BASTION

ИНТЕГРИРОВАННАЯ СИСТЕМА БЕЗОПАСНОСТИ

АПК «Бастион»

Web-сервер интеграции

Руководство инсталлятора и администратора

Версия 1.5

ассоциация Электронные системы

Оглавление

Общая информация

Этот документ предназначен для администраторов и инсталляторов web-сервера системы интеграции АПК «Бастион».

1 Установка модуля

Модуль интеграции предназначен для информационного взаимодействия с системой контроля и управления доступом (далее – СКУД) аппаратно-программного комплекса «Бастион» (далее – АПК Бастион).

Web-сервис является центральной транспортной частью системы. Его роль заключается в приеме, маршрутизации и отправке сообщений. Web-сервер должен быть доступен по протоколу HTTP (порт 80) со всех рабочих станций АПК «Бастион» во всех филиалах, где предполагается разместить клиентов схемы интеграции. При возникновении проблем с доступом к web-серверу всегда необходимо обращаться к системному администратору корпоративной сети.

1.1 Требования к ПК

Требования к аппаратной конфигурации компьютера, на который устанавливается модуль:

- Оперативная память – 2 Гб (и выше);
- Тактовая частота процессора – 2 ГГц (и выше);
- Жёсткий диск – 1 Гб свободного места на системном диске.

Требования к программному окружению:

- Операционная система – **Windows 7, Windows 8, Windows 8.1, Windows Server 2008 R2, Windows 2012, Windows Server 2012 R2;**
- Microsoft IIS версии не ниже 7.5;
- Microsoft .NET Framework 4.0.

1.2 Установка и настройка Microsoft IIS

1.2.1 Установка IIS на Windows 2008 Server R2

Первым этапом установки является установка IIS, под управлением которого будет работать web-модуль.

> ***Внимание!*** *Для корректной работы ASP.NET на сервере требуется, чтобы IIS был установлен до установки Microsoft .NET Framework. Если Microsoft .NET Framework был установлен до установки IIS, то необходимо выполнить перерегистрацию ASP.NET в IIS (см. инструкции ниже).*

Службы Internet Information Services в системе Windows 2008 имеют версию 7.5 и не устанавливаются по умолчанию.

Чтобы установить IIS в Windows 2008, необходимо выполнить добавление соответствующей роли и сервисов. Для этого необходимо нажать кнопку «*Пуск*», выбрать команды «*Панель управления* \ *Администрирование* \ *Диспетчер сервера*».

Далее следует открыть узел «Роли» и нажать кнопку «Добавить роли».

Далее необходимо добавить роль «Веб-сервер (IIS)», следуя инструкциям по добавлению этой роли в мастере. В окне «Службы ролей» следует также отметить все неотмеченные компоненты (со всеми вложенными элементами) во всех узлах кроме узла «Служба FTP-публикации».

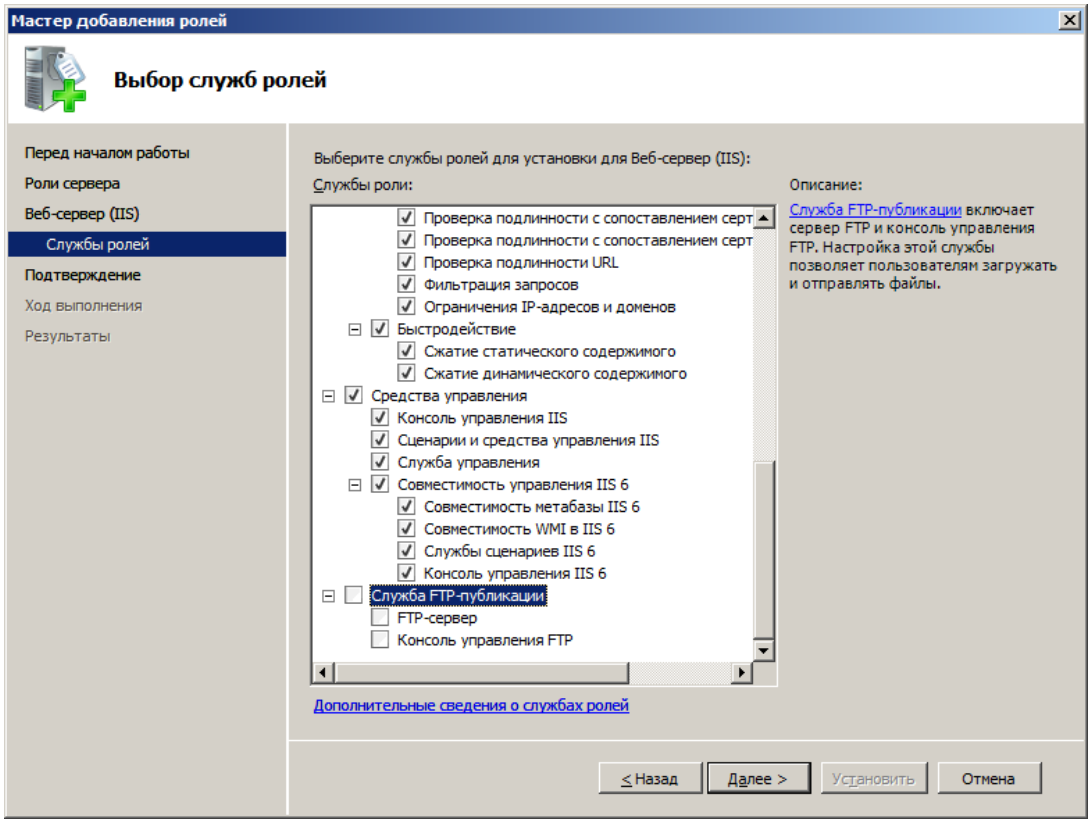


Рис. 1. Добавление служб ролей для Windows 2008

После успешного добавления роли нужно подтвердить установку указанных служб роли и дождаться окончания установки.

Следующим этапом является установка **Microsoft .Net Framework 4.0** и клиентского профиля Microsoft .NET Framework 4. Установить эти компоненты необходимо либо с диска АПК «Бастион», либо загрузить с сайта Microsoft.

Далее следует убедиться, что для пула приложений **DefaultAppPool** задана версия среды .NET Framework **4.0**. (рис. 2).

> ***Внимание!*** *Если Microsoft .NET Framework 4.0 был установлен до IIS, или если после установки при попытке открытия страницы сайта модуля сервер выводит сообщение об ошибке 500, то необходимо выполнить перерегистрацию ASP_NET в IIS. Сделать это*

можно путём запуска утилиты aspnet_regiis.exe с ключом –i. Утилита находится в каталоге %WINDIR%\Microsoft.NET\Framework\v4.0.30319.

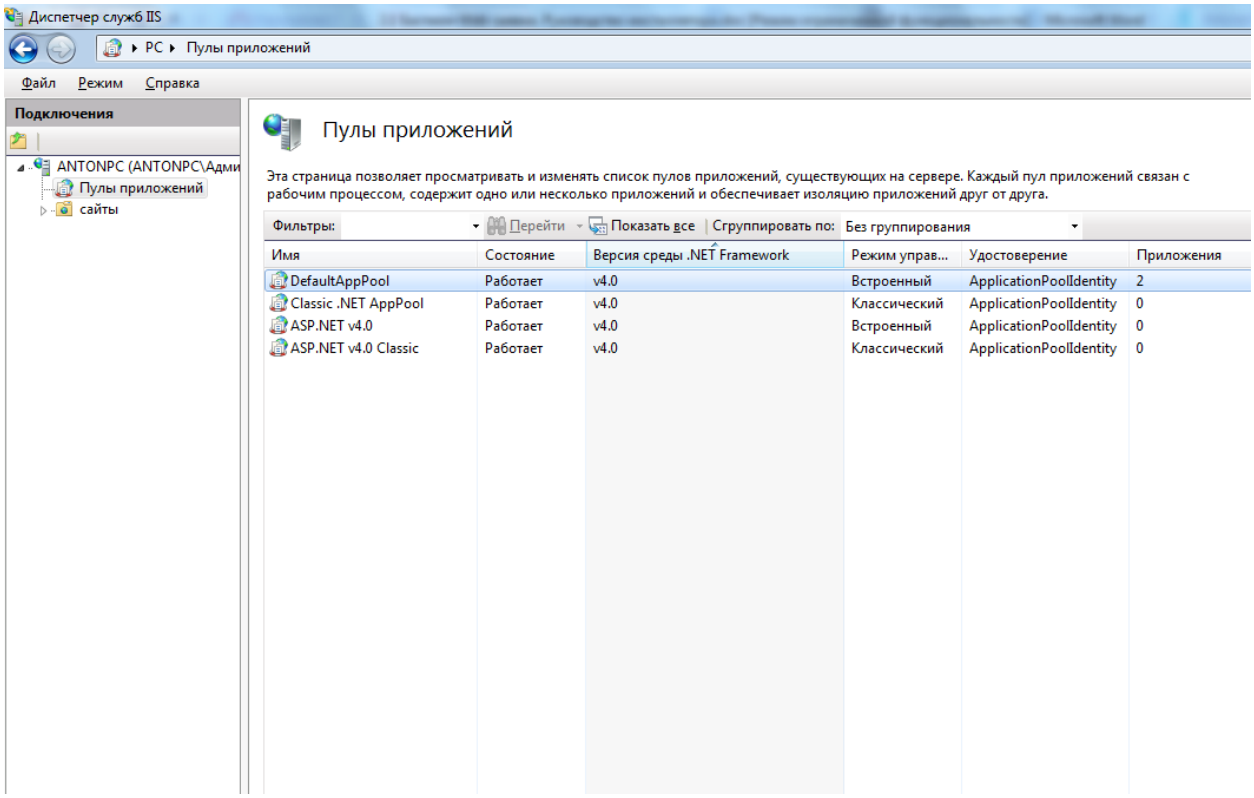


Рис. 2. Версия среды .NET Framework для DefaultAppPool

Полную информацию по настройке IIS можно найти на сайте **http://www.codenet.ru/webmast/iis/iis.php**.

1.2.2 Установка IIS на Windows server 2012

Для установки IIS необходимо открыть диспетчер серверов и выбрать на панели мониторинга пункт «Добавить роли и компоненты (рисунок 3).

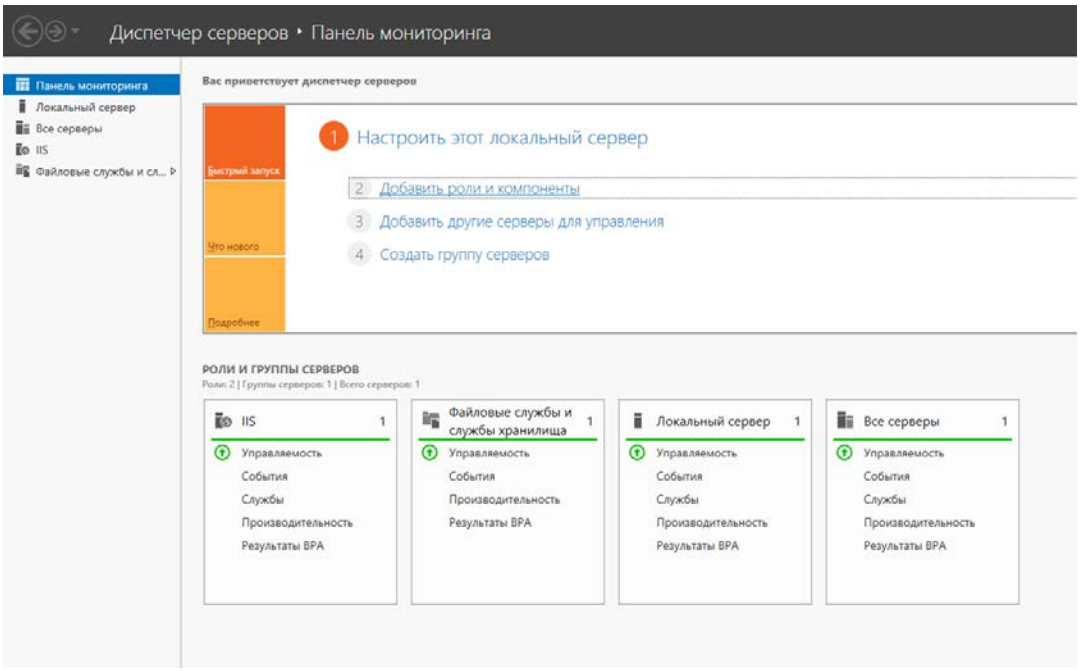


Рис. 3. Диспетчер серверов Windows Server 2012

В результате этого действия откроется мастер добавления ролей и компонентов. В нём необходимо путем нажатия кнопки «Далее» перейти на вкладку «Тип установки», где требуется выбрать пункт «Установка ролей и компонентов» (рисунок 4) и перейти к следующему шагу, нажав «Далее».

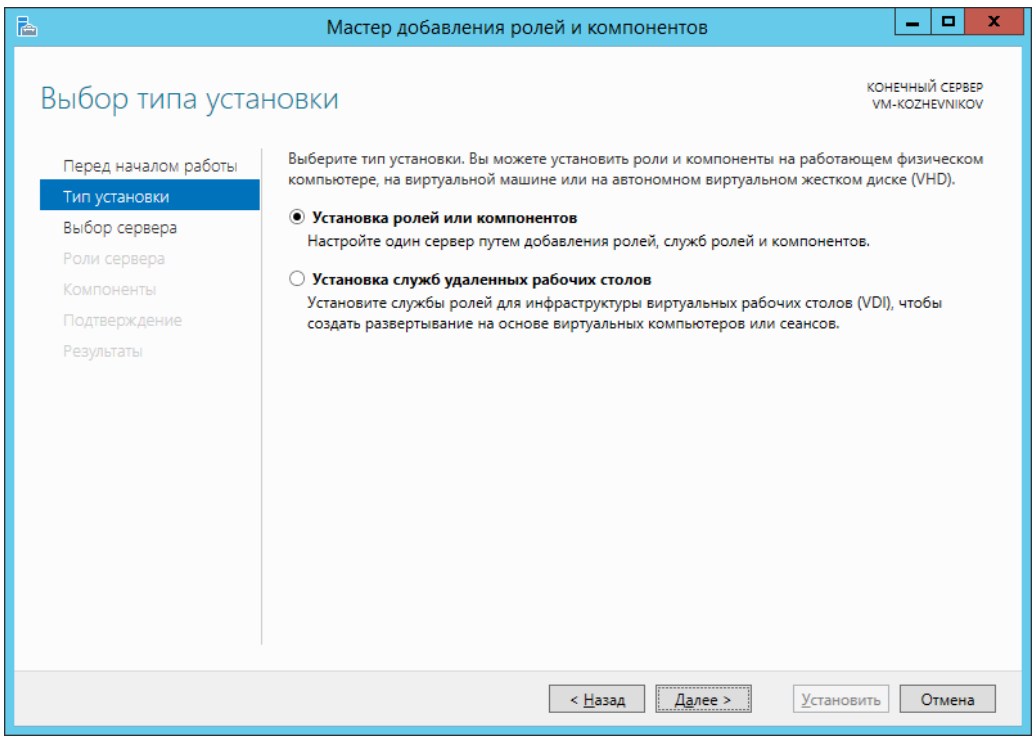


Рис. 4. Мастер добавления ролей и компонентов

Следующим шагом будет выбор сервера, где необходимо выбрать нужный сервер и перейти к выбору ролей сервера, где требуется в узле **Веб-сервер (IIS)** отметить галочками все элементы за исключением элементов подгруппы «FTP-сервер» так, как это показано на рисунке 5:

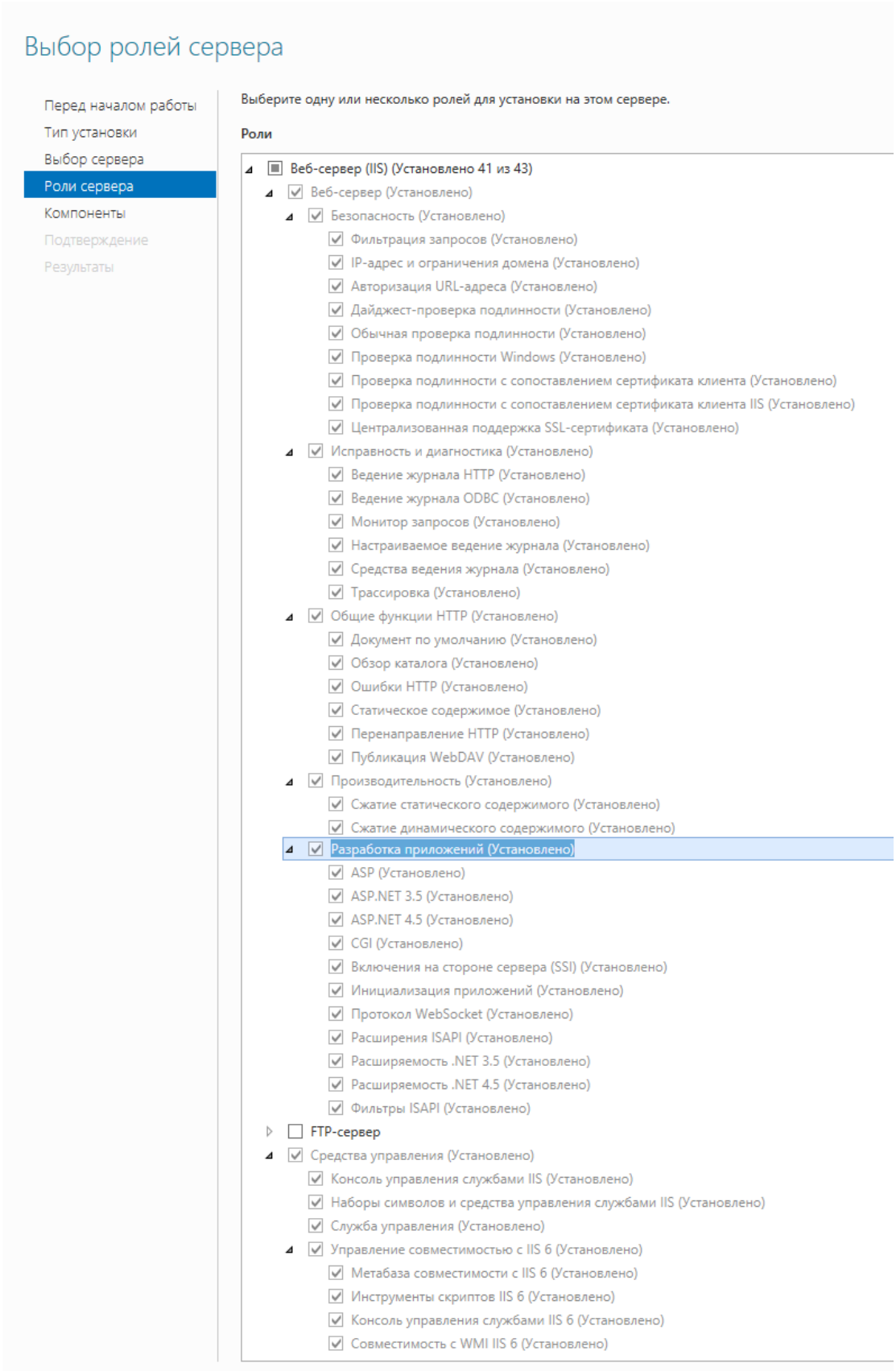


Рис. 5. Роли сервера

На следующем шаге необходимо отметить элементы "Активация не по HTTP", "Активация по HTTP" и все элементы группы "Службы WCF", входящие в .NET Framework:

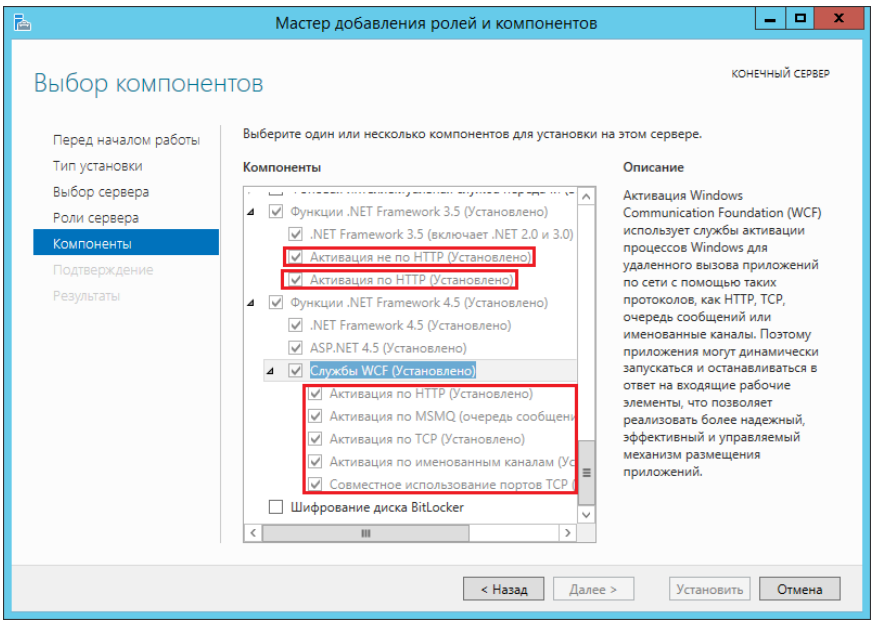


Рис. 6. Компоненты служб WCF и .NET Framework

В завершение нужно нажать кнопку «Установить» на вкладке «Подтверждение» и дождаться завершения установки добавленных компонентов.

1.2.3 Установка IIS на Windows 7, Windows 8 и Windows 8.1

Установка IIS в Windows 7/8/8.1 выполняется через Панель управления – Включение или отключение компонентов Windows. В узле «Службы IIS» следует отметить все компоненты (со всеми вложенными элементами) в узлах «Службы интернета» и «Средства управления веб-сайтом» так, как это показано на рисунке:

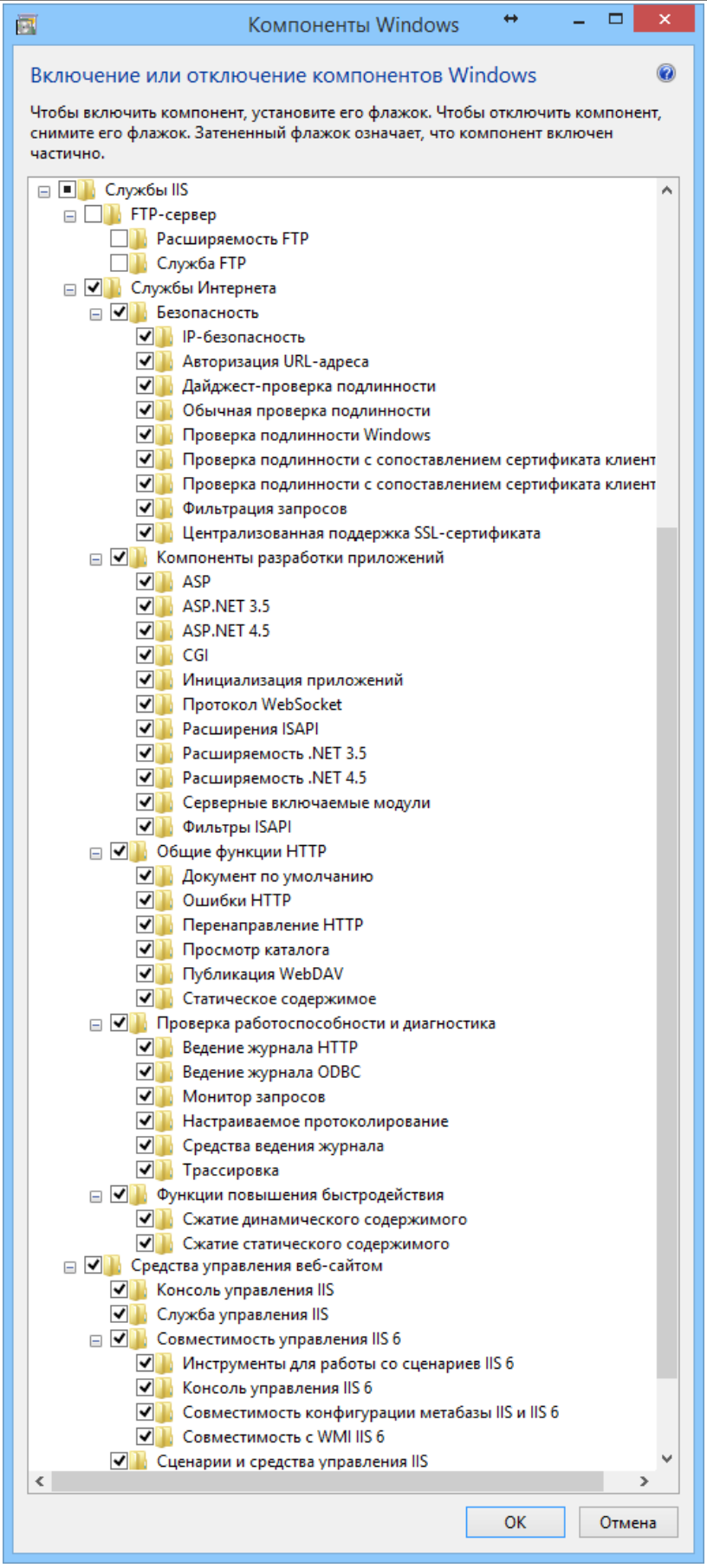


Рис. 7. Установка IIS в Windows 7, Windows 8 и Windows 8.1

1.2.3.1 Windows 7

Следующим этапом является установка **Microsoft .Net Framework 4.** Установить этот компонент необходимо либо с диска АПК «Бастион-2», либо загрузить с сайта Microsoft.

Далее следует убедиться, что для пула приложений **DefaultAppPool** задана версия среды .NET Framework **4.0**. (см. Рис. 8).

> ***Внимание!*** *Если Microsoft .NET Framework 4.0 был установлен до IIS, или если после установки при попытке открытия страницы сайта модуля сервер выводит сообщение об ошибке 500, то необходимо выполнить перерегистрацию ASP_NET в IIS. Сделать это можно путём запуска утилиты aspnet_regiis.exe с ключом –i. Утилита находится в каталоге %WINDIR%\Microsoft.NET\Framework\v4.0.30319.*

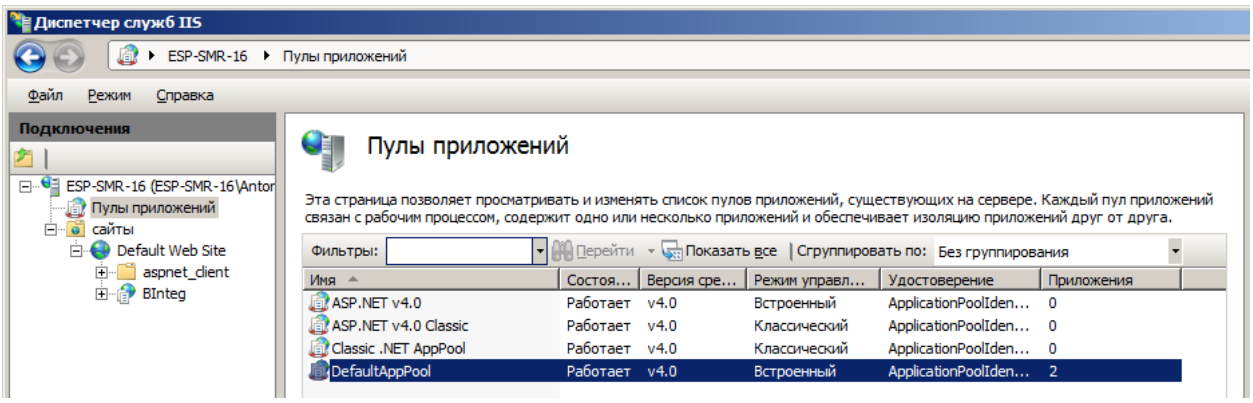


Рис. 8. Версия среды .NET Framework для DefaultAppPool

Полную информацию по настройке IIS можно найти на сайте **http://www.codenet.ru/webmast/iis/iis.php**.

1.2.3.2 Windows 8 и Windows 8.1

Под Windows 8/8.1 необходимо убедиться, что установлены дополнительные компоненты .NET Framework 3.5 и .NET Framework 4.5 так, как это показано на рисунке:

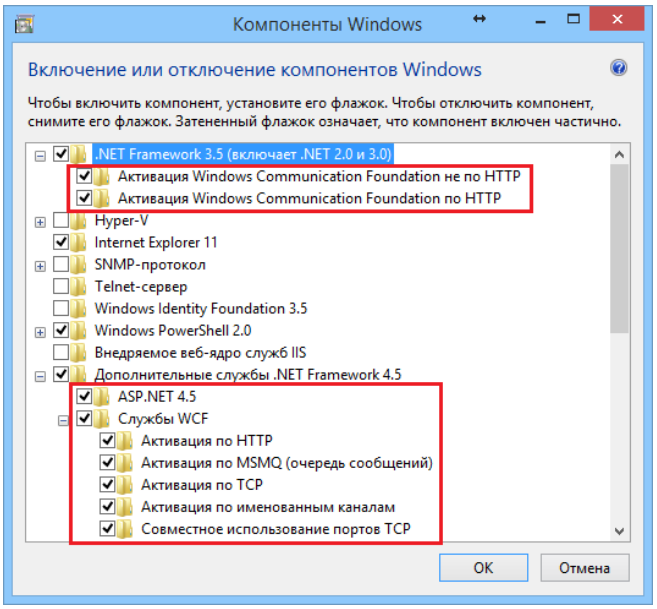


Рис. 9. Компоненты .NET Framework 3.5 и .NET Framework 4.5

1.3 Установка сервера интеграции

Для установки модуля необходимо запустить файл IntegInstall.exe. Следует нажать кнопку «Установка», по окончании инсталляции – нажать кнопку «Закрыть».

Запуск инсталлятора требует прав администратора.

Внимание! *Путь к инсталлятору не должен содержать скобки (пример недопустимого пути: «C:\IKS (distrib)\BIntegInstall.exe»). Также, не поддерживается запуск инсталлятора из сетевого расположения (UNC пути не поддерживаются).*

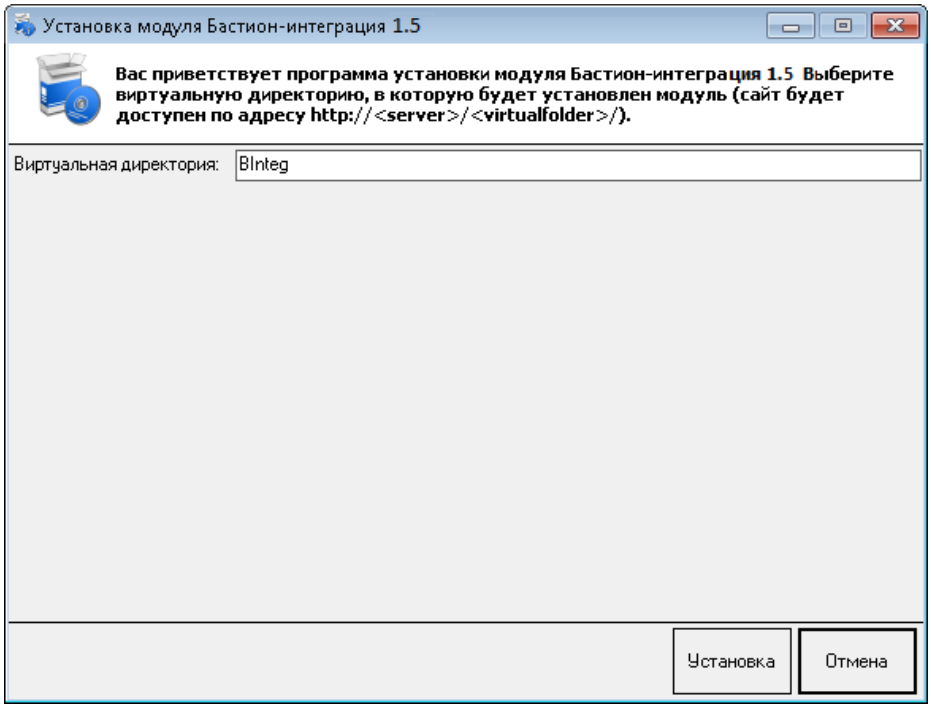


Рис. 10. Установка модуля

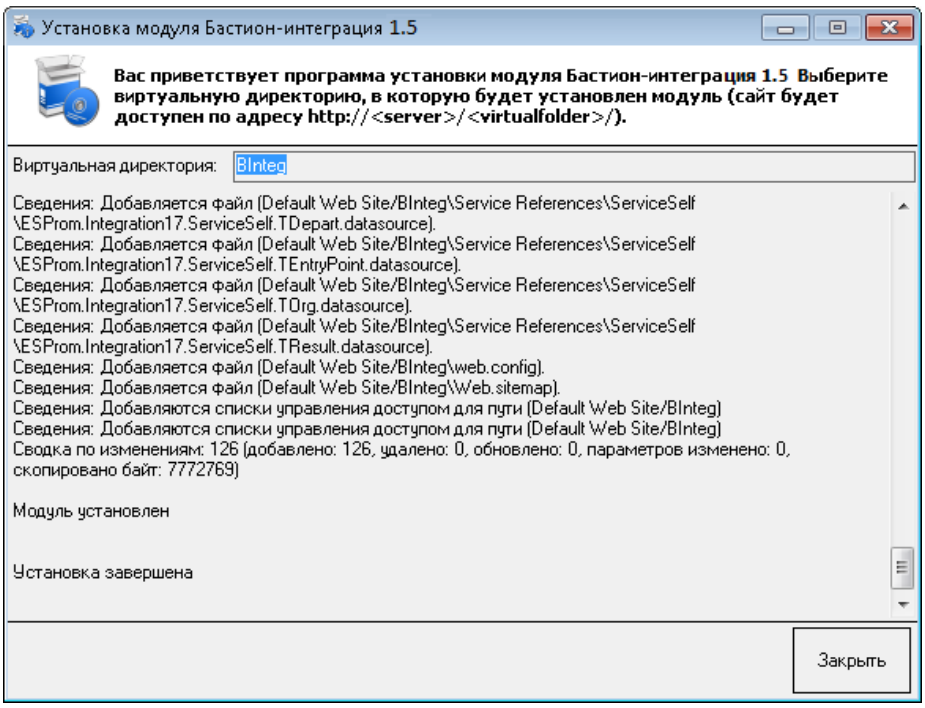


Рис. 11. Завершение установки

1.4 Настройка безопасности в Internet Information Services

Система доступа должна пропускать разрешенные внешние входящие подключения от клиентов интеграции. Наряду с этим, система должна блокировать все остальные подключения. Выполнить такое разграничение доступа можно, используя средство ограничения IP-адресов IIS.

Для этого необходимо раскрыть узел NInteg в консоли управления IIS (находится в узле сайты/Default Web Site) и открыть пункт «Ограничения IP-адресов и доменов».

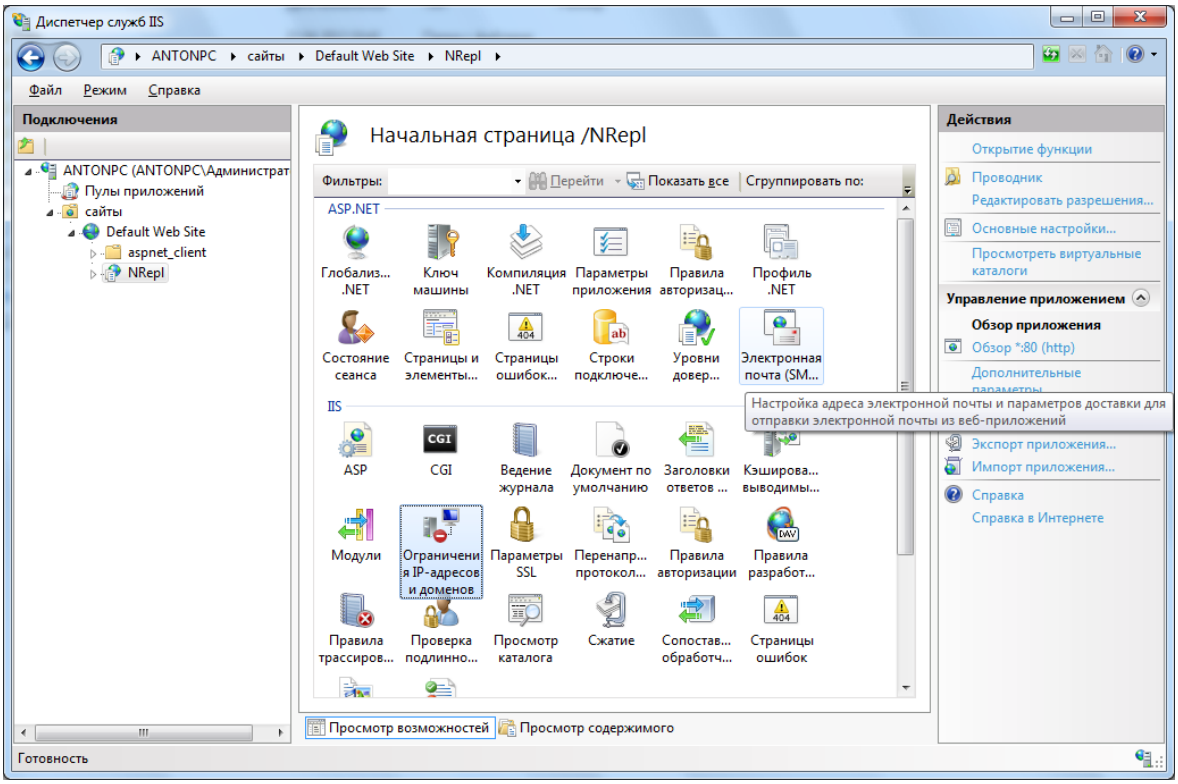


Рис. 12. Ограничения IP-адресов и доменов

В первую очередь следует запретить весь диапазон адресов. Для этого следует выбрать пункт «Добавить запрещающий элемент» и заполнить правило так, как показано на рисунке 13.

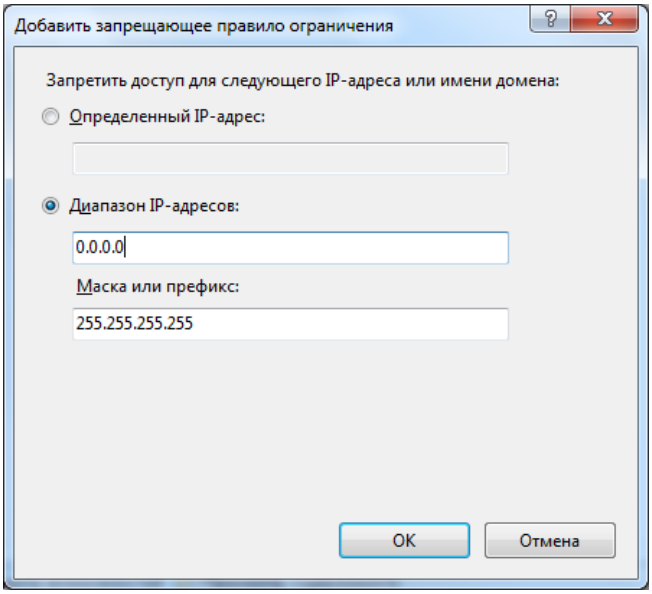


Рис. 13. Запрещающее правило для всех адресов

Затем следует добавить разрешающие правила для адреса 127.0.0.1 и для всех адресов, с которых предполагается использование системы интеграции.

В механизме ограничения IP-адресов Internet Information Services реализован механизм задания приоритета правил. Для настройки приоритетов сделан режим отсортированного списка, в котором положение правила сверху вниз определяет его приоритет. Самое верхнее правило имеет наивысший приоритет, и наоборот.

Для того чтобы система пропускала только те адреса, разрешения для которых были заданы администратором, нужно чтобы запрещающее правило, ограничивающее все IP-адреса имело самый низший приоритет. Это позволит подключаться разрешенным клиентам системы интеграции, и запретит всем остальным.

Для этого необходимо:

- выбрать на панели действий пункт «Просмотреть отсортированный список»;
- выделить запрещающее правило;
- нажатием ссылки «вниз» на панели действий поместить это правило в самый низ отсортированного списка;

После этих действий отсортированный список правил должен выглядеть примерно следующим образом:

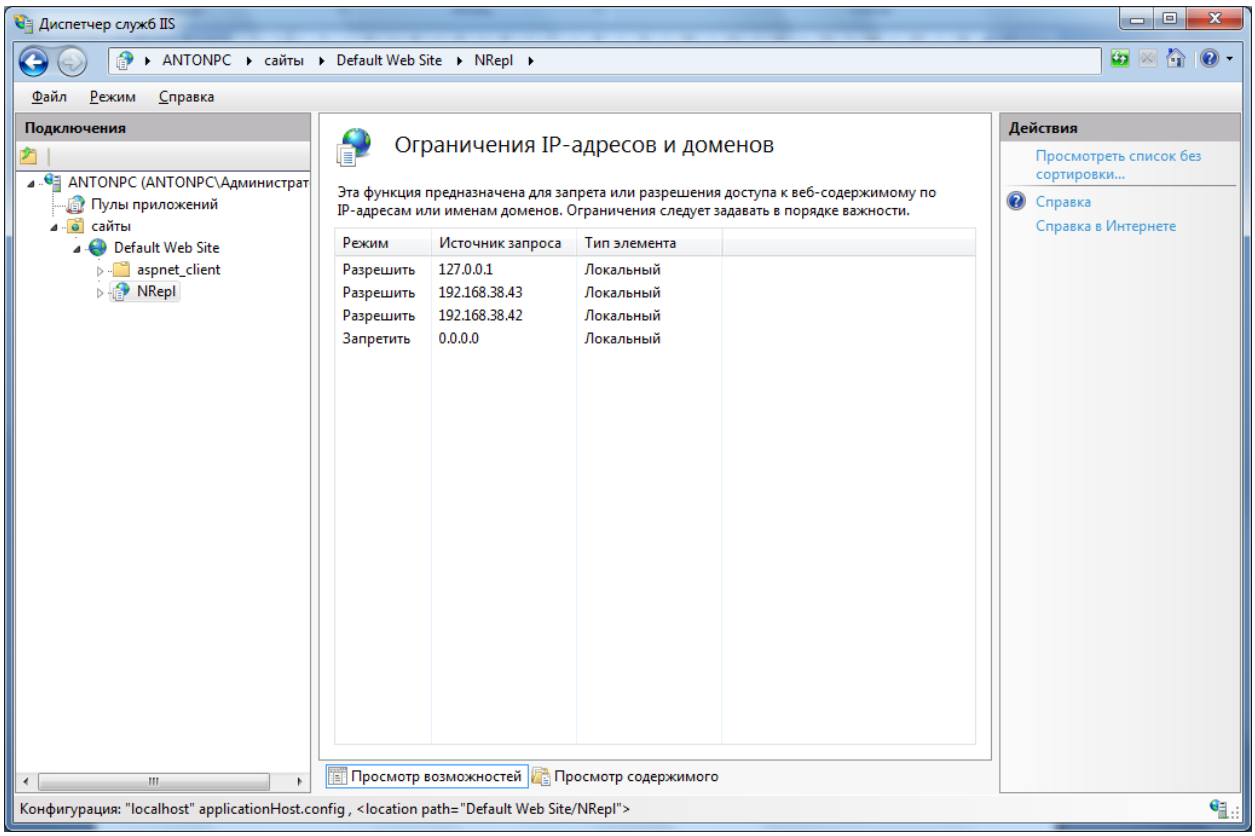


Рис. 14. Отсортированный список правил

Внимание! *При настройке безопасности IIS рекомендуется обратиться к системному администратору сети предприятия для корректного определения политики безопасности пользователей, от имени которых будут работать web-сервис и клиенты.*

С клиентских рабочих станций должны быть доступны web-портал в браузере и web-сервис с клиентов интеграции.

2 Лицензирование сервера интеграции

Перед началом работы необходимо получить лицензию на использование модуля интеграции с АПК «Бастион». Для этого необходимо запустить утилиту **LicenseInfo.exe**. При помощи которой необходимо сформировать файл запроса получения лицензии **IntegDataForLicense.dat**, который надо выслать в службу тех. поддержки АПК «Бастион».

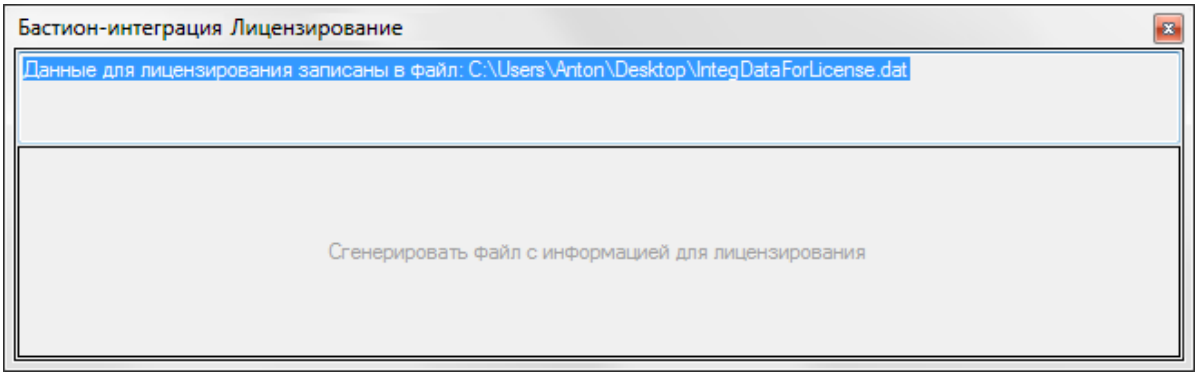


Рис. 15. Утилита формирования запроса лицензии

После того как служба тех. поддержки пришлёт лицензионный файл **License.dat**, его необходимо положить в корневую папку веб-портала (по умолчанию c:\inetpub\wwwroot\binteg). Количество серверов БД АПК «Бастион», сконфигурированных в файле Servers.xml, не должно превышать количества, прописанного в лицензионном файле.

3 Настройка модуля

3.1 Настройка протоколов сервиса интеграции

По умолчанию сервер интеграции сконфигурирован на работу по протоколу HTTP. Если поддержка HTTPS не требуется, то для дальнейшей настройки сервиса нужно перейти к разделу 3.2.

Если требуется настроить работу сервиса **только по протоколу HTTPS**, то необходимо выполнить инструкции из раздела **3.1.1**. Если требуется настроить сервер для работы по протоколам **HTTP и HTTPS одновременно**, то необходимо выполнить инструкции из раздела **3.1.2**

3.1.1 Настройка сервиса для работы только по протоколу HTTPS

Чтобы настроить сервис для работы по протоколу HTTPS без поддержки протокола HTTP необходимо выполнить следующие шаги:

1. Первым делом необходимо добавить в конфигурацию IIS сертификат SSL, который будет использоваться для доступа к сервису по протоколу HTTPS. Подробная информация о настройке сертификатов в Internet Information Services располагается по ссылке: http://www.codenet.ru/webmast/iis/htm/core/iicerts.php

2. Открыть в любом текстовом редакторе (**текстовый редактор должен быть запущен с правами администратора**) файл конфигурации web.config, который располагается в корневой папке веб-портала интеграции (по умолчанию

C:\Inetpub\wwwroot\BInteg\web.config). В нем необходимо найти узел <services>, который располагается в узле <system.ServiceModel>. Узел <services> содержит в себе четыре узла типа <endpoint>, первые два из которых обеспечивают подключения к сервису по протоколу http, а третий и четвертый для подключения по протоколу https. По умолчанию в конфигурации сервиса отключены точки подключения по протоколу https (третий и четвертый узлы заключены в комментарий вида **(<!-- -->)**). Для отключения поддержки HTTP и активации HTTPS необходимо снять комментарий с точек подключения HTTPS, и заключить в комментарий точки подключения HTTP. В результате выполненных действий блок <services> файла конфигурации примет следующий вид, изображенный на рисунке 16. Так же в файле конфигурации необходимо найти строку <serviceMetadata httpGetEnabled="true" httpsGetEnabled="false"/> и заменить её на <serviceMetadata httpGetEnabled="false" httpsGetEnabled="true"/>. После редактирования файл web.config необходимо сохранить, в результате чего IIS примет внесённые изменения.

```
<services>
  <service name="ESProm.Integration17.IntegrationService" behaviorConfiguration="integBehavior">
    <!--<endpoint
         address="http://localhost/BInteg/IntegrationService.svc"
         binding="basicHttpBinding" bindingConfiguration="bHttpBinding"
         contract="ESProm.Integration17.IIntegrationService"/>
    <endpoint address="http://localhost/BInteg/IntegrationService.svc/mex"
         binding="mexHttpBinding"
         contract="IMetadataExchange" />-->

    <endpoint
         address="https://localhost/BInteg/IntegrationService.svc"
         binding="wsHttpBinding" bindingConfiguration="TransportSecurity"
         contract="ESProm.Integration17.IIntegrationService"/>
    <endpoint address="https://localhost/BInteg/IntegrationService.svc/mex"
         binding="mexHttpsBinding"
         contract="IMetadataExchange" />
  </service>
</services>
```

Рис. 16. Конфигурация под HTTPS

3. Затем необходимо добавить в конфигурации web-узла IIS привязку HTTPS, и удалить привязку HTTP. Для выполнения этого действия нужно раскрыть консоль управления IIS, в дереве консоли развернуть папку «Сайты» так, чтобы был доступен узел «Default Web Site», после чего в контекстном меню узла «Default web site» выбрать пункт «Изменить привязки», в результате чего откроется окно, изображенное на рисунке 17. В этом окне необходимо выделить пункт «http», нажать кнопку «Удалить», подтвердить действие, затем нажать кнопку «Добавить», в результате чего откроется окно добавления привязки сайта, изображенное на рисунке 17. В окне необходимо установить значения поля «Тип» равное «https», в поле выбора сертификата SSL выбрать нужный сертификат и завершить настройку, нажав кнопку «Ок».

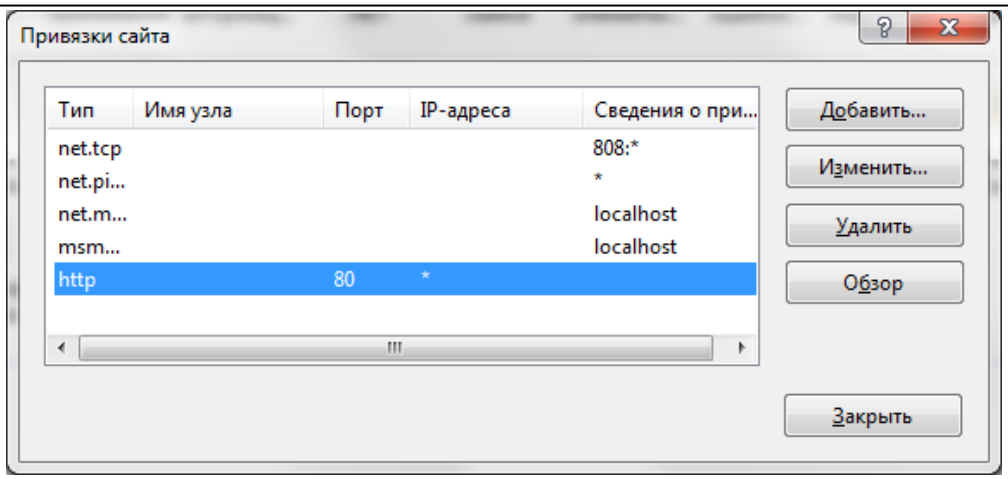


Рис. 17. Окно настройки привязок сайта

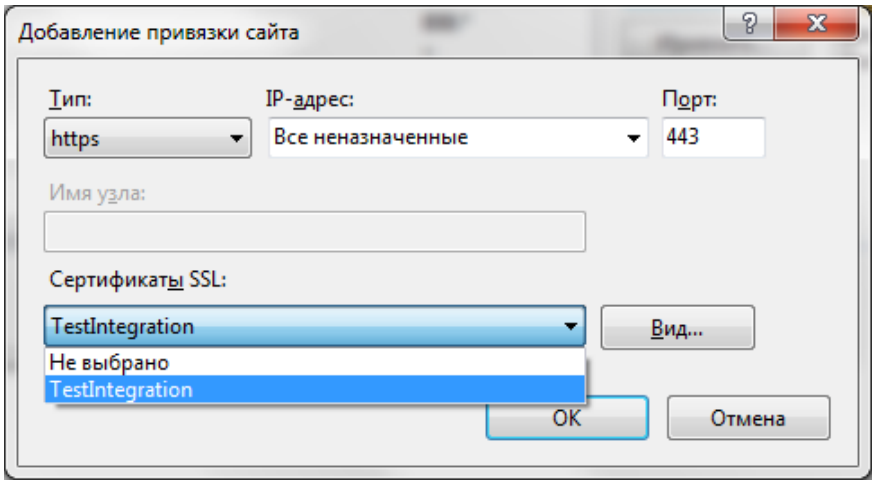


Рис. 18. Добавление привязки https

После выполнения этих действий веб-сервис интеграции будет доступен для клиентских подключений только по протоколу HTTPS.

3.1.2 Настройка сервиса для работы по протоколам HTTP и HTTPS одновременно.

Чтобы настроить сервис для работы по протоколам HTTP и HTTPS одновременно необходимо выполнить следующие шаги:

1. Первым делом необходимо добавить в конфигурацию IIS сертификат SSL, который будет использоваться для доступа к сервису по протоколу HTTPS. Подробная информация о настройке сертификатов в Internet Information Services располагается по ссылке: http://www.codenet.ru/webmast/iis/htm/core/iicerts.php

2. Открыть в любом текстовом редакторе (**текстовый редактор должен быть запущен с правами администратора**) файл конфигурации web.config, который располагается в корневой папке веб-портала интеграции (по умолчанию C:\Inetpub\wwwroot\BInteg\web.config). В нем необходимо найти узел <services>, который располагается в узле <system.ServiceModel>. Узел <services> содержит в себе четыре узла типа <endpoint>, первые два из которых обеспечивают подключения к сервису по протоколу http, а третий и четвертый для подключения по протоколу https.

По умолчанию в конфигурации сервиса отключены точки подключения по протоколу https (третий и четвертый узлы заключены в комментарий вида **(<!-- -->)**). Для активации HTTPS необходимо снять комментарий с точек подключения HTTPS. В результате выполненных действий блок <services> файла конфигурации примет следующий вид, изображенный на рисунке 19. Так же в файле конфигурации необходимо найти строку `<serviceMetadata httpGetEnabled="true" httpsGetEnabled="false"/>` и заменить её на `<serviceMetadata httpGetEnabled="true" httpsGetEnabled="true"/>`. После редактирования файл web.config необходимо сохранить, в результате чего IIS примет внесённые изменения.

```
<services>
  <service name="ESProm.Integration17.IntegrationService" behaviorConfiguration="integBehavior">
    <endpoint
         address="http://localhost/BInteg/IntegrationService.svc"
         binding="basicHttpBinding" bindingConfiguration="bHttpBinding"
         contract="ESProm.Integration17.IIntegrationService"/>
    <endpoint address="http://localhost/BInteg/IntegrationService.svc/mex"
         binding="mexHttpBinding"
         contract="IMetadataExchange" />

    <endpoint
         address="https://localhost/BInteg/IntegrationService.svc"
         binding="wsHttpBinding" bindingConfiguration="TransportSecurity"
         contract="ESProm.Integration17.IIntegrationService"/>
    <endpoint address="https://localhost/BInteg/IntegrationService.svc/mex"
         binding="mexHttpsBinding"
         contract="IMetadataExchange" />
  </service>
</services>
```

Рис. 19. Конфигурация под HTTP и HTTPS

3. Затем необходимо добавить в конфигурации web-узла IIS привязку HTTPS. Для выполнения этого действия нужно раскрыть консоль управления IIS, в дереве консоли развернуть папку «Сайты» так, чтобы был доступен узел «Default Web Site», после чего в контекстном меню узла «Default web site» выбрать пункт «Изменить привязки», в результате чего откроется окно, изображенное на рисунке 20. В этом окне необходимо нажать кнопку «Добавить», в результате чего откроется окно добавления привязки сайта, изображенное на рисунке 21. В окне необходимо установить значения поля «Тип» равное «https», в поле выбора сертификата SSL выбрать нужный сертификат и завершить настройку, нажав кнопку «Ок».

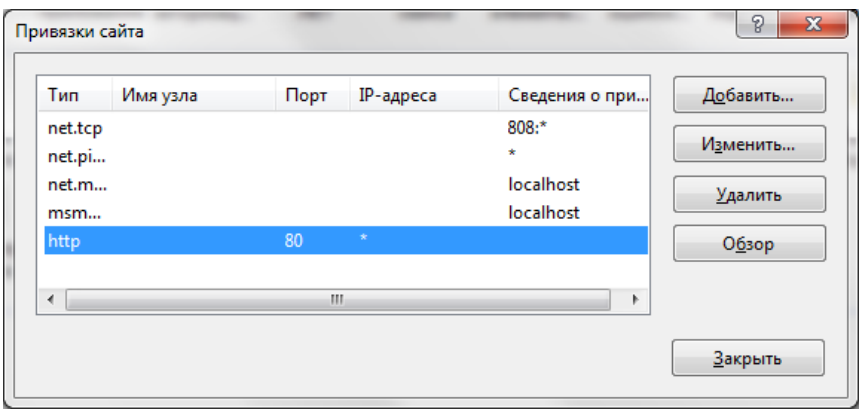


Рис. 20. Окно настройки привязок сайта

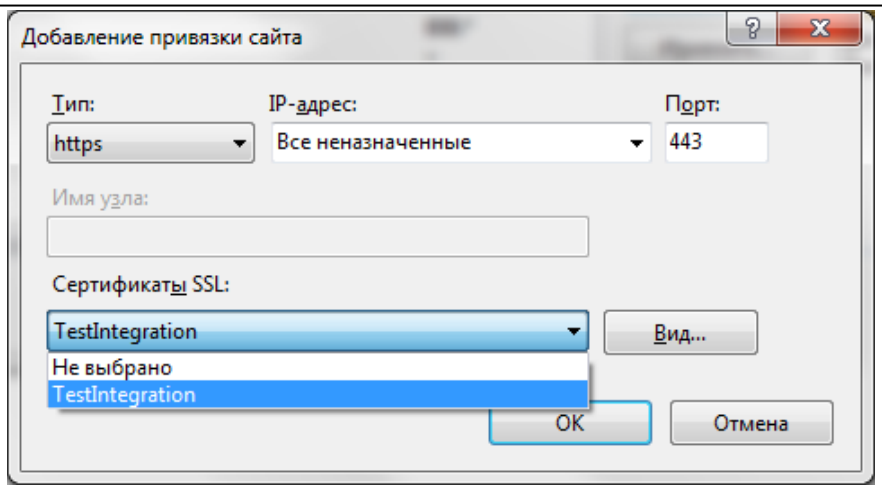


Рис. 21. Добавление привязки https

После выполнения этих действий веб-сервис интеграции будет доступен для клиентских подключений по протоколам HTTP и HTTPS одновременно.

3.2 Настройка схемы интеграции

Настройка схемы интеграции заключается в определении и создании описания для каждого из клиентов. Для добавления клиента в схему интеграции необходимы следующие данные:

- сетевой адрес сервера;
- путь к базе данных на сервере.

Для включения одного клиента в систему интеграции необходимо:

1. Войти на web-портал по ссылке

http://[имя сервера]/BInteg

1. Перейти на страницу «Конфигурация». Страница имеет следующий вид:

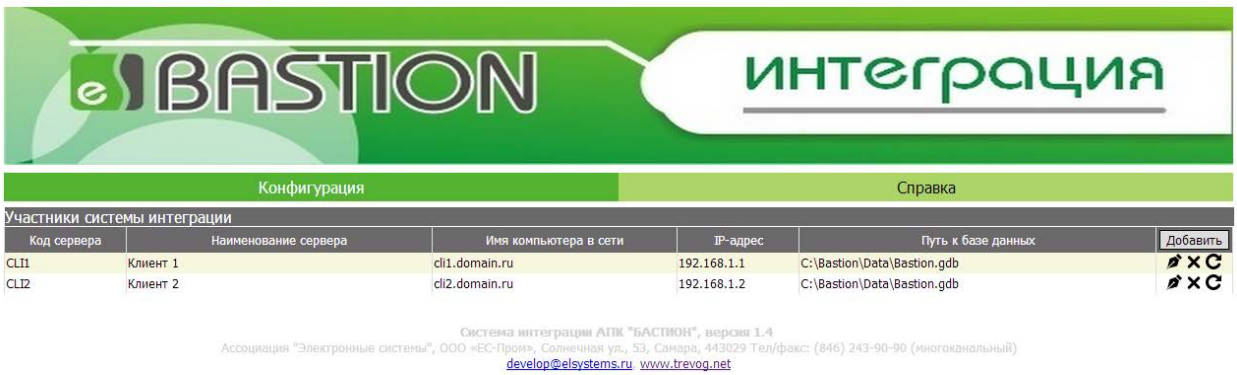
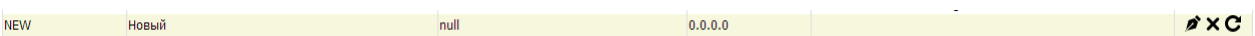


Рис. 22 - Список участников интеграции

2. Нажать кнопку Добавить. В таблицу будет добавлена строка с кодом «NEW».



3. Нажать кнопку «Изменить» напротив добавленной строки. Она примет вид:

4. Ввести в соответствующие столбцы описание участника (для примера):
   - код;
   - наименование сервера;
   - имя компьютера участника в корпоративной - *необязательное поле*;
   - IP-адрес;
   - Путь к базе данных.
5. По окончании ввода нажать кнопку ✔ «Сохранить». Таблица примет вид:

Подобным образом необходимо выполнить создание описаний для всех участников системы интеграции.

3.3 Обновление БД участников схемы интеграции

В случае если сервер-участник схемы интеграции имеет версию АПК «Бастион» ниже 1.7.5.7, то необходимо обновление его базы данных. Обновление базы данных для серверов с АПК «Бастион» версий 1.7.5.5 и 1.7.5.6 осуществляется при помощи файла скрипта, расположенного в папке «Скрипт для Бастиона версий 1.7.5.5-1.7.5.6», входящей в состав дистрибутива, а обновление базы данных для серверов с АПК «Бастион» версии 1.7.4.10 выполняется при помощи файла скрипта из папки «Скрипт для Бастиона версии 1.7.4.10». Скрипт для АПК «Бастион» версии 1.7.5.1 находится в папке «Скрипт для Бастиона версии 1.7.5.1».

> ***Внимание!*** *Перед выполнением скрипта для Бастиона версии 1.7.4.10 необходимо вручную создать в базе данных пользователя INTEG_ADMIN с паролем dfh578. О том, как добавить пользователя, написано в пункте 6.3.7 «Руководства системного администратора» АПК «Бастион» («Менеджер пользователей»).*

3.4 Проверка работы веб-сервиса

Для проверки веб-сервиса на веб-портале имеется кнопка проверки связи, а также ссылки на текстовое описание сервиса (WSDL). Для доступа к ним необходимо зайти на веб-портал и перейти на вкладку «Справка».

Результатом нажатия на кнопку «Проверить соединение с сервисом» должна быть надпись «Успешное соединением с сервисом» справа от кнопки. В противном случае веб-сервис или IIS настроены неправильно. Также при переходе по ссылкам «Строка для подключения» и «Текстовое описание web-сервиса» должны открываться страницы с описанием веб-сервиса.

> ***Внимание!*** *Если полное имя компьютера (<имя хоста>.<доменное имя>) имеет длину менее 9 символов, то ссылки с текстовым описанием веб-сервиса на странице «Справка» не будут открываться, а на операционной системе Windows 7 x64 может не работать кнопка проверки соединения с сервисом. В этом случае проверку работы сервиса*

необходимо проверять с помощью внешнего клиента, либо нужно переименовать рабочую станцию таким образом, чтобы её полное имя имело длину более 9 символов.

3.5 Настройка таймаута выполнения операций

Для настройки таймаута выполнения операций нужно отредактировать файл конфигурации web.config, который располагается в корневой папке веб-портала интеграции (по умолчанию C:\Inetpub\wwwroot\BInteg\web.config). В нем необходимо найти узел <appSettings>, в котором находится ключ **operationsTimeOut.** Значение этого ключа определяет продолжительность таймаута (в секундах).