



АПК «Бастион»

**Репликация персонала
и пост центрального наблюдения**

Руководство инсталлятора и администратора

Версия 1.7

Содержание

1	Общая информация	4
1.1	Установка web-сервиса и портала	4
1.2	Требования к ПК web-сервиса и web-портала.....	4
1.3	Установка под Windows 2003 Server.....	5
1.3.1	Установка Internet Information Services (IIS) и Microsoft .NET Framework 2.0 под Windows 2003	5
1.3.2	Установка web-портала под Windows 2003	6
1.3.3	Настройка web-портала в Internet Information Services под Windows 2003	6
1.3.4	Настройка безопасности в Internet Information Services под Windows 2003	9
1.4	Установка под Windows 7	11
1.4.1	Установка Internet Information Services (IIS) и Microsoft .NET Framework 2.0 под Windows 7	11
1.4.2	Установка web-портала под Windows 7.....	12
1.4.3	Настройка web-портала в Internet Information Services под Windows 7	13
1.5	Установка компонентов под Windows 2008	15
1.5.1	Установка Internet Information Services (IIS) и Microsoft .NET Framework 2.0 под Windows 2008	15
1.5.2	Установка web-портала под Windows 2008	18
1.5.3	Настройка web-портала в Internet Information Services под Windows 2008	18
1.6	Добавление web-портала в доверенную зону	19
1.7	Самоидентификация сервиса репликации и настройка NTFS.....	20
2	Настройка схемы репликации	22
2.1	Создание описания для клиентов репликации	22
2.2	Группы доступа	23
3	Установка клиента репликации	25
3.1	Требования к ПК клиента.....	25
3.2	Установка клиента	25
3.3	Настройка клиента	26
3.4	Настройка групп доступа в клиентах репликации.....	29
4	Настройка репликации в АПК «Бастион».....	30
4.1	Разграничение диапазонов табельных номеров	30
4.2	Настройка общих параметров репликации	31
4.3	Настройка маршрута по умолчанию	32
4.4	Настройка прав пользователей АПК «Бастион»	34

4.5	Настройка локального импорта личных карт и их изменений	35
4.6	Настройка локального экспорта личных карт и их изменений.....	36
4.7	Схема формирования корпоративного кода	36
5	Настройка модуля «Бастион-ПЦН»	37
5.1	Общие сведения	37
5.2	Настройка маршрута по умолчанию для событий	38
5.3	Включение выгрузки событий клиентом репликации	39
5.4	Окно «чужих» сообщений мониторинга	39
6	Включение выгрузки событий входа/выхода	40
7	Проверка работоспособности системы	41
8	Потеря и восстановление связи на медленных каналах.....	43
9	Обмен персональными данными с системами кадрового учёта.....	44
9.1	Обмен персональными данными через файлы XML.....	44
9.2	Обмен персональными данными через обменную таблицу.....	45
9.3	Обмен персональными данными через запрос на изменившиеся данные	45
9.4	Обмен событиями входа/выхода	46
9.5	Алгоритм репликации персональных данных и событий входа/выхода с кадровой системой.....	47
	Приложение А. Технические требования к серверу репликации	49
	Приложение Б. Спецификация обменного файла XML.....	52
	Приложение В. Спецификация обменных таблиц.....	54
	Приложение Г. Спецификация обменных полей.....	55
	Приложение Д. Спецификация обменных полей TABLE_FIELDS и TABLE_VALUES	56
	Приложение Е. Спецификация выходного файла с событиями учета рабочего времени ...	58
	Приложение Ж. Настройка фильтра исходящих событий	58
	Приложение З. Список иллюстраций.....	60

1 Общая информация

Этот документ предназначен для администраторов и инсталляторов системы репликации АПК «Бастион». Система репликации обеспечивает двунаправленную передачу персонала и событий между двумя и более базами данных СКУД АПК «Бастион».

Прежде, чем приступить к установке системы, внимательно ознакомьтесь с п. 1.1 документа «Репликация. Руководство оператора» для получения общих сведений о терминологии и принципах работы системы.

1.1 Установка web-сервиса и портала

Web-сервис является центральной транспортной частью системы. Его роль заключается в приеме, маршрутизации и отправке сообщений.

Установка web-сервиса является первым этапом и, как правило, производится один раз на web-сервере корпоративной сети предприятия. Web-сервер должен быть доступен по протоколу HTTP (порт 80) со всех рабочих станций АПК «Бастион» во всех филиалах, где предполагается разместить клиентов схемы репликации. При возникновении проблем с доступом к web-серверу всегда необходимо обращаться к системному администратору корпоративной сети.

1.2 Требования к ПК web-сервиса и web-портала

- оперативная память – 512 Мб (и выше);
- тактовая частота процессора – 2 ГГц (и выше);
- жёсткий диск – 1 Гб свободного места на системном диске;
- операционная система – **Windows 2003 Server Standard Edition + Service Pack 2**

(без использования Service Pack были замечены проблемы с настройкой авторизации к web-сервису)

или

Windows 7, или

Windows 2008 Server Standard Edition

- Internet Explorer 6 и выше (далее, IE 6);
- IIS 6.0 на Windows 2003 (наличие Front Page 2000 Server Extensions не обязательно);

или

IIS 7.5 на Windows 7 и Windows 2008.

- Microsoft .NET Framework 2.0 на любой версии Windows.

Требования к конфигурации программного обеспечения см. в Приложении А.

1.3 Установка под Windows 2003 Server

1.3.1 Установка Internet Information Services (IIS) и Microsoft .NET Framework 2.0 под Windows 2003

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

Службы Internet Information Services 6.0 устанавливаются по умолчанию в системе Windows 2003 Server Standard Edition.

Внимание! Система репликации стабильно работает и проверена на IIS 6.0 под Windows 2003. Использование на серверах более ранних версий IIS и Windows не рекомендуется, так как они содержат программные ограничения в количестве подключений к серверу репликации, устаревшую систему авторизации, а также иную потоковую модель обслуживания клиентов. Чтобы установить IIS, необходимо для серверной операционной системы добавить роль «Сервер приложений» с включенным ASP.NET. Для этого необходимо нажать кнопку Пуск, выбрать команды «Панель управления \ Администрирование \ Управление сервером (Manage Your Server)».

Далее нажать кнопку «Add Or Remove A Role», добавить роль «Application Server (Сервер приложений)» и следовать появляющимся на экране инструкциям для установки и включения компонентов IIS.

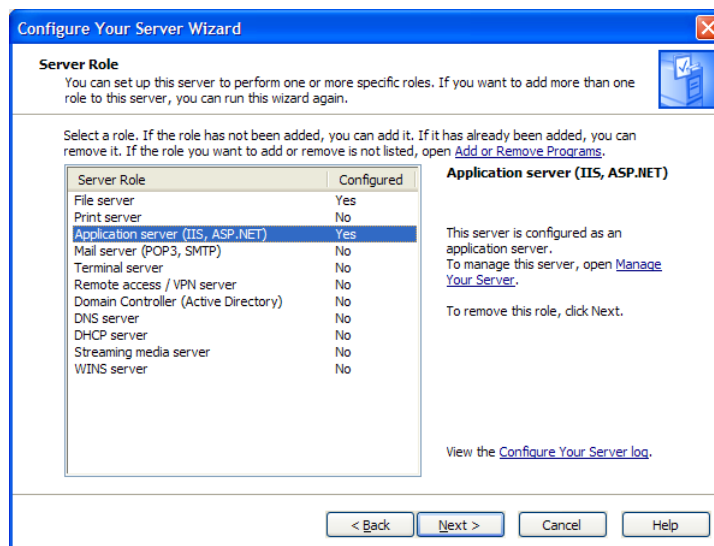


Рис. 1 –Установка роли сервера

Следующим этапом является установка **Microsoft .Net Framework 2.0**. Установить его необходимо либо с диска АПК «Бастион», либо загрузить с сайта Microsoft.

Если Microsoft .NET Framework 2.0 был установлен до IIS, то Microsoft .NET Framework 2.0 следует переустановить после установки IIS.

Более полную информацию по настройке IIS можно найти на общеизвестном сайте <http://www.codenet.ru/webmast/iis/iis.php>

1.3.2 Установка web-портала под Windows 2003

Для установки web-портала необходимо запустить `setup.exe` из подкаталога `Replication\ReplService`. Появится окно инсталлятора. Нажать кнопку «Далее»:

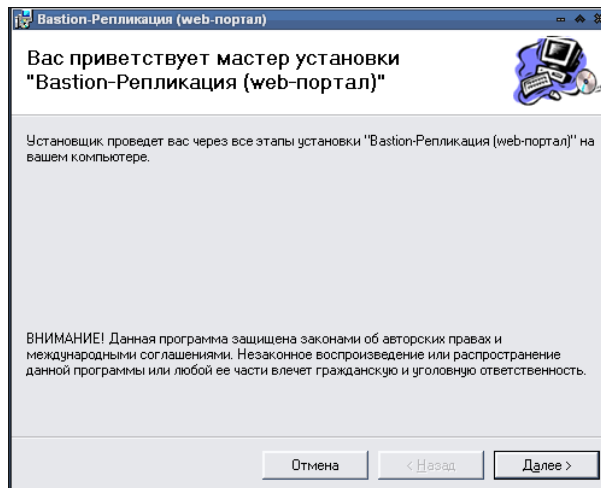


Рис. 2 –Установка web-портала

В следующем окне оставить параметры без изменения – веб-узел по умолчанию, имя виртуального каталога **NRepl** менять не рекомендуется.

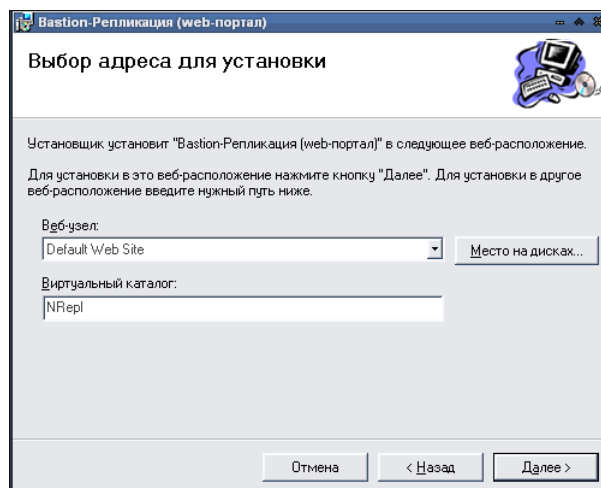


Рис. 3 –Установка web-портала

Нажать кнопку «Далее». Следовать инструкциям на экране и подтвердить установку. По окончании инсталляции нажать кнопку «Заккрыть».

1.3.3 Настройка web-портала в Internet Information Services под Windows 2003

Для настройки web-портала следует открыть консоль управления Internet Information Services (меню «Пуск \ Панель управления \ Администрирование \ Internet Information Services Manager»). Далее раскрыть дерево консоли до уровня веб-узла по умолчанию. Консоль должна иметь следующий вид (IIS 6.0):

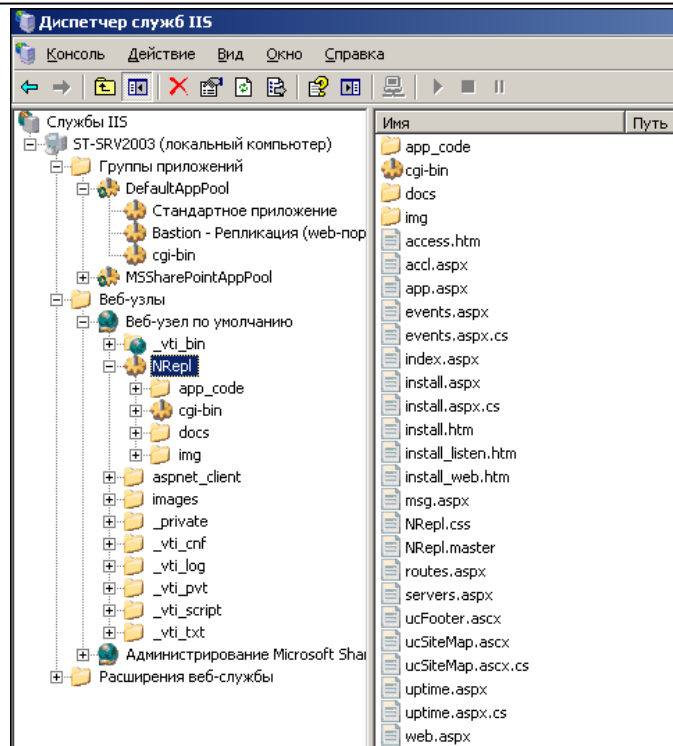


Рис. 4 - Консоль диспетчера служб IIS

Необходимо указать версию ASP.Net, под которой работает web-портал. Для этого необходимо нажать правую кнопку контекстного меню на узле «NRapl». Выбрать пункт «Properties». Открыть страницу «ASP.Net» и из списка «ASP.Net version» выбрать значение «2.0.50727». Результат выполнения показан ниже:

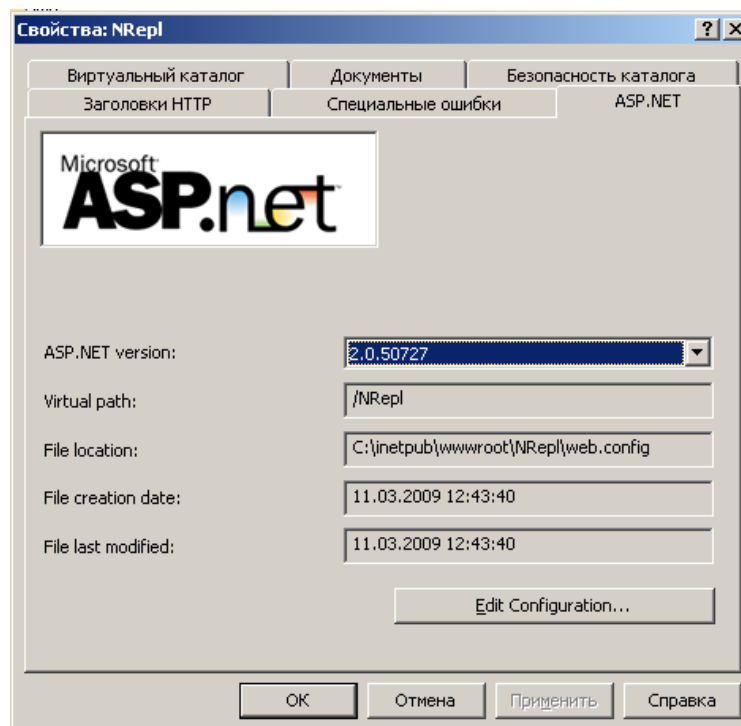


Рис. 5 - Установка версии ASP.Net

При использовании версии IIS 6.0 необходимо добавить web-сервис репликации в доверенные расширения сервера (*web service extensions*). Для этого необходимо:

- раскрыть узел *Web Service Extensions* в консоли управления IIS;
- добавить web-сервис кнопкой «Add a new Web service extension»;
- присвоить ему название «Nucleus Replication Server» в поле «Extension Name» открывшегося окна;
- выбрать файл *NRpl.dll* в папке *C:\inetpub\wwwroot\NRpl\cgi-bin*;
- установить галочку «Set status to allowed», разрешающую применение сервиса;
- нажать кнопку *OK*.

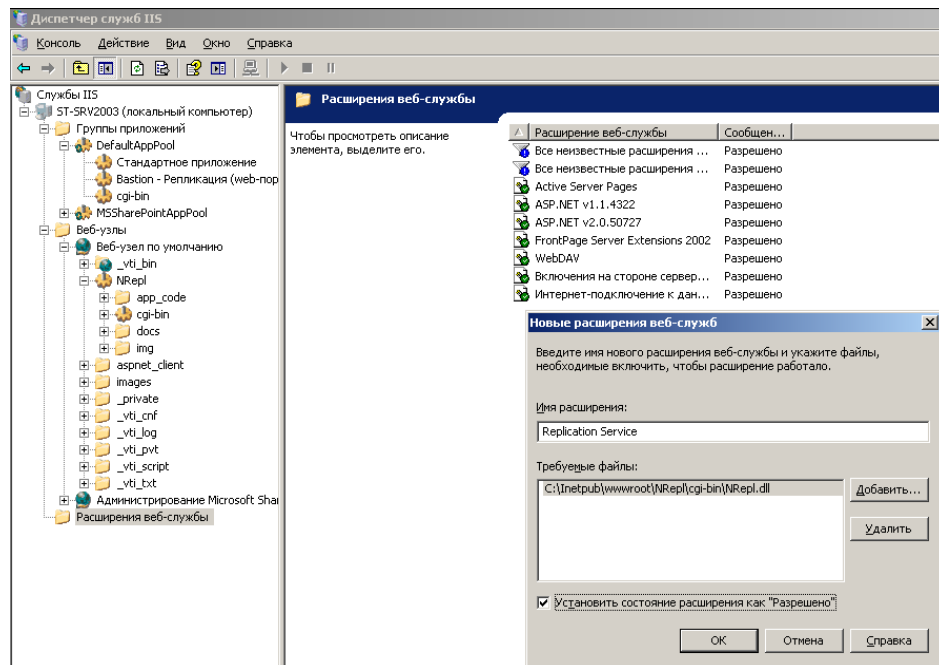


Рис. 6 - Консоль IIS в Windows 2003 Server

Также, в консоли IIS необходимо выделить элемент дерева «Web Service Extensions» и в правой части окна сервису ASP.NET v2.0.50727 необходимо установить статус «Allowed» («Разрешено»).

При использовании версии IIS 6.0 следует проверить настройки web-портала как процесса IIS. Папка *NRpl* должна отображаться иконкой **шестерёнки** – т.е. находится в пулах выполняемых приложений (чаще всего в *DefaultAppPool*). Это необходимо для того, чтобы при обращении к библиотеке web-сервиса сервер не воспринимал его как внешний файл.

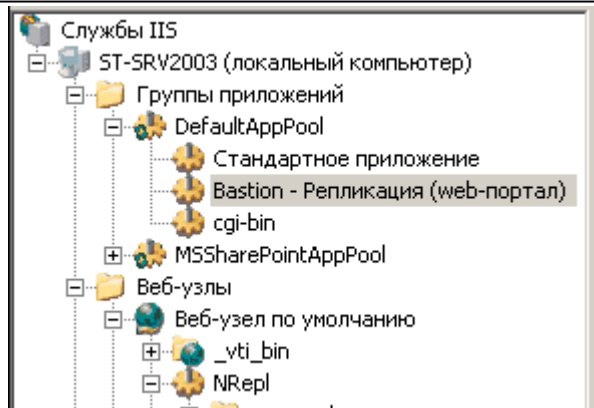


Рис. 7 - Фрагмент консоли IIS. Пул выполняемых приложений

Помещение папок в пулы IIS осуществляется кнопкой «Create» на странице «Directory» в свойствах папок IIS.

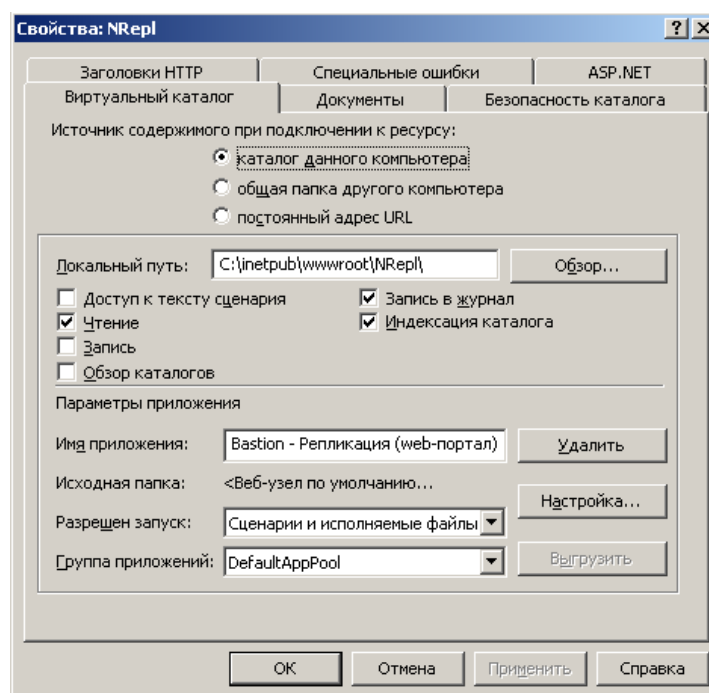


Рис. 8 - Свойства виртуального каталога

1.3.4 Настройка безопасности в Internet Information Services под Windows 2003

Система доступа должна пропускать разрешенные внешние входящие подключения от клиентов репликации. Наряду с этим, система должна блокировать все остальные подключения. Выполнить такое разграничение доступа можно, используя встроенную авторизацию Microsoft Windows.

Для этого необходимо открыть вкладку «Directory Security» в свойствах узла NRepl в консоли IIS.

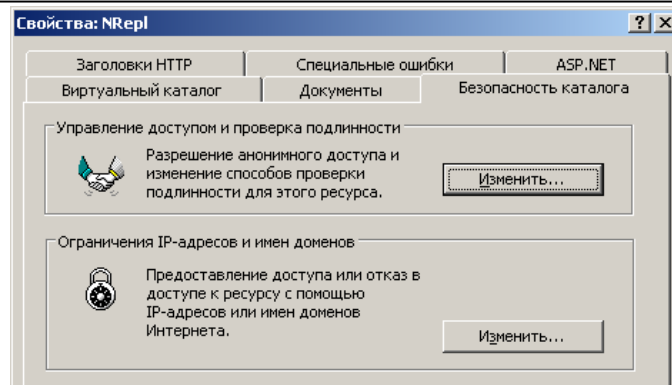


Рис. 9 - Безопасность виртуального каталога (Directory Security)

Далее нажать на кнопку «Edit anonymous access». Установить параметры следующим образом:

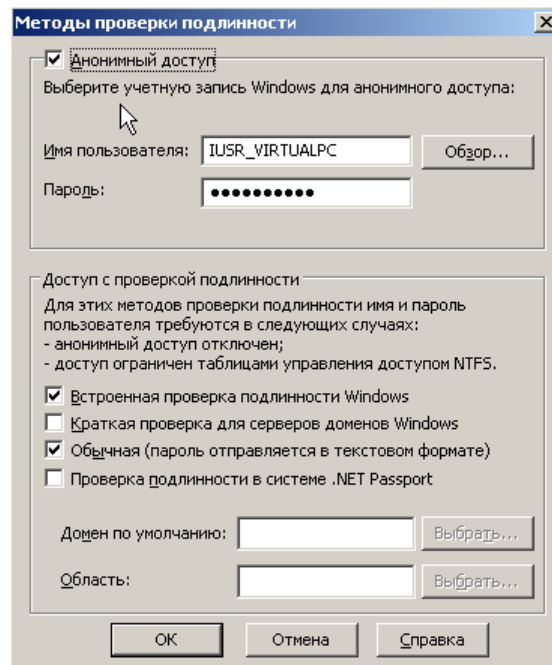


Рис. 10 - Безопасность виртуального каталога. Методы проверки подлинности

Если активна кнопка “Edit” в группе “IP address and domain name restrictions”, то в список разрешенных необходимо добавить рабочие станции, где установлены клиенты репликации.

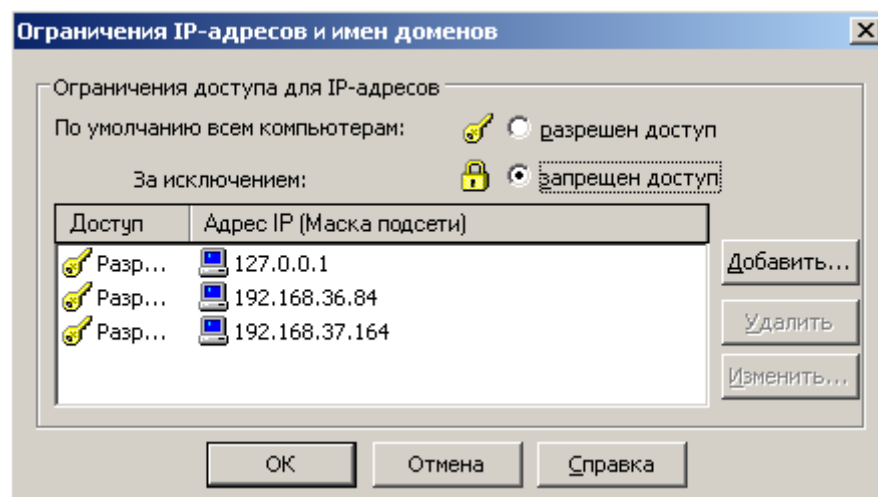


Рис. 11 - Безопасность виртуального каталога. Ограничения IP-адресов и имен доменов

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.

Выбрать методы авторизации следует таким образом, чтобы с клиентских рабочих станций и web-сервера были доступны web-портал в браузере и web-сервис с клиента репликации БЕЗ дополнительного окна ввода пароля.

Далее, следует выбрать разрешенные IP-адреса корпоративной сети, с которой пользователи, прошедшие встроенную проверку Windows, могут выполнять подключения клиентов и серверов репликации. Для этого нажать кнопку «Edit IP address...» и указать в списке все разрешенные рабочие станции сети, которые соответствуют серверам СУБД в сети.

1.4 Установка под Windows 7

1.4.1 Установка Internet Information Services (IIS) и Microsoft .NET Framework 2.0 под Windows 7

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

Службы Internet Information Services в системе Windows 7 имеют версию 7.5 и не устанавливаются по умолчанию.

Чтобы установить IIS в Windows 7, необходимо выполнить добавление компонентов для отображения web-сайтов. Для этого необходимо нажать кнопку Пуск, выбрать команды «Панель управления \ Программы и компоненты \ Включение\отключение компонентов Windows».

Далее, нужно включить узел «Службы IIS», а также вложенный узел в него узел «Средства управления веб-сайтом».

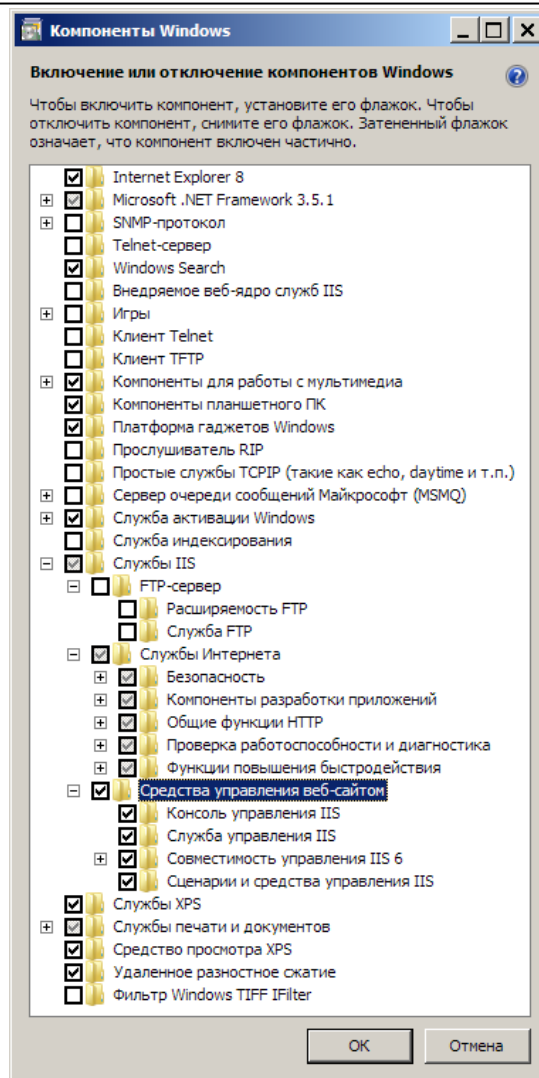


Рис. 1 –Добавление компонентов в Windows 7

Далее нажать кнопку «ОК» и следовать появляющимся на экране инструкциям для установки и включения компонентов IIS.

Следующим этапом установки является установка **Microsoft .Net Framework 2.0**. Установить его необходимо либо с диска АПК «Бастион», либо загрузить с сайта Microsoft.

Если Microsoft .NET Framework 2.0 был установлен до IIS, то Microsoft .NET Framework 2.0 следует переустановить после установки IIS.

Более полную информацию по настройке IIS можно найти на сайте <http://www.codenet.ru/webmast/iis/iis.php>

1.4.2 Установка web-портала под Windows 7

Для установки web-портала необходимо запустить setup.exe из каталога **Replication\ReplService**. Появится окно инсталлятора. Нажать кнопку «Далее».

В следующем окне нужно обязательно указать пул приложения как «*Classic .NET AppPool*». Остальные два параметра нужно оставить без изменения – веб-узел по умолчанию, имя виртуального каталога **NRepl** менять не рекомендуется.

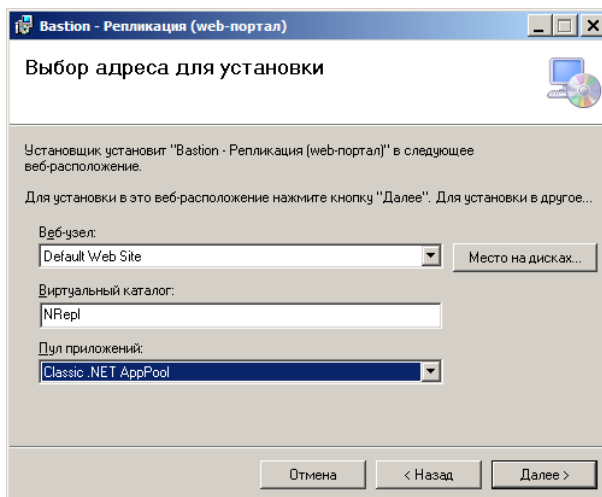


Рис. 12 –Установка web-портала

Нажать кнопку «Далее». Следовать инструкциям на экране и подтвердить установку. По окончании инсталляции нажать кнопку «Закреть».

1.4.3 Настройка web-портала в Internet Information Services под Windows 7

Для настройки web-портала следует открыть консоль управления Internet Information Services (меню «Пуск \ Панель управления \ Администрирование \ Диспетчер служб IIS»). Далее раскрыть дерево консоли до уровня веб-узла по умолчанию. Консоль должна иметь вид, подобный следующему (IIS 7.5):

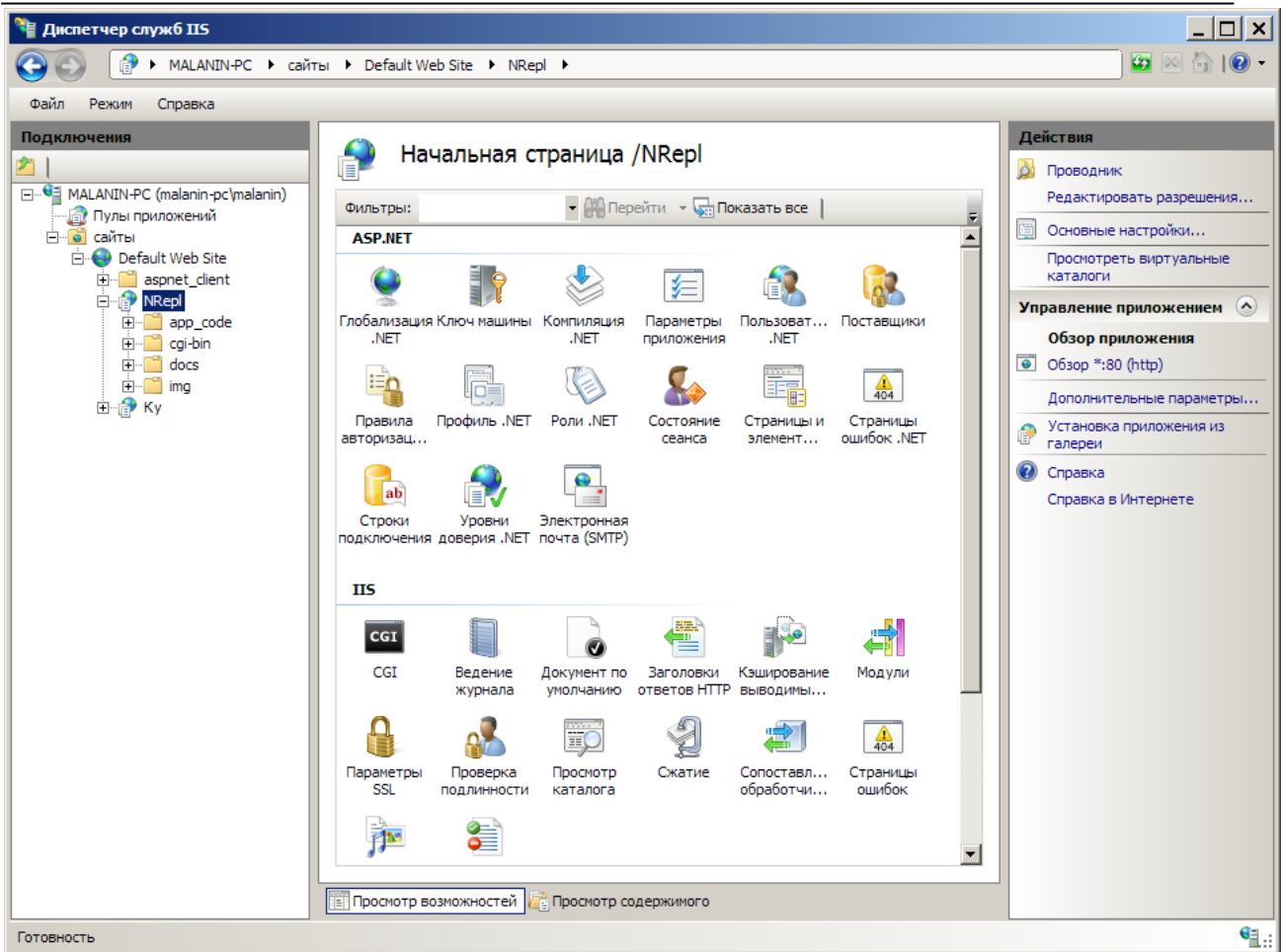


Рис. 13 - Консоль IIS под Windows 7

При использовании версии IIS 7.5 необходимо добавить web-сервис репликации в доверенные расширения сервера (*web service extensions*). Для этого необходимо:

- раскрыть узел сервера IIS в консоли управления IIS;
- открыть пункт «Ограничения ISAPI и CGI»;
- добавить web-сервис кнопкой «Добавить»;
- присвоить ему название «Nucleus Replication Server» в поле «Описание» открывшегося окна;
- выбрать файл NRepl.dll в папке C:\inetpub\wwwroot\NRepl\cgi-bin;
- установить галочку «Разрешить выполнение пути расширения», разрешающую применение сервиса;
- нажать кнопку ОК.

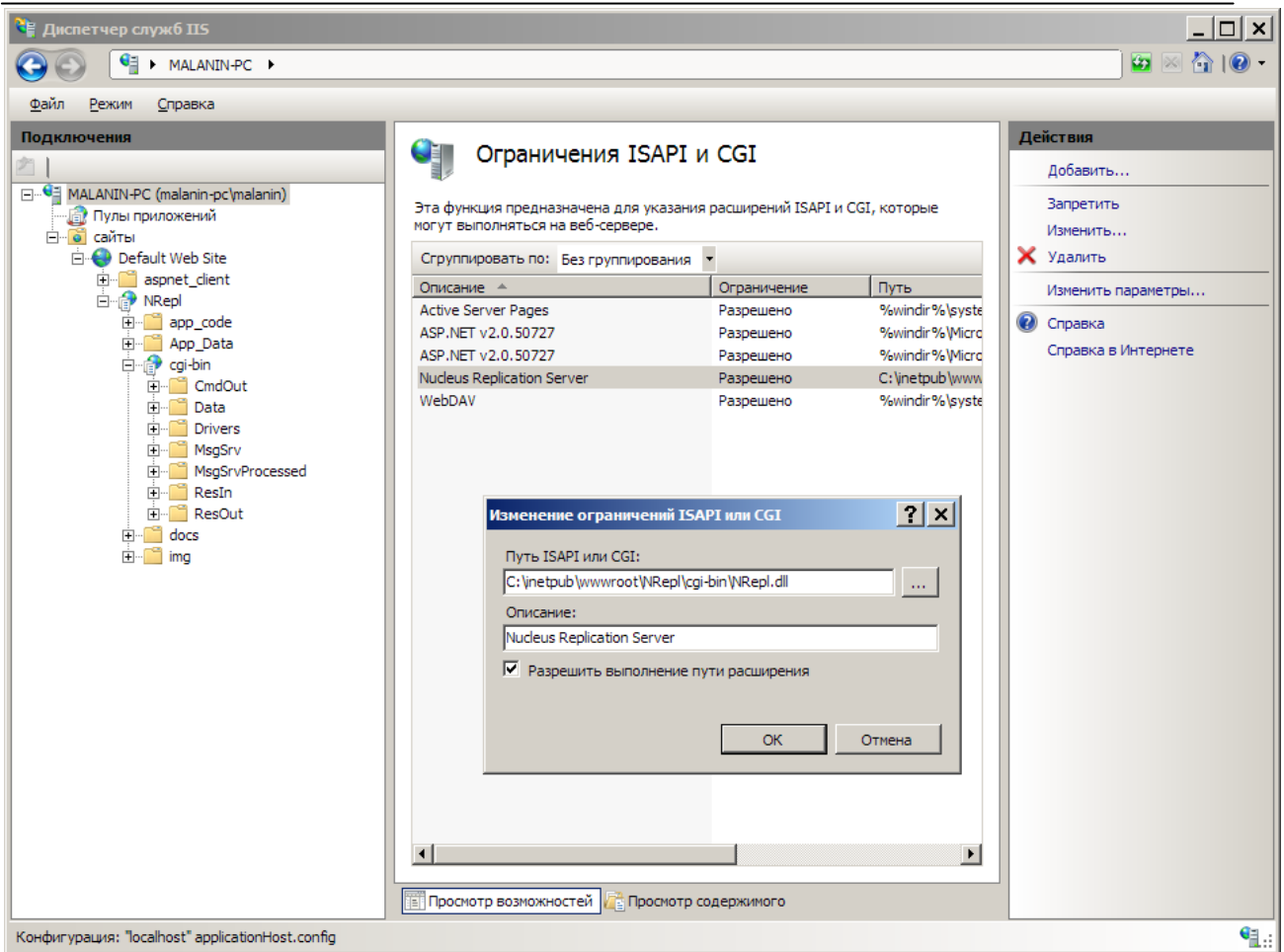


Рис. 14 - Консоль IIS под Windows 7. Изменение ограничений ISAPI или CGI

После завершения установки портала и настройки безопасности необходимо проверить доступ к web-порталу и web-сервису с каждой рабочей станции и сервера, открыв ссылку

[http://\[имя сервера или IP-адрес\]/NRepl](http://[имя сервера или IP-адрес]/NRepl)

в браузере Microsoft Internet Explorer.

1.5 Установка компонентов под Windows 2008

1.5.1 Установка Internet Information Services (IIS) и Microsoft .NET Framework 2.0 под Windows 2008

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

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 Start, выбрать команды «Administrative Tools \ Server Manager».

Далее, открыть узел «Roles» и нажать кнопку «Add Roles».

Далее, добавить роль «Web Server IIS», следуя инструкциям по добавлению этой роли в мастере.

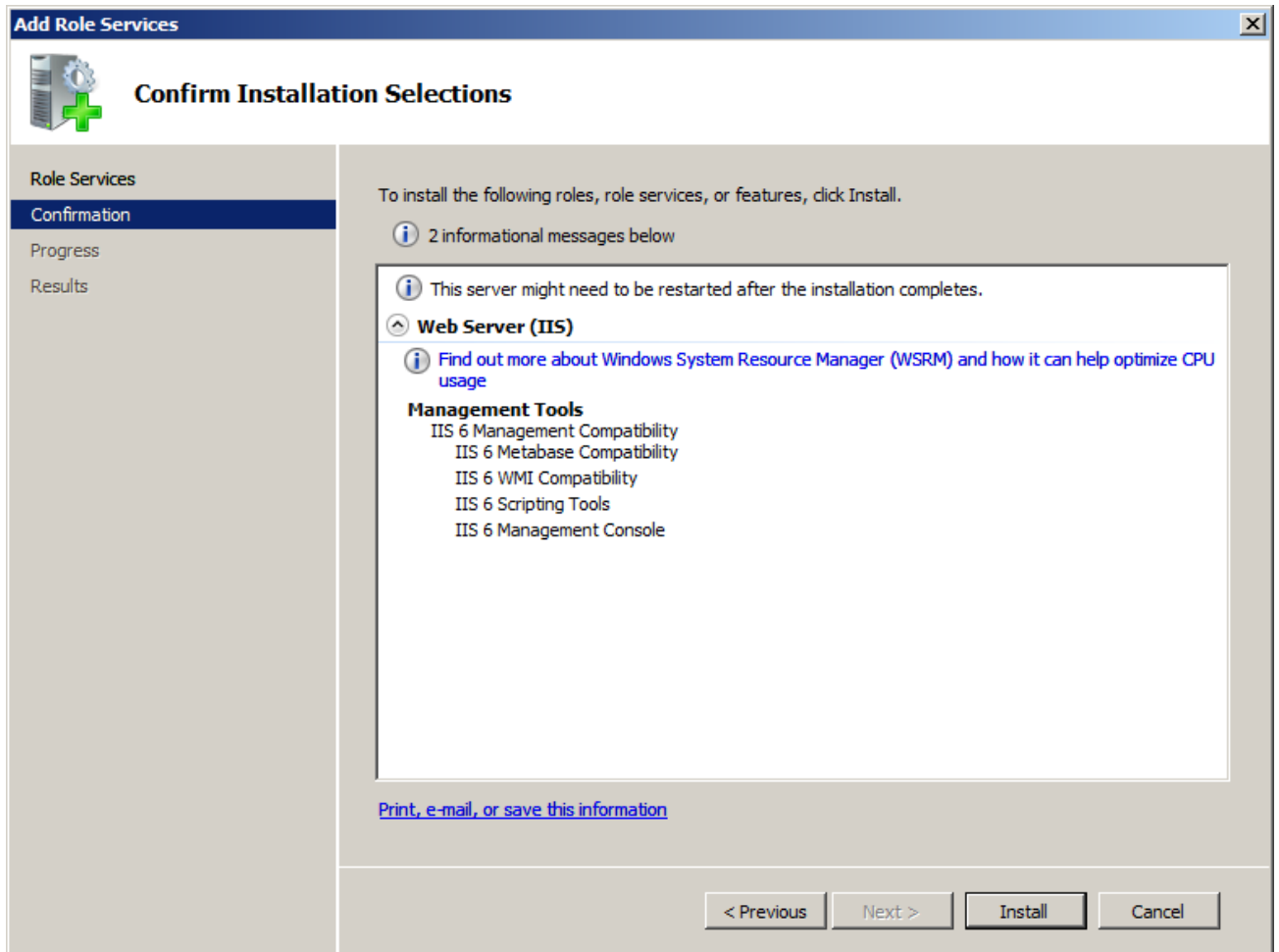


Рис. 16 – Добавление служб ролей для Windows 2008

После успешного добавления роли нужно нажать кнопку «Add Role Services» у роли «Web Server IIS» и отметить узел «IIS 6 Management Compatibility» со всеми вложенными элементами.

Далее, подтвердить установку указанных служб роли и дождаться окончания установки.

После выполнения указанных действий список ролей сервера должен выглядеть следующим образом:

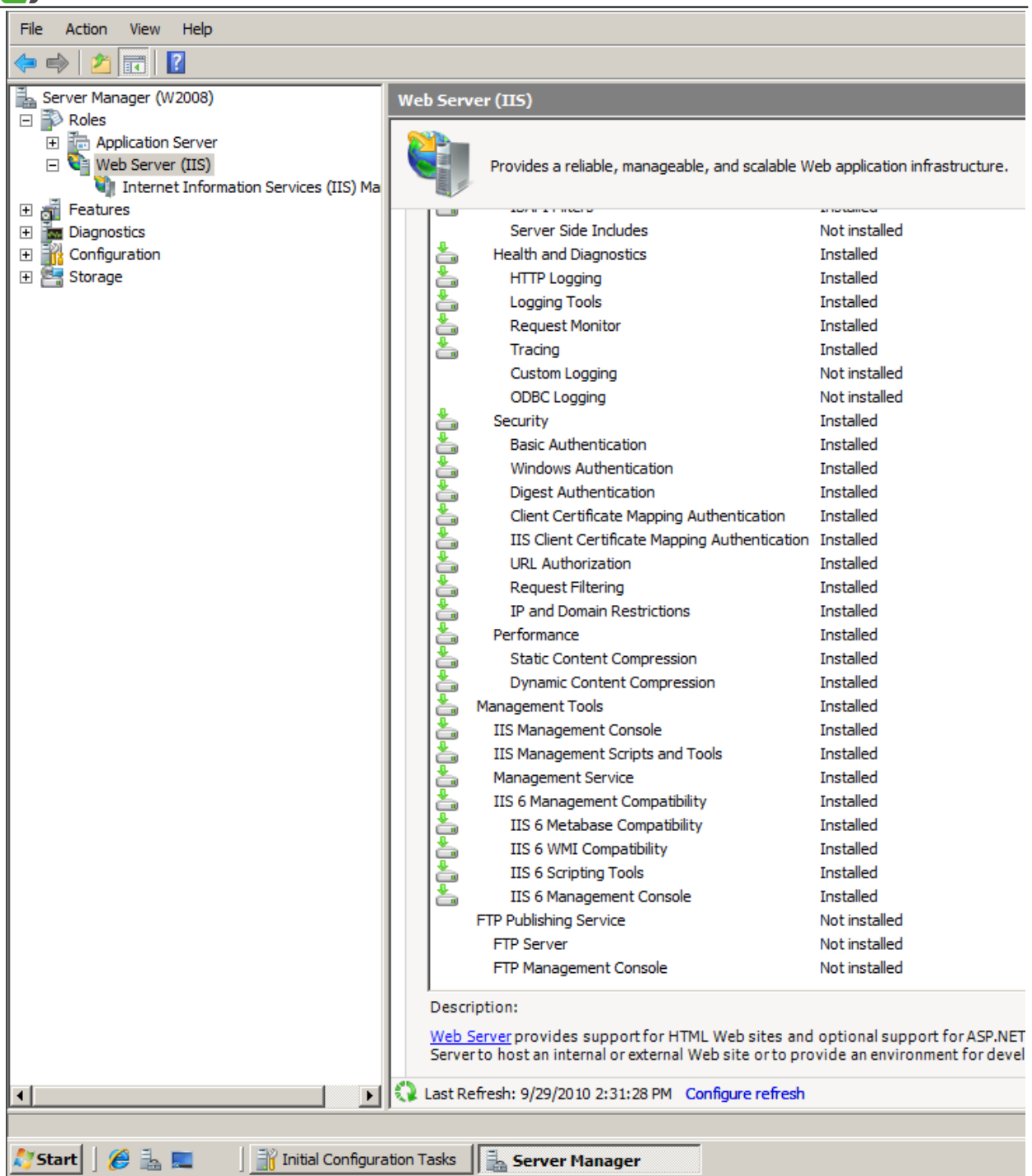


Рис. 16 –Список ролей сервера Windows 2008

Следующим этапом установки является установка **Microsoft .Net Framework 2.0**. Установить его необходимо либо с диска АПК «Бастион», либо загрузить с сайта Microsoft.

Если Microsoft .NET Framework 2.0 был установлен до IIS, то Microsoft .NET Framework 2.0 следует переустановить после установки IIS.

Более полную информацию по настройке IIS можно найти на сайте <http://www.codenet.ru/webmast/iis/iis.php>

1.5.2 Установка web-портала под Windows 2008

Для установки web-портала необходимо запустить `setup.exe` из каталога `Replication\ReplService`. Появится окно инсталлятора. Нажать кнопку «Далее».

В следующем окне нужно обязательно указать пул приложения как «*Classic .NET AppPool*». Остальные два параметра нужно оставить без изменения – веб-узел по умолчанию, имя виртуального каталога **NRepl** менять не рекомендуется (см. Рис. 12).

Нажать кнопку «Далее». Следовать инструкциям на экране и подтвердить установку. По окончании инсталляции нажать кнопку «Закреть».

1.5.3 Настройка web-портала в Internet Information Services под Windows 2008

Для настройки web-портала следует открыть консоль управления Internet Information Services (меню «Пуск \ Панель управления \ Администрирование \ Диспетчер служб IIS»). Далее раскрыть дерево консоли до уровня веб-узла по умолчанию. Консоль должна иметь следующий вид:

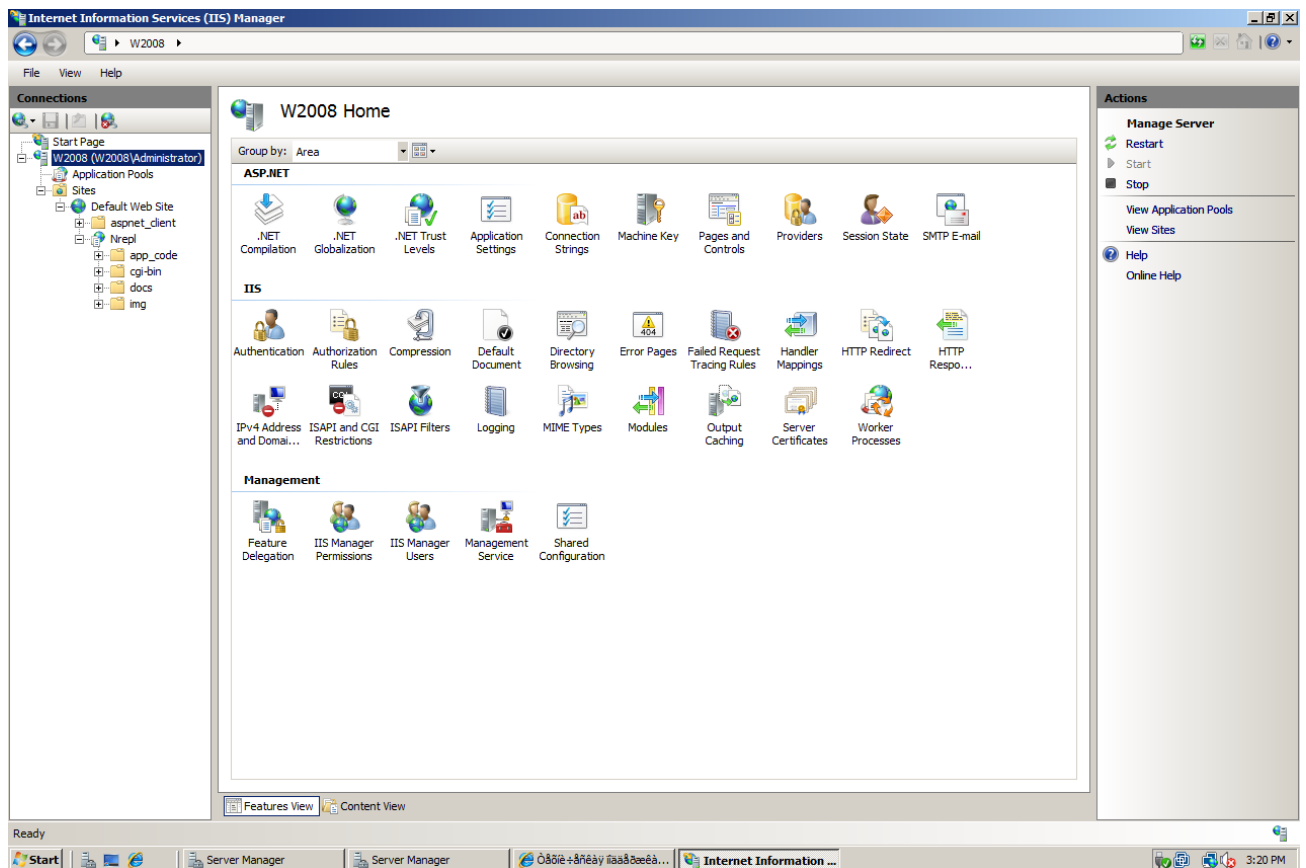


Рис. 15 - Консоль IIS под Windows 2008

При использовании версии IIS 7.5 необходимо добавить web-сервис репликации в доверенные расширения сервера (*web service extensions*). Для этого необходимо:

- раскрыть узел СЕРВЕРА IIS в консоли управления IIS, как правило имя компьютера;
- открыть двойным щелчком ярлычок «ISAPI and CGI Restrictions» / «Ограничения ISAPI и CGI» в группе «IIS»;

- добавить разрешающий фильтр web-сервис, нажав правую кнопку мыши в поле и выбрав команду «Add...» / «Добавить...»;
- в поле «Путь ISAPI и CGI» выбрать файл NRepl.dll в папке C:\inetpub\wwwroot\NRepl\cgi-bin;
- в поле «Описание» присвоить разрешающему фильтру название «Bastion Replication Server» в открывшемся окне;
- в поле «Разрешить выполнение пути расширения» установить флажок;
- нажать кнопку ОК.

Для запуска web-портала на платформах Windows 7 64 bit и Windows 2008 Server 64 bit необходимо включить поддержку 32-битных приложений CGI, которым и является web-портал. Для этого необходимо выполнить следующие действия:

- открыть узел в консоли с названием «Пулы приложений»
- выбрать элемент «Classic .NET AppPool» двойным щелчком левой кнопкой мыши
- свойства этого элемента должны быть такими, как указано на изображении:

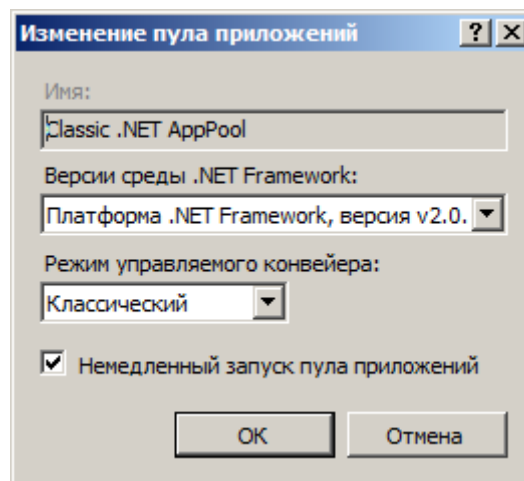


Рис. 16 – Свойства пула приложений

- нажать на кнопку ОК, закрыв окно свойств.
- нажать правой кнопкой на элементе «Classic .NET AppPool»
- выбрать элемент «Дополнительные параметры»
- установить флажок «Разрешены 32-разрядные приложения»
- нажать на кнопку ОК, закрыв окно параметров.

1.6 Добавление web-портала в доверенную зону

В зависимости от корпоративной политики предприятия может потребоваться добавление web-портала в доверенную зону.

Если нажатие на кнопку редактирования списка серверов на первой странице портала не приводит к видимым изменениям (кнопка «не откликается»), это означает что для web-портала запрещено выполнение Java-скриптов.

В этом случае необходимо зайти в меню браузера Internet Explorer «Сервис \ Свойства обозревателя» и переключиться на вкладку «Безопасность». Далее, необходимо выбрать зону «Местная интрасеть» или «Доверенные узлы» и добавить в доверенные узлы web-портал. Сделать это можно в окне «Узлы», указав нужный URL в поле «Добавить в зону следующий узел» и нажав кнопку «Добавить».

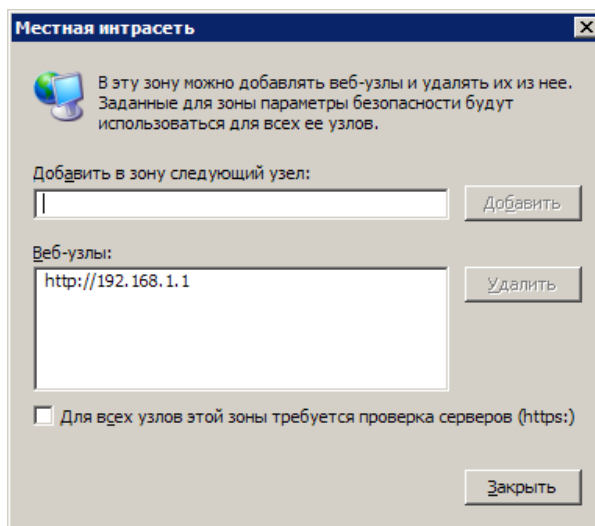


Рис. 17 - Доверенные зоны

После этого страницу с web-порталом требуется обновить.

1.7 Самоидентификация сервиса репликации и настройка NTFS

Самоидентификация сервиса репликации нужна для того, чтобы web-сервис смог принимать подключения клиентов и осуществлять маршрутизацию сообщений.

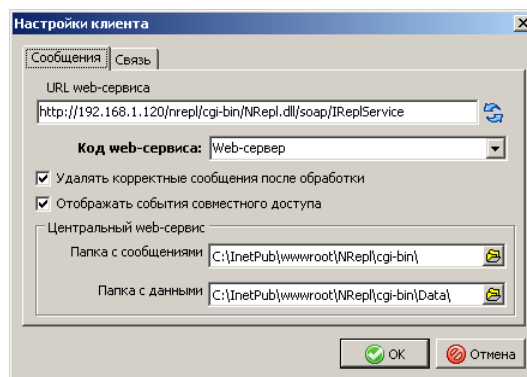
Для самоидентификации необходимо:

1. Запустить утилиту настройки веб-сервиса, которая располагается в меню «Пуск \ Все программы \ Бастион-Репликация \ Настройка web-сервиса»,
2. При первом запуске утилита спросит IP-адрес компьютера в сети, где установлен web-портал. При вводе можно использовать значение localhost.
3. Код web-сервиса в открывшейся форме «Настройки клиента» будет не определен. Необходимо закрыть утилиту настройки нажатием кнопки «ОК».
4. После этого будет выдано сообщение о том, что сейчас будут прописаны NTFS-права для пользователей IIS. После подтверждения будет выполнен командный файл, который автоматически проведет всю необходимую настройку прав NTFS. После окончания настройки прав NTFS web-портал станет доступным для редактирования.

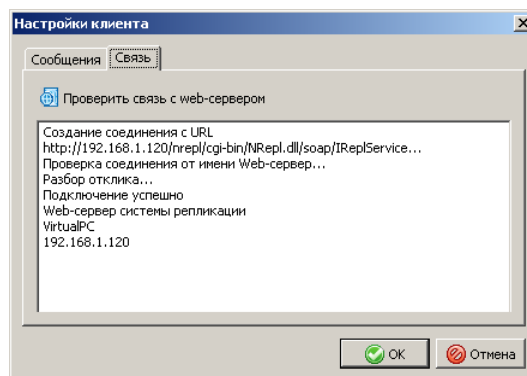
Для дальнейшей проверки все папки и файлы поддиректории NRerpl будут иметь полный доступ для следующих пользователей (обязательно согласуйте это с администратором интернет и корпоративной сети):

- ASPNET,
- NETWORK SERVICE,
- IUSR_<Имя компьютера>,
- IWAM_<Имя компьютера>,
- SYSTEM,
- Администраторы,
- СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ.

5. Далее на web-портале на странице «Клиенты» необходимо прописать IP-адрес и имя компьютера, где располагается web-сервис (в домене либо в рабочей группе).
6. После этого необходимо повторно запустить утилиту настройки веб-сервиса, которая располагается в меню «Пуск \ Все программы \ Бастион-Репликация \ Настройка web-сервиса».
7. После корректного ввода отобразится окно:



8. Если в поле «Код web-сервиса» стоит определенное значение, значит настройка выполнена правильно. После этого необходимо перейти на страницу «Связь» и выполнить проверку связи. После этого будет вновь выполнена настройка прав NTFS. Необходимо дождаться окончания выполнения командного файла.



После завершения самоидентификации можно переходить к настройке схемы репликации.

2 Настройка схемы репликации

2.1 Создание описания для клиентов репликации

Настройка схемы репликации заключается в определении и создании описания для каждого из клиентов. Перед этим должны быть выяснены организационные вопросы определения участников:

1. Какие сервера СКУД с установленным серверным АПК «Бастион» будут участвовать в системе репликации?
2. Будут ли базы пропусков синхронными, или одна база будет главной и наиболее полной, а все остальные содержать только филиальных работников?
3. Необходимо ли будет передавать изменения пропусков обратно в центральную базу?
4. Можно ли организовать сетевой доступ по протоколу http к web-сервису для всех участников репликации?

После выяснения этих вопросов можно создавать описания для каждого участника. Создание описания будет пояснено на примере. Для включения одного клиента в систему репликации необходимо:

1. Войти на web-портал по ссылке

http://[имя сервера]/NRepl

2. Перейти на страницу «Серверы/клиенты». Страница имеет следующий вид:

Клиенты системы репликации в филиалах

Главная 1. Клиенты 2. Группы доступа 3. Журнал сообщений Техническая поддержка Учет рабочего времени Видео

+ Добавить ✖ Удалить выбранное

Код сервера	Сокращение	Наименование сервера	IP-адрес	Имя компьютера в сети	Роль	
NSRV	Web-сервер	Web-сервер системы репликации НИЦ ФОРС	192.168.1.114	NucleusSrv	Web-сервис	
NUCL	NSRV	NucleusSRV	192.168.1.114	nucleussrv.fors.elsystems.ru	Клиент	
MAL	Mal	Маланин	192.168.1.97	malanin.fors.elsystems.ru	Клиент	
DSL	DevDSL	DevelopDSL	192.168.1.117	developdsl.fors.elsystems.ru	Клиент	
ST	STAROSTIN	Старостин		starostin.fors.elsystems.ru	Клиент	

Строка для подключения: <http://nucleussrv/NRepl/cgi-bin/NRepl.dll/soap/IRepService>

© 2001-2007
 Ассоциация «ЭЛЕКТРОННЫЕ СИСТЕМЫ»
 г.Самара, ул. Советской Армии, д. 217
 (846) 927-99-00, e-mail: _____

Система репликации персонала АПК "Бастион"

Рис. 18 - Список участников репликации

3. Нажать кнопку «Добавить». В таблицу будет добавлена строка с кодом «-1».

-1	Новый	Не указано			Клиент	
----	-------	------------	--	--	--------	--

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

-1	<input type="text" value="Новый"/>	<input type="text" value="Не указано"/>	<input type="text"/>	<input type="text"/>	Клиент	
----	------------------------------------	---	----------------------	----------------------	--------	--

5. Ввести в соответствующие столбцы описание участника (для примера):

- код (NEW_S),
- сокращенное наименование (Пример),
- полное наименование (Новый клиент),
- IP-адрес (для автоматического определения клиента самим собой) (192.168.1.213),
- имя компьютера участника в корпоративной сети (для автоопределения клиента) (SamplePC),
- роль участника из списка (Клиент).

6. По окончании ввода нажать кнопку  «Сохранить». Таблица примет вид:

NEW_S	 Пример	Новый клиент	192.168.1.213	SamplePC.fors.elsystems.ru	Клиент	
-------	--	--------------	---------------	----------------------------	--------	---

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

2.2 Группы доступа

Группа доступа – это глобальный уровень доступа, для которого в каждом клиенте репликации определяется свой локальный уровень доступа. Например, можно определить группу доступа «Руководство», для которой в центральном офисе будет поставлен в соответствие уровень доступа «Везде», а в филиалах – уровень доступа «Руководство». Уровни доступа в локальных БД АПК «Бастион» будут устанавливаться при репликации пропусков автоматически, в соответствии с заданными правилами.


Общий список групп доступа создается и хранится на web-сервере. А в каждом клиенте репликации можно установить соответствия уровней доступа из локальной БД АПК «Бастион» и глобальных групп доступа. Таблица этих соответствий хранится в БД АПК «Бастион».

Таким образом, каждому реплицируемому пропуску в системе ставится в соответствие группа доступа.

Каждая из групп доступа имеет текстовое название и *корпоративный код*, уникальный в сети предприятия. Список групп доступа хранится на web-портале.

Сервер системы репликации поставляется со встроенной группой доступа с кодом «ГОСТИ». Это можно увидеть на странице портала «Группы доступа».

Внимание! Группу доступа «ГОСТИ» удалять нельзя.

 **Группы доступа**

Главная 1. Клиенты 2. Группы доступа 3. Журнал сообщений Техническая поддержка Учет рабочих мест

 Добавить  Удалить выбранное Групп доступа 1 из 1 << < Страница 1 из 1 > >>

Наименование группы доступа	Корпоративный код	
Гостевая группа доступа	ГОСТИ	 

© 2001-2007
Ассоциация «ЭЛЕКТРОННЫЕ СИСТЕМЫ»
г.Самара, ул. Советской Армии, д. 217
(846) 927-99-00, e-mail: Система репликации персонала АПК "Бастион"

Рис. 19 - Группы доступа на web-портале

Если требуется добавить группы доступа, необходимо нажать кнопку «Добавить» и ввести название и корпоративный код группы.

Список групп доступа обновляется с web-сервера в АПК «Бастион» при каждом запуске или перезапуске клиентов репликации на местах.

Примечание:

- Изменение наименования группы доступа с сохранением корпоративного кода приведет к обновлению наименования групп доступа в базах данных на клиентах репликации.
- Изменение корпоративного кода в любом случае приведет к созданию новой группы доступа на клиентах репликации. Это сделано для того, чтобы исключить возможность потери данных при передаче от клиента к клиенту с разными сведениями. В этом случае неиспользуемые группы доступа необходимо будет удалять на клиентах вручную.

3 Установка клиента репликации

После того, как была завершена установка web-сервиса и заполнена схема репликации, можно выполнять установку клиентов репликации **на серверах БД АПК «Бастион»**.

Клиент репликации устанавливается **один на объект** – только на сервер БД АПК «Бастион» в головной СКУД и только на сервер БД каждой из филиальных СКУД.

3.1 Требования к ПК клиента

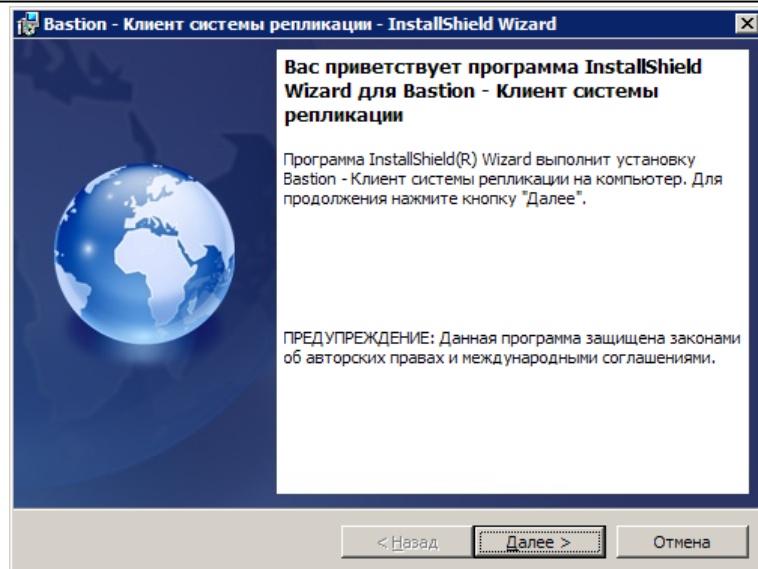
Технические и программные требования согласно списку технических требований АПК «Бастион».

- Установленный на ПК клиента АПК «Бастион» версии не ниже 1.6.0.6.
- Наличие сетевого соединения.
- Наличие доступа из браузера Internet Explorer к web-порталу репликации по ссылке **http:// [Имя сервера] / NRepl**
- Наличие доступа из браузера Internet Explorer к web-сервису репликации **http:// [Имя сервера] / NRepl / cgi-bin / NRepl.dll**

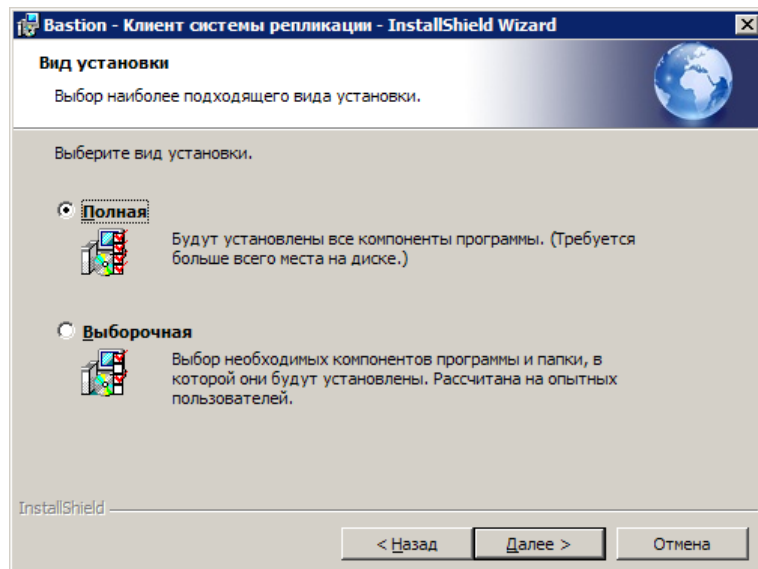
3.2 Установка клиента

Для установки участника необходимо:

1. Убедиться в том, что рабочая станция, которую требуется подключить к системе репликации, логически внесена администратором в корпоративную сеть предприятия и схему репликации (на странице «Клиенты» web-портала). Необходимо узнать идентификатор соответствующего ей подключаемого клиента.
2. Убедиться в наличии связи с web-сервисом системы (п. 4 в п. 3.1). Для этого войти на web-портал в соответствии со своими правами доступа и на странице "Техническая поддержка" нажать кнопку "Проверить связь с web-сервисом".
3. Запустить инсталляцию системы репликации **setup.exe**:



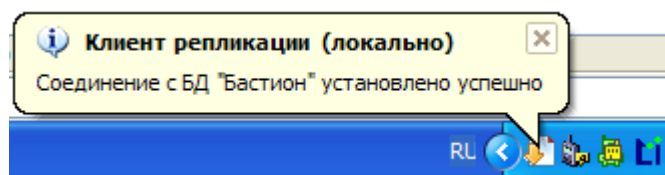
4. Установить полный набор компонентов:



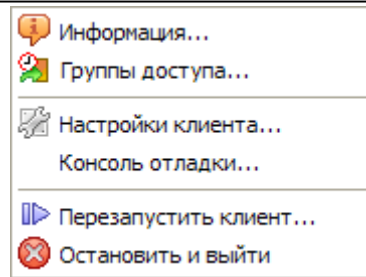
5. Запустить из меню "Пуск \ Программы \ Бастион \ Сервис отладки" пункт "Запустить сервис отладки". Подтвердить прохождение файла запуска нажатиями кнопки ОК.

3.3 Настройка клиента

1. Запустить из меню "Пуск \ Программы \ Бастион" пункт "Клиент системы репликации". При запуске клиент будет запущен в локальном режиме в области системных часов, т.е. без подключения к web-сервису.

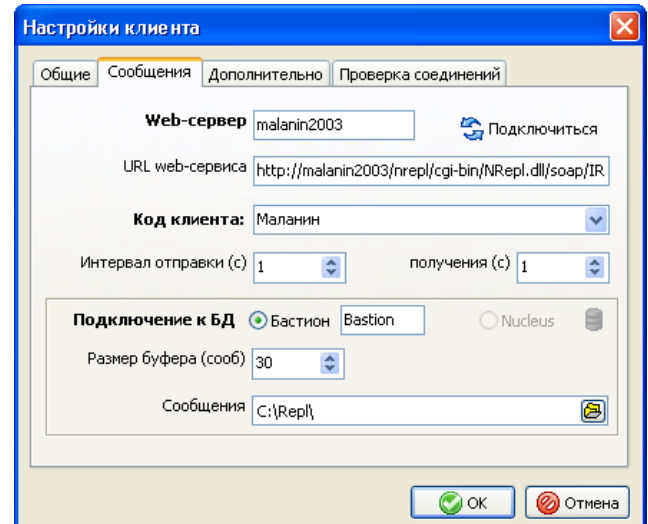
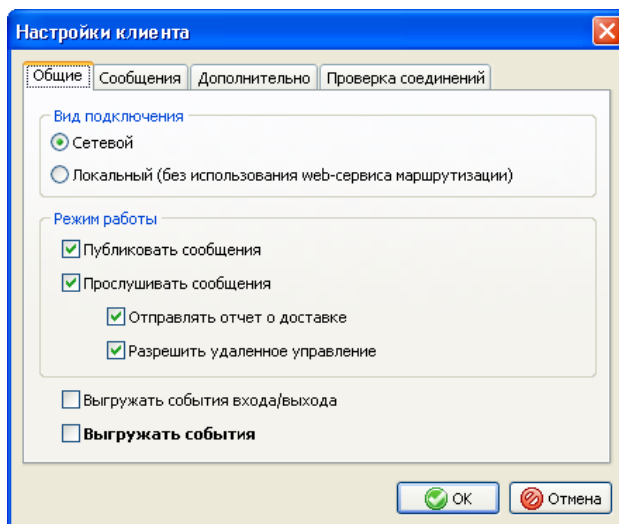



2. Выбрать в контекстном меню клиента пункт «Настройки клиента».

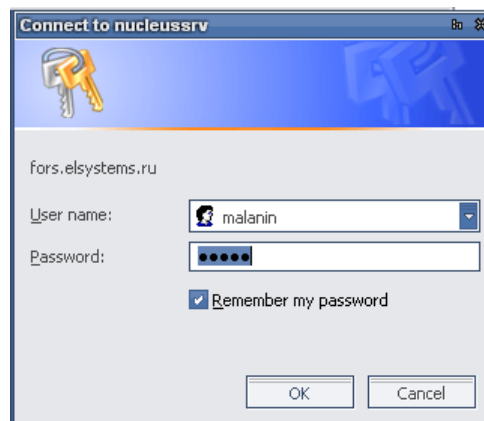


3. Перевести клиент в сетевой режим:


- установить вид подключения «Сетевой» на первой странице «Общие»,
- ввести имя web-сервера системы репликации на второй странице «Сообщения» в поле «Web-сервер».




4. Нажать кнопку  Подключиться . В окне подключения к web-сервису указать данные своей авторизации, которые использовались для доступа сайту, как на рисунке ниже: *Если последовало сообщение об ошибке и недоступности сервера, следует обратиться к системному администратору и выяснить, почему отсутствует соединение.*



5. В поле «Код клиента» автоматически появится идентификатор подходящего клиента согласно схеме репликации на сервере – *клиент должен идентифицировать сам себя (то есть, найти соответствующую себе запись в схеме репликации на web-сервере)*. В поле "URL web-сервиса" строка подключения к web-сервису сформируется автоматически.

Web-сервер  Подключиться







URL web-сервиса

Код клиента: 

http://[имя сервера репликации в сети]/nrepl/cgi-bin/NRepl.dll/soap/IReplService.

6. Клиент может не идентифицировать сам себя по следующим причинам:
 - не удалось выполнить подключение к web-сервису (запрещено firewall-ом, либо неверно указан адрес, либо служба IIS отключена или остановлена, либо по прочим ограничениям безопасности)
 - в схему репликации не внесена рабочая станция с клиентом репликации,
 - в схеме репликации неверно указан IP-адрес рабочей станции,
 - в схеме репликации неверно указано имя рабочей станции в сети предприятия.


В этом случае в списке "Код клиента" появятся все имеющиеся клиенты репликации и необходимо выбрать из списка необходимый, например:

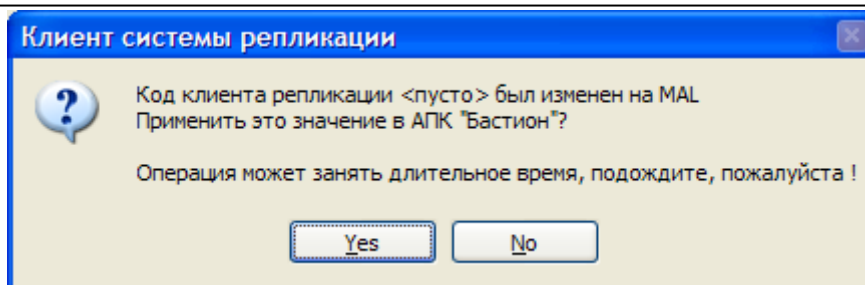
Malanin Слуш 			
	NSRV	NUCLEUS-сервер	Web-сервер NucleusSRV
	And_P	AndreyK Публ	Публ из Бастиона с AndreyK
	Mal_P	Malanin Публ	Публ из Бастиона с Malanin
	And_L	AndreyK Слуш	Слуш в Бастион на AndreyK
	Mal_L	Malanin Слуш	Слуш в Бастион на Malanin

7. Тип БД участника установить - "Бастион". В поле справа от него ввести имя псевдонима базы данных (алиаса), который используется для подключения локальной БД АПК "Бастион", которая будет принимать входящие сообщения и инициализировать СКУД. Обычно это имя «Bastion».
8. Дополнительно, на второй вкладке установить параметры, запускать ли клиента вместе с Windows и спрашивать ли подтверждение клиента при выходе.
9. Выполнить пункты проверки соединений с БД и web-сервисом на третьей вкладке.

Создание соединения с URL
 http://nucleussrv/nrepl/cgi-bin/NRepl.dll/soap/IReplService...
 Проверка соединения от имени Mal...
 Разбор отклика...
 Подключение успешно
 Web-сервер системы репликации НИЦ ФОРС
 nucleussrv.fors.elsystems.ru
 192.168.1.114

Проверка соединения с БД Bastion...
 Подключение успешно

10. После этого нажать кнопку . Система запросит подтверждение, чтобы сообщить АПК «Бастион» новый код клиента репликации. Это необходимо, чтобы АПК «Бастион» начал формировать сообщения репликации. Следует ответить утвердительно на этот вопрос, если действия настройки клиента не являются тестовыми, проверочными или ошибочными.



11. Клиент репликации будет автоматически перезапущен.

Внимание! Во время своей работы клиент будет перезапускаться каждые 60 минут. Это время можно изменить, отредактировав параметр *RestartInt* в файле *NRepl.ini*.

Если после выполнения настроек возникают ошибки, необходимо проверить:

- все введенные параметры,
- строку соединения с web-сервисом,
- права на участие в системе репликации,
- существуют ли сконфигурированные по умолчанию папки сообщений.

3.4 Настройка групп доступа в клиентах репликации

В сетевом режиме клиент репликации будет получать новые группы доступа с web-сервиса при каждом запуске. Об этом он будет сообщать во всплывающей подсказке, если группы доступа на web-портале были добавлены или изменены.

Внимание! Каждой группе доступа с помощью клиентов репликации в каждой из СКУД АПК «Бастион» необходимо сопоставить локальный уровень доступа. Иначе соответствующие входящие пропуска не будут привязываться к локальному уровню доступа и попадать в контроллеры СКУД.

Для настройки групп доступа из контекстного меню клиента репликации следует выбрать пункт «Группы доступа». Откроется следующая форма:

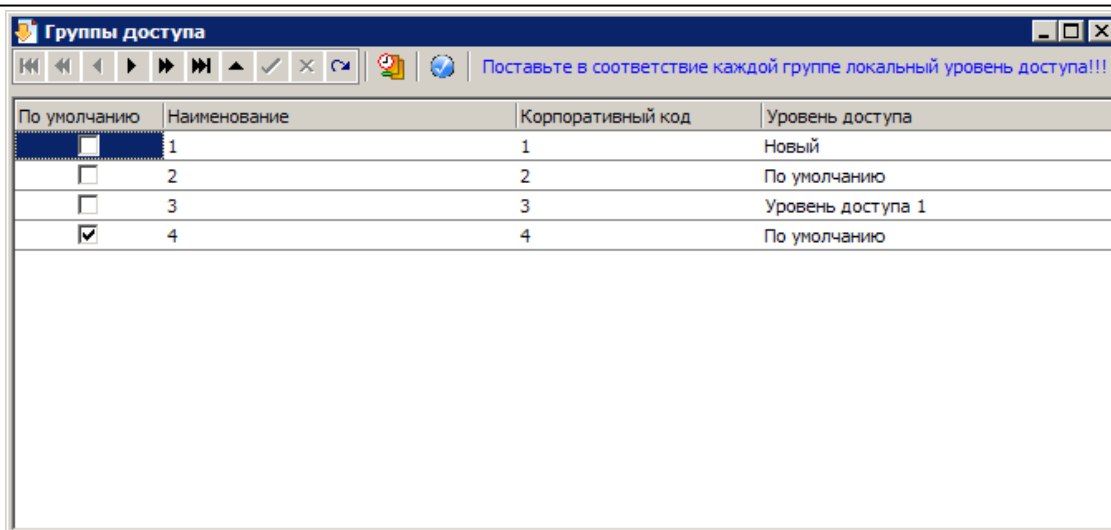


Рис. 20 - Группы доступа на клиенте репликации

После чистой установки АПК «Бастион» группа доступа ГОСТИ по умолчанию всегда соответствует уровню доступа «По умолчанию». Если требуется изменить уровень доступа, необходимо выделить ячейку столбца «Уровень доступа», щелкнуть левой кнопкой мыши один раз, после чего раскрыть появившийся список доступных уровней и выбрать нужный.

Внимание! В системе может существовать группа доступа по умолчанию. Это означает, что все новые работники будут реплицироваться на другие объекты с этой группой. Если группа доступа по умолчанию не указана, все новые работники будут сохраняться только локально – только на данном объекте.

Внимание! Для полного и одновременного слияния баз данных персонала двух и более объектов необходимо выполнить групповую операцию присвоения группы доступа всем работникам ДО ПРИСВОЕНИЯ маршрута по умолчанию всем «своим» записям, описанного в п. **Ошибка! Источник ссылки не найден..**

4 Настройка репликации в АПК «Бастион»

4.1 Разграничение диапазонов табельных номеров

По умолчанию АПК «Бастион» формирует табельные номера для новых заявок со стартового значения 0000000001. Поэтому следует учитывать, что в процессе создания заявок и выдачи пропусков неизбежно возникнет конфликт уникальности табельного номера в пределах каждой из СУБД филиалов.

Внимание! Диапазоны табельных номеров необходимо разграничивать между клиентами репликации во избежание конфликтов репликации.

Для разграничения диапазонов необходимо:

1. Пронумеровать филиалы, участвующие в системе репликации. Филиалы не должны иметь повторяющихся номеров.
2. Открыть окно «Конфигурация \ Общие настройки...» АПК «Бастион».

3. Перейти на узел «Пропуска \ Корпоративные коды»
4. Указать «Номер филиала для «своих» работников».
5. В каждом филиале нажать кнопку «Внести в табельные номера», чтобы внести номер филиала в табельные номера работников.
6. Нажать кнопку ОК.

Номер филиала вставляется в табельный номер, начиная с седьмой позиции в строке. Таким образом, для филиала с номером 1 табельные номера будут иметь вид: 1000001, для филиала с номером 2 – 2000001 и т.д.

Внимание! При выполнении этой операции табельные номера сохраняют только последние шесть знаков. Символы, начиная с седьмого, будут заменены на номер филиала.

Внимание! Эту процедуру нужно сделать ДО включения репликации в АПК «Бастион», пока все работники отмечены как «свои». Такая последовательность действий необходима для предотвращения обратной репликации работников в чужие филиалы после перенумерования.

4.2 Настройка общих параметров репликации

Настройка общих параметров модуля «Бастион-Репликация» производится в меню «Конфигурация \ Общие настройки» на странице «Репликация и персональные данные». Настройку параметров репликации в АПК «Бастион» следует производить после создания схемы репликации (см. документ «Бастион-репликация. Руководство инсталлятора»).

Так как основой репликации персональных данных служит протоколирование их изменений, то в первую очередь необходимо задать требуемый режим протоколирования изменений ПД на странице «Общие» в группе «Персональные данные».

Протоколировать только основные операции – в этом режиме сообщения репликации формироваться не будут, расширенный протокол изменений ПД выключен. При этом протоколироваться будут только основные операции с пропусками, такие как Создание, Выдача, Возврат пропуска. Изменения значений отдельных полей не протоколируются.

Вести расширенный протокол изменений – в этом режиме будут протоколироваться все изменения ПД, но клиент репликации не будет подключаться к web-сервису для обмена данными. Этот режим может использоваться в случае интеграции с кадровой системой, когда необходимо переносить изменения ПД из АПК «Бастион» во внешнюю систему. Также, этот режим может использоваться просто для сохранения расширенного протокола изменений ПД.

Включить репликацию на web-сервер и вести расширенный протокол изменений – в этом режиме будут протоколироваться все изменения ПД, а клиент репликации будет подключаться к web-сервису для обмена данными. Именно в этом режиме должна работать репликация между филиалами.

Флаг «Разрешить изменять записи с «чужих» серверов» определяет, разрешается ли в данном филиале изменение данных пропусков, поступивших с других филиалов.

Флаг «Разрешить команду «Повторить репликацию» для «чужих» записей» определяет, будет ли доступна оператору кнопка «Повторить репликацию» для «чужих» записей во всех формах изменения реплицируемых записей.

Флаг «Реплицировать временные/разовые пропуска» позволяет включить/отключить функцию репликации для этих типов пропусков.

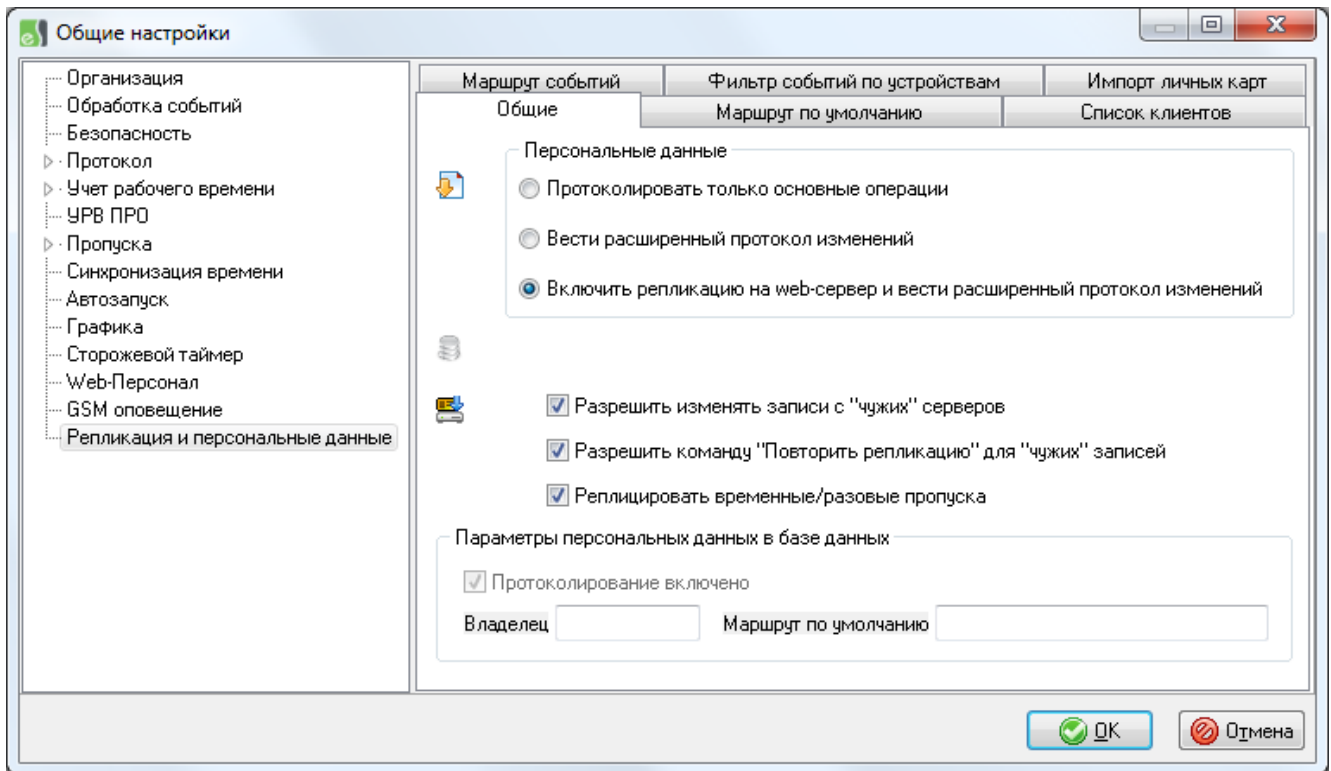


Рис. 21. Вкладка "Общие" настройки репликации и персональных данных

Дополнительно, права на работу с «чужими» записями могут быть ограничены полномочиями пользователей.

4.3 Настройка маршрута по умолчанию

На вкладке «Маршрут по умолчанию» следует указать тех клиентов, которым будут передаваться сообщения об изменениях пропусков из этого филиала по умолчанию.

Если возникнет необходимость выдать и отправить пропуск в филиал, который не входит в маршрут по умолчанию, то потребуется указать этот филиал в форме выдачи пропуска.

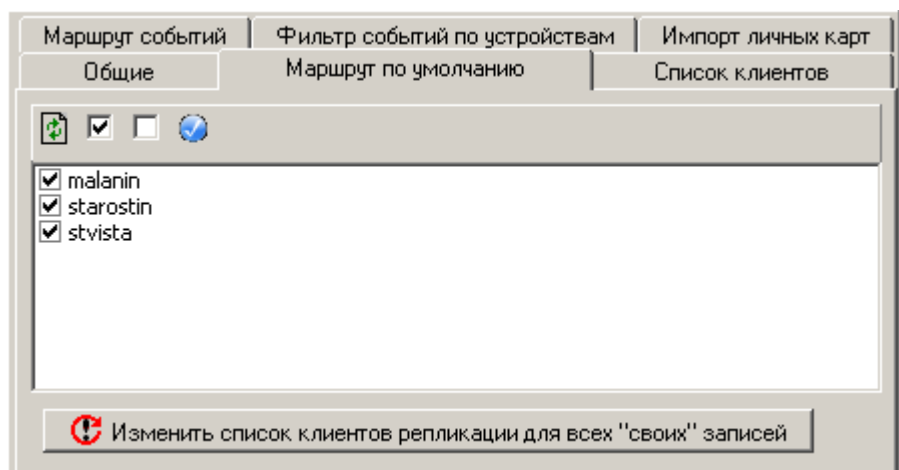





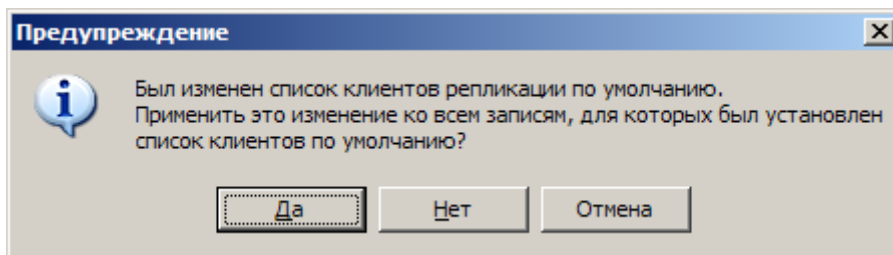


Рис. 22. Вкладка "Маршрут по умолчанию"

Пункты панели инструментов описаны в таблице.

Изображение	Описание
	<p>При изменении списка клиентов репликации для всех «своих» записей произойдет отправка ВСЕХ без исключения пропусков текущего филиала по текущему маршруту по умолчанию.</p> <p>Внимание! Использовать эту функцию следует на начальном этапе настройки, для отправки всех пропусков из текущей БД в филиалы. В остальных случаях пользоваться данной функцией следует с особой осторожностью, только если вы точно понимаете, зачем это нужно.</p>
	Обновить список клиентов в текущем окне.
	Включить всех клиентов в маршрут по умолчанию.
	Очистить маршрут по умолчанию.
	Отобразить в списке клиентов актуальный на данный момент маршрут по умолчанию.

В случае изменения маршрута по умолчанию система выдаст запрос:



При утвердительном ответе пользователя для всех записей со старым маршрутом по умолчанию будет установлен новый маршрут. Это приведет к выполнению репликации всех существующих записей на все новые клиенты, добавленные к маршруту.

В случае ответа «Нет» новый маршрут по умолчанию будет применяться только к новым записям.

На вкладке «Список клиентов» (см. Рис. 23) представлена информация о клиентах, указанная на web-сервисе. Данные в этой таблице формируются web-сервисом репликации, иллюстрируют схему репликации и служат для наглядности.

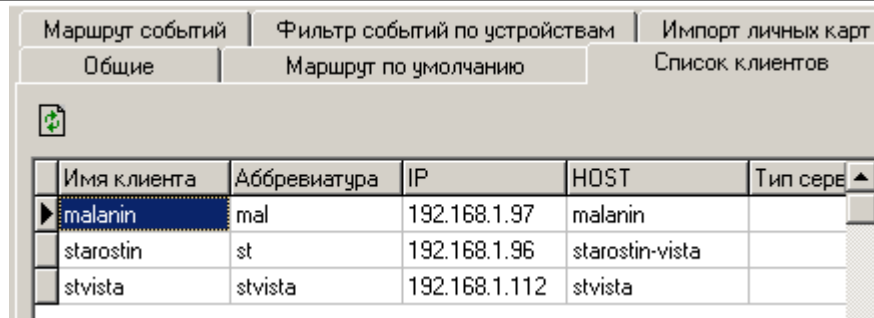


Рис. 23 Вкладка "Список клиентов"

4.4 Настройка прав пользователей АПК «Бастион»

В системе предусмотрены возможности разграничения прав пользователей к функциям системы репликации. Для настройки прав пользователей выберите пункт меню «Конфигурация \ Полномочия пользователей» и перейдите на страницу «Репликация» (Рис. 24).

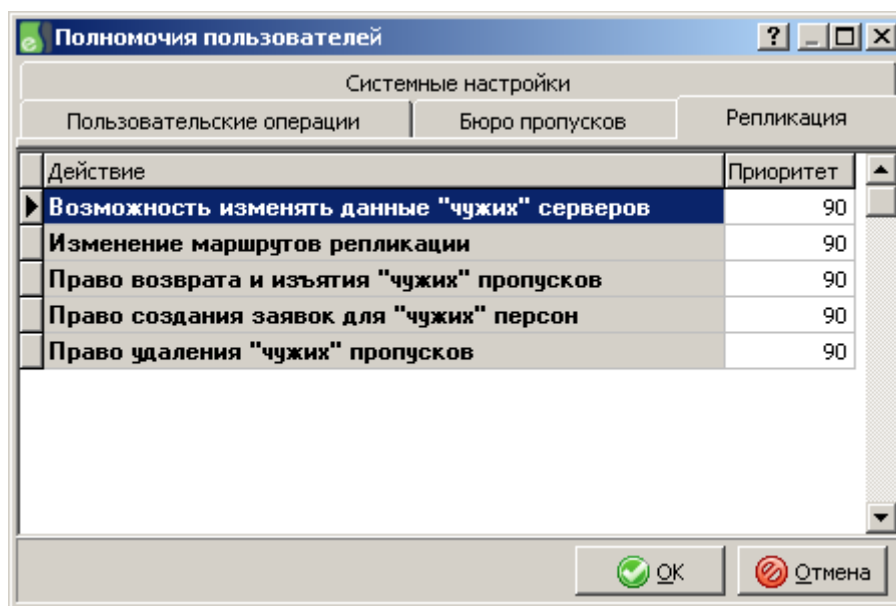


Рис. 24. Настройка полномочий пользователей для системы репликации

Возможность изменять данные «чужих» серверов. Определяет минимальный необходимый уровень полномочий оператора для изменения записей, добавленных системой репликации с других филиалов. (Также, должна быть включена настройка «Разрешить изменять записи с «чужих» серверов», см. п. 4.2).

Изменение маршрутов репликации. Определяет минимальный необходимый уровень полномочий оператора для изменения маршрутов репликации для записей вручную.

Право возврата и изъятия «чужих» пропусков. Определяет минимальный необходимый уровень полномочий оператора для операций возврата и изъятия пропусков, добавленных системой репликации с других филиалов.

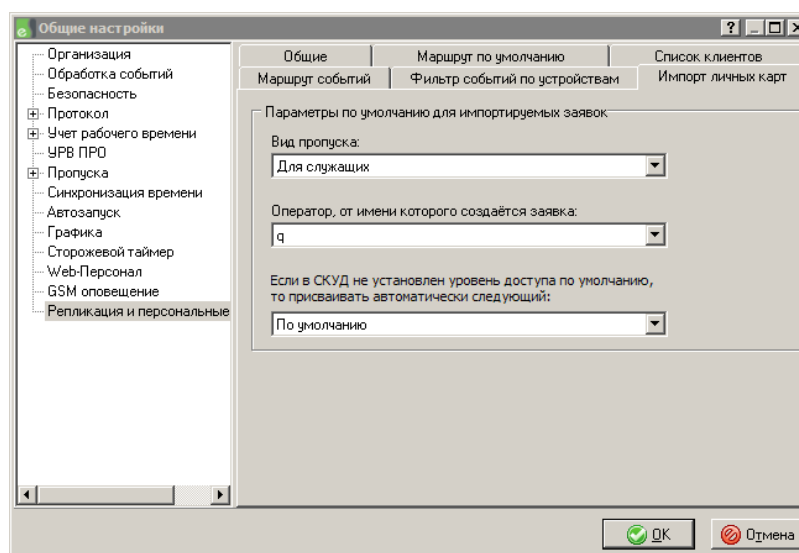
Право создания заявок для «чужих» персон. Определяет минимальный необходимый уровень полномочий оператора для создания новых заявок для персон, хранящихся в архиве и добавленных системой репликации с других филиалов.

Право удаления «чужих» пропусков. Определяет минимальный необходимый уровень полномочий оператора для удаления из архива пропусков, добавленных системой репликации с других филиалов.

4.5 Настройка локального импорта личных карт и их изменений

Система репликации в локальном режиме может использоваться для импорта сведений о персонале из систем кадрового учета.

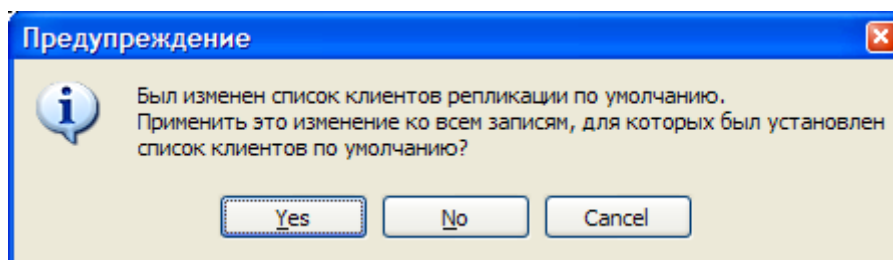
При этом на странице «Импорт личных карт» следует указать необходимые параметры для АПК «Бастион».



Уровень доступа будет присваиваться работнику в следующей последовательности:

1. Соответственно *корпоративному коду УД*, указанному во входящей xml-выгрузке для работника.
2. Если не указан первый, то будет присвоен УД, установленный по умолчанию *для организации и подразделения*.
3. Если не указаны первые два, то будет присвоен УД, установленный по умолчанию *глобально*.
4. Если не указаны первые три, будет присвоен УД *с данной формы настройки*.

После проведения настроек необходимо нажать кнопку ОК. Будет задан вопрос:



Внимание! Следует выбрать «Да», если требуется реплицировать уже существующие записи с использованием нового маршрута по умолчанию. Эта операция влечет за собой начало

процесса объединения баз данных участников репликации и может занимать продолжительное время.

Следует выбрать «Нет», если действия производятся на чистой СКУД, носят пробный характер, либо не требуется реплицировать существующий персонал и события по маршруту по умолчанию.

4.6 Настройка локального экспорта личных карт и их изменений

Система репликации в локальном режиме может экспортировать сведения о персонале и их изменения в XML-формате.

Для этого сервер СКУД протоколирует все действия в бюро пропусков и выгружает их лишь в XML-формат без отправки на web-сервис. Этот режим называется режимом «внешнего простого экспорта».

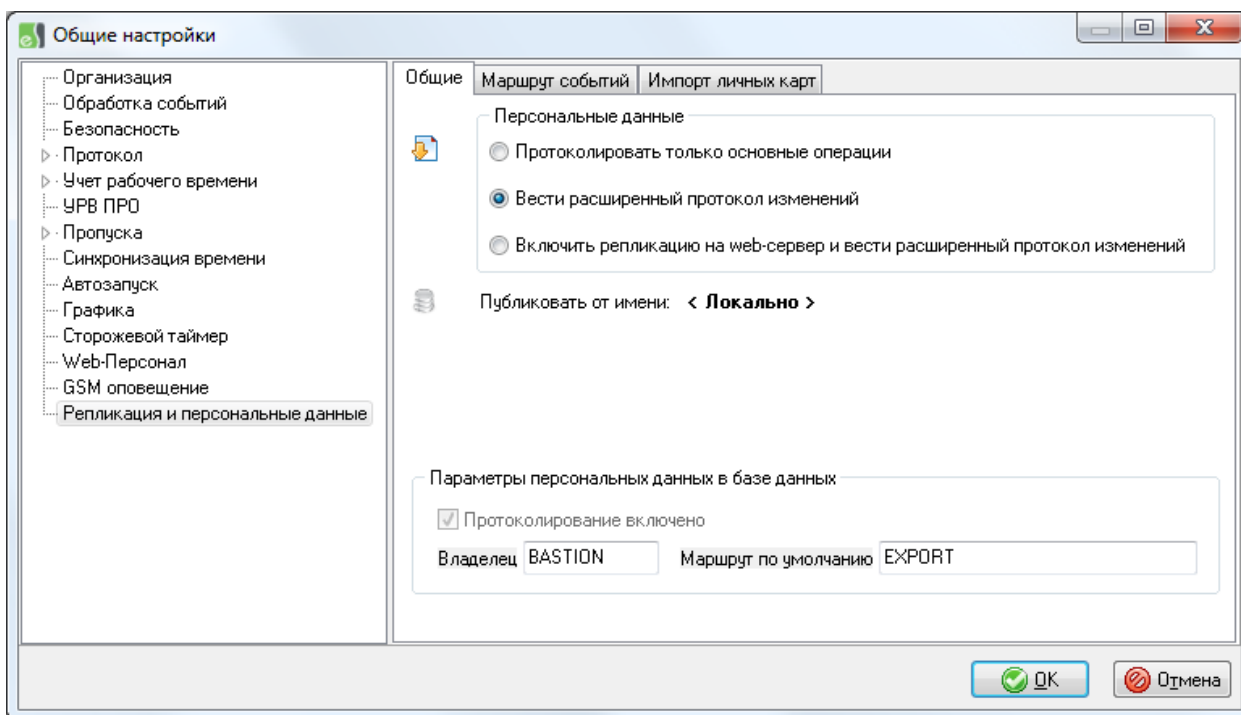
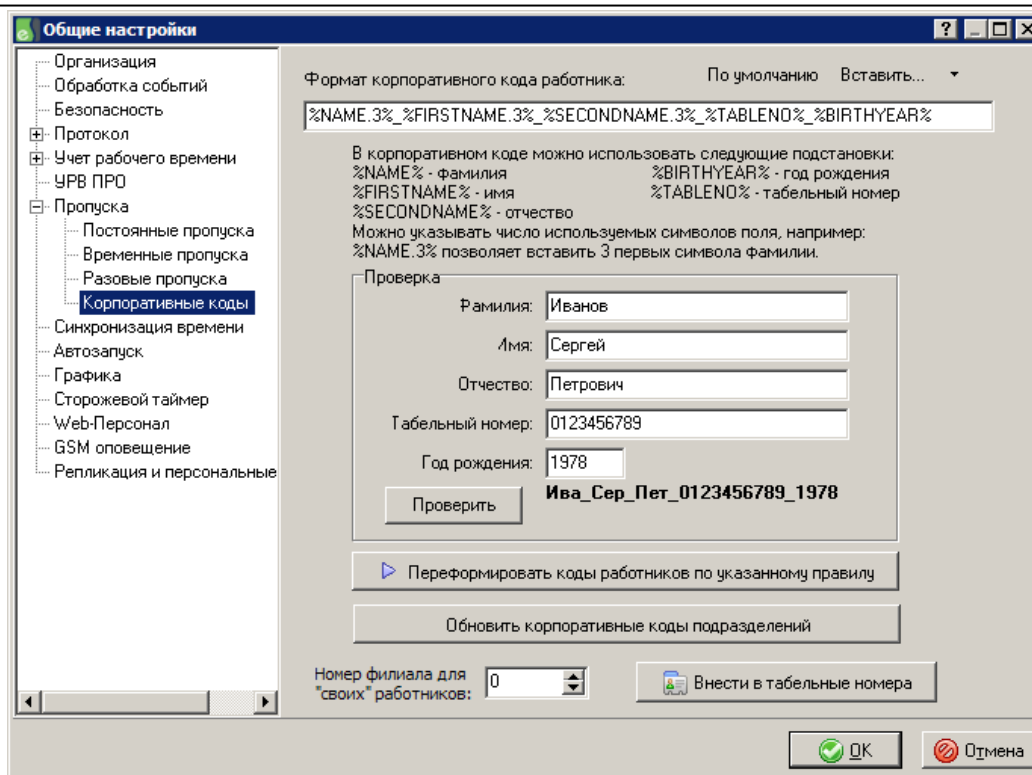


Рис. 25 - Включение режима внешнего простого экспорта

4.7 Схема формирования корпоративного кода

На этой вкладке также можно настроить правила формирования корпоративного кода работника для обеспечения его уникальности в пределах схемы репликации.



Для репликации между АПК «Бастион» рекомендуется использовать правило, включающее несколько полей.

При интеграции с системами кадрового учета формат корпоративных кодов должен быть согласован с интегрируемой системой.

5 Настройка модуля «Бастион-ПЦН»

5.1 Общие сведения

Модуль «Бастион-ПЦН» обеспечивает возможность централизованного мониторинга объектов. Например, события, формируемые в нескольких филиалах, могут передаваться в центральный офис, где расположен пост центрального наблюдения. При этом имеется возможность в каждом филиале определить фильтр для событий, которые будут передаваться на ПЦН.

Передача событий осуществляется с помощью того же механизма, что и репликация персонала. Для включения механизма передачи событий на ПЦН необходимо указать режим «Публиковать сообщения» в клиенте репликации. В филиале, где будет находиться собственно ПЦН, для клиента репликации необходимо указать режим «Прослушивать сообщения». Обмен сообщениями будет работать только при наличии лицензии «Бастион-ПЦН» в ключе защиты.

Последовательность обработки событий для двух филиалов («Центральный», где находится ПЦН, и «Филиал») при наличии модуля «Бастион-ПЦН» выглядит следующим образом:

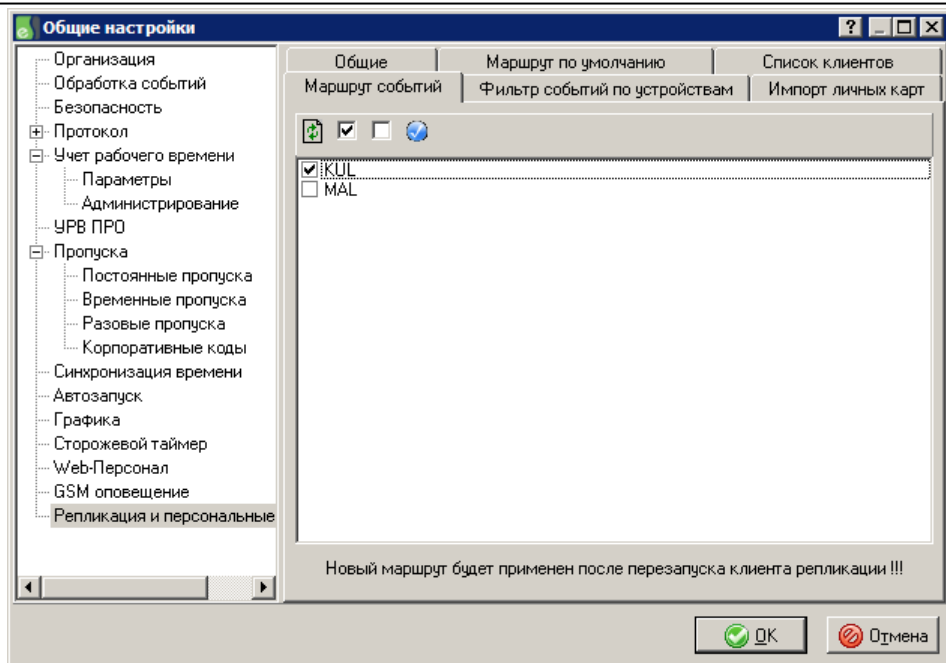
1. Событие возникает в Филиале:
 - a. Передается драйвером в ядро системы;
 - b. Обрабатывается в филиале согласно локальным правилам обработки событий;



- c. Сохраняется в журнал событий (протокол) Филиала.
2. Отправляющий клиент репликации в Филиале:
 - a. Выбирает события, проходящие по фильтру исходящих событий, из локального журнала событий;
 - b. формирует XML-сообщение для каждого выбранного события;
 - c. отправляет XML-сообщение в web-сервис.
3. Web-сервис раздает полученное сообщение всем клиентам, указанным в маршруте сообщения.
4. Принимающий клиент репликации в центральном офисе:
 - a. получает адресованные ему события;
 - b. обеспечивает протоколирование событий, приходящих от филиалов, в журнал центрального офиса;
 - c. передает полученные события в АРМ оператора ПЦН АПК «Бастион» для отображения.
5. АРМ оператора ПЦН отображает события из Филиалов в соответствии с их приоритетом и правилами, определенными в филиале. В качестве АРМ оператора ПЦН может выступать любое рабочее место АПК «Бастион». События в АРМ отображаются в окне «чужих» сообщений, при наличии соответствующих полномочий у оператора (задается в профиле оператора). Вывод расширенных сообщений и окон фотоидентификации по «чужим» событиям не предусмотрен.

5.2 Настройка маршрута по умолчанию для событий

В АПК «Бастион», который будет являться источником событий для ПЦН, необходимо отметить тех клиентов репликации, куда предполагается отправлять события (там, где будет собственно ПЦН). Это можно сделать на вкладке «Маршрут событий» в «Общих настройках». При этом должна быть разрешена репликация на web-сервер на странице «Общие».



Маршрут для передачи событий может отличаться от маршрута личных карт.

5.3 Включение выгрузки событий клиентом репликации

Для включения отправки событий на ПЦН в клиенте репликации, необходимо включить флаг «Выгружать события» в настройках клиента репликации, на странице «Общие».

Для получения и отображения «чужих» событий включать эту функцию не требуется.

5.4 Окно «чужих» сообщений мониторинга

В АРМ АПК «Бастион» на ПЦН, входящие «чужие» события отображаются в АПК «Бастион» в отдельных окнах, которые идентичны обычным окнам отображения штатных и нештатных событий:

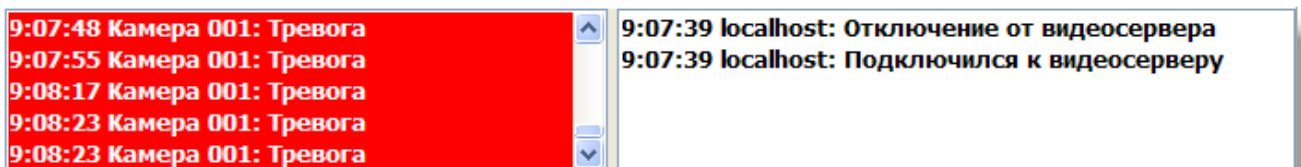


Рис. 26 – Окна отображения "чужих" сообщений

Чтобы включить это окно, необходимо установить флаг «Отображать журнал чужих сообщений (репликация)» в форме «Профили пользователя» для требуемых профилей. По умолчанию эти окна выключены для всех профилей пользователей.

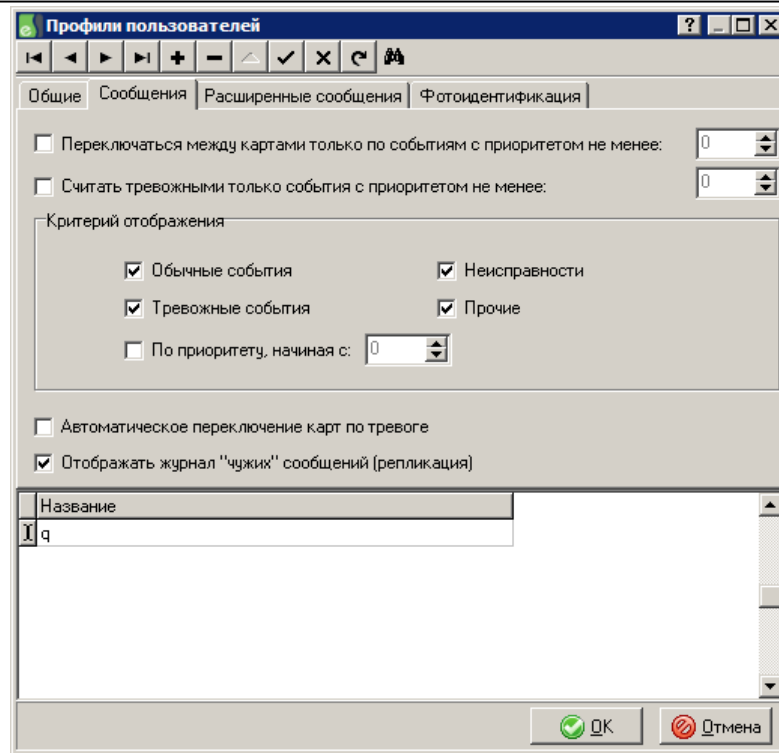


Рис. 27 - Включение журнала чужих сообщений

Внимание! Если клиент репликации сообщает ошибку «Interface not supported» при получении чужих событий и попытке их отобразить в окне «чужих» событий в «Бастиионе», нужно выполнить файл `regsrvs.bat` из папки, где установлен АПК «Бастиион».

6 Включение выгрузки событий входа/выхода

С помощью системы репликации можно настроить экспорт событий входа/выхода во внешние файлы CSV.

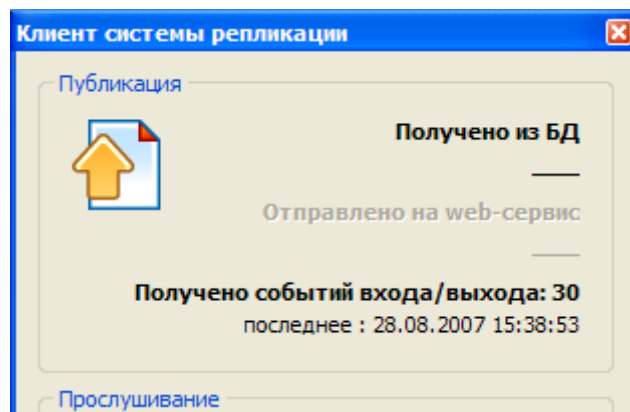


Рис. 28. Форма клиента репликации в режиме выгрузки событий входа/выхода

Для перевода клиента репликации в режим выгрузки событий UPB следует установить флаг «Выгружать события входа/выхода» в клиенте репликации. После этого для настройки выгрузки следует перейти на дополнительную вкладке:

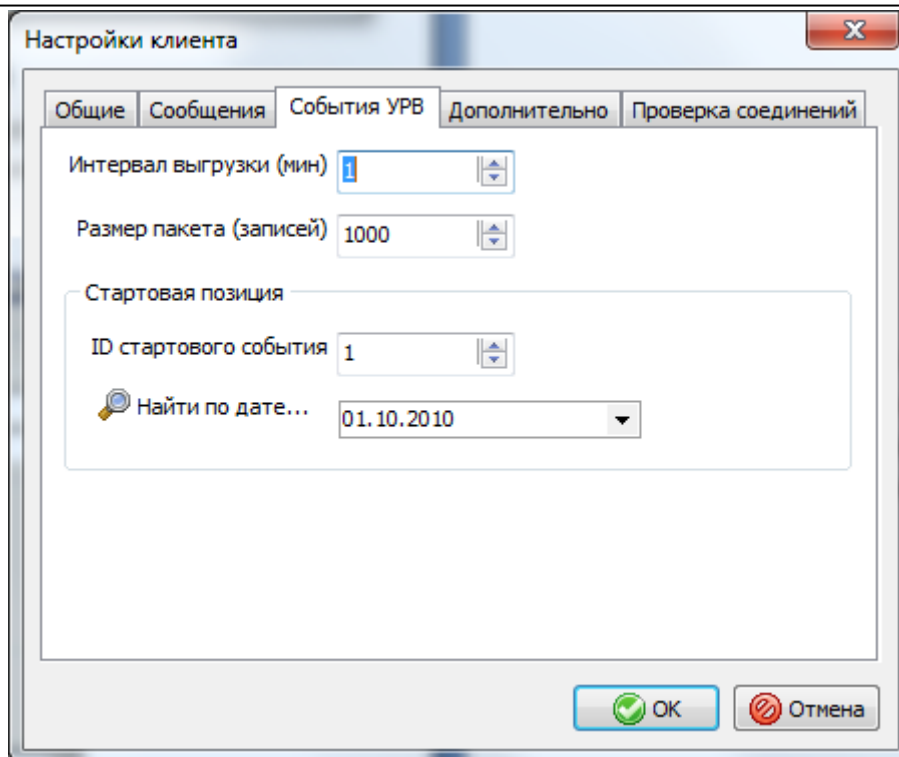


Рис. 29. Вкладка «События УРВ» формы настройки клиента

В поле «Интервал выгрузки» указывается периодичность в минутах, с которой будет происходить выгрузка событий входа/выхода. За один раз система выгрузит только 1 пакет, с максимальным числом записей, указанным в поле «Размер пакета».

Необходимо задать параметры так, чтобы *размер пакета превышал среднее количество событий входа/выхода, возникающих в системе за время, равное интервалу отправки.*

Экспорт данных производится из протокольной БД, начиная со стартового события, ID которого должен быть указан в поле «ID стартового события». Это поле – служебное характер и значение для него задается один раз. Для корректной установки этого значения рекомендуется использовать кнопку «Найти по дате...».

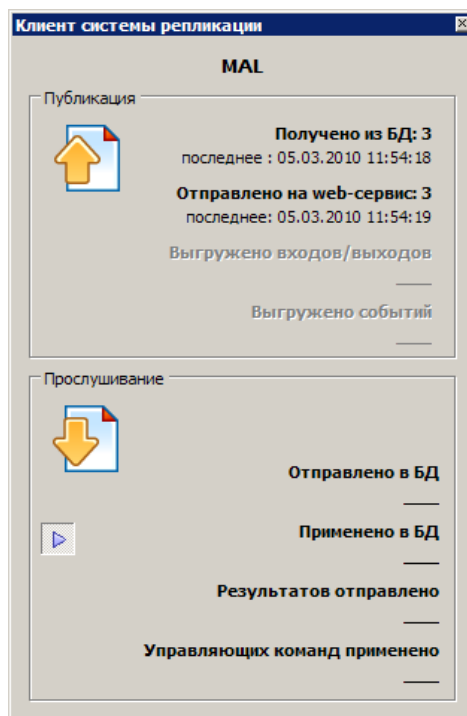
Пример. Пусть требуется начать экспорт данных, начиная с 19 апреля 2007 года. При этом пусть подсистема «Учет рабочего времени» в АПК «Бастион» была включена с 1 марта 2007 года. Чтобы начать экспорт, необходимо найти ID стартового события – первого наступившего после 1.03.2007 00:00:00. Следует ввести эту дату в поле «Найти по дате» и нажать кнопку «Найти по дате». ID подходящего первого события появится в поле.

7 Проверка работоспособности системы

Для проверки системы после установки согласно руководству «Репликация и шлюз событий. Руководство оператора» необходимо:

1. Выбрать для проверки два сервера СКУД.
2. Запустить и настроить на них клиенты репликации, как описано в главе 4.
3. Разрешить на них репликацию в АПК «Бастион», согласно главе 5.

4. Создать в первой СКУД заявку на пропуск – присвоить ему группу доступа ГОСТИ и выбрать любой локальный уровень доступа.
5. Выдать заявку, введя любую карту доступа и указав на странице «Репликация» в АПК «Бастион» маршрут по умолчанию.
6. Убедиться в том, что сообщения отправились на web-сервис:



7. Убедиться в аналогичном окне в том, что клиент на второй СКУД их принял.
8. Открыть бюро пропусков АПК «Бастион» и убедиться в том, что работник имеется в списке выданных пропусков подразделения, указанного в п.4.

Для проверки перекрестной репликации:

9. На второй СКУД следует изменить любой из реплицируемых параметров личной карты работника.
10. Убедиться, что сообщения отправились «назад» на первую СКУД.
11. Убедиться, что сообщения были получены и применены первой СКУД.
12. Убедиться, что изменение отразилось в бюро пропусков АПК «Бастион» первой СКУД.

Если какой либо из пунктов передачи, получения и применения сообщений (п.п. 6 – 8) не выполняется, то следует ознакомиться с Руководством «Система репликации персонала. Руководство пользователя» и выяснить случаи, в которых такая ситуация может возникнуть, и пути ее разрешения.

Для проверки репликации событий:

13. Добавить источник событий в базе-отправителе – драйвер устройства.
14. В клиенте репликации–отправителе установить флажок «Выгружать события».
15. Сгенерировать события, убедиться, что они были получены из БД.

16. Убедиться в том, что они отправились на web-сервис.
17. Убедиться в том, что на принимающей стороне включен режим прослушивания сообщений
18. Убедиться в том, что сообщения были приняты во входящих и применены в базу данных.
19. Убедиться в том, что профиль пользователя отображает окно «чужих» сообщений. По умолчанию оно выключено.

8 Потеря и восстановление связи на медленных каналах

Клиент репликации на медленных каналах может терять связь с web-сервером, где установлен Windows Server, по следующим причинам:

1. Через канал репликации отправляются большого размера сообщения (до 500 Кб и выше). Такие сообщения могут встречаться в репликации, если:
 - a. Интервалы отправки стоят в пределах нескольких часов.
 - b. Интенсивность событий после исходящей фильтрации превышает 3 события в секунду.
 - c. Производится репликация работников с фотографиями.

Потеря связи характеризуется сообщениями «ESOPHTTPException The operation timed out».

В этом случае клиент репликации пытается восстанавливать связь при отправке каждого исходящего сообщения репликации. Восстановление связи произойдет через интервал отправки.

2. Web-сервер недоступен физически.

Потеря связи характеризуется сообщениями «ESOPHTTPException Server unavailable».

В этом случае клиент репликации пытается восстанавливать связь по протоколу HTTP в течение отправки каждого сообщения репликации и связь будет восстановлена сразу после появления web-сервера в сети.

Клиент репликации полностью перезапускается раз в 1 час. Этот интервал можно изменить, отредактировав параметр RestartInt в файле NRepl.ini. Это необходимо для предотвращения потерь связи, если по каким-то причинам клиенту репликации не удалось ее восстановить при отправке сообщений.

Если значение RestartInt указать равным 0, то репликация будет работать без принудительного перезапуска.

9 Обмен персональными данными с системами кадрового учёта

Система репликации персонала может применяться и для интеграции с различными системами кадрового учета (далее SKU), например, компонентами системы «1С-Предприятие», «Босс-Кадровик».

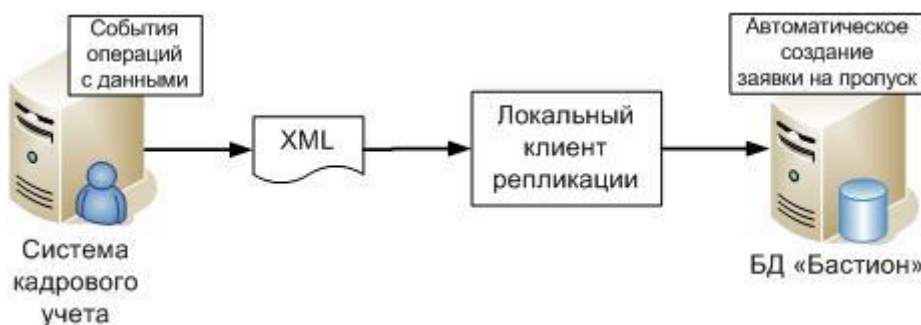


Обмен персональными данными с системами кадрового учета может осуществляться с помощью:

1. Обмена файлами
2. Прямого соединения баз данных кадрового учета и модуля «Бастиян-Репликация»

9.1 Обмен персональными данными через файлы XML

При использовании этого способа клиент репликации и кадровая система используют общую папку на жестком диске сервера АПК «Бастиян».



SKU внутри себя должна уметь отслеживать события добавления, изменения и удаления данных о сотрудниках. Далее, SKU должна уметь формировать соответствующий каждой операции XML-файл по определенной спецификации, которые «прослушивает» и импортирует клиент репликации.

Клиент репликации воспринимает эти файлы как команды на автоматический импорт персональных данных и их изменений.

Как правило, для этого дается общий доступ папке C:\Rep\In, которая будет автоматически создана клиентом репликации после установки на сервере АПК «Бастиян».

При использовании такого режима нужно выполнить настройку клиента репликации следующим образом:

1. Включить режим прослушивания сообщений.
2. Папку со входящими сообщениями необходимо обеспечить наполнением файлами XML.

9.2 Обмен персональными данными через обменную таблицу

При использовании этого способа клиент репликации и кадровая система используют общую обменную таблицу, которая расположена в кадровой системе.

В этом случае перед установкой репликации от кадровой системы ТРЕБУЕТСЯ обеспечить наличие обменной таблицы в своей СУБД. Поддерживаются следующие СУБД:

1. Oracle.
2. Microsoft SQL Server.
3. Firebird.
4. Sybase.

При использовании такого режима нужно выполнить настройку клиента репликации следующим образом:

1. Включить режим прослушивания сообщений.
2. Включить режим «Из внешней СУБД»
3. Выполнить подключение к внешней СУБД на вкладке «Внешняя СУБД...», указав логин и пароль к базе данных. Пароль к СУБД будет сохранен в открытом виде, поэтому для этого подключения целесообразно заведение ограниченных пользователей СУБД с доступом только к обменной таблице.
4. Ввести имя обменной таблицы в поле «Таблица для импорта сообщений». Как правило, оно равно REP_MSG или dbo.REP_MSG (для MS SQL Server).
5. Если наряду с основной обменной таблицей используются обменные таблицы для экспорта событий входа/выхода и/или фотографий работников, требуется ввести имена соответствующих таблиц. Эти схемы требуют дополнительного ознакомления, описания и обсуждения с разработчиками ООО «НИЦ ФОРС» всех деталей обмена дополнительно.

9.3 Обмен персональными данными через запрос на изменившиеся данные

При использовании этого способа клиент репликации и кадровая система используют запрос только на ИЗМЕНИВШИЕСЯ данные, который производится к СУБД кадровой системы.

В этом случае перед установкой репликации от кадровой системы ТРЕБУЕТСЯ разработать такой запрос и привести его к структуре обменной таблицы средствами SQL.

При использовании такого режима нужно выполнить настройку клиента репликации следующим образом:

1. Включить режим прослушивания сообщений.
2. Включить режим «Из внешней СУБД»
3. Выполнить подключение к внешней СУБД на вкладке «Внешняя СУБД...», указав логин и пароль к базе данных. Пароль к СУБД будет сохранен в открытом виде, поэтому для этого

подключения целесообразно заведение ограниченных пользователей СУБД с доступом только к обменной таблице.

4. Очистить имя обменной таблицы в поле «Таблица для импорта сообщений», введя туда пустую строку.
5. Ввести текст разработанного SQL-запроса на чтение данных в поле «SELECT» на вкладке «Запросы к внешней СУБД». Тексты запросов в полях «UPDATE» и «DELETE» нужно составить таким образом, чтобы они не выполняли никаких действий с данными, но не приводили к ошибке. Это зарезервированная возможность, которая будет использоваться в будущем.

9.4 Обмен событиями входа/выхода

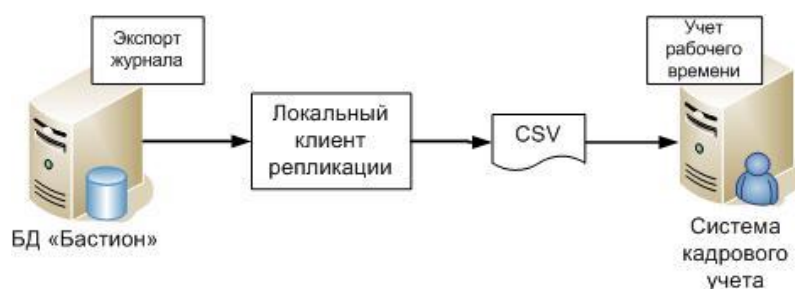
С помощью системы репликации возможна установка и использование решения, при котором учет рабочего времени также производится на стороне SKU. Такая архитектура может применяться в организациях, где для УРВ уже внедрены и используются комплексные системы работы с персоналом, такие как «1С», «Босс-Кадровик» и т.п.

Исходными данными для учета рабочего времени в SKU является журнал событий входа/выхода сотрудников на территорию предприятия. SKU обрабатывает его с целью расчета отработанного времени, выявления прогулов, опозданий и т. п.

Источником событий в этом случае служит клиент системы репликации АПК «Бастион». АПК «Бастион» может формировать события учета рабочего времени и через клиент репликации выгружать их во внешний файл в формате CSV. Выгружаются данные, разделенные точкой с запятой:

- корпоративный код сотрудника,
- дата и время события входа/выхода,
- тип события — вход или выход,
- номер карты доступа,
- серия карты доступа,
- комментарий.

Работа такого решения происходит по следующей схеме:



1. Клиент системы репликации должен быть запущен локально и переведен в режим выгрузки событий входа/выхода во внешний файл CSV.
2. В SKU должен быть организован прием и работа с файлами CSV. При этом:

- a. СКУ должна иметь возможность извлекать данные о событиях согласно спецификации.
- b. СКУ должна иметь возможность привязывать принятые события к сотрудникам в своей базе данных по корпоративному коду.

9.5 Алгоритм репликации персональных данных и событий входа/выхода с кадровой системой

1. В кадровой системе происходит заведение нового работника или указывается необходимость выдачи работнику новой карты доступа. В этот момент кадровая система должна сформировать некий сигнал, который будет затем транслирован в необходимость формирования сообщения репликации.
2. Кадровая система создает новую запись в своей обменной таблице REP_MSG, наполняя ее данными, которые имеются на работника последними и которые были введены операторами кадровой системы.
3. Модуль «Бастион-Репликация» целиком перемещает запись на работника из обменной таблицы кадровой системы в таблицу REP_MSG основной базы данных АПК «Бастион». В этот момент заполненная запись на работника именуется сообщением репликации из внешней СУБД.
4. Модуль «Бастион-Репликация»:
 - a. Иницирует применение сообщения репликации из внешней СУБД.
 - b. Создает заявку на работника, ранее несуществующего в СКУД.
 - c. Выполняет обновление персональных данных работника, ранее существовавшего в СКУД.
5. Оператор бюро пропусков СКУД выдает заявку и присваивает ей карту-пропуск.
6. Работник, который получил на руки выданную карту-пропуск, становится пользователем СКУД и начинает ее предъявление к считывателям СКУД.
7. Драйвер оборудования ELSYS АПК «Бастион» получает события предъявления карт доступа от считывателей СКУД.
8. Драйвер оборудования ELSYS АПК «Бастион» согласно настройкам областей контроля формирует события учета рабочего времени. Настройки областей контроля задаются в настройках СКУД.
9. Модуль «Бастион-Репликация» отслеживает события входа/выхода, записанные в протокольную базу данных АПК «Бастион».
10. Модуль «Бастион-Репликация» передает события входа/выхода в обменную таблицу кадровой системы для дальнейшего использования в её табельном учете.
11. Перед выдачей пропуска оператор бюро пропусков СКУД фотографирует работника.



12. Модуль «Бастион-Репликация» отслеживает сообщение репликации с фотографией и подготавливает его для передачи в кадровую систему.
13. Модуль «Бастион-Репликация» перемещает сформированное сообщение репликации с фотографией работника в кадровую систему.

Полученная схема описывает движение персональных данных от момента заведения нового работника в кадровой системе до выдачи пропуска в СКУД и передачи событий учета рабочего времени из СКУД в кадровую систему.

Внимание! Полученная схема также применима к механизму репликации ИЗМЕНЕНИЙ в персональных данных.

10 Шифрование персональных данных

Модуль репликации поддерживает шифрование данных, передаваемых по открытым каналам связи (через файловый обмен, через локальную сеть или через сеть Интернет).

Для обеспечения шифрования данных нужно установить флаг «Шифровать» в настройках клиента репликации.

При использовании шифрования следующие поля обменных файлов XML будут зашифрованы:

- TABLE_FIELDS (изменяемые поля)
- TABLE_VALUES (содержимое изменяемых полей)
- OPER_DATE (дата проведения операции)
- CORP_CODE (корпоративный код изменяемой записи).

Таким образом, при использовании шифрования в репликации персональные данные защищаются от несанкционированного доступа.

Приложение А. Технические требования к серверу репликации

Система репликации предполагает наличие **единственного** сервера, который осуществляет маршрутизацию сообщений репликации.

Сервер должен быть доступен в оснастке IIS по протоколу http со всех объектов, где устанавливаются клиенты репликации (порт 80 по умолчанию).

Технические характеристики рабочей станции сервера см. в п.1.2.

Доступность сервера может быть обеспечена тремя способами:

В корпоративной сети без использования VPN.

Если для передачи данных репликации предполагается использовать корпоративную сеть предприятия, то IP-адрес, либо DNS-имя сервера должны быть внутренними (например, 192.168.1.? или replserver).

Безопасность соединений обеспечивается средствами IIS:

- Запрещением доступа всем пользователям домена и всем IP-адресам за исключением администраторов и клиентов репликации.
- Программным брандмауэром – закрытием всех портов рабочей станции за исключением ping и http-портов.

В публичной сети без использования VPN.

Если предполагается использовать сеть Internet для передачи данных, то IP-адрес, либо DNS-имя должны быть внешними и получены у провайдера. Также провайдер должен сообщить маску подсети, шлюз и адреса DNS-серверов.

В этом случае выведение сервера в интернет может быть сделано либо с помощью аппаратного шлюза, либо напрямую через сеть провайдера.

Безопасность соединений обеспечивается средствами IIS 6.0:

- Запрещением доступа всем IP-адресам за исключением статических IP-адресов, с которых подключаются клиенты репликации.
- Программным либо аппаратным брандмауэром в шлюзе – закрытием всех портов рабочей станции за исключением ping и http-портов.

В публичной сети с использованием VPN

Сеть интернет можно использовать с построением VPN-туннелей. Такие соединения более безопасны во всех отношениях (используется протокол передачи данных IpSec) и упрощают стандарты формирования IP-адресов между удаленными подразделениями.

Безопасность соединения в любом из случаев может быть улучшена установкой сервера лицензий, SSL-шифрованием соединения и дополнительной аутентификацией клиентскими сертификатами Microsoft.

При проектировании репликации в рамках корпоративной сети:

Типовая архитектура сети репликации приведена ниже:

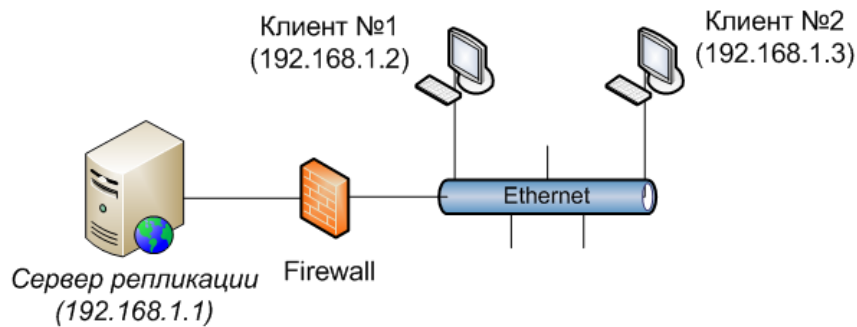


Рис. 30 - Схема репликации через корпоративную сеть

- Сервер может быть включен в домен предприятия, тогда ему должно быть присвоено DNS-имя. Подключение к серверу по http при этом будет производиться по DNS-имени.
- Сервер может быть не включен в домен предприятия, тогда ему должен быть присвоен статический IP-адрес. Обращение к серверу по http при этом будет производиться по IP-адресу.

При проектировании репликации в публичной сети без использования аппаратного шлюза:

Дополнительные требования к серверу репликации:

- Наличие входящего широкополосного подключения с выходом WAN (ADSL или иного).
- Установленный программный брандмауэр (например, Agnitum Outpost Firewall 4.0)

Типовая архитектура сети репликации приведена ниже:

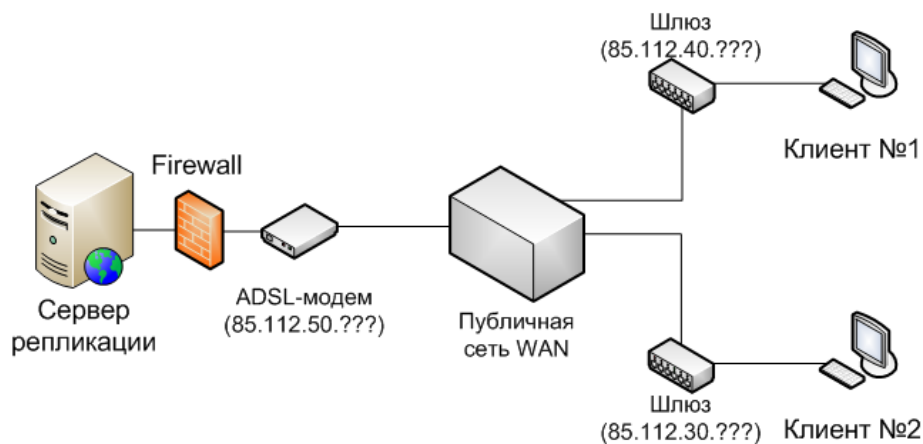


Рис. 31 - Схема репликации через публичную сеть без шлюза

Сервер аппаратно должен быть выведен в публичную сеть интернет, ему должен быть присвоен внешний IP-адрес. Для этого предприятию, устанавливающему сервер репликации, требуется обратиться к провайдеру услуг для получения одного внешнего IP-адреса для сервера.

На сервере в операционной системе должен быть установлен и настроен *программный* брандмауэр, чтобы закрыть все порты кроме порта системы репликации (по умолчанию 80-го). В этом случае требуется приобретение зарегистрированной копии брандмауэра. Такое соединение не подразумевает создание аппаратного VPN-туннеля, что делает систему более уязвимой.

При проектировании репликации с использованием Internet с использованием аппаратного шлюза:

Дополнительные требования к серверу репликации:

- Наличие входящего широкополосного подключения с выходом WAN (ADSL или иного).
- Шлюз со встроенным аппаратным брандмауэром.

Если доступ к серверу осуществляется с помощью шлюза, то аппаратный брандмауэр должен быть настроен на нём так, чтобы пропускать входящие соединения только от клиентов репликации по http-портам.

Организацию соединений с использованием шлюза можно проводить либо с созданием VPN-туннеля (если шлюз его поддерживает), либо без него (например, на базе маршрутизаторов D-Link DI-804HV).

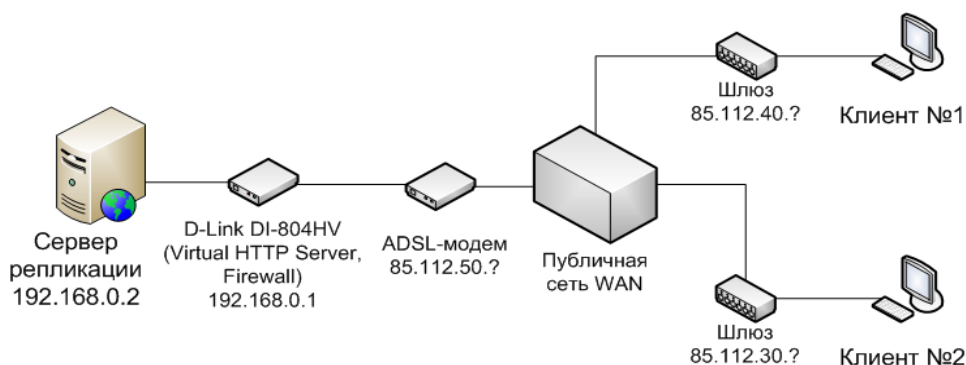


Рис. 32 - Схема репликации через публичную сеть со шлюзом

Построение VPN-туннеля возможно на базе двух маршрутизаторов D-Link DI-804HV. Первый будет устанавливаться для сервера, второй (и более) – для каждого клиента репликации, с которым предполагается держать постоянный канал связи. Однако следует учитывать, что вариант с этими маршрутизаторами не является базовым, поскольку VPN-соединение может быть неустойчивым.

При таком способе сервер репликации и все клиенты должны иметь статические адреса в интернет. Для построения такого аппаратного VPN-туннеля на базе D-Link DI-804HV можно руководствоваться следующей схемой:

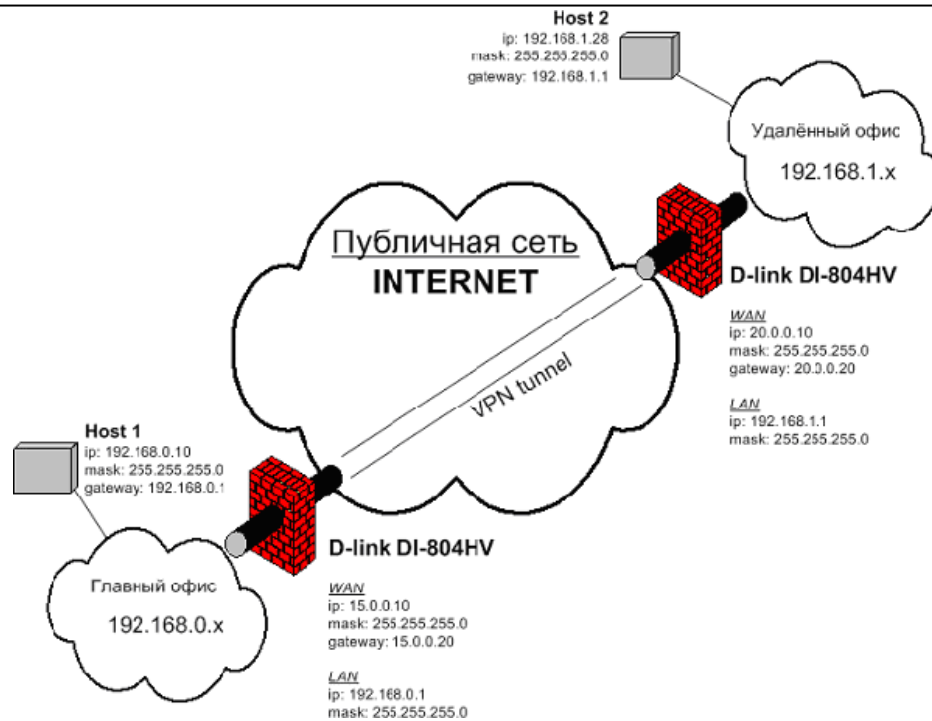


Рис. 33 - Виртуальная частная сеть VPN

Таким образом, для организации сервера репликации необходимо выполнить шаги:

- Установить на сервере программное обеспечение (Windows Server в роли сервера приложений, IIS, .Net Framework 2.0).
- Выбрать способ и сеть передачи данных репликации.
- Установить дополнительные средства по необходимости (модем, шлюз, брандмауэр).
- Собрать сеть и вывести сервер в корпоративную (публичную) сеть со статическим IP.
- Открыть в брандмауэрах требуемый порт http протокола TCP.
- Протестировать сеть и доступность сервер системы ping-тестами с клиентов и http-доступом через браузер.
- Установить файлы системы репликации на сервер репликации в IIS.
- Для настройки сервера и портала ознакомиться с руководством инсталлятора.

Примечание: на сервере репликации будет содержаться виртуальный каталог с именем NRepI, который должен работать под управлением IIS как приложение. Для обеспечения безопасности настройками IIS, порт http, где установлен каталог, следует открывать только для статических IP-адресов или доменных имен клиентов репликации. Кроме того, целесообразно перенести виртуальный каталог на порт, отличный от 80.

Приложение Б. Спецификация обменного файла XML

Обменный файл имеет формат XML версии 1.0 в кодировке Windows-1251 в соответствии со спецификацией в формате DTD.

Спецификация DTD для входного файла XML имеет следующий вид:

```
<?xml version="1.0" encoding="windows-1251"?>
<!-- Поля списка сообщений -->
<!ELEMENT MSG_ID (#PCDATA)>
<!ELEMENT MSG_STATE (#PCDATA)>
<!ELEMENT S_SERV_ID (#PCDATA)>
<!ELEMENT C_SERV_ID (#PCDATA)>
<!ELEMENT OPER_CODE (#PCDATA)>
<!ELEMENT OPER_DATE (#PCDATA)>
<!ELEMENT TABLE_NAME (#PCDATA)>
<!ELEMENT CORP_CODE (#PCDATA)>
<!ELEMENT NEW_ID (#PCDATA)>
<!ELEMENT OLD_ID (#PCDATA)>
<!ELEMENT TABLE_FIELDS (#PCDATA)>
<!ELEMENT TABLE_TYPES (#PCDATA)>
<!ELEMENT TABLE_VALUES (#PCDATA)>
<!-- Список сообщений -->
<!ELEMENT MSG_LIST (MSG*)>
<!ELEMENT MSG (MSG_ID, MSG_STATE, ROUTE_ID, S_SERV_ID, C_SERV_ID, OPER_CODE,
OPER_DATE, TABLE_NAME, CORP_CODE, NEW_ID, OLD_ID, TABLE_FIELDS, TABLE_TYPES,
TABLE_VALUES)>
```

Файл в режиме добавления нового работника (или изменения существующего) имеет следующий вид:

```
<?xml version="1.0" encoding="windows-1251"?>
<MSG_LIST>
<MSG>
    <MSG_ID>F6474873A4334687A9631E62FFEE4504</MSG_ID>
    <MSG_STATE>0</MSG_STATE>
    <MSG_FILENAME>_172206.xml</MSG_FILENAME>
    <ROUTE_ID></ROUTE_ID>
    <S_SERV_ID>1C_ГЛАБ</S_SERV_ID>
    <C_SERV_ID></C_SERV_ID>
    <OPER_CODE>U</OPER_CODE>
    <OPER_DATE>12.04.2007 17:00:05</OPER_DATE>
    <TABLE_NAME>PERSON</TABLE_NAME>
    <CORP_CODE>Вор_Пет_Але_05671</CORP_CODE>
    <NEW_ID></NEW_ID>
    <OLD_ID></OLD_ID>

    <TABLE_FIELDS>name;firstname;secondname;tableno;dep;org;post;corp_code</TABLE_FIELDS>
    <TABLE_TYPES></TABLE_TYPES>

    <TABLE_VALUES>Воробьев;Петр;Алексеевич;05671;ВЗ_УБ(Охрана)_871;ВЗ_Северсталь-метиз;Контролер_контрольно-пропускного_пункта;Вор_Пет_Але_05671</TABLE_VALUES>
</MSG>
</MSG_LIST>
```

Файл в режиме изменения только одного поля имеет вид:

```
<?xml version="1.0" encoding="windows-1251"?>
<MSG_LIST>
  <MSG>
    <MSG_ID>F6474873A4334687A9631E62FFEE4505</MSG_ID>
    <MSG_STATE>0</MSG_STATE>
    <MSG_FILENAME>_172206.xml</MSG_FILENAME>
    <ROUTE_ID></ROUTE_ID>
    <S_SERV_ID>1C_ГЛАБ</S_SERV_ID>
    <C_SERV_ID></C_SERV_ID>
    <OPER_CODE>U</OPER_CODE>
    <OPER_DATE>18.04.2007 16:20:05</OPER_DATE>
    <TABLE_NAME>PERSON</TABLE_NAME>
    <CORP_CODE>Ска_Оль_Сер_04130_1974</CORP_CODE>
    <NEW_ID></NEW_ID>
    <OLD_ID></OLD_ID>
```

```

        <TABLE_FIELDS>citizenship</TABLE_FIELDS>
        <TABLE_TYPES></TABLE_TYPES>
        <TABLE_VALUES>Россия</TABLE_VALUES>
    </MSG>
</MSG_LIST>

```

Файл в режиме удаления работника имеет вид:

```

<?xml version="1.0" encoding="windows-1251"?>
<MSG_LIST>
  <MSG>
    <MSG_ID>ABC74873A4334687A9631E62FFEE4505</MSG_ID>
    <MSG_STATE>0</MSG_STATE>
    <MSG_FILENAME>_172212.xml</MSG_FILENAME>
    <ROUTE_ID></ROUTE_ID>
    <S_SERV_ID>1C ГЛАВ</S_SERV_ID>
    <C_SERV_ID></C_SERV_ID>
    <OPER_CODE>D</OPER_CODE>
    <OPER_DATE>18.04.2007 16:58:05</OPER_DATE>
    <TABLE_NAME>PERSON</TABLE_NAME>
    <CORP_CODE>Ска_Оль_Сер_04130_1974</CORP_CODE>
    <NEW_ID></NEW_ID>
    <OLD_ID></OLD_ID>
    <TABLE_FIELDS></TABLE_FIELDS>
    <TABLE_TYPES></TABLE_TYPES>
    <TABLE_VALUES></TABLE_VALUES>
  </MSG>
</MSG_LIST>

```

Приложение В. Спецификация обменных таблиц

Таблица с персональными данными, которая должна быть создана во внешней СУБД, имеет нижеприведенную структуру:

Для СУБД Oracle:

```

CREATE TABLE REP_MSG
(
  MSG_ID VARCHAR2(32 CHAR) NOT NULL,
  OPER_DATE DATE NOT NULL,
  CORP_CODE VARCHAR2(100 BYTE) NOT NULL,
  TABLE_FIELDS VARCHAR2(1000 CHAR) NOT NULL,
  TABLE_VALUES VARCHAR2(1000 CHAR) NOT NULL,
  PHOTO VARCHAR2(255 BYTE),
  MSG_STATE INTEGER DEFAULT 0 NOT NULL,
  MSG_IN INTEGER DEFAULT 1 NOT NULL,
  TABLE_NAME VARCHAR2(10 CHAR) DEFAULT 'PERSON' NOT NULL,
  MSG_FILENAME VARCHAR2(10 CHAR) DEFAULT NULL,
  S_SERV_ID VARCHAR2(10 CHAR) DEFAULT NULL,
  C_SERV_ID VARCHAR2(10 CHAR) DEFAULT NULL,
  OPER_CODE VARCHAR2(2 CHAR) DEFAULT 'U' NOT NULL,
  TABLE_TYPES VARCHAR2(20 CHAR) DEFAULT NULL,
  NEW_ID INTEGER DEFAULT 0 NOT NULL,
  OLD_ID INTEGER DEFAULT 0 NOT NULL
)

```

Для СУБД MS SQL Server:

```

CREATE TABLE [dbo].[REP_MSG] (
  [MSG_ID] [int] IDENTITY(1,1) NOT NULL,
  [OPER_DATE] [datetime] NOT NULL,
  [CORP_CODE] [varchar] (100) NOT NULL,
  [TABLE_FIELDS] [varchar] (1000) NOT NULL,
  [TABLE_VALUES] [varchar] (1000) NOT NULL,
  [PHOTO] [varchar] (255) NULL,
  [MSG_STATE] [int] NOT NULL CONSTRAINT [DF_REP_MSG_MSG_STA_292A3BFC] DEFAULT ((0)),
  [MSG_IN] [int] NOT NULL CONSTRAINT [DF_REP_MSG_MSG_IN_2A1E6035] DEFAULT ((1)),
  [TABLE_NAME] [varchar] (10) NOT NULL CONSTRAINT [DF_REP_MSG_TABLE_N_2B12846E] DEFAULT ('PERSON'),
  [MSG_FILENAME] [varchar] (10) NULL CONSTRAINT [DF_REP_MSG_MSG_FIL_2C06A8A7] DEFAULT (NULL),
  [S_SERV_ID] [varchar] (10) NULL CONSTRAINT [DF_REP_MSG_S_SERV_2CFACCE0] DEFAULT (NULL),
  [C_SERV_ID] [varchar] (10) NULL CONSTRAINT [DF_REP_MSG_C_SERV_2DEEF119] DEFAULT (NULL),
  [OPER_CODE] [varchar] (2) NOT NULL CONSTRAINT [DF_REP_MSG_OPER_CO_2EE31552] DEFAULT ('U'),
  [TABLE_TYPES] [varchar] (20) NULL CONSTRAINT [DF_REP_MSG_TABLE_T_2FD7398B] DEFAULT (NULL),
  [NEW_ID] [int] NOT NULL CONSTRAINT [DF_REP_MSG_NEW_ID_30CB5DC4] DEFAULT ((0)),
  [OLD_ID] [int] NOT NULL CONSTRAINT [DF_REP_MSG_OLD_ID_31BF81FD] DEFAULT ((0)),
  CONSTRAINT [PK_REP_MSG] PRIMARY KEY CLUSTERED

```

```
(
  [MSG_ID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF, IGNORE_DUP_KEY = OFF, ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON) ON [PRIMARY]
) ON [PRIMARY]
```

Таблица с событиями входа/выхода данными, которая должна быть создана во внешней СУБД при необходимости:

```
CREATE TABLE BASTION_ATD (TB_TAB_NUM VARCHAR2 (100 CHAR) ,
  TB_EVENT_DATETIME DATE,
  TB_EVENT_TYPE INT) ; -- ВХОД ИЛИ ВЫХОД
```

Таблица с фотографиями, которая должна быть создана во внешней СУБД при необходимости:

```
CREATE TABLE BASTION_PHOTO (TB_TAB_NUM VARCHAR2 (100 CHAR) ,
  PHOTO BLOB,
  DATE_PHOTO DATE,
  TABLE_FIELDS VARCHAR2 (100 CHAR) ,
  TABLE_VALUES VARCHAR2 (100 CHAR) ) ;
```

Приложение Г. Спецификация обменных полей

В таблице 1 приведены поля, которые должны обязательно иметься в обменном файле или обменной таблице. При этом:

- элементы MSG_STATE, TABLE_NAME должны иметь строго определенное значение.
- элементы OPER_CODE, OPER_DATE, CORP_CODE, TABLE_VALUES должны формироваться на основании данных источника.
- элементы MSG_ID, MSG_FILENAME должны формироваться в момент экспорта файла из источника. Имя самого входного файла должно иметь значение MSG_FILENAME
- прочие элементы должны иметь пустое значение.

Таблица 1 – Спецификация и значения по умолчанию обменных полей

Наименование элемента	Тип данных	Описание	Пример значения
MSG_ID	Строка (до 32 символов)	GUID-идентификатор входящего сообщения	F6474873A4334687.. ..A9631E62FFEE4503
MSG_STATE	Число {0}		0
MSG_FILENAME	Имя файла в формате _[время формирования].xml	например: _172206.xml	_172206.xml
ROUTE_ID	- пусто -		
S_SERV_ID	Строка (до 32 символов)	Буквенный сокращенный идентификатор источника данных	1С_ГЛАВ
C_SERV_ID	- пусто -		
OPER_CODE	Символ {U} или {D}	U - для добавления работника, D - для удаления	U
OPER_DATE	Дата/время	Дата и время формирования сообщения в источнике данных	12.04.2007 17:00:05
TABLE_NAME	Строка {PERSON} или {PASS}	Если обменная запись относится к личной карте, то {PERSON}, если к пропуску (возврат, удаление, изъятие), то {PASS}	PERSON
CORP_CODE	Строка (до 100 символов)	Корпоративный код работника, сформированный по правилу через символ { }	Пах_Оль_Сер_04130_1974

		{3 символа фамилии, 3 символа имени, 3 символа отчества, табельный номер, год рождения}	
NEW_ID	- пусто -		
OLD_ID	- пусто -		
TABLE_FIELDS	Строка (до 1000 символов)	Строка имен полей БД Бастион	personcatid;name;firstname;... см. пункт 4
TABLE_TYPES	- пусто -		
TABLE_VALUES	Строка (до 4000 символов)		1_;Пахомова;Ольга;Сергеевна;04130;]null[; 2_Паспорт;... см. пункт 4

Приложение Д. Спецификация обменных полей TABLE_FIELDS и TABLE_VALUES

Поля TABLE_FIELDS и TABLE_VALUES используются для передачи персональных данных. Поскольку в каждой обменной записи набор и число полей персональных данных может отличаться, каждый элемент представляют собой строку, полученную соединением имен (значений) атрибутов персональных данных через символ {;}. Список атрибутов персональных данных приведен далее.

Поля, которые приведены ниже, могут формироваться в двух режимах:

Режим вставки или изменения данных – когда на источнике формируется запись о новом работнике или изменяется о существующем. В этом режиме в обменном файле или обменной записи должны присутствовать все обязательные поля.

Примечание 1: если совершена операция изменения данных, а такого работника в АПК «Бастион» нет, то репликацией будет совершена попытка вставки работника. Если во входном файле присутствуют не все обязательные поля, возникнет ошибка, которую можно отследить в журнале сообщений и разрешить повторной выгрузкой файла со ВСЕМИ заполненными полями.

Примечание 2: если поле после изменения на источнике имеет новое пустое значение, оно должно передаваться как выражение {]null[}.

Режим удаления данных – когда на источнике удаляется запись о работнике. В этом режиме поля должны быть пустыми, соответственно значения элементов TABLE_FIELDS и TABLE_VALUES должны быть пустыми.

Примечание: если удаляемый работник находится в выданных пропусках, то работник удалится из АПК «Бастион» в любом случае.

Таблица 2 – Спецификация и значения по умолчанию полей АПК «Бастион»

Обяз	Описание	Имя	Тип данных (размер)	Значение	Тип значения
	Категория работника	personcat	строка 100	Работник филиала	Словарь АПК «Бастион»
да	Фамилия	name	строка 20	Пахомова	данные источника
	Имя	firstname	строка 20	Ольга	- // -
	Отчество	secondname	строка 20	Сергеевна	- // -
да	Табельный номер	tableno	строка 20	04130	- // -
	Примечание	comments	строка 80	- пусто -	- // -
	Тип документа	doctype	строка 100	Паспорт	Словарь АПК

					«Бастион»
	Серия	docser	строка 12	3600	данные источника
	Номер	docno	строка 12	371145	- // -
	Дата выдачи документа	docissuedate	дата	11-NOV-2005	- // -
	Орган, выдавший документ	docissueorgan	строка 100	Светлоярским РОВД	Словарь АПК «Бастион»
	Дата рождения	birthdate	дата	28-JUN-1974	данные источника
	Место рождения	birthplace	строка 60	- пусто -	- // -
	Адрес	address	строка 255	ВОЛГОГРАД УЛ НИКОЛАЕВСКАЯ 4 52	- // -
	Гражданство	sitizenship	строка 100	Россия	Словарь АПК «Бастион»
	Приоритет	priority	число	0	предопределенное
да	Подразделение	dep	строка 100	ВЗ УБ(Охрана) 871	данные источника
да	Организация	org	строка 100	ВЗ Северсталь-метиз	данные источника
да	Должность	post	строка 100	Контролер_контрольно-пропускного_пункта	данные источника
	Телефон	phone	строка 15	871	данные источника
да	Корпоративный код	corp_code	строка 100	Пах_Оль_Сер_04130_1974	данные источника
	Корпоративный код существующего уровня доступа АПК «Бастион»	accl_cc	строка 100	По_умолчанию	данные источника
	Фотография	photo	двоичный-64	/9j/4AAQSkZJ...B/9k=	данные источника

Словарные данные АПК «Бастион» указываются полнотекстовой строкой наименования, не превышающей 100 символов. Например, если работник принадлежит к категории «Работник филиала», то в поле PERSONCAT следует занести непосредственное значение «Работник филиала». Если путем полнотекстового сравнения при импорте входного файла в АПК «Бастион» не обнаружится такой позиции, эта позиция будет создана.

Поскольку АПК «Бастион» поддерживает только двухуровневую вложенность структуры подразделений, то структуру подразделений источника необходимо привести бизнес-правилами к двухуровневому виду. Например, перенести все дочерние записи узла, стоящего на главном уровне, ему в подчинение вне зависимости от их собственной вложенности. При этом в поле ORG необходимо указать наименование главного узла первого уровня «Организации», а в поле DEP – подчиненного узла второго уровня «Подразделения».

При наличии фотографии поле PHOTO должно содержать JPEG-фотографию, преобразованную в формат Base-64. Если фотографии нет, поле PHOTO должно отсутствовать в элементах TABLE_FIELDS и TABLE_VALUES входного файла. Поле PHOTO всегда должно быть последним в списке значений.

Элементов MSG в корне MSG_LIST может быть несколько согласно спецификации DTD.

Приложение Е. Спецификация выходного файла с событиями учета рабочего времени

Общие сведения

Выходной файл имеет формат CSV (текстовый с разделителем точка с запятой). Он формируется с определенным интервалом и содержит в себе определенное число позиций.

Интервал формирования задается в минутах в настройках модуля «Бастион-Репликация». Как правило, это 240 минут (4 часа).

Число позиций задается в строках в настройках модуля «Бастион-Репликация». Этот размер должен перекрывать ориентировочное пиковое количество событий входа/выхода, происходящих в системе за интервал формирования. Как правило, это 2500 строк.

Имя файла формируется автоматически в формате:

[дата]([начало интервала]-[окончание интервала]).csv

Пример:

07-04-17(140216-144400).csv

Спецификация

В таблице 3 приведены значения, которые содержатся в выходном файле.

Таблица 3 – Спецификация выходного файла

Наименование элемента	Тип данных	Описание	Пример
CORP_CODE	Строка (до 100 символов)	Корпоративный код работника	Ска_Оль_Сер_04130_1974
ADATETIME	Дата/время события	Дата/время возникновения события входа/выхода	17.04.2007 14:20:25
IS_ENTRANCE	Число	0 – выход, 1 – вход	1
CARD_NO	Число	Номер карты доступа работника	452
SITECODE	Число	Серия карты доступа работника	86
COMMENTS	Строка	Комментарий, вводимый при ручном добавлении события в протокол	Вход по кнопке, забыл карту

Пример



```
Ска_Оль_Сер_04130_1974;17.04.2007 14:02:16;0;452;86
Ска_Оль_Сер_04130_1974;17.04.2007 14:02:42;1;452;86;Вход по кнопке, забыл карту
Вор_Пет_Але_05671_1967;17.04.2007 14:04:17;0;173;86
```

Приложение Ж. Настройка фильтра исходящих событий

Фильтр исходящих событий настраивается только с web-портала и при включенном удаленном управлении на клиенте.



Фильтр событий в текущей версии репликации распространяется только на **типы устройств**, а не на конкретные устройства, из-за сложности передачи и отображения всего массива оборудования с клиента на web-портал.



Ниже приведен пример, как установить фильтр тревог от видеокамер совместно с тревогами и неисправностями от видеосервера.

1. Необходимо зайти на web-портал на страницу «События» в браузере.
2. Выбрать клиента репликации из списка, которому надо установить фильтр на отправку.
3. Проверить, что физически на этой СКУД клиент репликации работает.
4. Нажать кнопку «Запросить список драйверов»
5. Дождаться всплывающего сообщения на клиенте репликации о получении команды запроса списка.
6. Обновить окно web-портала в браузере.
7. В таблице появится список активных драйверов и содержащихся в них типов устройств.
8. Далее, необходимо перейти в режим редактирования фильтра сервера нажатием кнопки  «».
9. Необходимо отметить все флажки типов событий напротив интересующих типов устройств, которые требуется отправлять с этого клиента.

Выберите клиента репликации из списка:

Укажите **драйвера и типы устройств**, от которых хотите получать события:

Клиент репликации	Наименование	Драйвер	Типы устройств	Штат.	Трев.	Неисп.	Номер СОМ-порта	Рабочая станция	Время последнего получения информации	
GUCB	axis	Бастион-AXIS	<input type="checkbox"/> Телекамера <input type="checkbox"/> Сервер	<input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>	не используется	Локальный компьютер	14.03.2008 15:00:37	
MAL		нет активных драйверов								

10. После необходимо сохранить состояние флажков кнопкой  «»

11. Дождаться всплывающего сообщения на клиенте о применении фильтра.

После появления сообщения фильтр на отправку автоматически применится. Фильтр можно просмотреть локально в «Бастионе» в общих настройках репликации на вкладке «Фильтр событий по устройствам».

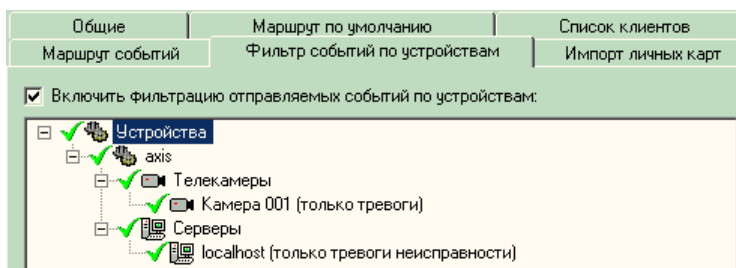


Рис. 34 - Фильтр отправляемых событий

Приложение 3. Список иллюстраций

Рис. 1 –Установка роли сервера.....	5
Рис. 2 –Установка web-портала.....	6
Рис. 3 –Установка web-портала.....	6
Рис. 4 - Консоль диспетчера служб IIS.....	7
Рис. 5 - Установка версии ASP.Net	7
Рис. 6 - Консоль IIS в Windows 2003 Server.....	8
Рис. 7 - Фрагмент консоли IIS. Пул выполняемых приложений.....	9
Рис. 8 - Свойства виртуального каталога.....	9
Рис. 9 - Безопасность виртуального каталога (Directory Security)	10
Рис. 10 - Безопасность виртуального каталога. Методы проверки подлинности	10
Рис. 11 - Безопасность виртуального каталога. Ограничения IP-адресов и имен доменов	10
Рис. 13 –Установка web-портала.....	13
Рис. 14 - Консоль IIS под Windows 7	14
Рис. 15 - Консоль IIS под Windows 7. Изменение ограничений ISAPI или CGI.....	15
Рис. 18 - Консоль IIS под Windows 2008	18
Рис. 19 - Доверенные зоны.....	20
Рис. 22 - Список участников репликации	22
Рис. 23 - Группы доступа на web-портале	24
Рис. 24 - Группы доступа на клиенте репликации.....	30
Рис. 3. Вкладка "Общие" настройки репликации и персональных данных	32
Рис. 4. Вкладка "Маршрут по умолчанию"	32
Рис. 5 Вкладка "Список клиентов"	34
Рис. 6. Настройка полномочий пользователей для системы репликации	34
Рис. 25 - Включение режима внешнего простого экспорта	36
Рис. 26 – Окна отображения "чужих" сообщений.....	39
Рис. 27 - Включение журнала чужих сообщений	40
Рис. 28. Форма клиента репликации в режиме выгрузки событий входа/выхода.....	40
Рис. 29. Вкладка «События УРВ» формы настройки клиента.....	41



Рис. 30 - Схема репликации через корпоративную сеть	50
Рис. 31 - Схема репликации через публичную сеть без шлюза	50
Рис. 32 - Схема репликации через публичную сеть со шлюзом	51
Рис. 33 - Виртуальная частная сеть VPN	52
Рис. 34 - Фильтр отправляемых событий	59