако такое решение существенно ниже по стоимости и часто оптимально. В случае развёртывания всей системы на одном узле, при необходимости, функции защиты могут быть отключены вообще.

2.1.2 Организация информационного обмена

Внутри системы СТАРТ-2ПС информационный обмен между узлами построен с использованием следующих протоколов прикладного уровня:

- DCOM OPC DA – для организации обмена с серверами OPC. Технология DCOM разработана Microsoft для распределённых приложений, OPC – набор протоколов консорциума OPC Foundation (http://opcfoundation.org), предназначенных для формализации доступа к оборудованию разных производителей
- HTTP – для публикации отчётов о работе системы. Протокол HTTP является одним из общепринятых протоколов Интернета
- .NET Remoting и UDP – для взаимодействия узлов между собой
- Windows 32 API - для запросов и ответов на самоконтроль

Взаимодействие ЭВМ узла с подключенным к ней устройствами обеспечивается с использованием аппаратно – зависимых протоколов, скрытых от конечного пользователя системы СТАРТ-2ПС.

Более подробно взаимодействие компонентов системы СТАРТ-2ПС между собой будет рассмотрено ниже.

С внешними по отношению к СТАРТ-2ПС сетями система взаимодействует по следующим протоколам

- HTTP – для публикации отчётов о работе системы
- DCOM OPC DA – для организации обмена с серверами OPC

В приложении Б изображён вариант топологии сети с рабочими местами (1, 2, 6, 7, 8, 9, 10), не входящими в систему СТАРТ-2ПС.

Рабочие места 1 и 2 подключены непосредственно к сегменту ЛВС подстанции. Рабочие места 9 и 10 подключены к ЛВС более высокого уровня (здесь - корпоративная ЛВС). Сегменты ЛВС подстанции и корпоративной ЛВС связаны с

помощью сетевого оборудования (здесь – сетевой коммутатор, 4). Рабочие места 6, 7 и 8 могут находиться в любой точке Мира и подключаются через Интернет (5). Для обеспечения безопасности ЛВС подстанции связана с Интернетом через брандмауэр (сетевой экран) (3).

На всех рабочих местах возможно предоставление доступа к отчётам системы СТАРТ-2ПС посредством протокола HTTP. При этом установки специального программного обеспечения не требуется: взаимодействие с генератором отчётов осуществляется с помощью Интернет – обозревателей (Microsoft Internet Explorer, Opera, Firefox и др.). С помощью настроек параметров безопасности входящего в состав системы СТАРТ-2ПС интернет – сервера, а также с помощью настроек брандмауэра можно указать, кому и в каком объёме предоставляется фактический доступ.

В рамках ЛВС подстанции и корпоративной ЛВС, при необходимости, может быть организован доступ программного обеспечения сторонних производителей к входящим в состав системы серверам OPC. Доступ предоставляется посредством протокола DCOM OPC DA. Параметры безопасности доступа при этом настраиваются средствами DCOM.

2.1.3 Организационные группы

На крупной подстанции с разветвлённой топологией оборудование может быть разбито на группы, управление которыми может быть поручено разным операторам. Для поддержания такого сценария система СТАРТ-2ПС может быть разбита на организационные группы, соответствующие сферам ответственности операторов.

Приложение В иллюстрирует подобное разбиение. Здесь в сферу ответственности операторов группы 1 входят узлы 1…6, в сферу ответственности группы 2 – узлы 5…10. Как видно на рисунке, часть узлов входит в исключительное ведение операторов группы 1 (узлы 1…4), другая часть – в ведение группы 2 (узлы 7…10), и часть узлов входит в совместное ведение обоих операторов (узлы 5 и 6).

Узлы 1…6 и 5…10 в процессе работы «видят» друг друга и между ними автоматически устанавливается взаимодействие. Операторы могут непосредственно наблюдать процессы, происходящие в группах, при этом они не перегружены излишней информацией. Управление процессами системы для каждого из операторов ограничено узлами его группы, а также совместными узлами в соответствии с полномочиями оператора.

2.1.4 Состав и взаимодействие компонентов узла

Состав программных компонентов узла (Приложение Г) зависит от его назначения. Однако на каждый узел всегда устанавливаются компоненты инфраструктуры. К компонентам инфраструктуры относятся следующие компоненты:

- Служба сетевого информатора
- Шаблоны (файлы описания конфигурации устройств)
- Служба аварийного контроля

Остальные компоненты устанавливаются по мере необходимости. К таким компонентам относятся, в частности:

- Программа оперативного контроля
- Мнемосхемы пользователя
- Хранилище
- Генератор отчётов
- Сервер терминалов РЗА (ROPC)

2.2 Назначение компонентов системы Старт-2 ПС

2.2.1 Программа оперативного контроля

«Программа оперативного контроля» является основным компонентом, обеспечивающим наблюдение за системой и управление всеми её функциями. Компонент выполнен в виде обычного интерактивного Windows – приложения.

Программа может дополнительно оснащаться подключаемыми «Мнемосхемами пользователя». Каждый такой компонент реализует одну мнемосхему энергосистемы; количество таких модулей принципиально не ограничено. Мнемосхемы в необходимом количестве разрабатываются под каждую подстанцию в процессе проектирования и пуско-наладочных работ. Разработка мнемосхем может быть осуществлена персоналом, занятым пуско-наладочными работами, самостоятельно. Для разработки мнемосхем ЗАО «РАДИУС Автоматика» предоставляет комплект разработчика.

При каждом старте «Программа оперативного контроля» обнаруживает установленные мнемосхемы, подключает их и запускает в работу. С этого момента подключаемые модули становятся частью «Программы оперативного контроля».

2.2.2 Хранилище

Компонент «Хранилище» предназначен для сбора и архивирования информации, циркулирующей в системе в процессе её работы. Компонент выполнен в виде службы Windows NT и запускается автоматически при старте компьютера. Базы данных компонента размещаются в системе управления базами данных (СУБД), в качестве которой используется продукт Microsoft SQL Server, также реализованный в виде службы Windows NT. Использование СУБД MS SQL Server является внутренним механизмом, скрытым от конечного пользователя.

Дочерним компонентом службы хранилища является компонент «Генератор отчётов». Он устанавливается одновременно с установкой компонента «Хранилище» и предназначен для генерации отчётов о работе системы. Технически «Генератор отчётов» выполнен в виде WEB – сайта, построенного на технологиях ASP NET и AJAX. Сайт работает внутри IIS (Internet Information Service) – встроенного компонента операционной системы Windows. В качестве источника данных для генератора отчётов используются базы данных, накапливающие информацию в процессе работы компонента «Хранилище».

При типовых требованиях к архиву (для небольших подстанций), компоненты «Хранилище» и «Генератор отчётов» размещаются на ЭВМ с настольной операционной системой MS Windows XP (и выше). В качестве СУБД при этом используется бесплатный компонент MS SQL Server Express Edition. При этом обеспечиваются удовлетворительные производительность и глубина хранения данных, а также поддерживается до 10 одновременных клиентских подключений к генератору отчётов.

При повышенных требованиях к хранилищу, эти компоненты должны размещаться на ЭВМ с серверной операционной системой MS Windows Server 2003 Std (и выше), а в качестве СУБД должен применяться дополнительно приобретаемый MS SQL Server Std Edition (и выше). При этом снимаются ограничения по глубине хранения данных и количеству одновременных клиентских ограничений; кроме того серверные продукты имеют существенно более высокую производительность.

2.2.3 Сервер терминалов РЗА (ROPC)

Компонент «Сервер терминалов РЗА» обеспечивает взаимодействие с оборудованием узла посредством аппаратно-программных интерфейсов. Скрывая особенности взаимодействия с оборудованием, компонент обеспечивает стандартизированный доступ других компонентов системы к функциям оборудования

по протоколу DCOM OPC DA. Как уже указывалось, такой же доступ может быть предоставлен внешним компонентам сторонних производителей.

В качестве аппаратно – программных интерфейсов типично используются решения на основе RS-232, USB, RS-485; поддерживается обмен с удалённым оборудованием посредством модема и телефонных линий.

Компонент «Сервер терминалов РЗА» спроектирован таким образом, чтобы была возможность его использования вне системы СТАРТ-2ПС, в связи с чем алгоритмы его взаимодействия с системой отличаются от других компонентов (см. ниже).

ПРИМЕЧАНИЕ - В рамках настоящего документа в качестве наименования компонента «Сервер терминалов РЗА» может использоваться его краткий синоним "ROPC".

2.2.4 Служба сетевого информатора

Компонент «Служба сетевого информатора» предназначен для организации сетевого взаимодействия компонентов системы между собой.

2.2.5 Шаблоны (файлы описания конфигурации устройств)

Шаблоны – описатели устройств представляют собой набор файлов в формате XML, в которых формально описаны характеристики устройств и способы визуализации параметров, предоставляемых устройствами.

2.2.6 Служба аварийного контроля

Служба аварийного контроля предназначена для контроля работоспособности других служб системы, а также для восстановления их работы в случае отказа.

2.3 Взаимодействие компонентов системы Старт-2 ПС

После старта ЭВМ в узле автоматически запускаются в работу компоненты "Служба сетевого информатора" и "Служба аварийного контроля" (Приложение Г).

«Служба сетевого информатора» считывает конфигурацию компонентов узла и готовит её для публикации. Одновременно с этим по протоколу UDP она рассылает широковещательный запрос для поиска аналогичных служб в других узлах системы СТАРТ-2ПС (через интерфейс взаимообнаружения). Службы сетевого информатора других узлов, имеющих такой же идентификатор системы, отвечают на запрос, передавая описание параметров доступа к собственному интерфейсу информатора.

ПРИМЕЧАНИЕ: работа механизма взаимообнаружения может быть запрещена, в этом случае список входящих в систему узлов задаётся статически (см. раздел административных настроек).

Данные о собственной конфигурации объединяется с данными об информаторах в других узлах системы, образуя сведения о сетевой конфигурации системы. Сведения о сетевой конфигурации становятся доступными через интерфейс информатора. Для интерфейса информатора используется внутренний протокол, основанный на .NET Remoting операционной системы Windows.

Клиент («Программа оперативного контроля», «Хранилище») запрашивает сведения о сетевой конфигурации у службы сетевого информатора, после чего планирует свою дальнейшую работу: подключается к компонентам ROPC узлов системы, генераторам отчётов, взаимодействует с оператором и пр.

По принятым в системе СТАРТ-2ПС соглашениям, после старта клиента, он обязан сообщить о начале своей работы службе сетевого информатора через её интерфейс контроля состояния. Для этого интерфейса также используется внутренний протокол, основанный на .NET Remoting операционной системы Windows.

В процессе работы с помощью того же интерфейса клиент должен периодически сообщать службе о своей работоспособности, а перед окончанием работы – сообщить о плановом завершении работы.

Данные о работоспособности компонентов являются частью сведений о сетевой конфигурации и могут быть отображены на экране компонента «Программа оперативного контроля».

Сбор данных о состоянии компонента «Сервер терминалов РЗА» производится несколько иначе. Для анализа состояния ROPC производится анализ состояния Windows NT-службы ROPC, для чего используется встроенный в операционную систему компонент, управляющий службами (SCM).

Состояния компонентов системы служба сетевого информатора передаёт для документирования всем узлам системы, на которых установлено хранилище. Для этих целей компонент «Служба хранилища» реализует интерфейс протоколирования состояний, также основанный на протоколе .NET Remoting.

Для документирования действий оператора «программы оперативного контроля», этот компонент вызывает методы интерфейса протоколирования действий «Хранилища» всех узлов системы. Этот интерфейс также основан на протоколе .NET Remoting.

Все экземпляры компонентов «Хранилище» на всех узлах системы работают параллельно, обеспечивая сбор и архивирование данных, поступающих от всех компонентов «Сервер терминалов РЗА», «Программа оперативного контроля» и «Служба сетевого информатора», обеспечивая тем самым горячее резервирование функций архива.

Компонент «Сервер терминалов РЗА» запускается при подключении к нему первого клиента. В связи с необходимостью обеспечения самоописания, конфигурация устройств, подключенных к ЭВМ, хранится в конфигурационных файлах ROPC. Это требование связано с необходимостью предоставления доступа к устройствам со стороны внешних по отношению к системе программных компонентов сторонних производителей. Такое поведение является частью протокола OPC.

В процессе работы компонент «Сервер терминалов РЗА» осуществляет сбор данных, поступающих из устройств в соответствии с параметрами клиентских подписок, а также отправляет в устройства управляющие воздействия и параметры настроек.

Компонент «Генератор отчётов» формирует WEB - страницы, на которых можно выбрать вид и параметры отчёта, и возвращает готовые отчёты в виде WEB – страниц. На страницах отчёта доступны также средства для генерации готовых к печати форм в PDF формате.

Хотя отображаемая генератором отчётов информация и размещается во встроенном окне компонента «Программа оперативного контроля», для обеспечения унификации доступ к генератору из него всё равно осуществляется по протоколу HTTP. Это гарантирует идентичность отчётов, получаемых как с помощью «программы оперативного контроля», так и с помощью внешних Интернет – обозревателей.

В процессе своей работы компонент "Служба аварийного контроля" периодически требует проведения самоконтроля от других компонентов - служб системы. В случае отсутствия ответа на запрос самоконтроля, контролируемая служба считается неисправной и производится её перезапуск.

3 Условия выполнения программы

3.1 Технические требования к оборудованию

Компоненты программного комплекса могут запускаться как по отдельности на разных компьютерах, так и на одном компьютере одновременно. Ниже приведены минимальные требования для работы каждого компонента ПО «СТАРТ-2ПС».

1. Сервер терминалов РЗА. Для работы с 8-ю портами RS-485 при обработке информации с 40 терминалов:

   1.1.Процессор: Intel Pentium, 1ГГц

   1.2.Оперативная память: 512МБ

   1.3.Дисплей: можно без дисплея

   1.4.Жесткий диск: согласно минимальным требованиям операционной системы плюс 2 ГБ

   1.5.Операционная система:

      1.5.1.Windows XP Professional Service Pack 3 (32-х разрядная)

      1.5.2.Windows Vista Business Service Pack 2 (32-х разрядная)

      1.5.3.Windows Vista Ultimate Service Pack 2 (32-х разрядная)

      1.5.4.Windows 7 Professional (32-х и 64-х разрядная)

      1.5.5.Windows 7 Ultimate (32-х и 64-х разрядная)

      1.5.6.Windows Server 2003 Std Service Pack 2 (32-х разрядная)

      1.5.7.Windows Server 2008 Std Service Pack 2 (32-х разрядная)

      1.5.8.Windows Server 2008 R2 Std Service Pack 1 (64-х разрядная)

2. Хранилище и WEB генератор отчетов.

   2.1.Процессор: Intel Pentium, 1.4ГГц

   2.2.Оперативная память: 1ГБ

   2.3.Дисплей: можно без дисплея

   2.4.Жесткий диск: согласно минимальным требованиям операционной системы плюс 8 ГБ

   2.5.Операционная система:

      2.5.1.Windows XP Professional Service Pack 3 (32-х разрядная)

2.5.2.Windows Vista Business Service Pack 2 (32-х разрядная)

2.5.3.Windows Vista Ultimate Service Pack 2 (32-х разрядная)

2.5.4.Windows 7 Professional (32-х и 64-х разрядная)

2.5.5.Windows 7 Ultimate (32-х и 64-х разрядная)

2.5.6.Windows Server 2003 Std Service Pack 2 (32-х разрядная)

2.5.7.Windows Server 2008 Std Service Pack 2 (32-х разрядная)

3. Программа оперативного контроля.

3.1.Процессор: Intel Pentium, 1.4ГГц

3.2.Оперативная память: 512МБ

3.3.Дисплей: 17”, 1280x1024

3.4.Жесткий диск: согласно минимальным требованиям операционной системы плюс 2 ГБ

3.5.Операционная система (32-х разрядная):

3.5.1.Windows XP Professional Service Pack 3 (32-х разрядная)

3.5.2.Windows Vista Business Service Pack 2 (32-х разрядная)

3.5.3.Windows Vista Ultimate Service Pack 2 (32-х разрядная)

3.5.4.Windows 7 Professional (32-х и 64-х разрядная)

3.5.5.Windows 7 Ultimate (32-х и 64-х разрядная)

3.5.6.Windows Server 2003 Std Service Pack 2 (32-х разрядная)

3.5.7.Windows Server 2008 Std Service Pack 2 (32-х разрядная)

Для подключения терминалов можно использовать преобразователи «RS485 – RS232», «RS485 – USB», «RS485 – Ethernet».

При проектировании коммуникационных сетей необходимо учитывать скорость обработки запросов терминалами. Для эффективной работы сети желательно не подключать к одной линии более 5 терминалов.

Сервер терминалов РЗА работает только по протоколу MODBUS. Для правильной работы программы необходимо выставить одинаковую скорость обмена (зависит от характеристик линии связи) в настройках терминалов, подключенных к одной линии. Адреса терминалов в сети должны быть уникальными для предотвращения коллизий. Параметры формата посылок MODBUS рекомендуется выбрать следующими:

- Количество бит данных – 8
- Количество стоп битов – 1
- Бит четности – нет

Для терминалов с портом USB необходимо установить драйвер, который находится на диске вместе с ПО «СТАРТ-2ПС» в директории «FTDI». Для установки данного драйвера необходимо подключить терминал к компьютеру и в появившемся диалоге указать путь к драйверу.

3.2 Технические требования к локальной сети

- Все компьютеры системы должны быть объединены в локальную сеть с помощью оборудования, обеспечивающего скорость не ниже 100Mb/s.
- Локальная сеть должна поддерживать протоколы TCP/IP и UDP.
- В качестве сетевых IP - адресов могут быть использованы как динамические, так и статические адреса; все компьютеры системы должны иметь одинаковую маску подсети. ПРИМЕЧАНИЕ: В состав системы могут быть вручную включены компьютеры из другой подсети (имеющей другую маску подсети). Подробнее - см раздел административных настроек.
- Компьютеры системы могут быть **либо** членами рабочей группы, **либо** членами домена.
- Для дистанционного доступа к архивам системы "Старт-2ПС" со сторонних компьютеров, компьютер с установленным компонентом "Хранилище" должен быть виден в сети по протоколу HTTP (порт 80); инфраструктура сети (брандмауэр, мосты, Proxy-сервер и пр.) должны иметь соответствующую настройку. Удалённый компьютер должен быть оснащён Интернет-обозревателем с поддержкой Java (Microsoft IE, Opera, Mozilla Firefox, Google Chrome и пр.).

Дополнительные сведения для администраторов сети содержатся в разделе "Административные настройки" данного руководства.

3.2.1 Рекомендации по выбору параметров сети

В качестве IP - адресов следует использовать адреса из диапазонов, выделеных по соглашению для внутрикорпоративного применения:

- 10.0.0.0 ... 10.255.255.255

- 172.16.0.0...172.31.255.255
- 192.168.0.0 ...192.168.255.255

В случае использования статических сетевых адресов следует внимательно следить за уникальностью адреса на каждом компьютере; все адреса должны быть из одного диапазона и иметь одинаковую маску подсети, например:

- Компьютер 1 - адрес 192.168.0.1, маска подсети 255.255.255.0
- Компьютер 2 - адрес 192.168.0.2, маска подсети 255.255.255.0
- Компьютер 3 - адрес 192.168.0.3, маска подсети 255.255.255.0

и т.д.

ПРИМЕЧАНИЕ: В состав системы могут быть вручную включены компьютеры из другой подсети (имеющей другую маску подсети). Подробнее - см раздел административных настроек.

Порядок настройки имени рабочей группы и назначения сетевых адресов рассмотрены ниже.

4 Выполнение программы

4.1 Подготовка компьютера для установки системы

В данном разделе описывается процесс подготовки компьютера к развёртыванию системы "Старт-2ПС" в наиболее распространённой конфигурации сети с небольшим количеством компьютеров, а именно:

- Компьютеры системы являются членами рабочей группы.
- Сетевые адаптеры компьютеров используют статические IP - адреса.

Дополнительные сведения по иным вариантам развёртывания системы содержатся в разделе "Административные настройки" данного руководства.

Требование, чтобы все компьютеры системы входили в одну рабочую группу не является обязательным, однако за счёт включения всех компьютеров системы в одну рабочую группу можно несколько повысить быстродействие сети. Кроме того, упрощаются некоторые эксплуатационные процедуры, такие как учёт и пр.

В качестве имени рабочей группы можно использовать предлагаемое по умолчанию имя WORKGROUP или задать другое, более осмысленное имя.

4.1.1 Типы установки

Учитывая, что система "Старт-2ПС" может быть развёрнута как для реальной эксплуатации, так и в ознакомительных целях, процедура установки условно разбита на два типа:

- Основной (сетевой) тип установки.
- Локальный тип установки.

Основной (сетевой) тип установки предназначен для реальной эксплуатации. Этот тип установки обеспечивает работоспособность системы в полном объёме в составе из одного и более компьютеров, с защитой от несанкционированного доступа к функциям системы.

Локальный тип установки предназначен для ознакомительных целей. Этот тип установки является более простым, но обеспечивает работоспособность системы только в составе из одного компьютера и не в полной мере обеспечивает защиту от несанкционированного доступа к функциям системы.

В связи с этим разделы, описывающие подготовку компьютера для каждой из операционных систем разбиты на части, первая из которых содержит общие для обоих

типов установки подготовительные операции, а вторая содержит дополнительные операции, необходимые для основного (сетевого) типа установки.

Перед началом работы рекомендуется распечатать лист сводки параметров (находится в конце книги) и по мере настройки компьютера заполнить его графы.

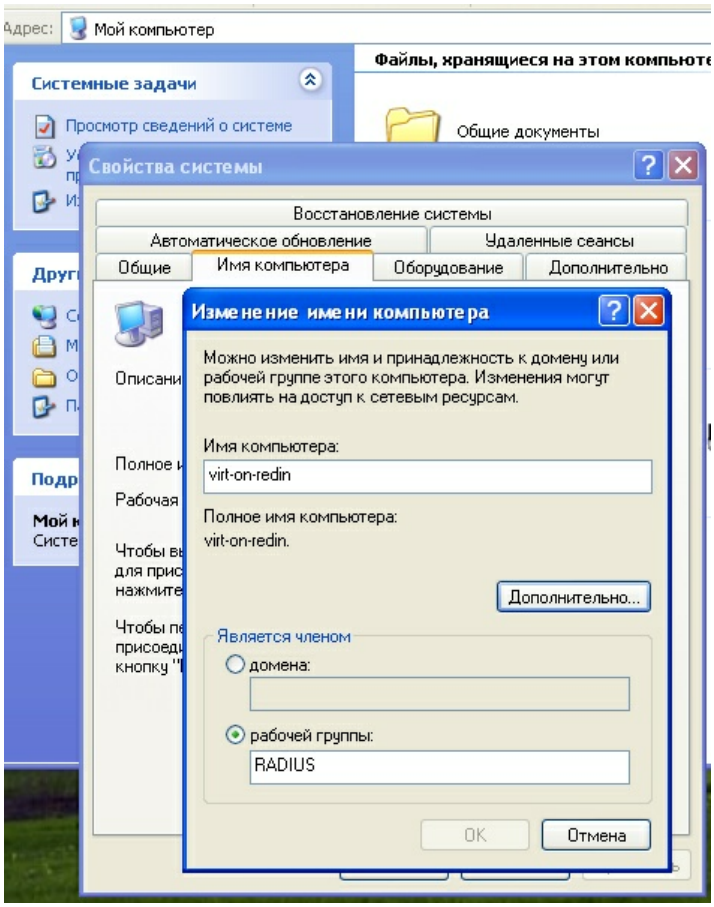
4.1.2 Операционная система Windows XP SP3

4.1.2.1 Основная и локальная установка

1. Установите Windows XP SP3.
2. Имя компьютера, имя рабочей группы и сетевой адрес обычно задаётся в процессе установки операционной системы, однако это можно сделать и сейчас следующим образом:

   2.1.Назначение имени компьютера и имени рабочей группы:

   2.1.1.Вызовите окно "Изменение имени компьютера" одним из способов, например "Пуск --> Мой компьютер --> Просмотр сведений о системе --> Вкладка "Имя компьютера" --> Кнопка "Изменить""

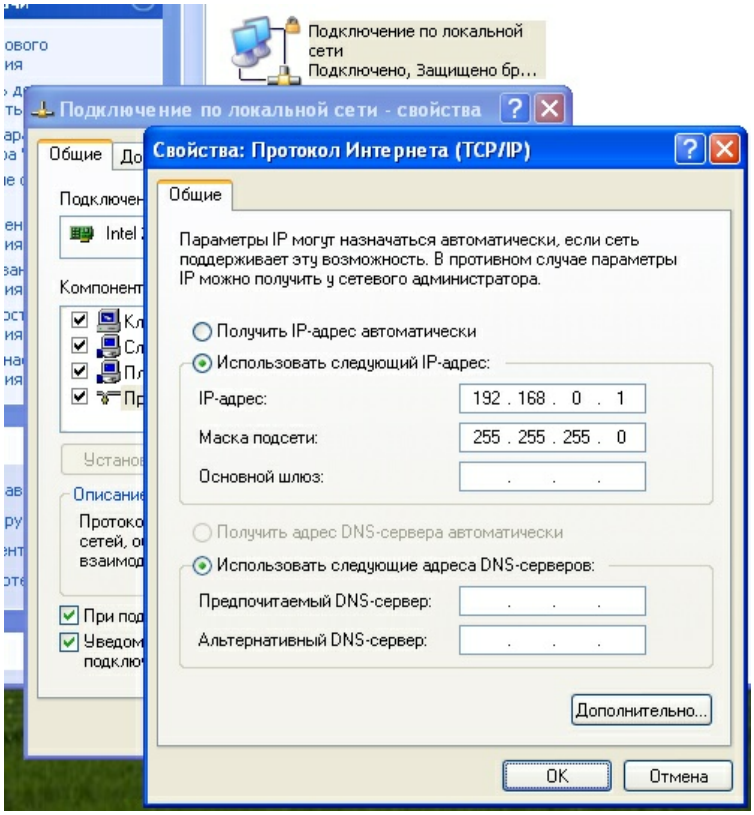


   2.1.2.В появившемся окне введите новое имя компьютера и имя рабочей группы
   Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

2.1.3.По окончании ввода (нажата кнопка "OK") система предложит перезагрузку. Перезагрузите операционную систему

2.2.Назначение сетевого адреса:

2.2.1.Вызовите окно "Свойства: Протокол Интернета (TCP/IP)" одним из способов, например "Панель управления --> Сетевые подключения --> выберите настраиваемое подключение (обычно "Подключение по локальной сети") --> Правая кнопка мыши --> меню Свойства --> элемент списка: Протокол Интернета (TCP/IP) --> Кнопка Свойства"



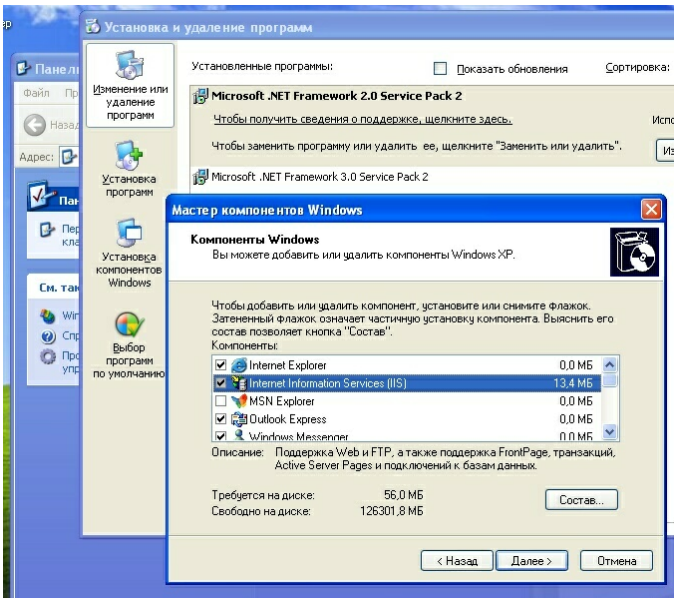
2.2.2.Введите сетевой адрес в соответствии с рекомендациями по выбору парметров сети (см. выше). Маска подсети после ввода корректного адреса, как правило, устанавливается автоматически. Остальные поля заполнять не обязательно.

Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

2.2.3.По окончании ввода система может предложить перезагрузиться

3. Если на этом компьютере планируется установка компонента «Хранилище», установите компонент ОС – Internet Information Services (IIS) («Панель управления --> Установка и удаление программ --> Установка компонентов Windows». (ПРИМЕЧАНИЕ: **Установку компонента IIS нужно выполнить до установки** компонента Microsoft .Net Framework 3.5, в противном случае не происходит

автоматической настройки IIS для работы ASP .NET страниц генератора отчётов хранилища)



4. Установите компонент Microsoft .Net Framework 3.5 (каталог «Компоненты для предустановки ОС\DotNet 3.5» инсталляционного диска) последовательно запустив

   4.1.dotnetfx35.exe

   4.2.NDP35SP1-KB958484-x86.exe

   4.3. dotnetfx35langpack_x86ru.exe

5. Установите последние обновления ОС (с сайта www.microsoft.com или с помощью оснастки "Центр обновления" панели управления).

6. Если на этом компьютере планируется установка компонента «Хранилище», установите продукт «SQL Server 2008 Express Edition» (каталог «Компоненты для предустановки ОС\SQL Server 2008 Express 32» инсталляционного диска), для чего необходимо:

   6.1.Установить WindowsXP-KB942288-v3-x86.exe (это необходимое обновление для успешной работы установщика Windows). По окончании установки может потребоваться перезагрузка компьютера

   6.2.Запустить SQLServerExpressSetup.bat и дождаться окончания всех действий по установке. Этот способ запуска процесса установки устраняет необходимость отвечать на многочисленные вопросы, задаваемые в процессе работы установщика

   6.3.По окончании установки открывается окно блокнота, индицирующего результат работы установщика, а также удаляются временные файлы

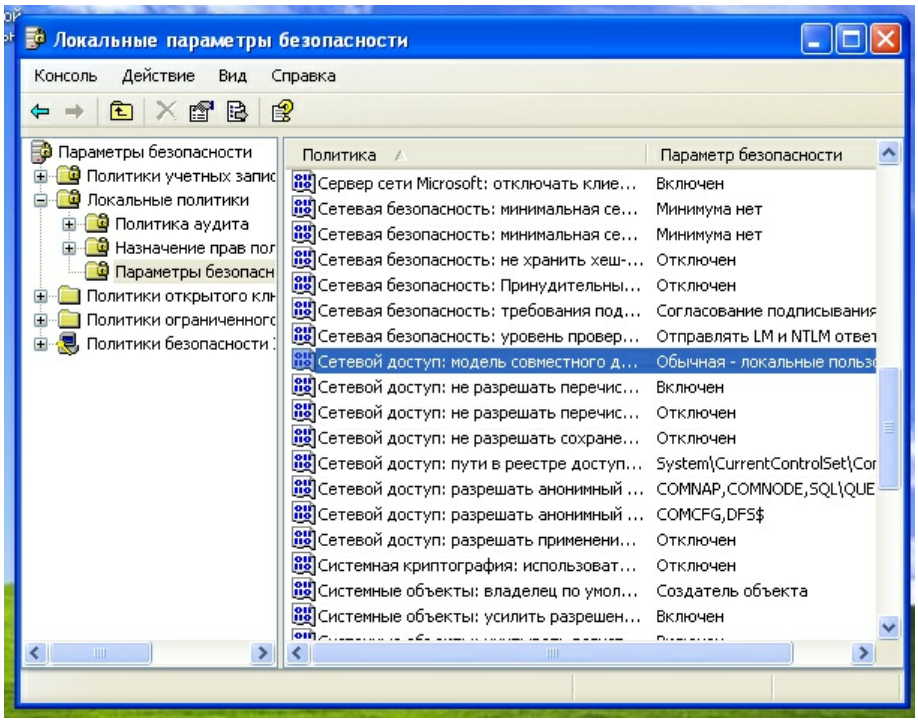
4.1.2.2 Основная установка

Продолжение подготовки. Далее описаны действия, которые необходимо выполнить только для основной (сетевой) установки системы

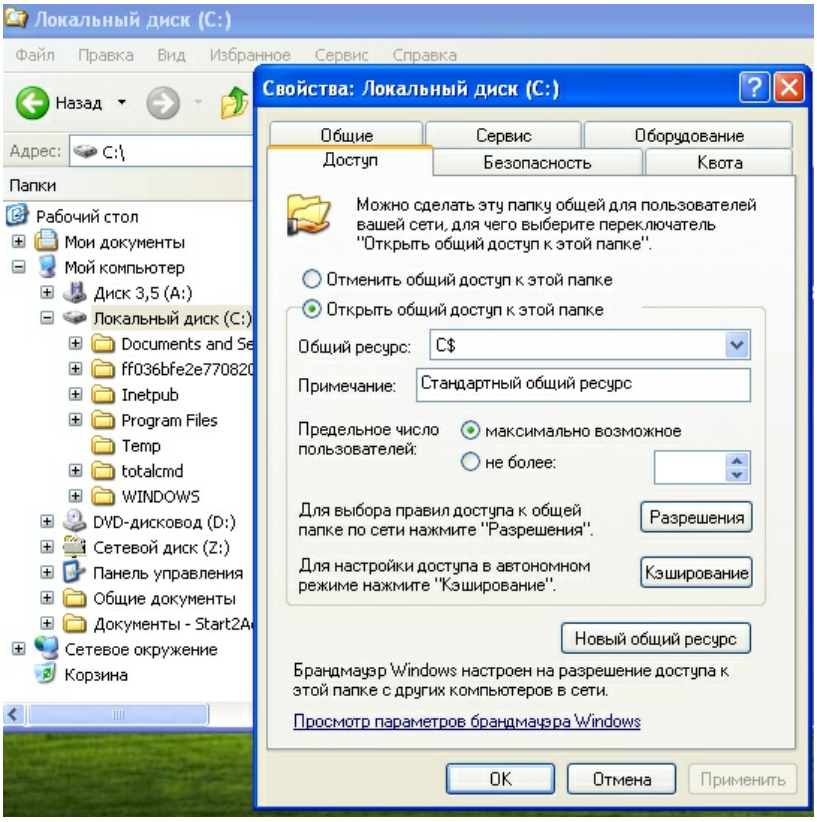
1. Настройте Локальную политику безопасности, для этого:

   1.1. Откройте "Панель управления --> Администрирование --> Локальная политика безопасности --> Локальные политики --> Параметры безопасности"

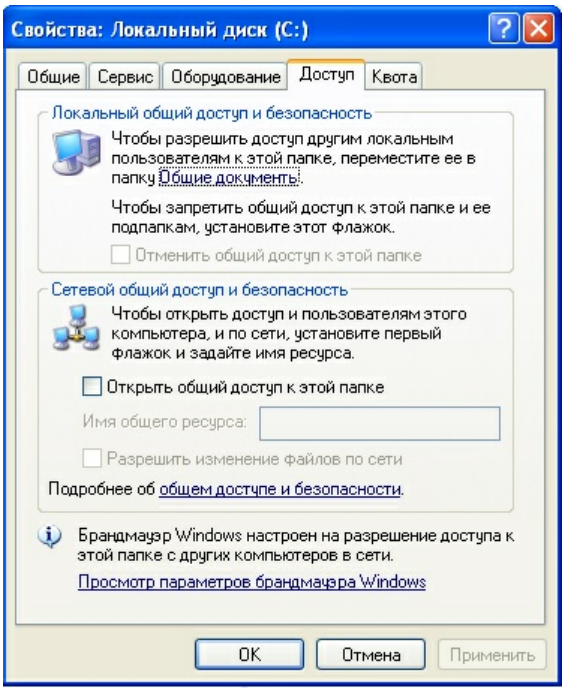
   1.2. Установите параметр "Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей" в значение "Обычная – локальные пользователи удостоверяются как они сами".



2. Для обеспечения видимости компьютера в локальной сети, включите общий доступ к файлам и принтерам. Для этого необходимо выбрать в Проводнике диск C: --> Свойства --> Доступ: Включить общий доступ к файлам и принтерам (просто включить, без использования мастера). В итоге окно свойств примет один из двух видов:



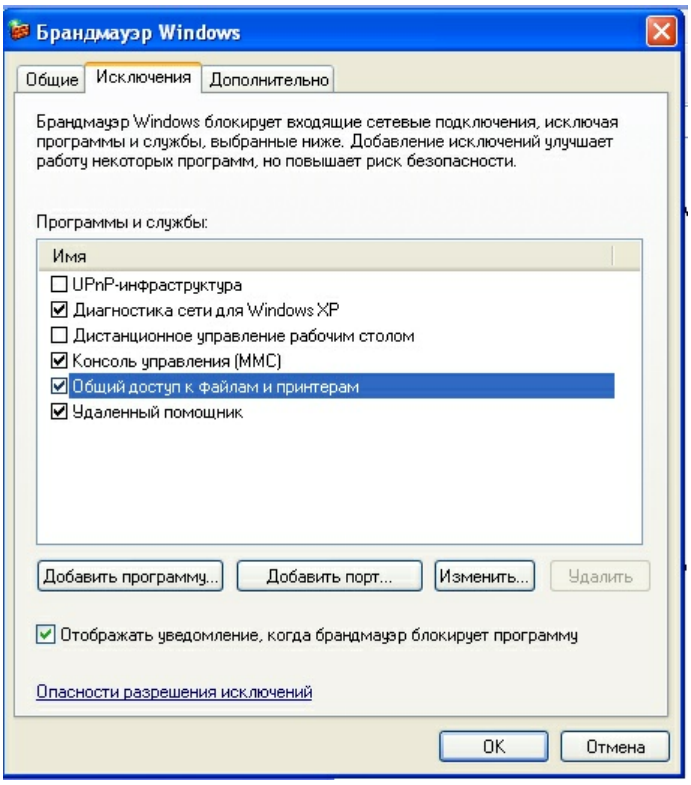
или



Вид окна зависит от режима использования общего доступа к файлам и принтерам (нижний вид окна отображается в режиме "Простой общий доступ к файлам и принтерам"). Сам режим для системы Старт-2ПС значения не имеет и его можно не менять. Открывать сетевой доступ к дискам и каталогам компьютера также не требуется.

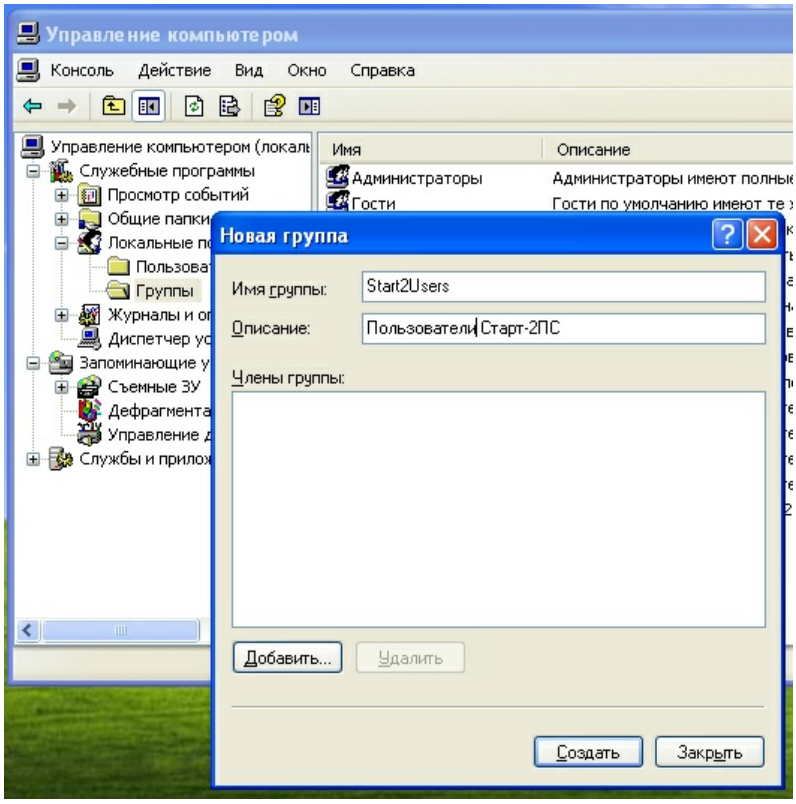
3. Убедитесь в том, что в брандмауэре Windows разрешено исключение «Общий доступ к файлам и принтерам». Для этого зайдите в «Панель управления», выберите

«Брандмауэр Windows», перейдите на вкладку "Исключения", проверьте флажок «Общий доступ к файлам и принтерам»

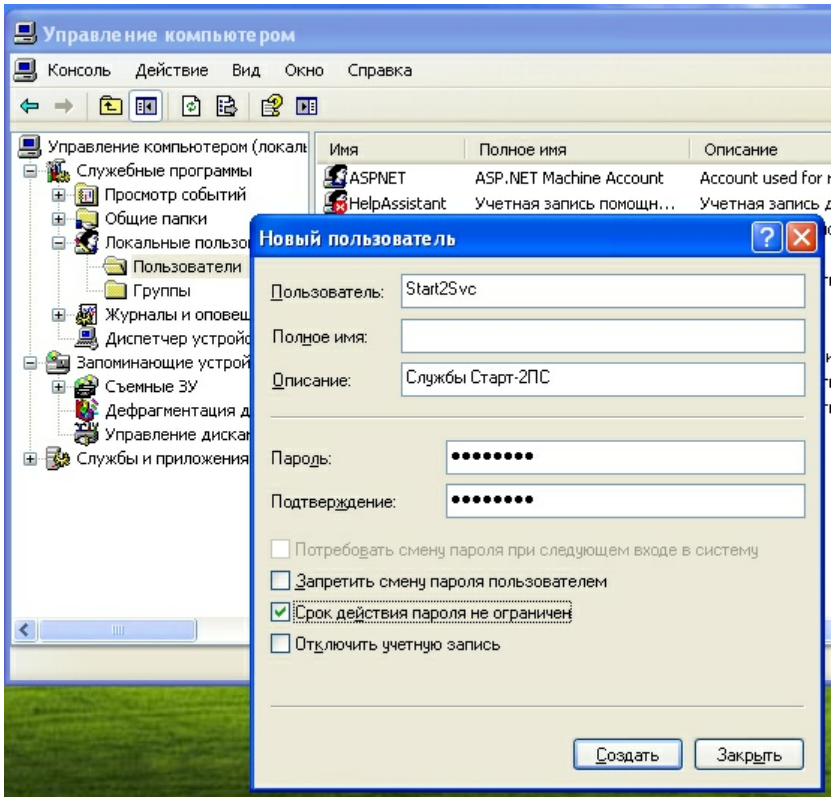


4. Настройте список пользователей Windows. Если компьютеры локальной сети объединены в рабочую группу, на каждом компьютере системы должен быть создан одинаковый набор учётных записей системы безопасности операционной системы:

4.1.Создайте группу безопасности, члены которой впоследствии получат доступ к функциям системы "Старт-2ПС", рекомендуемое имя - «Start2Users». Для этого запустите диалог управления компьютером "Панель управления --> Администрирование --> Управление компьютером". Выберете в дереве "Служебные программы --> Локальные пользователи и группы --> Группы". Создайте группу (вызов диалога - правой кнопкой мыши)



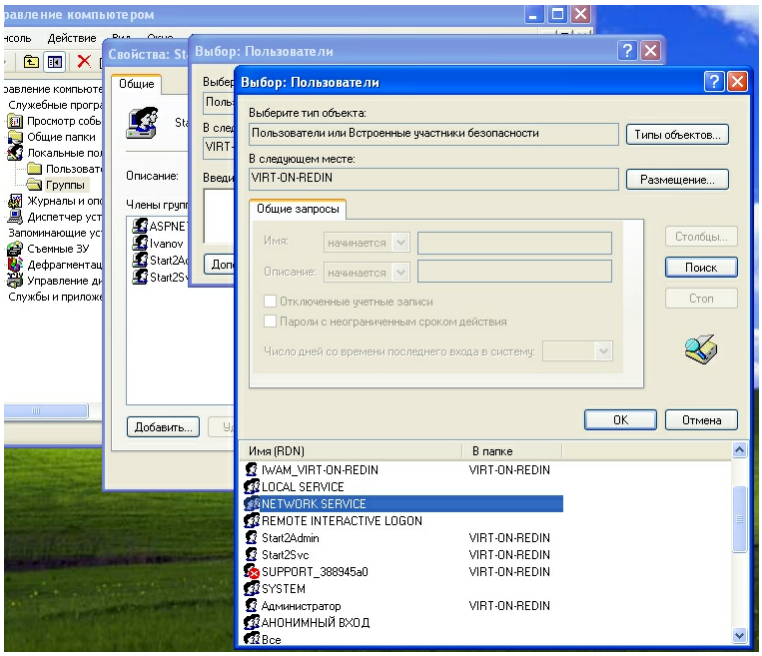
4.2.Создайте учётную запись **с непустым паролем** для служб системы "Старт-2 ПС", рекомендуемое имя - «Start2Svc». Для этого в ветви "Пользователи" щелчком правой кнопки мыши вызовите диалог



4.3.Последовательно заполняя форму и нажимая кнопку "Создать", создайте учётные записи **с непустыми паролями** для администратора системы (рекомендуемое имя «Start2Admin») и для всех операторов системы «Старт-2

ПС» (например, «Ivanov», «Petrov» и пр).

4.4.Включите в группу «Start2Users» только что созданные учетные записи, а также встроенные учётные записи Windows ASPNET и NETWORK SERVICE



4.5.Дополнительно включите учётные записи "Start2Svc", "Start2Admin" в группу "Администраторы". Их членство в группе "Пользователи" можно исключить.

4.6.Проверьте, что учётные записи операторов включены в группу "Пользователи" и "Start2Users" и не включены в группу "Администраторы". Излишние полномочия у операторов системы могут отрицательно сказаться на безопасности и устойчивости работы системы.

5. Запомните имена учётных записей и пароли к ним. Эти имена и пароли должны быть сохранены в безопасном месте.
Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

6. Настройте параметры безопасности в механизме COM/DCOM. Для этого необходимо:

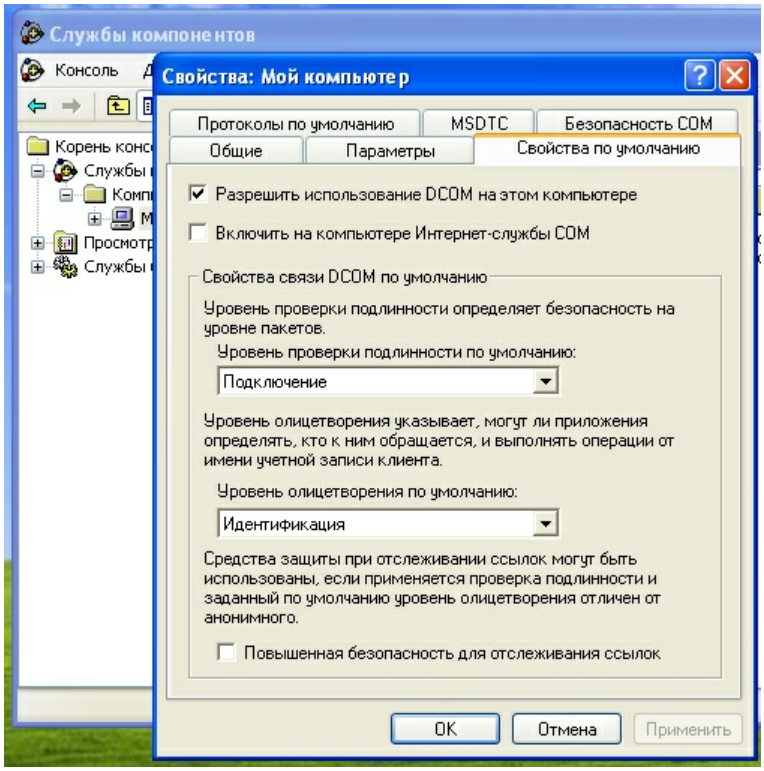
6.1.Запустить оснастку «Службы компонентов» в папке «Администрирование» панели управления.

6.2.Убедиться, что параметры вкладки «Свойства по умолчанию» (Службы компонентов --> Компьютеры --> Мой компьютер --> Свойства) имеют следующие значения:

6.2.1.Разрешить исп. DCOM на этом компьютере: вкл

6.2.2.Уровень проверки подлинности по умолчанию: Подключение

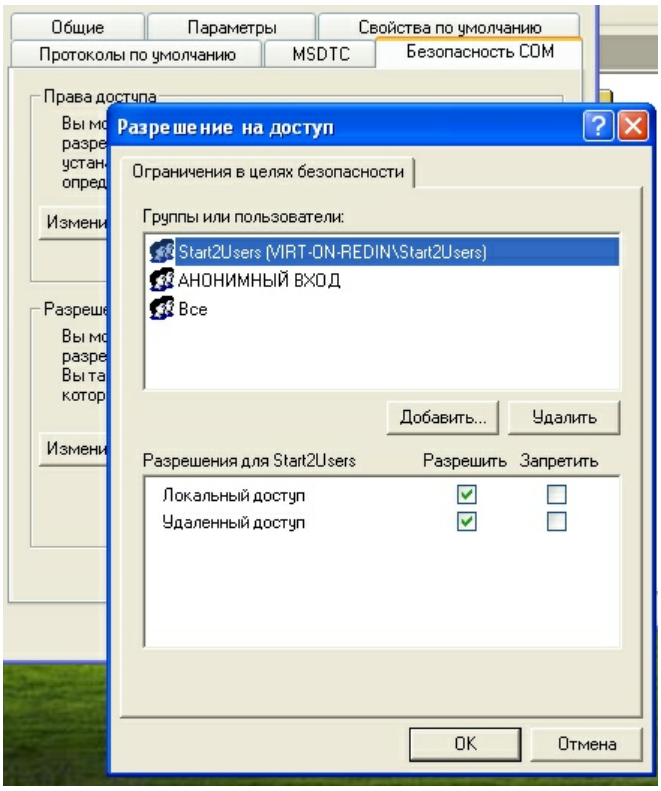
6.2.3.Уровень олицетворения по умолчанию: Идентификация



6.3.На вкладке «Безопасность COM»

6.3.1.Права доступа --> Кнопка «Изменить ограничения»

6.3.1.1.Добавить группу «Start2Users»



6.3.1.2.Разрешить ей

6.3.1.2.1.«Локальный доступ»

6.3.1.2.2.«Удалённый доступ»

6.3.1.3.Убедиться в том, что «АНОНИМНЫЙ ВХОД» имеет разрешение «Локальный доступ»

6.3.1.4.Убедиться в том, что группа «Все» имеет разрешения

6.3.1.4.1.«Локальный доступ»

6.3.1.4.2.«Удалённый доступ»

6.3.2.Права доступа --> Кнопка «Изменить настройки по умолчанию»

6.3.2.1.Добавить группу «Start2Users»

6.3.2.2.Разрешить ей

6.3.2.2.1.«Локальный доступ»

6.3.2.2.2.«Удалённый доступ»

6.3.2.3.Убедиться в том, что «SELF» имеет разрешения

6.3.2.3.1.«Локальный доступ»

6.3.2.3.2.«Удалённый доступ»

6.3.2.4.Убедиться в том, что «SYSTEM» имеет разрешение

6.3.2.4.1.«Локальный доступ»

6.3.3.Разрешение на запуск и активацию --> Кнопка «Изменить ограничения»

6.3.3.1.Добавить группу «Start2Users»

6.3.3.2.Разрешить ей

6.3.3.2.1.«Локальный запуск»

6.3.3.2.2.«Удалённый запуск»

6.3.3.2.3.«Локальная активация»

6.3.3.2.4.«Удалённая активация»

6.3.3.3.Убедиться в том, что группа «Администраторы» имеет разрешения

6.3.3.3.1.«Локальный запуск»

6.3.3.3.2.«Удалённый запуск»

6.3.3.3.3.«Локальная активация»

6.3.3.3.4.«Удалённая активация»

6.3.3.4.Убедиться в том, что группа «Все» имеет разрешения

6.3.3.4.1.«Локальный запуск»

6.3.3.4.2. «Локальная активация»

6.3.4.Разрешение на запуск и активацию --> Кнопка «Изменить настройки по умолчанию»

6.3.4.1.Добавить группу «Start2Users»

6.3.4.2.Разрешить ей

6.3.4.2.1.«Локальный запуск»

6.3.4.2.2.«Удалённый запуск»

6.3.4.2.3.«Локальная активация»

6.3.4.2.4.«Удалённая активация»

6.3.4.3.Убедиться в том, что «SYSTEM» имеет разрешения

6.3.4.3.1.«Локальный запуск»

6.3.4.3.2. «Локальная активация»

6.3.4.4.Убедиться в том, что группа «Администраторы» имеет разрешения

6.3.4.4.1.«Локальный запуск»

6.3.4.4.2.«Удалённый запуск»

6.3.4.4.3.«Локальная активация»

6.3.4.4.4.«Удалённая активация»

6.3.4.5.Убедиться в том, что группа «ИНТЕРАКТИВНЫЕ» имеет разрешения

6.3.4.5.1.«Локальный запуск»

6.3.4.5.2. «Локальная активация»

7. Перезагрузите компьютер.
8. Войдите как администратор

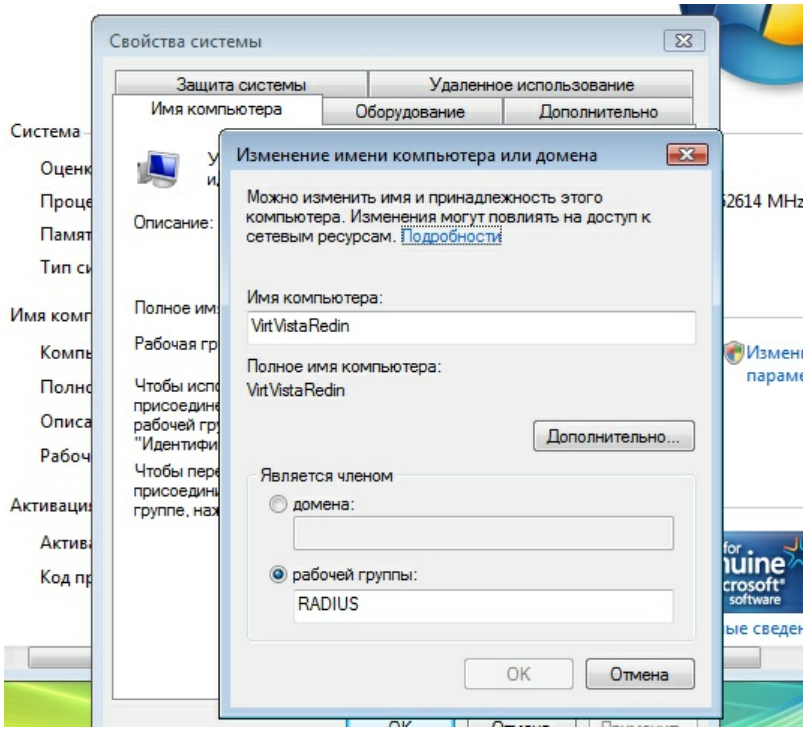
4.1.3 Операционная система Windows Vista Business / Ultimate SP2

4.1.3.1 Основная и локальная установка

1. Установите Windows Vista Business (или Ultimate) SP2
2. Имя компьютера, имя рабочей группы и сетевой адрес обычно задаётся в процессе установки операционной системы, однако это можно сделать и сейчас следующим образом:

2.1.Назначение имени компьютера и имени рабочей группы:

2.1.1.Вызовите окно "Изменение имени компьютера или домена" одним из способов, например "Панель управления --> Система --> раздел "Имя компьютера, имя домена и параметры рабочей группы" --> Изменить параметры --> Вкладка "Имя компьютера" --> Кнопка "Изменить""

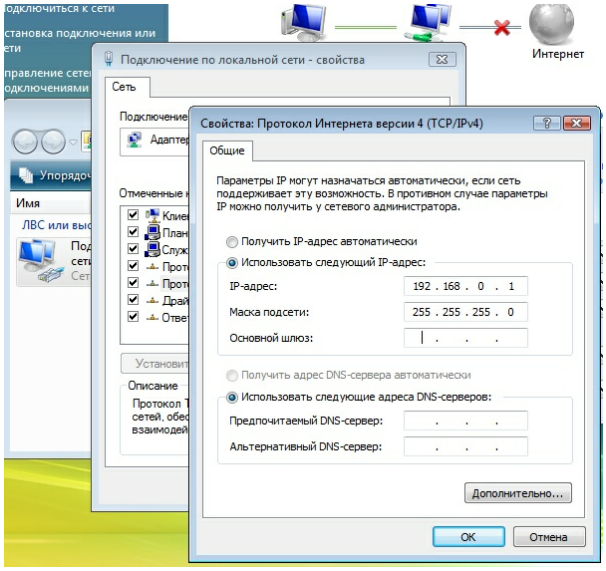


2.1.2.В появившемся окне введите новое имя компьютера и имя рабочей группы Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

2.1.3.По окончании ввода (нажата кнопка "OK") система предложит перезагрузку. Перезагрузите операционную систему

2.2.Назначение сетевого адреса:

2.2.1.Вызовите окно "Свойства: Протокол Интернета версии 4 (TCP/IPv4)" одним из способов, например "Панель управления --> Центр управления сетями и общим доступом --> Управление сетевыми подключениями --> выберите настраиваемое подключение (обычно "Подключение по локальной сети") --> Правая кнопка мыши --> меню Свойства --> элемент списка: Протокол Интернета версии 4 (TCP/IPv4) --> Кнопка Свойства"



2.2.2.Введите сетевой адрес в соответствии с рекомендациями по выбору парметров сети (см. выше). Маска подсети после ввода корректного адреса, как правило, устанавливается автоматически. Остальные поля заполнять не обязательно.

Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

2.2.3.По окончании ввода система может предложить перезагрузиться

3. Если на этом компьютере планируется установка компонента «Хранилище», установите компонент ОС – Internet Information Services (IIS) («Панель управления --> Программы и компоненты --> Включение и отключение компонентов Windows», для чего необходимо включить флажок "Службы IIS". Проконтролируйте и, при необходимости, включите следующие составляющие компонента IIS:

3.1.Службы IIS --> Службы интернета --> Безопасность

3.1.1.Фильтрация запросов

3.2.Службы IIS --> Службы интернета --> Компоненты разработки приложений:

3.2.1.ASP .NET

3.2.2.Расширения ISAPI

3.2.3.Расширяемость .NET

3.2.4.Фильтры ISAPI

3.3.Службы IIS --> Службы интернета --> Основные функции Http

3.3.1.Документ по умолчанию

3.3.2.Ошибки HTTP

3.3.3.Просмотр каталога

3.3.4.Статическое содержимое

3.4.Службы IIS --> Службы интернета --> Проверка работоспособности и диагностика

3.4.1.Ведение журнала HTTP

3.4.2.Монитор запросов

3.5.Службы IIS --> Службы интернета --> Функции повышения быстродействия

3.5.1.Сжатие статического содержимого

3.6.Службы IIS --> Средства управления веб-узлом

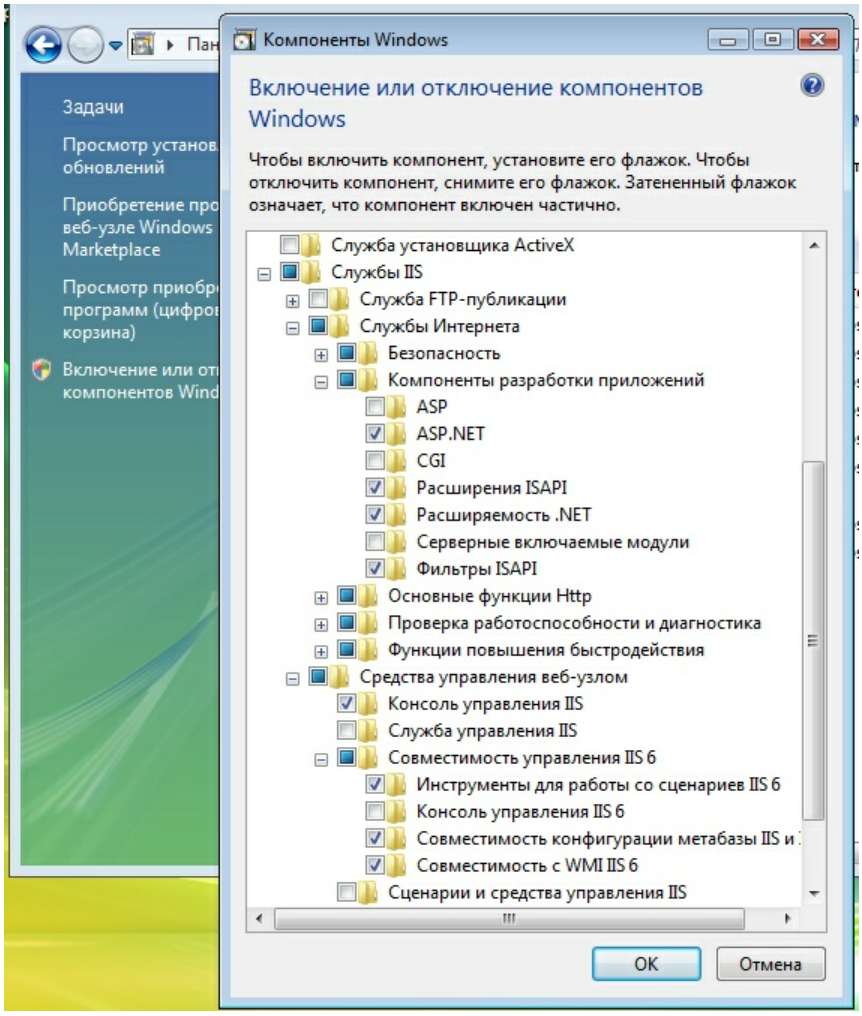
3.6.1.Консоль управления IIS

3.7.Службы IIS --> Средства управления веб-узлом --> Совместимость управления IIS 6

3.7.1.Инструменты для работы со сценариев IIS 6

3.7.2.Совместимость конфигурации метабазы IIS и IIS 6

3.7.3.Совместимость с WMI IIS 6



4. Установите последние обновления ОС (с сайта www.microsoft.com или с помощью оснастки "Центр обновления" панели управления). Обычно при установке обновлений автоматически устанавливается компонент Microsoft .Net Framework 3.5. Если установка обновлений невозможна, необходимо установить Microsoft .Net Framework 3.5 вручную, для этого:

   4.1.Откройте каталог «Компоненты для предустановки ОС\DotNet 3.5» инсталляционного диска и последовательно запустите

   4.1.1.dotnetfx35.exe

   4.1.2.NDP35SP1-KB958484-x86.exe

   4.1.3. dotnetfx35langpack_x86ru.exe

5. Если на этом компьютере планируется установка компонента «Хранилище», установите продукт «SQL Server 2008 Express Edition» (каталог «Компоненты для предустановки ОС\SQL Server 2008 Express 32» инсталляционного диска), для чего необходимо:

   5.1.Запустить SQLServerExpressSetup.bat и дождаться окончания всех действий по установке. Этот способ запуска процесса установки устраняет необходимость отвечать на многочисленные вопросы, задаваемые в процессе работы установщика

   5.2.По окончании установки открывается окно блокнота, индицирующего результат работы установщика, а также удаляются временные файлы

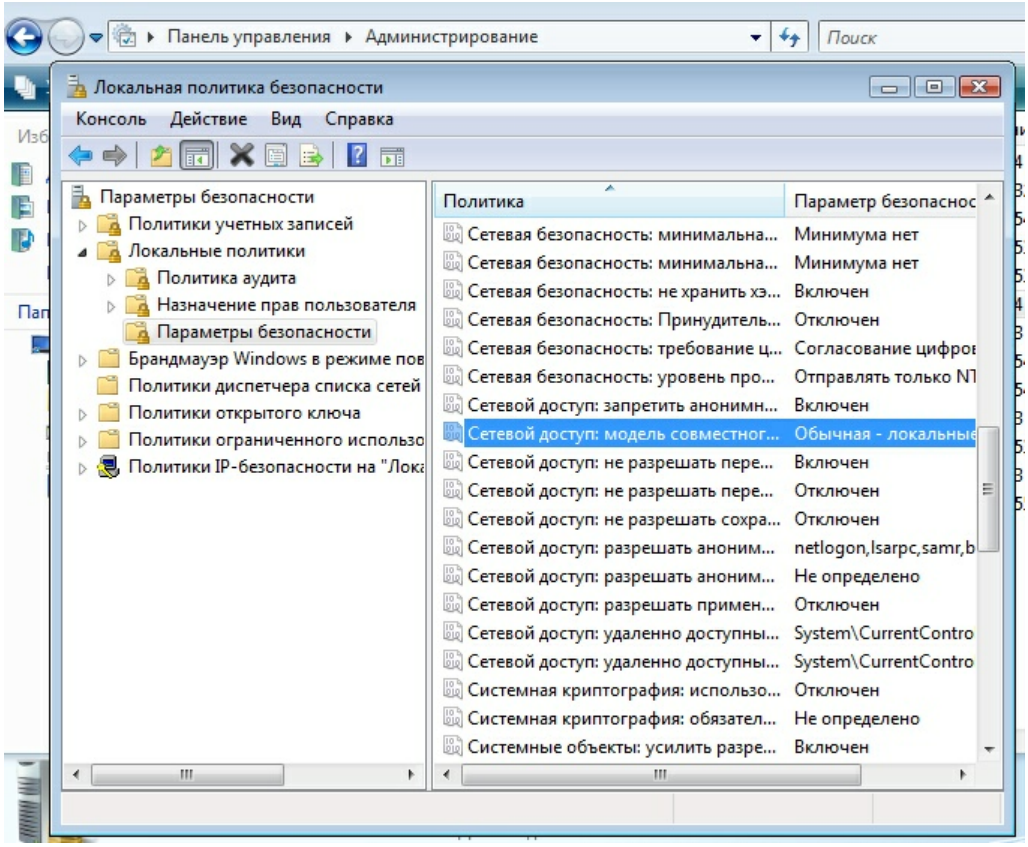
4.1.3.2 Основная установка

Продолжение подготовки. Далее описаны действия, которые необходимо выполнить только для основной (сетевой) установки системы.

1. Проверьте правильность настройки Локальной политики безопасности, для этого:

   1.1.Откройте "Панель управления --> Администрирование --> Локальная политика безопасности --> Локальные политики --> Параметры безопасности"

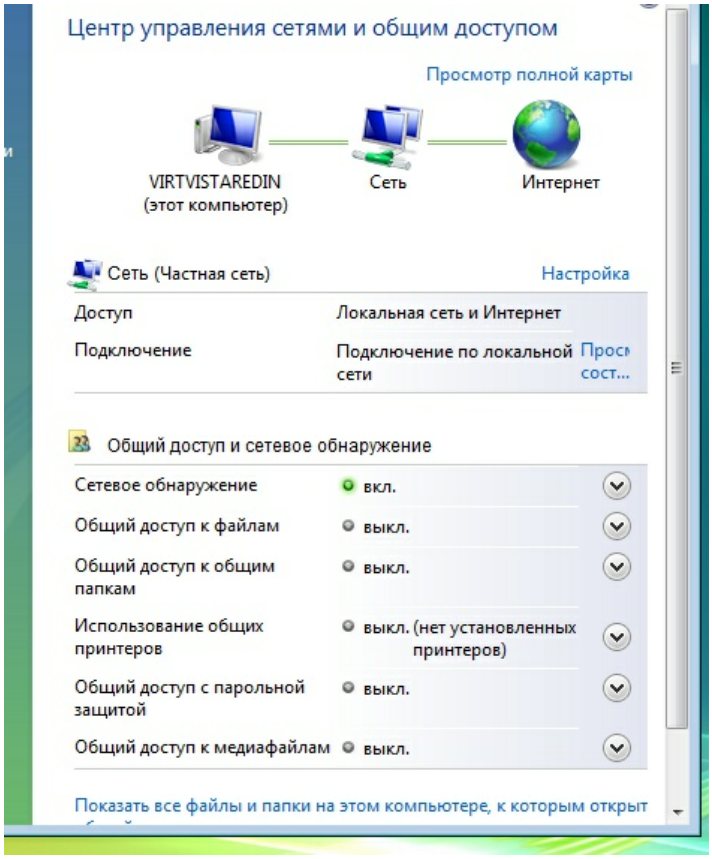
   1.2.Параметр "Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей" должен иметь значение "Обычная – локальные пользователи удостоверяются как они сами".



2. Проверьте правильность настройки сетевого обнаружения. Для этого:

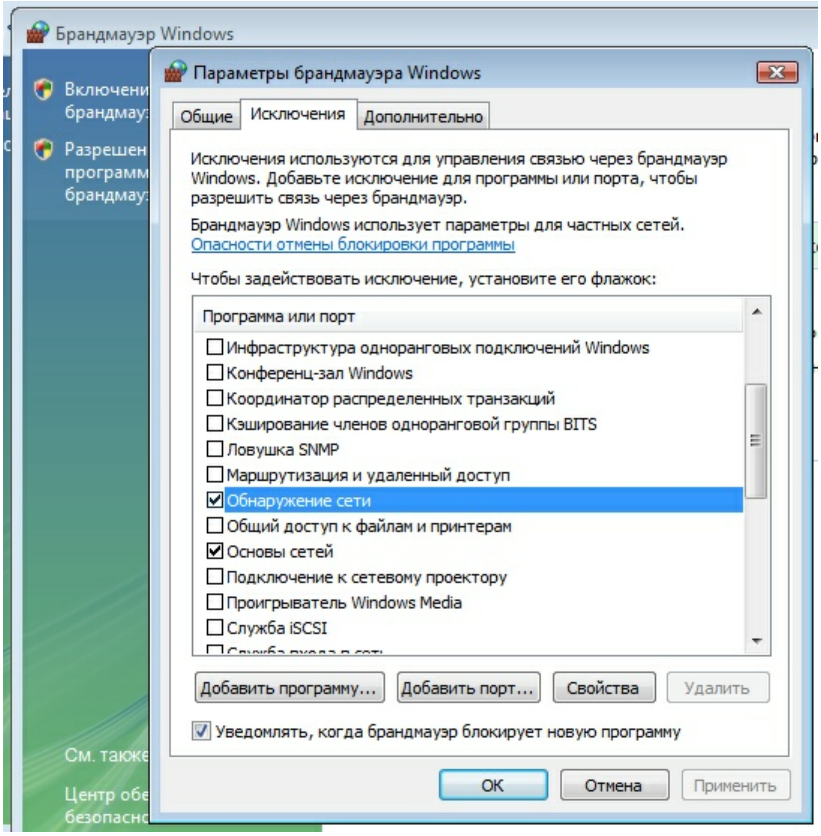
2.1.Запустите "Панель управления --> Центр управления сетями и общим доступом"

2.2.Проверьте что параметр "Сетевое обнаружение" включен



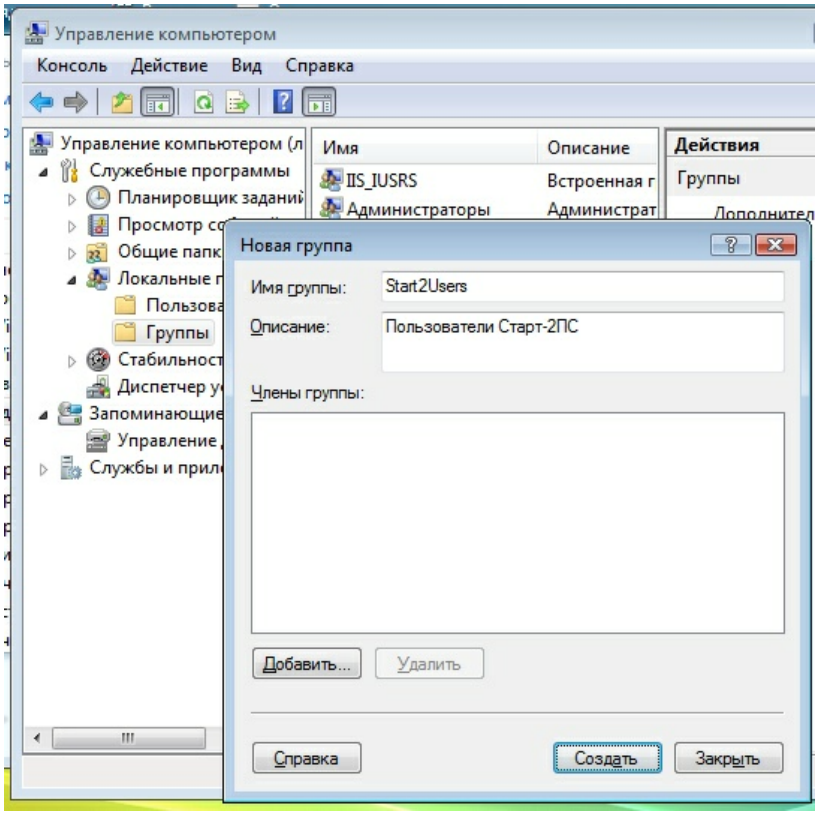
3. Убедитесь в том, что в брандмауэре Windows разрешены исключения "Обнаружение сети" и "Основы сетей". Для этого:

3.1.Запустите "Панель управления --> Брандмауэр Windows --> Разрешение запуска программ через брандмауэр Windows" и проверьте состояние флажков "Обнаружение сети" и "Основы сетей"

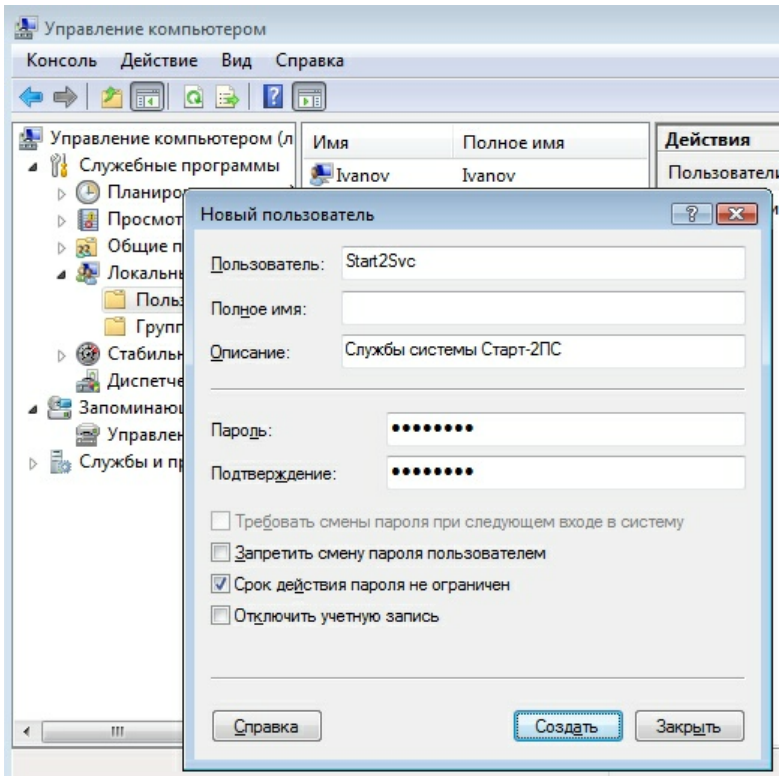


4. Настройте список пользователей Windows. Если компьютеры локальной сети объединены в рабочую группу, на каждом компьютере системы должен быть создан одинаковый набор учётных записей системы безопасности операционной системы:

4.1.Создайте группу безопасности, члены которой впоследствии получат доступ к функциям системы "Старт-2ПС", рекомендуемое имя - «Start2Users». Для этого запустите диалог управления компьютером "Панель управления --> Администрирование --> Управление компьютером". Выберете в дереве "Служебные программы --> Локальные пользователи и группы --> Группы". Создайте группу (вызов диалога - правой кнопкой мыши)



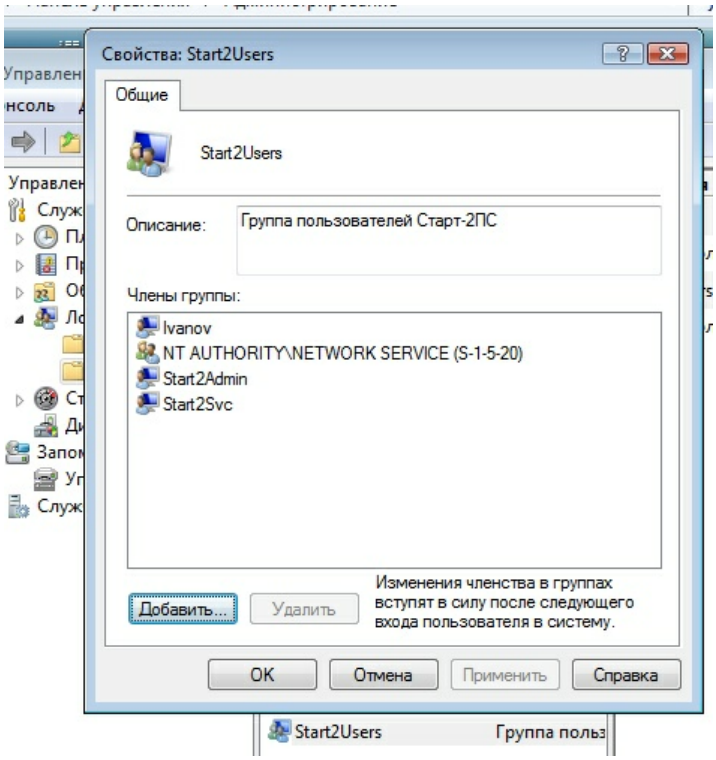
4.2.Создайте учётную запись **с непустым паролем** для служб системы "Старт-2 ПС", рекомендуемое имя - «Start2Svc». Для этого в ветви "Пользователи" щелчком правой кнопки мыши вызовите диалог



4.3.Последовательно заполняя форму и нажимая кнопку "Создать", создайте учётные записи **с непустыми паролями** для администратора системы (рекомендуемое имя «Start2Admin») и для всех операторов системы «Старт-2

ПС» (например, «Ivanov», «Petrov» и пр).

4.4.Включите в группу «Start2Users» только что созданные учетные записи, а также встроенную учётную запись Windows NETWORK SERVICE



4.5.Дополнительно включите учётные записи «Start2Svc», «Start2Admin» в группу «Администраторы». Их членство в группе "Пользователи" можно исключить.

4.6.Проверьте, что учётные записи операторов включены в группу «Пользователи» и "Start2Users" и не включены в группу "Администраторы". Излишние полномочия у операторов системы могут отрицательно сказаться на безопасности и устойчивости работы системы.

5. Запомните имена учётных записей и пароли к ним. Эти имена и пароли должны быть сохранены в безопасном месте.
Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

6. Настройте параметры безопасности в механизме COM/DCOM. Для этого необходимо:

6.1.Запустить оснастку «Службы компонентов», вызвав её с помощью командной строки:

6.2."Пуск --> Все программы --> Стандартные --> Командная строка"

6.3.В появившемся окне ввести dcomcnfg и нажать Enter на клавиатуре

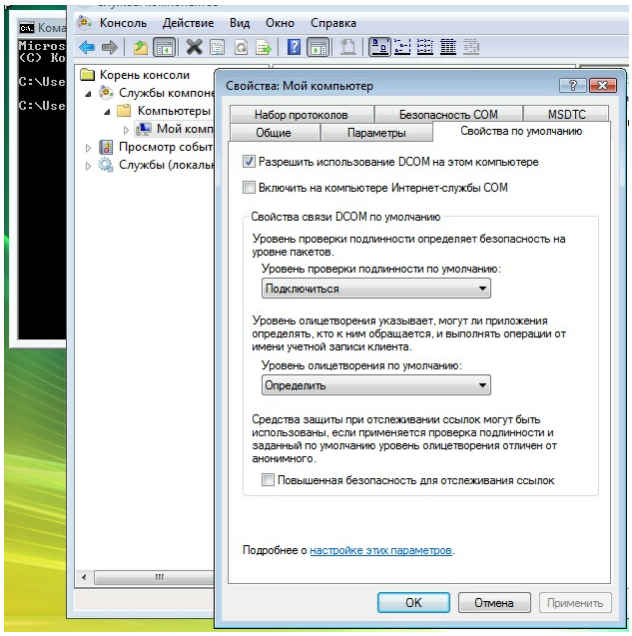
6.4.Убедиться, что параметры вкладки «Свойства по умолчанию» (Службы

компонентов --> Компьютеры --> Мой компьютер --> Свойства) имеют следующие значения:

6.4.1.Разрешить исп. DCOM на этом компьютере: вкл

6.4.2.Уровень проверки подлинности по умолчанию: Подключиться

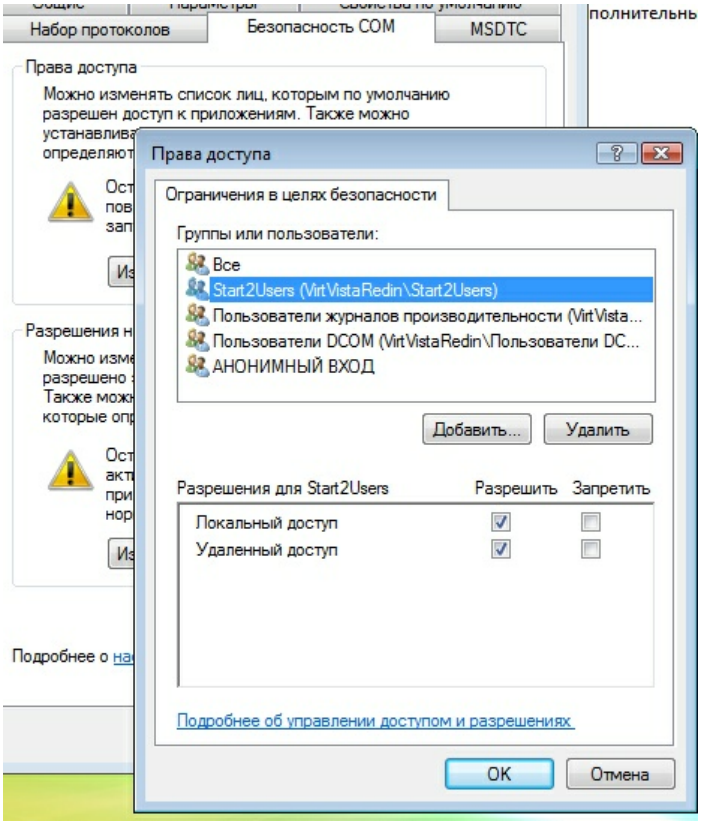
6.4.3.Уровень олицетворения по умолчанию: Определить



6.5.На вкладке «Безопасность COM»

6.5.1.Права доступа --> Кнопка «Изменить ограничения»

6.5.1.1.Добавить группу «Start2Users»



6.5.1.2.Разрешить ей

6.5.1.2.1.«Локальный доступ»

6.5.1.2.2.«Удалённый доступ»

6.5.1.3.Убедиться в том, что «АНОНИМНЫЙ ВХОД» имеет разрешение «Локальный доступ»

6.5.1.4.Убедиться в том, что группа «Все» имеет разрешения

6.5.1.4.1.«Локальный доступ»

6.5.1.4.2.«Удалённый доступ»

6.5.2.Права доступа --> Кнопка «Изменить умолчания»

6.5.2.1.Добавить группу «Start2Users»

6.5.2.2.Разрешить ей

6.5.2.2.1.«Локальный доступ»

6.5.2.2.2.«Удалённый доступ»

6.5.2.3.Убедиться в том, что «SELF» имеет разрешения

6.5.2.3.1.«Локальный доступ»

6.5.2.3.2.«Удалённый доступ»

6.5.2.4.Убедиться в том, что «SYSTEM» имеет разрешение

6.5.2.4.1.«Локальный доступ»

6.5.3.Разрешение на запуск и активацию --> Кнопка «Изменить ограничения»

6.5.3.1.Добавить группу «Start2Users»

6.5.3.2.Разрешить ей

6.5.3.2.1.«Локальный запуск»

6.5.3.2.2.«Удалённый запуск»

6.5.3.2.3.«Локальная активация»

6.5.3.2.4.«Удалённая активация»

6.5.3.3.Убедиться в том, что группа «Администраторы» имеет разрешения

6.5.3.3.1.«Локальный запуск»

6.5.3.3.2.«Удалённый запуск»

6.5.3.3.3.«Локальная активация»

6.5.3.3.4.«Удалённая активация»

6.5.3.4.Убедиться в том, что группа «Все» имеет разрешения

6.5.3.4.1.«Локальный запуск»

6.5.3.4.2. «Локальная активация»

6.5.4.Разрешение на запуск и активацию --> Кнопка «Изменить умолчания»

6.5.4.1.Добавить группу «Start2Users»

6.5.4.2.Разрешить ей

6.5.4.2.1.«Локальный запуск»

6.5.4.2.2.«Удалённый запуск»

6.5.4.2.3.«Локальная активация»

6.5.4.2.4.«Удалённая активация»

6.5.4.3.Убедиться в том, что «SYSTEM» имеет разрешения

6.5.4.3.1.«Локальный запуск»

6.5.4.3.2. «Локальная активация»

6.5.4.4.Убедиться в том, что группа «Администраторы» имеет разрешения

6.5.4.4.1.«Локальный запуск»

6.5.4.4.2.«Удалённый запуск»

6.5.4.4.3.«Локальная активация»

6.5.4.4.4.«Удалённая активация»

6.5.4.5.Убедиться в том, что группа «ИНТЕРАКТИВНЫЕ» имеет разрешения

6.5.4.5.1.«Локальный запуск»

6.5.4.5.2. «Локальная активация»

7. Перезагрузите компьютер.
8. Войдите как администратор.

4.1.4 Операционная система Windows 7 Professional/Ultimate

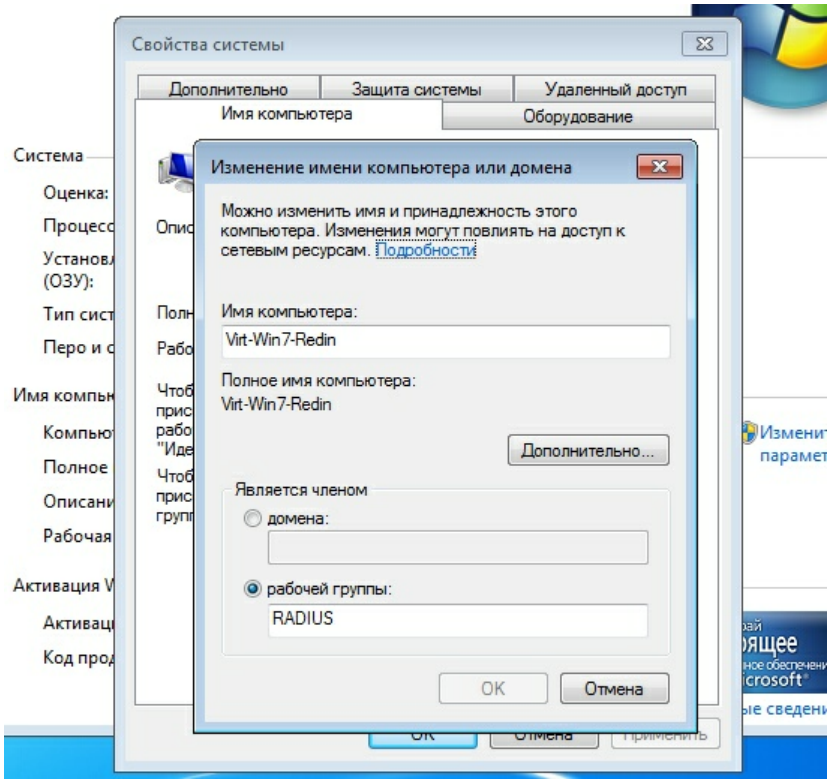
4.1.4.1 Основная и локальная установка

1. Установите Windows 7 Professional или Ultimate
2. Имя компьютера, имя рабочей группы и сетевой адрес обычно задаётся в процессе установки операционной системы, однако это можно сделать и позже следующим

образом:

2.1.Назначение имени компьютера и имени рабочей группы:

2.1.1.Вызовите окно "Изменение имени компьютера или домена" одним из способов, например "Панель управления --> Система --> раздел "Имя компьютера, имя домена и параметры рабочей группы" --> Изменить параметры --> Вкладка "Имя компьютера" --> Кнопка "Изменить""

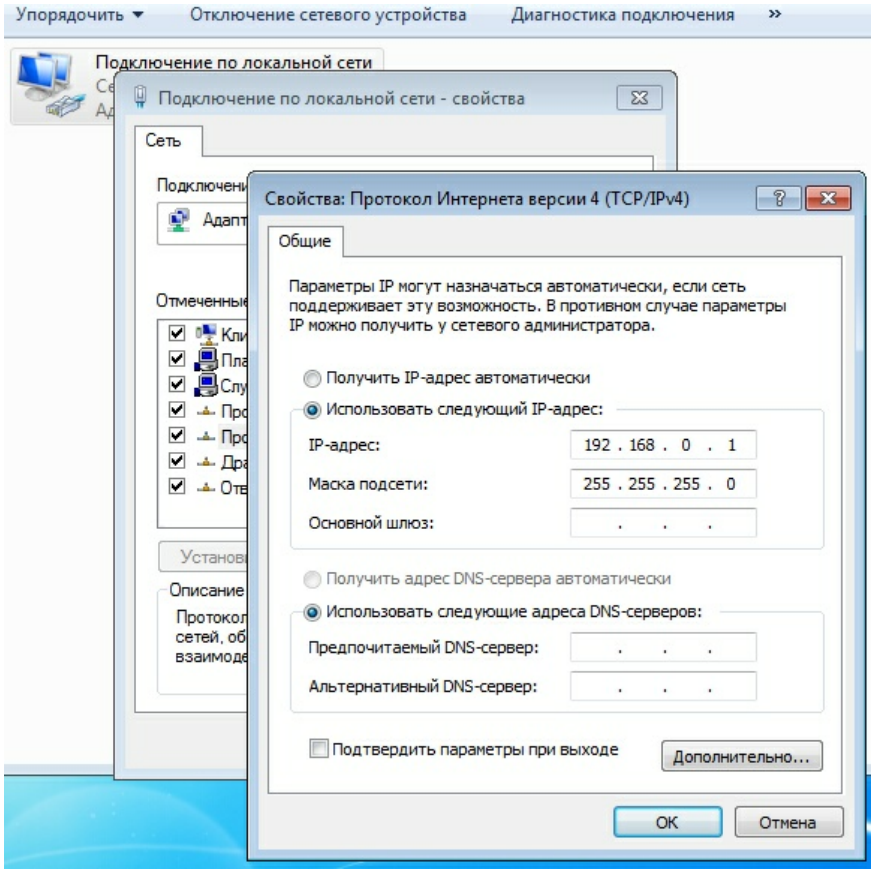


2.1.2.В появившемся окне введите новое имя компьютера и имя рабочей группы Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

2.1.3.По окончании ввода (нажата кнопка "OK") система предложит перезагрузку. Перезагрузите операционную систему

2.2.Назначение сетевого адреса:

2.2.1.Вызовите окно "Свойства: Протокол Интернета версии 4 (TCP/IPv4)" одним из способов, например "Панель управления --> Центр управления сетями и общим доступом --> Изменение параметров адаптера --> выберите настраиваемое подключение (обычно "Подключение по локальной сети") --> Правая кнопка мыши --> меню Свойства --> элемент списка: Протокол Интернета версии 4 (TCP/IPv4) --> Кнопка Свойства"



2.2.2.Введите сетевой адрес в соответствии с рекомендациями по выбору парметров сети (см. выше). Маска подсети после ввода корректного адреса, как правило, устанавливается автоматически. Остальные поля заполнять не обязательно.

Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

2.2.3.По окончании ввода система может предложить перезагрузиться

3. Если на этом компьютере планируется установка компонента «Хранилище», установите компонент ОС – Internet Information Services (IIS) («Панель управления --> Программы и компоненты --> Включение и отключение компонентов Windows», для чего необходимо включить флажок "Службы IIS". Проконтролируйте и, при необходимости, включите следующие составляющие компонента IIS:

3.1.Службы IIS --> Службы интернета --> Безопасность

3.1.1.Фильтрация запросов

3.2.Службы IIS --> Службы интернета --> Компоненты разработки приложений:

3.2.1.ASP .NET

3.2.2.Расширения ISAPI

3.2.3.Расширяемость .NET

3.2.4.Фильтры ISAPI

3.3.Службы IIS --> Службы интернета --> Общие функции HTTP

3.3.1.Документ по умолчанию

3.3.2.Ошибки HTTP

3.3.3.Просмотр каталога

3.3.4.Статическое содержимое

3.4.Службы IIS --> Службы интернета --> Проверка работоспособности и диагностика

3.4.1.Ведение журнала HTTP

3.4.2.Монитор запросов

3.5.Службы IIS --> Службы интернета --> Функции повышения быстродействия

3.5.1.Сжатие статического содержимого

3.6.Службы IIS --> Средства управления веб-сайтом

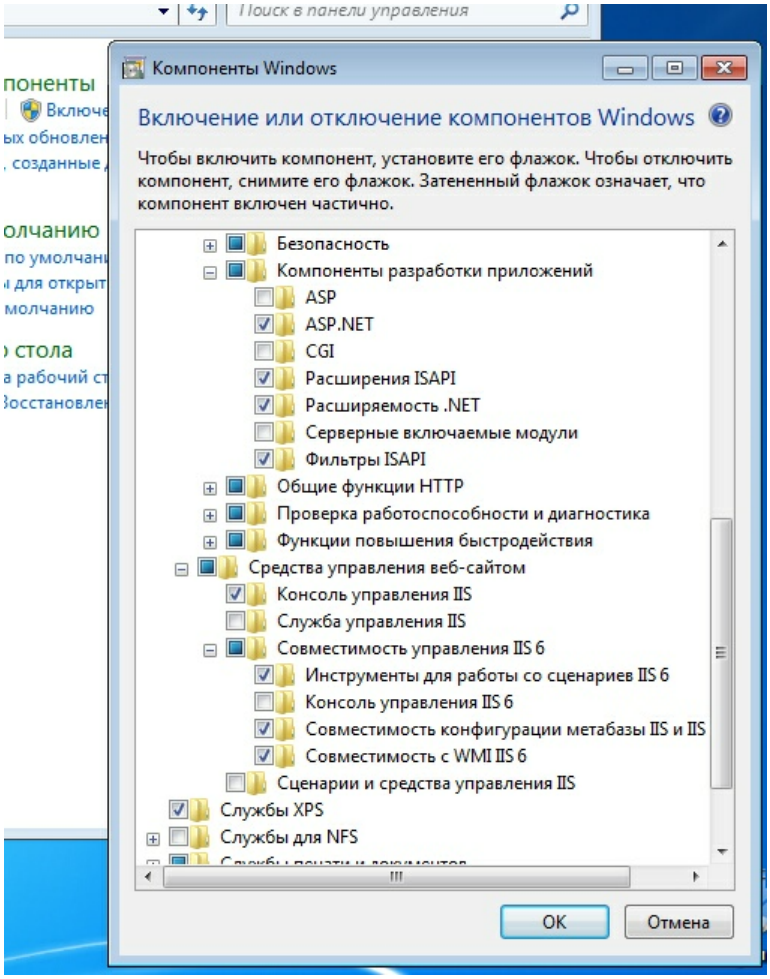
3.6.1.Консоль управления IIS

3.7.Службы IIS --> Средства управления веб-сайтом --> Совместимость управления IIS 6

3.7.1.Инструменты для работы со сценариев IIS 6

3.7.2.Совместимость конфигурации метабазы IIS и IIS 6

3.7.3.Совместимость с WMI IIS 6



4. Установите последние обновления ОС (с сайта www.microsoft.com или с помощью оснастки "Центр обновления" панели управления).

5. Если на этом компьютере планируется установка компонента «Хранилище», установите продукт «SQL Server 2008 Express Edition» (каталог инсталляционного диска «Компоненты для предустановки ОС\SQL Server 2008 Express 32» (для 32-х разрядной системы) или «Компоненты для предустановки ОС\SQL Server 2008 Express 64» (для 64-х рязрядной системы)), для чего необходимо:

   5.1. Запустить SQLServerExpressSetup.bat **от имени администратора** и дождаться окончания всех действий по установке. Этот способ запуска процесса установки устраняет необходимость отвечать на многочисленные вопросы, задаваемые в процессе работы установщика

   Примечание: Для запуска исполняемого файла от имени администратора необходимо выбрать его **правой** кнопкой мыши и в появившемся меню выбрать пункт "Запуск от имени администратора". В зависимости от настроек безопасности, может быть выдан дополнительный запрос на исполнение операции.

   5.2. По окончании установки открывается окно блокнота, индицирующего результат работы установщика, а также удаляются временные файлы

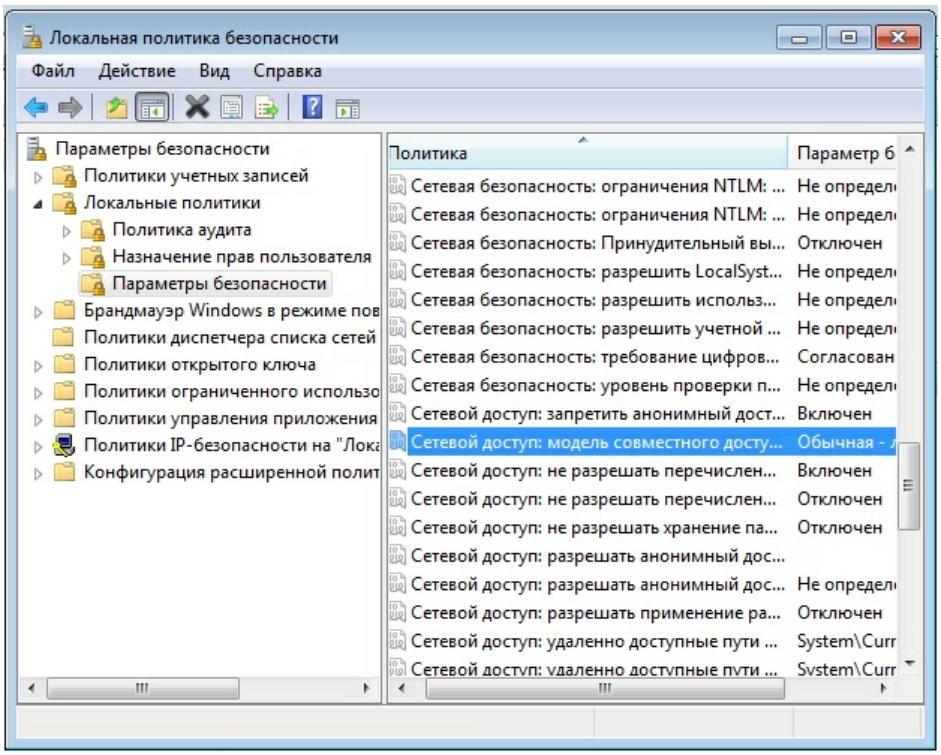
4.1.4.2 Основная установка

Продолжение подготовки. Далее описаны действия, которые необходимо выполнить только для основной (сетевой) установки системы.

1. Проверьте правильность настройки Локальной политики безопасности, для этого:

   1.1. Откройте "Панель управления --> Администрирование --> Локальная политика безопасности --> Локальные политики --> Параметры безопасности"

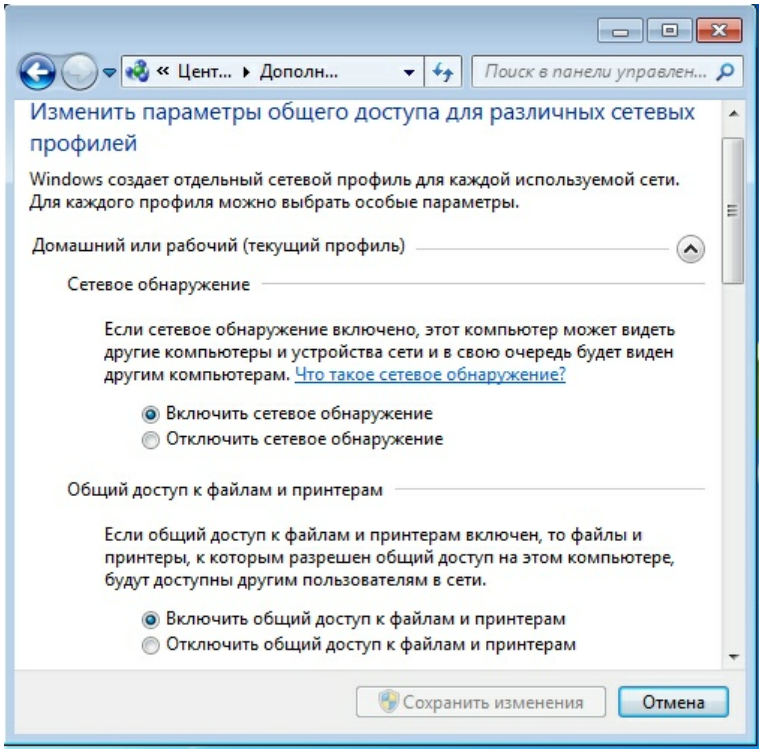
   1.2. Параметр "Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей" должен иметь значение "Обычная – локальные пользователи удостоверяются как они сами".



2. Проверьте правильность настройки сетевого обнаружения. Для этого:

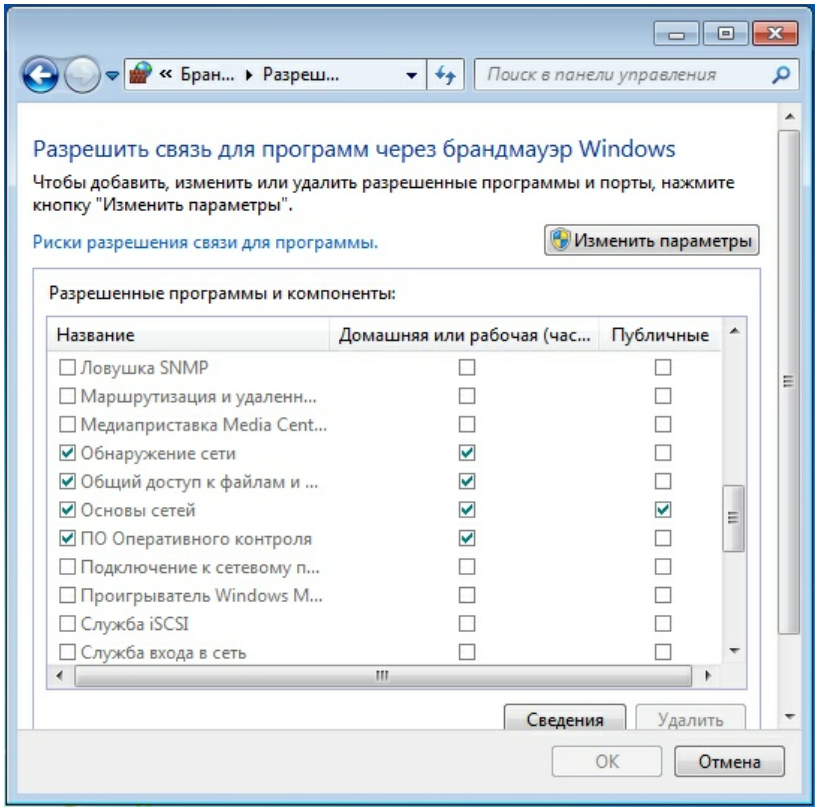
   2.1. Запустите "Панель управления --> Центр управления сетями и общим доступом --> Изменить дополнительные параметры общего доступа"

   2.2. Проверьте что параметр "Домашний или рабочий (текущий профиль) --> Включить сетевое обнаружение" включен



3. Убедитесь в том, что в брандмауэре Windows разрешены исключения "Обнаружение сети" и "Основы сетей". Для этого

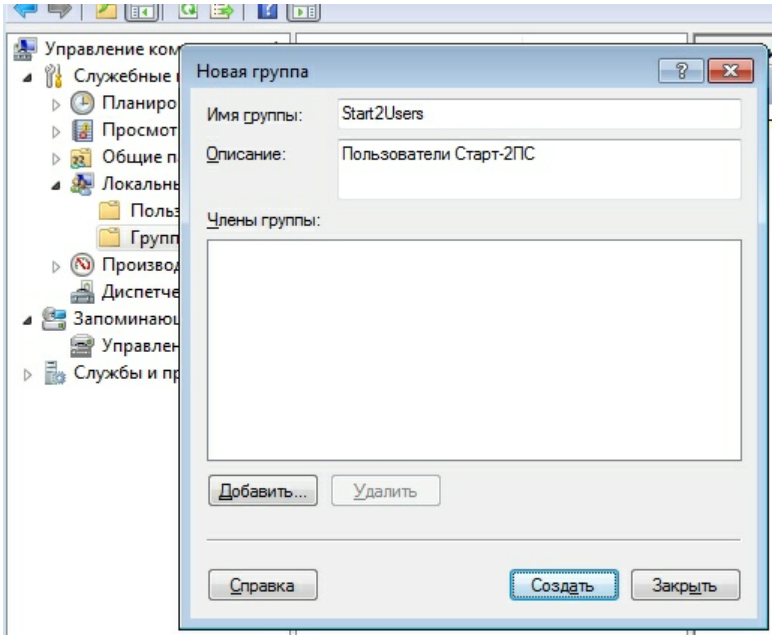
   3.1.Запустите "Панель управления --> Брандмауэр Windows --> Разрешить запуск программы или компонента через брандмауэр Windows" и проверьте состояние флажков "Обнаружение сети" и "Основы сетей"



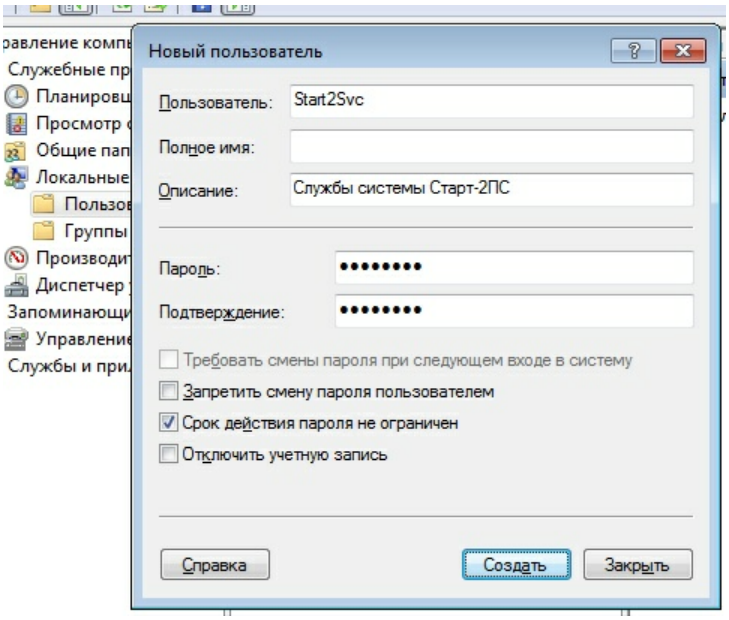
4. Настройте список пользователей Windows. Если компьютеры локальной сети

объединены в рабочую группу, на каждом компьютере системы должен быть создан одинаковый набор учётных записей системы безопасности операционной системы:

4.1.Создайте группу безопасности, члены которой впоследствии получат доступ к функциям системы "Старт-2ПС", рекомендуемое имя - «Start2Users». Для этого запустите диалог управления компьютером "Панель управления --> Администрирование --> Управление компьютером". Выберете в дереве "Служебные программы --> Локальные пользователи и группы --> Группы". Создайте группу (вызов диалога - правой кнопкой мыши)



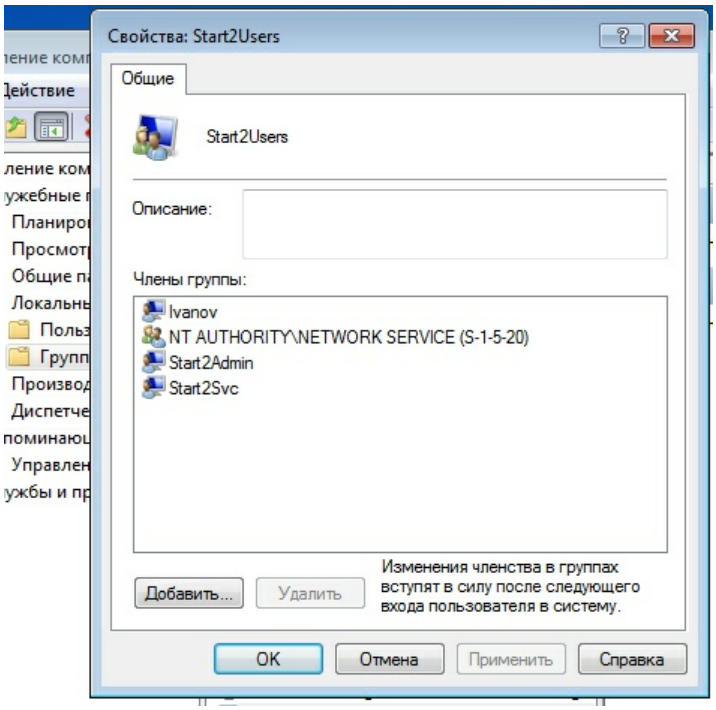
4.2.Создайте учётную запись **с непустым паролем** для служб системы "Старт-2 ПС", рекомендуемое имя - «Start2Svc». Для этого в ветви "Пользователи" щелчком правой кнопки мыши вызовите диалог



4.3.Последовательно заполняя форму и нажимая кнопку "Создать", создайте

учётные записи **с непустыми паролями** для администратора системы (рекомендуемое имя «Start2Admin») и для всех операторов системы «Старт-2 ПС» (например, «Ivanov», «Petrov» и пр).

4.4.Включите в группу «Start2Users» только что созданные учетные записи, а также встроенную учётную запись Windows NETWORK SERVICE



4.5.Дополнительно включите учётные записи «Start2Svc», «Start2Admin» в группу «Администраторы». Их членство в группе "Пользователи" можно исключить.

4.6.Проверьте, что учётные записи операторов включены в группу «Пользователи» и "Start2Users" и не включены в группу "Администраторы". Излишние полномочия у операторов системы могут отрицательно сказаться на безопасности и устойчивости работы системы.

5. Запомните имена учётных записей и пароли к ним. Эти имена и пароли должны быть сохранены в безопасном месте.
Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

6. Настройте параметры безопасности в механизме COM/DCOM. Для этого необходимо:

6.1.Запустить оснастку «Службы компонентов», вызвав её с помощью панели управления: "Панель управления --> Администрирование --> Службы компонентов"

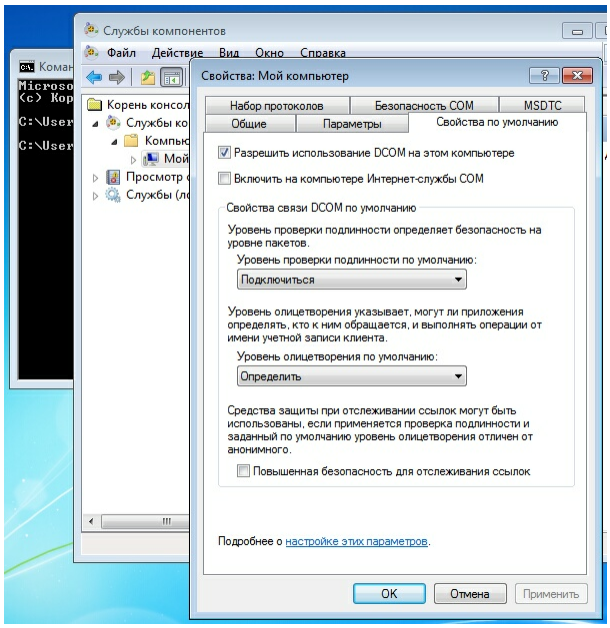
6.2.Убедиться, что параметры вкладки «Свойства по умолчанию» (Службы компонентов --> Компьютеры --> Мой компьютер --> Свойства) имеют следующие

значения:

6.2.1.Разрешить исп. DCOM на этом компьютере: вкл

6.2.2.Уровень проверки подлинности по умолчанию: Подключиться

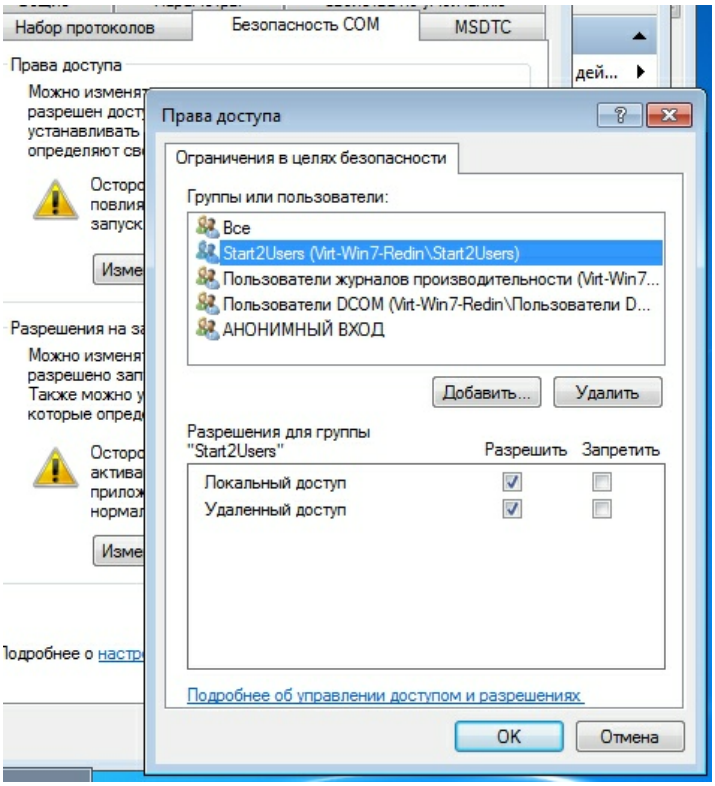
6.2.3.Уровень олицетворения по умолчанию: Определить



6.3.На вкладке «Безопасность COM»

6.3.1.Права доступа --> Кнопка «Изменить ограничения»

6.3.1.1.Добавить группу «Start2Users»



6.3.1.2.Разрешить ей

6.3.1.2.1.«Локальный доступ»

6.3.1.2.2.«Удалённый доступ»

6.3.1.3.Убедиться в том, что «АНОНИМНЫЙ ВХОД» имеет разрешение «Локальный доступ»

6.3.1.4.Убедиться в том, что группа «Все» имеет разрешения

6.3.1.4.1.«Локальный доступ»

6.3.1.4.2.«Удалённый доступ»

6.3.2.Права доступа --> Кнопка «Изменить умолчания»

6.3.2.1.Добавить группу «Start2Users»

6.3.2.2.Разрешить ей

6.3.2.2.1.«Локальный доступ»

6.3.2.2.2.«Удалённый доступ»

6.3.2.3.Убедиться в том, что «SELF» имеет разрешения

6.3.2.3.1.«Локальный доступ»

6.3.2.3.2.«Удалённый доступ»

6.3.2.4.Убедиться в том, что «система» имеет разрешение

6.3.2.4.1.«Локальный доступ»

6.3.3.Разрешение на запуск и активацию --> Кнопка «Изменить ограничения»

6.3.3.1.Добавить группу «Start2Users»

6.3.3.2.Разрешить ей

6.3.3.2.1.«Локальный запуск»

6.3.3.2.2.«Удалённый запуск»

6.3.3.2.3.«Локальная активация»

6.3.3.2.4.«Удалённая активация»

6.3.3.3.Убедиться в том, что группа «Администраторы» имеет разрешения

6.3.3.3.1.«Локальный запуск»

6.3.3.3.2.«Удалённый запуск»

6.3.3.3.3.«Локальная активация»

6.3.3.3.4.«Удалённая активация»

6.3.3.4.Убедиться в том, что группа «Все» имеет разрешения

6.3.3.4.1.«Локальный запуск»

6.3.3.4.2. «Локальная активация»

6.3.4.Разрешение на запуск и активацию --> Кнопка «Изменить умолчания»

6.3.4.1.Добавить группу «Start2Users»

6.3.4.2.Разрешить ей

6.3.4.2.1.«Локальный запуск»

6.3.4.2.2.«Удалённый запуск»

6.3.4.2.3.«Локальная активация»

6.3.4.2.4.«Удалённая активация»

6.3.4.3.Убедиться в том, что «система» имеет разрешения

6.3.4.3.1.«Локальный запуск»

6.3.4.3.2. «Локальная активация»

6.3.4.4.Убедиться в том, что группа «Администраторы» имеет разрешения

6.3.4.4.1.«Локальный запуск»

6.3.4.4.2.«Удалённый запуск»

6.3.4.4.3.«Локальная активация»

6.3.4.4.4.«Удалённая активация»

6.3.4.5.Убедиться в том, что группа «ИНТЕРАКТИВНЫЕ» имеет разрешения

6.3.4.5.1.«Локальный запуск»

6.3.4.5.2. «Локальная активация»

7. Перезагрузите компьютер.
8. Войдите как администратор.

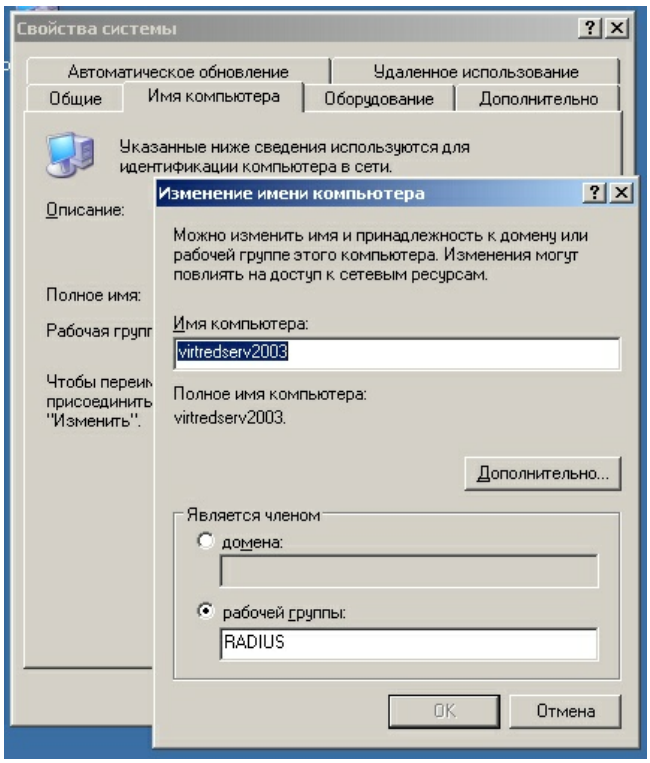
4.1.5 Операционная система Windows Server 2003 Std SP2

4.1.5.1 Основная и локальная установка

1. Установите Windows Server 2003 Standart Edition SP2.
2. Имя компьютера, имя рабочей группы и сетевой адрес обычно задаётся в процессе установки операционной системы, однако это можно сделать и сейчас следующим образом:

2.1.Назначение имени компьютера и имени рабочей группы:

2.1.1.Вызовите окно "Изменение имени компьютера" одним из способов, например "Пуск --> Мой компьютер --> Правая кнопка мыши: "Свойства" --> Вкладка "Имя компьютера" --> Кнопка "Изменить""

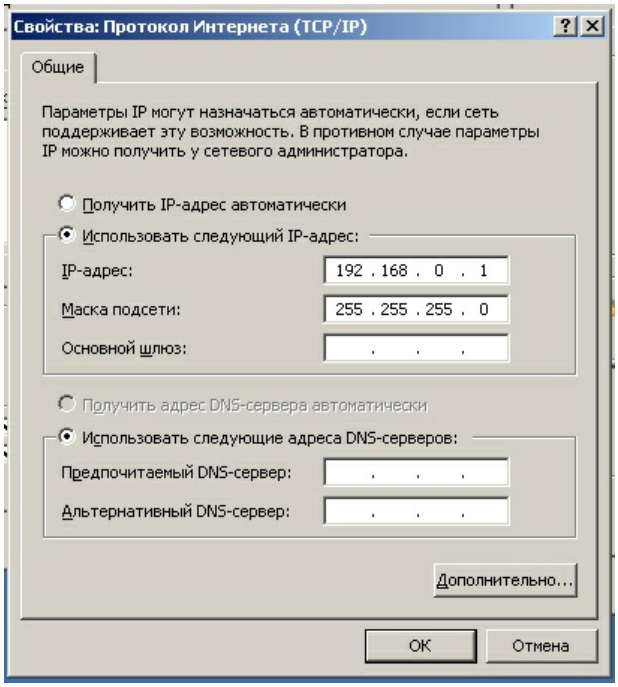


2.1.2.В появившемся окне введите новое имя компьютера и имя рабочей группы Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

2.1.3.По окончании ввода (нажата кнопка "OK") система предложит перезагрузку. Перезагрузите операционную систему

2.2.Назначение сетевого адреса:

2.2.1.Вызовите окно "Свойства: Протокол Интернета (TCP/IP)" одним из способов, например "Панель управления --> Сетевые подключения --> выберите настраиваемое подключение (обычно "Подключение по локальной сети") --> Кнопка "Свойства" --> элемент списка: Протокол Интернета (TCP/IP) --> Кнопка Свойства"



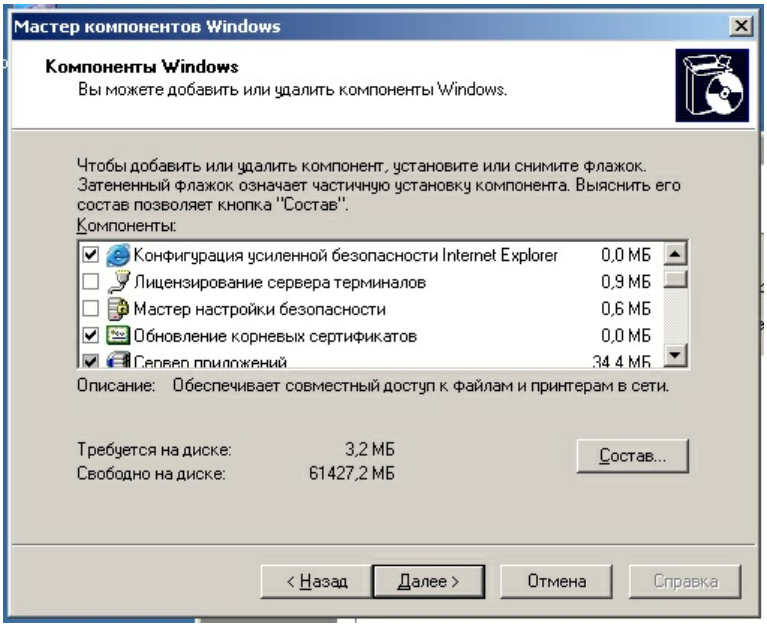
2.2.2.Введите сетевой адрес в соответствии с рекомендациями по выбору парметров сети (см. выше). Маска подсети после ввода корректного адреса, как правило, устанавливается автоматически. Остальные поля заполнять не обязательно.

Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

2.2.3.По окончании ввода система может предложить перезагрузиться

3. Если на этом компьютере планируется установка компонента «Хранилище», установите компонент ОС – Internet Information Services (IIS) («Панель управления --> Установка и удаление программ --> Установка компонентов Windows».

3.1.В открывшемся окне



выберите компонент "Сервер приложений" и нажмите кнопку "Состав"

3.2.Последовательно углубляясь в набор компонентов (нажимая кнопку "Состав" в каждом вложенном окне), проконтролируйте, что флажки следующих компонентов включены:

3.2.1.ASP.NET.

3.2.2.Консоль сервера приложений.

3.2.3.Службы IIS --> Состав -->

3.2.3.1.Диспетчер служб IIS

3.2.3.2.Общие файлы

3.2.3.3.Служба WWW --> Состав -->

3.2.3.3.1.Служба WWW

3.3.Вернитесь в окно "Компоненты Windows" и **сбросьте** флажок компонента "Конфигурация усиленной безопасности Internet Explorer" (этот компонент предназначен для контроля доверия к WWW узлам; в процессе своей работы он задаёт многочисленные вопросы о принадлежности к доверенным узлам и создаёт неудобства при работе с генератором отчётов).

3.4.Запустите выполнение мастера кнопкой "Далее".

4. Установите последние обновления ОС (с сайта www.microsoft.com или с помощью оснастки "Центр обновления" панели управления). Обычно в процессе установки обновлений автоматически устанавливается компонент Microsoft .Net Framework 3.5., если установка обновлений невозможна, установите Microsoft .Net Framework 3.5 вручную (установочные файлы прилагаются, это каталог «Компоненты для предустановки ОС\DotNet 3.5» инсталляционного диска) последовательно запустив

4.1.dotnetfx35.exe

4.2.NDP35SP1-KB958484-x86.exe

4.3. dotnetfx35langpack_x86ru.exe

5. Если на этом компьютере планируется установка компонента «Хранилище»:

5.1.Установите продукт «SQL Server 2008 Express Edition» (каталог «Компоненты для предустановки ОС\SQL Server 2008 Express» инсталляционного диска), для чего необходимо:

5.1.1.Установить WindowsServer2003-KB942288-v4-x86.exe (это необходимое обновление для успешной работы установщика Windows). По окончании

установки может потребоваться перезагрузка компьютера.

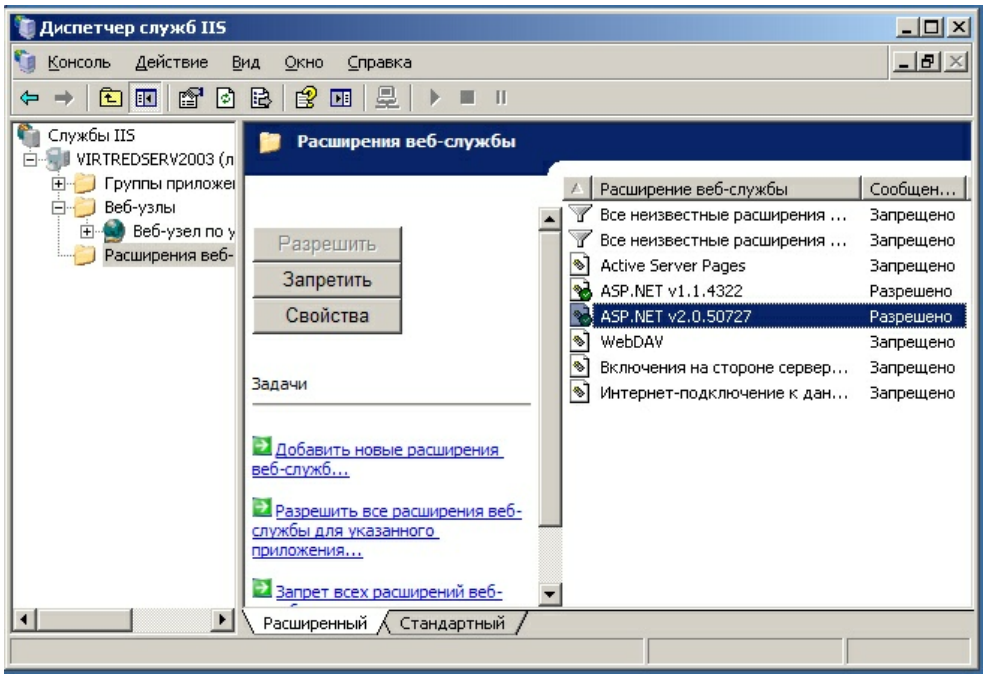
5.1.2.Запустить SQLServerExpressSetup.bat и дождаться окончания всех действий по установке. Этот способ запуска процесса установки устраняет необходимость отвечать на многочисленные вопросы, задаваемые в процессе работы установщика.

5.1.3.По окончании установки открывается окно блокнота, индицирующего результат работы установщика, а также удаляются временные файлы.

5.2.Проверьте правильность настройки службы IIS, для чего:

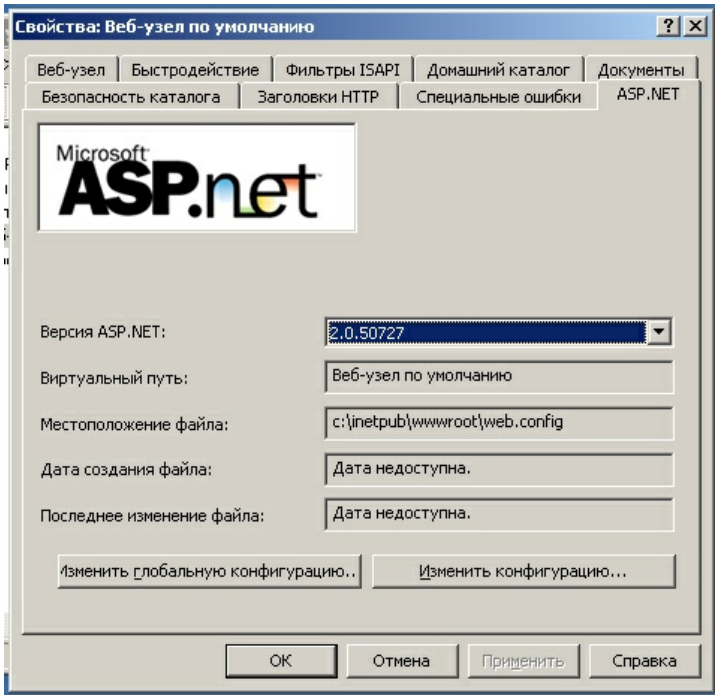
5.2.1.Запустите оснастку "Диспетчер служб IIS": "Пуск --> Администрирование --> Диспетчер служб IIS"

5.2.2.Выберите в дереве узел "Расширения веб-службы". Проконтролируйте, что все расширения, имена которых начинаются с "ASP .NET", разрешены.

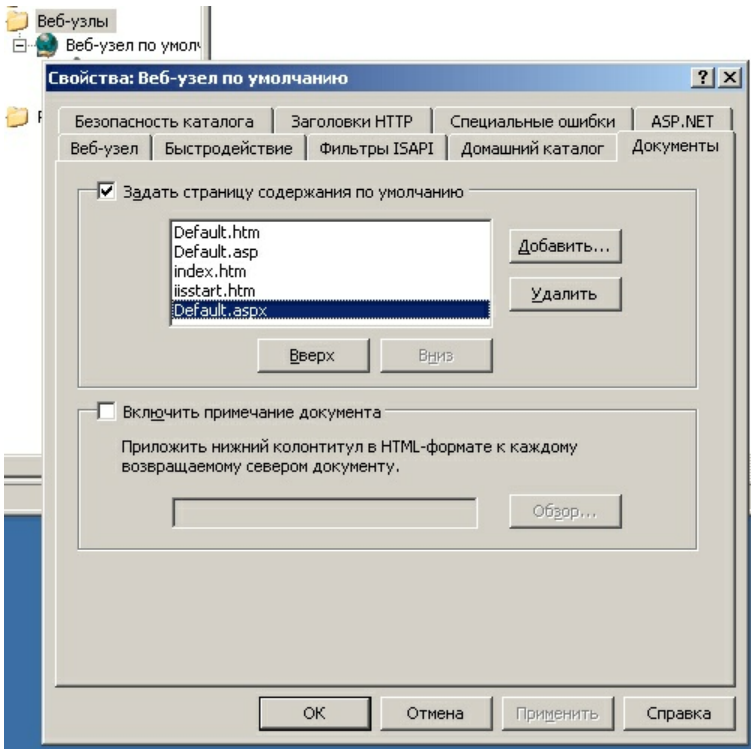


5.2.3.Вызовите окно свойств веб-узла по умолчанию (в дереве узел "Веб-узлы --> Веб-узел по умолчанию --> Правая кнопка мыши: пункт меню Свойства"

5.2.4.На вкладке "ASP .NET" проверьте и, при необходимости, скорректируйте версию ASP .NET: должно быть установлено значение "2..0.50727"



5.2.5.На вкладке "Документы" проверьте наличие и, при необходимости, добавьте в список "Задать страницу содержания по умолчанию" имя страницы "Default. aspx"



4.1.5.2 Основная установка

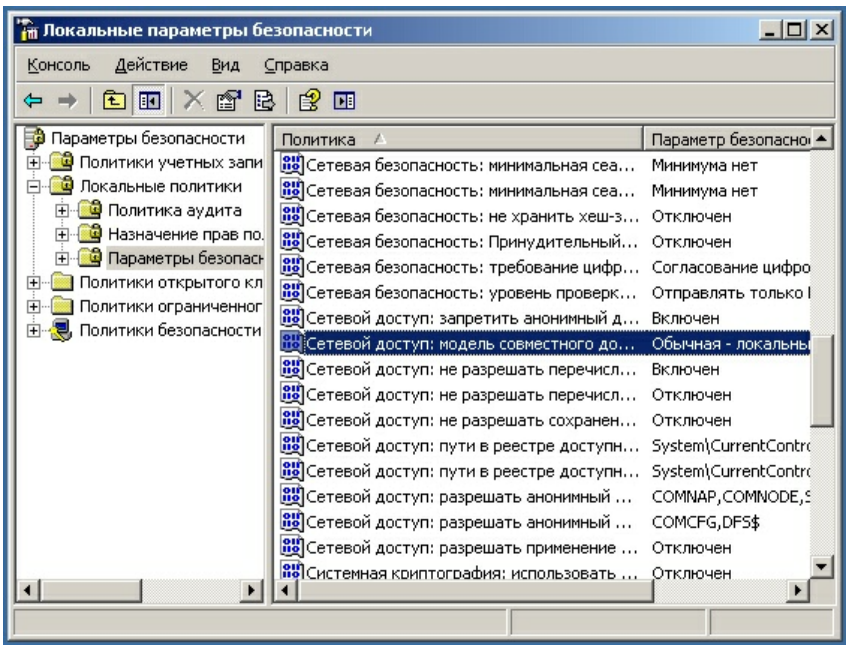
Продолжение подготовки. Далее описаны действия, которые необходимо выполнить только для основной (сетевой) установки системы

1. Проверьте правильность настройки локальной политики безопасности, для этого:

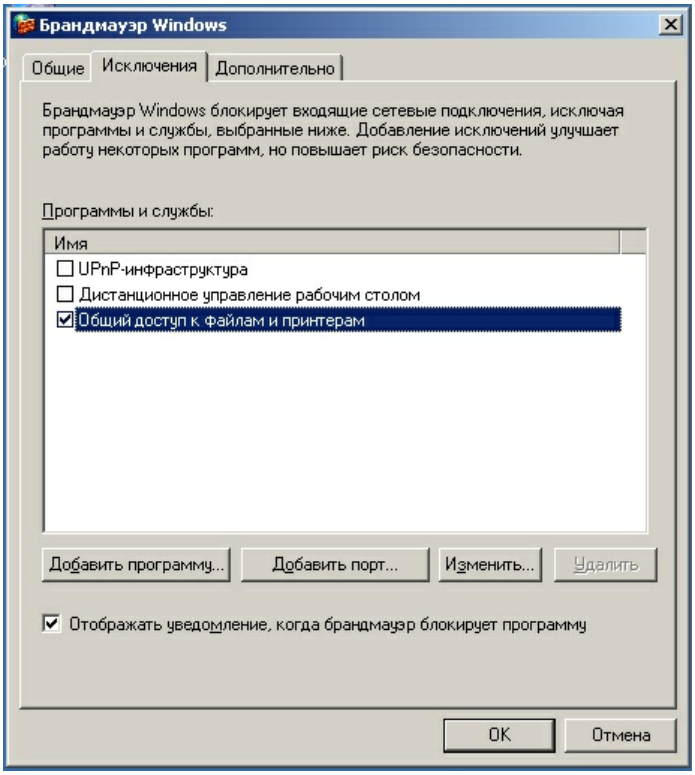
1.1.Откройте "Пуск --> Администрирование --> Локальная политика безопасности -->

Локальные политики --> Параметры безопасности"

1.2.Параметр "Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей" должен иметь значение "Обычная – локальные пользователи удостоверяются как они сами".



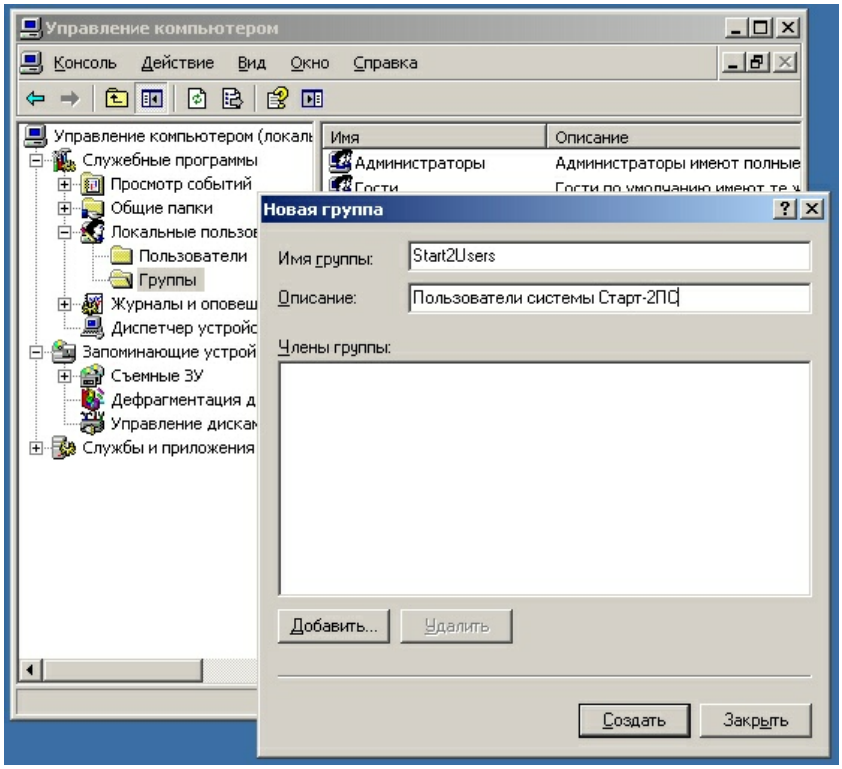
2. Убедитесь в том, что в брандмауэре Windows разрешено исключение «Общий доступ к файлам и принтерам». Для этого зайдите в «Панель управления», выберите «Брандмауэр Windows», перейдите на вкладку "Исключения", проверьте флажок «Общий доступ к файлам и принтерам»



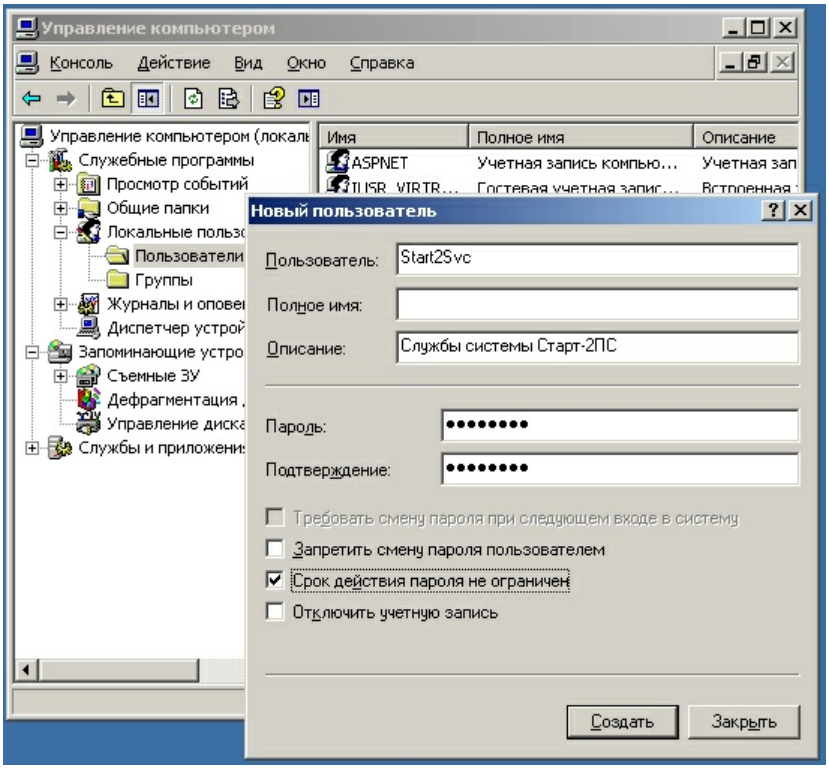
3. Настройте список пользователей Windows. Если компьютеры локальной сети

объединены в рабочую группу, на каждом компьютере системы должен быть создан одинаковый набор учётных записей системы безопасности операционной системы:

3.1.Создайте группу безопасности, члены которой впоследствии получат доступ к функциям системы "Старт-2ПС", рекомендуемое имя - «Start2Users». Для этого запустите диалог управления компьютером "Пуск --> Администрирование --> Управление компьютером". Выберете в дереве "Служебные программы --> Локальные пользователи и группы --> Группы". Создайте группу (вызов диалога - правой кнопкой мыши)

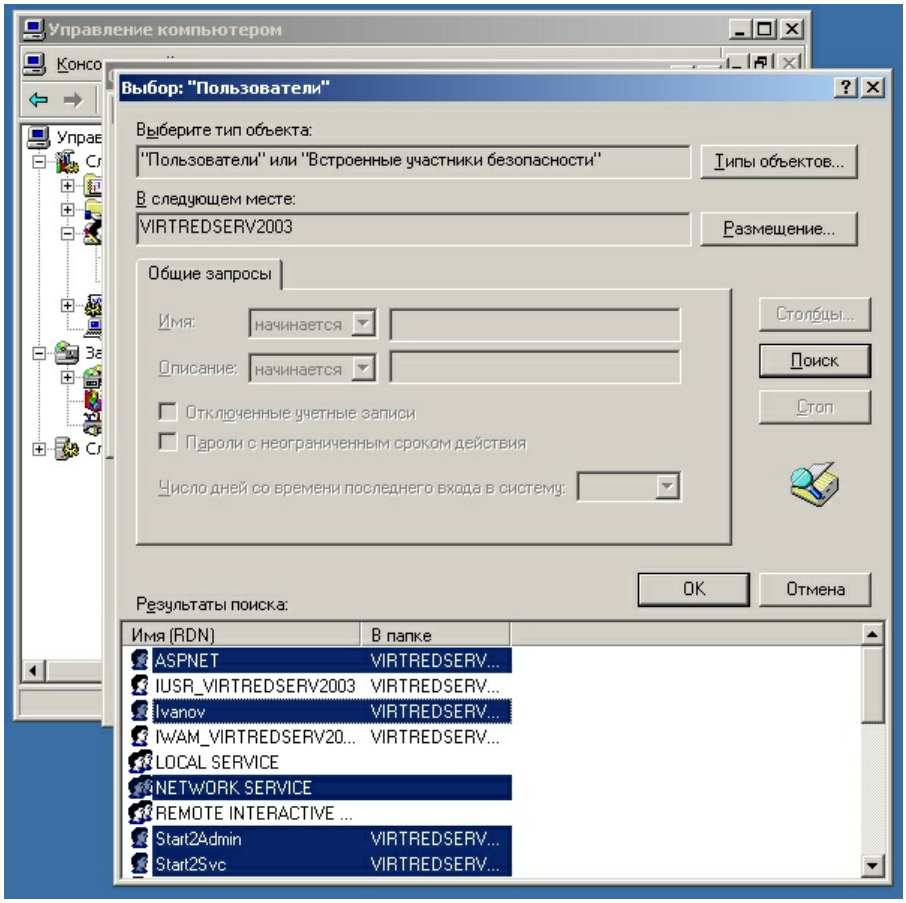


3.2.Создайте учётную запись **с непустым паролем** для служб системы "Старт-2 ПС", рекомендуемое имя - «Start2Svc». Для этого в ветви "Пользователи" щелчком правой кнопки мыши вызовите диалог



3.3.Последовательно заполняя форму и нажимая кнопку "Создать", создайте учётные записи **с непустыми паролями** для администратора системы (рекомендуемое имя «Start2Admin») и для всех операторов системы «Старт-2 ПС» (например, «Ivanov», «Petrov» и пр).

3.4.Включите в группу «Start2Users» только что созданные учетные записи, а также встроенные учётные записи Windows ASPNET и NETWORK SERVICE



3.5.Дополнительно включите учётные записи "Start2Svc", "Start2Admin" в группу "Администраторы". Их членство в группе "Пользователи" можно исключить.

3.6.Проверьте, что учётные записи операторов включены в группу "Пользователи" и "Start2Users" и не включены в группу "Администраторы". Излишние полномочия у операторов системы могут отрицательно сказаться на безопасности и устойчивости работы системы.

4. Запомните имена учётных записей и пароли к ним. Эти имена и пароли должны быть сохранены в безопасном месте.
Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

5. Настройте параметры безопасности в механизме COM/DCOM. Для этого необходимо:

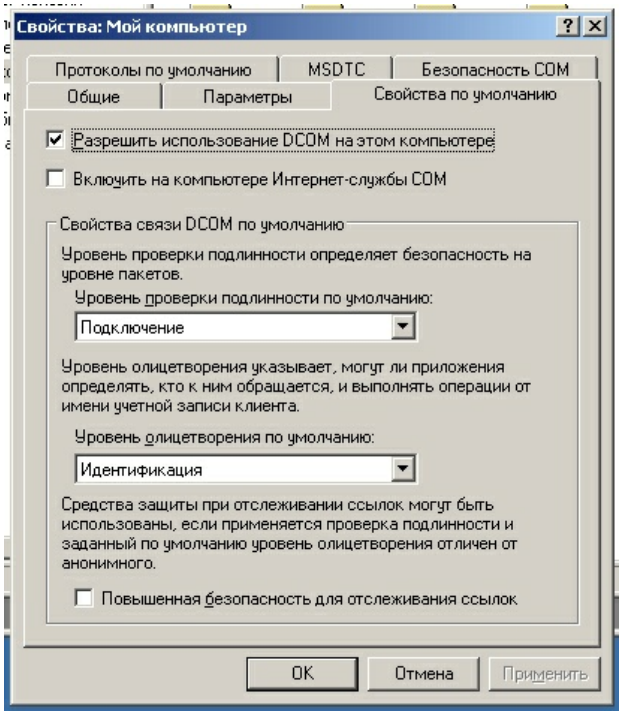
5.1.Запустить оснастку «Службы компонентов» («Пуск --> Администрирование --> «Службы компонентов».

5.2.Убедиться, что параметры вкладки «Свойства по умолчанию» (Службы компонентов --> Компьютеры --> Мой компьютер --> Свойства) имеют следующие значения:

5.2.1.Разрешить исп. DCOM на этом компьютере: вкл

5.2.2.Уровень проверки подлинности по умолчанию: Подключение

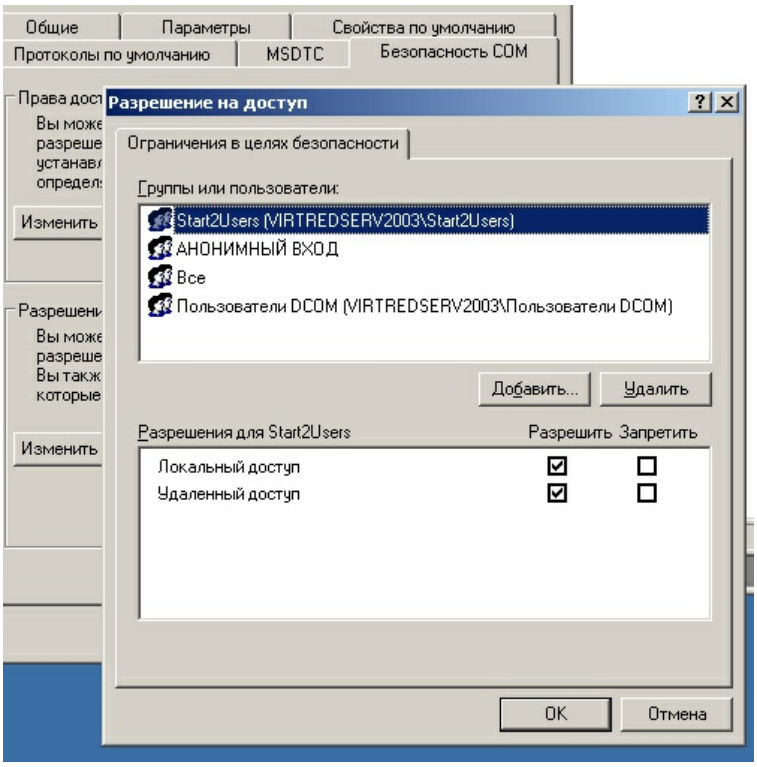
5.2.3.Уровень олицетворения по умолчанию: Идентификация



5.3.На вкладке «Безопасность COM»

5.3.1.Права доступа --> Кнопка «Изменить ограничения»

5.3.1.1.Добавить группу «Start2Users»



5.3.1.2.Разрешить ей

5.3.1.2.1.«Локальный доступ»

5.3.1.2.2.«Удалённый доступ»

5.3.2.Права доступа --> Кнопка «Изменить настройки по умолчанию»

5.3.2.1.Добавить группу «Start2Users»

5.3.2.2.Разрешить ей

5.3.2.2.1.«Локальный доступ»

5.3.2.2.2.«Удалённый доступ»

5.3.2.3.Убедиться в том, что «SELF» имеет разрешения

5.3.2.3.1.«Локальный доступ»

5.3.2.3.2.«Удалённый доступ»

5.3.2.4.Убедиться в том, что «SYSTEM» имеет разрешение

5.3.2.4.1.«Локальный доступ»

5.3.3.Разрешение на запуск и активацию --> Кнопка «Изменить ограничения»

5.3.3.1.Добавить группу «Start2Users»

5.3.3.2.Разрешить ей

5.3.3.2.1.«Локальный запуск»

5.3.3.2.2.«Удалённый запуск»

5.3.3.2.3.«Локальная активация»

5.3.3.2.4.«Удалённая активация»

5.3.4.Разрешение на запуск и активацию --> Кнопка «Изменить настройки по умолчанию»

5.3.4.1.Добавить группу «Start2Users»

5.3.4.2.Разрешить ей

5.3.4.2.1.«Локальный запуск»

5.3.4.2.2.«Удалённый запуск»

5.3.4.2.3.«Локальная активация»

5.3.4.2.4.«Удалённая активация»

5.3.4.3.Убедиться в том, что «SYSTEM» имеет разрешения

5.3.4.3.1.«Локальный запуск»

5.3.4.3.2. «Локальная активация»

5.3.4.4.Убедиться в том, что группа «Администраторы» имеет разрешения

5.3.4.4.1.«Локальный запуск»

5.3.4.4.2.«Удалённый запуск»

5.3.4.4.3.«Локальная активация»

5.3.4.4.4.«Удалённая активация»

5.3.4.5.Убедиться в том, что группа «ИНТЕРАКТИВНЫЕ» имеет разрешения

5.3.4.5.1.«Локальный запуск»

5.3.4.5.2. «Локальная активация»

6. Перезагрузите компьютер.
7. Войдите как администратор

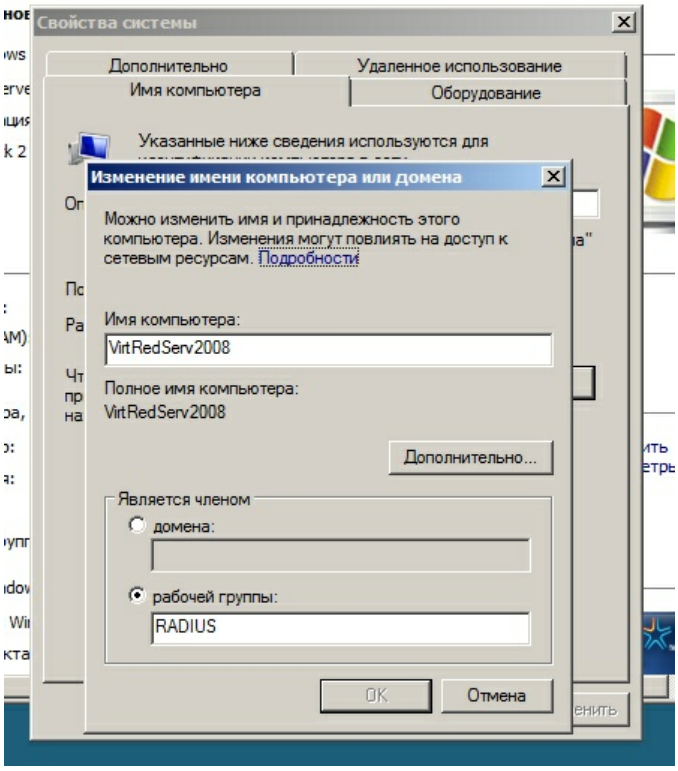
4.1.6 Операционная система Windows Server 2008 Std SP2 (2008 R2)

4.1.6.1 Основная и локальная установка

1. Установите Windows Server 2008 Std SP2 Rus / Windows Server 2008 R2 Std SP1 Rus.
2. Имя компьютера, имя рабочей группы и сетевой адрес обычно задаётся в процессе установки операционной системы, однако это можно сделать и сейчас следующим образом:

   2.1.Назначение имени компьютера и имени рабочей группы:

   2.1.1.Вызовите окно "Изменение имени компьютера или домена" одним из способов, например "Панель управления --> Система --> раздел "Имя компьютера, имя домена и параметры рабочей группы" --> Изменить параметры --> Вкладка "Имя компьютера" --> Кнопка "Изменить""

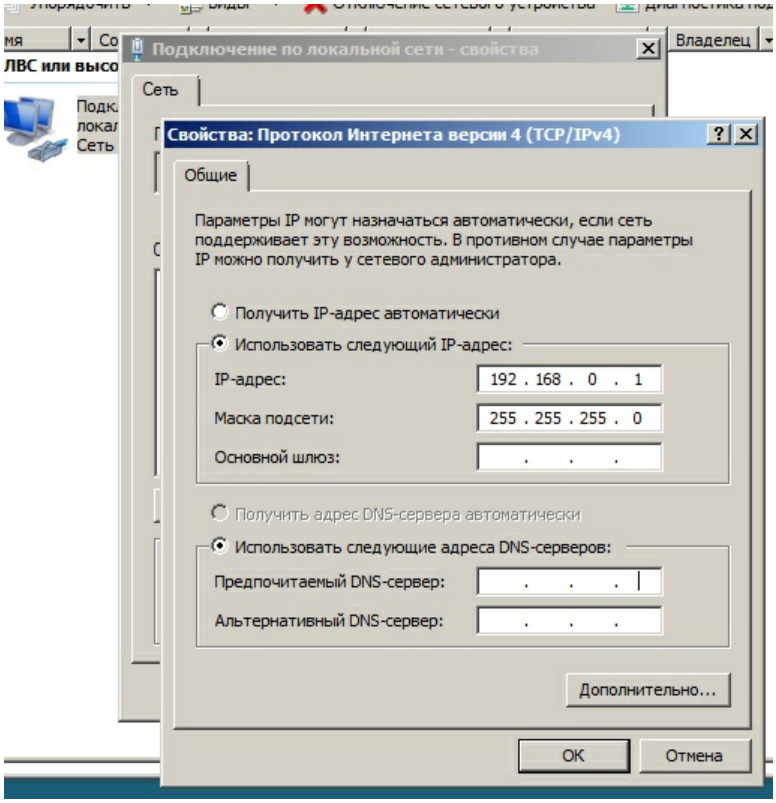


2.1.2.В появившемся окне введите новое имя компьютера и имя рабочей группы Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

2.1.3.По окончании ввода (нажата кнопка "OK") система предложит перезагрузку. Перезагрузите операционную систему

2.2.Назначение сетевого адреса:

2.2.1.Вызовите окно "Свойства: Протокол Интернета версии 4 (TCP/IPv4)" одним из способов, например "Панель управления --> Центр управления сетями и общим доступом --> Управление сетевыми подключениями --> выберите настраиваемое подключение (обычно "Подключение по локальной сети") --> Правая кнопка мыши --> меню Свойства --> элемент списка: Протокол Интернета версии 4 (TCP/IPv4) --> Кнопка Свойства"



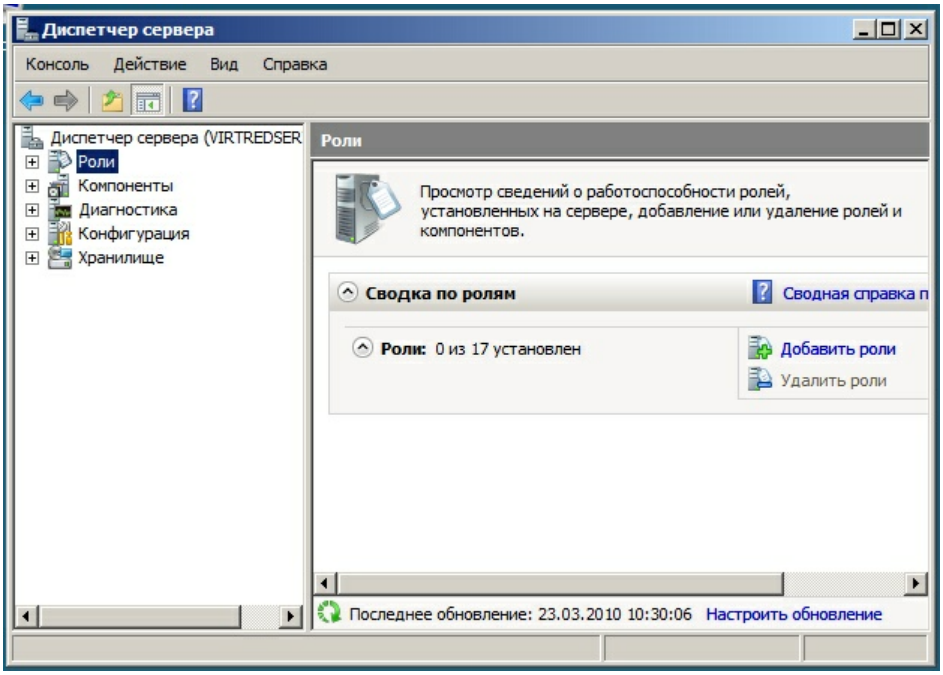
2.2.2.Введите сетевой адрес в соответствии с рекомендациями по выбору парметров сети (см. выше). Маска подсети после ввода корректного адреса, как правило, устанавливается автоматически. Остальные поля заполнять не обязательно.

Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

2.2.3.По окончании ввода система может предложить перезагрузиться

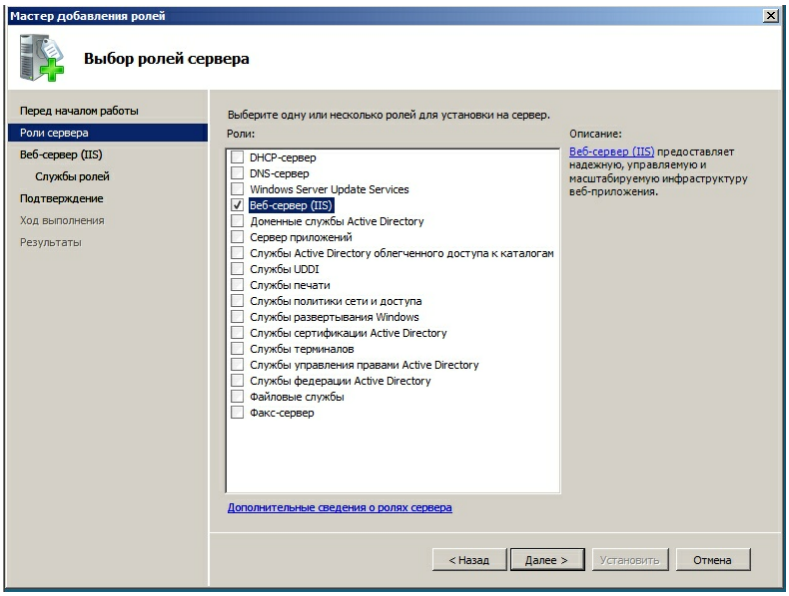
3. Если на этом компьютере планируется установка компонента «Хранилище», установите компонент ОС – Internet Information Services (IIS). Для этого:

3.1.Вызовите оснастку "Диспетчер сервера": "Пуск --> Администрирование --> Диспетчер сервера" и выберите в дереве узел "Роли"

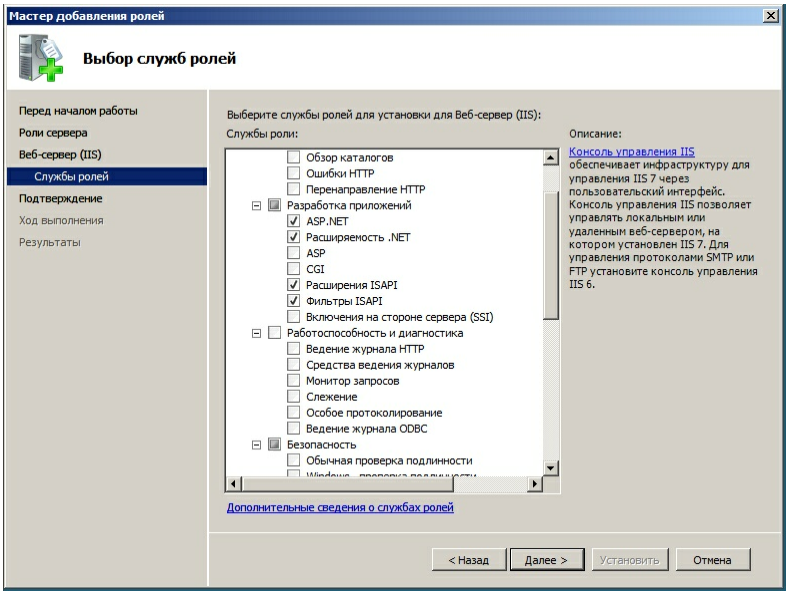


3.2.В правой области окна щёлкните по кнопке "Добавить роли".

3.3.В открывшемся окне мастера "Выбор ролей сервера" выберите роль "Веб-сервер (IIS)" и нажмите кнопку "Далее"



3.4.Последовательно нажимая кнопку "Далее" в последующих окнах мастера, дойдите до окна "Выбор служб ролей"



3.5.В дереве "Службы роли" включите флажки

3.5.1."ASP .NET" ("Веб-сервер --> Разработка приложений --> ASP .NET")

3.5.2."Консоль управления IIS" ("Веб-сервер --> Средства управления --> Консоль управления IIS")

3.5.3."Совместимость управления IIS 6" ("Веб-сервер --> Средства управления --> Совместимость управления IIS 6")

ПРИМЕЧАНИЕ: При установке указанных флажков автоматически включаются зависимые флажки, о чём может быть выдано соответствующее предупреждение.

3.6.Проконтролируйте, что все необходимые флажки находятся во включенном состоянии:

3.6.1."Веб-сервер --> Основные возможности HTTP", флажки

3.6.1.1."Стандартный документ"

3.6.1.2."Статическое содержимое"

3.6.2."Веб-сервер --> Разработка приложений", флажки

3.6.2.1."ASP .NET"

3.6.2.2."Расширяемость .NET"

3.6.2.3."Расширения ISAPI"

3.6.2.4."Фильтры ISAPI"

3.6.3."Веб-сервер --> Безопасность", флажки

3.6.3.1."Фильтрация запросов"

3.6.4."Веб-сервер --> Средства управления", флажки

3.6.4.1."Консоль управления IIS"

3.6.5."Веб-сервер --> Средства управления --> Совместимость управления IIS 6", флажки

3.6.5.1."Совместимость метабазы IIS 6"

3.6.5.2."Совместимость WMI в IIS 6"

3.6.5.3."Службы сценариев в IIS 6"

3.6.5.4."Консоль управления IIS 6"

3.7.Нажмите в текущем окне кнопку "Далее", а дойдя до окна подвтерждения, нажмите кнопку "Установить".

3.8.В следующих окнах действуйте по указаниям мастера установки.

4. Установите последние обновления ОС (с сайта www.microsoft.com или с помощью оснастки "Центр обновления" панели управления). Обычно при установке обновлений автоматически устанавливается компонент Microsoft .Net Framework 3.5. Если установка обновлений невозможна, необходимо установить Microsoft .Net Framework 3.5 вручную. В зависимости от релиза ОС это можно сделать одним из указанных способов:

4.1.Вызвать оснастку "Диспетчер сервера" (Пуск -> Администрирование -> Диспетчер сервера), в левой части окна выбрать элемент дерева "Компоненты", правой кнопкой мыши вызвать меню и выбрать пункт "Добавить компоненты". В появившемся окне "Выбор компонентов" включить флажок "Возможности .NET Framework 3.5" и надать кнопку "Далее". Если появится окно с предложением включить зависимые компоненты, согласиться с ним. Пройти по следующим окнам мастера, нажимая кнопку "Далее".

4.2.При отсутствии возможности выполнить действия, описанные в предыдущем подпункте - открыть каталог «Компоненты для предустановки ОС\DotNet 3.5» инсталляционного диска и последовательно запустить **от имени администратора**

4.2.1.dotnetfx35.exe

4.2.2.NDP35SP1-KB958484-x86.exe

4.2.3. dotnetfx35langpack_x86ru.exe

Примечание: Для запуска исполняемого файла от имени администратора необходимо выбрать его **правой** кнопкой мыши и в появившемся меню

выбрать пункт "Запуск от имени администратора". В зависимости от настроек безопасности, может быть выдан дополнительный запрос на исполнение операции.

5. Если на этом компьютере планируется установка компонента «Хранилище», установите продукт «SQL Server 2008 Express Edition» (каталог «Компоненты для предустановки ОС\SQL Server 2008 Express» инсталляционного диска), для чего необходимо:

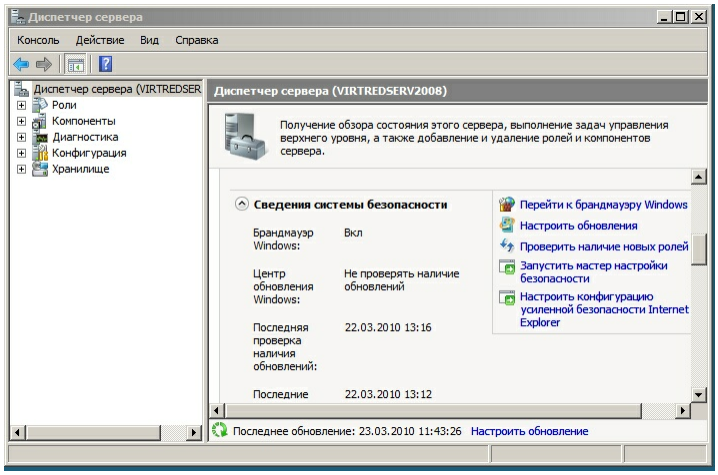
   5.1. Запустить SQLServerExpressSetup.bat **от имени администратора** и дождаться окончания всех действий по установке. Этот способ запуска процесса установки устраняет необходимость отвечать на многочисленные вопросы, задаваемые в процессе работы установщика
   Примечание: Для запуска исполняемого файла от имени администратора необходимо выбрать его **правой** кнопкой мыши и в появившемся меню выбрать пункт "Запуск от имени администратора". В зависимости от настроек безопасности, может быть выдан дополнительный запрос на исполнение операции.

   5.2. По окончании установки открывается окно блокнота, индицирующего результат работы установщика, а также удаляются временные файлы

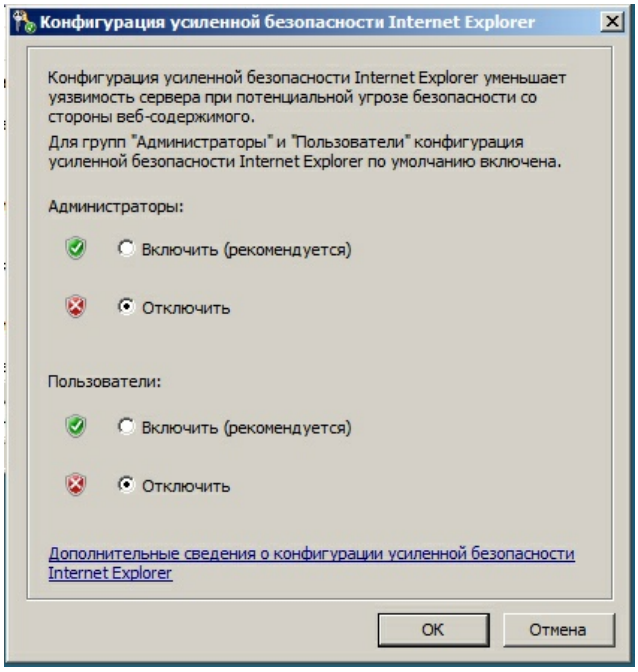
6. Если с этого компьютера предполагается обращаться к генератору отчётов (локальному или удалённому), рекомендуется отключить конфигурацию повышенной безопасности Internet Explorer" (этот режим предназначен для контроля доверия к WWW узлам; в процессе своей работы он задаёт многочисленные вопросы о принадлежности к доверенным узлам и создаёт неудобства при работе с генератором отчётов). Для этого:

   6.1. Вызовите оснастку "Диспетчер сервера": "Пуск --> Администрирование --> Диспетчер сервера" и выберите в дереве корневой узел.

   6.2. В разделе "Сведения системы безопасности" (правая панель окна) щёлкните по кнопке "Настроить конфигурацию усиленной безопасности Internet Explorer"



6.3.В появившемся окне отключите конфигурацию усиленной безопасности и для администраторов, и для пользователей и нажмите кнопку "Ok".



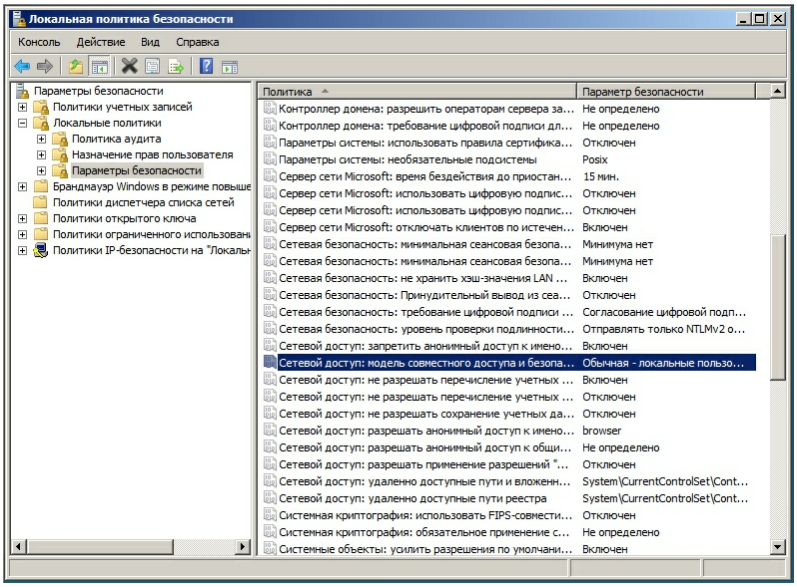
4.1.6.2 Основная установка

Продолжение подготовки. Далее описаны действия, которые необходимо выполнить только для основной (сетевой) установки системы.

1. Проверьте правильность настройки Локальной политики безопасности, для этого:

1.1.Откройте "Пуск --> Администрирование --> Локальная политика безопасности --> Локальные политики --> Параметры безопасности"

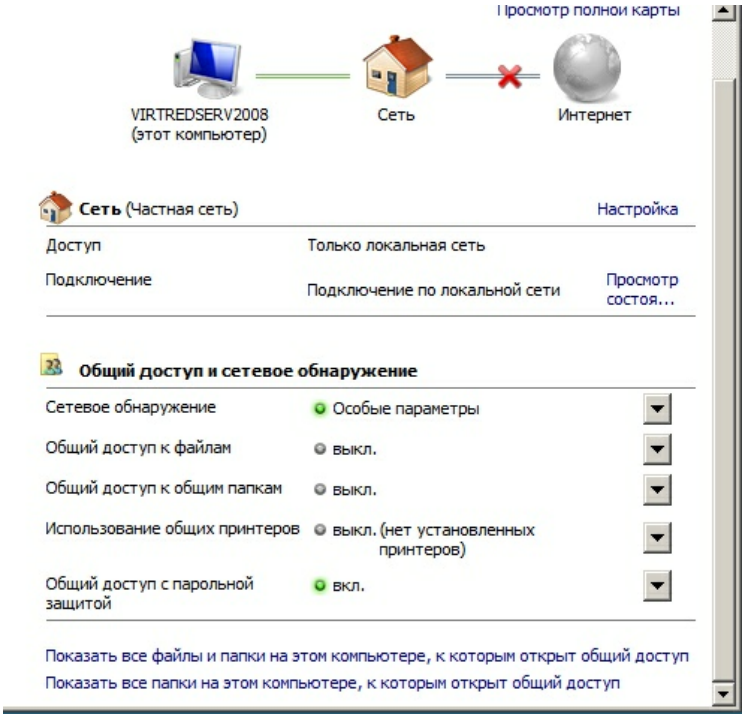
1.2.Параметр "Сетевой доступ: Модель совместного доступа и безопасности для локальных учетных записей" должен иметь значение "Обычная – локальные пользователи удостоверяются как они сами".



2. Проверьте правильность настройки сетевого обнаружения. Для этого:

   2.1.Запустите "Панель управления --> Центр управления сетями и общим доступом"

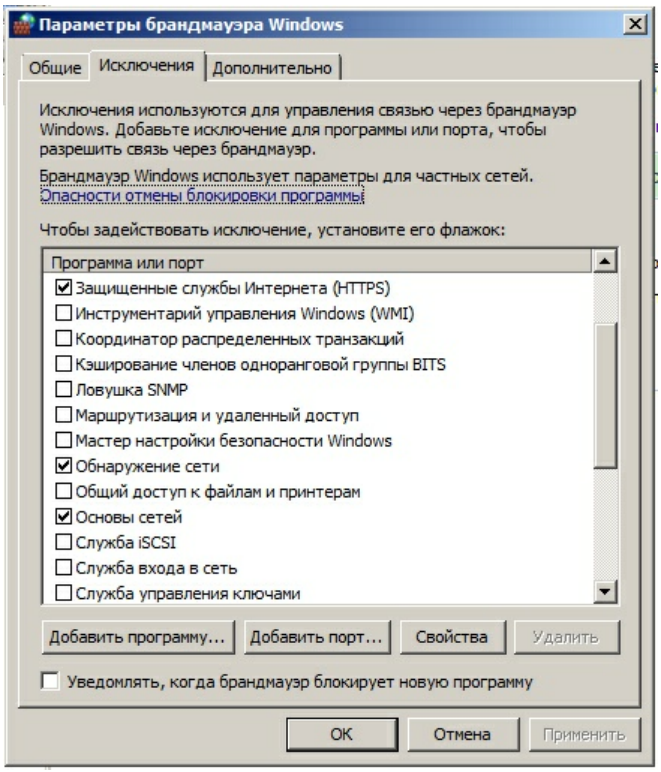
   2.2.Проверьте что параметр "Сетевое обнаружение" включен ("вкл." или "Особые параметры")



   Примечание: в зависимости от релиза ОС, наборы элементов экранных форм могут несколько отличаться и для доступа к функциям настройки общего доступа может потребоваться выбор дополнительного окна, например "Изменить дополнительные параметры общего доступа".

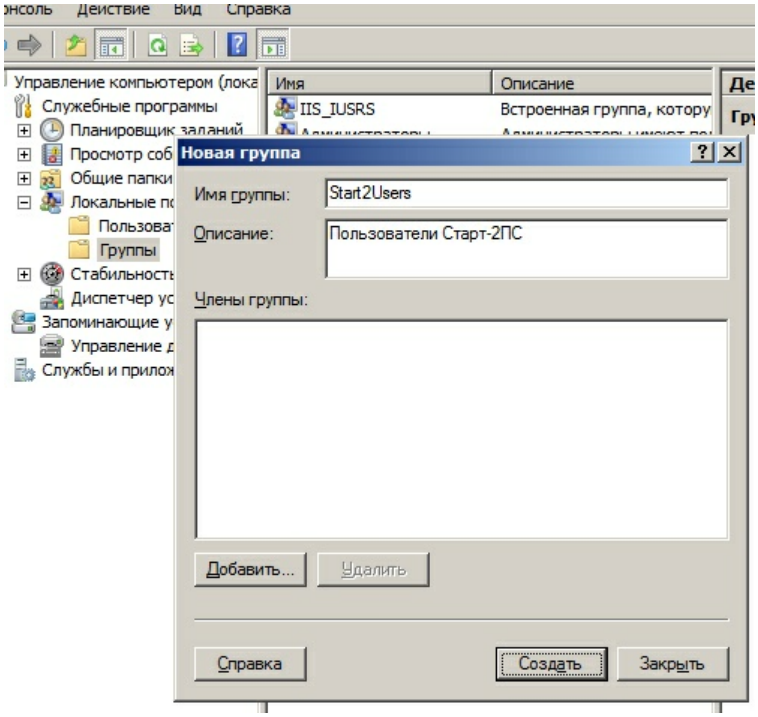
3. Убедитесь в том, что в брандмауэре Windows разрешены исключения "Обнаружение сети" и "Основы сетей". Для этого:

3.1.Запустите "Панель управления --> Брандмауэр Windows --> Разрешение запуска программ через брандмауэр Windows" и проверьте состояние флажков "Обнаружение сети" и "Основы сетей"

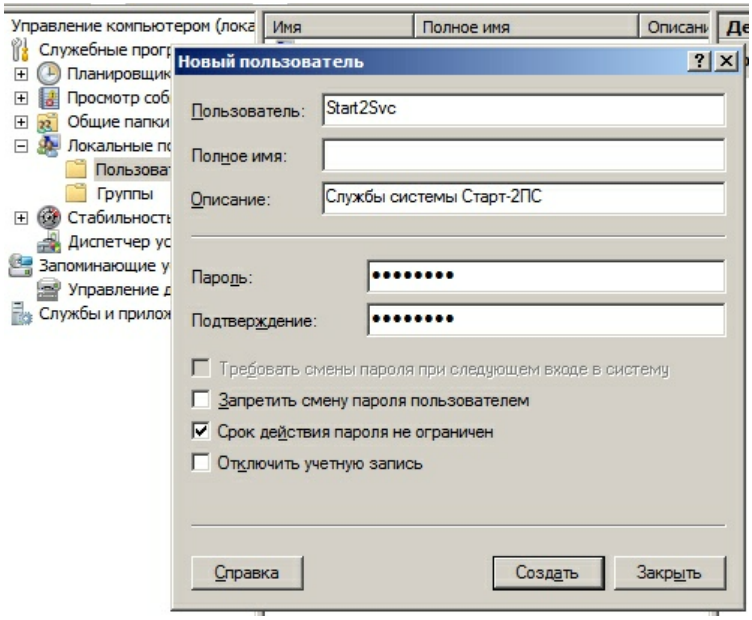


4. Настройте список пользователей Windows. Если компьютеры локальной сети объединены в рабочую группу, на каждом компьютере системы должен быть создан одинаковый набор учётных записей системы безопасности операционной системы:

4.1.Создайте группу безопасности, члены которой впоследствии получат доступ к функциям системы "Старт-2ПС", рекомендуемое имя - «Start2Users». Для этого запустите диалог управления компьютером "Пуск --> Администрирование --> Управление компьютером". Выберете в дереве "Служебные программы --> Локальные пользователи и группы --> Группы". Создайте группу (вызов диалога - правой кнопкой мыши)

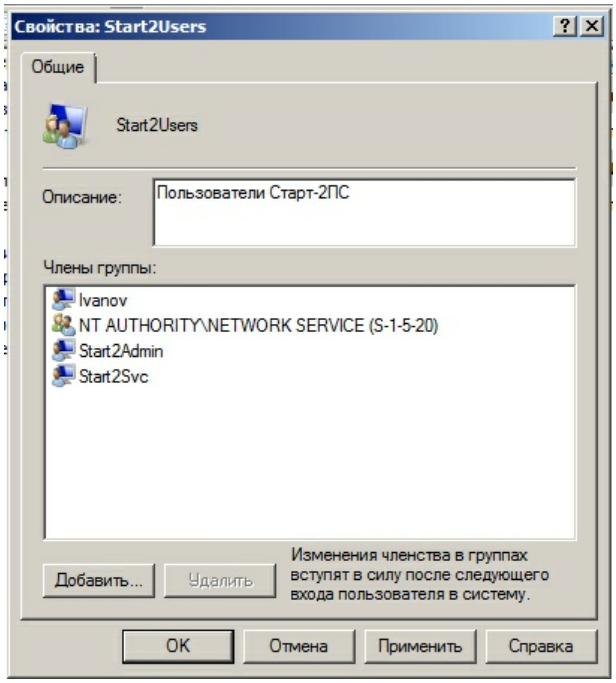


4.2.Создайте учётную запись **с непустым паролем** для служб системы "Старт-2 ПС", рекомендуемое имя - «Start2Svc». Для этого в ветви "Пользователи" щелчком правой кнопки мыши вызовите диалог



4.3.Последовательно заполняя форму и нажимая кнопку "Создать", создайте учётные записи **с непустыми паролями** для администратора системы (рекомендуемое имя «Start2Admin») и для всех операторов системы «Старт-2 ПС» (например, «Ivanov», «Petrov» и пр).

4.4.Включите в группу «Start2Users» только что созданные учетные записи, а также встроенную учётную запись Windows NETWORK SERVICE



4.5.Дополнительно включите учётные записи «Start2Svc», «Start2Admin» в группу «Администраторы». Их членство в группе "Пользователи" можно исключить.

4.6.Проверьте, что учётные записи операторов включены в группу «Пользователи» и "Start2Users" и не включены в группу "Администраторы". Излишние полномочия у операторов системы могут отрицательно сказаться на безопасности и устойчивости работы системы.

5. Запомните имена учётных записей и пароли к ним. Эти имена и пароли должны быть сохранены в безопасном месте.
Примечание: эти сведения рекомендуется внести в распечатанный лист сводки параметров.

6. Настройте параметры безопасности в механизме COM/DCOM. Для этого необходимо:

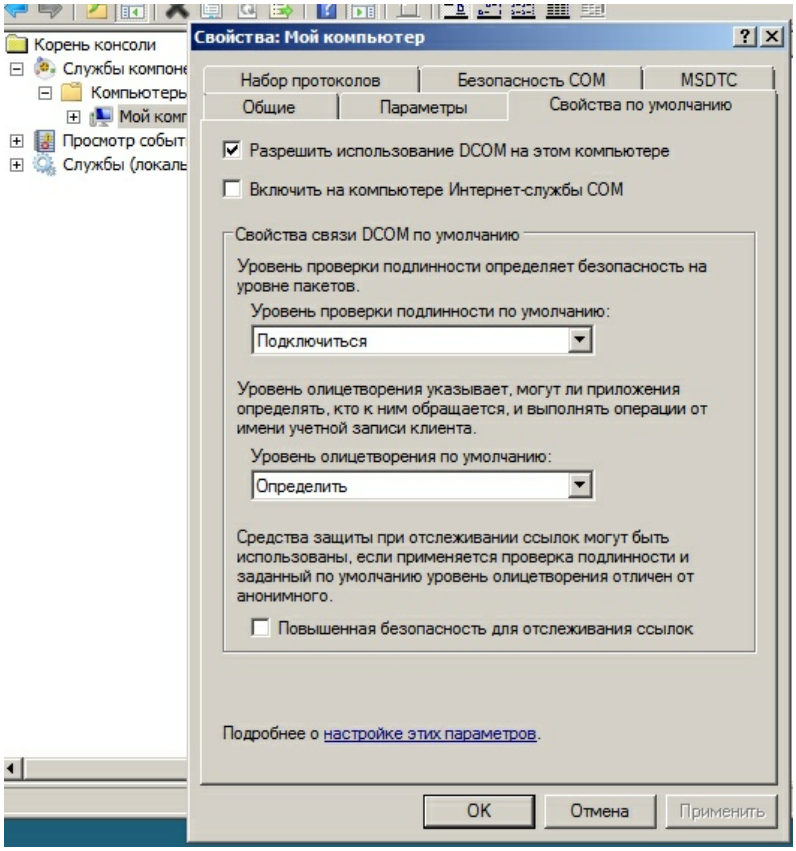
6.1.Запустить оснастку «Службы компонентов»: "Пуск --> Администрирование --> Службы компонентов".

6.2.Убедиться, что параметры вкладки «Свойства по умолчанию» (Службы компонентов --> Компьютеры --> Мой компьютер --> Свойства) имеют следующие значения:

6.2.1.Разрешить исп. DCOM на этом компьютере: вкл

6.2.2.Уровень проверки подлинности по умолчанию: Подключиться

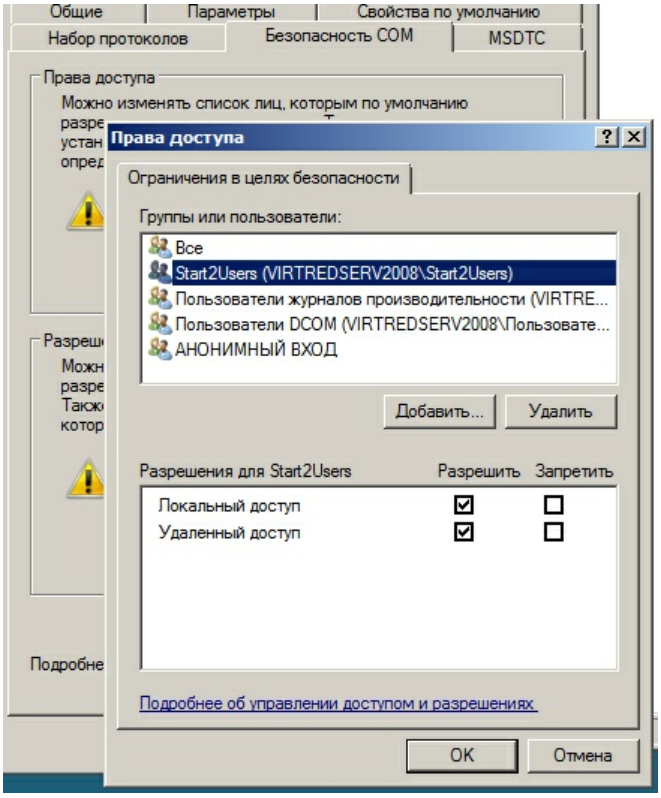
6.2.3.Уровень олицетворения по умолчанию: Определить



6.3.На вкладке «Безопасность COM»

6.3.1.Права доступа --> Кнопка «Изменить ограничения»

6.3.1.1.Добавить группу «Start2Users»



6.3.1.2.Разрешить ей

6.3.1.2.1.«Локальный доступ»

6.3.1.2.2.«Удалённый доступ»

6.3.1.3.Убедиться в том, что «АНОНИМНЫЙ ВХОД» имеет разрешение «Локальный доступ»

6.3.1.4.Убедиться в том, что группа «Все» имеет разрешения

6.3.1.4.1.«Локальный доступ»

6.3.1.4.2.«Удалённый доступ»

6.3.2.Права доступа --> Кнопка «Изменить умолчания»

6.3.2.1.Добавить группу «Start2Users»

6.3.2.2.Разрешить ей

6.3.2.2.1.«Локальный доступ»

6.3.2.2.2.«Удалённый доступ»

6.3.2.3.Убедиться в том, что «SELF» имеет разрешения

6.3.2.3.1.«Локальный доступ»

6.3.2.3.2.«Удалённый доступ»

6.3.2.4.Убедиться в том, что «SYSTEM» имеет разрешение

6.3.2.4.1.«Локальный доступ»

6.3.3.Разрешение на запуск и активацию --> Кнопка «Изменить ограничения»

6.3.3.1.Добавить группу «Start2Users»

6.3.3.2.Разрешить ей

6.3.3.2.1.«Локальный запуск»

6.3.3.2.2.«Удалённый запуск»

6.3.3.2.3.«Локальная активация»

6.3.3.2.4.«Удалённая активация»

6.3.3.3.Убедиться в том, что группа «Администраторы» имеет разрешения

6.3.3.3.1.«Локальный запуск»

6.3.3.3.2.«Удалённый запуск»

6.3.3.3.3.«Локальная активация»

6.3.3.3.4.«Удалённая активация»

6.3.3.4.Убедиться в том, что группа «Все» имеет разрешения

6.3.3.4.1.«Локальный запуск»

6.3.3.4.2. «Локальная активация»

6.3.4.Разрешение на запуск и активацию --> Кнопка «Изменить умолчания»

6.3.4.1.Добавить группу «Start2Users»

6.3.4.2.Разрешить ей

6.3.4.2.1.«Локальный запуск»

6.3.4.2.2.«Удалённый запуск»

6.3.4.2.3.«Локальная активация»

6.3.4.2.4.«Удалённая активация»

6.3.4.3.Убедиться в том, что «SYSTEM» имеет разрешения

6.3.4.3.1.«Локальный запуск»

6.3.4.3.2. «Локальная активация»

6.3.4.4.Убедиться в том, что группа «Администраторы» имеет разрешения

6.3.4.4.1.«Локальный запуск»

6.3.4.4.2.«Удалённый запуск»

6.3.4.4.3.«Локальная активация»

6.3.4.4.4.«Удалённая активация»

6.3.4.5.Убедиться в том, что группа «ИНТЕРАКТИВНЫЕ» имеет разрешения

6.3.4.5.1.«Локальный запуск»

6.3.4.5.2. «Локальная активация»

7. Перезагрузите компьютер.
8. Войдите как администратор.

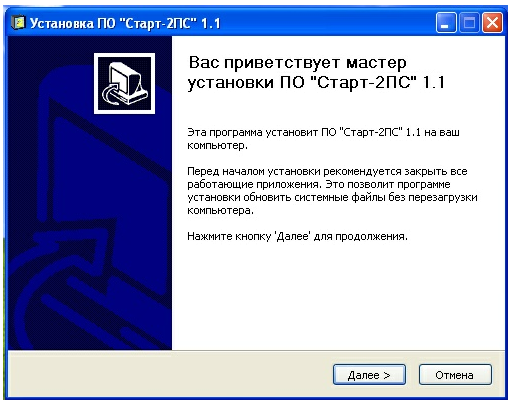
4.2 Установка и удаление системы

4.2.1 Установка Старт-2ПС

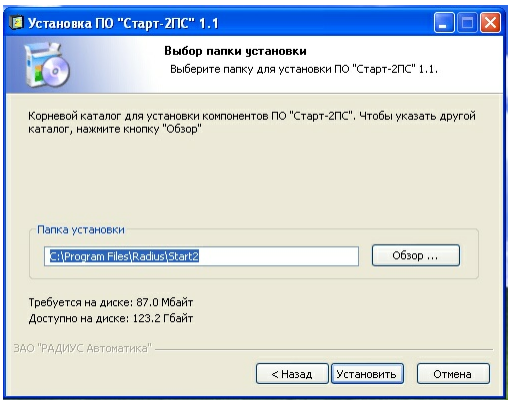
1. Убедитесь в том, что компьютер подготовлен для установки системы Старт-2ПС.
2. Войдите в систему как администратор.
3. Запустите на исполнение программу установки Start2Setup_v_*.* (где *.* - цифры, обозначающие номер версии системы). Программа установки находится в корне

инсталляционного диска.

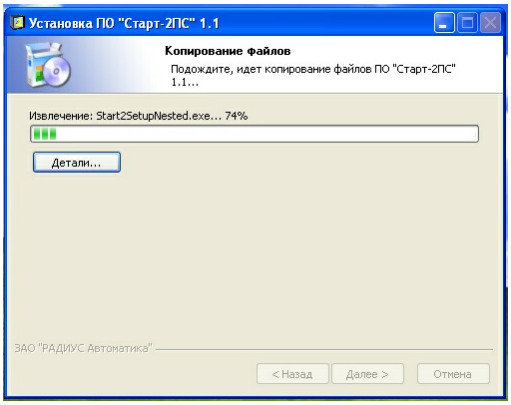
4. В появившемся окне приветствия нажмите кнопку "Далее"



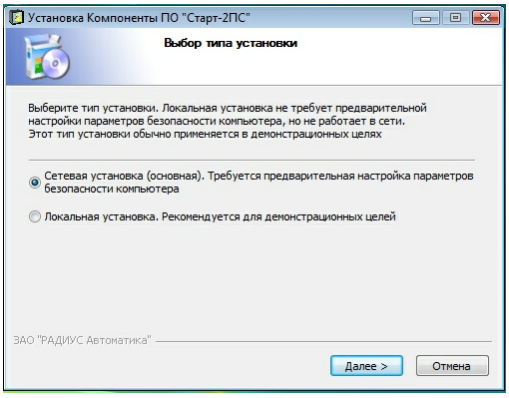
5. В следующем окне предлагается выбрать корневую папку для установки системы. С целью облегчения последующей технической поддержки, не изменяйте предлагаемый вариант без серьёзных оснований



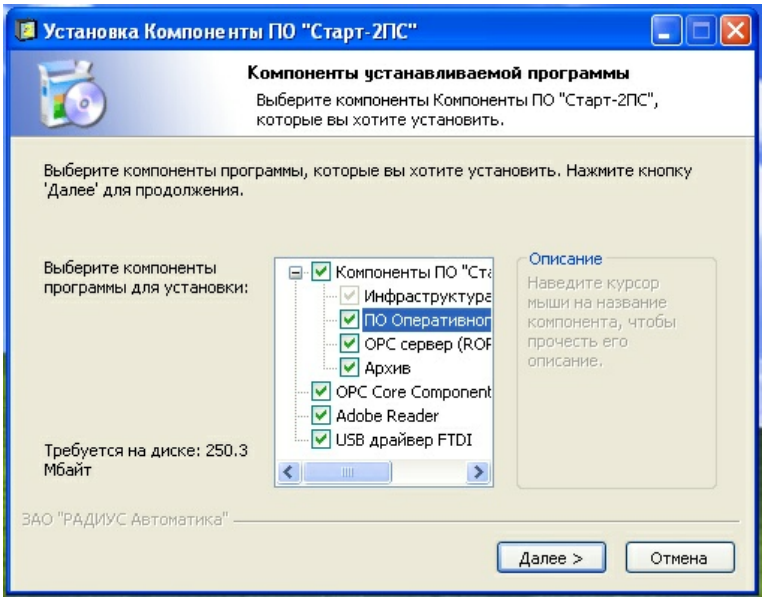
6. По окончании распаковки файлов...



7. ... предлагается выбрать тип установки - сетевая (основная) или локальная установка



8. Далее выдаётся окно для выбора устанавливаемых компонентов



9. Выберите устанавливаемые компоненты в соответствии с требованиями и нажмите кнопку "Далее". К установке предлагаются следующие компоненты системы:

9.1."ПО Оперативного контроля" - Программа оперативного контроля.

9.2."ОРС сервер (ROPC)" - Сервер терминалов РЗА (ROPC).

9.3."Архив" - Хранилище и генератор отчётов.

9.4."Инфраструктура" - компоненты инфраструктуры (служба сетевого информатора, шаблоны и пр.). Отменить установку инфраструктуры нельзя.

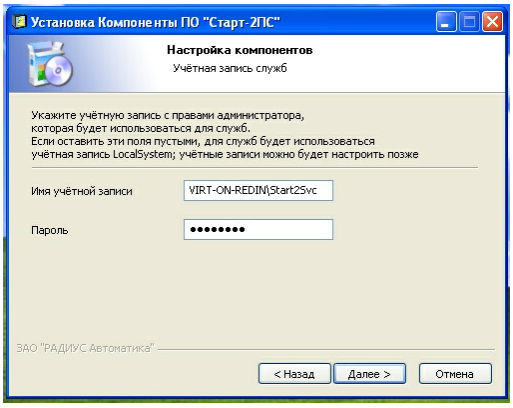
9.5.OPC Core Components - компоненты ядра OPC, функции которого используются всеми компонентами системы. Если компоненты ядра были установлены ранее, повторную установку можно не производить.

9.6.Adobe Reader - компонент, предназначенный для отображения и печати файлов в PDF-формате. Если на данном компьютере предполагается просматривать отчёты, генерируемые генератором отчётов хранилища, этот компонент нужно установить. Если Adobe Reader был установлен ранее, его установку можно не производить. Установка компонента введена в программу установки только для

удобства.

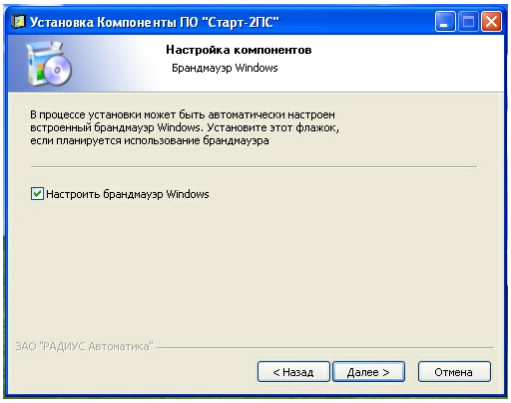
9.7. USB драйвер FTDI - компонет, представляющий собой набор файлов для установки драйвера FTDI. Эти файлы будут размещены в подкаталоге FTDI папки установки. Драйвер FTDI имеет смысл устанавливать, если предполагается подключать к этому компьютеру оборудование посредством интерфейса USB. Установка компонента введена в программу установки только для удобства.

10. Если выбран сетевой тип установки, в следующем окне предлагается указать имя и пароль учётной записи, под которой будут работать службы системы (это служба ROPC - один из модулей компонента сервера терминалов РЗА и служба Start2. StroreService - один из модулей компонента Хранилище). Именно для этого в разделе подготовки компьютера предусматривалось создание учётной записи "Start2Svc". Если оставить поля пустыми (не рекомендуется), службы будут настроены для работы под локальной учётной записью, но взаимодействие с ними будет невозможно из-за настроек безопасности. Однако, учётную запись для этих служб можно будет назначить и позже. Имя учётной записи должно быть введено в формате <имя компьютера>\<имя учётной записи> для локальной учётной записи или <имя домена>\<имя учётной записи> для доменной учётной записи. Для упрощения ввода имени учётной записи, окно предлагает заранее заполненный шаблон



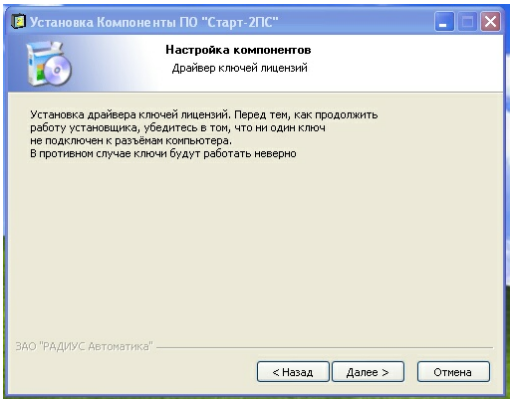
11. В следующем окне будет предложено автоматически настроить брандмауэр Windows. Если использование брандмауэра Windows вообще не планируется (не рекомендуется) или используется продукт стороннего производителя, отмените настройку.

ПРИМЕЧАНИЕ: если используется брандмауэр стороннего производителя, его настройку придётся выполнить вручную. При настройке списка разрешений брандмауэра воспользуйтесь контрольным листом настройки



12.В следующем окне предлагается убедиться, что ключ лицензий не установлен в разъёмы компьютера. В противном случае установка драйвера ключа может завершится с ошибкой или ключ будет работать неправильно.

ПРИМЕЧАНИЕ: если эта ошибка была всё-таки допущена или по каким - то другим причинам ключ не работает, драйвер ключа может быть установлен позже. Установочные файлы копируются в подкаталог Guardant папки установки.

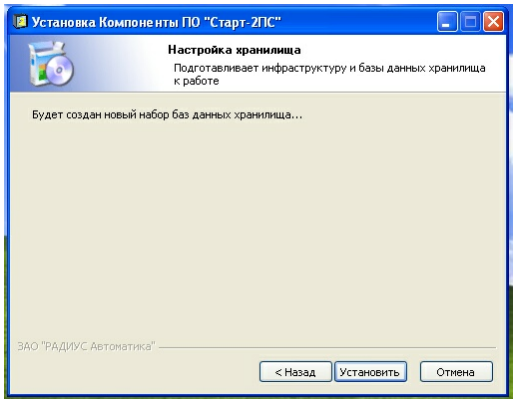


13.Начинается процесс установки

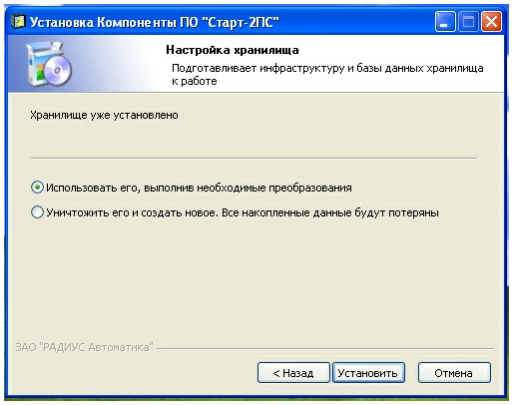
14.В процессе установки, в зависимости от выбранной конфигурации будут выдаваться дополнительные окна. Некоторые из них не требуют реакции (отображают прогресс), другие требуют подтверждения или выбора

14.1.Установка хранилища

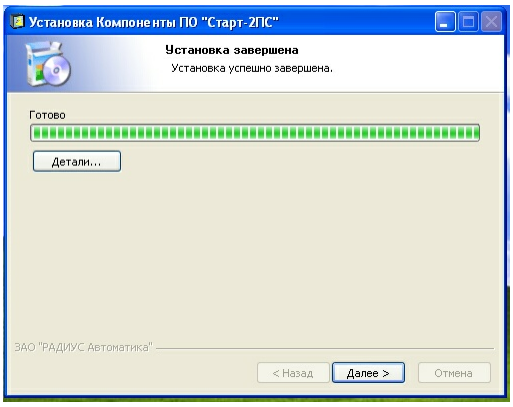
14.1.1.Если на данном компьютере хранилище устанавливается впервые, выдаётся окно, информирующее о намерении создать новые базы данных хранилища



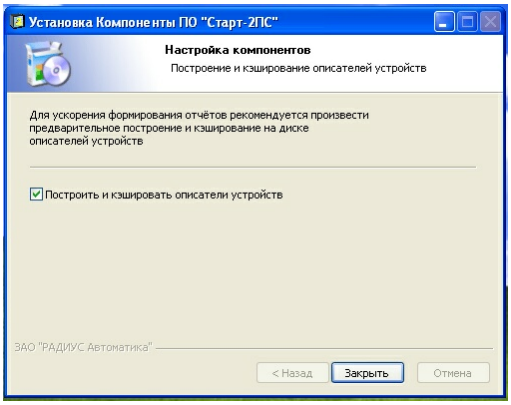
14.1.2.Если на данном компьютере обнаружено существующее хранилище, выдаётся запрос на его использование (с сохранением всех накопленных архивных данных) или на создание нового взамен существующего



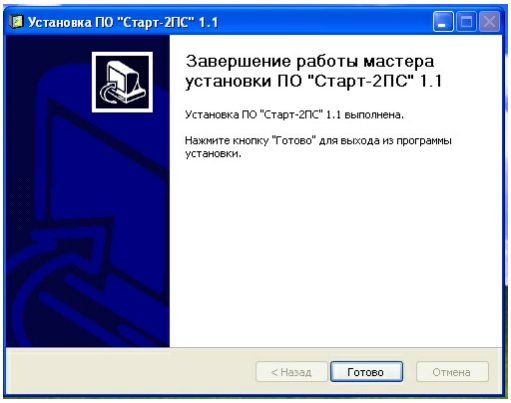
15.По окончании установки компонентов может быть произведена их автоматическая настройка. Нажмите кнопку "Готово" для продолжения



16.Для ускорения формирования страниц генератора отчётов рекомендуется построить и кэшировать (сохранить с контрольной суммой) описатели устройств. Это длительная операция (занимает несколько минут). Если в этом окне отменить операцию кэширования (не рекомендуется), процесс установки завершится быстрее, однако вызовет заметные задержки при построении страниц отчётов (особенно при первом вызове страниц), т.к. кэширование будет выполняться при запросе страницы, "на лету".



17.Обязательно дождитесь итогового окна, сообщающего об окончании установки



4.2.2 Установка системы поверх существующей

С целью обновления версии системы Старт-2ПС или для исправления дефектов предыдущей установки допускается устанавливать новую копию системы поверх существующей. Для этого используется та же самая установочная программа.

Особенности установки новой копии поверх существующей:

- Возможно, что в установке будет отказано. Это может произойти, например, при попытке установки более низкой, чем установлена, версии системы, если нет возможности автоматически привести текущие настройки и базы данных в нужное состояние;
- Все ранее установленные компоненты Старт-2ПС обновляются, отменить их установку в этом режиме нельзя (установка опционных компонентов может быть отменена);
- Если обнаружено действующее хранилище, будет предложено использовать его, при необходимости выполнив нужные преобразования. На такие преобразования может потребоваться некоторое время;
- Перед началом установки требуется завершить работу всех программ комплекса (ПО оперативного контроля, конфигуратор ROPC);

- Рекомендуется остановить службы Start2.StoreService и Start2.NetInformer. Это необязательная рекомендация, но её выполнение позволяет лучше сохранить данные и ускорить процесс. Кроме того это исключает нежелательные побочные эффекты от извлечения ключа лицензий "на лету";
- Перед началом установки не забывайте извлекать ключ лицензии.

4.2.3 Удаление системы или её компонентов

Для удаления системы или отдельных компонентов используется стандартная оснастка Windows: "Панель управления --> Установка и удаление программ".

Особенности работы программы удаления:

- Если в процессе удаления компонентов будут выбраны все компоненты Старт-2ПС, также удаляется и инфраструктура системы.
- При удалении компонента "Хранилище " предлагается сохранить базы данных для использования в будущем. Если это не требуется, выберите вариант с полным удалением баз данных; это освободит место на жёстком диске.

4.3 Конфигурирование программного обеспечения

Конфигурирование программного обеспечения рассмотрено в документе "Программное обеспечение Старт-2ПС Руководство оператора 643.БПВА.10002-01 34"

5 Административные настройки

Данный раздел содержит сведения, предназначенные для системных администраторов и подразумевает наличие у административного персонала соответствующей подготовки.

В разделе описываются особенности развёртывания и функционирования системы в конфигурациях, отличных от конфигурации, описанной в разделе "Подготовка компьютера для установки системы".

5.1 Особенности развёртывания системы в домене

При развёртывании системы в домене, настройки безопасности целесообразно перенести на уровень контроллера домена: вместо локальных групп и учётных записей использовать доменные группы и учётные записи.

Для обеспечения работоспособности системы "Старт-2ПС" следует учитывать следующие соображения:

- Все компоненты системы должны иметь доступ на чтение/изменение по отношению к скрытому каталогу "Document and Settings\All Users\ Application Data\Radius" (Windows XP / Windows Server 2003) или скрытому каталогу "ProgramData\RADIUS" (Windows Vista / Windows 7 / Windows Server 2008) и всем его дочерним. С этой целью программа - установщик назначает полный доступ к нему для локальных групп "Пользователи", "Опытные пользователи" и встроенной учётной записи NETWORK SERVICE. Локальная группа "Администраторы" наследует разрешения от корня. Посредством локальной группы "Пользователи" к этому каталогу также получает доступ учётная запись ASPNET (в Windows XP). В домене Windows по умолчанию все доменные учётные записи включаются (посредством доменных групп) в локальные группы (доменные администраторы - в локальные администраторы, доменные пользователи - в локальные пользователи и пр.). Соответственно, следует иметь в виду, что все учётные записи домена получат доступ к указанному каталогу. Если это нежелательно, измените настройки вручную, назначив полный доступ к каталогу только доменной группе пользователей "Старт-2ПС" (Start2Users).
- Предоставление доступа через DCOM осуществляется посредством адресного назначения группе пользователей "Старт-2ПС" (Start2Users) полных прав на локальные и удалённые действия (запуск, активация и пр.)

- Настройки локальной политики безопасности в домене игнорируются; соответствующие пункты настройки компьютера можно пропустить.
- По умолчанию базы данных компонента "Хранилище" создаются на системном диске, в одном из подкаталогов каталога Program Files. Если это нежелательно, SQL Server 2008 Express нужно устанавливать вручную (вызвать SQLEXPR32_x86_ENU.exe вместо вызова SQLServerExpressSetup.bat). При этом, в одном из диалогов можно указать конкретное место для баз данных.

В остальном в проблемных случаях следует руководствоваться контрольным листом настройки компьютера.

5.2 Настройка компонентов ПО

Задачу конфигурирования системы "Старт-2ПС" можно разделить на две подзадачи:

- Настройка компонентов программного обеспечения (ПО).
- Настройка конфигурации оборудования подстанции.

Настройка компонентов ПО выполняется для обеспечения работоспособности системы в различных сетевых окружениях. Настройка компонентов ПО частично выполняется в процессе подготовки компьютера перед установкой системы, а частично - в процессе работы программы - установщика.

Настройка конфигурации оборудования подстанции подготавливает систему для работы с конкретным оборудованием подстанции, в соответствии с проектом. Процесс настройки конфигурации оборудования описан в документе "Программное обеспечение Старт-2ПС Руководство оператора 643.БПВА.10002-01 34".

Стандартной настройки компонентов ПО в большинстве случаев достаточно для нормальной работы системы. Однако, при необходимости, стандартные установки можно изменить вручную. В настоящем разделе описана методика ручной настройки и содержится описание параметров, которые при этом можно настроить.

5.2.1 Общие сведения о настройке компонентов ПО

Большая часть программных компонентов системы "Старт-2ПС" написана для работы в программной оболочке Microsoft .NET Framework, вследствие чего настройка компонентов ПО "Старт-2ПС" осуществляется по соглашениям, принятым в этой среде.

Конфигурационная информация для приложений .NET Framework хранится в

виде текстового файла в XML формате. В зависимости от области действия, конфигурационная информация может быть сохранена в конфигурационном файле уровня пользователя, уровня приложения и уровня операционной системы.

- Конфигурационный файл уровня пользователя предназначен для хранения конфигурационной информации, действительной только для конкретного пользователя. Этот файл сохраняется в каталоге, содержащем профиль указанного пользователя. Обычно конфигурационный файл уровня пользователя содержит только те настройки, которые специфичны для пользователя; если в нём содержатся настройки, определённые в конфигурационных файлах уровня приложения и уровня операционной системы, он их переопределяет. В системе "Старт-2ПС" конфигурационные файлы уровня пользователя не применяются.
- Конфигурационный файл уровня приложения размещается в каталоге приложения и определяет конфигурацию, действительную для этого приложения. Если в нём содержатся настройки, определённые в конфигурационном файле уровня операционной системы, он их переопределяет. Имя файла конфигурации уровня приложения обычно имеет вид <имя_файла_приложения>.exe.config, например "Start2.StoreService.exe. config".
- Конфигурационный файл уровня операционной системы определяет конфигурацию, действительную для всех приложений и всех пользователей системы, если иное не определено в файлах конфигурации уровня приложения и уровня пользователя. Конфигурационный файл уровня операционной системы размещается в системном каталоге (в настоящее время это каталог "C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727 \CONFIG\" - для 32-х разрядных систем или "C:\WINDOWS\Microsoft. NET\Framework 64\v2.0.50727\CONFIG\" - для 64-х разрядных) и имеет имя "machine.config".

Обычно при поиске конфигурационной информации приложение просматривает конфигурационные файлы в следующем порядке: файл уровня пользователя, файл уровня приложения и, наконец, файл уровня системы. Если нужный параметр в процессе поиска не найден, применяется значение по умолчанию (определённое программистом значение).

5.2.2 Структура файла конфигурации

Файл конфигурации любого из уровней имеет структуру следующего вида:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
      <configSections>
            <!-- Описатели секций конфигурирования -->
            <section name="sectionName1" type="..." .../>
            <section name="sectionName2" type="..." .../>
            ...
            <!-- Описатели групп секций конфигурирования -->
            <sectionGroup name="groupName1" type="..." ...>
                  <!-- Описатели секций конфигурирования в группе -->
                  <section name="sectionName3" type="..." .../>
                  <section name="sectionName4" type="..." .../>
                  ...
            </sectionGroup>
      </configSections>

      <!-- Секции конфигурирования -->
      <sectionName1 paramName1="paramValue" paramName2="paramValue" ... />
      <sectionName2 paramName1="paramValue" paramName2="paramValue">
            <!-- Дочерние элементы секции -->
      </sectionName2>

      <!-- Секции конфигурирования в группе -->
      <groupName1>
            <sectionName3 paramName1="paramValue" paramName2="paramValue" ... />
            <sectionName4 paramName1="paramValue" paramName2="paramValue" ... />
      </groupName1>
</configuration>
```

Создавать файлы конфигурации вручную, как правило, не требуется - эти файлы создаются автоматически, при инсталляции системы. Процесс ручного конфигурирования заключается в редактировании этих файлов с помощью текстового редактора, например, штатного Notepad операционной системы.

ПРИМЕЧАНИЕ: В операционных системах MS Windows Vista, MS Windows 7 и MS Windows Server 2008 программу - редактор необходимо вызывать в режиме "От имени администратора", даже если Вы работаете под учётной записью с административными правами.

Конфигурация описывается в узле <configuration> XML файла. Этот узел является корневым.

Узел <configSections> содержит узлы <section> описателей секций конфигурирования и узлы <sectionGroup> описателей групп секций конфигурирования. Секции конфигурирования могут быть самостоятельными или могут быть вложены в описатели групп.

Узлы <section> и <sectionGroup> содержат обязательные атрибуты "name" и "type". С помощью этих атрибутов секция или группа идентифицируется в XML документе, и ей присваивается тип. Атрибут "type" может иметь несколько форматов. Минимально строка типа должна состоять из имени типа и имени сборки, разделённые запятыми. Именно в этом формате дано описание типов в настоящем документе. Узел может содержать и другие (необязательные) атрибуты, их назначение описано в документации MSDN, например на сайте http://msdn.microsoft.com в разделе .NET Framework.

В узле <configuration>, но после узла <configSections> размещаются сами секции конфигурирования (в нашем примере - "sectionName1" и "sectionName2"). Если описатель секции в верхней части документа размещён в описателе группы, секция конфигурирования должна быть описана в качестве дочернего узла в узле с именем группы (в нашем примере - "sectionName3" и "sectionName4" описаны в узле "groupName1").

Как правило, конфигурируемые параметры секции конфигурирования описываются атрибутами XML узла вида paramName="paramValue", но в некоторых случаях конфигурируемые параметры могут описываться дочерними узлами секции (секция "sectionName2").

Процесс ручного редактирования заключается в редактировании списка описателей группы и/или секции конфигурирования в узле <configSections> и редактировании (или добавлении) узлов групп и секций конфигурирования в нижней части XML документа.

ПРИМЕЧАНИЕ: При вводе данных необходимо соблюдать регистр букв.

5.2.3 Настройки уровня операционной системы

Конфигурационный файл уровня операционной системы в текущей версии операционных систем размещается в каталоге "C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\CONFIG\" (для 32-х разрядных систем) или "C:\WINDOWS\Microsoft.NET\Framework 64\v2.0.50727\CONFIG\" (для 64-х разрядных систем) и имеет имя "machine.config". Для его редактирования в ОС MS Windows Vista, MS Windows 7 и MS Windows Server 2008 программу - редактор необходимо вызывать в режиме "От имени администратора", даже если Вы работаете под учётной записью с административными правами.

Ниже приведены параметры конфигурирования, имеющие отношение к системе "Старт-2ПС".

- <sectionGroup name="**start2**" type="Start2.Net.Start2ConfigGroup, Start2.Net" />, описатель группы секций системы "Старт-2ПС"
  - <section name="**start2Config**" type="Start2.Net.Start2Config, Start2.Net" />, описатель секции сетевых настроек системы, параметры
    - **id** - идентификатор системы, строка. Предназначен для нужд автоматического взаимообнаружения других компьютеров системы (узлов системы) в локальной сети. Значение параметра должно содержать строку (латиница), однозначно идентифицирующую имя системы. Для создания организационных групп эта строка может содержать несколько имён, разделённых запятыми; в одну организационную группу входят системы, у которых в списке имён есть совпадающие имена. Значение по умолчанию: "Default". Пример настройки - см. ниже.
    - **broadcastEnabled** - разрешение работы механизма взаимообнаружения, построенного на основе широковещательного обмена. Значение по умолчанию: "true". Присвоение значения "false" выключает этот механизм. При такой настройке в состав системы включается только данный узел и узлы, указанные в списке статически заданных узлов (см. **staticHosts**). Параметр id и все параметры настройки широковещательного обмена при этом игнорируются.
    - **broadcastPort** - номер порта широковещательного обмена между узлами, целое число. Используется в механизме взаимообнаружения; на всех компьютерах системы должно использоваться одинаковое значение. Значение по умолчанию: 6000.
    - **multicastGroupAddress** - групповой адрес для широковещательного обмена, строка, кодирующая IP-адрес. Используется в механизме взаимообнаружения; на всех компьютерах системы должно использоваться одинаковое значение. Значение по умолчанию: "224.0.0.1".
    - **broadcastPeriod** - периодичность рассылки широковещательных сообщений в сек., целое число больше нуля. Используется в механизме взаимообнаружения. Значение по умолчанию: 5.
    - **maxLostBroadcastMsg** - максимально допустимое количество потеряных широковещательных пакетов, после превышения которого делается вывод о неисправности узла, целое число больше нуля. Используется в механизме взаимообнаружения. Значение по умолчанию: 3.

- Дочерний узел **staticHosts** - список статически заданных узлов системы. Узлы, указанные в списке, включаются в состав системы принудительно, минуя механизм взаимообнаружения. Это позволяет подключать компьютеры, недоступные для широковещательного обмена (например, находящиеся в другой подсети TCP/IP), а также в случаях, когда механизм взаимообнаружения выключен по требованию корпоративной политики локальной сети. Каждый статически заданный узел включается в узел "staticHosts" в качестве дочернего элемента вида <add name="имя_узла" ... />, где обязательным атрибутом является атрибут "name", задающий имя компьютера (без доменного префикса), а остальные атрибуты должны быть такие же, как в секции "hostDescriptor" компьютера, включаемого в список. Кроме того, может быть задан атрибут "staticIPAddr", содержащий действительный статический IP-адрес этого узла (строка вида "192.168.0.33"). Злоупотреблять этим атрибутом не следует, т.к. при его наличии служба DNS локальной сети не используется и вероятны проблемы после изменения сетевого адреса узла. Основное назначение атрибута - добиться работоспособности системы в сетях со статическими IP-адресами при ненадёжной работе DNS.

- <section name="**hostDescriptor**" type="Start2.Net.HostDescriptorConfig, Start2.Net" />, описатель секции сетевых настроек узла, параметры
  - **timeout** - таймаут клиентского подключения службы сетевого информатора в миллисек., целое число больше нуля. Значение по умолчанию: 10000.
  - **port** - номер порта для клиентского соединения службы сетевого информатора, целое число больше нуля. Значение по умолчанию: 5000.
- <section name="**clientDescriptor**" type="Start2.Net.ClientDescriptorConfig, Start2.Net" />, описатель секции сетевых параметров ПО Оперативного контроля, параметры
  - **appName** - имя приложения, строка. Указанное имя будет использовано при протоколировании работы программного компонента, а также выведено в заголовок главного окна приложения. Значение по умолчанию - "Оперативный Контроль".
  - **componentId** - идентификатор приложения, строка, представляющая GUID. Уникально идентифицирует программный компонент в системе. Устанавливается автоматически при инсталляции, значения по умолчанию нет.
  - **port** - номер порта для вызова служб компонента, целое число больше нуля. Резерв.

- **timeout** - таймаут клиентского подключения к службам компонента в миллисек., целое число больше нуля. Резерв.

- <section name="**storeServiceDescriptor**" type="Start2.Net. StoreServiceDescriptorConfig, Start2.Net" />, описатель секции сетевых настроек хранилища, параметры
  - **appName** - имя приложения, строка. Указанное имя будет использовано при протоколировании работы программного компонента. Значение по умолчанию: "Архив".
  - **componentId** - идентификатор приложения, строка, представляющая GUID. Уникально идентифицирует программный компонент в системе. Устанавливается автоматически при инсталляции, значения по умолчанию нет.
  - **port** - номер порта для вызова служб компонента, целое число больше нуля. Значение по умолчанию: 5001.
  - **timeout** - таймаут клиентского подключения к службам компонента в миллисек., целое число больше нуля. Значение по умолчанию: 10000.
  - **webReporterUrl** - URL начальной страницы генератора отчётов, строка, кодирующая URL. Значение по умолчанию: "Start2.WEBReporter"
- <section name="**ropcDescriptor**" type="Start2.Net.ROPCDescriptorConfig, Start2.Net" />, описатель секции сетевых настроек сервера терминалов РЗА (ROPC), параметры
  - **appName** - имя приложения, строка. Указанное имя будет использовано при протоколировании работы программного компонента. Значение по умолчанию: "OPC сервер ROPC".
  - **componentId** - идентификатор приложения, строка, представляющая GUID. Уникально идентифицирует программный компонент в системе. Устанавливается автоматически при инсталляции, значения по умолчанию нет.
  - **port** - номер порта для вызова служб компонента, целое число больше нуля. Резерв.
  - **timeout** - таймаут клиентского подключения к службам компонента в миллисек., целое число больше нуля. Резерв.
  - **path** - путь к COM-серверу приложения, строка. Значение по умолчанию: "ROPC/{FCC7ECAB-7129-4A77-9A9E-F8483DF523CB}"

5.2.3.1 Примеры настройки уровня операционной системы

5.2.3.1.1 Пример настройки организационных групп

Пример настройки идентификатора системы для создания организационных групп. Пусть данный компьютер требуется включить в организационные группы "35kV" и "110kV".

- Запустите редактор Notepad операционной системы (для MS Windows Vista и MS Windows 7 его нужно запустить от имени администратора - правой кнопкой мыши на иконке в меню).
- Откройте на редактирование файл "C:\WINDOWS\Microsoft. NET\Framework\v2.0.50727\CONFIG\machine.config" ("C:\WINDOWS\Microsoft. NET\Framework 64\v2.0.50727\CONFIG\machine.config")
- Проверьте, что в узле <configSections> содержится узел <sectionGroup> описателя группы секций "start2", а в этом узле есть узел, описывающий саму секцию "start2Config". Атрибут "type" описателей группы и секции может содержать дополнительные сведения о версии, культуре и пр. При ручном создании описателя эти сведения можно не вводить.
- Отредактируйте узел <start2>, добавив в него секцию <start2Config> с параметром id="35kV,110kv":

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <configSections>
    ...
    <sectionGroup name="start2" type="Start2.Net.Start2ConfigGroup, Start2.Net"
>
      <section name="start2Config" type="Start2.Net.Start2Config, Start2.Net" />
    </sectionGroup>
    ...
  </configSections>
  ...
  <start2>
    ...
    <start2Config id="35kV,110kV"/>
    ...
  </start2>
  ...
</configuration>
```

Внесённые изменения вступят в действие после перезагрузки операционной системы.

5.2.3.1.2 Пример настройки статически заданных узлов

Пример настройки списка статически заданных узлов. Механизм взаимообнаружения выключен, на одном из узлов используется нестандартный номер порта:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    <sectionGroup name="start2">
      ...
      <section name="start2Config" type="Start2.Net.Start2Config, Start2.Net"/>
      ...
    </sectionGroup>
  </configSections>

  <start2>
    ...
    <start2Config broadcastEnabled="false" >
      <staticHosts>
        <add name="petrov" />
        <add name="opcserver" port="5010" />
        <add name="operator" />
      </staticHosts>
    </start2Config>
    ...
  </start2>
</configuration>
```

Внесённые изменения вступят в действие после перезагрузки операционной системы.

5.2.4 Настройка службы сетевого информатора

Конфигурационный файл службы сетевого информатора находится в каталоге <каталог установки_Старт-2ПС>\Radius\Start2\NetInformer и имеет имя Start2.NetInformer.exe.config. Для его редактирования в ОС MS Windows Vista, MS Windows 7 и MS Windows Server 2008 программу - редактор необходимо вызывать в режиме "От имени администратора", даже если Вы работаете под учётной записью с административными правами.

Для настройки доступны следующие параметры службы сетевого информатора:

- <section name="**netInformer**" type="Start2.NetInformer.Managment.NetInformerConfig, Start2.NetInformer.Managment" />, описатель секции конфигурирования службы, параметры
  - **writeLogInfo** - управляет разрешением записи в журнал Windows информационных сообщений службы, булевский, возможные значения "true", "false". Значение по

умолчанию: "true".

- **writeLogWarning** - управляет разрешением записи в журнал Windows предупреждающих сообщений службы, булевский, возможные значения "true", "false". Значение по умолчанию: "true".
- **writeLogError** - управляет разрешением записи в журнал Windows сообщений об ошибках службы, булевский, возможные значения "true", "false". Значение по умолчанию: "true".

Пример настройки конфигурации службы, запрещающей запись в журнал Windows информационных сообщений.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    ...
    <section name="netInformer"
      type="Start2.NetInformer.Managment.NetInformerConfig, Start2.NetInformer.
Managment" />
    ...
  </configSections>

  ...
  <netInformer writeLogInfo="false" />
  ...
</configuration>
```

Изменения в настройке вступают в действие после перезапуска службы сетевого информатора или после перезагрузки операционной системы.

5.2.5 Настройка компонента "Хранилище"

Конфигурационный файл компонента "Хранилище" находится в каталоге <каталог установки_Старт-2ПС>\Radius\Start2\StoreService и имеет имя Start2.StoreService.exe.config. Для его редактирования в ОС MS Windows Vista, MS Windows 7 и MS Windows Server 2008 программу - редактор необходимо вызывать в режиме "От имени администратора", даже если Вы работаете под учётной записью с административными правами.

Для настройки доступны следующие параметры компонента "Хранилище":

- <section name="**storeService**" type="Start2.StoreService.Managment.StoreServiceConfSection, Start2.StoreService.Managment" />, описатель секции конфигурирования службы хранилища, параметры
  - **writeLogInfo** - управляет разрешением записи в журнал Windows информационных сообщений службы, булевский, возможные значения "true", "false". Значение по

умолчанию: "false".

- **writeLogWarning** - управляет разрешением записи в журнал Windows предупреждающих сообщений службы, булевский, возможные значения "true", "false". Значение по умолчанию: "true".
- **writeLogError** - управляет разрешением записи в журнал Windows сообщений об ошибках службы, булевский, возможные значения "true", "false". Значение по умолчанию: "true".
- **maintenancePeriod** - периодичность обслуживания хранилища, строка, кодирующая TimeSpan. Значение по умолчанию: "1:0:0" (один час, ноль минут, ноль секунд).

• <section name="**dataStore**" type="Start2.Store.Rules.DataStoreConfSection, Start2.Store.Rules" />, описатель секции конфигурирования хранилища, параметры

- **serverName** - имя сервера баз данных, строка. Значение по умолчанию "(local)\SQLExpress"
- **connStrTemplate** - шаблон строки подключения к SQL-серверу, строка. Значение по умолчанию: "server={0};database={1};Trusted_Connection=sspi; MultipleActiveResultSets=true"
- **registerDbName** - имя базы данных регистра, строка. Значение по умолчанию: "Start2_Register"
- **storageDbBaseName** - базовое имя баз данных-накопителей, строка. Значение по умолчанию: "Start2_Store_"
- **historyDepth** - глубина хранения архива, дней, целое число больше нуля. Значение по умолчанию: 1100. В демо - режиме игнорируется.
- **maxSize** - максимальный объём текущего раздела, Мбайт, целое число больше нуля. Значение по умолчанию: 100.
- **maxHistorySize** - максимальный суммарный объём разделов истории, Мбайт, целое число больше нуля. Значение по умолчанию: 4096.
- **actualMaxAge** - максимальный "возраст" текущего раздела, дней, целое число больше нуля. Значение по умолчанию: 30. В демо - режиме игнорируется.
- **aspLoginName** - имя учётной записи ASP NET (Только для Windows XP), строка. Значение по умолчанию - "ASPNET".

• <section name="**errorBehaviorInformator**" type="Radius.Common.ErrorBehaviorInformatorConfSection, Radius.Common" />, описатель секции

конфигурирования анализатора ошибок, параметры

- **maxErrors** - максимально допустимое количество некритических ошибок с начала работы приложения, целое число. После превышения указанного значения служба останавливается. Значение по умолчанию: -1 (минус один - отключено).
- **maxHourFrequencyErrors** - максимальная частота поступления некритических ошибок, ошибок/час, целое число. После превышения указанного значения служба останавливается. Значение по умолчанию: 1000
- **thresholdErrors** - пороговый коэффициент для параметров maxErrors и maxHourFrequencyErrors ошибки. По достижении порога генерируется предупреждение, число с плавающей запятой. Значение по умолчанию: 0.7

- <section name="**dataKind**" type="Start2.DataProviders.DataKindConfSection, Start2.DataProviders" />, описатель секции конфигурирования разновидностей собираемых данных, параметры,
  - **oscillogram** - включает и выключает функцию сбора осциллограмм от всех устройств, булевский, возможные значения "true", "false". Значение по умолчанию: "true".
  - **event** - включает и выключает функцию сбора событий от всех устройств, булевский, возможные значения "true", "false". Значение по умолчанию: "true".
  - **notify** - включает и выключает функцию сбора уведомлений от всех устройств, булевский, возможные значения "true", "false". Значение по умолчанию: "true".
  - **srab** - включает и выключает функцию сбора срабатываний от всех устройств, булевский, возможные значения "true", "false". Значение по умолчанию: "true".
  - **paramSet** - включает и выключает функцию сбора наборов данных от всех устройств, булевский, возможные значения "true", "false". Значение по умолчанию: "true".

Пример настройки конфигурации компонента, устанавливающий глубину хранения архива 365 дней.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <configSections>
    ...
    <section name="dataStore"
      type="Start2.Store.Rules.DataStoreConfSection,Start2.Store.Rules" />
    ...
  </configSections>

  ...
```

```
  <dataStore historyDepth="365" />
  ...
</configuration>
```

Пример настройки конфигурации компонента, отключающей сбор наборов данных от всех устройств

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
 <configSections>
  ...
  <section name="dataKind"
        type="Start2.DataProviders.DataKindConfSection,Start2.DataProviders" />
  ...
 </configSections>

 ...
 <dataKind oscillogram="true" event="true" notify="true" srab="true" paramSet="false" />
 ...
</configuration>
```

Изменения в настройке вступают в действие после перезапуска службы хранилища или после перезагрузки операционной системы.

6 Устранение неполадок

6.1 Контрольный лист настройки компьютера

После окончания установки на всех компьютерах системы, система должна быть полностью работоспособна и обеспечивать сетевое взаимодействие в полном объёме. Однако после установки обновлений операционной системы, а также после установки другого программного обеспечения, работоспособность системы может быть нарушена.

Для восстановления работоспособности системы «СТАРТ-2ПС» воспользуйтесь следующим контрольным листом, содержащим полный список настраиваемых параметров.

Таблица 1 - Контрольный лист настраиваемых параметров

Контрольный параметр	Win XP/2003	Win Vista/2008	Win 7
Операционная система установлена в полном объёме, назначено имя компьютера и сетевой адрес	К	К	К
Установлен компонент ОС Internet Information Services и все его составляющие (обязательный компонент, если установлено «Хранилище»)	К	К	К
Существует учётная запись ASPNET (если установлено "Хранилище")	К		
Установлен пакет .NET 3.5	К	К	
Компонент IIS операционной системы установлен до установки .NET	К		
Установлен SQL Server 2008 Express Edition (обязательный компонент, если установлено «Хранилище»).	К	К	К
Только для рабочих групп: Настроена локальная политика: «Локальные пользователи удостоверяются как они сами» (обновления операционной системы могут изменить эту настройку).	К	К	К
Включен общий доступ к файлам и принтерам	К		
Включено сетевое обнаружение		К	К
Брандмауэр разрешает: Общий доступ к файлам и принтерам	К		
Брандмауэр разрешает: Сетевое обнаружение		К	К
Брандмауэр разрешает: Порт «DCOM», TCP, 135	К	К	К
Брандмауэр разрешает: Программа «Сервер терминалов РЗА» (ROPC), если этот компонент установлен	К	К	К
Брандмауэр разрешает: Программа «ПО Оперативного контроля» (если этот компонент установлен)	К	К	К
Брандмауэр разрешает: Программа «Start2.StoreService», если установлен компонент «Хранилище»	К	К	К
Брандмауэр разрешает: Порт « UDP 6000», UDP, 6000	К	К	К
Брандмауэр разрешает: Порт « TCP 5000», TCP, 5000	К	К	К
Брандмауэр разрешает: Порт « TCP 5001», TCP, 5001, если установлен компонент «Хранилище»	К	К	К
Брандмауэр разрешает: Порт «TCP 80», TCP, 80, если установлен компонент «Хранилище»	К	К	К
Только для рабочих групп: На всех компьютерах, входящих в систему, создан одинаковый набор учётных записей системы безопасности операционной системы. Обеспечивается попарное совпадение параметров ИМЯ УЧЁТНОЙ ЗАПИСИ/ПАРОЛЬ. Регистр букв для пароля должен полностью	К	К	К

Контрольный параметр	Win XP/2003	Win Vista/2008	Win 7
соблюдаться			
Группы безопасности "Пользователи", "Опытные пользователи", "Администраторы" и учётная запись NETWORK SERVICE имеют доступ, как минимум, по чтению/изменению к каталогу "Document and Settings\All Users\Application Data\Radius" и ко всем его дочерним каталогам	К		
Группы безопасности "Пользователи", "Опытные пользователи", "Администраторы" и учётная запись NETWORK SERVICE имеют доступ, как минимум, по чтению/изменению к каталогу "ProgramData\RADIUS" и ко всем его дочерним каталогам		К	К
Настроены параметры безопасности в механизме COM/DCOM	К	К	К
Только для рабочих групп: **Службы ROPC и Start2.StoreService стартуют от имени учётной записи «Start2Svc»**.	К	К	К
В системном журнале отсутствуют ошибки источников COM и DCOM (разделы «Приложения» и «Система»).	К	К	К

Примечания

- "К" - параметр применим и контролируется;
- При использовании брандмауэра сторонних производителей (например, в составе антивирусного ПО), необходимые разрешения должны быть настроены в нём вручную.

7 Часто задаваемые вопросы

7.1 Что такое демо-режим?

Демо-режим предназначен для демонстрации основных функций системы с целью помочь в принятии решения о приобретении нужного количества лицензий.

Демо-режим работы системы включается при первом запуске ПО без ключа лицензий. После первого запуска ПО с установленным ключом лицензий система переходит в лицензионный режим. Демо-режим работы системы отличается следующими особенностями:

- Программа оперативного контроля отображает только локальный узел;
- Не работают мнемосхемы;
- Глубина хранения данных в архивах хранилища составляет одни сутки;
- Время работы в демо-режиме не ограничено.

Если в процессе работы системы в лицензионном режиме ключ лицензий был извлечён, то происходит следующее:

- Программа оперативного контроля продолжает работать, но останавливается в непредсказуемый момент времени;
- При повторном запуске программы оперативного контроля она работает в демо-режиме;
- Служба хранилища останавливается. В системном журнале служба сообщает о внезапном изъятии ключа и невозможности дальнейшей работы;
- При попытке повторного запуска службы хранилища она не запускается. Это сделано с целью предотвратить потерю данных, накопленных во время работы в лицензионном режиме.

Если система внезапно перешла в демо-режим, следует проверить, вставлен ли ключ лицензий в USB-разъём компьютера. Если ключ вставлен, попробуйте переустановить драйвер ключа.

Для этого:

- **Извлеките ключ из разъёма**

- Запустите программу установки драйвера. Программа установки Setup.exe находится в подкаталоге Guardant\Drivers корневого каталога установки
- После окончания установки вставьте ключ и проверьте, что он правильно определяется Windows.

7.2 Как узнать версию системы?

Чтобы узнать версию системы, нужно воспользоваться оснасткой Windows, управляющей установкой и удалением программ.

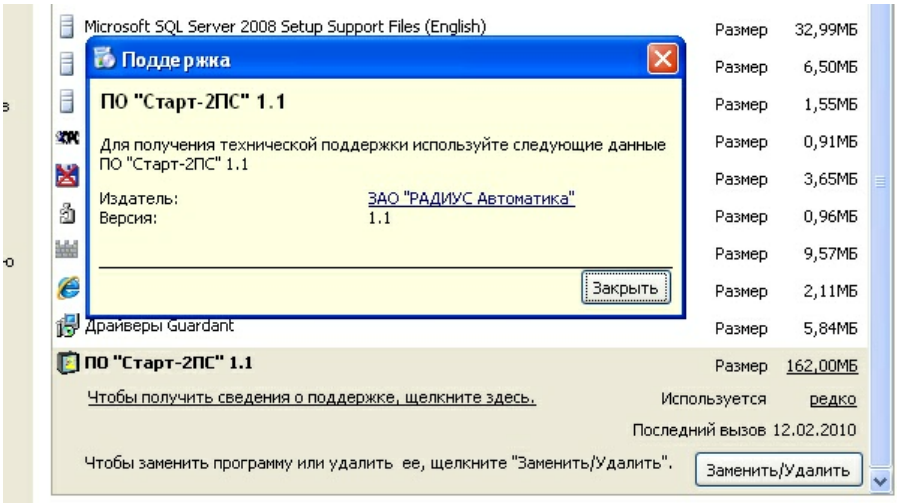
1. Windows XP:

1.1."Панель управления --> Установка и удаление программ"

1.2.В появившемся списке найти элемент вида "ПО Старт-2ПС 1.1", где 1.1 - искомая версия ПО

1.3.Для ознакомления с подробностями щелкните по ссылке "Чтобы получить сведения о поддержке щёлкните здесь"

1.4.Сведения о версии и другие подробности появятся во всплывшем окне

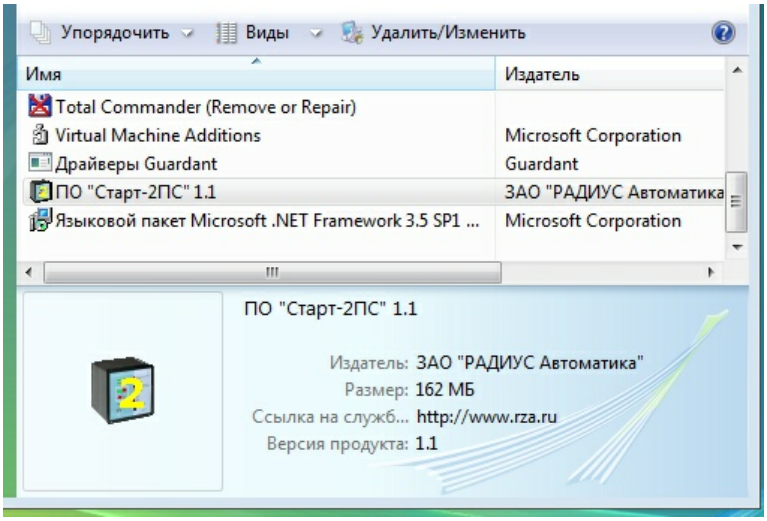


2. Windows Vista:

2.1."Панель управления --> Программы и компоненты"

2.2.В появившемся списке найти элемент вида "ПО Старт-2ПС 1.1", где 1.1 - искомая версия ПО

2.3.Подробности приведены в нижней панели. Если панель подробностей не видна, включите её следующим образом: "Упорядочить --> Раскладка --> Панель подробностей"

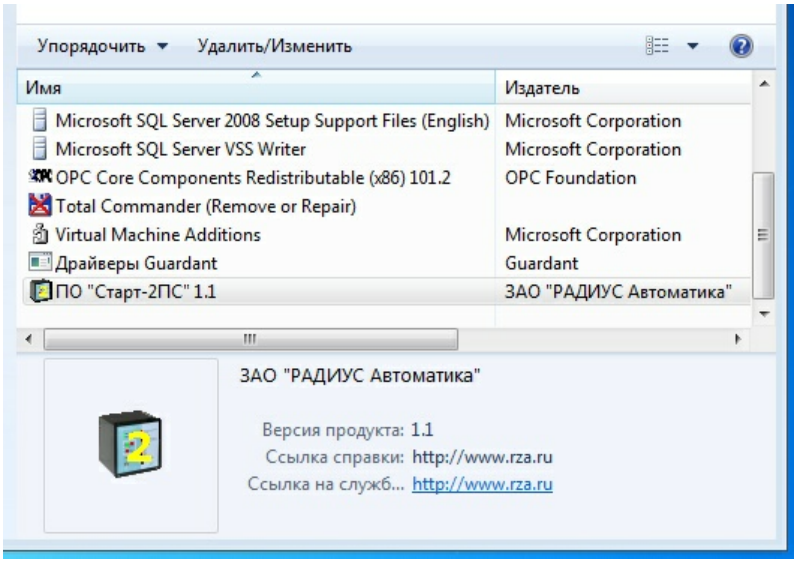


3. Windows 7

3.1."Панель управления --> Программы и компоненты"

3.2.В появившемся списке найти элемент вида "ПО Старт-2ПС 1.1", где 1.1 - искомая версия ПО

3.3.Подробности приведены в нижней области сведений. Если область сведений не видна, включите её следующим образом: "Упорядочить --> Представление --> Область сведений"



7.3 Как убрать окно приветствия при запуске Windows XP?

При работе компьютера в составе рабочей группы при старте Windows XP отображается окно приветствия

Это не всегда удобно, т.к. в нём одновременно отображаются иконки для всех учётных записей системы, в том числе административных и служебных. Кроме того, при этом повышается риск взлома системы злоумышленниками. При необходимости, можно настроить Windows, чтобы взамен окна приветствия отображалось окно ввода имени учётной записи и пароля. Для этого, в системе:

- Запустить "Панель управления --> Учётные записи пользователей --> Изменение входа пользователей в систему"
- Снять флажок "Использовать страницу приветствия"
- Нажать кнопку "Применение параметров"
- В результате, при следующем входе в систему будет отображаться окно стандартного входа с вводом имени и пароля

7.4 Где найти диагностические сообщения системы?

Диагностические сообщения системы некоторых компонентов "Старт-2ПС" записываются в системный журнал Windows, к которому можно получить доступ, например, через панель управления: "Панель управления --> Администрирование -->

Просмотр событий".

Выберите и откройте журнал с именем "Start 2" - для доступа к основному журналу системы "Старт-2ПС", и "Radius" - для доступа к журналу службы аварийного контроля.

7.5 Как управлять службами Windows?

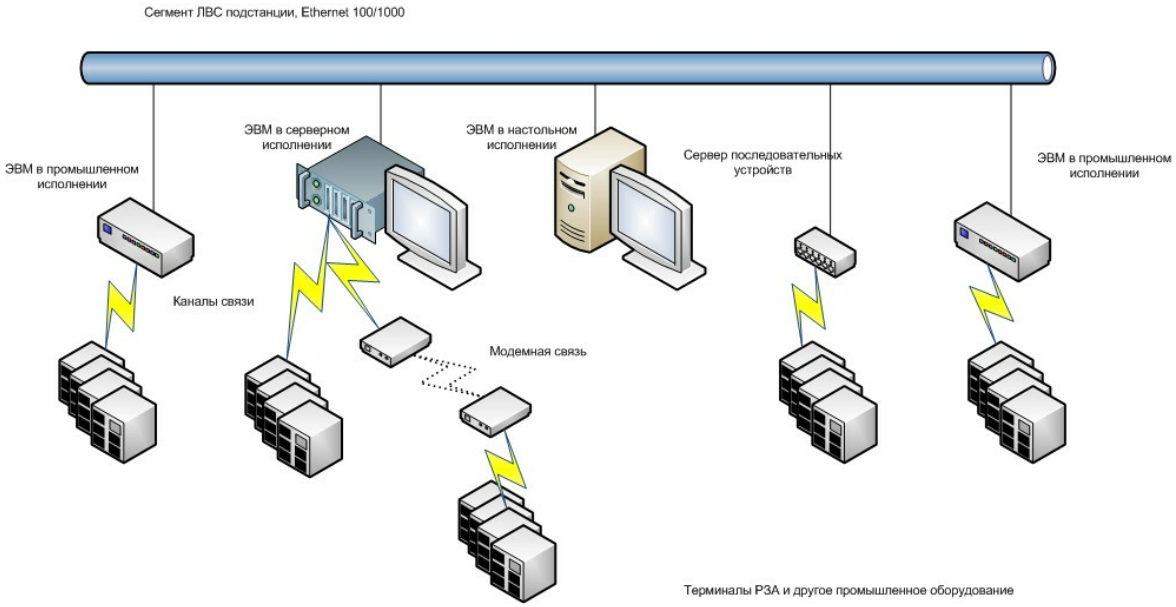
Для управления службами Windows необходимо войти в систему в качестве администратора. Доступ к оснастке служб можно получить, например, через панель управления: "Панель управления --> Администрирование --> Службы". Выбрав службу в списке, можно управлять её состоянием: запускать и останавливать, управлять свойствами и пр.

Для справки: В качестве служб Windows в системе "Старт-2ПС" устанавливаются следующие программные компоненты

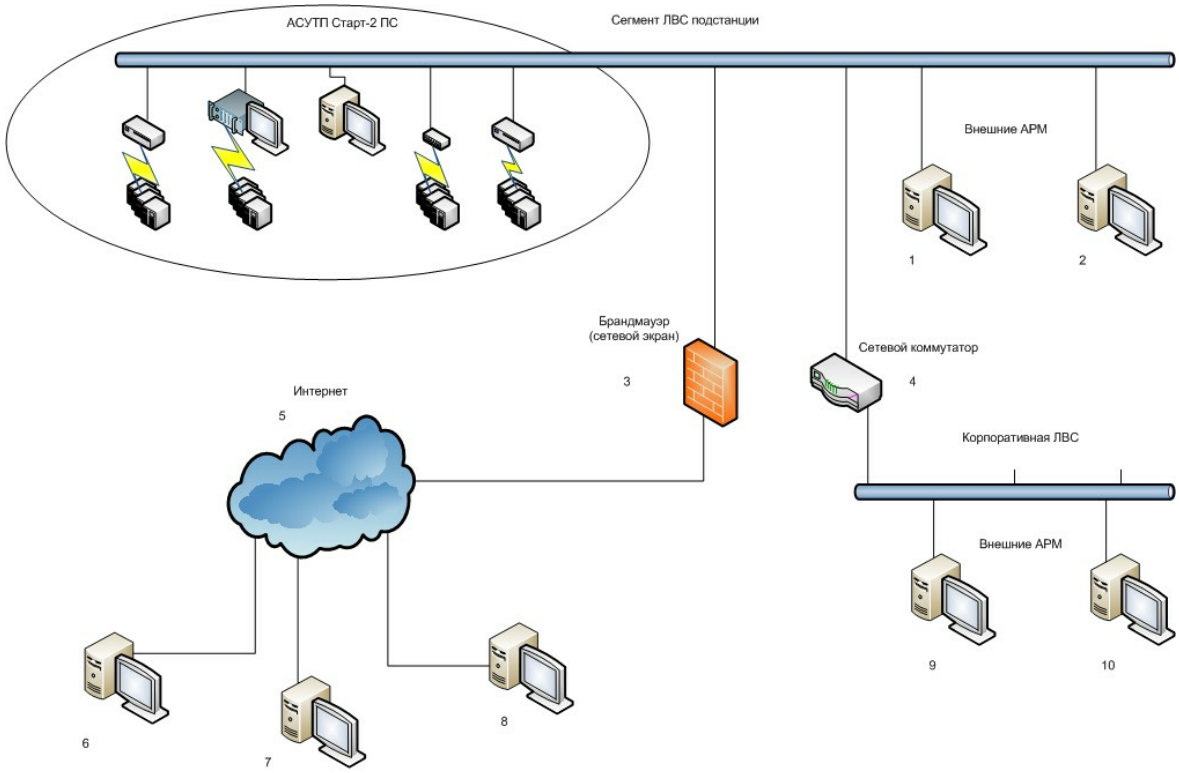
- ROPC - Сервер терминалов РЗА (ROPC)
- Start2.NetInformer - Служба сетевого информатора
- Start2.StoreService - Служба хранилища
- Radius.WatchDogService - Служба аварийного контроля

8 Приложения

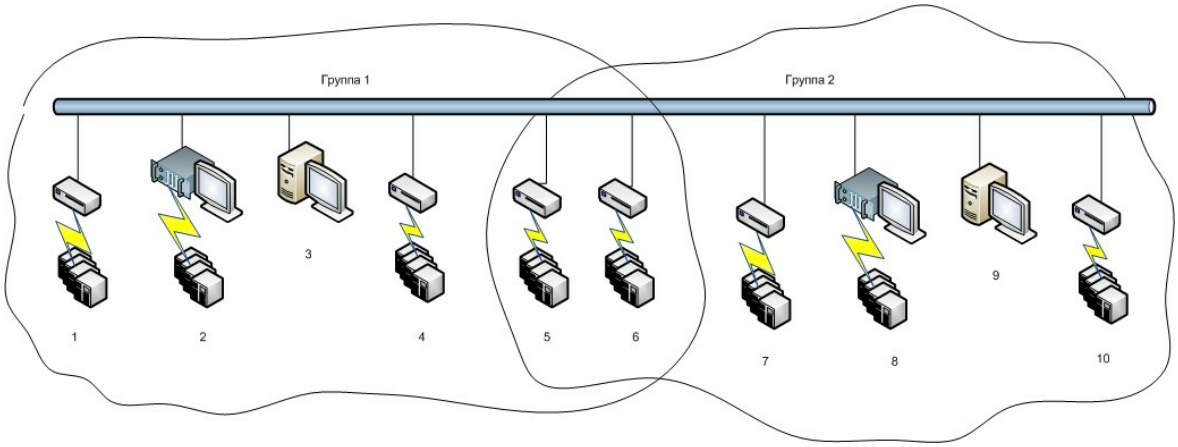
8.1 Приложение А. Архитектура АСУТП



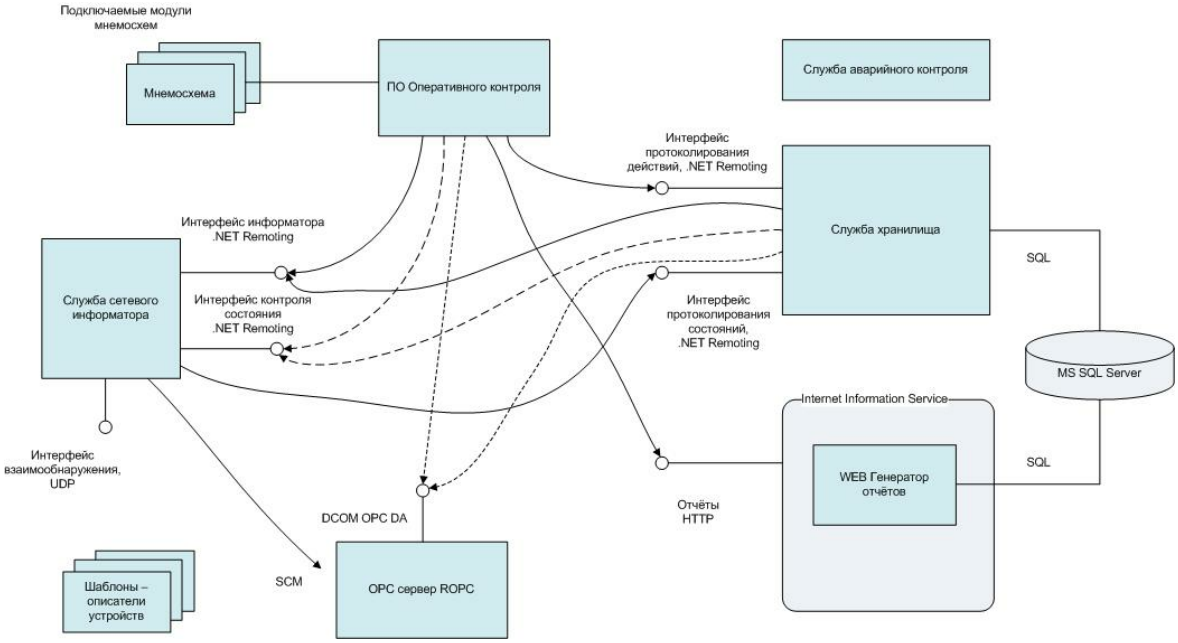
8.2 Приложение Б. Взаимодействие с внешними сетями



8.3 Приложение В. Организационные группы



8.4 Приложение Г. Взаимодействие компонентов узла



9 Лист сводки параметров

Сетевые параметры

Имя компьютера

.....

Имя рабочей группы / имя домена

.....

IP - адрес

.....

Прочие сетевые настройки

.....

.....

.....

Учётные записи

Локальный администратор

Имя.....Пароль.....

Администратор Старт-2ПС (Start2Admin)

Имя.....Пароль.....

Службы системы Старт-2ПС (Start2Svc)

Имя.....Пароль.....

Учётные записи пользователей

Имя.....Пароль.....

Имя.....Пароль.....

Имя.....Пароль.....

Имя.....Пароль.....

Имя.....Пароль.....

Имя.....Пароль.....

Прочие отметки

.....

.....

Подп. и дата

Инв.№ дубл.

Взам. инв. №

Подп. и дата

Инв.№ подл

Изм	Лист	№ докум	Подп	Дата

643.БПВА.10002-02 32

Лист 108

Копировал Формат А4