

ПО Р-08. Настройка DCOM в Windows 7 РП 15, Редакция 1 04.10.2012

#### Назначение

Для корректной сетевой работы модулей программного обеспечения необходимо выполнить настройку DCOM.

#### Используемое оборудование

Название	Дополнительная информация
Название оборудования	Версия 3.5.6 или выше

#### Описание

Настройки производятся в четырёх местах системы.

Добавить АНОНИМНЫЙ ВХОД в список Групп и пользователей в разделе Безопасность Свойств папок

- 1. **Рубеж**
- 2. **SIGMA-IS** (в системной папке ProgramData)

И дать ВСЕ Разрешения для этой группы (АНОНИМНЫЙ ВХОД).

- Так же, в Службе компонентов (Панель управления \ Администрирование), добавить тот же АНОНИМНЫЙ ВХОД в Разделе Служба компонентов – Компьютеры – Мой компьютер в окне Безопасность ком Свойств раздела Мой компьютер. Затем так же дать ему все разрешения.
- 4. В Брандмауэре необходимо
  - Чтобы он был ВЫКЛЮЧЕН
  - В Дополнительных параметрах, в Правилах для входящих подключений должна быть строка DCOM, в Окне свойств которой должны быть указаны, в закладке Протоколы и Порты, Тип протокола TCP, Локальный порт (номер Специального порта) 135.

Порядок проведения всех четырёх настроек не имеет значения.

Далее всё это и порядок всех действий будет приведён в иллюстрирующих скриншотах (копиях с экрана компьютера) и дополнительных пояснениях к ним.



# Настройка Брандмауэра Windows 7 Брандмауэр находится в Панели управления Windows (меню Пуск)

Он должен быть выключен:

		Summer Street or other			
🔾 💭 🛛 🔐 🕨 Панель управлен	ия 🕨 Все элементы панели управления 🕨 Бра	ндмауэр Windows	<ul> <li>◄</li> <li>Поиск в панел</li> </ul>		
Панель управления - домашняя страница Разрешить запуск программы или компонента через брандмауэр Windows Улменение параметров уведомлений Включение и отключение брандмауэра Windows	Защитите свой компьютер с помон Брандмауэр Windows помогает предотвратит вредоносных программ к этому компьютеру Как брандмауэр помогает защитить компью Дополнительные сведения о сетевых размещ Обновить параметры брандмауэра В брандмауэре Windows не использую рекомендуемые параметры для защит	цью брандмауэра Window ь несанкционированный доступ з через Интернет или локальную с rep? мили покальную с гер? мили покальную с гер? мили покальную с мили покальни покальн	VS лоумышленников или еть. рекомен. параметры		
<ul> <li>восстановить умолчания</li> <li>Дополнительные параметры</li> <li>Устранение неполадок в сети</li> </ul>	компьютера. Каковы рекомендуемые параметры?				
	🕺 Доменные сети		Не подключено 📎		
	🕺 Домашние или рабочие (ча	астные) сети	Подключено 🕥		
	Сети дома или на работе, когда вам известны использующие сеть люди и устройства				
	Состояние брандмауэра Windows:	Выкл.			
	Входящие подключения:	Блокировать подключения которые не включены в сп программ	нк программам, писок разрешенных		
	Активные домашние или рабочие (частные	сети: 🏠 Сеть 5			
	Состояние уведомления:	Уведомлять, когда брандма блокирует новую програм	ауэр Windows му		
	🔇 Общественные сети		Не подключено 🕑		
См. также Центр поддержки					
Центр управления сетями и общим доступом					



Дальнейшие настройки надо будет провести войдя в раздел Брандмауэра – Дополнительные параметры (в левом его окне) четвёртая позиция (со щитом), кликнув мышкой по этой надписи. После чего откроется окно - Брандмауэр Windows в режиме повышенной безопасности:





В его левой части кликните мышкой по позиции – Правила для входящих И среднее окно будет изменено на список Правил входящих подключений:

💮 Брандмауэр Windows в режиме повышенно	й безопасности		-	X	
Файл Действие Вид Справка					
<ul> <li>Брандмауэр Windows в режиме повышенн</li> <li>Правила для входящих подключений</li> <li>Правила для исходящего подключения</li> <li>Правила безопасности подключения</li> </ul>	Правила для входящих подключении			Действия	
	Имя	Группа	Профиль Вк.	<ul> <li>Правила для входящих подключен</li> </ul>	
	🔇 AudioRS.exe		Домен Да	🔯 Создать правило	
Наблюдение	AudioRS.exe		Домен Да	Фильтровать по профилю	
	ConfigROrganaizer.exe		Домен Да		
	ConfigROrganaizer.exe		Домен Да	Фильтровать по состоянию	
	🕑 crtdb.exe		Домен Да	Фильтровать по группе	
	🕑 crtdb.exe	Свойства: DCOM	-		
	OBPicker.exe				
	OBPicker.exe	Протоколы и порты	Область Дополни	тельно Пользователи	
<b>A</b>	OCOM	Оощие П;	рограммы и службы	Компьютеры	
	GeViRubeg.exe	Общие			
	Gevikubeg.exe	Имя:			
	KillProcess.exe	DCOM			
	C KillProcess.exe	Описание:			
				-	
	I oader eve				
	Microsoft Office Groove	Включено			
	Microsoft Office Groove	Действие			
	Microsoft Office OneNote	🧿 Разрешить г	подключение		
	Microsoft Office OneNote	🔨 🖉 💿 Разрешить т	только безопасное под	ключение	
	Microsoft Office Outlook	Настроить			
	🕑 Opera Internet Browser	1100.00010	····		
	🔇 Opera Internet Browser	🔘 Блокировате	ь подключение		
	🔇 Opera Internet Browser				
	🕑 Opera Internet Browser				
	🕜 Opera Internet Browser - Plugin wrapper				
	🔇 Opera Internet Browser - Plugin wrapper				
	🔇 Opera Internet Browser - Plugin wrapper				
	🔮 Opera Internet Browser - Plugin wrapper				
	Ø R08Srv.exe	Подробнее об этих парам	етрах		
	W R08Srv.exe				
< <u> </u>	< III				
and the second second	·		OK	Отмена Применить	



В списке Правил для входящих найдите позицию DCOM и кликните по ней мышкой. В открывшемся окне выберите закладку Протоколы и порты, там должен быть указан номер порта 135 и его тип TCP:

Панель управлен домашняя страни Разрешить запусс	ь управления > Все элементы панели управления > Брандмауэр Windows • 4 Лоиск в понел р Брандмауэр Windows в режиме повышенной безопасности Файл Действие Вид Справка	X
переграммы кий и через брандмауз Ульецение парар В илочение парар В илочение и отк брандмизера Vin В восстановить ум Фололнительные Устранение непо	Бранила для входящих подключений Правила для входящих подключения Правила для исходящего подключения Правила безопасности подключения Наблюдение Ваблюдение Сойства: DCOM Сойства: DCOM СОЙСТВА	Дейсти *         Правила для Бходящих подключен ▲           Разрец         Создать правило           Разрец         Фильтровать по профилю           Разрец         Фильтровать по состоянию           Разрец         Обновить           Разрец         Экспортировать список           Разрец         ОСОМ           Разрец         Ступочнить правило           Разрец         Фильтровать           Разрец         Осомить           Разрец         Осом           Разрец         Осом           Разрец         Осом           Разрец         Сорака           Разрец         Фильтровать           Разрец         Осом           Разрец         Удалить           Разрец         Сравка           Разрец         Сравка           Разрец         Сравка           Разрец         Сравка           Разрец         Сравка           Разрец         Сравка           Разрец         Сравк
См. также Центр поддержки Центр управлени общим доступом	Сополнительные сведения о протоколах и портах ОК Отмена Приденить Орега Internet Browser - Plugin Домен Да Окоб Стимена Орега Internet Browser - Plugin Домен Да Окоб Стимена Окоб Стимена С	Paspei Paspei Paspei Paspei Paspei Paspei Paspei Paspei Paspei Paspei Paspei Paspei

Если в списке Правил Входящих подключений строка DCOM, по любой причине отсутствует, её потребуется создать.



Для этого в правой крайней части окна кликните по позиции – Создать правило. Откроется окно мастера. В окне мастера создания правила для Входящих выберите позицию – для порта и нажмите Далее:





В следующем открывшемся окне мастера выберите тип порта TCP и ниже введите его номер 135 (позиция «Определённые локальные порты») и нажмите – Далее:



Это всё что требуется задать и установить в Брандмауэре Windows.

Далее надо будет вводить в параметры настроек Службы компонентов и папок Рубеж и SIGMA-IS позицию АНОНИМНЫЙ ВХОД с заданием ей всех разрешений для всех доступных действий.



#### Введение АНОНИМНОГО ВХОДА в параметрах Windows.

В меню Пуск выбрать позицию – Панель управления, в открывшемся окне найти позицию – Администрирование и в следующем открывшемся окне выбрать – Службы компонентов:





В левой части окна Службы компонентов кликнуть мышкой по позиции Службы компонентов. У данной позиции, ниже, откроется древовидная структура. Спуститесь по ней на позицию – Мой компьютер и встав на ней маркером правой кнопкой мышки откройте контекстное меню, в котором кликните мышкой по позиции – Свойства:

🧆 Службы компонентов	Married Street	The second	Same Country	and the second second	
Файл Действие В	Вид Окно Спр	авка	1 3-3-,		_ 5 ×
			121 🎹 🖽		
<ul> <li>Корень консоли</li> <li>Службы компонентов</li> <li>Компьютеры</li> <li>Мой ко</li> </ul>	Имя		Действия Май		
	Приложени Настройка	DCOM		Лополнительные действия	
Мои ко В Просмотр соб	Обновить все н	омпоненты рцессы			Henes and service Heneroland
👂 🎑 Службы (лока	Вид		пределенны		
	Новое окно от	сюда			
	Экспортироват	ъ список	эк		
	Свойства				
Справка	Справка				
Открытие окна свойств в	ыбранного объек	та.			



Откроется окно - Свойства: Мой компьютер, в котором выберите закладку – Безопасность СОМ:



В этом окне в двух местах надо будет ввести (проверить наличие) группу **АНОНИМНЫЙ ВХОД** и задать ей (разрешить) все действия.

Для этого сначала кликните по кнопке - Изменить ограничения в разделе - **Права доступа** Второе место – это такая же кнопка в разделе - **Разрешения на запуск и активацию**. (см. ДВА следующих скрина).









ЕСЛИ В ВЕРХНЕМ ОКНЕ отсутствует группа АНОНИМНЫЙ ВХОД - её нужно добавить.

Эта операция одинакова как для Службы компонентов, так и для ввода данной группы в Свойства Безопасности папок Рубеж и SIGMA-IS.

Порядок действий будет показан в следующих скринах.



В Окне (Права доступа или Разрешения на запуск и активацию), мышкой, нажать кнопку Добавить:



В открывшемся окне выбора Пользователей Компьютером или Учётных записей служб нажать кнопку – Далее. Откроется следующее окно.



④ Службы компонентов	and the second s					
🤌 Файл Действие Вид Окно Справка						
🗢 🔿 🖄 📅 🗙 🖾 🗟 😹 🛛 🖬	1 1 📭 🗄 🗰 🏛					
Корень консоли ▲ Эслужбы компонентов ▲ Компьютеры ▶ № Мой компьютер ■ Проскотр событий (Локальный) ▷ Службы (локальные)	Иня Свойства: Мой компьютер Общие Параметры Набор протоколов Безопасн Права доступа Можно изменять стикок лиц, которе разрешен доступ к припожениям. Та устанавливать ограничения на прил определяют свои собственные разр Осторожно: изменение разр Осторожно: изменение разр Осторожно: изменение разр Осторожно: изменение разр Осторожно: изменение разр Пользователи", "Компьютеры" Выбор: "Пользователи", "Компьютеры" Выбор: "Пользователи", "Компьютеры" Выберите тип объекта: "Пользователи", "Группы" или "Встрое В спедующем месте: sigma local Введите умена выбираемых объектов (и	Разрешение на запуск и активацию Разрешение на запуск и активацию Ограничения в целях безопасности Группы или пользователи: Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы" С Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы" С Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы" С Выбор: "Пользователи", "Группы" или "Встроенные субъекты безопасности" Выборите тип объекта: "Пользователи", "Группы" или "Встроенные субъекты безопасности" В следующем месте: зigma local Общие запросы Имя: начинается с Отислечные учетные записи Отислечные учетные записи Поиск Стоп				
	Подробнее о настройке этих параметров.	Результаты поиска: Имя (RDN) Злектронная п Описание В папке				
	ОК					



В этом окне нажать кнопку – Поиск:

🛞 Службы компонентов		
💩 Файл Действие Вид Окно Спр	авка – Б х	
🖕 🔿 🖄 📰 🗙 🖾 🗟 🛃 🛽		
📄 Корень консоли		
🔺 💩 Службы компонентов	Разрешение на запуск и активацию	
и 🧮 Компьютеры	Свойства: Мой компьютер Ограничения в целях безопасности	
Мой компьютер	Общие Параметры Групры или пользоватери:	CONT.
Ба Просмотр событии (Локальный) Службы (докальные)	Набор протоколов Безопасни	
	Права доступа 🦓 Администраторы (Тр-soft \Администраторы)	
	Можно изменять список лиц, которе Выбор: "Пользователи", "Компьютеры", "Учетные записи служб" или "Группы"	×
	устанавливать ограничения на прили определяют свои собственные разри Выберите тип объекта:	
	👃 Осторожно: изменение разд Пользователи", "Группы" или "Встроенные субъекты безопасности" Типы объектов	
	В следующем месте:	
	Выбор: "Пользователи", "Компьютеры", ". sigma local Размещение	
	Выберите тип объекта: Общие запросы	
	"Пользователи", "Группы" или "Встроенны Имя: начинается ( 🔻	
	В следующем месте:	- II
	sigma.local Описание: начинается с 🖤	
	Введите имена выбираемых объектов (при Отключенные учетные записи Стоп	
	Пароли с неограниченным сроком деиствия	
	Число дней со времени последнего входа в систему. 💌 🌱	
	Результаты поиска:	
	Подробнее о настройке этих параметров. Имя (RDN) Электронная п Описание В папке	^
	Szrazhevsky sigma.local/Users	
	ОК С Ха sigma.loca/Users	
	Администрат Администратор sigma.local/Users	
	Anekcangp C sigma.local/Users	
	анонимны	
	Safoñues An sigma.local/Users	
	sigma Jocal/Users	-

В списке, появившемся в нижней части последнего окна, найдите и выберите мышкой позицию АНОНИМНЫЙ ВХОД после чего нажмите кнопку - ОК.



Последнее окно закроется и в меньшем, предыдущем окне, появится запись АНОНИМНЫЙ ВХОД:



В этом окне также нажмите кнопку – ОК. Это окно закроется и запись АНОНИМНЫЙ ВХОД появится в списке Окна Права доступа (или Разрешение на запуск и активацию), в зависимости от того в которую позицию вы взялись добавить отсутствующую там позицию АНОНИМНЫЙ ВХОД.





После чего в нижнем окне можно добавить (доставить чекеры – «галочки») на непомеченных разрешениях. Когда все разрешения будут заданы – нажмите мышкой кнопу – ОК. Окно закроется.

Когда в обоих позициях (Права доступа / Разрешения на запуск и активацию) будет всё введено (либо проверено наличие) в окне Свойства Мой компьютер можно нажать кнопку Применить и ОК. Окно закроется. Настройка в разделе Службы компонентов – закончена.



Далее необходимо **проверить наличие введённой** позиции АНОНИМНЫЙ ВХОД в Свойствах Безопасности папок Рубеж и SIGMA-IS или **при необходимости добавить.** 

Открываете проводник Windows, в нём переходите в корневой каталог диска находите там и встаёте маркером мышки на папку Рубеж. Правой кнопкой мышки открываете контекстное меню и выбираете нижнюю позицию – Свойства. В открывшемся окне свойств папки Рубеж (или SIGMA-IS) выбираете закладку – Безопасность:



#### Примечание.

Это папка создаётся по умолчанию на диске С в корневом каталоге. Если во время установки ПО Р-08 вы перенаправили местоположение папки Рубеж, значит всё нужно будет проделать там, где она по факту находиться.

В списке Группы или пользователи проверяете наличие позиции АНОНИМНЫЙ ВХОД. Если последняя присутствует, устанавливаете на неё маркер мышкой и смотрите чтобы в нижнем окне – Разрешения для группы АНОНИМНЫЙ ВХОД стояли все чекеры («галочки») на РАЗРЕ-ШИТЬ !!!

Если чекеры установлены не все – доставьте их.

Если в верхнем списке отсутствует позиция АНОНИМНЫЙ ВХОД – её следует добавить.



Для чего нажмите мышкой кнопку Изменить. Далее, в открывшемся окне (см. скрин ниже) всё делается по аналогии с добавлением АНОНИМНОГО ВХОДА в Службе компонентов. После чего установить в нижнем окне все разрешения для вновь добавленной позиции.



# Тоже самое следует сделать для папки SIGMA – IS Находящейся в системной папке ProgramData

(доступ к ней, скорее всего, придётся открыть в Свойствах папок (Панель управления)

На этом все необходимые настройки DCOM для нормальной сетевой работы удалённых APM можно считать законченными.



#### ЗАКЛЮЧЕНИЕ

Данные настройки необходимо проводить на всех компьютерах в системе безопасности P-08 в случаях если:

- 1. Вы переустанавливали наше ПО Р-08
- 2. На удалённом АРМ при работе наших программ начало появляться сообщение Рубеж-Логгер не доступен.
- В программах, к примеру как Р-Монитор визуализаторы теряют цвет и становятся серыми, Фотоидентификация – не выводится фото и (или) другая информация по пользователю.