Программно-аппаратный комплекс "Соболь". Версия 3.1

Комментарии к версии 3.1.3 кода расширения BIOS платы, версиям программного обеспечения 2.0.109 для ОС семейства MS Windows и 3.0.9-5 для ОС семейства Linux

Данный документ содержит описание новых возможностей продукта "Программно-аппаратный комплекс "Соболь". Версия 3.1" (далее — ПАК "Соболь") версии 3.1.3 кода расширения BIOS платы по сравнению с версией 1.0.180. В документ также включены сведения об особенностях и ограничениях, которые необходимо учитывать при эксплуатации комплекса.

Оглавление

1. Комплект поставки ПО и документации

1.1. Размещение файлов на компакт-диске

Каталог	Содержимое
\Documentation\	Комплект документации в формате PDF
\Setup\Windows\	Дистрибутив ПО ПАК "Соболь" для ОС MS Windows
\Setup\Linux\	Дистрибутивы ПО ПАК "Соболь" для семейства ОС Linux
\Tools\	Дополнительное ПО
SblAutorun.exe	Файлы для автоматического запуска с компакт-диска для ОС MS Windows
SblAutorun.ini	
Autorun.inf	

2. Изменения и новые возможности

2.1. Плата

1. Реализована поддержка новой платы Mini PCI-E Half.

2.2. Версия ПЛИС 12.3

2. Версия ПЛИС 12.3 (Mini PCI-E Half) функционально не отличается.

2.3. Версия 2.0.109 ПО для ОС MS Windows

3. Изменен каталог установки ПО по умолчанию.

4. Переход на новую версию библиотеки BCGControlBar Pro.

5. Добавлена поддержка новой платы формфактора Mini PCI-E Half.

6. Изменено лицензионное соглашение.

2.4. Версия 3.0.9-5 ПО для ОС семейства Linux

7. Разработаны новые пакеты для операционных систем МСВС 5.0 (для ядра 2.6.32-358.14.1.el6), Альт Линукс 7.0 Кентавр (для ядра 3.10.32-std-def-alt1), Astra Linux Special Edition "Смоленск" 1.4 (для ядра 3.16.0-16–generic, 3.16.0-16-pax), CentOS 6.5 (2.6.32-431.el6), Debian 7.6 (3.2.57-3), Mandriva ROSA "Никель" (для ядра 3.0.69-selinux-desktop-4rosa.lts), Red Hat Enterprise Linux 7.0 (3.10.0-123.el7), Ubuntu 14.04 LTS (3.13.0-24-generic), VMware vSphere ESXi 5.5 (ESXi 5.5).

8. Добавлена поддержка новой платы формфактора Mini PCI-E Half.

2.5. Версия 3.1.3 кода расширения BIOS

9. Добавлена поддержка новой платы формфактора Mini PCI-E Half.

10. Добавлена поддержка работоспособности на платформах Bay Trail (в связи с наличием в них официально признанной ошибки при переключении видеорежимов).

3. Информация о совместимости

11. В эксплуатационную документацию добавлена информация о поддержке операционных систем МСВС 5.0 (для ядра 2.6.32-358.14.1.el6), Альт Линукс 7.0 Кентавр (для ядра 3.10.32-std-def-alt1), Astra Linux Special Edition "Смоленск" 1.4 (для ядра 3.16.0-16–generic, 3.16.0-16-pax), CentOS 6.5 (2.6.32-431.el6), Debian 7.6 (3.2.57-3), Mandriva ROSA "Никель" (для ядра 3.0.69-selinux-desktop-4rosa.lts), Red Hat Enterprise Linux 7.0 (3.10.0-123.el7), Ubuntu 14.04 LTS (3.13.0-24-generic), VMware vSphere ESXi 5.5 (ESXi 5.5).

12. ПО ПАК "Соболь" для ОС MS Windows совместимо с программами управления АПКШ "Континент" 3.x.

13. ПО ПАК "Соболь" для ОС MS Windows совместимо с СКЗИ "КриптоПро CSP" версий 2.x (32-разрядный вариант) и 3.x (32- и 64-разрядный варианты).

4. Особенности работы и ограничения

4.1. Общие

14. При формировании шаблонов КЦ перед запуском процедур расчета и проверки контрольных сумм необходимо отключить от USB-портов компьютера все устройства класса USB Mass Storage Device (flash-накопители, CD-, DVD-приводы и т. п.).

15. ПО ПАК "Соболь" для ОС VMware vSphere ESXi 5.5 не поддерживает совместную работу с RAID-контроллером.

4.2. Установка и удаление ПО ПАК "Соболь" для ОС MS Windows

16. ПО устанавливается в каталог %ProgramFiles%\Sobol.

17. Файлы шаблонов КЦ всегда располагаются в каталоге \Sobol на первом логическом диске в системе (как правило, C:\Sobol или D:\Sobol).

18. При включенном в Windows режиме User Account Control (UAC) невозможна установка ПО ПАК "Соболь" с помощью MSI-файла (необходимо запустить Setup.exe).

19. На компьютере, функционирующем под управлением MS Windows Server 2008 x32/x64, необходимо обновить Kernel Mode Driver Framework Runtime (%SYSTEMROOT%\ System32\Drivers\Wdf01000.sys) на версию 1.9 (пакет обновления размещается на диске поставки в каталоге \Tools\Microsoft\Kernel Mode Driver Framework v1.9) или более новую. При этом должна быть запущена служба обновления Windows, после обновления необходимо перезагрузить компьютер.

20. По умолчанию ПО ПАК «Соболь устанавливается в каталог %Program Files%\Sobol, при обновлении – в каталог %Program Files%\Infosec\Sobol.

21. Для корректной совместной работы ПАК "Соболь" и СКЗИ "КриптоПро CSP" 3.6 в операционной системе MS Windows (64-разрядный вариант) необходимо добавить в системный реестр HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\AppPath\snellock64.dll и %SystemRoot%\System32\snellock64.dll.

22. После удаления ПО при установленной плате ПАК в системе остается драйвер платы.

4.3. Программа управления шаблонами КЦ для ОС MS Windows

23. В случае изменения конфигурации физических дисков в системе (например, создания или удаления раздела) перед работой с программой требуется перезагрузка компьютера.

4.4. Установка и удаление ПО ПАК "Соболь" для ОС семейства Linux

24. Файлы шаблонов КЦ всегда располагаются в каталоге /boot/sobol на первом логическом диске в системе (как правило, C:/boot/sobol).

4.5. Программа управления шаблонами КЦ для ОС семейства Linux

25. Отсутствует поддержка дисков с GUID Partition Table (GPT).

26. Не поддерживается обработка флагов ядра Linux файловой системы ext4:

- EXT4_FEATURE_INCOMPAT_LARGEDIR
- EXT4_FEATURE_INCOMPAT_INLINE_DATA

27. Не поддерживается контроль целостности PCI-устройств и структур SMBIOS компьютера.

28. Не поддерживается контроль целостности следующих ресурсов:

- нерегулярные файлы (символьные ссылки, файлы устройств и т. д.);
- временные файлы;
- файлы, длина имени и пути к которым превышает 126 символов (для файловых систем EXT2, EXT3, EXT4);
- файлы, длина имени которых превышает 253 символа;
- файлы, длина имени и пути к которым превышает 249 символов (в ОС FreeBSD для файловых систем UFS, UFS2);
- в ОС VMware vSphere ESXi 5.5 файлы с длинными именами (имена в формате, отличном от "8.3"), расположенных на дисках с файловой системой FAT16 или FAT32;
- в ОС VMware vSphere ESXi 5.5 файлы с именами, содержащими символы кириллицы;
- файлы, расположенные на дисках с неподдерживаемыми файловыми системами (JFS, ReiserFS и т. д.);
- файлы, расположенные на дисках с виртуальными файловыми системами и дисках, являющихся наборами томов LVM.
- файлы, расположенные на дисках за пределами 3 ТБ на файловой системе ext4.

29. Не поддерживается контроль целостности ресурсов при включенном механизме предварительного связывания динамических библиотек prelink.

30. Контроль целостности объектов файловых систем EXT2, EXT3, EXT4 с именами, содержащими символы кириллицы, обеспечивается только в кодировке UTF8.

31. Если при наличии в системе нескольких физических дисков во время расчета контрольных сумм возникают ошибки поиска соответствующих файлов, то может помочь выполнение следующих рекомендаций:

- использование конфигураций с одним физическим диском в системе;

- использование в системе только физических дисков SATA;
- установка в BIOS Setup системного физического диска в качестве основного загрузочного диска;
- неиспользование мультизагрузчиков с возможностью загрузки нескольких ОС.

32. В ОС VMware vSphere ESXi 5.5 контроль целостности поддерживается лишь в том случае, если в системе присутствуют не более двух жестких дисков, причем возможен контроль лишь ресурсов с системного диска, расположенных на разделах /scratch, /bootbank, /altbootbank, /store.

33. После удаления ПО для ОС VMware vSphere ESXi 5.5 в системе остаются файлы–шаблоны для контроля целостности.

34. Для корректной работы программы управления шаблонами КЦ в ОС Astra Linux Special Edition "Смоленск" 1.4 необходимо установить библиотеку libglade.

4.6. Код расширения BIOS

35. В серверах HP Proliant поколения Gen8 не поддерживается совместная работа с встроенным RAID-контроллером HP Dynamic Smart Array B320i. Для корректной работы ПАК "Соболь" необходимо использовать другую модель RAID-контроллера или отказаться от использования RAID. При использовании RAID-контроллера HP Dynamic Smart Array P420 необходимо, чтобы в настройках BIOS Setup -> Boot Controller Order пункт "HP Smart Array 420" был не на первом месте.

36. Для корректной работы ПАК "Соболь" с RAID-контроллерами не рекомендуется после инициализации ПАК изменять параметры RAID-массива.

37. Для корректной работы ПАК "Соболь" рекомендуется использовать следующие значения параметров BIOS Setup:

- Boot to Network (Enabled);
- PXE boot to LAN (Enabled);
- Launch PXE OpROM (Enabled);
- Slot Security (Enabled);
- Lan Option ROM (Enabled).
- UEFI Boot (Disabled);
- CSM Support (Enabled/Legacy Only);
- Secure Boot -> OS Type (Other OS).

38. При наличии поддержки технологии UEFI для корректной работы ПАК "Соболь" необходимо в настройках BIOS Setup отключить загрузку EFI-Shell (или других приложений стандарта EFI/UEFI) или, по крайней мере, поставить EFI-Shell не на первое место в параметрах задания приоритетности загрузочных устройств. Кроме того, необходимо использовать механизм сторожевого таймера.

39. При наличии поддержки технологии UEFI для корректной работы ПАК "Соболь" операционная система должна быть установлена на диск с Master Boot Record (MBR).

40. Если каталог с файлами шаблонов КЦ не найден или в этом каталоге отсутствуют файлы шаблонов, то параметрам "Контроль файлов и секторов", "Контроль элементов реестра" и "Контроль PCI-устройств" и "Контроль SMBIOS" присваивается значение "Нет". Для включения контроля целостности файлов, секторов, элементов реестра и конфигурации компьютера укажите точный путь к каталогу с файлами шаблонов КЦ, который отображается:

- в строке "Путь к шаблонам контроля целостности" окна "О программе" для ОС Windows;
- в строке "BIOS платы" окна "Информация" для ОС Linux с графической оболочкой;
- в результате выполнения команды scheck --ls-path для ОС Linux.

41. Для корректной работы с файлами шаблонов КЦ на жестком диске необходимо отключить в BIOS Setup режим "Hard Disk Write Protect" (если такой режим присутствует).

42. При задании пути к файлам шаблонов КЦ для FAT не поддерживается возможность задания путей в длинном виде.

43. Для корректной работы контроля целостности необходимо чтобы первый раздел на жестком диске был основным (primary), а не расширенным (extended).

44. При выполнении расчета эталонов и контроля целостности файлов с длинными именами на FAT32 отображаются короткие имена файлов.

45. Не поддерживается контроль целостности ресурсов более чем для 32 логических дисков.

46. Не поддерживается контроль целостности ресурсов, расположенных на дисках с файловыми системами exFAT и ReFS.

47. Не поддерживается возможность контроля целостности секторов, расположенных на диске за пределами 2 ТБ.

48. Не поддерживается возможность контроля целостности файлов, полный путь которых (в коротком виде) превышает 253 символа (в ОС Windows для файловых систем FAT16, FAT32).

49. Не поддерживается возможность контроля целостности файлов, полный путь которых (в коротком виде) превышает 209 символов (в ОС Windows для файловых систем NTFS).

50. Не поддерживается контроль целостности файлов, расположенных на динамических и виртуальных дисках.

51. Не поддерживается контроль целостности объектов файловых систем UFS, UFS2 с именами, содержащими символы кириллицы.

52. Размер блока данных (кластера) для файловых систем EXT2, EXT3, EXT4, NTFS не должен превышать 4 КБ.

53. Не допускается использование символьных ссылок и жестких ссылок в файловой системе NTFS (NTFS Symbolic Link и NTFS Hardlink) и точек соединения ОС Windows (Windows Junction Point).

54. Не допускается преобразовывать диски, на которых располагается каталог (по умолчанию C:\Sobol), содержащий служебные файлы механизма контроля целостности, криптографическими программами (BestCrypt или аналогичными), программами сжатия дисков (Drivespace и аналогичными) и т. п.

55. Не поддерживается контроль целостности файлов, расположенных на разделах (томах) с файловой системой NTFS, для которых установленная и настроенная операционная система поддерживает возможность различения регистра символов имен файлов.

56. При использовании механизма сторожевого таймера невозможен выход компьютера из спящих режимов вида ACPI STR (Suspend To RAM). При выходе из спящего режима компьютер будет перезагружен. Во избежание потери данных не рекомендуется использовать указанные варианты спящих режимов.

57. При использовании в ОС MS Windows режима гибернации системой могут вноситься изменения в загрузочные секторы разделов дисков. В этом случае при восстановлении сеанса работы ПАК "Соболь" может фиксировать ошибки контроля целостности соответствующих областей, если они установлены на контроль.

58. При расчете эталонов и проверке целостности имена файлов и каталогов из ОС Linux, содержащих символы кириллицы, отображаются некорректно.

59. При обновлении кода расширения BIOS платы для файлов, расположенных на дисках с файловой системой FAT16 и FAT32, длинные имена нужно указывать в коротком виде, например pci-m~1.bin.

4.7. Плата ПАК "Соболь"

60. Не поддерживается корректное функционирование ПАК "Соболь" на некоторых моделях материнских плат (см. таблицу совместимости на сайте компании по ссылке).

Между тем, в некоторых случаях может помочь вариант старта ПАК "Соболь" в режиме загрузочного устройства (Initial Program Load или IPL) при условии обязательного использования механизма сторожевого таймера.

Для использования ПАК «Соболь» в режиме IPL должны быть предусмотрены и приняты меры, обеспечивающие невозможность модификации (через boot- меню, утилиту BIOS Setup или каким-либо другим способом) порядка загрузки операционной системы с загрузочных устройств любыми субъектами, кроме администратора.

61. Для корректной работы ПАК "Соболь" с некоторыми моделей материнских плат требуется обновление их BIOS.

62. Для использования механизма сторожевого таймера инициализацию изделия следует производить с подключенным кабелем. Если инициализация была произведена без подключения кабеля механизма сторожевого таймера, последующее подключение кабеля в рабочем режиме может приводить к циклическим перезагрузкам компьютера.

4.8. Особенности работы с USB-идентификаторами

63. При включенном режиме поддержки USB-идентификаторов 2.0 не поддерживается загрузка с USB-устройств.

64. При включенном режиме поддержки USB-идентификаторов 2.0 при использовании USB-клавиатуры:

- во время сеанса работы с ПАК "Соболь" не действует комбинация клавиш "Ctrl-Alt-Del";
- во время сеанса работы с ПАК "Соболь" отсутствует возможность ввода символов кириллицы;
- во время сеанса работы с ПАК "Соболь" не рекомендуется переподключение клавиатуры;
- после завершения сеанса работы с ПАК "Соболь" и до момента старта операционной системы клавиатура не реагирует на нажатия клавиш.

65. На некоторых конфигурациях не поддерживается работа с USB-идентификаторами, подключенными к портам USB 3.0 (такие порты отличаются пятью дополнительными контактами и как правило выделены синим цветом и/или имеют маркировку SS - SuperSpeed).

66. Не поддерживается работа с USB-идентификаторами на серверах HP ProLiant DL160/DL180.

67. Если при регистрации будут предъявлены USB-ключи Rutoken/Rutoken RF/iKey 2032, ранее не использовавшиеся в ПАК "Соболь" и имеющие PIN-коды, отличные от PIN-кодов по умолчанию, то на экране может появиться окно запроса на ввод PIN-кода идентификатора (PIN-коды по умолчанию для Rutoken/Rutoken RF — "12345678", для iKey 2032 — "default SO password."). Необходимо ввести PIN-код и нажать клавишу "Enter".

68. При работе с USB-идентификаторами eToken PRO не поддерживается использование PIN-кодов, содержащих символы кириллицы.

69. На некоторых конфигурациях USB-считыватели Athena ASEDrive IIIe USB V3, предназначенные для работы со смарткартами eToken PRO, функционируют нестабильно. В таких случаях рекомендуется использовать USB-считыватели Athena ASEDrive IIIe USB V2.

4.9. Особенности контроля целостности системного реестра

70. Не поддерживается возможность контроля целостности элементов реестра, полный путь которых превышает 512 символов.

71. Количество контролируемых записей реестра ОС Windows не должно превышать 10000.

72. Количество контролируемых файлов реестра не должно превышать 100.

73. Не рекомендуется проводить контроль целостности сессионных ключей и параметров системного реестра, которые пересоздаются или изменяются при каждой загрузке операционной системы, так как это приводит к ошибкам контроля целостности.

74. В СЗИ Secret Net в режиме совместной работы с ПАК "Соболь" не поддерживается возможность управления контролем целостности элементов системного реестра ОС MS Windows средствами ПАК "Соболь". Настройку контроля целостности элементов системного реестра ОС MS Windows средствами ПАК "Соболь" следует выполнять с помощью ПО ПАК "Соболь" до включения режима совместной работы.

4.10. Особенности контроля аппаратной конфигурации компьютера

75. Поддерживается возможность контроля лишь PCI-устройств, для которых в ОС MS Windows установлены драйверы.

76. На ряде компьютеров в конфигурационное пространство некоторых PCI-устройств регулярно вносятся изменения, так что их контроль в стандартном и расширенном режиме приведёт к ошибкам проверки целостности.

77. На ряде компьютеров в содержимое таблиц ACPI регулярно вносятся изменения, так что их контроль приведёт к ошибкам проверки целостности.

78. В случае изменения адреса PCI-устройства необходимо снять его с контроля и заново установить на контроль.

79. В СЗИ Secret Net в режиме совместной работы с ПАК "Соболь" не поддерживается возможность управления контролем аппаратной конфигурации компьютера средствами ПАК "Соболь". Настройку контроля аппаратной конфигурации компьютера средствами ПАК "Соболь" следует выполнять с помощью ПО ПАК "Соболь" до включения режима совместной работы.

ООО "КОД БЕЗОПАСНОСТИ"

Почтовый адрес:	115127, Москва, а/я 66
Телефон:	8 495 982-30-20
e-mail:	info@securitycode.ru
Web:	http://www.securitycode.ru