BASTION

ИНТЕГРИРОВАННАЯ СИСТЕМА БЕЗОПАСНОСТИ

Руководство системного администратора

Версия 1.7.5

ассоциация Электронные системы

Содержание

1 Введение

Этот документ предназначен для инсталляторов АПК «Бастион», а также для персонала, ответственного за его эксплуатацию. Сведения о работе со вспомогательными программами рассмотрены в отдельных инструкциях на эти программы. Сведения о конфигурировании драйверов находятся в инструкциях на соответствующий драйвер.

2 Общие сведения

2.1 Архитектура и состав АПК «Бастион»

АПК «Бастион» предназначен для интеграции в единую систему безопасности следующих подсистем:

- видеонаблюдения и/или видеорегистрации;
- охранно-пожарной сигнализации (ОПС);
- систем контроля и управления доступом (СКУД);
- систем управления технологическими процессами.

Компьютерная сеть АПК «Бастион» включает в себя следующие функциональные узлы (см. Рис. 1):

Сервер баз данных (БД). Здесь хранится вся информация о конфигурации системы. Сервер БД всегда один на весь комплекс. Этот компьютер должен работать в круглосуточном режиме, так как доступ к базе данных необходим для работы всех подсистем комплекса. В качестве СУБД используется Firebird 2.5.

Один или несколько (до 15) компьютеров, к которым подключено оборудование подсистем безопасности (серверы оборудования). Каждый сервер оборудования может обслуживать до 15 подсистем (драйверов).

Неограниченное число клиентских рабочих мест без подключенного оборудования.

Несколько территориально распределенных объектов с АПК «Бастион» могут объединяться с использованием системы «Бастион-Репликация». При этом каждый объект работает со своей базой данных АПК «Бастион».

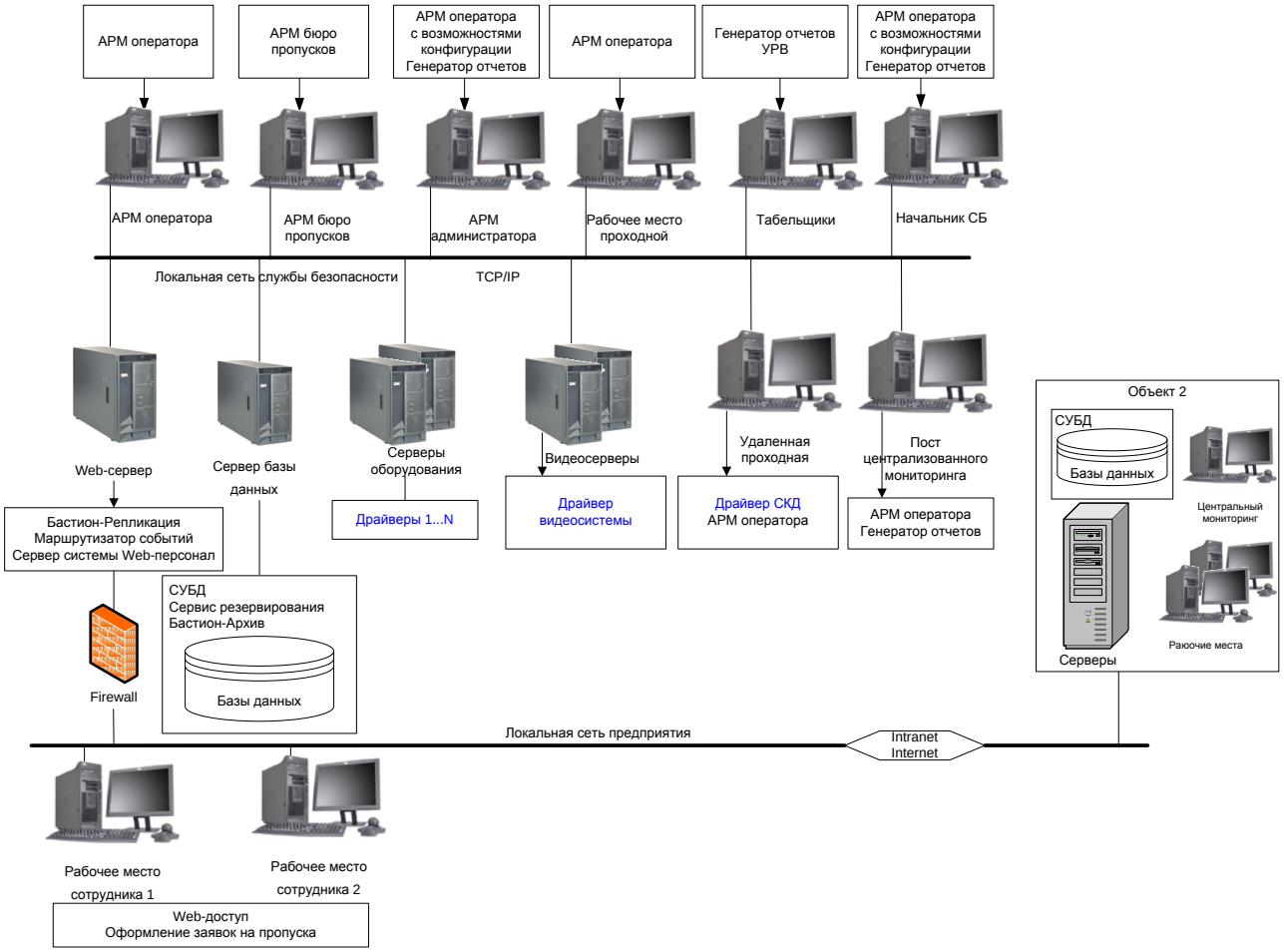


Рис. 1. Структура сети АПК «Бастион»

Все перечисленные узлы могут совмещаться на одном компьютере. Например, как правило, объединяется сервер баз данных и сервер оборудования.

Сеть АПК «Бастион» построена на основе протокола TCP/IP, поэтому перед установкой системы необходимо на каждом компьютере установить и сконфигурировать данный протокол.

Программное обеспечение АПК «Бастион» структурно разделяется на три основные группы: драйверы, модуль «Бастион-Сеть» и дополнительные программные модули (см. Рис. 2). Информация о возможности использования модулей и драйверов на конкретном рабочем месте находится в ключе защиты «HASP», устанавливаемом на каждом рабочем месте системы.

Подробную информацию о правилах комплектации АПК «Бастион» можно найти в документе «Правила комплектации» или в каталоге продукции.

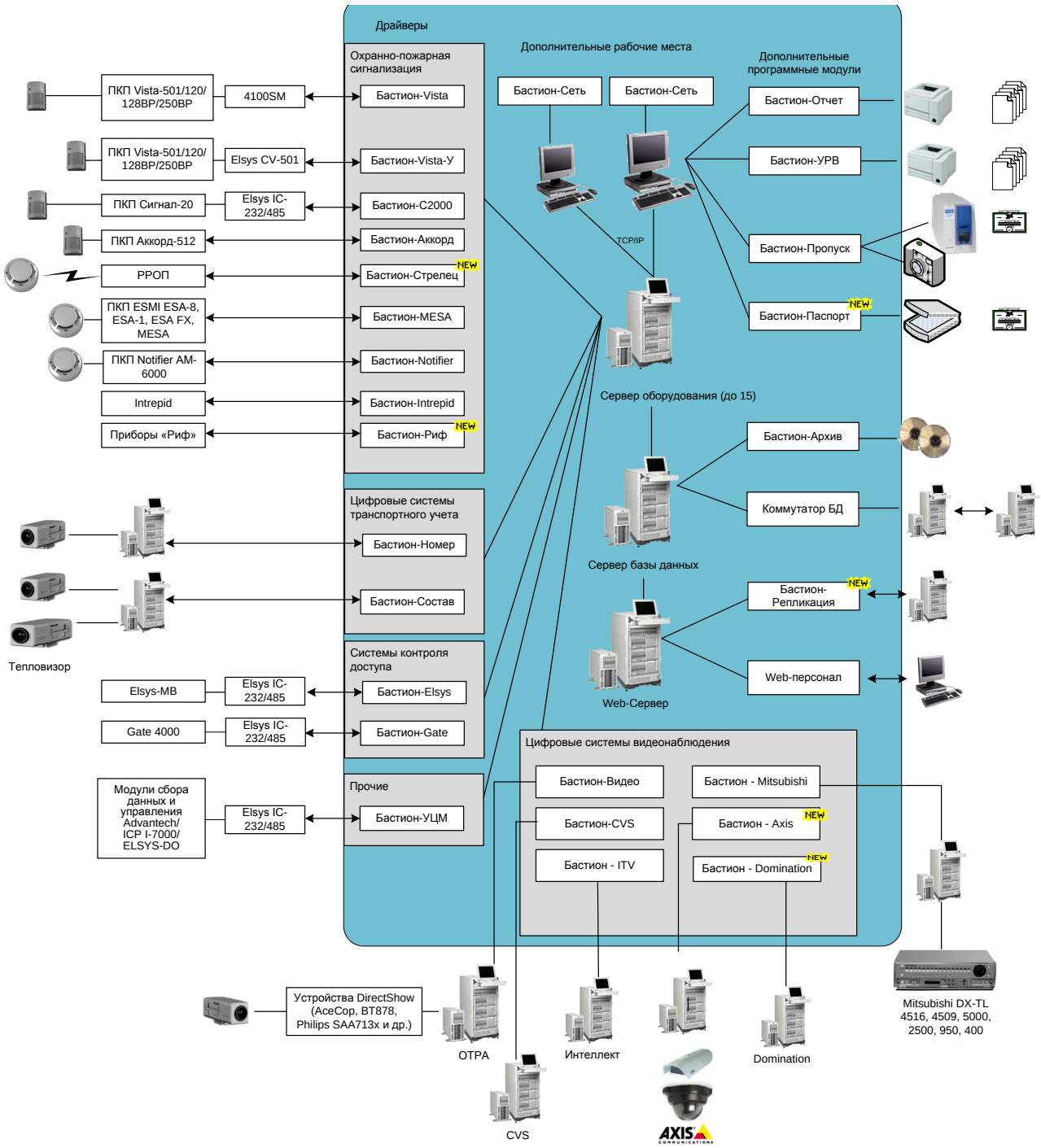


Рис. 2. Структура модулей АПК «Бастион»

Список файлов АПК «Бастион» приведен в Приложении 1.

3 Инсталляция АПК «Бастион»

3.1 Установка программного обеспечения

Программное обеспечение «Бастион» должно быть установлено на всех компьютерах в сети комплекса. Один из компьютеров является сервером баз данных – он должен быть постоянно включен. Обычно сервер баз данных совмещают с сервером оборудования. При

установке сетевой версии на всех рабочих станциях должен быть предварительно установлен и сконфигурирован протокол TCP/IP (сведения об этом есть в инструкции на соответствующую операционную систему), а для дальнейшей настройки ПО «Бастион» необходимо знать имена или IP-адреса компьютеров.

Поддерживаемые операционные системы: Windows 7, Windows 8, Windows 8.1, Windows 2008 Server R2, Windows 2012 Server R2. Поддерживается работа на 32-х и 64-х разрядных операционных системах.

Не поддерживаются Windows 2000, Windows XP и Windows 2003 Server, Windows 2008.

Для проведения установки необходимо обладать правами администратора ОС.

Запустите программу установки АПК «Бастион» (из оболочки, появляющейся при автозапуске диска, либо запустив файл <CDROM>:\Install\Setup.exe). В процессе установки необходимо ответить на ряд вопросов.

Выбор каталога установки (по умолчанию – на диск, где установлена операционная система, в каталог Bastion; важно, чтобы на диске, куда будет устанавливаться «Бастион», было достаточно места, с учётом требуемого места под основную и протокольную базу данных).

Вид установки. При выборе *серверного* варианта будут установлены все компоненты системы. Этот вариант установки следует выбирать на сервере базы данных (т. е. на компьютере, где будет располагаться основная и протокольная базы данных). При выборе *клиентского* варианта будут установлены все компоненты системы, за исключением базы данных. Этот вариант установки рекомендуется выполнять на клиентских рабочих местах.

Путь для установки Firebird 1.5 (по умолчанию – в папку «Program Files\Firebird\Firebird_1_5»).

Путь для основной и протокольной базы данных, а также имя компьютера, который будет сервером баз данных (Рис. 3). Если компьютер в системе один, поле «Сервер» можно не заполнять.

> ***Внимание!*** *В ОС Windows Vista не поддерживается локальный протокол доступа к серверу БД Firebird. Поэтому для доступа к БД всегда указывается сервер. Для локального компьютера это будет localhost. Инсталлятор подставляет значение localhost, если поле «Сервер» оставить пустым.*

Если при установке ПО «Бастион» были неправильно заданы имя сервера и пути к базам данных, позже это можно исправить с помощью утилиты «BDE Administrator». Описание этого процесса приведено в п. 6.6.

Пароль для подключения к базе данных. Необходимо ввести пароль для учетной записи APP_ADMIN, которая используется для подключения к БД. Если оставить поле пустым (не рекомендуется), будет использовано значение пароля по умолчанию (см. п. 6.4).

При установке на клиентских местах пароль будет записан в зашифрованном виде в локальное хранилище. Если же выполняется установка сервера Firebird (серверный вариант

установки), то указанный пароль будет дополнительно прописан в БД пользователей Firebird.

> ***Внимание!*** *Если при установке на клиентском месте ввести неверный пароль, то сменить его можно с помощью утилиты «Обслуживание БД» (BArchive.exe). Более подробно см. документацию на этот модуль.*

Для смены пароля в БД пользователей Firebird следует воспользоваться утилитой IBExpert или командой gsec.exe.

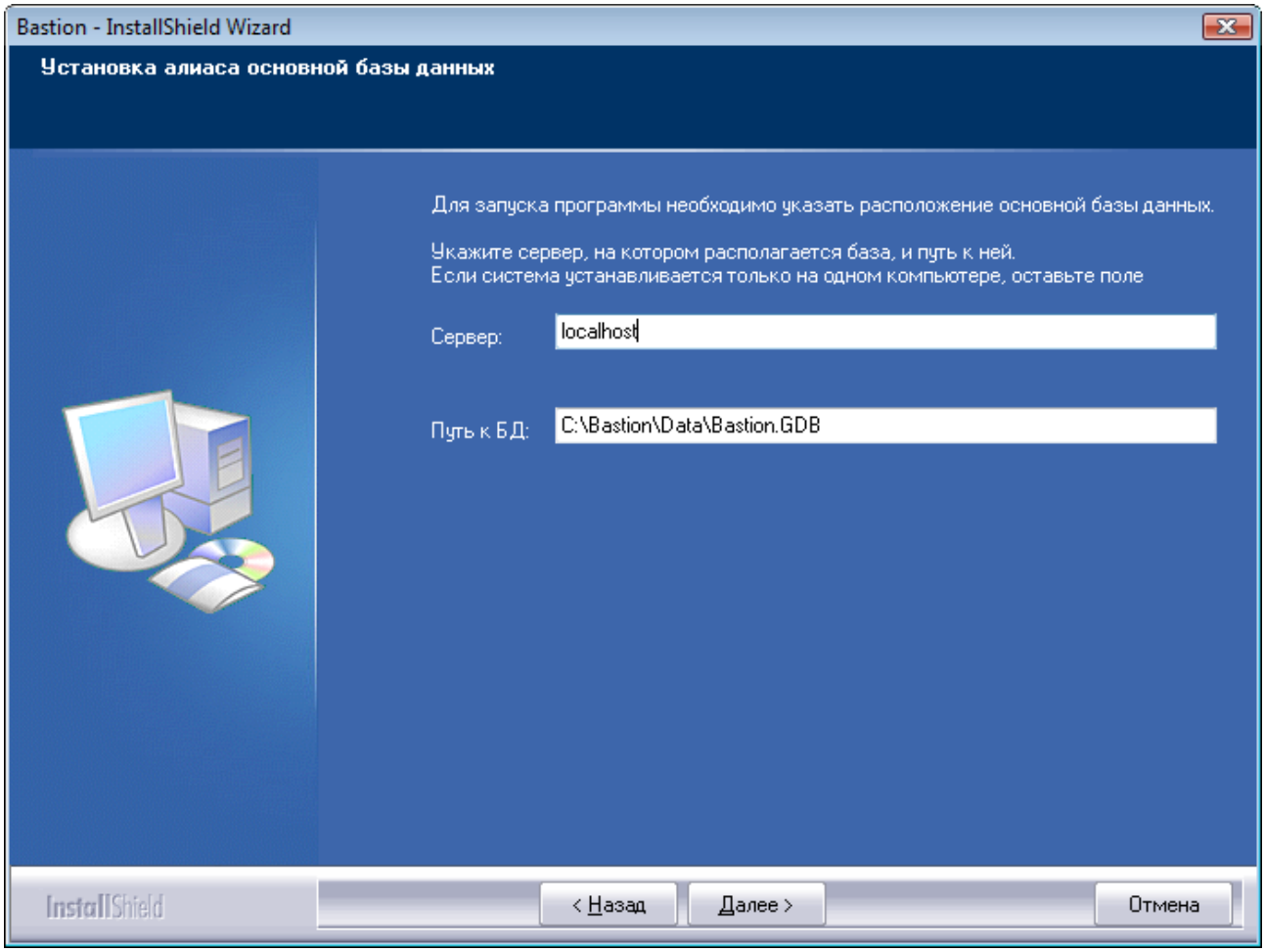


Рис. 3. Настройка путей к БД при установке ПО «Бастион».

При завершении установки может потребоваться перезагрузить компьютер.

После этого программное обеспечение готово к запуску.

3.2 Запуск и выгрузка системы

Основное приложение комплекса – Bastion.exe – может запускаться в любой последовательности на всех рабочих местах комплекса. Запустите ПО «Бастион», щёлкнув дважды мышью по ярлыку на рабочем столе или выбрав пункт «Бастион» в главном меню. **При первом запуске следует ввести имя пользователя – «q» и пароль**

«q». Этот пользователь имеет максимальные полномочия, и он пока единственный в базе данных ПО «Бастион». В дальнейшем рекомендуется изменить этот пароль.

Запуск программы невозможен при отсутствии связи с базой данных. В ходе работы системы при потере связи с БД блокируются функции настройки системы, а также ряд сервисных возможностей. После восстановления связи работа системы продолжается в штатном режиме.

Для запуска системы без полномочий администратора см. п. 5.3.

4 Подготовка программного обеспечения к эксплуатации

4.1 Работа с формами редактирования баз данных

Все формы для работы с отдельными таблицами базы данных имеют сходный интерфейс для навигации по таблице и редактирования данных.

В верхней части таких форм находится специальный элемент управления, имеющий следующий вид:

Рис. 4. Навигатор по таблице базы данных

Назначение кнопок:

 Переход к первой записи.

 Переход к предыдущей записи.

 Переход к следующей записи.

 Переход к последней записи.

 Добавить новую запись.

 Удалить текущую запись.

 Войти в режим редактирования текущей записи.

 Сохранить изменения в текущей записи (сохранить запись).

 Отменить изменения текущей записи.

 Обновить (перечитать из базы данных) содержимое таблицы.

 Вызов окна поиска.

Отдельные кнопки в ряде случаев могут отсутствовать. Следует иметь в виду, что:

Редактирование данных производится только в специальных элементах управления, но не в таблице в нижней части окна;

Переход из режима просмотра в режим редактирования текущей записи происходит автоматически при попытке изменить содержимое любого поля;

Сохранение изменений текущей записи происходит автоматически при попытке выбрать любую из кнопок (кроме кнопки «отмены изменений записи») навигатора.

Поиск данных производится в отдельном окне и позволяет искать записи по 1 или 2 полям, объединяя условия поиска по «*и*» или «*или*». Поиск может производиться по любым текстовым и числовым полям, принадлежащим редактируемой таблице.

Горячие клавиши для редактирования данных:

Ins	Вставка новой записи.
Ctrl+S	Сохранение текущей записи.
Esc	Отмена изменений в текущей записи.
Enter	Переход в режим редактирования текущей записи, если при нажатии была активна таблица.
Ctrl+F	Вызов окна поиска.

4.2 Последовательность действий при настройке

Настройку системы рекомендуется производить в следующем порядке:

1. Определить конфигурацию компьютерной сети и портов, к которым будет подключаться оборудование системы безопасности.
2. Добавить рабочие станции (п. 4.3), а затем драйверы (п. 4.4).
3. Настроить полномочия, список пользователей (п. 4.5), и профили пользователей (п. 4.6).
4. Настроить добавленные драйверы (см. инструкцию на соответствующий драйвер).
5. Расставить пиктограммы на графических планах (п. 4.7).
6. Настроить параметры обработки событий (п. 4.8), сценарии и реакции на события.
7. Настроить области контроля, глобальный контроль последовательности прохода и систему учёта рабочего времени.
8. Выполнить все остальные требуемые настройки (можно производить в произвольном порядке).
9. Далее рассматриваются указанные действия в правильной последовательности.

4.3 Конфигурация рабочих станций

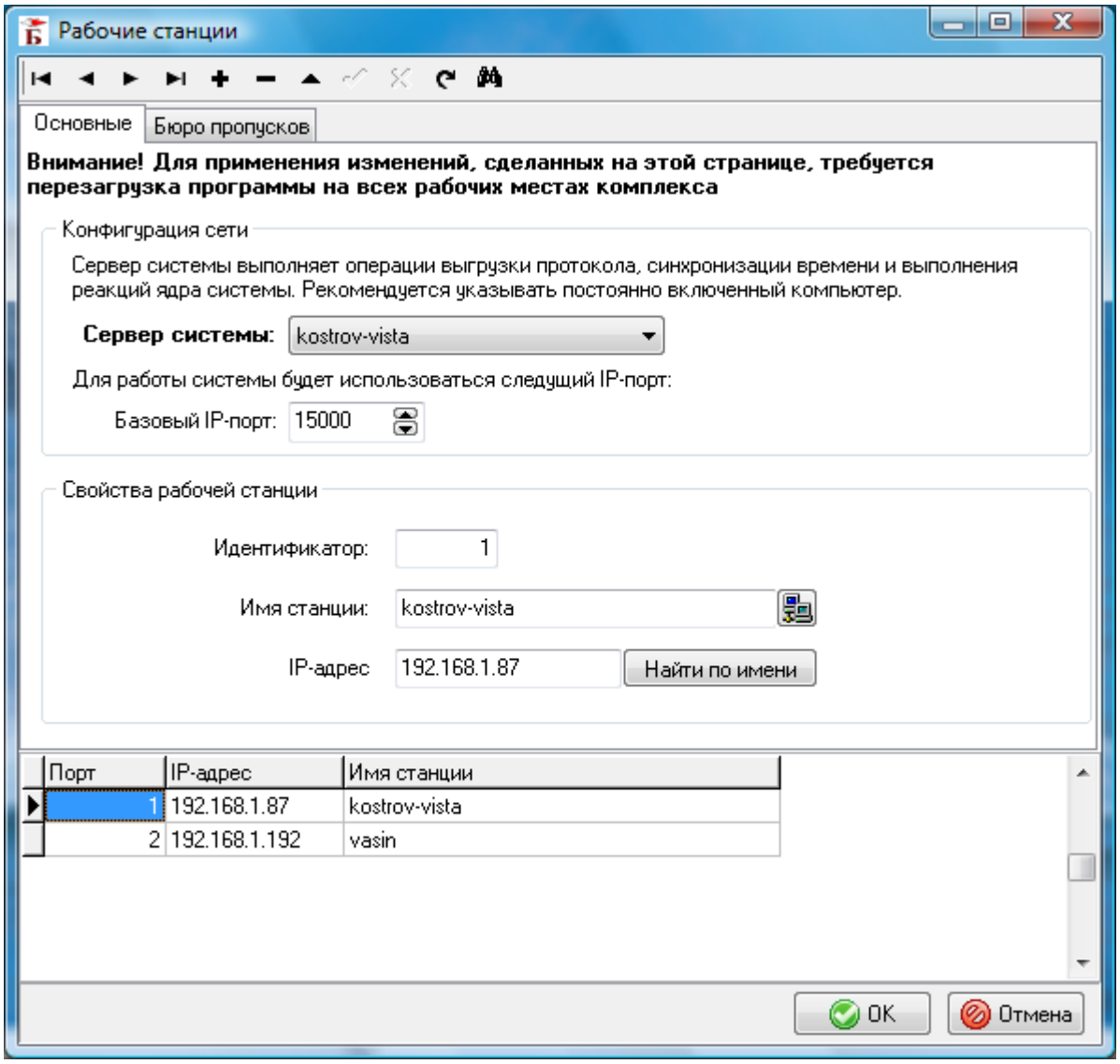


Рис. 5. Добавление рабочих станций

Для добавления, удаления и редактирования свойств рабочих станций системы необходимо выбрать пункт меню «Конфигурация→Рабочие станции».

Для обмена информацией между рабочими станциями комплекс использует протокол TCP/IP. В сети АПК «Бастион» используется схема подключений «каждый с каждым».

При первом запуске Bastion.exe в базу данных прописывается локальный компьютер со своим коротким dns-именем и IP-адресом.

В случае если по каким-либо причинам системе не удастся получить сетевые параметры локального компьютера (например, в компьютере не установлено ни одной сетевой карты, или в имени компьютера использованы русские буквы), в базе данных будет присутствовать рабочая станция с именем «Локальный компьютер», адресом 127.0.0.1 и номером порта 0.

> ***Внимание!*** *Использовать «Локальный компьютер» для установки драйверов можно только в том случае, если в системе не планируется других рабочих мест.*

Для каждой рабочей станции необходимо ввести:

Идентификатор – Цифровой идентификатор станции. Для каждой станции должно быть указано уникальное значение.

> ***Внимание!*** *Следует иметь ввиду, что установка драйверов возможна только для рабочих станций с идентификаторами в диапазоне [1-15].*

Имя станции – реальное имя компьютера в сети. Следует использовать краткое имя (например *Security*, а не *www.security.mycompany.com*).

IP-адрес – адрес компьютера в сети.

Группа «Конфигурация сети» содержит параметры:

Сервер системы - выполняет операции выгрузки протокола, синхронизации времени и выполнения реакций ядра системы. Рекомендуется указывать постоянно включенный компьютер.

> ***Внимание!*** *Если сервер системы не указан, выполнение ряда функций системы будет невозможно.*

Базовый IP-порт – порт, который будет использован для общения между рабочими станциями системы. По умолчанию – 15000.

> ***Внимание!*** *Для корректной работы системы обмен по Базовому IP-порту должен быть разрешен для всех рабочих станций.*

4.4 Работа со списком драйверов системы

Экземпляры драйверов устройств можно добавить, выбрав пункт меню «Конфигурация→ Драйверы» (См. Рис. 6).

Для добавления устройства (экземпляра драйвера) необходимо нажать кнопку «добавить запись», ввести название устройства, выбрать один из доступных управляющих драйверов (соответствующий типу добавляемого устройства), номер последовательного порта (если требуется) и имя рабочей станции.

Флаг *«Показывать устаревшие драйвера»* позволяет вывести полный список всех драйверов АПК «Бастион». По умолчанию отключено.

Назначение и правила заполнения полей базы данных устройств:

Название устройства - служит для ввода уникального названия устройства, обеспечивающего его идентификацию при дальнейшей настройке ПО. Поле может содержать любые печатные символы в русском и / или английском регистрах. Общая длина названия (включая пробелы) не должна превышать 40 символов, например, «Система ТВ наблюдения».

Драйвер - поле служит для выбора драйвера, обеспечивающего взаимодействие основного модуля ПО (ядра программы) с физическим устройством.

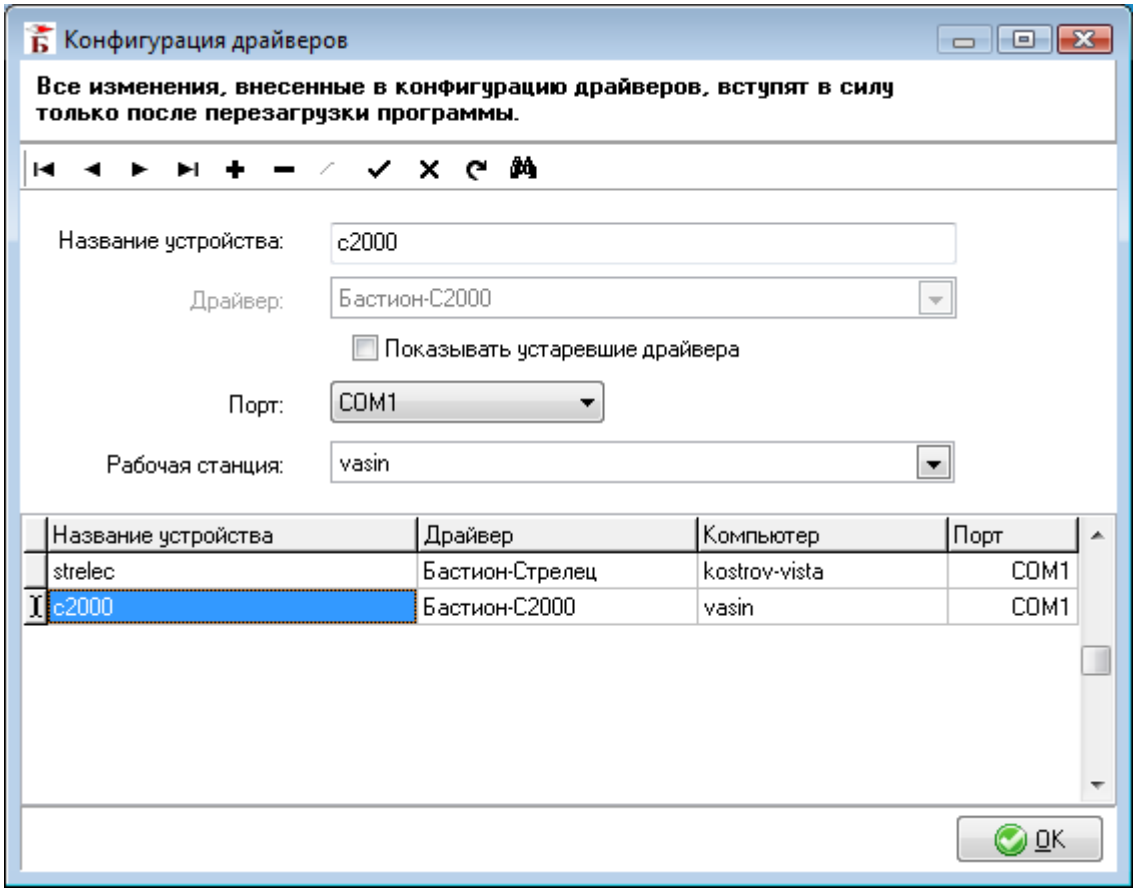


Рис. 6. Добавление экземпляров драйверов

Порт - определяет номер COM-порта той рабочей станции, к которой подключено устройство. Номер может быть выбран из диапазона от 1 до 15, однако реальное количество свободных COM-портов может быть меньше. Для корректного выбора необходимо определить номера доступных (не занятых другими устройствами) COM-портов на выбранной рабочей станции.

> ***Внимание!*** *Использование недоступных номеров COM-портов (например, занятых другими устройствами - мышью или модемом) приведет после перезагрузки программы к сообщению об ошибке: «Ошибка инициализации драйвера <Название драйвера>. Невозможно открыть порт <Номер порта>». При появлении такого сообщения необходимо либо освободить указанный порт, либо задать другой порт в окне «Конфигурация драйверов».*

Рабочая станция – обеспечивает выбор рабочей станции, к которой подключено оборудование, взаимодействующее с указанным драйвером и COM-портом. Если в комплексе используется только один компьютер, в этом поле может быть установлено значение «Локальный компьютер». Однако рекомендуется, даже если компьютер в системе один, задавать имя рабочей станции (если в дальнейшем потребуется расширить систему, могут быть трудности с переназначением рабочих станций, и, вероятно, потребуется заново настраивать драйвер). В списке рабочих станций будут отображены только те компьютеры, для которых значение IP-порта было задано в диапазоне 1-15.

Для того чтобы внесенные изменения вступили в силу, необходимо перезапустить программу на всех рабочих станциях системы безопасности.

После добавления драйвера и перезапуска ПО «Бастион» в нижней части меню «Конфигурация» появятся пункты, относящиеся к настройке добавленного драйвера (Рис. 7).

Ряд пунктов меню (для драйвера СКУД «Elsys» - пункты «Управление оборудованием» и «Поиск устройств») доступны лишь на том компьютере, к которому подключено оборудование, относящееся к выбранному драйверу. Если же эти пункты не появились, значит, либо на этой рабочей станции установлено сетевое рабочее место, либо были допущены ошибки при вводе имени компьютера и его IP-адреса.

Другие пункты меню (для драйвера СКУД «Elsys» это – «Конфигурация оборудования» и «Инициализация оборудования») доступны на всех рабочих станциях комплекса.

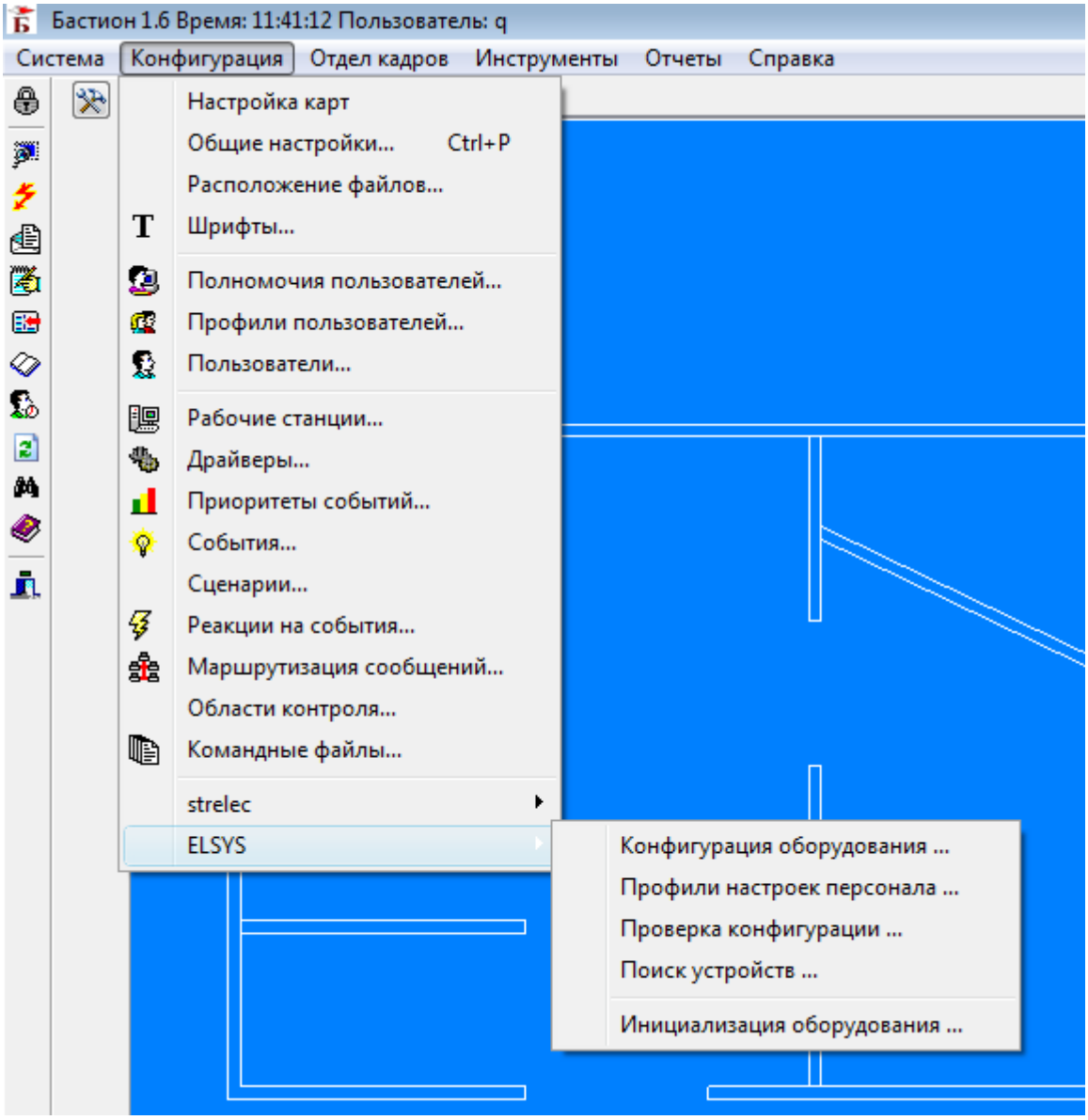


Рис. 7. Пример меню драйвера

4.5 Настройка пользовательских полномочий и добавление пользователей

Окно настройки пользовательских полномочий доступно из меню «Конфигурация→Полномочия пользователей», (Рис. 8). Окно содержит несколько вкладок, в соответствии с установленными подсистемами.

Поле *«Приоритет»* определяет минимально необходимый уровень пользовательских полномочий для выполнения операции. Большинство настроек полномочий пользователей можно оставить без изменений.

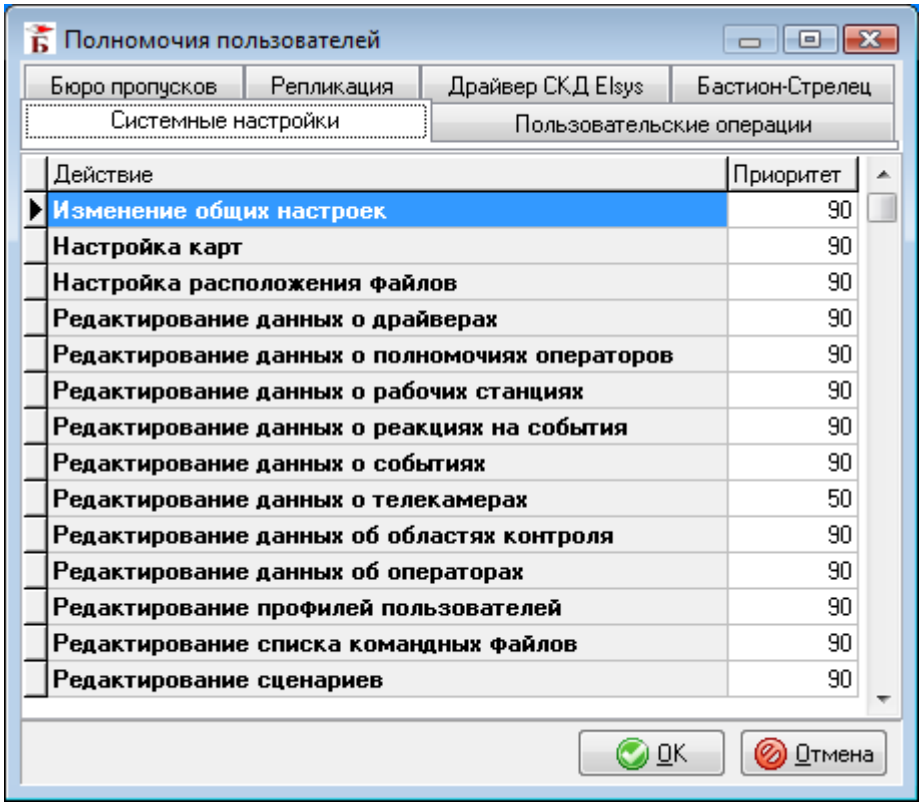


Рис. 8. Окно настройки полномочий пользователей

Для добавления пользователей и редактирования их полномочий следует выбрать пункт меню «Конфигурация→Пользователи» (Рис. 9).

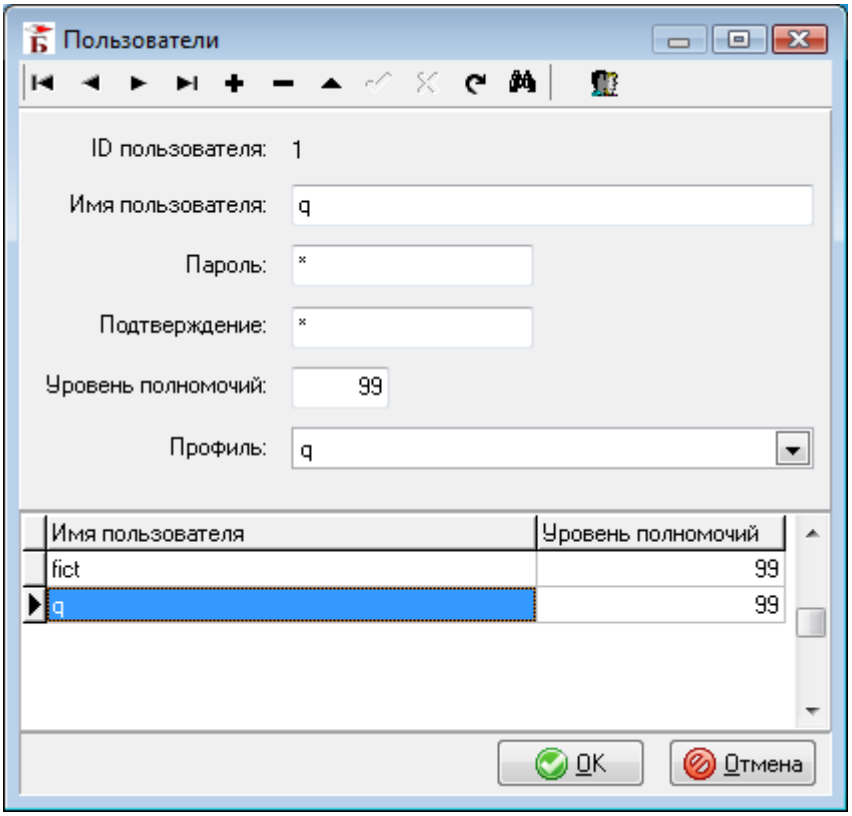


Рис. 9. Форма редактирования данных о пользователях

Для *добавления* нового пользователя необходимо:

- нажать клавишу «добавить запись»;
- ввести имя и пароль пользователя в соответствующих полях окна. Имя и пароль могут содержать любые печатные символы в русском или английском регистрах и цифры, причем строчные и прописные буквы различаются при анализе пароля;
- подтвердить введенный пароль, набрав его повторно;
- указать требуемый профиль и уровень полномочий пользователя;
- нажать клавишу «сохранить запись».

Рекомендуется добавлять отдельного оператора комплекса «Бастион» на каждого человека, работающего с системой. Это может быть полезно при анализе протокола событий (например, определить, в чью смену случилось происшествие или кто изменял настройки). При смене дежурства следует проводить повторный вход в ПО «Бастион» под новым именем. Для каждого пользователя назначается один из настроенных заранее профилей пользователей.

Обычно рекомендуется дежурному оператору поста охраны присвоить уровень полномочий 10, оператору бюро пропусков – 50, администратору – 90..99.

При первоначальной настройке можно для всех пользователей указать один профиль.

4.6 Настройка профилей пользователей

4.6.1 Общие настройки

Для настройки профилей пользователей следует выбрать пункт меню «Конфигурация→Профили пользователей». Профиль пользователя (Рис. 10) задаёт ряд настроек пользовательского интерфейса, специфичных для группы операторов. Кроме того, на основе профилей пользователей осуществляется маршрутизация сообщений, разграничивающая зоны ответственности пользователей и распределяющая поток событий между операторами системы. При входе в программу, независимо от компьютера, на котором это производится, загружается тот профиль, который указан для пользователя. Один и тот же профиль можно назначить нескольким пользователям.

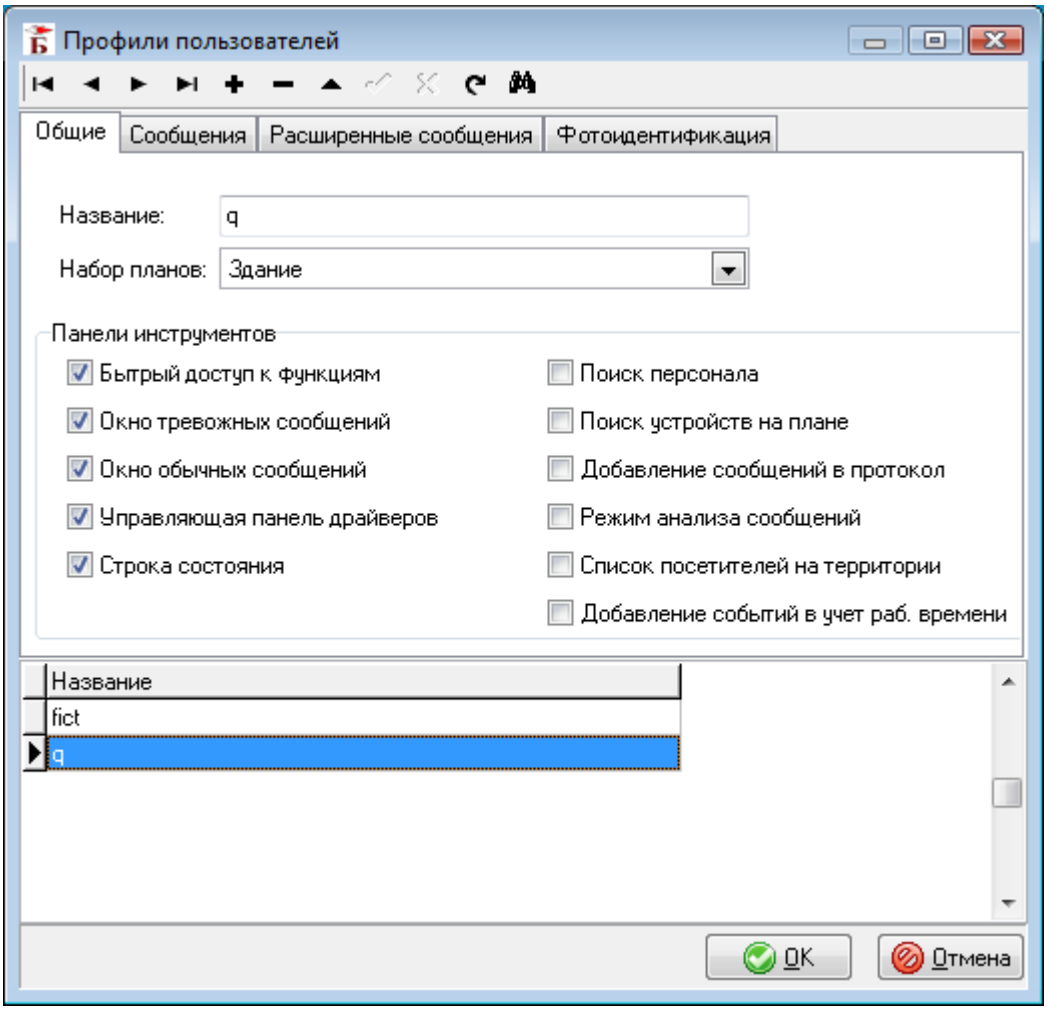


Рис. 10. Окно настройки профилей пользователей

На вкладке «Общие» можно задать *название профиля,* определить *набор графических планов,* используемых для профиля, и выбрать, какие панели инструментов показать, а какие скрыть.

4.6.2 Параметры отображения сообщений

На странице «Сообщения» (Рис. 11) можно задать, какие сообщения будут отображаться системой. Следует иметь в виду, что параметры отображения и параметры записи в

протокол не влияют друг на друга. Поэтому, даже если сообщение не отображается, оно может быть записано в журнал событий.

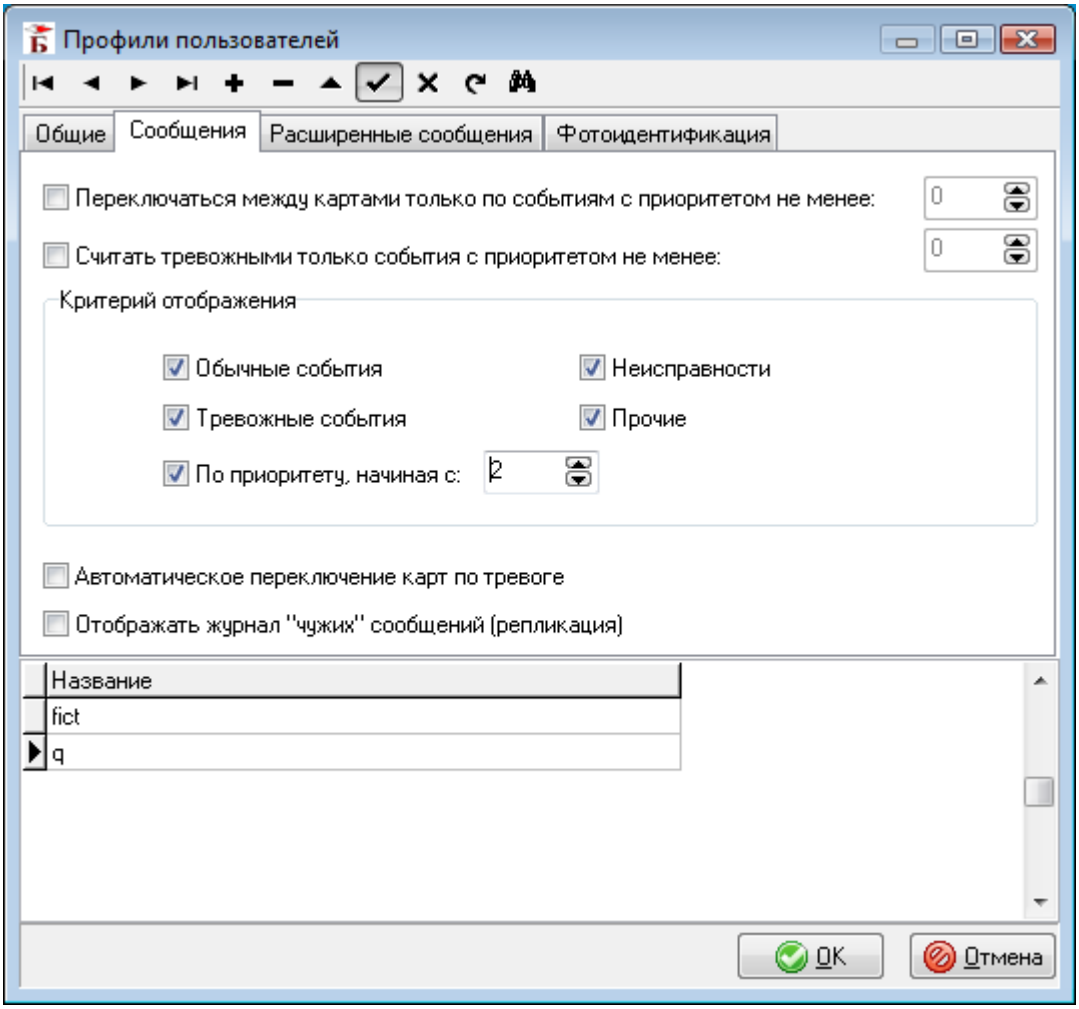


Рис. 11. Настройка параметров отображения сообщений

Система позволяет определять критерий отображения на основе типа сообщений (обычное, тревожное, неисправность, прочие), и их приоритета.

Флаги типов сообщений объединяются по логическому «или», а флаг отбора по приоритету – по логическому «и» со всеми остальными. Так, изображённые на Рис. 11 настройки обеспечивают вывод сообщений для всех событий с приоритетом от 2.

Автоматическое переключение карт по тревоге – при установленном флаге графические планы будут автоматически переключаться для отображения места возникновения последнего тревожного события.

Переключаться между картами только по событиям с приоритетом не менее заданного – опция имеет смысл только при включенном режиме автопереключения по событиям. В этом режиме при возникновении тревожного события система перейдет к тому графическому плану, на котором установлено устройство-источник данного события. Исключить излишне частое переключение планов можно, при помощи соответствующей настройки приоритетов событий.

Считать тревожными только события с приоритетом не менее заданного – с помощью этой настройки можно переопределить тип события, присваиваемый системой по умолчанию (например, низкоприоритетные тревоги могут считаться обычными сообщениями).

Отображать журнал «чужих» сообщений (репликация) – позволяет отобразить или скрыть окно сообщений, получаемых с удаленных объектов через систему «Бастион-Репликация».

4.6.3 Параметры отображения расширенных сообщений

Страница «Расширенные сообщения» (Рис. 12) предназначена для настройки параметров отображения расширенных сообщений.

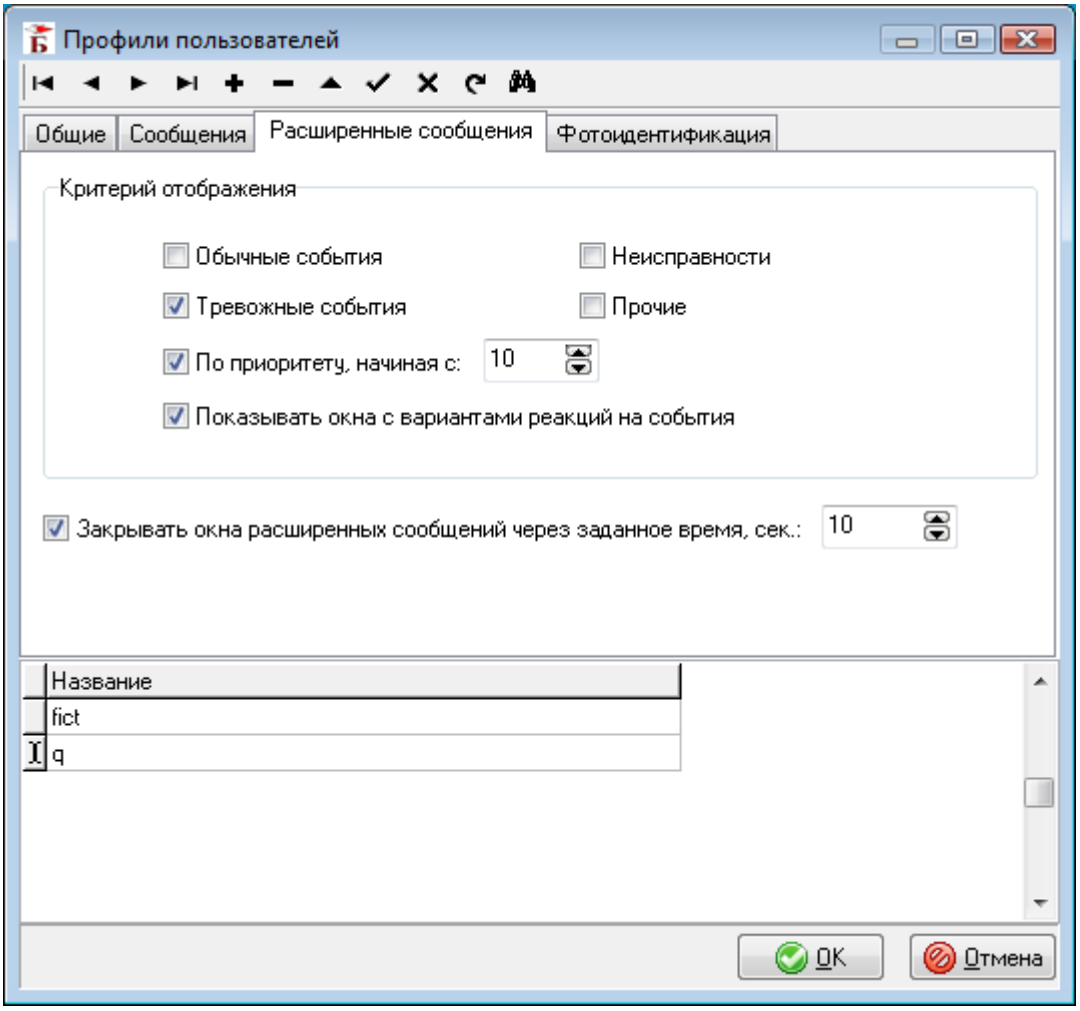


Рис. 12. Настройка параметров отображения расширенных сообщений

Окна расширенных сообщений (Рис. 13) предназначены для привлечения внимания оператора к особо важным сообщениям, поэтому к установке режима их отображения следует относиться особенно внимательно.

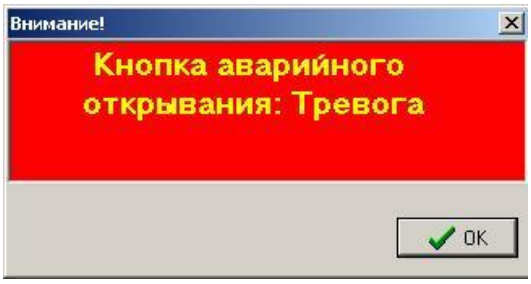


Рис. 13. Окно расширенного сообщения

Так же как и для простых текстовых сообщений, система предоставляет возможность установки фильтра по типу события и его приоритету. Так, изображённые на Рис. 12 настройки обеспечивают вывод расширенных сообщений только для тревожных событий с приоритетом равным или большим 10.

> ***Внимание!*** *Для вывода расширенного сообщения, кроме выполнения условий фильтрации, у события должен быть приоритет, с включенной опцией «Выводить расширенное сообщение» (см. п. 4.8.3).*

Опция «*Закрывать окна расширенных сообщений автоматически*» (через заданный промежуток времени) предназначена для предотвращения загромождения основного окна программы излишней (устаревшей) информацией.

4.6.4 Параметры отображения фотоидентификации

Фотоидентификация может использоваться, если в состав АПК «Бастион» входит драйвер СКУД (например, СКУД ELSYS). Режим фотоидентификации сотрудников предназначен для проведения сравнения лица, предъявившего карту, с фотографией подлинного владельца карты доступа и принятия решения о предоставлении или не предоставлении доступа.

Вкладка «Фотоидентификация» (см. Рис. 14) предназначена для настройки режима отображения окон фотоидентификации. Фотографии сотрудников должны быть предварительно занесены в базу данных программы.

Система позволяет регулировать отображение окон фотоидентификации по следующим признакам:

Использовать для событий с приоритетом не менее заданного. Опция позволяет установить фильтр на вывод окон фотоидентификации по приоритету события.

Использовать для карточек с приоритетом не более заданного. Опция позволяет установить фильтр на вывод окон фотоидентификации по приоритету карты доступа.

Закрывать окно фотоидентификации автоматически через заданный промежуток времени. Позволяет закрывать окна с устаревшей информацией автоматически.

Максимальное число одновременно отображаемых окон. Позволяет автоматически закрывать окна фотоидентификации при предъявлении новых карт доступа. Допустимые значения – от 0 до 16. При установке значения 0 ограничение отсутствует.

Показывать фотоидентификацию при открытых модальных окнах. Если выключено (по умолчанию), то при работе в любых окнах настройки системы окна фотоидентификации отображаться не будут.

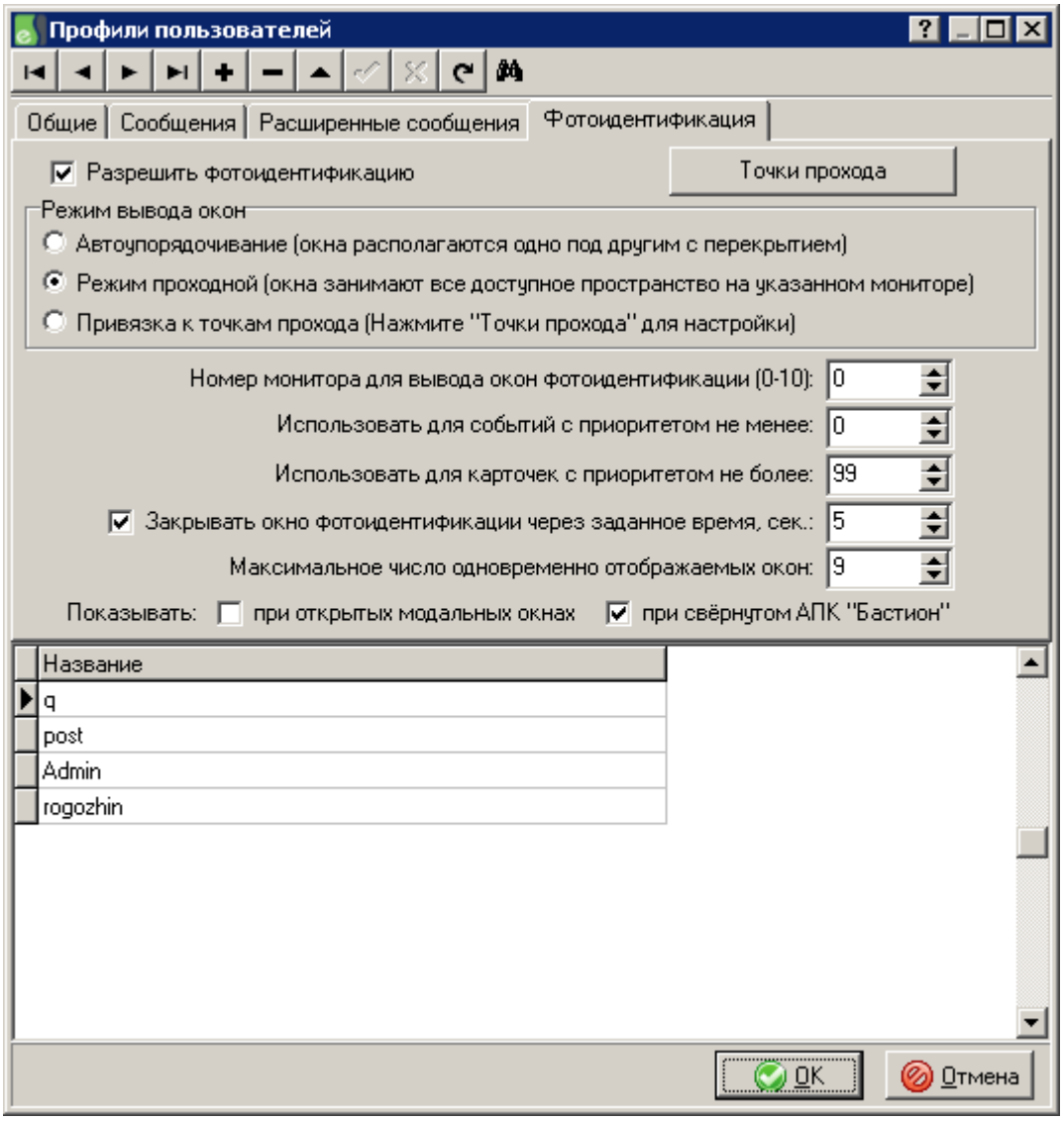


Рис. 14. Окно настройки параметров фотоидентификации

Также, можно настроить режим вывода окон фотоидентификации.

Автоупорядочивание. В этом режиме окна фотоидентификации будут располагаться друг под другом с перекрытием на основном мониторе.

Режим проходной (окна занимают все доступное пространство на указанном мониторе). Этот режим можно использовать на рабочем месте поста охраны на проходной. При этом, окна с фотографиями владельцев карт будут занимать все доступное пространство на указанном мониторе. Окна фотоидентификации не будут перекрывать друг друга. Основной монитор имеет номер 0.

Привязка к точкам прохода. В этом режиме положение окна фотоидентификации будет зависеть от точки прохода, от которой пришло событие. Настроить расположение окон можно, нажав кнопку «Точки прохода» (см. ниже).

Кнопка *«Точки прохода»* позволяет задать список точек доступа, события от которых должны участвовать в фотоидентификации (Рис. 15) для выбранного профиля пользователя.

Кроме того, в этой же форме можно настроить расположение окон фотоидентификации с привязкой к:

- точкам прохода (список турникетов, дверей и т.п.)*;*
- *направлению прохода в каждой точке* (входные события / выходные события).

Для этого нажмите кнопку «Установить расположение форм фотоидентификации» вверху формы. После этого, для каждой точки фотоидентификации появится отдельная форма, с соответствующим заголовком. Расположите формы так, как вы их хотите видеть в дежурном режиме, и нажмите кнопку «Сохранить расположение форм фотоидентификации» (Рис. 15). Если в системе используется несколько мониторов, можно задействовать их все. Координаты (верхний левый угол) каждой формы также можно скорректировать вручную (Рис. 15).

Рис. 15. Окно определения точек прохода для фотоидентификации

4.7 Настройка графических планов

Использование графических планов обеспечивает интерактивное управление устройствами и наглядное отображение текущего состояния устройств в системе.

На Рис. 16 изображены контекстные меню, с помощью которых оператор может управлять режимами различных устройств.

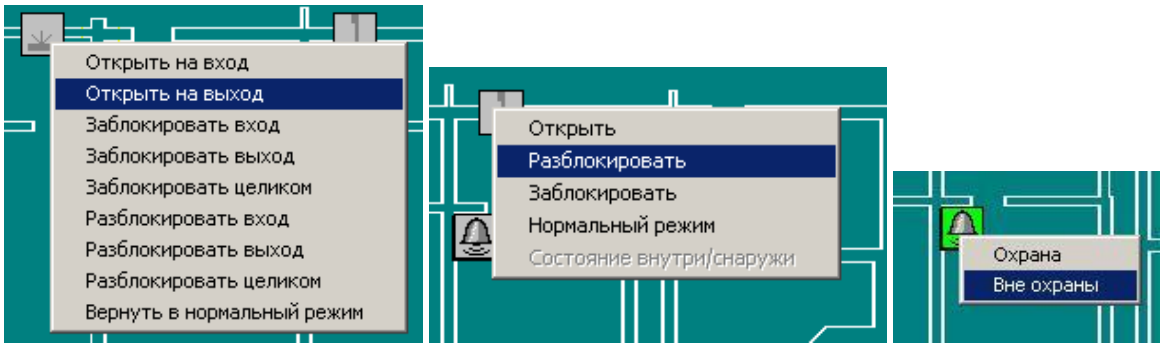


Рис. 16. Контекстные меню для управления устройствами.

В качестве графических планов могут быть использованы изображения как векторном (*.DXF), так и в растровом (*.JPG, *.BMP) форматах. Для более корректного масштабирования плана рекомендуется использовать векторные планы. Не рекомендуется использовать растровые файлы с разрешением более 1024x1024.

4.7.1 Работа с деревом планов

Для входа в режим настройки графических планов выберите пункт меню «Конфигурация→Настройка карт». При этом на экране появится отдельное окно с деревом устройств (Рис. 17).

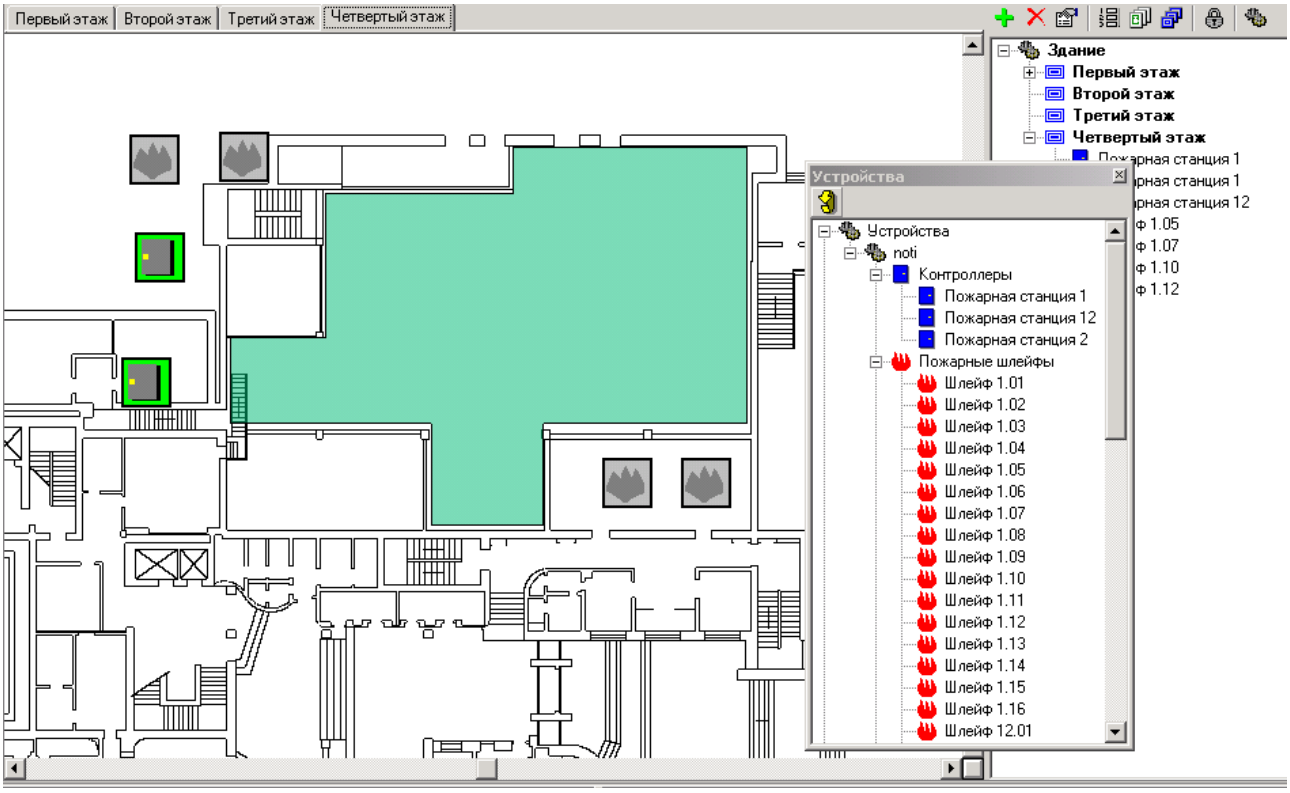
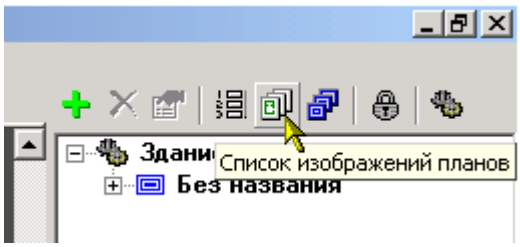


Рис. 17. Режим настройки карт

Изображения планов хранятся в базе данных. Управление ими осуществляется с помощью окна *«Список изображений планов»* (Рис. 18). Оно вызывается из панели над деревом планов или из окон свойств/добавления планов. В этом окне можно добавить из файла, удалить, переименовать или экспортировать в файл изображение плана.



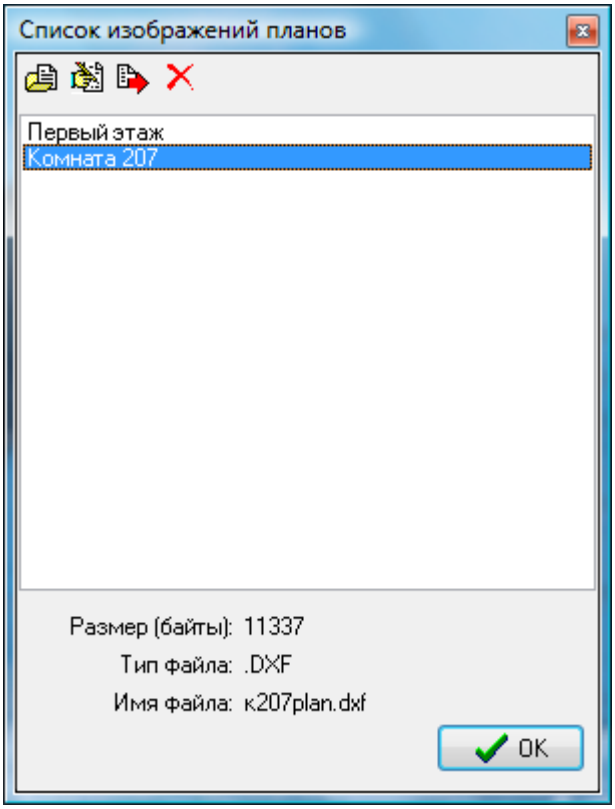


Рис. 18. Окно список изображений планов

Для добавления нового плана выберите верхний узел дерева и из контекстного меню выберите пункт «Добавить» или кнопку «+» на панели над деревом планов. В появившемся окне укажите изображение и следующие параметры:

Описание. Текст, появляющийся в качестве названия плана (например, на закладках основной формы). Планы не могут иметь одинаковые названия.

Приоритет. Используется при включенном режиме автопереключения планов по событиям для выбора наиболее приоритетного плана с пиктограммой устройства-источника события.

Цвета. Для векторных файлов можно указать цвет отображения фона, линий и шрифтов. Для этого нужно нажать кнопку «Цвета». В появившемся окне выбрать один из пунктов: Фон, Линии или Шрифт и щелкнуть по цветному квадрату слева. Появится окно выбора цвета.

После добавления плана в главном окне появляется дополнительная вкладка с именем плана. Всего планов добавлено может быть до 255.

Окно свойств любого объекта дерева планов (в правой части экрана) может быть вызвано из контекстного меню.

Для удаления объекта (плана, пиктограммы) из дерева планов, выберите этот объект и в контекстном меню щелкните на пункте «Удалить» или кнопку «–» на панели над деревом планов.

Существует возможность редактирования наборов планов для разных профилей пользователей. Для этого нажмите на кнопку «Список наборов планов» на панели над деревом планов. В появившемся окне «Выбор набора планов» можно создать, удалить или импортировать из файла набор планов. Выбор осуществляется двойным щелчком по названию набора или выделением набора и нажатием кнопки «ОК».

Рис. 19. Окно выбора набора планов

Привязка набора планов к профилю пользователя осуществляется в окне «Профили пользователей» (Рис. 10).

Для выхода из режима настройки планов ещё раз выберите пункт меню «Конфигурация→Настройка карт».

4.7.2 Расстановка пиктограмм

После добавления одного или нескольких планов на них могут быть вынесены пиктограммы устройств. Пиктограммы перетаскиваются (механизм «drag and drop») на план из окна дерева устройств (появляется при переходе в режим настройки карт). Все устройства в этом окне разделены на группы. Каждая группа соответствует одному драйверу, включенному в систему. Также существует возможность вынесения на план пиктограммы другого графического плана для оперативного переключения и мониторинга состояния.

В режиме настройки карт возможно также перемещение, удаление или настройка свойств любых имеющихся на плане пиктограмм (с помощью контекстных меню пиктограмм). Имеется возможность выделять и выполнять основные действия (перемещение, удаление, изменение свойств) сразу нескольких пиктограмм. Для выделения группы пиктограмм поочерёдно щелкайте по ним мышью, удерживая клавишу Shift.

Перемещение пиктограмм и полигонов можно запретить для текущего плана. Для этого нажмите на кнопку «Фиксация иконок» на панели над деревом планов.

Удалить пиктограмму можно, выделив её и выбрав из её контекстного меню пункт «Удалить».

4.7.3 Рисование многоугольников

Каждое устройство в АПК «Бастион» может быть представлено на плане не только пиктограммой, но и многоугольником произвольной формы (см. Рис. 17).

Для того, чтобы нарисовать многоугольник проделайте следующие операции:

Перейдите в режим рисования многоугольников. Для этого щелкните правой кнопкой на свободном месте на плане и выберите пункт «Полигон».

Левой кнопкой мыши щелкайте в углах требуемого многоугольника.

Для завершения рисования щелкните правой кнопкой мыши. Две крайние вершины будут соединены между собой. На экране появится окно с деревом устройств. Выберите устройство, которое будет обозначать многоугольник.

Для выхода из режима рисования многоугольников из контекстного меню плана выберите пункт «Выбор».

4.7.4 Настройка свойств пиктограмм

С каждой пиктограммой или многоугольником связано окно свойств, вызывающееся из её контекстного меню в режиме настройки планов. Это окно состоит из двух страниц (Рис. 20 и Рис. 21).

На первой странице (Рис. 20) редактируются общие для всех типов устройств (кроме пиктограмм графических планов) свойства:

Направление пиктограммы. Кнопки со стрелками позволяют выбрать одно из направлений отображения пиктограммы. Для некоторых устройств доступна только часть направлений.

Размер. С помощью кнопок в группе размер можно установить требуемый масштаб пиктограммы.

Уровень доступа к устройству. Определяет минимальный уровень доступа, которым должен обладать оператор для того, чтобы иметь возможность управлять данным устройством. Следует иметь в виду, что уровень доступа назначается на устройство, а не на отдельную пиктограмму, поэтому, если устройство отображается в нескольких местах, уровень доступа можно установить только для одной из пиктограмм.

Устройство. Позволяет выбрать устройство, отображаемое пиктограммой.

Не показывать пиктограмму в нормальном состоянии. Позволяет установить режим, при котором пиктограмма будет отображаться только при возникновении тревоги или неисправности (обычно этот режим используется для охранных шлейфов).

Вид. Если устройство может отображаться при помощи нескольких разных пиктограмм, то из выпадающего списка «Вид» можно выбрать вид пиктограммы.

Для многоугольников в этом же окне можно задать *степень прозрачности* в процентах (0 – непрозрачный, 100 – полностью прозрачный).

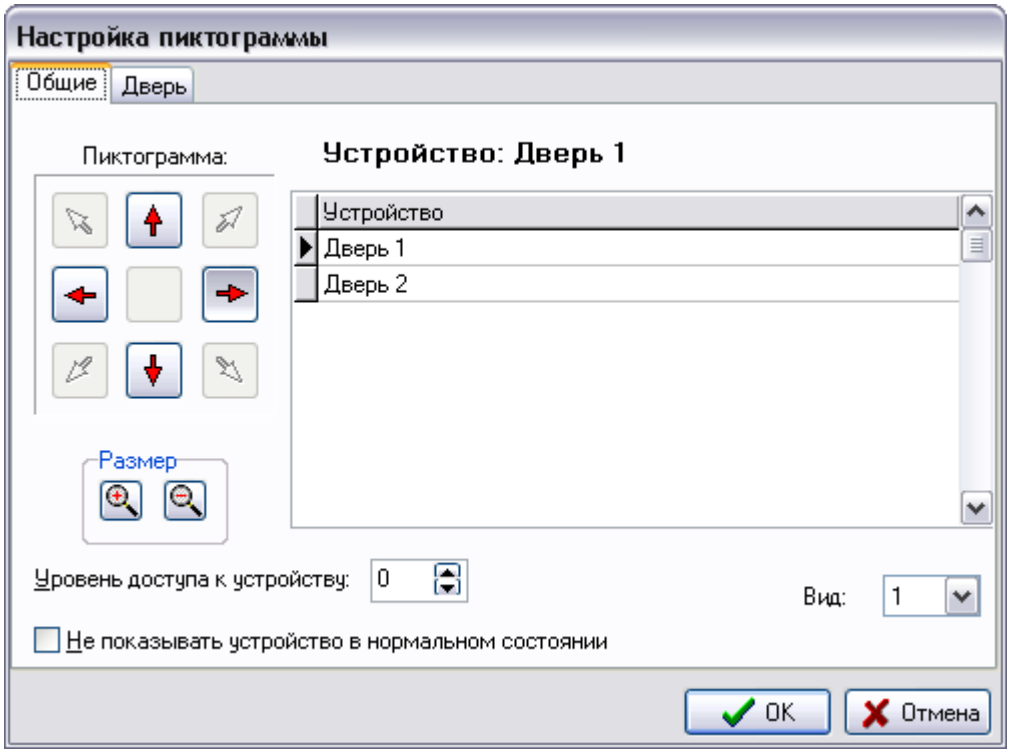


Рис. 20. Страница общих свойств пиктограммы

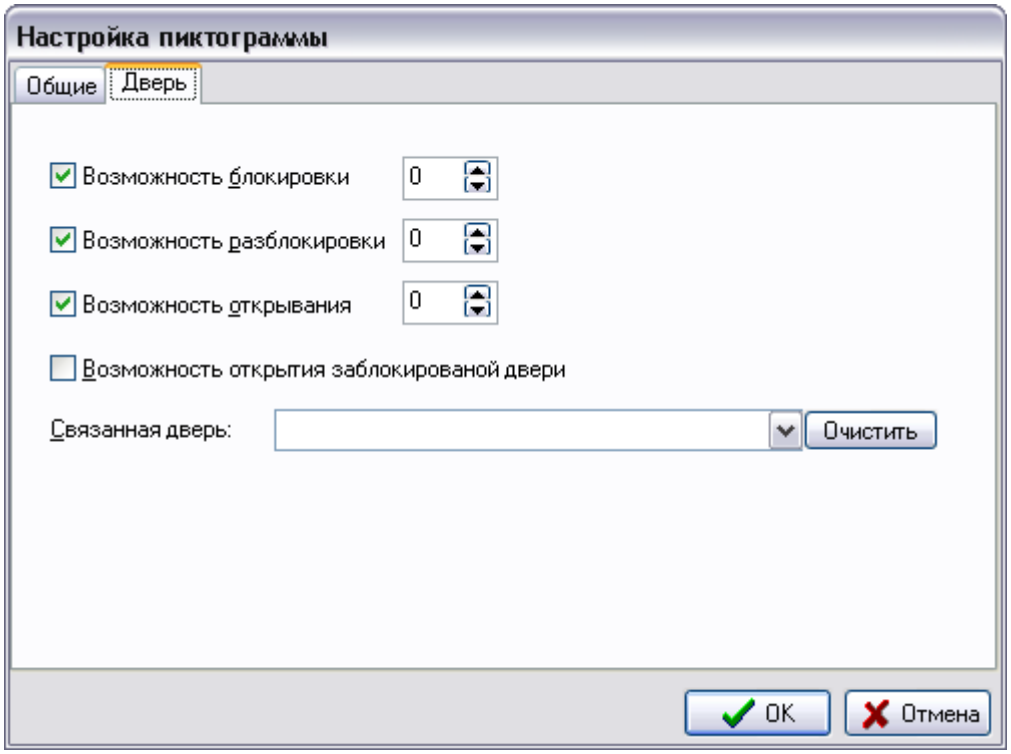


Рис. 21. Страница свойств типа устройства для пиктограммы

Вторая страница (Рис. 21) предназначена для изменения свойств, специфичных для конкретного типа устройств. Рассмотрим эти свойства подробнее:

Свойства охранного/пожарного шлейфа

Возможность постановки на охрану по разделам. Позволяет установить, можно ли выполнять постановку/снятие с охраны раздела из контекстного меню данной пиктограммы.

Возможность постановки на охрану по зонам. Позволяет установить, можно ли выполнять постановку/снятие с охраны зоны из контекстного меню данной пиктограммы.

Сброс тревоги (дымовых извещателей). Позволяет установить, можно ли выполнять сброс тревоги из контекстного меню данной пиктограммы.

По умолчанию для всех вновь добавляемых пиктограмм шлейфов перечисленные опции выключены.

Свойства выхода

Возможность включения, возможность выключения, возможность подачи импульса. Данные параметры определяют возможность и необходимый уровень полномочий оператора для соответствующих операций со выходом.

Свойства тревожной кнопки

Возможность сброса тревоги по зонам, возможность сброса тревоги по разделам. Данные параметры определяют возможность и необходимый уровень полномочий оператора для соответствующих операций с тревожной кнопкой.

Свойства двери

Возможность блокировки, возможность разблокировки, возможность открывания. Данные параметры определяют возможность и необходимый уровень полномочий оператора для соответствующих операций с дверью.

Возможность открытия заблокированной двери. Данный параметр связан с особенностями работы оборудования. Если заблокированную дверь можно открыть из программы, включите данный флаг.

Связанная дверь. Служит для создания шлюзов. Для обычных дверей оставьте это поле пустым.

Свойства турникета

Возможность полной блокировки, возможность блокировки входа, возможность блокировки выхода, возможность полной разблокировки, возможность разблокировки входа, возможность разблокировки выхода, возможность открывания на вход, возможность открывания на выход. Данные параметры определяют возможность и необходимый уровень полномочий оператора для соответствующих операций с турникетом.

Свойства ворот

Возможность открывания, возможность закрывания, возможность остановки. Данные параметры определяют возможность и необходимый уровень полномочий оператора для соответствующих операций с воротами.

Автозакрытие. Позволяет включить режим автозакрывания ворот и определить время, в которое оператору будет выдано специальное сообщение о том, что ворота не закрыты.

Свойства телекамеры

Устройство отображения по умолчанию. Если телекамера подключена к нескольким телевизионным устройствам, данная настройка определяет, на какое устройство будет выведено изображение по щелчку левой кнопкой мыши на пиктограмме.

Монитор отображения по умолчанию. Определяет номер монитора или окна полиэкрана, в котором будет выведено изображение по левому щелчку мыши по пиктограмме.

Возможность режима увеличения. Определяет, имеется ли возможность управлять увеличением изображения с пиктограммы.

Вызвать предустановку. Если устройство, к которому подключена телекамера, имеет возможность создания предустановок, то можно указать номер предустановки, которая будет вызвана по левому щелчку мыши.

Возможность поворота. Определяет, имеется ли возможность управлять поворотным устройством телекамеры с пиктограммы.

4.7.5 Дополнительные параметры графической подсистемы

Если у Вас возникают проблемы с отображением графических планов, то следует изменить один из параметров графической подсистемы АПК «Бастион». Это можно сделать, выбрав

пункт меню «Конфигурация→Общие настройки→Графика» (см. Рис. 22), а также прямым редактированием файла settings.ini, который находится в каталоге <Bastion>\Maps.

В случае если при большом количестве планов и пиктограмм программа занимает более 50% ресурсов процессора, можно попробовать изменить цветовой режим в Windows – с 24-битного на 16-битный.

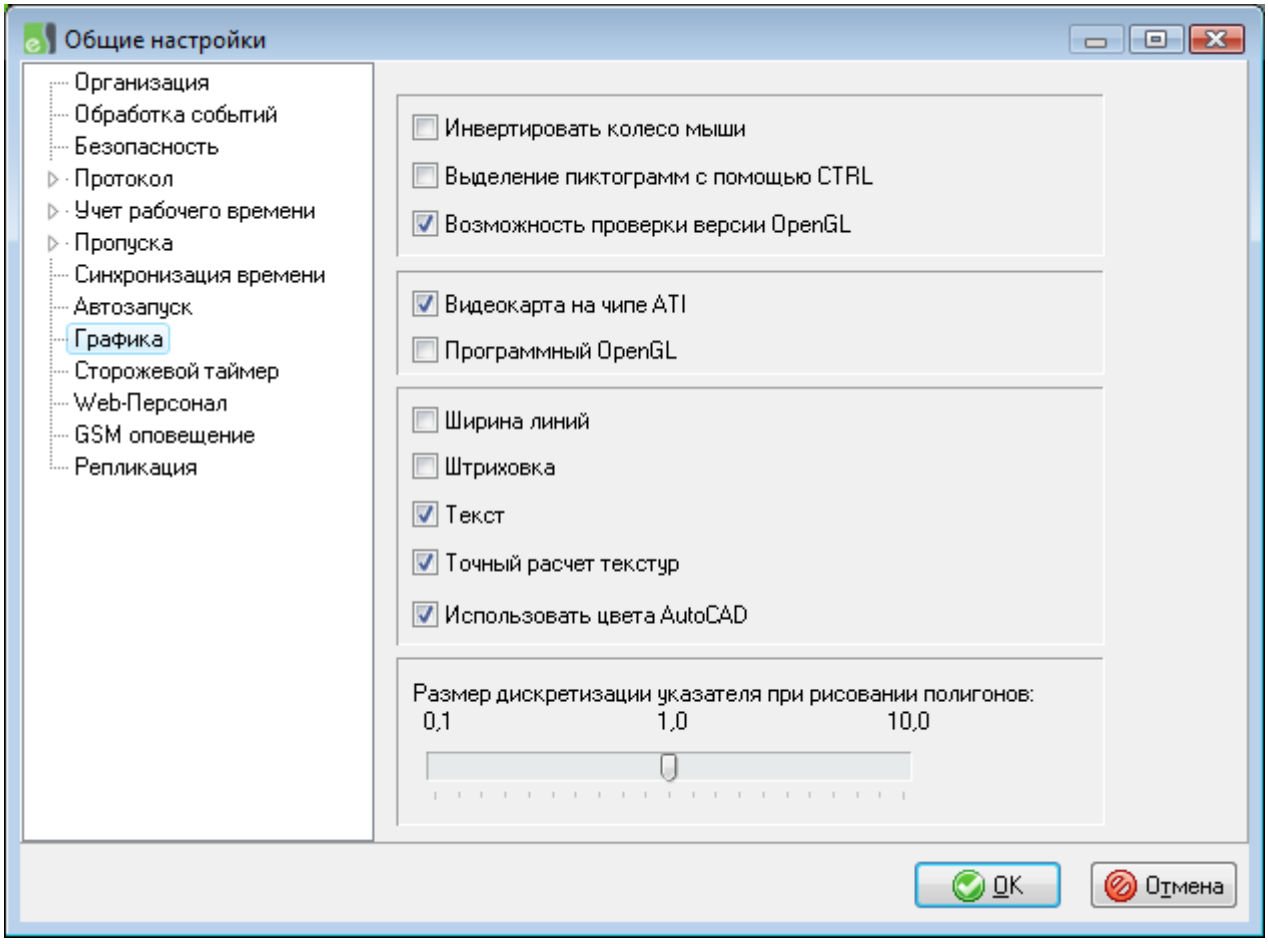


Рис. 22. Окно настройки параметров графической подсистемы

Листинг файла settings.ini (приведены установки по умолчанию):

[AddDevTree] DViewLeft=792 DViewTop=258 DViewWidth=209 DViewHeight=365 **[TreePosition]** DTreePos=219	Положение окон на экране (не редактировать).
[MAIN]	Основные настройки (возможные варианты: ON/OFF).

WHEELINVERT=OFF	Инвертирование направления колеса прокрутки мыши.
CTRLSELECT=OFF	Множественный выбор пиктограмм будет осуществляться с помощью кнопки CTRL, а не SHIFT.
CHECKOPENGL=OFF	Возможность проверки версии OpenGL (для этого надо сделать активным дерево планов и нажать CTRL+ SHIFT+F8).
ATI=OFF	Устранение проблем с видеокартами ATI (отключается прорисовка сплайнов).
SOFTGL=OFF	Использование библиотек программной эмуляции OpenGL. Следует установить в ON, если драйверы видеокарты не поддерживают OpenGL. Следует иметь ввиду, что отображение текста в DXF-планах будет отключено при использовании программной эмуляции.
[DXF]	Режимы DXF-планов.
LINEWIDTH=OFF	Линии в DXF будут иметь ширину и при увеличении будут шире.
HATCH=OFF	Прорисовка заливки в DXF (не рекомендуется).
TEXT=ON	Если OFF, то отключается прорисовка текста.
USECOLOR=ON	Использовать цвета AutoCAD в планах DXF.
[TEXTURE]	Режимы растровых планов.
LINEAR=ON	Точный расчет текстур, обеспечивает улучшенную передачу изображения. На слабых компьютерах рекомендуется отключать (OFF).
EARLYENABLE=OFF	

4.8 Настройка параметров обработки событий

4.8.1 Время актуальности событий

Система позволяет указать длительность времени, в течение которого событие будет считаться актуальным (Конфигурация – Общие настройки – обработка событий). Время актуальности события позволяет указать, что для событий, пришедших с опозданием на заданное время (в минутах), не требуется:

- выводить расширенное сообщение;
- выполнять реакции на событие;
- производить фотоидентификацию.

Если указать 0 – то время актуальности событий ограничиваться не будет.

Дополнительно, можно запретить выводить устаревшие события совсем, если снять флаг «Выводить устаревшие события».

4.8.2 Параметры записи протокола

Для настройки параметров записи протокола следует выбрать пункт меню «Конфигурация→Основные настройки» и открыть страницу «Протокол→Режим записи» (Рис. 23).

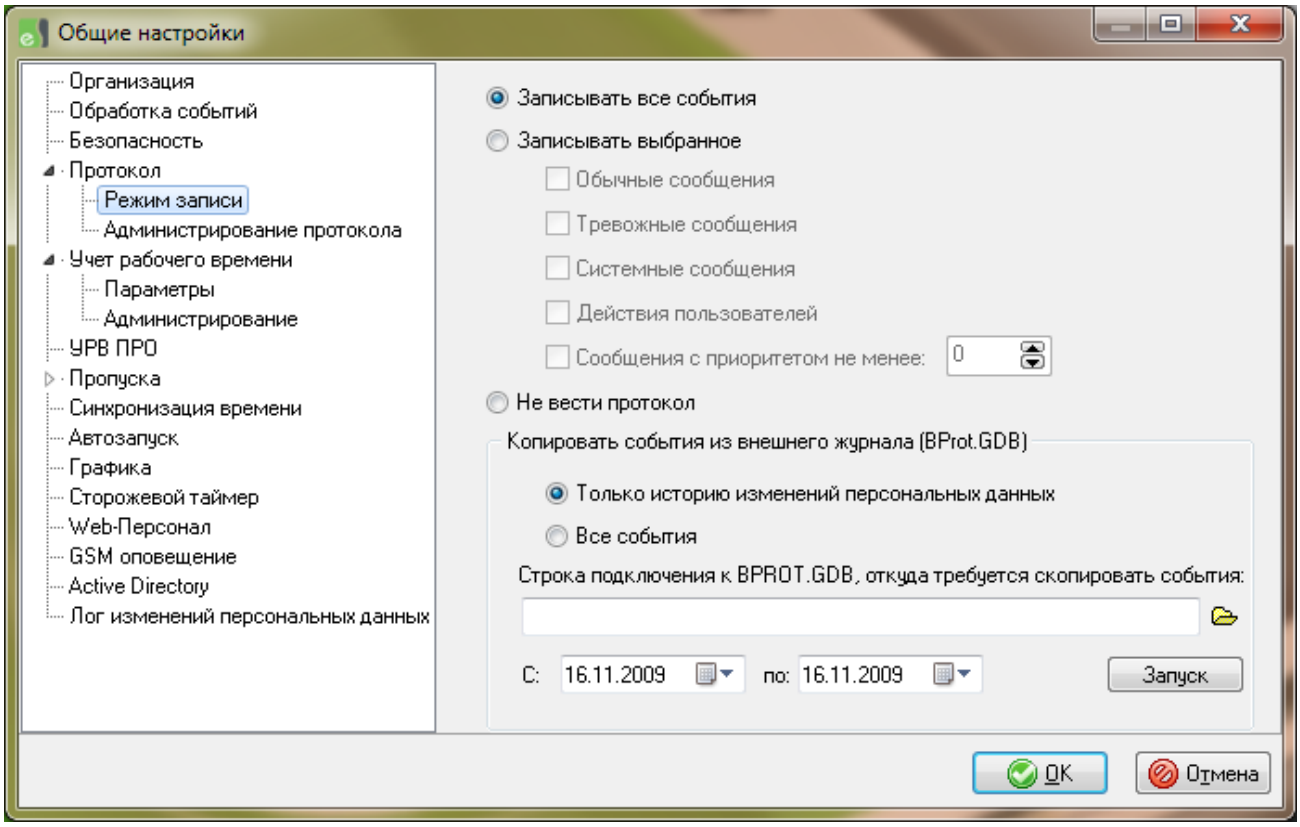


Рис. 23. Страница свойств режима записи протокола

На этой странице можно указать, какие события будут записываться в базу данных протокола. Варианты записи основного протокола:

- записывать все события (по умолчанию);
- записывать выбранное;
- не вести протокол событий.

Если выбрана опция «записывать выбранное», то активизируется список опций, определяющих критерий записи:

Обычные сообщения. При включенной опции обычные (не тревожные) сообщения, поступающие от оборудования комплекса, будут записываться в протокол.

Тревожные сообщения. При включенной опции тревожные сообщения будут записываться в протокол. Выключать данную опцию не рекомендуется.

Системные сообщения. Эта группа сообщений включает в себя сообщения, генерируемые самой программой (например, запуск системы).

Действия пользователей. При включенной опции действия пользователей, такие как подтверждения событий, редактирование базы данных и т.д. будут записываться в протокол.

Сообщения с приоритетом не менее указанного. Если флаг включен, то дополнительно будет проверяться приоритет сообщения. Запись будет произведена только в том случае, если приоритет сообщения больше либо равен указанному и сообщение входит в одну из перечисленных выше групп.

Также, имеется возможность выполнить копирование событий в текущую протокольную базу данных (BProt.GDB) из другой протокольной БД (из внешнего журнала). Для этого:

1. Укажите строку подключения к внешнему журналу (путь к BProt.GDB. Если файл находится на другом сервере – укажите строку в формате <Имя сервера>:<Путь>), откуда необходимо скопировать данные.
2. Выберите диапазон дат, за которые следует скопировать события.
3. Укажите, следует копировать все события или только события изменений персональных данных.
4. Нажмите кнопку «Запуск» и следуйте инструкциям программы.

4.8.3 Редактирование событий

Текст и приоритет событий, заданные по умолчанию, можно произвольно изменять. При этом имеется возможность указать отдельно для каждого устройства свои параметры обработки событий.

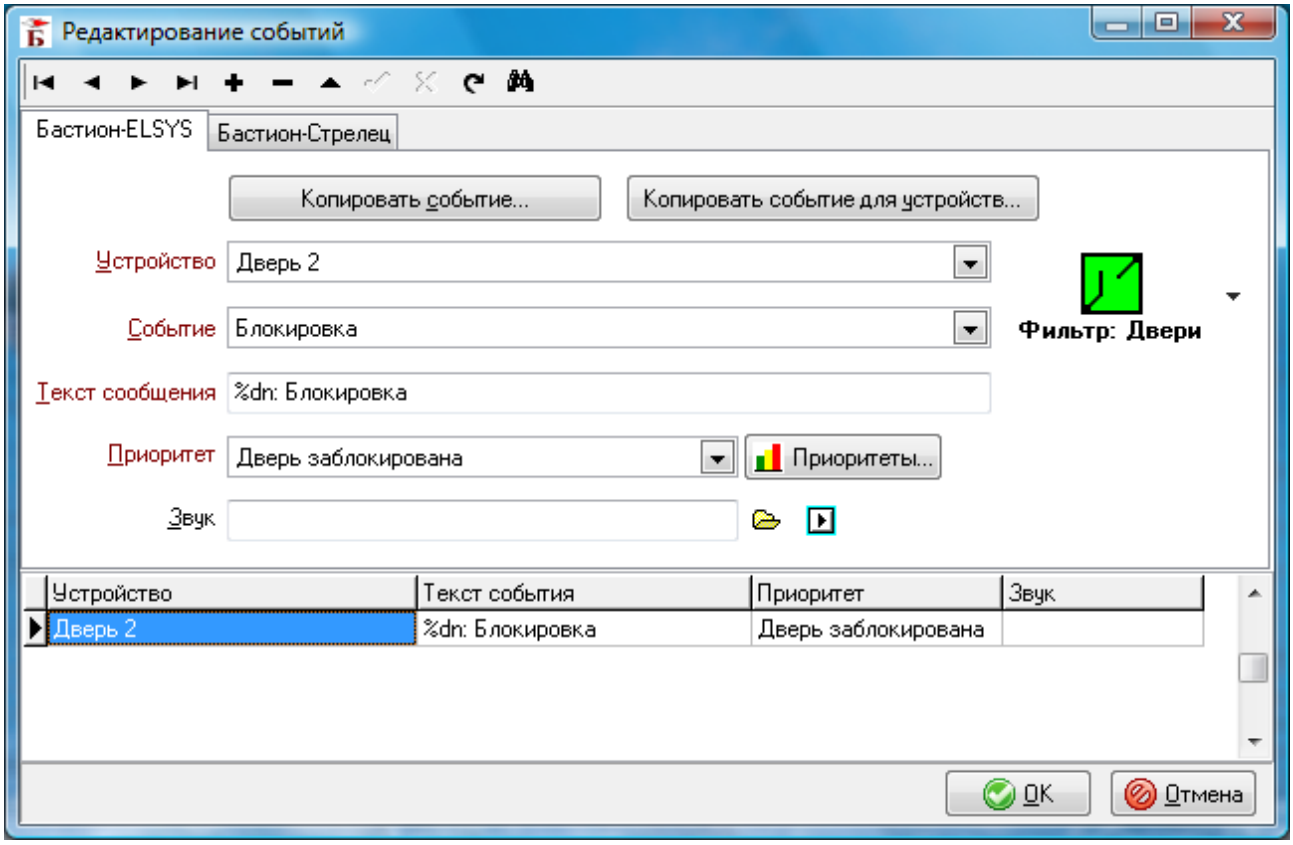


Рис. 24. Окно редактирования событий

Для выполнения этих действий следует выбрать пункт меню «Конфигурация→События», после чего появится окно «Редактирование событий», изображённое на Рис. 24. Закладки, расположенные в верхней части окна, обеспечивают выбор драйвера устройства, для которого необходимо переопределить событие.

Назначение отдельных параметров событий:

Устройство – позволяет выбрать устройство-источник события. Для упрощения поиска нужного устройства служит кнопка с выпадающим списком *«Фильтр»*, позволяющая отфильтровать список устройств по их типу.

Событие - служит для выбора события, параметры которого необходимо переопределить.

Текст события - служит для ввода нового текстового сообщения для выбранного события, которое будет отображаться в одной из областей сообщений основного окна ПО. Текст события может содержать *символы форматирования*, обеспечивающие вставку переменной информации. Такие символы могут находиться в любом месте сообщения и обеспечивают вывод следующих данных:

%dn Название устройства, вызвавшего событие. Может использоваться с любым типом драйвера.

%cn Номер карты доступа. Позволяет включить в сообщение номер предъявленной карты доступа для сообщений, формируемых устройствами системы контроля доступа. Если событие не содержит кода карты, символ будет выведен без

изменений.

%nm Фамилия владельца карты доступа. Символ используется в тех же случаях, что и предыдущий.

%n1 Имя владельца карты доступа.

%n2 Отчество владельца карты доступа.

%pn PIN-код, набранный владельцем карты доступа.

%st Site-код (серия) предъявленной карты доступа.

%us Имя текущего пользователя программного обеспечения.

%nb Распознанный номер. Используется для систем транспортного учета («Бастион-Номер», «Бастион-Состав»).

Указанные коды могут использоваться в любой комбинации.

Некоторые драйверы (например, «Бастион-Стрелец») позволяют использовать и другие символы форматирования. Об их использовании см. инструкцию на соответствующий драйвер.

Приоритет – позволяет назначить один из заранее созданных приоритетов текущему событию.

Звук – позволяет выбрать файл звукового оповещения о событии. Это поле не является обязательным, поэтому его можно оставить пустым. «Бастион» использует звуковые файлы формата Wave audio (.wav), которые по умолчанию должны располагаться в каталоге «<Bastion>\SOUND\». Имя файла можно задать вручную (непосредственный ввод текста в поле) или выбрать из имеющихся в стандартном окне открытия файла. Выбранный звуковой файл можно прослушать с помощью кнопок «  ».

Существует возможность выполнить копирование событий. Для этого служат кнопки "Копировать событие для устройств..." и "Копировать событие...". В первом случае, пользователь получает возможность установить для нескольких устройств один и тот же вид обработки какого-либо события сразу. Во втором – установить для текущего устройства одинаковые параметры обработки нескольких различных событий.

4.8.4 Настройка приоритетов событий

Для редактирования приоритетов событий выберите пункт меню «Конфигурация – Приоритеты событий…». То же самое окно можно вывести нажатием кнопки «Приоритет» в окне «Редактирование событий» (Рис. 25).

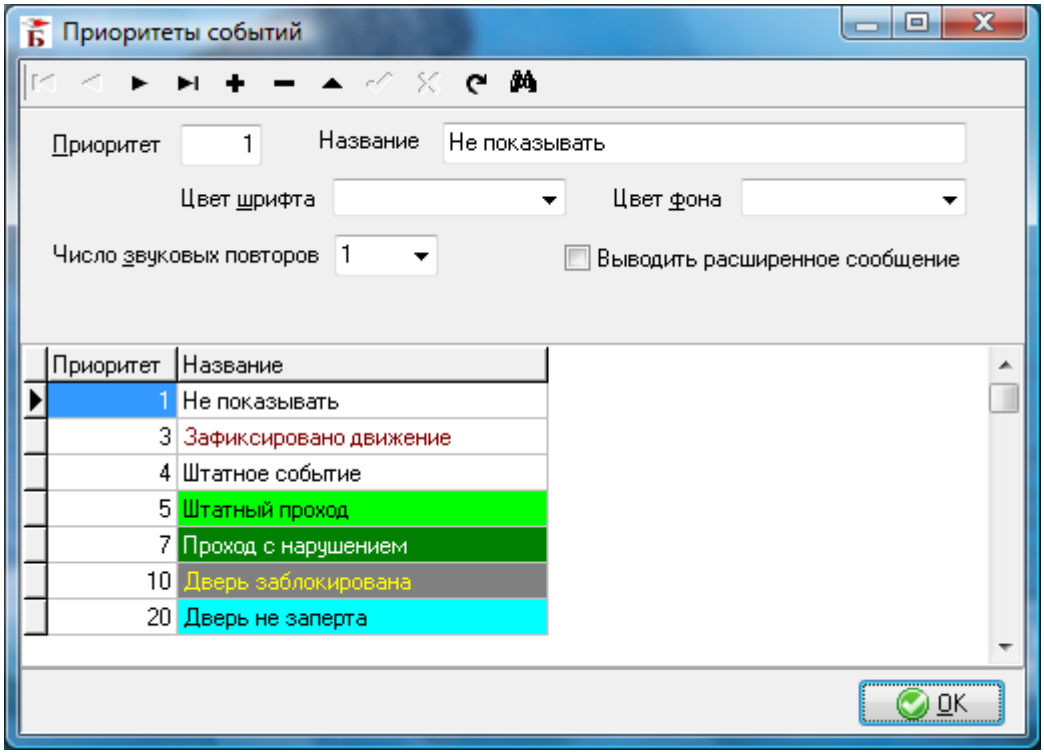


Рис. 25. Окно настройки приоритетов событий

Под *приоритетом события* уровень важности события, определяющий способ его вывода и обработки. Например, можно выводить только события с приоритетом больше заданного, выводить окно фотоидентификации для событий с приоритетом не менее заданного и т.д.

Каждая запись в таблице приоритетов событий содержит следующие поля:

Приоритет – служит для ввода числового значения уровня приоритета события. Число должно находится в диапазоне от 0 до 99. Самый низкий приоритет имеет значение 0, самый высокий – 99.

Название – позволяет ввести название приоритета. Длина названия не должна превышать 40 символов, включая пробелы, например «Не показывать».

Цвет шрифта – обеспечивает выбор цвета шрифта, которым в окно тревожных или штатных сообщений будет выведено сообщение о событии с данным приоритетом.

Цвет фона – служит для выбора цвета фона, на котором в окно тревожных или штатных сообщений будет выведено сообщение о событии с данным приоритетом.

Число звуковых повторов – служит для указания количества повторов голосового сообщения при возникновении события с данным приоритетом.

Выводить расширенное сообщение – установка этого флага обеспечивает вывод окна расширенного сообщения для событий, требующих повышенного внимания оператора системы. **Этот флаг действует, если настройки профиля пользователя разрешают вывод данного сообщения как расширенного.**

4.8.5 Установка шрифтов для отображения событий

Система позволяет задать вид и размер шрифтов, используемых для отображения обычных и тревожных сообщений. Для этого необходимо выбрать пункт меню «Конфигурация→Шрифты». Шрифты задаются на каждом рабочем месте отдельно и не привязываются к профилю пользователя. Цвет шрифта задаётся приоритетом события и в данном окне не регулируется.

4.8.6 Маршрутизация сообщений

Маршрутизация сообщений позволяет установить, каким пользователям, в зависимости от их профиля, будут передаваться сообщения от определенных устройств. Перед настройкой маршрутизации необходимо определить профили пользователей (см. П. 4.6). Для включения режима маршрутизации следует установить флаг *«Разрешить маршрутизацию сообщений»* в окне на Рис. 26. По умолчанию маршрутизация выключена, то есть все пользователи получают все сообщения, с учётом фильтров в профиле пользователя. Для настройки маршрутизации сообщений необходимо выбрать пункт меню «Конфигурация→Маршрутизация сообщений».

В появившемся окне (см. Рис. 26) необходимо выбрать профиль пользователя и отметить те устройства (поставить знак «✓» напротив названия устройства), наблюдение за которыми будут осуществлять пользователи с данным профилем.

> ***Внимание!*** *Если новые устройства были добавлены после включения маршрутизации сообщений, то, чтобы от них начали поступать сообщения, необходимо включить эти устройства в окне настройки маршрутизации для каждого пользовательского профиля, где это требуется.*

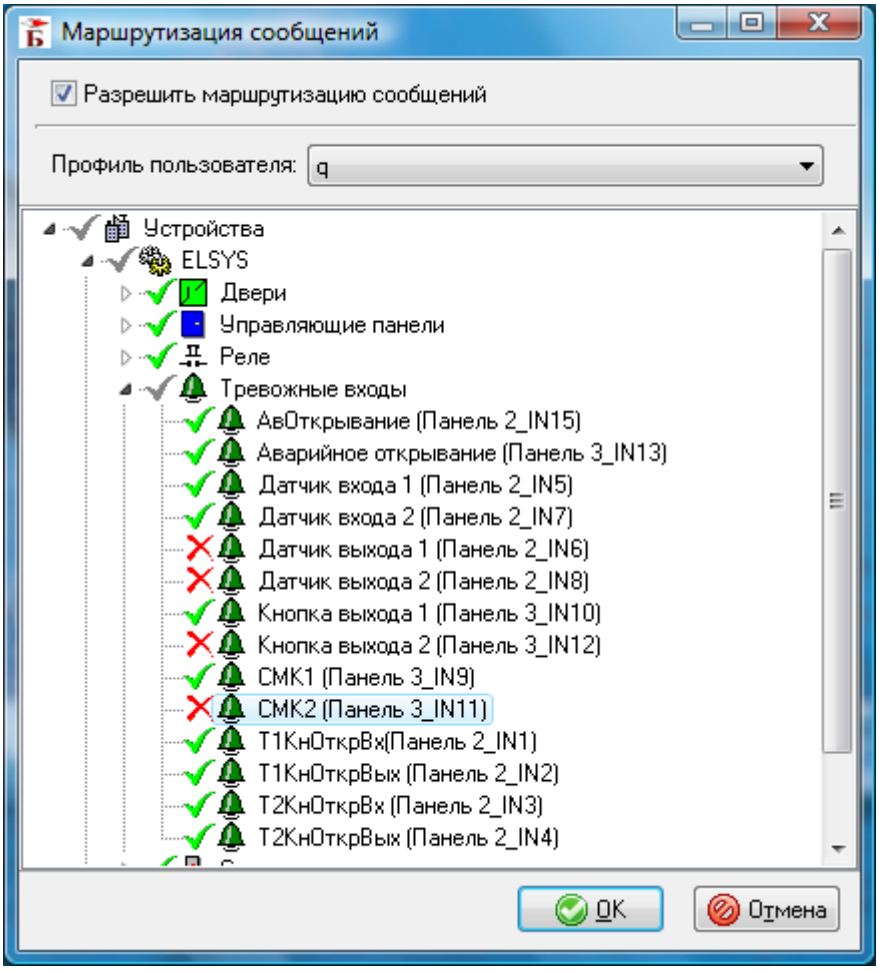


Рис. 26. Окно настройки маршрутизации сообщений.

4.9 Настройка сценариев

Сценарий – это последовательность действий, которая может выполняться автоматически по приходу какого-либо события (см. настройку реакций на события), либо выполняться по команде оператора, в том числе в ответ на событие из окна расширенных сообщений, с выбором из возможных вариантов (Рис. 30).

Для создания и редактирования сценариев выберите пункт меню «Конфигурация→Сценарии». При этом будет выведено окно следующего вида:

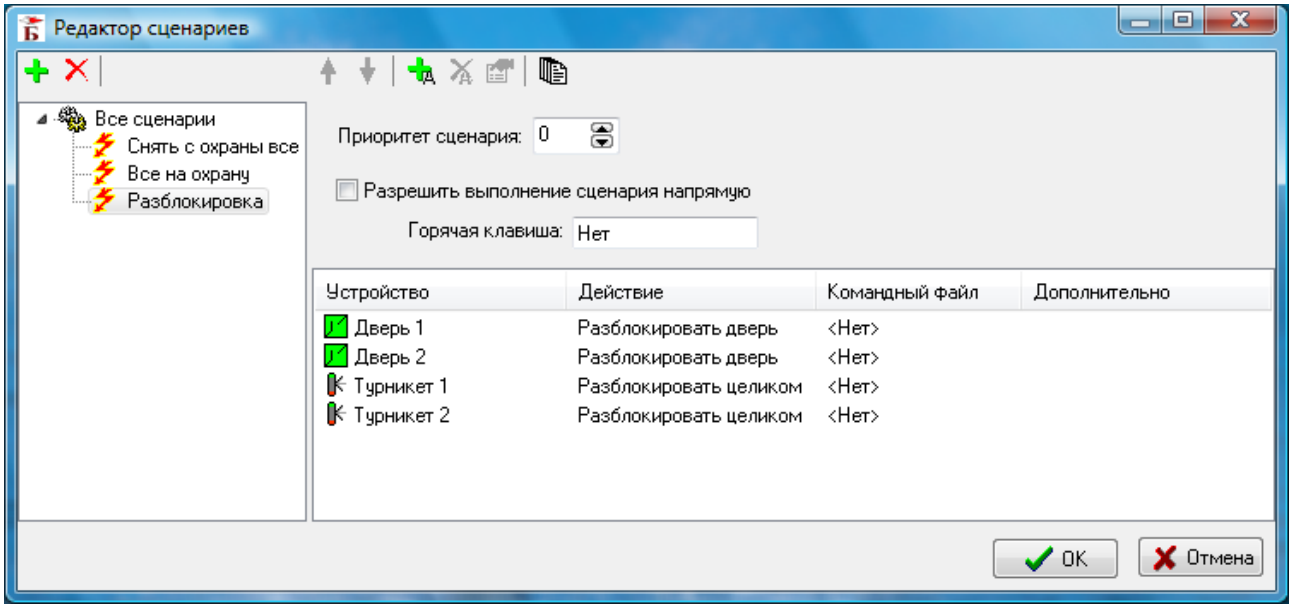


Рис. 27. Окно редактирования сценариев

Для *добавления нового сценария* нажмите кнопку "+" в левом верхнем углу окна, либо выберите пункт «Создать сценарий» в контекстном меню списка сценариев. Укажите имя сценария и его параметры:

Приоритет сценария. Используется для определения, имеет ли право оператор системы выполнять данный сценарий. Параметр имеет смысл, только если установлен следующий флаг.

Разрешить выполнение сценария напрямую. Если данный флаг установлен, то сценарий появится в списке доступных для выполнения сценариев (если уровень полномочий оператора >= приоритету сценария).

Заново созданный сценарий не содержит действий. Для *добавления действия* нажмите кнопку "+" в середине панели инструментов. При этом появится окно редактирования элементов сценария (Рис. 28).

Все действия сценария выполняются в том порядке, в котором они присутствуют в списке действий.

Для *удаления действия или сценария* выберите требуемый элемент и нажмите соответствующую кнопку «  » в панели инструментов, либо выберите нужный пункт из контекстного меню.

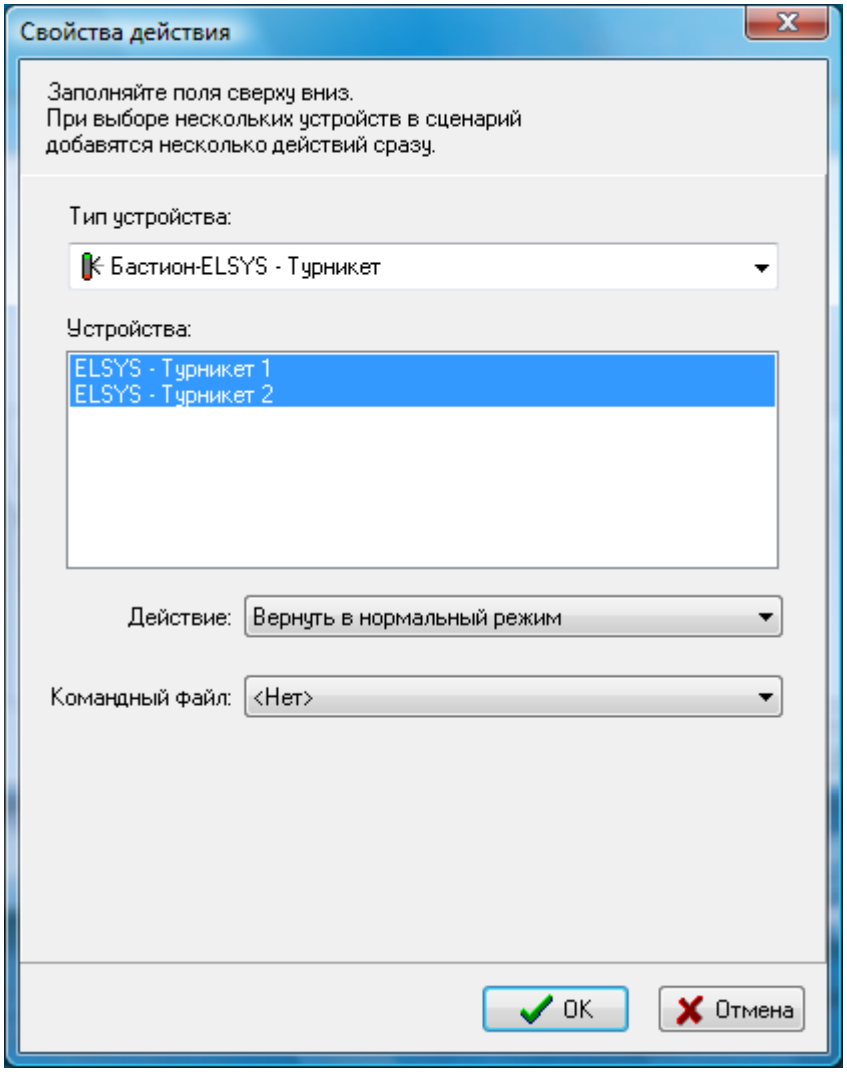


Рис. 28. Окно редактирования элементов сценария

Поддерживается ряд системных действий (устройство – «Система»), которые всегда выполняются на сервере АПК «Бастион», указанном в настройках рабочих станций:

1. *Запустить файл.* В командной строке указывается имя файла (без пути, если файл находится в том же каталоге, что и bastion.exe, с полным путём в остальных случаях) и параметры для его запуска. В командной строке могут быть использованы следующие спецификаторы, заменяемые при выполнении реакции на события на соответствующие значения:
    a. Код события (%evc). Подставляется поле БД MSGTYPES.MESSAGECODE.
    b. Код источника события (устройства) (%dev). Подставляется поле БД SUBDEVID.SUBDEVICENO.
    c. Название устройства-источника события (%dn). Подставляется поле БД SUBDEVID.SUBDEVICENAME.
    d. Тип устройства-источника события (Integer) (%dtp). Подставляется поле БД SUBDEVID.SUBDEVICETYPE.

e. Код драйвера устройства-источника события (%drv). Подставляется поле БД DEVICES.DRIVERNO.

f. Приоритет события (%pr). Подставляется поле БД MESSAGES.PRIORITY или MSGTYPS.PRIORITY, в зависимости от того, переопределено событие пользователем или нет.

g. Дата/время события (%dtm).

h. Текст сообщения (%ms). Подставляется текст сообщения, как он выводится на экран, с подставленными значениями параметров. Например: «Штатный вход Иванов Иван Иванович, карта 5555 65».

То есть, можно например, в сценарии запускать файл таким образом:

Test.exe dev=%dev evc=%evc dn="%dn" ms="%ms"

2. Вернуть предъявленную карту (см. п. 4.17).
3. Отправить SMS. Отправляется SMS с полным текстом сообщения или с заданным текстом. SMS отправляется через подключенный на сервере GSM-модем.

Действие может содержать не только прямую команду для устройства, но и *командный файл*.

Командный файл представляет собой последовательность команд, записанных непосредственно в кодах, понимаемых оборудованием. Не все драйверы поддерживают выполнение командных файлов (поддержка есть только для драйверов в текстовым протоколом обмена с оборудованием). Например: Бастион-Elsys, Бастион-С2000 – не поддерживают эту функцию.

> ***Внимание!*** *Система не отслеживает состояние устройств, в которое они переходят после выполнения командных файлов. Поэтому состояние пиктограмм может отличаться от реального состояния устройств после выполнения командных файлов.*

Для добавления, просмотра и редактирования списка доступных командных файлов нажмите кнопку «  » в панели инструментов окна редактирования сценариев.

Командные файлы не сохраняются в базе данных, а должны находиться на локальном жестком диске того компьютера, к которому подключено оборудование (по умолчанию – в каталоге Bastion\Cmd). Командные файлы должны иметь расширение CMD. Подготавливать командные файлы можно в любом текстовом редакторе. Не следует включать полный путь к файлу при выборе командного файла.

4.10Настройка реакций на события

АПК «Бастион» предоставляет возможности организации взаимодействия между различными подсистемами через *аппарат реакций на события*. Это позволяет при

возникновении определенного события отправить одну или несколько команд управления другим подсистемам комплекса. Например, по предъявлению карты заданному считывателю можно вызвать на монитор телевизионной системы соответствующее изображение, по пожарной тревоге разблокировать двери, по срабатыванию извещателя включить видеозапись. В качестве реакции, также, может выступать команда для ядра системы (например, вернуть предъявленную карту доступа или отправить SMS-оповещение).

Реакция на событие реализуется при помощи сценариев. Комплекс позволяет назначить для одного и того же события несколько вариантов реакций (несколько сценариев). В таком случае, окончательное решение о виде реакции принимает оператор комплекса, а при его бездействии в течение определенного времени, выполняются реакции по умолчанию.

Для редактирования списка реакций выберите пункт меню «Конфигурация→Реакции на события» (Рис. 29).

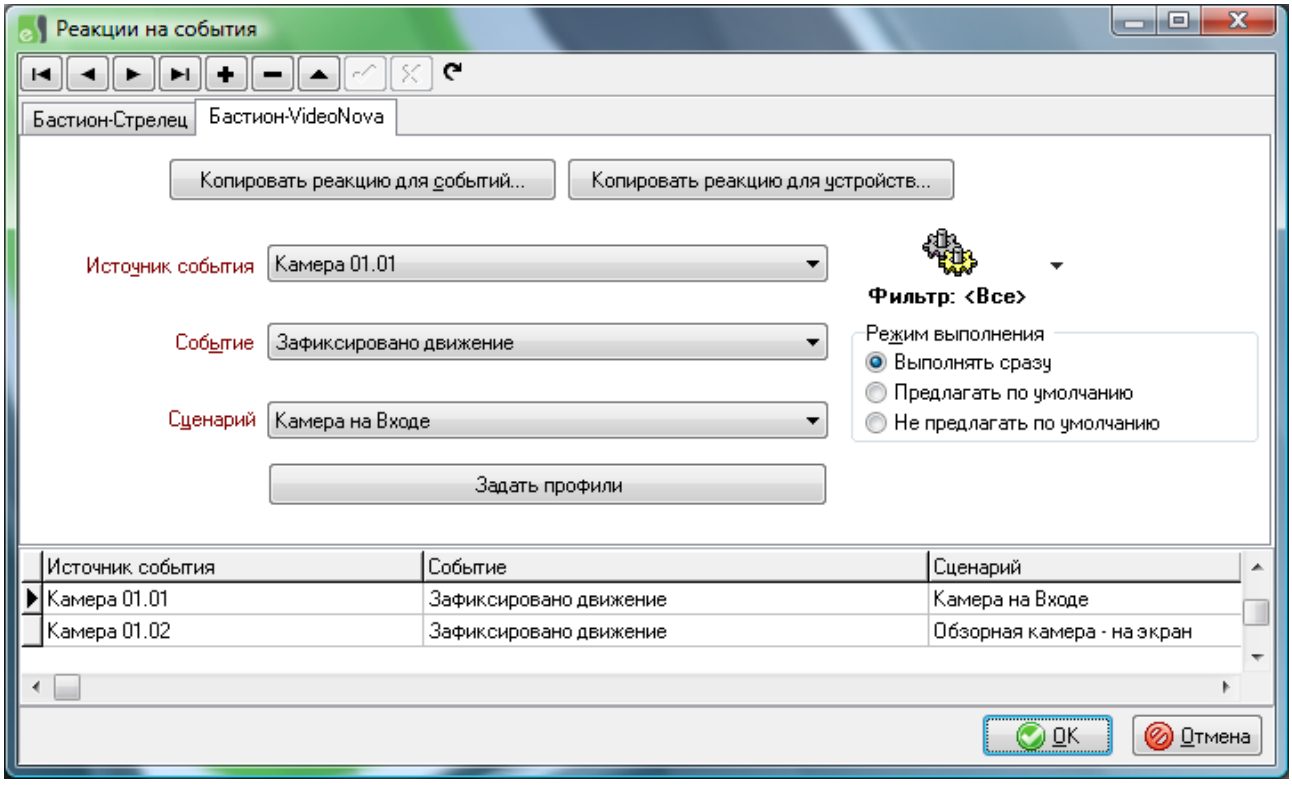


Рис. 29. Окно редактирования реакций на события

Все события в этом окне разделены закладками по драйверам.

Назначение параметров реакции на событие:

Источник события – обеспечивает выбор устройства, которое является источником события. Кнопка «*Фильтр*» позволяет оставить в списке источников события только устройства определенного типа (например, только двери).

Событие – служит для выбора события, при возникновении которого будет выполнена данная реакция.

Сценарий – позволяет выбрать сценарий, выполняемый при возникновении выбранного события.

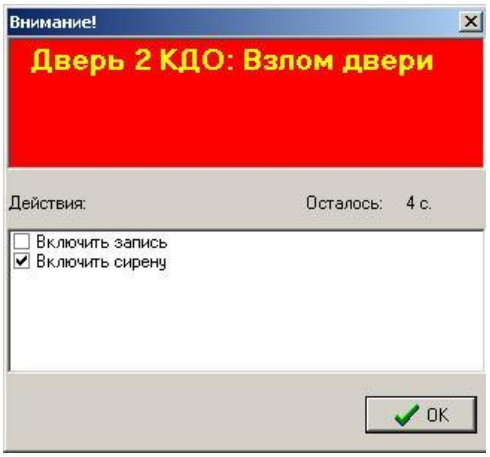


Рис. 30. Окно расширенного сообщения с вариантами реакций

Режим выполнения – реакции на события могут выполняться в разных режимах: сразу при поступлении события или после реакции оператора. При этом часть вариантов реакций может быть выделена сразу (Рис. 30, режим «Предлагать по умолчанию»). По истечении заданного времени (время автоматического закрытия окон расширенных сообщений) или нажатию кнопки ОК, выделенные реакции будут выполнены.

Система позволяет выполнять или не выполнять реакцию в зависимости от текущего пользователя. Эту функцию удобно использовать, например, для фильтрации выводимых на экран клиентских рабочих мест видеокамер, в зависимости от зоны ответственности операторов. Для установки такого фильтра служит кнопка *«Задать профили»*.

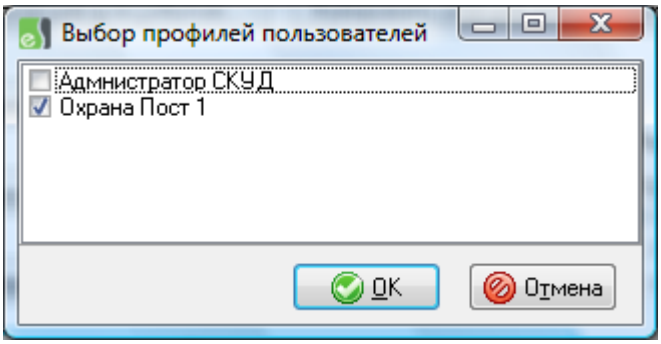


Рис. 31. Окно привязки реакции на событие к профилям пользователей

Окно создания привязки реакции к профилю представлено на Рис. 31.

По умолчанию реакция выполняется для всех профилей пользователей. Следует иметь ввиду, что реакция может выполняться либо на сервере оборудования (например – разблокировать дверь), либо на компьютере клиента (например – вывести камеру на экран). Привязка работает на том компьютере, где выполняется реакция.

Существует возможность выполнить копирование реакций на события. Для этого используются кнопки «Копировать реакцию для устройств...» и «Копировать реакцию для событий...». В первом случае пользователь получает возможность установить для нескольких устройств один и тот же вид реакции на какое-либо событие. Во втором –

установить для текущего устройства одинаковые параметры обработки нескольких различных событий.

При назначении реакции в некоторых случаях могут использоваться дополнительные параметры исходных событий. Например, если в исходном событии присутствует параметр «Дальность», то можно назначать разные сценарии на одно и то же событие для различных значений этого параметра (Рис. 32).

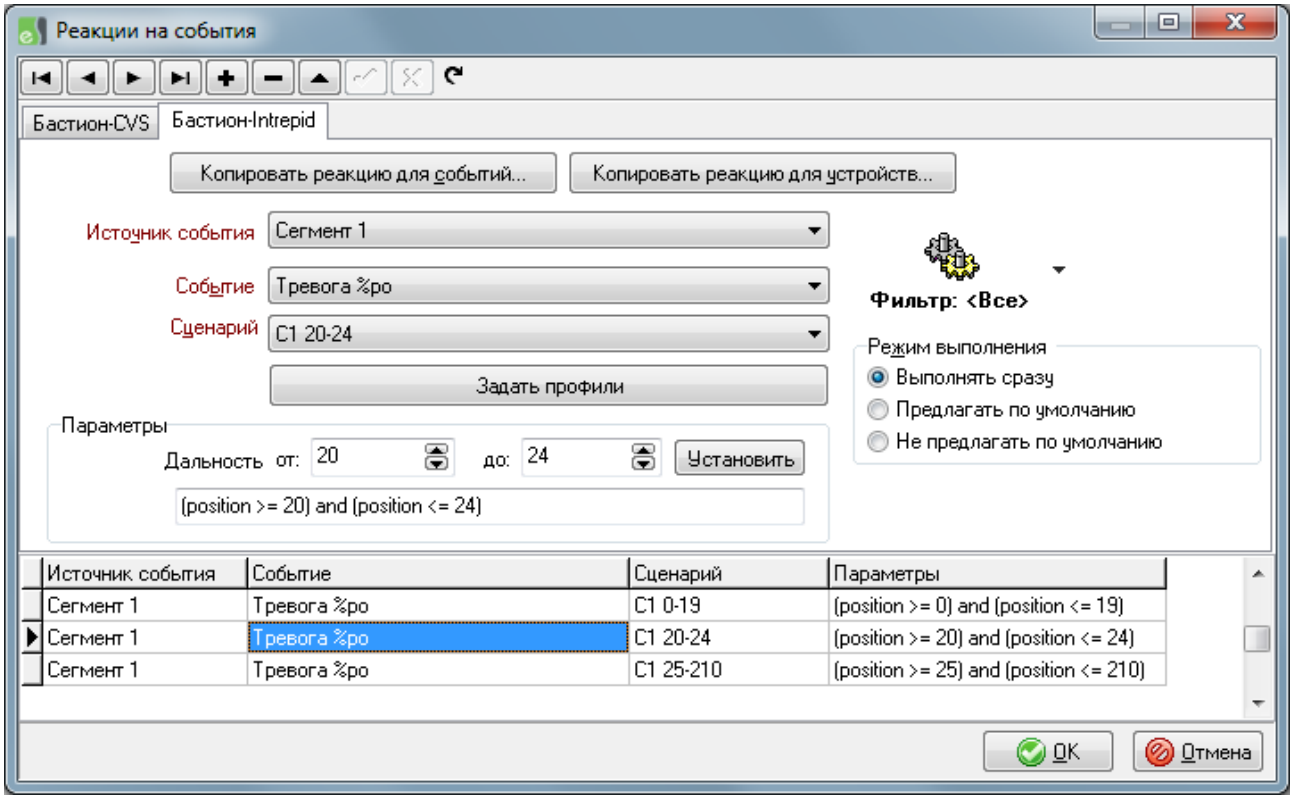


Рис. 32. Создание реакций на события с параметрами

Для установки ограничений по значениям параметра используется формула. Реакция будет выполнена только в том случае, если значение формулы с подставленным значением параметра будет больше 0 (TRUE).

Для упрощения ввода формулы предусмотрен редактор в группе «Параметры», где можно задать минимальное и максимальное значение параметра в полях «От:» и «до:». Для обновление формулы в соответствии с введенными значениями, следует нажать кнопку «Установить». Формулу также можно редактировать вручную, используя логические операции AND, OR, NOT, =, >, <, >=, <=, арифметические операции +, -, *, / и скобки (). Имена параметров и операции не зависят от регистра.

В настоящее время поддерживается только параметр «Дальность» для событий периметральных систем охраны. В формуле этот параметр обозначается как “position”.

4.11Настройка областей контроля

Под *областью контроля* в АПК «Бастион» понимается некоторое пространство, ограниченное одной или несколькими точками прохода (дверями, турникетами, воротами и т.д.). Такой областью может являться одно конкретное помещение, группа помещений,

здание целиком, территория завода и т.д. Области контроля могут быть вложенными. Например, область контроля «Все здание» может содержать несколько других областей – "Цех 1", "Бухгалтерия" и т.д. Тем не менее, следует учитывать, что вложенность носит чисто информативный характер и не используется программой.

Области контроля используются программным обеспечением в следующих случаях:

- Для обеспечения подсчета людей в области контроля.
- В качестве ограничивающей области в системе учета рабочего времени. При этом вход в область контроля считается приходом на работу, а выход из нее - уходом с работы.
- Для организации режима глобального контроля последовательности прохода (Global Antipassback).

Для настройки областей контроля выберите пункт меню «Конфигурация→Области контроля». При этом появится окно, представленное на Рис. 33.

По умолчанию в системе определены 2 области: «На территории» и «Вне территории». Эти области удалить нельзя. Область «На территории» всегда используется как «ограничитель территории предприятия», то есть по ней определяется вход и выход с объекта. Также, по умолчанию эта область используется для учета рабочего времени и подсчета людей.

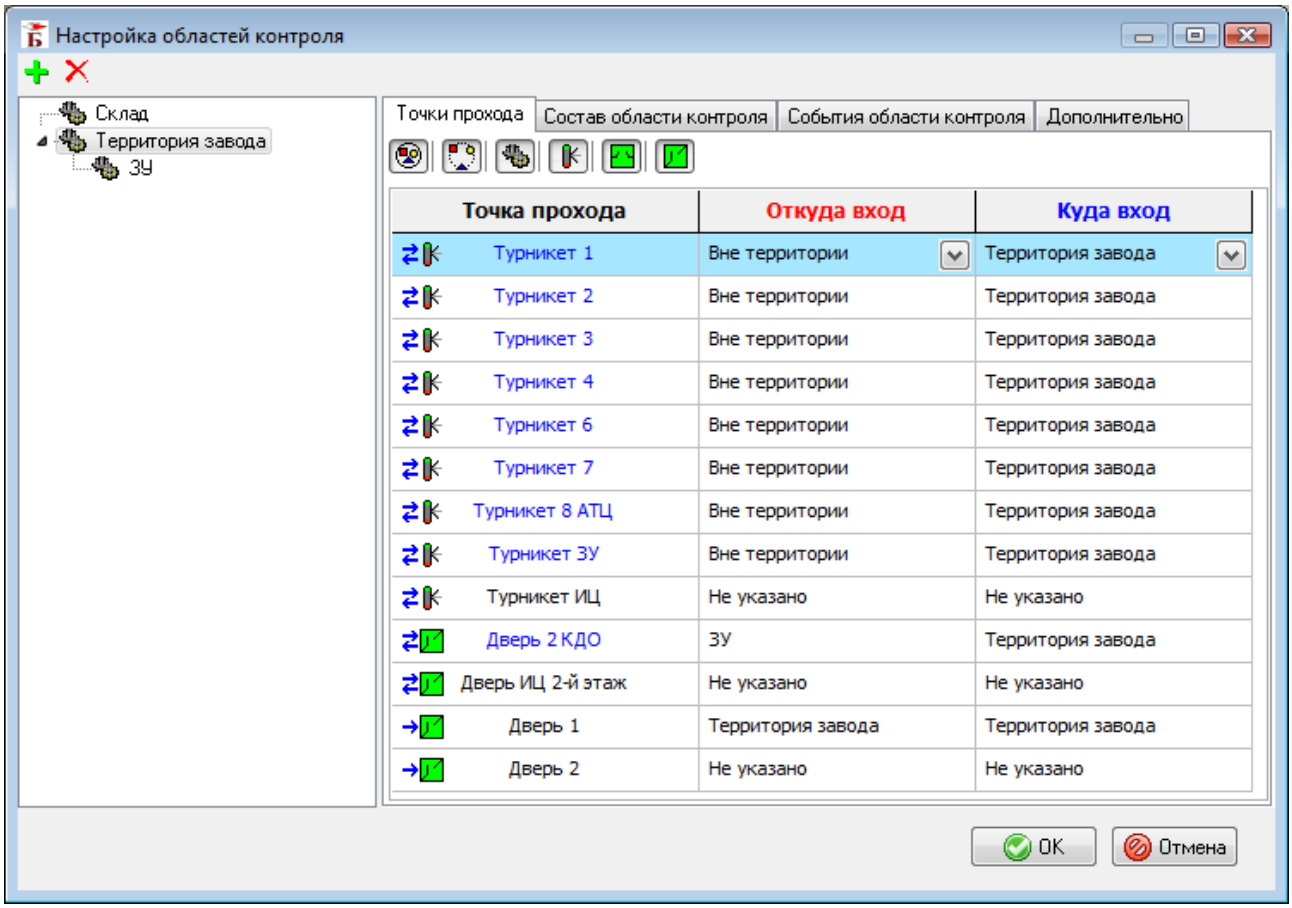


Рис. 33. Окно настройки областей контроля

Для *добавления области контроля* необходимо нажать кнопку «  » в панели инструментов или выбрать соответствующий пункт из контекстного меню в дереве областей контроля и ввести название области контроля.

После добавления областей контроля следует определить участие в них точек прохода. Для этого необходимо указать, откуда и куда ведет точка прохода. Например, на Рис. 33 «Турникет 2» ведет из области «Вне территории» в область «Территория завода».

> *Односторонние точки прохода также могут участвовать в областях контроля. Это имеет смысл, например, при использовании глобального антипассбэка – в этом случае, доступ по карточке не предоставляется в этой точке прохода, пока её владелец не зашел в область контроля, ограничивающую эту точку. При этом следует выбирать одну и ту же область в столбцах «Откуда вход» и «Куда вход». Например, на Рис. 33, односторонняя «Дверь 1» находится внутри области «Территория завода».*

Цветами шрифта отображается статус точки прохода в текущей области контроля (синий – входная точка, красный – выходная, черный – в текущей области не используется).

Также, можно отфильтровать список точек прохода с помощью кнопок в панели управления:

	Показывать точки прохода, используемые в областях контроля или в текущей области контроля (зависит от положения кнопки ).
	Показывать точки прохода, не используемые ни в одной области контроля.
	Все области контроля. Если нажата, то действие остальных кнопок относится ко всем областям контроля. Если нет – только к текущей области.
	Показывать турникеты.
	Показывать двери.
	Показывать ворота.

На странице «Состав области контроля» можно посмотреть конфигурацию выбранной области (см. Рис. 34).

Страница «События области контроля» (см. Рис. 35) предоставляет дополнительный контроль над событиями, которые будут использованы для фиксации входа и выхода из области контроля. Конфигурация событий по умолчанию для входной точки приведена на Рис. 35. Если точка прохода – выходная для области, то наоборот, входные события для точки прохода будут выходными для области контроля. Такой конфигурации достаточно для большинства случаев.

> ***Внимание!*** *Не изменяйте конфигурацию событий областей контроля, если не уверены в своих действиях!*

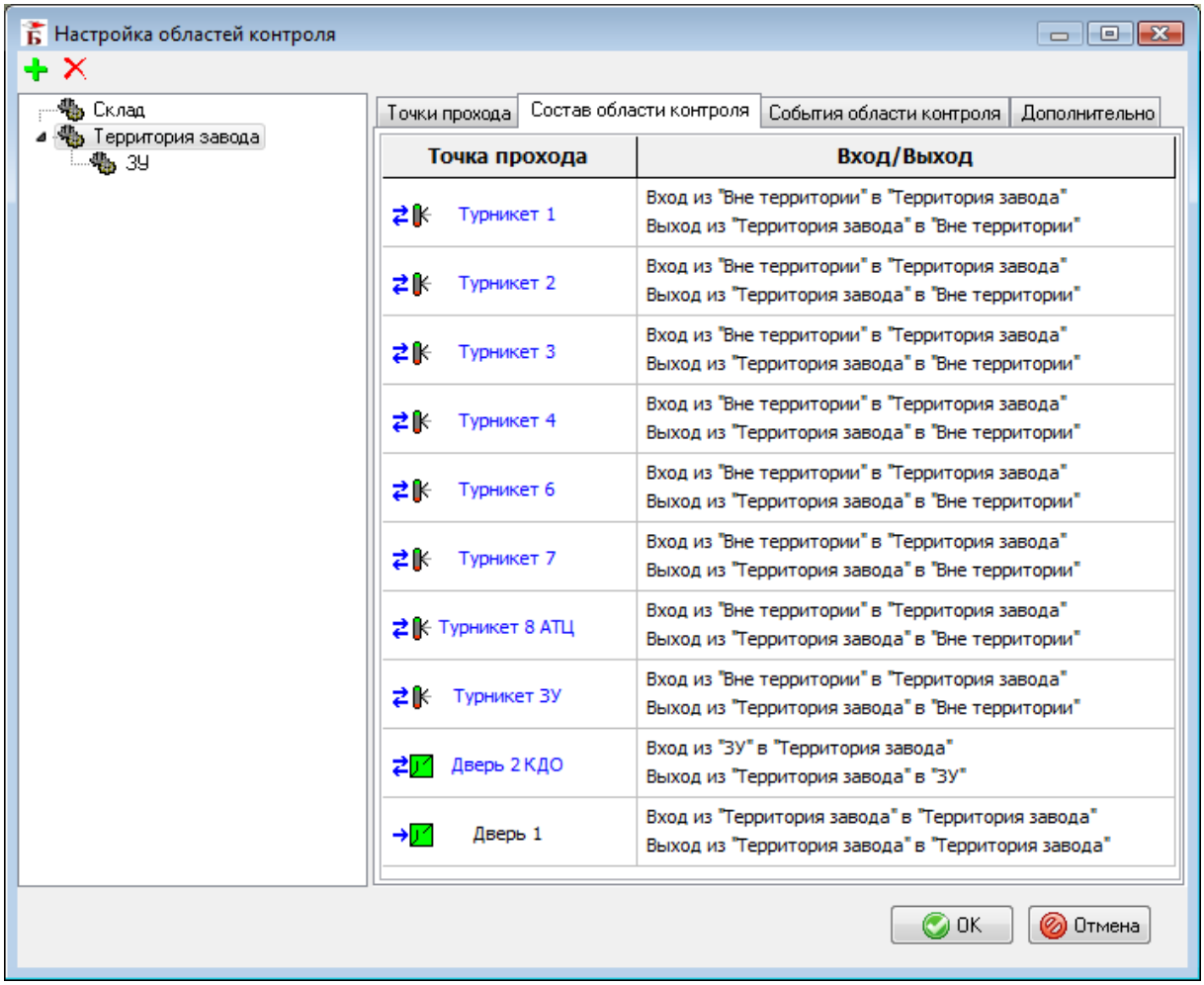


Рис. 34. Состав области контроля

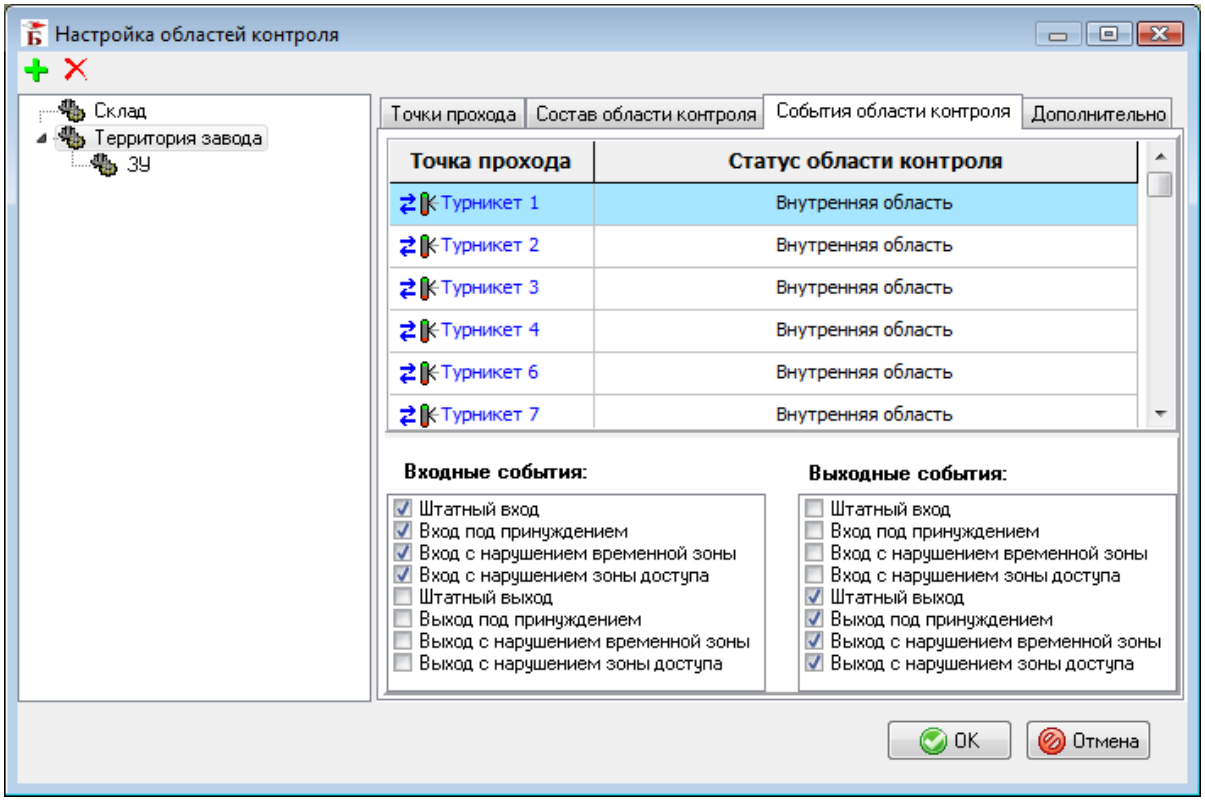


Рис. 35. События области контроля

На странице «Дополнительно» доступен еще ряд параметров области контроля:

Использовать для учета рабочего времени. Если флаг установлен, то события по этой области контроля будут засчитываться как приход/уход с работы. В дальнейшем, в генераторе отчетов по рабочему времени можно будет выбрать область контроля, по которой формировать выбранный отчет.

Вести подсчет людей. Если данный флаг установлен, программное обеспечение будет вести подсчет количества людей в области контроля на основе определенных для нее входных и выходных событий.

Сбрасывать значение счетчика в 1:00 ночи. При установленном флаге счетчик людей будет сброшен в указанное значение в 1:00 ночи.

4.12 Настройка глобального контроля последовательности прохода

СКУД «Elsys» обеспечивает возможность работы глобального контроля последовательности прохода («Antipassback»), причём его функционирование возможно и при отсутствии компьютера на линии связи.

При настройке функции «Глобальный контроль последовательности прохода» следует учитывать следующие ограничения:

- каждый контроллер доступа может обслуживать не более двух областей контроля;
- глобальный контроль последовательности прохода работает либо в пределах одной линии связи RS-485, либо в пределах системы, построенной с использованием КСК «Elsys-MB-Net», поскольку отсутствует обмен информацией контроллеров доступа, подключенным к разным COM-портам, между собой и контроллерами, подключенными к КСК «Elsys-MB-Net»;
- контроллеры «Elsys-MB-SM» поддерживают функцию «Глобальный контроль последовательности прохода», если в памяти контроллера содержится не более 150 карт доступа.

Для настройки глобального контроля последовательности прохода необходимо, в первую очередь, сконфигурировать области контроля (см. п. 4.11).

Затем необходимо включить функцию глобального контроля последовательности прохода в настройках драйвера ELSYS или сетевого контроллера, нажав на кнопку **«Включить»** (Рис. 36).

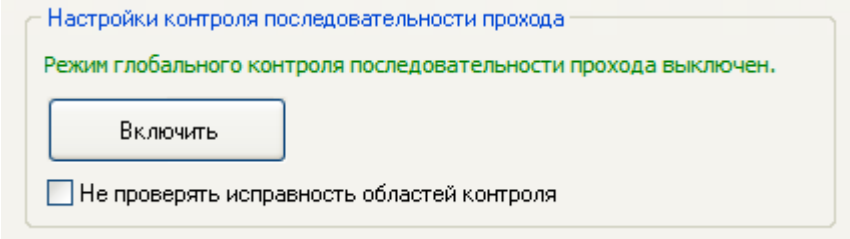


Рис. 36. Функция глобального контроля последовательности прохода выключена

Если необходимо выключить функцию глобального контроля последовательности прохода, то необходимо нажать кнопку **«Выключить»** (Рис. 37) в настройках драйвера или сетевого контроллера.

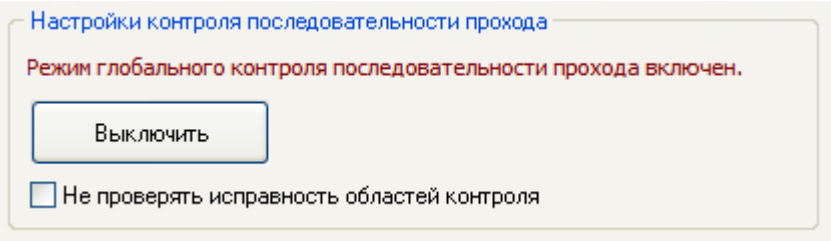


Рис. 37. Функция глобального контроля последовательности прохода включена

При необходимости следует включить настройки **«Сброс в полночь»** контроллеров «Elsys-MB» и **«Не проверять исправность областей контроля»** (см. «Бастион-ELSYS. Руководство инсталлятора»). Эти настройки вступают в силу после инициализации оборудования.

В свойствах пропуска (см. инструкцию «Бюро пропусков») имеется опция **«Не отслеживать последовательность прохода»** (по умолчанию выключена). Её включение позволяет отключить функцию **«Глобальный контроль последовательности прохода»** для отдельных лиц.

Инициализация контроллеров происходит автоматически при закрытии окна конфигуратора драйвера или окна настройки областей контроля.

Если необходимо исключить контроллер из системы глобального контроля последовательности прохода, то необходимо в настройках контроля последовательности прохода для контроллера доступа выставить значение **«Не использовать»**.

4.13Настройка счётчиков персонала

С каждой областью контроля может быть связан счётчик персонала. Начальное значение данного счётчика можно установить вручную. Для этого необходимо выбрать пункт меню «Инструменты→Сброс счётчиков персонала». В появившемся окне выберите требуемую область контроля, установите значение счётчика и нажмите кнопку «ОК». Также имеется возможность задать режим, при котором счётчик будет сбрасываться в определённое значение каждые сутки в 1:00 ночи. Следует иметь ввиду, что при подсчёте людей в областях контроля не могут быть учтены проходы по кнопкам, проход нескольких человек по одной карте и ряд аналогичных случаев.

4.14Синхронизация времени

Комплекс «Бастион» предоставляет возможность синхронизации времени всех рабочих станций комплекса, а также оборудования (при поддержке функции установки времени), с сервером системы. Синхронизация времени позволяет более точно отслеживать последовательность событий, происходящих в системе.

Пользователю предоставляется возможность выбора следующих параметров синхронизации («Конфигурация→Общие настройки→Синхронизация времени»):

Синхронизировать время при запуске программы. При установке этого флага время будет синхронизироваться при подключении любой рабочей станции к комплексу.

Периодическая синхронизация. Доступные варианты: никогда, раз в час и раз в день. Также можно указать время, в которое будет производиться синхронизация.

При синхронизации время будет браться с компьютера, указанного в качестве сервера системы (см. п. 4.3).

4.15Сторожевой таймер

Сторожевой таймер предназначен для автоматического перезапуска системы при ее зависании. Таймер периодически проверяет активность основного потока главного программного модуля (bastion.exe), и в случае, если он не отвечает, производит перезапуск программы. Не отслеживаются сбои оборудования и операционной системы. Таймер реализован в виде службы Windows.

Для активизации таймера необходимо выбрать пункт меню «Конфигурация→Общие настройки» и перейти на страницу «Сторожевой таймер». Таймер имеет 2 параметра:

Время отсутствия отклика. Если основной поток программы не отвечает в течение этого времени, система будет перезапущена.

Задержка перед перезапуском. Система будет запущена повторно через заданное время после ее аварийного завершения.

4.16Выгрузка протокола системы

Если в системе установлен модуль «Бастион-Архив», то появляется возможность периодически выгружать данные из протокола событий системы во внешний файл в формате csv.

Имеется возможность отдельно задать параметры для выгрузки основного журнала и журнала учета рабочего времени. Настройка параметров производится в окне «Общие настройки» меню «Конфигурация», на страницах «Протокол→Администрирование протокола» и «Учет рабочего времени→Администрирование».

Возможно 2 режима работы автоматической выгрузки – с удалением старых данных и с переносом их во внешний файл.

Дополнительно, для системы выгрузки необходимо указать следующие параметры:

Время выполнения действия. Рекомендуется указывать время наименьшей активности системы, так как операция может быть длительной и снижать общую производительность системы. Для основного протокола и УРВ рекомендуется указывать разное время.

Частота выполнения. Возможные варианты: раз в неделю, раз в месяц, раз в два месяца, раз в три месяца. Выгрузку рекомендуется производить не реже раза в месяц.

День выполнения. Указывается, в какой день выполнять операцию.

Оставлять данные в протоколе за: возможные варианты: от 1 месяца до 3-х лет.

Каталог сохранения: путь на сервере системы, где будут храниться архивные файлы. Для работы системы указанный каталог должен существовать.

Кнопка «Запустить выгрузку данных» позволяет выполнить выгрузку немедленно с параметрами, указанными в текущем окне.

Выгрузку осуществляет компьютер, указанный в качестве сервера системы.

4.17 Организация возврата временных и разовых пропусков

В системе предусмотрено 2 варианта организации возврата временных и разовых электронных пропусков.

Первый вариант предполагает наличие специальной точки прохода (турникета, шлюза) и рабочего места оператора, контролирующего выход по временным и разовым пропускам. При этом система должна быть настроена таким образом, чтобы решение об открывании точки прохода на выход принимал оператор. При предъявлении карты на выход у оператора появляется окно фотоидентификации с двумя дополнительными кнопками «Сдал» и «Не сдал». Если выходящий сдает пропуск оператору, то оператор должен нажать кнопку «Сдал». При этом в программе пропуск переводится в архив, в протокол записывается соответствующее событие, а карта доступа может быть выдана повторно. При нажатии кнопки «Не сдал» окно фотоидентификации закрывается и система не производит никаких дополнительных действий.

Для использования такого режима работы необходимо выполнить следующие настройки. Открыть форму конфигурации рабочих станций («Конфигурация→Рабочие станции») и перейти на страницу «Бюро пропусков». Выбрать рабочую станцию, на которой будет организовано рабочее место для возврата пропусков. Установить флаг «*Разрешить возврат временных пропусков на этом рабочем месте*» и сохранить изменения. После этого становятся доступны опции:

Точка прохода. Точка доступа, при предъявлении карты к которой будет осуществляться возврат пропуска.

Событие для возврата пропуска. Событие, по которому будет выведено окно фотоидентификации для возврата пропуска. Конкретное событие может быть разным, в зависимости от настроек системы.

Второй вариант предполагает использование специального картосборника со встроенным считывателем. В этом случае для выхода за территорию предприятия посетитель должен поместить карту доступа в картосборник, после чего точка прохода открывается на выход.

Для реализации такого режима необходимо настроить реакцию на событие «Предоставление доступа на выход» и в качестве реакции указать сценарий, содержащий действие «Вернуть предъявленную карту». После выполнения этого сценария карту доступа можно будет выдавать повторно.

4.18Настройка расположения файлов

Для выполнения настойки расположения файлов комплекса «Бастион» выберите пункт меню «Конфигурация→Расположение файлов» (Рис. 38).

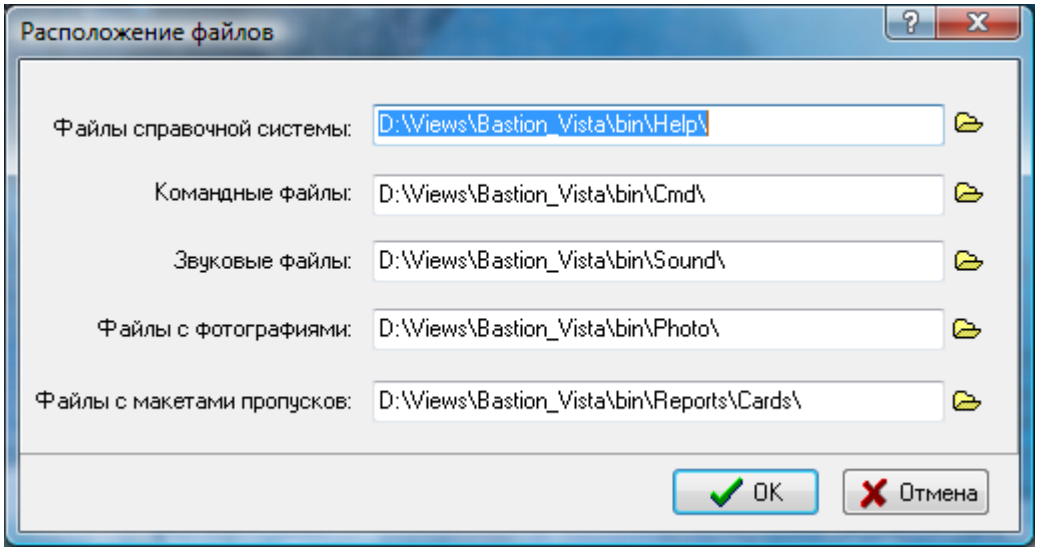


Рис. 38. Форма настройки расположения файлов

Система позволяет установить пути к следующим группам файлов (в скобках указан путь по умолчанию):

- Файлы справки (<Bastion>\Help)
- Файлы графических планов (<Bastion>\Maps)
- Командные файлы (<Bastion>\Cmd)
- Звуковые файлы (<Bastion>\Sound)
- Файлы фотографий – используются только при начальной настройке системы (для ввода фотографий в базу данных) при наличии СКУД (<Bastion>\Photo).
- Файлы с макетами пропусков (<Bastion>\Patterns)

Для вызова окна выбора папки нажмите кнопку «Обзор» справа от соответствующей строки редактирования.

Обычно без особой необходимости не следует изменять расположение файлов, используемое по умолчанию.

4.19Особенности работы генератора отчётов и системы учёта рабочего времени

Модули BrepGen.exe и Attendance.exe могут работать без установленной BDE и использовать для получения отчётов файлы баз данных, отличные от используемых комплексом в текущий момент. Пути к протокольной и основной базам данных можно указать вручную, нажав кнопку «  » в панели инструментов генератора отчётов или УРВ.

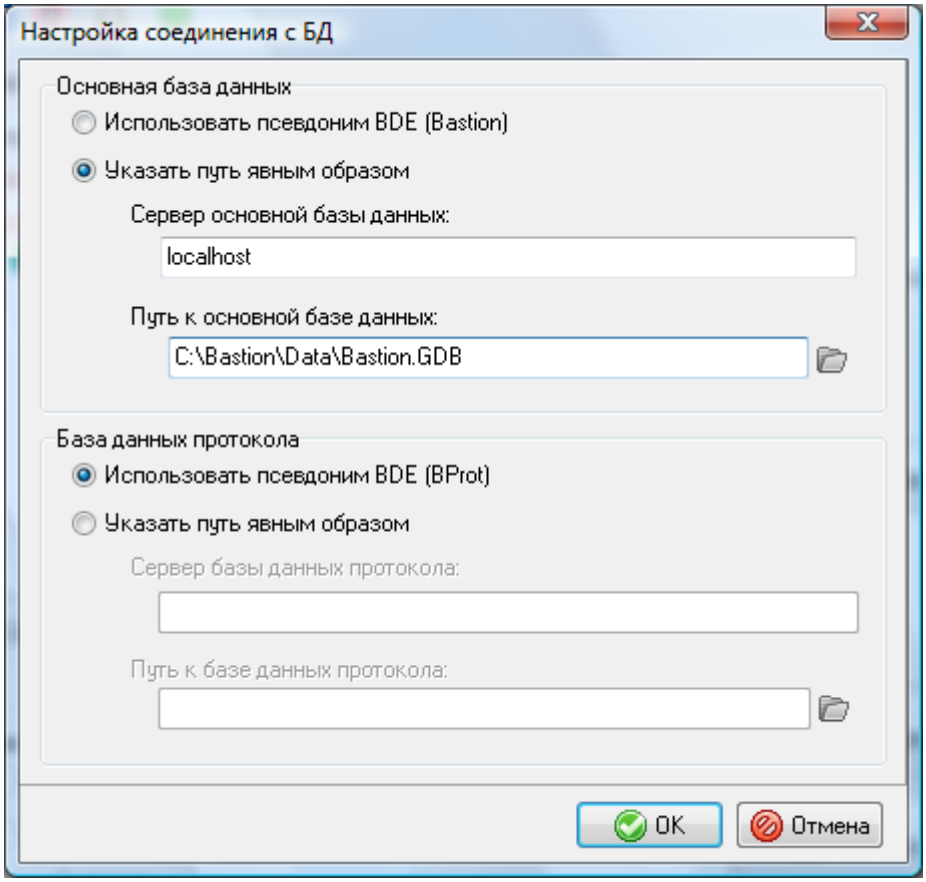


Рис. 39. Настройка путей к основной и протокольной базам данных

По умолчанию выбраны настройки «Использовать псевдоним BDE». В этом случае используется путь к базам данных, с которыми в текущий момент работает комплекс «Бастион». Если для получения отчётов необходимо использовать другие файлы (например, архивные копии файлов Bprot.gdb и Bastion.gdb), следует указать путь к ним явным образом.

Настройка путей к БД сохраняется в системном реестре.

Файл Bprot.gdb, в котором содержится протокол событий, и журнал учёта рабочего времени, при интенсивном потоке событий (СКУД среднего и большого масштаба) значительно увеличивается в объёме за достаточно короткое время (1 Гб и более за несколько недель работы). При большом размере файла базы данных производительность системы может заметно снижаться (в задачах протоколирования текущих событий, а также формирования отчётов). Для решения этой проблемы можно использовать 2 подхода:

Регулярно выполнять резервное копирование и восстановление (backup/restore) БД протокола. При этом оптимизируется внутренняя структура БД и таким образом ускоряется работа системы.

Регулярная замена файла BProt.GDB файлом чистой (пустой) БД. Такой файл находится на дистрибутивном диске в каталоге «<CD>\Install\Database». После копирования файлов с компакт-диска у них следует снять атрибут «Только чтение».

> ***Внимание!*** *После замены протокольной базы на чистую, после выполнения импорта базы данных персонала и в некоторых других случаях (если по невыясненным причинам в отчётах отсутствует ряд сотрудников) требуется выполнить синхронизацию баз данных. Для выполнения синхронизации следует нажать кнопку «Синхронизация данных» в главном окне генератора отчетов по событиям или рабочему времени, после чего необходимые сведения будут перенесены в БД протокола.*

5 Расширенные возможности запуска системы

5.1 Параметры командной строки

Исполняемый файл "bastion.exe", а также модули генератора отчетов (BRepGen.exe) и УРВ (Attendance.exe) могут быть запущены с одним или несколькими из следующих параметров, предназначенных для автоматизации процесса запуска системы:

user=<UserName> - имя пользователя для входа в программу

pwd=<Password> - пароль пользователя

nouser. Этот параметр используется для запуска комплекса в режиме мониторинга. При этом осуществляется взаимодействие с оборудованием, однако все функции управления комплексом недоступны.

quickexit. Если программа запущена с этим параметром, то при выходе из программы не будет запрашиваться подтверждение.

Общий синтаксис командной строки:

```
bastion.exe [user=<UserName> pwd=<Password>] [nouser] [quickexit]
```

5.2 Запуск системы с ожиданием загрузки драйвера HASP

В состав АПК «Бастион» входит специальная утилита (DelayedLaunch.exe), позволяющая ожидать загрузки драйвера ключа HASP перед запуском требуемой программы.

Например, эта утилита используется при установке Bastion.exe вместо оболочки Windows (см. п. 5.4). Также, рекомендуется использовать утилиту DelayedLaunch.exe в том случае, если требуется прописать Bastion.exe (или любую другую программу, требующую наличия ключа HASP) в папку автозагрузки ОС.

Синтаксис использования командной строки DelayedLaunch.exe:

```
DelayedLaunch.exe app=<исполняемый модуль> [user=<UserName> pwd=<Password>]
[nouser] [quickexit] [delay=<seconds>]
```

Назначение параметров см. выше, в п. 5.1.

Параметр delay определяет минимальную задержку, которая будет выдержана перед запуском программы.

5.3 Запуск системы без полномочий администратора

5.3.1 Доступ к разделам системного реестра

Для запуска основного приложения комплекса (Bastion.exe) пользователями, не обладающими правами администратора в ОС, не требуется выполнения каких-либо специальных действий. Однако для работы генератора отчётов, системы учёта рабочего времени и подсистемы архивации протокола этим пользователям необходимо дать права доступа на чтение и запись к следующему разделу системного реестра:

```
HKEY_LOCAL_MACHINE\Software\Borland
```

Сделать это можно с помощью редактора реестра regedit.exe. Для его запуска необходимо выбрать меню «Пуск→Выполнить…» и набрать в появившемся окне “regedit”. В запустившейся программе нужно выделить указанные ключи в реестре (Рис. 40) и выбрать пункт меню «Правка→Разрешения».

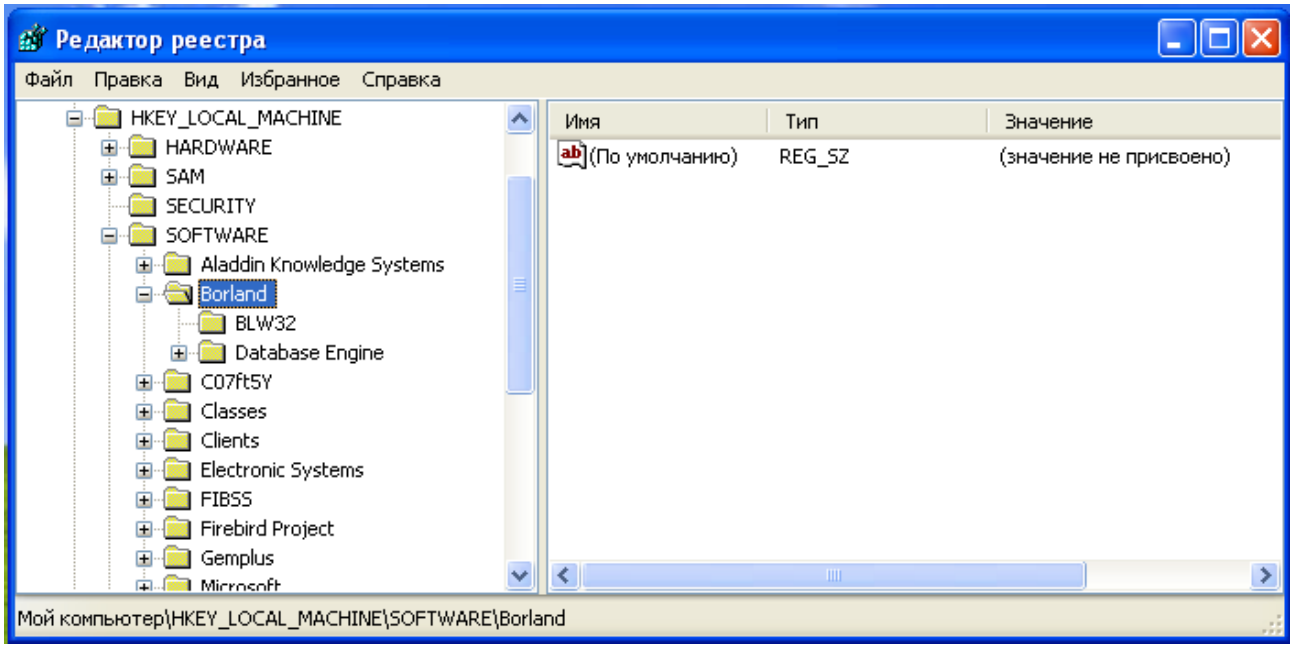


Рис. 40. Редактор реестра. Ключ Borland

В случае, если требуемого пользователя или группы нет в окне разрешений, нажать кнопку «Добавить» и набрать имя пользователя или группы, которым необходимо дать доступ (рекомендуется добавлять группу "Пользователи (<ИМЯ_КОМПЬЮТЕРА>\Пользователи)", см. Рис. 41). Установить флаг «Полный доступ» в колонке «Разрешить». Например, на Рис. 41 установлен полный доступ для всех пользователей компьютера ANDREYK-VIRTXP.

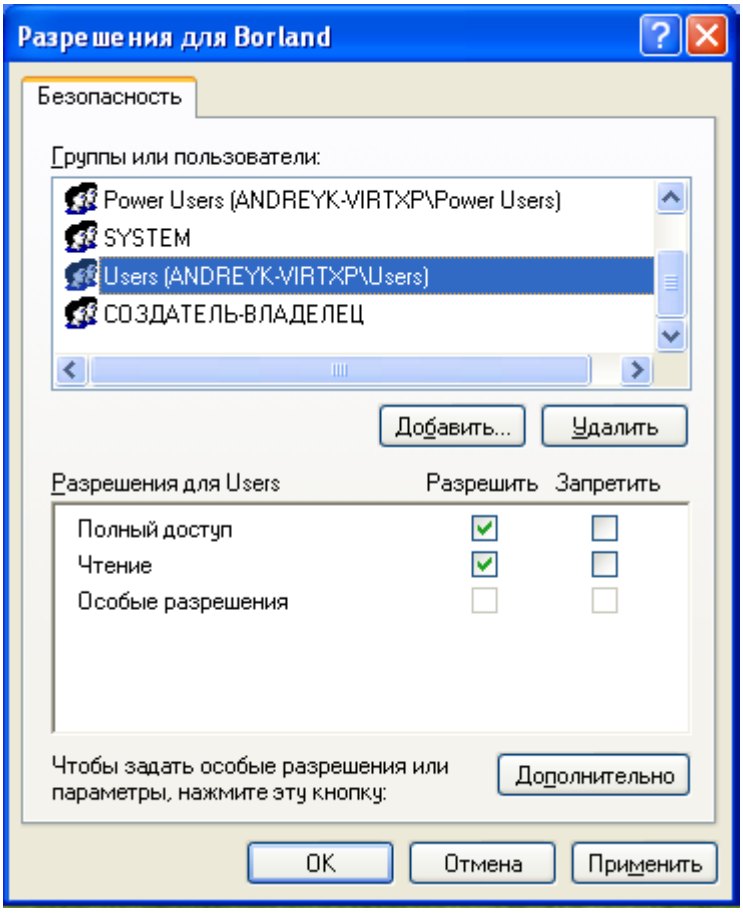


Рис. 41. Окно разрешений для ключа реестра Borland

5.3.2 Параметры безопасности NTFS

Если система установлена в раздел NTFS, то пользователи Windows, работающие с АПК «Бастион», должны иметь полный доступ к следующим каталогам АПК «Бастион»: **Net**, **Priv**, **Tables, Maps, Reports, Transform,** а также к основному каталогу **Bastion**.

Далее приводится инструкция, как дать полный доступ к папке АПК «Бастион» и всем её подпапкам всем пользователям компьютера. Настройки, приведенные ниже, гарантировано позволяют работать с АПК «Бастион» без прав администратора. Если, дополнительно, требуется ограничить права пользователей на операции с отдельными файлами, следует схожим образом настроить параметры безопасности для каждого этих файлов, убрав лишние разрешения.

Для предоставления полных прав на все объекты папки Bastion всем пользователям компьютера:

1. Выберите в проводнике главный каталог АПК «Бастион» (например, c:\Bastion) и из контекстного меню выберите «Свойства». В открывшемся окне перейдите на страницу «Безопасность» (см. Рис. 42).
2. Выберите группу "Пользователи (<ИМЯ_КОМПЬЮТЕРА>\Пользователи)" или “Users (<ИМЯ_КОМПЬЮТЕРА>\Users”), см. Рис. 42).

3. Установите флаг «Полный доступ» в колонке «Разрешить». Например, на Рис. 42 установлен полный доступ для всех пользователей компьютера ANDREYK-VIRTXP.

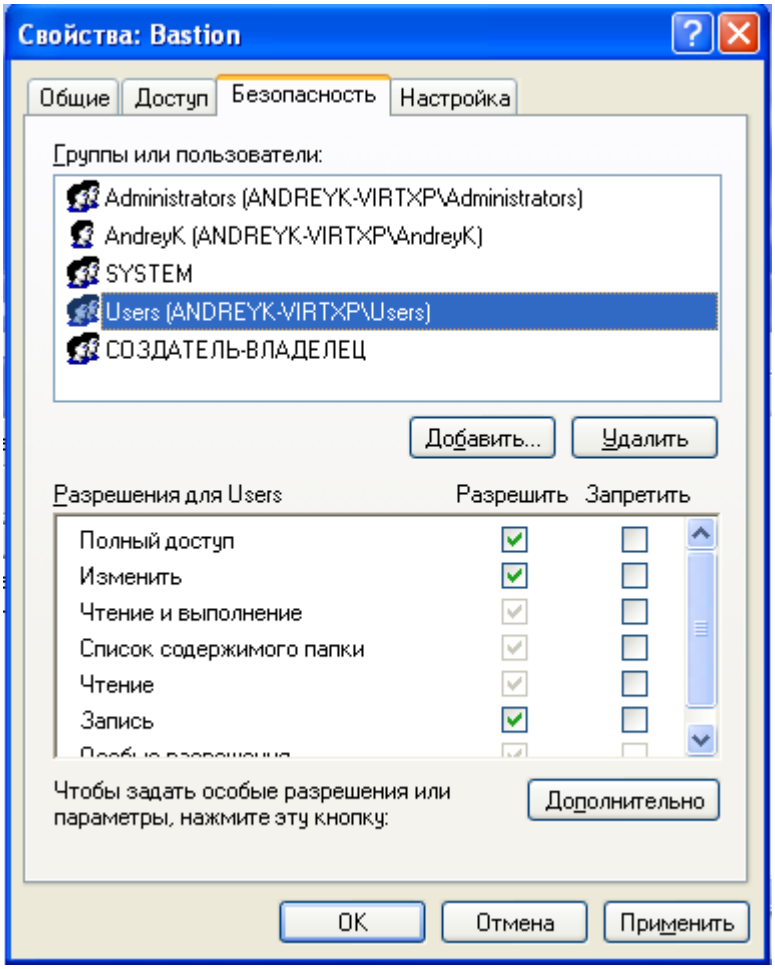


Рис. 42. Предоставление доступа к папке Bastion

4. Нажмите кнопку «Дополнительно». В открывшемся окне (см. Рис. 44) снимите флаг «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добавляя их к явно заданным в этом окне». Появится запрос (Рис. 43), нажмите кнопку «Удалить».

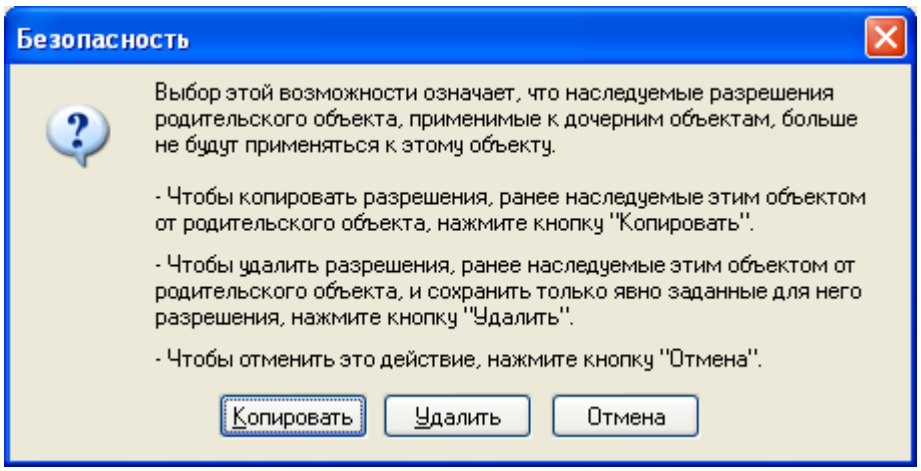


Рис. 43. Запрос подтверждения отмены наследования разрешений

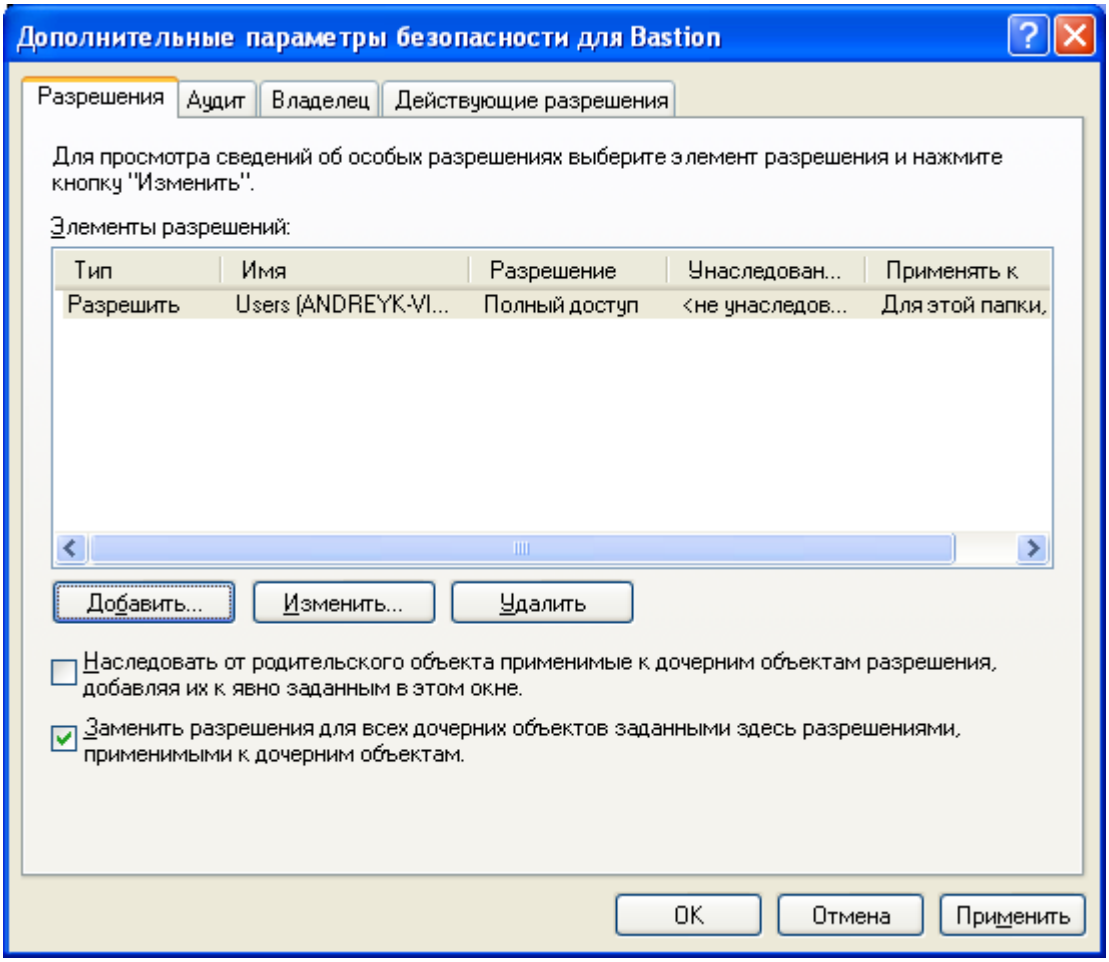


Рис. 44. Дополнительные параметры безопасности папки Bastion

5. В окне дополнительных параметров (Рис. 44) нажмите кнопку «Добавить». Введите имя добавляемой группы (“Пользователи” или “Users”) и нажмите ОК.
6. Появится окно установки прав для группы Users (Рис. 45). Установите флаг «Полный доступ» в колонке «Разрешить», как показано на Рис. 45 и нажмите ОК.
7. В окне на Рис. 44 установите флаг «Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам». Окно должно принять вид, представленный на Рис. 44. Нажмите кнопку ОК.

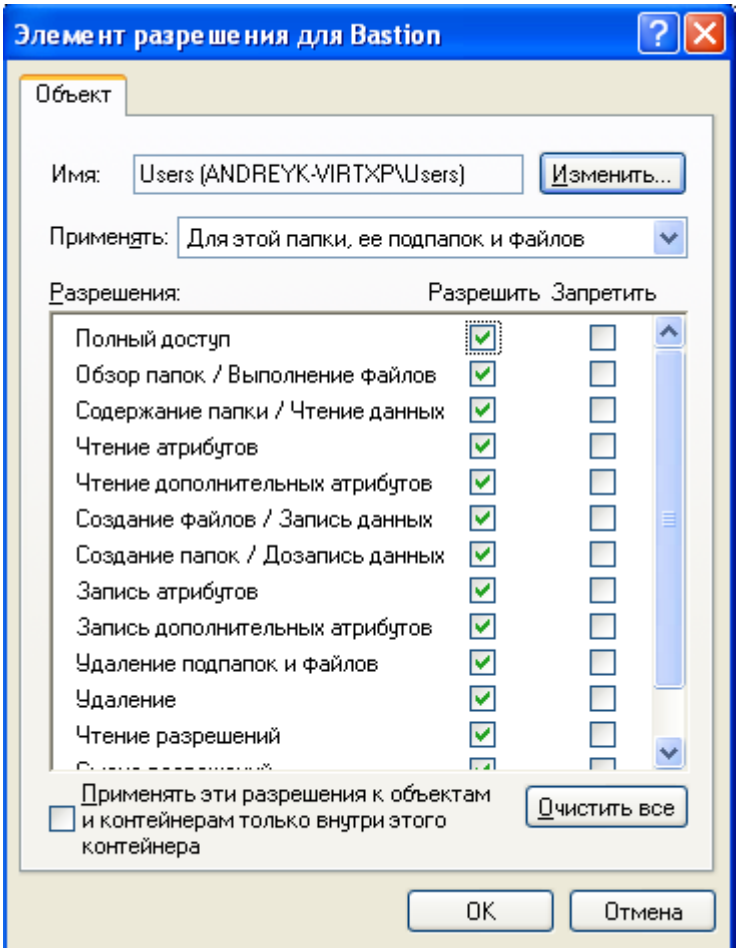


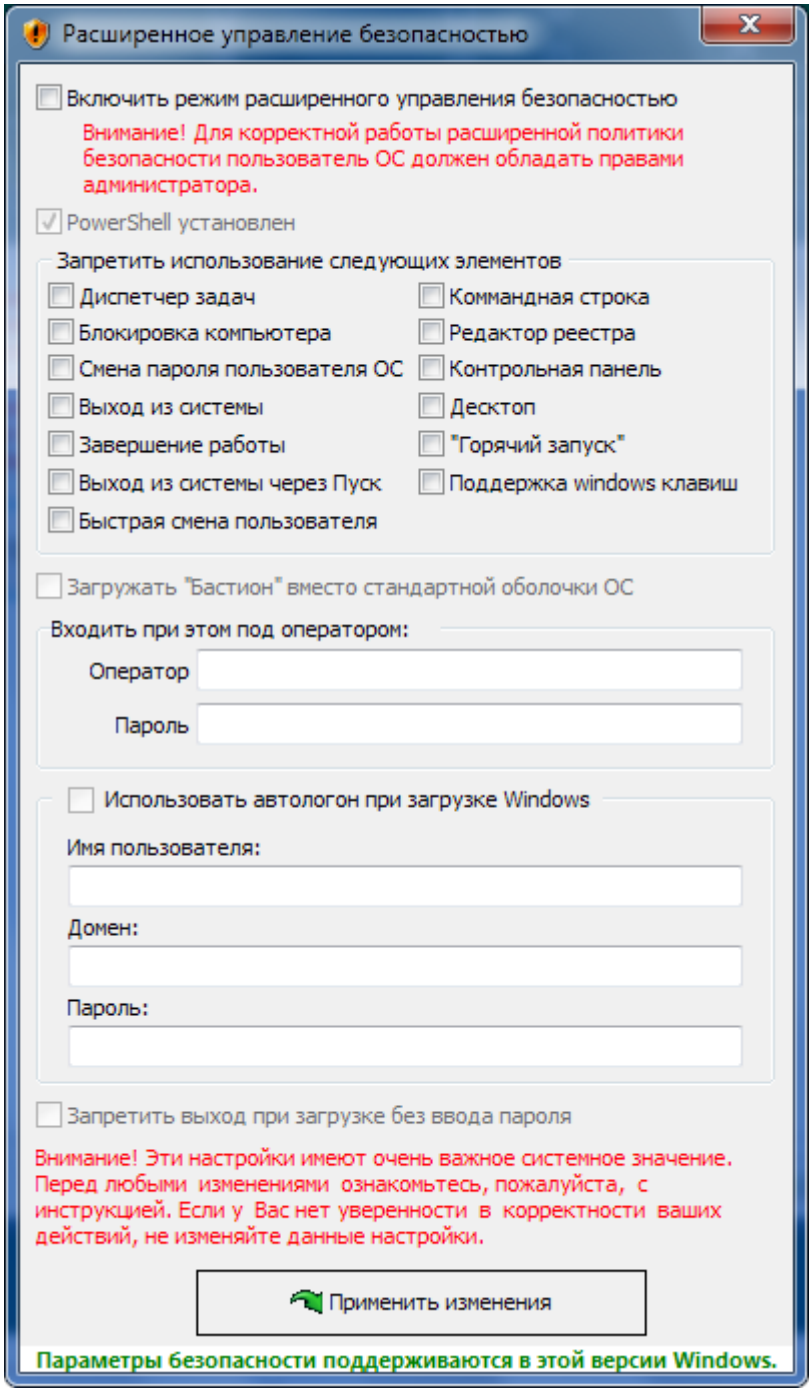
Рис. 45. Установка прав для группы Users

5.4 Использование режима расширенной безопасности

Основное назначение режима расширенной безопасности – разграничить полномочия оператора АПК «Бастион» для доступа к функциям операционной системы.

> ***Внимание!*** *Для правильной работы этих настроек необходимо зайти под пользователем, для которого будет производиться настройка и пользователь Windows должен обладать правами администратора.*

Для включения режима расширенной безопасности необходимо в общих настройках (Конфигурация→Общие настройки…) на странице «Безопасность» запустить специальную утилиту.



В данной утилите доступны следующие настройки:

Включить режим расширенного управления политикой безопасности – если опция выключена, то все параметры безопасности выключены, если включена – то доступ к функциям Windows определяется профилем оператора АПК «Бастион».

Здесь же можно задать ряд общих параметров режима расширенной безопасности:

PowerShell установлен - Проставляется автоматически и недоступна администратору, при установленной опции часть безопасности устанавливается через эту утилиту. Необходима для установки групповых политик и политик ограничения программ.

Загружать “Бастион” вместо стандартной оболочки ОС – эта опция позволяет автоматически загружать «Бастион» вместо оболочки Windows (вместо проводника) и блокировать доступ к элементам рабочего стола и меню программ.

Входить при этом под оператором – позволяет указать оператора АПК «Бастион», под чьим именем будет произведен автоматический вход в АПК «Бастион» при его загрузке. Если оператора не указать – будет выведено окно с запросом имени и пароля.

> ***Внимание!*** *Не допускается использование пользователей без пароля.*

Использовать автологон – предназначен для автоматического ввода имени пользователя, домена и пароля при запросе ОС (т.е. при загрузке ОС не надо нажимать Ctrl+Alt+Del и вводить имя и пароль).

В блоке опций «Запретить использование следующих элементов» можно выбрать доступность или запретить запуск элементов из предложенного списка.

> ***Внимание!*** *В момент нажатия на кнопку «применить изменения» происходит установка изменений. Формируется лог сообщений об ошибках. И перечитывается текущее состояние из ОС. Если произошёл сбой и система не установила настройку, - то не установленные опции будут скинуты в неустановленное состояние.*

После изменения настроек расширенной безопасности необходимо перезапустить операционную систему.

> ***Внимание!*** *Если после установок параметров безопасности загрузить компьютер не удается (если «Бастион» не может загрузиться, а «Проводник» недоступен), рекомендуется загрузить Windows в «Безопасном режиме с поддержкой командной строки». Из командной строки выполнить regedit и в редакторе реестра исправить значение*
>
> `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell на «explorer.exe».`

5.5 Использование службы Active Directory (AD) и двухфакторная авторизация

5.5.1 Общие настройки

АПК «Бастион», начиная с версии 1.7.4.6, позволяет использовать службу Active Directory для идентификации пользователей. Настройка этой функции производится форме «Общие настройки» (см. Рис. 46 Настройка Active Directory).

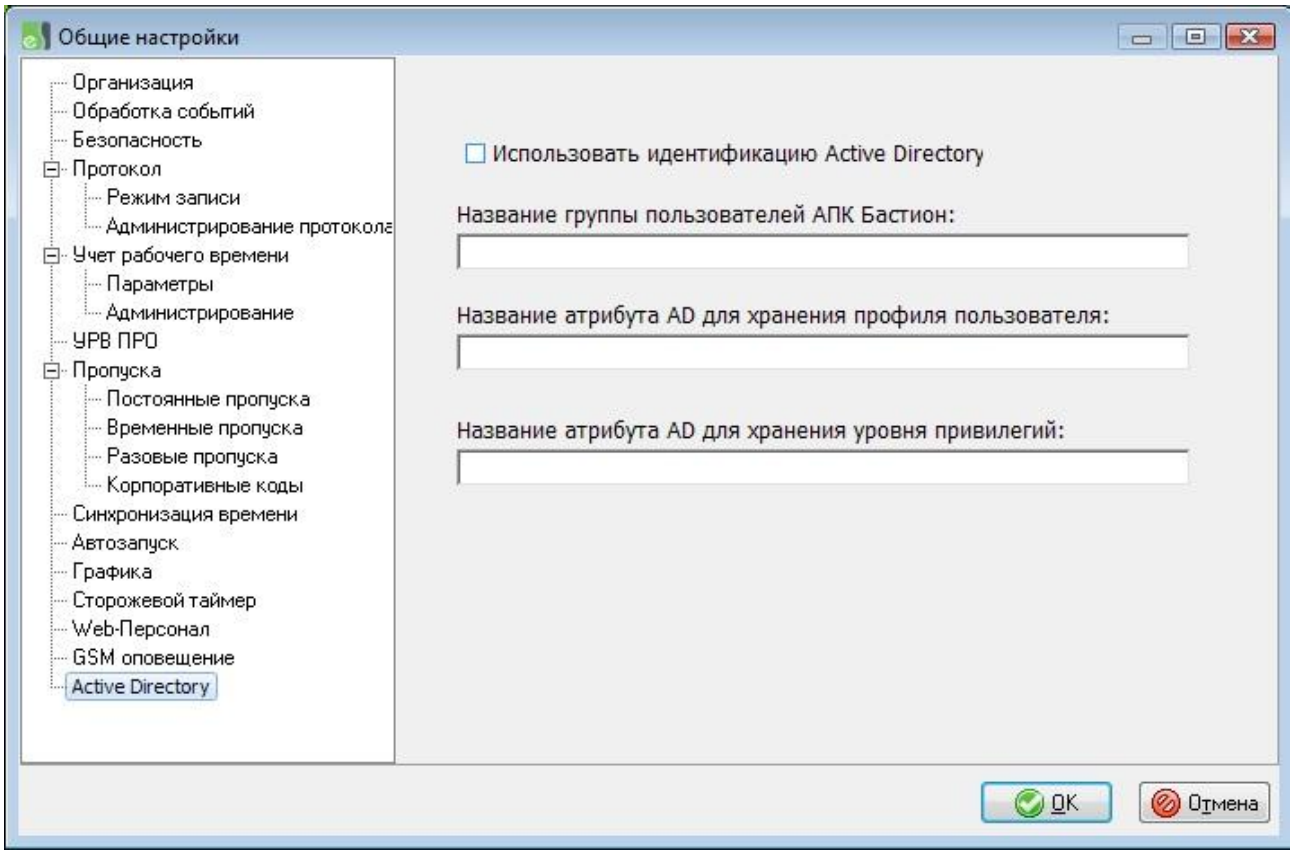


Рис. 46 Настройка Active Directory

Опция «Использовать идентификацию Active Directory» позволяет либо использовать (флаг установлен), либо не использовать (флаг не установлен) эту возможность. По умолчанию, флаг не установлен.

Поле «Название группы пользователей АПК Бастион» должно содержать название группы Active Directory, в которую входят пользователи АПК «Бастион». По умолчанию, группа называется APK_BASTION_USERS.

Поле «название атрибута AD для хранения профиля пользователя» должно содержать название атрибута, где в свойствах пользователя в AD должно храниться название профиля оператора АПК «Бастион». По умолчанию, это атрибут extensionAttribute13. Профиль в этом поле в свойствах пользователя AD должен соответствовать профилю, существующему в АПК «Бастион» (см. п. 4.6 по настройке профилей). Выбранный атрибут должен быть текстовым.

Поле «название атрибута AD для хранения уровня привилегий» должно содержать название атрибута, где в свойствах пользователя в AD должен храниться уровень привилегий оператора АПК «Бастион». По умолчанию, это атрибут extensionAttribute14. Уровень, число от 0 до 99, определяет, какие возможности доступны данному оператору АПК «Бастион» (см. п. 4.5 по настройке уровня полномочий). Выбранный атрибут должен быть текстовым.

5.5.2 Алгоритм работы

Если установлен флаг опции «Использовать идентификацию Active Directory», то в момент запуска, АПК «Бастион» проверяет, существует ли пользователь с именем, равным имени пользователя операционной системы «Windows» в БД СКУД. Собирается информация из службы AD по данному пользователю. Далее происходит анализ:

1) Пользователь в AD имеет заполненные атрибуты, позволяющие ему пользоваться АПК «Бастион», но в БД СКУД данные о нём отсутствуют – данный пользователь добавляется в БД СКУД. Окно ввода пароля не появляется, блокировка АПК «Бастион» – отключается.

2) Пользователь в AD имеет заполненные атрибуты, не позволяющие ему пользоваться АПК «Бастион», в БД СКУД данные о нём отсутствуют – подключение к БД СКУД происходит штатно. Появляется окно ввода логина и пароля, опция блокировки АПК «Бастион» – включена.

3) Пользователь в AD имеет заполненные атрибуты, не позволяющие ему пользоваться АПК «Бастион», в БД СКУД данные о нём присутствуют – сначала удаляется пользователь из БД СКУД и далее подключение происходит штатно. Появляется окно ввода логина и пароля, опция блокировки АПК «Бастион» – включена.

4) Пользователь в AD имеет заполненные атрибуты, позволяющие ему пользоваться АПК «Бастион», и в БД СКУД данные о нём присутствуют – данный пользователь подключается к БД СКУД. Окно ввода пароля не появляется, блокировка АПК «Бастион» – отключается.

Во всех 4 случаях происходит синхронизация данных пользователя из AD в БД СКУД. Т.е. в момент входа в АПК «Бастион» происходит обновление данных о нём, что можно использовать администратором AD для изменения профиля пользователя или уровня полномочий.

Ответственность за актуальность и правильность данных у пользователя «Windows» в Active Directory лежит на администраторе службы Active Directory.

5.5.3 Возможные ошибки

У пользователя в атрибутах Active Directory обязательно должны быть прописаны - First Name (GivenName) и DisplayName (DisplayName). Отсутствие их приводит к невозможности подключиться к Active Directory для получения данных о пользователе. Ошибка в «логе» выглядит как «GetCurrentUserNameEx: 1332».

5.5.4 Двухфакторная авторизация

Двухфакторная авторизация подразумевает использование двух признаков для авторизации пользователя (например, пароль и USB-ключ, пароль и биометрический признак).

Двухфакторная авторизация может быть настроена в доменной сети предприятия на основе Active Directory. В этом случае, для авторизации в АПК «Бастион» может быть использован такой же способ авторизации. При входе в сессию Windows пользователь подтверждает свои права по двум признакам. При запуске «Бастиона», автоматически проверяются в AD данные по авторизованному пользователю. Если он входит в группу пользователей АПК «Бастион», то ему предоставляется право входа в систему согласно прописанным в AD уровням доступа. В ином случае, открывается стандартная форма ввода логина\пароля. Подробнее описано в алгоритме работы (п.5.5.2).

5.5.5 Настройка Active Directory для работы с АПК «Бастион»

5.5.5.1 Добавление атрибутов в схему Active Directory

На контроллере домена следует запустить **regsvr32 schmmgmt.dll** с правами локального администратора. Эта оснастка по умолчанию не зарегистрирована. После этого открыть из консоли **mmc** оснастку **Схема Active Directory** и перейти в раздел **Attributes (Атрибуты)**. Для добавления нового атрибута также потребуются права Администратора схемы. Если ваш административный пользователь имеет права "Администратор предприятия", то этого достаточно.

Для добавления нового атрибута потребуется ввести X.500 OID – уникальный идентификатор объекта. Для формирования корректного идентификатора можно воспользоваться Power Shell скриптом (https://gallery.technet.microsoft.com/scriptcenter/Generate-an-Object-4c9be66a)

```
#---

$Prefix="1.2.840.113556.1.8000.2554"

$GUID=[System.Guid]::NewGuid().ToString()

$Parts=@()

$Parts+=[UInt64]::Parse($guid.SubString(0,4),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(4,4),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(9,4),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(14,4),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(19,4),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(24,6),"AllowHexSpecifier")

$Parts+=[UInt64]::Parse($guid.SubString(30,6),"AllowHexSpecifier")
```

```
$OID=[String]::Format("{0}.{1}.{2}.{3}.{4}.{5}.{6}.{7}",$prefix,$Parts[0],$Parts[1]
,$Parts[2],$Parts[3],$Parts[4],$Parts[5],$Parts[6])


$oid


#---
```

Скрипт необходимо скопировать в окно консоли PowerShell и выполнить его.

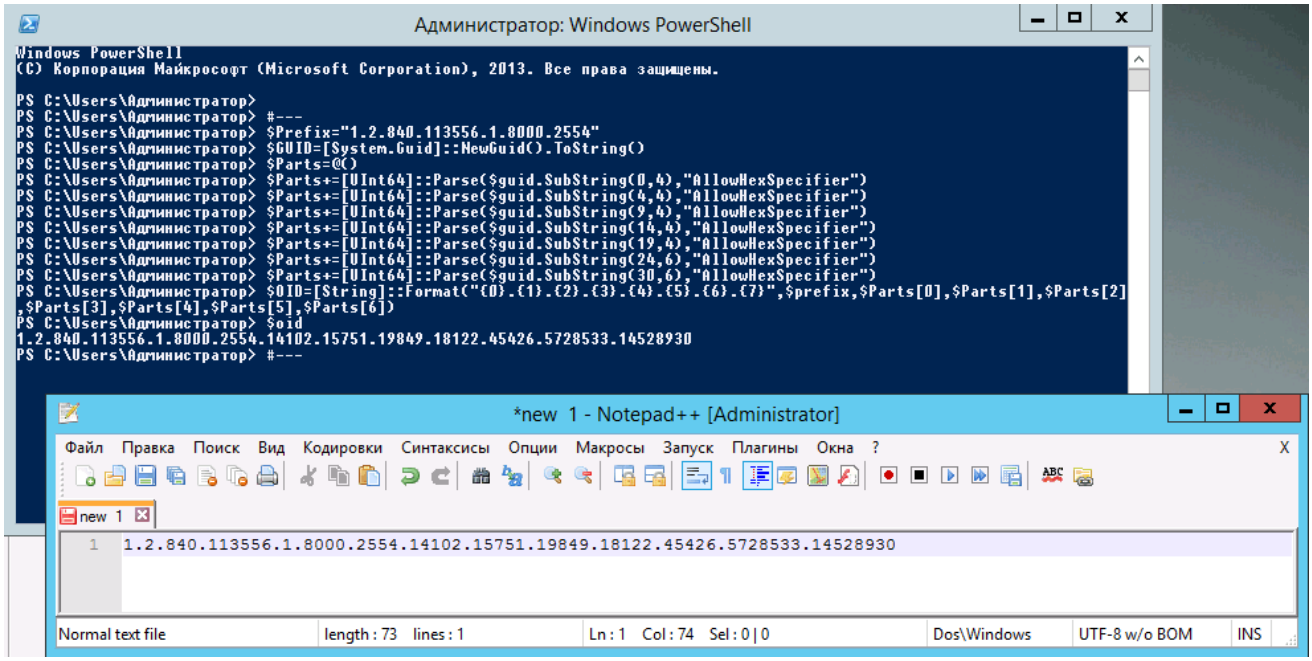


Рис. 47. Генерация X.500 OID

Результат выполнения скрипта – новый X.500 OID, который нужно будет ввести в соответствующее поле на форме создания атрибута.

Далее следует создать новый атрибут **bastionopers** (синтаксис «Строка Юникода»), необходимый для хранения профиля (см. Рис. 48), и атрибут **bastionpriviledges**, необходимый для хранения уровня привилегий пользователя АПК «Бастион» (см. Рис. 49). Минимальное значение этого атрибута должно быть 0, максимальное – 99 (пороговые значения как для привилегий АПК «Бастион»).

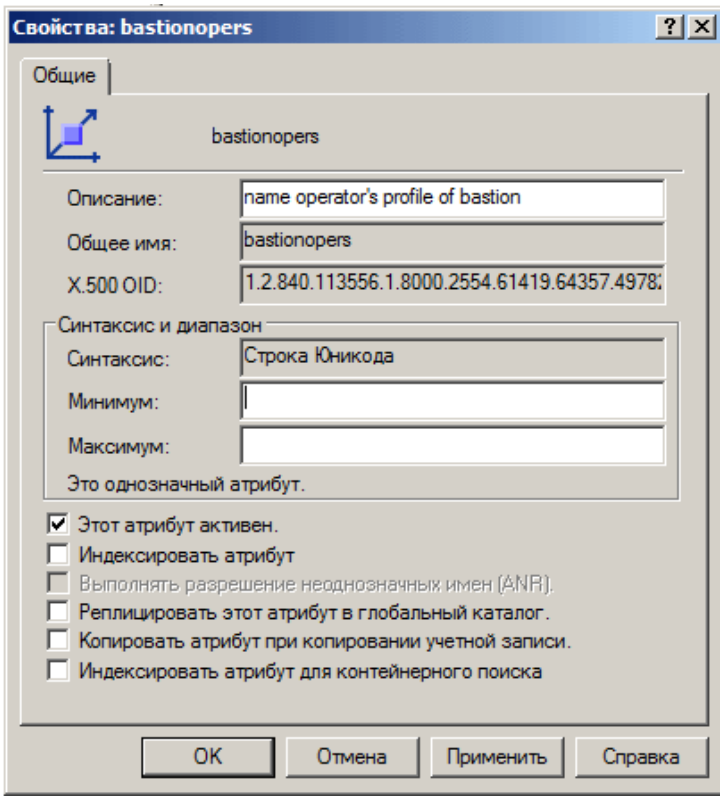


Рис. 48. Добавление атрибута bastionopers

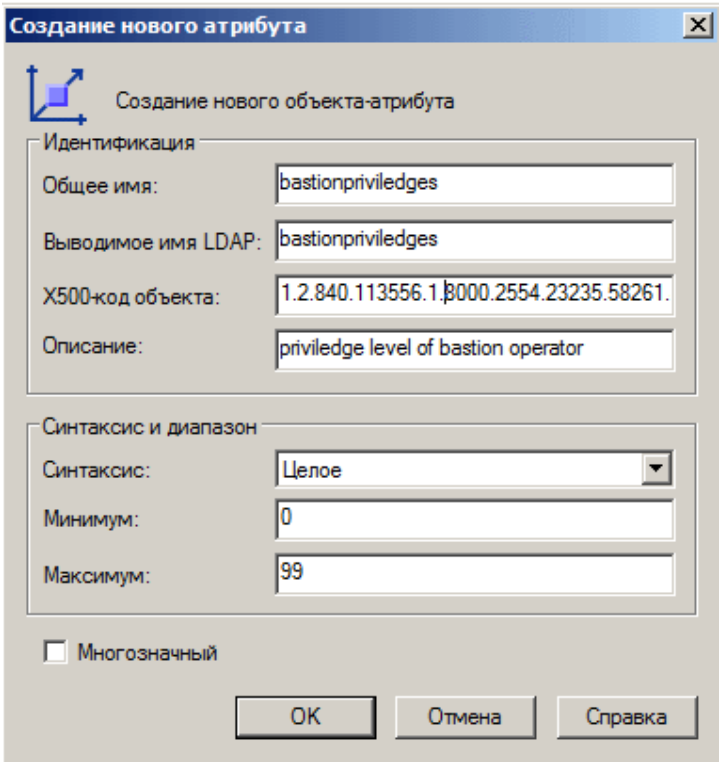


Рис. 49. Добавление атрибута bastionpriveleges

Затем следует добавить атрибут в класс **user**. Для этого в оснастке «Схема Active Directory» можно перейти в раздел **Classes (Классы)**.

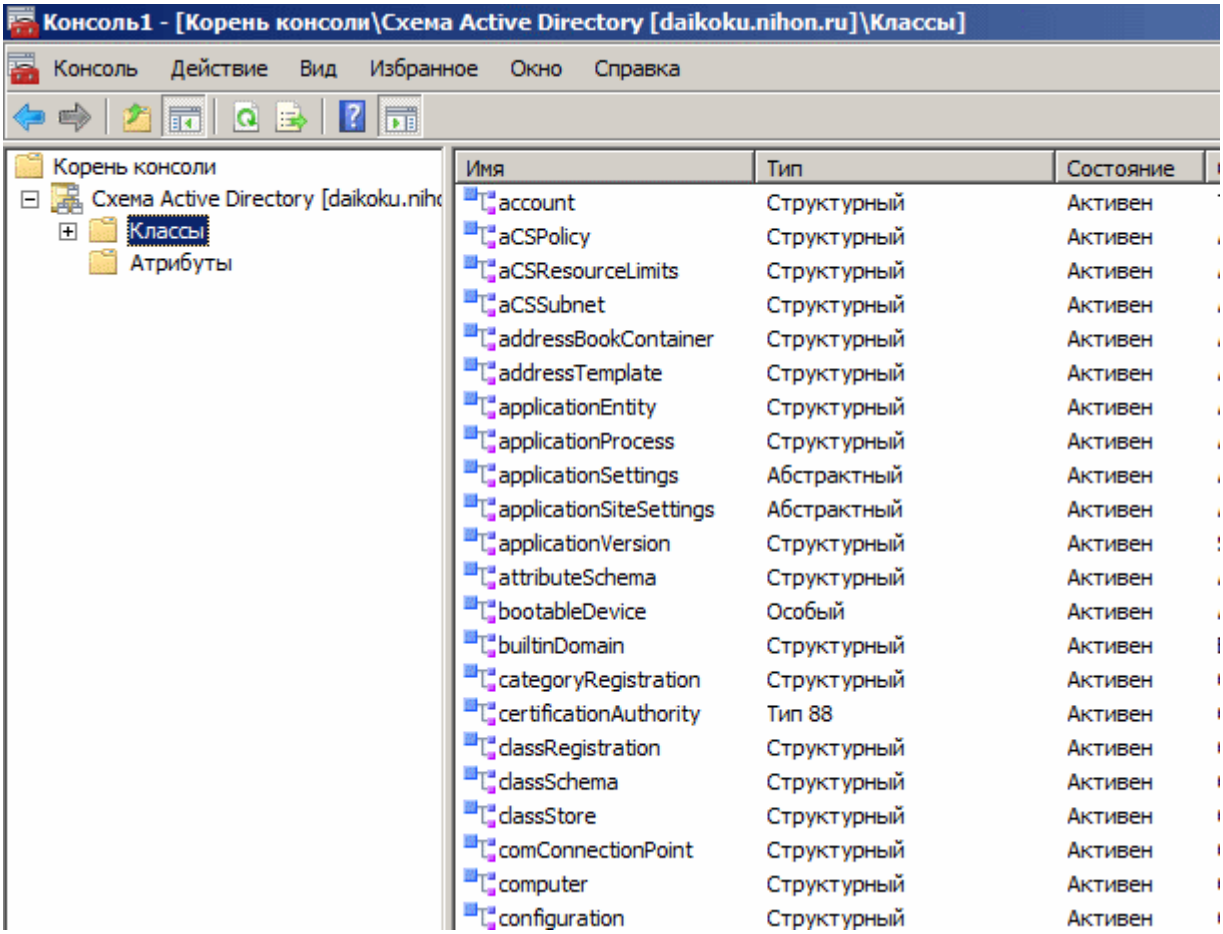


Рис. 50. Раздел "Классы" схемы Active Directory

В свойствах класса **user** необходимо перейти на закладку **Attributes (Атрибуты)** и там добавить новые атрибуты класса.

Командой **adsiedit.msc** можно запустить редактор **ADSI Edit (Редактирование ADSI)** чтобы сделать новые атрибуты видимыми в оснастке **Active Directory Users and Computers**. В параметрах подключения следует выбрать **Configuration**. Затем перейти к контейнеру **CN=419, CN=Display Specifiers, CN=Configuration**. Для отображения в англоязычной консоли CN=409. Для отображения атрибутов на уровне OU выбираем контейнер **CN=organizationalUnit-Display**. В свойствах контейнера необходимо найти атрибут extraColumns, который отвечает за вывод дополнительных атрибутов. Добавляем в него строку в формате:

1) Название атрибута;
2) Заголовок колонки, в которой будет отображаться атрибут;
3) Будет ли отображаться по умолчанию (ставим 1);
4) Ширина колонки в пикселях, значение 1 означает автоматический подбор ширины;
5) Зарезервированное значение (ставим 0).

Например: *ExtraColumns bastionopers.Bastion_operator.1.1.0*

Внимание! *Для того, чтобы новые атрибуты стали видны в оснастке* ***Active Directory Users and Computers****, после добавления атрибутов её необходимо переоткрыть.*

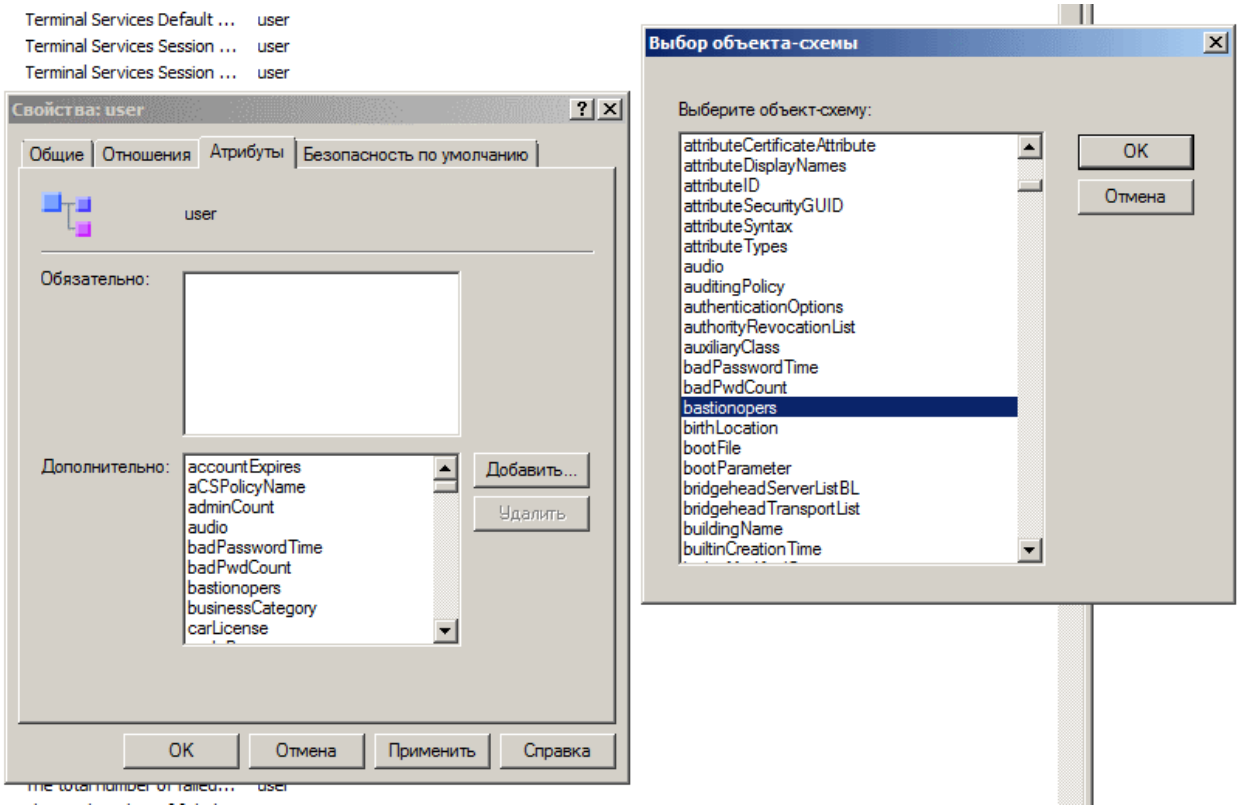


Рис. 51. Атрибуты класса user

5.5.5.2 Настройка идентификации пользователя Active Directory для АПК «Бастион»

Для настройки идентификации пользователей Active Directory для АПК «Бастион» следует выполнить последовательность действий, представленную ниже.

На контроллере домена Active Directory запустить оснастку Active Directory Users and Computers, выбрать в дереве слева узел Users и создать отдельную группу (**group),** предназначенную для пользователей АПК «Бастион», например, с именем apk_bastion_users.

Внимание! *Имя группы должно быть без пробелов и спецсимволов.*

Поместить в созданную группу тех пользователей AD, которые будут впоследствии работать с Бастионом с учетной записью AD (закладка member of в свойствах пользователя, см. Рис. 52).

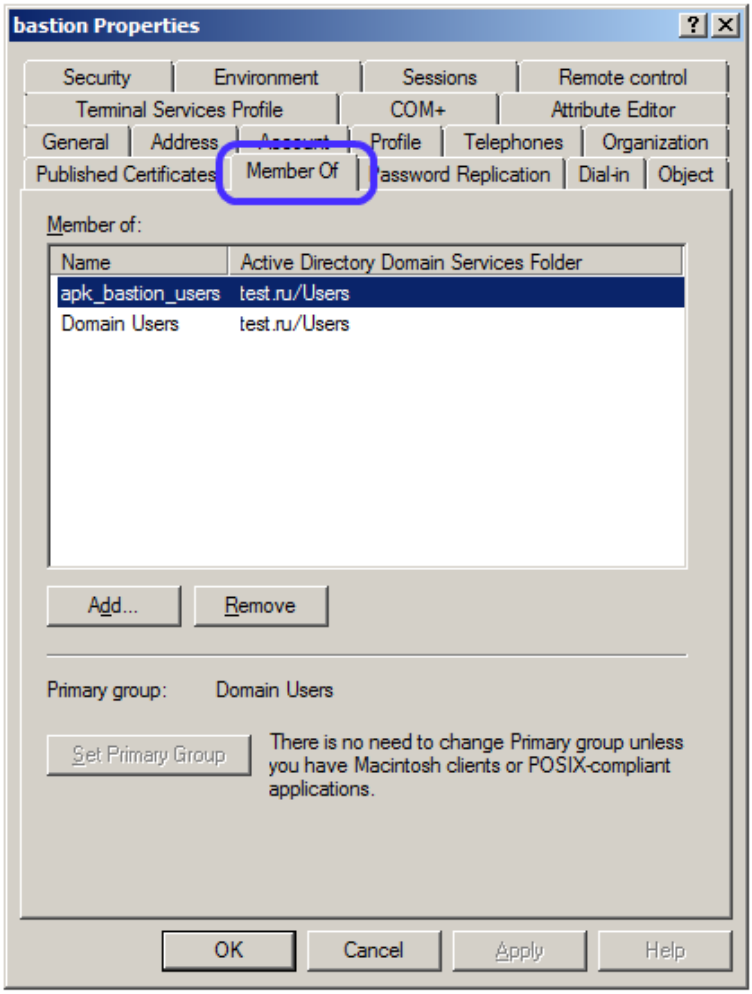


Рис. 52. Настройка членства в группах для пользователя АПК «Бастион»

Если в свойствах пользователя отображается закладка attribute editor (см. Рис. 53), то следует найти в списке атрибутов пользователя атрибуты, заранее созданные для хранения уровня полномочий и профиля пользователя АПК «Бастион». После чего необходимо:

1. Затем присвоить атрибуту, предназначенному для хранения профиля (созданного в АПК «Бастион») пользователя АПК «Бастион» символьное значение, совпадающее с именем профиля.

2. Присвоить атрибуту, предназначенному для хранения уровня привилегий пользователя АПК «Бастион» значение от 0 до 99 (необходимый уровень привилегий).

Если таких атрибутов нет, то следует:

1. Найти любой незанятый атрибут, который принимает **символьные значения** (например, sn). Это будет атрибут для хранения профиля пользователя АПК «Бастион». Присвоить этому атрибуту символьное значение, совпадающее с именем профиля АПК «Бастион», созданного в АПК «Бастион» для пользователей AD.

2. Найти любой незанятый атрибут, который принимает **числовые значения** (например, revision). Это будет атрибут для хранения полномочий оператора. Присвоить этому атрибуту необходимый уровень привилегий (число от 0 до 99).

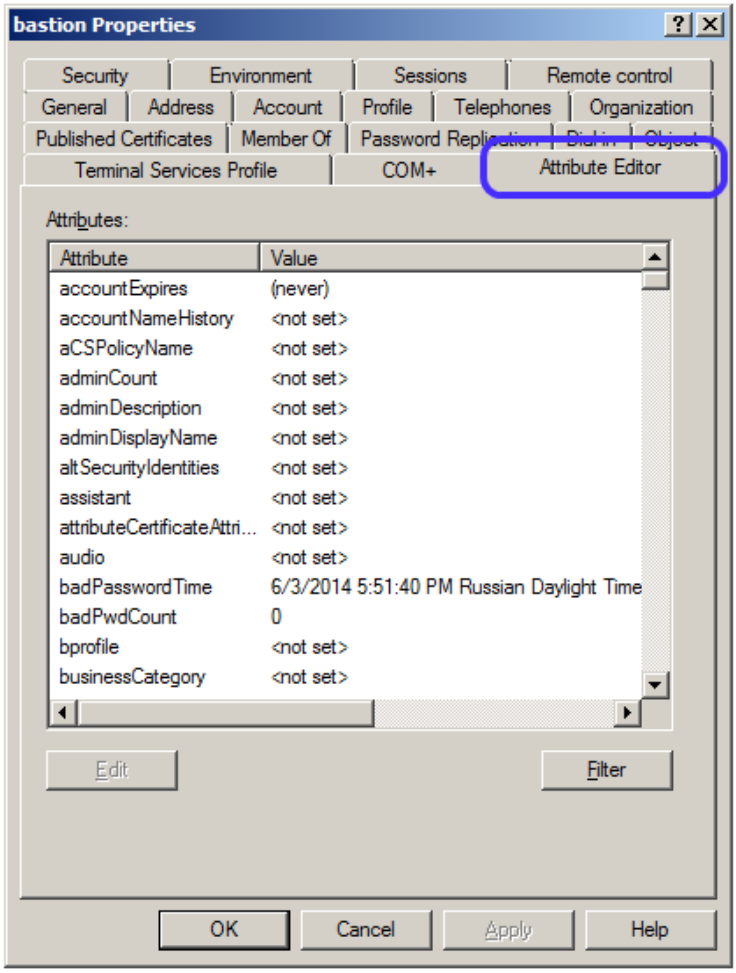


Рис. 53. Attribute Editor

Если в свойствах пользователя не отображается закладка attribute editor, тогда следует в меню «View» («Вид») выбрать опцию «Advanced features» («Расширенные возможности»). После этого attribute editor станет доступным (см. Рис. 54).

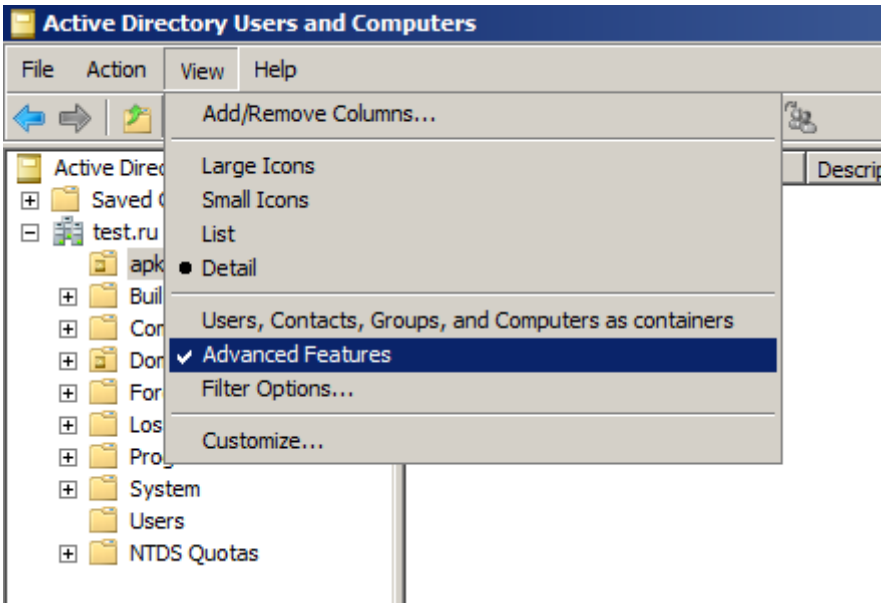


Рис. 54. Настройка отображение консоли Active Directory

После этого следует добавить рабочую станцию, где установлен АПК «Бастион» в домен Active Directory.

Затем, в общих настройках АПК «Бастион» выбрать Active Directory. Отметить флаг «Использовать идентификацию Active Directory» (см. Рис. 55).

В поле «название группы пользователей АПК Бастион» ввести название созданной группы.

В поле «Название атрибута AD для хранения профиля пользователя» ввести название атрибута AD, специально созданного или выбранного для этого ранее.

В поле «Название атрибута AD для хранения привилегий пользователя» ввести название атрибута AD, специально созданного или выбранного для этого.

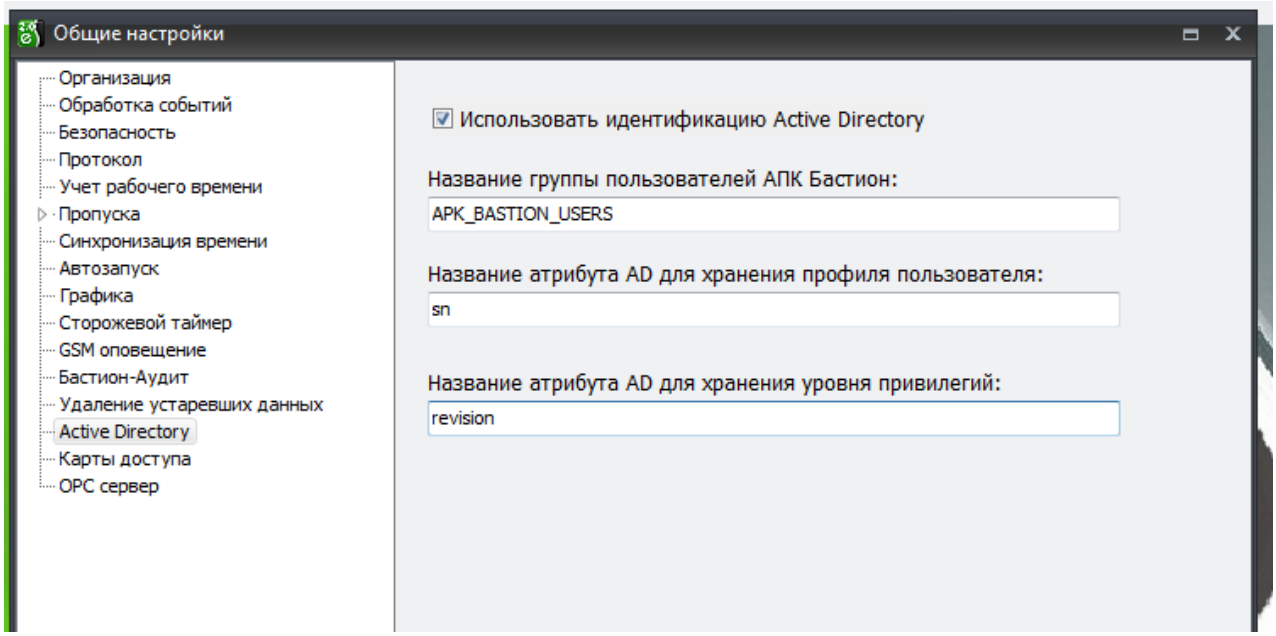


Рис. 55. Общие настройки АПК «Бастион» для Active Directory

После этого при первом запуске АПК «Бастион» в таблице OPERS должен будет появиться пользователь одноименный с пользователем Active Directory, под которым выполнен вход в систему на данной рабочей станции.

> ***Внимание!*** *Это необходимо проверить. Если после перезагрузки АПК «Бастион» не затребовал логина и пароля, следовательно, связку АПК «Бастион» и Active directory настроили корректно.*

5.5.5.3 Использование авторизации Active Directory совместно с функциями расширенной безопасности АПК «Бастион»

Для настройки совместной работы авторизации Active Directory и фукций расширенной безопасности АПК «Бастион», откройте форму "Общие настройки" в АПК «Бастион» и запустите программу настройки расширенного управления безопасностью (см. Рис. 56).

Для того, чтобы АПК «Бастион» запускался вместо проводника и использовал доменную авторизацию, следует:

1. Отметить флаг «Загружать вместо стандартной оболочки ОС». Логин и пароль оператора Бастиона не указывать.

2. Отметить флаг «использовать автологон при загрузке Windows». Там указать имя пользователя Active Directory, который будет работать на данной рабочей станции, и его пароль.

Если необходимо — можно запретить использование консолей и управляющих элементов.

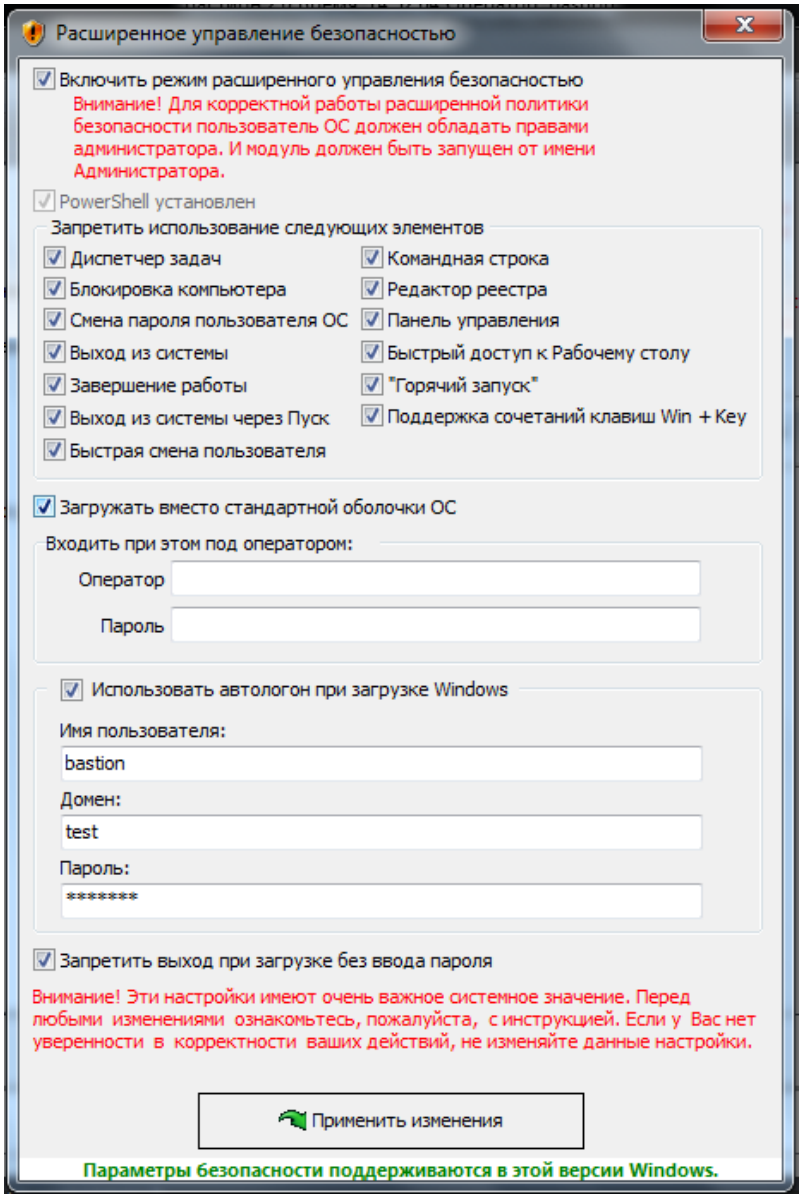


Рис. 56. Программа настройки расширенного управления безопасностью

После перезагрузки рабочей станции должен автоматически загрузиться АПК «Бастион» под оператором, одноименным с именем доменного пользователя, заданного в настройках АПК «Бастион».

6 Обслуживание баз данных

6.1 Общие сведения

АПК «Бастион» работает с двумя отдельными базами данных – основной и протокольной (файлы Bastion.GDB и Bprot.GDB соответственно, расположены в каталоге Bastion\Data).

Под обслуживанием БД понимается выполнение операций резервного копирования, восстановления из резервной копии, проверки БД на ошибки, изменения параметров БД и параметров подключения.

Для выполнения этих операций в комплект поставки АПК «Бастион» входит ряд средств:

- Утилита «Обслуживание БД» (BArchive.exe), начиная с версии 1.7.1.
- IBExpert. Универсальное средство администрирования баз данных Firebird.
- Утилита «Time To Backup», позволяющая автоматизировать процесс регулярного резервного копирования. Утилита работает как сервис Windows.
- Встроенные средства СУБД Firebird с интерфейсом командной строки.
- BDE Administrator. Утилита для установки параметров подключения к БД через BDE.

Полную резервную копию системы можно получить, создав копию каталогов <Bastion> и <Firebird>, а также ключа системного реестра HKEY_CURRENT_USER\Software\ES.

Не рекомендуется производить резервное копирование БД путём простого копирования файлов. В этом случае перед осуществлением копирования необходимо отсоединяться от базы данных, то есть полностью выгружать комплекс на всех рабочих местах. При использовании же средств СУБД резервное копирование производится в режиме online.

Ещё одним преимуществом такого способа копирования является то, что при последующем восстановлении БД регенерируются индексы, что ускоряет работу системы в целом.

Рекомендуется запланировать резервное копирование таким образом, чтобы на время копирования приходилось наименьшее число событий в системе.

> ***Внимание!*** *Не рекомендуется делать резервную копию на логический диск с базой данных – в этом случае при недостатке доступного на диске места возможно нарушение целостности исходной БД.*

Восстановление баз данных, резервные копии которых были сделаны с помощью средств СУБД (BArchive, Time To Backup или IB Expert), производится также специальными средствами.

Документация на систему Time To Backup находится в отдельном документе (Пуск – Бастион – Сервис резервного копирования – Документация).

6.2 Использование утилиты «Обслуживание БД» (BArchive.exe)

6.2.1 Основные понятия и принцип работы

Программа «Обслуживание баз данных АПК «Бастион» предназначена для резервирования, восстановления и архивирования баз данных АПК «Бастион», а также для изменения пароля пользователя в Firebird, под которым работает АПК «Бастион».

Осуществлять резервирование можно с любого рабочего места системы, на котором установлен АПК «Бастион». Тем не менее, рекомендуется выполнять его на сервере баз данных, чтобы не загружать сеть. Резервирование осуществляются в «горячем» режиме, т.е. для его выполнения не нужно останавливать службу сервера СУБД Firebird и выгружать «Бастион» на всех рабочих станциях.

> ***Внимание!*** *Для выполнения процедур резервирования, восстановления и архивирования необходимо, чтобы пользователь Windows имел права на создание каталогов на логических дисках.*

6.2.2 Резервирование и восстановление баз данных

Для выполнения операций резервирования, восстановления или архивирования необходимо:

1. Запустить утилиту BArchive.exe из меню «Пуск – Программы – Бастион – Администрирование – Обслуживание БД». Откроется форма «Обслуживание баз данных АПК «Бастион» (Рис. 57).

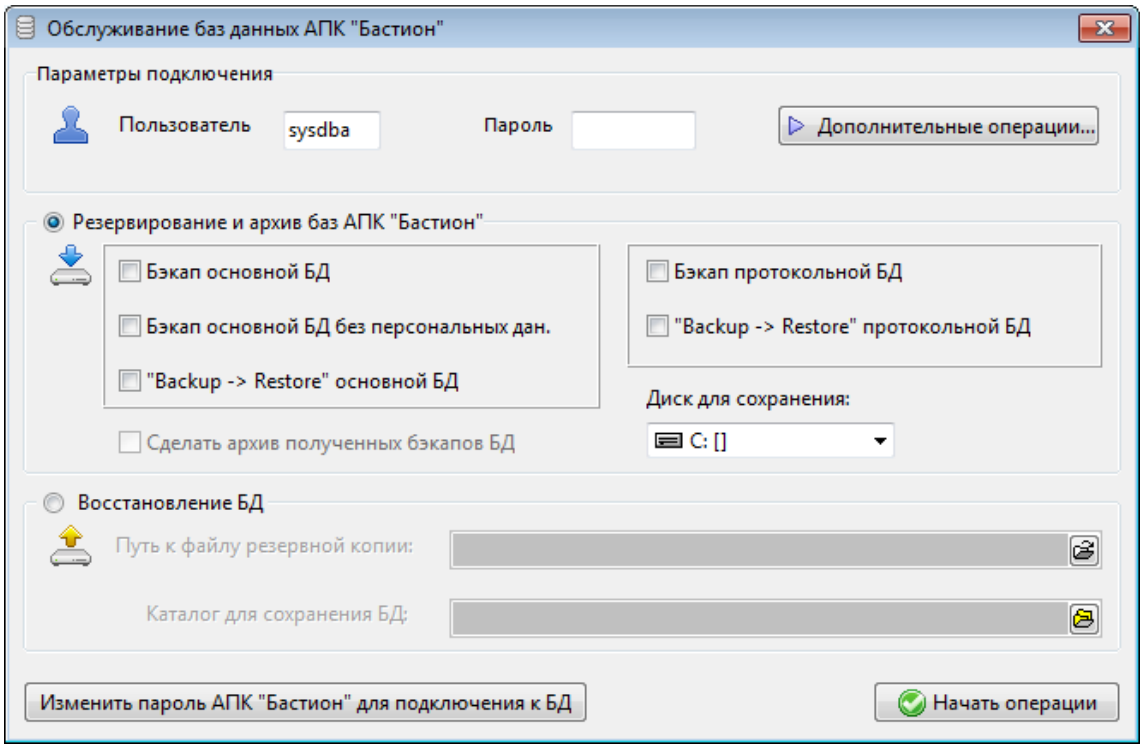


Рис. 57. Форма «Обслуживание баз данных АПК «Бастион»

2. Ввести имя и пароль для подключения к базам данных (в верхней части формы на Рис. 57). Путь к базам данных считывается из конфигурации BDE (можно посмотреть в BDE Administrator).

3. В открывшейся форме выбрать функции, которые требуется выполнить. В приложении реализованы следующие операции:
   - «Бэкап основной БД» – снятие резервной копии основной базы данных «Бастиона»;
   - «Бэкап основной БД без фото сотрудников» – снятие резервной копии основной базы данных с удалением фотографий сотрудников;
   - «Бэкап протокольной БД» – снятие резервной копии протокольной базы данных «Бастиона»;
   - «Сделать архив полученных Бэкапов БД» – помещает в архив полученные файлы резервных копий;
   - «Backup - Restore» основной БД» – выполняет процедуру резервного копирования с последующим восстановлением основной базы данных. Эту процедуру необходимо выполнять в профилактических целях, поскольку она очищает базу от лишнего «мусора», восстанавливает индексы;
   - «Backup - Restore» протокольной БД» - выполняет процедуру резервного копирования последующим восстановлением резервной базы данных;
   - «Восстановить БД» - восстанавливает базу данных из резервной копии. В поле «Путь к файлу резервной копии» необходимо указать путь к файлу резервной копии, а в поле «Каталог для сохранения БД» указать папку, в которой сохранится восстановленная база данных;
4. Указать «Диск для сохранения» – логический диск, на котором будет создана папка «Backup_<текущая дата>», где будут сохраняться файлы резервных копий.
5. Нажать на кнопку «Начать операции». После этого появится консольное окно, показывающее процесс выполнения (Рис. 58).

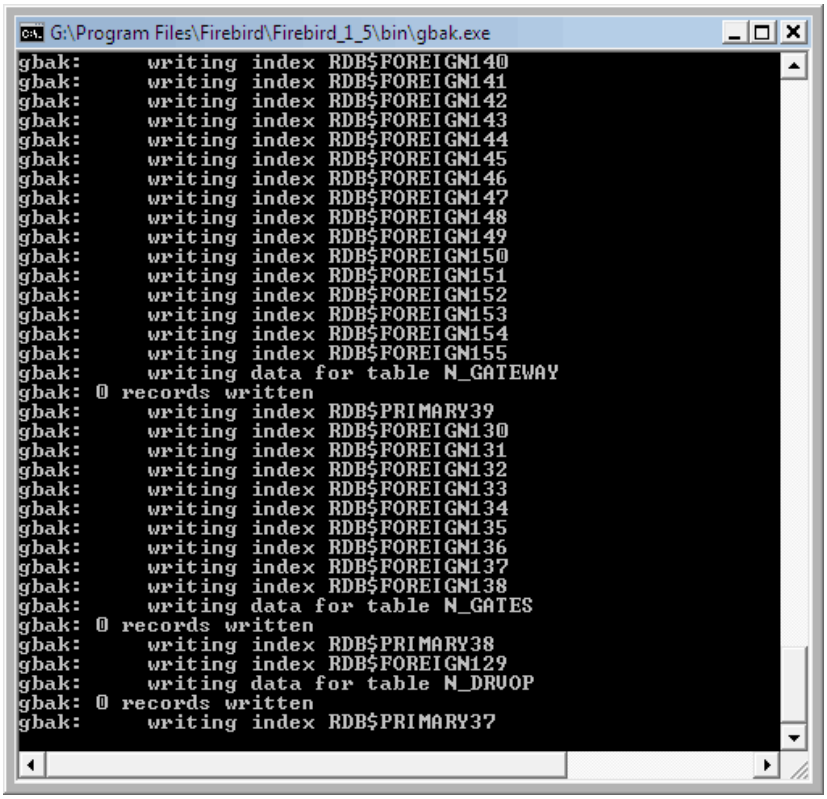


Рис. 58. Консольная форма

6. По окончании выполнения операций консольное окно закроется автоматически, и поле «Результат» отобразит результат (Рис. 59). Этот результат также сохраняется в папке <Диск для сохранения>:\Backup_(текущая дата).

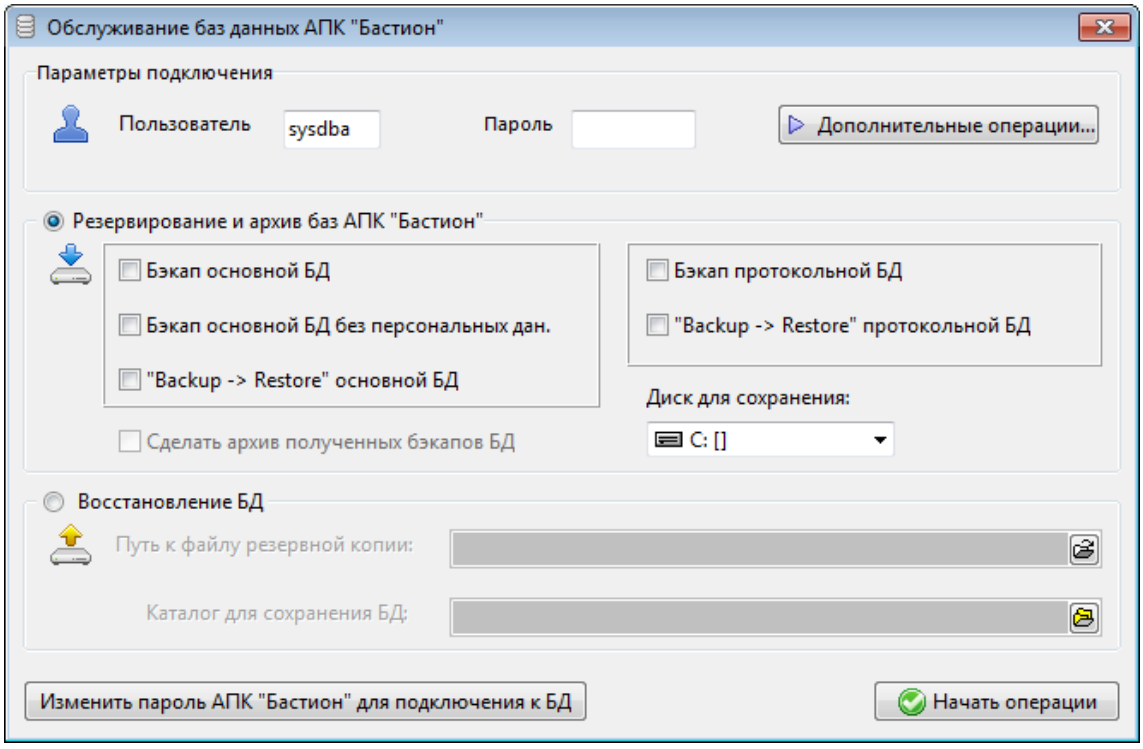


Рис. 59. Форма «Обслуживание баз данных АПК «Бастион» с результатом выполненных операций

6.2.3 Если карта числится выданной, но никому не принадлежит

Иногда бывают ситуации, когда карту не получается выдать – бюро пропусков АПК «Бастион» выдает ошибку, что карта выдана другому лицу, хотя глобальным поиском ее найти не удается. Такие карточки накапливаются в базе данных Бастиона вследствие непрерывной работы и подлежат фиксации и возврату в обращение.

С помощью утилиты обслуживая БД можно сделать такие карты не активными и использовать повторно.

Для этого нужно нажать кнопку «Дополнительные операции», после чего нажать кнопку «Выполнить» в группе «Возврат неиспользуемых карт в обращение».

6.2.4 Если подразделение пустое, а удалить его невозможно

Вследствие непрерывной работы АПК «Бастион» в бюро пропусков пустые подразделения не всегда получается удалить – возникает ошибка, что «В подразделении числится 1 или более сотрудников».

С помощью утилиты обслуживая БД можно удалить такие подразделения, проведя перед этим безопасную очистку таблицы PERSON.

Для этого нужно нажать кнопку «Дополнительные операции», после чего нажать кнопку «Выполнить» в группе «Удаление пустых подразделений». Будет выполнена очистка таблицы «PERSON» без повреждения имеющихся данных, после чего зависшие подразделения можно удалить.

Все операции по обслуживанию можно производить с любой рабочей станции АПК «Бастион» при условии верно введенного пароля пользователя SYSDBA.

6.2.5 Удаление дубликатов в архиве разовых пропусков

Если одному и тому же посетителю в разное время выдавалось несколько разовых пропусков, то информация о каждом пропуске хранится в архиве БД Бюро пропусков. В окне списка пропусков на странице «Архив» каждый такой пропуск будет отображаться отдельной строкой.

Чтобы оставить в архиве данные только о последнем выданном пропуске, можно воспользоваться специальной функцией. Для этого в окне «Дополнительные операции» необходимо нажать кнопку «Выполнить» в группе «Удаление дубликатов в архиве разовых пропусков».

6.2.6 Удаление дубликатов словарных значений

Если в процессе эксплуатации системы в словарях появились дубликаты словарных значений, то необходимо избавиться от них. Для этого нужно нажать на кнопку «Дополнительные операции». В открывшейся форме из выпадающего списка выбрать «Удаление дубликатов в словарях с заменой табельных номеров» или «Удаление дубликатов в словарях без замены табельных номеров». В первом случае, организации, имеющие одинаковое название, объединятся в одну, а конфликты по табельным номерам разрешаться формированием новых значений для конфликтующих табельных номеров. Во втором случае, организации, имеющие одинаковое название, будут переименованы. К названию добавится ключевое слово «Дубль».

6.2.7 Выполнение произвольных скриптов на БД АПК «Бастион»

В окне дополнительных операций также имеется возможность выполнить произвольные скрипты на основной или протокольной базе данных АПК «Бастион».

Текст скрипта можно скопировать из буфера обмена, либо набрать вручную. Команды в скрипте должны разделяться через «;». Скрипт не должен содержать конструкций SET TERM и COMMIT.

6.3 Использование IBExpert для обслуживания БД

6.3.1 Настройка среды IBExpert

Рекомендуется выполнить ряд общих настроек перед началом работы в IBExpert.

Для русификации пользовательского интерфейса выберите пункт меню «Options – Environment Options». В поле «Interface Language» выберите Russian и нажмите ОК.

Рекомендуется в том же окне установить также опции:

Версия сервера по умолчанию – Firebird 1.5.

Default Character set – WIN1251.

6.3.2 Регистрация БД в IBExpert

Для работы с базами данных в IB Expert, их необходимо предварительно зарегистрировать.

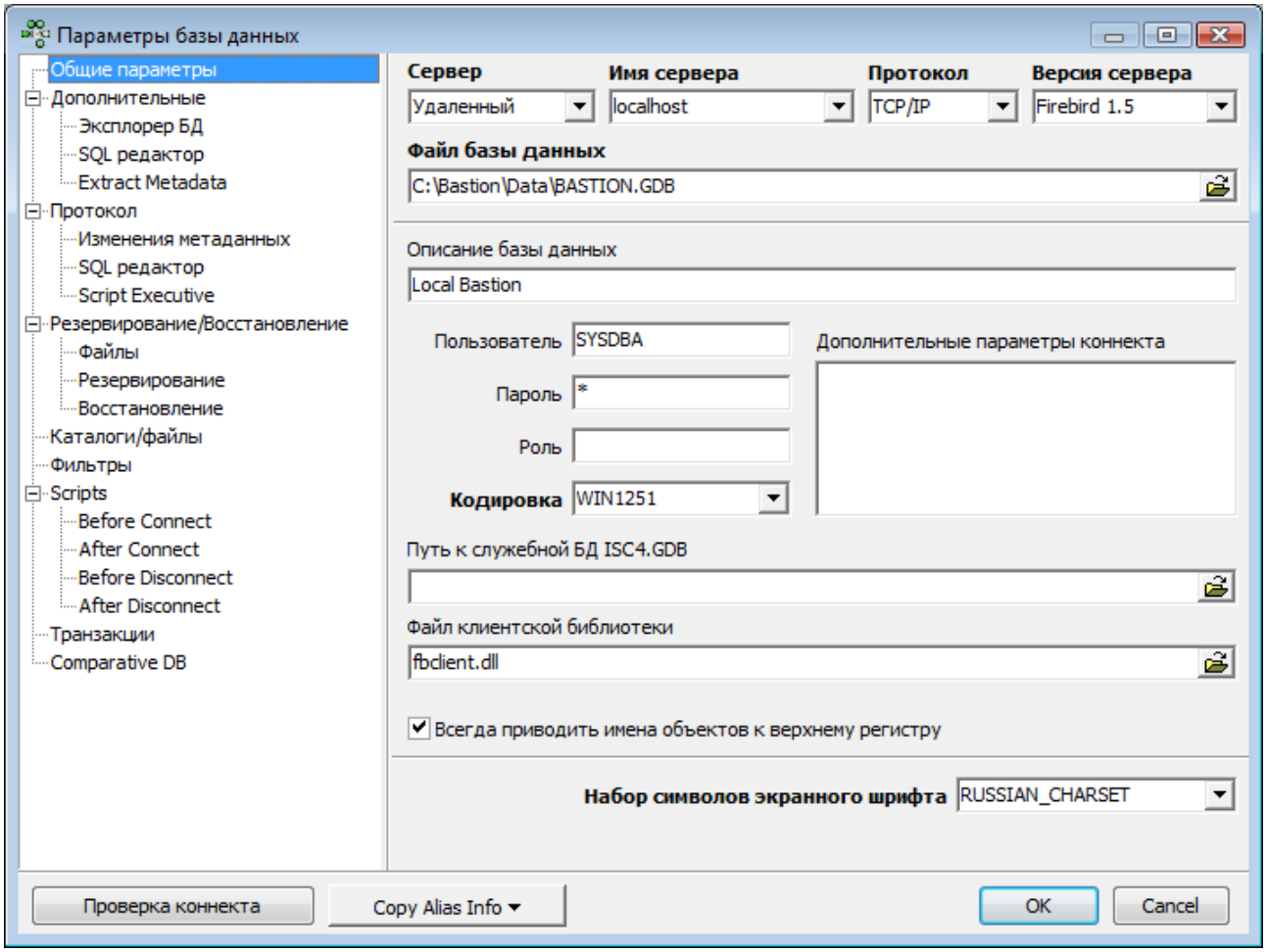


Рис. 60. Окно регистрационной информации базы данных IB Expert

Для этого нажмите в левой части главного окна IB Expert сочетание клавиш «Shift+Alt+R» и укажите в появившемся окне (Рис. 60) следующие параметры:

Сервер. Локальный – если БД располагается на локальном компьютере, Удаленный – если на удалённом. В случае удалённого сервера также необходимо указать его имя и протокол TCP/IP.

> ***Внимание!*** *В Windows Vista и выше всегда следует указывать Удаленный сервер. Если БД расположена локально, в качестве имени сервера введите localhost (Рис. 60).*

Версия сервера – для версий Бастиона, начиная с 1.5.368.1, следует устанавливать Firebird 1.5, для более ранних – Firebird 1.0.

Файл базы данных. Путь к файлу с БД.

Описание базы данных. Имя, под которым будет зарегистрирована БД, например, «Бастион» или «Протокол».

Пользователь, пароль. Имя пользователя и пароль для доступа к БД. Следует использовать имя и пароль администратора Firebird Server (по умолчанию при установке АПК «Бастион» - SYSDBA, «masterkey»).

Кодировка. WIN1251.

Font Characters Set. RUSSIAN_CHARSET.

После заполнения данных полей нажмите кнопку «Register».

Вы можете ввести большинство параметров по умолчанию в окне «Настройки – Настройки среды». В дальнейшем эти параметры будут использоваться при регистрации всех БД.

6.3.3 Резервное копирование БД

Резервное копирование может производиться при работающем АПК «Бастион».

Для выполнения резервного копирования в IBExpert необходимо:

1. Выбрать пункт меню «Службы – Резервирование базы данных».
2. Выбрать базу данных из списка зарегистрированных в IBExpert.
3. Указать файл резервной копии (*.fbk, *.gbk).
4. Установить опции резервирования, как показано на Рис. 61.
5. Нажать кнопку «Начать резервное копирование».

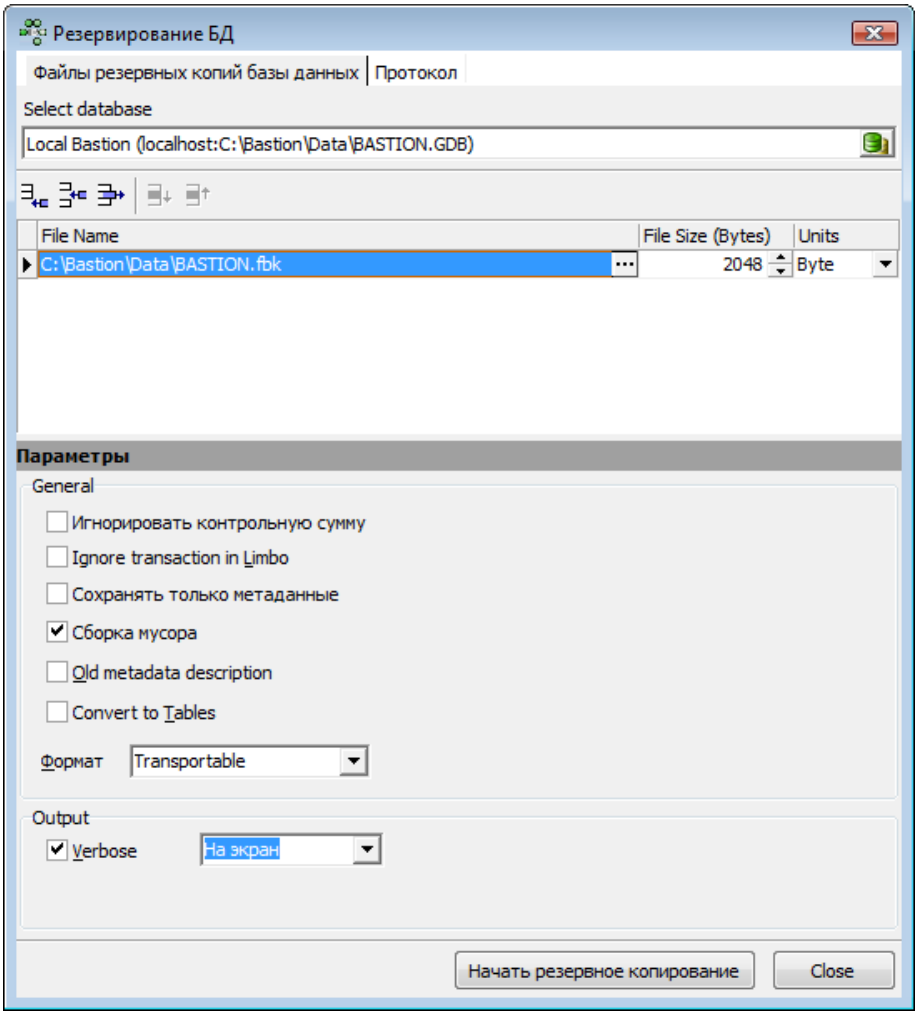


Рис. 61. Окно резервирования БД

6.3.4 Восстановление БД

Перед выполнением восстановления базы данных (любым способом) необходимо полностью выгрузить «Бастион» на всех рабочих местах.

Для восстановления БД необходимо загрузить IB Expert и выбрать пункт меню «Службы→Восстановление базы данных». БД можно восстановить поверх уже существующего файла (опция Restore into existing database), либо в новый файл (Restore into new database). В первом случае базу данных необходимо предварительно зарегистрировать.

> ***Внимание!*** *Перед восстановлением поверх существующего файла убедитесь в наличии рабочей резервной копии!*

В поле «File Name» необходимо указать путь к файлу с резервной копией.

Размер страницы указывать не менее 4096 (рекомендуется указывать значение, равное размеру кластера на жёстком диске). Остальные параметры следует оставить со значениями по умолчанию.

Для запуска процедуры нажмите кнопку «Start Restore» и введите имя и пароль доступа к БД с необходимыми полномочиями.

Если вы выбирали вариант восстановления в новый файл, то после завершения операции скопируйте его на место старого. После этого программа готова к запуску. Более подробную информацию о возможностях восстановления БД смотрите в документации на СУБД.

6.3.5 Изменение параметров БД

Каждая БД обладает набором параметров, определяющих режим работы с ней. Наиболее существенным для надежности системы является режим записи данных – синхронный или асинхронный.

Синхронный режим (Forced Writes) предполагает, что данные, записываемые в БД, не будут кэшироваться системой, а сразу же записываться на жесткий диск. Данный режим гарантирует, что при нештатном выключении питания или некорректном выходе из программы не произойдет разрушения базы данных. В то же время, использование данного режима снижает общую производительность системы, в частности, скорость обработки событий. Синхронный режим включен по умолчанию для обеих БД.

Асинхронный режим не гарантирует сохранности БД при нештатных выключениях, однако обеспечивает высокую скорость работы.

> ***Внимание!*** *Перед изменением параметров БД необходимо отключиться от нее (выйти из Бастиона на всех компьютерах системы).*

Для переключения режима записи можно использовать IB Expert. Необходимо зарегистрировать БД, как описано выше, а затем выбрать пункт меню «Службы→Параметры базы данных». В строке «Database» следует указать зарегистрированную БД. Для включения синхронного режима необходимо установить флаг «Forced Writes» и нажать кнопку «ОК».

6.3.6 Проверка баз данных

Проверка базы данных позволяет определить наличие ошибок в структуре БД. Ошибки в БД могут возникать по причинам нештатных отключений питания, принудительной остановке сервера БД, при аппаратных сбоях и др. (Подробнее, см. документ «Руководство по восстановлению баз данных»).

> ***Внимание!*** *Операция проверки БД требует эксклюзивного подключения к БД. Для этого необходимо выйти из АПК «Бастион» на всех рабочих станциях.*

Для выполнения проверки БД в IBExpert выберите пункт меню «Службы – Проверка БД». Установите параметры так, как показано на Рис. 62.

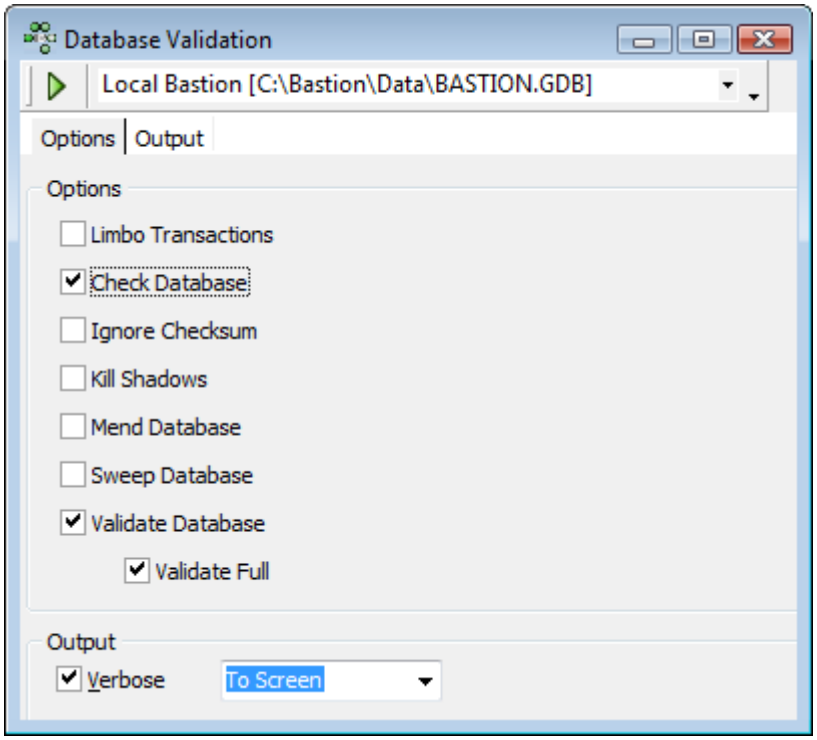


Рис. 62. Параметры проверки БД

Нажмите кнопку “Start Validation” в левом верхнем углу. Будет выведен запрос имени и пароля для подключения к БД. Введите имя и пароль для SYSDBA.

Результаты проверки будут отображены на странице Output.

6.3.7 Менеджер пользователей

Менеджер пользователей IB Expert предназначен для редактирования учетных записей пользователей СУБД Firebird. Для его запуска выберите пункт меню «Инструменты – Менеджер пользователей» и введите пароль пользователя SYSDBA (после установки АПК «Бастион» этот пароль «masterkey»). После этого отобразится список имеющихся на сервере пользователей (Рис. 63).

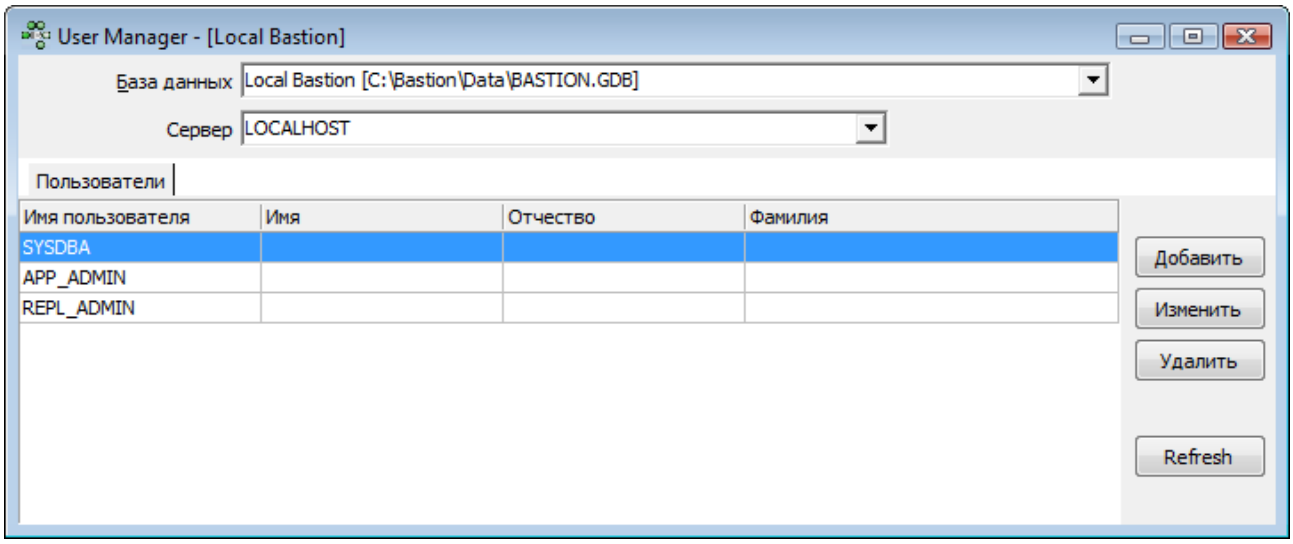


Рис. 63. Менеджер пользователей IB Expert

Для изменения данных пользователя выберите его в списке и нажмите кнопку «Изменить».

> ***Внимание!*** *В целях безопасности рекомендуется сменить пароль SYSDBA после установки системы.*

6.4 Установка паролей для доступа к базам данных

Для доступа к базам данных АПК «Бастион» использует учетную запись APP_ADMIN. Пароль для этой учетной записи запрашивается при установке системы. В дальнейшем его также можно изменить. По умолчанию используется пароль Lhj7Rfsa.

Пароль для подключения к БД хранится на каждом рабочем месте АПК «Бастион» в системном реестре в зашифрованном виде. При отсутствии соответствующего ключа в реестре, АПК «Бастион» запрашивает пароль при запуске.

Для изменения пароля учетной записи APP_ADMIN необходимо:

1. Сменить пароль на сервере БД с помощью IBExpert (см. п. 6.3.7).
2. Ввести новый пароль на каждом рабочем месте АПК «Бастион» при помощи утилиты «Обслуживание БД».

Для выполнения последней операции запустите утилиту BArchive.exe из меню «Пуск – Программы – Бастион – Администрирование – Обслуживание БД». Откроется форма «Обслуживание баз данных АПК «Бастион» (см. Рис. 57).

Нажмите кнопку «Изменить пароль АПК «Бастион» для подключения к БД». Откроется форма с запросом старого пароля (Рис. 64).

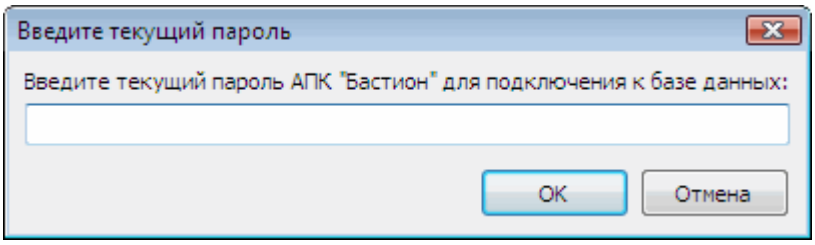


Рис. 64 – Форма с запросом старого пароля

Здесь необходимо указать старый пароль и нажать на кнопку «ОК». После этого, если пароль введен верно, откроется окно для ввода нового пароля (Рис. 65).

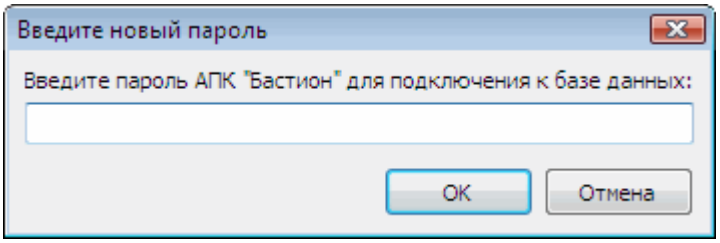


Рис. 65 – Форма с запросом нового пароля

Здесь необходимо указать новый пароль и нажать на кнопку «ОК».

Внимание! *Если вы смените пароль на сервере БД и не выполните операцию по его изменению на рабочих станциях – АПК «Бастион» загружаться не будет!*

6.5 Конфигурация сервера Firebird вручную

Если по каким-либо причинам Вы не устанавливали сервер Firebird с помощью программы установки «Бастион», то для работы системы необходимо выполнить следующие действия по конфигурации сервера.

Для работы программ Бастиона необходимо создать пользователя базы данных с именем **APP_ADMIN (**пароль по умолчанию – **Lhj7Rfsa)**. Вы можете изменить пароль пользователя APP_ADMIN. Для того чтобы АПК «Бастион» использовал новый пароль, необходимо ввести его в утилите «Обслуживание БД» (BArchive.exe). Новый пароль потребуется ввести на всех компьютерах комплекса.

Для работы программного обеспечения необходимо, чтобы сервер Firebird был настроен на использование протокола TCP/IP. Для этого необходимо наличие следующей строки в файле services:

```
gds_db      3050/tcp
```

Этот файл находится в каталоге <Windows>\System32\Drivers\Etc.

6.6 Конфигурация BDE вручную

Если по каким-либо причинам Вы не устанавливали BDE с помощью программы установки «Бастион» или неправильно указали при установке пути к БД, то для работы системы необходимо выполнить следующие действия по конфигурации псевдонимов (алиасов) BDE.

Для настройки BDE предназначена утилита BDE Administrator, вид которой представлен на Рис. 66 (находится в «Панели управления» Windows).

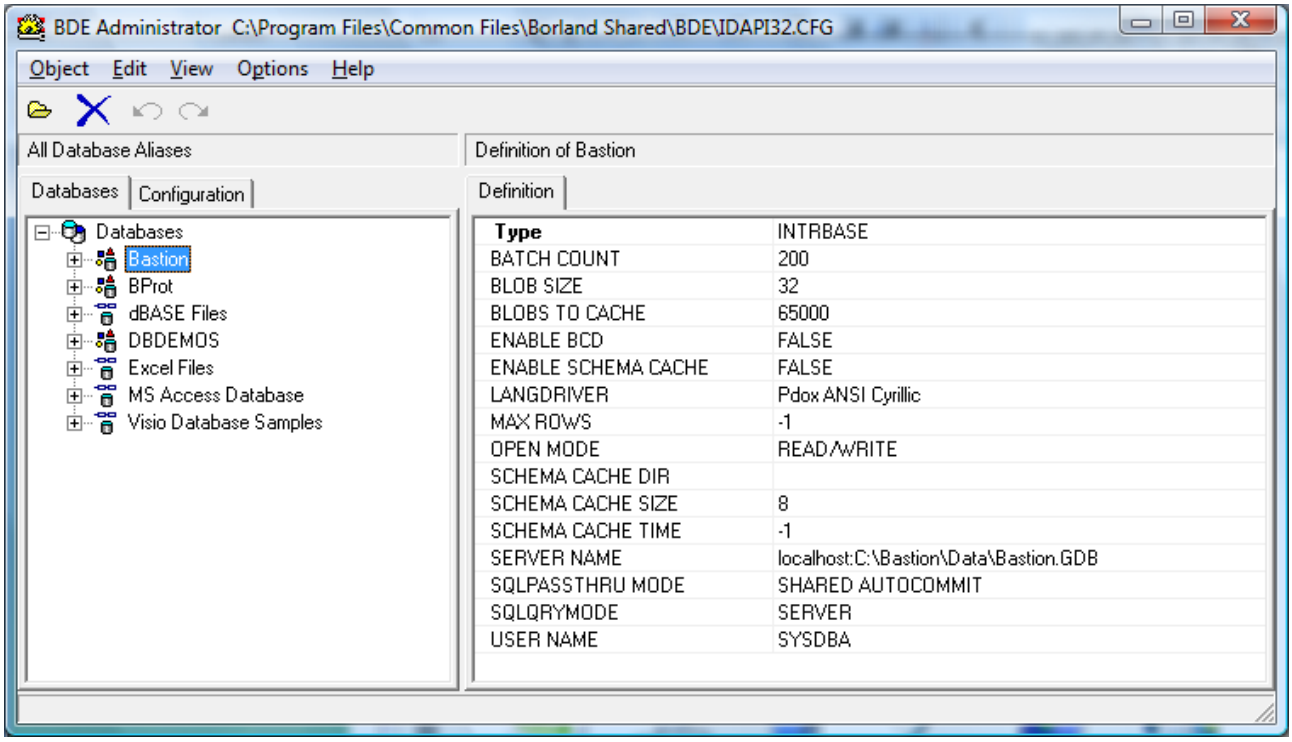


Рис. 66. Настройка псевдонима в BDE Administrator

Для правильной работы программ необходимо создать псевдонимы баз данных в BDE с именами **Bastion** и **Bprot** (если их нет в списке (Рис. 66))**,** а также проверить конфигурацию системных параметров BDE.

Для выполнения настройки псевдонимов выполните следующие действия:

1. Из панели управления запустите BDE Administrator (на ОС Windows 8 или выше BDE Administrator следует запускать от имени администратора).
2. Создайте псевдонимы (меню **Object→New**) с именами **Bastion** и **BProt**. Установите Database Driver Name в INTRBASE.
3. Установите для псевдонимов следующие параметры:

Type	INTRBASE
LANGDRIVER	Pdox ANSI Cyrillic
SQLPASSTHRU MODE	SHARED AUTOCOMMIT
SQLQRY MODE	Server
SERVER NAME	Путь к файлу базы данных в формате: **Имя сервера:путь к файлу** (например: server:c:\bastion\data\bastion.gdb).

BLOBS TO CACHE	65000

Также необходимо установить следующие параметры на странице **Configuration**:

System\INIT\LOCAL SHARE	TRUE
System\INIT\LANGDRIVER	<пусто>
System\INIT\Formats\Date\FOURDIGITYEAR	TRUE
System\INIT\Formats\Date\MODE	1
System\INIT\Formats\Time\TWELVEHOUR	FALSE
Drivers\Native\DBase\LANGDRIVER	dBASE RUS cp866
Drivers\Native\Paradox\LANGDRIVER	Pdox ANSI Cyrillic

7 Обновление системы

7.1 Добавление новых компонент

Объём лицензии, или набор программных модулей и драйверов определяется информацией, записанной в ключе аппаратной защиты (HASP). Программирование ключа HASP производится утилитой LicenseManager.exe, входящей в комплект поставки программного комплекса («Пуск-Программы-Бастион-Администрирование-Менеджер лицензий HASP»).

Работа с утилитой LicenseManager.exe описана в инструкции «Менеджер лицензий HASP. Руководство пользователя».

7.2 Обновление версии программного обеспечения

При обновлении версии программного обеспечения необходимо строго следовать инструкциям по обновлению для конкретной версии. В случае необходимости, рекомендуется проконсультироваться со службой технической поддержки АПК «Бастион», так как в зависимости от номера используемой версии может различаться порядок действий.

Как правило, при установке новой версии требуется провести обновление баз данных. Перед обновлением баз данных обязательно следует закрыть все приложения комплекса «Бастион» на всех рабочих станциях и сделать резервные копии баз данных.

Обновление осуществляется при помощи SQL-скриптов, поставляемых вместе с новой версией. Файлы скриптов находятся на дистрибутивном диске в каталоге «<CD>\Install\Updates», а также в каталоге, где установлен Бастион («<Bastion>\Updates»).

Скрипты имеют имена вида: bastion_XXX.sql, bprot_XXX.sql, pcn_XXX.sql.

где XXX – номер версии, до которой производится обновление. Первые предназначены для базы данных Bastion.GDB, вторые – для Bprot.GDB, третьи – для Pcn.GDB.

Обновление можно производить с помощью специальной программы DBPatch.exe («Пуск–Программы–Бастион–Администрирование–Обновление баз данных») или с помощью утилиты IB Expert.

7.2.1 Обновление БД с помощью программы DBPatch

Эта программа позволяет в автоматизированном режиме выполнить все необходимые обновления баз данных.

> ***Внимание!*** *Программа обновляет те базы данных, на которые установлен текущий путь алиаса (псевдонима BDE). Перед обновлением не забудьте сделать резервную копию.*

При запуске программы DBPatch необходимо ввести имя и пароль для подключения к базе данных.

Для запуска обновления необходимо указать следующее:

Обновить базы данных. Указываются БД, которые следует обновить. По умолчанию обновляются основная БД, протокольная БД и БД ПЦН.

Путь к файлам обновлений. Каталог, где лежат файлы с обновлениями. По умолчанию – каталог запуска программы DBPatch. Файлы обновлений должны располагаться в каталогах, имя которых равно соответствующей версии. Например, файлы скриптов для версии 1.4.356.1 должны лежать в каталоге «1.4.356.1».

Версия установленной БД. Версия программы, с которой производится обновление. Программа попытается определить текущую версию самостоятельно. Версию можно посмотреть в окне «О Программе» Бастиона. Если вашей версии нет в списке, значит надо выбрать версию с ближайшим меньшим номером.

Новая версия БД. Версия, на которую производится обновление. По умолчанию – последняя версия.

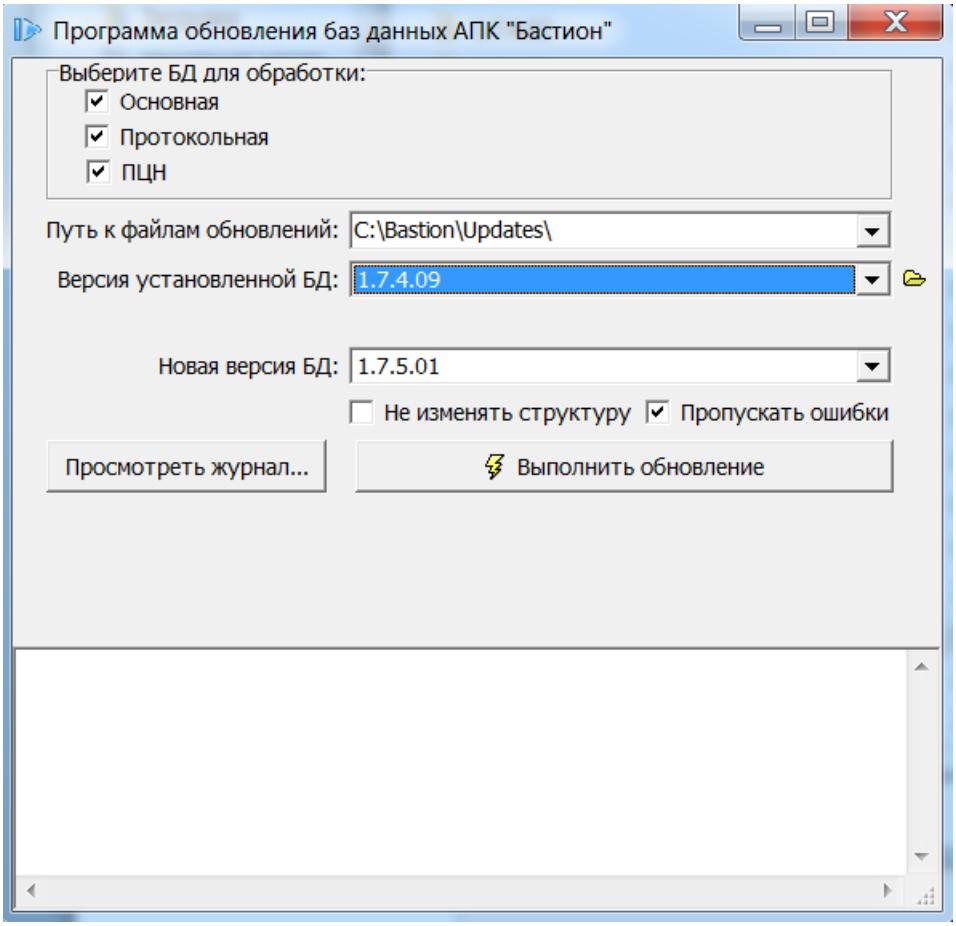


Рис. 67. Окно программы DBPatch

Флаг «*Не изменять структуру*» предназначен для того, чтобы не менять структуру БД, но выполнять команды вставки, изменения и удаления данных. Не включайте этот флаг, если точно не уверены в своих действиях.

После того, как вы указали все требуемые параметры, нажмите кнопку «Выполнить обновление». В нижней части окна будет отображаться ход операции. Операция обновления может занять несколько минут.

Если программе не удается выполнить какой-либо скрипт, будет выведено соответствующее сообщение. В этом случае обращайтесь в службу технической поддержки (необходимо будет точно сказать текст сообщения об ошибке и номер выполняемого скрипта). Все сообщения об ошибках будут сохранены в файл dbpatch.log. Этот файл можно просмотреть, нажав кнопку «Просмотреть журнал».

7.2.2 Обновление БД с помощью IB Expert

Скрипты необходимо выполнять в порядке возрастания их версии. Так, например, если требуется обновить систему с версии 1.4.0.310 до версии 1.4.0.312, то следует сначала выполнить скрипт bastion_311.sql, а затем bastion_312.sql.

Чтобы узнать номер версии ПО, следует выбрать пункт меню «Справка→О программе». Информацию об установленных компонентах можно получить, нажав кнопку «Установленные компоненты».

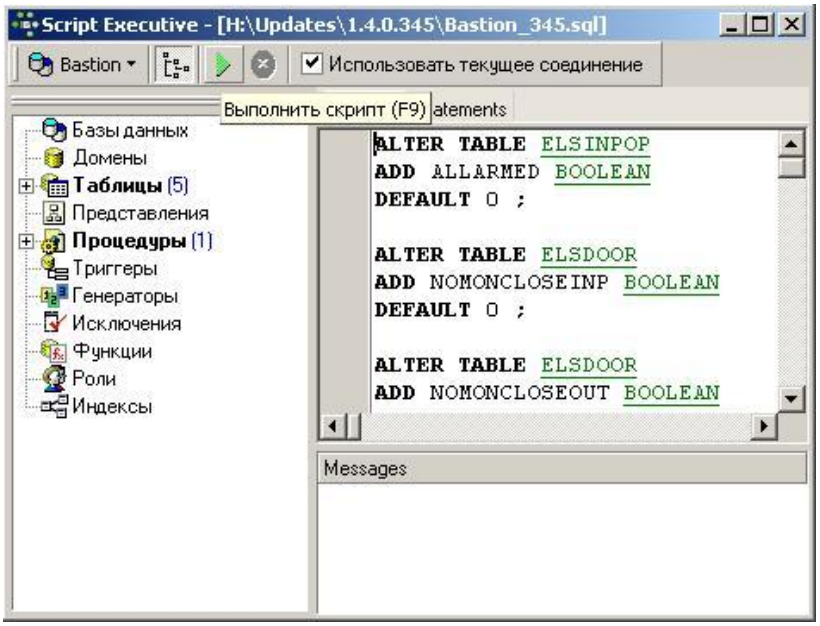


Рис. 68. Окно выполнения скрипта

Перед выполнением скрипта зарегистрируйте требуемую базу данных в IB Expert (см. п. 6.3.1) и откройте её двойным щелчком мыши по названию БД. Для вызова диалогового окна выполнения скриптов нажмите Ctrl+F12. В появившемся окне установите флаг «Использовать текущее соединение». Загрузите файл скрипта в редактор, выбрав в его контекстном меню пункт «Загрузить из файла».

Для выполнения скрипта нажмите кнопку «  » (Рис. 68). По завершении выполнения скриптов программа выведет соответствующее сообщение. После этого всё готово для запуска новой версии. Рекомендуется после каждого выполненного скрипта отключаться от базы данных и подключаться заново.

Если в процессе выполнения скриптов возникают ошибки, обращайтесь в службу технической поддержки.

7.2.3 Сравнение структуры базы данных с эталонной базой

Иногда при обновлении базы данных возникают ошибки. В этом случае рекомендуется выполнить сравнение структуры рабочей базы с эталонной, взятой из дистрибутива соответствующей версии.

Для сравнения необходимо:

1. Выгрузить Бастион на всех рабочих местах.
2. Восстановить базу данных из резервной копии, сделанной перед неудачной попыткой обновления.
3. Скопировать эталонную базу той же версии, что и рабочая с дистрибутива ПО Бастион (дистрибутив\Install\Database\Bastion.gdb) в какой-либо каталог (например c:\Etalon\Bastion.gdb).

4. Зарегистрировать обе базы в IBExpert, установить флаг «Use UPDATE instead of DESCRIBE» в регистрационной информации БД, чтобы IB Expert генерировал правильный скрипт для описаний:

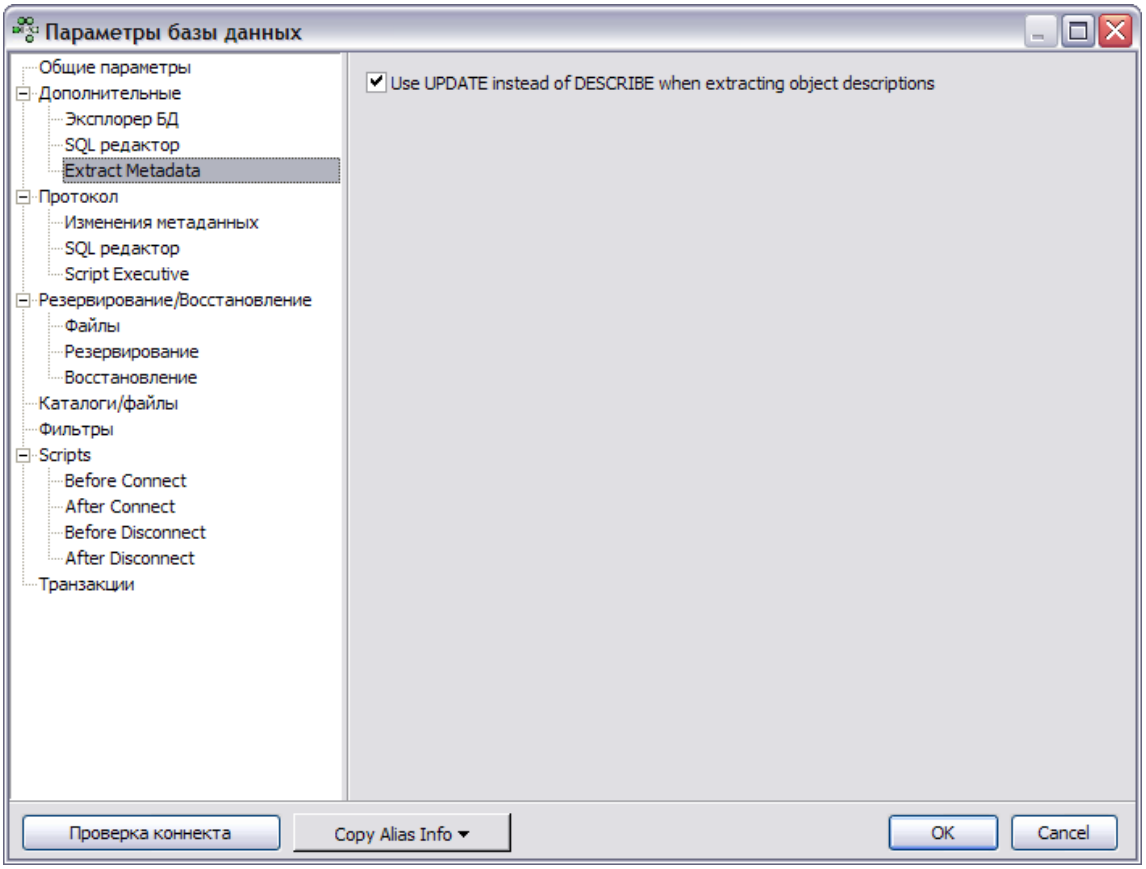


Рис. 69. Установка флага «Use UPDATE instead of DESCRIBE»

5. Выбрать в меню Tools пункт Database Comparer.
6. В появившемся диалоге указать сравниваемые базы (в верхней строке – эталонную, в нижней – рабочую), и запустить сравнение.
7. Результатом сравнения будет скрипт, который необходимо выполнить на рабочей базе, чтобы её структура соответствовала эталонной. После выполнения скрипта должно появиться сообщение об успешном выполнении.
8. Повторить шаги 2-6 для протокольной базы (BProt.GDB).
9. Повторить шаги 2-6 для базы данных ПЦН (PCN.GDB).
10. Провести обновление баз до новой версии с помощью программы DBPatch.

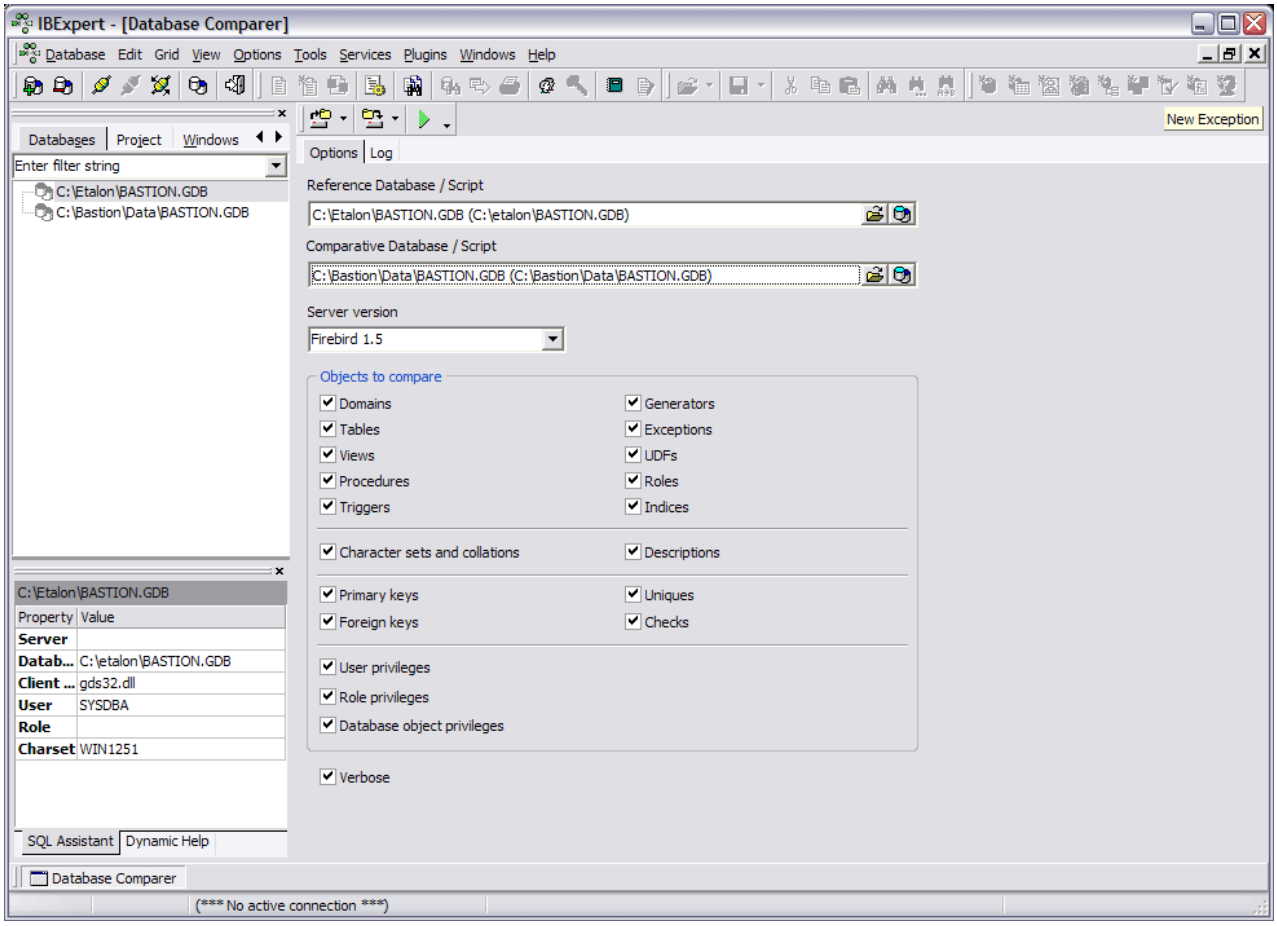


Рис. 70. Сравнение БД с эталонной

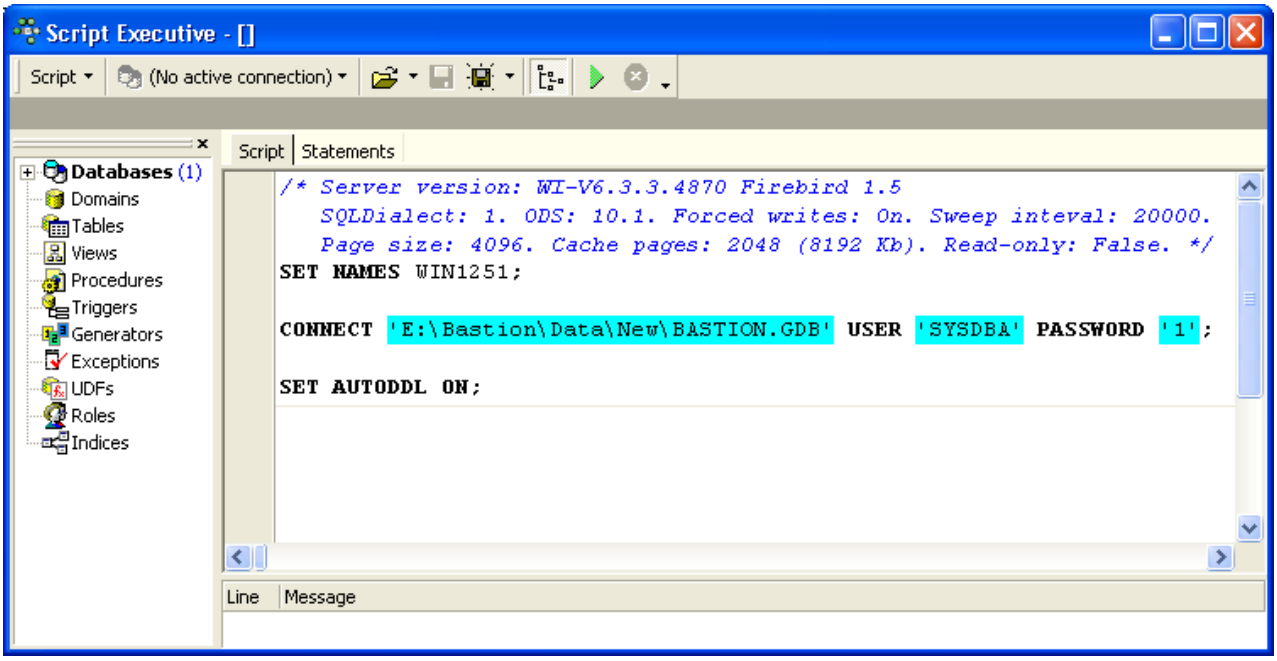


Рис. 71. Скрипт – результат сравнения БД

8 Отладочный сервис АПК «Бастион»

8.1 Общие сведения

Начиная с версии 1.7.4, в комплект поставки АПК «Бастион» входит отладочный сервис (NDebugSvc) для протоколирования отладочных сообщений системы.

Все сообщения, выводимые через отладочный сервис, могут записываться в файлы (по умолчанию – выключено).

Отладочный сервис может автоматически переименовывать или удалить лог-файлы при достижении ими заданного размера.

По умолчанию, лог-файлы сохраняются в каталог **<Bastion>\Logs**. Для включения режима записи отладочных сообщений можно запустить файл **<ProgramFiles>\Common Files\Fors\NDebug\debug_mode_on.reg**. Для отключения режима записи отладочных сообщений – файл **<ProgramFiles>\Common Files\Fors\NDebug\debug_mode_off.reg**.

8.2 Настройки отладочного сервиса АПК «Бастион»

Настройки отладочного сервиса сохраняются в системном реестре:

HKEY_LOCAL_MACHINE \SOFTWARE\Fors\NDebug

Основные настройки:

DebugMode	DWORD	Если = 0, то вывод отладочных сообщений и запись их в файл отключена. Если = 1, то вывод отладочных сообщений и запись их в файл включена. Значение по умолчанию – 1.
WriteLog	DWORD	Если = 0, то запись отладочных сообщений в файл отключена. Если = 1, то запись отладочных сообщений в файл включена. Значение по умолчанию – 1.
LogPath	STRING	Полный путь к каталогу, где будут храниться лог-файлы. По умолчанию все лог-файлы хранятся в каталоге Logs, находящегося в каталоге в том же каталоге, куда установлен АПК «Бастион». Если невозможно определить путь к установленному АПК «Бастион», то лог файлы будут храниться в системном каталоге Windows.
LogSizeLimit	DWORD	Максимальный размер лог-файла в МБ. При достижении указанного размера лог-файл будет переименовываться путем добавления числа в конец названия файла, например, bastion.log.1, bastion.log.2 и т.д. По умолчанию – 0.
DeleteOldLogs	DWORD	Если = 1, то будет сохраняться только последний и предпоследний лог-файл. То есть при достижении лог файлом заданного размера, все

<table>
<tr><td></td><td></td><td>старые лог файлы будут удаляться, текущий лог-файл переименовываться, а запись последующих сообщений будет осуществляться в новый лог-файл.

По умолчанию – 1.</td></tr>
<tr><td>LogMessageFormat</td><td>STRING</td><td>Формат строки лога.

Для указания формата используется строка, в которой через запятую указывается порядок вывода параметров лога.
Условные обозначения параметров лога следующие:
PN - имя приложения
PID - идентификатор приложения (Thread ID)
MOD - модуль
EVT - тип события
MSG - сообщение

По умолчанию – «PN,PID,MOD,MSG», что будет выглядеть следующим образом:
[30.06.2009 15:11:01] [OperandProt.dll] [00000ADC] [Бастион-Операнд] (COM3) OperandDrv Create</td></tr>
<tr><td>LogsFilenames</td><td>STRING</td><td>В этой ветке находятся настройки протоколирования, которые позволяют выводить лог от различных модулей в разные файлы.

Все параметры в данной ветке являются строковыми.

Наименование параметра определяет фильтр, по которому будут выбираться сообщения, а значение параметра определяет имя файла, в который будет сохраняться сообщения.

Внимание! Необходимо указывать только имя файла без пути.

Пример:
<table>
<tr><th>Имя параметра
(фильтр)</th><th>Значение параметра
(имя лог-файла)</th></tr>
<tr><td>Bastion.*</td><td>bastion.log</td></tr>
<tr><td>ndebugwin.*</td><td>ndebug.log</td></tr>
<tr><td>BNetSvc.*</td><td>bnetsvc.log</td></tr>
<tr><td>Bastion.Операнд</td><td>operand.log</td></tr>
<tr><td>OperandProt.*</td><td>operand.log</td></tr>
<tr><td>Bastion.Elsys</td><td>elsys.log</td></tr>
</table>
Фильтр состоит из двух частей: первая часть (до точки) – имя исполняемого файла, вторая – фильтр событий.

Определение соответствия производится по совпадению фильтра и строки в логе, звездочка в фильтре событий указывает на любое событие.
Например, для следующей строки лога:

[30.06.2009 15:11:01] [OperandProt.dll] [00000ADC] [Бастион-Операнд] (COM3) OperandDrv Create</td></tr>
</table>

		Сработает один фильтр - OperandProt.* и сообщение будет записано в файл operand.log.

9 Часто задаваемые вопросы по настройке АПК «Бастион»

9.1 Общие вопросы

Окна программы имеют неестественный вид: отсутствуют кнопки, упомянутые в инструкции и необходимые для работы, некоторые элементы окна видны наполовину. Изменение размеров окон не помогает. Что делать?

Вероятнее всего, в настройках Windows был установлен крупный шрифт. ПО «Бастион» не рассчитано на работу с настройками Windows, отличными от стандартных. Следует установить мелкий шрифт (В большинстве версий Windows эту опцию следует искать в свойствах рабочего стола).

Сетевое рабочее место «Бастиона» не подключается к серверу, хотя связь с компьютером-сервером и базой данных есть.

При настройке сети для использования АПК «Бастион» следует учитывать следующее:

- Нельзя использовать динамические IP-адреса для компьютеров комплекса;
- В доменной сети из диапазона динамических IP-адресов необходимо исключить адреса компьютеров АПК «Бастион».

При загрузке системы выдается сообщение «Permission denied. File xxxx. Dir yyyy» или «Доступ запрещен. Файл xxxx. Каталог yyyy». Система на загружается.

Нет доступа к одному из каталогов Бастиона на NTFS-диске у текущего пользователя Windows. Необходимо дать требуемые полномочия (см. п. 5.3).

После нештатного выключения питания на каждое событие «Бастион» стал выдавать сообщение об ошибке. Генератор отчётов и учёт рабочего времени не запускаются.

По всей вероятности, при выключении питания была повреждена протокольная база данных. Следует закрыть все программы комплекса «Бастион» на всех рабочих местах, затем сделать копию файла Bprot.gdb, а оригинальный файл заменить файлом с чистой базой. Если файл чистой базы копировался с дистрибутивного диска, следует снять с него атрибут «Только чтение». Если в системе используется драйвер СКУД, следует после запуска ПО «Бастион» выполнить синхронизацию основной и протокольной баз данных (см. п. 4.19). Для восстановления повреждённой базы данных протокола необходима достаточно высокая квалификация, причём не всегда есть возможность восстановить все данные. Для предотвращения подобных случаев рекомендуется: во-первых, устанавливать источник резервного питания (UPS) на сервер баз данных; во-вторых, включить режим синхронной записи для баз данных (см. 6.3.5).

На сервере баз данных произошло аварийное выключение питания. При старте и выгрузке программы «Бастион» сообщает об ошибке. Невозможно выдать карту доступа. Генератор отчётов не работает. Как восстановить работоспособность системы?

Причина – та же, что и в предыдущем случае – разрушение протокольной базы данных. Следует заменить файл «BProt.gdb», а повреждённую базу попытаться восстановить.

Возникла необходимость изменить номер порта, к которому подключен драйвер. Как это лучше сделать?

Многие драйверы не допускают непосредственного изменения номера порта в базе данных АПК «Бастион» (так, драйвер «Бастион-Elsys» позволяет осуществлять «перевешивание портов» лишь начиная с версии 1.4.353). Можно посоветовать изменить номер COM-порта в Диспетчере Устройств.

Необходимо перенести сервер оборудования на другой компьютер, при этом у компьютера будут новые имя и IP-адрес. Переназначить драйвер на другую рабочую станцию не получается. Что делать?

Если изменяется номер рабочей станции, выполняются действия, аналогичные «Перевешиванию» портов, но не все драйверы позволяют это сделать. Следует изменить имя рабочей станции и IP-адрес в таблице «Рабочие станции» («Конфигурация→Рабочие станции»), не изменяя номера рабочей станции (поле «Идентификатор»).

Отсутствует левая часть окна «Бюро пропусков» со списком подразделений и точек прохода. В группах «Заявки» и «Выданные» отсутствует большинство пропусков.

Следует нажать кнопку  , которая находится в правой верхней части экрана и которая позволяет включить/выключить отображение списка подразделений и точек прохода. Проверить, какие установлены фильтры для отображения пропусков, и при необходимости их снять.

9.2 Генератор отчетов и система учета рабочего времени

Для печати отчётов по событиям предполагалось использовать имевшийся на объекте матричный принтер EPSON-LX-300 с использованием рулонной подачи бумаги. Однако из генератора отчётов печать осуществляется в альбомной ориентации (нужна портретная ориентация, а таких настроек в «Бастионе» нет), к тому же качество печати в таком режиме совершенно неприемлемое.

Расположение страниц в отчётах настраивается автоматически и зависит от количества заданных полей. Вам следует уменьшить количество полей в отчёте, и расположение страниц станет портретным. Разборчивость печати матричного принтера в таком режиме существенно выше. Скорость и качество печати матричных принтеров при печати из приложений Windows (в том числе и ПО «Бастион») очень невысоки, поэтому рекомендуется использовать струйный или лазерный принтер.

В генераторе отчётов при просмотре отчётов для печати вместо русских букв отображаются непонятные символы. Что делать?

На установочном компакт-диске в каталоге Redist находится программа FixFonts. Для решения проблемы её необходимо запустить, нажать кнопку «ОК» и перезагрузить компьютер. Проблема должна исчезнуть.

9.3 Драйверы оборудования

При использовании драйвера «Бастион-Виста» в тексте событий и в отчётах отсутствует фамилия пользователя ПКП «Vista-501», хотя в настройках драйвера было задано соответствие номера пользователя и его фамилии.

Следует задать для всех интересующих событий параметр «%us» (Следует выбрать пункт меню «Конфигурация→События»).

При расширении системы было установлено новое оборудование (два контроллера «Elsys-MB»). Поиском приборов оборудование находится, в базу данных контроллеры добавлены, однако события от них отсутствуют.

Наиболее вероятная причина – перед добавлением приборов была включена маршрутизация сообщений. Следует настроить маршрутизацию сообщений от данных приборов для каждого пользовательского профиля.

Как реализовать механизм переноса выходных для драйвера Elsys-MB, о котором упоминается в рекламных материалах?

Проиллюстрируем это на примере. Пусть 8 Марта приходится на четверг, а в соответствии с Российским законодательством выходной с воскресенья переносится на пятницу. Предприятие работает по пятидневной рабочей неделе. Таким образом, требуется для 8 и 9 марта назначить режим выходных дней, а для 11 марта (воскресенье) назначить режим рабочего дня. Следует назначить 8 и 9 марта праздниками первого типа, а 11 марта – праздником второго типа, и во всех временные зонах, где активны рабочие дни, сделать активными праздники первого типа, а во временных зонах, где выбраны выходные дни, выбрать также праздники второго типа. Аналогичным образом следует поступить и для других праздничных дней, используя один тип праздника для задания рабочего дня выходным, а другой тип праздника – для задания выходного дня рабочим. На следующий год потребуется заново создать подобное расписание.

В составе ПО «Бастион» используется драйвер «Бастион-С2000». Были вынесены на план и настроены пиктограммы охранных зон (разрешены постановка на охрану и снятие с неё). Пункты «Поставить зону на охрану» и «Снять зону с охраны» активны, однако при их выборе приборы не управляются.

Вероятно, при настройке драйвера «Бастион-С2000» не были добавлены операторы комплекса «Бастион».

Приложение 1. Перечень файлов, входящих в состав комплекса

	Bastion.exe	Основной исполняемый модуль, содержит все драйверы системы.
	BrepGen.exe	Генератор отчётов по событиям.
	Attendance.exe	Генератор отчётов системы учёта рабочего времени
	BProtSrv.exe	Сервис протоколирования и автоматической выгрузки протокола
	BGraphSrv.dll	Библиотека отображения графических планов
	NotiProt.dll	Библиотека драйвера Бастион-Notifier
	GateProt.dll	Библиотека драйвера Бастион-Gate
	Cvsdll.dll	Библиотека драйвера Бастион-CVS
	EsmiDriver.dll	Библиотека драйвера Бастион-MESA
	ItvDriver.dll	Библиотека драйвера Бастион-ITV
	DelayedLaunch.exe	Утилита отложенного запуска программ (ожидание загрузки драйвера HASP)
	WatchDog.exe	Сервис программного перезапуска системы в случае ее зависания
	Data\Bastion.GDB	Основная база данных в формате Firebird 1.5
	Data\Bprot.GDB	Протокольная база данных в формате Firebird 1.5
	Maps\dlist.xml	Правила отображения векторных пиктограмм (XML)
	Maps\settings.ini	Настройки графической подсистемы
	Help*.*	Файлы справочной системы
	Docs*.pdf	Файлы документации
	Patterns*.frf	Файлы с шаблонами для печати пропусков
	DXF2Pictogram*.*	Редактор списка пиктограмм
	ElsConfigs*.els	Примеры конфигурации контроллеров Elsys-MB
	HaspProg\LicenseManager.exe	Менеджер лицензий
	Redist*.*	Установщики сторонних программы, поставляемые с АПК «Бастион»
	TimeToBackup*.*	Служба резервного копирования баз данных по

		расписанию
	Transform*.xtr	Файлы трансформаций для работы с форматом XML
	Updates*.*	Программа и скрипты для обновления баз данных
	ElsysMBProg*.*	Программатор контроллеров Elsys-MB
	fruser.hlp, fruser.cnt	Файлы справки построителя отчетов FastReport
	<System32>\midas.dll	Библиотека для работы с БД
	<Firebird>\UDF\FreeUdfLib.dll	Библиотека дополнительных функций для СУБД
	<Firebird>\UDF\N2000_udf.dll	Библиотека дополнительных функций для СУБД

В процессе работы программой могут быть созданы следующие файлы:

Bsettings.stg BRepGen.stg	Конфигурация внешнего вида форм программы.
VPro.stg	Конфигурация драйвера «Бастион-Видео»
Каталоги NET, PRIV, TABLES	Служебные каталоги BDE
Data\Lbprot_*.csv	Файлы с журналом событий. Создаются при невозможности записать события на сервер базы данных.
Except.log Bastion.log	Сообщения об ошибках системы

а также log файлы различных драйверов (*.log).