Программно-аппаратный комплекс "Соболь". Версия 3.0 (релиз 3.0.6)

Комментарии к версии 1.0.180 кода расширения BIOS платы, версиям программного обеспечения 2.0.88 для ОС семейства MS Windows и 3.0.41, 3.0.40 для ОС семейства Linux

Данный документ содержит описание новых возможностей продукта "Программно-аппаратный комплекс "Соболь". Версия 3.0" (далее — ПАК "Соболь") версии 1.0.180 кода расширения BIOS платы по сравнению с версией 1.0.153. 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. Версия 1.0.180 кода расширения BIOS

1. Реализована возможность работы ПАК "Соболь" с USB-идентификаторами на компьютерах, оснащенных только высокоскоростными USB-контроллерами.

2. Реализована поддержка файловой системы EXT4.

3. Реализована регистрация событий нарушения контроля целостности при входе администратора ПАК "Соболь".

3. Информация о совместимости

4. В эксплуатационную и техническую документацию добавлена информация о поддержке операционной системы Windows 8.

5. ПО ПАК "Соболь" для ОС MS Windows совместимо с СЗИ Secret Net 5.x (платы PCI/PCI-E)/6 (платы PCI/PCI-E)/7 (платы PCI/PCI-E/Mini PCI-E).

6. В режиме совместной работы ПАК "Соболь" и СЗИ Secret Net не могут использоваться идентификаторы iButton DS1992.

Рекомендация: В режиме совместной работы ПАК "Соболь" и СЗИ Secret Net рекомендуется использовать идентификаторы iButton DS1995, DS1996, смарт-карты и USB-ключи, поддерживаемые ПАК.

7. В СЗИ Secret Net 5.x, 6 в режиме совместной работы с СЗИ Secret Net отсутствует поддержка дисков с GUID Partition Table (GPT).

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

9. ПО ПАК "Соболь" для ОС MS Windows совместимо с СКЗИ "КриптоПро CSP" версий 2.0 (32-разрядный вариант) и 3.x (32- и 64-разрядный варианты).

4. Особенности работы и ограничения

4.1. Общие

10. Не поддерживается работа ПО ПАК "Соболь" под управлением ОС MS Windows 2000.

Рекомендация: Для работы под управлением ОС Windows 2000 рекомендуется использовать версию ПО 2.0.42.

11. Для работы под управлением ОС MS Windows Vista необходима установка SP1 или SP2.

12. 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.).

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

13. ПО всегда устанавливается только в каталог %Program Files%\Infosec\Sobol.

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

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

16. На компьютере, функционирующем под управлением ОС MS Windows XP x64, MS Windows Server 2003 x64, MS Windows Vista x32/x64 или 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.

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

4.3. Программа управления шаблонами КЦ для ОС MS Windows

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

19. Невозможен экспорт/импорт шаблонов КЦ между последними версиями программы управления (2.0.82 и 2.0.88) и более ранними версиями программы.

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

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

21. Во время загрузки дистрибутива Red Hat Enterprise Linux 4.1/МСВС 3.0 с сервисом kudzu на компьютере с установленной платой ПАК "Соболь" появляется информационное окно утилиты автоматического определения устройств. Для продолжения корректной работы выберите "Игнорировать".

22. В случае совместной работы ПО "Соболь" и "Континент-АП" при удалении одного из пакетов следует перезапустить сервис оставшегося в системе пакета (/etc/init.d/sobol или /etc/init.d/cts соответственно).

23. Для корректного удаления объединенного пакета sobol-3.0-b18.sh необходимо наличие файла /boot/sobol.

4.5. Программа управления шаблонами КЦ для ОС семейства Linux

24. Отсутствует поддержка дисков с GPT.

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

26. Не поддерживается контроль целостности следующих ресурсов:

- нерегулярные файлы (символьные ссылки, файлы устройств и т. д.);
- временные файлы;
- файлы, длина имени которых превышает 253 символа;
- файлы с длинными именами, расположенные на дисках с файловой системой FAT;
- 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.

27. Контроль целостности файлов в ОС VMware vSphere ESX 4.1/4.1 Update 1/4.1 Update 2 x64, установленных с разбиением диска по умолчанию (автоматически), осуществляется только для раздела /boot.

28. Для корректной работы программы управления шаблонами КЦ в ОС Astra Linux Special Edition "Смоленск" версии 1.1 необходимо установить библиотеки libparted и libglade.

29. 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.

30. Для объединенного пакета sobol-3.0-b18.sh невозможно удаление несуществующих ресурсов из шаблонов КЦ с использованием командной строки, за исключением вариантов очистки или восстановления шаблонов (ключи –-clear или –-reset).

31. Для объединенного пакета sobol-3.0-b18.sh при добавлении или удалении ресурсов по списку с использованием командной строки в списке не должны присутствовать ресурсы, содержащие в имени пробелы.

32. В ОС "Альт Линукс СПТ 6.0" не поддерживается корректное взаимодействие с платой ПАК "Соболь" и управление списками объектов КЦ при использовании механизма мандатного управления доступом (МАС) с многоуровневой моделью безопасности (MLS).

4.6. Код расширения BIOS

33. 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).

34. 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.

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

36. 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.

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

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

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

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

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

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

43. Не поддерживается возможность контроля целостности файлов, полный путь которых (в коротком виде) превышает 255 символов.

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

45. Если текущее время ожидания сторожевого таймера для плат PCI и PCI-E меньше времени от момента включения компьютера до момента передачи управления ПАК "Соболь", то при инициализации значение времени ожидания сторожевого таймера по умолчанию устанавливается равным 512. В этом случае желательно скорректировать значение времени ожидания сторожевого таймера или провести повторную инициализацию.

46. 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.

47. 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.

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

49. При обновлении кода расширения BIOS платы Mini PCI-E для файлов, размещающихся на дисках с файловой системой FAT16 и FAT32, длинные имена (более 8 символов) нужно указывать в коротком виде, например "pci-m~1.bin.

4.7. Плата ПАК "Соболь"

50. Не поддерживается корректное функционирование ПАК "Соболь" на некоторых моделях материнских плат, например:

- MS-7507, MS-7519, MS-7528, MS-7529, MS-7379, MS-9830, MS-9832;
- GIGABYTE GA-Q 35M-S2;
- GIGABYTE GA-P55-US3L;
- Intel DH55TC/DH55HC;
- Intel DQ57TM;
- Intel DG41MJ;
- Intel Xeon MP X7560;
- Intel Star Lake S5000PSL.

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.

51. На некоторых компьютерах возможна некорректная работа или зацикливание загрузки при использовании механизма сторожевого таймера, например:

- ASUS P5G41T-M LX;
- ASUS P5P43TD;
- ASUS P7P55;
- ASUS P8P67 PRO;
- ASUS P5Q Turbo;
- Gigabyte GA-D525TUD;
- Gigabyte GA-G41M-ES2L;
- Intel DQ45CB.

Использование ПАК "Соболь" при отключенном механизме сторожевого таймера допускается лишь в том случае, если работу ПАК невозможно отключить при помощи настроек BIOS Setup.

52. 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

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

54. 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.

55. 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).

56. В СЗИ Secret Net 5.x не поддерживается управление USB-идентификаторами у пользователей ПАК "Соболь" (данная возможность присутствует в СЗИ Secret Net 6 и 7).

57. В СЗИ Secret Net 6 версии ниже 6.5.333.53 не поддерживается управление смарт-картами eToken PRO для пользователей, которым разрешен вход в ПАК "Соболь".

58. В СЗИ Secret Net 6 не поддерживается управление USB-ключами eToken PRO (JAVA) для пользователей, которым разрешен вход в ПАК "Соболь".

59. 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".

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

61. 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

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

63. 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.

64. 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

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

66. 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.

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

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

69. 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:	127018, Москва, а/я 55
Телефон:	8 495 980-23-45
Факс:	8 495 980-23-45
e-mail:	info@securitycode.ru
Web:	http://www.securitycode.ru