КОД БЕЗОПАСНОСТИ

Программно-аппаратный комплекс

"Соболь". Версия 3.2

Руководство администратора

Управление шаблонами контроля целостности в семействе ОС Linux

RU.88338853.501410.021 91 2

Почтовый адрес:	**115127, Россия, Москва, а/я 66** **ООО "Код Безопасности"**
Телефон:	**8 495 982-30-20**
E-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Оглавление

Введение **4**

Установка, удаление и обновление ПО комплекса **6**

Установка программы управления шаблонами КЦ 6

Удаление программы управления шаблонами КЦ 7

Обновление программы управления шаблонами КЦ 8

Настройка механизма контроля целостности **9**

Настройка механизма КЦ с использованием графического интерфейса 9

Запуск программы управления шаблонами КЦ 9

Корректировка списков объектов КЦ 10

Формирование отчета об объектах контроля 12

Настройка механизма КЦ с использованием командной строки 13

Корректировка списка контролируемых файлов 13

Корректировка списка контролируемых секторов 14

Расчет эталонных значений контрольных сумм 15

Приложение **16**

Формат утилиты scheck 16

Сообщения об ошибках при выполнении утилиты scheck 17

Документация **19**

Введение

Данное руководство предназначено для администраторов изделия "Программно-аппаратный комплекс "Соболь". Версия 3.2" (далее — комплекс "Соболь", комплекс, ПАК "Соболь"). В нем содержатся сведения, необходимые для установки и настройки программного обеспечения (ПО) комплекса "Соболь" на компьютерах, функционирующих под управлением следующих дистрибутивов Linux:

Табл.1 Дистрибутивы Linux, поддерживаемые ПАК "Соболь"

Название дистрибутива	Версия ядра
МСВС 5.0 x64	2.6.32-358.14.1.el6
Альт Линукс 7.0 Кентавр x86/x64	3.10.32-std-def-alt1
РОСА «Никель» x32	3.14.44-nrj-desktop-pae-5rosa.lts-i586
Astra Linux Special Edition "Смоленск" 1.4 x64	3.16.0-16-generic 3.16.0-16-pax
Astra Linux 1.5	4.2.0-23-generic 4.2.0-23-pax 4.2.0-24-generic
Astra Linux 1.6	4.15.3-1
CentOS 6.5 x86/x64	2.6.32-431.el6
ContinentOS 4.2 x64	3.16.0-16
Debian 7.6 x86/x64	3.2.57-3
Mandriva РОСА "Никель" x86/x64	3.0.69-selinux-desktop-4rosa.lts
Red Hat Enterprise Linux 7.0 x64	3.10.0-123.el7
Ubuntu 14.04 LTS Desktop/Server x86/x64	3.13.0-24-generic
VMware vSphere ESXi 5.5 x64	ESXi 5.5

Основные сведения об установке, настройке и эксплуатации комплекса приводятся в документе "Программно-аппаратный комплекс "Соболь". Версия 3.2. Руководство администратора". Сведения, необходимые пользователю, содержатся в документе "Программно-аппаратный комплекс "Соболь". Версия 3.2. Руководство пользователя".

Структура руководства

Материал руководства организован следующим образом:

- раздел "Установка, удаление и обновление ПО комплекса" содержит сведения об установке, удалении и обновлении программы управления шаблонами контроля целостности (КЦ);
- в разделе "Настройка механизма контроля целостности" содержатся сведения о настройке программы управления шаблонами КЦ.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Важная и дополнительная информация оформлена в виде примечаний, начинающихся со слов **Внимание**, **Пояснение**, **Совет** и др.

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 в авторизованных учебных центрах. Перечень учебных центров и условия обучения представлены на сайте компании http://www.securitycode.ru/company/education/training- courses/ . Связаться с представителем компании по вопросам организации обучения можно по электронной почте (education@securitycode.ru).

Глава 1
Установка, удаление и обновление ПО комплекса

Программа управления шаблонами КЦ является компонентом, входящим в комплект поставки комплекса "Соболь". Программа позволяет создавать и корректировать списки объектов (файлов и секторов жестких дисков), целостность которых требуется контролировать, и сохранять эти списки в специальных файлах — шаблонах КЦ.

Пояснение. Шаблоны КЦ представляют собой служебные файлы **bootfile.nam**, **bootfile.chk**, **bootsect.nam**, **bootsect.chk**, содержащие полный путь к каждому контролируемому файлу, координаты каждого контролируемого сектора, их контрольные суммы.
Файлы-шаблоны КЦ хранятся в каталоге, имя и местоположение которого указываются в окне "Информация" программы управления шаблонами КЦ (обычно **/boot/sobol**). Для определения пути к файлам-шаблонам КЦ, используя программу эмулятора терминала, выполните команду **scheck --ls-path**.

Установка и удаление ПО комплекса осуществляется из командной строки с привилегиями системного администратора. Программное обеспечение рекомендуется устанавливать до установки в компьютер платы комплекса.

Установка программы управления шаблонами КЦ

Установка программы управления шаблонами КЦ в зависимости от используемой операционной системы (ОС) семейства Linux с помощью файла-скрипта или установочных vib-/rpm-/deb-пакетов (см. табл.2).

Табл.2 Установка программы управления шаблонами КЦ

Название дистрибутива	Архитектура	Установочный пакет
МСВС 5.0	x64	sobol-3.0.9-5.vniins5.0.x86_64.rpm
Альт Линукс 7.0 Кентавр	x86	sobol-3.0.9-5.alt7.0.4.i686.rpm
	x64	sobol-3.0.9-5.alt7.0.4.x86_64.rpm
РОСА «Никель» x32	x86	sobol-3.0.m2-2- rosa.lts2012.0_ 3.14.i686.rpm
Astra Linux Special Edition "Смоленск" 1.4	x64	sobol_3.0.9-5-astra1.4-generic_ amd64.deb sobol_3.0.9-5-astra1.4-pax_amd64.deb
Astra Linux 1.5	x64	sobol_3.0.m2-2-astra1.5_ amd64.deb
Astra Linux 1.6	x64	sobol_3.0.m2-3-astra1.6_amd64.deb
ContinentOS 4.2	x64	sobol-3.0.9-5.continentos4.x86_64.rpm
CentOS 6.5	x86	sobol-3.0.9-5.centos6.5.i686.rpm
	x64	sobol-3.0.9-5.centos6.5.x86_64.rpm
Debian 7.6	x86	sobol_3.0.9-5-debian7.6_i386.deb
	x64	sobol_3.0.9-5-debian7.6_amd64.deb
Mandriva РОСА "Никель"	x86	sobol-3.0.9-5-rosa.lts2012.0.i686.rpm
	x64	sobol-3.0.9-5-rosa.lts2012.0.x86_64.rpm
Red Hat Enterprise Linux 7.0	x64	sobol-3.0.9-5.el7.0.x86_64.rpm
Ubuntu 14.04 LTS Desktop/Server	x86	sobol_3.0.9-5-ubuntu14.04_i386.deb
	x64	sobol_3.0.9-5-ubuntu14.04_amd64.deb

Название дистрибутива	Архитектура	Установочный пакет
VMware vSphere ESXi 5.5	x64	sobol-3.0.9-5-vmw5.vib

Для установки программного обеспечения в среде ОС VMware vSphere ESXi 5.5:

1. Выключите все виртуальные машины (ВМ) на сервере ВМ, функционирующем под управлением ОС VMware vSphere ESXi 5.5 (далее — система ESXi).
2. Для копирования установочного пакета на сервер ВМ выполните команду:

   ```
   scp sobol.vib root@<ip>
   ```

   где <ip> — IP-адрес сервера ВМ.
3. Выполните SSH-соединение с сервером ВМ. Для этого:
   - загрузите систему ESXi;
   - нажмите клавишу F2;
   - введите пароль администратора (он задается при установке системы ESXi);
   - активируйте в главном меню команду "Troubleshooting Options" l "Enable SSH";
   - подключитесь к серверу ВМ посредством SSH-клиента:

   ```
   ssh <ip> -l root
   ```

   где <ip> — IP-адрес ВМ.
4. Переведите сервер ВМ в режим maintenance mode:

   ```
   vim-cmd hostsvc/maintenance_mode_enter
   ```
5. Установите vib-пакет с ПО комплекса "Соболь":

   ```
   esxcli software vib install --no-sig-check -v /sobol.vib
   ```
6. Отключите режим maintenance mode:

   ```
   vim-cmd hostsvc/maintenance_mode_exit
   ```

Результатом выполнения процедуры является развертывание на сервере виртуальных машин ПО комплекса "Соболь".

Для установки программного обеспечения в среде других ОС:

1. Поместите установочный компакт-диск в привод DVD/CD-ROM. Запустите программу эмулятора терминала. Войдите в каталог установки программы для соответствующего дистрибутива Linux.
2. В зависимости от используемого дистрибутива и архитектуры платформы (см. табл.2 на стр.**6**) выполните команду:
   - для rpm-пакетов:

   ```
   rpm -ivh <ИМЯ ПАКЕТА>
   ```

   - для deb-пакета:

   ```
   dpkg -i <ИМЯ ПАКЕТА>
   ```

Результатом выполнения команды является развертывание на компьютере ПО комплекса "Соболь" и формирование списка объектов КЦ по умолчанию.

Удаление программы управления шаблонами КЦ

В зависимости от используемого дистрибутива и архитектуры платформы (см. табл.2 на стр.**6**) для удаления программы управления шаблонами КЦ используются различные команды.

Для удаления программы в среде ОС VMware vSphere ESXi 5.5:

1. Выключите все виртуальные машины на сервере ВМ.

2. Переведите сервер ВМ в режим maintenance mode:

```
vim-cmd hostsvc/maintenance_mode_enter
```

3. Удалите vib-пакет с ПО комплекса "Соболь":

```
esxcli software vib remove --vibname=sobol
```

4. Отключите режим maintenance mode:

```
vim-cmd hostsvc/maintenance_mode_exit
```

Результатом выполнения процедуры является удаление программы управления шаблонами КЦ.

Для удаления программы в среде других ОС:

1. Для rpm-пакетов выполните команду:

```
rpm –e sobol
```

2. Для deb-пакета выполните команду:

```
dpkg --purge sobol
```

Результатом выполнения команды является удаление программы управления шаблонами КЦ, в том числе файлов-шаблонов КЦ.

Обновление программы управления шаблонами КЦ

В текущей версии комплекса "Соболь" обновление программы управления шаблонами КЦ реализуется в операционных системах МСВС 5.0, Mandriva РОСА "Никель", Альт Линукс 7.0 и CentOS 6.5.

Для обновления программы:

Выполните команду:

```
rpm –U <ИМЯ ПАКЕТА> --nopreun --nopostun
```

Результатом выполнения команды является обновление программы управления шаблонами КЦ, в том числе файлов-шаблонов КЦ.

Глава 2
Настройка механизма контроля целостности

Механизм КЦ комплекса "Соболь" обеспечивает контроль неизменности файлов и физических секторов жесткого диска (дисков) до загрузки ОС.

Для настройки механизма используется программа управления шаблонами КЦ. Программа позволяет создавать и корректировать списки файлов и секторов жестких дисков, целостность которых требуется контролировать, и сохранять эти списки в шаблонах КЦ.

Внимание. При формировании шаблонов КЦ и перед запуском процедуры расчета КЦ отключите от USB-портов компьютера все устройства класса USB Mass Storage Device (флеш-накопители, CD-, DVD-приводы и т. п.).

В комплексе "Соболь" реализованы два способа настройки механизма КЦ — с использованием графического интерфейса и командной строки.

Настройка механизма контроля целостности выполняется в следующем порядке:

- корректировка списков объектов КЦ (см. стр.**10**, стр.**13**);
- включение механизма контроля целостности, если он был отключен (см. стр.**19**, документ [1], глава 3, раздел "Контроль целостности");
- расчет эталонных значений контрольных сумм (см. стр.**15**).

Внимание. Если механизм КЦ настроен и используется на компьютере, работающем под управлением ОС семейства Linux, и были произведены операции по созданию или удалению разделов (например, с помощью программы fdisk), подлежащих КЦ с помощью комплекса "Соболь", то необходимо восстановить исходные шаблоны КЦ и рассчитать эталонные значения контрольных сумм.

Настройка механизма КЦ с использованием графического интерфейса

Запуск программы управления шаблонами КЦ

Для запуска программы:

1. Запустите программу, используя ярлык "Управление шаблонами КЦ". В зависимости от оконного менеджера ярлык размещается следующим образом:
   - ELK — "Пуск" | "Настройка" | "Панель управления ELK" | "Безопасность" | "Управление шаблонами КЦ";
   - FLY — "Настройка" | "Панель управления" | "Безопасность" | "Управление шаблонами КЦ";
   - GNOME — "Приложения" | "Системные" | "Управление шаблонами КЦ";
   - KDE (ОС Mandriva) — "Главное меню"  | "Утилиты" | "Управление шаблонами КЦ";
   - KDE, XFCE — "Система" | "Управление шаблонами КЦ".
2. В окне введите пароль системного администратора и нажмите "ОК".

   На экране появится окно программы управления шаблонами КЦ.

   Пояснение. Если программа управления шаблонами КЦ не запускается, это означает, что предыдущий сеанс работы программы не завершен. Убедитесь в наличии файла **gtk-scheck** в каталоге **/var/log**. Удалите файл и повторите процедуру запуска программы.

При отсутствии в компьютере платы комплекса "Соболь" на экране появится соответствующее предупреждение. Для продолжения работы с программой нажмите "ОК".

Корректировка списков объектов КЦ

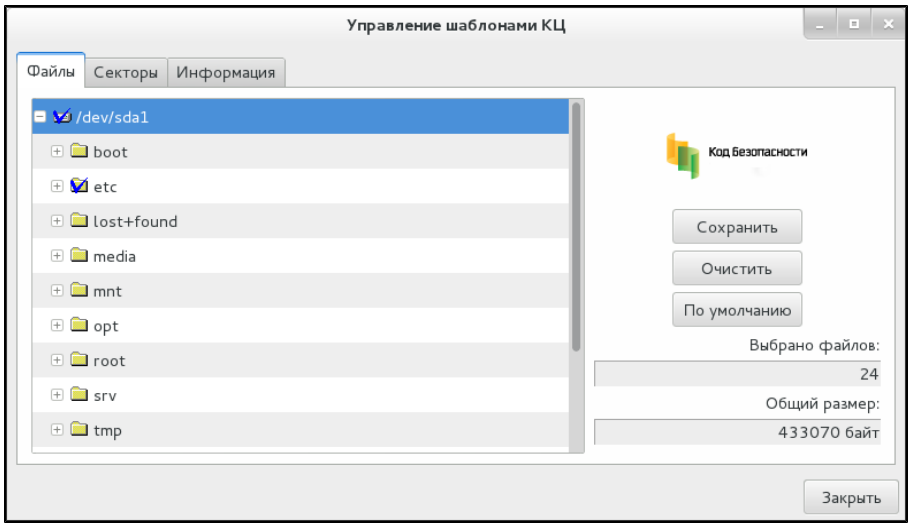
Исходные списки файлов и секторов, целостность которых требуется контролировать, создаются после установки ПО комплекса "Соболь". Корректировка списков заключается в добавлении и исключении объектов КЦ.

Пояснение. Приведенные ниже элементы интерфейса представлены в графической оболочке GNOME дистрибутива Red Hat Enterprise Linux 7.0.

Для корректировки списка файлов:

1. Запустите программу управления шаблонами КЦ (см. стр.**9**).
2. В окне программы управления шаблонами КЦ выберите вкладку "Файлы".

   В области "Файлы" появится файловая структура жесткого диска (дисков) компьютера, представленная в виде дерева:



3. Отметьте файлы, целостность которых требуется контролировать.

Внимание. Запрещается включать в список контролируемых объектов:

- файлы логических дисков, являющихся наборами томов LVM;
- файлы, размещенные на неподдерживаемых файловых системах;
- нерегулярные файлы;
- временные файлы;
- файлы, длина имени которых более 253 символов;
- файлы с именами более 8 символов, расположенные на разделах списка с файловыми системами FAT.

Для выбора/исключения файлов из выборки используйте следующие способы.

- Для выбора/исключения файла из выборки совместите указатель с пиктограммой (или) и нажмите правую кнопку мыши.

  Совет. Для выбора расположенных подряд нескольких файлов выделите нажатием левой кнопки мыши имя первого из выбираемых файлов. Затем, удерживая нажатой клавишу <Shift>, совместите указатель с пиктограммой (но не именем) последнего из выбираемых файлов и нажмите правую кнопку мыши. Пиктограмма последнего из выбираемых файлов не должна содержать отметку. При выделении нескольких файлов, исключаемых из выборки, файл, завершающий ряд, должен быть отмечен.

- Для выбора/исключения файлов, содержащихся на диске или в каталоге и во всех его подкаталогах, подведите указатель к пиктограмме ( ) или ( ) и нажмите правую кнопку мыши.

- Для задания списка выбранных файлов по умолчанию нажмите кнопку "По умолчанию" и подтвердите свое решение, нажав кнопку "Да" в появившемся на экране окне запроса. В этом случае в выборку войдут только те файлы, которые включаются в шаблон для контроля целостности файлов по умолчанию.
- Для удаления всех отметок нажмите "Очистить" и подтвердите свое решение, нажав "Да" в появившемся на экране окне запроса.

4. Завершив выбор файлов, нажмите кнопку "Сохранить".

   В появившемся на экране окне запроса нажмите кнопку:
   - "Да" — чтобы сохранить изменения и перезаписать файл-шаблон;
   - "Нет" — для отказа от сохранения изменений.
5. Нажмите кнопку "Закрыть" для завершения работы с программой.

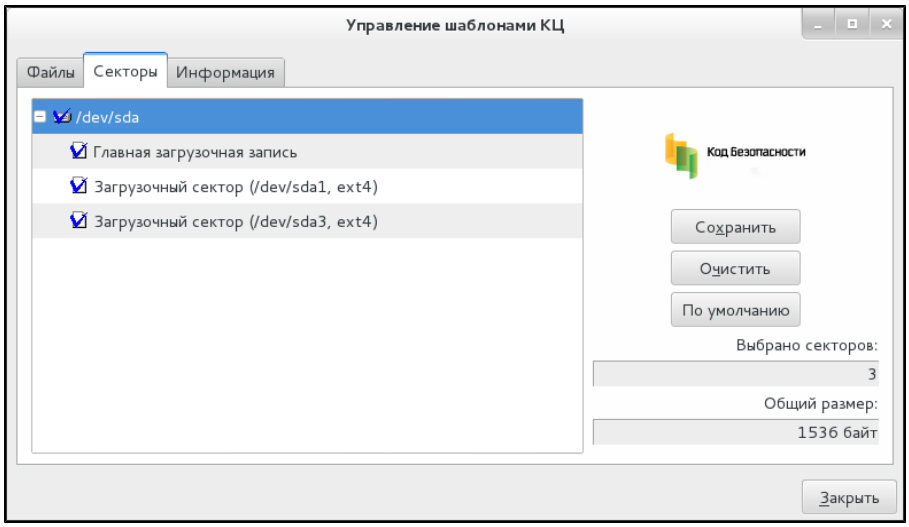
Список выбранных файлов сохранится в файле **bootfile.nam**.

Внимание. После корректировки списка файлов выполните расчет эталонных значений контрольных сумм (см. стр.15).

Для корректировки списка контролируемых секторов:

1. Запустите программу управления шаблонами КЦ (см. стр.9).
2. В окне программы управления шаблонами КЦ выберите вкладку "Секторы".

   В области "Секторы" появится структура жесткого диска (дисков):



3. Отметьте секторы, целостность которых требуется контролировать.

   Для выбора/исключения секторов из выборки используйте следующие способы.
   - Для выбора/исключения сектора из выборки совместите указатель с пиктограммой (или) и нажмите правую кнопку мыши.

     Совет. Для выбора/исключения из выборки всех секторов жесткого диска или его раздела совместите указатель с пиктограммой ( ) или ( ) и нажмите правую кнопку мыши.
   - Для восстановления исходного шаблона нажмите кнопку "По умолчанию" и подтвердите свое решение, нажав кнопку "Да" в появившемся на экране окне запроса. В этом случае в выборку будут включены все имеющиеся секторы.
   - При необходимости удаления всех отметок нажмите кнопку "Очистить" и подтвердите свое решение, нажав кнопку "Да" в появившемся на экране окне запроса.
4. Завершив выбор секторов, нажмите кнопку "Сохранить".

   В появившемся на экране окне запроса нажмите кнопку:
   - "Да" — чтобы сохранить изменения и перезаписать файл-шаблон;

- "Нет" — для отказа от сохранения изменений.

5. Нажмите кнопку "Закрыть" для завершения работы с программой.

Список выбранных секторов сохранится в файле **bootsect.nam**.

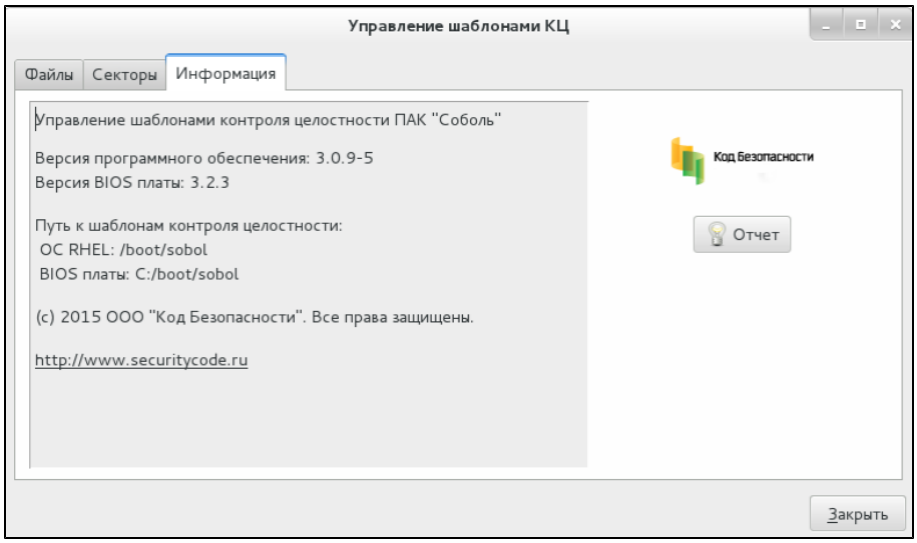
Внимание. После корректировки списка секторов выполните расчет эталонных значений контрольных сумм (см. стр.15).

Формирование отчета об объектах контроля

Для формирования отчета:

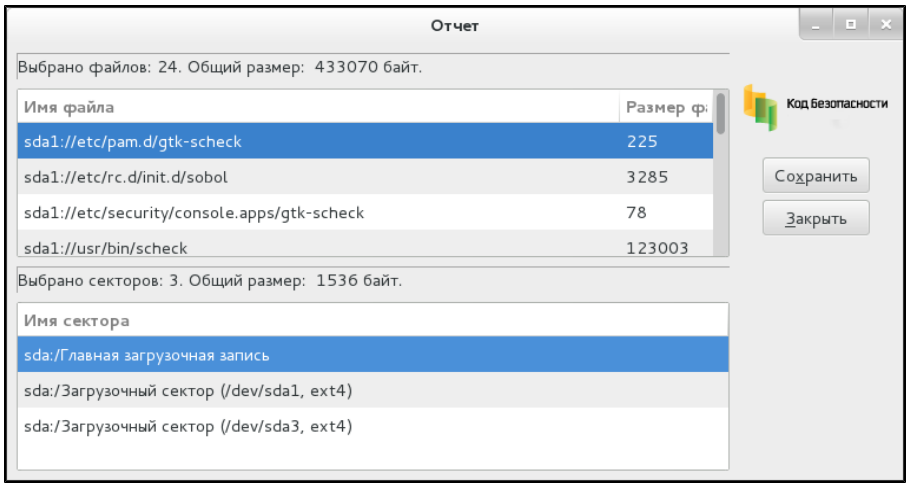
1. Запустите программу управления шаблонами КЦ (см. стр.9).
2. В окне программы управления шаблонами КЦ выберите вкладку "Информация".

   Диалог "Информация" позволяет ознакомиться с данными о программе управления шаблонами КЦ:



3. Нажмите кнопку "Отчет".

   На экране появится следующее окно:



4. Нажмите кнопку "Сохранить" для сохранения отчета в файле.
5. В появившемся на экране диалоге укажите каталог, в котором будет сохранен файл, имя файла и его формат. Затем нажмите кнопку "Сохранить".
6. Для завершения работы с отчетом нажмите кнопку "Закрыть".

Настройка механизма КЦ с использованием командной строки

Формат утилиты управления шаблонами КЦ **scheck** приводится на стр.**16**.

Корректировка списка контролируемых файлов

Утилита **scheck** предоставляет возможность добавления файлов в список КЦ и их исключения двумя способами — по одному файлу и списком.

Для добавления/исключения одного файла:

1. Для добавления файла выполните команду:

   ```
   scheck --add-file <ПУТЬ><ФАЙЛ>
   ```

   где <ПУТЬ> — путь к файлу, <ФАЙЛ> — имя файла.

   Пример 1. Необходимо поставить на КЦ файл **sshd_config**, находящийся в каталоге **bin** в разделе sda3 с точкой монтирования mnt. В этом случае команда имеет следующий формат:

   ```
   scheck --add-file /mnt/bin/sshd_config
   ```

   или

   ```
   scheck --add-file sda3:/bin/sshd_config
   ```

2. Для исключения файла выполните команду:

   ```
   scheck --rm-file <ПУТЬ><ФАЙЛ>
   ```

   где <ПУТЬ> — путь к файлу, <ФАЙЛ> — имя файла.

   Пример 2. Необходимо исключить из выборки контролируемый файл **sshd_config**, находящийся в каталоге **bin** в разделе sda3 с точкой монтирования mnt. В этом случае команда имеет следующий формат:

   ```
   scheck --rm-file /mnt/bin/sshd_config
   ```

   или

   ```
   scheck --rm-file sda3:/bin/sshd_config
   ```

3. Для исключения несуществующего файла выполните команду:

   Пояснение. Под несуществующим понимается файл, удаленный с диска компьютера, но оставленный в шаблоне КЦ.

   ```
   scheck --rm-file <ПУТЬ><ФАЙЛ>
   ```

   где <ПУТЬ> — путь к несуществующему файлу с обязательным указанием имени логического диска, на котором он располагался, <ФАЙЛ> — имя несуществующего файла.

   Пример 3. Необходимо исключить из шаблона КЦ несуществующий файл **sshd_config**, который располагался в каталоге **bin** на диске C: компьютера. В этом случае сначала выполните команду вывода на экран списка контролируемых файлов:

   ```
   scheck --ls-files
   ```

   затем выясните правильный путь к файлу **sshd_config** и исключите его из списка:

   ```
   scheck --rm-file C:/bin/sshd_config
   ```

Для добавления/исключения файлов списком:

1. Для добавления файлов выполните команду:

   ```
   scheck --add-ls-files <ПУТЬ><ФАЙЛ>
   ```

   где <ПУТЬ> — путь к файлу, <ФАЙЛ> — имя текстового файла, содержащего список включаемых на КЦ файлов.

Для составления списка в каждой строке текстового файла необходимо указать <ПУТЬ><ФАЙЛ>, где <ПУТЬ> — путь к добавляемому файлу, <ФАЙЛ> — имя файла.

2. Для исключения файлов выполните команду:

```
scheck --rm-ls-files <ПУТЬ><ФАЙЛ>
```

где <ПУТЬ> — путь к файлу, <ФАЙЛ> — имя текстового файла, содержащего список исключаемых из КЦ файлов.

Список исключаемых файлов формируется аналогично списку добавляемых файлов.

Внимание. После корректировки списка файлов выполните расчет эталонных значений контрольных сумм (см. стр.15).

Корректировка списка контролируемых секторов

Утилита **scheck** предоставляет возможность добавления секторов в список КЦ и их исключения двумя способами — по одному сектору и списком.

Внимание. В системе ESXi формат отображения секторов имеет следующий вид: t10.ATA_____ WDC_WD5000AAKX2D001CA0_____WD2DWCAYUHH63857:0.

Для добавления/исключения одного сектора:

1. Для добавления сектора выполните команду:

```
scheck --add-sector <УСТРОЙСТВО>:<НОМЕР>
```

где <УСТРОЙСТВО> — имя диска (или раздела диска), на котором находится добавляемый сектор, <НОМЕР> — номер сектора на диске (или номер сектора внутри раздела диска). Нумерация секторов начинается с 0.

Пример 4. Необходимо добавить на КЦ загрузочный сектор устройства **sda**. В этом случае команда имеет следующий формат:

```
scheck --add-sector sda:0
```

2. Для исключения сектора выполните команду:

```
scheck --rm-sector <УСТРОЙСТВО>:<НОМЕР>
```

где <УСТРОЙСТВО> — имя диска (или раздела диска), на котором находится исключаемый сектор, <НОМЕР> — номер сектора на диске (или номер сектора внутри раздела диска). Нумерация секторов начинается с 0.

Пример 5. Необходимо исключить из выборки контролируемый первый сектор раздела КЦ **sda3**. В этом случае команда имеет следующий формат:

```
scheck --rm-sector sda3:0
```

3. Для исключения несуществующего сектора выполните команду:

```
scheck --rm-sector <УСТРОЙСТВО>:<НОМЕР>
```

где <УСТРОЙСТВО> — номер физического диска в шестнадцатеричном представлении, на котором находится исключаемый сектор, <НОМЕР> — номер сектора на диске. Нумерация секторов начинается с 0.

Пример 6. Необходимо исключить из шаблона КЦ первый сектор несуществующего диска 0x81. В этом случае сначала выполните команду вывода на экран списка контролируемых секторов:

```
scheck --ls-sectors
```

затем найдите в списке требуемый сектор и исключите его из шаблона КЦ:

```
scheck --rm-sector 0x81:0
```

Для добавления/исключения секторов списком:

1. Для добавления секторов выполните команду:

   ```
   scheck --add-ls-sectors <ПУТЬ><ФАЙЛ>
   ```

   где <ПУТЬ> — путь к файлу, <ФАЙЛ> — имя текстового файла, содержащего список включаемых на КЦ секторов.

   Для составления списка в каждой строке текстового файла необходимо указать <УСТРОЙСТВО>:<НОМЕР>, где <УСТРОЙСТВО> — имя диска (или раздела диска), на котором находится добавляемый сектор, <НОМЕР> — номер сектора на диске (или номер сектора внутри раздела диска).

2. Для исключения секторов выполните команду:

   ```
   scheck --rm-ls-sectors <ПУТЬ><ФАЙЛ>
   ```

   где <ПУТЬ> — путь к файлу, <ФАЙЛ> — имя текстового файла, содержащего список исключаемых из КЦ файлов.

   Список исключаемых секторов формируется аналогично списку добавляемых секторов.

Внимание. После корректировки списка секторов выполните расчет эталонных значений контрольных сумм (см. стр.15).

Расчет эталонных значений контрольных сумм

После корректировки списков объектов КЦ и их сохранения в файлах-шаблонах необходимо рассчитать эталонные значения контрольных сумм.

Для расчета контрольных сумм:

1. Перезагрузите компьютер (или сервер виртуальных машин) и войдите в систему с правами администратора комплекса "Соболь" (см. стр. **19**, документ [1], глава 3, раздел "Общий порядок настройки").
2. Включите механизм контроля целостности (см. стр.**19**, документ [1], глава 3, раздел "Контроль целостности").
3. В меню администратора 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. После того как все выявленные недостатки будут устранены, повторите процедуру расчета эталонных значений контрольных сумм. Подробный список сообщений об ошибках содержится в приложении документа [1].

Приложение

Формат утилиты scheck

Утилита управления шаблонами КЦ **scheck** имеет следующий формат:
scheck [ключ] [аргумент].

Ключ	Назначение	Аргумент	Примечание
--help (-h)	Вывод на экран справки программы	Отсутствует	
--version (-V)	Вывод на экран версии программы	Отсутствует	
--verbose (-v)	Вывод на экран сообщений о работе программы	Отсутствует	Не функционирует в среде ОС VMware vSphere ESXi 5.5
--ls-path	Вывод на экран пути к файлам-шаблонам в формате DOS	Отсутствует	
--ls-drives	Вывод на экран информации об используемых устройствах и разделах	Отсутствует	
--ls-files	Вывод на экран списка файлов, поставленных на КЦ	Отсутствует	
--ls-sectors	Вывод на экран списка секторов, поставленных на КЦ	Отсутствует	
--add-file	Добавление файла в список файлов, поставленных на КЦ	<ПУТЬ><ФАЙЛ>	<ПУТЬ> — путь к файлу. <ФАЙЛ> — имя файла
--rm-file	Исключение файла из списка контролируемых файлов		
--add-sector	Добавление сектора в список секторов, поставленных на КЦ	<УСТРОЙСТВО>:<НОМЕР>	<УСТРОЙСТВО> — имя диска (или раздела диска), на котором находится добавляемый/исключаемый сектор. <НОМЕР> — номер сектора на диске (или номер сектора внутри раздела диска)
--rm-sector	Исключение сектора из списка контролируемых секторов		
--add-ls-files	Добавление файлов, указанных в текстовом файле, в список контролируемых файлов	<ПУТЬ><ФАЙЛ>	<ПУТЬ> — путь к текстовому файлу. <ФАЙЛ> — имя текстового файла, содержащего список контролируемых файлов или секторов
--rm-ls-files	Исключение файлов, указанных в текстовом файле, из списка контролируемых файлов		
--add-ls-sectors	Добавление секторов, указанных в текстовом файле, в список контролируемых секторов		
--rm-ls-sectors	Исключение секторов, указанных в текстовом файле, из списка контролируемых секторов		
--clear-files	Очистка списка файлов, поставленных на КЦ	Отсутствует	
--reset-files	Восстановление списка контролируемых файлов по умолчанию	Отсутствует	

Ключ	Назначение	Аргумент	Примечание
--clear-sectors	Очистка списка секторов, поставленных на КЦ	Отсутствует	
--reset-sectors	Восстановление списка контролируемых секторов по умолчанию	Отсутствует	

Сообщения об ошибках при выполнении утилиты scheck

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

Пояснение. В системе ESXi сообщения об ошибках выводятся на английском языке.

```
Неверный ключ
```

```
scheck: (null) is invalid option
```

Причина: В записи команды **scheck** неправильно указан или отсутствует обязательный ключ.

Действие: Исправьте или добавьте необходимый ключ. Информация о формате команды приводится на стр.**16**.

```
Ошибка при добавлении файла:
файл <ПУТЬ><ФАЙЛ> не найден
```

```
Error adding file to integrity check templates:
file <PATH><FILE> is not found
```

Причина: При добавлении файла на КЦ могут быть неправильно указаны путь к файлу, его имя или файл, не поддерживаемый механизмом КЦ ПАК "Соболь".

Действие: Выясните причину появления ошибки, укажите правильный путь к файлу.

```
Ошибка при добавлении файла:
файл <ПУТЬ><ФАЙЛ> уже поставлен на контроль целостности
```

```
Error adding file to integrity check templates:
file <PATH><FILE> is already in templates
```

Причина: При добавлении файла на КЦ был выбран файл, ранее установленный на контроль.

Действие: При необходимости повторите добавление файла, указав другой файл.

```
Ошибка при удалении файла:
файл <ПУТЬ><ФАЙЛ> не найден
```

```
Error removing file from integrity check templates:
file <PATH><FILE> is not in templates
```

Причина: При исключении файла из списка контролируемых объектов могут быть неправильно указаны путь к файлу, его имя или несуществующий файл.

Действие: Выясните и устраните причину появления ошибки. Если в шаблоне указан несуществующий файл, исключите его из списка контролируемых файлов (см. стр.**13**).

```
Ошибка при добавлении файлов по списку:
файл-список <ПУТЬ><ФАЙЛ> не найден
```

```
Error adding files list to integrity check templates:
file <PATH><FILE> is not found
```

Причина: При добавлении файлов на КЦ по списку могут быть неправильно указаны путь к текстовому файлу со списком контролируемых файлов, имя файла-списка.

Действие: Выясните и устраните причину появления ошибки.

```
Ошибка при удалении файлов по списку:
файл-список <ПУТЬ><ФАЙЛ> не найден
```

```
Error removing files list from integrity check templates:
file <PATH><FILE> is not found
```

Причина: При исключении контролируемых файлов по списку могут быть неправильно указаны путь к текстовому файлу со списком контролируемых файлов, имя файла-списка.

Действие: Выясните и устраните причину появления ошибки.

```
Ошибка при добавлении сектора:
сектор <УСТРОЙСТВО>:<НОМЕР> не найден
```

```
Error adding sector to integrity check templates:
sector <DEVICE>:<NUMBER> is not found
```

Причина: При добавлении сектора на КЦ могут быть неправильно указаны имя диска (или раздела диска), номер сектора на диске (или номер сектора внутри раздела).

Действие: Выясните и устраните причину появления ошибки.

```
Ошибка при добавлении сектора:
сектор <УСТРОЙСТВО>:<НОМЕР> уже поставлен на контроль
целостности
```

```
Error adding sector to integrity check templates:
sector <DEVICE>:<NUMBER> is already in templates
```

Причина: При добавлении сектора на КЦ был выбран сектор, ранее установленный на контроль.

Действие: При необходимости повторите добавление сектора, указав другой сектор.

```
Ошибка при удалении сектора:
сектор <УСТРОЙСТВО>:<НОМЕР> не найден
```

```
Error adding sector to integrity check templates:
sector <DEVICE>:<NUMBER> is not found
```

Причина: При исключении сектора из списка контролируемых секторов могут быть неправильно указаны имя диска (или раздела диска), номер сектора на диске (или номер сектора внутри раздела) или несуществующий сектор.

Действие: Выясните и устраните причину появления ошибки. Если в шаблоне указан несуществующий сектор, удалите его из списка контролируемых секторов (см. стр.**14**).

```
Ошибка при добавлении секторов по списку:
файл-список <ПУТЬ><ФАЙЛ> не найден
```

```
Error adding sectors list to integrity check templates:
file <PATH><FILE> is not found
```

Причина: При добавлении секторов на КЦ по списку могут быть неправильно указаны путь к текстовому файлу со списком контролируемых секторов, имя файла-списка.

Действие: Выясните и устраните причину появления ошибки.

```
Ошибка при удалении секторов по списку:
файл-список <ПУТЬ><ФАЙЛ> не найден
```

```
Error removing sectors list from integrity check templates:
file <PATH><FILE> is not found
```

Причина: При исключении контролируемых секторов по списку могут быть неправильно указаны путь к текстовому файлу со списком контролируемых секторов, имя файла-списка.

Действие: Выясните и устраните причину появления ошибки.

Документация

1	Программно-аппаратный комплекс "Соболь". Версия 3.2. Руководство администратора	RU.88338853.501410.021 91 1
2	Программно-аппаратный комплекс "Соболь". Версия 3.2. Руководство администратора. Управление шаблонами контроля целостности в семействе ОС Linux	RU.88338853.501410.021 91 2
3	Программно-аппаратный комплекс "Соболь". Версия 3.2. Руководство пользователя	RU.88338853.501410.021 92
4	Программно-аппаратный комплекс "Соболь". Версия 3.2. Правила применения (исполнение 1)	RU.88338853.501410.021 ПП 1
5	Программно-аппаратный комплекс "Соболь". Версия 3.2. Правила применения (исполнение 2)	RU.88338853.501410.021 ПП 2