Программно-аппаратный комплекс "Соболь". Версия 4 (релиз 4.2)

Комментарии к версиям 13.1/13.2/13.3 ПЛИС плат, версии 4.2.334 UEFI/BIOS, версии 4.2.28 ПО Windows, версии 4.1-7 ПО ОС семейства Linux

Данный документ содержит описание особенностей и ограничений продукта "Программно-аппаратный комплекс "Соболь". Версия 4" (далее — ПАК "Соболь") версий 13.1/13.2/13.3 ПЛИС плат, версии 4.2.334 кода расширения UEFI/BIOS платы, версии 4.2.28 программного обеспечения (ПО) для ОС семейства MS Windows и версии 4.1-7 ПО для ОС семейства Linux.

Оглавление

1. Комплект поставки ПО и документации

1.1. Размещение файлов на компакт-диске

Каталог	Содержимое
\Documentation\	Комплект документации в формате PDF
\Firmware\	Файлы с кодом расширения UEFI BIOS и с кодом ПЛИС.
\Setup\Windows\	Дистрибутив вспомогательного ПО ПАК "Соболь" для ОС MS Windows
\Setup\Linux\	Дистрибутивы вспомогательного 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. Особенности работы и ограничения

2.1. Общие

1. 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.

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

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

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

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

5. 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.

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

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

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

2.4. Режим совместного использования

8. Для работы ПО Secret Net Studio или Secret Net LSP в режиме совместного использования с ПАК "Соболь", надо установить в ОС ПО Соболь (для Windows и Linux соответственно).

2.5. Контроль целостности

9. Длина полного пути любого контролируемого файла для файловых систем FAT16 и FAT32 не должна превышать 256 символов.

10. Для ОС Windows длина полного пути любого контролируемого файла для файловой системы NTFS не должна превышать 259 символов.

11. Длина имени файла или директории для файловой системы NTFS не должна превышать 255 символов.

12. Длина пути любого контролируемого файла в ОС Linux (для файловых систем EXT2, EXT3, EXT4) не должна превышать 255 символов.

13. Количество контролируемых файлов не должно превышать 10000.

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

15. 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).

16. Обеспечивается контроль целостности объектов файловых систем EXT2, EXT3, EXT4 с именами, содержащими символы кириллицы, только в кодировке UTF8.

17. Не поддерживается КЦ файлов, преобразованных криптографическими программами (BestCrypt или аналогичными), программами сжатия дисков, за исключением сжатых файлов NTFS, и т. п.

18. Не поддерживается КЦ для логических дисков, расположенных на динамических дисках и/или являющихся наборами томов (например, LVM, StripeSet, Volume set, Software RAID).

19. Не поддерживается КЦ альтернативных потоков (streams) данных для файлов и директорий, расположенных на разделах (томах) с файловой системой NTFS.

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

21. Не поддерживается КЦ Списков Контроля Доступа(ACL) к файловым объектам для файловых систем их поддерживающих. (ограничение драйвера ext, можно снять доработкой, ограничение приложения для создания шаблонов).

22. На компьютерах с ОС Windows не рекомендуется ставить на контроль целостности файлы BCD, BCD.LOG, Bootstat.dat, расположенные в папке \EFI\Microsoft\Boot на системном EFI-разделе. Эти файлы изменяются при каждой загрузке ОС.

2.6. 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.

24. Не допускается преобразовывать каталог (по умолчанию C:\Sobol), содержащий служебные файлы механизма контроля целостности, программами сжатия дисков, включая сжатие файлов NTFS и т. п.

25. Не допускается размещать каталог (по умолчанию C:\Sobol), содержащий служебные файлы механизма контроля целостности на динамическом диске.

26. Не допускается преобразовывать диски, на которых располагается каталог (по умолчанию C:\Sobol), содержащий служебные файлы механизма контроля целостности, криптографическими программами (BestCrypt или аналогичными).

2.7. Программа управления шаблонами КЦ для ОС семейства Linux

27. Не поддерживается контроль целостности следующих ресурсов:

- нерегулярные файлы (символьные ссылки, файлы устройств и т. д.);
- временные файлы;
- файлы, расположенные на дисках с неподдерживаемыми файловыми системами (JFS, ReiserFS и т. д.);
- файлы, расположенные на дисках с виртуальными файловыми системами.

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

29. Для файловой системы ext4 не поддерживается обработка флага EXT4_FEATURE_INCOMPAT_LARGEDIR ядра Linux.

30. На некоторых материнских платах для ОС VMware vSphere ESXi 5.5 не поддерживается контроль целостности файлов на разделах с файловой системой FAT32 (ошибка в UEFI BIOS материнских плат).

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

2.8. Код расширения BIOS

32. Если каталог с файлами шаблонов КЦ не найден или в этом каталоге отсутствуют файлы шаблонов, то в разделе настроек контроля целостности отключается контроль соответствующих типов объектов. Для включения контроля целостности файлов, секторов, элементов реестра и конфигурации компьютера укажите точный путь к каталогу с файлами шаблонов КЦ.

33. 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.

34. 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.

35. 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.

36. 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.

37. Запрещается устанавливать системную дату ранее 01.01.2010 года.

38. Пароли длиной более 16 символов несовместимы между версиями 4.0.1 и более поздними. Для решения проблемы надо сменить пароль на более короткий.

39. На некоторых материнских платах некорректно работает клавиша Shift: после отпускания клавиши следующая буква все равно получается заглавной.

2.9. Плата ПАК "Соболь"

40. Не поддерживается корректное функционирование ПАК "Соболь" на некоторых моделях материнских плат (см. таблицу совместимости на сайте компании по ссылке, строки с указанием версий BIOS 4.0, 4.1, 4.2).

41. На некоторых моделях материнских плат Соболь версии 4 не функционирует в режиме Legacy.

42. 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/UEFI Setup.

43. Для корректной работы ПАК "Соболь" с некоторыми моделями материнских плат требуется обновление их BIOS.

44. 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.

2.10. Особенности работы с USB-идентификаторами

45. USB-ключи семейства JaCarta перед первым использованием совместно с ПАК «Соболь» надо инициализировать в «Едином Клиенте JaCarta» (https://www.aladdin-rd.ru/support/downloads/jacarta). Если этого не сделать, то ПАК «Соболь» не позволит войти зарегистрированному пользователю (сообщение о неверном идентификаторе или пароле). Если USB-

ключ до работы с ПАК «Соболь» уже использовался совместно с Secret Net Security Studio, инициализация не требуется.

46. Если при регистрации будут предъявлены USB-ключи Rutoken, 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 — "12345678"). Необходимо ввести PIN-код и нажать клавишу "Enter".

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

48. Идентификаторы JaCarta несовместимы между версиями «Соболя» 4.0.1 и более поздними.

49. Идентификаторы eToken в исполнении smartcard несовместимы между версиями «Соболя» 4.0.1 и более поздними.

50. Идентификатор Guardant ID, отформатированный в ПАК «Соболь», несовместим с Secret Net Studio и наоборот.

2.11. Особенности контроля целостности системного реестра

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

52. 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.

2.12. Особенности контроля аппаратной конфигурации компьютера

53. Поддерживается возможность контроля только тех PCI-устройств, для которых в ОС MS Windows установлены драйверы.

54. 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.

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

56. На некоторых материнских платах при включенном контроле SMBIOS после изменения аппаратной конфигурации (например, при перестановке модуля памяти в другой слот) при осуществлении контроля может быть выдана ошибка, не соответствующая ситуации (пример: «Объект не найден» при проверке процессора). Это вызвано особенностями BIOS материнской платы.

ООО "КОД БЕЗОПАСНОСТИ"

Почтовый адрес:	105318, Москва, а/я 101
Телефон:	8 495 982-30-20
e-mail:	info@securitycode.ru
Web:	http://www.securitycode.ru