

Код безопасности

Программно-аппаратный комплекс

Соболь

Версия 3.0



Руководство администратора

RU.40308570.501410.001 91 1



Код Безопасности

© Компания "Код Безопасности", 2014. 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:	105318, г. Москва, а/я 101, ООО "Код Безопасности"
Телефон:	8 495 982-30-20
E-mail:	info@securitycode.ru
Web:	http://www.securitycode.ru

Оглавление

Список сокращений	5
Введение	6
Глава 1. Общие сведения	7
Назначение	7
Принципы функционирования	7
Механизм идентификации и аутентификации.....	8
Механизм блокировки загрузки операционной системы со съемных носителей	9
Механизм контроля целостности	10
Механизм сторожевого таймера	11
Требования к оборудованию и программному обеспечению	12
Варианты применения	13
Эксплуатационные ограничения	14
Глава 2. Установка и удаление комплекса	18
Установка комплекса	18
Установка программного обеспечения	18
Установка платы PCI-E, PCI	20
Установка плат Mini PCI-E, Mini PCI-E Half	22
Инициализация комплекса	25
Подготовка комплекса к эксплуатации	33
Обновление программного обеспечения	34
Исправление программного обеспечения.....	34
Удаление комплекса	35
Удаление программного обеспечения	35
Изъятие платы комплекса из компьютера	35
Глава 3. Настройка и эксплуатация комплекса	37
Общий порядок настройки	37
Настройка общих параметров	40
Контроль целостности.....	42
Управление пользователями.....	43
Регистрация пользователя.....	44
Настройка параметров учетной записи	48
Удаление учетной записи пользователя.....	50
Принудительная смена пароля и аутентификатора пользователя	50
Смена пароля и аутентификатора администратора	51
Контроль работоспособности комплекса	55
Тест памяти платы	55
Тест датчика случайных чисел.....	56
Тест идентификатора	56
Последовательное выполнение всех тестов	57
Работа с журналом регистрации событий.....	57
Просмотр записей журнала.....	57
Очистка журнала	58
Служебные операции	59
Создание копии идентификатора администратора.....	59
Форматирование идентификатора	60
Программная инициализация комплекса.....	60
Обновление кода расширения BIOS плат Mini PCI-E, Mini PCI-E Half.....	61
Глава 4. Настройка механизма контроля целостности.....	62
Модель данных механизма контроля целостности.....	62
Запуск программы управления шаблонами КЦ	63
Корректировка шаблонов контроля целостности	64
Создание одиночных ресурсов.....	64
Создание групп ресурсов	66

Добавление объектов в задание на контроль целостности	75
Удаление объектов из задания на контроль целостности	76
Формирование отчета о контролируемых объектах.....	76
Сохранение, импорт и экспорт модели данных.....	77
Сохранение	77
Экспорт.....	77
Импорт.....	77
Расчет эталонных значений контрольных сумм	78
Приложение	79
Сообщения комплекса "Соболь"	79
Сообщения о событиях, приводящих к блокировке компьютера	79
Предупреждающие и информационные сообщения	81
Сообщения механизма контроля целостности	83
Сообщения об ошибках при тестировании комплекса	90
События, регистрируемые комплексом "Соболь".....	91
Эксплуатация в режиме совместного использования.....	92
Меню администратора	92
Общие параметры	92
Журнал регистрации событий	92
Управление пользователями	92
Расчет контрольных сумм	92
Информационное окно	93
Терминологический справочник	94
Документация	96

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
ПЛИС	Программируемая логическая интегральная схема
ПО	Программное обеспечение
ПСЗИ	Программное средство защиты информации
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
УНП	Уникальный номер платы
ЭВТ	Электронная вычислительная техника
ACPI	Advanced Configuration and Power Interface — расширенный интерфейс конфигурирования и управления питанием компьютера
BIOS	Basic Input/Output System — базовая система ввода-вывода
EHCI	Enhanced Host Controller Interface — USB-интерфейс
OHCI	Open Host Controller Interface — USB-интерфейс
NVRAM	Nonvolatile Random Access Memory — энергонезависимая оперативная память
SMBIOS	System Management BIOS — системное управление BIOS
UHCI	Universal Host Controller Interface — USB-интерфейс
XHCI	Extensible Host Controller Interface — USB-интерфейс

Введение

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

Сведения об установке и настройке ПО комплекса на компьютерах, функционирующих под управлением семейства ОС Linux, приводятся в документе [[2](#)].

Сведения, необходимые пользователю комплекса "Соболь", содержатся в документе [[3](#)].

Структура руководства

Материал руководства организован следующим образом:

- в **Глава 1** содержат общие сведения о функционировании защитных механизмов комплекса "Соболь";
- в **Глава 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 предупреждающего 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).

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@itsecurity.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, eToken PRO (Java), iKey 2032, Rutooken, Rutooken RF (см. [Табл. 1](#));
- защита от несанкционированной загрузки операционной системы со съемных носителей — дискет, оптических и магнитооптических дисков, ZIP-устройств, USB-устройств и др.;
- контроль целостности программного и аппаратного обеспечения защищаемого компьютера до загрузки операционной системы:
 - файлов и физических секторов жесткого диска;
 - элементов системного реестра компьютера;
 - журнала транзакций;
 - PCI-устройств;
 - структур SMBIOS;
 - таблиц ACPI;
 - конфигурации оперативной памяти;
- блокировка компьютера при условии, что после его включения управление не передано расширению BIOS комплекса "Соболь";
- 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, СЗИ vGate-S R2, СЗИ vGate R2, СЗИ Security Studio Honeypot Manager, СКЗИ "Континент-АП" и СКЗИ "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 программного и аппаратного обеспечения защищаемого 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. 20), настройка общих параметров (см. стр. 26), настройка контроля целостности (см. стр. 28), регистрация администратора (см. стр. 29).

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 осуществляются 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	eToken PRO (Java)	
DS1994	Rutoken	
DS1995	Rutoken RF	
DS1996	iKey 2032	

USB-ключи, USB-считыватели Athena ASEDrive IIIe USB V2/V3 смарт-карт eToken PRO подключаются к штатным USB-разъемам компьютера. Идентификаторы iButton подключаются к контактному устройству (считывателю) для iButton.

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

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

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

Для всех идентификаторов eToken PRO и eToken PRO (Java) 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 ком-

плекса должен установить PIN-код, отличный от PIN-кода по умолчанию. В этом случае после предъявления eToken PRO/PRO (Java) 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/PRO (Java), 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 НСД 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 НСД 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 ПАК "Соболь".

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 программных и аппаратных ресурсов компьютера до загрузки его операционной системы. Контроль целостности — это функция, которая предназначена для слежения за изменением параметров заданных ресурсов.

Используемый в комплексе "Соболь" механизм контроля целостности позволяет контролировать следующие объекты:

Табл. 2. Объекты контроля целостности ПАК "Соболь"

Объект КЦ	Пояснение
Файлы	Комплекс "Соболь" позволяет контролировать неизменность одиночных файлов, групп файлов, каталогов и подкаталогов, расположенных на жестком диске компьютера
Секторы жесткого диска	В комплексе реализован контроль целостности служебных областей жесткого диска (Master Boot Record, NTFS Boot Sector и др.)
Элементы системного реестра	Комплекс "Соболь" позволяет контролировать следующие элементы (объекты) системного реестра ОС Windows: <ul style="list-style-type: none"> • ключи реестра; • параметры (переменные)
PCI-устройства	Контроль целостности PCI-устройств заключается в контроле устройств, использующих шины стандарта PCI, PCI-X, PCI Express, Mini PCI Express, с установленными в системе соответствующими драйверами. В ПАК "Соболь" реализованы три режима контроля: <ul style="list-style-type: none"> • упрощенный — заключается в контроле наличия/отсутствия PCI-устройства; • стандартный — контролируется стандартное 256-байтное конфигурационное адресное пространство, выделяемое каждому PCI-устройству; • расширенный — контролируется стандартное 256-байтное и расширенное 4-килобайтное конфигурационное адресное пространство, выделяемое каждому PCI-устройству
SMBIOS	В комплексе реализован контроль целостности структур SMBIOS, содержащих информацию о компонентах системной платы (сведения о производителе, системной плате, процессоре, системных слотах, памяти, BIOS и др.)
ACPI	Комплекс "Соболь" позволяет контролировать неизменность содержащего таблиц ACPI. В таблицах содержатся данные об аппаратном и программном интерфейсах, обеспечивающих учет и конфигурирование компонентов системной платы компьютера
Оперативная память	Контроль целостности оперативной памяти компьютера заключается в контроле неизменности распределения адресного пространства памяти
Журнал транзакций	Контроль целостности заключается в проверке сведений о незавершенных операциях в журнале транзакций NTFS, EXT3, EXT4. Предшествует процедуре контроля целостности файлов и секторов

Реализация контроля целостности в комплексе "Соболь" основывается на вычислении некоторых контрольных значений проверяемых объектов и их сравнении с ранее рассчитанными для каждого из этих объектов эталонными значениями.

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

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.

Пояснение. Шаблоны КЦ представляют собой служебные файлы, содержащие имена контролируемых объектов и их контрольные суммы:

- Bootfile.nam, Bootfile.chk — шаблоны КЦ файлов;
- Bootsect.nam, Bootsect.chk — шаблоны КЦ секторов;
- Bootreg.nam, Bootreg.chk — шаблоны КЦ элементов системного реестра;
- Bootpci.nam, Bootpci.chk — шаблоны КЦ PCI-устройств;
- Bootsmbs.nam, Bootsmbs.chk — шаблоны КЦ структур SMBIOS.

Исходные шаблоны создаются во время установки программы управления шаблонами.

Эталонные значения КЦ таблиц ACPI и адресного пространства оперативной памяти формируются в процессе инициализации комплекса и хранятся в защищенной памяти платы ПАК.

Проверка контрольных сумм контролируемых объектов осуществляется при входе администратора и 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. При обнаружении нарушений целостности файлов-шаблонов или контролируемых объектов в журнале событий регистрируется событие "Ошибка при контроле целостности".

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 мягком — вход пользователя разрешается.

Механизм сторожевого таймера

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

Блокировка доступа к компьютеру осуществляется двумя способами:

- путем принудительной автоматической перезагрузки компьютера с помощью стандартной процедуры Reset. Для блокировки питания используется входящий в комплект поставки соединительный кабель для механизма сторожевого таймера;
- либо принудительным автоматическим выключением питания (в случае отсутствия в защищаемом компьютере разъема Reset). Для блокировки питания компьютера используется специальное устройство (см. [Рис. 1](#)), поставляемое по желанию заказчика. Устройство предназначено для использования в компьютерах формфактора ATX.

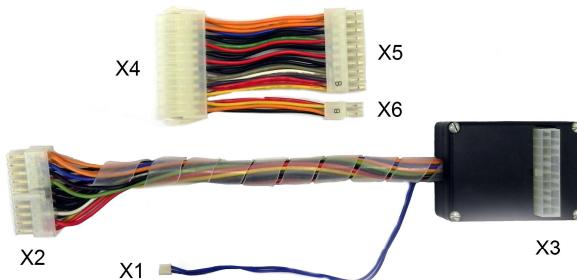


Рис. 1. Устройство блокировки питания

Для использования механизма сторожевого таймера необходимо правильно подключить к плате комплекса "Соболь" соединительный кабель или устройство блокировки питания (см. п. 3 процедуры на стр. [21](#) для PCI-E/PCI и п. 4 на стр. [23](#) для Mini PCI-E/Mini PCI-E Half). Без подключения кабеля или устройства механизм сторожевого таймера не функционирует.

Рекомендуемое время ожидания сторожевого таймера определяется автоматически на этапе инициализации комплекса. Администратор может корректировать значение времени ожидания в режимах инициализации и эксплуатации комплекса. Максимальное значение параметра для платы PCI/PCI-E составляет 512 секунд, для платы Mini PCI-E/Mini PCI-E Half — до 65534 секунд.



Во избежание потери 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.

Требования к оборудованию и программному обеспечению

Комплекс "Соболь" устанавливается на компьютеры, оснащенные 32- или 64-разрядными процессорами. Для подключения платы комплекса у компьютера должен быть свободный разъем системной шины либо стандарта PCI-E версии 1.0a и выше, либо стандарта PCI версий 2.0/2.1/2.2/2.3 с напряжением питания 5 В/3,3 В, либо стандарта Mini PCI-E.

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 КЦ функционирует в среде следующих ОС с файловыми системами FAT16, FAT32, NTFS, UFS, UFS2, EXT2, EXT3, EXT4:

Семейство ОС	Плата PCI-E, PCI	Плата Mini PCI-E	Плата Mini PCI-E Half
MS Windows	<ul style="list-style-type: none"> • Windows 8/8.1; • Windows 7/7 x64 Edition; • Windows Vista/Vista x64 Edition; • Windows XP Professional/XP Professional x64 Edition; • Windows Server 2012/Server 2012 R2; • Windows Server 2008/Server 2008 x64 Edition/Server 2008 R2; • Windows Server 2003/Server 2003 x64 Edition/Server 2003 R2/Server 2003 R2 x64 Edition 		
Linux	<ul style="list-style-type: none"> • Альт Линукс СПТ 6.0.0 x86/x64; • Astra Linux Special Edition "Смоленск" 1.1/1.2/1.3 x64; • CentOS 6.2 x64; • Debian 6.0.3 x86/x64; • Mandriva ROSA Desktop2011.0 x86/x64; • Red Hat Enterprise Linux 6.0 x86/x64; • VMware vSphere ESXi 5.1 Update 1/5.1 Update 2/5.5 x64 • MCBC 3.0 x86 • ContinentOS 1.0 x86/x64 	<ul style="list-style-type: none"> • Astra Linux Special Edition "Смоленск" 1.3 x64; • VMware vSphere ESXi 5.1 Update 1/5.1 Update 2/5.5 x64 	
Unix	<ul style="list-style-type: none"> • FreeBSD 6.2/6.3/7.2/8.2 		



Программные компоненты механизма КЦ, обеспечивающие управление шаблонами КЦ в среде ОС FreeBSD, ContinentOS 1.0, в комплект поставки ПАК "Соболь" не включаются.

Работа механизма КЦ характеризуется следующими особенностями:

- при задании пути к файлам-шаблонам КЦ для FAT не поддерживается возможность задания пути в длинном виде;
- не поддерживается контроль целостности файлов на дисках, размеченных как GUID Partition Table;
- не поддерживается контроль целостности ресурсов на более чем 32 логических дисках;
- не поддерживается возможность контроля целостности секторов, расположенных на диске за пределами 2 ТБ;
- не поддерживается контроль целостности файлов, расположенных на динамических дисках.



При использовании механизма контроля целостности:

- 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 ОС семейства Windows (volume set и stripe set), не поддерживается.

Системная плата компьютера должна иметь хотя бы один из разъемов:

- для подачи сигнала системного сброса Reset;
- для подключения устройства блокировки питания;

и обеспечивать возможность подключения кабеля механизма сторожевого таймера или устройства блокировки питания, входящих в комплект поставки ПАК.

При подаче сигнала сброса Reset на разъем системной платы компьютера, к которому подключен кабель механизма сторожевого таймера, должна обеспечиваться перезагрузка компьютера. При подаче сигнала на разъем питания системной платы компьютера, к которому подключено устройство блокировки питания, должно обеспечиваться выключение питания компьютера. Возможность влияния на этот механизм со стороны программных и аппаратных средств компьютера (например, путем отключения из BIOS Setup) должна быть исключена.

Разъем питания системной платы компьютера должен отвечать требованиям спецификации ATX и иметь 20 или 24 контакта, блок питания должен удовлетворять требованиям спецификации ATX.

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 с АПКШ "Континент", СЗИ Secret Net, СЗИ vGate-S R2, СЗИ vGate R2, СЗИ Security Studio Honeypot Manager, СКЗИ "Континент-АП" и СКЗИ "КриптоПро CSP".

Работа комплекса "Соболь" в составе СЗИ семейства Secret Net или АПКШ "Континент" осуществляется в режиме совместного использования. Ограничения этого режима рассматриваются на стр. [92](#).

Эксплуатационные ограничения

Представленные ниже требования относятся к комплексу "Соболь", имеющему сертификат ФСБ России.

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 средствам 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 соединительного кабеля или устройства блокировки питания механизма сторожевого таймера, входящих 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 **16**.

- "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/EXT3/EXT4);
- "Контроль элементов реестра" — "Да";
- "Число попыток тестирования ДСЧ" — "1";
- "Предельное число неудачных входов пользователя" — не более "10";
- "Ограничение времени на вход в систему (мин.)" — 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 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/PRO (Java), Rutoken/Rutoken RF;
- 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 1 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 (с помощью 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.** Регламентные работы по техническому обслуживанию комплекса и компьютера должны проводиться не реже 1 раза в год.
- 18.** 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.
- 19.** Компьютер, в котором установлен комплекс "Соболь", должен быть аттестован в качестве объекта ЭВТ 2-й или 3-й 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 от 30.08.2002 г. № 282, и иметь соответствующее Предписание на эксплуатацию.
При этом на расстоянии не менее 5 метров от ЭВТ 2-й или 3-й 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 (см. ниже);
- установка платы (см. стр. 20, 22);
- инициализация комплекса (см. стр. 25);
- подготовка комплекса к эксплуатации (см. стр. 33).



Порядок установки программного обеспечения комплекса "Соболь" в семействе ОС Linux рассмотрен в документе [2].



Установка программного обеспечения

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

Для 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.

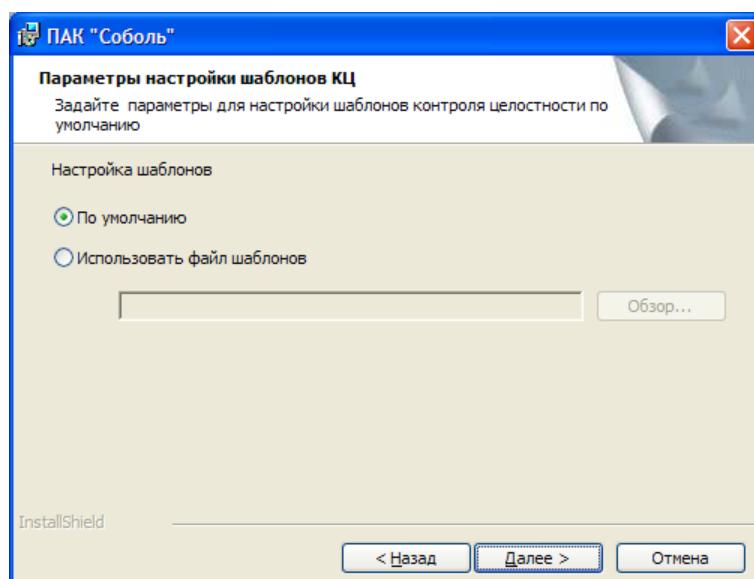
На экране появится диалог с текстом лицензионного соглашения.

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 развертыванию программного обеспечения на жестком диске 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, 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 автоматического запуска программы управления шаблонами КЦ после установки ПО комплекса отметьте поле "Запуск программы управления шаблонами КЦ".

7. Нажмите кнопку "Готово".

Обычно перезагрузка компьютера после завершения установки не требуется.

Установка плат PCI-E, PCI

Для установки платы PCI-E/PCI:

1. Выключите компьютер, откройте корпус системного блока.
2. Снимите перемычку, установленную на разъем J0 платы (см. Рис. 2, Рис. 3).

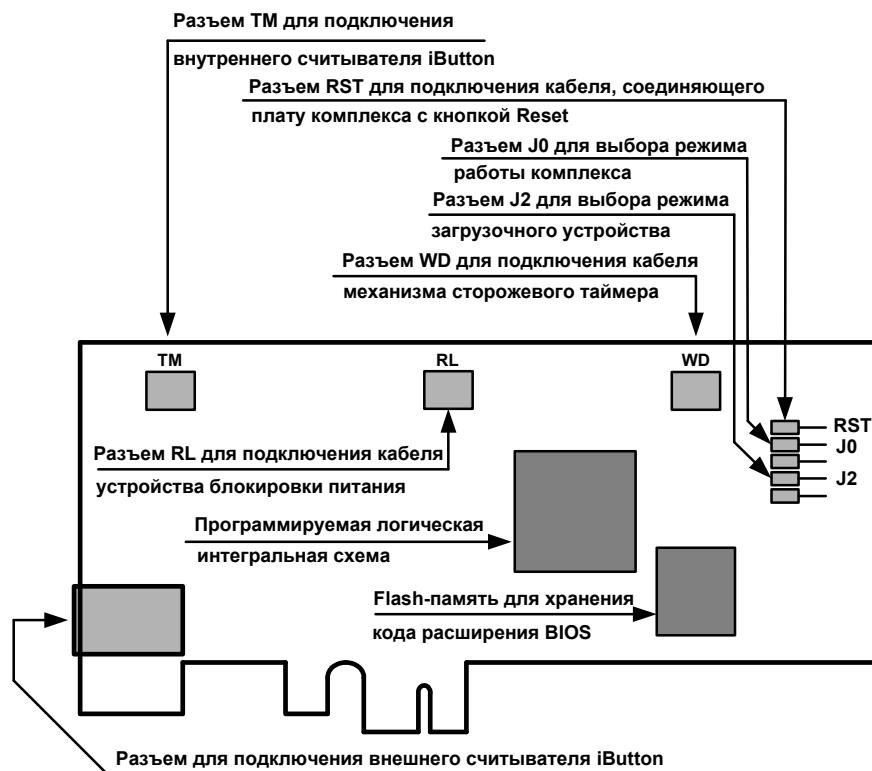


Рис. 2. Расположение разъемов на плате PCI-E

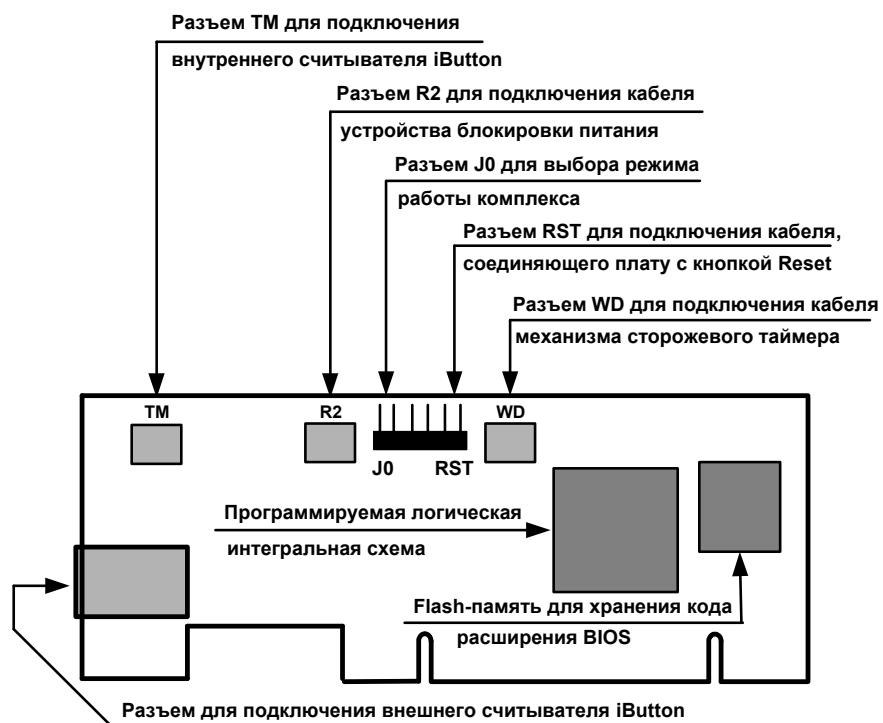


Рис. 3. Расположение разъемов на плате PCI

- 3.** Для использования механизма сторожевого таймера:
 - в режиме автоматической перезагрузки компьютера:
 - 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](#));
 - 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;
 - в режиме автоматического выключения питания компьютера:
 - вариант 24-контактного разъема ATX:
 - отключите стандартный кабель питания от разъема ATX, расположенного на материнской плате;
 - подключите стандартный кабель питания к разъему X4 устройства блокировки питания (см. [Рис. 1](#));
 - подключите разъем X5 к разъему X3;
 - подключите разъемы X2 и X6 к разъему питания ATX, расположенному на материнской плате;
 - подключите разъем X1 к разъему RL платы PCI-E (см. [Рис. 2](#)) или R2 платы PCI (см. [Рис. 3](#));
 - вариант 20-контактного разъема ATX:
 - отключите стандартный кабель питания от разъема ATX, расположенного на материнской плате;
 - подключите стандартный кабель питания к разъему X3 устройства блокировки питания (см. [Рис. 1](#));
 - подключите разъем X2 к разъему питания ATX, расположенному на материнской плате;
 - подключите разъем X1 к разъему RL платы PCI-E (см. [Рис. 2](#)) или R2 платы PCI (см. [Рис. 3](#)).
- 4.** Выберите свободный слот системной шины PCI-E/PCI и установите в него соответствующую плату комплекса "Соболь".
- 5.** 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.
- 6.** Закройте корпус системного блока.
- 7.** При необходимости подключите USB-считыватель смарт-карт Athena ASE-Drive IIIe USB V2/V3.

Установка плат Mini PCI-E, Mini PCI-E Half

В зависимости от формфактора защищаемого компьютера платы комплекса Mini PCI-E, Mini PCI-E Half (см. [Рис. 4](#), [Рис. 6](#)) могут устанавливаться автономно или с адаптером (см. [Рис. 5](#), [Рис. 7](#)) совместно с кронштейном Standard/Low Profile.

Для установки платы Mini PCI-E совместно с адаптером:

1. Выключите компьютер, откройте корпус компьютера.
2. Установите переключатель платы SW 1 в положение OFF (см. [Рис. 4](#)).
3. Подключите штекер TM кабеля адаптера (см. [Рис. 5](#)) к разъему TM платы Mini PCI-E (см. [Рис. 4](#)).

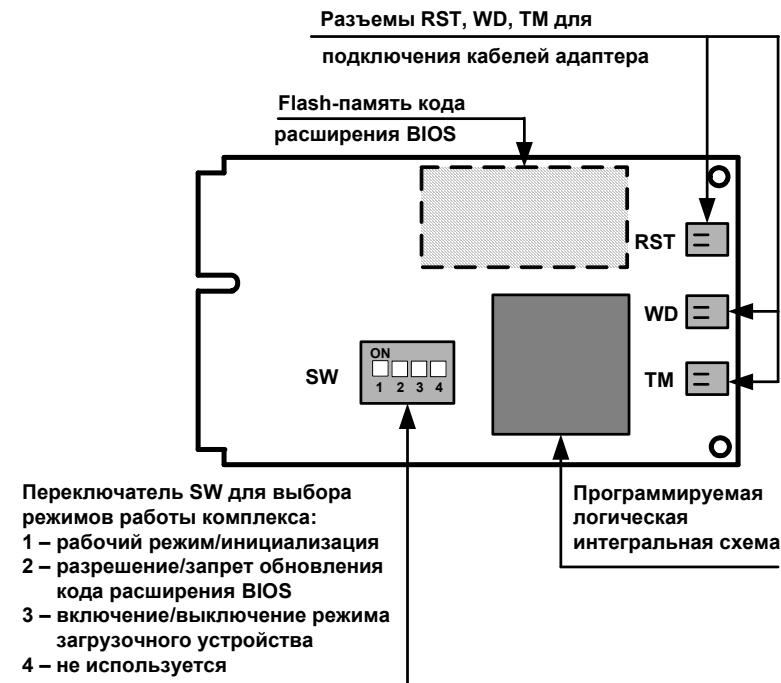


Рис. 4. Расположение разъемов на плате Mini PCI-E

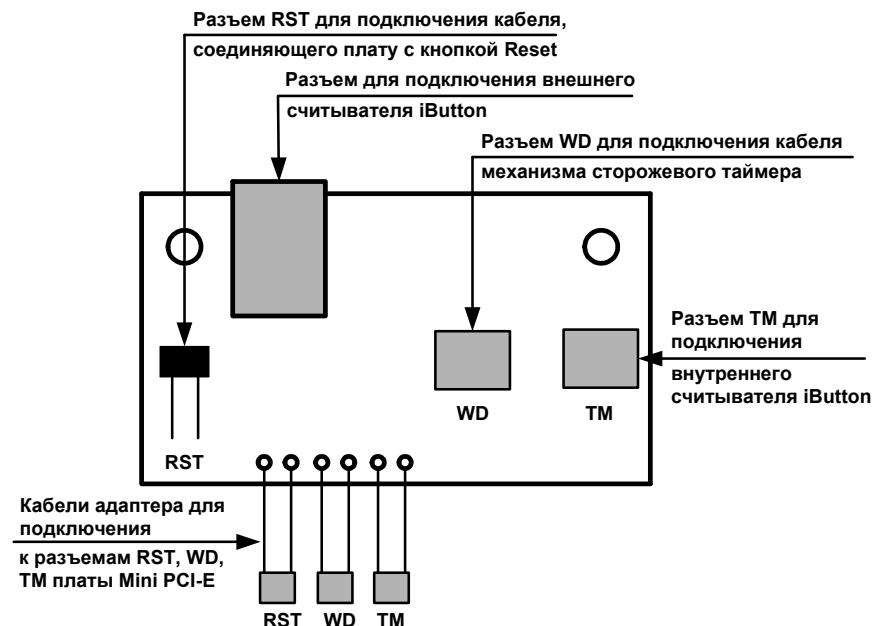


Рис. 5. Расположение разъемов на адаптере для платы Mini PCI-E

4. Для использования механизма сторожевого таймера в режиме автоматической перезагрузки компьютера:
 - подключите штекеры RST, WD кабелей адаптера к соответствующим разъемам RST, WD платы Mini PCI-E;
 - отключите штекер стандартного кабеля кнопки "Reset" от разъема Reset, расположенного на материнской плате;
 - подключите штекер стандартного кабеля кнопки "Reset" к разъему RST адаптера;
 - подключите штекер кабеля механизма сторожевого таймера, входящего в комплект поставки, к разъему WD адаптера. Затем подключите другой штекер этого кабеля к разъему Reset материнской платы.
5. Выберите свободный слот системной шины Mini PCI-E и установите в него плату комплекса "Соболь".
6. Выберите свободный слот системного блока защищаемого компьютера и установите в него адаптер.
7. При необходимости подключите к адаптеру считыватель iButton:
 - при использовании внешнего считывателя подключите его штекер к соответствующему разъему адаптера (см. [Рис. 5](#));
 - при использовании внутреннего считывателя — к разъему TM адаптера.
8. Закройте корпус компьютера.
9. При необходимости подключите USB-считыватель смарт-карт Athena ASE-Drive IIIe USB V2/V3.

Для установки платы Mini PCI-E Half совместно с адаптером:

1. Выключите компьютер, откройте корпус компьютера.
2. Установите переключатель платы SW 1 в положение OFF (см. [Рис. 6](#)).
3. Подключите кабель адаптера к соответствующим разъемам платы Mini PCI-E Half (см. [Рис. 6](#)) и адаптера (см. [Рис. 7](#)).
4. Для использования механизма сторожевого таймера в режиме автоматической перезагрузки компьютера:
 - отключите штекер стандартного кабеля кнопки "Reset" от разъема Reset, расположенного на материнской плате;
 - подключите штекер стандартного кабеля кнопки "Reset" к разъему RST адаптера;
 - подключите штекер кабеля механизма сторожевого таймера, входящего в комплект поставки, к разъему WD адаптера. Затем подключите другой штекер этого кабеля к разъему Reset материнской платы.

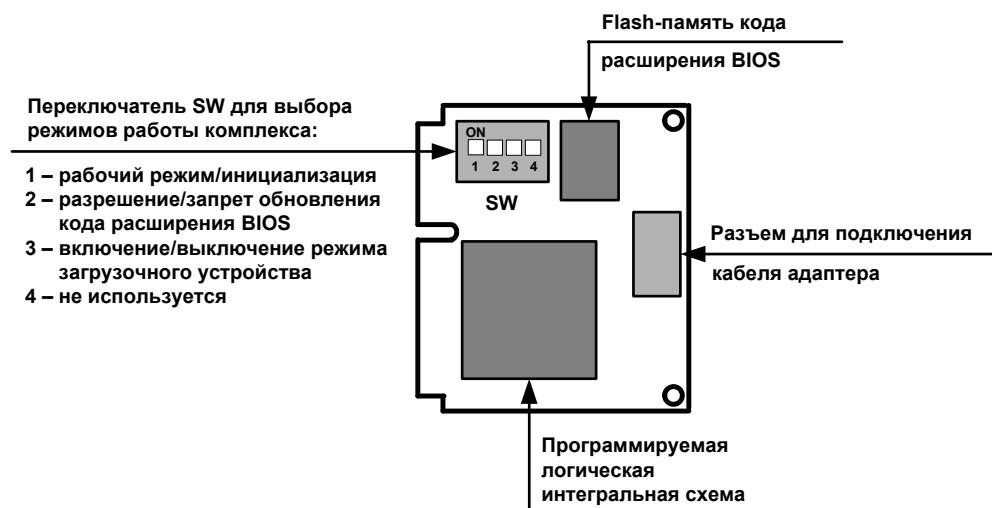
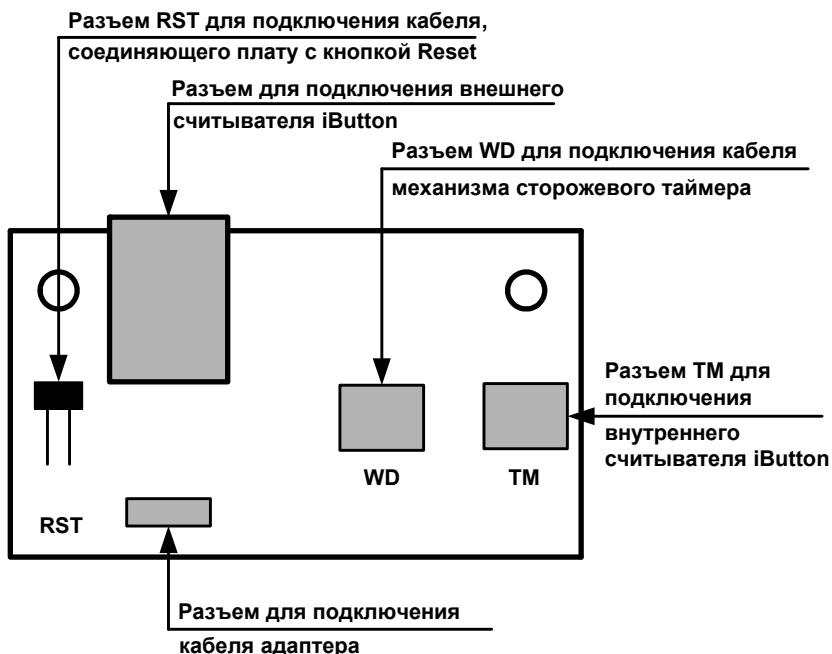


Рис. 6. Расположение разъемов на плате Mini PCI-E Half

**Рис. 7. Расположение разъемов на адаптере для платы Mini PCI-E Half**

5. Выберите свободный слот системной шины Mini PCI-E и установите в него плату комплекса "Соболь".
6. Выберите свободный слот системного блока защищаемого компьютера и установите в него адаптер.
7. При необходимости подключите к адаптеру считыватель iButton:
 - при использовании внешнего считывателя подключите его штекер к соответствующему разъему адаптера (см. [Рис. 7](#));
 - при использовании внутреннего считывателя — к разъему TM адаптера.
8. Закройте корпус компьютера.
9. При необходимости подключите USB-считыватель смарт-карт Athena ASE-Drive IIIe USB V2/V3.

Для автономной установки платы Mini PCI-E/Mini PCI-E Half:

1. Выключите компьютер, откройте корпус компьютера.
2. Установите переключатель платы SW 1 в положение OFF (см. [Рис. 4](#), [Рис. 6](#)).
3. Выберите свободный слот системной шины Mini PCI-E и установите в него плату комплекса "Соболь". Закройте корпус компьютера.
4. Закройте корпус компьютера.
5. При необходимости подключите USB-считыватель смарт-карт Athena ASE-Drive IIIe USB V2/V3.

Инициализация комплекса

Инициализация комплекса "Соболь" выполняется в следующем порядке:

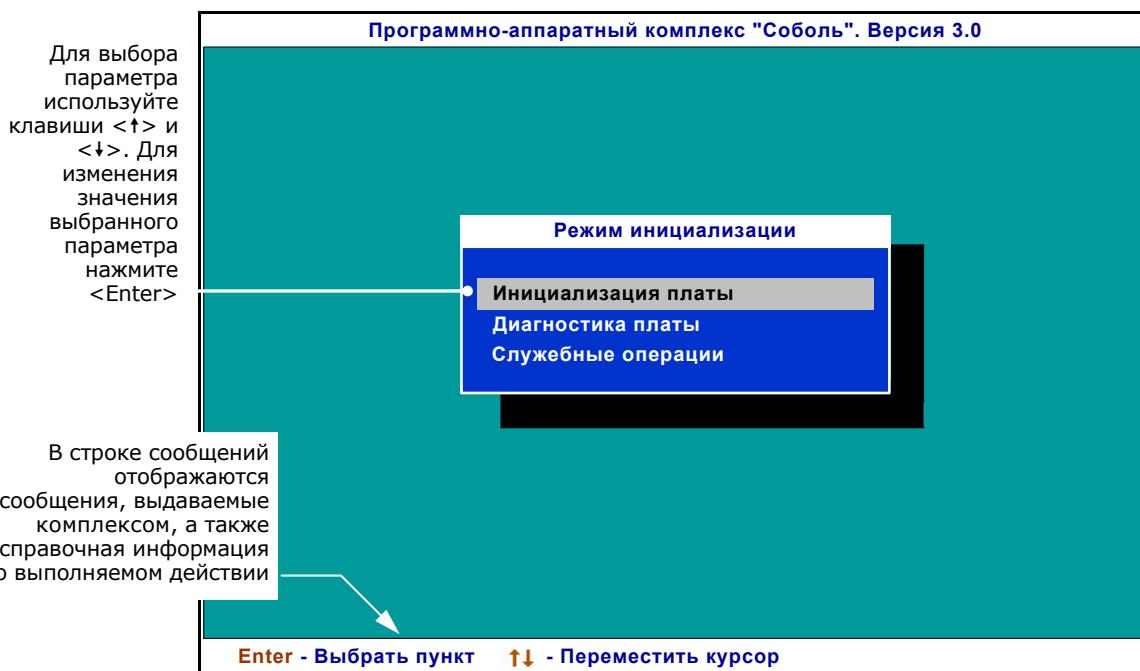
1. Запуск процедуры инициализации (см. ниже)
2. Настройка общих параметров комплекса (см. стр. 26)
3. Настройка контроля целостности (см. стр. 28)
4. Регистрация администратора комплекса (см. стр. 29)
5. Расчет контрольных сумм (см. стр. 32)

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

Шаг 1. Запуск процедуры инициализации

1. Включите питание компьютера.

Управление передается ПАК "Соболь". На экране появится окно:



Если после включения питания компьютера управление не передается ПАК "Соболь", в BIOS Setup разрешите загрузку операционной системы с модулей расширения BIOS сетевых плат.

Если управление по-прежнему не передается модулю расширения BIOS комплекса, используйте ПАК "Соболь" (на базе платы PCI-E/Mini PCI-E/Mini PCI-E Half) в режиме загрузочного устройства. Для этого:

- установите: на плате PCI-E – перемычку на разъем J2 (см. Рис. 2), на плате Mini PCI-E/Mini PCI-E Half – переключатель SW 3 в положение ON (см. Рис. 4, Рис. 6);
- обязательно подключите механизм сторожевого таймера (см. п. 3 процедуры на стр. 21 для PCI-E/PCI и п. 4 на стр. 23 для Mini PCI-E/Mini PCI-E Half);
- в BIOS Setup определите плату ПАК "Соболь" первым загрузочным устройством.

В этом случае загрузка операционной системы осуществляется только с жесткого диска при условии его наличия в меню загрузки BIOS Setup.

При использовании ПАК "Соболь" на базе платы PCI обратитесь к разработчику комплекса.

В центре окна располагается меню "Режим инициализации".

Совет. Прежде чем приступить к инициализации, рекомендуется проверить работоспособность комплекса "Соболь". Для этого в меню "Режим инициализации" выберите команду "Диагностика платы" и нажмите <Enter>. В появившемся на экране меню выберите команду "Выполнить все тесты" и нажмите <Enter>. После успешного завершения всех тестовых процедур нажмите клавишу <Esc>. Подробные инструкции по выполнению команд "Диагностика платы" содержатся на стр. 55.

Перед инициализацией комплекса также предоставляется возможность отформатировать персональный идентификатор iButton. Для этого в меню "Служебные операции" выберите команду "Форматирование идентификатора". Подробные инструкции по ее выполнению содержатся на стр. 60.

2. Выберите в меню "Режим инициализации" 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.)	-	20
Период тестирования сторожевого таймера (дней)	-	0
Поддержка USB-идентификаторов	-	Нет

Рис. 8. Диалог настройки общих параметров (режим инициализации)

Назначение общих параметров разъясняется в Табл. 3, 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. 44) 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 <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 <Enter>;

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

- параметр "Поддержка USB-идентификаторов" может принимать два значения — "Нет" или "2.0" (см. стр. 27).
- 2. Выполнив настройку параметров, нажмите <Esc> для сохранения изменений и перехода к настройке контроля целостности.

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

Число попыток тестирования ДСЧ
Определяет число попыток тестирования правильности работы ДСЧ комплекса, выполняемого при входе в систему. 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
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, "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, "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 блокировка 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 значение параметра для платы PCI/PCI-E от 4 до 512 секунд с дискретностью 2 секунды (4, 6, 8, 10 и т. д.), для платы Mini PCI-E/Mini PCI-E Half от 4 до 65534 секунд с дискретностью 1 секунда.
Для использования данного механизма необходимо правильно подключить к плате комплекса "Соболь" кабель/устройство блокировки питания механизма сторожевого таймера. Если кабель/устройство не подключены — механизм сторожевого таймера не функционирует
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
Определяет типы используемых идентификаторов. Параметр может принимать два значения: "Нет" — вход в систему осуществляется только с помощью идентификаторов iButton, "2.0" — с помощью идентификаторов iButton и USB-идентификаторов любого типа, поддерживаемых ПАК "Соболь" (см. Табл. 1).
Выбор значения "2.0" обеспечивает совместимость комплекса с USB-контроллерами EHCI, UHCI, OHCI, а также с USB-разветвителями (хабами)

Шаг 3. Настройка контроля целостности

На экране появится следующий диалог:

Контроль целостности		
Каталог с шаблонами КЦ	-	C:\SOBOL
Контроль файлов и секторов	-	Да
Контроль журнала транзакций	-	Нет
Контроль элементов реестра	-	Да
Контроль PCI-устройств	-	Упрощенный
Контроль ACPI	-	Нет
Контроль SMBIOS	-	Да
Контроль оперативной памяти	-	Нет

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 <Enter>;
 - значение изменится на противоположное ("Да" или "Нет");
 - параметр "Контроль PCI-устройств" может принимать четыре значения — "Нет"/"Упрощенный"/"Стандартный"/"Расширенный".



Настройка контроля целостности PCI-устройств в режимах "Стандартный" и "Расширенный" должна проводиться опытным администратором.



Файлы-шаблоны КЦ хранятся в каталоге, имя и местоположение которого указываются в программе управления шаблонами КЦ: в строке "Путь к шаблонам контроля целостности" окна "О программе" для ОС Windows, в строке "BIOS платы" окна "Информация" для ОС Linux. Для определения пути к файлам-шаблонам КЦ при работе в режиме командной строки (для ОС Linux) выполните команду `scheck --ls-path`.

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

При попытке изменить значение параметра "Каталог с шаблонами КЦ" для указания точного пути к каталогу с файлами-шаблонами на экране появится диалоговое окно. Введите путь к заданному каталогу и нажмите <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 "prog~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 шаблонов КЦ параметры "Контроль файлов и секторов", "Контроль элементов реестра", "Контроль PCI-устройств", "Контроль SMBIOS" 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 <Esc> для продолжения инициализации комплекса.

Начнется автоматическое 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 и присваивается персональный идентификатор. Процедура регистрации может выполняться в одном из двух вариантов: первичная (см. ниже) и повторная (см. стр. 31).

Первичная регистрация администратора. При ее выполнении в идентификатор администратора записывается новая служебная информация о регистрации. Если идентификатор содержит служебные данные, например, записанные 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 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/Rutoken RF/iKey 2032/eToken PRO/eToken PRO (Java), ранее не использовавшиеся в комплексе "Соболь" и имеющие PIN-коды, отличные от PIN-кодов по умолчанию (для Rutoken/Rutoken RF — **12345678**, для iKey 2032 — **default SO password**, для eToken PRO/PRO (Java) — **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 USB-идентификатор eToken PRO/PRO (Java), то на экране появится окно с сообщением об отсутствии в нем файловой системы. Выполните инициализацию предъявленного USB-ключа 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 <Enter>.

На экране появится диалог для ввода пароля администратора.



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. 27), и не может превышать 16 символов. Если значение указанного параметра равно "0", можно назначить администратору пустой пароль. Для этого нажмите <Enter>, оставив поле ввода пароля пустым.

2. Введите с клавиатуры пароль администратора и нажмите <Enter>. На экране появится диалог для подтверждения пароля администратора.
3. Повторно введите тот же пароль и нажмите <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:

Предъявите персональный идентификатор . . .

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 <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 <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:

**Структура данного персонального идентификатора нарушена.
Персональный идентификатор необходимо переформатировать.
Произвести форматирование?**

Да **Нет**

или

**Не хватает свободного места для добавления новой записи.
Персональный идентификатор необходимо переформатировать.
Произвести форматирование?**

Да **Нет**



При форматировании идентификатора iButton вся информация, содержащаяся в его памяти, будет полностью утеряна без возможности восстановления. При форматировании USB-ключей и смарт-карт 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 <Enter>.

На экране появится повторный запрос:

**Вся информация на идентификаторе будет уничтожена!
Вы уверены, что собираетесь форматировать идентификатор?**

Да Нет

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

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

Создать резервную копию идентификатора администратора?

Да Нет

Если вы уверены в том, что создавать резервные копии не требуется, выберите вариант "Нет" и нажмите <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 потерян.

- Выберите вариант "Да" и нажмите <Enter>.

На экране появится запрос персонального идентификатора.

- 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.

- 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 <Enter>.

Перейдите к выполнению заключительного этапа инициализации — расчету контрольных сумм.

Для повторной регистрации администратора:

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

На экране появится диалог для ввода пароля администратора.

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

На экране появится запрос на предъявление идентификатора.

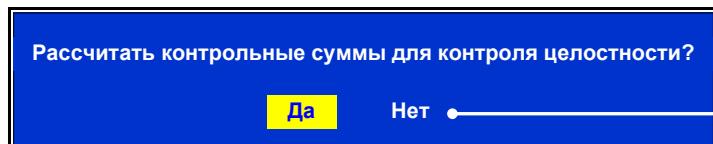
- Предъявите персональный идентификатор, присвоенный администратору при его первичной регистрации на другом комплексе "Соболь".

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

Если параметрам "Контроль файлов и секторов"/"Контроль элементов реестра"/"Контроль PCI-устройств"/"Контроль SMBIOS" присвоено значение "Да" (см. стр. 28), на экране появится запрос, предлагающий рассчитать контрольные суммы:



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

- Выберите вариант "Да" и нажмите <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 объектов контроля, заданных шаблонами КЦ, по окончании процедуры расчета на экране появятся следующие запросы:

**Расчет контрольных сумм файлов и секторов завершился с ошибкой.
Запретить контроль целостности файлов и секторов?**

Да Нет

**Расчет контрольных сумм элементов реестра завершился с ошибкой.
Запретить контроль целостности элементов реестра?**

Да Нет

**Расчет контрольных сумм параметров конфигурации завершился с ошибкой.
Запретить контроль целостности параметров конфигурации?**

Да Нет

Выберите вариант продолжения процедуры и нажмите <Enter>:

- "Да" — для отключения контроля целостности, выполняемого при входе пользователей в систему.

Пояснение. В этом случае следует выполнить корректировку шаблонов КЦ (см. стр. 64), рассчитать эталонные значения контрольных сумм (см. стр. 78) и включить контроль целостности (см. стр. 28).

- "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. 64), затем повторно рассчитайте эталонные значения контрольных сумм (см. стр. 78).

По окончании инициализации на экране появится сообщение:

Инициализация платы завершена. После выключения питания компьютера установите перемычку, переводящую плату в рабочий режим.

Ok

2. Нажмите <Enter>.

Компьютер выключится автоматически.

Если выключение не произойдет, 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 (плата PCI-E/PCI):

- 1.** Выключите компьютер, откройте 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.** Извлеките плату комплекса "Соболь" из разъема шины PCI-E/PCI.
- 4.** Установите перемычку на разъем J0 платы (см. [Рис. 2](#), [Рис. 3](#)).

Внимание! Для эксплуатации ПАК "Соболь" на базе платы PCI-E в режиме загрузочного устройства (см. стр. [25](#)) также должна быть установлена перемычка на разъем J2.

- 5.** Установите плату комплекса "Соболь" в разъем системной шины PCI-E/PCI.
- 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.
- 8.** При необходимости подключите USB-считыватель смарт-карт Athena ASE-Drive IIIe USB V2/V3.

Выполнив все указанные действия, включите компьютер и перейдите к настройке комплекса "Соболь" (см. стр. [37](#)).

Для подготовки к эксплуатации (плата Mini PCI-E/Mini PCI-E Half):

- 1.** Выключите компьютер, откройте корпус компьютера.
- 2.** Переключите плату комплекса "Соболь" в рабочий режим. Для этого установите переключатель SW 1 в положение ON (см. [Рис. 4](#), [Рис. 6](#)).

Внимание! Для эксплуатации ПАК "Соболь" на базе платы Mini PCI-E/Mini PCI-E Half в режиме загрузочного устройства (см. стр. [25](#)) переключатель SW 3 платы также должен быть установлен в положение ON.

- 3.** Закройте корпус компьютера.
- 4.** При необходимости подключите USB-считыватель смарт-карт Athena ASE-Drive IIIe USB V2/V3.

Выполнив все указанные действия, включите компьютер и перейдите к настройке комплекса "Соболь" (см. стр. [37](#)).



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 Linux рассмотрен в документе [[2](#)].

Для обновления программного обеспечения:

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

На экране появится окно с предложением продолжить обновление ПО комплекса "Соболь".

2. Нажмите кнопку "Да" для продолжения обновления.

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

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

Программа установки приступит к обновлению программного обеспечения комплекса. Ход процесса копирования отображается на экране в виде индикатора прогресса.

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

4. Нажмите кнопку "Готово".

Исправление программного обеспечения



Порядок исправления программного обеспечения комплекса "Соболь" в среде ОС Linux рассмотрен в документе [[2](#)].

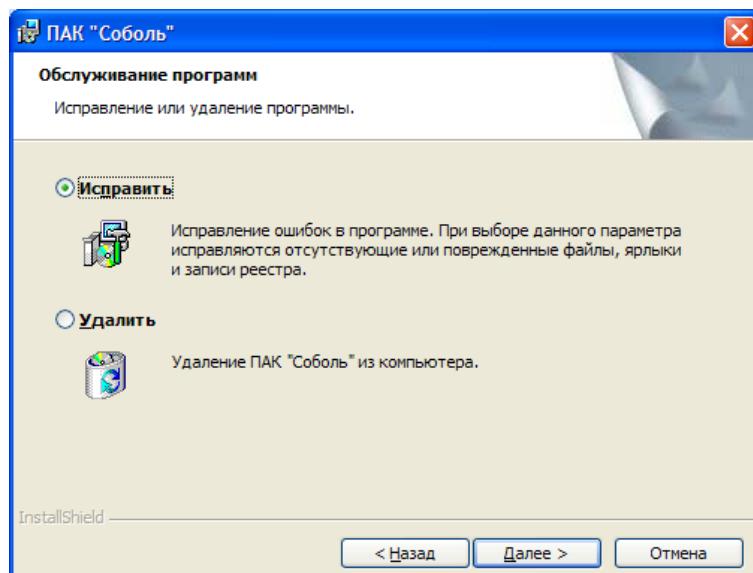
Для исправления программного обеспечения:

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 "Далее >".

На экране появится диалог "Обслуживание программ":



3. Отметьте поле "Исправить" и нажмите "Далее >".

На экране появится окно "Исправление ПАК "Соболь"".

4. Нажмите "Установить".

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

5. Нажмите "Готово".

Удаление комплекса

Следует обратить внимание на то, что после удаления ПАК "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 ПАК, исключающие возможность бесконтрольного доступа к ней. Для удаления служебной информации из памяти комплекса используйте процедуру инициализации в режиме первичной регистрации администратора (см. стр. 29).

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 Linux рассмотрен в документе [2].

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.

После завершения подготовительных действий на экране появится стартовый диалог программы установки.

2. Нажмите "Далее >".

На экране появится диалог "Обслуживание программ".

3. Отметьте поле "Удалить" и нажмите "Далее >".

На экране появится окно "Удаление ПАК "Соболь".

4. Нажмите "Удалить".

После успешного выполнения процедуры удаления на экране появится завершающий диалог программы установки.

5. Нажмите "Готово".

Изъятие платы комплекса из компьютера



Если после удаления программного обеспечения плата комплекса "Соболь" не извлечена из компьютера, то при каждой загрузке ОС семейства Windows на экране возможно появление сообщения об обнаружении неизвестного устройства.

Для изъятия платы PCI-E/PCI:

1. Выключите компьютер (если он включен). Откройте корпус компьютера.

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 ТМ (см. Рис. 2, Рис. 3).

- 3.** Извлеките плату комплекса "Соболь" из разъема системной шины PCI-E/PCI.
- 4.** Если использовался механизм сторожевого таймера в режиме автоматической перезагрузки компьютера, выполните следующие действия:
 - отключите кабель, обеспечивающий работу этого механизма, от разъема WD платы комплекса "Соболь" и от разъема Reset материнской платы;
 - отключите штекер кабеля кнопки "Reset" от разъема платы RST и подключите этот штекер к разъему Reset материнской платы.
- 5.** Если использовался механизм сторожевого таймера в режиме автоматического выключения питания компьютера, выполните следующие действия:
 - вариант 24-контактного разъема ATX:
 - отключите разъем X1 устройства блокировки питания (см. [Рис. 1](#)) от разъема RL платы PCI-E или R2 платы PCI (см. [Рис. 2](#), [Рис. 3](#));
 - отключите разъемы X2 и X6 от разъема питания ATX, расположенного на материнской плате;
 - отключите разъем X5 от разъема X3;
 - отключите стандартный кабель питания ATX от разъема X4 устройства блокировки питания;
 - подключите стандартный кабель питания к разъему ATX, расположенному на материнской плате;
 - вариант 20-контактного разъема ATX:
 - отключите разъем X1 устройства блокировки питания (см. [Рис. 1](#)) от разъема RL платы PCI-E или R2 платы PCI (см. [Рис. 2](#), [Рис. 3](#));
 - отключите разъем X2 от разъема питания ATX, расположенного на материнской плате;
 - отключите стандартный кабель питания ATX от разъема X3 устройства блокировки питания;
 - подключите стандартный кабель питания к разъему ATX, расположенному на материнской плате.
- 6.** Закройте корпус системного блока.

Для изъятия адаптера и платы Mini PCI-E/Mini PCI-E Half:

- 1.** Выключите компьютер (если он включен). Откройте корпус компьютера.
- 2.** При наличии подключенного к адаптеру считывателя iButton отсоедините считыватель от адаптера:
 - при использовании внешнего считывателя отключите его штекер от соответствующего разъема адаптера (см. [Рис. 5](#), [Рис. 7](#));
 - при использовании внутреннего считывателя — от разъема TM адаптера (см. [Рис. 5](#), [Рис. 7](#)).
- 3.** Извлеките плату из разъема системной шины Mini PCI-E.
- 4.** Извлеките адаптер из слота системного блока компьютера.
- 5.** Если использовался механизм сторожевого таймера в режиме автоматической перезагрузки компьютера, выполните следующие действия:
 - отключите кабель, обеспечивающий работу этого механизма, от разъема WD адаптера и от разъема Reset материнской платы;
 - отключите штекер кабеля кнопки "Reset" от разъема адаптера RST и подключите этот штекер к разъему Reset материнской платы.
- 6.** Закройте корпус компьютера.

Для изъятия платы Mini PCI-E/Mini PCI-E Half:

- 1.** Выключите компьютер (если он включен). Откройте корпус компьютера.
- 2.** Извлеките плату из разъема системной шины Mini PCI-E.
- 3.** Закройте корпус компьютера.

Глава 3

Настройка и эксплуатация комплекса

При вводе комплекса в эксплуатацию администратору необходимо:

- настроить общие параметры комплекса (см. стр. 40);
- зарегистрировать пользователей комплекса (см. стр. 44);
- настроить параметры работы пользователей (см. стр. 48);
- настроить механизм контроля целостности (см. стр. 62).

В процессе эксплуатации комплекса администратор может:

- управлять общими параметрами комплекса (см. стр. 40);
- управлять списком пользователей и параметрами их работы (см. стр. 43);
- менять свой пароль и аутентификатор (см. стр. 51);
- менять пароли и аутентификаторы других пользователей (см. стр. 50);
- просматривать записи журнала регистрации событий (см. стр. 57);
- управлять работой механизма контроля целостности (см. стр. 62);
- осуществлять ряд служебных операций (см. стр. 59).

Общий порядок настройки

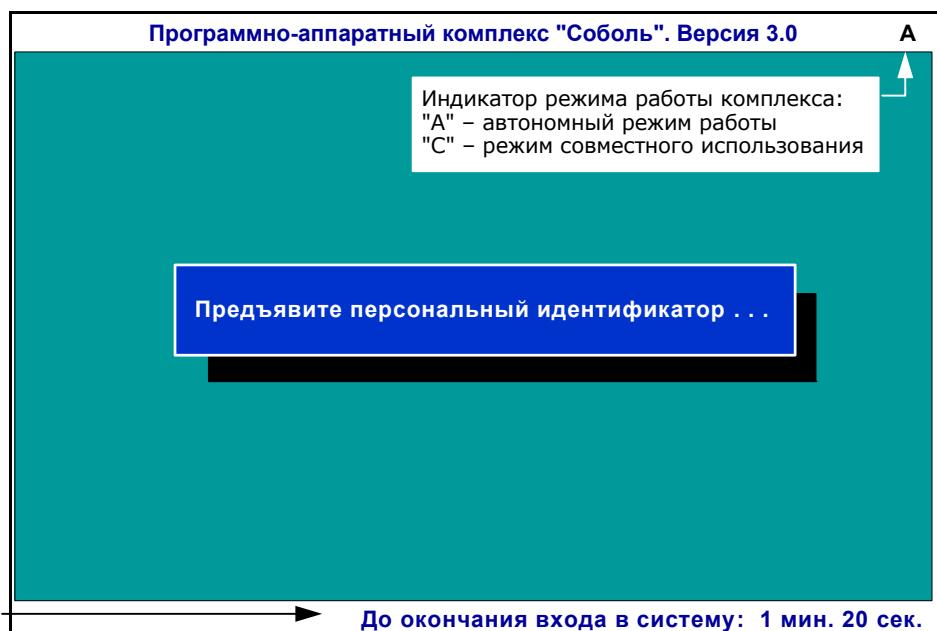
Настройка комплекса "Соболь" выполняется в следующем порядке:

1. Вход в систему администратора (см. ниже).
2. Настройка комплекса (см. стр. 39).
3. Загрузка или выключение компьютера (см. стр. 40).

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

Шаг 1. Вход в систему

1. Включите питание компьютера или выполните перезагрузку компьютера.
- На экране появится окно с запросом персонального идентификатора:



Обратите внимание на следующие особенности процедуры входа в систему.

- При включенном режиме ограничения времени, отводящегося пользователю на вход в систему (см. стр. 42, 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 <Enter>, а затем — любую клавишу.
- При включенном режиме автоматического входа в систему (см. стр. 42, 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:

Ведите пароль:

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 идентификатора.

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

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

Номер идентификатора	eToken PRO 3459-0434
Время текущего входа	15:43 01/02/14
Имя последнего пользователя	Иванов
Номер идентификатора последнего пользователя	DS1992 75-0022005E3459-07
Время входа последнего пользователя	15:20 01/02/14
Суммарное количество неудачных попыток входа	0

Окно содержит следующую информацию:

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 зарегистрированный пользователь не осуществлял вход в систему или его учетная запись после входа была 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 при надлежащий им персональный идентификатор

5. Для продолжения работы нажмите любую клавишу.

На экране появится меню администратора:

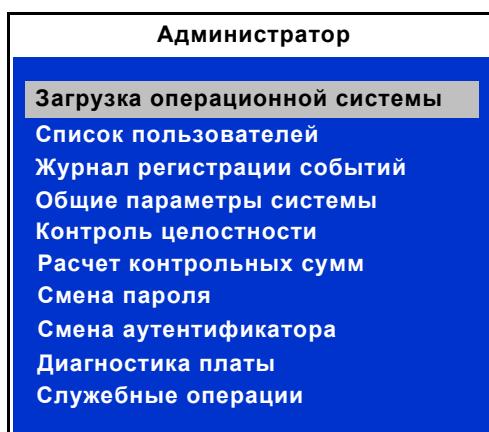


Рис. 9. Меню администратора

Пояснение. При эксплуатации комплекса в режиме совместного использования часть команд меню будет недоступна. Об особенностях настройки комплекса в этом режиме читайте на стр. 92.

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 справочную техническую информацию о комплексе и защищаемом компьютере. Для этого нажмите клавишу <F1>. На экране появится информационное окно (описание содержимого окна см. на стр. 93). Чтобы продолжить работу, нажмите любую клавишу.

Шаг 2. Настройка комплекса

- Выберите в меню администратора команду и нажмите <Enter>:
 - "Список пользователей" — команда используется для управления пользователями комплекса (см. стр. 43);
 - "Журнал регистрации событий" — для просмотра записей журнала (см. стр. 57);
 - "Общие параметры системы" — для настройки общих параметров комплекса (см. стр. 40);
 - "Контроль целостности" — для настройки параметров функционирования механизма контроля целостности (см. стр. 42);
 - "Расчет контрольных сумм" — для расчета эталонных значений контрольных сумм объектов, заданных шаблонами КЦ (см. стр. 78);
 - "Смена пароля" — для изменения пароля администратора (см. стр. 51);
 - "Смена аутентификатора" — для смены аутентификатора администратора (см. стр. 51);
 - "Диагностика платы" — для проверки работоспособности комплекса (см. стр. 55);

- "Служебные операции" — для создания резервной копии идентификатора администратора, форматирования идентификатора и реализации программной инициализации комплекса (см. стр. 59).
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 <Enter>.

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

Процесс проверки можно прервать, нажав <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. 78). Подробный список сообщений об ошибках содержится на стр. 83.

По завершении процесса проверки целостности начнется загрузка ОС.



Во время загрузки дистрибутивов MCBC 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
Звуковой сигнал при автоматическом входе в систему	- Да
Время ожидания сторожевого таймера (сек.)	- 20
Период тестирования сторожевого таймера (дней)	- 0
Поддержка USB-идентификаторов	- Нет

Рис. 10. Диалог настройки общих параметров (режим эксплуатации)

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

Для настройки параметров:

1. Выберите параметр, значение которого нужно изменить, и нажмите <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 <Enter>;
 - параметр "Поддержка USB-идентификаторов" может принимать два значения — "Нет" или "2.0" (см. стр. 27).
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, "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. 92)
Число попыток тестирования ДСЧ (см. стр. 27)
Тестирование ДСЧ для пользователя (см. стр. 27)
Параметр недоступен для управления в режиме совместного использования. В этом режиме параметру автоматически присваивается значение "Да"
Показ статистики пользователю (см. стр. 27)
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, "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. 27)
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. 49), 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. 49)
Предельное число неудачных входов пользователя (см. стр. 27)
Параметр недоступен для управления в режиме совместного использования
Время ожидания сторожевого таймера (см. стр. 27)
Период тестирования сторожевого таймера (см. стр. 27)
Поддержка USB-идентификаторов (см. стр. 27)

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 присутствовать 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".

В случае наличия в списке зарегистрированных пользователей пользователя с именем AUTOLOAD доступ к параметру блокируется при присвоении параметру "Ограничение времени на вход в систему" значения, отличного от "0".

Звуковой сигнал при автоматическом входе в систему

Позволяет включить или выключить звуковой сигнал при автоматическом входе в систему без предъявления персонального идентификатора пользователя или администратора. Параметр может принимать два значения: "Да" — звуковой сигнал включен, "Нет" — звуковой сигнал выключен.

Доступ к параметру блокируется при отсутствии в списке зарегистрированных пользователей пользователя с именем AUTOLOAD.

В случае наличия в списке зарегистрированных пользователей пользователя с именем AUTOLOAD доступ к параметру блокируется при присвоении параметру "Ограничение времени на вход в систему" значения, отличного от "0".

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, "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. 9) команды "Контроль целостности" на экране появится следующий диалог:

Контроль целостности		
Каталог с шаблонами КЦ	-	C:\SOBOL
Контроль файлов и секторов	-	Да
Контроль журнала транзакций	-	Нет
Контроль элементов реестра	-	Да
Контроль PCI-устройств	-	Упрощенный
Контроль ACPI	-	Нет
Контроль SMBIOS	-	Да
Контроль оперативной памяти	-	Нет

- 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 <Enter>;
 - значение изменится на противоположное ("Да" или "Нет");
 - параметр "Контроль PCI-устройств" может принимать четыре значения — "Нет"/"Упрощенный"/"Стандартный"/"Расширенный".



Особенности настройки параметров диалога "Контроль целостности" описываются в примечании на стр. 28.

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. 9) команды "Список пользователей" на экране появится следующий диалог:

Имя пользователя:	Иванов
Номер идентификатора:	DS1994 1A-0000005E3459-04
Время последнего входа:	15:43 01/02/14
Общее количество входов:	3
Количество неудачных попыток входа:	3
Текущий статус пользователя:	Не блокирован
Режим контроля целостности:	Жесткий
Запрет загрузки с внешних носителей:	Да
Запрет смены пароля:	Нет
Ограничение срока действия пароля:	Нет
Замена аутентификатора при смене пароля:	Нет
Иванов	Список пользователей. Если нет зарегистрированных пользователей, например, после инициализации комплекса, список пользователей будет пуст
Петров	
AUTOLOAD	

Enter—Выбрать пункт Ins—Добавить Del—Удалить Tab—Пароль Esc—Выход

Рис. 11. Окно "Зарегистрированные пользователи"

В сведениях о выбранном пользователе содержится следующая информация:

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 <Enter> при вводе пароля
Общее количество входов	Число удачных попыток входа пользователя в систему с момента его регистрации в списке пользователей



Список пользователей недоступен для управления при эксплуатации комплекса "Соболь" в режиме совместного использования (см. стр. 41, параметр "Автономный режим работы").

В этом диалоге администратор может:

- зарегистрировать нового пользователя (см. ниже);
- изменить параметры учетной записи пользователя (см. стр. 48);
- удалить учетную запись пользователя (см. стр. 50);
- сменить пароль и аутентификатор пользователя (см. стр. 50).

Выполнив все необходимые действия, нажмите <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. 47).

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/Rutoken RF/iKey 2032/eToken PRO/eToken PRO (Java), ранее не использовавшиеся в комплексе "Соболь" и имеющие PIN-коды, отличные от PIN-кодов по умолчанию (для Rutoken/Rutoken RF — **12345678**, для iKey 2032 — **default SO password.**, для eToken PRO/PRO (Java) — **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/PRO (Java), то на экране появится окно с сообщением об отсутствии в нем файловой системы. Выполните инициализацию предъявленного eToken PRO/PRO (Java) стандартными программными средствами компании — производителя идентификатора.
- При регистрации пользователя на нескольких компьютерах, оснащенных комплексами "Соболь", действуйте по 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. 11), 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. 50) и повторить процедуру регистрации.

На экране появится диалог для ввода имени пользователя:

Имя пользователя:

Имя пользователя может содержать до 40 символов латинского и русского алфавита, 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 <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:

Производится первичная регистрация пользователя?

Да **Нет**

3. Выберите вариант "Да" и нажмите <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. 41) — диалог для ввода пароля примет следующий вид:

Это поле содержит пароль, автоматически генерируемый комплексом "Соболь"

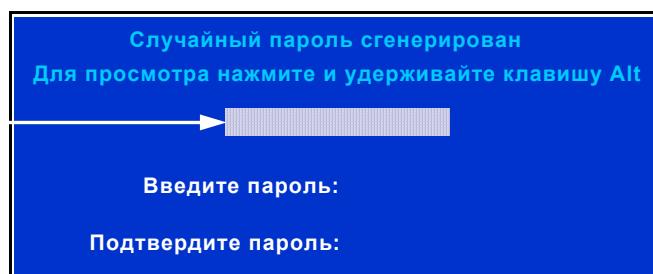


Рис. 12. Диалог для ввода случайного пароля

Для просмотра пароля, предлагаемого программой, нажмите и удерживайте в таком положении клавишу <Alt>. Запомните 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. 41), 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 <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. 41) — диалог для ввода пароля примет следующий вид:

Введите новый пароль:

Введите пароль пользователя и нажмите <Enter>.



Основные правила ввода пароля описаны в примечании на стр. 29.

Длина вводимого пароля не может быть меньше числа, заданного общим параметром "Минимальная длина пароля" (см. стр. 27), 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, 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:

Подтвердите новый пароль:

Повторно введите тот же пароль и нажмите <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:

Предъявите персональный идентификатор . . .

- Предъявите персональный идентификатор, присваиваемый пользователю.

Если идентификатор предъявлен неправильно, 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 <Enter>

Возможно данный идентификатор зарегестрирован на одном из компьютеров.

При первичной регистрации содержимое идентификатора перезаписывается заново.

Продолжить?

Да

Нет



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. 30).



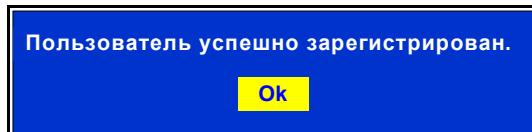
При форматировании идентификатора iButton вся информация, содержащаяся в его памяти, будет полностью утеряна без возможности восстановления. При форматировании USB-ключей и смарт-карт будет утеряна только информация, относящаяся к ПАК "Соболь" и программам, его использующим. Для отказа от форматирования 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 <Enter>.

На экране появится повторный запрос на форматирование идентификатора.

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

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



6. Нажмите <Enter>.

Имя нового пользователя появится в списке пользователей. Перейдите к настройке параметров учетной записи этого пользователя (см. стр. 48).

Для повторной регистрации пользователя:

1. Выполните действия **1–2**, приведенные в процедуре первичной регистрации пользователя (см. стр. 44).

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

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

На экране появится диалог для ввода текущего пароля пользователя:



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

На экране появится запрос:



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

Если идентификатор предъявлен неправильно, 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-читывателе.

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 <Enter>.

Имя нового пользователя появится в списке пользователей. Перейдите к настройке параметров учетной записи этого пользователя (см. стр. [48](#)).



Количество символов в пароле зарегистрированного пользователя (длина пароля) может оказаться меньше значения общего параметра "Минимальная длина пароля" (см. стр. [27](#)). 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. [41](#), параметр "Автономный режим работы").

Для настройки параметров:

1. В списке пользователей окна "Зарегистрированные пользователи" (см. [Рис. 11](#)) выберите необходимое имя и нажмите <Enter>.
2. В списке параметров учетной записи выбранного пользователя выберите параметр, значение которого нужно изменить, и нажмите <Enter>. Значение параметра изменится на противоположное, например, "Да" — "Нет", "Не блокирован" — "Блокирован", "Жесткий" — "Мягкий".
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. [27](#)) 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 <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, "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, "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, "Нет" — загрузка ОС со съемных носителей разрешена.

Для того чтобы исключить возможность модификации защищенной энергонезависимой памяти комплекса "Соболь" в режиме совместного использования (см. стр. 41, 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, "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, "Нет" — режим отключен.

При включении этого режима по истечении периода времени, заданного общим параметром "Максимальный срок действия пароля" (см. стр. 41), 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 <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, "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. 49) 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. 49) и перезагрузите компьютер.

Удаление учетной записи пользователя

Для удаления учетной записи:

- В списке пользователей окна "Зарегистрированные пользователи" (см. Рис. 11) выберите необходимое имя и нажмите <Delete>.

На экране появится запрос:

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



- Выберите вариант "Да" и нажмите <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 [3]).
- 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:

- В списке пользователей окна "Зарегистрированные пользователи" (см. Рис. 11) выберите необходимое имя и нажмите <Tab>.

На экране появится предупреждение:

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



- Если вы уверены в необходимости смены пароля и аутентификатора пользователя, выберите вариант "Да" и нажмите <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. 9) выберите команду "Смена пароля" и нажмите <Enter>.

На экране появится диалог для ввода текущего пароля администратора:

Ведите старый пароль:

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

2. Введите текущий (старый) пароль администратора и нажмите <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. 41) — на экране появится диалог для ввода случайного пароля (см. Рис. 12).

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

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 <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. 41) — диалог для ввода пароля примет следующий вид:

Ведите новый пароль:

Введите новый пароль администратора и нажмите <Enter>.



Основные правила ввода пароля описаны в примечании на стр. 29.

Длина вводимого пароля не может быть меньше числа, заданного общим параметром "Минимальная длина пароля" (см. стр. 27), 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:

Подтвердите новый пароль:

Повторно введите тот же пароль и нажмите <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:

Предъявите персональный идентификатор . . .

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-читывателе, сообщение будет присутствовать на экране. После изъятия идентификатора на экране вновь появится запрос персонального идентификатора. Предъявите идентификатор администратора или нажмите <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:

Установить новый пароль для резервной копии персонального идентификатора администратора?

Да

Нет



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 <Enter>.

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

На экране появится запрос персонального идентификатора.

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

Если идентификатор предъявлен неправильно, 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-читывателе. 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.

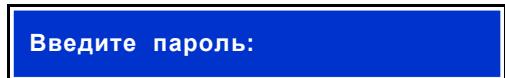
7. При необходимости повторите действия **5–6** для очередной резервной копии или завершите процедуру нажатием клавиши <Esc>.

На экране вновь появится меню администратора.

Для смены аутентификатора администратора:

1. В меню администратора (см. [Рис. 9](#)) выберите команду "Смена аутентификатора" и нажмите <Enter>.

На экране появится диалог для ввода текущего пароля администратора:



Введите пароль:

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

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

На экране появится запрос:



Предъявите персональный идентификатор . . .

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 неверный 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:



Смена аутентификатора

ВНИМАНИЕ: если после предыдущей смены аутентификатора не был произведен вход на все системы, где зарегистрирован ваш персональный идентификатор, после смены текущего аутентификатора доступ к этим системам будет невозможен.

Продолжить?

Да

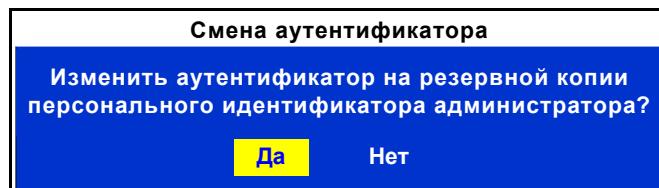
Нет

Для прекращения процедуры выберите вариант "Нет" и нажмите <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 затем повторить процедуру смены аутентификатора.

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

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

На экране появится запрос персонального идентификатора.

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

Если идентификатор предъявлен неправильно, 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 <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 <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 <Enter>.

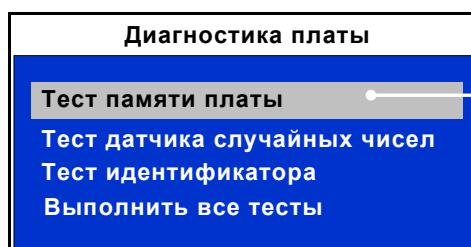
На экране вновь появится меню администратора.

Контроль работоспособности комплекса

Для контроля работоспособности активируйте команду "Диагностика платы":

- в меню "Режим инициализации" (см. стр. 25) — перед инициализацией комплекса;
- в меню "Администратор" (см. стр. 39) — во время его эксплуатации.

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



Для выбора команды используйте клавиши управления курсором <↑> и <↓>. Для выполнения выбранной команды нажмите <Enter>. Для возврата к меню администратора нажмите <Esc>

Рис. 13. Меню "Диагностика платы"

По завершении каждой процедуры на экран выводится окно с сообщением о ее результате. Подробный список сообщений содержится на стр. 90.

Тест памяти платы

Тест проверяет работоспособность 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 <Enter>.

Начнется процедура проверки, ход которой отображает следующее окно:



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

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



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

На экране вновь появится меню "Диагностика платы".

Тест датчика случайных чисел

Тест проверяет работоспособность двухканального аппаратного ДСЧ 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 <Esc>.

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



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

На экране вновь появится меню "Диагностика платы".

Тест идентификатора

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



Тестирование eToken PRO, eToken PRO (Java), iKey 2032, Rutooken, Rutooken RF возможно только после включения режима поддержки USB-идентификаторов.

Для проверки идентификатора:

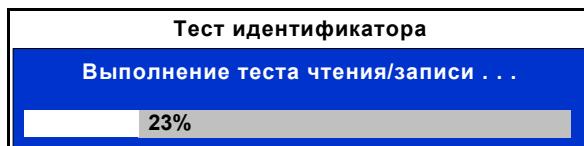
1. Выберите команду "Тест идентификатора" и нажмите <Enter>.

На экране появится запрос персонального идентификатора:



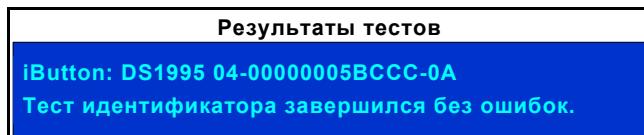
2. Предъявите проверяемый персональный идентификатор.

Начнется процедура проверки, ход которой отображает следующее окно:



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

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



3. Ознакомьтесь с полученными результатами и нажмите <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 <Enter>.

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

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

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

2. Ознакомьтесь с полученными результатами и нажмите <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 ранее всех других, т. е. самую старую запись.

Просмотр записей журнала

Для просмотра записей:

1. В меню администратора (см. Рис. 9) выберите команду "Журнал регистрации событий" и нажмите <Enter>.

На экране появится окно, фрагмент которого представлен ниже:

15:18 01/02/14 DS1994 1A-0000005E3459-04	Вход администратора
15:17 01/02/14 DS1994 1A-0000005E3459-04	Не рассчитаны контрольные суммы
15:16 01/02/14 DS1994 1A-0000005E3459-04	Перерасчет контрольных сумм
15:15 01/02/14 DS1994 1A-0000005E3459-04	Вход администратора
15:13 01/02/14 iKey 2032 9027-6153	Идентификатор не зарегистрирован
13:12 01/02/14 Иванов	Вход пользователя
1	2
3	4

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 критичные события, белым — события, связанные с успешными действиями пользователя. Полный перечень регистрируемых событий приведен на стр. 91.

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 ранее всех остальных.

Столбцы таблицы (см. рисунок выше) 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 события

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. 41, параметр "Автономный режим работы") очистка журнала запрещена.

Для очистки журнала:

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

На экране появится запрос:

Вы хотите удалить журнал регистрации событий?	
Да	Нет

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

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

Служебные операции

В комплексе "Соболь" реализованы операции, позволяющие создать копии идентификатора администратора, выполнить форматирование идентификатора, осуществить программную инициализацию комплекса, обновить его код расширения BIOS. В текущей версии обновление кода расширения BIOS доступно только для платы Mini PCI-E/Mini PCI-E Half.



Команды "Копирование идентификатора администратора" и "Инициализация платы", входящие в меню "Служебные операции", перед инициализацией комплекса являются недоступными.

Создание копии идентификатора администратора

Для создания копии идентификатора администратора:

1. В меню администратора (см. Рис. 9) выберите команду "Служебные операции" и нажмите <Enter>.

На экране появится окно "Служебные операции":

- для платы PCI/PCI-E:



Рис. 14. Окно "Служебные операции" для платы PCI/PCI-E

- для платы Mini PCI-E/Mini PCI-E Half:

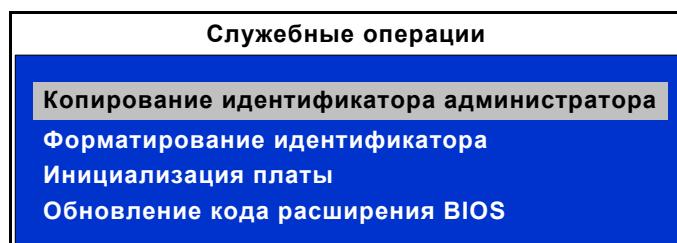


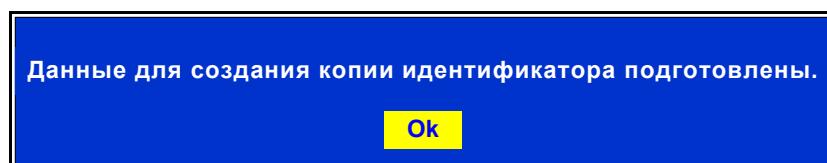
Рис. 15. Окно "Служебные операции" для платы Mini PCI-E/Mini PCI-E Half

2. В окне "Служебные операции" выберите команду "Копирование идентификатора администратора" и нажмите <Enter>.
3. В появившемся окне введите текущий пароль администратора и нажмите <Enter>.

На экране появится запрос существующего персонального идентификатора.

4. Предъявите исходный идентификатор.

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



5. Нажмите <Enter>.

На экране появится запрос персонального идентификатора.

6. 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. 44).

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 выберите вариант "Да" и нажмите <Enter>.
- Если необходимое количество резервных копий уже создано, выберите вариант "Нет" и нажмите <Enter>.

Форматирование идентификатора



При форматировании идентификатора iButton все данные, содержащиеся в его памяти, будут утеряны без возможности восстановления. При форматировании USB-ключей и смарт-карт будут утеряны только данные, относящиеся к комплексу "Соболь" и программам, его использующим.

Для форматирования идентификатора:

1. В окне "Служебные операции" выберите команду "Форматирование идентификатора" и нажмите <Enter>.

На экране появится запрос персонального идентификатора.

2. Предъявите идентификатор.

- Если идентификатор **зарегистрирован** на данном компьютере, в строке сообщений окна ПАК "Соболь" появится предупреждение "Идентификатор зарегестрирован на данном компьютере". Дальнейшее форматирование предъявленного идентификатора невозможно.
- Если идентификатор **не зарегистрирован** на данном компьютере, на экране появится предупреждение:

**Вся информация на идентификаторе будет уничтожена!
Вы уверены, что собираетесь форматировать идентификатор?**

Да Нет

Выберите вариант "Да" и нажмите <Enter>. Для отказа от форматирования выберите вариант "Нет" и нажмите <Enter>.

После форматирования идентификатора на экране появится следующее сообщение:

Идентификатор успешно отформатирован.

Ok

3. Нажмите <Enter>.

Программная инициализация комплекса

Для инициализации комплекса:

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

На экране появится следующее окно:

Вы уверены, что хотите произвести инициализацию платы?

Да Нет

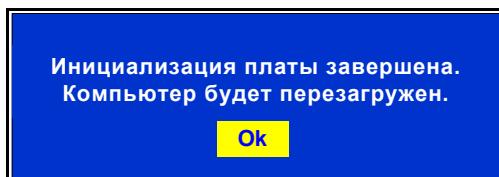
Если вы решили отказаться от инициализации, выберите вариант "Нет" и нажмите <Enter>

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

На экране появится диалог "Общие параметры системы" (см. Рис. 8).

3. Выполните действия, указанные в **шагах 2–4** процедуры инициализации комплекса (см. стр. 25).

По окончании инициализации на экране появится сообщение:



4. Нажмите <Enter>.

Обновление кода расширения BIOS плат Mini PCI-E, Mini PCI-E Half

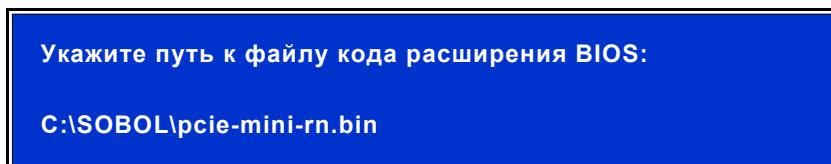


Для реализации процедуры обновления кода расширения BIOS плат Mini PCI-E, Mini PCI-E Half установите переключатель SW 2 в положение ON (см. Рис. 4, Рис. 6).

Для обновления кода расширения BIOS:

1. В окне "Служебные операции" (см. Рис. 15) выберите команду "Обновление кода расширения BIOS" и нажмите <Enter>.

На экране появится окно с указанием пути к файлу, содержащему код расширения BIOS:



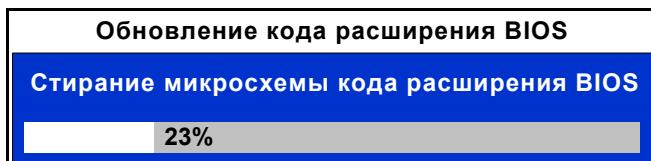
2. Для продолжения процедуры обновления кода расширения BIOS нажмите <Enter>.



Если путь к файлу кода расширения BIOS указан неправильно, то на экране появится сообщение "Неверно указан путь к файлу кода расширения BIOS". Выполните следующие действия:

- нажмите <Enter>;
- в появившемся окне укажите правильный путь и нажмите <Enter>. Учитывайте, что для файлов, размещающихся на дисках с файловой системой FAT16 и FAT32, длинные имена (более 8 символов) нужно указывать в краткой форме, например "pci-m~1.bin".

Начнется процедура обновления кода расширения BIOS, ход которой отображает следующее окно:



По окончании процедуры на экране появится окно с сообщением об успешном завершении обновления кода расширения BIOS.

3. Нажмите <Enter>.



Новая версия кода расширения BIOS плат Mini PCI-E, Mini PCI-E Half станет рабочей только после перезагрузки компьютера.

Глава 4

Настройка механизма контроля целостности

Механизм контроля целостности комплекса "Соболь" обеспечивает контроль программного и аппаратного обеспечения защищаемого компьютера до загрузки операционной системы (см. стр. [10](#)).



Порядок настройки механизма контроля целостности комплекса "Соболь" в среде ОС Linux рассмотрен в документе [[2](#)].

Для настройки механизма используется программа управления шаблонами КЦ. Программа позволяет создать исходные списки объектов, целостность которых требуется контролировать, и сохранить эти списки в специальных файлах-шаблонах. Помимо этого программа дает возможность корректировать исходные шаблоны — добавлять новые объекты, удалять объекты, не требующие контроля, восстанавливать исходные шаблоны.

Если корректировка исходных шаблонов не требуется, то для настройки контроля целостности достаточно выполнить расчет эталонных значений контрольных сумм при инициализации комплекса (см. стр. [32](#)).

Программа управления шаблонами позволяет настраивать КЦ следующих объектов:

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

Настройка механизма КЦ выполняется в следующем порядке:

- корректировка шаблонов контроля целостности (см. стр. [64](#));
- включение контроля целостности, если он был отключен (см. стр. [42](#));
- расчет эталонных значений контрольных сумм (см. стр. [78](#)).



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, элементы системного реестра, PCI-устройства, структуры SMBIOS. Их описание однозначно определяет местонахождение ресурса и его тип
Группа ресурсов	Объединяет множество описаний ресурсов одного типа (файлы, секторы, элементы реестра, PCI-устройства, структуры SMBIOS). 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.

Запуск программы управления шаблонами КЦ

Для запуска программы:

В зависимости от версии установленной операционной системы:

- на компьютере под управлением ОС Windows 8/8.1/Server 2012/Server 2012 R2 в меню приложений в группе "ПАК 'Соболь'" активируйте приложение "Управление шаблонами КЦ";
- на компьютере под управлением другой ОС семейства Windows нажмите кнопку "Пуск" и активируйте в главном меню команду "Все программы" | "ПАК 'Соболь" | "Управление шаблонами КЦ".

На экране появится главное окно программы:

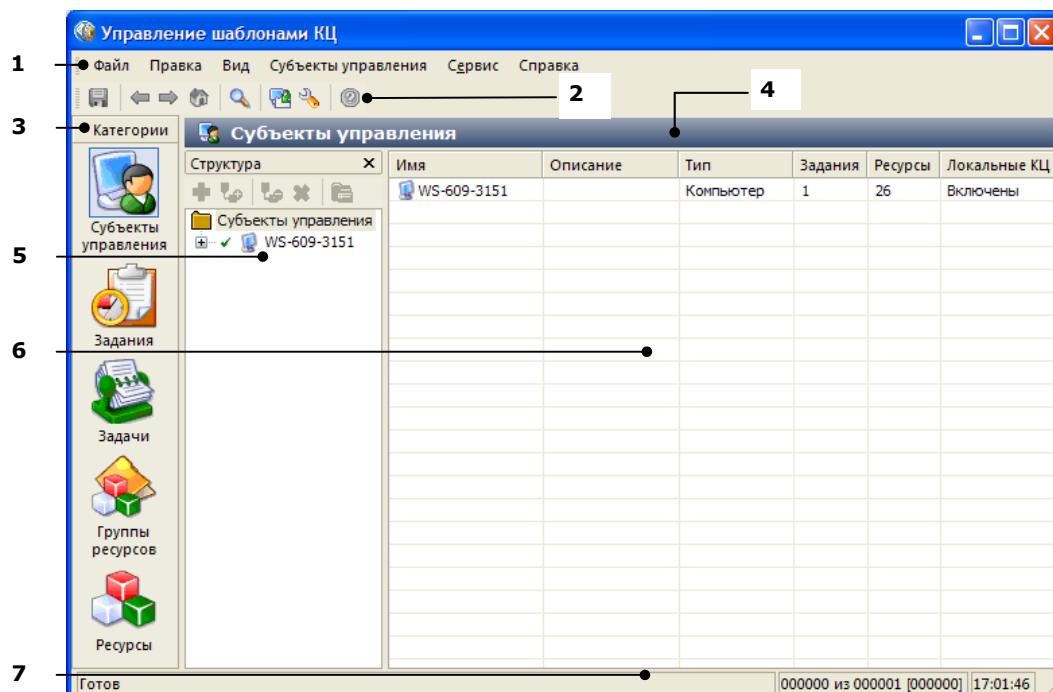


Рис. 16. Главное окно программы управления шаблонами КЦ

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"
Предназначается 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 среди 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. Стока 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) Страна 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:

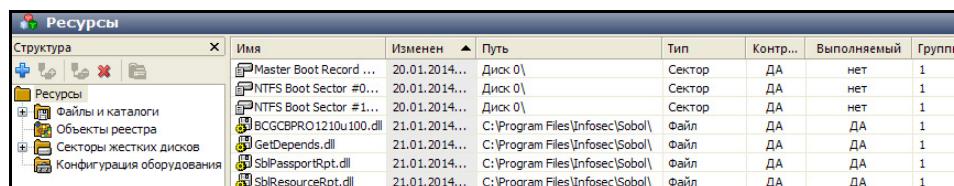
- создание новых объектов (одиночных ресурсов, групп ресурсов) для контроля целостности;
- добавление групп ресурсов в задание на контроль целостности для комплекса "Соболь";
- удаление объектов, для которых контроль целостности не требуется.

Создание одиночных ресурсов

Для создания одиночного ресурса (файл, сектор, элемент реестра, PCI-устройство, структура SMBIOS):

1. В области "Категории" главного окна программы управления шаблонами КЦ (см. Рис. 16) выберите категорию "Ресурсы".

Окно "Ресурсы" примет вид, подобный следующему:

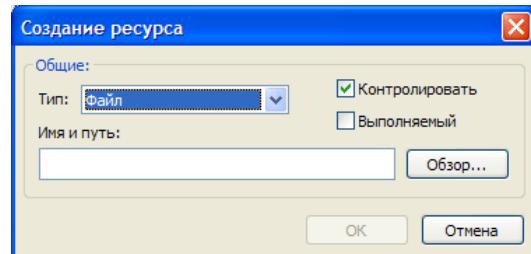


Имя	Изменен	Путь	Тип	Контр...	Выполняемый	Группы
Master Boot Record ...	20.01.2014...	Диск 0\	Сектор	ДА	нет	1
NTFS Boot Sector #0...	20.01.2014...	Диск 0\	Сектор	ДА	нет	1
NTFS Boot Sector #1...	20.01.2014...	Диск 0\	Сектор	ДА	нет	1
BCCGPBRO1210u100.dll	21.01.2014...	C:\Program Files\Infosec\Sobol\	Файл	ДА	ДА	1
GetDepends.dll	21.01.2014...	C:\Program Files\Infosec\Sobol\	Файл	ДА	ДА	1
SblPassportRpt.dll	21.01.2014...	C:\Program Files\Infosec\Sobol\	Файл	ДА	ДА	1
SblResourceRpt.dll	21.01.2014...	C:\Program Files\Infosec\Sobol\	Файл	ДА	ДА	1

Пояснение. Папки "Файлы и каталоги", "Объекты реестра", "Секторы жестких дисков", "Конфигурация оборудования" 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"/"Конфигурация оборудования".



Ресурс "Конфигурация оборудования" включает в себя PCI-устройства и структуры SMBIOS.

- Нажмите кнопку "Обзор".
 - В появившемся соответствующем окне "Выбор файла"/"Просмотр реестра"/"Секторы"/"Конфигурация оборудования" выберите необходимый ресурс и нажмите "Открыть"/"OK".
- В списке "Имя и путь" окна "Создание ресурса" появится путь к выбранному ресурсу.
- Нажмите "OK".

Окно "Ресурсы" примет вид, подобный следующему:

Структура	Имя	Изменен	Путь	Тип	Контр...	Выполняемый	Группы
Ресурсы	BIOS #0000	28.01.2014...	SMBIOS\	SMBIOS т...	ДА	нет	0
	IOProcs	28.01.2014...	HKEY_USERS\S-1-5-18\Console\	Ключ	ДА	нет	0
	ColorTable00	28.01.2014...	HKEY_USERS\S-1-5-18\Console\	Переменная	ДА	нет	0
	IntelChipset.log	28.01.2014...	C:\Intel\Logos\	Файл	ДА	нет	0
	BCGCBPDR1210u100.dll	21.01.2014...	C:\Program Files\Infosec\Sobol\	Файл	ДА	ДА	1
	GetDepends.dll	21.01.2014...	C:\Program Files\Infosec\Sobol\	Файл	ДА	ДА	1
	SblPassportRpt.dll	21.01.2014...	C:\Program Files\Infosec\Sobol\	Файл	ДА	ДА	1

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:

Структура	Имя	Изменена	Описание	Тип	Принадлежит	Ресурсы
Группы ресурсов	Секторы жестких д...	20.01.2014 ...		Секторы жест...	1	3
	Модули ПО для ПАК...	20.01.2014 ...	Модули ПО для ПАК...	Файлы/Каталоги	1	23

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":

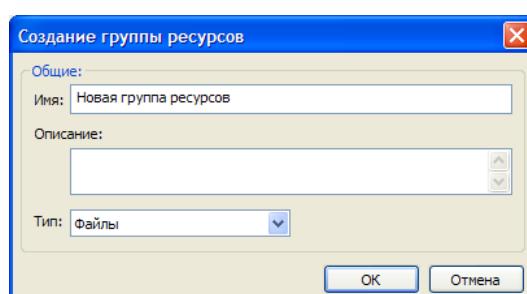


Рис. 17. Окно "Создание группы ресурсов"

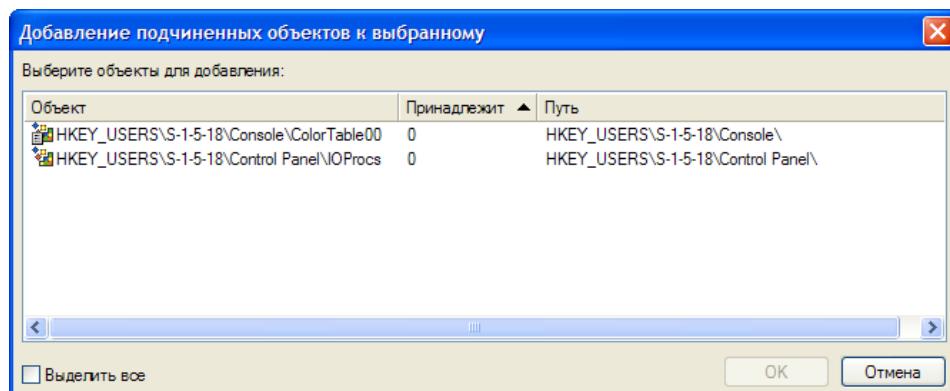
- Выполните следующие действия:
 - в поля "Имя" и "Описание" введите соответственно имя создаваемой группы (например, "Группа Файл"/"Группа Реестр"/"Группа Сектор"/"Группа Оборудование") и при необходимости краткую дополнительную информацию о группе;
 - в раскрывающемся списке "Тип" выберите "Файлы"/"Объекты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

Окно "Группы ресурсов" примет вид, подобный следующему:

Структура	Имя	Изменена	Описание	Тип	Принадлежит	Ресурсы
Группы ресурсов	Секторы жестких д...	20.01.2014 ...		Секторы жест...	1	3
	Модули ПО для ПАК "Соболь"	20.01.2014 ...	Модули ПО для ПАК...	Файлы/Каталоги	1	23
	Группа Файл	28.01.2014 ...		Файлы/Каталоги	0	0
	Группа Реестр	28.01.2014 ...		Объекты реест...	0	0
	Группа Сектор	28.01.2014 ...		Секторы жест...	0	0
	Группа Оборудование	28.01.2014 ...		Конфигурация...	0	0

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

На экране появится диалоговое окно, подобное следующему:



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

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

Структура	Имя	Изменен	Путь	Тип	Контр...	Выполняемый	Группы
Группы ресурсов	10Procs	28.01.2014...	HKEY_USERS\S-1-5-18\Contr...	Ключ	ДА	нет	1
	ColorTable00	28.01.2014...	HKEY_USERS\S-1-5-18\Console\	Перененная	ДА	нет	1

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

Окно "Группы ресурсов" примет вид, подобный следующему:

Структура	Имя	Изменена	Описание	Тип	Принадлежит	Ресурсы
+ Группы ресурсов	Секторы жестких д...	20.01.2014 ...		Секторы жест...	1	3
+ Секторы жестких дисков	Модули ПО для ПАК...	20.01.2014 ...	Модули ПО для ПАК...	Файлы/Каталоги	1	23
+ Модули ПО для ПАК "Соболь"	Каталог 'C:\logs'	28.01.2014 ...	Группа по каталогу ...	Файлы/Каталоги	0	1
+ Каталог 'C:\logs'						

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. 17).

2. Выполните следующие действия:

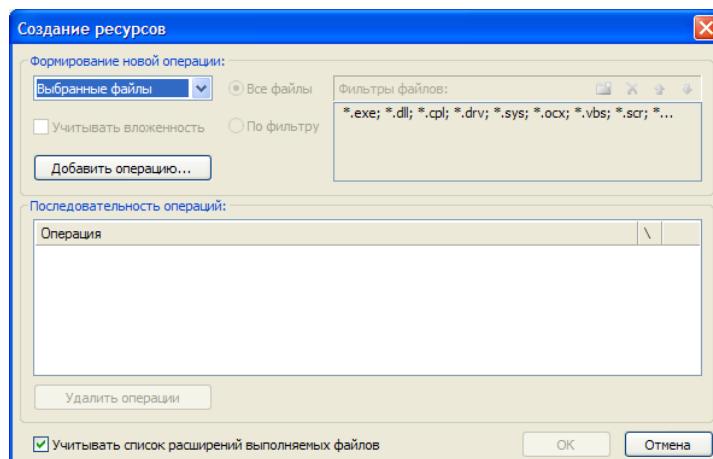
- в поля "Имя" и "Описание" введите соответственно имя создаваемой группы (например, "Группа 1") и при необходимости краткую дополнительную информацию о группе;
- в раскрывающемся списке "Тип" выберите "Файлы";
- нажмите "OK".

Окно "Группы ресурсов" примет вид, подобный следующему:

Структура	Имя	Изменена	Описание	Тип	Принадлежит	Ресурсы
+ Группы ресурсов	Секторы жестких д...	20.01.2014 ...		Секторы жест...	1	3
+ Секторы жестких дисков	Модули ПО для ПАК...	20.01.2014 ...	Модули ПО для ПАК...	Файлы/Каталоги	1	23
+ Модули ПО для ПАК "Соболь"	Каталог 'C:\logs'	28.01.2014 ...	Группа по каталогу ...	Файлы/Каталоги	0	1
+ Каталог 'C:\logs'	Группа 1	28.01.2014 ...		Файлы/Каталоги	0	0

3. В области "Структура" вызовите контекстное меню папки созданной группы и выполните команду "Добавить ресурсы" | "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	Доступны 2 варианта: <ul style="list-style-type: none"> "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:

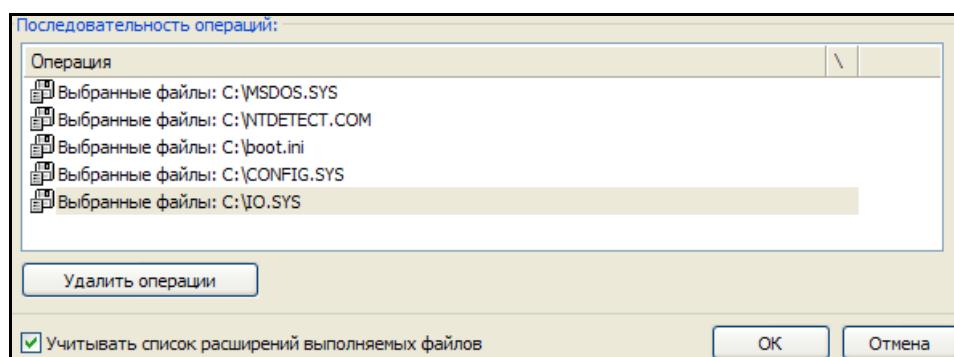
Если выбрано...	...перейдите к действию:
Выбранные файлы	5
Файлы по каталогу	7

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:

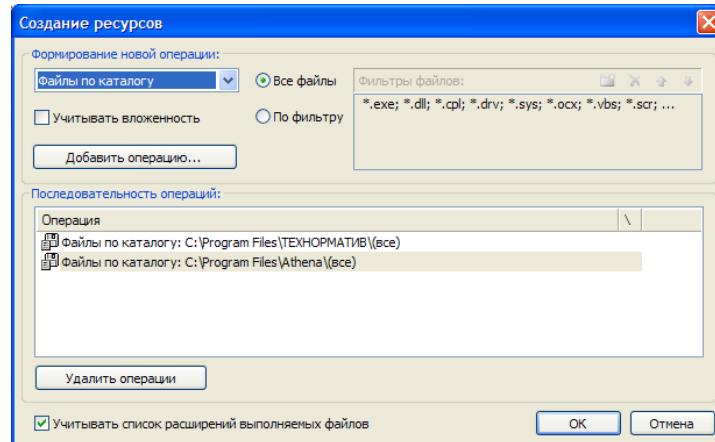
- Если другие ресурсы добавлять не требуется, перейдите к действию **9**.
- Если требуется добавить другие ресурсы, вернитесь к выполнению действия **4** данной процедуры.

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".

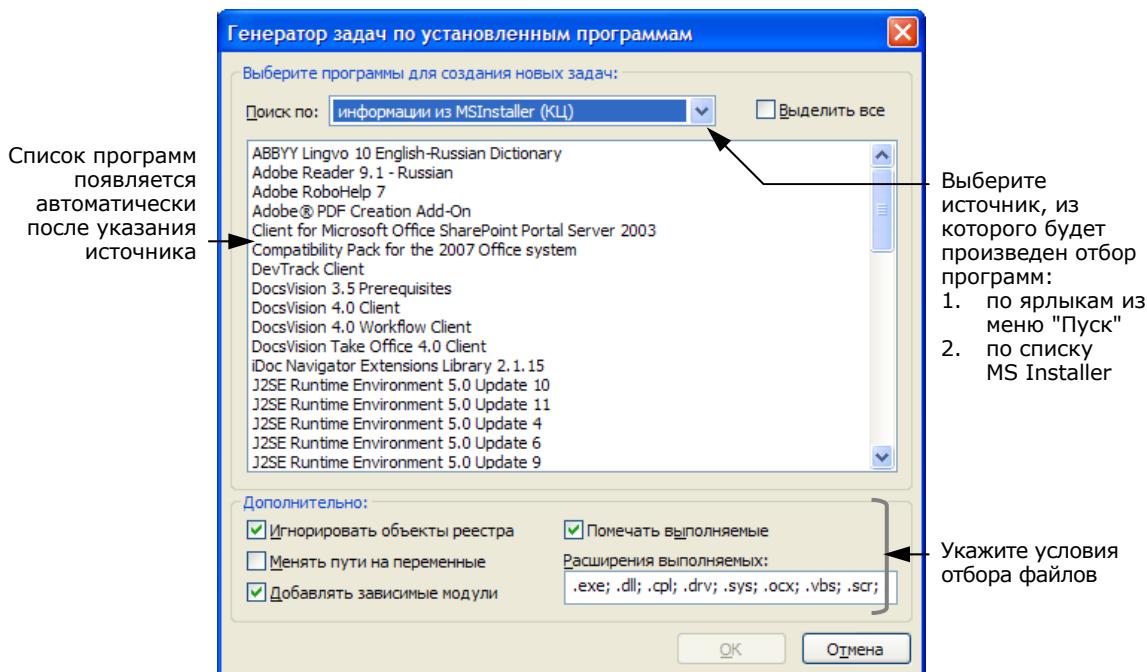
Диалог "Создание ресурсов" закроется. Окно "Группы ресурсов" примет вид, подобный следующему:

Структура	Имя	Изменен	Путь	Тип	Контр...	Выполняемый	Группы
+ Группы ресурсов	MSDOS.SYS	28.01.2014...	C:\	Файл	ДА	ДА	1
+ Секторы жестких дисков	NTDETECT.COM	28.01.2014...	C:\	Файл	ДА	ДА	1
+ Модули ПО для ПАК "Соболь"	boot.ini	28.01.2014...	C:\	Файл	ДА	нет	1
+ Каталог C:\logs	CONFIG.SYS	28.01.2014...	C:\	Файл	ДА	ДА	1
+ Группа 1	IO.SYS	28.01.2014...	C:\	Файл	ДА	ДА	1
	1.xml	28.01.2014...	C:\Program Files\ТЕХНОМАТ...	Файл	ДА	нет	1
	Client_network.exe	28.01.2014...	C:\Program Files\ТЕХНОМАТ...	Файл	ДА	ДА	1

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" | "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"

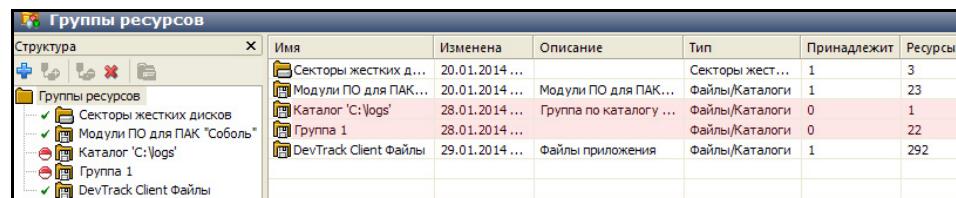
При выборе из списка MS Installer можно задать каждое из приведенных выше дополнительных условий. При выборе по ярлыкам из меню "Пуск" можно задать только два условия: "Менять пути на переменные" и "Помечать выполняемые".

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" | "Вручную".
На экране появится диалоговое окно "Создание группы ресурсов" (см. Рис. 17).
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 "OK".

Окно "Группы ресурсов" примет вид, подобный следующему:

Структура	Имя	Изменена	Описание	Тип	Принадлежит	Ресурсы
Группы ресурсов	Секторы жестких д...	20.01.2014 ...	Секторы жест...	1	3	
	Модули ПО для ПАК...	20.01.2014 ...	Модули ПО для ПАК...	Файлы/Каталоги	1	23
	Группа 2	29.01.2014 ...	Секторы жест...	0	0	

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

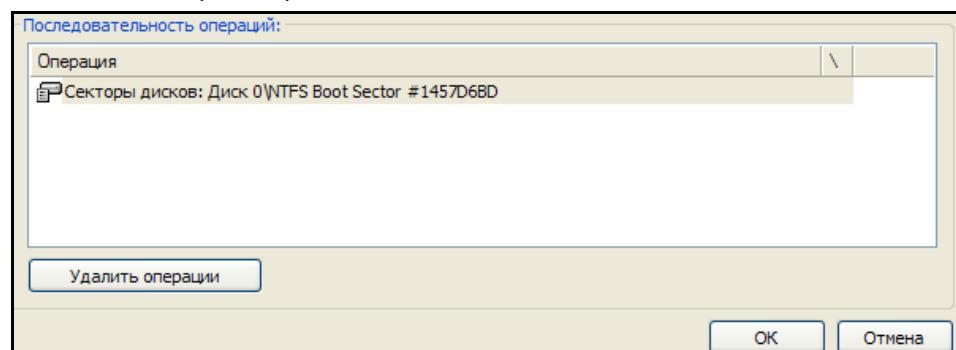
На экране появится диалоговое окно "Создание ресурсов".

5. Нажмите кнопку "Добавить операцию".

На экране появится диалог выбора секторов.

6. Выберите нужные секторы и нажмите "OK".

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 "OK".

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

Структура	Имя	Изменен	Путь	Тип	Контр...	Выполняемый	Группы
Группы ресурсов	NTFS Boot Sector #1457D6BD	20.01.2014...	Диск 0\	Сектор	ДА	нет	2

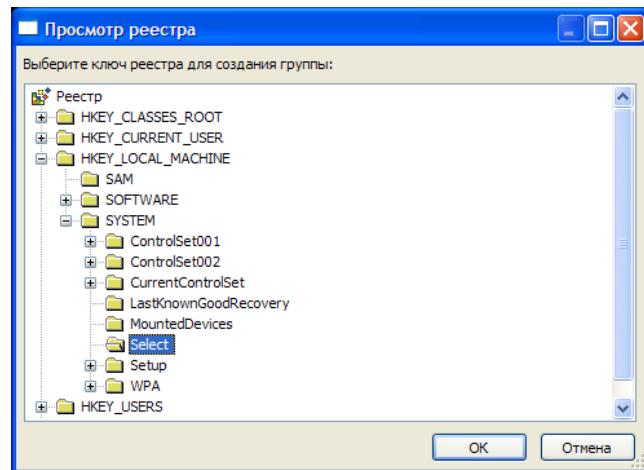
Создание группы элементов системного реестра

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" | "По ключу реестра".

На экране появится окно "Просмотр реестра":



- Выберите необходимый элемент реестра и нажмите "OK". В появившемся информационном окне "Управление шаблонами КЦ" нажмите "OK".

Окно "Группы ресурсов" примет вид, подобный следующему:

Группы ресурсов		Имя	Изменен	Путь	Тип	Контр...	Выполняемый	Группы
	+	Select	29.01.2014...	HKEY_LOCAL...	Ключ	ДА	нет	1
	+	Current	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1
	+	Default	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1
	+	Failed	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1
	+	LastKnownGood	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1

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

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

На экране появится диалоговое окно "Создание группы ресурсов" (см. Рис. 17).

- Выполните следующие действия:

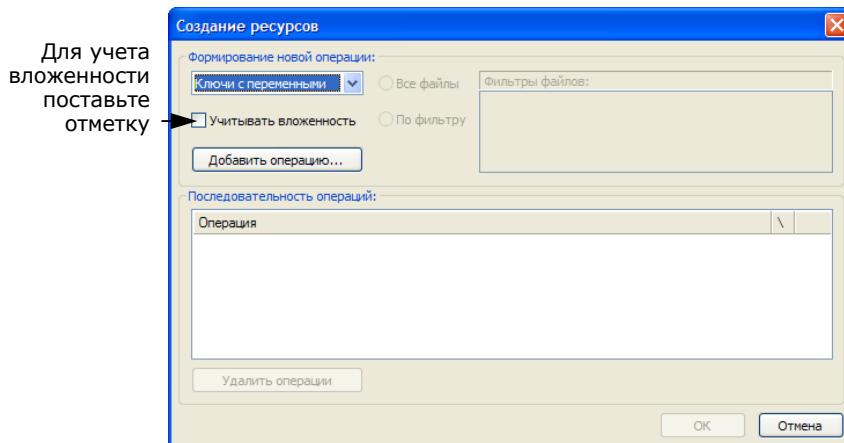
- в поля "Имя" и "Описание" введите соответственно имя создаваемой группы (например, "Группа 3") и при необходимости краткую дополнительную информацию о группе;
- в раскрывающемся списке "Тип" выберите "Объекты реестра";
- нажмите "OK".

Окно "Группы ресурсов" примет вид, подобный следующему:

Группы ресурсов		Имя	Изменена	Описание	Тип	Принадлежит	Ресурсы
	+	Секторы жестких дисков	20.01.2014...		Секторы жестк...	1	3
	+	Модули ПО для ПАК "Соболь"	20.01.2014...	Модули ПО для ПАК "Соб...	Файлы/Каталоги	1	23
	+	Группа 3	29.01.2014 ...		Объекты реестра	0	0

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

На экране появится диалоговое окно "Создание ресурсов":

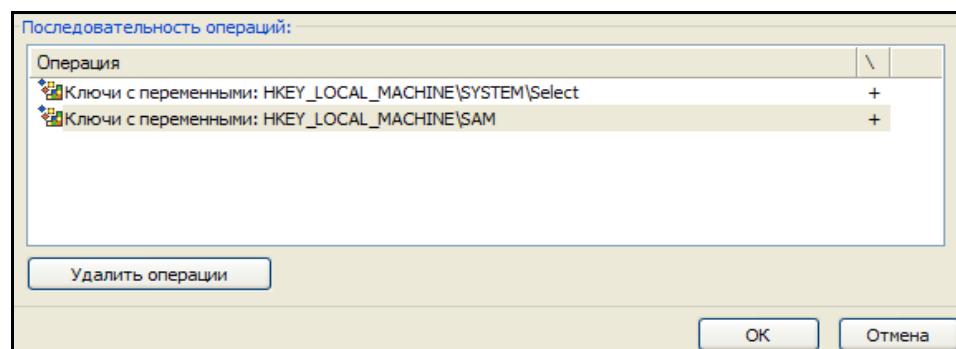


5. Выберите параметр "Ключи с переменными". Нажмите кнопку "Добавить операцию".

На экране появится окно "Просмотр реестра".

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

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



7. Нажмите "OK".

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

Группы ресурсов								
Структура	Имя	Изменен	Путь	Тип	Контр...	Выполняемый	Группы	
+ Группы ресурсов	Select	29.01.2014...	HKEY_LOCAL...	Ключ	ДА	нет	1	
+ Секторы жестких дисков	Current	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1	
+ Модули ПО для ПАК "Соболь"	Default	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1	
+ Группа 3	Failed	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1	
	LastKnownGood	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1	
	SAM	29.01.2014...	HKEY_LOCAL...	Ключ	ДА	нет	1	

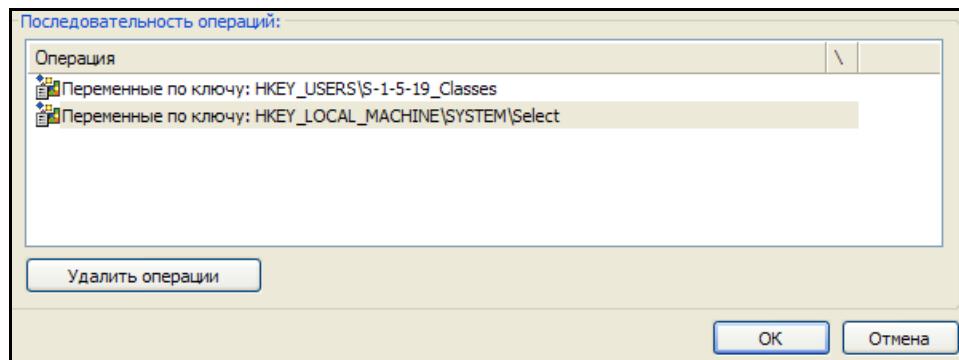
Для создания группы переменных ключей реестра:

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 "OK".

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



4. Нажмите "OK".

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

Группы ресурсов								
Структура	Имя	Изменен	Путь	Тип	Контр...	Выполняемый	Группы	
	Current	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1	
	Default	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1	
	Failed	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1	
	LastKnownGood	29.01.2014...	HKEY_LOCAL...	Переменная	ДА	нет	1	
	Группа 3							

Для создания группы PCI-устройств, структур SMBIOS:

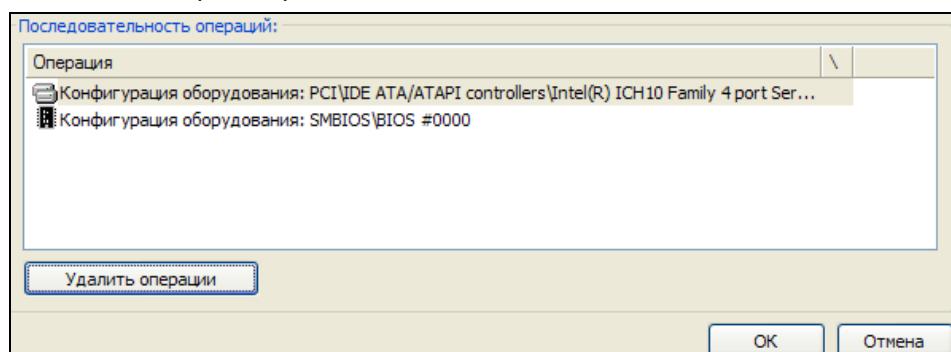
1. В области "Категории" главного окна программы управления шаблонами КЦ выберите категорию "Группы ресурсов".
2. В области "Структура" вызовите контекстное меню папки "Группы ресурсов" и выполните команду "Создать группу" | "Вручную".
На экране появится диалоговое окно "Создание группы ресурсов" (см. Рис. 17).
3. Выполните следующие действия:
 - в поля "Имя" и "Описание" введите соответственно имя создаваемой группы (например, "Группа 4") и при необходимости краткую дополнительную информацию о группе;
 - в раскрывающемся списке "Тип" выберите "Конфигурация оборудования";
 - нажмите "OK".

Окно "Группы ресурсов" примет вид, подобный следующему:

Группы ресурсов						
Структура	Имя	Изменена	Описание	Тип	Принадлежит	Ресурсы
	Секторы жестких дисков	20.01.2014 ...		Секторы жестк... 1	3	
	Модули ПО для ПАК "Соболь"	20.01.2014 ...	Модули ПО для ПАК "Соболь"	Файлы/Каталоги 1	23	
	Группа 4	31.01.2014 ...		Конфигурация ... 0	0	

4. В области "Структура" вызовите контекстное меню папки созданной группы и выполните команду "Добавить ресурсы" | "Несколько новых".
На экране появится диалоговое окно "Создание ресурсов".
5. Нажмите кнопку "Добавить операцию".
На экране появится диалог выбора PCI-устройств и структур SMBIOS.
6. Выберите нужные ресурсы и нажмите "OK".

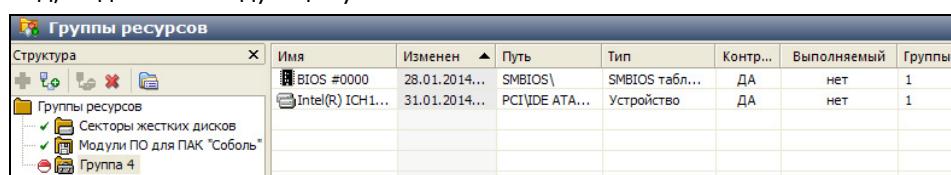
В нижней части диалога "Создание ресурсов" появится список операций, подобный следующему:



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

7. Нажмите "OK".

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

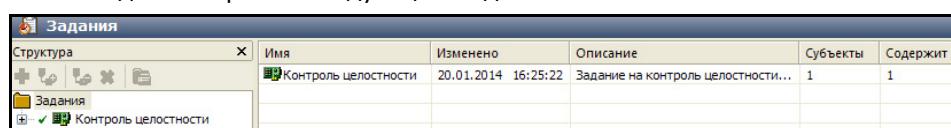


Добавление объектов в задание на контроль целостности

Для добавления объектов:

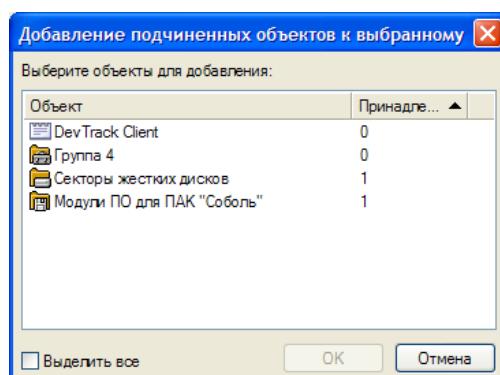
1. В панели категорий главного окна программы "Управление шаблонами КЦ" выберите категорию "Задания".

Окно "Задания" примет следующий вид:



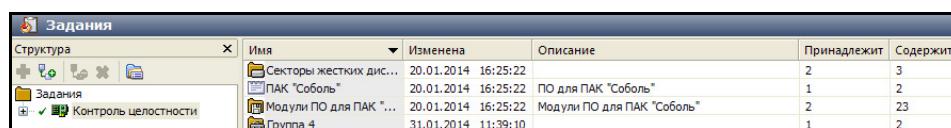
2. В области "Структура" вызовите контекстное меню папки "Контроль целостности" и выполните команду "Добавить задачи/группы" | "Существующие".

На экране появится диалоговое окно, подобное следующему:



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

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".

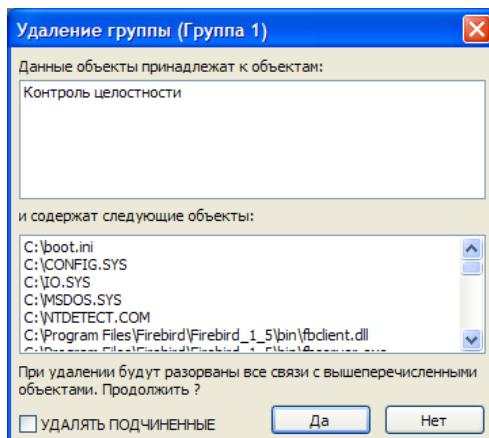
На экране появится информационное окно "Управление шаблонами КЦ".

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. [74](#)).
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. 16](#)) 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:

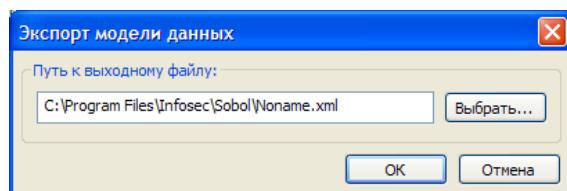
- в панели инструментов нажмите кнопку "Сохранить модель";
- нажмите комбинацию клавиш <Ctrl>+<S>;
- в меню "Файл" активируйте команду "Сохранить".

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 "OK".

На экране появится информационное сообщение о результатах экспорта модели данных.

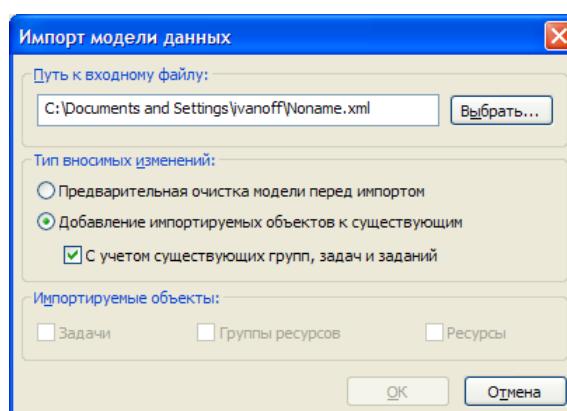
4. Нажмите "OK".

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

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 (флеш-накопители, CD-, DVD-приводы, съемные жесткие диски и т. п.).

Для расчета контрольных сумм:

1. Перезагрузите компьютер и войдите в систему с правами администратора комплекса "Соболь" (см. стр. [37](#)).
2. В меню администратора (см. [Рис. 9](#)) выберите команду "Расчет контрольных сумм" и нажмите <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 шаблон КЦ файлов, исключив из него отсутствующие на диске файлы (см. стр. [64](#)). После того как все выявленные недостатки будут устранены, повторите процедуру расчета эталонных значений контрольных сумм. Подробный список сообщений об ошибках содержится на стр. [83](#).

Приложение

Сообщения комплекса "Соболь"

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/Mini PCI-E, 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 КБ 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/Mini PCI-E, в который плата установлена. Если ошибку устранить не удалось, выполните инициализацию комплекса "Соболь" (см. стр. 25).

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. 25).

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. 50) и заново выполните их регистрацию (см. стр. 44). 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. 58).

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. 62).

Тест ДСЧ завершился с ошибкой

Причина: При старте комплекса "Соболь" выполняется тестирование ДСЧ. 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 Mini PCI-E/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. 27). Компьютер блокируется для входа данного пользователя.

Действие: Чтобы разрешить данному пользователю вход в систему, присвойте параметру "Количество неудачных попыток входа" значение "0" (см. стр. 48). Затем присвойте параметру "Текущий статус пользователя" значение "не блокирован" (см. стр. 48).

Ваш вход в систему запрещен администратором

Причина: Администратор заблокировал вход в систему для данного пользователя — параметру "Текущий статус пользователя" присвоено значение "блокирован" (см. стр. 48). 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 менее числа, заданного общим параметром "Минимальная длина пароля" (см. стр. 27).

Действие: Введите пароль допустимой длины.

Данный персональный идентификатор не принадлежит администратору

Причина: Предъявленный персональный идентификатор не принадлежит администратору.

Действие: Предъявите персональный идентификатор администратора.

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:** Во время регистрации нового пользователя, при смене пароля пользователя и администратора при включенном режиме использования случайных паролей введенный пароль не совпал с предложенным случайным паролем.**Действие:** Повторите ввод пароля, не допуская ошибок.**Неподдерживаемый тип идентификатора****Причина:** Предъявлен не поддерживаемый комплексом "Соболь" идентификатор.**Действие:** Используйте идентификаторы, поддерживаемые комплексом "Соболь" (см. Табл. 1).**Идентификатор 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.

Расчет контрольных сумм

** Расчет контрольных сумм остановлен

Причина: Процесс расчета контрольных сумм остановлен администратором.

Действие: Не требуется.

** Расчет контрольных сумм параметров конфигурации завершился с ошибкой

Причина: Во время расчета контрольных сумм параметров конфигурации произошла ошибка.

Действие: Выясните и устраните причину, из-за которой произошла ошибка. Восстановите шаблоны КЦ PCI-устройств и структур SMBIOS (Bootpci.nam, Bootpci.chk, Bootsmbs.nam, Bootsmbs.chk). Рассчитайте эталонные значения контрольных сумм.

** Расчет контрольных сумм файлов и секторов завершился с ошибкой

Причина: Во время расчета контрольных сумм файлов и секторов произошла ошибка.

Действие: Выясните и устраните причину, из-за которой произошла ошибка. Восстановите шаблоны КЦ файлов и секторов (Bootfile.nam, Bootfile.chk, Bootsect.nam, Bootsect.chk). Рассчитайте эталонные значения контрольных сумм.

** Расчет контрольных сумм элементов реестра завершился с ошибкой

Причина: Во время расчета контрольных сумм элементов реестра произошла ошибка.

Действие: Выясните и устраните причину, из-за которой произошла ошибка. Восстановите шаблоны КЦ элементов реестра (Bootreg.nam, Bootreg.chk). Рассчитайте эталонные значения контрольных сумм.

Контроль файлов

** Изменилось содержимое файла

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

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

** Изменилось содержимое шаблонов КЦ файлов

Причина: Модифицировано содержимое файлов Bootfile.nam и (или) Bootfile.chk.

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

** Ошибка записи шаблонов КЦ файлов

Причина: Произошла ошибка при записи данных в файлы Bootfile.nam и (или) Bootfile.chk.

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

**** Ошибка чтения шаблонов КЦ файлов**

Причина: Произошла ошибка при чтении данных из файлов Bootfile.nam и (или) Bootfile.chk.

Действие: Восстановите шаблоны КЦ файлов и рассчитайте эталонные значения 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 устранитте причину, по которой содержимое файла недоступно для чтения. 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 устранитте причину, по которой файл не найден. При необходимости исключите этот файл из шаблонов КЦ файлов и выполните расчет эталонных значений контрольных сумм.

**** Шаблоны КЦ файлов не найдены**

Причина: Не найдены файлы Bootfile.nam и (или) Bootfile.chk.

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

**** Шаблоны КЦ файлов разрушены**

Причина: Нарушена структура файлов Bootfile.nam и (или) Bootfile.chk.

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

Контроль секторов жестких дисков**** Изменилось содержимое сектора**

Причина: Этalonное значение контрольной суммы указанного сектора не совпало с текущим значением контрольной суммы, рассчитанным для этого сектора.

Действие: Выясните и устранитте причину, из-за которой содержимое сектора изменилось. Выполните расчет эталонных значений контрольных сумм.

**** Изменилось содержимое шаблонов КЦ секторов**

Причина: Модифицировано содержимое файлов Bootsect.nam и (или) Bootsect.chk.

Действие: Если изменение файла Bootsect.nam вызвано корректировкой списка контролируемых секторов в программе управления шаблонами КЦ, рассчитайте эталонные значения контрольных сумм. В остальных случаях выясните причину модификации указанных файлов, устранитте ее, а затем восстановите шаблоны КЦ секторов жестких дисков и рассчитайте эталонные значения контрольных сумм.

**** Ошибка записи шаблонов КЦ секторов**

Причина: Произошла ошибка при записи данных в файлы Bootsect.nam и (или) Bootsect.chk

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

**** Ошибка чтения шаблонов КЦ секторов**

Причина: Произошла ошибка при чтении данных из файлов Bootsect.nam и (или) Bootsect.chk.

Действие: Восстановите шаблоны КЦ секторов 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 устранитте причину, по которой содержимое сектора недоступно для чтения. Выполните расчет эталонных значений контрольных сумм.

**** Сектор не найден**

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

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

**** Шаблоны КЦ секторов не найдены**

Причина: Не найдены файлы Bootsect.nam и (или) Bootsect.chk.

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

**** Шаблоны КЦ секторов разрушены**

Причина: Нарушена структура файлов Bootsect.nam и (или) Bootsect.chk.

Выясните и устранитте причину изменения структуры файла(ов). Восстановите шаблоны КЦ секторов и рассчитайте эталонные значения контрольных сумм.

Контроль элементов системного реестра**** Изменилось содержимое ключа реестра**

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

Действие: Выясните и устранитте причину, из-за 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.

Действие: Выясните и устранитте причину, из-за которой изменилось содержимое параметра ключа. Выполните расчет эталонных значений контрольных сумм.

**** Изменилось содержимое шаблонов КЦ элементов реестра**

Причина: Модифицировано содержимое файлов Bootreg.nam и (или) Bootreg.chk.

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

**** Ключ реестра не найден**

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

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

**** 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 шаблонов КЦ элементов реестра и выполните расчет эталонных значений контрольных сумм.

**** Ошибка записи шаблонов КЦ элементов реестра**

Причина: Произошла ошибка при записи данных в файлы Bootreg.nam и (или) Bootreg.chk.

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

**** Ошибка чтения шаблонов КЦ элементов реестра**

Причина: Произошла ошибка при чтении данных из файлов Bootreg.nam и (или) Bootreg.chk.

Действие: Восстановите шаблоны КЦ элементов реестра и рассчитайте эталонные значения 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 устранитте причину, по которой содержимое файла реестра недоступно для чтения. Выполните расчет эталонных значений контрольных сумм.

**** Параметр реестра не найден**

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

Действие: Выясните и устранитте причину, по которой переменная не найдена. При необходимости исключите эту переменную из шаблонов КЦ элементов реестра 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 устранитте причину, по которой файл реестра не найден. При необходимости исключите эту ветку реестра из шаблонов КЦ элементов реестра и выполните расчет эталонных значений контрольных сумм.

**** Файл реестра разрушен**

Причина: Нарушена структура файла реестра для указанной ветки реестра.

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

**** Шаблоны КЦ элементов реестра не найдены**

Причина: Не найдены файлы Bootreg.nam и (или) Bootreg.chk.

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

**** Шаблоны КЦ элементов реестра разрушены**

Причина: Нарушена структура файлов Bootreg.nam и (или) Bootreg.chk.

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

Контроль PCI-устройств**** Изменилось содержимое шаблонов КЦ PCI-устройств**

Причина: Модифицировано содержимое файлов Bootpci.nam и (или) Bootpci.chk.

Действие: Если изменение файла Bootpci.nam вызвано корректировкой списка контролируемых устройств PCI в программе управления шаблонами, рассчитайте эталонные значения контрольных сумм. В остальных случаях выясните причину модификации указанных файлов, устранитте ее, а затем восстановите шаблоны КЦ устройств PCI и рассчитайте эталонные значения контрольных сумм.

**** Изменилось состояние PCI-устройства**

Причина: Эталонное значение контрольной суммы указанного PCI-устройства не совпало с текущим значением контрольной суммы, рассчитанным для этого устройства. Устройство отсутствует или изменилось содержимое его конфигурационного пространства.

Действие: Выясните и устранитте причину, по которой изменилось состояние PCI-устройства. Выполните расчет эталонных значений контрольных сумм.

**** Изменилось состояние адресного пространства PCI-устройства**

Причина: Эталонное значение контрольной суммы неиспользуемого адресного пространства PCI-устройств не совпало с текущим значением контрольной суммы.

Действие: Выясните и устранитте причину, по которой изменилось состояние неиспользуемого адресного пространства PCI-устройств. Выполните расчет эталонных значений контрольных сумм.

**** Изменился адрес PCI-устройства**

Причина: Устройство присутствует в системе, но его адрес не совпадает с адресом, указанным в файле Bootpci.nam.

Действие: Выясните и устранитте причину, по которой изменился адрес PCI-устройства. Выполните расчет эталонных значений контрольных сумм.

**** Ошибка записи шаблонов КЦ PCI-устройств**

Причина: Произошла ошибка при записи данных в файлы Bootpci.nam и (или) Bootpci.chk.

Действие: Восстановите шаблоны КЦ устройств PCI и рассчитайте эталонные значения контрольных сумм.

**** Ошибка чтения шаблонов КЦ PCI-устройств**

Причина: Произошла ошибка при чтении данных из файлов Bootpci.nam и (или) Bootpci.chk.

Действие: Восстановите шаблоны КЦ устройств PCI и рассчитайте эталонные значения контрольных сумм.

**** Расширенное адресное пространство PCI-устройств не найдено**

Причина: В системе не найдено расширенное конфигурационное адресное пространство PCI-устройств. Возможно, оно отсутствует или доступ к нему отключен в BIOS Setup.

Действие: Выясните и устранитте причину, по которой не найдено расширенное конфигурационное адресное пространство PCI-устройств. При необходимости выполните расчет эталонных значений контрольных сумм.

**** PCI-устройство не найдено**

Причина: Указанное устройство не найдено на PCI-шине. Появление ошибки при расчете контрольных сумм в стандартном и расширенном режимах возможно в случае неправильного указания адреса устройства.

Действие: Выясните и устранитте причину, по которой устройство PCI не найдено. При необходимости исключите это устройство из шаблонов КЦ устройств PCI и выполните расчет эталонных значений контрольных сумм.

**** Шаблоны КЦ PCI-устройств не найдены**

Причина: Не найдены файлы Bootpci.nam и (или) Bootpci.chk.

Действие: Восстановите шаблоны КЦ устройств PCI и рассчитайте эталонные значения контрольных сумм.

**** Шаблоны КЦ PCI-устройств разрушены**

Причина: Нарушена структура файлов Bootpci.nam и (или) Bootpci.chk.

Действие: Восстановите шаблоны КЦ устройств PCI и рассчитайте эталонные значения контрольных сумм.

Контроль структур SMBIOS

** Изменилось содержимое структуры SMBIOS

Причина: Эталонное значение контрольной суммы указанной структуры или параметра одной из структур SMBIOS не совпало с текущим значением контрольной суммы.

Действие: Выясните и устраните причину, из-за которой содержимое указанной структуры или параметра одной из структур SMBIOS изменилось. Выполните расчет эталонных значений контрольных сумм.

** Изменилось содержимое шаблонов КЦ структур SMBIOS

Причина: Модифицировано содержимое файлов Bootsmbs.nam и (или) Bootsmbs.chk.

Действие: Если изменение файла Bootsmbs.nam вызвано корректировкой списка контролируемых структур SMBIOS в программе управления шаблонами, рассчитайте эталонные значения контрольных сумм. В остальных случаях выясните причину модификации указанных файлов, устраните ее, а затем восстановите шаблоны КЦ структур SMBIOS и рассчитайте эталонные значения контрольных сумм.

** Ошибка записи шаблонов КЦ структур SMBIOS

Причина: Произошла ошибка при записи данных в файлы Bootsmbs.nam и (или) Bootsmbs.chk.

Действие: Восстановите шаблоны КЦ структур SMBIOS и рассчитайте эталонные значения контрольных сумм.

** Ошибка контроля структуры SMBIOS

Причина: Не найдена указанная структура или параметр одной из структур SMBIOS.

Действие: Выясните и устраните причину, по которой указанная структура или параметр не найден. При необходимости выполните расчет эталонных значений контрольных сумм.

** Ошибка чтения шаблонов КЦ структур SMBIOS

Причина: Произошла ошибка при чтении данных из файлов Bootsmbs.nam и (или) Bootsmbs.chk.

Действие: Восстановите шаблоны КЦ структур SMBIOS и рассчитайте эталонные значения контрольных сумм.

** Структуры SMBIOS не найдены

Причина: В системе не найдены структуры SMBIOS. Возможно, они отсутствуют или доступ к ним отключен в BIOS Setup.

Действие: Выясните и устраните причину, по которой указанные структуры отсутствуют в системе или были отключены в BIOS Setup. При необходимости выполните расчет эталонных значений контрольных сумм.

** Шаблоны КЦ структур SMBIOS не найдены

Причина: Не найдены файлы Bootsmbs.nam и (или) Bootsmbs.chk.

Действие: Восстановите шаблоны КЦ структур SMBIOS и рассчитайте эталонные значения контрольных сумм.

** Шаблоны КЦ структур SMBIOS разрушены

Причина: Нарушена структура файлов Bootsmbs.nam и (или) Bootsmbs.chk.

Действие: Восстановите шаблоны КЦ структур SMBIOS и рассчитайте эталонные значения контрольных сумм.

Контроль таблиц ACPI

**** Изменилось содержимое таблиц ACPI**

Причина: Эталонное значение контрольной суммы содержимого таблиц ACPI не совпало с текущим значением контрольной суммы.

Действие: Выясните и устраните причину, из-за которой изменилось содержимое таблиц ACPI. Выполните расчет эталонных значений контрольных сумм.

**** Таблицы ACPI не найдены**

Причина: В системе не найдены таблицы ACPI. Возможно, они отсутствуют или доступ к ним отключен в BIOS Setup.

Действие: Выясните и устраните причину, по которой указанные параметры отсутствуют в системе или были отключены в BIOS Setup. При необходимости выполните расчет эталонных значений контрольных сумм.

Контроль распределения адресного пространства памяти

**** Изменилось содержимое таблицы распределения памяти**

Причина: Эталонное значение контрольной суммы таблицы адресного пространства памяти не совпало с текущим значением контрольной суммы.

Действие: Выясните и устраните причину, из-за которой изменилось распределение памяти. Выполните расчет эталонных значений контрольных сумм.

**** Таблица распределения памяти не найдена**

Причина: Не найдена таблица распределения адресного пространства памяти.

Действие: Выясните и устраните причину отсутствия таблицы распределения адресного пространства памяти.

Контроль журнала транзакций

**** Ошибка контроля журнала транзакций**

Причина: В журнале транзакций могут содержаться данные о незавершенных изменениях.

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

Сообщения об ошибках при тестировании комплекса

При обнаружении ошибок в ходе проверки работоспособности комплекса "Соболь" (см. стр. 55) на экран выводятся следующие сообщения.

Ошибки тестирования памяти платы

Тест памяти платы (банк ...) завершился с ошибкой: нет подтверждения приема данных.

Тест памяти платы (банк ...) завершился с ошибкой: считанные данные не соответствуют записанным.

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

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

Ошибки тестирования ДСЧ

Тест канала 0 ДСЧ неудачен ... раз(а) из ... попыток.

Тест канала 1 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.

Ошибки тестирования идентификатора

Ошибка чтения данных идентификатора.

Ошибка записи данных идентификатора.

Ошибка чтения номера идентификатора.

Причина: Произошла ошибка при записи/чтении данных в/из идентификатор(а). Возможно, неисправен идентификатор (iButton, eToken PRO, eToken PRO (Java), iKey 2032, Rutooken, Rutooken RF) 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 неисправен, 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, eToken PRO (Java), iKey 2032, Rutooken, Rutooken RF) 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-шаблоны КЦ
Перерасчет контрольных сумм	Администратор выполнил расчет эталонных значений контрольных сумм (см. стр. 78)
Переход в автономный режим	Администратор включил автономный режим работы комплекса (см. стр. 41)
Переход в сетевой режим	Администратор включил режим, позволяющий использовать комплекс совместно с другими средствами защиты (см. стр. 41)
Превышено число попыток входа	Количество неудачных попыток входа данного пользователя в систему превысило значение соответствующего параметра (см. стр. 27)
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, СЗИ семейства 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:



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](#).

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 СЗИ 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 СЗИ Secret Net.

Информационное окно

После нажатия клавиши <F1> на экране появится информационное окно, подобное следующему:



Окно содержит следующие сведения о комплексе "Соболь" и защищаемом компьютере:

Пункт	Вариант отображения	Пояснение
Версия кода расширения BIOS	1.0.189	Номер текущей версии кода расширения BIOS комплекса
	1.0.189 IPL	Номер текущей версии кода расширения BIOS комплекса, работающего в режиме загрузочного устройства (режим IPL)
Тип слота	Mini PCI-E PCI-E PCI	Стандарт используемой системной шины
Версия платы	8.14 — для PCI 8.15 — для PCI-E 11.2 — для Mini PCI-E 11.3 — для Mini PCI-E Half	Номер текущей версии кода ПЛИС платы
PnP тип платы	Network Adapter	Сетевая плата компьютера
Тип USB-контроллера	EHCI, UHCI UHCI, OHCI EHCI EHCI, OHCI XHCI XHCI, EHCI	USB-контроллеры компьютера

Терминологический справочник

A

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, eToken PRO (Java), iKey 2032, Rutoken, Rutoken RF, 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 программного и аппаратного обеспечения 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

Структуры SMBIOS В структурах SMBIOS содержится информация о компонентах системной платы — сведения о производителе, системной плате, процессоре, системных слотах, памяти, BIOS и др.

Считыватель Устройство, предназначенное для чтения (ввода) идентификационных признаков. В комплексе "Соболь" используются USB-считыватели Athena ASEDrive IIIe USB V2/V3 смарт-карт eToken PRO и считыватели для идентификаторов iButton

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

T

Таблицы ACPI В таблицах ACPI содержатся данные об аппаратном и программном интерфейсах, обеспечивающих учет и конфигурирование компонентов системной платы компьютера

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 семействе ОС Linux. Руководство администратора	RU.40308570.501410.001 91 2
3	Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство пользователя	RU.40308570.501410.001 92