ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ МОДУЛЯ ЗАЩИТЫ

Руководство администратора

643.18184162.00090-01 90

Листов 14

АННОТАЦИЯ

В настоящем руководстве содержится информация о назначении программного обеспечения модуля защиты (далее по тексту - программное изделие), его функциях, условиях применения, порядке работы и настройке.

Руководство администратора программного изделия предназначено для системных администраторов, сервисных инженеров и специалистов по информационной безопасности.

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Обозначение и наименование программного изделия

Наименование – Программное обеспечение модуля защиты.

Обозначение программного изделия – 643.18184162.00090-01.

1.2. Назначение программного изделия

Программное изделие предназначено для:

– контроля целостности (КЦ) программной среды;

– КЦ аппаратной среды;

– регистрации в журнале:

1) событий изменения программной конфигурации;

2) событий изменения аппаратной конфигурации.

1.3. Условия применения

1.3.1. Программное обеспечение, необходимое для функционирования программного изделия.

Для функционирования программного изделия требуется:

1) наличие программного кода, обеспечивающего вызов программного изделия до этапа поиска загрузчика операционной системы (ОС) компьютера;

2) наличие программного кода, обеспечивающего пользовательский интерфейс и интерфейс взаимодействия с программным изделием.

1.3.2. Языки программирования, на которых написано программное изделие

При разработке программного изделия использовались следующие языки программирования: Ассемблер, Си.

1.3.3. Требования к программному обеспечению

Для работы программного изделия дополнительное программное обеспечение (ПО) не требуется.

2. ОПИСАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

2.1. Структура программного изделия

Программное изделие поставляется в предустановленном виде и состоит из следующего ПО:

– ПО интеграции;

– модули безопасности.

2.1.1. ПО интеграции

ПО интеграции обеспечивает пользовательский интерфейс для настройки и управления программным изделием.

2.1.2. Состав модулей безопасности

Программное изделие позволяет управлять следующими модулями безопасности:

– *Контроль целостности оборудования;*

– *Контроль целостности файловой системы;*

– *Журнал событий.*

3. РАБОТА ПРОГРАММНОГО ИЗДЕЛИЯ

При описании последовательности действий приводятся:

1) названия клавиш клавиатуры – в квадратных скобках [];

2) названия режимов работы и модулей безопасности, названия экранных страниц, разделов, пунктов (параметров) оболочки, пунктов меню диалоговых окон, а также ролей пользователей – курсивом (пример: страница *Настройки*);

3) значения параметров – в кавычках («»);

4) тексты экранных сообщений – моноширинным шрифтом или в виде соответствующих рисунков.

Выбор пунктов (параметров) оболочки, действий и записей на экранных страницах и диалоговых окнах осуществляется клавишами [↑] и [↓] клавиатуры.

3.1. Режимы функционирования

При первом запуске компьютера отображается информация, приведенная на рис.1

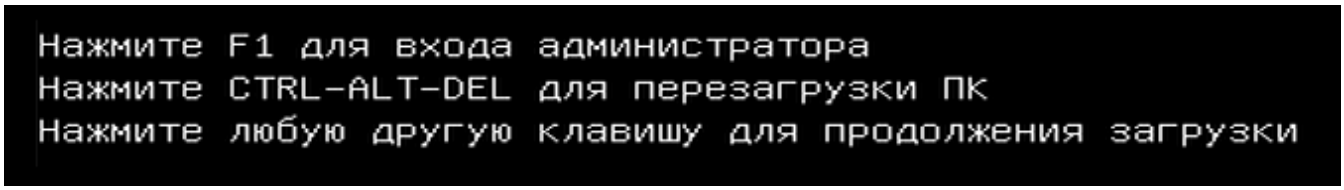

Рис.1

Нажмите клавишу [F1] для отображения меню выбора действия. Выберите п. *Создать пароль администратора* и нажмите клавишу [Enter]. Отображаются окна для ввода и повторного ввода пароля. Введите пароль и нажмите клавишу [Enter]. Длина пароля должна быть не менее 3 символов.

После задания пароля *Администратора* и перезагрузки компьютера нажатие клавиши [F1] приводит к отображению окна с предложением ввести ранее созданный пароль *Администратора* для аутентификации. Созданный пароль *Администратора* позволяет получить доступ в оболочку программного изделия.

Программное изделие начинает функционировать в следующих двух режимах:

1) *режим Администратора*, вход в который осуществляется по паролю при помощи клавиши [F1];

2) *режим пользователя*, предусматривающий только принудительную загрузку установленной на компьютере ОС.

3.2. Вход в ПО

Программное изделие проводит проверку целостности программных модулей, и, в случае успеха, отображается стартовая страница (главное меню) оболочки.

3.3. Работа с программным изделием

3.3.1. Модуль *Контроль целостности оборудования*

Модуль предназначен для проверки целостности аппаратного обеспечения компьютера путем сравнения контрольных сумм (КС) и сигнализации при обнаружении изменений. При нарушении целостности осуществлять управление программным изделием сможет только пользователь с правами *Администратора*.

Для включения модуля следует:

1) выбрать п. *Контроль целостности оборудования*, в главном меню оболочки;

2) нажать клавишу [Enter], отображается страница отображается страница *Контроль целостности оборудования*;

3) нажать клавишу [Enter], отображается диалоговое окно, запрашивающее подтверждение на включение модуля;

4) нажать клавишу [Enter], выполняется включение модуля *Контроль целостности оборудования;*

5) нажать клавишу [Esc], отображается главное меню оболочки, статус модуля изменяется с «Выкл» на «Вкл».

П р и м е ч а н и е. При нарушении целостности аппаратной среды выдается сообщение о нарушении КЦ аппаратной среды и на странице КЦ оборудования появляется пункт «Ошибка устройства» с описанием измененной конфигурации.

Для выключения модуля следует:

1) выбрать п. *Контроль целостности оборудования*, в главном меню оболочки;

2) нажать клавишу [Enter], отображается страница отображается страница *Контроль целостности оборудования*;

3) нажать клавишу [Enter], отображается диалоговое окно, запрашивающее подтверждение на выключение модуля;

4) нажать клавишу [Enter], выполняется выключение модуля *Контроль целостности оборудования;*

5) нажать клавишу [Esc], отображается главное меню оболочки, статус модуля изменяется с «Вкл» на «Выкл».

Сброс списка оборудования, подлежащего КЦ применяется для обновления данных при контроле целостности оборудования.

Для сброса списка оборудования, подлежащего КЦ, следует:

1) выбрать п. *Контроль целостности оборудования* в главном меню оболочки;

2) нажать клавишу [Enter], отобразится страница *Контроль целостности оборудования*;

3) выбрать п. *Сбросить список оборудования*;

4) нажать клавишу [Enter], отобразится окно, запрашивающее подтверждение на сброс списка оборудования;

5) нажать клавишу [Enter], происходит сброс ранее созданного списка оборудования, подлежащих КЦ, появится сообщение «Список оборудования обновлен Нажмите любую клавишу для продолжения»;

6) нажать клавишу [Esc], для возврата в главное меню оболочки.

Примечания:

1. Вывод результата последнего выполнения процедуры КЦ оборудования возможен только после включения модуля *Контроль целостности оборудования* и первой перезагрузки компьютера для создания контрольного списка оборудования.

2. При возникновении *Ошибки устройства* и последующем устранении ошибки, путем замены старого устройства на новое, необходимо выбрать п. *Сбросить список оборудования*, для создания нового списка, при следующей перезагрузке для КЦ новой конфигурации оборудования.

3. Сбросить список оборудования, подлежащих КЦ, возможно только после включения модуля *Контроль целостности оборудования*.

4. Информация от модуля *Контроль целостности оборудования* сохраняется в журнале событий.

3.3.2. Модуль *Контроль целостности файловой системы*

Для включения модуля следует:

1) выбрать п. *Контроль целостности файловой системы*, в главном меню оболочки;

2) нажать клавишу [Enter], отображается страница отображается страница *Контроль целостности файловой системы*;

3) нажать клавишу [Enter], отображается диалоговое окно, запрашивающее подтверждение на включение модуля;

4) нажать клавишу [Enter], выполняется включение модуля *Контроль целостности файловой системы* с возможностью выбора хеш-функции*;*

5) выбрать п. *Выберите хеш-функцию;*

6) нажать клавишу [Enter] для выбора хеш-функции из списка;

7) выбрать требуемую хэш-функцию клавишами [↑], [↓] для процедуры КЦ данных;

8) нажать клавишу [Enter];

9) если хеш-функция изменилась, то будет диалоговое окно для подтверждения изменений;

10) нажать клавишу [Esc], отображается главное меню оболочки, статус модуля изменяется с «Выкл» на «Вкл».

Примечание. Выбор хеш-функции осуществляется исходя из политики безопасности в организации.

Для выключения модуля следует:

1) выбрать п. *Контроль целостности файловой системы*, в главном меню оболочки;

2) нажать клавишу [Enter], отображается страница отображается страница *Контроль целостности файловой системы*;

3) нажать клавишу [Enter], отображается диалоговое окно, запрашивающее подтверждение на выключение модуля и удаления всех списков КЦ;

4) нажать клавишу [Enter], выполняется выключение модуля *Контроль целостности файловой системы* и удаление всех списков КЦ*;*

5) нажать клавишу [Esc], отображается главное меню оболочки, статус модуля изменяется с «Вкл» на «Выкл».

Для создания списка файлов, подлежащих КЦ, следует:

1) выбрать п. *Контроль целостности файловой системы* в главном меню оболочки;

2) нажать клавишу [Enter], отобразится страница *Контроль целостности файловой системы*;

3) выбрать п. *Добавить новый список файлов* раздела *Выбор задачи*;

4) нажать клавишу [Enter], отображается страница *Создание списка файлов*;

5) выбрать п. *Название списка файлов*;

6) нажать клавишу [Enter], отображается окно для ввода названия списка файлов;

7) ввести название списка файлов и нажать клавишу [Enter];

8) выбрать п. С*писок файлов*;

9) нажать клавишу [Enter], отображается окно файлового менеджера, в котором предлагается выбрать объекты (файлы, папки), подлежащие КЦ;

10) выбрать требуемые локальные диски клавишами [↑], [↓];

11) при необходимости выполнять КЦ целых дисков, выделить диски, подлежащие КЦ, клавишей [Пробел];

12) при необходимости выбрать другие объекты (файлы, папки), подлежащие КЦ, расположенные на определенном локальном диске, нажать клавишу [Enter] на данном диске для входа в файловую систему диска;

13) выделить объекты (файлы, папки), подлежащие КЦ, клавишей [Пробел] для возврата на уровень выше (выход из папки, выход из диска) следует использовать клавишу [Esc];

14) удалить объект или объекты, которые не подлежат КЦ, из панели *Список файлов* при необходимости;

15) нажать клавишу [F2] для сохранения сделанных изменений и выхода из файлового менеджера;

16) отображается окно, информирующее об успешном обновлении (создании) КС файлов;

17) нажать клавишу [Enter];

18) выбрать п. *Сохранить список файлов*;

19) нажать клавишу [Enter], отображается окно, информирующее о выполнении сохранения списка файлов;

20) нажать клавишу [Enter], отображается окно *Контроль целостности файловой системы*, с именем созданного списка в разделе *Контрольные списки файлов*. Справа вверху высветится информация о списке – даты и времена создания, изменения и последней проверки, а также общее число элементов.

Примечания:

1. Создание списка файлов, подлежащих КЦ, возможно только после включения модуля *Контроль целостности файловой системы*.

2. Выбор требуемых объектов выполняется клавишами [↑], [↓].

3. Выделение объектов выполняется следующим образом:
   - выбрать объект, который подлежит КЦ;
   - нажать клавишу [Пробел].

4. Чтобы выйти из окна файлового менеджера без сохранения сделанных изменений следует воспользоваться клавишей [Esc].

3.3.3. Модуль *Журнал событий*

Для включения модуля следует:

1) выбрать п. *Журнал событий*, в главном меню оболочки;

2) нажать клавишу [Enter], отображается страница *Журнал событий*;

3) нажать клавишу [Enter], отображается диалоговое окно, запрашивающее подтверждение на включение модуля;

4) нажать клавишу [Enter], выполняется включение модуля *Журнал событий;*

5) нажать клавишу [Esc], отображается главное меню оболочки, статус модуля изменяется с «Выкл» на «Вкл».

Для выключения модуля следует:

1) выбрать п. *Журнал событий*, в главном меню оболочки;

2) нажать клавишу [Enter], отображается страница отображается страница *Журнал событий*;

3) нажать клавишу [Enter], отображается диалоговое окно, запрашивающее подтверждение на выключение модуля;

4) нажать клавишу [Enter], выполняется выключение модуля *Журнал событий;*

5) нажать клавишу [Esc], отображается главное меню оболочки, статус модуля изменяется с «Вкл» на «Выкл».

Для просмотра журнала событий следует:

1) выбрать п. *Журнал событий* в главном меню оболочки;

2) нажать [Enter], отображается страница *Журнал событий*;

3) выбрать строку *Поиск в журнале*;

4) нажать клавишу [Enter], откроется окно для ввода данных;

5) ввести строку символов для поиска в журнале событий;

6) нажать клавишу [Enter] для подтверждения и начала поиска;

7) отображается результат поиска по заданной строке.

Примечания:

1. Формат записи событий в журнал:

`Дата_событий Время_событий Субъект,_вызвавший_событие Описание_события`

2. Перемещение по строкам записей журнала выполняется клавишами [↑] и [↓].

3. Перемещение курсора на первую и последнюю строки записей журнала событий выполняется клавишами [Page Up], [Page Down].

4. Постраничный вывод записей журнала событий выполняется клавишей [Enter], при перемещении курсора на строку <Следующая страница> или <Предыдущая страница>.

5. В журнале применяется цветовая индикация событий. Цвет записи события в журнале зависит от типов событий. Каждое событие журнала может быть одного цвета и принадлежать к одному из следующих типов:

– **зеленый** – сведения. Событие, которое обозначает успешное выполнение какой-либо задачи (например, событие с типом «Сведения» будет записано при успешном создании профиля пользователя);

– **желтый** – предупреждение. Событие может не быть важным, но может указывать на возможность возникновения отрицательных последствий в дальнейшем (например, предупреждение будет записано в журнал, когда будет отключен модуль КЦ оборудования);

– **красный** – ошибка. Событие обозначает нарушение КЦ системы (например, когда нарушена целостность оборудования системы).

3.3.4. Модуль *Журнал событий МЗСПО*

Журнал событий МЗСПО хранится в самом замке и предназначен для логирования четырёх событий: включение платы, нарушение целостности оборудования, нарушение целостности подключаемых устройств и нарушение целостности файловой системы.

3.3.5. Поддержка переключения между двумя BIOS (Dual BIOS)

Реализовано три способа переключения порядка SPI с BIOS:

1) автоматический: при старте ПК запускается таймер. За время, пока таймер не закончился от BIOS должна прийти команда успешной загрузки. Если она не пришла, то считаем, что BIOS не запустился. В таком случае выключаем ПК и переключаем порядок SPI. Значение таймера устанавливается в меню МЗСПО;

2) ручное управление: в меню МЗСПО имеем возможность настроить порядок SPI;

3) переключение по кнопке Reset: если кнопка Reset нажата более 5 с, то при следующем старте меняется порядок SPI.

3.3.6. Контроль целостности BIOS при старте

В меню МЗСПО имеется возможность активировать контроль целостности БИОС при старте, контролируется только первый БИОС. При активации подсчитывается КС таблицы регионов БИОС и значение КС сохраняется в МЗСПО. При старте МЗСПО подсчитывает КС таблицы регионов БИОС и сравнивает её с уже сохранённой. Если целостность нарушена, то выдаётся ошибка, и доступ пользователю ограничивается и при следующем старте меняется порядок SPI. В меню МЗСПО также имеется возможность сбросить значение сохранённой КС. В этом случае КС будет пересчитана при следующем старте и её новое значение будет записано в МЗСПО.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

Сокращение	Наименование/Определение
КЦ	Контроль целостности
ОС	Операционная система
КС	Контрольная сумма
ПО	Программное обеспечение

Лист регистрации изменений									
Изм.	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подп.	Дата
	изменен-ных	заменен-ных	новых	аннули-рован-ных					