Программно-аппаратный комплекс "Соболь". Версия 3.0 (релиз 3.0.M2)

Комментарии к версиям 8.14/11.11/11.12/12.1/12.6 ПЛИС плат, версии 1.0.227 BIOS, 1.0.230 BIOS, версии 2.0.113 ПО Windows, версии 3.0.m2-1/3.0.m2-2 ПО ОС семейства Linux

Данный документ содержит описание новых возможностей продукта "Программно-аппаратный комплекс "Соболь". Версия 3.0" (далее — ПАК "Соболь") версий 8.14/11.11/11.12/12.1/12.6 ПЛИС плат, версии 1.0.227, 1.0.230 кода расширения BIOS платы (по сравнению с версией 1.0.227), в версиях 2.0.113 программного обеспечения (ПО) для ОС семейства MS Windows (по сравнению с версией 2.0.109) и 3.0.m2-1/3.0.m2-2 ПО для ОС семейства Linux (по сравнению с версией 3.0.9-5). 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. Выпущена новая плата формфактора PCI-E M.2.

2. Выпущены новые адаптеры, универсальные для плат Mini PCI-E Half и PCI-E M.2.

3. Добавлена возможность подключения механизма сторожевого таймера посредством подключения к стандартному кабелю кнопки Power.

2.2. Версии ПЛИС 8.14, 11.11, 11.12, 12.1, 12.6

4. Версии ПЛИС 11.11 (плата Mini PCI-E), 11.12 (Mini PCI-E Half), 12.1 (PCI-E), 12.6 (PCI-E M.2) функционально не отличаются.

2.3. Версия 2.0.113 ПО для ОС MS Windows

5. Добавлена поддержка новой платы формфактора PCI-E M.2.

6. Добавлена поддержка ОС Windows 10.

7. Обновлен драйвер Sobol64.sys.

8. Обновлена библиотека SblApi.dll.

2.4. Версии ПО для ОС семейства Linux 3.0.m2-1, 3.0.m2-2

9. Добавлена поддержка новой платы формфактора PCI-E M.2.

10. Добавлена поддержка ОС Astra Linux 1.5, РОСА "Никель" x32.

2.5. Версия 1.0.230 кода расширения BIOS

11. Добавлена поддержка новой платы формфактора PCI-E M.2.

3. Информация о совместимости

12. ПО ПАК "Соболь" для ОС MS Windows совместимо с СЗИ Secret Net 6.x (платы PCI)/7 (платы PCI/PCI-E/Mini PCI-E/Mini PCI-E Half/Mini PCI-E M.2).

13. 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.

14. В СЗИ Secret Net 6, 7 в режиме совместной работы с ПАК "Соболь" отсутствует поддержка дисков с GUID Partition Table (GPT).

15. В СЗИ Secret Net 6, 7 в режиме совместной работы с ПАК "Соболь" отсутствует поддержка внешнего журнала ПАК "Соболь".

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

4. Особенности работы и ограничения

4.1. Общие

17. 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.).

18. Размер файла для сохранения кода расширения BIOS должен быть не менее емкости микросхемы флеш-памяти, используемой для хранения кода расширения BIOS. По умолчанию его размер составляет 1 МБ.

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

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

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

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

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

23. 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.

24. После обновления предыдущих версий ПО ПАК «Соболь» программа управления шаблонами устанавливается в каталог %Program Files%\Infosec\Sobol.

25. 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.

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

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

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

4.4. Программа управления шаблонами КЦ для ОС MS Windows

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

4.5. Программа управления шаблонами КЦ для ОС семейства Linux

29. Отсутствует поддержка дисков с GPT.

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

31. 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 и пути к которым превышает 249 символов (в ОС FreeBSD для файловых систем UFS, UFS2);
    - 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.

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

33. Не поддерживается обработка флагов ядра Linux файловой системы ext4:
    - EXT4_FEATURE_INCOMPAT_LARGEDIR
    - EXT4_FEATURE_INCOMPAT_INLINE_DATA

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

35. Не поддерживается контроль целостности объектов файловых систем EXT2, EXT3, EXT4 с именами, содержащими символы кириллицы в кодировке KOI8-R (данная кодировка используется по умолчанию в ОС МСВС).

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

37. 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;
    - отказ от использования мультизагрузчиков с возможностью загрузки нескольких ОС.

38. 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.

39. В ОС VMware vSphere ESXi 5.5 не поддерживается контроль целостности файлов с длинными именами (имена в формате, отличном от "8.3"), расположенных на дисках с файловой системой FAT16 или FAT32.

40. В ОС VMware vSphere ESXi 5.5 не поддерживается контроль целостности файлов с именами, содержащими символы кириллицы.

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

4.6. Код расширения BIOS

42. 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.

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

44. 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).

45. 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.

46. При наличии поддержки технологии UEFI для корректной работы ПАК "Соболь" операционная система должна быть установлена на диск с Master Boot Record (MBR) в режиме Legacy-mode.

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

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

49. При задании пути к файлам шаблонов КЦ, расположенных на дисках с файловой системой FAT, не поддерживается возможность задания путей в длинном виде.

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

51. При выполнении расчета эталонов и контроля целостности файлов с длинными именами, расположенных на дисках с файловой системой FAT32, отображаются короткие имена файлов.

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

53. Не поддерживается возможность контроля целостности секторов, расположенных на диске за пределами 2 ТБ (поддерживается адресация LBA 32).

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

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

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

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

58. Не поддерживается контроль целостности журнала транзакций для файловых систем UFS, UFS2.

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

60. 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).

61. 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.

62. 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.

63. Если текущее время ожидания сторожевого таймера для платы PCI 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.

64. 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.

65. 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.

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

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

68. При входе в систему с использованием идентификатора, присвоенного пользователю средствами СЗИ Secret Net 7 в режиме совместной работы, в ПАК "Соболь" может регистрироваться событие "Ошибка КС в памяти идентификатора". Ошибка регистрируется в случае, если в идентификатор не записаны пароль пользователя и закрытый ключ, и не влияет на функционирование ПАК "Соболь" и СЗИ. Регистрация события прекращается после записи в идентификатор пароля или закрытого ключа пользователя.

69. При вводе стойкого пароля необходимо соблюдать следующие правила:

- пароль должен содержать хотя бы одну цифру;
- пароль должен содержать хотя бы одну букву верхнего регистра (заглавная буква);
- пароль должен содержать хотя бы одну букву нижнего регистра (строчная буква);
- пароль должен содержать хотя бы один специальный символ;
- пароль не должен содержать двух или более рядом стоящих одинаковых символов;
- пароль не должен содержать двух или более рядом стоящих цифр, образующих
- возрастающую последовательность вида 123... или убывающую 987...;
- при смене пароля новый пароль не должен совпадать с текущим.

70. При переводе системного времени/даты назад необходимо учитывать появление возможности его отставания от времени/даты установки пароля пользователя. В этом случае вход пользователя в систему будет заблокирован.

71. Минимальный размер внешнего журнала ПАК "Соболь" составляет 20 записей, максимальный — 1968.

72. Запрещается устанавливать системную дату ранее 01.01.2014 года.

4.7. Плата ПАК "Соболь"

73. 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 выполнение старта ПАК "Соболь" в режиме загрузочного устройства (Initial Program Load или IPL) при условии обязательного использования механизма сторожевого таймера.

74. На некоторых компьютерах возможна некорректная работа или зацикливание загрузки при использовании механизма сторожевого таймера.

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

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

76. 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.

77. При отсутствии возможности использовать разъём Reset для функционирования механизма сторожевого таймера рекомендуется использовать вариант параллельного подключения к стандартному кабелю кнопки Power по схеме, описанной в документации.

4.8. Особенности работы с USB-идентификаторами

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

79. 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 букв 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.

80. 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).

81. 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".

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

83. 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".

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

85. 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

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

87. Число контролируемых записей реестра ОС Windows не должно превышать 10000.

88. Число контролируемых файлов реестра не должно превышать 100.

89. 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.

4.10. Особенности контроля аппаратной конфигурации компьютера

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

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

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

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

94. 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