Код безопасности
ГК «Информзащита»

Программно-аппаратный комплекс

Соболь
Версия 3.0

Руководство администратора

RU.40308570.501410.001 91 1

© Компания "Код Безопасности", 2010. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Этот документ входит в комплект поставки изделия. На него распространяются все условия лицензионного соглашения. Без специального письменного разрешения компании "Код Безопасности" этот документ или его часть в печатном или электронном виде не могут быть подвергнуты копированию и передаче третьим лицам с коммерческой целью.

Информация, содержащаяся в этом документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны компании "Код Безопасности".

Почтовый адрес:	**127018, г. Москва, ул. Сущевский Вал, дом 47, стр. 2, помещение №1**
Телефон:	**(495) 980-23-45**
Факс:	**(495) 980-23-45**
e-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Последнее обновление: 15-07-10

Оглавление

Список сокращений

АИП	Аутентифицирующая информация пользователя
АПКШ	Аппаратно-программный комплекс шифрования
ВТСС	Вспомогательные технические средства и системы
ДСЧ	Датчик случайных чисел
КПП	Ключ преобразования паролей
КС	Контрольная сумма
КЦ	Контроль целостности
НЖМД	Накопитель на жестком магнитном диске
НСД	Несанкционированный доступ
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
ПСЗИ	Программное средство защиты информации
СЗИ	Средство защиты информации
УНП	Уникальный номер платы
ЭВТ	Электронная вычислительная техника

Введение

Данное руководство предназначено для администраторов изделия "Программно-аппаратный комплекс "Соболь". Версия 3.0" RU.40308570.501410.001 (далее — комплекс "Соболь", комплекс). В нем содержатся сведения, необходимые для установки, настройки и эксплуатации комплекса "Соболь".

Сведения об установке и настройке ПО комплекса на компьютерах, функционирующих под управлением ОС МСВС 3.0 и VMware ESX, приводятся в документах [2] и [3] соответственно.

Сведения, необходимые пользователю комплекса "Соболь", содержатся в документе [4].

Структура руководства

Материал руководства организован следующим образом:

- **Глава 1** содержит общие сведения о функционировании защитных механизмов комплекса "Соболь";
- в **Главе 2** содержатся сведения об установке и удалении комплекса в среде ОС Windows;
- в **Главах 3** и **4** содержится информация, относящаяся к настройке и эксплуатации комплекса;
- в **Приложении** приведена необходимая справочная информация.

Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Некоторые примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru и hotline@infosec.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем учебного центра можно по электронной почте (edu@infosec.ru).

Глава 1
Общие сведения

Назначение

Комплекс "Соболь" предназначен для предотвращения несанкционированного доступа посторонних лиц к ресурсам защищаемого компьютера.

Комплекс "Соболь" реализует следующие основные функции:

- идентификация и аутентификация пользователей компьютера при их входе в систему с помощью персональных электронных идентификаторов iButton, eToken PRO, iKey 2032, Rutoken S, Rutoken RF S (см. Табл. 1 на стр. 8);
- защита от несанкционированной загрузки операционной системы со съемных носителей — дискет, оптических дисков, ZIP-устройств, магнитооптических дисков, USB-устройств и др.;
- блокировка компьютера при условии, что после его включения управление не передано расширению BIOS комплекса "Соболь";
- контроль целостности файлов, физических секторов жесткого диска, элементов системного реестра компьютера до загрузки операционной системы;
- контроль работоспособности основных компонентов комплекса — датчика случайных чисел, энергонезависимой памяти, персональных электронных идентификаторов;
- регистрация событий, имеющих отношение к безопасности системы;
- совместная работа с АПКШ "Континент", СЗИ Secret Net, vGate, Security Studio Honeypot Manager, "Континент-АП" и "КриптоПро CSP".

Комплекс "Соболь" может использоваться на территории Российской Федерации в качестве средства защиты от НСД к конфиденциальной информации, не содержащей сведения, составляющие государственную тайну, а также к информации, содержащей сведения, составляющие государственную тайну со степенью секретности "совершенно секретно" включительно.

Принципы функционирования

Действие комплекса "Соболь" состоит в проверке полномочий пользователя на вход в систему. Если предъявлены необходимые атрибуты — персональный идентификатор и пароль, то пользователь получает право на вход. При их отсутствии вход в систему данного пользователя запрещается.

Пояснение. Пользователь получает допуск к компьютеру после регистрации его в списке пользователей комплекса "Соболь". Регистрация пользователей осуществляется администратором и состоит в присвоении пользователю имени, персонального идентификатора и назначении пароля. Регистрация администратора осуществляется при инициализации комплекса.

В комплексе "Соболь" реализованы следующие основные защитные механизмы:

- идентификация и аутентификация пользователей;
- блокировка загрузки ОС со съемных носителей;
- контроль целостности файлов, секторов жесткого диска, элементов системного реестра компьютера;
- сторожевой таймер;
- регистрация событий, имеющих отношение к безопасности системы.

Пояснение. Комплекс "Соболь" может функционировать как с использованием механизмов контроля целостности и сторожевого таймера, так и без них.

Комплекс "Соболь" функционирует в двух режимах — инициализации и эксплуатации (рабочем режиме).

Режим инициализации предназначен для подготовки комплекса к эксплуатации. В комплексе "Соболь" реализованы два способа инициализации — **аппаратный** и **программный**.

Аппаратная инициализация выполняется до начала рабочего режима комплекса и заключается в реализации следующих основных процедур: переключение платы комплекса в режим инициализации (см. стр. 22), настройка общих параметров (см. стр. 24), настройка контроля целостности (см. стр. 26), регистрация администратора (см. стр. 26).

Программная инициализация отличается от аппаратной тем, что она выполняется во время рабочего режима функционирования комплекса и не требует переключения платы в режим инициализации. Остальные процедуры реализуются аналогично.

Механизм идентификации и аутентификации

Механизм идентификации и аутентификации обеспечивает проверку полномочий пользователя на вход при попытке входа в систему.

Идентификация (распознавание) и аутентификация (проверка подлинности) пользователей осуществляется при каждом входе пользователя в систему.

Для идентификации пользователей в комплексе "Соболь" используются уникальные номера аппаратных устройств — идентификаторов (см. Табл. 1). При аутентификации осуществляется проверка правильности указанного пользователем пароля с использованием аутентификатора пользователя.

Пояснение. Аутентификатор — структура данных, хранящаяся в персональном идентификаторе пользователя (в преобразованном виде), которая наравне с паролем пользователя участвует в процедуре аутентификации пользователя.

Табл. 1. Идентификаторы, используемые в комплексе "Соболь"

Идентификаторы iButton	USB-идентификаторы	
	USB-ключи	Смарт-карты
DS1992	eToken PRO	eToken PRO
DS1993	Rutoken S	
DS1994	Rutoken RF S	
DS1995	iKey 2032	
DS1996		

В зависимости от типа предъявляемого идентификатора в комплексе "Соболь" поддерживаются двухфакторный (для iButton, iKey 2032, Rutoken S, Rutoken RF S) и усиленный двухфакторный (для eToken PRO) способы аутентификации.

При реализации двухфакторной аутентификации сначала предъявляется персональный идентификатор iButton/iKey 2032/Rutoken S/Rutoken RF S, затем вводится пароль пользователя.

При осуществлении усиленной двухфакторной аутентификации сначала предъявляется персональный идентификатор eToken PRO, затем вводятся его PIN-код и пароль пользователя.

Для всех eToken PRO (как USB-ключей, так и смарт-карт) производителем устанавливается PIN-код по умолчанию — **1234567890**, который обеспечивает при его предъявлении автоматический доступ к памяти идентификатора. Для повышения эффективности защиты информации от НСД администратор комплекса должен установить PIN-код, отличный от PIN-кода по умолчанию. В этом случае после предъявления eToken PRO комплекс обязательно запрашивает его значение. Необходимо ввести установленный PIN-код и нажать "Enter".

Внимание. В случае установки администратором значения PIN-кода USB-идентификатора eToken PRO, отличного от PIN-кода по умолчанию, администратор обязан при выдаче пользователю идентификатора сообщить ему это значение.

В случае предъявления персонального идентификатора, не зарегистрированного в системе:

- вход пользователя в систему запрещается;
- в журнале регистрации событий фиксируется попытка несанкционированного доступа к компьютеру.

В случае ввода пароля, не соответствующего предъявленному идентификатору:

- вход пользователя в систему запрещается;

- счетчик неудачных попыток входа пользователя в систему увеличивается на единицу;

  Пояснение. В том случае, когда число неудачных попыток входа пользователя сравняется с максимально допустимым значением, заданным администратором, вход данного пользователя в систему блокируется. Если число неудачных попыток меньше максимально допустимого значения, то счетчик неудачных попыток сбрасывается (обнуляется) при первом успешном входе пользователя в систему.

- в журнале регистрации событий фиксируется попытка несанкционированного доступа к компьютеру.

Служебная информация о регистрации пользователя (имя, номер присвоенного персонального идентификатора и т. д.) хранится в энергонезависимой памяти комплекса "Соболь".

Комплекс "Соболь" предоставляет администратору следующие дополнительные возможности по управлению процедурой идентификации и аутентификации и процедурами смены пароля и аутентификатора пользователя:

- ограничение времени, отводящегося пользователю при входе в систему для предъявления персонального идентификатора и ввода пароля;
- ограничение времени действия пароля и аутентификатора пользователя, по истечении которого пользователь будет вынужден сменить свой пароль и аутентификатор;

  Пояснение. Эта возможность доступна только при использовании персональных идентификаторов iButton DS1994.

- режим использования случайных паролей для процедур смены пароля пользователя и администратора и процедуры регистрации нового пользователя;
- ограничение минимально допустимой длины пароля пользователя.

Внимание! В режиме совместного использования комплекса "Соболь" с другими системами защиты (например, СЗИ семейства Secret Net) управление паролями и аутентификаторами администратора и пользователя осуществляется средствами управления той системы защиты, совместно с которой функционирует этот комплекс.

Механизм блокировки загрузки операционной системы со съемных носителей

Блокировка несанкционированной загрузки операционной системы с внешних съемных носителей (дискет, оптических дисков, ZIP-устройств, магнитооптических дисков, USB-устройств и др.) осуществляется путем блокирования доступа к указанным устройствам с момента включения компьютера и до завершения процесса загрузки штатной копии ОС. После успешной загрузки штатной копии ОС доступ к этим устройствам восстанавливается.

Запрет распространяется на всех пользователей компьютера, за исключением администратора.

Администратор может разрешить отдельным пользователям компьютера выполнять загрузку операционной системы со съемных носителей.

Механизм контроля целостности

Механизм контроля целостности обеспечивает контроль целостности содержимого ресурсов компьютеров. Контроль целостности — это функция, которая предназначена для слежения за изменением параметров заданных ресурсов.

Используемый в комплексе "Соболь" механизм контроля целостности позволяет контролировать неизменность файлов, физических секторов жесткого диска, элементов системного реестра компьютера до загрузки операционной системы. Для этого вычисляются некоторые контрольные значения проверяемых объектов и сравниваются с ранее рассчитанными для каждого из этих объектов эталонными значениями.

Формирование списка подлежащих контролю объектов производится с помощью программы управления шаблонами контроля целостности. Программа вхо-

дит в комплект поставки комплекса. Списки контролируемых объектов и значения их контрольных сумм хранятся в виде файлов-шаблонов на жестком диске компьютера. Пути к файлам-шаблонам хранятся в защищенной памяти платы ПАК.

Пояснение. Шаблоны КЦ представляют собой служебные файлы Bootfile.chk, Bootfile.nam, Bootsect.chk, Bootsect.nam, Bootreg.chk и Bootreg.nam. Эти файлы определяют местоположение каждого контролируемого объекта. Исходные шаблоны создаются при установке программы управления шаблонами.

Возможность расчета контрольных сумм предоставляется только администратору комплекса "Соболь". При расчете значения контрольных сумм контролируемых объектов записываются в файлы-шаблоны. После этого рассчитываются контрольные суммы самих файлов-шаблонов и их значения сохраняются в защищенной памяти платы комплекса. Значения контрольных сумм рассчитываются по алгоритму ГОСТ 28147-89 в режиме выработки имитовставки.

Проверка контрольных сумм контролируемых объектов осуществляется при входе пользователей в систему. Процедура контроля целостности сначала рассчитывает контрольные суммы файлов-шаблонов и сравнивает их со значениями, сохраненными в защищенной памяти платы ПАК. После этого рассчитываются и проверяются контрольные суммы всех контролируемых объектов.

Механизм контроля целостности реализует два режима: "жесткий" и "мягкий". Режим работы устанавливается администратором для каждого пользователя компьютера индивидуально.

В "жестком" режиме при обнаружении нарушений целостности файлов-шаблонов или контролируемых объектов вход пользователя в систему запрещается и компьютер блокируется. В журнале событий регистрируется событие "Ошибка при контроле целостности".

В "мягком" режиме при обнаружении нарушений целостности файлов-шаблонов или контролируемых объектов вход пользователя в систему разрешается. В журнале событий регистрируется событие "Ошибка при контроле целостности".

В комплексе "Соболь" процедуре контроля целостности файлов и секторов жестких дисков предшествует проверка содержимого журнала транзакций NTFS, EXT3. Если в журнале имеются сведения о незавершенных операциях, то контроль целостности не проводится и осуществляется блокировка компьютера.

Механизм сторожевого таймера

Механизм сторожевого таймера обеспечивает блокировку доступа к компьютеру при условии, что после включения компьютера и по истечении заданного интервала времени управление не передано расширению BIOS комплекса "Соболь".

Блокировка доступа к компьютеру осуществляется путем принудительной автоматической перезагрузки компьютера с помощью стандартной процедуры Reset.

Во избежание потери данных приложений, вызванной срабатыванием механизма сторожевого таймера во время выхода компьютера из ждущего режима, не используйте ждущий режим ОС Windows, если в параметрах BIOS включен энергосберегающий режим ACPI "S3" или "S4" (Suspend To RAM). В этих случаях рекомендуется вместо ждущего режима использовать в ОС Windows спящий режим или изменить энергосберегающий режим BIOS.

Для использования данного механизма необходимо правильно подключить к плате комплекса "Соболь" кабель механизма сторожевого таймера (см. п. **4** процедуры на стр. 22). Если кабель не подключен — механизм сторожевого таймера не действует.

Требования к оборудованию и программному обеспечению

Комплекс "Соболь" устанавливается на компьютеры, оснащенные 32- или 64-разрядными процессорами. Для подключения платы комплекса системная плата компьютера должна быть оснащена:

- либо шиной стандарта PCI Express (далее — PCI-E) версии 1.0a и выше, на которой должен быть в наличии хотя бы один свободный разъем;
- либо шиной стандарта PCI версий 2.0/2.1/2.2/2.3 с напряжением питания 5 В или 3,3 В, на которой должен быть в наличии хотя бы один свободный разъем.

На системной плате компьютера должен находиться разъем Reset, обеспечивающий возможность подключения кабеля механизма сторожевого таймера из комплекта поставки ПАК, подачу сигналов на который невозможно отключить из BIOS Setup или каким-либо другим образом.

Комплекс "Соболь" поддерживает работу с идентификаторами iButton (DS1992, DS1993, DS1994, DS1995, DS1996), USB-ключами eToken PRO, iKey 2032, Rutoken S, Rutoken RF S, смарт-картами eToken PRO.

Работоспособность комплекса "Соболь" не зависит от типа используемой операционной системы, поэтому комплекс можно устанавливать на компьютеры, работающие под управлением различных операционных систем.

Реализованный в комплексе механизм контроля целостности включает в свой состав программные компоненты, успешная работа которых зависит от операционной системы компьютера. Механизм функционирует в среде следующих ОС с файловыми системами FAT 16, FAT 32, NTFS, UFS2, UFS, EXT2, EXT3:

- Windows Server 2008/Server 2008 x64 Edition/Server 2008 R2;
- Windows 7/7 x64 Edition;
- Windows Vista (Enterprise, Business, Ultimate)/Vista (Enterprise, Business, Ultimate) x64 Edition;
- Windows Server 2003/Server 2003 x64 Edition/Server 2003 R2/ Server 2003 R2 x64 Edition;
- Windows XP Professional/XP Professional x64 Edition;
- Trustverse Linux XP Desktop 2008 Secure Edition;
- МСВС 3.0;
- VMware ESX 3.5/4.0.

Механизм контроля целостности позволяет контролировать целостность файлов и секторов жестких дисков в среде ОС FreeBSD 5.3/6.2/ 6.3/7.2 с файловой системой UFS, UFS2. Однако программные компоненты, обеспечивающие управление шаблонами контроля целостности в среде ОС FreeBSD, в комплект поставки не включены.

При использовании механизма контроля целостности необходимо соблюдать следующие требования:

- Запрещается использование на компьютере любых менеджеров загрузки ОС (boot manager), обеспечивающих функционирование нескольких ОС. Например, ОС Windows XP при использовании boot manager Windows XP.
- Невозможен контроль целостности файлов, преобразованных любыми другими программами, например, криптографии (BestCrypt и т. п.) или сжатия дисков (Drivespace и т. п.).
- Запрещается подвергать сжатию каталог, содержащий служебные файлы механизма контроля целостности.
- Применение механизма контроля целостности для логических дисков, являющихся наборами томов Windows XP/2003/Vista/7/2008 (volume set и stripe set), не поддерживается.

Работа механизма КЦ характеризуется следующими особенностями:

- При задании пути к файлам шаблонов КЦ для FAT не поддерживается возможность задания путей в длинном виде.
- Не поддерживается контроль целостности файлов на дисках, размеченных как GUID Partition Table.
- Не поддерживается контроль целостности ресурсов на более чем 26 логических дисках.

- Не поддерживается возможность контроля целостности секторов, расположенных на диске за пределами 2 Тбайт.
- Не поддерживается контроль целостности файлов, расположенных на динамических дисках.

Перед созданием автоматизированной системы в защищенном исполнении с применением ПАК "Соболь" целесообразно проведение работ по проверке совместимости ПАК и компьютеров, в составе которых предполагается его использование.

Варианты применения

Возможны следующие варианты применения комплекса "Соболь":

- автономный комплекс, обеспечивающий защиту автономных компьютеров, а также рабочих станций и серверов, входящих в состав локальной вычислительной сети;
- комплекс, обеспечивающий защиту автономных компьютеров, рабочих станций сети и серверов в составе СЗИ семейства Secret Net;
- комплекс, обеспечивающий защиту от несанкционированного вмешательства посторонних лиц в работу криптографического шлюза АПКШ "Континент";
- комплекс, функционирующий совместно со средствами защиты информации "Континент-АП", "КриптоПро CSP", Security Studio Honeypot Manager, vGate.

Работа комплекса "Соболь" в составе СЗИ семейства Secret Net или АПКШ "Континент" осуществляется в режиме совместного использования. Ограничения этого режима рассматриваются на стр. 82.

Специальные рекомендации

Комплекс "Соболь" может быть использован в качестве средства защиты от НСД к техническим, программным и информационным ресурсам компьютеров, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну со степенью секретности до "совершенно секретно" включительно, при условии проведения проверки выполнения требований, изложенных в разделе "Требования к оборудованию и программному обеспечению" и в данном разделе, специализированной организацией с последующей экспертизой в войсковой части 43753, а также при условии выполнения следующих требований:

- соблюдение условий и правил эксплуатации, установленных в эксплуатационной документации комплекса и в Предписании на эксплуатацию компьютера с установленным ПАК;
- сохранение в тайне аутентификаторов и паролей администратора и пользователей, а также информации, записанной в энергонезависимую память платы комплекса "Соболь".

Комплекс "Соболь" может быть использован в качестве средства защиты от НСД к техническим, программным и информационным ресурсам при запуске компьютеров, обрабатывающих конфиденциальную информацию, не содержащую сведений, составляющих государственную тайну, при условии выполнения следующих требований:

- соблюдение условий и правил эксплуатации, установленных в эксплуатационной документации комплекса;
- сохранение в тайне личных аутентификаторов и паролей администратора и пользователей, а также информации, записанной в энергонезависимую память платы комплекса "Соболь".

При эксплуатации комплекса должны выполняться следующие требования:

1. На компьютере с установленным комплексом "Соболь" должны быть проведены исследования технических средств компьютера (в том числе исследования системной программы BIOS) на предмет отсутствия в их реализации аппаратно-программных механизмов, которые могут привести к нарушению правильности функционирования компьютера и комплекса или к утечке защищаемой информации.
2. Должны быть приняты организационно-технические меры по сохранению целостности корпуса компьютера, исключающие НСД к аппаратным средст-

вам изделия и техническим средствам компьютера, расположенным внутри его системного блока.

3. Должны быть предусмотрены меры, препятствующие модификации (перепрограммированию) как системной программы BIOS, так и расширений BIOS в компьютере с установленным комплексом "Соболь".
4. Продолжительность сеанса работы изделия, то есть время между включением (перезагрузкой) компьютера и началом загрузки ОС, не должна превышать 24 часов.
5. Количество комплексов, инициализируемых и обслуживаемых одним администратором, не должно превышать 256.
6. Максимальный срок действия КПП и УНП не должен превышать 3 лет. Для выполнения этого требования необходимо не реже чем 1 раз в 3 года проводить инициализацию всех ПАК, обслуживаемых данным администратором, с первичной регистрацией администратора на первом комплексе.
7. При установке аппаратных компонентов комплекса обязательно подключение кабеля механизма сторожевого таймера, входящего в комплект поставки.
8. При использовании комплекса "Соболь" для защиты от НСД ресурсов компьютеров, обрабатывающих конфиденциальную информацию, не содержащую сведений, составляющих государственную тайну, администратор должен установить следующие значения параметров:
   - "Версия криптографической схемы" — "2.0";
   - "Автономный режим работы" — "Да";

     Пояснение. Значение "Нет" может быть установлено только при выполнении условия **17**.
   - "Контроль файлов и секторов" — "Да";

Также необходимо настроить контроль целостности объектов ОС в составе, достаточном для ее гарантированной загрузки и контроля необходимых файлов пользователей.

   - "Контроль журнала транзакций" — "Да" (в случае контроля целостности файлов, расположенных на томах с файловой системой NTFS или EXT3);
   - "Контроль элементов реестра" — "Да";
   - "Число попыток тестирования ДСЧ" — "1";
   - "Предельное число неудачных входов пользователя" — не более "10";
   - "Ограничение времени на вход в систему" — не более "5";
   - "Время ожидания сторожевого таймера" определяется автоматически на этапе инициализации комплекса или может быть выбрано таким образом, чтобы оно превосходило время появления приглашения на предъявление идентификатора не более чем на 10 секунд;
   - "Период тестирования сторожевого таймера (дней)" — "1";
   - "Режим контроля целостности" — "Жесткий" для всех зарегистрированных пользователей, за исключением привилегированных;
   - "Запрет загрузки с внешних носителей" — "Да" для всех зарегистрированных пользователей.
9. При использовании комплекса "Соболь" для защиты от НСД ресурсов компьютеров, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну со степенью секретности до "совершенно секретно" включительно, администратор должен выполнить следующие требования:
   - провести настройку комплекса в соответствии с условием **8**, а также установить следующие значения параметров:
     - "Использование случайных паролей" — "Да";
     - "Минимальная длина пароля пользователя" — не менее "8", при этом администратор должен использовать пароль длиной не менее 11 символов;
     - "Предельное число неудачных входов пользователя" — не более "8";
     - "Ограничение срока действия пароля" — "Да" для всех зарегистрированных пользователей;

Пояснение. При этом всем пользователям следует при регистрации присваивать персональные идентификаторы iButton DS1994.

- "Замена аутентификатора при смене пароля" — "Да" для всех зарегистрированных пользователей;
- "Максимальный срок действия пароля (дней)" — не более "92" для всех зарегистрированных пользователей;

Требование справедливо при условии, что количество попыток доступа зарегистрированного пользователя и администратора на всех комплексах, где они зарегистрированы с использованием одной и той же АИП (аутентификатора и пароля), не превосходит 10 раз за сутки или не более 920 раз за время действия АИП

- разрешается использовать персональные идентификаторы следующих типов: iButton модификаций DS1992, DS1993, DS1994, DS1995, DS1996, а также USB-идентификаторы eToken PRO и Rutoken S/RF S;
- рекомендуется применять в качестве персональных идентификаторов пользователей носители типа iButton DS1994;
- запрещается использовать в качестве персональных идентификаторов USB-идентификаторы iKey2032;
- администратор должен проводить смену собственного пароля и аутентификатора исходя из условия, что количество входов на все комплексы, которые он обслуживает, не должно превышать 920 (в среднем 10 входов в сутки), но не реже одного раза в 92 дня. Если используются персональные идентификаторы пользователей, отличные от iButton типа DS1994, то администратор должен обеспечить смену паролей и личных аутентификаторов пользователей до истечения срока их действия, который определяется так же, как для администратора. Для выполнения этого требования должны быть разработаны организационные меры;
- запрещается регистрация пользователя с именем AUTOLOAD и присвоение параметру "Время ожидания автоматического входа в систему" значения, отличного от "0";
- при эксплуатации комплекса в режиме совместного использования запрещается устанавливать режим ввода пароля с персонального идентификатора пользователя (при помощи внешнего по отношению к комплексу программного обеспечения) путем установки 5-го бита переменной поля Flags параметров пользователя в 1.

10. После блокирования учетной записи пользователя должно проводиться исследование причин блокирования. При выявлении попытки НСД или при невозможности установления причины блокирования учетные записи данного пользователя должны быть удалены на всех комплексах, в которых он был зарегистрирован, и проведена его перерегистрация (на первом комплексе должна быть проведена первичная регистрация) с вводом нового пароля.
11. При утере персонального идентификатора или компрометации его содержимого учетные записи данного пользователя должны быть удалены со всех комплексов, где он был зарегистрирован, и проведена его перерегистрация (на первом из комплексов перерегистрация должна проводиться в режиме первичной регистрации).
12. При утере персонального идентификатора администратора комплекса или компрометации его содержимого должна быть проведена инициализация всех комплексов, обслуживаемых данным администратором, при этом на первом из комплексов перерегистрация администратора должна проводиться в режиме первичной регистрации.
13. Периодичность просмотра администратором журнала регистрации событий должна быть определена из конкретных условий эксплуатации комплекса таким образом, чтобы исключить возможность бесконтрольной утери информации, вызванной переполнением журналов.
14. Должна быть обеспечена невозможность загрузки ОС с внешних устройств, то есть устройств, подключаемых к внешним интерфейсным разъемам компьютера, например, SATA, за исключением устройств, подключаемых через интерфейсы USB и IEEE 1394. Если BIOS компьютера не удовлетворяет требованиям спецификации Enhanced Disk Drive (EDD) версии 3.0, то должна

быть обеспечена невозможность загрузки ОС с внешних устройств, то есть устройств, подключаемых к внешним интерфейсным разъемам компьютера. Проверка полноты реализации спецификации EDD версии 3.0 и, при необходимости, невозможности загрузки ОС с внешних устройств, подключаемых через интерфейс eSATA, должна проводиться при исследовании системной программы BIOS компьютера.

Необходимо обеспечить невозможность загрузки ОС со всех загрузочных устройств, за исключением загрузочного системного НЖМД, после передачи управления ПАК программе — загрузчику ОС, записанной в главной корневой записи (Master Boot Record) системного НЖМД.

15. При использовании комплекса "Соболь" в составе ПСЗИ необходимо обеспечить средствами ПСЗИ невозможность модификации или уничтожения файлов заданий на контроль целостности.

16. Комплекс "Соболь" может применяться в режиме совместного использования с внешними ПСЗИ при условии выполнения следующих требований:

- обеспечение невозможности доступа субъектов, не входящих в систему защиты, к конфигурационной и служебной информации комплекса;
- обеспечение смены паролей и аутентификаторов администратора и пользователей до истечения срока их действия. После истечения сроков действия пароля и/или аутентификатора пользователя в случае невозможности их смены учетные записи данного пользователя должны быть заблокированы или удалены на всех комплексах, где он зарегистрирован;
- при передаче по каналам связи обеспечение целостности данных комплекса с характеристиками не хуже, чем характеристики функции комплекса по контролю целостности программной среды;
- при передаче по каналам связи обеспечение недоступности данных комплекса или их конфиденциальности с характеристиками не хуже, чем характеристики функции комплекса по защите образцов для проведения идентификации/аутентификации пользователей.

Выполнение перечисленных требований должно проверяться при проведении исследований работы комплекса совместно с ПСЗИ специализированной организацией с последующей экспертизой в войсковой части 43753.

17. Перед выводом комплекса из эксплуатации должна быть проведена очистка энергонезависимой памяти платы комплекса путем проведения инициализации, при этом администратор должен быть зарегистрирован в режиме первичной регистрации. Персональный идентификатор, использованный для его регистрации, в дальнейшем может быть использован, при этом на первом комплексе он может применяться для регистрации администратора или пользователя только в режиме первичной регистрации.

18. Регламентные работы по техническому обслуживанию комплекса и компьютера должны проводиться не реже 1 раза в год.

19. Компьютер, в котором установлен комплекс "Соболь", должен быть аттестован в качестве объекта ЭВТ 2 или 3 категории в зависимости от степени секретности обрабатываемой информации или по требованиям нормативно-методического документа "Специальные требования и рекомендации по технической защите конфиденциальной информации" (СТР-К), утвержденного приказом Гостехкомиссии России № 282 от 30.08.2002 г., и иметь соответствующее Предписание на эксплуатацию.

При этом на расстоянии не менее 5 метров от ЭВТ 2 или 3 категории не допускается неконтролируемое размещение посторонних технических средств и кабелей.

20. Комплекс "Соболь" не налагает ограничений на возможность ведения секретных переговоров в помещениях, где он размещается.

21. При эксплуатации комплекса "Соболь" запрещается вносить изменения в его конструкцию и работать с открытой крышкой системного блока.

Глава 2
Установка и удаление комплекса

Установка комплекса

Установка комплекса "Соболь" осуществляется в следующем порядке:

- установка программного обеспечения комплекса (см. ниже);
- подготовка комплекса к инициализации (см. стр. 22);
- инициализация комплекса (см. стр. 23);
- подготовка комплекса к эксплуатации (см. стр. 31).

Порядок установки программного обеспечения комплекса "Соболь" в среде ОС МСВС 3.0 и VMware ESX рассмотрен в документах [2] и [3] соответственно.

Установка программного обеспечения комплекса

Программное обеспечение комплекса "Соболь" рекомендуется устанавливать до установки в компьютер платы комплекса.

Установку ПО комплекса "Соболь" на компьютеры можно осуществить двумя способами: локально (см. ниже) или централизованно (см. стр. 18).

Локальная установка

Локальный способ заключается в установке администратором ПО комплекса непосредственно на каждом защищаемом компьютере.

Для локальной установки программного обеспечения:

1. Поместите установочный компакт-диск в привод DVD/CD-ROM и запустите на исполнение файл Setup.exe.

   Программа установки выполнит подготовку к установке. После завершения подготовительных действий на экране появится стартовый диалог программы установки.

2. Ознакомьтесь с информацией, содержащейся в стартовом диалоге, и нажмите кнопку "Далее >" для продолжения установки.

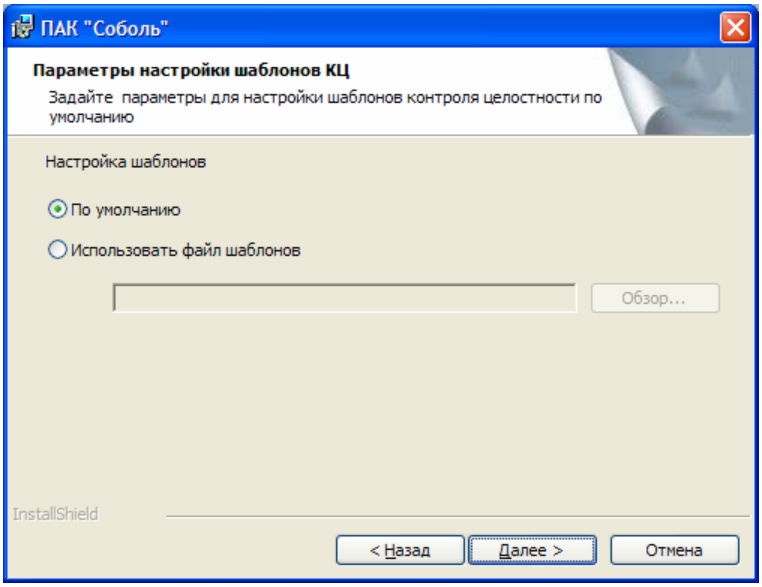
   На экране появится диалог с текстом лицензионного соглашения.

3. Ознакомьтесь с содержанием лицензионного соглашения. Если вы согласны с условиями лицензионного соглашения, отметьте поле "Я принимаю условия лицензионного соглашения" и нажмите кнопку "Далее >".

   На экране появится диалог с указанием пути размещения ПО комплекса.

4. Нажмите кнопку "Далее >".

   На экране появится диалог для выбора файла, в котором хранится список подлежащих контролю целостности объектов:



По умолчанию исходный список подлежащих контролю целостности объектов содержится в файлах SICInstall.xml и SICInstall64.xml для 32- и 64-разрядных ОС соответственно. Файлы хранятся в каталоге %SystemDrive%\Program Files\Infosec\Sobol. Вы можете выбрать другие файлы. Для этого:

- отметьте поле "Использовать файл шаблонов" и нажмите кнопку "Обзор";
- в появившемся диалоге выберите необходимый файл;
- нажмите кнопку "Открыть".

5. Нажмите кнопку "Далее >".

   На экране появится диалог, предлагающий начать процедуру установки.

6. Нажмите кнопку "Установить".

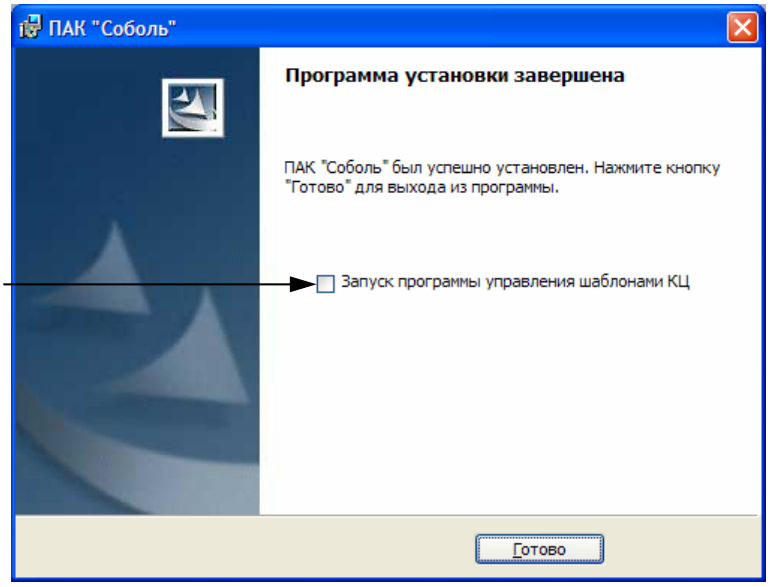
   Программа установки приступит к копированию файлов на жесткий диск компьютера. Ход процесса копирования отображается на экране в виде индикатора прогресса.

В некоторых случаях на экране может появиться диалог со списком программ, использующих в данный момент системные файлы, которые должна обновить программа установки.

- Для обновления системных файлов без перезагрузки компьютера закройте перечисленные в списке программы, а затем нажмите в диалоге кнопку "Повторить".
- Для немедленного продолжения установки нажмите кнопку "Пропустить", но в этом случае по завершении установки вам, скорее всего, будет предложено перезагрузить компьютер.

Затем программа установки регистрирует в системе драйвер платы комплекса "Соболь" и формирует шаблоны контроля целостности.

После успешного выполнения процедуры установки на экране появится завершающий диалог программы установки:



Для запуска программы управления шаблонами КЦ после установки ПО комплекса отметьте соответствующее поле.

7. Нажмите кнопку "Готово".

Обычно перезагрузка компьютера после завершения установки не требуется.

В результате установки:

- в главном меню Windows в подменю "Все программы" появится команда запуска программы управления шаблонами КЦ:

Рис. 1. Команда запуска программы управления шаблонами КЦ

- в случае автоматического запуска на экране появится окно "Управление шаблонами КЦ".

Централизованная установка

Централизованный способ заключается в создании и реализации групповой политики автоматической установки ПО на компьютерах домена средствами ОС Windows.

Централизованная установка комплекса "Соболь" осуществляется в следующем порядке:

- создание общедоступного сетевого ресурса с установочным дистрибутивом ПО комплекса (см. ниже);
- создание файла — сценария установки (см. стр. 19);
- создание организационных подразделений (см. стр. 19);
- создание групповых политик для организационных подразделений (см. стр. 20);
- включение централизованной установки ПО комплекса (см. стр. 20).

Для создания общедоступного ресурса:

Далее имена каталогов, файлов, организационных подразделений и групповых политик, используемые в примерах, выделяются курсивом.

1. На сетевом ресурсе создайте каталог (например, *Distrib*) и откройте к нему общий доступ.

Рекомендуется не размещать общедоступный сетевой ресурс на системном диске или контроллере домена.

2. В созданный каталог скопируйте файлы Data1.cab, Sobol.msi, Sobol-x64.msi, находящиеся в каталоге Setup установочного компакт-диска комплекса "Соболь". Вызовите диалоговое окно настройки свойств каждого скопированного файла и удалите отметку (если она присутствует) в поле "Атрибуты: Только чтение" вкладки "Общие".
3. В случае использования шаблонов КЦ, отличных от шаблона КЦ по умолчанию, создайте файлы-шаблоны (например, *UserTemplate.xml* и *UserTemplate-x64.xml* для 32- и 64-разрядных компьютеров соответственно) и скопируйте их в сформированный общедоступный каталог.

Для создания командного файла — сценария установки:

Для компьютеров с 32- и 64-разрядной ОС Windows создаются отдельные сценарии с использованием соответствующих файлов-шаблонов КЦ (Sobol.msi/*UserTemplate.xml* и Sobol-x64.msi/*UserTemplate-x64.xml*).

1. Откройте текстовый редактор, позволяющий сохранять текст в кодировке ASCII.
2. В зависимости от выбранного варианта установки (обновления) ПО комплекса "Соболь" введите, к примеру, следующие команды:
   - для установки ПО комплекса "Соболь" на компьютер с 32-разрядной ОС Windows с шаблоном КЦ по умолчанию:
     ```
     start /wait msiexec /i "\\<Имя сетевого ресурса>\Distrib\
     Sobol.msi" /qn ALLUSERS=1
     ```
   - для установки ПО комплекса "Соболь" на компьютер с 32-разрядной ОС Windows с шаблоном КЦ, отличным от шаблона КЦ по умолчанию:
     ```
     start /wait msiexec /i "\\<Имя сетевого ресурса>\Distrib\
     Sobol.msi" /qn ALLUSERS=1 TEMPLATE_ACTUAL="\\<Имя сетевого
     ресурса>\Distrib\UserTemplate.xml"
     ```
   - для обновления ПО комплекса "Соболь" на компьютере с 32-разрядной ОС Windows с сохранением шаблона КЦ предыдущей версии:
     ```
     start /wait msiexec /i "\\<Имя сетевого ресурса>\Distrib\
     Sobol.msi" /qn ALLUSERS=1 REINSTALL=ALL REINSTALLMODE=vomus
     IS_MINOR_UPGRADE=1
     ```
   - для обновления ПО комплекса "Соболь" на компьютере с 32-разрядной ОС Windows с шаблоном КЦ, отличным от шаблона КЦ по умолчанию:
     ```
     start /wait msiexec /i "\\<Имя сетевого ресурса>\Distrib\
     Sobol.msi" /qn ALLUSERS=1 REINSTALL=ALL REINSTALLMODE=vomus
     IS_MINOR_UPGRADE=1 TEMPLATE_ACTUAL="\\<Имя сетевого
     ресурса>\Distrib\UserTemplate.xml"
     ```

Для установки и обновления ПО на компьютерах с 64-разрядной ОС Windows в соответствующих командах укажите файлы Sobol-x64.msi/*UserTemplate-x64.xml*.

3. Сохраните файл сценария с расширением cmd (например, *Scrypt.cmd*) в созданном общедоступном каталоге.

Для создания организационных подразделений:

1. На контроллере домена откройте оснастку "Active Directory — пользователи и компьютеры" ("Start | Administrative Tools | Active Directory Users and Computers") и выберите в дереве объектов домен, для компьютеров которого необходимо настроить автоматическую установку ПО.
2. Вызовите контекстное меню выбранного домена и активируйте команду "Создать" I "Подразделение" ("New | Organizational Unit"). Создайте в домене отдельные организационные подразделения для компьютеров с установленной 32- и 64-разрядной ОС Windows (например, "*AutosetupX32*" и "*AutosetupX64*" соответственно).
3. Переместите в созданные подразделения компьютеры домена, на которых необходимо выполнить автоматическую установку ПО комплекса "Соболь".

После выполнения автоматической установки ПО комплекса переместите компьютеры из созданных организационных подразделений обратно в исходные места домена.

Для создания групповых политик:

1. На контроллере домена откройте оснастку "Active Directory — пользователи и компьютеры" ("Active Directory Users and Computers"), выберите сформированное организационное подразделение, на компьютерах которого будет проводиться автоматическая установка, и вызовите диалоговое окно настройки свойств организационного подразделения.
2. Перейдите на вкладку "Групповая политика" и нажмите кнопку "Создать".

На контроллере домена на базе ОС Windows Server 2008 для создания групповой политики подразделения воспользуйтесь оснасткой "Управление групповой политикой" ("Start | Administrative Tools | Group Policy Management"). Перейдите к сформированному организационному подразделению и выберите для него "Create a GPO in this domain, and link it here…".

3. Введите имя создаваемой политики (например, "*AutosetupX32*"/ "*AutosetupX64*") и нажмите клавишу <Enter>.
4. Нажмите кнопку "Изменить" ("Edit").

   На экране появится окно редактора групповых политик.
5. В дереве объектов политики перейдите к разделу "Конфигурация компьютера" I "Конфигурация Windows" I "Сценарии" ("Computer Configuration | Policies | Windows Settings | Scripts (Startup/Shutdown)") и вызовите диалоговое окно настройки свойств параметра "Автозагрузка" ("Startup").
6. В диалоговом окне нажмите кнопку "Добавить" ("Add").

   На экране появится диалог "Добавление сценария".
7. Заполните поля диалога:
   - в поле "Имя сценария" введите полное имя (с указанием пути) файла сценария, размещенного в общедоступном сетевом ресурсе (например, \\<Имя сетевого ресурса>*Distrib**Scrypt.cmd*);
   - в поле "Параметры сценария" введите сетевой путь к общедоступному каталогу (например, \\<Имя сетевого ресурса>*Distrib*).
8. Нажмите "ОК", затем в диалоговом окне настройки свойств последовательно нажмите кнопки "Применить", "ОК" и закройте остальные окна.

Совет. Если для автоматической установки ПО используется несколько организационных подразделений, то создавать отдельные групповые политики для каждого подразделения необязательно. В остальных подразделениях можно добавить ссылку на созданную групповую политику первого подразделения (для этого используйте кнопку "Добавить" на вкладке "Групповая политика" в окне настройки свойств организационного подразделения).

Для включения централизованной установки ПО комплекса:

1. На контроллере домена откройте оснастку "Active Directory — пользователи и компьютеры" ("Active Directory Users and Computers"), выберите организационное подразделение, на компьютерах которого будет проводиться автоматическая установка, и вызовите диалоговое окно настройки свойств организационного подразделения.
2. Перейдите на вкладку "Групповая политика", выберите политику автоматической установки ПО и нажмите кнопку "Изменить" ("Edit").

   На экране появится окно редактора групповых политик.

На контроллере домена на базе ОС Windows Server 2008 для создания групповой политики подразделения воспользуйтесь оснасткой "Управление групповой политикой" ("Start | Administrative Tools | Group Policy Management").

3. В дереве объектов политики перейдите к разделу "Конфигурация компьютера" I "Административные шаблоны" I "Система" ("Computer Configuration | Policies | Administrative Template| System") и в зависимости от ОС контроллера домена установите значения параметров, приведенные ниже в таблицах.

Табл. 2. Параметры для ОС Windows Server 2003, Server 2008

Подраздел	Параметр	Значение
Вход в систему (Logon)	Всегда ожидать инициализации сети при загрузке и входе в систему (Always wait for the network at computer startup and logon)	Включен
Сценарии (Scripts)	Асинхронное выполнение сценариев загрузки (Run startup scripts asynchronously)	Отключен
Групповая политика (Group policy)	Обработка политики сценариев (Scripts policy processing)	Включен
	Не применять во время периодической фоновой обработки (Do not apply during periodic background processing)	Поставить отметку
	Обрабатывать, даже если объекты групповой политики не изменились (Process even if the Group Policy objects have not changed)	Поставить отметку

Пояснение. Механизм автоматической установки ПО комплекса "Соболь" начинает действовать на компьютерах после обновления групповых политик на этих компьютерах. Применение заданных групповых политик осуществляется на компьютерах автоматически в соответствии с установленным режимом обновления политик. Для немедленного применения групповых политик на отдельном компьютере используйте стандартные средства (например, локальная утилита gpupdate).

Автоматическая установка осуществляется на этапе загрузки компьютера до входа пользователя в систему, поэтому для запуска процесса установки пользователю необходимо перезагрузить компьютер.

Подготовка комплекса к инициализации

Для подготовки к инициализации:

1. Переключите плату комплекса "Соболь" в режим инициализации. Для этого снимите перемычку, установленную на разъеме **J0** платы (см. Рис. 2, 3).

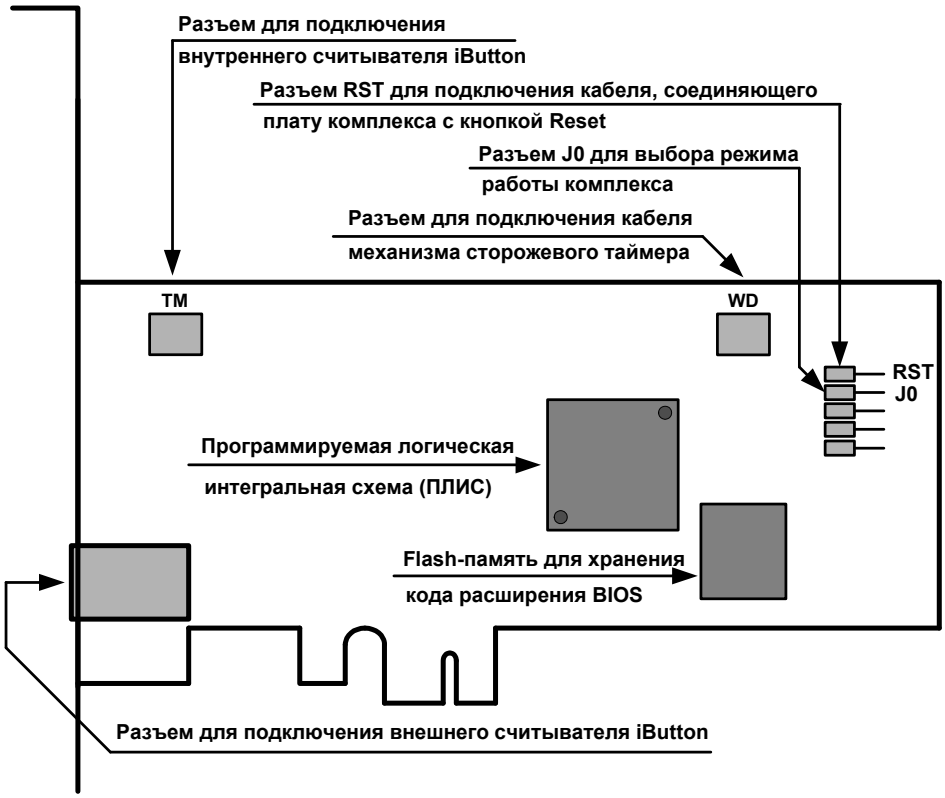


Рис. 2. Расположение разъемов на плате комплекса "Соболь" для шины PCI-E

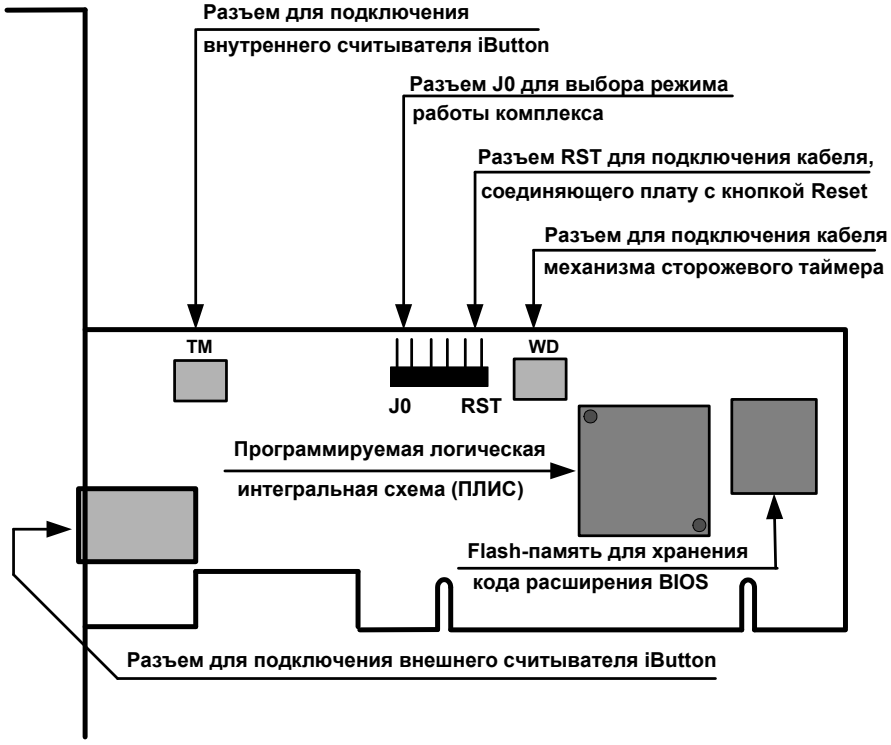


Рис. 3. Расположение разъемов на плате комплекса "Соболь" для шины PCI

2. Выключите компьютер.
3. Вскройте корпус системного блока.
4. Для использования механизма сторожевого таймера:
   - отключите штекер стандартного кабеля кнопки "Reset" от разъема Reset, расположенного на материнской плате;
   - подключите штекер стандартного кабеля кнопки "Reset" к разъему **RST** платы комплекса "Соболь" (см. Рис. 2 , Рис. 3 на стр. 22);
   - подключите штекер кабеля механизма сторожевого таймера, входящего в комплект поставки, к разъему платы **WD**. Затем подключите другой штекер этого кабеля к разъему Reset, расположенному на материнской плате.
5. Выберите свободный слот системной шины PCI-E/PCI и аккуратно вставьте в него соответствующую плату комплекса "Соболь".
6. При необходимости подключите к плате считыватель iButton:
   - при использовании внешнего считывателя подключите его штекер к разъему платы, расположенному на задней панели системного блока;
   - при использовании внутреннего считывателя подключите его штекер к разъему **TM**.
7. Закройте корпус системного блока.

Инициализация комплекса

Инициализация комплекса "Соболь" выполняется в следующем порядке:

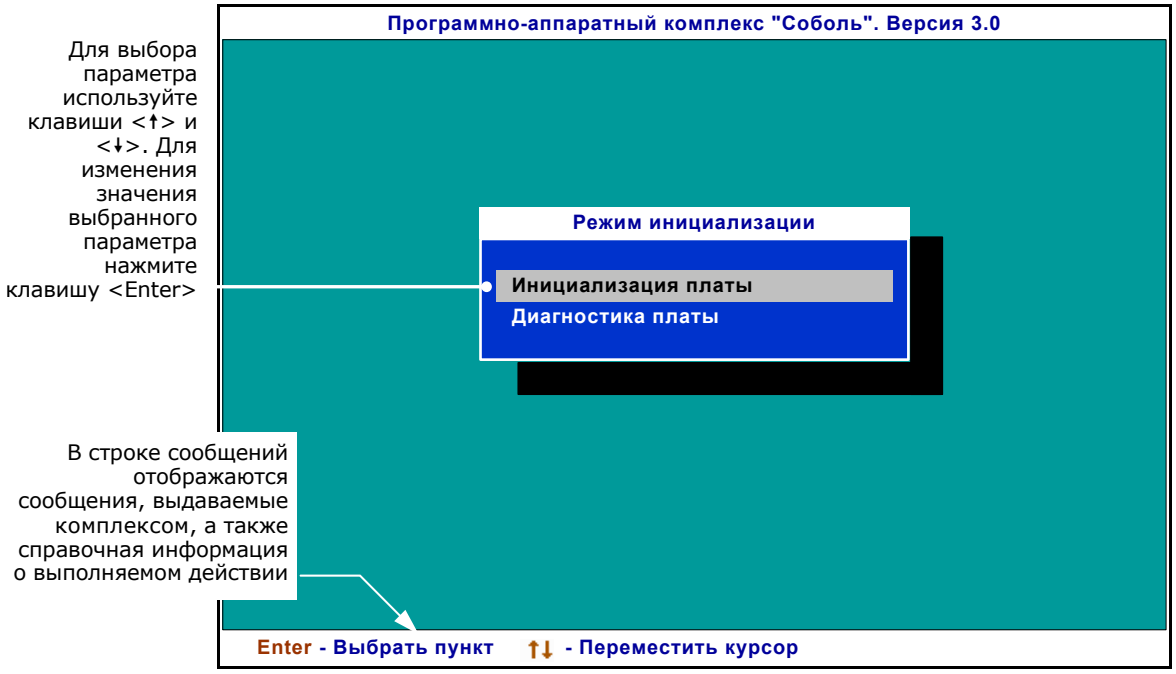
1. Запуск процедуры инициализации (см. ниже)
2. Настройка общих параметров комплекса (см. стр. 24)
3. Настройка контроля целостности (см. стр. 26)
4. Регистрация администратора комплекса (см. стр. 26)
5. Расчет контрольных сумм (см. стр. 29)

Внимание! Перед запуском процедуры инициализации отключите от USB-портов компьютера все устройства класса USB Mass Storage Device (flash-накопители, CD-, DVD-приводы и т. п.).

Шаг 1. Запуск процедуры инициализации

1. Включите питание компьютера.

   На экране появится окно:



Если после включения питания компьютера управление не было передано модулю расширения BIOS комплекса, то окно, показанное на рисунке, на экране не появится. В этом случае необходимо в BIOS Setup разрешить загрузку операционной системы с модулей расширения BIOS сетевых плат.

В центре окна располагается меню режима инициализации.

Совет. Прежде чем приступить к инициализации, рекомендуется проверить работоспособность комплекса "Соболь". Для этого выберите в меню команду "Диагностика платы" и нажмите клавишу <Enter>. В появившемся на экране меню выберите команду "Выполнить все тесты" и нажмите клавишу <Enter>. После успешного завершения всех тестовых процедур нажмите клавишу <Esc>. Подробные инструкции по проведению контроля работоспособности содержатся на стр. 50.

2. Выберите в меню команду "Инициализация платы" и нажмите <Enter>.

Шаг 2. Настройка общих параметров

На экране появится следующий диалог:

Общие параметры системы

Версия криптографической схемы	-	2.0
Число попыток тестирования ДСЧ	-	3
Тестирование ДСЧ для пользователя	-	Да
Показ статистики пользователю	-	Нет
Минимальная длина пароля	-	8
Предельное число неудачных входов пользователя	-	65535
Время ожидания сторожевого таймера (сек.)	-	18
Период тестирования сторожевого таймера (дней)	-	0
Поддержка USB-идентификаторов	-	Нет

Рис. 4. Диалог настройки общих параметров (режим инициализации)

Назначение общих параметров разъясняется в Табл. 3 на стр. 25, за исключением параметра "Версия криптографической схемы", настройка которого выполняется только при инициализации комплекса "Соболь" и является обязательной.

Внимание! Администратор, обслуживающий несколько комплексов "Соболь", должен на всех обслуживаемых комплексах установить одинаковую версию криптографической схемы.

Установите для параметра "Версия криптографической схемы" значение:

- "2.0" — если не требуется обеспечивать совместимость с предыдущими версиями комплекса. Рекомендуется выбирать это значение параметра.

  Пояснение. В этом случае невозможна повторная регистрация администратора (см. ниже) и пользователей (см. стр. 39) данного комплекса "Соболь" на комплексах предыдущих версий. Также невозможна повторная регистрация администратора и пользователей комплексов предыдущих версий на данном комплексе "Соболь".

- "1.0" — чтобы обеспечить совместимость с предыдущими версиями комплекса.

1. Для настройки параметра выберите клавишей <↑> или <↓> строку с его названием и нажмите клавишу <Enter>. В зависимости от выбранного параметра:
   - значение изменится на противоположное ("Да" или "Нет");
   - появится диалог для ввода значения параметра. В этом случае введите значение с клавиатуры и нажмите клавишу <Enter>;

     Совет. При исправлении ошибок ввода используйте клавиши <←> и <→> для перемещения курсора, а клавиши <Backspace> или <Delete> — для удаления символа. Нажмите клавишу <Esc>, чтобы отказаться от изменения значения.

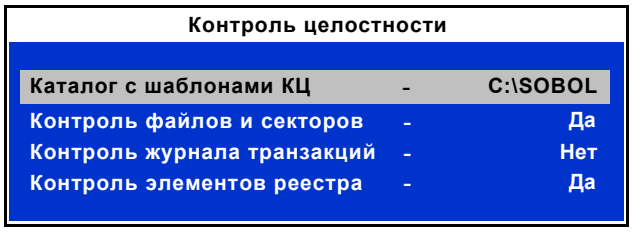
   - параметр "Поддержка USB-идентификаторов" может принимать три значения — "Нет"/"2.0"/"1.1".
2. Выполнив настройку параметров, нажмите клавишу <Esc> для сохранения изменений и переходу к настройке контроля целостности.

Табл. 3. Общие параметры комплекса "Соболь" (режим инициализации)

Число попыток тестирования ДСЧ
Определяет число попыток тестирования правильности работы ДСЧ комплекса "Соболь", выполняемого при входе в систему пользователей. Параметр может принимать значения от 1 до 3. Тестирование ДСЧ выполняется до первой удачной попытки, после чего тестирование прекращается и считается завершившимся успешно. Работа комплекса продолжается. Если же число неудачных попыток тестирования ДСЧ достигло числа, заданного данным параметром, выдается сообщение об ошибке тестирования ДСЧ и компьютер блокируется для входа всех пользователей, включая администратора.
Тестирование ДСЧ для пользователя
Позволяет включить или отключить тестирование правильности работы ДСЧ комплекса "Соболь", выполняющееся при входе в систему пользователей. Тестирование ДСЧ при входе в систему администратора отключить нельзя, оно выполняется всегда. Параметр может принимать два значения: "Да" — тестирование ДСЧ выполняется или "Нет" — тестирование ДСЧ отключено.
Показ статистики пользователю
Позволяет разрешить или запретить вывод на экран информационного окна, содержащего статистические сведения о работе пользователя. Окно появляется на экране после успешной идентификации пользователя. Параметр может принимать два значения: "Да" — разрешить вывод окна или "Нет" — запретить вывод окна.
Минимальная длина пароля
Определяет минимальную длину пароля пользователя в символах. Пользователю нельзя назначить пароль, число символов в котором меньше числа, заданного этим параметром. Параметр может принимать значения от 0 до 16. Если значение этого параметра равно "0", пользователю можно назначить пустой пароль, разрешив ему входить в систему без указания пароля (запрос пароля на экране не появится). Если при увеличении значения этого параметра длина паролей некоторых пользователей окажется меньше нового значения параметра, при входе в систему им будет предложено сменить свой старый пароль, без чего они не смогут загрузить ОС.
Предельное число неудачных входов пользователя
Определяет, сколько раз пользователь может допустить ошибку при входе в систему, указав неверный пароль. Параметр может принимать значения от 0 до 65535. Значение "0" означает, что число неудачных попыток входа пользователей в систему не ограничено. Если число неудачных попыток входа пользователя в систему равно числу, заданному этим параметром, вход этого пользователя в систему будет автоматически блокирован. Если текущее число неудачных входов пользователя в систему меньше значения этого параметра и данный пользователь успешно вошел в систему, то значение счетчика неудачных попыток входа автоматически сбрасывается (приравнивается нулю).
Время ожидания сторожевого таймера
Определяет интервал времени в секундах, по истечении которого осуществляется автоматическая перезагрузка компьютера, при условии, что за это время управление не передано расширению BIOS комплекса "Соболь". Рекомендуемое время ожидания сторожевого таймера определяется автоматически на этапе инициализации комплекса. В дальнейшем администратор может корректировать значения от 6 до 512 секунд с дискретностью 2 секунды (6, 8, 10, 12 и т. д.). Для использования данного механизма необходимо правильно подключить к плате комплекса "Соболь" кабель механизма сторожевого таймера (см. п. **4** процедуры на стр. 23). Если кабель не подключен — механизм сторожевого таймера не действует.
Период тестирования сторожевого таймера
Определяет периодичность, с которой будет выполняться процедура тестирования механизма сторожевого таймера. Параметр может принимать значения от 0 до 999 дней. Значение "0" означает, что тестирование механизма сторожевого таймера не выполняется. Процедура тестирования механизма сторожевого таймера выполняется при входе пользователя в систему с периодичностью, заданной данным параметром.
Поддержка USB-идентификаторов
Задает типы персональных идентификаторов. Параметр может принимать три значения: • "Нет" — вход в систему осуществляется только с помощью идентификаторов iButton. • "2.0" — вход в систему может осуществляться с помощью идентификаторов iButton, eToken PRO, iKey 2032, Rutoken S, Rutoken RF S. Рекомендуется выбирать это значение параметра. Если при входе произошла ошибка, в результате которой вход в систему невозможен, выберите значение "1.1". • "1.1" — вход в систему может осуществляться с помощью идентификаторов iButton, eToken PRO, iKey 2032, Rutoken S, Rutoken RF S. При этом после входа в систему будет невозможна загрузка с USB-дисков. Рекомендуется выбирать это значение в случае, если невозможен вход в систему при значении параметра "2.0".

Шаг 3. Настройка контроля целостности

На экране появится следующий диалог:



1. Для настройки параметра выберите клавишей <↑> или <↓> строку с его названием и нажмите <Enter>. В зависимости от выбранного параметра:
   - появится диалог для ввода значения параметра. В этом случае введите значение с клавиатуры и нажмите клавишу <Enter>;
   - значение изменится на противоположное ("Да" или "Нет").

Файлы шаблонов КЦ хранятся:

- для ОС Windows и МСВС 3.0 — в каталоге, имя и местоположение которого указывается в программе управления шаблонами КЦ в окнах "О программе" и "Информация" (см. документ [2]) соответственно;
- для VMware ESX — в каталоге /boot/sobol (см. документ [3]).

Если каталог с файлами шаблонов КЦ не найден или в этом каталоге отсутствуют файлы шаблонов ненулевой длины, то параметрам "Контроль файлов и секторов", "Контроль элементов реестра" присваивается значение "Нет".

При попытке изменить значение параметра "Каталог с шаблонами КЦ" для указания точного пути к каталогу с файлами шаблонов на экране появится диалоговое окно. Введите путь к заданному каталогу, который отображается:

- в строке "BIOS платы" окна "О программе" для ОС Windows;
- в строке "BIOS платы" окна "Информация" для ОС МСВС 3.0;
- в результате выполнения команды scheck--ls-path для ОС VMware ESX

и нажмите клавишу <Enter>.

Учитывайте, что для каталогов, размещающихся на дисках с файловой системой FAT16 и FAT32, длинные имена (более 8 символов) нужно указывать в краткой форме, например "progra~1". Узнать краткую форму записи имени можно с помощью команды DIR или менеджеров файлов, например, Total Commander.

При обнаружении заданного каталога и находящихся в нем файлов шаблонов КЦ параметры "Контроль файлов и секторов", "Контроль элементов реестра" примут значение "Да", иначе значение параметров не изменится и на экране появится сообщение "Отсутствуют файлы шаблонов контроля целостности либо неверно указан путь к файлам шаблонов в программно-аппаратном комплексе".

2. Выполнив настройку параметров, нажмите клавишу <Esc> для продолжения инициализации комплекса.

   Начнется тестирование правильности работы ДСЧ.

   - Если тестирование ДСЧ завершилось с ошибкой, в строке сообщений появится сообщение об этом. Для продолжения работы требуется перезагрузить компьютер — нажмите любую клавишу. В строке сообщений появится дополнительное сообщение о необходимости перезагрузки. Нажмите еще раз любую клавишу. Компьютер будет перезагружен.
   - Если тестирование ДСЧ завершено успешно (получен положительный результат), инициализация комплекса будет продолжена.

Шаг 4. Регистрация администратора

На экране появится запрос:

При регистрации администратора ему назначается пароль для входа в систему и присваивается персональный идентификатор. Процедура регистрации может выполняться в одном из двух вариантов: первичная (см. ниже) и повторная (см. стр. 29).

Первичная регистрация администратора. При ее выполнении в персональный идентификатор администратора записывается новая служебная информация о регистрации. Если идентификатор содержит служебную информацию, например, записанную в идентификатор при инициализации другого комплекса "Соболь", она будет уничтожена и администратор не сможет управлять работой другого комплекса.

Совет. Прежде чем приступить к первичной регистрации администратора, приготовьте нужное количество персональных идентификаторов, в том числе и для создания резервных копий персонального идентификатора администратора.

Повторная регистрация администратора. При ее выполнении служебная информация, записанная в персональный идентификатор при первичной регистрации администратора, считывается из идентификатора без изменения, что позволяет администратору использовать один и тот же идентификатор для входа в систему на нескольких компьютерах, оснащенных комплексами "Соболь".

Рекомендации.

- Если при регистрации администратора будут предъявлены идентификаторы Rutoken S / Rutoken RF S/iKey 2032/eToken PRO, ранее не использовавшиеся в комплексе "Соболь" и имеющие PIN-коды, отличные от PIN-кодов по умолчанию (для Rutoken S/Rutoken RF S — **12345678**, для iKey 2032 — **default SO password.**, для eToken PRO — **1234567890**), то на экране появится окно запроса на ввод PIN-кода идентификатора. Введите его PIN-код и нажмите "Enter".
- Если при регистрации администратора будет предъявлен неинициализированный идентификатор eToken PRO (USB-ключ, смарт-карта), то на экране появится окно с сообщением об отсутствии в нем файловой системы. Выполните инициализацию предъявленного eToken PRO стандартными программными средствами компании — производителя идентификатора.
- Если при установке нескольких комплексов "Соболь" на первом из них выполняется первичная регистрация администратора, а на всех остальных — повторная, то администратор сможет управлять всеми комплексами, используя один и тот же персональный идентификатор.
- При выполнении повторной инициализации находящегося в эксплуатации комплекса "Соболь" рекомендуется проводить повторную регистрацию администратора.

Для первичной регистрации администратора:

1. Выберите вариант "Да" и нажмите клавишу <Enter>.

   На экране появится диалог для ввода пароля администратора.

2. Введите с клавиатуры пароль администратора и нажмите клавишу <Enter>.

   При вводе нового пароля соблюдайте следующие правила:

   - пароль может содержать латинские символы, цифры и служебные символы;
   - разрешается использовать различные регистры клавиатуры (например, "Dog" или "dog"). При этом помните, что заглавные и строчные буквы считаются различными ("Dog" и "dog" — это разные пароли);
   - количество символов в пароле (длина пароля) не может быть меньше числа, заданного общим параметром "Минимальная длина пароля" (см. стр. 25), и не может превышать 16 символов. Если значение указанного параметра равно "0", можно назначить администратору пустой пароль. Для этого нажмите клавишу <Enter>, оставив поле ввода пароля пустым.

   На экране появится диалог для подтверждения пароля администратора.

3. Повторно введите тот же пароль и нажмите клавишу <Enter>.

   При обнаружении ошибок в строке сообщений появится сообщение об этом. Нажмите любую клавишу и повторите ввод нового пароля еще раз.

   Если оба значения пароля совпали и длина пароля не меньше заданной минимальной длины пароля, на экране появится запрос на предъявление персонального идентификатора.

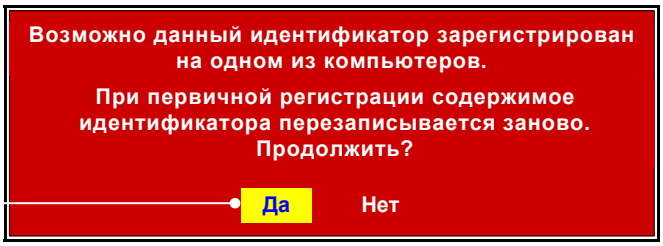
4. Предъявите идентификатор, присваиваемый администратору комплекса.

Если идентификатор предъявлен неправильно, то окно запроса останется на экране. Повторите предъявление идентификатора.

При присвоении персонального идентификатора в него записывается служебная информация.

- Если идентификатор регистрировался ранее на другом компьютере и уже содержит служебную информацию, на экране появится предупреждение:

Если вы уверены в том, что данный идентификатор никем больше не используется, предъявите его, выберите вариант "Да" и нажмите клавишу <Enter>



Помните, что при записи информации в персональный идентификатор служебная информация, содержащаяся в его памяти, будет полностью утеряна без возможности восстановления. При этом пользователь, которому принадлежит этот идентификатор, не сможет больше воспользоваться им для входа в систему.

Нажмите клавишу <Esc> и повторите действие **4**, используя другой персональный идентификатор.

- Если же структура данных персонального идентификатора нарушена или в нем недостаточно свободного места для записи служебной информации, на экране появятся соответствующие запросы на его форматирование:

или

При форматировании идентификатора iButton вся информация, содержащаяся в его памяти, будет полностью утеряна без возможности восстановления. При форматировании USB-идентификатора будет утеряна только информация, относящаяся к ПАК "Соболь" и программам, его использующим. Для отказа от форматирования нажмите <Esc>, на экране вновь появится запрос персонального идентификатора.

Если вы уверены в том, что данный персональный идентификатор необходимо форматировать, выберите вариант "Да" и нажмите клавишу <Enter>.

На экране появится повторный запрос:

Для выполнения форматирования выберите вариант "Да", предъявите идентификатор и нажмите клавишу <Enter>.

После того как администратору будет присвоен персональный идентификатор, на экране появится запрос, предлагающий создать резервную копию персонального идентификатора администратора:

Если вы уверены в том, что создавать резервные копии не требуется, выберите вариант "Нет" и нажмите клавишу <Enter>

Рекомендуется создать как минимум одну резервную копию персонального идентификатора администратора. Созданные резервные копии могут использоваться администратором для экстренного входа в систему в тех случаях, когда оригинал испорчен или утерян.

5. Выберите вариант "Да" и нажмите клавишу <Enter>.

   На экране появится запрос персонального идентификатора.

6. Предъявите персональный идентификатор, приготовленный для создания резервной копии идентификатора администратора.

   Пояснение. При появлении на экране запросов и сообщений действуйте в соответствии с инструкциями п. **4** данной процедуры.

   При успешном создании резервной копии на экране появится запрос, предлагающий создать еще одну резервную копию идентификатора.

7. Выберите вариант продолжения процедуры:
   - Для создания очередной резервной копии еще раз выполните действия **5**, **6**.
   - Если необходимое количество резервных копий уже создано, выберите вариант "Нет" и нажмите клавишу <Enter>.

Перейдите к выполнению заключительного этапа инициализации — расчету контрольных сумм.

Для повторной регистрации администратора:

1. Выберите в окне запроса вариант "Нет" и нажмите клавишу <Enter>.

   На экране появится диалог для ввода пароля администратора.

2. Введите с клавиатуры пароль, назначенный администратору при его первичной регистрации на другом комплексе "Соболь", и нажмите клавишу <Enter>.

   На экране появится запрос на предъявление идентификатора.

3. Предъявите персональный идентификатор, присвоенный администратору при его первичной регистрации на другом комплексе "Соболь".

   При успешном предъявлении идентификатора выполняется сопоставление введенного пароля с информацией, хранящейся в памяти идентификатора.
   - Если введенный пароль указан неверно или предъявлен не принадлежащий администратору идентификатор, то в строке сообщений появится сообщение об ошибке. До тех пор пока USB-ключ находится в разъеме USB/идентификатор iButton касается считывателя/смарт-карта находится в USB-считывателе, сообщение будет присутствовать на экране. После изъятия идентификатора на экране вновь появится запрос, предлагающий выбрать режим регистрации администратора.
   - Если введенный пароль соответствует предъявленному идентификатору, выполняется считывание служебной информации из идентификатора и запись этой информации в энергонезависимую память комплекса.

Шаг 5. Расчет контрольных сумм

В том случае, если параметру "Контроль файлов и секторов" либо "Контроль элементов реестра" присвоено значение "Да" (см. стр. 26), на экране появится запрос, предлагающий рассчитать контрольные суммы:

Чтобы отказаться от расчета контрольных сумм, выберите вариант "Нет" и нажмите клавишу <Enter>

1. Выберите вариант "Да" и нажмите клавишу <Enter>.

   Начнется расчет эталонных значений контрольных сумм объектов, заданных исходными шаблонами КЦ, при этом на экране будет отображаться процесс расчета.

   Если при расчете контрольных сумм не найдены один или несколько файлов, секторов или элементов реестра, заданных шаблонами КЦ, по окончании процедуры расчета на экране появятся следующие запросы:

   Выберите вариант продолжения процедуры и нажмите клавишу <Enter>:

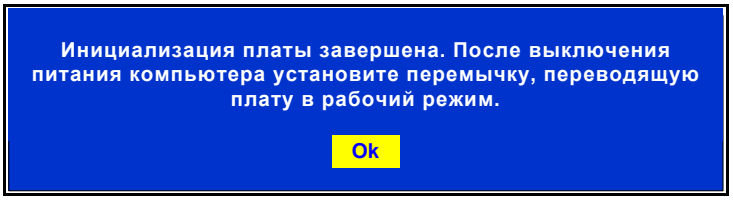
   - "Да" — для отключения контроля целостности файлов и секторов, элементов реестра, выполняемого при входе пользователей в систему.

     Пояснение. В этом случае следует выполнить корректировку шаблонов КЦ (см. стр. 58), рассчитать эталонные значения контрольных сумм (см. стр. 70) и включить контроль целостности (см. стр. 26).

   - "Нет" — чтобы не отключать контроль целостности.

     Пояснение. В этом случае контроль целостности будет выполняться с ошибками, что приведет к невозможности входа пользователей в систему. Завершив инициализацию, обязательно выполните корректировку шаблонов КЦ (см. стр. 58), затем повторно рассчитайте эталонные значения контрольных сумм (см. стр. 70).

   По окончании инициализации на экране появится сообщение:



2. Нажмите "OK".

   Компьютер выключится автоматически.

   Если выключение не произойдет, то в строке сообщений появится сообщение "Теперь компьютер можно выключить...". Выключите компьютер самостоятельно.

Далее переключите комплекс в режим эксплуатации.

Подготовка комплекса к эксплуатации

Для подготовки к эксплуатации:

1. Выключите компьютер. Вскройте корпус системного блока.
2. При наличии подключенного к плате комплекса "Соболь" считывателя iButton отсоедините считыватель от платы:
   - при использовании внешнего считывателя отключите его штекер от разъема платы, расположенного на задней панели системного блока;
   - при использовании внутреннего считывателя отключите его штекер от разъема **TM**.
3. Аккуратно извлеките плату комплекса "Соболь" из разъема шины PCI-E/PCI.
4. Установите перемычку на разъеме **J0** платы (см. Рис. 2 , Рис. 3 на стр. 22).
5. Аккуратно вставьте плату комплекса "Соболь" в разъем системной шины PCI-E/PCI и закрепите планку крепления платы крепежным винтом.
6. При необходимости подключите к плате считыватель iButton:
   - при использовании внешнего считывателя подключите его штекер к разъему платы, расположенному на задней панели системного блока;
   - при использовании внутреннего считывателя подключите его штекер к разъему **TM**.
7. Закройте корпус системного блока.

Выполнив все указанные действия, включите компьютер и перейдите к настройке комплекса "Соболь" (см. стр. 33).

На компьютерах, работающих под управлением ОС Windows XP/2003, при первом входе в систему после установки комплекса "Соболь" на экране появится начальный диалог мастера установки оборудования. Для завершения установки комплекса пройдите все шаги мастера оборудования, оставляя без изменения значения параметров, предлагаемые мастером по умолчанию.

Обновление программного обеспечения

Порядок обновления программного обеспечения комплекса "Соболь" в среде ОС МСВС 3.0, VMware ESX рассмотрен в документах [2] и [3] соответственно.

Для обновления версии программного обеспечения комплекса "Соболь" выполните установку новой версии программного обеспечения так, как это описано на стр. 16. В процессе установки компоненты старой версии будут автоматически заменены компонентами новой версии.

Для сохранения шаблонов КЦ предыдущей версии ПО комплекса отметьте поле "Учитывать шаблоны контроля целостности от предыдущей версии ПО" диалога "Параметры настройки шаблонов КЦ".

Удаление комплекса

Следует обратить внимание на то, что после удаления комплекса "Соболь" из компьютера вся служебная информация о настройке комплекса сохраняется в неизменном виде в его энергонезависимой памяти. Поэтому данный комплекс без повторной инициализации можно установить и эксплуатировать на данном или другом компьютере при условии сохранности регистрационной информации в персональных идентификаторах администратора и пользователей. В связи с этим после удаления комплекса администратор должен обеспечить условия хранения платы комплекса, исключающие возможность бесконтрольного доступа к ней. Для удаления служебной информации из памяти комплекса используйте процедуру инициализации в режиме первичной регистрации администратора (см. стр. 26).

Удаление комплекса "Соболь" осуществляется в следующем порядке:

- удаление программного обеспечения (см. ниже);
- изъятие платы комплекса из компьютера (см. ниже).

Удаление программного обеспечения

Порядок удаления программного обеспечения комплекса "Соболь" в среде ОС МСВС 3.0, VMware ESX рассмотрен в документах [2] и [3] соответственно.

Удаление ПО комплекса "Соболь" можно выполнить как с помощью программы установки, так и стандартными средствами операционных систем.

Для удаления с помощью программы установки:

1. Поместите установочный компакт-диск в привод DVD/CD-ROM и запустите на исполнение файл Setup.exe.

   Программа установки выполнит подготовку к работе. После завершения подготовительных действий на экране появится стартовый диалог программы установки.

2. Нажмите кнопку "Далее >".

   На экране появится диалог, предлагающий начать процедуру удаления.

3. Нажмите кнопку "Удалить".

   Ход процесса удаления отображается на экране в виде индикатора прогресса. После успешного выполнения процедуры удаления на экране появится завершающий диалог программы установки.

4. Нажмите кнопку "Готово".

Изъятие платы комплекса из компьютера

Если после удаления программного обеспечения плата комплекса "Соболь" не извлечена из компьютера, то при каждой загрузке ОС Windows XP/2003/Vista/7/2008 на экране будет появляться сообщение об обнаружении неизвестного устройства.

Для изъятия платы из компьютера:

1. Выключите компьютер (если он включен).
2. Вскройте корпус системного блока.
3. При наличии подключенного к плате комплекса "Соболь" считывателя iButton отсоедините считыватель от платы:
   - при использовании внешнего считывателя отключите его штекер от разъема платы, расположенного на задней панели системного блока;
   - при использовании внутреннего считывателя отключите его штекер от разъема **TM** (см. Рис. 2 , Рис. 3 на стр. 22).
4. Отверните винт, которым закреплена планка крепления платы, и аккуратно извлеките плату комплекса "Соболь" из разъема системной шины PCI-E/PCI.
5. Если использовался механизм сторожевого таймера, отключите кабель, обеспечивавший работу этого механизма, от разъема **WD** платы комплекса "Соболь" и от разъема Reset, находящегося на материнской плате. Затем отключите штекер кабеля кнопки "Reset" от разъема платы **RST** и подключите этот штекер к разъему Reset, находящемуся на материнской плате.
6. Закройте корпус системного блока.

Глава 3

Настройка и эксплуатация комплекса

При вводе комплекса в эксплуатацию администратору необходимо:

- настроить общие параметры комплекса (см. стр. 36);
- зарегистрировать пользователей комплекса (см. стр. 39);
- настроить параметры работы пользователей (см. стр. 44);
- настроить механизм контроля целостности (см. стр. 56).

В процессе эксплуатации комплекса администратор может:

- управлять общими параметрами комплекса (см. стр. 36);
- управлять списком пользователей и параметрами их работы (см. стр. 39);
- менять свой пароль и аутентификатор (см. стр. 46);
- менять пароли и аутентификаторы других пользователей (см. стр. 45);
- просматривать записи журнала регистрации событий (см. стр. 53);
- управлять работой механизма контроля целостности (см. стр. 56);
- осуществлять ряд служебных операций (см. стр. 54).

Общий порядок настройки

Настройка комплекса "Соболь" выполняется в следующем порядке:

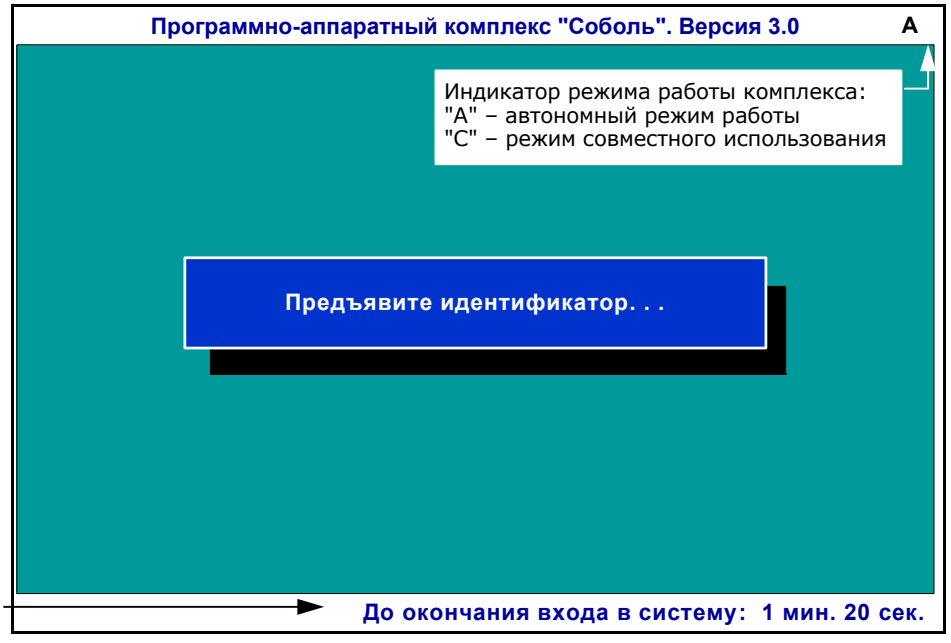
1. Вход в систему администратора (см. ниже).
2. Настройка комплекса (см. стр. 35).
3. Загрузка или выключение компьютера (см. стр. 35).

Внимание! Перед входом в систему отключите от USB-портов компьютера все устройства класса USB Mass Storage Device (flash-накопители, CD-, DVD-приводы и т. п.).

Шаг 1. Вход в систему

1. Включите питание компьютера или выполните перезагрузку компьютера.

   На экране появится окно с запросом персонального идентификатора:



Строка сообщений. В данном случае строка содержит счетчик времени, оставшегося пользователю для предъявления идентификатора и ввода пароля

Обратите внимание на следующие особенности процедуры входа в систему.

- При включенном режиме ограничения времени, отводящегося пользователю на вход в систему (см. стр. 37, параметр "Ограничение времени на вход в систему"), в строке сообщений будет отсчитываться время в минутах и секундах, оставшееся пользователю для предъявления идентификатора и ввода пароля. Если пользователь не успел за отведенное время выполнить эти действия, на экране появится сообщение о завершении сеанса входа в систему. Чтобы повторить попытку входа, нажмите клавишу <Enter>, а затем — любую клавишу.
- При включенном режиме автоматического входа в систему (см. стр. 38, параметр "Время ожидания автоматического входа в систему") в строке сообщений будет отсчитываться время в секундах, оставшееся до загрузки операционной системы.

2. Предъявите персональный идентификатор администратора.

После успешного считывания информации из идентификатора на экране появится диалог для ввода пароля:

3. Введите пароль администратора.

Все введенные символы отображаются знаком "✳". Если при вводе пароля допущены ошибки, вы можете исправить их. Используйте клавиши <←> и <→> для перемещения курсора, а клавиши <Backspace> или <Delete> для стирания символа. Для отказа от ввода пароля нажмите клавишу <Esc>, после чего на экране вновь появится запрос персонального идентификатора.

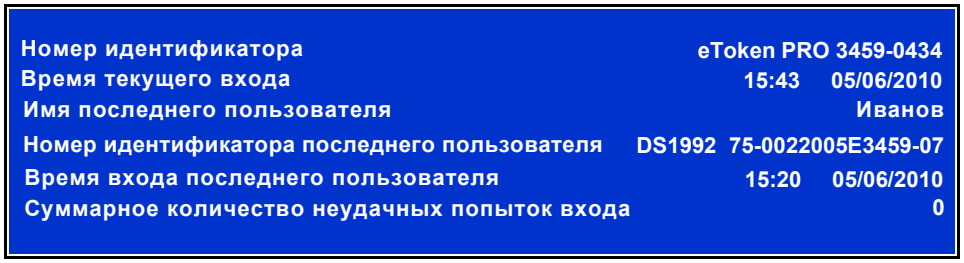
4. Нажмите клавишу <Enter>.

Если введенный пароль не соответствует предъявленному идентификатору, в строке сообщений появится сообщение: "Неверный персональный идентификатор или пароль". Нажмите любую клавишу и повторите еще раз действия **2**–**4**. Используйте персональный идентификатор администратора и не допускайте ошибок при вводе пароля.

При вводе правильного пароля начнется процедура тестирования датчика случайных чисел, а в строке сообщений появится сообщение об этом.

Если тестирование датчика случайных чисел завершилось с ошибкой, то в строке сообщений появится соответствующее сообщение. Для продолжения работы нажмите любую клавишу. Для перезапуска компьютера еще раз нажмите любую клавишу. Если после перезапуска тестирование датчика случайных чисел вновь завершилось с ошибкой, обратитесь за помощью в службу технической поддержки поставщика комплекса.

При успешном завершении тестирования на экране появится информационное окно, подобное следующему:



Разъяснение информации, содержащейся в этом окне, приводится на стр. 71.

5. Для продолжения работы нажмите любую клавишу.

На экране появится меню администратора:

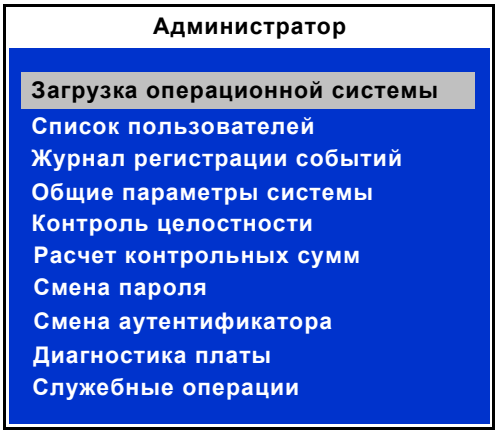


Рис. 5. Меню администратора

Пояснение. При эксплуатации комплекса в режиме совместного использования часть команд меню будет недоступна. Об особенностях настройки комплекса в этом режиме читайте на стр. 82.

Все действия, выполняемые администратором при настройке и эксплуатации комплекса "Соболь", осуществляются посредством этого меню.

Совет. Во время работы с комплексом можно в любой момент запросить дополнительную техническую информацию о комплексе. Для этого нажмите клавишу <F1>. На экране появится информационное окно. Чтобы продолжить работу, нажмите любую клавишу.

Шаг 2. Настройка комплекса

1. Выберите в меню администратора команду и нажмите клавишу <Enter>:
   - "Список пользователей" — команда используется для управления пользователями комплекса (см. стр. 39);
   - "Журнал регистрации событий" — для просмотра записей журнала (см. стр. 53);
   - "Общие параметры системы" — для настройки общих параметров комплекса (см. стр. 36);
   - "Контроль целостности" — для настройки параметров функционирования механизма контроля целостности (см. стр. 38);
   - "Расчет контрольных сумм" — для расчета эталонных значений контрольных сумм объектов, заданных шаблонами КЦ (см. стр. 70);
   - "Смена пароля" — для изменения пароля администратора (см. стр. 46);
   - "Смена аутентификатора" — для смены аутентификатора администратора (см. стр. 46);
   - "Диагностика платы" — для проверки работоспособности комплекса (см. стр. 50);
   - "Служебные операции" — для создания резервной копии идентификатора администратора и реализации программной инициализации комплекса (см. стр. 54).
2. Выполните все действия, необходимые для настройки комплекса.

Шаг 3. Загрузка операционной системы или выключение компьютера

- Выберите вариант завершения работы:
  - Если продолжение работы на компьютере не требуется, завершите работу, выключив питание компьютера.

    Пояснение. Все внесенные изменения в этом случае также сохраняются.
  - Если требуется продолжить работу на компьютере, выберите в меню администратора команду "Загрузка операционной системы" и нажмите клавишу <Enter>.

В том случае если режим контроля целостности включен, перед загрузкой ОС начнется проверка целостности заданных объектов.

Процесс проверки можно прервать, нажав клавишу <Esc>. При обнаружении ошибки процесс проверки останавливается и на экран выводится сообщение об ошибке. Изучите это сообщение. Для возобновления проверки нажмите любую клавишу.

При обнаружении ошибок (не найден заданный файл, изменено содержимое файла, сектора, ключа реестра и т. д.) необходимо выяснить и устранить причины возникновения ошибок. После того как все выявленные недостатки устранены, необходимо заново рассчитать эталонные значения контрольных сумм для проверяемых объектов (см. стр. 70). Подробный список сообщений об ошибках содержится на стр. 76.

По завершении процесса проверки целостности начнется загрузка ОС.

Во время загрузки ОС МСВС 3.0 на экране может появиться сообщение консольной утилиты настройки оборудования об обнаружении сетевой платы. Нажмите кнопку "Игнорировать".

В случае необходимости возврата к управлению комплексом после того, как осуществлена загрузка операционной системы, выполните действия, предусмотренные в ОС для перезагрузки компьютера, и вновь войдите в систему, предъявив идентификатор администратора.

Настройка общих параметров

После активации в меню администратора команды "Общие параметры системы" на экране появится следующий диалог:

Общие параметры системы

Автономный режим работы	-	**Да**
Число попыток тестирования ДСЧ	-	**3**
Тестирование ДСЧ для пользователя	-	**Да**
Показ статистики пользователю	-	**Нет**
Использование случайных паролей	-	**Нет**
Минимальная длина пароля	-	**8**
Максимальный срок действия пароля (дней)	-	**42**
Предельное число неудачных входов пользователя	-	**65535**
Ограничение времени на вход в систему (мин.)	-	**0**
Время ожидания автоматического входа в систему (сек.)	-	**0**
Время ожидания сторожевого таймера (сек.)	-	**18**
Период тестирования сторожевого таймера (дней)	-	**0**
Поддержка USB-идентификаторов	-	**Нет**

Рис. 6. Диалог настройки общих параметров (режим эксплуатации)

Назначение общих параметров разъясняется в Табл. 4 на стр. 37. Ряд общих параметров комплекса и их настройка в режимах эксплуатации и инициализации (см. Табл. 3 на стр. 25) идентичны.

Для настройки параметров:

1. Выберите параметр, значение которого нужно изменить, и нажмите клавишу <Enter>. В зависимости от выбранного параметра:
   - значение меняется на противоположное ("Да" или "Нет");
   - появится диалог для ввода значения параметра. В этом случае введите значение с клавиатуры и нажмите клавишу <Enter>;

     Совет. При исправлении ошибок ввода используйте клавиши <←> и <→> для перемещения курсора, а клавиши <Backspace> или <Delete> — для удаления символа. Нажмите клавишу <Esc>, чтобы отказаться от изменения значения.

   - параметр "Поддержка USB-идентификаторов" может принимать три значения — "Нет"/"2.0"/"1.1".
2. Выполнив настройку параметров, нажмите клавишу <Esc> для сохранения изменений и выхода из диалога.

На экране вновь появится меню администратора.

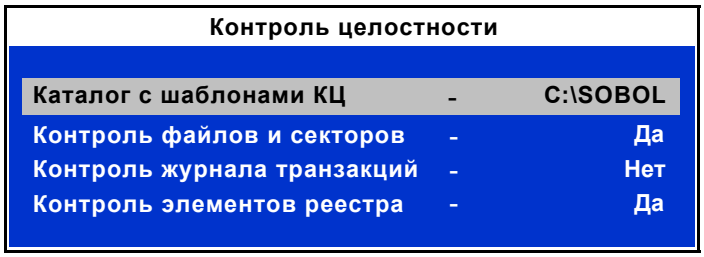
Табл. 4. Общие параметры комплекса "Соболь" (режим эксплуатации)

Автономный режим работы
Определяет режим работы комплекса "Соболь". Параметр может принимать два значения: "Да" — автономный режим или "Нет" — режим совместного использования. **Автономный режим.** Если комплекс функционирует в автономном режиме, любым внешним программам запрещен доступ к энергонезависимой памяти комплекса "Соболь". При этом управление общими параметрами, пользователями и журналом регистрации осуществляется администратором без ограничений. **Режим совместного использования.** Этот режим позволяет использовать комплекс "Соболь" совместно с другими средствами защиты. В этом случае внешним программам разрешен доступ к энергонезависимой памяти комплекса, но права администратора по управлению общими параметрами, пользователями и журналом регистрации ограничены (см. стр. 82). Параметр доступен для управления в любом режиме работы комплекса.
Число попыток тестирования ДСЧ (см. стр. 25)
Параметр доступен для управления как в автономном, так и в любом режиме работы комплекса.
Тестирование ДСЧ для пользователя (см. стр. 25)
Параметр недоступен для управления в режиме совместного использования. В этом режиме параметру автоматически присваивается значение "Да".
Показ статистики пользователю (см. стр. 25)
Параметр недоступен для управления в режиме совместного использования. В этом режиме параметру автоматически присваивается значение "Нет".
Использование случайных паролей
Позволяет включить или отключить режим использования случайных паролей при регистрации нового пользователя, смене пароля пользователя и администратора. Параметр может принимать два значения: "Да" — режим включен или "Нет" — режим отключен. Параметр доступен для управления в любом режиме работы комплекса, но доступ к нему блокируется при присвоении параметру "Минимальная длина пароля" значения, равного "0".
Минимальная длина пароля (см. стр. 25)
Параметр недоступен для управления в режиме совместного использования.
Максимальный срок действия пароля
Определяет период времени в днях, на протяжении которого действителен текущий пароль пользователя. Параметр может принимать значения от 0 до 999 дней. Значение "0" означает, что срок действия пароля неограничен. По истечении заданного периода времени текущий пароль пользователя перестает быть действительным и при входе в систему пользователю будет предложено сменить свой пароль, без чего он не сможет загрузить операционную систему. Если для пользователя включен режим замены аутентификатора при смене пароля (см. стр. 45), то в этом случае ограничение срока действия пароля распространяется и на аутентификатор пользователя. Данное ограничение действует только для тех пользователей, которым присвоены персональные идентификаторы DS1994, имеющие встроенный таймер, и у которых параметру "Ограничение срока действия пароля" присвоено значение "Да" (см. стр. 45). Параметр доступен для управления в любом режиме работы комплекса.
Предельное число неудачных входов пользователя (см. стр. 25)
Параметр недоступен для управления в режиме совместного использования.
Ограничение времени на вход в систему
Определяет интервал времени в минутах, отводящийся пользователям на вход в систему. Может принимать значения от 0 до 20 минут. Значение "0" означает, что время, отводящееся пользователям на вход в систему, не ограничено. При входе пользователя в систему в строке сообщений отсчитывается время, оставшееся ему для предъявления идентификатора и ввода пароля. Если пользователь не успел за отведенное время выполнить эти действия, на экране появится сообщение о завершении сеанса входа в систему. Параметр доступен для управления в любом режиме работы комплекса, но доступ к нему блокируется при присвоении параметру "Время ожидания автоматического входа в систему" значения, отличного от "0".

Время ожидания автоматического входа в систему
Определяет интервал времени в секундах, по истечении которого автоматически выполняется загрузка операционной системы компьютера. Может принимать значения "0" и от 5 до 40 секунд. Значение "0" означает, что автоматическая загрузка ОС без предъявления персонального идентификатора пользователя или администратора запрещена. Для организации автоматического запуска компьютера в списке зарегистрированных пользователей должен содержаться пользователь с именем AUTOLOAD. Если этот пользователь отсутствует в списке, то автоматическая загрузка ОС невозможна, данный параметр недоступен для управления и ему присвоено значение "0". Параметр доступен для управления в любом режиме работы комплекса, но доступ к нему блокируется при присвоении параметру "Ограничение времени на вход в систему" значения, отличного от "0".
Время ожидания сторожевого таймера (см. стр. 25)
Параметр доступен для управления в любом режиме работы комплекса.
Период тестирования сторожевого таймера (см. стр. 25)
Параметр доступен для управления в любом режиме работы комплекса.
Поддержка USB-идентификаторов (см. стр. 25)
Параметр доступен для управления в любом режиме работы комплекса.
Звуковой сигнал
Позволяет включить или выключить режим звукового сопровождения событий, необходимый для работы с криптографическим шлюзом АПКШ "Континент" без монитора. Параметр может принимать два значения: "Да" — звуковое сопровождение событий включено или "Нет" — звуковое сопровождение событий отключено. Параметр присутствует в диалоге только в случае эксплуатации комплекса "Соболь" в составе криптографического шлюза АПКШ "Континент".

Контроль целостности

После активации в меню администратора (см. Рис. 5 на стр. 35) команды "Контроль целостности" на экране появится следующий диалог:



1. Для настройки параметра выберите клавишей <↑> или <↓> строку с его названием и нажмите клавишу <Enter>. В зависимости от выбранного параметра:
   - появится диалог для ввода значения параметра. В этом случае введите значение с клавиатуры и нажмите клавишу <Enter>;
   - значение изменится на противоположное ("Да" или "Нет").

Особенности настройки параметров диалога "Контроль целостности" описываются в примечании на стр. 26.

2. Выполнив настройку параметров, нажмите клавишу <Esc> для сохранения изменений и настройки контроля целостности.

На экране вновь появится меню администратора.

Управление пользователями

После активации в меню администратора (см. Рис. 5 на стр. 35) команды "Список пользователей" на экране появится следующий диалог:

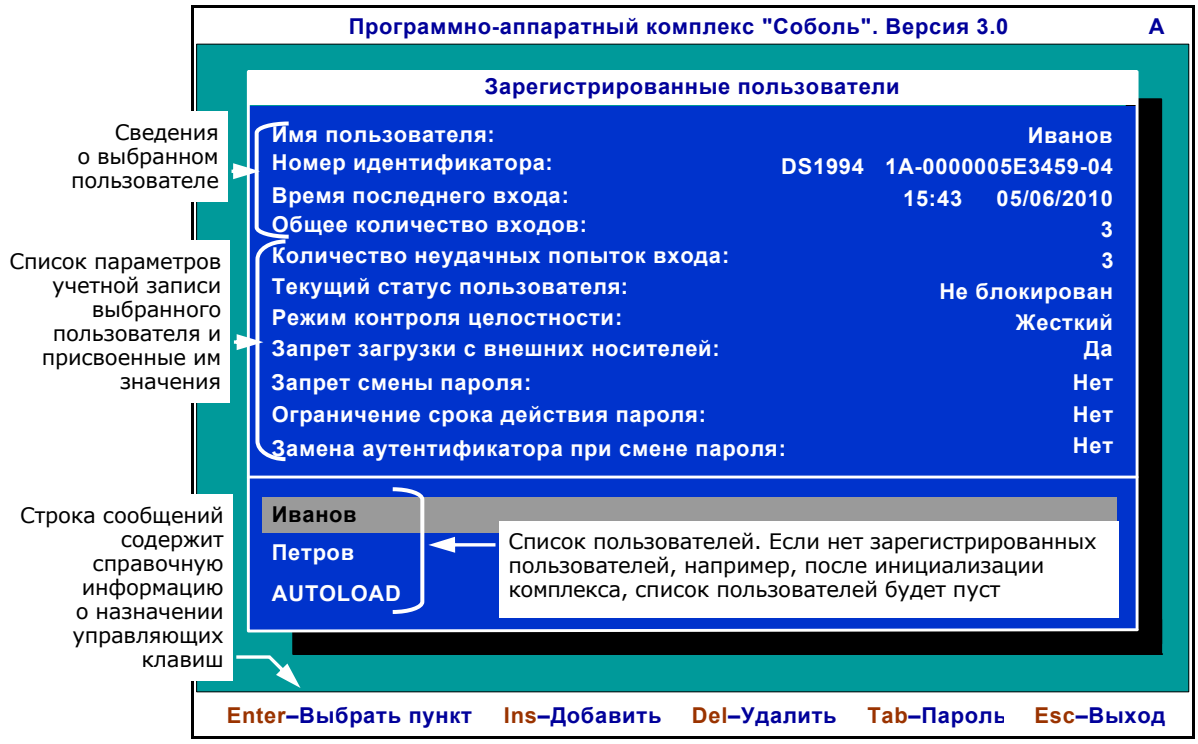


Рис. 7. Окно "Зарегистрированные пользователи"

Назначение сведений о пользователе разъясняется на стр. 71.

Список пользователей недоступен для управления при эксплуатации комплекса "Соболь" в режиме совместного использования (см. стр. 37, параметр "Автономный режим работы").

В этом диалоге администратор может:

- зарегистрировать нового пользователя (см. ниже);
- изменить параметры учетной записи пользователя (см. стр. 44);
- удалить учетную запись пользователя (см. стр. 45);
- сменить пароль и аутентификатор пользователя (см. стр. 45).

Выполнив все необходимые действия, нажмите клавишу <Esc> для сохранения изменений и выхода из диалога. На экране вновь появится меню администратора.

Регистрация пользователя

При регистрации нового пользователя в списке пользователей комплекса "Соболь" ему присваиваются следующие атрибуты:

- имя;
- аутентификатор и пароль для входа в систему;
- персональный идентификатор.

Служебная информация о пользователе сохраняется в энергонезависимой памяти комплекса "Соболь" — создается учетная запись пользователя. Кроме того, в персональный идентификатор, присвоенный пользователю, записывается служебная информация о регистрации.

Список пользователей может содержать не более 32 учетных записей.

Процедура регистрации пользователя может выполняться в одном из двух вариантов: первичная (см. ниже) и повторная (см. стр. 43).

Первичная регистрация пользователя, при выполнении которой в персональный идентификатор пользователя записывается новая служебная информация о регистрации. Если идентификатор уже содержит служебную информацию о регистрации пользователя на другом компьютере, оборудованном комплексом "Соболь", она будет уничтожена и пользователь не сможет работать на том компьютере.

Совет. Прежде чем приступить к первичной регистрации пользователя, приготовьте персональный идентификатор для записи в него служебной информации о регистрации.

Повторная регистрация пользователя, при выполнении которой служебная информация, записанная в персональный идентификатор при первичной регистрации пользователя на другом компьютере, считывается из идентификатора без ее изменения. В этом случае пользователь может использовать один и тот же идентификатор для входа в систему на нескольких компьютерах, оснащенных комплексами "Соболь".

Для повторной регистрации необходимо присутствие самого пользователя, так как при выполнении этой процедуры запрашивается текущий пароль пользователя.

Рекомендации.

- Если при регистрации пользователя будут предъявлены идентификаторы Rutoken S / Rutoken RF S/iKey 2032/eToken PRO, ранее не использовавшиеся в комплексе "Соболь" и имеющие PIN-коды, отличные от PIN-кодов по умолчанию (для Rutoken S/Rutoken RF S — **12345678**, для iKey 2032 — **default SO password.**, для eToken PRO — **1234567890**), то на экране появится окно запроса на ввод PIN-кода идентификатора. Введите его PIN-код и нажмите "Enter".
- Если при регистрации пользователя будет предъявлен неинициализированный идентификатор eToken PRO (USB-ключ, смарт-карта), то на экране появится окно с сообщением об отсутствии в нем файловой системы. Выполните инициализацию предъявленного eToken PRO стандартными программными средствами компании — производителя идентификатора.
- При регистрации пользователя на нескольких компьютерах, оснащенных комплексами "Соболь", следуйте следующей схеме. На первом из них выполните первичную регистрацию пользователя, а на всех остальных — повторную. В этом случае пользователь сможет входить в систему на всех этих компьютерах, используя один и тот же персональный идентификатор.

Для первичной регистрации пользователя:

1. Находясь в списке пользователей окна "Зарегистрированные пользователи" (см. Рис. 7 на стр. 39), нажмите клавишу <Insert>.

   Если в энергонезависимой памяти комплекса "Соболь" недостаточно свободного места для записи служебной информации о новом пользователе, на экране появится сообщение о том, что список пользователей исчерпан. Для добавления нового пользователя необходимо удалить из списка одну или несколько учетных записей (см. стр. 45) и повторить процедуру регистрации.

   На экране появится диалог для ввода имени пользователя:

   Имя пользователя может содержать до 40 символов латинского и русского алфавитов, в том числе цифры и любые служебные символы, включая "пробел".

   Совет. Для переключения в режим русского алфавита нажмите клавиши <Ctrl>+правый <Shift>, для возврата в режим латинского алфавита — <Ctrl>+левый <Shift>. Редактирование выполняется клавишами <←>, <→> и <Backspace> или <Delete>.

2. Введите имя нового пользователя и нажмите клавишу <Enter>.

Если введено имя, совпадающее с именем одного из зарегистрированных ранее пользователей, в строке сообщений появится сообщение — "Введенное имя уже зарегистрировано". Нажмите любую клавишу и повторите ввод имени еще раз, указав другое имя.

На экране появится запрос:

3. Выберите вариант "Да" и нажмите клавишу <Enter>.

   На экране появится один из диалогов для ввода пароля пользователя.

4. Введите и подтвердите пароль пользователя.

   - Если включен режим использования случайных паролей — общему параметру "Использование случайных паролей" присвоено значение "Да" (см. стр. 37) — диалог для ввода пароля примет следующий вид:

Это поле содержит пароль, автоматически генерируемый комплексом "Соболь"

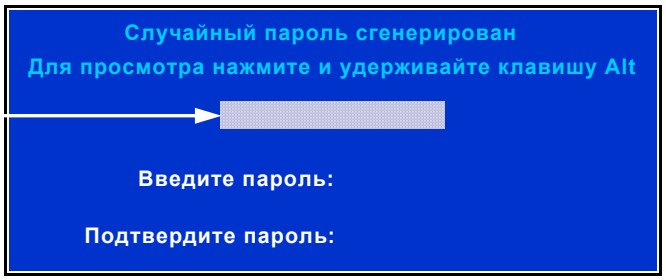


Рис. 8. Диалог для ввода случайного пароля

Для просмотра пароля, предлагаемого программой, нажмите и удерживайте в таком положении клавишу <Alt>. Запишите этот пароль для передачи его пользователю. Если предложенный пароль вас не устраивает, нажмите клавишу <F8> для генерирования нового пароля.

Пояснение. Случайные пароли состоят только из латинских символов, цифр и некоторых служебных символов. Заглавные и строчные символы считаются различными ("D1z$" и "d1z$" — это разные пароли). Длина генерируемого пароля в символах всегда не меньше значения, заданного параметром "Минимальная длина пароля" (см. стр. 37), но может превышать его на 1–4 символа.

Введите пароль, предложенный программой, и нажмите <Enter>.

Если введенный пароль не совпал с предложенным программой паролем, в строке сообщений появится сообщение — "Пароль введен неверно". Нажмите любую клавишу и повторите ввод пароля еще раз.

Повторно введите тот же пароль и нажмите клавишу <Enter>.

При обнаружении ошибок в строке сообщений появится сообщение — "Введенные пароли не совпадают". Нажмите любую клавишу и повторите ввод пароля еще раз.

   - Если режим использования случайных паролей отключен — общему параметру "Использование случайных паролей" присвоено значение "Нет" (см. стр. 37) — диалог для ввода пароля примет следующий вид:

Введите пароль пользователя и нажмите клавишу <Enter>.

Основные правила ввода пароля описаны в примечании на стр. 27.

Длина вводимого пароля не может быть меньше числа, заданного общим параметром "Минимальная длина пароля" (см. стр. 25), и не может превышать 16 символов. Если значение указанного параметра равно "0", можно назначить пользователю пустой пароль.

Если длина введенного пароля меньше минимально допустимого числа символов, то на экране появится сообщение — "Минимальная длина пароля … символа(ов)". Нажмите любую клавишу и повторите ввод пароля еще раз, учитывая данное ограничение.

На экране появится диалог для подтверждения пароля пользователя:

Повторно введите тот же пароль и нажмите клавишу <Enter>.

При обнаружении ошибок в строке сообщений появится соответствующее сообщение. Нажмите любую клавишу и повторите ввод нового пароля еще раз.

При правильном вводе пароля на экране появится запрос:

5. Предъявите персональный идентификатор, присваиваемый пользователю.

Если идентификатор предъявлен неправильно, то окно запроса останется на экране. Повторите предъявление идентификатора.

Если же предъявленный идентификатор принадлежит одному из зарегистрированных ранее пользователей, в строке сообщений появится сообщение — "Персональный идентификатор уже зарегистрирован на данном компьютере", которое будет присутствовать на экране до тех пор, пока USB-ключ находится в разъеме USB/идентификатор iButton касается считывателя/смарт-карта находится в USB-считывателе. Предъявите другой идентификатор.

При присвоении персонального идентификатора в него записывается служебная информация.

- Если персональный идентификатор регистрировался ранее на другом компьютере и уже содержит служебную информацию, на экране появится предупреждение:

Если вы уверены в том, что данный идентификатор никем больше не используется, предъявите его, выберите вариант "Да" и нажмите клавишу <Enter>

Помните, что при записи информации в персональный идентификатор служебная информация, содержащаяся в его памяти, будет полностью утеряна без возможности восстановления. При этом пользователь, которому принадлежит этот идентификатор, не сможет больше воспользоваться им для входа в систему.

Нажмите клавишу <Esc> и повторите действие **5**, используя другой персональный идентификатор.

- Если же структура данных персонального идентификатора нарушена или в нем недостаточно свободного места для записи служебной информации, на экране появятся соответствующие запросы на форматирование персонального идентификатора (см. стр. 28).

При форматировании идентификатора iButton вся информация, содержащаяся в его памяти, будет полностью утеряна без возможности восстановления. При форматировании USB-идентификатора будет утеряна только информация, относящаяся к ПАК "Соболь" и программам, его использующим. Для отказа от форматирования нажмите клавишу <Esc>, на экране вновь появится запрос персонального идентификатора.

Если вы уверены в том, что данный персональный идентификатор необходимо форматировать, выберите вариант "Да" и нажмите клавишу <Enter>.

На экране появится повторный запрос на форматирование идентификатора.

Для выполнения форматирования выберите вариант "Да", предъявите идентификатор и нажмите клавишу <Enter>.

После успешного присвоения пользователю персонального идентификатора и записи служебной информации о регистрации в энергонезависимую память комплекса "Соболь" на экране появится сообщение:

6. Нажмите клавишу <Enter>.

Имя нового пользователя появится в списке пользователей. Перейдите к настройке параметров учетной записи этого пользователя (см. стр. 44).

Для повторной регистрации пользователя:

1. Выполните действия **1**–**2**, приведенные в процедуре первичной регистрации пользователя (см. стр. 40).

Имя, назначаемое пользователю при его повторной регистрации на другом компьютере, может отличаться от имени, назначенном при первичной регистрации.

2. Выберите вариант "Нет" и нажмите клавишу <Enter>.

На экране появится диалог для ввода текущего пароля пользователя:

3. Введите текущий пароль пользователя и нажмите клавишу <Enter>.

На экране появится запрос:

4. Предъявите персональный идентификатор, присвоенный пользователю при его первичной регистрации на другом компьютере.

Если идентификатор предъявлен неправильно, то окно запроса останется на экране. Повторите предъявление идентификатора.

Если же предъявленный идентификатор принадлежит одному из зарегистрированных ранее пользователей, в строке сообщений появится сообщение — "Персональный идентификатор уже зарегистрирован на данном компьютере", которое будет присутствовать на экране до тех пор, пока USB-ключ находится в разъеме USB/идентификатор iButton касается считывателя/смарт-карта находится в USB-считывателе.

При успешном предъявлении идентификатора выполняется сопоставление введенного пароля с информацией, хранящейся в памяти идентификатора.

- Если введенный пароль не соответствует предъявленному идентификатору (указан неправильный пароль или предъявлен идентификатор, не принадлежащий пользователю) — в строке сообщений появится сообщение "Неверный персональный идентификатор или пароль". До тех пор пока USB-ключ находится в разъеме USB/идентификатор iButton касается считывателя/смарт-карта находится в USB-считывателе, сообщение будет присутствовать на экране. После изъятия идентификатора на экране вновь появится диалог для ввода имени пользователя. Повторите действия **2**–**4**.
- Если введенный пароль соответствует предъявленному идентификатору, выполняется считывание служебной информации из идентификатора и запись этой информации в энергонезависимую память комплекса "Соболь".

После успешной записи служебной информации в память комплекса "Соболь" на экране появится сообщение об успешной регистрации пользователя.

5. Нажмите клавишу <Enter>.

Имя нового пользователя появится в списке пользователей. Перейдите к настройке параметров учетной записи этого пользователя (см. стр. 44).

Количество символов в пароле зарегистрированного пользователя (длина пароля) может оказаться меньше значения общего параметра "Минимальная длина пароля" (см. стр. 25). В этом случае при первом входе в систему пользователь будет вынужден сменить свой старый пароль, иначе он не сможет загрузить операционную систему компьютера.

Настройка параметров учетной записи

Параметры учетной записи определяют ее текущее состояние и позволяют выбрать для данного пользователя режимы работы защитных механизмов.

Параметры учетной записи недоступны для управления при эксплуатации комплекса "Соболь" в режиме совместного использования (см. стр. 37, параметр "Автономный режим работы").

Для настройки параметров:

1. В списке пользователей окна "Зарегистрированные пользователи" (см. Рис. 7 на стр. 39) выберите необходимое имя и нажмите клавишу <Enter>.
2. В списке параметров учетной записи выбранного пользователя выберите параметр, значение которого нужно изменить, и нажмите клавишу <Enter>.

   Значение параметра изменится на противоположное, например, "Да" — "Нет", "Не блокирован" — "Блокирован", "Жесткий" — "Мягкий".

   Назначение параметров учетной записи разъясняется ниже в Табл. 5.
3. Выполнив настройку параметров, нажмите клавишу <Esc> для сохранения изменений и выхода из режима настройки параметров.

Осуществится возврат к списку пользователей.

Табл. 5. Параметры учетной записи

Количество неудачных попыток входа
Значение данного параметра равно "0", если число неудачных попыток входа, выполненных пользователем во время последнего сеанса входа в систему, меньше значения общего параметра "Предельное число неудачных входов пользователя" (см. стр. 25) и пользователь завершил сеанс успешным входом в систему. Значение данного параметра больше "0", если число неудачных попыток входа, выполненных пользователем во время последнего сеанса входа в систему, достигло числа, заданного общим параметром "Предельное число неудачных входов пользователя". При этом вход пользователя в систему блокируется автоматически. Для разблокирования входа пользователя в систему выберите строку с названием данного параметра и нажмите клавишу <Enter>. Параметр примет значение "0". Затем установите для параметра "Текущий статус пользователя" значение "Не блокирован".
Текущий статус пользователя
Управляет блокировкой входа пользователя в систему. Параметр может принимать два значения: "Блокирован" — вход пользователя в систему запрещен или "Не блокирован" — вход пользователя в систему разрешен. Если вход пользователя в систему запрещен, то при попытке входа в систему, даже если пользователь правильно указал пароль, на экран выводится сообщение "Ваш вход в систему запрещен администратором" и компьютер блокируется.
Режим контроля целостности
Определяет для данного пользователя режим работы механизма контроля целостности. Параметр может принимать два значения: "Жесткий" — включен жесткий режим или "Мягкий" — включен мягкий режим. **Жесткий режим.** Если при входе данного пользователя в систему обнаружены нарушения целостности контролируемых объектов, вход пользователя в систему запрещается и компьютер блокируется. В журнале регистрируется событие "Ошибка при контроле целостности". **Мягкий режим.** Если при входе данного пользователя в систему обнаружены нарушения целостности контролируемых объектов, вход пользователя в систему разрешается. В журнале событий регистрируется событие "Ошибка при контроле целостности".
Запрет загрузки с внешних носителей
Позволяет запретить пользователю загружать операционную систему со съемных носителей — дискет, DVD/CD-ROM, ZIP-устройств, магнитооптических дисков, USB-устройств и др. Параметр может принимать два значения: "Да" — загрузка ОС со съемных носителей запрещена или "Нет" — загрузка ОС со съемных носителей разрешена. Для того чтобы исключить возможность модификации защищенной энергонезависимой памяти комплекса "Соболь" в режиме совместного использования (см. стр. 37, параметр "Автономный режим работы"), рекомендуется запретить всем пользователям загрузку ОС со съемных носителей.

Запрет смены пароля
Позволяет запретить пользователю смену пароля. Параметр может принимать два значения: "Да" — смена пароля запрещается или "Нет" — разрешается. При включении этого режима параметр "Замена аутентификатора при смене пароля" становится недоступным для изменения.
Ограничение срока действия пароля
Позволяет включить для пользователя режим устаревания пароля. Параметр может принимать два значения: "Да" — режим включен или "Нет" — режим отключен. При включении этого режима по истечении периода времени, заданного общим параметром "Максимальный срок действия пароля" (см. стр. 37), текущий пароль пользователя перестает быть действительным и при входе в систему пользователю будет предложено сменить свой пароль, без чего он не сможет загрузить операционную систему. Если для пользователя включен режим замены аутентификатора при смене пароля, то ограничение срока действия распространяется и на аутентификатор пользователя. Для присвоения параметру значения "Да" требуется присутствие данного пользователя. На экране появится диалог для ввода текущего пароля пользователя. Попросите пользователя ввести свой пароль и нажать клавишу <Enter>, затем предъявите персональный идентификатор данного пользователя. Если пароль введен правильно, параметру будет присвоено значение "Да". Параметр доступен для управления только в том случае, когда пользователю присвоен персональный идентификатор DS1994, имеющий встроенный таймер.
Замена аутентификатора при смене пароля
Позволяет включить для пользователя режим принудительной замены аутентификатора при выполнении им процедуры смены пароля. Параметр может принимать два значения: "Да" — режим включен или "Нет" — режим отключен.

Для смены пароля пользователя, у которого истекло время действия пароля и которому запрещена самостоятельная смена пароля, выполните следующие действия:

- войдите в комплекс на правах администратора, снимите запрет на смену пароля пользователем (см. стр. 45) и перезагрузите компьютер;
- дайте возможность пользователю выполнить вход в комплекс и сменить свой пароль;
- перезагрузите компьютер;
- войдите в комплекс на правах администратора, запретите пользователю самостоятельно менять пароль (см. стр. 45) и перезагрузите компьютер.

Удаление учетной записи пользователя

Для удаления учетной записи:

1. В списке пользователей окна "Зарегистрированные пользователи" (см. Рис. 7 на стр. 39) выберите необходимое имя и нажмите клавишу <Delete>.

   На экране появится запрос:

Для отказа от удаления выберите вариант "Нет" и нажмите клавишу <Enter>

2. Выберите вариант "Да" и нажмите клавишу <Enter>.

Программа удалит учетную запись выбранного пользователя из энергонезависимой памяти комплекса "Соболь". Имя этого пользователя исчезнет из списка.

Принудительная смена пароля и аутентификатора пользователя

Перед выполнением данной процедуры примите во внимание следующее:

- Эта возможность предусмотрена только для **экстренной** смены пароля и аутентификатора пользователя администратором в случае компрометации пароля. Во всех остальных случаях смена пароля выполняется пользователем самостоятельно (см. документ [4]).

- Процедура принудительной смены пароля и аутентификатора приводит к корректному результату только тогда, когда пользователь зарегистрирован с использованием данного персонального идентификатора на одном компьютере, оснащенном комплексом "Соболь".
- Если пользователь зарегистрирован при помощи данного идентификатора на нескольких компьютерах, то после принудительной смены пароля и аутентификатора пользователь теряет доступ ко всем компьютерам, кроме того, на котором выполнена эта процедура. В этом случае следует снова выполнить повторную регистрацию пользователя на остальных компьютерах.

Для смены пароля и аутентификатора пользователя:

1. В списке пользователей окна "Зарегистрированные пользователи" (см. Рис. 7 на стр. 39) выберите необходимое имя и нажмите клавишу <Tab>.

   На экране появится предупреждение:

Для отказа от смены пароля пользователя выберите вариант "Нет" и нажмите клавишу <Enter>

2. Если вы уверены в необходимости смены пароля и аутентификатора пользователя, выберите вариант "Да" и нажмите клавишу <Enter>.

   На экране появится один из диалогов для ввода нового пароля пользователя.

Пояснение. Текущий (старый) пароль пользователя в данном случае не запрашивается.

Далее процедура смены пароля и аутентификатора пользователя соответствует действиям **3**–**4** процедуры смены пароля администратора (см. ниже).

Смена пароля и аутентификатора администратора

Администратор комплекса "Соболь" может сменить пароль для входа в систему и аутентификатор. При смене пароля или аутентификатора изменяется содержимое персонального идентификатора администратора.

Так как режим устаревания пароля не действует для администратора комплекса "Соболь", то администратор должен выполнять смену пароля и аутентификатора самостоятельно с периодичностью, установленной политикой безопасности организации.

Для смены пароля администратора:

1. В меню администратора (см. Рис. 5 на стр. 35) выберите команду "Смена пароля" и нажмите клавишу <Enter>.

   На экране появится диалог для ввода текущего пароля администратора:

Совет. До предъявления персонального идентификатора администратора можно отказаться от смены пароля. Для этого нажмите клавишу <Esc>.

2. Введите текущий (старый) пароль администратора и нажмите клавишу <Enter>.

   На экране появится один из диалогов для ввода нового пароля.

3. Введите и подтвердите новый пароль администратора.
   - Если включен режим использования случайных паролей — общему параметру "Использование случайных паролей" присвоено значение "Да" (см. стр. 37) — на экране появится диалог для ввода случайного пароля (см. Рис. 8 на стр. 41).

Чтобы увидеть пароль, предлагаемый программой, нажмите и не отпускайте клавишу <Alt>. Запишите и заучите этот пароль. Если предложенный пароль вас не устраивает, нажмите клавишу <F8> для генерирования нового пароля.

Введите пароль, предложенный программой, и нажмите клавишу <Enter>.

Если введенный пароль не совпал с предложенным программой паролем, в строке сообщений появится сообщение — "Пароль введен неверно". Нажмите любую клавишу и повторите ввод пароля еще раз.

Повторно введите тот же пароль и нажмите клавишу <Enter>.

При обнаружении ошибок в строке сообщений появится сообщение — "Введенные пароли не совпадают". Нажмите любую клавишу и повторите ввод пароля еще раз.

- Если режим использования случайных паролей отключен — общему параметру "Использование случайных паролей" присвоено значение "Нет" (см. стр. 37) — диалог для ввода пароля примет следующий вид:

Введите новый пароль администратора и нажмите клавишу <Enter>.

Основные правила ввода пароля описаны в примечании на стр. 27.

Длина вводимого пароля не может быть меньше числа, заданного общим параметром "Минимальная длина пароля" (см. стр. 25), и не может превышать 16 символов. Если значение указанного параметра равно "0", можно назначить пользователю пустой пароль.

Если длина введенного пароля меньше минимально допустимого числа символов, то на экране появится сообщение — "Минимальная длина пароля … символа(ов)". Нажмите любую клавишу и повторите ввод пароля еще раз, учитывая данное ограничение.

На экране появится диалог для подтверждения нового пароля администратора:

Повторно введите тот же пароль и нажмите клавишу <Enter>.

При обнаружении ошибок в строке сообщений появится сообщение об этом. Нажмите любую клавишу и повторите ввод нового пароля еще раз.

При правильном вводе пароля на экране появится запрос:

4. Предъявите идентификатор администратора.

При правильном предъявлении идентификатора выполняется сопоставление введенного старого пароля с информацией, хранящейся в памяти идентификатора.

- Если старый пароль не соответствует предъявленному идентификатору — указан неправильный пароль или предъявлен не принадлежащий администратору идентификатор — в строке сообщений появится сообщение "Неверный персональный идентификатор или пароль". До тех пор пока USB-ключ находится в разъеме USB/идентификатор iButton касается считывателя/смарт-карта находится в USB-считывателе, сообщение будет присутствовать на экране. После изъятия идентификатора на экране вновь появится запрос персонального идентификатора. Предъявите идентификатор администратора или нажмите клавишу <Esc> и повторите процедуру смены пароля.
- Если старый пароль соответствует предъявленному идентификатору, в идентификатор записывается служебная информация, соответствующая новому паролю администратора.

После успешной записи служебной информации на экране появится запрос:

Рекомендуется устанавливать новый пароль для всех резервных копий персонального идентификатора администратора, созданных при инициализации комплекса "Соболь". Это позволит вам и далее пользоваться этими резервными копиями.

5. При наличии резервных копий выберите вариант "Да" и нажмите клавишу <Enter>.

Совет. Чтобы отказаться от смены пароля для резервных копий, нажмите клавишу <Esc> или выберите вариант "Нет" и нажмите клавишу <Enter>.

На экране появится запрос персонального идентификатора.

6. Предъявите персональный идентификатор, являющийся резервной копией идентификатора администратора.

Если идентификатор предъявлен неправильно, то окно запроса останется на экране. Повторите предъявление идентификатора.

Если же предъявленный идентификатор не является резервной копией идентификатора администратора, в строке сообщений появится сообщение — "Неверный персональный идентификатор или пароль", которое будет присутствовать на экране до тех пор, пока USB-ключ находится в разъеме USB/идентификатор iButton касается считывателя/смарт-карта находится в USB-считывателе. После изъятия идентификатора на экране вновь появится запрос персонального идентификатора. Предъявите идентификатор, являющийся резервной копией персонального идентификатора администратора.

При правильном предъявлении идентификатора в него записывается служебная информация, соответствующая новому паролю администратора, после чего на экране вновь появится диалог, предлагающий установить новый пароль для следующей резервной копии.

7. При необходимости повторите действия **5**–**6** для очередной резервной копии или завершите процедуру нажатием клавиши <Esc>.

На экране вновь появится меню администратора.

Для смены аутентификатора администратора:

1. В меню администратора (см. Рис. 5 на стр. 35) выберите команду "Смена аутентификатора" и нажмите клавишу <Enter>.

На экране появится диалог для ввода текущего пароля администратора:

Совет. До предъявления персонального идентификатора администратора можно отказаться от смены аутентификатора. Для этого нажмите клавишу <Esc>.

2. Введите текущий пароль администратора и нажмите клавишу <Enter>.

На экране появится запрос:

3. Предъявите персональный идентификатор администратора.

При правильном предъявлении идентификатора выполняется сопоставление введенного пароля с информацией, хранящейся в памяти идентификатора.

Если введенный пароль не соответствует предъявленному идентификатору — указан неправильный пароль или предъявлен не принадлежащий администратору идентификатор — в строке сообщений появится сообщение "Неверный персональный идентификатор или пароль". До тех пор пока USB-ключ находится в разъеме USB/идентификатор iButton касается считывателя/смарт-карта находится в USB-считывателе, сообщение будет присутствовать на экране. После изъятия идентификатора на экране вновь появится диалог для ввода пароля. Повторите действия **2**–**3** или нажмите клавишу <Esc> для отказа от смены аутентификатора.

Если введенный пароль соответствует предъявленному идентификатору, выполняется чтение служебной информации из идентификатора.

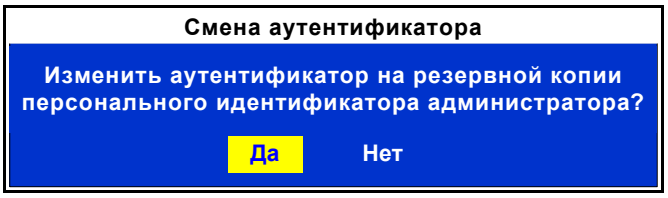
- При первой смене аутентификатора новый аутентификатор записывается в персональный идентификатор администратора. При этом старый аутентификатор сохраняется в памяти персонального идентификатора. В результате после смены аутентификатора администратор не теряет доступ к другим компьютерам, на которых он зарегистрирован в качестве администратора комплекса "Соболь".
- При всех последующих сменах аутентификатора на экране появится предупреждение:

Для прекращения процедуры выберите вариант "Нет" и нажмите клавишу <Enter>

Пояснение. Персональный идентификатор администратора хранит два аутентификатора — текущий и старый. При записи нового аутентификатора в память персонального идентификатора старый аутентификатор удаляется, а текущий сохраняется, что позволяет администратору осуществлять доступ к другим компьютерам, на которых он зарегистрирован в качестве администратора комплекса "Соболь". Если администратор с момента последней смены аутентификатора ни разу не выполнил вход на какой-либо из этих компьютеров, он потеряет право доступа к нему, так как старый аутентификатор, который требуется для аутентификации администратора на этом компьютере, удален из персонального идентификатора. В этом случае рекомендуется прекратить процедуру смены аутентификатора, выполнить вход на соответствующие компьютеры и только потом повторить процедуру смены аутентификатора.

Для записи нового аутентификатора в персональный идентификатор администратора выберите вариант "Да", предъявите идентификатор и нажмите клавишу <Enter>.

После успешной записи служебной информации на экране появится запрос:



Рекомендуется менять аутентификатор на всех резервных копиях персонального идентификатора администратора, созданных при инициализации комплекса "Соболь". Это позволит вам и далее пользоваться этими резервными копиями.

4. При наличии резервных копий выберите вариант "Да" и нажмите клавишу <Enter>.

Совет. Для отказа от смены аутентификатора на резервных копиях нажмите клавишу <Esc> или выберите вариант "Нет" и нажмите клавишу <Enter>.

На экране появится запрос персонального идентификатора.

5. Предъявите персональный идентификатор, являющийся резервной копией идентификатора администратора.

Если идентификатор предъявлен неправильно, то окно запроса останется на экране. Повторите предъявление идентификатора.

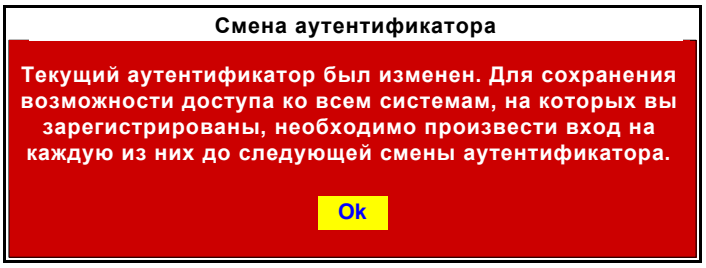
Если же предъявленный идентификатор не является резервной копией идентификатора администратора, в строке сообщений появится сообщение — "Неверный персональный идентификатор или пароль", которое будет присутствовать на экране до тех пор, пока USB-ключ находится в разъеме USB/идентификатор iButton касается считывателя/смарт-карта находится в USB-считывателе. После изъятия идентификатора на экране вновь появится запрос персонального идентификатора. Предъявите идентификатор, являющийся резервной копией персонального идентификатора администратора.

При появлении на экране предупреждения о том, что в случае отмены текущей операции данный идентификатор будет непригоден для входа в систему, рекомендуется продолжить выполнение операции. Для этого выберите вариант "Да" и нажмите клавишу <Enter>.

При правильном предъявлении идентификатора в него записывается новый аутентификатор администратора, после чего на экране вновь появится диалог, предлагающий изменить аутентификатор на следующей резервной копии.

6. При необходимости повторите действия **4**–**5** для очередной резервной копии или завершите процедуру нажатием клавиши <Esc>.

По окончании процедуры на экране появится предупреждающее сообщение:



Пояснение. После смены аутентификатора обязательно до следующей смены аутентификатора выполните вход на все компьютеры, на которых вы зарегистрированы в качестве администратора комплекса "Соболь".

7. Нажмите клавишу <Enter>.

На экране вновь появится меню администратора.

Контроль работоспособности комплекса

Для контроля работоспособности активируйте команду "Диагностика платы":

- в меню "Режим инициализации" (см. стр. 23) — перед инициализацией комплекса;
- в меню "Администратор" (см. стр. 35) — во время его эксплуатации.

На экране появится меню, команды которого запускают процедуры проверки работоспособности компонентов комплекса:

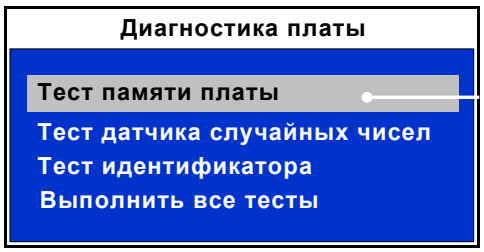


Рис. 9. Меню "Диагностика платы"

По завершении каждой процедуры на экран выводится окно с сообщением о ее результате. Подробный список сообщений содержится на стр. 80.

Тест памяти платы

Этот тест проверяет работоспособность энергонезависимой памяти (NVRAM) платы комплекса "Соболь". В ходе проверки осуществляются попытки доступа на чтение и запись для каждого сегмента двух банков памяти.

Процедура проверки не приводит к потере данных, хранящихся в NVRAM, но только при соблюдении следующего запрета — во время выполнения проверки запрещается проводить перезагрузку компьютера и отключать питание.

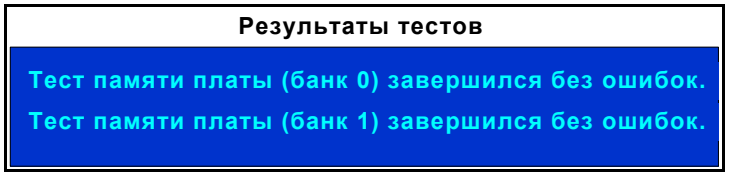
Для проверки NVRAM:

1. Выберите команду "Тест памяти платы" и нажмите клавишу <Enter>.

   Начнется процедура проверки, ход которой отображает следующее окно:

Совет. Если требуется прервать процедуру проверки, нажмите клавишу <Esc>.

   При завершении проверки раздается звуковой сигнал и на экране появляется окно, сообщающее о результате проверки:



2. Ознакомьтесь с полученными результатами и нажмите клавишу <Esc>.

На экране вновь появится меню "Диагностика платы".

Тест датчика случайных чисел

Этот тест проверяет работоспособность аппаратного датчика случайных чисел комплекса "Соболь". Тестирование заключается в проверке равномерности распределения случайных чисел, генерируемых датчиком.

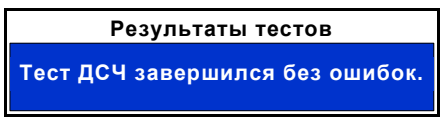
Для проверки датчика случайных чисел:

1. Выберите команду "Тест датчика случайных чисел" и нажмите <Enter>.

   Начнется процедура проверки, ход которой отображает следующее окно:

Совет. Если требуется прервать процедуру проверки, нажмите клавишу <Esc>.

   При завершении проверки раздается звуковой сигнал и на экране появляется окно, сообщающее о результате проверки:



2. Ознакомьтесь с полученными результатами и нажмите клавишу <Esc>.

На экране вновь появится меню "Диагностика платы".

Тест идентификатора

Тест проверяет правильность записи/чтения данных в/из идентификатор(а).

Тестирование eToken PRO, iKey 2032, Rutoken S, Rutoken RF S возможно только после включения режима поддержки USB-идентификаторов.

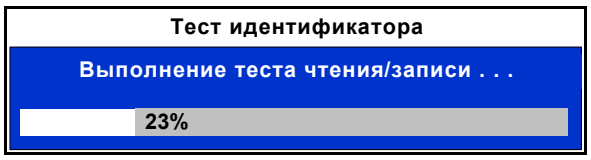
Для проверки идентификатора:

1. Выберите команду "Тест идентификатора" и нажмите клавишу <Enter>.

   На экране появится запрос персонального идентификатора:

2. Предъявите проверяемый персональный идентификатор.

   Начнется процедура проверки, ход которой отображает следующее окно:



Совет. Если требуется прервать процедуру проверки, нажмите клавишу <Esc>.

   При завершении проверки раздается звуковой сигнал и на экране появляется окно, сообщающее о результате проверки:

3. Ознакомьтесь с полученными результатами и нажмите клавишу <Esc>.

На экране вновь появится меню "Диагностика платы".

Последовательное выполнение всех тестов

При использовании этой процедуры обратите внимание на особенность выполнения теста идентификатора — запрос персонального идентификатора на экран не выводится. Поэтому следует заблаговременно предъявить предназначенный для проверки идентификатор.

Для выполнения всех проверок:

1. Выберите команду "Выполнить все тесты" и нажмите клавишу <Enter>.

   Начнется последовательное выполнение всех проверок. Ход каждой проверки отображают соответствующие окна, представленные в предыдущих пунктах.

   Совет. Если требуется прервать процедуру проверки, нажмите клавишу <Esc>.

   При завершении последней проверки раздается звуковой сигнал и на экране появляется окно, сообщающее о результатах проверок.

2. Ознакомьтесь с полученными результатами и нажмите клавишу <Esc>.

На экране вновь появится меню "Диагностика платы".

Работа с журналом регистрации событий

Записи о событиях, регистрируемых комплексом "Соболь" во время своей работы, хранятся в журнале регистрации событий, который размещается в специальной области энергонезависимой памяти комплекса. Размер этой области памяти ограничен и позволяет хранить не более 80 записей.

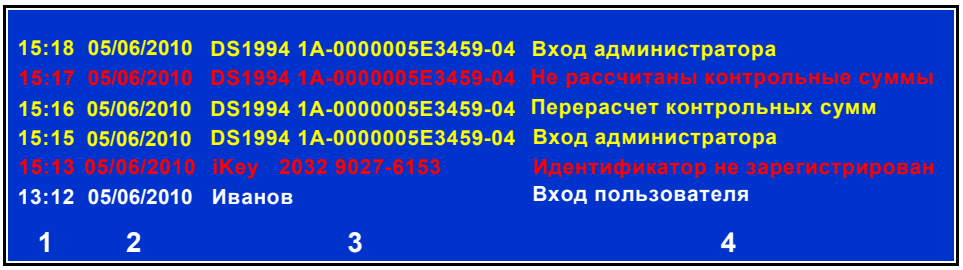
При заполнении всей области памяти, отведенной для хранения журнала, новые записи помещаются на место уже существующих записей, затирая их. Если журнал полностью заполнен (содержит 80 записей), то следующая запись заменит запись, помещенную в журнал раньше всех других, т. е. самую старую запись.

Просмотр записей журнала

Для просмотра записей:

1. В меню администратора (см. Рис. 5 на стр. 35) выберите команду "Журнал регистрации событий" и нажмите клавишу <Enter>.

   На экране появится окно, фрагмент которого представлен ниже:



   Записи о событиях, зарегистрированных комплексом "Соболь", представляются в табличной форме и выделяются цветом. Желтым цветом обозначаются события, связанные с успешными действиями администратора. Красным цветом выделяются критические события, белым — события, связанные с успешными действиями пользователя. Полный перечень регистрируемых событий приведен на стр. 81.

   Каждая строка журнала содержит сведения об одном событии. Первая строка содержит запись о самом последнем из зарегистрированных событий, а нижняя строка — запись о событии, зарегистрированном раньше всех остальных.

   Столбцы таблицы (см. рисунок) содержат следующие сведения о событиях:

1	Время регистрации события (в формате "часы : минуты")
2	Дата регистрации события (в формате "день/месяц/год")
3	Имя пользователя, действия которого привели к регистрации события. Для администратора, а также для пользователей, не зарегистрированных на данном компьютере, указываются тип и номер предъявленного при входе персонального идентификатора. После удаления учетной записи пользователя в записях журнала, относящихся к его работе, вместо имени этого пользователя указываются тип и номер принадлежавшего ему персонального идентификатора
4	Описание событий

2. Ознакомьтесь с содержанием журнала регистрации событий.

   Совет. Для перемещения курсора используйте клавиши <↑> и <↓>, для пролистывания записей — <PgUp> и <PgDn>, для сдвига записей влево или вправо — <→> и <←>.

3. Нажмите клавишу <Esc> для возврата к меню администратора.

Очистка журнала

Прежде чем выполнить очистку журнала, ознакомьтесь с его содержанием.

При эксплуатации комплекса "Соболь" в режиме совместного использования (см. стр. 37, параметр "Автономный режим работы") очистка журнала запрещена.

Для очистки журнала:

1. Находясь в окне просмотра записей журнала, нажмите клавишу <Delete>.

   На экране появится запрос:

2. Выберите вариант "Да" и нажмите клавишу <Enter>.

Все имеющиеся записи будут удалены из журнала, при этом в журнал добавится новая запись — "Удаление системного журнала".

Служебные операции

В текущей версии комплекса "Соболь" реализованы служебные операции, позволяющие создать копии идентификатора администратора и осуществить программную инициализацию комплекса.

Программная инициализация комплекса

Для инициализации комплекса:

1. В меню администратора (см. Рис. 5 на стр. 35) выберите команду "Служебные операции" и нажмите клавишу <Enter>.

   На экране появится окно "Служебные операции":

Рис. 10. Диалоговое окно "Служебные операции"

2. В окне "Служебные операции" выберите команду "Инициализация платы" и нажмите клавишу <Enter>.

   На экране появится следующее окно:

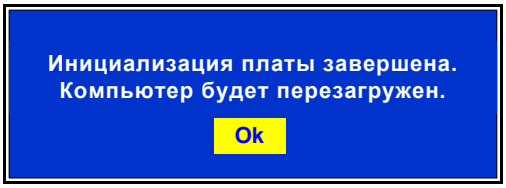
Если вы решили отказаться от инициализации, выберите вариант "Нет" и нажмите клавишу <Enter>

3. Для продолжения процедуры инициализации выберите вариант "Да" и нажмите клавишу <Enter>.

   На экране появится диалог "Общие параметры системы" (см. Рис. 4 на стр. 24).

4. Выполните действия, указанные выше в **шагах 2, 3, 4** процедуры инициализации комплекса (см. стр. 23).

   По окончании инициализации на экране появится сообщение:



5. Нажмите клавишу <Enter>.

Создание резервной копии идентификатора администратора

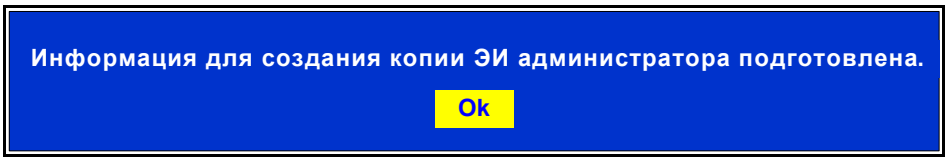
Для создания копии идентификатора администратора:

1. В окне "Служебные операции" (см. Рис. 10 на стр. 54) выберите команду "Создание копии ЭИ администратора" и нажмите клавишу <Enter>.
2. В появившемся окне введите текущий пароль администратора и нажмите клавишу <Enter>.

   На экране появится следующее окно:

3. Предъявите исходный идентификатор.

   После считывания служебной информации из идентификатора на экране появится следующее сообщение:



4. Нажмите <Enter>.

   На экране появится запрос персонального идентификатора.
5. Предъявите идентификатор, приготовленный для создания резервной копии идентификатора администратора.

> **Пояснение.** При появлении на экране запросов и сообщений действуйте в соответствии с инструкциями п. **4** процедуры первичной регистрации администратора (см. стр. 27).

   При успешном создании резервной копии на экране появится запрос, предлагающий создать еще одну резервную копию идентификатора.
6. Выберите вариант продолжения процедуры:
   - Для создания очередной резервной копии выберите вариант "Да" и нажмите клавишу <Enter>.
   - Если необходимое количество резервных копий уже создано, выберите вариант "Нет" и нажмите клавишу <Enter>.

Глава 4
Настройка механизма контроля целостности

Механизм контроля целостности комплекса "Соболь" (см. стр. 9) обеспечивает до загрузки операционной системы контроль следующих объектов:

- файлы;
- секторы жесткого диска;
- элементы (объекты) системного реестра:
  - параметры ключей (переменные по ключу, переменная реестра);
  - ключи реестра с параметрами и вложенными ключами (ключи с переменными).

Порядок настройки механизма контроля целостности комплекса "Соболь" в среде ОС МСВС 3.0, VMware ESX рассмотрен в документах [2] и [3] соответственно.

Для настройки механизма используется программа управления шаблонами КЦ. Программа позволяет определить списки объектов, целостность которых требуется контролировать, и сохранить эти списки в специальных файлах-шаблонах.

Если корректировка исходных шаблонов не требуется, то для настройки контроля целостности достаточно выполнить расчет эталонных значений контрольных сумм при инициализации комплекса (см. стр. 29).

Для добавления новых объектов, удаления объектов, не требующих контроля, восстановления исходных шаблонов требуется настройка механизма КЦ.

В этих случаях настройка выполняется в следующем порядке:

- корректировка шаблонов контроля целостности (см. 58);
- расчет эталонных значений контрольных сумм (см. стр. 70);
- включение контроля целостности, если он был отключен (см. стр. 38).

Если при настроенном механизме контроля целостности были изменены имена логических дисков, например, с помощью программы Disk Manager, то необходимо восстановить шаблоны КЦ и рассчитать эталонные значения контрольных сумм.

Модель данных механизма контроля целостности

Параметры, определяющие работу механизма контроля целостности комплекса "Соболь", объединены в рамках единой модели данных. Модель данных представляет собой иерархическое описание объектов и связей между ними. В модели используются 5 категорий объектов:

Объект	Пояснение
Ресурс	Ресурсы — это файлы, секторы диска и элементы системного реестра. Описание файлов, секторов и элементов однозначно определяет местонахождение ресурса и его тип
Группа ресурсов	Объединяет множество описаний ресурсов одного типа (файлы, секторы, элементы реестра). Однозначно определяется типом входящих в группу ресурсов
Задача	Задача — это набор групп ресурсов одного и того же или разных типов. Например, задача может одновременно включать группу системных файлов и секторов
Задание	Включает в себя набор задач и групп ресурсов, подлежащих контролю
Субъект управления	Субъектом управления является компьютер, защищаемый комплексом "Соболь"

Объекты одной категории являются подчиненными или вышестоящими по отношению к объектам другой категории. Так, ресурсы являются подчиненными по отношению к группам ресурсов, а группы — к задачам. Включение ресурсов в группы, групп ресурсов в задачи, а задач — в задания называется установлением связей между объектами. В конечном итоге задания назначаются субъектам.

Программа управления шаблонами контроля целостности

Нажмите кнопку "Пуск" и активируйте в главном меню Windows команду "Все программы" I "ПАК 'Соболь'" I "Управление шаблонами КЦ".

На экране появится главное окно программы:

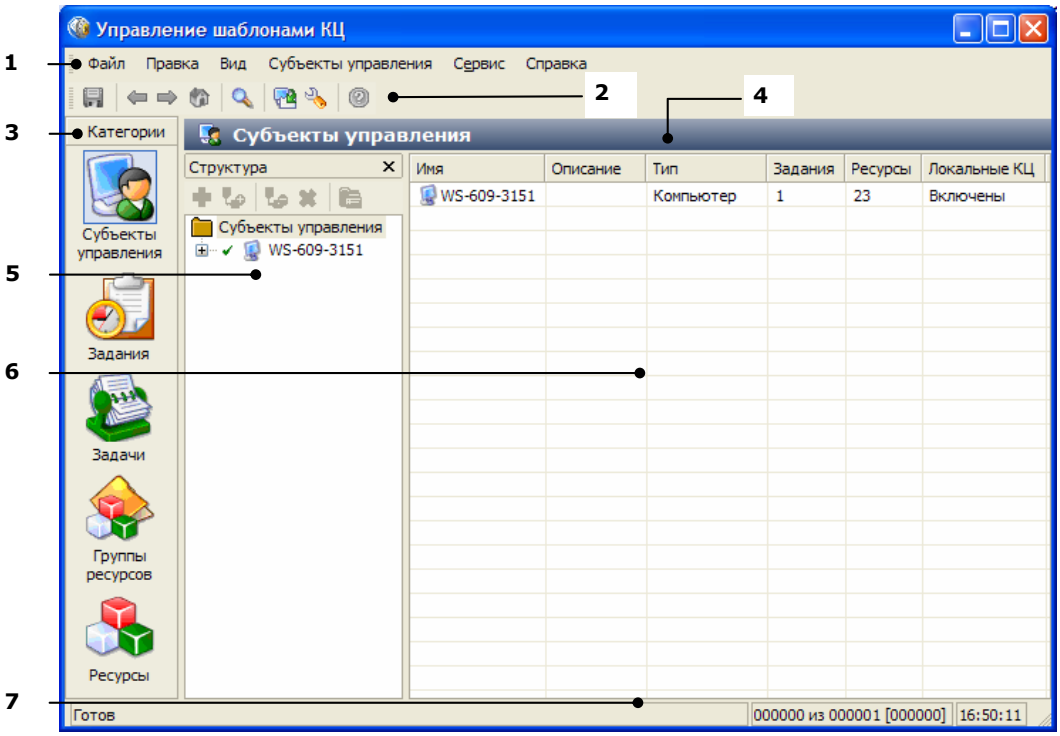


Рис. 11. Главное окно программы управления шаблонами КЦ

Основное окно программы содержит следующие основные элементы интерфейса:

(1) Меню
Содержит команды управления программой
(2) Панель инструментов основного окна
Содержит кнопки быстрого вызова команд управления и программных средств
(3) Область "Категории"
Предназначена для выбора категории представления объектов. Содержит ярлыки вызова одноименных команд меню "Вид". Чтобы отобразить в программе объекты, относящиеся к категории, выберите на панели ее ярлык (например, для вывода списка имеющихся заданий на контроль целостности среды выберите ярлык "Задания"). Если места для отображения всех ярлыков недостаточно, в верхней и/или нижней части панели появляются кнопки прокрутки. Используйте эти кнопки для перехода к нужному ярлыку
(4) Заголовок активной категории
Отображает название выбранной категории представления объектов
(5) Область "Структура"
Предназначено для выбора объекта в иерархическом списке. Корневым элементом иерархии является выбранная категория. Структура объектов создается посредством создания вложенных объектов или связывания с объектами, которые относятся к другим категориям. Для наглядности отображения пиктограммы объектов, которые предполагают наличие связей с другими объектами, отмечены специальными знаками: • (красным цветом окрашена нижняя половина кружка) — объект не включает в себя другие объекты; • (красным цветом окрашена верхняя половина кружка) — объект не включен ни в один из других объектов; • — объект никак не связан с другими объектами; • ✓ — для объекта установлены все предполагаемые связи с другими объектами. Панель инструментов, расположенная в верхней части окна, содержит кнопки быстрого вызова команд управления списком объектов

(6) Область "Список объектов"
Предназначена для отображения списка объектов, входящих в выбранный объект. Информация об объектах представлена в табличной форме. Элементы списка отображаются в определенном цветовом оформлении. Строка таблицы выделяется соответствующим цветом, если объект находится в одном из следующих состояний: • для объекта установлены все предполагаемые связи с другими объектами — по умолчанию текст на белом фоне; • объект предполагает наличие одной из связей, но она отсутствует — по умолчанию текст на розовом фоне; • ресурс не поставлен на контроль — по умолчанию текст на сером фоне.
(7) Строка состояния
Содержит служебные сообщения программы. В правой части строки выделены зоны, в которых помещается следующая информация (по порядку слева направо): • порядковый номер выбранного объекта, общее количество и количество выделенных объектов в области списка объектов; • текущее время.

Корректировка шаблонов контроля целостности

Корректировка шаблонов с помощью программы управления шаблонами КЦ заключается в реализации следующих основных процедур:

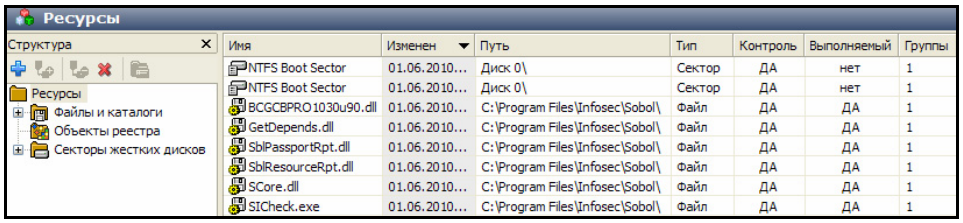
- создание новых объектов (одиночных ресурсов, групп ресурсов) для контроля целостности;
- добавление групп ресурсов в задание на контроль целостности для комплекса "Соболь";
- удаление объектов, для которых контроль целостности не требуется.

Создание одиночных ресурсов

Для создания одиночного ресурса (файл, сектор, элемент реестра):

1. В области "Категории" главного окна программы управления шаблонами КЦ (см. Рис. 11 на стр. 57) выберите категорию "Ресурсы".

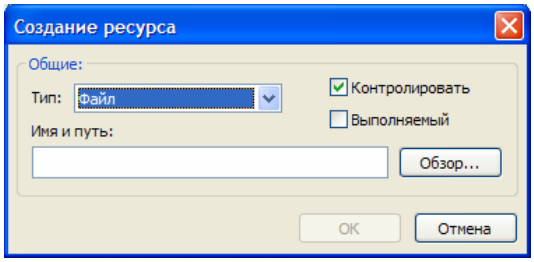
   Окно "Ресурсы" примет вид, подобный следующему:



   Пояснение. Папки "Файлы и каталоги", "Объекты реестра" и "Секторы жестких дисков" созданы по умолчанию во время установки ПО комплекса.

2. В панели инструментов области "Структура" нажмите кнопку  "Добавить новый (Insert)".

   На экране появится диалоговое окно "Создание ресурса":



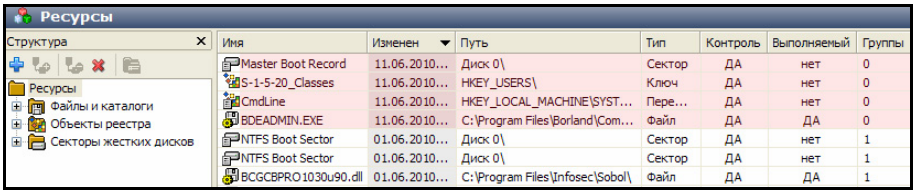
3. Выполните следующие действия:
   - В раскрывающемся списке "Тип" выберите необходимый ресурс "Файл"/"Переменная реестра"/"Ключ реестра"/"Секторы диска".
   - Нажмите кнопку "Обзор".

- В появившемся соответствующем окне "Выбор файла"/"Просмотр реестра"/"Секторы" выберите необходимый ресурс и нажмите "Открыть"/"ОК".

  В списке "Имя и путь" окна "Создание ресурса" появится путь к выбранному ресурсу.

- Нажмите "ОК".

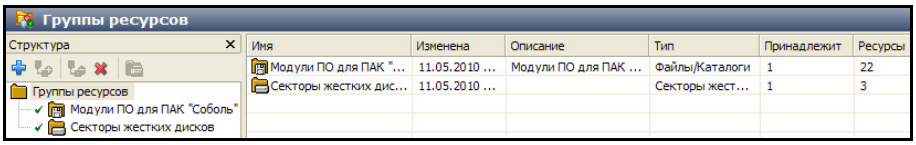
  Окно "Ресурсы" примет вид, подобный следующему:



4. Добавьте выбранные одиночные ресурсы в группы ресурсов. Для этого:

- В области "Категории" главного окна программы управления шаблонами КЦ выберите категорию "Группы ресурсов".

  Окно "Группы ресурсов" примет следующий вид:



Пояснение. Группы ресурсов "Модули ПО для ПАК "Соболь" и "Секторы жестких дисков" созданы по умолчанию во время установки ПО комплекса.

- В панели инструментов области "Структура" нажмите кнопку  "Добавить новый (Insert)".

  На экране появится диалоговое окно "Создание группы ресурсов":

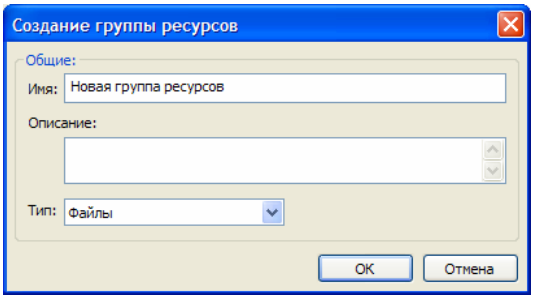
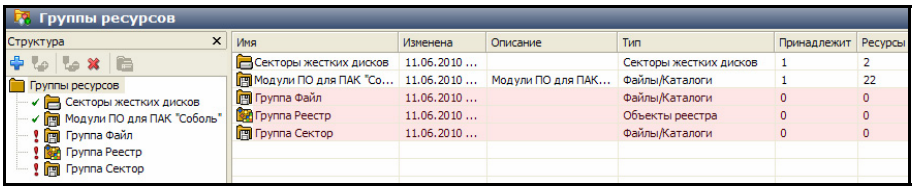


Рис. 12. Окно "Создание группы ресурсов"

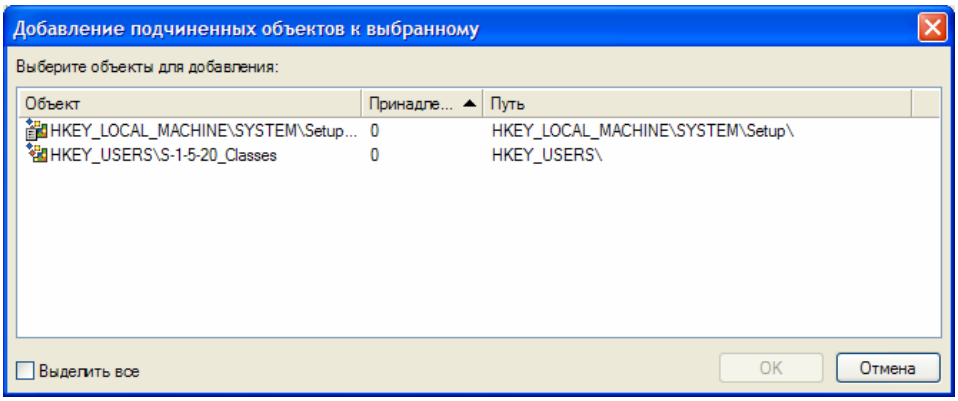
- Выполните следующие действия:
  - в поля "Имя" и "Описание" введите соответственно имя создаваемой группы (например, "Группа Файл"/"Группа Реестр"/"Группа Сектор") и при необходимости краткую дополнительную информацию о группе;
  - в раскрывающемся списке "Тип" выберите "Файлы"/"Объекты реестра"/"Секторы жестких дисков";
  - нажмите "ОК".

  Окно "Группы ресурсов" примет вид, подобный следующему:



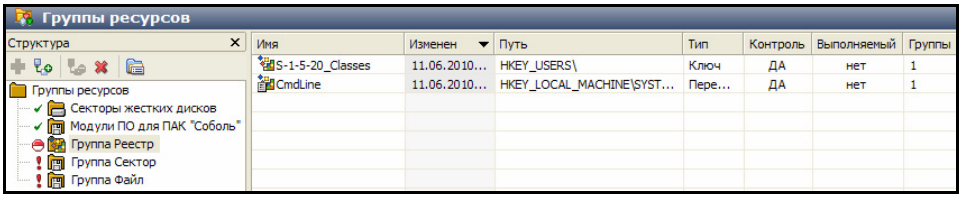
5. В области "Структура" вызовите контекстное меню созданной папки (например, "Группа Реестр") и выполните команду "Добавить ресурсы" I "Существующие".

На экране появится диалоговое окно, подобное следующему:



6. Выберите ресурсы, которые вы планируете включить в группу ресурсов, и нажмите "ОК".

   В областях "Структура" и "Список объектов" появятся выбранные объекты:



Создание групп ресурсов

Создание группы файлов

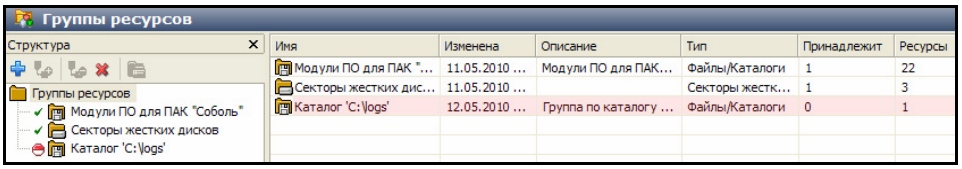
Группы файлов для КЦ можно создавать посредством команд "По каталогу", "Вручную", с помощью генератора задач.

Для создания группы файлов (команда "По каталогу"):

1. В области "Категории" главного окна программы управления шаблонами КЦ выберите категорию "Группы ресурсов".
2. В области "Структура" вызовите контекстное меню папки "Группы ресурсов" и выполните команду "Создать группу" I "По каталогу".

   На экране появится стандартный диалог обзора папок ОС Windows.
3. Выберите необходимый каталог и нажмите "ОК". В появившемся информационном окне "Управление шаблонами КЦ" нажмите "ОК".

   Окно "Группы ресурсов" примет вид, подобный следующему:

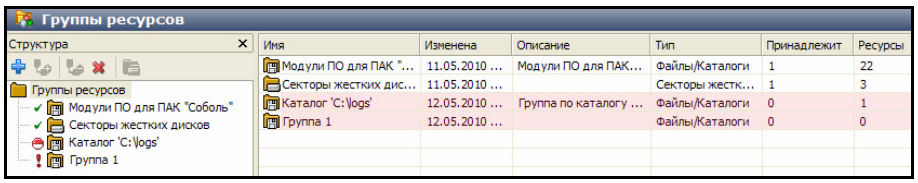


Для создания группы файлов (команда "Вручную"):

1. В области "Категории" главного окна программы управления шаблонами КЦ выберите категорию "Группы ресурсов". В панели инструментов области "Структура" нажмите кнопку  "Добавить новый (Insert)".

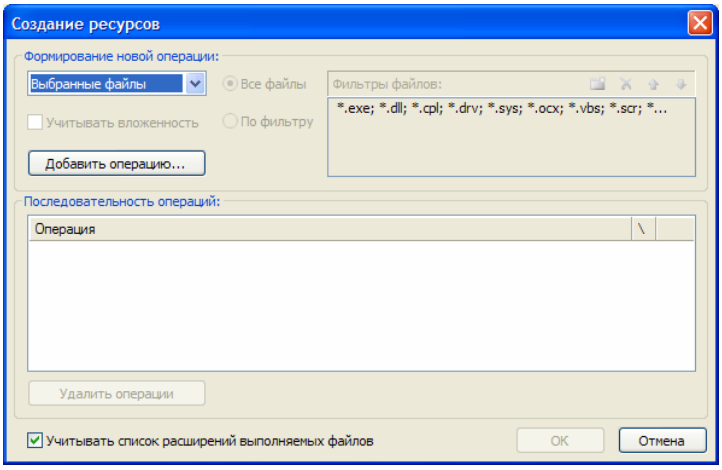
   На экране появится диалоговое окно "Создание группы ресурсов" (см. Рис. 12 на стр. 59).
2. Выполните следующие действия:
   - в поля "Имя" и "Описание" введите соответственно имя создаваемой группы (например, "Группа 1") и при необходимости краткую дополнительную информацию о группе;
   - в раскрывающемся списке "Тип" выберите "Файлы";
   - нажмите "ОК".

Окно "Группы ресурсов" примет вид, подобный следующему:



3. В области "Структура" вызовите контекстное меню папки созданной группы и выполните команду "Добавить ресурсы" I "Несколько новых".

   На экране появится диалоговое окно "Создание ресурсов":



Диалог состоит из двух частей. Верхняя часть диалога (группа полей "Формирование новой операции") предназначена для указания варианта отбора ресурсов и задания дополнительных условий. Для одного и того же варианта может быть задано несколько условий. Добавление ресурсов по варианту и соответствующему ему дополнительному условию называется операцией. Для одного и того же варианта может быть выполнено несколько операций.

Чтобы выполнить операцию, необходимо выбрать вариант, задать дополнительные условия и затем нажать кнопку "Добавить операцию".

Нижняя часть диалога (группа полей "Последовательность операций") предназначена для отображения последовательности выполненных операций.

Параметры, используемые при выполнении операции добавления новых файлов для КЦ, описаны в следующей таблице:

Параметр	Пояснение
Вариант выбора ресурсов	Доступно 2 варианта: • "Выбранные файлы" (стандартная процедура выбора файлов; дополнительные условия недоступны). • "Файлы по каталогу" (добавляются файлы, входящие в указанный каталог, учитывается вложенность, можно использовать фильтр).
Учитывать вложенность **Все файлы** **По фильтру**	Параметры активны только для варианта "Файлы по каталогу"

4. Настройте параметры выбора ресурсов.

   Далее, в зависимости от выбранного варианта, перейдите к действию процедуры, указанному в таблице:

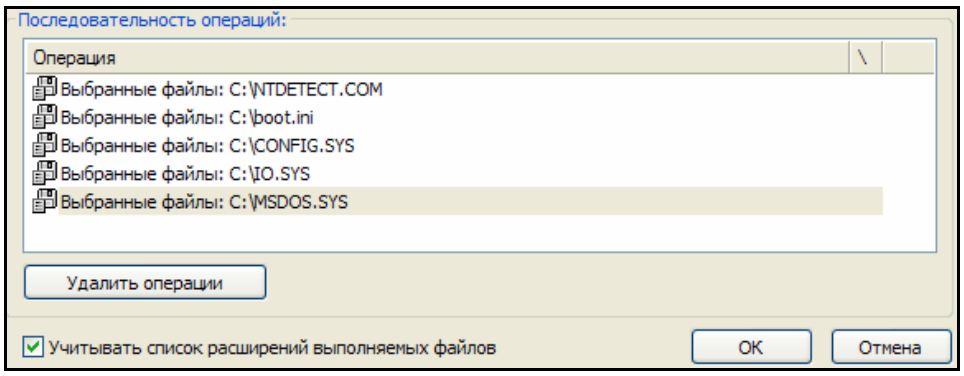
Если выбрано...	...перейдите к действию:
Выбранные файлы	5
Файлы по каталогу	7

5. Нажмите кнопку "Добавить операцию".

   На экране появится стандартный диалог выбора файлов ОС Windows.

6. Выберите необходимые файлы.

В нижней части диалога появится список операций, подобный следующему:



Каждому выбранному файлу соответствует своя операция.

Если требуется удалить операции, выделите их в списке и нажмите кнопку "Удалить операции".

Далее:

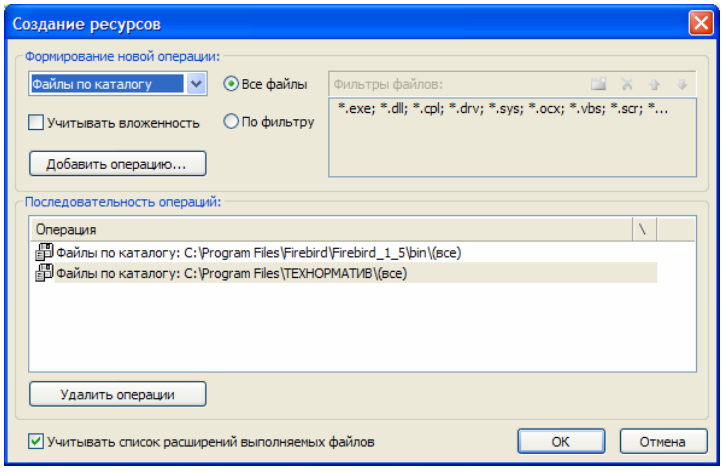
- Если другие ресурсы добавлять не требуется, перейдите к действию **9**.
- Если требуется добавить другие ресурсы, вернитесь к выполнению действия **4** данной процедуры.

7. Настройте дополнительные параметры (при использовании фильтра выделите его строку в списке "Фильтры файлов") и нажмите кнопку "Добавить операцию".

На экране появится стандартный диалог выбора каталога ОС Windows.

8. Выберите каталог и нажмите "OK".

Диалог выбора каталога закроется и в нижней части диалога "Создание ресурсов" добавится описание выполненной операции, подобное следующему:

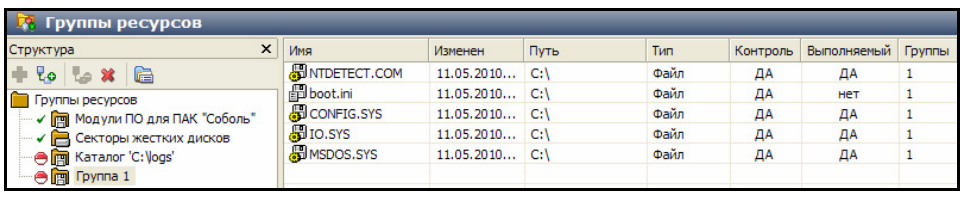


Далее:

- Если другие ресурсы добавлять не требуется, перейдите к действию **9**.
- Если требуется добавить другие ресурсы, вернитесь к выполнению действия **4** данной процедуры.

9. Проанализируйте список выполненных операций и, если он содержит все ресурсы, планируемые для включения в модель данных, нажмите "OK".

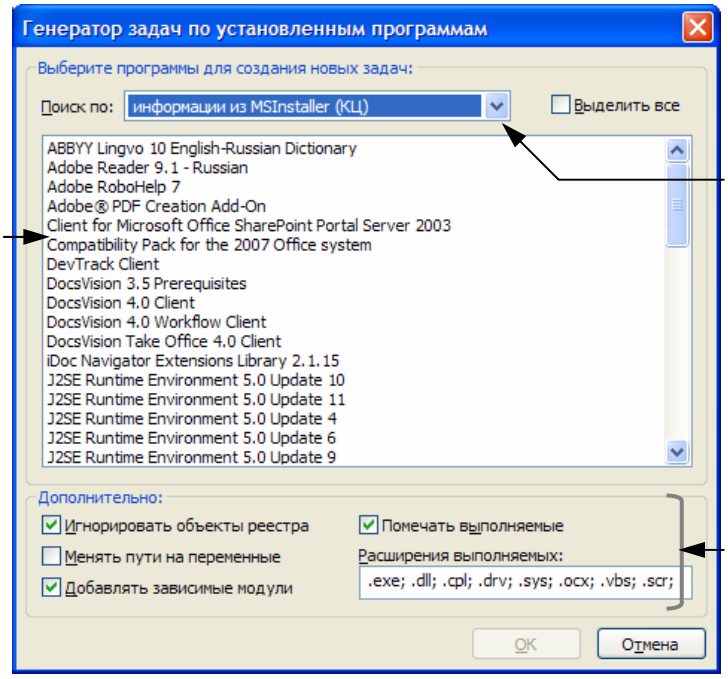
Диалог "Создание ресурсов" закроется. Окно "Группы ресурсов" примет вид, подобный следующему:



Для создания группы файлов с помощью генератора задач:

1. В области "Категории" главного окна программы управления шаблонами КЦ выберите категорию "Группы ресурсов". В меню главного окна программы управления шаблонами КЦ активируйте команду "Сервис" I "Генератор задач".

   На экране появится следующее диалоговое окно:



   Диалог предназначен для выбора программ, а также задания дополнительных условий отбора ресурсов.

2. В раскрывающемся списке "Поиск по" выберите источник, из которого будет произведен выбор программ.

3. Выберите в списке программы и укажите в нижней части диалога дополнительные условия отбора ресурсов.

Для выделения нескольких программ используйте клавишу <Ctrl>. Для выделения всего списка поставьте отметку в поле "Выделить все".

Условие	Пояснение
Игнорировать объекты реестра	Ресурсы, являющиеся элементами реестра, в задачи не включаются
Менять пути на переменные	При записи в модель данных абсолютные пути к файлам и каталогам меняются на имена переменных окружения ОС Windows
Добавлять зависимые модули	Зависимые модули — это файлы, от которых зависит исполнение исходных файлов. Например, это могут быть драйверы и библиотеки, не входящие непосредственно в запускаемые пользователем приложения, но без которых работа этих приложений невозможна. Зависимые модули добавляются в ту же группу ресурсов, где находится исходный файл
Помечать выполняемые	Используется для выделения файлов с заданными расширениями в столбце "Выполняемый" области "Список объектов"

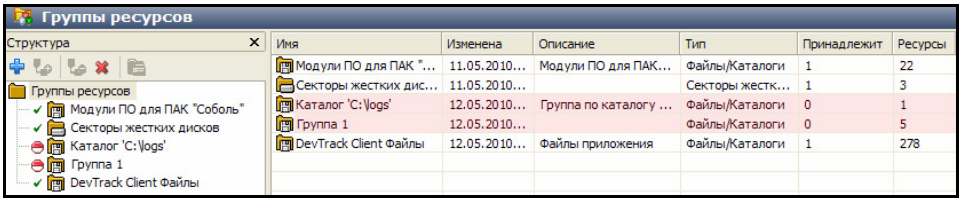
При выборе из списка MS Installer можно задать каждое из приведенных выше дополнительных условий. При выборе по ярлыкам из меню "Пуск" можно задать только два условия: "Менять пути на переменные" и "Помечать выполняемые".

4. Нажмите "OK".

   Начнется процесс генерации. Затем появится сообщение о его успешном завершении.

5. Нажмите "OK" в окне сообщения.

   Окно "Группы ресурсов" примет вид, подобный следующему:



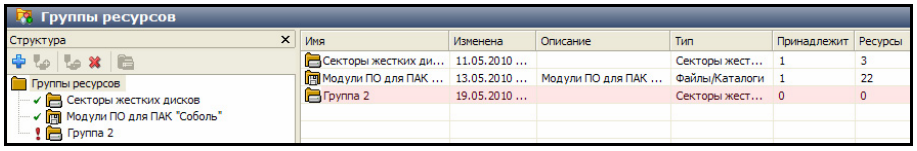
Создание группы секторов

Для создания группы секторов жесткого диска:

1. В области "Категории" главного окна программы управления шаблонами КЦ выберите категорию "Группы ресурсов".
2. В области "Структура" вызовите контекстное меню папки "Группы ресурсов" и выполните команду "Создать группу" I "Вручную".

   На экране появится диалоговое окно "Создание группы ресурсов" (см. Рис. 12 на стр. 59).
3. Выполните следующие действия:
   - в поля "Имя" и "Описание" введите соответственно имя создаваемой группы (например, "Группа 2") и при необходимости краткую дополнительную информацию о группе;
   - в раскрывающемся списке "Тип" выберите "Секторы жестких дисков";
   - нажмите "ОК".

   Окно "Группы ресурсов" примет вид, подобный следующему:

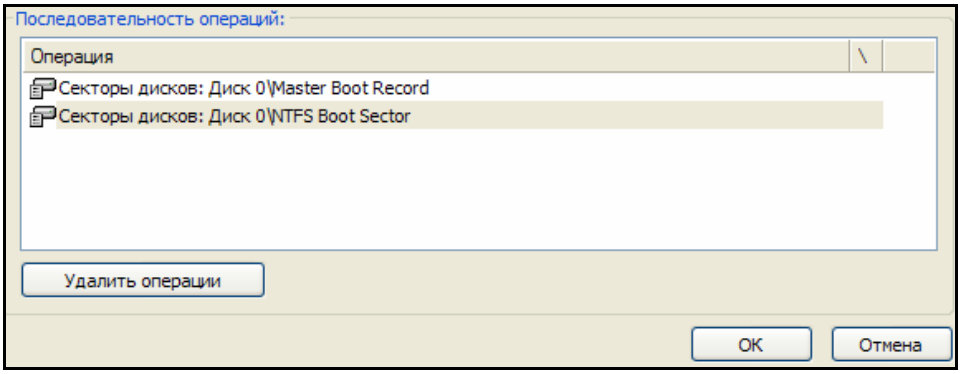


4. В области "Структура" вызовите контекстное меню папки созданной группы и выполните команду "Добавить ресурсы" I "Несколько новых".

   На экране появится диалоговое окно "Создание ресурсов".
5. Нажмите кнопку "Добавить операцию".

   На экране появится диалог выбора секторов.
6. Выберите нужные секторы и нажмите "ОК".

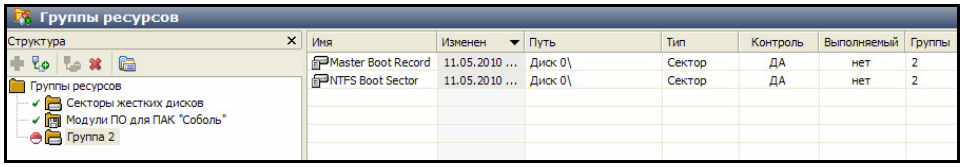
   В нижней части диалога "Создание ресурсов" появится список операций, подобный следующему:



Если требуется удалить операции, выделите их в списке и нажмите кнопку "Удалить операции".

7. Нажмите "ОК".

   Диалог "Создание ресурсов" закроется. Окно "Группы ресурсов" примет вид, подобный следующему:



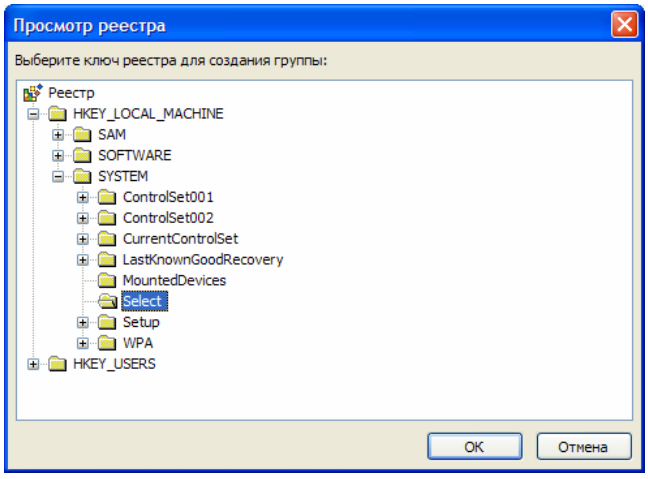
Создание группы элементов системного реестра

Программа управления шаблонами позволяет формировать для механизма КЦ следующие группы элементов системного реестра: ключи реестра с переменными (посредством команд "По ключу реестра", "Вручную") и переменные ключей реестра.

Для создания группы ключей реестра с переменными (команда "По ключу реестра"):

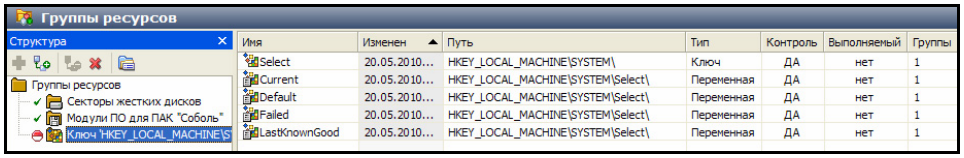
1. В области "Категории" главного окна программы управления шаблонами КЦ выберите категорию "Группы ресурсов".
2. В области "Структура" вызовите контекстное меню папки "Группы ресурсов" и выполните команду "Создать группу" I "По ключу реестра".

   На экране появится окно "Просмотр реестра":



3. Выберите необходимый элемент реестра и нажмите "ОК". В появившемся информационном окне "Управление шаблонами КЦ" нажмите "ОК".

   Окно "Группы ресурсов" примет вид, подобный следующему:

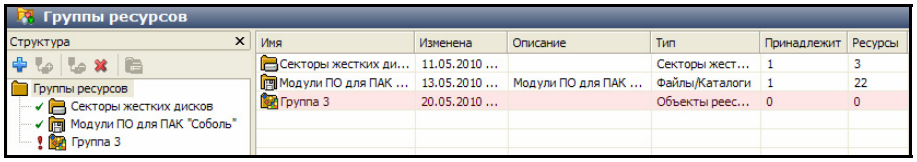


Для создания группы ключей реестра с переменными (команда "Вручную"):

1. В области "Категории" главного окна программы управления шаблонами КЦ выберите категорию "Группы ресурсов".
2. В области "Структура" вызовите контекстное меню папки "Группы ресурсов" и выполните команду "Создать группу" I "Вручную".

   На экране появится диалоговое окно "Создание группы ресурсов" (см. Рис. 12 на стр. 59).
3. Выполните следующие действия:
   - в поля "Имя" и "Описание" введите соответственно имя создаваемой группы (например, "Группа 3") и при необходимости краткую дополнительную информацию о группе;
   - в раскрывающемся списке "Тип" выберите "Объекты реестра";
   - нажмите "ОК".

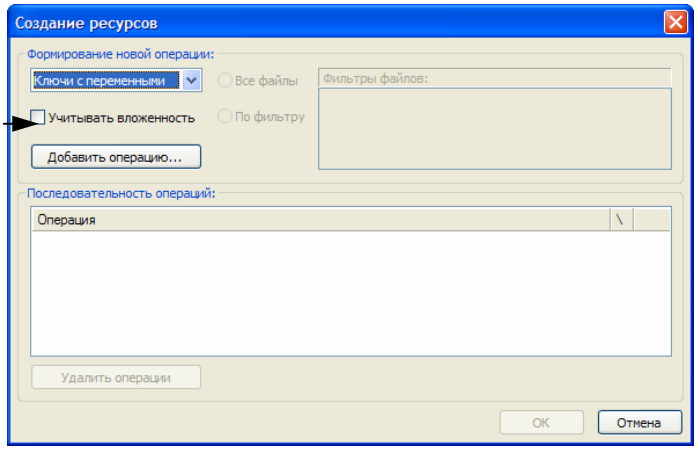
     Окно "Группы ресурсов" примет вид, подобный следующему:



4. В области "Структура" вызовите контекстное меню папки созданной группы и выполните команду "Добавить ресурсы" I "Несколько новых".

   На экране появится диалоговое окно "Создание ресурсов":

Для учета вложенности поставьте отметку

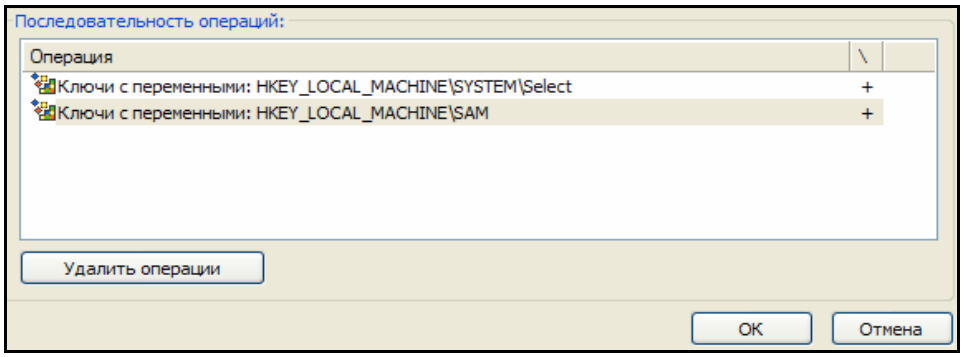


5. Выберите параметр "Ключи с переменными". Нажмите кнопку "Добавить операцию".

   На экране появится окно "Просмотр реестра".

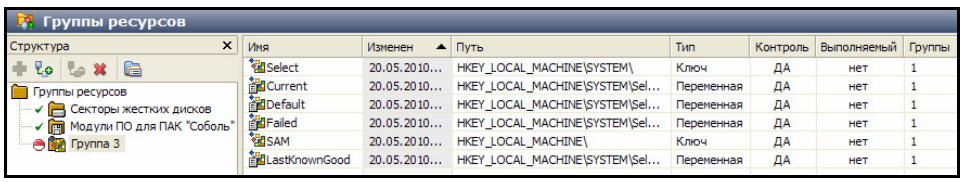
6. Выберите необходимые элементы реестра и нажмите "ОК".

   В нижней части диалога "Создание ресурсов" появится список операций, подобный следующему:



7. Нажмите "ОК".

   Диалог "Создание ресурсов" закроется. Окно "Группы ресурсов" примет вид, подобный следующему:



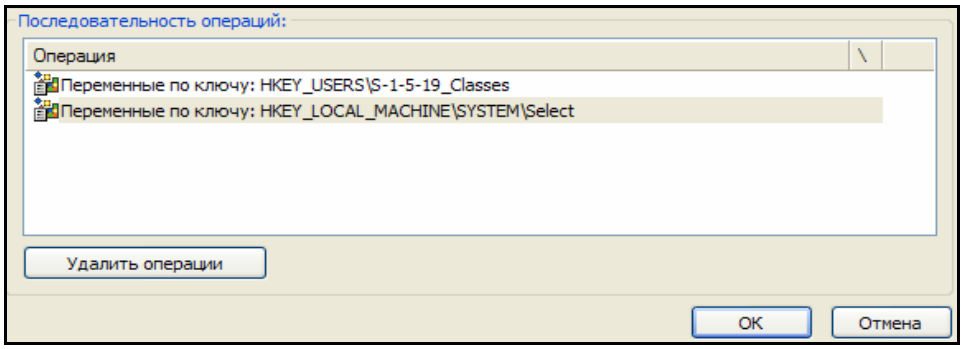
Для создания группы переменных ключей реестра:

1. Выполните действия **1**–**4** предыдущей процедуры создания группы ключей реестра с переменными.
2. Выберите параметр "Переменные по ключу". Нажмите кнопку "Добавить операцию".

   На экране появится окно "Просмотр реестра".

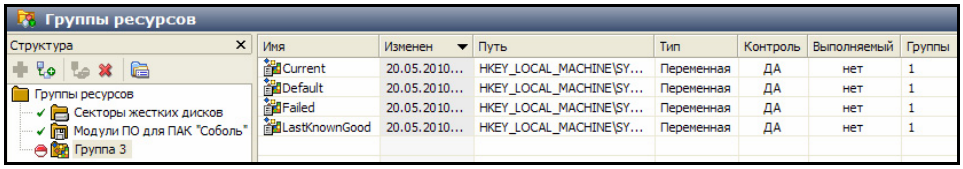
3. Выберите необходимые элементы реестра и нажмите "ОК".

В нижней части диалога "Создание ресурсов" появится список операций, подобный следующему:



4. Нажмите "ОК".

   Диалог "Создание ресурсов" закроется. Окно "Группы ресурсов" примет вид, подобный следующему:

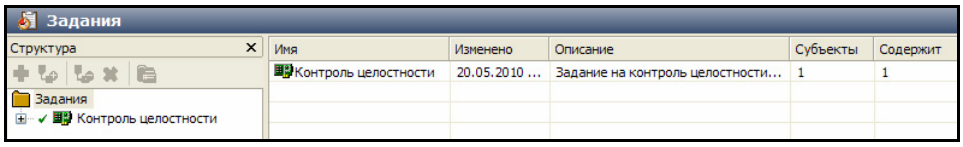


Добавление объектов в задание на контроль целостности

Для добавления объектов:

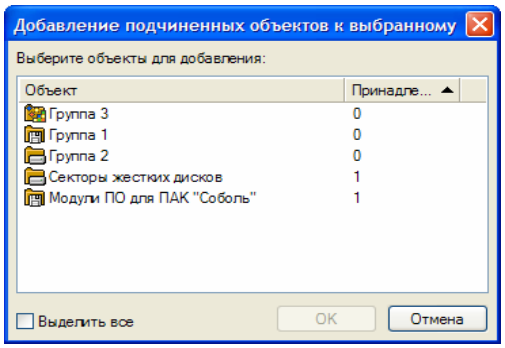
1. В панели категорий главного окна программы "Управление шаблонами КЦ" выберите категорию "Задания".

   Окно "Задания" примет следующий вид:



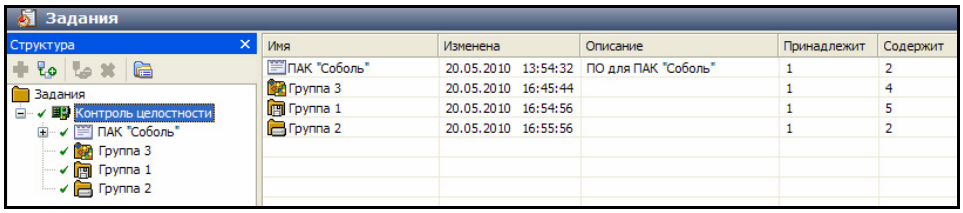
2. В области "Структура" вызовите контекстное меню папки "Контроль целостности" и выполните команду "Добавить задачи/группы" | "Существующие".

   На экране появится диалоговое окно, подобное следующему:



3. Выберите объекты, которые вы планируете включить в задание на контроль целостности, и нажмите "ОК".

   В областях "Структура" и "Список объектов" появятся выбранные объекты:



Удаление объектов из задания на контроль целостности

В программе управления шаблонами КЦ предусмотрены два варианта удаления объектов: окончательное удаление и удаление с возможностью восстановления.

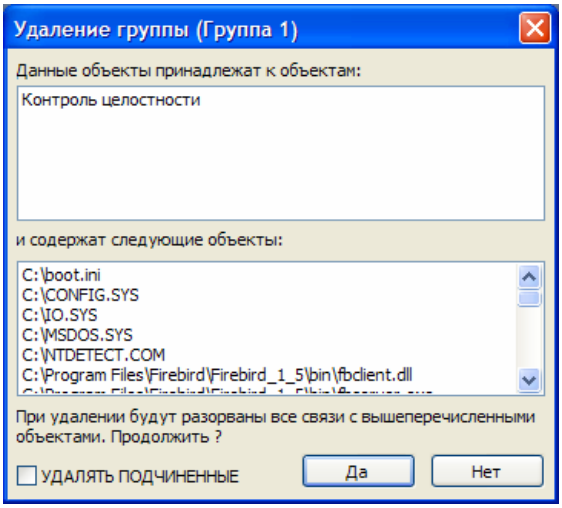
Для удаления объектов:

1. В панели категорий главного окна программы "Управление шаблонами КЦ" выберите категорию "Задания".
2. В области "Структура" или "Список объектов" вызовите контекстное меню папки объекта, который вы намереваетесь исключить из задания на КЦ с возможностью восстановления. Выполните для группы ресурсов команду "Исключить из" | "Задачи/Задания", для задачи — "Исключить из" | "Задания".

   На экране появится информационное окно "Управление шаблонами КЦ".
3. Нажмите кнопку "Да".

   Выбранный объект будет исключен из задания.
4. Для восстановления объекта выполните действия **2**, **3** процедуры "Добавление объектов в задание на контроль целостности" (см. стр. 67).
5. Для окончательного удаления объекта из задания в области "Структура" или "Список объектов" вызовите контекстное меню папки объекта и выполните команду "Удалить".

   На экране появится окно, подобное следующему:



6. Нажмите кнопку "Да".

   Выбранный объект будет исключен из задания окончательно.

Формирование отчета о контролируемых объектах

Программа предоставляет возможность создать rtf-файл со списком объектов, включенных в шаблоны КЦ, с указанием их полного пути.

Для формирования отчета:

1. В меню главного окна программы управления шаблонами КЦ (см. Рис. 11 на стр. 57) активируйте команду "Сервис" | "Отчеты" | "Ресурсы рабочей станции".
2. В появившемся на экране диалоге "Ресурсы рабочей станции" при необходимости измените имя файла-отчета и его место размещения. Нажмите кнопку "Дополнительно" и установите параметры отображения отчета.
3. Нажмите кнопку "Построить".

Сохранение, импорт и экспорт модели данных

Сохранение

Любые изменения в модели данных, выполненные в ходе эксплуатации программы управления шаблонами КЦ, при необходимости могут быть сохранены.

Для сохранения изменений:

Выполните одно из следующих действий:

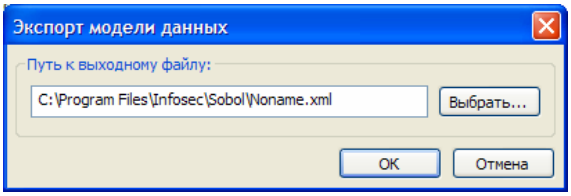
- в панели инструментов нажмите кнопку  "Сохранить модель";
- нажмите комбинацию клавиш <Ctrl>+<S>;
- в меню "Файл" активируйте команду "Сохранить".

Экспорт

Для экспорта текущей модели данных:

1. В меню "Файл" активируйте команду "Экспорт модели в XML".

   На экране появится диалог "Экспорт модели данных":



2. В поле "Путь к выходному файлу" введите полное имя файла, в котором будут храниться данные об объектах экспортируемой модели. При необходимости укажите другой путь размещения xml-файла. Для задания нового пути используйте клавиатуру или стандартный диалог ОС Windows, который вызывается путем нажатия кнопки "Выбрать".
3. В диалоге "Экспорт модели данных" нажмите "ОК".

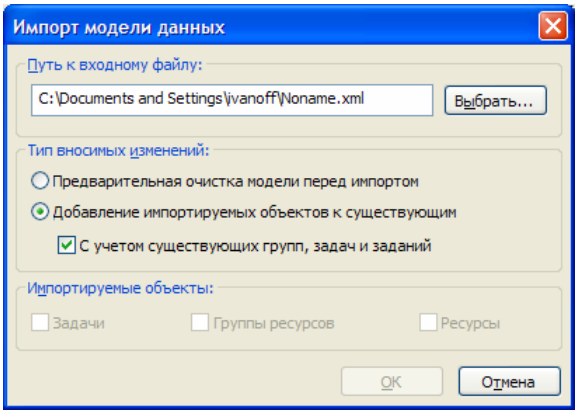
   На экране появится информационное сообщение о результатах экспорта модели данных.
4. Нажмите "ОК".

Импорт

Для импорта модели данных:

1. В меню "Файл" активируйте команду "Импорт модели из XML".
2. Если с момента последнего сохранения модели в ней были сделаны изменения, то на экране появится сообщение, предупреждающее о потере изменений после загрузки модели. Нажмите кнопку "Да".

   На экране появится диалог "Импорт модели данных":



3. В поле "Путь к входному файлу" введите полное имя файла, в котором хранятся данные об объектах импортируемой модели, и путь к нему. Для ввода используйте клавиатуру или стандартный диалог ОС Windows, который вызывается путем нажатия кнопки "Выбрать".
4. В группе полей "Тип вносимых изменений" выберите режим импорта. Для этого установите отметку в одном из следующих полей:

Предварительная очистка модели перед импортом
Перед импортом удаляются все объекты текущей модели данных. После импорта модель будет состоять только из объектов, взятых из импортируемого файла
Добавление импортируемых объектов к существующим
После импорта модель будет содержать как импортированные объекты, так и объекты текущей модели данных. При импорте возможна ситуация "дублирования" объектов. Это происходит, если отключен параметр "С учетом существующих групп, задач и заданий" или в модели уже есть объекты этих категорий с такими же названиями. Если объекты относятся к категориям "Задачи" или "Группы ресурсов", то после импорта модель данных будет содержать пары дублирующихся объектов. Добавляемый объект каждой пары будет иметь имя: *имя_объекта*<*N*>, где "*N*" — порядковый номер дублируемого объекта. Для объектов категории "Ресурсы" дублирующиеся объекты не создаются.

5. В группе полей "Импортируемые объекты" выберите категории объектов, которые следует импортировать. Для этого установите отметки в полях с названиями соответствующих категорий (если в выбранном файле нет данных об объектах какой-либо категории, соответствующее ей поле заблокировано).
6. В диалоге "Импорт модели данных" нажмите "ОК".

   На экране появится информационное сообщение о результате импорта модели данных.
7. Нажмите "ОК".

Расчет эталонных значений контрольных сумм

После корректировки шаблонов КЦ необходимо заново рассчитать эталонные значения контрольных сумм.

Внимание! Перед запуском процедуры расчета КЦ отключите от USB-портов компьютера все устройства класса USB Mass Storage Device (flash-накопители, CD-, DVD-приводы и т. п.).

Для расчета контрольных сумм:

1. Перезагрузите компьютер и войдите в систему с правами администратора комплекса "Соболь" (см. стр. 33).
2. В меню администратора (см. Рис. 5 на стр. 35) выберите команду "Расчет контрольных сумм" и нажмите клавишу <Enter>.

   Начнется расчет эталонных значений контрольных сумм объектов, заданных шаблонами КЦ. При этом на экране появится окно, которое отображает процесс расчета контрольных сумм.

   Процесс расчета можно прервать, нажав клавишу <Esc>. При обнаружении ошибки процесс расчета останавливается и на экран выводится сообщение об ошибке. Изучите это сообщение. Для возобновления расчета нажмите любую клавишу.

Расчет эталонных значений контрольных сумм считается завершившимся успешно, если в процессе расчета не зафиксировано ни одной ошибки (поле "Найдено ошибок" содержит значение "0").

При обнаружении ошибок (не найден заданный файл или сектор и т. д.) необходимо выяснить и устранить причины их возникновения. Например, если не найдены заданные файлы, откорректируйте шаблоны КЦ файлов, исключив из него отсутствующие на диске файлы (см. стр. 58). После того как все выявленные недостатки будут устранены, повторите процедуру расчета эталонных значений контрольных сумм. Подробный список сообщений об ошибках содержится на стр. 76.

Приложение

Сообщения комплекса "Соболь"

Информация, сообщаемая администратору при входе в систему

Параметр	Пояснение
Номер идентификатора	Тип и номер персонального идентификатора, предъявленного администратором при входе в систему
Время текущего входа	Время ("часы : минуты") и дата ("день/месяц/год") того момента времени, когда администратор ввел свой пароль при текущем входе в систему
Имя последнего пользователя	Имя пользователя комплекса "Соболь", выполнившего вход в систему последним перед текущим входом администратора. Параметр отсутствует, если учетная запись этого пользователя удалена из списка пользователей комплекса "Соболь"
Номер идентификатора последнего пользователя	Тип и номер персонального идентификатора, предъявленного пользователем, выполнившим вход в систему последним перед текущим входом администратора
Время входа последнего пользователя	Время ("часы : минуты") и дата ("день / месяц / год") того момента времени, когда был выполнен вход в систему пользователя, предшествующий текущему входу администратора. Номер персонального идентификатора этого пользователя содержится в строке "Номер идентификатора последнего пользователя"
Суммарное количество неудачных попыток входа	Число, показывающее, сколько раз с момента последней инициализации комплекса "Соболь" пользователи допустили ошибку при входе в систему, неверно указав пароль или предъявив не принадлежащий им персональный идентификатор

Сведения о пользователе, отображаемые в списке пользователей

Параметр	Пояснение
Имя пользователя	Имя, присвоенное пользователю при его регистрации в списке пользователей
Номер идентификатора	Тип и номер персонального идентификатора, принадлежащего пользователю
Время последнего входа	Время ("часы : минуты") и дата ("день/месяц/год") того момента времени, когда пользователь осуществил успешный вход в систему последний раз. Время и дата фиксируются в момент нажатия пользователем клавиши <Enter> при вводе пароля
Общее количество входов	Число удачных попыток входа пользователя в систему с момента его регистрации в списке пользователей

Сообщения о событиях, приводящих к блокировке компьютера

При эксплуатации комплекса "Соболь" ряд событий может приводить к блокировке компьютера. При этом на экран обычным текстом или в строке сообщений выводится сообщение о характере события, приведшего к блокировке компьютера. Затем при нажатии любой клавиши компьютер блокируется и на экране появляется сообщение:

```
Компьютер заблокирован...
```

Причина: Произошло одно из событий, приводящих к блокировке компьютера.

Действие: Выясните причину блокировки компьютера.

Следующие сообщения могут предшествовать блокировке компьютера:

```
Sobol Card: Pentium or higher processor required
```

Причина: Для нормальной работы платы комплекса "Соболь" необходим процессор с частотой 500 МГц и выше. Данный компьютер не удовлетворяет предъявляемому требованию. Компьютер блокируется для входа всех пользователей, включая администратора.

Действие: Установите комплекс "Соболь" на компьютер с требуемыми характеристиками процессора.

```
Sobol Card: Error detecting hardware
```

Причина: При старте платы комплекса "Соболь" не найден порт ввода/вывода, адрес которого находится в диапазоне адресов портов ввода/вывода, используемых этой платой. Компьютер блокируется для входа всех пользователей, включая администратора.

Действие: Проверьте исправность платы комплекса "Соболь" и разъема системной шины PCI-E/PCI, в который плата установлена.

```
Sobol Card: CPU test failed
```

Причина: При старте платы комплекса "Соболь" выполняется тестирование корректности работы процессора. Если обнаружено, что процессор работает некорректно — неправильно выполняет команды переходов, арифметические операции и т. д., то компьютер блокируется для входа всех пользователей, включая администратора.

Действие: Проверьте исправность процессора.

```
Sobol Card: Cannot find a free memory segment to relocate
ROM to
```

Причина: В первых 640 Кбайт оперативной памяти компьютера недостаточно свободного места для работы комплекса "Соболь". Компьютер блокируется для входа всех пользователей, включая администратора.

Действие: Необходимо обеспечить загрузку расширения BIOS комплекса "Соболь" до загрузки расширений BIOS других аппаратных устройств, которыми оборудован компьютер.

```
ПАК "Соболь": целостность кода нарушена. Система
остановлена
```

Причина: Нарушена целостность программного кода расширения BIOS комплекса "Соболь" или неверно выполняется алгоритм контроля целостности. Компьютер блокируется для входа всех пользователей, включая администратора.

Действие: Извлеките плату комплекса "Соболь" из компьютера и проверьте корректность функционирования оперативной памяти компьютера с помощью доступных тестов. При обнаружении ошибок замените оперативную память компьютера. Если устранить неисправность не удалось, обратитесь к поставщику комплекса.

Ошибка чтения памяти платы

Причина: Произошла ошибка при чтении данных из энергонезависимой памяти комплекса "Соболь", например, по причине нарушения структуры энергонезависимой памяти. Компьютер блокируется для входа всех пользователей, включая администратора.

Действие: Перезагрузите компьютер. Если сообщение вновь появилось на экране, проверьте исправность платы комплекса "Соболь" и разъема системной шины PCI-E/PCI, в который плата установлена. Если ошибку устранить не удалось, выполните инициализацию комплекса "Соболь" (см. стр. 23).

Нарушена целостность внутренних структур. Необходима переинициализация платы

Причина: При записи значений параметров в энергонезависимую память комплекса "Соболь" произошел сбой по техническим причинам, например, было внезапно отключено питание компьютера. В результате этого текущие значения контрольных сумм внутренних структур данных, рассчитываемые при старте системы, не совпали с эталонными значениями контрольной суммы. Компьютер заблокирован для входа всех пользователей, включая администратора.

Действие: Проведите инициализацию комплекса "Соболь" (см. стр. 23).

Нарушена целостность списка пользователей. Вход только администратором

Причина: При записи информации в список пользователей произошел сбой по техническим причинам, например, было внезапно отключено питание компьютера, что привело к изменению энергонезависимой памяти комплекса "Соболь". В результате этого текущее значение контрольной суммы списка пользователей, рассчитываемое при старте системы, не совпало с эталонным значением контрольной суммы. Компьютер заблокирован для входа всех пользователей, кроме администратора.

Действие: Перезагрузите компьютер. Если сбой повторяется, очистите список пользователей (см. стр. 45) и заново выполните их регистрацию (см. стр. 39). При повторении ситуации обратитесь к поставщику комплекса.

Нарушена целостность журнала регистрации событий. Вход только администратором

Причина: При записи в журнал регистрации событий произошел сбой по техническим причинам, например, было внезапно отключено питание компьютера, что привело к изменению энергонезависимой памяти комплекса "Соболь". В результате этого текущее значение контрольной суммы журнала, рассчитываемое при старте системы, не совпало с эталонным значением контрольной суммы. Компьютер заблокирован для входа всех пользователей, кроме администратора.

Действие: Очистите журнал регистрации событий (см. стр. 54).

Подсистема контроля целостности не сконфигурирована!

Причина: На компьютере не сконфигурирован механизм контроля целостности. Компьютер заблокирован для входа всех пользователей, кроме администратора и тех пользователей, для которых включен "мягкий" режим контроля целостности.

Действие: Выполните настройку механизма контроля целостности (см. стр. 56).

Тест ДСЧ завершился с ошибкой

Причина: При старте комплекса "Соболь" выполняется тестирование датчика случайных чисел. Если результат тестирования не соответствует требованиям ГОСТ, компьютер блокируется для входа всех пользователей, включая администратора.

Действие: Перезагрузите компьютер. При повторе ошибки тестирования проверьте правильность подключения платы комплекса "Соболь" и работоспособность разъема шины PCI-E/PCI, в который плата установлена.

Ваш вход в систему запрещен: Вы превысили предел неудачных попыток входа

Причина: Количество неудачных попыток входа данного пользователя в систему превысило величину параметра "Предельное число неудачных входов пользователя" (см. стр. 25). Компьютер блокируется для входа данного пользователя.

Действие: Чтобы разрешить данному пользователю вход в систему, присвойте параметру "Количество неудачных попыток входа" значение "0" (см. стр. 44). Затем присвойте параметру "Текущий статус пользователя" значение "не блокирован" (см. стр. 44).

Ваш вход в систему запрещен администратором

Причина: Администратор заблокировал вход в систему для данного пользователя — параметру "Текущий статус пользователя" присвоено значение "блокирован" (см. стр. 44). Компьютер блокируется при входе данного пользователя.

Действие: При необходимости разблокируйте вход в систему для пользователя, присвоив параметру "Текущий статус пользователя" значение "не блокирован".

Предупреждающие и информационные сообщения

Следующие сообщения комплекса "Соболь" предупреждают о неправильных действиях или информируют о текущем состоянии комплекса.

Введенное имя уже зарегистрировано

Причина: При регистрации нового пользователя указано имя, уже имеющееся в списке пользователей комплекса "Соболь".

Действие: Повторите ввод имени пользователя, указав другое имя.

Введенные пароли не совпадают

Причина: При регистрации администратора или пользователя либо при смене пароля администратора или пользователя введенный пароль не совпал с его подтверждением.

Действие: Повторите ввод пароля.

Минимальная длина пароля … символа(ов)

Причина: При регистрации администратора или пользователя либо при смене пароля администратора или пользователя введен пароль, число символов в котором меньше числа, заданного общим параметром "Минимальная длина пароля" (см. стр. 25).

Действие: Введите пароль допустимой длины.

Данный персональный идентификатор не принадлежит администратору

Причина: Предъявленный персональный идентификатор не принадлежит администратору.

Действие: Предъявите персональный идентификатор администратора.

Данный персональный идентификатор не принадлежит текущему пользователю

Причина: Предъявленный персональный идентификатор не принадлежит текущему пользователю.

Действие: Предъявите персональный идентификатор текущего пользователя.

Данный персональный идентификатор регистрируется впервые

Причина: Предъявленный персональный идентификатор ранее не регистрировался в системе.

Действие: Сообщение носит информационный характер и не влияет на результат регистрации. Продолжите регистрацию.

Журнал регистрации событий пуст

Причина: Журнал регистрации событий не содержит записей.

Действие: Сообщение носит информационный характер. Продолжайте работу.

Неверный персональный идентификатор или пароль

Причина: Предъявлен персональный идентификатор, не зарегистрированный в системе, или введен пароль, не соответствующий предъявленному идентификатору.

Действие: Предъявляйте принадлежащий вам идентификатор, вводите правильный пароль.

Причина: Нарушена целостность данных, хранящихся в памяти предъявленного персонального идентификатора.

Действие: Повторите процедуру регистрации с присвоением персонального идентификатора.

Пароль введен неверно

Причина: При повторной регистрации администратора или пользователя либо при смене пароля администратора или пользователя текущий пароль введен с ошибкой.

Действие: Повторите ввод пароля, не допуская ошибок.

Персональные идентификаторы типов DS1990 и DS1991 не поддерживаются

Причина: Предъявлен персональный идентификатор DS1990A или DS1991. Эти модели персональных идентификаторов не поддерживаются комплексом "Соболь".

Действие: Используйте идентификаторы DS1992, DS1993, DS1994, DS1995, DS1996.

Персональный идентификатор уже зарегистрирован на данном компьютере

Причина: При регистрации нового пользователя предъявлен идентификатор, принадлежащий другому пользователю, зарегистрированному на этом компьютере.

Действие: Повторите присвоение персонального идентификатора пользователю, предъявив идентификатор, не принадлежащий другим пользователям данного компьютера.

Производится чтение из ОЗУ…

Причина: Выполняется чтение данных из энергонезависимой памяти комплекса "Соболь".

Действие: Сообщение носит информационный характер. Если это сообщение слишком долго присутствует на экране, возможно, произошел сбой в работе системы. В этом случае перезагрузите компьютер.

Производится запись в ОЗУ…

Причина: Выполняется запись данных в энергонезависимую память комплекса "Соболь".

Действие: Сообщение носит информационный характер. Если это сообщение слишком долго присутствует на экране, возможно, произошел сбой в работе системы. В этом случае перезагрузите компьютер.

Сообщения механизма контроля целостности

При обнаружении ошибок в ходе работы механизма контроля целостности на экран выводятся следующие сообщения.

Пояснение. Если ошибка выявлена при проведении контроля целостности во время входа пользователя в систему, компьютер блокируется для входа всех пользователей, кроме администратора и тех пользователей, для которых включен "мягкий" режим контроля целостности.

**** Изменилось содержимое файла для контроля секторов**

Причина: Модифицировано содержимое файла Bootsect.nam, Bootsect.chk.

Действие: Если изменение файла Bootsect.nam вызвано корректировкой списка контролируемых секторов в программе управления шаблонами КЦ, рассчитайте эталонные значения контрольных сумм (см. стр. 70). Во всех остальных случаях выясните причину модификации указанных файлов, устраните ее, а затем восстановите шаблон КЦ секторов жестких дисков (см. стр. 58) и рассчитайте эталонные значения контрольных сумм.

**** Изменилось содержимое файла для контроля файлов**

Причина: Модифицировано содержимое файла Bootfile.nam, Bootfile.chk.

Действие: Если изменение файла Bootfile.nam вызвано корректировкой списка контролируемых файлов в программе управления шаблонами, рассчитайте эталонные значения контрольных сумм. Во всех остальных случаях выясните причину модификации указанных файлов, устраните ее, а затем восстановите шаблон КЦ файлов и рассчитайте эталонные значения контрольных сумм.

**** Изменилось содержимое файла для контроля реестра**

Причина: Модифицировано содержимое файла Bootreg.nam, Bootreg.chk.

Действие: Если изменение файла Bootreg.nam вызвано корректировкой списка контролируемых элементов реестра в программе управления шаблонами КЦ, рассчитайте эталонные значения контрольных сумм. Во всех остальных случаях выясните причину модификации указанных файлов, устраните ее, а затем восстановите шаблон КЦ элементов реестра и рассчитайте эталонные значения контрольных сумм.

**** Изменилось содержимое сектора**

Причина: Эталонное значение контрольной суммы указанного сектора не совпало с текущим значением контрольной суммы, рассчитанным для этого сектора. **Содержимое сектора модифицировано!**

Действие: Выясните и устраните причину, по которой содержимое сектора изменилось. Выполните расчет эталонных значений контрольных сумм.

**** Изменилось содержимое файла**

Причина: Эталонное значение контрольной суммы указанного файла не совпало с текущим значением контрольной суммы, рассчитанным для этого файла. **Содержимое файла модифицировано!**

Действие: Выясните и устраните причину, по которой изменилось содержимое файла. Выполните расчет эталонных значений контрольных сумм.

**** Изменилось содержимое ключа реестра**

Причина: Эталонное значение контрольной суммы указанного ключа не совпало с текущим значением контрольной суммы, рассчитанным для этого ключа. **Содержимое ключа модифицировано!**

Действие: Выясните и устраните причину, по которой изменилось содержимое ключа. Выполните расчет эталонных значений контрольных сумм.

**** Изменилось содержимое параметра реестра**

Причина: Эталонное значение контрольной суммы указанного параметра ключа реестра не совпало с текущим значением контрольной суммы, рассчитанным для этого параметра. **Содержимое параметра ключа модифицировано!**

Действие: Выясните и устраните причину, по которой изменилось содержимое параметра ключа. Выполните расчет эталонных значений контрольных сумм.

**** Ошибка чтения файла для контроля секторов**

Причина: Произошла ошибка при чтении данных из файла Bootsect.nam, Bootsect.chk.

Действие: Восстановите шаблон КЦ секторов и рассчитайте эталонные значения контрольных сумм.

**** Ошибка записи файла для контроля секторов**

Причина: Произошла ошибка при записи данных в файл Bootsect.nam, Bootsect.chk.

Действие: Восстановите шаблон КЦ секторов и рассчитайте эталонные значения контрольных сумм.

**** Ошибка чтения файла для контроля файлов**

Причина: Произошла ошибка при чтении данных из файла Bootfile.nam, Bootfile.chk.

Действие: Восстановите шаблон КЦ файлов и рассчитайте эталонные значения контрольных сумм.

**** Ошибка записи файла для контроля файлов**

Причина: Произошла ошибка при записи данных в файл Bootfile.nam, Bootfile.chk.

Действие: Восстановите шаблон КЦ файлов и рассчитайте эталонные значения контрольных сумм.

**** Ошибка чтения файла для контроля реестра**

Причина: Произошла ошибка при чтении данных из файла Bootreg.nam, Bootreg.chk.

Действие: Восстановите шаблон КЦ элементов реестра и рассчитайте эталонные значения контрольных сумм.

**** Ошибка записи файла для контроля реестра**

Причина: Произошла ошибка при записи данных в файл Bootsect.nam, Bootsect.chk.

Действие: Восстановите шаблон КЦ элементов реестра и рассчитайте эталонные значения контрольных сумм.

**** Ошибка чтения сектора**

Причина: Для указанного сектора не удалось рассчитать текущее значение контрольной суммы. Доступ к сектору на чтение завершился с ошибкой.

Действие: Выясните и устраните причину, по которой содержимое сектора недоступно для чтения. Выполните расчет эталонных значений контрольных сумм.

**** Ошибка чтения файла**

Причина: Для указанного файла не удалось рассчитать текущее значение контрольной суммы. Доступ к файлу на чтение завершился с ошибкой.

Действие: Выясните и устраните причину, по которой содержимое файла недоступно для чтения. Выполните расчет эталонных значений контрольных сумм.

**** Ошибка чтения файла реестра**

Причина: Для указанной ветки реестра не удалось рассчитать текущее значение контрольной суммы. Доступ к файлу реестра на чтение завершился с ошибкой.

Действие: Выясните и устраните причину, по которой содержимое файла реестра недоступно для чтения. Выполните расчет эталонных значений контрольных сумм.

**** Файл для контроля секторов разрушен**

Причина: Нарушена структура файла Bootsect.nam, Bootsect.chk.

Действие: Восстановите шаблон КЦ секторов жестких дисков и рассчитайте эталонные значения контрольных сумм.

**** Файл для контроля файлов разрушен**

Причина: Нарушена структура файла Bootfile.nam, Bootfile.chk.

Действие: Восстановите шаблон КЦ файлов и рассчитайте эталонные значения контрольных сумм.

**** Файл для контроля реестра разрушен**

Причина: Нарушена структура файла Bootreg.nam, Bootreg.chk.

Действие: Восстановите шаблон КЦ элементов реестра и рассчитайте эталонные значения контрольных сумм.

**** Файл реестра разрушен**

Причина: Нарушена структура файла реестра для указанной ветки реестра.

Действие: Выясните и устраните причину, по которой нарушена структура файла реестра для указанной ветки реестра. Выполните расчет эталонных значений контрольных сумм.

**** Файл для контроля секторов не найден**

Причина: Не найден файл Bootsect.nam, Bootsect.chk.

Действие: Восстановите шаблон КЦ секторов и рассчитайте эталонные значения контрольных сумм.

**** Файл для контроля файлов не найден**

Причина: Не найден файл Bootfile.nam, Bootfile.chk.

Действие: Восстановите шаблон КЦ файлов и рассчитайте эталонные значения контрольных сумм.

**** Файл для контроля реестра не найден**

Причина: Не найден файл Bootreg.nam, Bootreg.chk.

Действие: Восстановите шаблон КЦ элементов реестра и рассчитайте эталонные значения контрольных сумм.

**** Сектор не найден**

Причина: Указанный сектор жесткого диска не найден или к нему отсутствует доступ.

Действие: Выясните и устраните причину, по которой сектор не найден. При необходимости исключите этот сектор из шаблона КЦ секторов и выполните расчет эталонных значений контрольных сумм.

**** Файл не найден**

Причина: Указанный файл не найден по заданному пути или к нему отсутствует доступ.

Действие: Выясните и устраните причину, по которой файл не найден. При необходимости исключите этот файл из шаблона КЦ файлов и выполните расчет эталонных значений контрольных сумм.

**** Файл реестра не найден**

Причина: Файл реестра для указанной ветки реестра не найден по заданному пути или к нему отсутствует доступ.

Действие: Выясните и устраните причину, по которой файл реестра не найден. При необходимости исключите эту ветку реестра из шаблона КЦ элементов реестра и выполните расчет эталонных значений контрольных сумм.

**** Параметр реестра не найден**

Причина: Указанная переменная ключа не найдена или к ней отсутствует доступ.

Действие: Выясните и устраните причину, по которой переменная не найдена. При необходимости исключите эту переменную из шаблона КЦ элементов реестра и выполните расчет эталонных значений контрольных сумм.

**** Ключ реестра не найден**

Причина: Указанный ключ не найден или к нему отсутствует доступ.

Действие: Выясните и устраните причину, по которой ключ не найден. При необходимости исключите этот ключ из шаблона КЦ элементов реестра и выполните расчет эталонных значений контрольных сумм.

**** Ошибка расчета КС: один из томов может содержать ошибки**

Причина: Произошла ошибка при контроле целостности журнала транзакций.

Действие: Загрузите операционную систему. При выходе из операционной системы завершите все файловые операции.

**** Неподдерживаемый тип блока реестра**

Причина: Произошла ошибка при поиске указанного элемента реестра. Файл реестра для указанной ветки реестра содержит неподдерживаемый тип блока реестра.

Действие: Обратитесь к поставщику комплекса "Соболь". При необходимости исключите этот элемент из шаблона КЦ элементов реестра и выполните расчет эталонных значений контрольных сумм.

**** Процесс остановлен по желанию администратора**

Причина: Процесс расчета контрольных сумм остановлен администратором.

Действие: Не требуется.

Сообщения об ошибках при тестировании комплекса

При обнаружении ошибок в ходе проверки работоспособности комплекса "Соболь" (см. стр. 50) на экран выводятся следующие сообщения.

Ошибка NVRAM банк …: нет сигнала подтверждения приема данных

Ошибка NVRAM банк …: считанные данные не соответствуют записанным

Причина: Произошла ошибка при обмене данными с указанным банком NVRAM комплекса "Соболь". В первом случае ошибка вызвана нарушением механизма обмена данными с памятью, во втором — несовпадением записанных и прочитанных данных.

Действие: Повторите проверку NVRAM. При многократном повторении данного результата обратитесь в службу технической поддержки поставщика комплекса.

Тест ДСЧ неудачен … раз(а) из … попыток

Тест канала … ДСЧ неудачен … раз(а) из … попыток

Причина: Указанное число раз проверка равномерности распределения случайных чисел, генерируемых датчиком случайных чисел комплекса "Соболь", завершилась неудачей.

Действие: Повторите проверку датчика случайных чисел. При многократном повторении данного результата обратитесь в службу технической поддержки поставщика комплекса.

Ошибка чтения данных идентификатора по адресу …

Ошибка записи данных идентификатора по адресу …

Ошибка чтения номера идентификатора

Причина: Произошла ошибка при записи/чтении данных в/из идентификатор(а). Возможно, неисправен идентификатор (iButton, eToken PRO, iKey 2032, Rutoken S, Rutoken RF S) или считыватель iButton.

Действие: Повторите тест, предъявив другой идентификатор. Если тест завершился без ошибок — идентификатор/считыватель исправен. Выполните форматирование предъявленного ранее идентификатора и повторите тест. Если ошибка устойчиво повторяется — идентификатор **не** исправен, обратитесь в службу технической поддержки поставщика комплекса.

Ошибка чтения идентификатора: устройство отсутствует в считывателе

Причина: При последовательном выполнении всех тестов во время проверки идентификатора (iButton, eToken PRO, iKey 2032, Rutoken S, Rutoken RF S) не был предъявлен персональный идентификатор.

Действие: Предъявите персональный идентификатор и повторите процедуру или выполните проверку идентификатора отдельно от остальных проверок.

События, регистрируемые комплексом "Соболь"

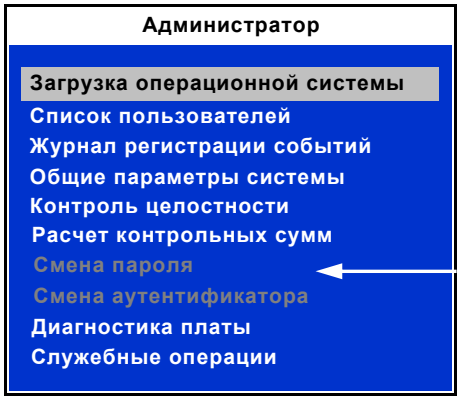
Событие	Описание события
Автоматический перерасчет КС	Расчет эталонных значений контрольных сумм выполнен по запросу, поступившему от внешней программы
Администратор сменил пароль пользователя	Администратор успешно выполнил принудительную смену пароля пользователя, имя которого указано во втором столбце таблицы записей
Администратор сменил свой пароль	Администратор успешно выполнил смену своего пароля для входа в систему
Вход администратора	Администратор осуществил успешный вход в систему
Вход пользователя	Пользователь осуществил успешный вход в систему
Добавлен новый пользователь	Администратор добавил нового пользователя в список пользователей комплекса
Запрос Все пользователи удалены	От внешней программы получен и успешно обработан запрос на удаление из списка пользователей комплекса всех пользователей
Запрос Добавление пользователя	От внешней программы получен и успешно обработан запрос на добавление нового пользователя в список пользователей комплекса
Запрос Удаление пользователя	От внешней программы получен и успешно обработан запрос на удаление пользователя из списка пользователей комплекса
Идентификатор не зарегистрирован	При входе в систему был предъявлен идентификатор, не принадлежащий ни одному из пользователей, зарегистрированных на данном компьютере. При входе администратора был указан неверный пароль
Изменены параметры загрузочного диска	Произошла смена основного загрузочного диска компьютера
Не рассчитаны контрольные суммы	Администратор не настроил механизм КЦ после инициализации комплекса — не выполнил расчет эталонных значений контрольных сумм. Если попытку входа в систему выполнял пользователь, для которого включен "жесткий" режим КЦ, его вход в систему был заблокирован
Неправильный пароль	При попытке входа в систему был предъявлен персональный идентификатор, принадлежащий зарегистрированному пользователю, но пароль был указан неверно. Ранее дважды была выполнена смена аутентификатора средствами других комплексов "Соболь" и при этом пользователь ни разу не выполнил вход в систему на данном компьютере
Обработаны внешние запросы	Запросы данных из энергонезависимой памяти комплекса, поступившие от внешних программ, обработаны без ошибок
Ошибка внешнего запроса	Невозможно обработать запрос данных из энергонезависимой памяти комплекса, поступивший от внешней программы
Ошибка КС в памяти идентификатора	Обнаружена ошибка при проверке контрольной суммы содержимого персонального идентификатора
Ошибка КС внешнего запроса	Не идентифицирована внешняя программа, от которой поступил запрос на доступ к энергонезависимой памяти комплекса
Ошибка при контроле целостности	При проверке целостности объектов перед загрузкой ОС обнаружено несовпадение эталонных значений контрольных сумм проверяемых объектов и их текущих значений для одного из проверяемых объектов. На диске отсутствуют файлы шаблонов КЦ
Перерасчет контрольных сумм	Администратор выполнил расчет эталонных значений контрольных сумм (см. стр. 70)
Переход в автономный режим	Администратор включил автономный режим работы комплекса (см. стр. 37)
Переход в сетевой режим	Администратор включил режим, позволяющий использовать комплекс совместно с другими средствами защиты (см. стр. 37)
Превышено число попыток входа	Количество неудачных попыток входа данного пользователя в систему превысило значение соответствующего параметра (см. стр. 25)
Пользователь блокирован	Пользователь, вход которого в систему блокирован, осуществил попытку входа
Пользователь сменил свой пароль	Пользователь, имя которого указано в третьем столбце таблицы записей, успешно выполнил смену своего пароля для входа в систему
Пользователь удален	Администратор удалил пользователя из списка пользователей комплекса
Смена аутентификатора администратора	Администратор успешно выполнил смену своего аутентификатора
Смена аутентификатора пользователя	Пользователь, имя которого указано в третьем столбце таблицы записей, успешно выполнил смену своего аутентификатора
Удаление системного журнала	Администратор выполнил очистку журнала регистрации событий

Эксплуатация в режиме совместного использования

Режим совместного использования позволяет применять комплекс "Соболь" совместно с другими системами защиты (например, семейство Secret Net или АПКШ "Континент"). В этом случае часть функций управления комплексом передается средствам управления той системы, совместно с которой он функционирует.

Меню администратора

В режиме совместного использования изменяется меню администратора:



Команды "Смена пароля" и "Смена аутентификатора" недоступны для использования в этом режиме

Эксплуатация комплекса в этом режиме имеет следующие особенности:

- запрещено управление некоторыми общими параметрами;
- список пользователей и журнал регистрации событий доступны администратору только для просмотра;
- администратору и пользователям не разрешается менять свой пароль и аутентификатор средствами управления комплекса "Соболь". Эти операции выполняются средствами управления той системы защиты, совместно с которой функционирует комплекс "Соболь".

Общие параметры

В режиме совместного использования недоступно управление параметрами:

- "Тестирование ДСЧ для пользователя". Параметру принудительно присваивается значение "Да" — отключить тестирование ДСЧ нельзя;
- "Показ статистики пользователю". Параметру принудительно присваивается значение "Нет" — при входе пользователей в систему информационное окно на экран не выводится;
- "Минимальная длина пароля";
- "Предельное число неудачных входов пользователя".

Подробная информация об общих параметрах содержится в Табл. 4 на стр. 37.

Журнал регистрации событий

В режиме совместного использования журнал регистрации событий доступен администратору только для просмотра. Запрещено выполнять очистку журнала.

Управление пользователями

В режиме совместного использования администратору разрешается только просматривать список пользователей и запрещается вносить в него любые изменения, в том числе менять параметры учетных записей.

Расчет контрольных сумм

При совместном использовании комплекса "Соболь" и системы защиты семейства Secret Net подготовку шаблонов КЦ и управление процедурой расчета эталонных значений контрольных сумм можно выполнять с помощью программы "Контроль программ и данных", входящей в состав системы Secret Net.

Терминологический справочник

А

Аутентификация — Проверка принадлежности субъекту (объекту) доступа предъявленного им идентификатора.

И

Идентификатор — Уникальный признак субъекта доступа, позволяющий однозначно выделить идентифицируемый субъект среди множества других субъектов. В качестве идентификаторов в комплексе "Соболь" используются таблетки iButton, USB-ключи eToken PRO, iKey 2032, Rutoken S, Rutoken RF S, смарт-карты eToken PRO, в которые с помощью специальной технологии занесены идентификационные признаки в виде кодовой информации.

Идентификация — Распознавание субъекта (объекта) по присущему или присвоенному ему идентификационному признаку.

Ж

Журнал регистрации событий — Хранилище с информацией о событиях, зарегистрированных в системе защиты, например, попытках входа в систему.

К

Ключ реестра — Запись в реестре Windows, содержащая уникальный идентификатор, присвоенный определенной части информации, находящейся в реестре. Каждый отдельный ключ может содержать элементы данных, которые называются параметрами (или переменными), а также дополнительные вложенные ключи.

Контроль целостности — Проверка наличия несанкционированной модификации файлов, секторов жесткого диска и элементов реестра защищаемого компьютера.

Контрольная сумма — Числовое значение, вычисляемое по специальному алгоритму и используемое для контроля неизменности данных.

Н

НСД — Доступ субъектов к объекту в нарушение установленных в системе правил разграничения доступа.

П

Параметр (переменная) реестра — Данные реестра, расположенные в его ключах. Каждый параметр может характеризоваться именем, типом и значением.

Р

Реестр — Иерархическая база данных, в которой ОС Windows хранит важную системную информацию.

С

Считыватель — Устройство, предназначенное для чтения (ввода) идентификационных признаков.

Субъект системы — Активный компонент системы, обычно представляемый в виде пользователя или устройства, которые могут явиться причиной потока информации от объекта к объекту или изменения состояния системы.

Документация

1	Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора	RU.40308570.501410.001 91 1
2	Программно-аппаратный комплекс "Соболь". Версия 3.0. Управление шаблонами контроля целостности в ОС МСВС 3.0. Руководство администратора	RU.40308570.501410.001 91 2
3	Программно-аппаратный комплекс "Соболь". Версия 3.0. Дополнение. Управление шаблонами контроля целостности в VMware ESX. Руководство администратора	RU.40308570.501410.001 91 3
4	Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство пользователя	RU.40308570.501410.001 92

Предметный указатель